

E D I C E

OPERAČNÍ SYSTÉMY



Windows[®] 2000 Server

Sítě TCP/IP



VŠECHNY CESTY
K INFORMACÍM

Microsoft[®]

Microsoft® Windows 2000 Server **Sítě TCP/IP**

**Computer Press
Praha
2000**

Microsoft® Windows 2000 Server Sítě TCP/IP

Copyright © Computer Press® 2000. Vydání první. Všechna práva vyhrazena.
Vydavatelství a nakladatelství Computer Press®,
Homocholupická 22, 143 00 Praha 4, <http://www.cpress.cz>

ISBN 80-7226-291-2

Prodejní kód: K0385

Překlad: Pavla Kocanová, Marek Kocan

Odborná korektura: Bohdan Cafourek,
Ludvík Roubíček

Jazyková korektura: Tomáš Rittich, Barbora Antonová

Vnitřní úprava: Petr Klíma, Jiří Matoušek

Sazba: Tomáš Doležal

Rejstřík: Pavlína Bauerová

Obálka: Jaroslav Novák

Komentář na zadní straně obálky: Ivo Magera

Odpovědný redaktor: Ivo Magera

Vedoucí technické redakce: Martin Hanslian

Produkce: Petr Baláš

Tisk: PBTISK

Copyright © 2000 by Microsoft Corporation.

Original English language edition Copyright © 2000 by Microsoft Corporation.

Translation: © Computer Press, 2000.

Autorizovaný překlad z originálního anglického vydání Microsoft® Windows® 2000 Server Resource Kit.

Originální copyright: © Microsoft Corporation Inc./Microsoft Corporation, 2000.

Překlad: © Computer Press, 2000.

Žádná část této publikace nesmí být publikována a šířena žádným způsobem a v žádné podobě bez výslovného svolení vydavatele.

Veškeré dotazy týkající se distribuce směřujte na:

Computer Press Brno, náměstí 28. dubna 48, 635 00 Brno-Bystrc,
tel. (05) 46 12 21 11, e-mail: distribuce@cpress.cz

Computer Press Bratislava, Hattalova 12, 831 03 Bratislava, Slovenská republika,
tel.: +421 (7) 44 45 20 48, 44 25 17 20, e-mail: distribucia@cpress.sk

Nejnovější informace o našich publikacích naleznete na adrese:

<http://www.cpress.cz/knihy/bulletin.html>.

Máte-li zájem o pravidelné zasílání bulletinu do Vaší e-mailové schránky, zašlete nám jakoukoli, i prázdnou zprávu na adresu bulletin@cpress.cz.



<http://www.vltava.cz>

Nejširší nabídka literatury, hudby, MP3,
multimediálního softwaru a videa za
bezkonkurenční ceny.



Vaše dotazy, vzkazy, náměty, připomínky ke knižní produkci
Computer Press přijímá 24 hodin denně naše horká linka:
knihy@cpress.cz

Obsah

Úvod	1
Použité konvence	1
Kompaktní disk sady Resource Kit	2
Politika podpory pro Resource Kit	2

ČÁST I

TCP/IP ve Windows 2000	5
-------------------------------	----------

1. KAPITOLA

Úvod do TCP/IP	7
Sada protokolů TCP/IP	8
Microsoft TCP/IP	8
Standardy TCP/IP	8
Architektura TCP/IP	9
Základní protokoly TCP/IP	11
Protokol IP	12
Protokol ARP	13
Protokol ICMP	13
Protokol IGMP	14
Protokol TCP	15
Protokol UDP	16
Rozhraní aplikací TCP/IP	17
Rozhraní Windows Sockets	18
Rozhraní NetBIOS	18
IP adresování	19
Třídy adres	20
Pravidla pro ID sítě	22
Pravidla pro ID hostitele	22
Podsítě a masky podsítí	23
Masky podsítě	24

Rozdělování sítě	26
Krok první: Určení počtu bitů hostitele	26
Krok druhý: Výpočet ID podsítí	29
Krok třetí: Výpočet adres IP pro každé ID podsítě	31
Vytváření podsítí s různou délkou	33
Vyvádění nadsítí a CIDR (Classless Interdomain Routing)	35
Dva různé pohledy na adresový obor	36
Veřejné a soukromé adresy	37
Veřejné adresy	37
Soukromé adresy	37
Překlad adres	39
Překlad názvů hostitele	39
Doménové názvy	39
Překlad adres za využití souboru Hosts	41
Překlad adres za využití DNS serveru	41
Kombinace lokální databáze a DNS	42
Přiřazování názvu NetBIOSu	43
Typy uzlů NetBIOSu	44
Směrování IP	44
Přímé a nepřímé doručení	45
Směrovací tabulka IP	46
Typy záznamů ve směrovací tabulce IP	46
Proces určení cesty	46
Příklad směrovací tabulky ve Windows 2000	47
Směrovací proces	48
IP na odesílajícím hostiteli	48
IP na směrovači	48
Statické a dynamické směrovače IP	49
Přiřazení fyzické adresy	50
Vyrovňovací paměť ARP	50
Proces ARP	51
Další informace	52

2. KAPITOLA

Windows 2000 TCP/IP	53
Přehled TCP/IP pro Windows 2000	54
Standardní vlastnosti a zlepšení výkonu	54

Dostupné služby	54
RFC týkající se Internetu podporovaná TCP/IP pro Microsoft Windows 2000	55
Architektura Microsoft TCP/IP pro Windows 2000	57
Rozhraní NDIS a další	58
NDIS a TCP/IP	58
Funkcionalita vrstvy připojení	60
Největší přenosová jednotka (MTU)	60
Komponenty základních protokolů	61
Protokol ARP (Address Resolution Protocol)	61
Používání nástroje ARP.	61
Stárnutí mezipaměti ARP.	62
Aktualizace záznamů v mezipaměti ARP.	62
Zprávy ARP a UDP	63
Protokol sítě Internet (Protokol IP)	63
Směrování.	63
Používání nástroje Route	65
Detekce duplikovaných adres IP	67
Vícedomost (Multihoming)	68
CIDR (Beztrídové mezidomenové směrování)	69
Víceměrové vysílání protokolu IP.	69
Protokol IP nad sítí ATM	69
Protokol ICMP (Internet Control Message Protocol)	69
Údržba směrovacích tabulek	70
Zjištění jednotky PMTU	70
Použití protokolu ICMP při diagnostice problémů	72
Řízení proudu za použití protokolu ICMP.	73
Zjišťování směrovače pomocí protokolu ICMP.	73
Služba QoS (Quality of Service) a protokol RSVP (Resource reservation Protocol)	73
Zabezpečení protokolu IP	74
Protokol IGMP (Internet Group Management Protocol)	75
Rozšíření víceměrového vysílání knihovny Windows Sockets	76
Použití víceměrového vysílání IP komponentami operačního systému Windows 2000.	77
Protokol TCP (Transmission Control Protocol)	77
Velikost přijímaného okna protokolu TCP a změna velikosti okna	77
Opožděná potvrzení.	79
Selektivní potvrzení protokolu TCP	79

Časová razítka protokolu TCP	80
Rozpoznání mrtvé brány.	82
Chování protokolu TCP při opakovaném přenosu.	83
Zprávy Keep-Alive protokolu TCP	84
Algoritmus pomalého spuštění a vyhnutí se zahlcení.	84
Syndrom SWS (Silly Window Syndrome)	85
Algoritmus Nagle	85
Zpoždění TIME-WAIT protokolu TCP.	86
Připojení protokolu TCP na vícedomé a z vícedomých počítačů	87
Činitelé propustnosti	88
Protokol UDP (User Datagram Protocol)	88
Protokol UDP a překlad názvu	89
Zásuvka pošty přes protokol UDP	89
Rozhraní síťových aplikací	89
Windows Sockets.	89
Aplikace	89
Překlad názvů a adres	
Podpora vícesměrového vysílání protokolu IP.	90
Parametr rezerva	90
Interpretace bitu řídicího neukládání ve vyrovnávací paměti (push bit)	90
NetBIOS pro TCP/IP	91
Názvy typu NetBIOS	92
Registrace a zjištění názvu typu NetBIOS	93
Registrace a zjištění názvu typu NetBIOS u vícedomých počítačů	95
Rozšíření rozhraní NetBIOS pro TCP/IP (NetBT) pro Internet/DNS v operačním systému Windows 2000	96
Relace rozhraní NetBIOS pro TCP/IP	98
Datagramové služby rozhraní NetBIOS.	98
Klientské služby a součásti	99
Automatická konfigurace klienta	99
Rozpoznání média (Media Sense).	100
Dynamická aktualizace klienta DNS	100
Služba DNS Resolver Cache Service	101
Filtrování protokolu TCP/IP.	101
Další informace	102
 3. KAPITOLA	
Řešení problémů protokolu TCP/IP	103
Přehled nástrojů pro řešení problémů protokolu TCP/IP.	104

Arp	105
Hostname	106
Ipconfig	106
Nbtstat	108
Netdiag	109
Syntaxe nástroje Netdiag	112
Netstat	113
Nslookup	116
PathPing	119
Výpočet ztrát	121
Ping	121
Nástroj Route	123
Tracert	124
Jak nástroj Tracert pracuje	125
Výklad výsledků použití nástroje Tracert	126
Přehled řešení problémů	126
Komunikace protokolu TCP/IP	127
Překlad názvu na adresu IP	127
Překlad názvu typu NetBIOS na adresu IP	127
Překlad názvu hostitele nebo doménového názvu na adresu IP	128
Určení, zda adresa je lokální nebo vzdálená	128
Je-li cílová adresa lokální, protokol IP použije k překladu na MAC adresu protokol ARP	128
Je-li adresa vzdálená, určí správnou bránu	128
Protokol ARP pro adresu brány	132
Nelze dosáhnout název hostitele nebo název typu NetBIOS	132
Error 53 (Chyba 53)	132
Nelze se připojit na vzdálené systémy používající název hostitele	133
Zkontrolujte si soubor Hosts	133
Zkontrolujte si konfiguraci DNS	134
Zkontrolujte soubor LMHOSTS	136
Zkontrolujte konfiguraci WINS	136
Nelze dosáhnout adresu IP	137
Zkontrolujte konfiguraci protokolu TCP/IP pomocí nástroje IPConfig ...	137
Zkontrolujte připojení k síti pomocí nástrojů Ping a PathPing	138
Vyčistíte mezipaměť ARP	140
Ověřte výchozí bránu	140
Proveďte příkaz Ping na vzdáleného hostitele	140

Test překladu adresy IP na adresu MAC pomocí protokolu ARP	141
Zjišťování duplikovaných adres IP za pomoci protokolu ARP	142
Zjišťování vadných záznamů v mezipaměti ARP	142
Ověřte trvalé záznamy směrovací tabulky	143
Použijte nástroje Tracert a PathPing	143
Ověřte služby serveru na vzdáleném počítači	143
Zkontrolujte zabezpečení protokolu IP na zahajujícím hostiteli	144
Zkontrolujte filtrování paketů	144
Řešení problémů směrování IP	145
Nelze se připojit k zadanému serveru	145
Připojení ke vzdálenému hostiteli visí	145
Prověření směrovací tabulky pomocí nástroje Route	146
Povolení směrování IP	146
Prověření cest pomocí nástroje Tracert	147
Řešení problémů s bránami	147
Řešení problémů protokolu ARP	147
Řešení problémů překladového přemostění	148
Používání nástroje Ping pro určení jednotky MTU	149
Řešení problémů jednotky PMTU směrovačů projevujících se jako černé díry	149
Zjištění jednotky PMTU pomocí provedení příkazu Ping	150
Služby pro řešení problémů	150
Nelze provést příkaz Ping přes směrovač jako klienta vzdáleného přístupu	151
Řešení problémů databázových souborů protokolu TCP/IP	151
Odebrání a opětná instalace protokolu TCP/IP	151
Klíče registru služby SNMP	152
Klíče registru služby TCP/IP Printing	152
Klíče registru služby Simple TCP/IP Services	152
Klíče registru služby DHCP	152
Klíče registru služby WINS	152
Klíče registru služby DNS	153
Další informace	153

ČÁST II

Přidělování adres a překlad názvu 155

4. KAPITOLA

Protokol DHCP 157**Co je to protokol DHCP? 158****Terminologie protokolu DHCP 158****Jak funguje protokol DHCP 159****Výhody protokolu DHCP 160****Nové vlastnosti 160**

Podpora klienta služby DHCP 161

Proces zápůjčky DHCP 163**Zprávy DHCP 163****Jak funguje proces zápůjčky 164****Stavy klienta DHCP v procesu zápůjčky 166**

Inicializace 167

Výběr 167

Požadavek 167

Vazba 169

Obnovení 169

Obnovení vazeb 170

Restartování klienta DHCP 171**Obnovování zápůjčky 171****Správa doby trvání zápůjčky 172****Správa oborů 172****Pravidlo 80/20 173****Správa rezervací 174****Superobory 175****Odebírání oborů 178****Předcházení konfliktům adres 178****Zjišťování konfliktů ze strany serveru 178****Zjišťování konfliktů ze strany klienta 179****Správa možností DHCP 179**

Parametry možností DHCP	182
Možnosti informace	182
Vnitřní Možnosti protokolu	182
Možnosti pro klienty se vzdáleným přístupem	183
Třídy možností	184
Třídy dodavatele	184
Třídy uživatele	185
Možnosti konfigurace	187
Priorita možností	187
Protokol DHCP s vícesměrovým vysíláním	187
Pozadí vícesměrového vysílání	188
Dynamické členství	188
Rozsahy adres vícesměrového vysílání	188
Podpora služby MADCAP	188
Databáze DHCP	189
Správa databáze	189
Správa záznamů	189
Správa úložného prostoru	190
Zálohy databáze	190
Soubory databáze služby DHCP	190
Podpora klientů BOOTP	192
Rozdíly mezi BOOTP a DHCP	193
Klienti BOOTP požadující pouze informace o adrese IP	193
Klienti BOOTP požadující informace o spouštěcím souboru	194
Možnosti DHCP podporované pro klienty BOOTP	194
Konfigurace tabulky BOOTP	195
Plánování pro protokol DHCP	195
Nejlepší postupy	195
Instalace služby DHCP	199
Aktualizace databáze DHCP pro Windows 2000	201
Konfigurování služby DHCP	202
Předcházení nepřátelským serverům DHCP	203
Jak jsou servery DHCP autorizovány	204
Jak jsou zjišťovány neautorizované servery	204
Clustering serverů DHCP	205
Příklad seskupených serverů DHCP	206

Scénáře služby DHCP	207
DHCP v malých sítích	207
DHCP ve velkých sítích	208
DHCP ve směrovaných sítích	208
Instalace přenosového agenta	209
Doporučená obecná konfigurace	210
Přenosoví agenti služby Routing and Remote Access pro Windows 2000 Server	210
Přenosoví agenti pro Windows NT Server 4.0	211
DHCP a služba Routing and Remote Access	211
Služby DHCP a WINS	213
Posílení odolnosti proti chybám služby DHCP/WINS	213
Další doporučení	214
Servery DHCP a DNS	214
Další doporučení	215
Klienti Windows DHCP a služba DNS s dynamickou aktualizací	216
Služba DHCP a APIPA	217
Vícedomé servery DHCP	217
Konfigurování vícedomého serveru DHCP	218
Správa přenosových agentů	219
Jak pracuje přenosový agent	221
Řešení problémů	221
Používání nástrojů Ipconfig a Winipcfg	222
Řešení problémů klientů DHCP	222
Řešení problémů serverů DHCP	223
Obvyklé problémy	224
Sledování výkonu serveru	227
Čítače Sledování systému služby DHCP	227
Statistické údaje Správce služby DHCP	229
Protokolování auditu DHCP	229
Názvy souborů protokolu auditu	230
Spuštění protokolu denního auditu	230
Kontroly disku	230
Ukončení protokolu denního auditu	231
Obnova dat serveru	231
Zjišťování poškození údajů aplikace DHCP Jet	232

Jednoduché zotavení: obnova ze zálohy	232
Znovuvytvoření zastaveného serveru DHCP	233
Přesun databáze serveru DHCP	234
Komprimace databáze serveru DHCP	234
Záchrana oborů pomocí vlastnosti Sloučit	235
Analýza souborů protokolu serveru	236
Formát souboru protokolu serveru DHCP	236
Kódy události protokolu serveru DHCP	236
Další informace	237

5. KAPITOLA

Úvod do DNS	239
Úvod do služby DNS	240
Obor doménových názvů	240
Doménový název	241
Obor doménových názvů Internetu	242
Základní koncepty DNS	243
Zóny	243
Servery DNS	245
Servery vyrovnávací paměti	246
Servery pro předávání a podřízené servery	246
Sdílení zatížení	247
Překlad názvu	247
Rekurzivní a iterativní dotazy	248
Ukládání do mezipaměti a TTL	249
Ukládání negativních odpovědí do mezipaměti	249
Záznamy prostředků a zóny	250
Formát záznamů prostředků	250
Typy záznamů prostředků	251
Záznamy prostředků SOA	251
Záznamy prostředků NS	252
Záznamy prostředků A	252
Záznamy PTR	252
Záznamy prostředků CNAME	252
Záznamy prostředků MX	253

Záznamy SRV	254
Méně časté záznamy prostředků	255
Záznamy prostředků nedefinované v dokumentech RFC	256
Delegace a společné záznamy	256
Zóny	257
Zóna dopředného vyhledávání	258
Zóna zpětného vyhledávání	258
Soubor odkazů na kořenové servery.	259
Spouštěcí soubor (soubor Boot)	260
Zónový přenos	261
Úplný zónový přenos	261
Přírůstkový zónový přenos	262
Upozornění DNS (DNS Notify)	263
Dynamická aktualizace	263
Standardy služby DNS.	264
Další informace	265

6. KAPITOLA

Služba Windows 2000 DNS	267
Úvod do implementace služby DNS v operačním systému Windows 2000	268
Vytváření názvů hostitelů a domén	270
Dodržování omezení názvů hostitelů a domén	272
Používání zásad skupiny ke specifikaci přípony DNS	274
Překladač pro operační systém Windows 2000	275
Překlad názvů	275
Překlad názvu DNS	276
Dotazy DNS.	277
Nastavení dotazů	283
Nastavení ukládání do mezipaměti a ukládání negativních odpovědí do mezipaměti	285
Nastavení priorit podsítě	287
Zabránění překladači v přijímání odpovědí od nedotázaných serverů	289
Nastavení služby DNS pro službu Active Directory.	290
Používání průvodce instalací služby Active Directory	291

Používání průvodce nastavením serveru DNS	292
Přidání zóny zpětného vyhledávání	294
Plánování zón zpětného vyhledávání	295
Nastavení standardní zóny zpětného vyhledávání	296
Nastavení a delegace beztřídové zóny zpětného vyhledávání In-addr.arpa ..	296
Integrace adresářové služby Active Directory a replikace Multimaster ...	299
Integrované ukládání	300
Umístění úložiště	303
Vytváření, převádění a odstraňování zón	305
Replikace multimaster	308
Kolize názvů	308
Vyvolání okamžité replikace	309
Dynamická aktualizace a zabezpečená dynamická aktualizace	309
Dynamická aktualizace	311
Proces dynamické aktualizace	312
Klienti a servery DHCP	313
Klienti se statickým nastavením a vzdáleným přístupem	319
Více domů klienti	319
Hodnota TTL	320
Řešení konfliktů názvů	321
Zabezpečená dynamická aktualizace	322
Nastavení zabezpečené dynamické aktualizace	322
Řízení přístupu aktualizace k zónám	322
Rezervace názvů	323
Standardy DNS pro zabezpečenou dynamickou aktualizaci	323
Proces zabezpečené dynamické aktualizace	324
Zabezpečení klientů DHCP nepodporujících možnost FQDN	326
Stárnutí a úklid paměti záznamů zastaralých názvů	327
Parametry stárnutí a úklidu paměti záznamů zastaralých názvů	328
Délka života záznamu	330
Chování serveru	331
Nastavení parametrů úklidu	332
Integrace se službou WINS	332
Formát záznamů prostředku WINS a WINS-R	333
Příklad vyhledávání WINS	334
Nastavení vyhledávání WINS	336
Upřesňující parametry vyhledávání WINS	336
Spolupráce s dalšími servery DNS	337

Úvahy o dynamické aktualizaci a zabezpečené dynamické aktualizaci .	337
Úvahy o spolupráci vyhledávání WINS	337
Používání odkazu WINS	338
Úvahy o zónovém přenosu	340
Úvahy o znakové sadě Unicode.	341
Nastavení serverů DNS s jiným operačním systémem než Windows 2000 k podpoře služby Active Directory	341
Podpora služby Active Directory pomocí jiných serverů DNS než společnosti Microsoft	342
Používání názvu delegované zóny jako domény služby Active Directory .	342
Používání názvu existující zóny jako názvu domény služby Active Directory	343
Úvahy o přístupu na síť internet	344
Plánování oboru názvů.	344
Příklad plánování oboru názvů	346
Nastavení vnějšího oboru názvů	346
Nastavení vnitřního oboru názvů	346
Příklady dotazů	348
Dotaz na název ve vnitřním oboru názvů	349
Dotaz na název ve vnějším oboru názvů	351
Dotaz na název ve vnějším oboru názvů organizace	353
Dotaz na název v oboru názvů připojené organizace	356
Řešení problémů.	357
Nástroje pro řešení problémů.	358
Nástroj Nslookup	358
Používání nástroje IPConfig.	361
Prohlížeč událostí.	362
Protokol DNS.	362
Zastavení a vyprázdnění mezipaměti	363
Sledování v konzole DNS	363
Rady pro nastavení a správu služby DNS	364
Ověření základního nastavení služby DNS.	365
Ověření, že server DNS může odpovídat na dotazy	365
Ověření správného nastavení zóny dopředného vyhledávání	366
Testování zón zpětného vyhledávání a záznamů prostředku PTR	366
Ověření nastavení služby DNS po instalaci služby Active Directory	367
Diagnostika problémů s překladem názvu	368
Nelze najít název nebo adresu IP.	375
Nesprávná odpověď	375
Hledání problémů se serverem DNS.	376

Diagnostika problémů s nesprávnými určujícími daty	377
Diagnostika problémů s rekurzí	378
Diagnostika problémů se zónovým přenosem	380
Řešení dalších běžných problémů služby DNS	381
Řešení problémů s dynamickou aktualizací	
a zabezpečenou dynamickou aktualizací	385
Řešení problémů s dynamickou aktualizací	385
Řešení problémů se zabezpečenou dynamickou aktualizací	386
Další informace	387

KAPITOLA 7

Služba Windows Internet Name Service	389
Celkový pohled na službu WINS	390
Inovace pro systém Windows 2000	390
Původ služby WINS	391
Dědictví rozhraní NetBIOS obsažené ve WINS.	392
Překlad názvů NetBIOS.	393
Všesměrové Vysílání v překladu názvů NetBIOS	394
Soubory LMHOSTS	395
Proč je služba WINS stále potřebná	395
Klienti služby Microsoft WINS	395
Jak registrují klienti WINS své názvy	397
Jak obnovují klienti WINS svoje názvy	398
Jak klienti uvolňují své názvy	399
Jak klienti WINS překládají názvy.	400
Konflikty klientů zjištěné během registrace	401
Chování klienta WINS	403
Denní spouštění.	403
Zapojování klienta do jiné podsítě	403
Prodloužená vypnutí	404
Vzájemné spojení dvou systémů WINS	404
Doporučené postupy pro klienty WINS	404
Konfigurace klientů pomocí plného seznamu serverů WINS	404
Používání příkazu Nbtstat -RR při správě propojitelnosti klienta	405
Postupy při konfiguraci klienta	405

Servery služby Microsoft WINS	405
Celkový pohled na servery WINS	406
Registrace názvů skupin	407
Speciální názvy skupin	408
Sekundární servery WINS	409
Server proxy služby Microsoft WINS	409
Dotazy pomocí serveru proxy WINS	411
Řízení shlukového přenosu	412
Jak funguje shlukové zpracování	412
Konfigurace podpory režimu shlukového zpracování	413
Clustering - seskupování	413
Doporučené postupy při práci se servery WINS	414
Používání výchozí konfigurace	414
Minimalizace počtu serverů WINS	414
Používání výkonného diskového hardwaru	415
Hardware pro síťové rozhraní přidávejte s rozvahou	415
Nastavení serveru tak, aby registroval sám sebe	415
Odolnost serveru WINS proti chybám	415
Nepoužívejte znaky rozšířených znakových sad	416
Srovnejte intervaly zapůjčení a obnovení názvů ve službách DHCP a WINS	416
Databáze WINS	417
Správa databáze serveru WINS	417
Zálohování databáze serveru WINS	418
Oprava databáze WINS	418
Obnovení dat pomocí replikace	419
Komprimování databáze WINS	420
Čištění databáze	420
Kontrola konzistence	422
Databázové soubory služby WINS	422
Časovače	423
Hodiny serveru	425
Mazání záznamů z databáze WINS	425
Příklad registrace záznamu a jeho označení za neplatný	425
Ruční označování záznamů za neplatné	427
Doporučené postupy při práci s databázemi služby WINS	428
Replikace WINS	430
Celkový pohled na proces replikace	430
Partnerské servery pro nabízenou a vyžádanou replikaci	432

Podrobná analýza příkladu replikace	432
Příklad replikace v malém měřítku	434
Vyžádání údajů z databáze WINS na základě čísla verze	438
Jak dochází ke změnám a aktualizacím záznamů	440
Konflikty zjištěné během replikace	441
Trvalá připojení	443
Automatické zjišťování partnerských serverů pro replikace	443
Doporučené postupy při replikování databáze WINS	444
Konfigurace partnerských serverů pro nabízenou a vyžádanou replikaci	444
Návrh replikace a konvergence WINS v paprskovitě rozmístěné síti s centrálním rozbočovačem	444
Replikace napříč bezpečností bránou (firewall)	444
Správa serverů WINS	445
Prohlížení operačního stavu serveru WINS	446
Konfigurace chování serveru a klienta	448
Správa mapování statických adres	450
Správa vícedomých serverů	450
Správa služby WINS napříč bezpečnostní bránou (firewall)	451
Doporučené postupy při práci s konzolou systémového řízení WINS	452
Zavádění služby Microsoft WINS	453
Příklady konfiguračního nastavení služby WINS	453
Přístup k síťovým přenosům	455
Typické síťové přenosy	456
Klientské přenosy ve směrovaných sítích	457
Přenosy a topologie	457
Kolik serverů je zapotřebí	458
Počet klientů na jeden server	458
Výkon serveru WINS	458
Konfigurační nastavení replikace	458
Automatická konfigurace partnerských serverů pro replikaci	459
Replikace mezi nedůvěryhodnými doménami	459
Replikace v rámci sítě WAN	459
Doba konvergence replikace	461
Příklad odolnosti serveru WINS proti chybám	462
Zatížení sítě duplicitními replikacemi	463
Partnerské servery pro replikace a konfigurace sítě	464
Vyřazení služby WINS z provozu	466

Změňte konfiguraci služby WINS klientských počítačů	466
Ověřte konfiguraci serverů DNS	466
Vyřazení serverů WINS	467
Omezení a přesměrování přenosů WINS	468
Interoperabilita	468
Používání serverů DHCP se servery WINS	468
Používání služby DNS spolu se službou WINS	469
Možnosti nastavení spolupráce WINS se službou DNS	469
Doporučené postupy	470
Konsolidujte podsítě	470
Aktualizace starších klientů	470
Odstraňování problémů spojených se službou WINS	470
Běžné problémy	471
Odstraňování problémů s klienty WINS	472
Odstraňování potíží se servery WINS	473
Odstraňování potíží s replikací WINS	475
Nástroje pro odstraňování potíží se serverem	475
Odstraňování potíží se serverem WINS	476
Prostředky	476
Názvy systému NetBIOS	476
Odkazy na názvy systému NetBIOS	476
Příkazy modulu NetShell	478
Specifikace služby WINS (RFC)	480
 ČÁST III	
Řízení a bezpečnost sítě	483
 KAPITOLA 8	
Zabezpečení protokolu IP	485
Otázky zabezpečení protokolu IP	486
Běžné typy síťových útoků	486
Tajné sledování	486
Záměna informací	486
Záměna identity (Padělání adresy IP)	486
Útok na zabezpečení heslem	486
Odmítnutí služby	487
Prostředník	487

Ohrožení bezpečnosti klíče	487
Štěníce	488
Útok na aplikační vrstvu	488
Představení zabezpečovacího protokolu IPSec	488
Důsledná ochrana	489
Agresivní zabezpečení proti útokům.	489
Zabezpečení vrstvy 3	490
Zabezpečení metodou zásad	491
Zjednodušené zavedení	491
Služby	492
Vlastnosti zabezpečení.	492
Ověřování na bázi certifikátu veřejného klíče	493
Ověřování s předběžným sdílením klíče	494
Šifrování veřejných klíčů	494
Integrita pomocí transformačních funkcí	494
Šifrování dat: Důvěrnost.	495
Standard šifrování DES	495
Správa klíčů.	496
Dynamické překlíčování	496
Délky klíčů	497
Typy protokolu IPSec	497
Ověřovací záhlaví.	497
Podpis paketu	498
Zabezpečení datové části zprávy zapouzdřením (ESP)	499
Podpis paketu a kódování.	500
Součásti protokolu IPSec	500
Služba Agent zásad IPSec	500
Výměna klíčů v síti Internet	501
Co je to SA?	502
SA typu Phase I	502
SA typu Phase II	503
Životnost přidružení zabezpečení.	504
Ochrana klíče.	504
Životnost klíče	504
Limit obnovení klíče relace	505
Skupiny typu Diffie-Hellman	505
Perfect Forward Secrecy	506

Řadič IPsec	506
Model IPsec	507
Tunelová propojení	508
Režim tunelového propojení ESP	509
Režim tunelového propojení AH	509
Struktura zásad IPsec	510
Dědičnost zásad	510
Pravidla	510
Filtrování paketů IP	511
Filtry	511
Akce filtrů	512
Typy připojení	512
Ověřování	513
Plánování zabezpečení protokolem IPsec	514
Doporučené postupy	514
Vytvoření plánu zabezpečení IPsec	515
Minimální zabezpečení	515
Standardní zabezpečení	515
Vysoký stupeň zabezpečení	516
Úvahy o specifických vlastnostech zabezpečení IPsec	516
Seznamy filtrů IP	516
Akce filtrů	516
Spojení se vzdáleným přístupem	516
SNMP	517
Zabezpečovací brány	517
Služby DHCP, DNS a WINS; řadiče domény	518
Předdefinované konfigurace	518
Klient (Jen odpovědět)	518
Server (Vyžaduje zabezpečení)	518
Zabezpečený server (Vyžaduje zabezpečení)	518
Předdefinovaná pravidla	518
Předdefinované akce filtru	519
Obecně použitelný příklad zabezpečení IPsec	519
Vyžadovaná zabezpečení	520
Odstraňování problémů	521
Odstraňování obecných problémů	521
Selhání komunikace se vzdáleným počítačem	521

Selhání komunikace uvnitř sítě intranet	521
Jiné příčiny selhání.	522
Řešení základních problému, spojených s protokolem IPSec	522
Chyba vyvolaná nesprávným přiřazením zásady IPSec	522
Zprávy „Chybné pakety SPI“ v Prohlížeči události	522
Ověřování spojení zabezpečených protokolem IPSec	523
Ověření, zda byla zásada vůbec přidělena	523
Nástroj Sledování IPSec	524
Selhávají pouze spojení zabezpečená protokolem IPSec	525
Porušené odkazy v součástech zásady	525
Restart služby Agent zásad	525
Opakovaná instalace součástí IPSec	526
Další zdroje	526

KAPITOLA 9

Technologie Quality of Service	529
Co je to Quality of Service?	530
Součásti technologie QoS v systému Windows 2000.	530
Na jakých principech technologie Quality of Service funguje	533
Spuštění služby QoS	534
Obecné rozhraní QoS API	534
Zprostředkovatel služby QoS (RSVP SP, služba RSVP).	535
Řízení přenosů	535
Součástí řízení přenosů	536
Obecný klasifikátor paketů (Msgpc.sys)	536
Plánovač paketů QoS (Psched.sys).	537
Označování paketů	537
Úroveň služeb přenosu.	537
Resource Reservation Protocol	539
Zprávy protokolu RSVP.	540
Specifikace toku dat a specifikace filtru	542
Specifikace filtru	542
Styl filtru	542
Jak funguje protokol RSVP.	544
Struktura zprávy RSVP	547

Podpora QoS v systému Windows 2000.	552
Architektura signalizované služby QoS.	552
Jakostní aplikace.	552
Integrace vrstvy 2	553
Odlišná třída služby	554
Integrované služby nad pomalým připojením	555
ATM	556
Dohody o úrovni služby	556
Služba řízení podsítě QoS v systému Windows 2000.	557
Jak funguje služba řízení podsítě QoS	558
Implementace služby QoS ACS	560
Zásady služby řízení podsítě QoS	562
Modul místních zásad	562
Zabezpečení.	563
Úložiště zásad	563
Definování zásad služby řízení podsítě QoS.	564
Hierarchie zásady	564
Zásady na úrovni rozlehlé (podnikové) sítě.	564
Zásady na úrovni podsítě	565
Objekty podsítě v konzole QoS ACS.	565
Odstraňování potíží.	566
Odstraňování základních problémů.	566
Obecné postupy při odstraňování problémů	567
Soubory protokolu služby QoS ACS.	570
Účtovací protokoly	571
Účtování	572
Protokoly RSVP	572
Chybové kódy RSVP	573
Nástroje.	576
PathPing	576
Wdsbm	576
Rsvptrace	577
NetMon.	578

Rsping	579
Tcmon	580
Sledování systému	581
Qtcp	581
Readpol	582
Rsvpsm	583
Qossp.aid, Rapolib.aid	583
Ttcp	583
Tracert	584
Další zdroje	584

KAPITOLA 10

Simple Network Management Protocol	587
Co je to SNMP?	588
Celkový pohled na SNMP	590
Správa a agenti	590
Management Information Base	591
Zprávy SNMP	592
Vlastnosti služby Agent SNMP systému Windows 2000	593
Zabezpečení	594
Depeše	594
Komunity	594
Možnosti konfigurace zabezpečení protokolu SNMP	596
Překladač událostí SNMP	597
Architektura protokolu SNMP v systému Windows 2000	597
Specifické otázky při implementaci protokolu SNMP	599
Změna nastavení portů SNMP	599
Ochrana zpráv SNMP pomocí zabezpečení protokolu IP	599
Správa služeb DHCP, Windows Internet Name Service a Internet Authentication Service	600
Používání programu Sledování systému	600
Správa služby DHCP	600
Správa služby WINS	600
Správa služby IAS	601
Nástroje služby SNMP	601

Nastavení položek registru	601
Odstraňování problémů s protokolem SNMP	602
Prohlížeč událostí	602
Služba WINS	602
Adresy IPX	602
Soubory služby SNMP	603
Další zdroje	603
 ČÁST IV	
Dodatky	605
 PŘÍLOHA A	
Model OSI	607
Vrstvy modelu OSI	608
Fyzická vrstva	608
Linková vrstva	609
Síťová vrstva	609
Transportní vrstva	610
Relační vrstva	611
Prezentační vrstva	611
Aplikační vrstva	611
Tok dat v modelu OSI	612
Terminologie vertikálního rozhraní v modelu OSI	613
 PŘÍLOHA B	
Síťová architektura systému Windows 2000	615
Přehled síťové architektury systému Windows 2000	616
Specifikace rozhraní síťového ovladače	618
Nové vlastnosti specifikace NDIS	619
Na spojení orientovaná specifikace NDIS	620
Režim Wake-On-LAN	620
Detekce média	620

Síť k okamžitému použití	621
Snížování zátěže sítě TCP/IP	621
Snížování zátěže výpočtů kontrolních součtů TCP/IP	621
Typy ovladačů rozhraní NDIS	622
Zprostředkující ovladače	622
Ovladače miniportů	623
Síťové protokoly	626
TCP/IP	627
Podpora velkých oken	627
Selektivní potvrzování	627
Odhad času okružní cesty	628
Zabezpečení protokolu IP	628
Obecná kvalita služby	628
Protokol ATM	628
Protokol NWLink	631
Protokol NetBEUI	631
Protokol AppleTalk	631
Protokol DLC	632
Protokoly IrDA	632
Vrstva rozhraní transportního ovladače	634
Moduly emulátorů	634
Síťová aplikační programová rozhraní	634
Rozhraní Winsock API	634
Architektura rozhraní Winsock	635
Soubory rozhraní Winsock	635
Aplikační programové rozhraní Winsock 1.1	637
Aplikační programové rozhraní Winsock 2.0	637
Poskytovatelé transportních služeb rozhraní Winsock 2.0 SPI	637
Vrstva poskytovatelů služeb vrstev	637
Knihovny pomocných modulů rozhraní Winsock	637
Poskytovatelé překladů názvů rozhraní Winsock 2.0	638
Obecná kvalita služby a protokol rezervace prostředků	638
Rozhraní telefonního subsystému	641
Rozhraní NetBIOS API	644
Rozhraní zpracování zpráv	645
Rozhraní WNet API	645
Další síťová aplikační programová rozhraní	645

Komunikace mezi procesy	646
Distribuovaný model Component Object Model	647
Výhody používání modelu DCOM	647
Vzdálené volání procedury	648
Překlad názvů RPC	650
Pojmenované kanály a poštovní přihrádky	650
Pojmenované kanály	651
Poštovní přihrádky	651
Systém Common Internet File System	651
Základní síťové služby	654
Služba serveru	654
Služba pracovní stanice	655
Přesměrovač Windows 2000 Redirector	656
Přístup ke vzdálenému souboru	657
Přístup k síťovým prostředkům	657
Hromadný zprostředkovatel univerzální konvence pro názvy	657
Směrovač hromadného zprostředkovatele	658
Další zdroje	659

PŘÍLOHA C

Přiřazení portů TCP a UDP	661
Úlohy portů a čísel protokolů	662
Dobře známé porty jsou přiřazovány organizací IANA	662
Přiřazení portů pro registrované porty	665
Přiřazení portů obecně používaným službám	666
Čísla protokolů	669
Další zdroje	670

PŘÍLOHA D

Vzdálené nástroje TCP/IP	671
Finger	672
Ftp	672
Rcp	674
Vzdálená oprávnění	675

Soubor Rhosts	675
Specifikování hostitelských počítačů	676
Vzdálené zpracování	676
Kopírování souborů	676
Syntaxe příkazu rcp	676
Rexec	677
Použití příkazu Rexec	677
Použití přesměrovacích symbolů	677
Použití interaktivních příkazů	678
Rsh	678
Použití nástroje Rsh	678
Použití přesměrovacích symbolů	678
Použití nástroje Rsh v doméně Windows 2000 Server	679
Soubor Rhosts	679
Telnet	679
Tftp	680

PŘÍLOHA E

Možnosti služby DHCP	681
Základní možnosti (RFC 1497)	682
Výplň (Pad Option)	682
Konec (End Option)	682
Maska podsítě (Subnet Mask)	682
Posunutí času (Time Offset)	683
Směrovač	683
Časový server (Time Server)	683
Názvový server IEN (IEN Name Server)	684
Server DNS (DNS Server)	684
Protokolovací server (Log Server)	684
Server Cookie (Cookie Server)	684
Server LPR (LPR Server)	685
Server Impress (Impress Server)	685
Server vyhledávání zdrojů (Resource Location Server)	685
Název hostitelského počítače (Host Name)	686

Velikost spouštěcího souboru (Boot File Size)	686
Soubor se stavem systému (Merit Dump File)	686
Název domény DNS	686
Odkládací server (Swap Server)	687
Kořenová cesta (Root Path)	687
Cesta rozšíření (Extensions Path)	687
Možnosti hostitelského počítače IP	688
Povolení a zákaz předávání protokolu IP	
(IP Forwarding Enable/Disable)	688
Povolení a zákaz směrování nemístních zdrojů	
(Nonlocal Source Routing Enable/Disable)	688
Filtr zásad (Policy Filter)	688
Maximální velikost znovu sestaveného datagramu	
(Maximum Datagram Reassembly Size)	689
Výchozí hodnota Time-To-Live protokolu IP (Default IP Time-To-Live) ..	689
Časový limit stárnutí jednotky MTU cesty (Path MTU Aging Time-out) ..	689
Cesta k tabulce MTU Plateau Table (Path MTU Plateau Table)	689
Možnosti rozhraní IP	690
Jednotka MTU rozhraní (Interface MTU)	690
Všechny podsítě jsou místní (All Subnets Are Local)	690
Adresa všesměrového vysílání (Broadcast Address)	690
Provést zjištění masky (Perform Mask Discovery)	691
Poskytovatel masky (Mask Supplier)	691
Provést zjištění směrovače (Perform Router Discovery)	691
Adresa oslovování směrovače (Router Solicitation Address)	691
Statická trasa (Static Route)	691
Možnosti linkové vrstvy	692
Zapouzdření koncové části (Trailer Encapsulation)	692
Časový limit mezipaměti ARP (ARP Cache Time-Out)	692
Zapouzdření sítě Ethernet (Ethernet Encapsulation)	692
Možnosti protokolu TCP	693
Výchozí hodnota TTL protokolu TCP (TCP Default TTL)	693

Interval udržení názvu protokolu TCP (TCP Keep-Alive Interval)	693
Posílání nepotřebných informací při udržení názvu protokolu TCP (TCP Keep-Alive Garbage).	693
Možnosti aplikační vrstvy	693
Název domény NIS (NIS Domain Name).	694
Servery NIS (NIS Servers).	694
Servery NTP (NTP Servers)	694
Servery písma systému X Window (X Window System Font Servers) . . .	694
Servery správy zobrazení systému X Window (X Window System Display Manager Servers).	695
Název domény NIS+ (NIS+ Domain Name).	695
Servery NIS+ (NIS+ Servers).	695
Mobilní domácí agenti IP (Mobile IP Home Agents).	695
Možnosti rozhraní NetBIOS pro TCP/IP.	696
Názvový server NetBIOS (NetBIOS Name Server)	696
Server distribuce datagramů rozhraní NetBIOS (NetBIOS Datagram Distribution (NBDD) Server)	696
Typ uzlu rozhraní NetBIOS (NetBIOS Node Type)	696
ID oboru rozhraní NetBIOS (NetBIOS Scope ID)	696
Možnosti specifické pro dodavatele	697
Informace specifické pro dodavatele (Vendor-Specific Information) . . .	697
Identifikátor třídy dodavatele (Vendor Class Identifier)	698
Možnosti třídy uživatele	698
Informace o třídě uživatele (User Class Information)	699
Rozšíření služby DHCP	699
Vyžadovaná adresa IP (Requested IP Address)	699
Doba zapůjčení adresy IP (IP Address Lease Time)	700
Přeplnění možnosti (Option Overload).	700
Název serveru TFTP (TFTP Server Name).	700
Název spouštěcího souboru (Boot File Name).	700
Typ zprávy DHCP (DHCP Message Type)	701
Identifikátor serveru (Server Identifier)	701

Seznam požadavků parametrů (Parameter Request List)	702
Nepovinná zpráva (Optional Message)	702
Maximální velikost zprávy (Maximum Message Size)	702
Časová hodnota obnovení (T1) (Renewal Time Value (T1))	703
Hodnota doby obnovení vazeb (T2) (Rebinding Time Value (T2))	703
Jedinečný identifikátor klienta (Client Unique Identifier).	703
Nedefinované možnosti.	704
Server SMTP (Simple Mail Transport Protocol (SMTP) Server)	704
Server POP3 (Post Office Protocol (POP3) Server)	704
Server NNTP (Network News Transport Protocol (NNTP) Server)	704
Výchozí server služby World Wide Web (Default World Wide Web Server)	705
Výchozí server služby Finger (Default Finger Server)	705
Výchozí server protokolu IRC (Default Internet Relay Chat Server)	705
Server protokolu StreetTalk (StreetTalk Server)	705
Server protokolu STDA (StreetTalk Directory Assistance Server)	706
Možnosti Microsoft.	706
Zakázat rozhraní NetBIOS pro TCP/IP (Disable NetBIOS over TCP/IP (NetBT))	706
Uvolnit zapůjčení DHCP při vypnutí (Release DHCP Lease on Shutdown)	706
Výchozí základ metriky směrovače (Default Router Metric Base)	707
Automatické zjišťování proxy pro Internet Explorer 5 (Proxy Autodiscovery for Internet Explorer 5 Only)	707

PŘÍLOHA F

Formát zpráv služby DHCP	709
Zprávy služby DHCP	710

PŘÍLOHA G

Typy objektů databáze MIB	715
Databáze informací o správě	716
Identifikátory objektů.	716

Agent protokolu SNMP v systému Windows 2000	717
Další zdroje	719

PŘÍLOHA H

Soubor LMHOSTS	721
Použití souboru LMHOSTS k nalezení počítačů a služeb	722
Vyhledávání vzdálených počítačů	723
Určování řadičů domén	724
Použití centralizovaných souborů LMHOSTS	724
Vytváření souboru LMHOSTS	724
Vytváření položek v souboru LMHOSTS	725
Přidávání názvů vzdálených systémů použitím klíčového slova #PRE.	727
Přidávání řadičů domény použitím klíčového slova #DOM.	728
Přidávání zvláštních skupin definovaných uživatelem	
použitím klíčového slova #SG.	729
Přidávání zařízení s více adresami použitím klíčového slova #MH.	729
Definování centrálního souboru LMHOSTS použitím klíčového slova	
#INCLUDE.	730
Nastavení TCP/IP pro použití překladu názvů souborem LMHOSTS	731
Údržba souboru LMHOSTS	731
Odstraňování potíží se souborem LMHOSTS	732

PŘÍLOHA I

Prohledávací služba v systému Windows 2000	733
Úvod do služby Browser	734
Přehled systému prohledávačů v systému Windows 2000	734
Určování prohledávacích počítačů	735
Role v systému prohledávačů	736
Počítač, který není prohledávačem (Non-Browser)	737
Potenciální prohledávač (Potential Browser)	737
Záložní prohledávač (Backup Browser)	737
Hlavní prohledávač (Master Browser).	738
Hlavní prohledávač domény.	738
Volby prohledávačů	739

Oznámení prohlédávačů	741
Oznámení počítačů, které nejsou prohlédávači	743
Oznámení potenciálních prohlédávačů	743
Oznámení záložních prohlédávačů	743
Nastavení času oznámení prohlédávače	744
Požadavky prohlédávače	744
Počet prohlédávačů v doméně nebo pracovní skupině	745
Vypnutí nebo selhání prohlédávače	745
Selhání počítače, který není prohlédávačem	746
Selhání záložního prohlédávače	746
Selhání hlavního prohlédávače	746
Selhání hlavního prohlédávače domény	746
Prohlédávací služba přes více pracovních skupin a domén	747
Prohlédávací služba přes směrovač IP	748
Překlad názvů	749
Prohlédávací služba přes směrovač IP s protokolem TCP/IP	750
Systém Domain Name System	750
Služba Windows Internet Name Service	750
Soubor LMHOSTS	751
Všesměrová vysílání názvové služby pro NetBIOS	751
Počítače se systémy Windows for Workgroups, Windows 95 a Windows 98 jako hlavní prohlédávače	752
Registrace a šíření	752
Testovací techniky	754
Sledování prohlédávačů	755
Vystopování problému	755
Další úvahy	762
Glosář	765
Rejstřík	815

Úvod

Vítáme vás v části *Průvodce distribuovanými systémy*, která patří do kompendia *Microsoft® Windows®2000 Server Resource Kit*.

Toto kompendium sestává z pěti svazků a dvou kompaktních disků (CD) a obsahuje nástroje, doplňkové referenční materiály a on-line verze těchto knih. Dodatky k *Windows 2000 Server Resource Kit* budou vydány, jakmile budou k dispozici nové poznatky. Aktualizace a informace můžete najít průběžně na stránkách WWW.

Průvodce distribuovanými systémy přináší koncepční, teoretický, funkční i praktický pohled na různé technologie, které daly vzniknout distribuovaným systémům Microsoft®Windows®2000. Tento průvodce obsahuje hluboké technické informace, které zahrnují čtyři hlavní oblasti: Službu Active Directory, distribuovanou bezpečnost, podnikovou technologii a správu konfigurace desktopu.

Použité konvence

V tomto průvodci užíváme následující konvence stylu písma terminologie:

prvek	význam
tučné písmo	Znaky, které píšete tak, jak je ukázáno, zahrnují příkazy a přepínače. Rovněž prvky uživatelského rozhraní jsou označeny tučně.
<i>kurzíva</i>	Proměnné, kterým zadáváte specifické hodnoty. Např. <i>Filename.ext</i> se může vztahovat k jakémukoli platnému jménu souboru.
monospace	Vzorky kódů.
%SystemRoot%	Složka, ve které je instalován systém Windows 2000.

upozornění čtenáři	význam
Tip	Upozorňuje vás na doplňkovou informaci, která není podstatná pro okamžité dokončení úlohy.
Poznámka	Upozorňuje vás na doplňkovou informaci.
Důležité	Upozorňuje vás na doplňkovou informaci, která je podstatná pro dokončení úlohy.
Pozor	Upozorňuje vás na možnou ztrátu dat, na narušení bezpečnosti nebo na jiné vážné problémy.
Varování	Upozorňuje vás na to, že selhání při provádění nebo vynechání určité činnosti může vést k fyzické újmě vaší nebo vašeho hardware.

Kompaktní disk sady Resource Kit

Kompendium *Windows 2000 Server Resource Kit* obsahuje CD, na kterém se nacházejí různé nástroje a zdroje, které vám umožní efektivněji pracovat se systémem Windows 2000.

Poznámka Všechny nástroje na CD byly navrženy a testovány na US verzi Windows 2000. Použití těchto programů na jiných verzích Windows 2000 nebo na verzi Microsoft® Windows NT® může vést k nepředvídatelným výsledkům.

Doprovodné CD obsahuje tyto informace:

Windows 2000 Server Resource Kit Online Books Jedná se o Help HTML verzi tištěných knih. Můžete ji používat k nalezení stejně podrobných informací o Windows 2000, jaké jsou v tištěné verzi. Vyhledávání jde přes všechny knihy a slouží pro nalezení věcné informace podstatné k okamžitému ukončení úlohy.

Windows 2000 Server Resource Kit Tools and Tools Help Obsahuje přes 2000 softwarových nástrojů, jejich dokumentaci a další zdroje, které umožní využít sílu Windows 2000. Tyto nástroje můžete použít pro řízení služby Active Directory, pro správu bezpečnostních vlastností, pro práci s registry, pro automatizaci opakujících se prací a pro mnoho dalších důležitých úloh. Používejte dokumentaci, abyste se dozvěděli o těchto nástrojích správy a naučili se s nimi zacházet.

Windows 2000 Resource Kit References Sada Help HTML referencí:

- **Pomoc při hlášení chyb a událostí** obsahuje většinu chybových hlášení a hlášení událostí generovaných ve Windows 2000. Každé hlášení je doprovázeno podrobným výkladem a doporučením, co může uživatel udělat.
- **Technické reference k registru** přinášejí detailní popis obsahu registru systému Windows 2000, jako např. podstromy, klíče, podklíče a záznamy, o kterých chtějí pokročilejší uživatelé vědět, včetně mnoha záznamů, které mohou být s použitím nástrojů nebo programových rozhraní Windows 2000 měněny.
- **Reference čítače výkonu** popisují všechny objekty a čítače výkonu, připravené pro použití s nástroji Performance snap-in v systému Windows 2000. Využijte tyto reference a naučte se, jak vám může pomoci sledování hodnot čítačů při diagnostikování problémů nebo při hledání úzkých profilů ve vašem systému.
- **Reference ke skupinové politice** vám zabezpečí detailní popis uspořádání skupinové politiky ve Windows 2000. Tyto popisy vysvětlují vliv aktivování, deaktivování nebo nekonfigurování každé politiky a také jak na sebe odpovídající politiky působí.

Politika podpory pro Resource Kit

Software, dodávaný v sadě *Windows 2000 Server Resource Kit* není podporován. Firma Microsoft nezaručuje výkonnost nástrojů *Windows 2000 Server Resource Kit*, dobu odezvy pro zodpovězení otázek nebo chyby řešení programu, v nich obsažených. Nicméně zajišťuje způsob jak zákazník, který si zakoupil sadu *Windows 2000 Server Resource Kit*, může hlásit chyby programu a získat možná řešení k jejich odstranění. Můžete to udělat tak, že zašlete e-mail na rkinput@microsoft.com. Tato e-mailová adresa

je pouze pro problematiku svázanou s *Windows 2000 Server Resource Kit*. S problematikou, spojenou s operačním systémem Windows 2000 se, prosím, využijte informace o podpoře obsažené ve vašem produktu.

ČÁST I

TCP/IP ve Windows 2000



Sada protokolů TCP/IP je strategickou internetovou technologií současnosti i budoucnosti. Tato část se zabývá základy TCP/IP včetně implementace ve Windows 2000.

V této části

Úvod do TCP/IP 7

Windows 2000 TCPI/IP 53

Řešení problémů protokolu TCP/IP 103

1. KAPITOLA

Úvod do TCP/IP



Operační systém Microsoft Windows 2000 disponuje kvalitní podporou sady protokolů TCP/IP (Transmission Control Protocol/Internet Protocol), a to jak samotných protokolů, tak i sadou služeb pro připojení a správu sítí na těchto protokolech vystavěných. Znalost základních myšlenek TCP/IP je nezbytná pro správné pochopení konfigurace, zavádění a řešení problémů vzniklých v sítích se systémy Microsoft Windows 2000 a Microsoft Windows NT, které tyto protokoly používají.

V této kapitole

Sada protokolů TCP/IP	8
Architektura TCP/IP	9
Překlad adres	39
Směrování IP	44
Přiřazení fyzické adresy	50

Související informace:

- Více informací o síťové architektuře Windows 2000 najdete v této knize v příloze „Síťová architektura Windows 2000“.
- Více informací o implementaci TCP/IP ve Windows 2000 najdete v dalších kapitolách této části.

Sada protokolů TCP/IP

TCP/IP je standardní sada protokolů určená pro propojení rozlehlých sítí WAN a byla vyvinuta v roce 1969 Agenturou pro pokročilé výzkumné projekty Ministerstva obrany Spojených států amerických (DARPA; U.S. Department of Defense Advanced Research Projects Agency) jako výsledek experimentu se sdílením prostředků nazvaného ARPANET (Síť Agentury pro pokročilé výzkumné projekty; Advanced Research Projects Agency Network). Od roku 1969 se ARPANET rozrostl do celosvětové společnosti sítí známé jako Internet.

Microsoft TCP/IP

Microsoft TCP/IP ve Windows 2000 podporuje podnikové sítě a propojování počítačů s Windows 2000 a Windows NT. Přidání podpory TCP/IP ke konfiguraci Windows 2000 nabízí následující výhody:

- Standardní podnikový síťový protokol, který je nejpůlnějším a nejvíce akceptovaným dostupným protokolem. Všechny moderní síťové operační systémy nabízejí podporu TCP/IP a největší sítě při většině síťového provozu se spoléhají právě na TCP/IP.
- Technologii pro propojení nepřibuzných systémů. Pro přístup a přenos dat mezi nepřibuznými systémy existuje množství standardních nástrojů, včetně FTP a Telnetu, protokolu emulujícího terminálové připojení. Některé z těchto standardních nástrojů jsou ve Windows 2000 obsaženy.
- Robustní, škálovatelný, víceplatformový systém klient/server. Microsoft TCP/IP nabízí rozhraní Windows Sockets, které je ideální pro vývoj aplikací klient/server využívajících produktů s tímto rozhraním kompatibilní od jiných výrobců.
- Způsob přístupu k Internetu. Internet se sestává z tisíců sítí po celém světě, které spojují výzkumné ústavy, univerzity, knihovny a soukromé společnosti.

Poznámka: Pojem *internet* (s malým i) zpravidla označuje řadu TCP/IP sítí spojených směrovači. Odkazy na *Internet* (s velkým I) se vztahují k celosvětovému veřejnému Internetu. Odkazy na intranet se vztahují například k soukromé či podnikové síti.

Standardy TCP/IP

Standardy pro TCP/IP jsou zveřejněny v řadě dokumentů nazvaných *Request for Comments* (RFCs). Tyto dokumenty popisují vnitřní stavbu Internetu. Některé popisují síťové služby nebo protokoly a jejich implementaci, zatímco ostatní shrnují důležité zásady. TCP/IP standardy jsou vždy uveřejňovány jako dokumenty RFC, ačkoli ne všechny dokumenty RFC jsou standardy.

TCP/IP standardy nebyly vyvinuty komisí, ale spíše na základě mnoha dohod, protože dokument určený ke zveřejnění jako RFC může dodat kdokoli. Dokumenty zkontroluje odborník nebo vydavatel RFC a přiřadí jim určitý typ. Tento typ určuje, jestli je dokument pokládán za standard či nikoli.

Existuje pět typů dokumentů RFC, viz tabulka 1.1

Tabulka 1.1 Typy dokumentů RFC

Typ	Popis
Požadovaný	Musí být implementován na všech hostitelích a branách založených na TCP/IP.
Doporučený	Doporučuje implementaci těchto specifikací na všechny hostitele a brány založené na TCP/IP. Doporučené RFC jsou implementovány zpravidla.
Volitelný	Implementace je v tomto případě zcela dobrovolná. Specifikace je od-souhlasena, ale není vyžadována.
Omezené použití	Nevhodné pro obecné použití.
Nedoporučený	Nedoporučené k implementaci.

Dokument pokládáný za standard prochází stádií vývoje, testování a přijetí známými jako Internet Standards Process. Tato stadia formálně označují úroveň vyspělosti, přičemž tři stadia standardů Internetu najdete v tabulce 1.2.

Tabulka 1.2 Úrovně vyspělosti standardů Internetu

Úroveň	Popis
Navržený standard	Standard této úrovně je relativně stabilní, řeší známé problémy návrhu, považuje se za dobře srozumitelný, obdržel podporu významného počtu lidí a zajímá tolik lidí, že se dá pokládat za přínosný.
Vybraný standard	Musí být dobře srozumitelný a stabilní jak ve vlastní sémantice, tak jako základ pro vývoj implementace.
Internetový standard	Standard této úrovně, označovaný také jednoduše jako „standard“, se vyznačuje vysokým stupněm technické vyspělosti a obecně sdílenou vírou, že určitý protokol nebo služba poskytuje Internetovému společenství významný užitek.

Při publikaci je dokumentu přiřazeno tzv. RFC číslo. Původní RFC nejsou nikdy aktualizovány, proto jsou prováděné změny publikovány vždy pod novým číslem. Je tedy velice důležité se ujistit, že opravdu máte pro potřebné téma nejnovější RFC.

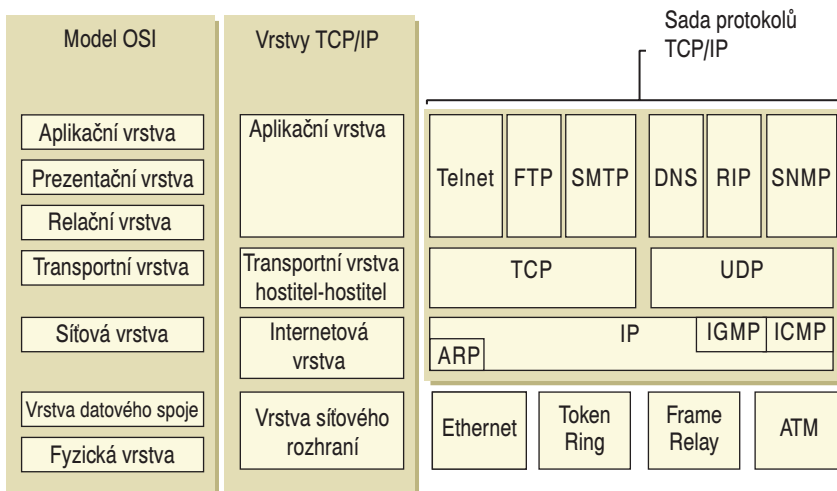
Dokumenty RFC lze získat několika způsoby. Chcete-li získat jakýkoli dokument RFC nebo plný a aktuálně indexovaný seznam všech dokumentů RFC publikovaných do dnešního dne, podívejte se na adresu

<http://windows.microsoft.com/windows2000/reskit/webresources>.

Architektura TCP/IP

Protokoly TCP/IP jsou založeny na čtyřvrstevném koncepčním modelu známém jako *model DARPA* pojmenovaném podle vládní agentury USA, která původně TCP/IP vyvinula. Čtyři vrstvy modelu DARPA jsou: aplikační, transportní, internetové a síťové rozhraní. Každá vrstva tohoto modelu odpovídá jedné nebo více vrstvám sedmiúrovňového referenčního modelu OSI (Open Systems Interconnection).

Na obrázku 1.1 vidíte architekturu TCP/IP.



Obrázek 1.1 Architektura protokolu TCP/IP

Vrstva síťového rozhraní

Vrstva síťového rozhraní (nazývaná též vrstva síťového přístupu) zodpovídá za předávání TCP/IP paketů síťovému médium a přijímání TCP/IP paketů z tohoto média. TCP/IP bylo navrženo tak, že je nezávislé na metodě přístupu k síti, použitém formátu rámce a médium. Tak může být TCP/IP použit při propojování různých typů sítí, včetně technologií LAN (například Ethernet a Token Ring) a technologií WAN (například X.25 a Frame Relay). Nezávislost na určité síťové technologii poskytuje TCP/IP schopnost adaptace na nové technologie, mezi které patří například ATM (Asynchronous Transfer Mode). Vrstva síťového rozhraní zahrnuje vrstvu datového spoje a fyzickou vrstvu referenčního modelu OSI. Uvědomte si, že internetová vrstva nevyužívá potvrzovacích služeb, které mohou být k dispozici ve vrstvě datového spoje.

Internetová vrstva

Internetová vrstva je zodpovědná za adresaci, balení a směrovací funkce. Základní protokoly této vrstvy jsou IP, ARP, ICMP a IGMP.

- *Internet Protokol (IP)* je směrovatelný protokol odpovědný za adresaci, směrování, rozdělování a opětovné skládání paketů.
- *Adress Resolution Protocol (ARP)* je odpovědný za překlad adres internetové vrstvy na adresy pro vrstvu síťového rozhraní, jako jsou hardwarové adresy.
- *Internet Control Message Protocol (ICMP)* je odpovědný za poskytování diagnostických funkcí a hlášení o problémech s doručení IP paketů.
- *Internet Group Management Protocol (IGMP)* je odpovědný za správu skupin pro víceměrové vysílání.

Internetová vrstva odpovídá síťové vrstvě v rámci referenčního modelu OSI.

Transportní vrstva

Transportní vrstva (nazývaná též transportní vrstva hostitel-hostitel) zodpovídá za zpřístupnění poskytování komunikačních služeb relací a datagramu. Hlavními protokoly transportní vrstvy jsou TCP (*Transmission Control Protocol*) a UDP (*User Datagram Protocol*).

- Protokol TCP poskytuje spolehlivé komunikační služby pro dvoubodové spojení. TCP odpovídá za ustavení TCP spojení, seřazení a potvrzení posílaných paketů a obnovení paketů ztracených během přenosu.
- Protokol UDP poskytuje nespolehlivé komunikační služby pro dvou či vícebodové spojení. UDP se používá v případě přenosu pouze malého množství dat (například data do velikosti pouze jednoho paketu), v případě nežádoucího ustavení nákladného TCP spojení nebo v případě, že aplikace nebo protokoly v horní vrstvě zaručují spolehlivé doručení.

Transportní vrstva zajišťuje všechny povinnosti transportní vrstvy referenčního modelu OSI a některé povinnosti vrstvy relační.

Aplikační vrstva

Aplikační vrstva umožňuje aplikacím přístup ke službám jiných vrstev a definuje protokoly používané aplikacemi k výměně dat. Existuje mnoho protokolů aplikační vrstvy a stále vznikají další.

Nejznámější protokoly aplikační vrstvy jsou protokoly používané k výměně uživatelských informací:

- Protokol HTTP (Hypertext Transfer Protocol) se používá k přenosu souborů tvořících webové stránky na Internetu.
- Protokol FTP (File Transfer Protocol) se používá k interaktivnímu přenosu souborů.
- Protokol SMTP (Simple Mail Transfer Protocol) se používá k přenosu poštovních zpráv a příloh.
- Protokol Telnet emuluje terminál a používá se ke vzdálenému přístupu k hostitelům v sítích.

Navíc používání a správu TCP/IP sítí pomáhají ulehčit tyto protokoly aplikační vrstvy:

- Protokol DNS (Domain Name System) se používá k překladu doménových názvů na konkrétní adresy IP.
- Protokol RIP (Routing Information Protocol) je používán směrovači k výměně směrovacích informací.
- Protokol SNMP (Simple Network Management Protocol) se používá mezi konzolami pro správu sítě a síťovými zařízeními (směrovače, mosty, inteligentní rozbočovače) ke sběru a výměně informací o stavu sítě.

Příkladem rozhraní aplikační vrstvy pro aplikace TCP/IP jsou rozhraní Windows Sockets nebo NetBIOS.

Windows Sockets poskytuje standardní aplikační rozhraní pod Windows 2000. NetBIOS nabízí průmyslový standard pro přístup k datagramům, relacím a překladům adres. Více informací o obou rozhráních najdete dále v této kapitole.

Základní protokoly TCP/IP

Komponenty TCP/IP instalované ve vašem síťovém operačním systému jsou sadou vzájemně propojených protokolů, tzv. základních (hlavních) protokolů TCP/IP. Všechny ostatní aplikace a další protokoly v TCP/IP jsou samozřejmě závislé na základních službách poskytovaných protokoly IP, ARP, ICMP, IGMP, TCP a UDP.

Protokol IP

Protokol IP je nespolehlivý datagramový protokol nespojovaný, který je především odpovědný za adresaci a směrování paketů mezi hostiteli. „Nespojovaný“ znamená, že před výměnou dat není ustaveno relace. „Nespolehlivý“ znamená, že není garantováno doručení paketů. Protokol IP se vždycky „snaží“ doručit paket, ale přesto může dojít k jeho ztrátě, duplikaci, zpoždění nebo doručení mimo sekvenci. Protokol IP se po tomto typu chyb nesnaží o obnovu paketu. Registrace doručených paketů a obnova ztracených paketů náleží protokolu ve vyšší vrstvě, například TCP. Protokol IP je definován v RFC 791.

Paket IP se sestává z IP hlavičky a vlastního obsahu. V tabulce 1.3 najdete popis klíčových polí v hlavičce.

Tabulka 1.3 Klíčová pole v IP hlavičce

Pole IP hlavičky	Funkce
Adresa IP zdroje	Adresa IP původního zdroje IP datagramu.
Adresa IP cíle	Adresa IP konečného cíle IP datagramu.
Identifikace	Používá se k identifikaci IP datagramu a identifikaci všech fragmentů určitého IP datagramu, pokud se fragmentace objeví.
Protokol	Informuje protokol IP u cíle (na straně příjemce), jestli má paket postoupit TCP, UDP, ICMP nebo jiným protokolům.
Kontrolní součet	Jednoduchý matematický výpočet používaný ke kontrole integrity IP hlavičky.
TTL (Time-to-Live)	Určuje počet sítí, po kterých může být datagram přenášen, než jej směrovač zahodí. TTL je nastaveno odesílatelem a slouží k prevenci nekonečného obíhání paketů po IP síti. Při každém předání IP paketu musí směrovače velikost tohoto parametru snižovat (minimálně o jedničku).

Rozdělování a opětovné skládání

Pokud směrovač obdrží IP paket, který je pro síť, do které je předáván, příliš velký, rozdělí IP protokol původní paket do menších paketů, které odpovídají parametrům příslušné sítě. Po doručení všech paketů příjemci tamější IP protokol tyto fragmenty opět složí do původního tvaru. Tento proces se označuje jako rozdělování a opětovné skládání (*fragmentace a kompletace*). Fragmentace se může objevit v prostředích, které používají smíšené síťové technologie, například Ethernet nebo Token Ring.

Rozdělování a opětovné skládání funguje následujícím způsobem:

- Při odesílání IP paketu umístí zdroj do identifikačního pole jedinečnou hodnotu.
- Směrovač tento paket přijme. IP směrovač zaznamená, že maximální jednotka přenosu (MTU, maximum transmission unit) sítě, na kterou má paket pokračovat, je menší než velikost IP paketu.
- IP rozdělí původní obsah paketu do fragmentů, které odpovídají parametrům sítě. Každý odesílaný fragment má vlastní IP hlavičku, která obsahuje:
 - Původní identifikační pole označující všechny k sobě patřící fragmenty.
 - Označení, že následují další fragmenty (More Fragments Flag). Toto označení není v posledním fragmentu, protože po něm už žádné další fragmenty nenásledují.

- Pole označující polohu fragmentu vzhledem k původnímu obsahu paketu (Fragment Offset field).

Po přijetí fragmentů IP protokolem na vzdáleném hostiteli jsou pomocí identifikačního pole určeny k sobě patřící fragmenty a pomocí pole označujícího polohu fragmentu vzhledem k původnímu obsahu paketu poskládány zpět v jeden celek.

Protokol ARP

Při odesílání IP paketů na sdíleném přístupu, tedy na síťových technologiích založených na všesměrovém vysílání jako je například Ethernet nebo Token Ring, musí být technologicky závislá adresa převedena na adresu odpovídající předávající IP adrese. ARP používá k převedení známé předávající adresy IP na adresu MAC všesměrové vysílání. ARP je definováno v RFC 826.

Více informací o protokolu ARP najdete dále v této kapitole.

Protokol ICMP

Protokol ICMP (Internet Control Message Protocol) poskytuje pomůcky k likvidaci problémů s nedoručitelnými pakety a chybová hlášení o těchto nedoručitelných paketech. Například, není-li IP protokol schopen doručit paket příjemci, pošle ICMP zdroji hlášení o nemožnosti dosažení adresáta. Nejobvyklejší hlášení ICMP najdete v tabulce 1.4.

Tabulka 1.4 Běžná hlášení protokolu ICMP

Hlášení ICMP	Funkce
Echo žádost	Hlášení používané ke kontrole připojitelnosti IP k požadovanému hostiteli. Je zasíláno například nástrojem ping.
Echo odpověď	Odpovídá na Echo žádost.
Přesměrování	Hlášení směrovače, které informuje odesílatele o lepší cestě k cíli.
Potlačení zdroje	Hlášení směrovače, které informuje odesílatele, že jeho IP datagramy jsou kvůli kapacitě směrovače zahazovány. Odesílatel následně sníží svoji rychlost přenosu. Toto hlášení je volitelné a není běžně implementováno.
Nedosažitelný adresát	Hlášení směrovače nebo cílového hostitele, které informuje odesílatele, že datagram nelze doručit.

Existuje celá řada definovaných ICMP hlášení o nedoručitelnosti. V tabulce 1.5 najdete ta nejobvyklejší.

Tabulka 1.5 Běžná hlášení protokolu ICMP o nedoručitelnosti

Hlášení o nedoručitelnosti	Popis
Nedosažitelná síť	Hlášení posílané IP směrovačem v případě, že nelze nalézt cílovou síť. Toto hlášení je již zastaralé.
Nedosažitelný hostitel	Hlášení posílané IP směrovačem v případě, že nelze nalézt cestu k cílové IP adrese.
Nedosažitelný protokol	Hlášení posílané IP uzlem cíle v případě, že pole Protokol v IP hlavičce nelze sladit s aktuálním IP protokolem klienta.

Hlášení o nedoručitelnosti Popis

Nedosažitelný port	Hlášení posílané IP uzlem cíle v případě, že port cíle v UDP hlavičce nelze sladit s procesem používajícím tento port.
Nutná fragmentace a DF je nastaven	Hlášení posílané IP směrovačem v případě, kdy je nutná fragmentace, ale kdy není povolena, protože zdrojový uzel nastavil příznak (DF, tj. Nedělit, v IP hlavičce).
Selhání zdrojového směrování	Hlášení posílané IP směrovačem v případě, že selže doručení IP paketu používající zdrojového směrování.

Protokol ICMP nepřispívá ke spolehlivosti IP protokolu. Protokol ICMP se snaží o hlášení chyb a za určitých podmínek i o poskytování zpětné vazby. Hlášení protokolu ICMP jsou přenášena jako nepotvrzované IP datagramy a jsou samy o sobě nespolehlivé. Protokol ICMP je definován v RFC 792.

Protokol IGMP

Protokol IGMP (Internet Group Management Protocol) je protokol, který spravuje členství hostitelů ve *skupině vícesměrového přenosu*. Skupina vícesměrového přenosu, známá též jako *skupina hostitelů*, je množinou hostitelů, kteří sledují provoz IP směrovaný na určitou adresu vícesměrového vysílání. Provoz adres vícesměrového vysílání je směrován na jednu MAC adresu, ale zpracováván mnoha IP hostiteli. Určitý hostitel sleduje určitou adresu IP vícesměrového vysílání a dostává všechny pakety směrované na tuto adresu IP. Zde jsou uvedeny některé další aspekty vícesměrového vysílání:

- Členství ve skupině hostitelů je dynamické, hostitelé mohou do skupiny přibývat a odcházet z ní kdykoli.
- Skupina hostitelů může být libovolně velká.
- Členové skupiny hostitelů mohou být rozmístěny pomocí IP směrovačů i ve vzdálených sítích. Tato situace vyžaduje podporu vícesměrového vysílání na IP směrovačích a schopnost hostitelů registrovat jejich členství ve skupině na lokálních směrovačích. Hostitelská registrace se provádí právě pomocí protokolu IGMP.
- Hostitel může zaslat provoz na jakoukoli adresu vícesměrového vysílání bez toho, že by musel náležet k příslušné skupině hostitelů.

Má-li hostitel přijmout adresu vícesměrového vysílání, musí být o tomto jeho IP protokol informován. Podporuje-li příslušná síťová technologie hardwarový multicasting, postoupí síťové rozhraní pakety určité IP adrese. U Ethernetu je síťový adaptér naprogramován tak, že reaguje na MAC adresy odpovídající specifickým IP adresám vícesměrového vysílání.

Hostitel podporuje vícesměrové vysílání na jedné z následujících úrovní:

- Úroveň 0: Žádná podpora vícesměrového provozu, ani zasílání, ani přijímání.
- Úroveň 1: Podpora zasílání, ale nikoli přijímání.
- Úroveň 2: Podpora jak zasílání, tak přijímání. Tuto úroveň podporují TCP/IP jak ve Windows 2000, tak Windows NT 3.5 a pozdější.

Protokolem k registraci skupin hostitelů je IGMP, který je vyžadován všemi hostiteli, kteří podporují druhou úroveň. Pakety IGMP jsou zasílány s použitím IP hlavičky.

Zprávy IGMP mají dvě podoby:

- Při přibytí hostitele do skupiny hostitelů zasílá tento hostitel hlášení o členství na adresu vícesměrového vysílání společnou všem hostitelům (224.0.0.1) nebo na určitou adresu IP. Tímto hlášením prokazuje své členství v určité skupině hostitelů odkazem na adresu vícesměrového vysílání.
- Při průzkumu sítě prováděném směrovačem za účelem zjištění, zda se zde nacházejí nějakí členové určité skupiny hostitelů, zasílá členům dotaz na adresu společnou všem hostitelům. Neobdrží-li směrovač po několika takových výzvěch žádnou odpověď, předpokládá se, že pro tuto síť neexistuje žádné členství v takové skupině a přestane podávat informace o této skupině dalším směrovačům.

Pro vícesměrové vysílání po směrovaných sítích používají směrovače k předávání informací o skupině hostitelů vícesměrové směrovací protokoly. Tak uvědomují všechny směrovače podporující vícesměrové předávání o tom, které síť obsahují členy té které skupiny hostitelů.

Protokol IGMP je definován v RFC 1112 a 2236.

Protokol TCP

Protokol TCP je spolehlivá doručovací spojovaná služba. Data jsou přenášena v segmentech. „Spojovaná služba“ znamená, že před výměnou dat mezi hostiteli musí být ustaveno spojení. Spolehlivost je dosažena přiřazením pořadového čísla každému přenášenému segmentu, přičemž přijetí všech segmentů dalším hostitelem se ověřuje potvrzením jejich přijetí. U každého odeslaného segmentu musí během určité doby přijímající hostitel vrátit potvrzení (ACK) přijatých bajtů. Nedojde-li potvrzení, jsou data přenesena znovu. Protokol TCP je definován v RFC 793.

Protokol TCP používá komunikaci na bázi bajtových proudů, v níž jsou data TCP segmentu považována za sled bajtů bez hranic záznamů. V tabulce 1.6 najdete popis klíčových polí hlavičky TCP.

Tabulka 1.6 Klíčová pole v TCP hlavičce

Pole	Funkce
Zdrojový port	TCP port odesilatele.
Port místa určení	TCP port příjemce.
Pořadové číslo	Pořadové číslo prvního bajtu v TCP segmentu.
Číslo potvrzení	Pořadové číslo bajtu, který odesílatel očekává jako další od druhé komunikující strany.
Okno	Aktuální velikost TCP vyrovnávací paměti na hostiteli odesílajícím TCP segment určené k ukládání příchozích segmentů.
TCP kontrola	Ověřuje integritu TCP hlavičky a TCP dat.

TCP porty

TCP port zajišťuje „místo“ pro doručování TCP segmentů. Porty s čísly pod 1024 jsou dobře známými porty a jsou přiřazovány organizací IANA (Internet Assigned Numbers Authority). V tabulce 1.7 najdete několik známých TCP portů.

Tabulka 1.7 Znamé TCP porty

Číslo TCP portu	Popis
20	FTP (datový kanál)
21	FTP (řídící kanál)
23	Telnet
80	HTTP používaný pro Web
139	Služba relace NetBIOS

Úplný seznam přiřazených TCP portů najdete pod odkazem IANA Port Numbers na <http://windows.microsoft.com/windows2000/reskit/webresources>.

TCP třicestné vyjednávání

TCP spojení je inicializováno přes třicestné vyjednávání. Jejím účelem je synchronizace pořadového čísla a potvrzovacích čísel obou stran spojení a výměna velikosti TCP oken. Tento proces je vymezen následujícími kroky:

1. Klient pošle na server TCP segment s počátečním pořadovým číslem pro připojení a velikostí okna označující velikost vyrovnávací paměti klienta určené k ukládání segmentů přicházejících ze serveru.
2. Server odešle zpět TCP segment obsahující počáteční pořadové číslo vybrané serverem, potvrzení klientského pořadového čísla a velikost okna označujícího velikost vyrovnávací paměti serveru určené k ukládání segmentů přicházejících od klienta.
3. Klient pošle na server TCP segment obsahující potvrzení pořadového čísla serveru.

K ukončení spojení používá TCP obdobný proces. Tím je zaručeno, že oba hostitelé ukončili přenos a že byla doručena všechna data.

Protokol UDP

Protokol UDP poskytuje datagramovou nespojovanou službu, která nabízí nespolehlivé doručení dat přenášných pomocí zpráv. To znamená, že není zaručeno ani dodání datagramů, ani správné seřazení doručených paketů. Protokol UDP neobnovuje ztracená data jejich opětovným přenosem a je definován v RFC 768.

Protokol UDP je používán aplikacemi, které nevyžadují potvrzení přijetí dat a které zpravidla přenášejí najednou malý objem dat. Příkladem aplikací a služeb používajících UDP jsou datagramové služby NetBIOS a SNMP. Tabulka 1.8 popisuje klíčová pole hlavičky UDP.

Tabulka 1.8 Klíčová pole UDP hlavičky

Pole	Funkce
Zdrojový port	UDP port odesílatele.
Port místa určení	UDP port příjemce.
Kontrolní součet	Používá se k ověření integrity UDP hlavičky a UDP dat.

UDP porty

Aby aplikace mohla používat protokol UDP, musí dodat adresu IP a číslo UDP portu cílové aplikace. Port poskytuje umístění pro odesílání zpráv. Port funguje jako vícenásobný

sobná fronta zpráv, to znamená, že může přijímat více zpráv najednou. Každý port má vlastní jedinečné identifikační číslo. Je důležité poznamenat, že UDP porty jsou odlišné a oddělené od TCP portů, i když některé z nich používají stejná čísla. V tabulce 1.9 najdete známé UDP porty.

Tabulka 1.9 Známé UDP porty

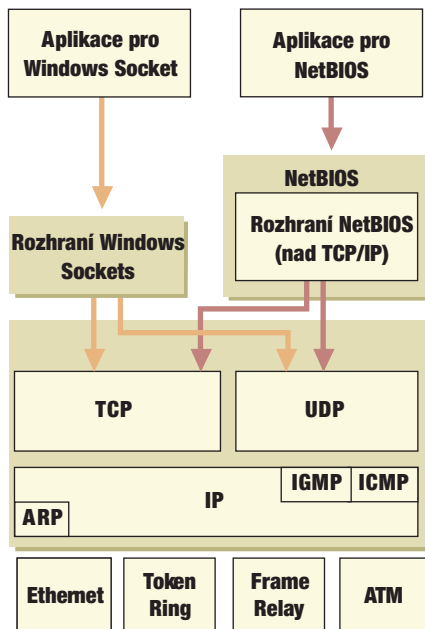
Číslo UDP portu	Popis
53	DNS (Domain Name System)
69	TFTP (Trivial File Transfer Protocol)
137	Překlad názvů NetBIOSu
138	Datagramová služba NetBIOSu
161	SNMP

Úplný seznam přiřazených UDP portů najdete pod odkazem IANA Port Numbers na.

Rozhraní aplikací TCP/IP

Aby mohly aplikace přistupovat ke službám nabízeným základními TCP/IP protokoly standardně, umožňují síťové operační systémy jako Windows 2000 použití standardního programového rozhraní, tedy sad funkcí a příkazů, které jsou programově volány kódem aplikace k provádění síťových funkcí. Například, aplikace webového prohlížeče, která se připojuje na webové server, potřebuje přístup ke službě TCP ustavující spojení.

Na obrázku 1.2 jsou znázorněna dvě běžná TCP/IP síťová rozhraní, Windows Sockets a NetBIOS a jejich vztah k základním protokolům.



Obrázek 1.2 API pro TCP/IP

Rozhraní Windows Sockets

Rozhraní Windows Sockets je standardním API pod Windows 2000 pro aplikace, které používají protokoly TCP a UDP. Aplikace napsané pod tímto rozhraní je možné provozovat na mnoha verzích TCP/IP. Příkladem aplikací napsaných podle tohoto rozhraní jsou nástroje TCP/IP a služba SNMP.

Rozhraní Windows Sockets zajišťuje služby umožňující aplikacím připojit se na určitý port a adresu IP hostitele, navázat a akceptovat spojení, posílat a přijímat data a uzavírat spojení. Existují dva typy soketů:

1. *Proudový* poskytuje dvoucestný, spolehlivý, seřazený a neduplikovaný proud dat používajících TCP.
2. *Datagramový* poskytuje obousměrný proud dat používajících UDP.

Soket je definován protokolem a adresou na hostiteli. Formát adresy se liší podle protokolu. U TCP/IP je adresa kombinací adresy IP a portu. Dva sokety, jeden pro každý konec spojení, tvoří obousměrnou komunikační cestu.

Ke komunikaci určuje aplikace protokol, adresu IP cíle a port cílové aplikace. Po připojení aplikace mohou být posílána a přijímána data.

Rozhraní NetBIOS

Rozhraní NetBIOS bylo vyvinuto pro společnost IBM v roce 1983 firmou Sytek Corporation s cílem umožnit komunikovat aplikacím přes síť. Rozhraní NetBIOS definuje dvě entity – rozhraní úrovně relace a protokol správy relace a přenosu dat.

Rozhraní NetBIOS je standardní API pro uživatelské aplikace určené pro správu síťového vstupu a výstupu a řízení příkazů podřízeným programům síťového protokolu. Aplikací program, který k síťové komunikaci používá API s rozhraním NetBIOS, může být spuštěn na jakémkoli protokolu podporujícím toto rozhraní.

NetBIOS také definuje protokol, který funguje na relační/transportní vrstvě. Tento protokol je implementován pomocí podřízeného software protokolu (například NetBIOS Frames Protocol (NBFP), komponenta NetBEUI nebo NetBIOS nad TCP/IP (NetBIOS over TCP/IP, NetBT)), a to za účelem realizace síťových vstupů a výstupů tak, aby odpovídaly sadě příkazů rozhraní NetBIOS. Rozhraní NetBIOS nad TCP/IP je definován v RFC 1001 a 1002.

NetBIOS nabízí příkazy a podporu správy názvů NetBIOS (NetBIOS Name Management), datagramům NetBIOS (NetBIOS Datagrams) a relacím NetBIOS (NetBIOS Sessions).

Správa názvů NetBIOS (NetBIOS Name Management)

Správa názvů poskytují následující funkce:

- Registrace názvů a jejich uvolňování

Při své inicializaci si TCP/IP hostitel zaregistruje své názvy NetBIOSu tím, že žádost o registraci takového názvu pošle na názvový server (NetBIOS Name Server), jako je například WINS server (Windows Internet Name Service). Jestliže si jiný hostitel zaregistroval stejný název, přímo tento hostitel nebo NetBIOS Name Server reaguje na registraci dotčeného jména negativně. Inicializující hostitel tak obdrží hlášení o inicializační chybě.

Po ukončení používání názvu nepokračuje hostitel ve vysílání negativní odpovědi na registraci názvu, a to v případě, že někdo jiný zkouší použít stejný název, a po-

šle na NetBIOS Name Server uvolnění takového názvu. V takovém případě se název uvolní a je dostupný pro použití jiným hostitelem.

- **Překlad názvů**

Jestliže chce aplikace využívající rozhraní NetBIOS komunikovat s jinou aplikací využívající stejné rozhraní, musí být nejdříve vyhodnoceny adresy IP dané aplikace. NetBT vykonává tuto funkci buď pomocí všesměrového vysílání dotazu na název na lokální síť nebo zaslání dotazu na NetBIOS Name Server.

Více informací o překladu názvů najdete v dalších částech této kapitoly.

Uvedená služba správy názvů využívá UDP port 137.

Datagramy NetBIOSu

Tato služba zajišťuje doručení datagramů, které jsou nespojované, neseřazené a nespolehlivé. Datagramy mohou být směrovány na určitý NetBIOS název nebo vysílány na skupinu názvů. Doručení je nespolehlivé, protože zprávy dostanou pouze uživatelé přihlášení v síti. Datagramová služba může iniciovat i přijímat jak všesměrově vysílané, tak jednosměrně vysílané zprávy. Tato služba používá UDP port 138.

Relace NetBIOSu

Tato služba zajišťuje doručení zpráv rozhraní NetBIOS, které jsou spojované, seřazené a spolehlivé. Relace používají spojení TCP a poskytují ustavení relace, jeho udržování a ukončení. Tato služba nabízí souběžný přenos dat oběma směry, a to za použití TCP portu 139.

IP adresování

Každý hostitel TCP/IP je identifikován pomocí logické *adresy IP*. adresa IP je adresa síťové vrstvy a není závislá na adrese vrstvy datového spoje (jako například MAC adresa síťového adaptéru). Pro každého hostitele a síťovou komponentu komunikující pomocí TCP/IP je nutná jedinečná adresa IP.

adresa IP určuje umístění systému na síti stejným způsobem, jako číslo domu určuje umístění domu na ulici. Stejně jako normální adresa musí určovat jedinečný dům, i adresa IP musí být jedinečná a mít jednotný formát.

Každá adresa IP obsahuje ID sítě a ID hostitele.

- *ID sítě* (známé též jako *síťová adresa*) identifikuje systémy, které jsou umístěné na stejné fyzické síti ohraničené IP směrovači. Všechny systémy na stejné fyzické síti musí mít stejné ID sítě. ID sítě musí být mezi sítěmi jedinečné.
- *ID hostitele* (známé též jako *adresa hostitele*) identifikuje pracovní stanici, server, směrovač nebo jiného TCP/IP hostitele v síti. ID každého hostitele musí být jedinečné a odlišné od ID sítě.

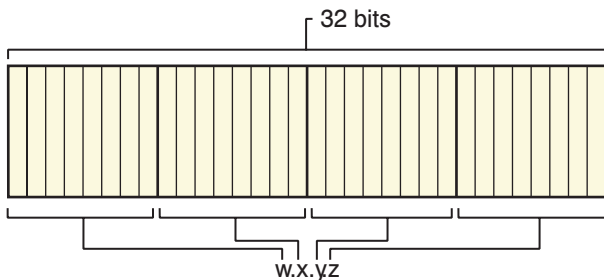
Poznámka: ID sítě znamená ID kterékoli IP sítě, bez ohledu na to, zda se jedná o síť pařící do třídy, podsítě či nadsítě. .

Adresa IP se sestává ze 32 bitů. Spíše než se všemi 32 bity najednou se zpravidla používá členění na 8bitové segmenty nazvané *oktety*. Každý oktet je převáděn na desítkové číslo (číslo v desítkové soustavě) v rozsahu 0 až 255 a oddělen tečkou. Tento formát se nazývá desítkovým zápisem či desítkovým zápisem s tečkou. V tabulce 1.10 najdete příklad adresy IP jak ve dvojkovém, tak v desítkovém formátu.

Tabulka 1.10 adresa IP ve dvojkovém a v desítkovém formátu

Dvojkový zápis	Desítkový zápis
11000000 10101000 00000011 00011000	192.168.3.24

Při odkazování na obecnou adresu IP je použito označení w.x.y.z (viz obr. 1.3).

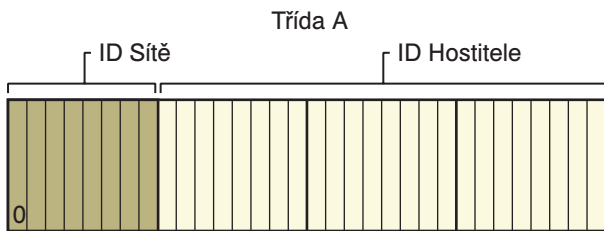
**Obrázek 1.3** Adresa IP

Třídy adres

V rámci Internetu bylo původně definováno pět adresových tříd, které náležely sítím různých velikostí. Microsoft TCP/IP podporuje adresy tříd A, B a C přiřazené hostitelům. Třída adresy určuje, které bity jsou použity pro ID sítě a které bity jsou použity pro ID hostitele. Určuje také možné množství sítí a množství hostitelů v síti.

Třída A

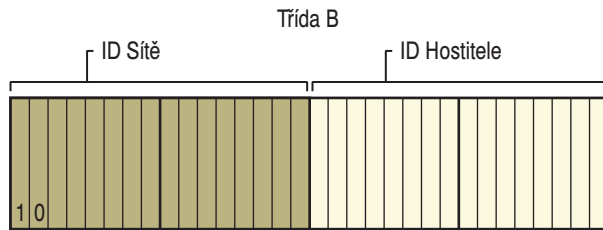
Adresy *třídy A* jsou přiřazovány sítím s velmi vysokým počtem hostitelů. Nejvýznamnější bit je v adrese třídy A vždy nastaven na nulu. Následujících sedm bitů (dokončujících první oktet) tvoří ID sítě. Zbývajících 24 bitů (poslední tři oktety) reprezentují ID hostitele. To umožňuje použití pro 126 sítí a 16.777.214 hostitelů na jednu síť. Na obrázku 1.4 je znázorněna struktura adres třídy A.

**Obrázek 1.4** Adresy IP třídy A

Třída B

Adresy *třídy B* jsou přiřazovány středně velkým až velkým sítím. Dva nejvýznamnější bity jsou v adrese třídy B vždy nastaveny na hodnotu 1 0. Následujících čtrnáct bitů (dokončujících první dva oktety) tvoří ID sítě. Zbývajících 16 bitů (poslední dva okte-

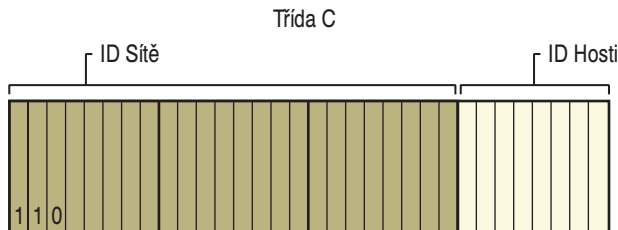
ty) reprezentují ID hostitele. To umožňuje použití pro 16.384 sítí a 65.534 hostitelů na jednu síť. Na obrázku 1.5 je znázorněna struktura adres třídy B.



Obrázek 1.5 Adresy IP třídy B

Třída C

Adresy třídy C jsou přiřazovány malým sítím. Tři nejvýznamnější bity jsou v adrese třídy C vždy nastaveny na hodnotu 1 1 0. Následujících 21 bitů (dokončujících první tři oktety) tvoří ID sítě. Zbývajících 8 bitů (poslední oktet) reprezentuje ID hostitele. To umožňuje použití pro 2.097.152 sítí a 254 hostitelů na jednu síť. Na obrázku 1.6 je znázorněna struktura adres třídy C.



Obrázek 1.6 Adresy IP třídy C

Třída D

Adresy třídy D jsou vyhrazeny adresám IP pro vícesměrové vysílání. Čtyři nejvýznamnější bity jsou v adrese třídy D vždy nastaveny na hodnotu 1 1 1 0. Zbývajících bity jsou vyhrazeny pro adresu, kterou rozpoznají zainteresovaní hostitelé. Microsoft podporuje adresy třídy D pro aplikace umožňující vícesměrové vysílání dat.

Třída E

Třída E je pokusná adresa vyhrazená pro budoucí použití. Nejvýznamnější bity jsou v adresách třídy E nastaveny na hodnotu 1111.

Tabulka 1.11 obsahuje souhrn adresových tříd A, B a C, které mohou být použity pro adresy IP hostitelů.

Tabulka 1.11 Třídy IP adres

Třída	Hodnota w¹	Část pro ID sítě	Část pro ID hostitele	Počet sítí	Počet hostitelů
A	1 – 126	w	x.y.z	126	16.777.214
B	128 – 191	w.x	y.z	16.384	65.534
C	192 – 223	w.x.y	z	2.097.152	254

¹ Adresa třídy A 127.x.y.z je vyhrazena pro testování zpětné smyčky a komunikaci mezi procesy na lokálním počítači.

Pravidla pro ID sítě

ID sítě určuje TCP/IP hostitele, kteří jsou umístěni na stejné fyzické síti. Všichni hostitelé na jedné fyzické síti musí mít přiřazené stejné ID sítě, aby byli schopni mezi sebou komunikovat.

Při přiřazování ID sítě dodržujte tato pravidla:

- ID sítě musí být vůči svému okolí jedinečné. Plánujete-li přímé směrované připojení na Internet, musí být ID v rámci Internetu jedinečné. Neplánujete-li připojení na veřejný Internet, musí být ID lokální sítě jedinečné v rámci vaší soukromé sítě.
- ID sítě nemůže začínat číslem 127. Číslo 127 je v adresách třídy A vyhrazeno pro interní funkce zpětné smyčky.
- Všechny bity v rámci ID sítě nemohou být nastaveny na 1. Použití všech 1 v ID sítě je vyhrazeno pro použití jako adresa všesměrového vysílání.
- Všechny bity v rámci ID sítě nemohou být nastaveny na 0. Použití všech 0 v ID sítě je vyhrazeno pro označení určitého hostitele v lokální síti a nejsou směrovány.

Tabulka 1.12 obsahuje platné rozsahy ID sítí založených na třídách IP adres. K označení ID sítí jsou všechny bity hostitele nastaveny na 0. Všimněte si, že přestože je ID sítě vyjádřeno v desítkovém formátu, není to adresa IP.

Tabulka 1.12 Rozsahy tříd ID sítě

Třída adresy	První ID sítě	Poslední ID sítě
Třída A	1.0.0.0	126.0.0.0
Třída B	128.0.0.0	191.255.0.0
Třída C	192.0.0.0	223.255.255.0

Pravidla pro ID hostitele

ID hostitele určuje TCP/IP hostitele v rámci sítě. Kombinace ID sítě a ID hostitele je IP adresou.

Při přiřazování ID hostitele dodržujte tato pravidla:

- ID hostitele musí být odlišné od ID sítě
- Všechny bity v rámci ID hostitele nemohou být nastaveny na 1, protože toto ID hostitele je vyhrazeno jako všesměrová vysílací adresa pro posílání paketů všem hostitelům na síti.

- Všechny bity v rámci ID hostitele nemohou být nastaveny na 0, protože toto ID hostitele je vyhrazeno jako označení ID sítě.

Tabulka 1.13 obsahuje platné rozsahy ID hostitele založených na třídách IP adres.

Tabulka 1.13 Rozsahy tříd ID hostitele

Třída adresy	První ID hostitele	Poslední ID hostitele
Třída A	w.0.0.1	w.255.255.254
Třída B	w.x.0.1	w.x.255.254
Třída C	w.x.y.1	w.x.y.254

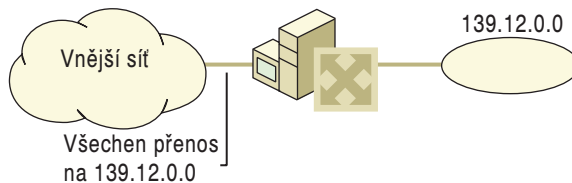
Podsítě a masky podsítí

Třídy internetových adres odpovídají třem stupňům IP sítí, kde je 32 bitů adresy IP rozděleno mezi ID sítě a ID hostitele v závislosti na tom, kolik je třeba sítí a kolik hostitelů na síti. Nicméně podívejte se na ID sítě třídy A, které může umístit více než 16 milionů hostitelů na jedné síti. Všichni hostitelé na jedné fyzické síti svázané IP směrovači sdílejí stejný všesměrový vysílací provoz, jsou ve stejné všesměrově vysílací doméně. Není praktické mít 16 milionů uzlů v jedné doméně – výsledkem je to, že většina z oněch 16 milionů hostitelských adres je nepřiraditelná a tedy proplývaná. Dokonce i síť třídy B se 65 tisíci hostiteli je nepraktická.

Při snaze vytvořit menší všesměrově vysílací domény a lépe využít bity v ID hostitele lze IP síť rozdělit na menší sítě, přičemž každá z nich je ohraničena IP směrovačem a má přiřazené nové ID podsítě, které je částí původního síťového ID založeného na třídách.

Tím se vytvoří podsítě, pododdíly IP sítě, každá s vlastním jedinečným ID podsítě. Tato ID jsou tvořena pomocí bitů z části hostitelského ID původního ID sítě založeného na třídách.

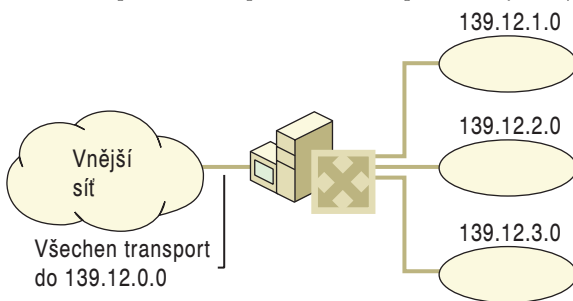
Podívejte se na příklad na obrázku 1.7. Síť třídy B 139.12.0.0 může mít až 65.534 uzlů. To je příliš mnoho a ve skutečnosti se současná síť začíná přesycovat provozem. Podsíťování (rozdělení) sítě 139.12.0.0 by mělo být provedeno tak, že se to nijak nedotýká rekonfigurace zbytku IP sítě a ani ji nijak nevyžaduje.



Obrázek 1.7 Síť 139.12.0.0 před rozdělením

Síť 139.12.0.0 je rozdělena pomocí využití prvních osmi hostitelských bitů (třetí oktet) pro nové ID podsítě. Po rozdělení sítě 139.12.0.0 (viz obrázek 1.8) jsou vytvořeny samostatné sítě s vlastními ID podsítí (139.12.1.0, 139.12.2.0, 139.12.3.0). Směrovač registruje ID samostatných podsítí a směruje IP pakety na příslušnou podsít.

Všimněte si, že zbytek IP sítě stále považuje všechny uzly na těchto třech podsítích jako součást sítě 139.12.0.0. Ostatní směrovače na IP síti neregistrují, že bylo na síti 139.12.0.0 provedeno „podsíťování“ a proto nevyžadují žádnou rekonfiguraci.



Obrázek 1.8 Síť 139.12.0.0 po rozdělení

Stále ovšem chybí klíčový prvek takového procesu. Jak směrovač, který rozděljuje síť 139.12.0.0, pozná, že tato síť je rozdělena, a jak pozná, které podsítě jsou dostupné na kterém rozhraní směrovače? Aby IP uzly získaly tuto novou úroveň znalosti, musí se dozvědět zcela přesně, jak rozlišovat ID nových podsítí nezávisle na třídách internetových adres. To, jestli se jedná o třídní nebo podsíťové ID, sděluje IP uzlu *maska podsítě*.

Masky podsítě

S příchodem podsítí se už nikdo nemusí více spoléhat na definice tříd IP adres, aby určil ID sítě v IP adrese. K určení, která část adresy IP je ID sítě a která část ID hostitele, bez ohledu na to, zda se jedná o třídní nebo podsíťové ID sítě, je třeba nová hodnota.

Masky podsítě (též adresová maska) definuje RFC 950 jako 32bitovou hodnotu, která je používána k odlišení ID sítě od ID hostitele v jakékoli IP adrese. Bity masky jsou určeny následujícím způsobem:

- Všechny bity, které odpovídají ID sítě, jsou nastaveny na 1.
- Všechny bity, které odpovídají ID hostitele, jsou nastaveny na 0.

Každý hostitel na TCP/IP síti vyžaduje masku podsítě dokonce i jen na jednotlivý segment sítě. Na každém TCP/IP uzlu je nakonfigurována buď přednastavená maska, která se používá při použití třídního ID sítě, nebo upravená maska, která se používá při rozdělování nebo slučování sítí.

Desítkový zápis masky podsítě

Masky jsou často vyjadřovány desítkovým zápisem (s tečkou). Po nastavení bitů na ID sítě a ID hostitele je výsledné 32bitové číslo převedeno do desítkového formátu. Všimněte si, že i když je maska podsítě vyjádřena v desítkovém formátu, není to adresa IP. Přednastavená maska podsítě je založena na třídách IP adres a používá se na TCP/IP sítích, které nejsou rozděleny do podsítí. Tabulka 1.14 obsahuje seznam přednastavených masek v desítkovém formátu.

Tabulka 1.14 Přednastavené masky (Desítkový záznam)

Třída adres	Dvojkový zápis	Desítkový zápis
Třída A	11111111 00000000 00000000 00000000	255.0.0.0
Třída B	11111111 11111111 00000000 00000000	255.255.0.0
Třída C	11111111 11111111 11111111 00000000	255.255.255.0

Upravené masky jsou ty, které se odlišují od přednastavených masek při rozdělování nebo slučování sítí. Například 138.96.58.0 je 8bitové ID podsítě třídy B. Osm bitů třídového ID hostitele se používá k vyjádření ID podsítě. Masku podsítě používá celkem 24 bitů (255.255.255.0), kterými definuje ID podsítě. ID podsítě a jeho odpovídající maska je potom vyjádřena v desítkovém zápisu (s tečkou) takto:

138.96.58.0, 255.255.255.0

Zápis pomocí síťové předpony

Vzhledem k tomu, že bity ID sítě musí být vždy vybírány v sestupném pořadí, existuje u masek podsítí zkrácený způsob označení počtu bitů, které určují ID sítě, a to tzv. síťová předpona používající zápis: /počet_bitů. Tabulka 1.15 obsahuje tento formát zápisu pro přednastavené masky.

Tabulka 1.15 Přednastavené masky – zápis pomocí síťové předpony

Třída adres	Maska podsítě	Síťová předpona
Třída A	11111111 00000000 00000000 00000000	/8
Třída B	11111111 11111111 00000000 00000000	/16
Třída C	11111111 11111111 11111111 00000000	/24

Například ID sítě třídy B 138.96.0.0 s maskou podsítě 255.255.0.0 by bylo pomocí tohoto zápisu vyjádřeno jako 138.96.0.0/16.

Příklad masky podsítě: 138.96.58.0 je 8bitové ID podsítě sítě třídy B. Masku podsítě používá pro definování ID podsítě celkem 24 bitů. ID podsítě a jemu odpovídající maska podsítě je potom vyjádřena v zápise pomocí síťové předpony jako:

138.96.58.0/24

Zápis se síťovou předponou je známý též jako zápis CIDR (Classless Interdomain Routing).

Poznámka: Vzhledem k tomu, že všichni hostitelé na stejné síti musí používat stejné ID sítě, musí všichni hostitelé na stejné síti používat stejné ID sítě definované stejnou maskou podsítě. Například 138.23.0.0/16 není stejné ID sítě jako 138.23.0.0/24. ID sítě 138.23.255.254 zahrnuje řadu platných hostitelských IP adres od 138.23.0.1 do 138.23.255.254. ID sítě 138.23.0.0/24 zahrnuje řadu platných hostitelských IP adres od 138.23.0.1 do 138.23.0.254. Z toho jasně vyplývá, že tato ID sítě nepředstavují stejný rozsah IP adres.

Určování ID sítě

Pro získání ID sítě z jakékoli adresy IP používající jakoukoli masku podsítě používá IP matematickou operaci logického součinu. Při tomto porovnání je výsledek dvou porovnávaných položek pravdivý pouze tehdy, když jsou pravdivé obě porovnávané položky. V opačném případě je výsledek nepravdivý. Při aplikaci tohoto principu na bity je výsledek 1 pouze tehdy, když jsou oba porovnávané bity rovny 1, v opačném případě je výsledek 0.

IP provádí logický součin u 32bitové adresy IP a 32bitové masky podsítě. Výsledkem srovnání adresy IP a masky je ID sítě.

Například, jaké je ID sítě IP uzlu 129.56.189.41 s maskou podsítě 255.255.240.0?

Výsledek dostanete tak, že převedete obě čísla do jejich dvojkové podoby a zapíšete je pod sebe. Pak na každém bitu provedete logický součin a zapíšete výsledek.

10000001 00111000 10111101 00101001 adresa IP

11111111 11111111 11110000 00000000 Maska podsítě

10000001 00111000 10110000 00000000 ID sítě

Výsledek logického součinu 32bitové adresy IP a masky podsítě je ID sítě, tedy 129.56.176.0.

Rozdělování sítě

Přestože je rozdělování sítě (podsíťování) pomocí využití bitů hostitele přímé a jednoduché, skutečný mechanismus je poněkud složitější a probíhá ve třech krocích:

1. Určení počtu bitů hostitele, které budou pro rozdělování použity.
2. Výpočet nových ID podsítí.
3. Výpočet IP adres pro každé nové ID podsítě.

Krok první: Určení počtu bitů hostitele

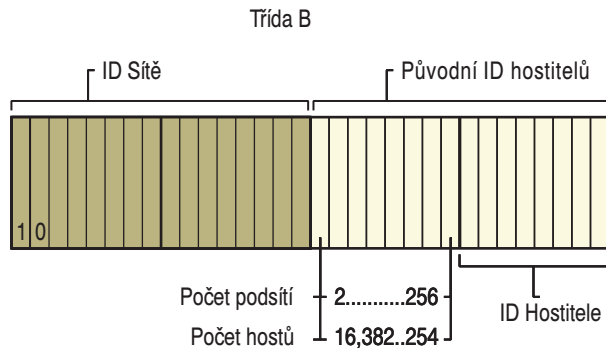
Počet bitů hostitele, které budou použity pro podsítě, určuje možný počet podsítí a hostitelů na každé podsíti. Předtím, než vyberete počet bitů hostitele, byste měli mít dobrou představu o tom, kolik podsítí a kolik hostitelů budete mít v budoucnu. Použijete-li pro masku podsítě více než nezbytný počet bitů, ušetříte si tím opětovné přiřazování IP adres v budoucnosti.

Čím více použijete bitů, tím více podsítí (ID podsítí) můžete mít – ovšem s menším počtem hostitelů. Použijete-li příliš mnoho bitů hostitele, umožníte růst počtu podsítí, ale omezíte počet jejich hostitelů. Použijete-li málo hostitelů, umožníte růst počtu hostitelů, ale omezíte růst počtu podsítí.

Například obrázek 1.9 znázorňuje rozdělení až do prvních osmi bitů hostitele sítě třídy B. Vyberete-li si jeden bit, dostanete dvě ID podsítí s 16.382 hostiteli na jednu podsít. Vyberete-li si 8 bitů, dostanete 256 podsítí s 254 hostiteli na každé ID.

Ve skutečnosti si síťový administrátor definuje maximální počet uzlů, které chce mít na jedné síti. Nezapomínejte, že všechny uzly na stejné síti sdílejí stejný všesměrově vysílací provoz, sídlí ve stejné všesměrově vysílací doméně. Proto je růstu počtu podsítí dávána přednost před růstem počtu hostitelů na jedné podsíti.

Při určování počtu bitů hostitele používaných pro rozdělování dodržujte následující pravidla:



Obrázek 1.9 Rozdělení sítě třídy B

1. Určete si, kolik podsítí potřebujete nyní a kolik jich budete potřebovat v budoucnu. Každá fyzická síť je podsítí. Spojení rozlehlých sítí lze též počítat za podsítě v závislosti na tom, zda vaše směrovače podporují nečíslovaná připojení.
2. Použijte další bity pro masku podsítě, pokud:
 - Nikdy nebudete požadovat tolik hostitelů na jednu podsít, kolik je dovoleno počtem zbývajících bitů.
 - Počet podsítí se bude v budoucnu zvyšovat a vyžadovat proto další bity hostitele.

Při určování schématu rozdělování vycházejte ze stávajícího ID sítě, které má být rozděleno. Takové ID sítě může být třídové ID sítě, ID podsítě nebo nadsítě. Stávající ID sítě obsahuje sadu bitů ID sítě, které jsou pevné, a sadu bitů ID hostitele, které jsou proměnné. V závislosti na vašich požadavcích na počet podsítí a počet jejich hostitelů vyberte určitý počet bitů hostitele, které budou použity pro rozdělení.

Tabulka 1.16 znázorňuje rozdělení sítě třídy A. Schéma lze vybrat na základě požadovaného počtu podsítí a maximálního počtu hostitelů v každé síti.

Tabulka 1.16 Rozdělení sítě třídy A

Požadovaný počet podsítí	Počet bitů podsítě	Maska podsítě	Počet hostitelů na jednotlivé podsíti
1-2	1	255.128.0.0 nebo /9	8,388,606
3-4	2	255.192.0.0 nebo /10	4,194,302
5-8	3	255.224.0.0 nebo /11	2,097,150
9-16	4	255.240.0.0 nebo /12	1,048,574
17-32	5	255.248.0.0 nebo /13	524,286
33-64	6	255.252.0.0 nebo /14	262,142
65-128	7	255.254.0.0 nebo /15	131,070
129-256	8	255.255.0.0 nebo /16	65,534
257-512	9	255.255.128.0 nebo /17	32,766
513-1,024	10	255.255.192.0 nebo /18	16,382
1,025-2,048	11	255.255.224.0 nebo /19	8,190
2,049-4,096	12	255.255.240.0 nebo /20	4,094

Požadovaný počet podsítí	Počet bitů podsítě	Maska podsítě	Počet hostitelů na jednotlivé podsíti
4,097-8,192	13	255.255.248.0 nebo /21	2,046
8,193-16,384	14	255.255.252.0 nebo /22	1,022
16,385-32,768	15	255.255.254.0 nebo /23	510
32,769-65,536	16	255.255.255.0 nebo /24	254
65,537-131,072	17	255.255.255.128 nebo /25	126
131,073-262,144	18	255.255.255.192 nebo /26	62
262,145-524,288	19	255.255.255.224 nebo /27	30
524,289-1,048,576	20	255.255.255.240 nebo /28	14
1,048,577-2,097,152	21	255.255.255.248 nebo /29	6
2,097,153-4,194,304	22	255.255.255.252 nebo /30	2

Tabulka 1.17 znázorňuje rozdělení sítě třídy B.

Tabulka 1.17 Rozdělení sítě třídy B

Požadovaný počet podsítí	Počet bitů podsítě	Maska podsítě	Počet hostitelů na jednotlivé podsíti
1-2	1	255.255.128.0 nebo /17	32,766
3-4	2	255.255.192.0 nebo /18	16,382
5-8	3	255.255.224.0 nebo /19	8,190
9-16	4	255.255.240.0 nebo /20	4,094
17-32	5	255.255.248.0 nebo /21	2,046
33-64	6	255.255.252.0 nebo /22	1,022
65-128	7	255.255.254.0 nebo /23	510
129-256	8	255.255.255.0 nebo /24	254
257-512	9	255.255.255.128 nebo /25	126
513-1,024	10	255.255.255.192 nebo /26	62
1,025-2,048	11	255.255.255.224 nebo /27	30
2,049-4,096	12	255.255.255.240 nebo /28	14
4,097-8,192	13	255.255.255.248 nebo /29	6
8,193-16,384	14	255.255.255.252 nebo /30	2

Tabulka 1.18 znázorňuje rozdělení sítě třídy C.

Tabulka 1.18 Rozdělení sítě tříd

Požadovaný počet podsítí	Počet bitů podsítě	Maska podsítě	Počet hostitelů na jednotlivé podsíti
1-2	1	255.255.255.128 nebo /25	126
3-4	2	255.255.255.192 nebo /26	62
5-8	3	255.255.255.224 nebo /27	30

Požadovaný počet podsítí	Počet bitů podsítě	Maska podsítě	Počet hostitelů na jednotlivé podsíti
9-16	4	255.255.255.240 nebo /28	14
17-32	5	255.255.255.248 nebo /29	6
33-64	6	255.255.255.252 nebo /30	2

Krok druhý: Výpočet ID podsítí

V závislosti na počtu bitů hostitele používaných pro rozdělování musíte sestavit nová ID podsítě. Existují dva základní přístupy:

- Dvojkový – sestavit všechny možné kombinace bitů vybraných pro rozdělení a převést každou kombinaci do desítkového formátu s tečkou.
- Desítkový – Přidat vypočítaný přírůstek ke každému dalšímu ID podsítě a převést ho do desítkového formátu s tečkou.

Obě metody mají tentýž výsledek, tedy seznam všech ID podsítě.

Poznámka: Pro rozdělování existuje celá řada dokumentovaných zkrácených metod. Nicméně ty fungují pouze za určitých omezení (například pouze do osmi bitů třídového ID sítě). Dále popsané metody jsou navrženy tak, aby fungovaly za jakékoli situace (třídové ID, více než osm bitů, vytváření nadsítí, rozdělování sítí různé délky).

► Výpočet ID podsítě za použití dvojkové metody

1. V závislosti na n , počtu bitů hostitele vybraných pro rozdělení, vytvořte třísloupcovou tabulku se $2n$ řádky. V prvním sloupci jsou čísla podsítě (počínající 1), ve druhém sloupci je dvojkové vyjádření ID podsítě a ve třetím sloupci je desítkové vyjádření ID podsítě.

V každém dvojkovém formátu jsou bity podsítě přiřazeny odpovídajícím hodnotám a zbývající bity hostitele jsou všechny nastaveny na 0. Bity hostitele vybrané pro rozdělení se různí.

2. V prvním řádku tabulky nastavte všechny bity podsítě na 0 a převedte do desítkového formátu. Původní ID sítě je rozdělováno se svou novou maskou podsítě.
3. V dalším řádku tabulky zvyšte hodnotu bitů podsítě.
4. Převedte dvojkový výsledek na desítkový formát.
5. Opakujte kroky 3 a 4 až do dokončení tabulky.

Vytvořte například 3bitovou podsít' ID soukromé sítě 192.168.0.0. Masku podsítě pro nové podsítě je 255.255.224.0 nebo /19. V závislosti na tom, že $n = 3$, vytvořte tabulku s 8 (=2³) řádky. Řádek pro podsít' 1 je všude nastaven na 0. Další řádky v tabulce jsou postupně přírůstky bitů podsítě, viz tabulka 1.19. Bity hostitele použité pro rozdělování jsou podtrženy.

Tabulka 1.19 Dvojková metoda rozdělování pro ID sítě 192.168.0.0

Podsít'	Dvojkový zápis	ID podsítě
1	11000000.10101000.00000000.00000000	192.168.0.0/19
2	11000000.10101000.00100000.00000000	192.168.32.0/19

Podsít'	Dvojkový zápis	ID podsítě
3	11000000.10101000.01000000.00000000	192.168.64.0/19
4	11000000.10101000.01100000.00000000	192.168.96.0/19
5	11000000.10101000.10000000.00000000	192.168.128.0/19
6	11000000.10101000.10100000.00000000	192.168.160.0/19
7	11000000.10101000.11000000.00000000	192.168.192.0/19
8	11000000.10101000.11100000.00000000	192.168.224.0/19

► **Výpočet ID podsítě za použití desítkové metody**

1. V závislosti na n , počtu bitů hostitele vybraných pro rozdělení, vytvořte tříslopcovou tabulku se $2n$ řádky. V prvním sloupci jsou čísla podsítě (počínající 1), ve druhém sloupci je desítkové vyjádření (základem je číslo 10) 32bitového ID podsítě a ve třetím sloupci je desítkové vyjádření (s tečkou) ID podsítě.

2. Převedte ID sítě ($w.x.y.z$) z desítkového formátu do N , desítkového vyjádření 32bitového ID sítě:

$$N = w*16777216 + x*65536 + y*256 + z$$

3. Vypočítejte přírůstkovou hodnotu I založenou na h , počtu zbývajících bitů hostitele:

$$I = 2h$$

4. V prvním řádku tabulky je desítkové vyjádření ID podsítě N a ID podsítě je $w.x.y.z$ se svou novou maskou podsítě.
5. V dalším řádku tabulky přičtete k výše uvedenému desítkovému vyjádření I .
6. Převedte desítkové vyjádření ID podsítě na desítkový formát ($W.X.Y.Z$), a to pomocí následujícího vzorce (kde s je desítkové vyjádření ID podsítě):

$$W = \text{INT}(s/16777216)$$

$$X = \text{INT}((s \bmod(16777216))/65536)$$

$$Y = \text{INT}((s \bmod(65536))/256)$$

$$Z = s \bmod(256)$$

7. Opakujte kroky 5 a 6 až do dokončení tabulky.

Vytvořte například 3bitovou podsít' ID soukromé sítě 192.168.0.0. V závislosti na tom, že $n = 3$, vytvořte tabulku s 8 (=23) řádky. Řádek pro podsít' 1 je všude nastaven na 0. N , desítkové vyjádření 192.168.0.0, je 3232235520, výsledek výpočtu $192*16777216 + 168*65536$. Vzhledem k tomu, že zbývá 13 bitů, je přírůstek I $2^{13} = 8192$. Další záznamy v tabulce jsou postupné přírůstky čísla 8192, viz tabulka 1.20.

Tabulka 1.20 Desítková metoda rozdělování pro ID sítě 192.168.0.0

Podsít'	Desítkový zápis	ID podsítě
1	3232235520	192.168.0.0/19
2	3232243712	192.168.32.0/19
3	3232251904	192.168.64.0/19
4	3232260096	192.168.96.0/19
5	3232268288	192.168.128.0/19

Podsít'	Desítkový zápis	ID podsítě
6	3232276480	192.168.160.0/19
7	3232284672	192.168.192.0/19
8	3232292864	192.168.224.0/19

Poznámka: Používání ID podsítě, kde jsou všechny bity použité pro rozdělování nastaveny na 0 (nulová podsít') a na 1 (jedničková podsít') bylo zakázáno v RFC 950. V prvním případě vznikaly problémy s dřívějšími směrovacími protokoly a podsít' druhého typu je v konfliktu s určitou vysílací adresou nazývanou všepodsít'ová směrovaná adresa IP všesměrového vysílání.

Nicméně RFC 1812 nyní povoluje používání výše uvedených typů podsítí v prostředí kompatibilním s CIDR. Tato prostředí používají moderní směrovací protokoly, které nemají problémy s nulovými podsítěmi a všepodsít'ové směrované všesměrové vysílání už není podstatné.

Nulové a jedničkové podsítě mohou působit problémy hostitelům nebo směrovačům pracujícím v plně třídném režimu. Před použitím nulových nebo jedničkových podsítí si ověřte, že jsou podporovány vašimi hostiteli a směrovači. Windows 2000 a Windows NT použití těchto podsítí podporují.

Krok třetí: Výpočet adres IP pro každé ID podsítě

V závislosti na výpočtu ID podsítě nyní musíte sestavit platné adresy IP pro nová ID podsítě. Sestavování každé adresy IP zvlášť by bylo příliš únavné. Namísto toho můžete provést výpočet IP adres pro každé ID podsítě pomocí definování rozsahu adres IP (první a poslední) pro každé ID podsítě. Existují dva hlavní přístupy:

- Dvojkový – Napište první a poslední adresu IP každého ID podsítě a převeďte je do desítkového formátu.
- Desítkový – Postupně přidávejte hodnoty odpovídající první a poslední adrese IP ke každému ID podsítě a převeďte je do desítkového formátu (s tečkou).

Obě metody mají tentýž výsledek, tedy rozsah platných adres IP pro každou podsít'.

► Výpočet rozsahu adres IP za použití dvojkové metody

1. V závislosti na n , počtu bitů hostitele vybraných pro rozdělení sítě, vytvořte třísloupcovou tabulku se $2n$ řádky. V prvním sloupci jsou čísla podsítí (počínající 1), ve druhém sloupci je dvojkové vyjádření první a poslední adresy IP ID podsítě a ve třetím sloupci je desítkové vyjádření první a poslední adresy IP ID podsítě. Je též možné přidat dva sloupce k tabulce 1.20 určené pro výpočet ID podsítí.
2. V každém dvojkovém formátu je první adresa IP adresou, ve které jsou všechny bity hostitele kromě posledního bitu hostitele nastaveny na 0. Poslední adresa IP je adresou, ve které jsou všechny bity hostitele kromě posledního nastaveny na 1.
3. Převeďte dvojkové vyjádření na desítkový formát.
4. Opakujte kroky 2 a 3 až do dokončení tabulky.

Například rozsah IP adres pro 3bitové ID podsítě 192.168.0.0 je uveden v tabulce 1.21. Bity hostitele použité pro rozdělování sítě jsou podtrženy.

Tabulka 1.21 Dvojkový zápis rozsahu IP adres

Podsít'	Dvojkový zápis	Rozsah adres IP
1	11000000.10101000. <u>000</u> 00000.00000001 – 11000000.10101000. <u>000</u> 11111.11111110	192.168.0.1 – 192.168.31.254
2	11000000.10101000. <u>001</u> 00000.00000001 – 11000000.10101000. <u>001</u> 11111.11111110	192.168.32.1 – 192.168.63.254
3	11000000.10101000. <u>010</u> 00000.00000001 – 11000000.10101000. <u>010</u> 11111.11111110	192.168.64.1 – 192.168.95.254
4	11000000.10101000. <u>011</u> 00000.00000001 – 11000000.10101000. <u>011</u> 11111.11111110	192.168.96.1 – 192.168.127.254
5	11000000.10101000. <u>100</u> 00000.00000001 – 11000000.10101000. <u>100</u> 11111.11111110	192.168.128.1 – 192.168.159.254
6	11000000.10101000. <u>101</u> 00000.00000001 – 11000000.10101000. <u>101</u> 11111.11111110	192.168.160.1 – 192.168.191.254
7	11000000.10101000. <u>110</u> 00000.00000001 – 11000000.10101000. <u>110</u> 11111.11111110	192.168.192.1 – 192.168.223.254
8	11000000.10101000. <u>111</u> 00000.00000001 – 11000000.10101000. <u>111</u> 11111.11111110	192.168.224.1 – 192.168.255.254

► **Výpočet rozsahu adres IP za použití desítkové metody**

1. V závislosti na n, počtu bitů hostitele vybraných pro rozdělení, vytvořte třísloupcovou tabulku se $2n$ řádky. V prvním sloupci jsou čísla podsítě (počínající 1), ve druhém sloupci je desítkové vyjádření první a poslední adresy IP ID podsítě a ve třetím sloupci je desítkové vyjádření první a poslední adresy IP ID podsítě (s tečkou). Je též možné přidat dva sloupce k tabulce 1.20 určené pro výpočet ID podsítí.

2. Vypočítejte přírůstkovou hodnotu J založenou na h, počtu zbývajících bitů hostitele:

$$J = 2^h - 2$$

3. Pro každé desítkové vyjádření je první adresa IP $N + 1$, kde N je desítkové vyjádření ID podsítě. Poslední adresa IP je $N + J$.
4. Převedte desítkové vyjádření první a poslední adresy IP ID podsítě na desítkový formát (W.X.Y.Z), a to pomocí následujícího vzorce (kde s je desítkové vyjádření první a poslední adresy IP):

$$W = \text{INT}(s/16777216)$$

$$X = \text{INT}((s \bmod 16777216)/65536)$$

$$Y = \text{INT}((s \bmod 65536)/256)$$

$$Z = s \bmod 256$$

INT() označuje celočíselné dělení, mod() označuje zbytek po dělení.

5. Opakujte kroky 3 a 4 až do dokončení tabulky.

Například rozsah IP adres pro 3bitovou podsít soukromé sítě 192.168.0.0 je znázorněn v tabulce 1.22. Přírůstek je $2^3 - 2 = 8190$.

Tabulka 1.20 Desítkový zápis IP adres

Podsít'	Desítkový zápis	Rozsah adres IP
1	3232235521 - 3232243710	192.168.0.1 - 192.168.31.254
2	3232243713 - 3232251902	192.168.32.1 - 192.168.63.254
3	3232251905 - 3232260094	192.168.64.1 - 192.168.95.254
4	3232260097 - 3232268286	192.168.96.1 - 192.168.127.254
5	3232268289 - 3232276478	192.168.128.1 - 192.168.159.254
6	3232276481 - 3232284670	192.168.160.1 - 192.168.191.254
7	3232284673 - 3232292862	192.168.192.1 - 192.168.223.254
8	3232292865 - 3232301054	192.168.224.1 - 192.168.255.254

Vytváření podsítí s různou délkou

Jedním z původních cílů vytváření podsítí bylo rozdělení třídivých identifikátorů sítě do řady stejně velkých podsítí. Například výsledkem 4bitového vytváření podsítí sítě třídy B bylo 16 stejně velkých podsítí (za použití nulových a jedničkových podsítí). Nicméně vytváření podsítí je obecnou metodou využití bitů hostitele k vyjádření podsítí, přičemž podsítě nemusí mít vždy stejnou velikost.

V rámci třídivého identifikátoru sítě mohou existovat podsítě různých velikostí. To odpovídá skutečným prostředím, kde sítě určité organizace obsahují různý počet hostitelů, takže k minimalizaci plýtvání adresami IP jsou třeba podsítě různých velikostí. Vytváření a rozvíjení podsítí různých velikostí je známé jako *Vytváření podsítí s různou délkou* a používá různou délku masek podsítí (VLSM, variable length subnet mask).

Vytváření podsítí s různou délkou je způsob alokace identifikátorů podsítí, které používají masky různých velikostí. Nicméně všechny identifikátory podsítí jsou jedinečné a lze je jeden od druhého odlišit pomocí jim odpovídajících masek.

Vytváření podsítí s různou délkou se používá především v případech rozdělování již rozdělených sítí. Při tomto procesu jsou příslušné bity určující identifikátory sítě pevně stanoveny a je vybrán určitý počet bitů hostitele, které vyjadřují podsítě.

Například u třídivého identifikátoru sítě 135.41.0.0/16 je požadovaná konfigurace jedna podsít' s až 32 000 hostiteli, 15 podsítí s až 2 000 hostiteli a osm podsítí s až 250 hostiteli.

Jedna podsít' s až 32 000 hostiteli

Požadavek na jednu podsít' s přibližně 32 000 hostiteli je realizován 1bitovým rozdělením třídivého identifikátoru sítě 135.41.0.0, čímž vzniknou dvě podsítě – 135.41.0.0/17 a 135.41.128.0/17. Toto rozdělení umožňuje umístit až 32 766 hostitelů na jednu podsít'. Požadavky splňuje identifikátor sítě 135.41.0.0/17.

V tabulce 1.23 je znázorněna podsít' s až 32 766 hostiteli.

Tabulka 1.23 Podsít' s až 32766 hostiteli

Číslo podsítě	Identifikátor sítě (desítkový formát s tečkou)	Identifikátor sítě (s předponou sítě)
1	135.41.0.0, 255.255.128.0	135.41.0.0/17

Patnáct podsítí s až 2 000 hostiteli

Požadavek na patnáct podsítí s přibližně 2 000 hostiteli je realizován 4bitovým rozdělením třídového identifikátoru sítě 135.41.128.0/17, čímž vznikne 16 podsítí (135.41.128.0/21, 135.41.136.0/21... 135.41.240.0/21, 135.41.248.0/21). Toto umožňuje umístit až 2 046 hostitelů na jednu podsít'. Požadavky splňuje prvních 15 identifikátorů podsítí (135.41.128.0/21 až 135.41.240.0/21).

V tabulce 1.24 je znázorněno 15 podsítí s až 2046 hostiteli.

Tabulka 1.24 Patnáct podsítí s až 2046 hostiteli

Číslo podsítě	Identifikátor sítě (desítkový formát s tečkou)	Identifikátor sítě (s předponou sítě)
1	135.41.128.0, 255.255.248.0	135.41.128.0/21
2	135.41.136.0, 255.255.248.0	135.41.136.0/21
3	135.41.144.0, 255.255.248.0	135.41.144.0/21
4	135.41.152.0, 255.255.248.0	135.41.152.0/21
5	135.41.160.0, 255.255.248.0	135.41.160.0/21
6	135.41.168.0, 255.255.248.0	135.41.168.0/21
7	135.41.176.0, 255.255.248.0	135.41.176.0/21
8	135.41.184.0, 255.255.248.0	135.41.184.0/21
9	135.41.192.0, 255.255.248.0	135.41.192.0/21
10	135.41.200.0, 255.255.248.0	135.41.200.0/21
11	135.41.208.0, 255.255.248.0	135.41.208.0/21
12	135.41.216.0, 255.255.248.0	135.41.216.0/21
13	135.41.224.0, 255.255.248.0	135.41.224.0/21
14	135.41.232.0, 255.255.248.0	135.41.232.0/21
15	135.41.240.0, 255.255.248.0	135.41.240.0/21

Osm podsítí s až 250 hostiteli

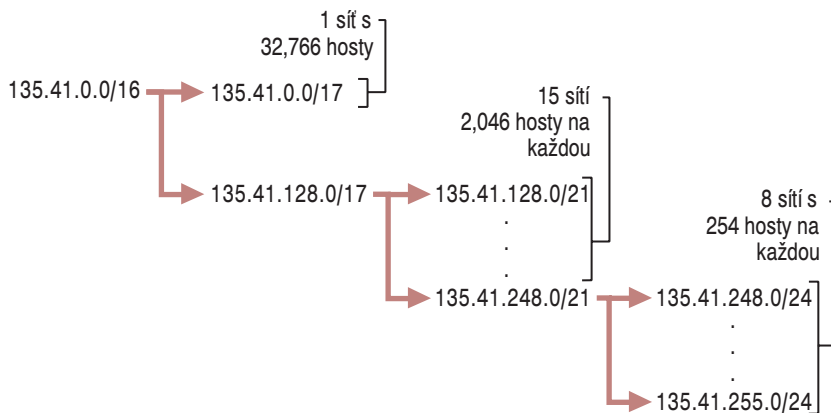
Požadavek na osm podsítí s přibližně 250 hostiteli je realizován 3bitovým rozdělením třídového identifikátoru sítě 135.41.248.0/21, čímž vznikne 8 podsítí (135.41.248.0/24, 135.41.249.0/24... 135.41.254.0/24, 135.41.255.0/24). Toto rozdělení umožňuje umístit až 254 hostitelů na jednu podsít'. Všechny osm identifikátorů podsítí (135.41.248.0/24 až 135.41.255.0/24) splňuje zadané požadavky.

V tabulce 1.24 je znázorněno 8 podsítí s až 254 hostiteli.

Tabulka 1.25 Osm podsítí s až 254 hostiteli

islo podsítě	Identifikátor sítě (desítkový formát s tečkou)	Identifikátor sítě (s předponou sítě)
1	135.41.248.0, 255.255.255.0	135.41.248.0/24
2	135.41.249.0, 255.255.255.0	135.41.249.0/24
3	135.41.250.0, 255.255.255.0	135.41.250.0/24
4	135.41.251.0, 255.255.255.0	135.41.251.0/24
5	135.41.252.0, 255.255.255.0	135.41.252.0/24
6	135.41.253.0, 255.255.255.0	135.41.253.0/24
7	135.41.254.0, 255.255.255.0	135.41.254.0/24
8	135.41.255.0, 255.255.255.0	135.41.255.0/24

Vytváření podsítí s různou délkou pro síť 135.41.0.0/16 je graficky znázorněno na obrázku 1.10.

**Obrázek 1.10 Vytváření podsítí s různou délkou pro síť 135.41.0.0/16**

Poznámka: V prostředích s dynamickým směrováním může být vytváření podsítí s různou délkou použito pouze tam, kde je maska podsítě ohlašována současně s identifikátorem sítě. Protokol RIP (Routing Information Protocol) for IP verze 1 vytváření podsítí s různou délkou nepodporuje. Protokoly RIP for IP verze 2, OSPF (Open Shortest Path First) a BGPv4 (Border Gateway Protocol verze 4) toto vytváření podsítí již podporují.

Vytváření nadsítí a CIDR (Classless Interdomain Routing)

Se stálým růstem Internetu začalo být Internetovým odborníkům jasné, že identifikátory sítí třídy B budou brzy vyčerpány. Pro většinu organizací neobsahují identifikátory sítí třídy C dostatek identifikátorů hostitelů a identifikátor sítě třídy B má dostatek bitů na to, aby umožňovala pružné vytváření podsítí v rámci organizace.

Z tohoto důvodu byla vypracována nová metoda přiřazování identifikátorů sítě, aby se tak předešlo vyčerpání identifikátorů sítě třídy B. Raději než identifikátory sítě třídy B přiřazuje organizace InterNIC řadu identifikátorů sítě třídy C, které obsahují dostatek identifikátorů hostitelů a sítí k uspokojení potřeb většiny organizací. To je známé jako *vytváření nadsítí (supernetting)*. Například spíše než by organizaci, která má více než 2000 hostitelů, InterNIC přidělila identifikátor sítě třídy B, alokuje pro tuto organizaci raději řadu osmi identifikátorů sítě třídy C. Každý identifikátor sítě třídy C obsluhuje 254 hostitelů, celkem pak 2 032 hostitelů.

I když tato metoda pomáhá zachovat identifikátory sítě třídy B, vytváří nový problém. Při použití konvenčních směrovacích technik musí mít nyní směrovače na internetu ve svých směrovacích tabulkách pro směrování paketů organizaci osm záznamů o identifikátorech sítě třídy C. Zahlcení směrovačů se předchází pomocí metody zvané *beztržidové doménové směrování (CIDR, Classless Interdomain Routing)*, která sloučí vícenásobné záznamy o identifikátorech sítě do jednoho záznamu odpovídajícího identifikátorům sítě třídy C přiřazeného této organizaci.

V zásadě tvoří CIDR záznam směrovací tabulky ve tvaru: [počáteční identifikátor sítě, počet], kde počáteční identifikátor sítě je první identifikátor sítě třídy C a počet je počet přidělených identifikátorů sítě třídy C. To znamená, že sloučená maska podsítě se používá k předávání stejných informací. Situace, kde je alokováno osm identifikátorů sítě třídy C počínajících identifikátorem sítě 220.78.168.0, vypadá takto:

Počáteční identifikátor sítě 220.78.168.0 11011100 01001110 10101000 00000000

Koncový identifikátor sítě 220.78.175.0 11011100 01001110 10101111 00000000

Všimněte si, že prvních 21 bitů (podtrženo) všech výše uvedených identifikátorů sítě je stejných. Poslední tři bity třetího oktetu se pohybují od 000 po 111. Záznam CIDR ve směrovací tabulce internetových směrovačů pak je:

Identifikátor sítě	Maska podsítě	Maska podsítě (dvojkový zápis)
220.78.168.0	255.255.248.0	11111111 11111111 11111000 00000000

V zápise se síťovou předponou nebo zápise CIDR je záznam CIDR 220.78.168.0/21.

Blok adres používajících CIDR je známý jako *blok CIDR*.

Poznámka: Protože masky podsítě se používají k vyjádření počtu, musí být třídivé identifikátory sítě alokovány ve skupinách odpovídajících násobku 2.

Abby mohly směrovače podporovat CIDR, musí být schopné vyměňovat informace jako páry [identifikátor sítě, maska podsítě]. Směrovací protokoly RIP for IP verze 2, OSPF a BGPv4 CIDR podporují. Protokol RIP for IP verze 1 CIDR nepodporuje.

Dva různé pohledy na adresový obor

Používání CIDR pro alokaci adres prosazuje nový pohled na identifikátory sítí IP. Ve výše uvedeném příkladě lze blok CIDR [220.78.168.0, 255.255.248.0] chápat dvěma způsoby:

- Blok osmi identifikátorů sítě třídy C.
- Adresový obor, ve kterém je 21 pevných bitů a 11 bitů přiřaditelných.

Ve druhém případě ztrácejí identifikátory sítě IP svoji příslušnost ke třídě a stávají se samostatnými obory adres IP, podmnožinou původního oboru adres IP definovaného 32bitovou adresou IP. Každý identifikátor sítě (třídové, rozdělené, s blokem CIDR) je adresovým oborem, ve kterém jsou určité bity pevně stanovené (bity identifikátoru sítě) a určité bity jsou proměnlivé (bity hostitele). Bity hostitele jsou přiřaditelné jako identifikátory hostitele nebo, za použití metod vytváření podsítí, je lze použít jakýmkoli způsobem, který nejvíce vyhovuje organizaci.

Veřejné a soukromé adresy

Není-li váš intranet připojen do Internetu, lze použít jakýkoli způsob adresace a rozsah adres. Jestliže je žádoucí přímá (přes směrovač) nebo nepřímá (například přes proxy server) připojitelnost na internet, je třeba použít jeden ze dvou typů adresování používaných na Internetu – veřejné adresy nebo soukromé adresy.

Veřejné adresy

Veřejné adresy přiřazuje organizace InterNIC a sestávají se z třídových identifikátorů sítě nebo bloků CIDR adres (bloků CIDR), u kterých je zaručena jejich jedinečnost v rámci celého Internetu.

Po přiřazení veřejných adres jsou naprogramovány cesty na směrovače tak, aby provoz určený přiřazeným veřejným adresám mohl dosáhnout svého místa určení.

Například poté, co je organizaci přidělen blok CIDR v podobě identifikátoru sítě a masky podsítě, existuje tento pár [identifikátor sítě, maska podsítě] také jako cesta na směrovačích. Pakety IP určené pro adresu uvedenou v bloku CIDR jsou směrovány na správné místo určení.

Ilegální adresy

Soukromé intranety, které nemají zájem o připojení k internetu, si mohou vybrat jakékoli adresy, které chtějí, dokonce i veřejné adresy, které již organizace InterNIC přidělila. V případě, že se později rozhodne o připojení tohoto intranetu k internetu, může být používaný adresový obor již přidělen jiné/jiným organizacím. Tyto adresy pak budou duplicitními (konfliktními) a vžilo se pro ně označení ilegální adresy. Z ilegálních adres se nelze k internetu připojit.

Například soukromá organizace se rozhodne jako svůj intranetový adresový obor používat 207.46.13.0/24. Veřejná adresa 207.46.130.0/24 již byla přiřazena společnosti Microsoft a na směrovačích existují cesty směřující všechny pakety určené na adresy 207.46.130.0/24 na směrovače společnosti Microsoft. Dokud se soukromá organizace nepřipojí k internetu, nenastává žádný problém, protože tyto dva adresové obory jsou použity pro fyzicky oddělené sítě. Jestliže se posléze soukromá organizace připojí přímo k internetu a dále používá jako svůj adresový obor 207.46.130.0/24, budou všechny požadavky na 207.46.130.0/24 směřovány na směrovače společnosti Microsoft a nikoli na směrovače soukromé organizace.

Soukromé adresy

Každý uzel IP vyžaduje adresu IP, která je v síti IP naprosto jedinečná. V případě internetu vyžaduje každý uzel na síti připojené k internetu adresu IP, která je jedinečná v celém internetu. Při růstu internetu vyžadovaly organizace připojující se k internetu veřejnou adresu pro každý uzel na jejich intranetu. Tento požadavek kladl obrovské nároky na množinu dostupných veřejných adres.

Při analýze adresových potřeb organizací se zjistilo, že u většiny organizací většina hostitelů na intranetu organizace nevyžaduje přímé spojení s hostiteli na internetu. Ti hostitelé, kteří vyžadují určité sady služeb internetu, například přístup k webu a elektronické poště, zpravidla přistupují k internetovým službám prostřednictvím brány aplikační vrstvy jako jsou proxy a poštovní servery. Výsledkem je, že většina organizací požadovala veřejné adresy jen pro málo uzlů (například pro proxy servery, směrovače, firewally a překladače adres) přímo připojených k Internetu.

U hostitelů, kteří v rámci organizace nevyžadují přímý přístup k internetu, bylo požadováno, aby jejich adresy neduplikovaly již přiřazené veřejné adresy. Pro řešení tohoto adresového problému byla vyhrazena část oboru adres IP, který se nazývá soukromý adresový obor. Adresa IP ze soukromého adresového oboru se nikdy nepřiděluje jako adresa veřejná. Adresy IP v rámci oboru soukromých adres jsou známy jako soukromé adresy. Vzhledem k tomu, že se obory veřejných a soukromých adres nepřekrývají, soukromé adresy nikdy neduplikují adresy veřejné.

Soukromý adresový obor specifikovaný v RFC 1918 je definován následujícími třemi bloky adres:

■ 10.0.0.0/8

Soukromá síť 10.0.0.0/8 je síť třídy A, která umožňuje následující rozsah platných adres: 10.0.0.1 až 10.255.255.254. Soukromá síť 10.0.0/8 má 24 bitů hostitele, které mohou být použity pro vytváření podsítí v rámci soukromé organizace.

■ 172.16.0.0/12

Soukromou síť 172.16.0.0/12 si lze představit jako blok 16 identifikátorů sítě třídy B nebo jako 20bitový přiřaditelný adresový obor (20 bitů hostitele), který lze použít pro jakékoli vytváření podsítí v rámci soukromé organizace. Soukromá síť 172.16.0.0/12 umožňuje následující rozsah platných adres: 172.16.0.1 až 172.31.255.254.

■ 192.168.0.0/16

Soukromou síť 192.168.0.0/16 se lze představit jako blok 256 identifikátorů sítě třídy C nebo jako 16bitový přiřaditelný adresový obor (16 bitů hostitele), který lze použít pro jakékoli vytváření podsítí v rámci soukromé organizace. Soukromá síť 192.168.0.0/16 umožňuje následující rozsah platných adres: 192.168.0.1 až 192.168.255.254.

Výsledkem toho, že mnoho organizací soukromé adresy používá je, že stejný adresový obor mohou opakovaně a současně využít různé organizace, čímž nedochází k vyčerpání veřejných adres.

Vzhledem k tomu, že adresy IP v soukromém adresovém oboru nikdy organizace InterNIC nepřiradí jako veřejné, nebudou nikdy na internetových směrovačích existovat příslušné záznamy o těchto adresách. Soukromé adresy jsou na internetu nedosažitelné. Proto musí hostitel, který má přiřazenou soukromou adresu, předat své požadavky na přístup k internetu buď aplikační mezivrstvě (například proxy serveru), který má platnou veřejnou adresu, nebo musí svou soukromou adresu nechat přeložit na platnou veřejnou adresu pomocí překladače síťových adres (NAT – network address translator). Více informací o překladači síťových adres najdete v části „Jednotné IP směrování“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Překlad adres

Zatímco protokol IP je navržen tak, že pracuje s 32bitovými adresami zdrojových a cílových hostitelů, uživatelé počítačů si mnohem lépe pamatují a lépe používají názvy než adresy IP.

Pokud se název používá jako alias pro adresu IP, musí existovat pro přiřazení tohoto názvu odpovídajícímu uzlu IP určitý mechanismus, aby byla zajištěna jedinečnost takového názvu a jeho přiřazení adrese IP.

V této části naleznete popis metod používaných pro přiřazování a vyhodnocování názvů hostitele (které používají aplikace Windows Sockets) a názvů NetBIOSu (které používají aplikace NetBIOSu).

Překlad názvů hostitele

Název hostitele (host name) je alias přiřazený uzlu IP tak, aby byl identifikován jako hostitel TCP/IP. Název hostitele může být až 255 znaků dlouhý a může obsahovat alfanumerické znaky a znaky „-“ a „.“. Stejnému hostiteli může být přiřazeno několik názvů. U počítačů založených na Windows 2000 nemusí být název hostitele stejný jako název počítače s Windows 2000.

Aplikace pro rozhraní Windows Sockets, například Microsoft® Internet Explorer a různé programy FTP, mohou ke kontaktu s adresátem používat jednu nebo dvě možnosti: adresu IP nebo název hostitele. Je-li určena adresa IP, již není třeba přiřazovat název. Je-li určen název hostitele, musí být tento název hostitele před počátkem komunikace s požadovaným zdrojem převeden na adresu IP.

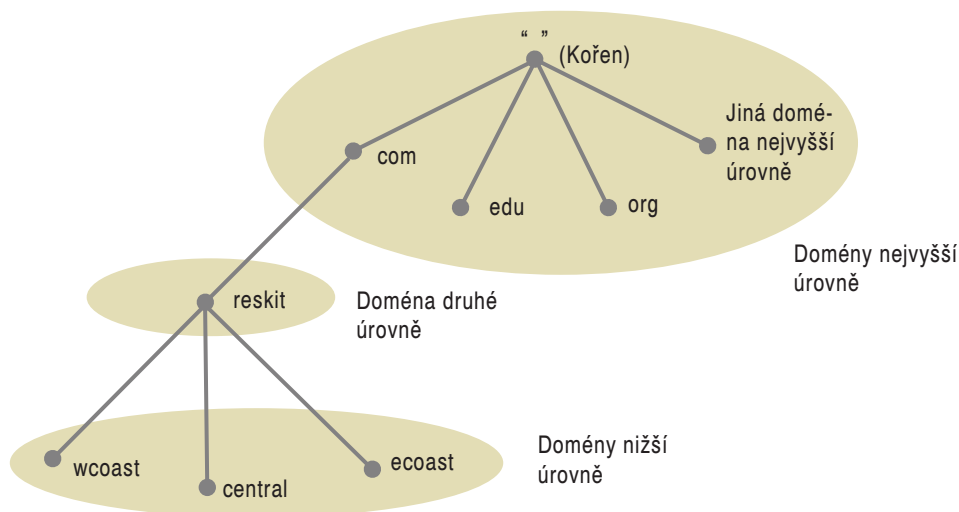
Názvy hostitele mohou být v různých formách. Dvěma nejběžnějšími formami jsou přezdívka a doménový název. Přezdívka je alias pro adresu IP, kterou mohou přiřazovat a používat jednotliví lidé. *Doménový název* je strukturovaný název, který se řídí konvencemi internetu.

Doménové názvy

Organizace InterNIC vytvořila a udržuje hierarchické názvové schéma nazvané Systém názvů domén (DNS, Domain Name Systém), aby usnadnila různým organizacím dosáhnout fungování ve stupňovitém a upravitelném názvovém schématu. DNS je názvové schéma, které vypadá podobně jako adresářová struktura pro soubory na disku. Nicméně namísto sledování souboru z kořenového adresáře přes podadresáře až do jeho konečného umístění a jeho názvu souboru je název hostitele sledován ze svého konečného umístění přes mateřské domény zpět ke kořeni. Jedinečný název hostitele reprezentující jeho pozici v hierarchii je nazýván Úplný doménový název (FQDN, Fully Qualified Domain Name). Obor názvů domén nejvyšší úrovně je znázorněn na obrázku 1.11 spolu s příkladem domén druhé úrovně a poddomén.

Obor názvů domény se sestává z:

- *Kořenové domény* (root domain), reprezentující kořen oboru názvů a označené „“ (null hodnota).
- *Domén nejvyšší úrovně* (top-level domains), které jsou přímo pod kořenem, označující typ organizace. Na Internetu je za správu názvů těchto domén odpovědná organizace InterNIC. Tabulka 1.26 obsahuje částečný seznam domén nejvyšší úrovně.



Obrázek 1.11 Struktura DNS

Tabulka 1.26 Názvy domén nejvyšší úrovně

Název domény	Význam
COM	Komerční organizace
EDU	Vzdělávací instituce
GOV	Vládní instituce
MIL	Vojenské instituce
NET	Hlavní síťové organizace
ORG	Organizace odlišné od výše uvedených
INT	Mezinárodní organizace
<kód státu/regionu>	Každý stát/oblast (geografické schéma)

- *Domén druhé úrovně*, umístěných pod doménami nejvyšší úrovně, identifikující určitou organizaci v rámci domény nejvyšší úrovně. Na Internetu je za správu a zajištění jedinečnosti názvů domén druhé úrovně odpovědná organizace InterNIC.
- *Poddomén* organizace, umístěných pod doménami druhé úrovně. Za vytvoření a správu poddomén odpovídá každá individuální organizace samostatně.

Například u FQDN **ftpsrv.wcoast.reskit.com**. platí:

- Koncová tečka (.) značí, že toto je FQDN s názvem vztaženým ke kořeni názvového oboru domény. Oddělovací tečka se zpravidla u FQDN nevyžaduje a není-li tam, považuje se za přítomnou
- **com** je doména nejvyšší úrovně označující komerční organizaci.
- **reskit** je doména druhé úrovně označující organizaci Windows 2000 Resource Kit.
- **wcoast** je poddoména **reskit.com** označující divizi organizace Windows 2000 Resource Kit na Západním pobřeží.

- **ftpsrv** je název serveru FTP v divizi na Západním pobřeží.

Názvy domén nejsou citlivé na velikost písmen.

Organizace, které nejsou připojené k internetu, mohou používat jakékoli názvy domén nejvyšší a druhé úrovně. Nicméně typické implementace odpovídají specifikacím InterNIC, takže případná účast na internetu nevyžaduje přejmenování domén.

Překlad adres za využití souboru Hosts

Jedním běžným způsobem překladu názvu hostitele na adresu IP je používání lokálního databázového souboru, který obsahuje přiřazení adres IP názvům hostitele. Na většině unixových systémů se jedná o soubor `/etc/hosts`. Ve Windows 2000 je tento soubor v adresáři `%SystemRoot%\system32\drivers\etc`.

Zde je uveden příklad obsahu souboru Hosts:

```
#
# Tabulka adres IP a názvů hostitelů (Table of IP addresses and host names)
#
127.0.0.1          localhost #hostitel
139.41.34.1        router #směrovač
167.91.45.121     server1.central.slate.com s1 #server
```

V souboru Hosts:

- Jedné adrese IP může být přiřazeno několik názvů hostitele. To znamená, že na server na adrese IP 167.91.45.121 se lze odkazovat jak jeho úplným názvem (server1.central.slate.com), tak jeho přezdívkou (s1). To dovoluje uživateli odkazovat se ze svého počítače na tento server pomocí přezdívkou s1 namísto vypisování úplného názvu.
- Záznamy, v závislosti na platformě, mohou být citlivé na velikost písma. Záznamy v souboru Hosts pro unixové počítače jsou na velikost písma citlivé, záznamy v souboru Hosts pro počítače na platformě Windows 2000 a Windows NT na velikost písma citlivé nejsou.

Výhodou používání tohoto lokálního souboru je to, že ho uživatel může sám upravit. Každý uživatel může vytvořit jakýkoli záznam včetně snadno zapamatovatelných přezdívek pro často používané prostředky. Nicméně individuální správa souboru Hosts není příliš vhodná pro ukládání velkého množství přiřazení úplných FQDN.

Překlad adres za využití DNS serveru

Aby bylo možno přiřazování názvů hierarchizovat a centrálně spravovat, je mapování adres IP pro FQDN uloženo na DNS serverech, počítačích, na kterých jsou uložena mapování FQDN na adresy IP. Dotazy na server DNS hostitelským počítačem jsou pomocí komponenty překladač DNS, který je zpřístupněn a nakonfigurován společně s adresou IP serveru DNS. Překladač DNS je vestavěnou komponentou TCP/IP protokolu dodávanou s většinou síťových operačních systémů, včetně Windows 2000.

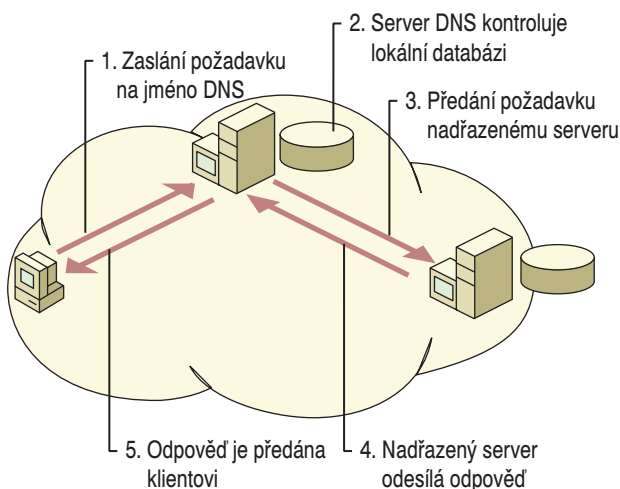
Poté, co aplikace Windows Sockets obdrží FQDN jako místo určení, vyvolá funkci, která přiřadí tomuto názvu adresu IP. Žádost je postoupena příslušné komponentě protokolu TCP/IP, tedy překladači DNS, který zabalí žádost o FQDN jako paket s dotazem na název DNS a pošle ji na server DNS.

DNS je distribuovaný názvový systém. Než by skladoval všechny záznamy celého názvového oboru na každém serveru DNS, skladuje každý server DNS záznamy určité části

názvového oboru. Server DNS je rozhodující pro tu část názvového oboru, která odpovídá záznamům uloženým na tomto serveru DNS. V případě internetu jsou různé části názvového oboru internetu uloženy na stovkách serverů DNS. Aby byly servery DNS schopny přiřadit adresu IP ke kterémukoli platnému doménovému názvu, jsou nakonfigurovány tak, že odkazují na záznamy na ostatních serverech DNS.

Následující postup ukazuje, co se stane, když překladač DNS hostitele zašle dotaz na server DNS. Tento proces je znázorněn na obrázku 1.12 a je zjednodušen, takže můžete pochopit základy přiřazovacího procesu.

1. Překladač DNS klienta zformátuje dotaz na DNS název obsahující FQDN a zašle ho na nakonfigurovaný server DNS.
2. Server DNS porovná FQDN v dotazu s lokálně uloženými záznamy o adresách. Jestliže najde příslušný záznam, pošle zpět klientovi adresu IP odpovídající dotazovanému FQDN.
3. Jestliže příslušný záznam nenajde, server DNS postoupí dotaz serveru DNS, který je pro FQDN nadřazený.
4. Nadřazený server DNS vrátí odpověď obsahující přiřazenou adresu IP zpět původnímu serveru DNS.
5. Původní server DNS zašle informace o přiřazení adresy IP klientovi.



Obrázek 1.12 Přiřazování FQDN za použití serverů DNS

Adresu IP serveru nadřazeného FQDN získají servery DNS na internetu tak, že rozesílají dotazy na více serverů DNS tak dlouho, dokud nenajdou nadřazený server. Podrobnější informace o tomto procesu najdete v této knize v části „Služba Windows 2000 DNS“.

Kombinace lokální databáze a DNS

Implementace protokolů TCP/IP, včetně Windows 2000, dovolují k přiřazování názvů hostitele použít jak soubor lokální databáze, tak server DNS. Poté, co uživatel určí název hostitele v příkazu nebo nástroji TCP/IP:

1. TCP/IP prohledá soubor lokální databáze (soubor Hosts), aby našel odpovídající název.
2. Nenajde-li odpovídající název v souboru lokální databáze, zabalí název hostitele jako dotaz na název DNS a pošle ho nakonfigurovanému serveru DNS .

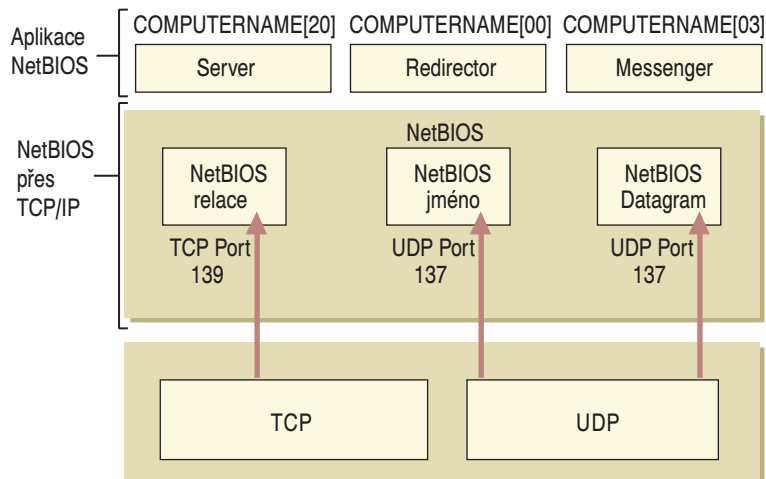
Kombinace obou metod poskytuje uživateli možnost využívat pro místní přezdívky soubor lokální databáze a pro FQDN možnost využívat globálně distribuované databáze DNS .

Přiřazování názvu NetBIOSu

Přiřazování názvu NetBIOSu je proces úspěšného přiřazování *názvu NetBIOSu* adrese IP. Název NetBIOSu je 16bajtová adresa používaná k identifikaci prostředku NetBIOSu na síti. Tento název je buď jedinečný (výlučný) nebo skupinový (nevýlučný). Při komunikaci procesu NetBIOSu s určitým procesem na určitém počítači je používán jedinečný název, při komunikaci procesu NetBIOSu s více procesy na více počítačích, je používán skupinový název.

Název NetBIOSu funguje jako identifikátor aplikace relační vrstvy. Například služba relace NetBIOSu pracuje nad TCP portem 139, všechny dotazy NetBIOSu nad relací TCP/IP jsou adresovány na adresátský port TCP 139. Při identifikaci aplikace NetBIOSu, která ustavuje relaci NetBIOSu, se používá název NetBIOSu.

Příkladem procesu používajícího název NetBIOSu je služba serveru sdílejícího soubory a tisk na počítači na platformě Windows 2000. Při startu počítače služba serveru zaregistruje jedinečný název NetBIOSu založený na názvu počítače. Přesný název používaný službou serveru je 15 znakový název počítače plus 16. znak 0x20. Není-li název počítače dlouhý 15 znaků, je zbytek počtu znaků vyplněn mezerami. Jiné síťové služby také používají název počítače při sestavování názvu NetBIOSu, takže jejich 16. znak je použit k jedinečné identifikaci každé služby, například služeb přesměrování, serveru nebo vzkazu. Na obrázku 1.13 jsou znázorněny názvy NetBIOSu spojené se službami Server, Redirector a Messenger.



Obrázek 1.13 Názvy NetBIOSu a služby

Snažíte-li se vytvořit připojení na sdílenou položku k počítači na platformě Windows 2000 podle názvu, služba serveru na souborovém serveru, který určíte, odpovídá určitému názvu NetBIOSu. Například když se snažíte připojit k počítači nazvanému CORPSEVER, je názvem NetBIOSu odpovídajícím službě serveru „CORPSEVER <20>“ (všimněte si vyplnění prostoru do 15 znaků délky mezerami). Před ustavením připojení sdílejího soubory a tisk musí být nejdříve vytvořeno připojení TCP. A aby mohlo být toto spojení vytvořeno, je nutno přiřadit název NetBIOSu „CORPSEVER <20>“ adrese IP.

K prohlédnutí názvů NetBIOSu registrovaných procesy NetBIOSu běžícími na počítači s Windows 2000 napište a příkazovém řádku Windows 2000 `nbtstat -n`.

Typy uzlů NetBIOSu

Přesný mechanismus, kterým jsou názvy NetBIOSu přiřazovány adresám IP, závisí na typu uzlu NetBIOSu, který je na uzlu nakonfigurován. RFC 1001 definuje typy uzlu NetBIOSu tak, jak vidíte v tabulce 1.27.

Tabulka 1.27 Typy uzlu NetBIOSu

Typ uzlu	Popis
Uzel B (broadcast)	Uzel B používá k registraci a přiřazení názvů všesměrově vysílané dotazy NetBIOSu na názvy. Uzel B má dva velké problémy: (1) na velkých sítích může všesměrové vysílání přesáhnout kapacitu sítě, a (2) směrovače zpravidla nepředávají všesměrová vysílání, takže lze přiřadit pouze názvy NetBIOSu na lokální síti.
Uzel P (peer-peer)	Uzel P používá k přiřazení názvu NetBIOSu serveru názvy NetBIOSu (NBNS), například WINS (Windows Internet Name Service). Uzel P nepoužívá všesměrové vysílání, ale místo toho se dotazuje serveru názvů přímo. Nejvýznamnějším problémem uzlu P je to, že všechny počítače musí být nakonfigurovány s adresou IP NBNS. Pokud NBNS nefunguje, počítače nejsou schopné komunikovat ani na lokální síti.
Uzel M (mixed – smíšený)	Uzel M je kombinací uzlu B a P. Primárně uzel M funguje jako uzel B. Teprve není-li schopen přiřadit název pomocí všesměrového vysílání, použije NBNS uzlu P.
Uzel H (hybridní)	Uzel H je kombinací uzlu P a B. Primárně uzel H funguje jako uzel P. Teprve není-li schopen přiřadit název pomocí NBNS, použije všesměrové vysílání.

Počítače na platformě Windows 2000 jsou primárně uzly B a uzlem H se stávají při konfiguraci na WINS server. Windows 2000 také k přiřazení vzdálených názvů NetBIOSu používají lokální databázový soubor nazvaný `Lmhosts`.

Více podrobností o WINS najdete v této knize v části „Služba Windows Internet Name Service“. Více podrobností o souboru `Lmhosts` najdete v této knize v části „Soubor `LMHOSTS`“.

Směrování IP

Po přiřazení názvu NetBIOSu adrese IP musí odesílající hostitel na přiřazenou adresu IP odeslat paket IP. *Směrování* je proces předávání paketu založený na adresátské adrese IP. Směrování se objevuje u odesílajícího TCP/IP hostitele a IP směrovače. *Směrovač* je zařízení, které předává pakety z jedné sítě na druhou. Směrovače jsou také běž-

ně označovány jako *brány*. V obou případech, jak u odesílajícího hostitele, tak u směrovače, se musí rozhodnout, kam bude paket dále předán.

Při tomto rozhodování vrstva IP konzultuje směrovací tabulku uloženou v paměti. Záznamy směrovací tabulky jsou vytvořeny primárně při inicializaci TCP/IP, dodatečné záznamy jsou přidány manuálně systémovým administrátorem nebo automaticky pomocí komunikace se směrovači.

Přímé a nepřímé doručení

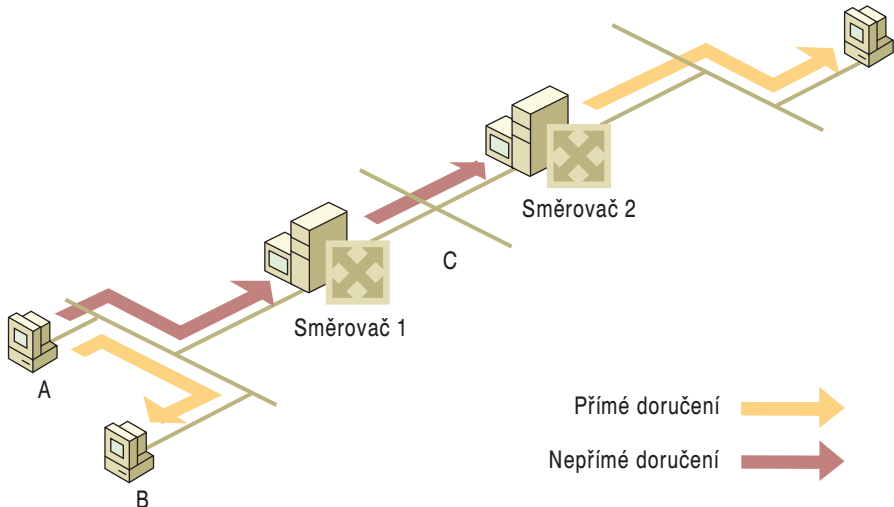
Předávané pakety IP používají minimálně jeden ze dvou způsobů doručení v závislosti na tom, jestli je IP paket předáván na konečné místo určení nebo jestli je předáván na směrovač IP. Tyto dva typy doručení jsou známy přímé a nepřímé doručení.

Jako *přímé doručení* se označuje předávání paketu IP uzlem (ať už odesílajícím nebo směrovačem IP) do konečného místa určení na přímo připojené síti. Uzel IP zabalí datagram IP do formátu určeného síťové vrstvě (například Ethernet nebo Token Ring) adresovaného na fyzickou adresu místa určení.

Jako *nepřímé doručení* se označuje předávání paketu IP uzlem (ať už odesílajícím nebo IP směrovačem) do zprostředkovatelského uzlu, protože místo konečného určení je na nepřímo připojené síti. IP uzel zabalí IP datagram do formátu rámce určeného vrstvě síťového rozhraní (například Ethernet nebo Token Ring) adresovaného na fyzickou adresu IP směrovače.

Směrování IP je kombinací přímého a nepřímého doručení.

Při zasílání paketů na uzel B provádí uzel A přímé doručení. Při zasílání paketů do uzlu C provádí uzel A nepřímé doručení na směrovač 1, který provádí nepřímé doručení na směrovač 2. Směrovač 2 provádí přímé doručení do uzlu C.



Obrázek 1.14 Přímé a nepřímé doručení

Směrovací tabulka IP

Směrovací tabulka existuje na všech uzlech IP. Ve směrovací tabulce jsou uloženy informace o sítích IP a o tom, jak je lze dosáhnout (ať už přímo či nepřímo). Vzhledem k tomu, že všechny uzly IP provádějí určitou formu směrování IP, nejsou směrovací tabulky výsadou pouze směrovačů IP. Jakýkoli uzel s protokolem TCP/IP má svou směrovací tabulku. V ní existuje několik přednastavených záznamů v závislosti na konfiguraci uzlu, lze do ní také dodatečně přidat záznamy buď manuálně pomocí nástrojů TCP/IP nebo dynamicky za pomoci spolupráce směrovačů.

Má-li být zaslán nějaký paket IP, použije se k určení následujících fakt směrovací tabulka:

1. Adresa IP předávacího místa nebo místa dalšího určení:

Při přímém doručení je předávací adresa IP i adresou konečného určení paketu IP.

Při nepřímém doručení je předávací adresa IP adresou IP směrovače.

2. Rozhraní použité k předávání:

Rozhraní identifikuje fyzické nebo logické rozhraní jako síťový adaptér, které je používáno k předání paketu buď na místo určení nebo na další směrovač.

Typy záznamů ve směrovací tabulce IP

Záznam ve směrovací tabulce IP obsahuje následující informace v tomto pořadí:

Identifikátor sítě. Identifikátor sítě nebo místo určení odpovídající cestě. Identifikátor sítě může být třídivý, podsítí nebo nadsítí nebo adresou IP hostitele.

Síťová maska. Maska používaná k přiřazení adresy IP místa určení identifikátoru sítě.

Příští skok. Adresa IP následujícího skoku (směrování) paketu.

Rozhraní. Označení toho, jaké síťové rozhraní je použito k předání paketu IP.

Metrika. Číslo používané k označení náročnosti cesty, aby bylo možno mezi několika možnými cestami do stejného místa určení vybrat tu nejlepší. Zpravidla se metrika používá k označení počtu skoků (překračovaných směrovačů) k identifikátorům sítě.

Záznamy směrovací tabulky lze použít k ukládání následujících typů cesty:

Identifikátory přímo připojených sítí. Cesty k identifikátorům sítí, které jsou přímo připojené. U přímo připojených sítí může být pole Následující skok prázdné nebo může obsahovat adresu IP rozhraní této sítě.

Identifikátory vzdálených sítí. Cesty pro identifikátory sítí, které nejsou přímo připojeny, ale jsou dosažitelné přes další směrovače. Pro vzdálené síť je pole Následující skok vyplněno adresou IP lokálního směrovače mezi předávajícím uzlem a vzdálenou sítí.

Hostitelské cesty. Cesta na určitou adresu IP. Hostitelské cesty umožňují zobrazování směrování podle adres IP. U hostitelských cest je identifikátor sítě adresou IP určitého hostitele a síťová maska je 255.255.255.255.

Výchozí cesta. Výchozí cesta je navržena k použití v případě, že není nalezen určitý identifikátor sítě nebo určitá hostitelská cesta. Identifikátor výchozí cesty je 0.0.0.0 se síťovou maskou 0.0.0.0.

Proces určení cesty

Při určování, které záznamy směrovací tabulky budou použity pro rozhodnutí o předání, probíhá v IP následující proces:

- U každého záznamu ve směrovací tabulce se mezi adresou IP místa určení a síťovou maskou provede bit po bitu logická operace AND. Následuje porovnání výsledků s identifikátorem sítě.
- Sestaví se seznam souhlasných záznamů, přičemž je vybrána nejvíce souhlasící cesta (cesta, u které s adresou IP místa určení souhlasí největší počet bitů). Nejdelší souhlasná cesta je nejbližší cestou k adrese IP místa určení. Najde-li se více takových záznamů (například více cest ke stejnému identifikátoru sítě), použije směrovač pro výběr nejlepší cesty nejnižší metriku. Existuje-li více takových záznamů, může si směrovač vybrat, který záznam směrovací tabulky použije.

Konečným výsledkem procesu určení cesty je výběr jedné jediné cesty ze směrovací tabulky. Vybraná cesta poskytuje předávací adresu (adresu IP příštího skoku) a rozhraní (port). Není-li proces určování cesty úspěšný, IP vyhlásí chybu směrování. U odesílajícího hostitele se chyba směrování interně označí v protokolu horní vrstvy, například v TCP nebo UDP. U směrovače je odesláno do odesílajícího hostitele hlášení o nedosažitelnosti místa určení/nedosažitelnosti hostitele.

Příklad směrovací tabulky ve Windows 2000

Tabulka 1.28 znázorňuje přednastavenou směrovací tabulku pro hostitele (nikoli pro směrovač) na platformě Windows 2000. Tento hostitel má jeden síťový adaptér a adresu IP 157.55.27.90, masku podsítě 255.255.240.0 (/20) a přednastavenou bránu 157.55.16.1.

Tabulka 1.28 Směrovací tabulka ve Windows 2000

Síť určení	Síťová maska	Brána	Rozhraní	Metrika	Účel
0.0.0.0	0.0.0.0	157.55.16.1	157.55.27.90	1	Default Route
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	Loopback Network
157.55.16.0	255.255.240.0	157.55.27.90	157.55.27.90	1	Directly Attached Network
157.55.27.90	255.255.255.255	127.0.0.1	127.0.0.1	1	Local Host
157.55.255.255	255.255.255.255	157.55.27.90	157.55.27.90	1	Network Broadcast
224.0.0.0	224.0.0.0	157.55.27.90	157.55.27.90	1	Multicast Address
255.255.255.255	255.255.255.255	157.55.27.90	157.55.27.90	1	Limited Broadcast

Výchozí cesta Záznam odpovídající výchozí konfiguraci brány je síťovým určením 0.0.0.0 se síťovou maskou 0.0.0.0. Jakákoli adresa IP určení spojená logickou operací AND s 0.0.0.0 dává výsledek 0.0.0.0. Proto lze výchozí cestu spojit s každou adresou IP. V případě, že se použije výchozí cesta, protože nebyla nalezena žádná jiná lepší cesta, je paket IP postoupen adrese IP ve sloupci brána za použití rozhraní odpovídajícího adrese IP ve sloupci rozhraní.

Síť zpětné smyčky Záznam sítě zpětné smyčky je navržen pro přijetí jakékoli adresy IP ve tvaru 127.x.y.z. a jejímu předání na zvláštní zpětnou adresu 127.0.0.1.

Přímo připojená síť Záznam lokální sítě odpovídá přímo připojené síti. Pakety IP určené pro přímo připojenou síť nejsou předávány směrovači, ale posílány přímo na místo určení. Všimněte si, že sloupce brána a rozhraní odpovídají adrese IP uzlu. To znamená, že paket je poslán ze síťového adaptéru odpovídajícího adrese IP uzlu.

Lokální hostitel Záznam lokálního hostitele je trasa hostitele (síťová maska 255.255.255.255) odpovídající adrese IP hostitele. Všechny datagramy IP na adresu IP hostitele jsou předávány na adresu zpětné vazby.

Síťový všesměrový vysílání Záznam síťového všesměrového vysílání je trasa hostitele (síťová maska 255.255.255.255) odpovídající adresám všesměrového vysílání v podsítích (všechny podsítě sítě 157.55.0.0 třídy B). Pakety adresované všesměrovému vysílání v podsítích jsou zasílány ze síťového adaptéru odpovídající adrese IP uzlu.

Adresa vícesměrového vysílání adresa vícesměrového vysílání se svou maskou sítě třídy D je používána ke směrování jakýchkoli vícesměrových IP paketů ze síťového adaptéru odpovídající adrese IP uzlu.

Omezený všesměrový vysílání Adresa omezeného všesm. vys. je trasa hostitele (síťová maska 255.255.255.255). Pakety adresované omezenému v. v. jsou posílány ze síťového adaptéru odpovídajícího IP adrese uzlu.

Směrovací tabulku si lze ve Windows 2000 prohlédnout tak, že na příkazovém řádku Windows 2000 napíšete route print.

Kdy se určuje adresa IP předání nebo příštího skoku cesty ve směrovací tabulce:

- Je-li adresa brány stejná jako adresa rozhraní, je adresa IP předání nastavena na adresu IP místa určení paketu IP.
- Není-li adresa brány stejná jako adresa rozhraní, adresa IP předání je nastavena na adresu brány.

Je-li například paket zaslán na 157.55.16.48, je nejurčitější cestou cesta pro přímo připojenou síť (157.55.16.0/20). Adresa IP předání je nastavena na adresu IP místa určení (157.55.16.48) a rozhraní je síťový adaptér, kterému byla přiřazena IP adresa 157.55.27.90.

Směrovací proces

Směrovací proces IP zainteresovaný na všech uzlech do doručení paketu IP obsahuje: odesílajícího hostitele, zprostředkovávající směrovače a hostitele určení.

IP na odesílajícím hostiteli

Po odeslání paketu odesílajícím hostitelem je paket předán z protokolu horní vrstvy (TCP, UDP nebo ICMP) protokolu IP. IP na odesílajícím hostiteli provede následující kroky:

1. Nastaví hodnotu TTL buď na přednastavenou hodnotu nebo hodnotu odpovídající určité aplikaci.
2. Zkusí ve směrovací tabulce najít optimální cestu na adresu IP určení. Nenajde-li žádnou cestu, vyše chybové směrové hlášení protokolu horní vrstvy (TCP, UDP, ICMP).
3. V závislosti na nejpřesněji určené cestě určí předávací adresu IP a rozhraní, které budou použity k předání paketu.
4. Předá paket, předávací adresu IP a rozhraní protokolu ARP. ARP poté přiřadí předávací IP adresu MAC adrese a předá paket.

IP na směrovači

Po přijetí paketu na směrovači je postoupen IP, který provede následující kroky:

1. Ověří kontrolní součet IP hlavičky. Jestliže hlavička IP neprojde kontrolou, je IP paket vyřazen bez uvědomění uživatele. Toto je známo jako tiché vyřazení.
2. Ověří, zda IP adresa určení v IP datagramu odpovídá adrese IP přiřazené rozhraní směrovače. Pokud odpovídá, směrovač zpracuje datagram jako adresátský hostitel (viz krok 3 v následující části „IP na cíli“).
3. Není-li adresou IP určení směrovač, sníží hodnotu TTL o 1. Je-li TTL 0, směrovač vyřadí paket a pošle odesílateli hlášení o vypršení časového limitu.
4. Je-li TTL 1 nebo větší, zaktualizuje pole TTL a vypočítá nový kontrolní součet hlavičky IP.
5. Zkusí ve směrovací tabulce vyhledat optimální cestu k adrese IP cíle v IP datagramu. Nenajde-li žádnou cestu, směrovač vyřadí paket a odesílateli pošle hlášení o nedosažitelnosti místa určení/nedosažitelnosti sítě.
6. V závislosti na nalezené optimální cestě IP určí předávací adresu IP a rozhraní, které budou použity pro předání paketu.
7. IP předá paket, předávací adresu IP a rozhraní protokolu ARP. Poté ARP předá paket příslušné MAC adrese.

Celý tento proces je opakován na každém směrovači na trase mezi zdrojovým hostitelem a cílem.

IP na cíli

Po přijetí paketu na adresátském hostiteli je postoupen IP, který provede následující kroky:

1. Ověří kontrolní součet hlavičky IP. Jestliže hlavička IP neprojde kontrolou, je IP paket tiše vyřazen.
2. Ověří, zda adresa IP určení v datagramu IP odpovídá adrese IP přiřazené hostiteli. Neodpovídá-li, paket IP je tiše vyřazen.
3. V závislosti na poli protokolu IP postoupí datagram IP bez hlavičky IP příslušnému protokolu vyšší vrstvy. Neexistuje-li takový protokol, ICMP odesílateli pošle hlášení o nedosažitelnosti místa určení/nedosažitelnosti protokolu.
4. U TCP a UDP paketů je zkontrolován port určení a zpracován TCP segment nebo UDP hlavička.

Neexistuje-li pro číslo UDP portu žádná aplikace, pošle ICMP odesílateli hlášení o nedosažitelnosti místa určení/nedosažitelnosti portu. Neexistuje-li pro číslo TCP portu žádná aplikace, pošle TCP odesílateli segment vynulování spojení.

Statické a dynamické směrovače IP

Aby mohlo směrování IP mezi směrovači na síti probíhat efektivně, musí mít směrovače přesné znalosti o identifikátorech vzdálených sítí nebo musí mít správně nakonfigurovány přednastavené cesty. Na velkých sítích je jedním z problémů, kterým čelí síťoví administrátoři, způsob spravování směrovacích tabulek na směrovačích IP tak, aby tok IP probíhal optimální cestou a byl tolerantní k chybám.

Existují dva způsoby správy směrovacích tabulek na směrovačích IP :

- Manuální – Statické směrovače IP mají směrovací tabulky, které se mění pouze v případě, že změny manuálně provede síťový administrátor.

Statické směrování závisí na manuální správě směrovacích tabulek. Statistické směrovače neregistrují identifikátory vzdálených sítí, které je nutno manuálně nakonfigurovat. Statické směrovače též nejsou tolerantní k chybám. Jestliže přestane statický směrovač fungovat, okolní směrovače to nezaznamenají a neinformují ostatní směrovače.

- Automatický – Dynamické směrovače IP mají směrovací tabulky, které se mění automaticky v závislosti na komunikaci s ostatními směrovači.

Dynamické směrování využívá směrovací protokoly, například RIP (Routing Information Protocol) a OSPF (Open Shortest Path First), s jejichž pomocí dynamicky aktualizuje směrovací tabulku podle informací vyměňovaných mezi směrovači. Dynamické směrovače registrují identifikátory vzdálených sítí a zapisují je automaticky do směrovací tabulky. Dynamické směrovače jsou tolerantní k chybám. Jestliže přestane dynamický směrovač fungovat, okolní směrovače to zaznamenají a informují ostatní směrovače v síti o změně směrovacích informací.

Více podrobností o směrovacích principech najdete v části „Přehled o jednosměrovém směrování“ v knize Průvodci sítí ve Windows 2000. Více podrobností o směrovacích protokolech IP najdete v části „Přehled o IP směrování“ v knize Průvodci sítí ve Windows 2000.

Přiřazení fyzické adresy

V závislosti na adrese IP určení a procesu určení cesty určuje IP předávací adresu IP a rozhraní, které budou použity k předání paketu. Následně je předán paket IP, předávací adresa IP a rozhraní protokolu ARP.

Je-li předávací adresa IP stejná jako adresa IP určení, ARP provede přímé doručení. Při přímém doručení musí být k IP adrese určení přiřazena odpovídající MAC adresa.

Není-li předávací adresa stejná jako adresa IP určení, ARP provede nepřímé doručení. Předávací adresa je adresou IP směrovače mezi aktuálním IP uzlem a konečným určením. Při nepřímém doručení musí být k adrese IP směrovače přiřazena odpovídající MAC adresa.

K přiřazení předávací adresy IP k jí odpovídající MAC adrese používá ARP všesměrové vysílání založené na síťových technologiích sdíleného přístupu (například Ethernet nebo Token Ring), pomocí kterého posílá všesměrový ARP dotaz. Odesílateli ARP dotazu přijde zpět ARP odpověď obsahující MAC adresu odpovídající dotazované předávací adrese IP.

Vyrovňovací paměť ARP

Aby byl udržen počet všesměrově vysílaných ARP dotazů na minimum, mnoho protokolů TCP/IP zahrnuje vyrovňovací paměť ARP, tabulku nejposledněji přiřazených adres IP a jim odpovídajících adres MAC. Na vyrovňovací paměť se ARP poprvé obrací před odesláním ARP dotazu. Každé rozhraní má vlastní vyrovňovací paměť ARP.

V závislosti na implementaci může vyrovňovací paměť ARP disponovat následujícími vlastnostmi:

- Záznamy vyrovňovací paměti ARP mohou být dynamické (založené na odpovědích ARP) nebo statické. Statické záznamy ARP jsou trvalé a jsou manuálně přidávány za pomoci nástrojů TCP/IP, jako je například nástroj ARP dodávaná s Windows 2000. Statické záznamy ARP se používají k zabránění dotazům ARP na běž-

ně používané lokální adresy IP, například směrovače nebo servery. Problémem těchto záznamů je, že musí být při změně vybavení síťového rozhraní aktualizovány manuálně.

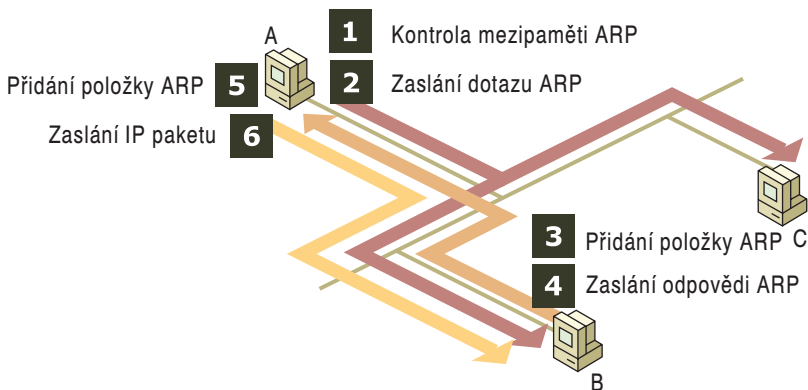
- Záznamům dynamické vyrovnávací paměti ARP je přiřazena hodnota časové platnosti, na základě které jsou záznamy z vyrovnávací paměti po určitém čase odstraněny. Záznamy dynamické vyrovnávací paměti ARP v TCP/IP pod Windows 2000 zůstávají v paměti maximálně 10 minut a poté jsou odstraněny.

Vyrovňovací paměť na počítači na platformě Windows 2000 si můžete prohlédnout, když na příkazovém řádku Windows 2000 napíšete `arp -a`.

Proces ARP

IP posílá informace ARP, který obdrží paket IP, předávací adresu IP a rozhraní, které budou použity při předání paketu. Bez ohledu na to, jestli se jedná o přímé nebo nepřímé doručení, ARP provádí následující úkony, viz 1.15:

1. V závislosti na rozhraní a předávací adrese IP ARP nahlíží do příslušné vyrovnávací paměti ARP a hledá tam záznam o předávací adrese IP. Nalezne-li takový záznam, přeskočí až do kroku 6.
2. Není-li takový záznam nalezen, ARP vytvoří dotaz ARP obsahující adresu MAC rozhraní odesílajícího ARP dotaz, adresu IP rozhraní odesílajícího dotaz ARP a předávací adresu IP. ARP pak pomocí příslušného rozhraní odešle dotaz ARP pomocí všesměrového vysílání.
3. Všichni hostitelé obdrží vyslaný dotaz a tento dotaz je zpracován. Jestliže adresa IP přijímajícího hostitele souhlasí s požadovanou adresou IP (předávací adresa IP), je jeho vyrovnávací paměť ARP aktualizována přiřazením adresy odesílatele dotazu. Jestliže adresa IP přijímajícího hostitele nesouhlasí s požadovanou adresou IP, je dotaz ARP tiše vyřazen.
4. Přijímající hostitel zformuluje odpověď ARP obsahující adresu MAC a pošle ji přímo odesílateli dotazu.
5. Po obdržení odpovědi ARP odesílatel dotazu je jeho vyrovnávací paměť ARP aktualizována přiřazením adresy.
6. Mezi dotazem ARP a odpovědí ARP si oba hostitelé uloží vzájemné přiřazení adres do svých vyrovnávacích pamětí ARP.
7. Paket IP je odeslán předávajícímu hostiteli pomocí adresování na přiřazenou adresu MAC.



Obrázek 1.15 Proces ARP

Další informace

Podrobnější informace o TCP/IP najdete v:

- *Internetworking with TCP/IP*, Vol. 1, 3rd Edition by Douglas Comer, 1996, Englewood Cliffs, NJ: Prentice Hall.
- *Microsoft Windows 2000 TCP/IP Protocols and Services Technical Reference* by Thomas Lee and Joseph Davies, 1999, Redmond, WA: Microsoft Press.
- *TCP/IP Illustrated, Volume 1, The Protocols* by Richard W. Stevens, 1994, Reading, MA: Addison-Wesley.

2. KAPITOLA

Windows 2000 TCP/IP

Microsoft používá pro své platformy TCP/IP jako klíčové protokoly pro síťový přenos. 32bitový TCP/IP společnosti Microsoft pro Microsoft® Windows® 2000 je vysokovýkonnostní, přenosná 32bitová implementace průmyslového standardu protokolu TCP/IP. Ovladač protokolu TCP/IP pro Windows 2000 je sdílen všemi 32bitovými sadami protokolu TCP/IP společnosti Microsoft, včetně TCP/IP pro Microsoft® Windows NT® Server, Microsoft® Windows NT® Workstation, Microsoft® Windows® 95 a Microsoft® Windows® 98. Nicméně jsou mezi nimi malé rozdíly v implementaci, metodách konfigurace a dostupných službách.

Tato kapitola je určena pro síťové inženýry a pracovníky podpory, kteří již znají TCP/IP nebo kteří již četli kapitolu „Úvod do TCP/IP“ a produktovou dokumentaci k TCP/IP dodávanou s Windows 2000.

V této kapitole najdete:

Přehled TCP/IP pro Windows 2000	54
Architektura Microsoft TCP/IP pro Windows 2000	57
Rozhraní NDIS a další	58
Komponenty základních protokolů	61
Rozhraní síťových aplikací	89
Klientské služby a součásti	99

Další informace v této knize

- Podrobnější informace o síťové architektuře Windows 2000 najdete v části „Síťová architektura systému Windows 2000“.
- Podrobnější informace o protokolu TCP/IP najdete v části „Úvod do TCP/IP“.
- Podrobnější informace o řešení problémů s TCP/IP najdete v části „Řešení problémů protokolu TCP/IP“.

Poznámka: V této kapitole najdete mnoho zmínek o záznamech registru ve Windows 2000 pro TCP/IP. Podrobnější informace o těchto záznamech najdete v adresáři *Technické odkazy na registr Windows 2000* (Regentry.chm) na CD-ROM dodávaném s touto knihou.

Přehled TCP/IP pro Windows 2000

Sada protokolů TCP/IP pro Windows 2000 je navržena tak, aby usnadňovala integraci systémů společnosti Microsoft do rozsáhlých sítí komerčních, vládních a veřejných a aby umožňovala bezpečnou práci nad těmito sítěmi. Pomocí TCP/IP se Windows 2000 mohou okamžitě připojit a pracovat na Internetu.

Standardní vlastnosti a zlepšení výkonu

TCP/IP pro Windows 2000 podporuje následující standardní vlastnosti:

- Možnost svázat více síťových adaptérů s různými typy médií
- Logický a fyzický multihoming
- Interního IP směrování
- IGMP (Internet Group Management Protocol, protokol na správu Internetových skupin) verze 2 (podpora pro víceměrové vysílání IP)
- Detekce zdvojených IP adres
- ICMP (Internet Control Message Protocol) vyhledání směrovače
- Vícenásobné konfigurovatelné přednastavené brány
- Detekce nefunkčních bran pro provoz TCP
- Automatické PMTU (Automatic Path Maximum Transmission Unit) vyhledání pro spojení TCP
- IPSec (Bezpečnost IP)
- QoS (Kvalita služeb)
- TCP/IP nad službami ATM
- Virtuální soukromé sítě (VPN)

Navíc má operační systém Windows 2000 následující zlepšení výkonu:

- Zvětšenou výchozí velikost oken
- Nastavitelnou velikost oken TCP
- SACK (Selective Acknowledgement) – výběrové potvrzování
- Rychlý opětovný přenos TCP
- Zlepšení výpočtu RTT (Round Trip Time) a RTO (Retransmission Timeout)

Dostupné služby

Operační systém Windows 2000 poskytuje následující služby:

- DHCP (protokol dynamické konfigurace hostitele) klient a server
- WINS a NetBIOS klient a server
- DNS klient a server
- Podpora vytáčení (protokol PPP/sériové linky)
- Protokol PPTP a L2TP používané pro virtuální soukromé sítě
- Síťový tisk TCP/IP (Lpr/Lpd)
- Agent protokolu SNMP
- Rozhraní NetBIOSu
- Rozhraní Windows Sockets verze 2

- Podpora prohledávání sítě přes IP směrovače
- Vysokovýkonnostní služby informací o Internetu
- Základní TCP/IP nástroje pro připojení, včetně Finger, FTP, Rcp, Rexec, Rsh, Telnet a Tftp.
- Software pro klienta i server pro jednoduché síťové protokoly, včetně Character Generator, Daytime, Discard, Echo a Quote of the Day.
- Nástroje pro správu a diagnostiku TCP/IP, včetně Arp, Hostname, Ipconfig, Lpq, Nbtstat, Netstat, Ping, Route, Nslookup, Tracert a Pathping.

RFC týkající se Internetu podporovaná TCP/IP pro Microsoft Windows 2000

Dokumenty RFC jsou plynule se rozrůstající řadou zpráv, návrhů protokolů a standardů protokolů používaných Internetovou veřejností. TCP/IP pro Windows 2000 podporuje RFC uvedené v tabulce 2.1.

Tabulka 2.1 RFC podporovaná Windows 2000

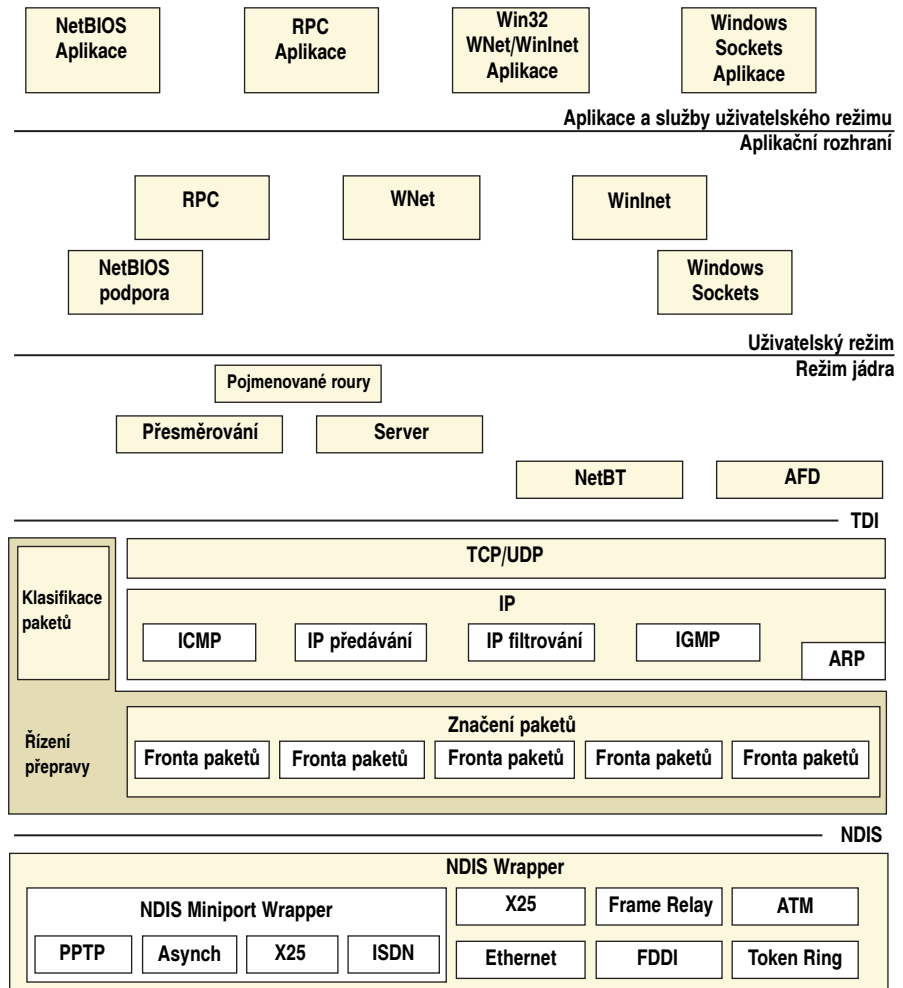
RFC	Název
768	User Datagram Protocol (UDP)
783	Trivial File Transfer Protocol (TFTP)
791	Internet Protocol (IP)
792	Internet Control Message Protocol (ICMP)
793	Transmission Control Protocol (TCP)
816	Fault Isolation and Recovery
826	Address Resolution Protocol (ARP)
854	Telnet Protocol (Telnet)
862	Echo Protocol (ECHO)
863	Discard Protocol (DISCARD)
864	Character Generator Protocol (CHARGEN)
865	Quote of the Day Protocol (QUOTE)
867	Daytime Protocol (DAYTIME)
894	IP over Ethernet
919, 922	IP Broadcast Datagrams (broadcasting with subnets)
950	Internet Standard Subnetting Procedure
959	File Transfer Protocol (FTP)
1001, 1002	NetBIOS Service Protocols
1009	Requirements for Internet Gateways
1034, 1035	Domain Name System (DNS)
1042	A Standard for the Transmission of IP Datagrams over IEEE 802 Networks
1055	Transmission of IP over Serial Lines (IP-SLIP)
1112	Internet Group Management Protocol (IGMP)
1122, 1123	Host Requirements (communications and applications)
1144	Compressing TCP/IP Headers for Low-Speed Serial Links

Tabulka 2.1 RFC podporovaná Windows 2000

RFC	Název
1157	Simple Network Management Protocol (SNMP)
1179	Line Printer Daemon Protocol
1188	IP over FDDI
1191	Path Discovery
1201	IP over ARCNET
1256	ICMP Router Discovery Messages
1323	TCP Extensions for High Performance
1332	PPP Internet Protocol Control Protocol (IPCP)
1334	PPP Authentication Protocols
1518	An Architecture for IP Address Allocation with Classless Inter-Domain Routing (CIDR)
1519	CIDR: An Address Assignment and Aggregation Strategy
1533	DHCP Options and Bootstrap Protocol (BOOTP) Vendor Extensions
1534	Interoperation Between DHCP and BOOTP
1552	PPP Internetwork Packet Exchange Control Protocol (IPXCP)
1661	Point-to-Point Protocol (PPP)
1662	PPP in HDLC-like Framing
1748	IEEE 802.5 MIB using SMIPv2
1749	IEEE 802.5 Station Source Routing MIB using SMIPv2
1812	Requirements for IP Version 4 Routers
1828	IP Authentication using Keyed MD5
1829	ESP DES-CBC Transform
1851	ESP Triple DES-CBC Transform
1852	IP Authentication using Keyed SHA
1878	Variable Length Subnet Table For IPv4
1994	PPP Challenge Handshake Authentication Protocol (CHAP)
2018	TCP Selective Acknowledgment Options
2085	HMAC-MD5 IP Authentication with Replay Prevention
2104	HMAC: Keyed Hashing for Message Authentication
2131	Dynamic Host Configuration Protocol (DHCP)
2132	Clarifications and Extensions for the Bootstrap Protocol
2136	Dynamic Updates in the Domain Name System (DNS UPDATE)
2205	Resource Reservation Protocol (RSVP) – Version 1 Functional Specification
2236	Internet Group Management Protocol, Version 2
2401	Security Architecture for the Internet Protocol
2402	IP Authentication Header (AH)
2406	IP Encapsulating Security Payload (ESP)
2637	Point-to-Point Tunneling Protocol (PPTP)
2661	Layer Two Tunneling Protocol (L2TP)

Architektura Microsoft TCP/IP pro Windows 2000

Prvky a služby protokolu jádra Microsoft TCP/IP a rozhraní mezi nimi jsou zobrazeny na obrázku 2.1. TDI (Transport Driver Interface) a NDIS (Network Device Interface Specification) jsou veřejně přístupné a jejich specifikace jsou dostupné ve společnosti Microsoft. Navíc existuje řada rozhraní vyšší úrovně dostupných aplikacím ze strany uživatele. Nejčastěji používané jsou Windows Sockets, RPC (Remote Procedure Call) a NetBIOS. Více podrobností o TDI, NDIS, Windows Sockets, RPC a NetBIOS najdete dále v části „Síťová architektura systému Windows 2000“. Více podrobností o podpoře Windows Sockets pro Windows 2000 TCP/IP najdete v části „Windows Sockets“. Více podrobností o podpoře NetBIOS pro Windows 2000 TCP/IP najdete v části „NetBIOS pro TCP/IP“.



Obrázek 2.1 TCP/IP v síťové architektuře Windows 2000

Rozhraní NDIS a další

Síťové protokoly společnosti Microsoft používají ke komunikaci s ovladači síťových karet NDIS (Network Device Interface Specification). Do sady protokolů je též implementováno mnoho z funkcionality vrstvy datového spoje referenčního modelu OSI (Open System Interconnection). To velmi usnadňuje vývoj ovladačů síťových karet.

NDIS a TCP/IP

NDIS 5.0 zahrnuje následující rozšíření:

- Správa napájení NDIS (požadováno pro správu napájení sítě a probuzení sítě).
- Plug and Play.
- Mechanismy odlehčení úloh pro úlohy jako kontrolní součet TCP a UDP a rychlé předávání paketů.
- Podpora QoS
- Podpora zprostředkujícího ovladače (požadované pro broadcast PC, VLAN, rozvržení paketů pro QoS a pro podporu NDIS síťových zařízení IEEE 1394).

NDIS může vypnout síťové adaptéry, když systém žádá o změnu úrovně spotřeby. Tento požadavek může iniciovat jak uživatel, tak systém. Například uživatel chce počítač uspat nebo počítač žádá změnu úrovně spotřeby na základě nulové aktivity klávesnice nebo myši. Navíc odpojení síťového kabelu může iniciovat žádost o vypnutí, tedy za předpokladu, že síťový adaptér tuto funkcionalitu podporuje. V takovém případě systém před vypnutím síťového adaptéru čeká určitou nastavitelnou dobu, protože odpojení může být výsledkem dočasných změn na vedení na síti spíše než odpojení kabelu od síťového zařízení jako takového.

Zásady NDIS správy spotřeby jsou založeny na nulové síťové aktivitě. To znamená, že všechny překrývající se síťové komponenty musí s žádostí souhlasit před tím, než může být síťový adaptér vypnut. Jestliže je nad sítí nějaká aktivní relace nebo otevřený soubor, žádost o vypnutí může být odmítnuta kteroukoli ze zainteresovaných komponent nebo všemi zainteresovanými komponentami.

Počítač může být také probuzen ze stavu s nízkou spotřebou energie na základě síťové události. Příčinou budícího signálu může být:

- Detekce změny ve stavu připojení k síti (například přepojení kabelu).
- Obdržení rámce probuzení sítě.
- Obdržení paketu Magic. Paket Magic je paket, který obsahuje 16 sousedících kopií MAC adresy síťového adaptéru.

Při inicializaci ovladače NDIS zjišťuje schopnosti ovladače miniportu, aby určil, zda podporuje takové věci jako paket Magic, souhlas vzorku nebo probuzení při změně propojení, a aby určil nejnížší požadovanou spotřebu pro každou metodu buzení. Síťové protokoly se pak dotáží na schopnosti miniportu. Při spuštění protokol nastaví zásady buzení pomocí speciálních vlastností, jako je Enable Wakeup, Set Packet Pattern a Remove Packet Pattern.

Aktuálně je Microsoft TCP/IP jedinou sadou protokolů společnosti Microsoft, která podporuje síťovou správu spotřeby. Při inicializaci miniportu registruje následující vzorky paketů:

- Odeslaný IP paket

- ARP všesměrové vysílání pro adresu IP stanice
 - NetBIOS nad TCP/IP všesměrovým vysíláním pro název počítače přiřazený stanici
- Ovladače kompatibilní s NDIS jsou dostupné pro široké spektrum síťových adaptérů od mnoha výrobců. Rozhraní NDIS umožňuje mnoha ovladačům protokolů různých typů, aby se navázaly na jeden ovladač síťového adaptéru, a umožňuje také jednomu protokolu se navázat na mnoho ovladačů síťových adaptérů. Specifikace NDIS popisuje vícenásobný mechanismus k tomu používaný. Vázání lze ve Windows 2000 prohlížet nebo měnit ze složky Network and Dial-up Connections.

Windows 2000 TCP/IP doporučuje:

- FDDI (Fiber Distributed Data Interface)
- Token Ring (IEEE 802.5)
- ATM (Asynchronous Transfer Mode)

Použití LANE (emulace LAN), ATM LAN karet v TCP/IP vypadá jako Ethernetová karta.
- ARCnet (Attached Resource Computer network)
- Vyhrazené linky WAN, například dataphone Digital Service (DDS) a T-carrier (Fractional T1, T1 a T3)
- WAN služby přepínané vytáčeným nebo trvalým okruhem, například analogový telefon, ISDN nebo xDSL.
- WAN služby přepínané paketem, například X.25, Frame Relay a ATM.
- Ethernet

Zapouzdření Ethernetu II je přednastavené. Pomocí změny hodnoty záznamu **ArpUseEtherSNAP** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters) na 1 můžete vybrat zapouzdření IEEE 802.3 SNAP. Windows 2000 TCP/IP přijímá oba typy rámce bez ohledu na hodnotu **ArpUseEtherSNAP**.

Upozornění: K přímému editování registru používejte editor registru jen tehdy, nemáte-li jinou možnost. Editory registru obcházejí standardní bezpečnostní opatření poskytované nástroji pro správu. Tato bezpečnostní opatření brání vložení konfliktního nastavení nebo nastavení, které pravděpodobně sníží výkon nebo poškodí systém. Přímé editování registru může mít vážné, neočekávané důsledky, které mohou bránit startu systému a mohou vyžadovat reinstalaci Windows 2000. Jakmile je to možné, používejte ke konfiguraci nebo upravení Windows 2000 programy v Ovládacích panelech nebo konzolu Microsoft Management Console.

► Výběr zapouzdření IEEE 802.3 SNAP

1. Na hlavním panelu klepněte na tlačítko Start a potom na tlačítko Spustit.
2. V dialogu Otevřít napište regedt32.exe a klepněte na OK.
3. V editoru registru přejděte na HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.
4. Vyberte záznam ArpUseEtherSNAP a změňte jeho hodnotu na 1.

Funkcionalita vrstvy připojení

Funkcionalita této vrstvy je rozdělena mezi kombinaci síťového adaptéru/ovladače a ovladač sady protokolů nízké úrovně. Pro LAN média jsou filtry kombinace síťového adaptéru/ovladače založeny na MAC adrese určení každého rámce.

Normálně hardware pro lokální síť odfiltruje všechny příchozí rámce kromě těch, které obsahují jednu z následujících adres určení:

- MAC adresa jednosměrného vysílání adaptéru.
- Adresa všesměrového vysílání (pro Ethernet je adresa všesměrového vysílání 0xFF-FF-FF-FF-FF-FF).
- Adresy vícesměrového vysílání, které jsou ovladačem přihlášeny v hardwaru.

Obsahuje-li rámec jednu z těchto adres jako adresu určení MAC, je v rámci pomoci kontrolního součtu zkontrolována integrita úrovně bitů.

Všechny rámce, které vyhoví testům adresy určení a kontrolního součtu, jsou poté prostřednictvím hardwarového přerušení postoupeny ovladači síťového adaptéru. Ovladač síťového adaptéru je software, který běží na počítači, takže všechny rámce, které projdou tak daleko, vyžadují ke zpracování určitý procesorový čas. Ovladač síťového adaptéru přenáší z karty rozhraní rámec do systémové paměti. Potom je rámec předán příslušným svázaným transportním ovladačům v tom pořadí, jak jsou svázané. Více podrobností o tomto procesu najdete ve specifikaci NDIS 5.0.

Jak paket přejde přes síť nebo několik sítí, je zdrojovou MAC adresou vždycky adresa síťového adaptéru, který paket vložil na médium a MAC adresou určení je adresa síťového adaptéru, který má paket stáhnout z média. To znamená, že na síti se směrovači se MAC adresy zdroje a určení mění s každým dalším směrováním přes zařízení síťové vrstvy (přepnutí směrovače nebo vrstvy 3).

Největší přenosová jednotka (MTU)

U každého typu média existuje maximální velikost rámce nazvaná největší přenosová jednotka, kterou nelze překročit. Úkolem vrstvy připojení je zjištění jednotky MTU a nahlášení této hodnoty protokolům uvedeným výše. Ovladače NDIS mohou být dotazovány na lokální MTU sadou protokolů. Znalost jednotky MTU rozhraní je používána protokoly horní vrstvy, například TCP, které pro každé médium automaticky optimalizují velikost paketů. Více podrobností najdete v diskusi o zpřístupnění *PMTU (Path Maximum Transmission Unit)* v části „Protokol ICMP (Internet Control Message Protocol)“ dále v této kapitole.

Používá-li ovladač síťového adaptéru – například ovladač ATM – režim emulace LAN, může hlásit, že má jednotku MTU vyšší než je očekáváno pro tento typ média. Například může emulovat Ethernet ale vykazovat jednotku MTU 9180 bajtů. Windows 2000 akceptují a používají velikost MTU vykazovanou adaptérem, i když přesahuje normální MTU pro příslušný typ média.

Někdy může být MTU nahlášené sadě protokolů menší než lze pro daný typ média očekávat. Například, použití standardu 802.1p často snižuje hlášené MTU o 4 bajty kvůli větším hlavičkám vrstvy datového spoje.

Komponenty základních protokolů

Komponenty základních protokolů jsou ty, které vidíte na obrázku 2.1 mezi rozhraními NDIS a TDI. Ve Windows 2000 jsou implementovány v ovladači Tcpip.sys a jsou dostupné přes rozhraní TDI a NDIS. Určitou podporu „syrovému“ přístupu k sadě protokolů poskytuje také rozhraní Winsock2.

Protokol ARP (Address Resolution Protocol)

Protokol ARP (Address Resolution Protocol) přiřazuje odesílaným paketům adresu IP k adrese MAC. Při zapouzdření každého odesílaného adresovaného IP datagramu do rámce musí být přidána adresa MAC zdroje a místa určení. Určení adresy MAC cíle pro každý rámec je úkolem protokolu ARP.

Jak již bylo uvedeno v části „Úvod do TCP/IP“, je výsledkem směrovacího procesu IP pro odchozí IP datagram výběr rozhraní (síťového adaptéru) a předávací adresy IP. protokol ARP porovnává předávací adresu IP u každého odchozího IP datagramu s mezipamětí ARP síťového adaptéru, přes který je paket odeslán. Je-li zde souhlasný záznam, je použita MAC adresa získaná z mezipaměti ARP. Není-li v mezipaměti ARP žádný souhlasný záznam, protokol ARP prostřednictvím všesměrového vysílání odešle žádost na lokální podsít, aby vlastník příslušné adresy IP ve své odpovědi sdělil svou MAC adresu. Po obdržení odpovědi ARP dojde k aktualizaci mezipaměti ARP novými informacemi a adresování paketu na vrstvě datového spojení.

Poznámka Popsaný proces a funkcionality protokolu ARP se aplikuje pouze na jednosměrové IP vysílání. Vícesměrové IP vysílání je posíláno na zvláštní vícesměrovou MAC adresu, která závisí na vícesměrové adrese IP. Více podrobností najdete dále v této kapitole v části „Protokol IGMP (Internet Group Management Protocol)“.

Používání nástroje ARP

Nástroj ARP můžete používat k prohlížení, přidávání nebo odstranění záznamů v mezipaměti ARP, viz následující příklady. Všimněte si, že záznamy přidávané manuálně jsou statické a nejsou automaticky z mezipaměti ARP po uplynutí určité lhůty odstraněny.

Příkaz **arp -a** lze použít k prohlížení mezipaměti ARP takto:

```
C:\>arp -a
```

```
Interface: 192.168.40.123
  Internet Address      Physical Address      Type
  192.168.40.1          00-00-0c-1a-eb-c5    dynamic
  192.168.40.124        00-dd-01-07-57-15    dynamic
Interface: 10.57.8.190
  Internet Address      Physical Address      Type
  10.57.9.138           00-20-af-1d-2b-91    dynamic
```

Počítač je v tomto případě vícedomý (má více než jeden síťový adaptér), takže pro každé rozhraní existuje zvláštní mezipaměť ARP.

V následujícím příkladě je použit příkaz **arp -s** k přidání statického záznamu pro hostitele, jehož adresa IP je 10.57.10.32 a jehož MAC adresa je 00-60-8C-0E-6C-6A, do mezipaměti ARP jako druhého rozhraní:

```
C:\>arp -s 10.57.10.32 00-60-8c-0e-6c-6a 10.57.8.190
```

```
C:\>arp -a
```

```
Interface: 192.168.40.123
  Internet Address   Physical Address   Type
  192.168.40.1       00-00-0c-1a-eb-c5   dynamic
  192.168.40.124     00-dd-01-07-57-15   dynamic
```

```
Interface: 10.57.8.190
  Internet Address   Physical Address   Type
  10.57.9.138        00-20-af-1d-2b-91   dynamic
  10.57.10.32        00-60-8c-0e-6c-6a   static
```

Pro vymazání záznamů z mezipaměti použijte příkaz **arp -d**. Například pro odstranění záznamu pro 10.57.10.32 z mezipaměti ARP takto:

```
C:\>arp -d 10.57.10.32
```

```
C:\>arp -a
```

```
Interface: 192.168.40.123
  Internet Address   Physical Address   Type
  192.168.40.1       00-00-0c-1a-eb-c5   dynamic
  192.168.40.124     00-dd-01-07-57-15   dynamic
```

```
Interface: 10.57.8.190
  Internet Address   Physical Address   Type
  10.57.9.138        00-20-af-1d-2b-91   dynamic
```

Stárnutí mezipaměti ARP

Operační systém Windows 2000 automaticky upravuje velikost mezipaměti ARP tak, aby odpovídala potřebám systému. Jestliže záznam v mezipaměti není využit žádným odchozím datagramem po dobu dvou minut, dojde k odstranění takového záznamu z mezipaměti ARP. Záznamům, na které se odkazovalo, se tato doba prodlužuje vždy po dvouminutových přírůstcích až do celkové doby platnosti 10 minut. Po deseti minutách je záznam z mezipaměti ARP odstraněn a musí být za pomoci rámce požadavku ARP znovu zpřístupněn. K úpravě doby, po kterou neodkazovaný záznam může zůstat v mezipaměti ARP, změňte hodnotu v klíči **ArpCacheLife** a **ArpCacheMinReferencedLife** (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

Statické záznamy přidané pomocí příkazu **arp -s** nejsou z mezipaměti automaticky odstraňovány. Mezipaměť ARP je mazána na základě inicializace protokolu TCP/IP. Statické záznamy mezipaměti ARP zůstanou při každém startu počítače, když vytvoříte soubor příkazů s příkazy ARP a do složky Po spuštění umístíte zástupce tohoto souboru.

Aktualizace záznamů v mezipaměti ARP

Kromě vytváření záznamů mezipaměti ARP prostřednictvím přijetí ARP odpovědi, jsou záznamy mezipaměti ARP aktualizovány při přijetí mapování prostřednictvím požadav-

ku ARP. Jinak řečeno, jestliže je adresa IP odesílatele ARP požadavku v mezipaměti, záznam se aktualizuje MAC adresou odesílatele. Takto jsou uzly, které mají v mezipaměti ARP o odesílateli statické nebo dynamické záznamy, aktualizovány aktuální MAC adresou odesílatele pomocí ARP požadavku. Uzel, jehož rozhraní a MAC adresa se změní, aktualizuje mezipaměti ARP obsahující záznam pro tento uzel při následujícím odeslání ARP požadavku.

Zprávy ARP a UDP

Ve frontě ARP je pouze jeden odchozí IP datagram pro určitou adresu určení, zatímco tato adresa IP je přiřazována MAC adrese. Jestliže aplikace na bázi UDP pošle několik IP datagramů na jednu adresu určení bez jakýchkoli mezer mezi nimi, některé z datagramů mohou být zahozeny, pokud neexistuje žádný záznam v mezipaměti ARP. Aplikace toto může kompenzovat voláním rutiny Iphlpapi.dll SendArpO, přičemž tato rutina vytvoří před odesláním proudu paketů záznam mezipaměti ARP. Další informace najdete v knize SDK (Software Development Kit).

Protokol sítě Internet (Protokol IP)

Vezmeme-li v úvahu zásobníky protokolu TCP/IP, je protokol IP místem, kde probíhá třídění a doručování paketů. V této vrstvě se na každý příchozí nebo odchozí paket odkazuje jako na datagram. Každý IP datagram nese zdrojovou adresu IP odesílatele a cílovou adresu IP zamýšleného adresáta. Na rozdíl od MAC adres zůstávají adresy IP v datagramu po celou cestu přes veřejnou síť nebo síť typu Intranet, pokud nejsou změněny službou NAT (Network Address Translator). Vrstva IP funguje tak, jak je popsáno v následujících částech.

Směrování

Směrování je primární funkcí protokolu IP. Datagramy jsou protokolu IP předávány ze síťových adaptérů. Každý datagram je označen adresou IP zdroje a místa určení. Protokol IP na každém datagramu zkontroluje cílovou adresu, porovná ji s lokálně spravovanou směrovací tabulkou IP a rozhodne, co se bude dít dál. Pro každý datagram existují tři možnosti:

- Může být postoupen protokolové vrstvě nad protokolem IP na lokálním hostiteli.
- Může být předán pomocí jednoho z lokálně připojených síťových adaptérů.
- Může být vyřazen.

Záznam ve směrovací tabulce IP ve Windows 2000 obsahuje následující informace:

Cíl v síti ID sítě odpovídající cestě. Cíl v síti může být třídní, podsíťový nebo nadsíťový nebo adresa IP trasy hostitele.

Síťová maska Maska používaná k přiřazení cílové adresy IP cíli v síti.

Brána Předávací adresa IP nebo adresa IP s dalším směrováním na cíl v síti.

Rozhraní adresa IP odpovídající síťovému rozhraní, které je použito k předání IP datagramu.

Metrika Číslo používané k vyjádření nákladů na trasu tak, aby bylo možno vybrat nejlepší možnou trasu mezi mnoha trasami na stejný cíl. Běžně se metrika používá

k označení počtu dalších předání (přechodů směrovačů) k cíli v síti. Jestliže dvě trasy mají stejný cíl v síti a stejnou síťovou masku, je nejlepší trasou ta s nejnižší metrikou.

Záznamy směrové tabulky mohou být použity k uložení následujících typů trasy:

Trasy přímo připojených ID sítě Tyto trasy jsou pro ID sítě, která jsou přímo připojena. Pro přímo připojené síť je adresa IP brány adresou IP rozhraní na této síti.

Trasy vzdálených ID sítě Tyto trasy jsou pro ID sítě, která nejsou přímo připojena, ale jsou dostupná přes další směrovače. Pro nepřímo připojené síť je adresa IP brány adresou IP lokálního směrovače mezi předávajícím uzlem a vzdálenou sítí.

Hostitelské trasy Tyto trasy jsou pro určité adresy IP. Hostitelské trasy umožňují, že se směrování odehrává na základě jednotlivých IP adres. U hostitelských tras je cíl v síti adresou IP určitého hostitele a maska podsítě je 255.255.255.255.

Výchozí trasy Tyto trasy jsou navrženy pro použití v případě, že nebylo nalezeno určitější ID sítě nebo hostitelská trasa. Cíl v síti u přednastavené trasy je 0.0.0.0 s maskou podsítě 0.0.0.0.

Proces určení trasy

Při určování jednotlivé trasy k předání IP datagramu používá protokol IP následující postup:

1. Pro každou trasu ve směrovací tabulce protokol IP provede logický součin mezi cílovou adresou IP a síťové masky. IP porovná výsledek logického součinu s cílem v síti. Jestliže souhlasí, protokol IP označí trasu jako souhlasící s cílovou adresou IP.
2. Ze seznamu souhlasných tras IP určí trasu, která má v síťové masce nejvíce bitů. To je trasa, která odpovídala nejvíce bitům v cílové adrese IP, a je proto nejurčitější trasou pro IP datagram. Toto je známo jako hledání nejdelsí nebo nejvíce shodné trasy.
3. Je-li nalezeno více nejvíce shodných tras, protokol IP použije trasu s nejnižší metrikou.
4. Je-li nalezeno více nejvíce shodných tras s nejnižší metrikou, protokol IP z těchto tras vybere náhodným výběrem.

Při určování předávací adresy IP nebo adresy IP s dalším předáním z vybrané trasy používá protokol IP následující postup:

- Je-li adresa IP brány stejná jako adresa rozhraní, je předávací adresa IP nastavena na cílovou adresu IP IP paketu.
- Není-li adresa IP brány stejná jako adresa rozhraní, je předávací adresa IP nastavena na adresu brány.

Koncovým výsledkem *procesu určení trasy* je výběr jediné trasy ze směrovací tabulky. Vybraná trasa poskytuje předávací adresu IP (adresa IP brány nebo cílová adresa IP IP datagramu) a rozhraní (určené prostřednictvím adresy IP rozhraní). Jestliže proces určení trasy nenajde žádnou adresu, protokol IP vyhlásí směrovací chybu. U odesílajícího hostitele je směrovací chyba interně oznámena protokolu horní vrstvy, například protokolu TCP nebo UDP. Co se týče směrovače, je IP datagram vyřazen a zdrojovému hostiteli je poslána zpráva „Destination Unreachable-Host Unreachable“.

Používání nástroje Route

K prohlížení, přidávání nebo odstraňování tras ze směrovací IP tabulky lze používat nástroje Route.

Prohlížení směrovací IP tabulky

K prohlížení směrovací tabulky z příkazového řádku můžete použít příkaz **route print**. Následující směrovací IP tabulka je pro počítač na platformě Windows 2000 s adresou IP 10.1.1.99, maskou podsítě 255.255.255.0 a výchozí bránou 10.1.1.1:

```
C:\>route print
```

Interface List

```
0x1 ..... MS TCP Loopback interface
0x2 ...00 a0 24 e9 cf 45 ..... 3Com 3C90x Ethernet Adapter
```

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	10.1.1.1	10.1.1.99	1
	10.1.1.0	255.255.255.0	10.1.1.99	10.1.1.99	1
	10.1.1.99	255.255.255.255	127.0.0.1	127.0.0.1	1
	10.255.255.255	255.255.255.255	10.1.1.99	10.1.1.99	1
	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
	224.0.0.0	224.0.0.0	10.1.1.99	10.1.1.99	1
	255.255.255.255	255.255.255.255	10.1.1.99	10.1.1.99	1

Persistent Routes:

None

Výchozí směrovací IP tabulka pro počítač na platformě Windows 2000 obsahuje následující trasy:

Výchozí trasa Výchozí trasou je trasa s cílem v síti 0.0.0.0 a síťovou maskou 0.0.0.0. Logický součin jakékoli cílové adresy IP s 0.0.0.0 má za výsledek opět 0.0.0.0. Proto lze výchozí trasu použít pro jakoukoli adresu IP. Jestliže je výchozí trasa vybrána z důvodu absence vhodnější trasy, je IP datagram předán na adresu IP ve sloupci brána za použití rozhraní odpovídajícího adrese IP uvedené ve sloupci rozhraní.

Přímo připojená síť Trasa s cílem v síti 10.1.1.0 a síťovou maskou 255.255.255.0 je trasou pro přímo připojenou síť. IP pakety určené pro přímo připojenou síť nejsou předávány směrovači, ale jsou přímo posílány na místo určení. Všimněte si, že adresa brány a rozhraní jsou adresou IP uzlu. To znamená, že paket je poslán ze síťového adaptéru odpovídajícího adrese IP uzlu.

Lokální hostitel Trasa s cílem v síti 10.1.1.99 a síťovou maskou 255.255.255.255 je hostitelskou trasou odpovídající adrese IP hostitele. Všechny IP datagramy posílané na adresu IP hostitele jsou předávány na zpětnou smyčku.

Všesměrové vysílání na všech podsítích Trasa s cílem v síti 10.255.255.255 a síťovou maskou 255.255.255.255 je hostitelskou trasou pro adresu všesměrového vysílání na všech podsítích pro ID sítě třídy A 10.0.0.0. Všesměrové vysílání na všech podsítích je navrženo tak, aby zasáhlo všechny podsítě třídy ID sítě. Pakety adresované všes-

měrovému vysílání na všech podsítích budou posílány ze síťového adaptéru odpovídajícího adrese IP uzlu. Hostitelská trasa pro všesměrové vysílání na všech podsítích existuje pouze pro ID sítě, která jsou podsítěmi třídivého ID sítě.

Síť zpětné smyčky Trasa s cílem v síti 127.0.0.0 a síťovou maskou 255.0.0.0 je trasou navrženou tak, aby přijala jakoukoli adresu IP ve tvaru 127.x.y.z a předala ji na zvláštní zpětnou smyčku 127.0.0.1.

Adresa vícesměrového vysílání Trasa s cílem v síti 224.0.0.0 a síťovou maskou 224.0.0.0 je trasou pro všechny adresy více směrového vysílání třídy D. IP datagram odpovídající této trase je poslán ze síťového adaptéru odpovídajícího adrese IP uzlu.

Omezené všesměrové vysílání Trasa s cílem v síti 255.255.255.255 a síťovou maskou 255.255.255.255 je hostitelskou trasou pro omezené všesměrové vysílání. IP pakety určené pro omezené všesměrové vysílání jsou posílány ze síťového adaptéru odpovídajícího adrese IP uzlu.

Poznámka Pořadí tras ve zobrazení na základě příkazu route print nijak neovlivní výkon procesu určení trasy.

Například když tento hostitel odesílá pakety na 10.1.1.72, procesu určení vyhovují dvě trasy – výchozí trasa a trasa přímo připojené sítě. Trasa přímo připojené sítě je nejvíce shodnou trasou, protože zde je v síťové masce 24 bitů na rozdíl od 0 bitů v výchozí trase. Vzhledem k tomu, že adresa brány a adresa rozhraní jsou v případě přímo připojené sítě stejné, je předávací adresa IP nastavena na adresu určení 10.1.1.72. Rozhraní, na kterém se má IP datagram předávat, je určen adresou IP ve sloupci rozhraní. V tomto případě je rozhraní 3Com 3C90x Ethernet Adapter, kterému je přiřazena adresa IP 10.1.1.99.

Když tento hostitel pošle pakety na 172.16.48.4, proces určení trasy použije výchozí trasu. I když v masce podsítě výchozí cesty nejsou žádné bity, které by souhlasily s 172.16.48.4, výchozí trasa stále odpovídá cílové adrese IP. Vzhledem k tomu, že adresa brány a adresa rozhraní pro trasu přímo připojené sítě jsou rozdílné, je předávací adresa IP nastavena na adresu IP ve sloupci brány, tedy 10.1.1.1. Rozhraní, na kterém se má IP datagram předávat, je určeno adresou IP ve sloupci rozhraní. V tomto případě je rozhraní 3Com 3C90x Ethernet Adapter, kterému je přiřazena adresa 10.1.1.99.

Ve většině případů je směrovací tabulka spravována automaticky. Při inicializaci hostitele jsou přidávány trasy pro lokální síť, zpětné smyčky, vícesměrové vysílání a konfigurace výchozí brány. V tabulce se může objevit více tras tak, jak se o nich vrstva protokolu IP dozvídá. například výchozí brána pro hostitele může (za pomoci ICMP) přijít na lepší trasu k určitému hostiteli. Trasy lze též vkládat manuálně za pomoci příkazu route nebo směrovacího protokolu.

Ke specifikaci trvalých tras lze v příkazu **route** použít přepínač **-p** (persistent, trvalý). Trvalé trasy jsou uloženy v registru v podklíči PersistentRoutes

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes.

Windows 2000 zavádějí novou možnost konfigurování metriky výchozích bran. Tato metrika umožňuje lepší řízení toho, která výchozí brána je v tom kterém okamžiku aktivní. Přednastavenou hodnotou metriky je 1. Trasy s nižší metrikou jsou upřednostňovány před trasami s metrikou vyšší. V případě výchozích bran počítač používá výchozí bránu s nejnižší metrikou, pokud se nejeví jako neaktivní. V takovém případě roz-

poznání mrtvé brány může aktivovat přepnutí na další výchozí bránu s nejnižší metrikou v seznamu. Metriku výchozích bran lze nastavit prostřednictvím upřesňujících možností konfigurace protokolu TCP/IP. Servery DHCP mohou poskytovat základní metriku a seznam výchozích bran. Když server DHCP poskytne základní metriku 100 a seznam tří výchozích bran, budou brány nakonfigurovány s metrikou 100, 101 a 102. Základní metrika poskytovaná serverem DHCP se nevztahuje na staticky konfigurované výchozí brány.

Většina směrovačů AS (Autonomous System) používá k výměně směrovacích tabulek s ostatními směrovači protokol, jako je například protokol RIP nebo OSPF. Windows 2000 Server podporuje tyto protokoly pomocí služby Routing and Remote Access. Operační systém Windows 2000 také podporuje protokol Silent RIP za použití služby RIP Listener, volitelné síťové služby.

Podle výchozího nastavení se systémy na platformě Windows 2000 nechovají jako směrovače a nepředávají IP datagramy mezi rozhraními. Služba Routing and Remote Access je obsažena ve Windows 2000 Serveru a lze ji zpřístupnit a nakonfigurovat tak, aby poskytovala plně více protokolové směrovací služby. Více podrobností najdete v části „Služba Routing and Remote Access“ v knize *Microsoft® Windows® 2000 Server Inter-networking*.

Konfigurace směrování pro prostředí více sítí nebo prostředí Proxy ARP

Při použití více logických podsítí na stejné fyzické síti, nazvané *multinetting*, je nutno přidat trasy tak, aby všechny adresy IP lokálně připojeného segmentu sítě byly dosažitelné prostřednictvím přímého doručení. Například pokud segment sítě používá ID sítě třídy C 192.168.168.1/24 a 192.168.2.0/24 a hostitel má nakonfigurovanou adresu IP 192.168.2.31, další trasu kvůli dosažitelnosti všech adres na 192.168.1.0/24 lze přidat pomocí následujícího příkazu:

```
route add 192.168.1.0 MASK 255.255.255.0 192.168.2.31
```

Protokol IP bude považovat všechny podsítě jako lokální a používat pro cíl přímo protokol ARP po použití tohoto příkazu:

```
route add 0.0.0.0 MASK 0.0.0.0 <my local ip address>
```

Tak jsou pakety určené pro „nelokální“ podsítě přenášeny přímo na lokální médium namísto odesílání na směrovač. Jinak řečeno, adaptér lokální sítě může být označen jako přednastavená brána. To může být užitečné při použití několika ID sítě třídy C na jedné fyzické síti bez směrovače navenek.

V prostředí proxy ARP předává jménem hostitelů požadavky ARP ostatním segmentům oddělené zařízení. Stejně jako v prostředí více sítí je přímo dostupných více sad adres. Příslušné trasy lze do směrovací tabulky hostitele přidat pomocí příkazu **route**.

Detekce duplikovaných adres IP

Detekce duplikovaných adres zajišťuje jedinečnost adresy IP používané IP uzlem v připojeném segmentu sítě. při první inicializaci zásobníku pošle operační systém Windows 2000 požadavek ARP na vlastní adresu IP hostitele známý jako gratuitous ARP (nevyžádaný požadavek ARP). Počet těchto požadavků je určen v registru hodnotou záznamu **ArpRetryCount**

(HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters), jehož výchozí nastavení je 3. Jestliže na některý z těchto požadavků ARP odpoví jiný hostitel, je již adresa

IP používána. Když nastane tato situace, počítač na platformě Windows 2000 se stále ještě spouští. Nicméně dojde ke znepřístupnění protokolu IP pro tuto adresu, vygenerování záznamu v systémovém protokolu a zobrazení chybového hlášení.

Jestliže je hostitel, který používá takovou kolidující adresu, také počítač na platformě Windows 2000, vygeneruje se záznam v systémovém protokolu a zobrazí se chybové hlášení také na tomto počítači, ale jeho rozhraní funguje dále. Vzpomeňte si, že záznamy mezipaměti ARP jsou aktualizovány při přijetí požadavků ARP. Proto po jednosměrném vysílání odpovědi ARP na kolidující počítač pošle bránící se počítač všesměrovým vysíláním dodatečný gratuitous (nevyžádaný) požadavek ARP tak, aby ostatní hostitelé na síti měli v mezipaměti ARP správné mapování této adresy.

Počítač používající duplikovanou adresu IP můžete spustit, pokud není připojen k síti, takže není detekován žádný konflikt. Nicméně pokud ho potom připojíte k síti, jakmile poprvé pošle požadavek ARP na jinou adresu IP, jakýkoli počítač na platformě Windows 2000 s kolidující adresou IP detekuje konflikt a zůstane funkční. Pokud oba počítače používají Windows 2000, protokol IP zůstane funkční pro duplikovanou adresu na obou počítačích. Počítač detekující konflikt zobrazí chybové hlášení a запиše do systémového protokolu detailní popis události. Záznam v protokolu může vypadat například takto:

```
** The system detected an address conflict for IP address 199.199.40.123
with the system having network hardware address 00:DD:01:0F:7A:B5. Network
operations on this system may be disrupted as a result. **
```

Klienti na platformě Windows 2000 s povoleným protokolem DHCP provádějí detekci duplikovaných adres IP přitom, jak se klient přesouvá do stavu výběru protokolu DHCP. Jestliže je detekována duplikovaná adresa IP, klient DHCP pošle serveru DHCP zprávu protokolu DHCP o odmítnutí a přepne se do stavu inicializace protokolu DHCP. Na základě přijaté zprávy protokolu DHCP o odmítnutí server DHCP označí tutp adresu IP jako nepoužitelnou.

Více podrobností o zprávách protokolu DHCP a stavech klienta DHCP najdete v části „Protokol DHCP“.

Vícedomost (Multihoming)

Jestliže má počítač nakonfigurovánu více než jednu adresu IP, označuje se jako *vícedomý* systém. Vícedomost je podporována třemi různými způsoby:

- Více adres IP na jeden síťový adaptér.

NetBIOS nad protokolem TCP/IP (NetBT) se váže pouze na jednu adresu IP na jeden síťový adaptér. Po odeslání registrace názvu typu NetBIOS bude na jeden adaptér registrována pouze jedna adresa IP. Tato registrace se projeví u adresy IP, která je zařazena jako první ve vlastnostech protokolu TCP/IP dotčeného adaptéru.

- Více síťových adaptérů pro fyzickou síť.

Neexistuje jiné než hardwarové omezení.

- Více typů sítí a médií.

Neexistuje jiné omezení než hardwarové a podpora médií.

Po odeslání IP datagramu z vícedomého hostitele proces určení trasy IP určí příslušnou předávací adresu IP a rozhraní. Proto datagram může obsahovat zdrojovou adresu IP jednoho rozhraní ve vícedomém hostitele, ačkoli byl umístěn na médium jiným rozhraním. Zdrojová MAC adresa rámce je adresa rozhraní, které skutečně předalo rámec na

médium a zdrojová adresa IP je adresa IP odesílající aplikace, ne nutně jedna z adres IP spojených s odesílajícím rozhraním.

Je-li počítač vícedomý za použití síťových adaptérů připojených k více vzájemně odděleným segmentům sítě, nebo segmentům sítě, které jsou jeden od druhého odděleny IP směrovačem, je třeba zvážit přidání dalších tras.

Ačkoli je možné nakonfigurovat výchozí adresu IP brány pro každé síťové rozhraní, ve směrovací tabulce IP existuje pouze jediná aktivní výchozí trasa. Je-li ve směrovací tabulce IP více výchozích tras (předpokládáme hodnotu metriky jako 1), je při inicializaci protokolu TCP/IP vybírána určitá výchozí trasa náhodným výběrem. Toto chování může vést ke zmatku a ztrátě připojitelnosti. Při konfigurování vícedomého počítače na dvou oddělených sítích je třeba výchozí IP brány nakonfigurovat na rozhraní, které je připojeno k IP síti, které obsahuje nevíce segmentů sítě. Pak je třeba buď přidat statické trasy, nebo použít směrovací protokol tak, aby byla zajištěna připojitelnost vzdálených sítí dosažitelných přes další rozhraní.

Více podrobností o registraci názvů a zjištění a výběru síťového adaptéru na datagramech odchozích z vícedomých počítačů najdete v částech „Protokol TCP (Transmission Control Protocol)“, „Windows Sockets“ a „NetBIOS pro TCP/IP“ dále v této kapitole.

CIDR (Beztrídové mezidoménové směrování)

Operační systém Windows 2000 poskytuje plnou podporu beztrídovému mezidoménovému směrování (CIDR), popsanému ve standardech RFC 1518 a 1519. Operační systém Windows 2000 také poskytuje podporu používání nulových a jedničkových podsítí v souladu se standardy RF 1812 a 1878. Ověřte si, že ostatní hostitelé a směrovače na vaší síti také podporují CIDR a používání nulových a jedničkových podsítí.

Vícesměrové vysílání protokolu IP

Operační systém Windows 2000 plně podporuje vícesměrové vysílání protokolu IP, a to včetně schopnosti odesílat a přijímat vícesměrný provoz IP, a plně podporuje protokol IGMP (Internet Group Management Protocol) verze 2. Více podrobností o podpoře protokolu IGMP najdete v části „Protokol IGMP (Internet Group Management Protocol)“ dále v této kapitole.

Protokol IP nad sítí ATM

Operační systém Windows 2000 zavádí podporu odesílání IP datagramů nad sítí ATM. Protokol IP nad sítí ATM, popsaný ve standardu RFC 1577, je známý jako klasický protokol IP na sítí ATM. Windows 2000 TCP/IP také podporuje protokol IP nad LAN emulací sítě ATM (LANE). Více podrobností o podpoře protokolu IP nad sítí ATM ve Windows 2000 najdete v části „Asynchronous Transfer Mode“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Protokol ICMP (Internet Control Message Protocol)

Protokol ICMP je protokol údržby specifikovaný v dokumentu RFC 792 a normálně se pokládá za součást vrstvy protokolu IP. Hlášení protokolu ICMP jsou zapouzdřeny v IP datagramech, takže mohou být směrovány po síti. Protokol ICMP je operačním systémem Windows 2000 používán následujícím způsobem:

- Výstavba a udržování směrovacích tabulek.
- Pomoc při zjišťování jednotky PMTU.
- Diagnostické problémy.

- Úprava řízení proudu pro prevenci nasycení linky nebo směrovače.
- Zjišťování směrovačů.

Údržba směrovacích tabulek

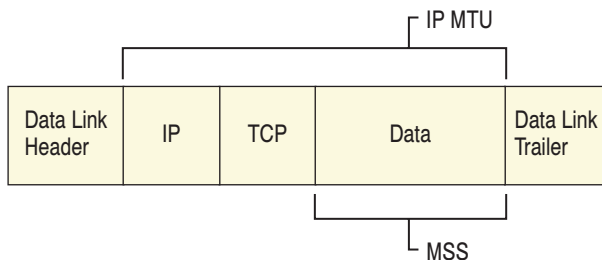
Hostitel na platformě Windows 2000 má zpravidla nakonfigurovanou adresu IP, masku podsítě a výchozí bránu. Při inicializaci protokolu TCP/IP se ve směrovací tabulce IP hostitele vytvoří sada směrovačů založených na této konfiguraci, viz část „Směrovací tabulka IP“. Jestliže hostitel předá IP datagram na svou výchozí bránu a existuje lepší trasa přes směrovač, která má rozhraní na stejném segmentu sítě jako odesílající hostitel a přednastavená brána, přednastavená brána hostitele předá datagram a pošle hostiteli zprávu ICMP o přesměrování, které ho informuje o adrese IP lepšího směrovače pro dosažení cílové adresy IP.

Když počítač na platformě Windows 2000 přijme hlášení ICMP o přesměrování, protokol IP ověří, že skutečně přišlo z brány prvního předání na aktuální trase a že brána je na přímo připojené síti. Pokud ano, je do směrovací tabulky pro cílovou adresu IP přidána hostitelská trasa s životností 10 minut. Pokud hlášení o přesměrování nepřišlo z brány prvního předání na aktuální trase, nebo pokud není brána na přímo připojené síti, hlášení ICMP o přesměrování je ignorováno.

Zjištění jednotky PMTU

Windows 2000 používá pro spojení TCP zjišťování jednotky PMTU (Path Maximum Transmission Unit) popsané v dokumentu RFC 1191.

Po ustanovení spojení si oba zúčastnění hostitelé vymění své hodnoty MSS (*maximum segment size*, největší velikost segmentu) protokolu TCP. Pro spojení je použita nižší z obou hodnot MSS. Původně byla hodnota MSS hostitele jeho MTU na vrstvě připojení mínus 40 bajtů na hlavičku IP a TCP. Nicméně podpora přídavných možností protokolu TCP, například časové razítko, zvětšila typickou hlavičku TCP a IP na 52 nebo více bajtů. Vztah mezi MTU protokolu IP a MSS protokolu TCP je znázorněn na obrázku 2.2.



Obrázek 2.2 MTU protokolu IP a MSS protokolu TCP

Dle výchozího nastavení jsou všechny TCP segmenty ve Windows 2000 odesílány s nastaveným příznakem Don't Fragment v hlavičce IP. Směrovače, které se snaží segment TCP fragmentovat, narazí na příznak Don't Fragment. V tomto okamžiku směrovač se zachová jedním z následujících způsobů:

- Směrovač zahodí IP datagram a pošle hlášení ICMP Destination Unreachable-Fragmentation Needed and DF Set zpět odesílajícímu hostiteli. To je původní účel těchto hlášení.

- Směrovač vyřadí IP datagram a pošle odesílajícímu hostiteli hlášení ICMP Destination Unreachable-Fragmentation Needed and DF Set obsahující jednotku MTU následujícího předání. MTU, která je povolena pro další předání, je uložena v prvních 16 bitech hlavičky ICMP, které jsou v dokumentu RFC 792 označeny jako „nevyužité“. Formát tohoto hlášení najdete v dokumentu RFC 1191, oddíl 4. To se vztahuje na směrovače PMTU kompatibilní.
- Směrovač vyřadí IP datagram bez odeslání hlášení ICMP Destination Unreachable-Fragmentation Needed a hlášení DF Set. Tento typ směrovačů je známý jako směrovač projevující se jako *černá díra pro PMTU*.

Po přijetí hlášení ICMP Destination Unreachable-Fragmentation Needed and DF Set obsahující jednotku MTU příštího předání implementace protokolu TCP v operačním systému Windows 2000 upraví své MSS pro novou MTU tak, aby jakékoli další pakety odesílané na spojení nebyly větší než největší velikost, které lze po cestě přenést bez fragmentace. Minimální MTU dovolená v dokumentu RFC 791 je 68 bajtů a Windows 2000 TCP/IP tento limit posiluje.

Jestliže na síti nejsou žádné směrovače PMTU kompatibilní, nebo jestliže tam jsou směrovače projevující se jako černé díry, může být nezbytné změnit konfiguraci chování zjišťování PMTU. Problémy způsobené „směrovači, které se projevují jako černé díry, můžete redukovat pomocí nastavení hodnot záznamů **EnablePMTUBHDetect** a **EnablePMTUDiscovery** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters) na 1. Vysvětlení těchto záznamů v registru je následující:

EnablePMTUBHDetect Upravuje algoritmus zjišťování PMTU ve snaze detekovat směrovače projevující se jako černé díry. Detekce směrovačů projevujících se ve vztahu k PMTU jako černé díry je ve výchozím nastavení zakázána.

EnablePMTUDiscovery Povoluje nebo zakazuje mechanismus zjišťování PMTU. Je-li zjišťování PMTU zakázáno, je provoz připojení TCP posílán bez nastavení příznaku Don't Fragment na hodnotu 1. Ve výchozím nastavení je zjišťování PMTU povoleno.

► **Problémy způsobené směrovači projevujícími se jako černé díry lze omezit takto:**

1. V editoru registru přejděte na HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.
2. Vyberte záznam EnablePMTUBHDetect a změňte jeho hodnotu na 1.
3. Zavřete editor registru.

PMTU mezi dvěma hostiteli může být zjištěno i manuálně za pomoci příkazu **ping** s přepínačem **-f** (don't fragment), viz dále:

```
ping -f -n <number of pings> -l <size> <destination IP address>
```

Parametr velikost se může měnit až do doby zjištění MTU příštího předání. Všimněte si, že parametr velikost používaný příkazem Ping je velikost volitelných dat v požadavku ICMP Echo Request a neobsahuje hlavičku tohoto požadavku (dlouhou 8 bajtů) a IP hlavičku (zpravidla dlouhou 20 bajtů). Proto je pro Ethernet maximální velikost vyrovnávací paměti příkazu Ping 1500-8-20 nebo 1472. Následující příklad znázorňuje výsledek příkazu Ping přes směrovač na síti Ethernet s velikostí vyrovnávací paměti 1472 a pak 1473:

```
C:\>ping -f -n 1 -l 1472 10.99.99.10
```

```

Pinging 10.99.99.10 with 1472 bytes of data:
Reply from 10.99.99.10: bytes=1472 time<10ms TTL=128
Ping statistics for 10.99.99.10:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping -f -n 1 -l 1473 10.99.99.10
Pinging 10.99.99.10 with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Ping statistics for 10.99.99.10:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

V tomto příkladě vrstva protokolu IP vrátila chybové hlášení ICMP, který příkaz Ping vyložil. Jestliže je směrovač směrovačem, který se vůči PMTU projevuje jako černá díra, nelze na odpověď ICMP Echo Reply příkazem Ping odpovědět, pokud jeho velikost přesáhla jednotku MTU příštího předání. Příkaz Ping lze takto použít k detekci směrovače, který se vůči PMTU projevuje jako černá díra.

Následující snímek obrazovky znázorňuje vzorové hlášení PMTU kopmatibilního protokolu ICMP Destination Unreachable-Fragmentation Needed and DF Set:

```

+ FRAME: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
+ IP: ID = 0x4401; Proto = ICMP; Len: 56
  ICMP: Destination Unreachable: 10.99.99.10 See frame 3
    ICMP: Packet Type = Destination Unreachable
    ICMP: Unreachable Code = Fragmentation Needed, DF Flag Set
    ICMP: Checksum = 0xA05B
    ICMP: Next Hop MTU = 576 (0x240)
    ICMP: Data: Number of data bytes remaining = 28 (0x001C)
+ ICMP: Description of original IP frame

```

Toto hlášení bylo generováno za použití příkazu ping -f -l 1000 na hostiteli na platformě Ethernet, který měl předat datagram o velikosti 1028 bajtů přes rozhraní směrovače, které podporuje MTU pouze 576 bajtů. Když se směrovač snažil umístit velký datagram na síti s menší jednotkou MTU, zjistil, že fragmentace datagramu není povolena. Směrovač poté IP datagram vyřadil a poslal zpět hlášení ICMP oznamující, že největší možný datagram, který lze předat, je pouze 0x240 nebo 576 bajtů.

Použití protokolu ICMP při diagnostice problémů

Utilita Ping se používá k posílání požadavky ICMP Echo Request na adresu IP a k čekání na odpovědi ICMP Echo Reply. Ping hlásí počet přijatých odpovědí a časový interval mezi odesláním požadavku a přijetím odpovědi. Existuje mnoho dalších možností, jak utilitu Ping využívat. Více podrobností o tom, jak používat utilitu Ping k řešení problémů, najdete v části „Řešení problémů protokolu TCP/IP“ v této knize.

Tracert je nástroj pro sledování trasy, který pracuje na principu odesílání požadavků ICMP Echo Request na určitou adresu IP se zvyšující se hodnotou TTL v hlavičce IP. První požadavek Echo Request má TTL 1. První směrovač sníží TTL na 0 a odešle odesílateli zprávu ICMP Time Exceeded-TTL Expired in Transit. Odesílající hostitel pak z pole zdrojové adresy IP ICMP zprávy zjistí adresu IP rozhraní směrovače. Tracert pak

odešle požadavek Echo Request s TTL 2 atd. Tento proces pokračuje, dokud není určen celý seznam rozhraní směrovačů od odesílajícího hostitele k cíli.

Více podrobností o příkazu Tracert a jeho použití při řešení problémů najdete v Řešení problémů TCP/IP v této knize.

Řízení proudu za použití protokolu ICMP

Když se směrovač zahltí a začne vyhazovat IP datagramy, může odesílajícímu hostiteli odeslat o vyhozených datagramech zprávu ICMP Source Quench. Windows 2000 TCP/IP ctí zprávu ICMP Source Quench o TCP provozu za předpokladu, že obsahuje fragment hlavičky jednoho z vlastních datagramů z aktivního TCP spojení. Směrovač na platformě Windows 2000 zprávy ICMP Source Quench neposílá.

Zjišťování směrovače pomocí protokolu ICMP

Jak je specifikováno v dokumentu RFC 1256, Windows 2000 TCP/IP poskytuje hostitelskou podporu *zjišťování směrovače* pomocí protokolu ICMP. Zjišťování směrovače poskytuje vylepšenou metodu detekce a konfigurování výchozích bran. Namísto konfigurování výchozí brány manuálního nebo pomocí protokolu DHCP, může hostitel dynamicky zjišťovat nejlepší výchozí bránu, kterou má použít na podsíti, a může v případě selhání výchozí brány nebo změny preferencí směrovače síťovým administrátorem automaticky přepnout na jinou výchozí bránu.

Při inicializaci zjišťování směrovače podporovaném hostitelem se přidá ke skupině všesměrového vysílání pro IP všech hostitelů (224.0.0.1) a naslouchá hlášením ICMP Router Advertisement. Směrovače kompatibilní se zjišťováním směrovačů pomocí protokolu ICMP periodicky posílají hlášení ICMP Router Advertisement obsahující jejich adresu IP, úroveň preference a čas, po kterém mohou být vypnuté. Hostitelé přijímají hlášení ICMP Router Advertisement a vybírají jako svou přednastavenou bránu směrovač s nejvyšší úrovní předvolby.

Hostitelé mohou také na adresu IP všesměrového vysílání všech směrovačů (224.0.0.2) posílat hlášení ICMP Router Solicitation, a to buď při inicializaci rozhraní nebo poté, co hostitel nepřijme oznámení směrovače z aktuální výchozí brány v oznamovaném čase platnosti. Hostitel na platformě Windows 2000 pošle maximálně tři výzvy v intervalu přibližně 600 milisekund. Používání zjišťování směrovače je určeno hodnotou záznamu **PerformRouterDiscovery** and **SolicitationAddressBCast** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

Služba Routing and Remote Access ve Windows 2000 podporuje zjišťování směrovače pomocí protokolu ICMP jako směrovač. Více podrobností najdete v části „Jednosměrné IP směrování“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Služba QoS (Quality of Service) a protokol RSVP (Resource reservation Protocol)

Další novou vlastností je v operačním systému Windows 2000 podpora služby QoS a protokolu RSVP.

Služba Generic QoS (GQoS) je rozšířením programovacího rozhraní Winsock. Poskytuje API a systémové komponenty, které mají zajišťovat síťovým aplikacím metodu rezervace šířky pásma mezi klientem a serverem. Protokol RSVP je implementací protokolu pro rezervaci šířky pásma, který je podporovaný operačním systémem Windows 2000. GQoS poskytuje aplikační rozhraní přes Winsock2 na protokol RSVP a jeho komponenty.

ty. Vzhledem k tomu, že se služba QoS skládá z modulů a protokol RSVP z komponent, je možné ke zvýšení funkcionality přidávat další komponenty. Například jestliže chcete poskytovat služby QoS aplikacím, které mají tyto služby zakázány, lze k protokolu RSVP přistupovat prostřednictvím řídicí nebo správcovské aplikace.

Více podrobností o těchto konceptech a protokolech najdete v části „Technologie Quality of Service“ v této knize.

Zabezpečení protokolu IP

Zabezpečení IPsec je další novou vlastností operačního systému Windows 2000. Zabezpečení IPsec používá pro poskytování řízení přístupu, integrity bez připojení, ověření původu dat, ochrany proti opakování, důvěrnosti a důvěrnosti omezeného proudu provozu zabezpečení založené na kryptografii. Vzhledem k tomu, že zabezpečení IPsec je poskytováno na vrstvě protokolu IP, jsou jeho služby dostupné v zásobníku pro protokoly horní vrstvy a jsou transparentně dostupné existujícím aplikacím.

Zabezpečení IPsec umožňuje systému vybírat bezpečnostní protokoly, rozhodovat, které algoritmy budou používány pro jeho služby, a zakládat a udržovat kryptografické klíče pro každý vztah zabezpečení. IPsec může chránit cesty mezi hostiteli, mezi bránami zabezpečení nebo mezi hostiteli a bránami zabezpečení. Služby, které jsou dostupné a požadované provozem, jsou konfigurovány na základě zásad zabezpečení IPsec. Zásady zabezpečení IPsec mohou být nakonfigurovány na počítači lokálně, nebo mohou být přiřazeny prostřednictvím mechanismu Windows 2000 Group Policy za použití služby Active Directory™. Při použití služby Active Directory hostitelé nejprve detekují přiřazení zásad, načtou je a pravidelně kontrolují, zda tyto zásady byly aktualizovány. Zásady zabezpečení IPsec specifikují, jak počítače důvěřují jeden druhému. Nejsnazší použitelná důvěryhodnost je důvěryhodnost domén Windows 2000 založená na protokolu Kerberos. Předdefinované zásady bezpečnosti IPsec jsou nakonfigurovány tak, aby důvěřovaly ostatním počítačům ve stejných nebo jiných důvěryhodných doménách Windows 2000.

Každý datagram zpracováváný na vrstvě protokolu IP je porovnáván se sadou filtrů poskytovaných zásadami zabezpečení, které pro počítač, uživatele, skupinu nebo celou doménu udržuje administrátor. Protokol IP může s datagramem udělat jednu ze tří věcí:

- Použít na něj služby IPsec
- Umožnit jeho průchod v nezměněné podobě
- Vyřadit ho

Nastavení zabezpečení IPsec zahrnuje popsání znaků (například zdrojová nebo cílová adresa IP, protokol a port) provozu, který se bude filtrovat, a pak specifikaci znaků služby, které se mají použít na provoz, který projde filtry. Například ve velice jednoduchém případě mohou být dva samostatné počítače nakonfigurovány tak, aby mezi sebou používaly zabezpečení IPsec, tím, že budou členy stejné domény Windows 2000 a budou mít aktivovanou zásadu uzamčení. Jestliže tyto dva počítače nejsou členy stejné domény nebo důvěryhodné domény, pak musí být důvěryhodnost ustavena za použití hesla nebo „předsdíleného“ klíče v režimu uzamčení prostřednictvím:

- Nastavení filtru, který specifikuje veškerý provoz mezi těmito dvěma počítači.
- Výběru metody ověření. (Vyber předsdílený klíč a zadej heslo.)
- Výběru zásad vyjednávání (v tomto případě uzamčení, které značí, že veškerý provoz odpovídající filtrům, musí používat zabezpečení IPsec).

- Specifikace typu připojení (LAN, vytáčené nebo všechna připojení).

Jakmile jsou zásady ustaveny, provoz odpovídající filtrům používá služby poskytované zabezpečením IPsec. Při směrování IP provozu (včetně něčeho tak jednoduchého, jako je v tomto případě příkaz Ping) jedním hostitelem na jiného hostitele se prostřednictvím krátké konverzace přes port 500 protokolu UDP (za použití protokolu ISAKMP) vytvoří přidružení zabezpečení a pak začne probíhat provoz.

Vzhledem k tomu, že zabezpečení IPsec zpravidla zakóduje veškerá přenášená data IP, zachycení datagramu zabezpečení IPsec poslaného za přidružením zabezpečení v podstatě nic neříká o skutečném obsahu datagramu. Jedinými částmi paketu, které lze pomocí služby Network Monitoring analyzovat, jsou hlavičky Ethernet a IP.

Více podrobností o vlastnostech a implementaci zabezpečení IPsec najdete v části „Zabezpečení protokolu IP“ v této knize.

Protokol IGMP (Internet Group Management Protocol)

Operační systém Windows 2000 poskytuje podporu 2. úrovně (plnou podporu) vícesměrovému vysílání IP a protokolu IGMP verze 2, jak je popsáno v dokumentech RFC 1112 a RFC 2236. Přehled vícesměrového vysílání IP a protokolu IGMP najdete v části „Úvod do TCP/IP“ v této knize.

Adresy hostitelských skupin jsou v rozsahu třídy D od 224.0.0.0 do 239.255.255.255 (jak byly definovány nastavením prvních čtyřech bitů na 1110). Adresy vícesměrového vysílání v rozsahu 224.0.0.0 až 224.0.0.255 jsou vyhrazeny pro lokální podsítě a nejsou IP směrovači předávány bez ohledu na TTL v hlavičce IP.

Vícesměrová trasa

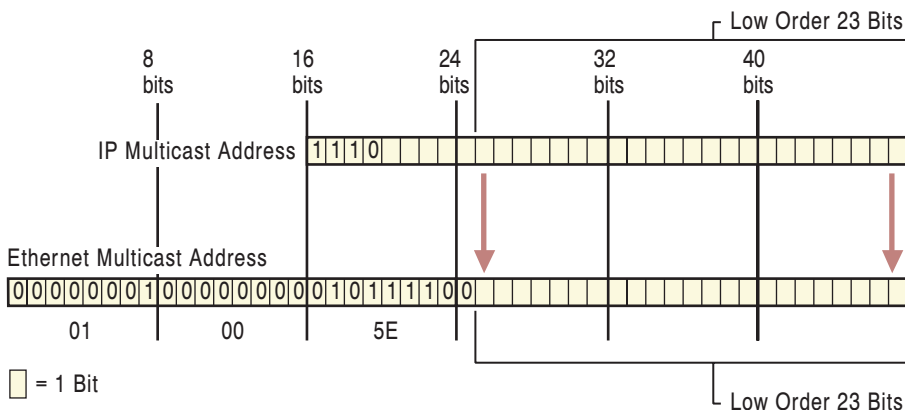
Na hostiteli je k podpoře vícesměrového vysílání IP definována přídatná trasa. Tato trasa určuje, že při odesílání datagramu hostitelské skupině vícesměrového vysílání by měl být odeslán na adresu IP hostitelské skupiny prostřednictvím karty lokálního rozhraní a neměl by být předán na předávací bránu. Toto je znázorněno na následující trase:

Network	Destination	Netmask	Gateway	Interface	Metric
	224.0.0.0	224.0.0.0	10.1.1.99	10.1.1.99	1

Mapování IP adres vícesměrového vysílání na MAC adresy

provoz vícesměrového vysílání IP nepoužívá k přiřazování MAC adres pro odchozí IP datagramy protokol ARP. K podpoře vícesměrového vysílání IP vyhradili internetoví odborníci pro provoz vícesměrového vysílání IP rozsah adres vícesměrového vysílání Ethernetu mezi 01-00-5E-00-00-00 a 01-00-5E-7F-FF-FF. Prvních 25 bitů 48bitové adresy Ethernetu je pevných a dalších 23 bitů je měnitelných, viz obrázek 2.3.

Při mapování adresy vícesměrového vysílání IP na adresu vícesměrového vysílání Ethernet je nejméně významných 23 bitů adresy vícesměrového vysílání IP namapováno přímo na 23 nejméně významných bitů adresy vícesměrového vysílání Ethernet. Vzhledem k tomu, že první 4 bity adresy vícesměrového vysílání IP je pevných kvůli konvenci třídy D, existuje v adrese vícesměrového vysílání IP 5 bitů, které se na adresu vícesměrového vysílání Ethernet nemapují. Proto Ethernet hostitel může zpracovávat pakety vícesměrového vysílání IP pro skupiny, ke kterým nepatří. Tato nadbytečná vícesměrová vysílání jsou bez upozornění vyhozena.



Obrázek 2.3 Mapování adres vícesměrového vysílání IP na MAC adresy

Například datagram adresovaný na adresu vícesměrového vysílání 225.0.0.5 by byl poslán na Ethernet MAC adresu 0x01-00-5E-00-00-05. Tato MAC adresa je tvořena spojením 01-00-5E a 23 nejméně významných bitů 255.0.0.5 (0x00-00-05).

Adresy vícesměrového vysílání IP mapuje na MAC adresy také rozhraní FDDI (Fiber Data Distributed Interface).

Kvůli povaze MAC adresování na síti Token Ring a omezení adaptéru Token Ring je všechen provoz vícesměrového vysílání IP mapován na funkční MAC adresu sítě Token Ring 0xC0-00-00-04-00-00.

Rozšíření vícesměrového vysílání knihovny Windows Sockets

Vícesměrové vysílání IP je aktuálně podporováno pouze na datagramech skupiny protokolů IP a nezpracovaných soketech. Dle výchozího nastavení jsou posílány datagramy vícesměrového vysílání IP s TTL 1. Aplikace mohou pro specifikaci hodnoty TTL používat funkci **setsockopt()** knihoven Windows Sockets.

Dle konvencí používají směrovače vícesměrového vysílání mezní hodnoty TTL k tomu, aby určily, jak daleko se bude datagram předávat. Tyto mezní hodnoty TTL jsou definovány takto:

- Datagramy vícesměrového vysílání s počáteční hodnotou TTL 0 jsou omezeny na stejného hostitele.
- Datagramy vícesměrového vysílání s počáteční hodnotou TTL 1 jsou omezeny na stejnou podsít.
- Datagramy vícesměrového vysílání s počáteční hodnotou TTL 32 jsou omezeny na stejné sídlo.
- Datagramy vícesměrového vysílání s počáteční hodnotou TTL 64 jsou omezeny na stejnou oblast.
- Datagramy vícesměrového vysílání s počáteční hodnotou TTL 128 jsou omezeny na stejný kontinent.
- Datagramy vícesměrového vysílání s počáteční hodnotou TTL 255 nejsou nijak omezeny.

Použití vícesměrového vysílání IP komponentami operačního systému Windows 2000

Provoz vícesměrového vysílání IP používají následující protokoly a služby operačního systému Windows 2000:

- Zjišťování směrovače pomocí protokolu ICMP (224.0.0.1, adresa vícesměrového vysílání všech hostitelů, a 224.0.0.2, adresa vícesměrového vysílání všech směrovačů).
- Protokol RIP verze 2 (224.0.0.9), používaný službou Routing and Remote Access.
- Protokol OSPF (224.0.0.5 a 224.0.0.6), používaný službou Routing and Remote Access.
- K inzerování konferencí vícesměrového vysílání IP na síti se používá služba Site Server LDAP. Lze ji také použít ke zveřejnění mapování adres IP pro telefonní subsystém H.323.
- Server WINS používá vícesměrové vysílání (224.0.1.24) při snaze lokalizovat replikační partnery. Více podrobností o WINS najdete v části „Služba Windows Internet Name Service“ v této knize.

Protokol TCP (Transmission Control Protocol)

Protokol TCP poskytuje aplikacím spolehlivé služby bajtových proudů založené na připojení. Síť společnosti Microsoft spoléhají na protokol TCP při procesu přihlášení, sdílení souborů a tisku, replikaci informací mezi řadiči domén, přenosu seznamů prohledávání sítě a dalších běžných funkcích. Lze ho použít pouze ke komunikaci jednoho k jednomu (one-to-one). Windows 2000 TCP je kompatibilní s dokumentem RFC 793 a částí 4.2 dokumentu RFC 1122.

Protokol TCP používá pro chyby přenosu jak na hlavičce TCP, tak na každém segmentu datové části kontrolní součet, aby minimalizoval možnost nedetekované chyby sítě. NDIS 5.0 podporuje odstraňování úloh, přičemž operační systém Windows 2000 toho využívá tím, že za předpokladu, že síťový adaptér takovou funkci podporuje, dovoluje síťovému adaptéru provést výpočty kontrolního součtu protokolu TCP. Přemístění výpočtů kontrolního součtu na hardware může ve velmi propustných prostředích zlepšit výkon. Ve Windows 2000 byla zvýšena též odolnost protokolu TCP a tento protokol prošel interní bezpečnostní revizí tak, aby lépe odolával budoucím útokům hackerů.

Velikost přijímaného okna protokolu TCP a změna velikosti okna

Velikost přijímaného okna protokolu TCP je množství přijímaných dat (v bajtech), které je možno při připojení najednou uložit do vyrovnávací paměti. Odesílající hostitel může před potvrzením odeslaných dat a aktualizace okna od přijímajícího hostitele odeslat pouze takovéto množství dat. Protokol TCP/IP v operačním systému Windows 2000 je navržen tak, že se ve většině prostředí sám optimalizuje a používá dle výchozího nastavení větší velikost oken než jeho dřívější verze.

Místo velikosti přijímaného okna přednastavené pevně v kódu se protokol TCP upravlí na sudé násobky MSS (Maximum Segment Size) vyjednaného během nastavení připojení. Přizpůsobování přijímaného okna sudým násobkům MSS zvyšuje procento TCP segmentů maximální velikosti používaných během celkového přenosu dat.

Velikost přijímaného okna je přednastavena na hodnotu vypočítanou následujícím způsobem:

1. Požadavek na první připojení poslaný vzdálenému hostiteli inseruje velikost přijímaného okna 16 KB nebo 16384 bajtů.
2. Při vytváření připojení je velikost přijímaného okna zaokrouhlena na celý násobek MSS protokolu TCP, který byl dojednán během nastavení připojení.
3. Pokud není zaokrouhlená hodnota alespoň čtyřnásobek MSS, je upravena na čtyřnásobek maximální velikosti dat TCP ($4 * MSS$) s maximální velikostí 64 KB, pokud neplatí možnost změny velikosti (dokument RFC 1323).

U TCP připojení na platformě Ethernet je okno zpravidla nastaveno na 17520 bajtů nebo 16 KB zaokrouhlených na dvanáct 1460bajtových segmentů. V předchozích verzích protokolu Microsoft® Windows NT® TCP/IP mělo okno sítě Ethernet 8760 bajtů nebo šest segmentů velikosti MSS.

Velikost přijímaného okna lze na určitou hodnotu nastavit dvěma způsoby:

- Záznam **TcpWindowSize** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interface\<interface>).
- Na základě jednotlivých soketů pomocí funkce knihovny Windows Sockets `setsockopt()`.

Kvůli zvýšení výkonu na sítích s velkou šířkou pásma a velkým zpožděním podporuje protokol Windows 2000 TCP *změnu velikosti okna* protokolu TCP popisovanou v dokumentu RFC 1323. Změna velikosti okna protokolu TCP podporuje přijímaná okna větší než 64 KB pomocí vyjednávání faktoru změny okna během třicestného vyjednávání. To umožňuje přijímat okno až do 1 GB.

Při čtení zachycených záznamů připojení, která byla vytvořena dvěma počítači podporujícími nastavitelná okna, mějte na paměti, že velikost okna inzerovaného v segmentu musí být zvětšena vyjednaným faktorem zvětšení. Faktor zvětšení velikosti okna se objevuje pouze v prvních dvou segmentech třicestného vyjednávání protokolu TCP. Faktor zvětšení je 2s, kde s je vyjednaný faktor zvětšení. Například u inzerovaného okna o velikosti 65536 a faktoru zvětšení 3 je skutečná velikost přijímaného okna 524280 nebo $23 * 65535$.

Následující snímek služby Network Monitoring znázorňuje možnost změny velikosti okna v segmentu SYN protokolu TCP:

```
Src Addr  Dst Addr  Protocol  Description
HOST100  CORPSVR  TCP       ....S., len:0, seq:725163-725163, ack:0,
win:65535, src:1217 dst:139
```

```
+ FRAME: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
+ IP: ID = 0xB908; Proto = TCP; Len: 64
  TCP: ....S., len:0, seq:725163-725163, ack:0, win:65535, src:1217
dst:139 (NBT Session)
  TCP: Source Port = 0x04C1
  TCP: Destination Port = NETBIOS Session Service
  TCP: Sequence Number = 725163 (0xB10AB)
  TCP: Acknowledgement Number = 0 (0x0)
  TCP: Data Offset = 44 (0x2C)
```

```

TCP: Reserved = 0 (0x0000)
+ TCP: Flags = 0x02 : ....S.
TCP: Window = 65535 (0xFFFF)
TCP: Checksum = 0x8565
TCP: Urgent Pointer = 0 (0x0)
TCP: Options
+ TCP: Maximum Segment Size Option
TCP: Option Nop = 1 (0x1)
TCP: Window Scale Option
    TCP: Option Type = Window Scale
    TCP: Option Length = 3 (0x3)
    TCP: Window Scale = 5 (0x5)
    TCP: Option Nop = 1 (0x1)
    TCP: Option Nop = 1 (0x1)
+ TCP: Timestamps Option
    TCP: Option Nop = 1 (0x1)
    TCP: Option Nop = 1 (0x1)
+ TCP: SACK Permitted Option

```

Změna velikosti okna je dle výchozího nastavení povolena a používá se automaticky kdykoli je velikost okna protokolu TCP pro připojení nastavena na hodnotu větší než 64 KB, a to buď přes položku **TCPWindowSize** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interface\<interface>), nebo přes funkci **setsockopt()** v knihovně Windows Sockets. Změna velikosti okna protokolu TCP může být povolena přes položku **Tcp1323Opts** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

Opožděná potvrzení

Jak je specifikováno v dokumentu RFC 1122, protokol TCP používá ke snížení počtu paketů posílaných na médium opožděná potvrzení (ACK). Spíše než aby odesílal potvrzení na každý přijatý TCP segment, protokol Windows 2000 TCP běžně používá opožděná potvrzení. Protokol TCP přijímá data na daném připojení a potvrzení zpět posílá pouze v případě, že je splněna některá z následujících podmínek.

- Nebylo odesláno žádné potvrzení předchozího přijatého segmentu.
- Segment je přijat, ale během následujících 200 milisekund nepříjde z tohoto připojení žádný další segment.

Zpravidla je potvrzení odesíláno na každý druhý segment protokolu TCP přijatý při připojení, pokud nevyprší časovač opožděného potvrzení (200 milisekund). Časovač opožděného potvrzení lze nastavit pro každé rozhraní pomocí hodnoty záznamu **TCPCongestionControl** v registru

(HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<interface>), který byl poprvé představen v Microsoft® Windows NT® version 4.0, Service Pack 4.

Selektivní potvrzení protokolu TCP

Operační systém Windows 2000 zavádí podporu důležité vlastnosti výkonu známé jako *selektivní potvrzení* (SACK), které je popsáno v dokumentu RFC 2018. Selektivní potvrzení je velmi důležité pro připojení používající velké velikosti okna protokolu TCP. Před tím, než bylo zavedeno selektivní potvrzení, mohl příjemce potvrdit pouze číslo poslední sekvence souvislých dat, která přijal, neboli levý okraj přijímaného okna. Když

je povoleno selektivní potvrzení, příjemce pokračuje ve zpožděném potvrzování levého okraje přijímaného okna, ale může také samostatně potvrzovat nesouvislé bloky přijímaných dat.

Selektivní potvrzení používá možnosti hlavičky TCP k tomu, aby vyjednalo použití selektivního potvrzení během vytváření připojení TCP a aby stanovilo levý a pravý okraj bloků přijímaných dat. Lze stanovit více přijatých bloků. Více podrobností najdete v dokumentu RFC 2018. Dle výchozího nastavení je selektivní potvrzení povoleno.

Jestliže přijde segment nebo řada segmentů nesouvisle, je příjemce schopen informovat odesílatele přesně o tom, která data byla přijata, tedy implicitně i o tom, která data přijata nebyla. Odesílatel pak může selektivně znovuzaslat chybějící data bez nutnosti zasílat bloky dat, které byly úspěšně přijaty. Selektivní potvrzení je dle výchozího nastavení hodnotou záznamu **SackOpts** v registru

(HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

Následující snímek služby Network Monitoring znázorňuje potvrzení všech dat až do čísla sekvence 54857340 a dat s číslu sekvence 54858789 až 54861684.

```
+ FRAME: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
+ IP: ID = 0x1A0D; Proto = TCP; Len: 64
  TCP: .A...., len:0, seq:925104-925104, ack:54857341, win:32722, src:1242
  dst:139
    TCP: Source Port = 0x04DA
    TCP: Destination Port = NETBIOS Session Service
    TCP: Sequence Number = 925104 (0xE1DB0)
    TCP: Acknowledgement Number = 54857341 (0x3450E7D)
    TCP: Data Offset = 44 (0x2C)
    TCP: Reserved = 0 (0x0000)
+ TCP: Flags = 0x10 : .A....
  TCP: Window = 32722 (0x7FD2)
  TCP: Checksum = 0x4A72
  TCP: Urgent Pointer = 0 (0x0)
  TCP: Options
    TCP: Option Nop = 1 (0x1)
    TCP: Option Nop = 1 (0x1)
  + TCP: Timestamps Option
    TCP: Option Nop = 1 (0x1)
    TCP: Option Nop = 1 (0x1)
    TCP: SACK Option
      TCP: Option Type = 0x05
      TCP: Option Length = 10 (0xA)
      TCP: Left Edge of Block = 54858789 (0x3451425)
      TCP: Right Edge of Block = 54861685 (0x3451F75)
```

Časová razítka protokolu TCP

V předchozích verzích protokolu Microsoft TCP/IP vypočítával protokol TCP dobu od odeslání požadavku do příchodu ozvěny (RTT) pouze pro jeden vzorek v každém okně z posílaných dat, aby upravil časový limit opakovaného odesílání (RTO). Pro výpočet doby od odeslání požadavku do příchodu ozvěny protokol TCP zaznamenal čas, kdy byl segment odeslán, a čas, kdy přišlo potvrzení přijetí segmentu. Velikost okna byla například 8760 (šest plných segmentů), běžná hodnota pro Ethernet, jeden ze šes-

ti segmentů byl použit k novému výpočtu RTT. To je adekvátní počet vzorků pro takhle malé okno. Nicméně u podpory změny velikosti okna protokolu TCP není vzorek jednoho segmentu z celkové velikosti okna dostačující. Například u maximální velikosti okna 1 GB na síti Ethernet by byl pouze jeden vzorek na každých 735440 segmentů.

Jako možnosti hlavičky TCP jsou implementována *časová razítka protokolu TCP*, která zaznamenávají čas odeslání segmentu. Časové razítko odeslaného segmentu protokolu TCP má odezvu v potvrzení. Více podrobností najdete v dokumentu RFC 1323.

Následující snímek služby Network Monitoring znázorňuje možnosti časového razítka protokolu TCP:

```
+ FRAME: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
+ IP: ID = 0x1A0D; Proto = TCP; Len: 64
    TCP: .A...., len:0, seq:925104-925104, ack:54857341, win:32722, src:1242
    dst:139
        TCP: Source Port = 0x04DA
        TCP: Destination Port = NETBIOS Session Service
        TCP: Sequence Number = 925104 (0xE1DB0)
        TCP: Acknowledgement Number = 54857341 (0x3450E7D)
        TCP: Data Offset = 44 (0x2C)
        TCP: Reserved = 0 (0x0000)
+ TCP: Flags = 0x10 : .A....
    TCP: Window = 32722 (0x7FD2)
    TCP: Checksum = 0x4A72
    TCP: Urgent Pointer = 0 (0x0)
    TCP: Options
        TCP: Option Nop = 1 (0x1)
        TCP: Option Nop = 1 (0x1)
        TCP: Timestamps Option
            TCP: Option Type = Timestamps
            TCP: Option Length = 10 (0xA)
            TCP: Timestamp = 2525186 (0x268802)
            TCP: Reply Timestamp = 1823192 (0x1BD1D8)
            TCP: Option Nop = 1 (0x1)
            TCP: Option Nop = 1 (0x1)
+ TCP: SACK Option
```

Časová razítka protokolu TCP jsou dle výchozího nastavení zakázána a lze je povolit změnou hodnoty záznamu **Tcp1323Opts** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

Ochrana proti přetečení čísel sekvence

Používání časových razítek protokolu TCP poskytuje *ochranu proti přetečení čísel sekvence* (PAWS, protection against wrapped sequence numbers). Číslo sekvence protokolu TCP je 32bitová hodnota, která označuje první bajt dat v segmentu. S 32 bity v čísle sekvence může být mezi odesílatelem a příjemcem přeneseno pouze 4 GB dat, než číslo sekvence začne přetékat a stane se nejasným. Zatímco není pravděpodobné, že by se toto stalo v typickém prostředí sítě Ethernet nebo Token Ring, ve vysokokapacitních sítích, které používají technologie přenášející gigabity za sekundu (Gbps) nebo terabity za sekundu (Tbps), mohou čísla sekvence protokolu TCP přetéci během několika sekund. Jestliže je segment vynechán nebo zpožděn, může pod stejným číslem se-

kvence existovat jiný segment. Poškozená data mohou mít za následek, že příjemce zamění nové číslo sekvence se starým číslem sekvence, jehož příjem očekává.

Časové razítko protokolu TCP se používá jako rozšíření čísla sekvence, pomocí kterého se brání zmatku při zdvojení čísla sekvence. Aktuální pakety mají aktuální a postupující časová razítka. Starý paket má staré časové razítko a je vyřazen.

Rozpoznání mrtvé brány

Rozpoznání mrtvé brány je používáno provozem protokolu TCP k rozpoznání selhání výchozí brány a úpravě směrovací tabulky IP tak, aby byla použita jiná výchozí brána. Protokol Windows 2000 TCP/IP používá mírně upravenou metodu spouštění opětovného výběru popsanou v dokumentu RFC 816.

Když se jakékoli TCP připojení, které je směrováno přes výchozí bránu, snaží odeslat paket protokolu TCP na místo určení tolikrát, kolik je jedna polovina hodnoty záznamu **TcpMaxDataRetransmissions** v registru (výchozí nastavení je 5) bez obdržení odpovědi, je předávací adresa IP pro cílovou adresu IP změněna tak, aby byl použita výchozí brána, která je další v seznamu. Po přesunu 25 procent připojení protokolu TCP na další výchozí bránu protokol TCP informuje protokol IP, aby aktualizoval výchozí trasu pro příslušnou adresu IP další výchozí bránou, kterou aktuálně používají změněná připojení.

Předpokládejme například u hostitele:

- Existují připojení protokolu TCP na 11 různých IP adres, které jsou směrovány přes výchozí bránu.
- Hostitel má nakonfigurováno několik výchozí bran.
- Hodnota **TcpMaxDataRetransmissions** je nastavena na přednastavenou hodnotu 5.

Když padne výchozí brána, následující proces přepne na výchozí bránu, která je další v seznamu:

1. Když se první připojení protokolu TCP snaží odeslat data, nedostane žádné potvrzení. Po třetím opakovaném přenosu je předávací adresa IP pro tuto vzdálenou adresu IP přepnuta na další výchozí bránu v seznamu. V tomto okamžiku jsou všechna připojení protokolu TCP na tuto vzdálenou adresu IP přepnuta na novou výchozí bránu, ale ostatní připojení se stále budou snažit použít původní výchozí bránu.
2. Když se druhé připojení protokolu TCP snaží odeslat data, stane se totéž. Nyní dvě z 11 připojení používají novou bránu.
3. Když se snaží odeslat data třetí připojení protokolu TCP, je jeho výchozí brána změněna na další v seznamu. Tři z 11 připojení jsou přepnuta na druhou výchozí bránu. Vzhledem k tomu, že se změnilo více než 25 procent připojení, aktualizuje se adresa IP výchozí brány trasy ve směrovací tabulce adresou IP nové brány.
4. Nová výchozí brána zůstává pro tento počítač jako primární až do doby, kdy nastanou problémy, které způsobí, že díky rozpoznání mrtvé brány dojde k přepnutí na další bránu na seznamu, nebo do doby restartu počítače.

Když vyhledávání dosáhne konce seznamu výchozích bran, vrátí se zpět na jeho začátek.

Chování protokolu TCP při opakovaném přenosu

Protokol TCP spustí časovač opakovaného přenosu po předání každého odchozího segmentu protokolu IP. Když neobdrží žádné potvrzení přijetí dat daného segmentu před vypršením časového limitu, znovu segment přeneše. U požadavků na nové připojení je časovač opakovaného přenosu inicializován do 3 sekund a požadavek na připojení protokolu TCP je poslán znovu tolikrát, kolik činí hodnota záznamu **TcpMaxConnectRetransmissions** (dle výchozího nastavení 2) v registru

(HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters). Na existujících připojeních je počet opakovaných přenosů řízen hodnotou záznamu **TcpMaxDataRetransmissions** (dle výchozího nastavení 5)

(HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

Časový limit opakovaného odesílání (RTO) je upravován průběžně tak, aby odpovídal znakům připojení, za použití výpočtů SRTT (Smoothed Round Trip Time) a Karnův algoritmus. Více podrobností o Karnově logaritmu najdete v části „Další informace“ později v této kapitole.

Časovač pro daný segment je po každém opakovaném přenosu tohoto segmentu zdvojen. Za použití tohoto algoritmu se protokol TCP optimalizuje na „normální“ opoždění připojení. Připojení protokolu TCP přes linky s velkým zpožděním zabere mnohem více času než připojení přes linky s krátkým zpožděním.

Následující snímek služby Network Monitoring znázorňuje algoritmus opakovaného přenosu pro dva hostitele připojené přes Ethernet na stejné podsíti. Právě probíhal přenos souboru pomocí protokolu FTP, když byl přijímající hostitel odpojen od sítě. Protože SRTT pro toto připojení byl velmi malý, byl první opakovaný přenos uskutečněn asi po půlce vteřiny. Časovač byl potom pro každý další opakovaný přenos zdvojeňován. Po patnáctém opakovaném přenosu byl časovač znovu zdvojen a, protože před vypršením časového limitu nedošlo žádné potvrzení, bylo připojení zrušeno.

```
time source ip      dest ip      pro flags description
0.000 10.57.10.32    10.57.9.138 TCP .A., len: 1460, seq: 8043781, ack:
8153124, win: 8760
0.521 10.57.10.32    10.57.9.138 TCP .A., len: 1460, seq: 8043781, ack:
8153124, win: 8760
1.001 10.57.10.32    10.57.9.138 TCP .A., len: 1460, seq: 8043781, ack:
8153124, win: 8760
2.003 10.57.10.32    10.57.9.138 TCP .A., len: 1460, seq: 8043781, ack:
8153124, win: 8760
4.007 10.57.10.32    10.57.9.138 TCP .A., len: 1460, seq: 8043781, ack:
8153124, win: 8760
8.130 10.57.10.32    10.57.9.138 TCP .A., len: 1460, seq: 8043781, ack:
8153124, win: 8760
```

Rychlý opakovaný přenos

Existují některé okolnosti, za kterých protokol TCP opakovaně přeneše data ještě před tím, než vyprší časový limit. Nejobvyklejší okolnost se objevuje díky vlastnosti známé jako *rychlý opakovaný přenos*. Když příjemce, který podporuje rychlý opakovaný přenos, obdrží data s vyšším číslem sekvence, než očekával, je pravděpodobné, že některá data byla ztracena. Aby uvědomil odesílatele o této události, odešle příjemce okamžitě opožděné potvrzení (ACK) s číslem potvrzení nastaveným na číslo sekvence, které očekával. Dělá to tak u každého dalšího segmentu protokolu TCP, který dorazí a obsahuje data následující po chybějících datech v příchozím proudu.

Když odesílatel začne dostávat proud opožděných potvrzení (ACK), která potvrzují stejné číslo sekvence, a toto číslo sekvence předchází odesílanému číslu sekvence, může z toho usoudit, že se ztratil nějaký segment (nebo segmenty). Odesílatelé, kteří podporují rychlý opakovaný přenos, okamžitě odešlou segment, který příjemce očekává, aby se zaplnila mezera v datech, bez toho, že by čekali na vypršení časového limitu tohoto segmentu. Tato optimalizace velice zvyšuje výkon v síťových prostředích s velkými ztrátami.

Dle výchozího nastavení operační systém Windows 2000 znovu pošle segment, když obdrží tři opožděná potvrzení (ACK) pro stejné číslo sekvence, které je nižší než aktuálně odesílané pořadové číslo. a toto pořadové číslo zaostává za aktuálním. Maximální počet duplicitních potvrzení, která spouští nové zaslání, je určen hodnotou **TcpMaxDupAcks** položky registru

(HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

Zprávy Keep-Alive protokolu TCP

Paket protokolu TCP keep-alive je jednoduše opožděné potvrzení (ACK) s číslem sekvence nastaveným na o jednu menší, než je aktuální číslo sekvence pro připojení. Hostitel, který obdrží takové ACK, bude odpovídat ACK s aktuálním číslem sekvence. Vlastnost Keep-Alive může být použita k ověření, že počítač na vzdáleném konci připojení je stále dostupný. Chování vlastnosti Keep-Alive v protokolu Windows 2000 TCP lze upravovat změnou hodnot položek **KeepAliveTime** a **KeepAliveInterval** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters). Hlášení Keep-Alive protokolu TCP může být odesláno jednou za určitou dobu specifikovanou hodnotou **KeepAliveTime** (výchozí nastavení je 7200000 milisekund, tedy dvě hodiny), pokud se přes připojení protokolu TCP nepřenesou jiná data nebo hlášení Keep-Alive vyšší úrovně. Pokud na toto hlášení není žádná odpověď, je opakováno jednou za nastavenou dobu specifikovanou hodnotou **KeepAliveInterval** vyjádřenou v sekundách. Dle výchozího nastavení je záznam **KeepAliveInterval** nastaven na hodnotu jedné sekundy.

Připojení typu NetBT, například připojení používaná mnoha síťovými komponentami společnosti Microsoft, posílá hlášení Keep-Alive typu NetBIOS častěji, takže normálně nejsou na připojení typu NetBIOS posílána žádná hlášení Keep-Alive protokolu TCP. Dle výchozího nastavení jsou hlášení Keep-Alive protokolu TCP zakázána, ale aplikace knihovny Windows Sockets je mohou pomocí funkce **setsockopt()** knihovny Windows Sockets povolit.

Algoritmus pomalého spuštění a vyhnutí se zahlcení

Protokol Windows 2000 TCP je kompatibilní s algoritmy pro pomalé spuštění a vyvarování se zahlcení. Více podrobností o těchto algoritmech najdete v části „Další informace“ později v této kapitole.

Po vytvoření připojení protokol TCP posílá data nejprve pomalu, aby zhodnotil šířku pásma připojení a aby se vyhnul zahlcení přijímajícího hostitele nebo některých dalších zařízení nebo linek na cestě. Poslané okno je nastaveno na dva segmenty protokolu TCP a po potvrzení obou segmentů se posílané okno zvětší na tři segmenty. Pokud jsou potvrzeny, je posílané okno znovu zvětšeno a tak to postupuje dál až do té doby, kdy množství dat odeslaných v jednom shluku dosáhne velikosti přijímaného okna inzerovaného vzdáleným hostitelem. V tomto okamžiku se už nepoužívá algoritmus pomalého spuštění a řízení proudu ovládá inzerované přijímané okno.

Kdykoli během přenosu se může objevit zahlcení. Zahlcení je detekováno poté, co vyprší časový limit opakovaného přenosu, nebo když hostitel obdrží hlášení ICMP Source Quench o segmentu protokolu TCP, který byl směrovačem vyřazen. Když nastane tato situace, je použit ke snížení velikosti posílaného okna algoritmus protokolu TCP pro vyvarování se zahlcení, který zmenší velikost okna na polovinu jeho velikosti v okamžiku, kdy se zahlcení objevilo. Pak je opět použit algoritmus pomalého spuštění, který zvětší postupně velikost posílaného okna na velikost přijímaného okna přijímajícího hostitele.

Syndrom SWS (Silly Window Syndrome)

Syndrom SWS je inzerování velikostí přijímacího okna, která je menší než plný segment protokolu TCP. Syndrom SWS může způsobit odesílání velmi malých segmentů protokolu TCP, výsledkem čehož je neefektivní využití sítě. Protokol Windows 2000 TCP/IP implementuje vyvarování se syndromu SWS u odesílatele i u příjemce tak, jak je specifikováno v dokumentu RFC 1122. Vyvarování se syndromu SWS na straně příjemce je implementováno neotevíráním přijímacího okna v přírůstku menším než je jeden segment protokolu TCP. Vyvarování se syndromu SWS na straně odesílatele je implementováno neodesláním více dat, dokud není dostatečná velikost okna inzerovaná přijímajícím koncem, aby mohl být poslán celý segment. Pro odesílatele existují z tohoto pravidla výjimky, které jsou popsány v dokumentu RFC 11.22.

Algoritmus Nagle

Protokol Windows 2000 TCP/IP implementuje algoritmus Nagle popsáný v dokumentu RFC 896. Účelem tohoto algoritmu je snížení počtu odeslaných malých segmentů, zvláště na (vzdálených) propojeních s dlouhou prodlevou. Malým segmentem se rozumí segment menší než MSS. Algoritmus Nagle dovoluje v jednom časovém okamžiku existenci pouze jednoho nedokončeného malého segmentu bez potvrzení.

jestliže je vygenerováno více malých segmentů, když se čeká na potvrzení (ACK) toho prvního, jsou tyto malé segmenty akumulovány do jednoho většího segmentu. Jakýkoli plně velký segment, za předpokladu, že je dostupné dostatečné přijímací okno, je přenesen okamžitě. Algoritmus Nagle je účinný při snižování počtu paketů posílaných interaktivními aplikacemi, jako je například Telnet, zvláště přes pomalé propojení.

Algoritmus Nagle si můžete prohlédnout v následujícím snímku služby Network Monitoring. Byla vytvořena relace protokolu Telnet (ve znakovém režimu), pak byla na pracovní stanici Windows 2000 stisknuta klávesa Y. Ve všech případech byl poslán jeden segment a ostatní znaky Y byly zadrženy zásobníkem, dokud nebylo přijato potvrzení předchozího segmentu. V tomto příkladě byly pokaždé ve vyrovnávací paměti uloženy tři až čtyři znaky Y a poslány dohromady v jednom segmentu. Díky algoritmu Nagle tak byl počet posílaných segmentů snížen asi na třetinu.

Time	Source IP	Dest IP	Prot	Description
0.644	204.182.66.83	199.181.164.4	TELNET	To Server Port = 1901
0.144	199.181.164.4	204.182.66.83	TELNET	To Client Port = 1901
0.000	204.182.66.83	199.181.164.4	TELNET	To Server Port = 1901
0.145	199.181.164.4	204.182.66.83	TELNET	To Client Port = 1901
0.000	204.182.66.83	199.181.164.4	TELNET	To Server Port = 1901
0.144	199.181.164.4	204.182.66.83	TELNET	To Client Port = 1901
. . .				

Každý segment obsahoval několik znaků Y. První segment je podrobněji rozebrán níže a dávky dat jsou zvýrazněny v šestnáctkovém (hexadecimálním) formátu na konci.

```
Time Source IP      Dest IP      Prot  Description
0.644 204.182.66.83 199.181.164.4 TELNET To Server Port = 1901

+ FRAME: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
+ IP: ID = 0xEA83; Proto = TCP; Len: 43
+ TCP: .AP..., len: 3, seq:1032660278, ack: 353339017, win: 7766, src:
1901 dst: 23 (TELNET)
  TELNET: To Server From Port = 1901
    TELNET: Telnet Data

D2 41 53 48 00 00 52 41 53 48 00 00 08 00 45 00 .ASH..RASH....E.
00 2B EA 83 40 00 20 06 F5 85 CC B6 42 53 C7 B5 .+..@. ....BS..
A4 04 07 6D 00 17 3D 8D 25 36 15 0F 86 89 50 18 ...m..=.%6....P.
1E 56 1E 56 00 00 79 79 79 .V.V..yyy
```

Aplikace knihovny Windows Sockets mohou zakázat používání algoritmu Nagle pro svá připojení nastavením možnosti soketu na **TCP_NODELAY**. Nicméně tento krok by neměl být používán jindy než v případech naprosté nutnosti, protože zvyšuje zatížení sítě. Některé síťové aplikace nemusí fungovat správně, pokud jejich návrh nebere v úvahu vliv přenášení velkého množství malých paketů a algoritmu Nagle.

Algoritmus Nagle není aplikován na připojení zpětné smyčky protokolu TCP z důvodů výkonu. Windows 2000 NetBt zakazuje použití algoritmu Nagle pro připojení typu NetBIOS přes protokol TCP stejně jako pro připojení přesměrovač/server jiného typu než NetBIOS, což může zlepšit výkon aplikací zpracovávajících malé soubory. Příkladem je aplikace, která často používá zamykání/odemykání souboru.

Zpoždění TIME-WAIT protokolu TCP

Po zavření připojení protokolu TCP je pár soketů uveden do stavu známého jako TIME-WAIT, takže nové připojení nepoužívá stejný protokol, zdrojovou adresu IP, cílovou adresu IP, zdrojový port a cílový port, pokud neuplyne dostatek času na to, aby se systém přesvědčil, že již nebudou neočekávaně doručeny nějaké segmenty, které se zpozdily nebo zabloudily. Doba, po kterou by neměl být pár soketů znovu využit, specifikuje dokument RFC 793 jako dvě nejdelší doby platnosti (2MLS) nebo 240 sekund (čtyři minuty). To je výchozí nastavení ve Windows 2000. Nicméně s tímto přednastaveným nastavením některé síťové aplikace, které provádějí mnoho odchozích připojení během krátké doby, mohou vyčerpat všechny dostupné porty ještě před tím, než se mohou recyklovat.

Operační systém Windows 2000 nabízí dvě metody řízení tohoto chování. Zprv, tuto hodnotu lze změnit v záznamu **TcpTimedWaitDelay** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters). Operační systém Windows 2000 umožňuje nastavení této hodnoty až na minimum 30 sekund, což by nemělo ve většině prostředí působit žádné problémy. Za druhé, počet efemérních portů dostupných uživateli, které je možnou použít pro připojení odchozí ze zdroje, je ovlivnitelný záznamem **MaxUserPort** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters). Dle výchozího nastavení je při požadavku aplikace na soket systému pro odchozí volání přiřazen port mezi hodnotami 1024 a 5000. Pro nastavení hodnoty nejvyššího čísla portu použitelného

pro odchozí volání můžete použít záznam MaxUserPort v registru. Například nastavení této hodnoty na 10000 by umožnilo pro odchozí volání používat přibližně 9000 uživatelských portů. Více podrobností najdete v dokumentu RFC 793. Viz též nastavení **MaxFreeTcbs** a **MaxHashTableSize** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

Připojení protokolu TCP na vícedomé a z vícedomých počítačů

Když se protokol TCP připojuje na vícedomého hostitele, snaží se klient WINS i DNR (Domain Name Resolver) zjistit, jestli je některá z cílových adres IP poskytnutých názvovým serverem na stejné podsíti jako kterékoli rozhraní lokálního počítače. Pokud ano, jsou takové adresy zařazeny na začátek seznamu, takže aplikace je může zkusit ještě před použitím adres, které nejsou na stejné podsíti. Pokud není žádná z těchto adres na podsíti společné s lokálním počítačem, je chování různé v závislosti na oboru názvů. Zařazení adres lokální podsítě na začátek seznamu lze zabránit pomocí záznamu **PrioritizeRecordData** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

V oboru názvů WINS je za vybrání náhodné adresy z poskytnutých adres zodpovědný klient. Server WINS vždy zobrazí seznam adres ve stejném pořadí a klient WINS si z něj náhodným výběrem vybere jednu adresu pro každé připojení.

V oboru názvů DNS je server DNS zpravidla nakonfigurován tak, aby poskytoval adresy v cyklickém pořadí. DNR nevybírá adresu náhodně. V některých situacích je žádoucí se připojit na určité rozhraní na vícedomém počítači. Nejlepší cesta, jak toho dosáhnout, je vybavit rozhraní vlastní položkou DNS. Například počítač pojmenovaný Počítač by mohl mít dva oddělené záznamy DNS se stejným názvem, jeden pro každou adresu IP, a pak záznamy v DNS pro Počítač1 a Počítač2, každý asociovaný s právě jednou adresou IP přiřazenou počítači.

Co se týče připojení protokolu TCP realizovaných z vícedomého hostitele, jestliže je připojení připojením typu Winsock používající obor názvů DNS, jakmile je známá cílová adresa IP připojení, protokol TCP se snaží připojit z nejlepší dostupné zdrojové adresy IP. K tomuto určení je použita směrovací tabulka IP a jestliže v ní je zapsáno rozhraní lokálního počítače, které je na stejné podsíti jako cílová adresa IP, je jako zdroj v požadavku připojení použita tato adresa IP. Pokud ve směrovací tabulce není žádná nejlepší adresa IP, systém jednu vybere náhodně.

Jestliže je připojení připojením typu NetBIOS používající přesměrovač, je na úrovni aplikací dostupných malé množství směrovacích informací. Rozhraní NetBIOS podporuje připojení přes různé protokoly a nezná protokol IP. Namísto toho přesměrovač umísťuje volání na všechny logické sítě, které jsou na něj navázané. Pokud jsou na počítači dvě rozhraní a nainstalovaný jeden protokol, jsou přesměrovači dostupné dvě logické sítě. Volání jsou umísťována na obě sítě a NetBIOS nad protokolem TCP/IP (NetBT) odešle žádost zásobníku za použití adresy IP z každého rozhraní. Je možné, že obě volání budou úspěšná. Pokud ano, přesměrovač jedno z nich zruší. Výběr, které volání bude zrušeno, závisí na hodnotě záznamu **ObeYBindingOrder** v registru. Je-li hodnota záznamu 0 dle výchozího nastavení, je primární logická síť určená závazným pořadím preferována a přesměrovač před přijetím připojení sekundárního transportu čeká na vypršení časového limitu primárního transportu. Je-li hodnota 1, je závazné pořadí ignorováno a přesměrovač přijme první připojení, které je úspěšné a zruší všech na další připojení.

Činitelé propustnosti

Protokol Windows 2000 TCP/IP se může adaptovat na většinu podmínek sítě a může dynamicky poskytovat nejlepší možnou propustnost a spolehlivost pro každé připojení. Snahy o manuální vyladění jsou zpravidla kontraproduktivní, pokud je neprovádí odborník po důkladném prozkoumání datového proudu.

Protokol TCP je navržen tak, aby poskytoval optimální výkon za různých podmínek na propojeních a operační systém Windows 2000 obsahuje jeho vylepšení, například vylepšení podporující dokument RFC 1323. Skutečná průchodnost propojení závisí na množství proměnných, ale mezi nejdůležitější faktory patří:

- Rychlost propojení (bity za sekundu, které lze přenést).
- Prodleva šíření.
- Velikost okna (množství nepotvrzených dat, která mohou být na připojení protokolu TCP otevřená).
- Spolehlivost propojení.
- Zahlčení sítě a zprostředkovávajícího zařízení.

Klíčové činitelé propustnosti:

- Kapacita komunikačního kanálu označovaného také jako kanál, je známá jako produkt zpoždění šířky pásma a je to šířka pásma (v bitech) vynásobená časem RTT (od odeslání požadavku po příjem odezvy). Pokud má propojení nižší počet chyb na úrovni bitů, velikost okna by pro nejlepší výkon měla být větší nebo stejná jako produkt zpoždění šířky pásma, aby odesílatel mohl naplnit kanál. Bez změny velikosti okna je největší velikost okna 65535 a může být specifikována pomocí 16bitového pole okna v hlavičce TCP. Změna velikosti okna může být použita pro velikosti okna až do 1 GB.
- Propustnost nemůže nikdy přesáhnout velikost okna dělenou časem RTT.
- Pokud má propojení velké množství chyb na úrovni bitů nebo je velmi zahlceno a dochází ke ztrátám paketů, použití většího okna nemusí propustnost zlepšit. Operační systém Windows 2000 podporuje potvrzení SACK (pro lepší výkon ve vysoce ztrátových prostředích) a časová razítka protokolu TCP (pro lepší odhad času RTT).
- Zpožděné šíření je závislé na rychlosti přenosu elektrických nebo optických signálů v různých médiích a čekacích dobách v přenosových zařízeních a zprostředkujících systémech.
- Zpoždění přenosu závisí na rychlosti média a povaze řídicího schématu přístupu k médiu.
- U jednotlivých cest je zpoždění šíření pevné, ale zpoždění přenosu závisí na velikosti paketu a zahlčení.
- Při nízkých rychlostech je limitujícím faktorem zpoždění přenosu. Při vysokých rychlostech se limitujícím faktorem může stát zpoždění šíření.

Protokol UDP (User Datagram Protocol)

Protokol UDP poskytuje nespolehlivou transportní službu bez připojení. Často se používá pro komunikaci jeden k mnoha (one-to-many), která používá všesměrové vysílání nebo vícesměrové IP datagramy. Doručení datagramů protokolu UDP není zaručeno, aplikace používající protokol UDP musí ztracené datagramy protokolu UDP kom-

penzovat pomocí jednoduchého opakovaného přenosu nebo jiných spolehlivých mechanismů. Síť Microsoft používají protokol UDP pro přihlášení se, prohledávání a překlad názvu typu NetBIOS. Protokol UDP lze také použít k zajištění vícesměrových proudů IP pro aplikace, jako je například Microsoft® NetShow™.

Protokol UDP a překlad názvu

Protokol UDP se používá k překladu názvu typu NetBIOS prostřednictvím jednosměrového vysílání na názvový server NetBIOS nebo prostřednictvím všesměrového vysílání na podsítěch a k překladu DNS názvu hostitele adresy IP. Překlad názvu typu NetBIOS probíhá přes port 137 protokolu UDP. Dotazy DNS používají port 53 protokolu UDP. Vzhledem k tomu, že protokol UDP sám nezaručuje doručení datagramů, používají obě tyto služby v případě neobdržení žádné odpovědi na svůj dotaz vlastní schémata opakovaného přenosu. Datagramy protokolu UDP ve všesměrovém vysílání nejsou zpravidla předávány přes IP směrovače, takže překlad názvu typu NetBIOS v prostředí se směrovači vyžaduje názvový server, například server WINS, nebo použití statického datábázového souboru, například souboru Lmhosts.

Zásuvka pošty přes protokol UDP

Mnoho aplikací typu NetBIOS používá posílání zpráv přes zásuvky pošty. Zásuvka pošty druhé třídy je jednoduchý mechanismus pro odesílání zpráv z jednoho názvu typu NetBIOS na jiný přes protokol UDP. Zprávy na zásuvku pošty mohou být všesměrově vysílány na podsíti nebo směrovány na určitého hostitele.

Rozhraní síťových aplikací

Existuje řada způsobů, kterými mohou síťové aplikace komunikovat za použití zásobníku protokolu TCP/IP. některé z nich, například pojmenované kanály, procházejí přes síťový přesměrovač, který je součástí služby workstation. Mnoho starších aplikací bylo napsáno pro rozhraní NetBIOS, které je podporováno službou NetBIOS pro protokol TCP/IP. V této části knihy najdete přehled rozhraní Windows Sockets Interface a rozhraní NetBIOS Interface.

Windows Sockets

Rozhraní Windows Sockets specifikuje programovací rozhraní založené na běžném rozhraní soketů z Kalifornské univerzity v Berkeley. Zahrnuje sadu rozšíření navržených tak, aby využívaly výhody zprávami řízeného charakteru operačního systému Microsoft Windows. Verze 1.1 byla uvolněna v lednu 1993 a verze 2.2.0 byla publikována v květnu 1996. Operační systém Windows 2000 podporuje verzi 2.2, která se běžně označuje jako Winsock2.

Aplikace

Existuje mnoho dostupných aplikací pro rozhraní Windows Sockets. Řada nástrojů, které náleží k operačnímu systému Windows 2000 je založena na rozhraní Windows Sockets, například nástroje Ping a Tracert, klient a server FTP a DHCP a klient Telnet. Existují také programovací rozhraní vysoké úrovně, která se spoléhají na Winsock, například Windows Internet API (WININET) používaný programem Microsoft® Internet Explorer.

Překlad názvů a adres

Aplikace rozhraní Windows Sockets pro přiřazení názvu hostitele IP adres obecně používají funkci **gethostbyname()**. Dle výchozího nastavení funkce **gethostbyname()** používá následující pořadí vyhledávání názvu:

1. Zkontroluj, jestli dotazovaný název odpovídá názvu hostitele.
2. Zkontroluj, jestli odpovídá nějaký záznam názvu v souboru hosts.
3. Je-li nakonfigurován server DNS, dotaž se ho.
4. Není-li nalezen žádný odpovídající záznam, vyzkoušej sekvenci překladu názvu typu NetBIOS popsanou v části „NetBIOS pro TCP/IP“ později v této kapitole až do bodu, ve kterém je zkoušeno překlad DNS.

Některé aplikace používají funkci **gethostbyaddr()** k přiřazení adresy IP názvu hostitele. Volání **gethostbyaddr()** používá následující (dle výchozího nastavení) pořadí:

1. Zkontroluje, jestli je v souboru hosts odpovídající záznam adresy.
2. Je-li nakonfigurován server DNS, dotáže se ho.
3. Pošle požadavek NetBIOS Adapter Status Request na hledanou adresu IP a pokud odpoví seznamem názvů typu NetBIOS registrovaných pro adaptér, analyzuje ho a hledá název počítače.

Podpora vícesměrového vysílání protokolu IP

Winsock2 podporuje vícesměrové vysílání protokolu IP. Vícesměrové vysílání je popsáno ve specifikaci Windows Sockets 2.0 a v části „Protokol IGMP (Internet Group Management Protocol)“ dříve v této kapitole. Vícesměrové vysílání protokolu IP je aktuálně podporováno pouze pro datagramy protokolu IP a pro holé sokety.

Parametr rezerva

Aplikace serveru Windows Sockets obecně vytvářejí soket a pak na něm pro příjem požadavků o připojení používají funkci **listen()**. Jedním z parametrů zadávaných při používání funkce **listen()** je rezerva požadavků na připojení, které by aplikace chtěla zařadit do fronty na soket. Specifikace Windows Sockets 1.1 určuje, že maximální povolená hodnota pro rezervu je 5. Microsoft® Windows NT® version 3.51 nicméně akceptuje rezervu až do hodnoty 100, Microsoft® Windows NT® 4.0 Server a Windows 2000 Server až do 200 a Microsoft® Windows NT® 4.0 Workstation a Windows 2000 Professional akceptují rezervu 5 (což snižuje obsazení v paměti).

Interpretace bitu řídicího neukládání ve vyrovnávací paměti (push bit)

Dle výchozího nastavení protokol Windows 2000 TCP dokončuje funkci Windows Sockets **recv()** při splnění jedné z následujících podmínek:

- Data dorazí s nastaveným bitem neukládání do vyrovnávací paměti. Bit řídicí neukládání do vyrovnávací paměti se používá k určení protokolu TCP, že data v segmentu protokolu TCP a všechna další data v přijímací vyrovnávací paměti (která souvisí se segmentem protokolu TCP) musí být okamžitě postoupena aplikaci.
- Vyrovnávací paměť uživatele funkce **recv()** je plná.
- Od příchodu jakýchkoli dat uplynulo 0,5 sekundy.

Pokud je na počítači s implementací protokolu TCP, která odesílaným operacím nenastavuje bit řídicí neukládání ve vyrovnávací paměti, spuštěna klientská aplikace, mohou být výsledkem zpoždění odpovědi. Nejlepší je toto opravit přímo na klientském počítači, nicméně lze také použít nastavení záznamu **IgnorePushBitOnReceives** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Afd\Parameters) na 1, takže bude všechny příchozí pakety brát tak, jako kdyby měly nastavený bit určující neukládání ve vyrovnávací paměti.

NetBIOS pro TCP/IP

Implementace rozhraní *NetBIOS pro TCP/IP* v operačním systému Windows 2000 se označuje jako NetBT. NetBT používá následující porty protokolu TCP a UDP:

- UDP port 137 (názvové služby)
- UDP port 138 (datagramové služby)
- TCP port 139 (relační služby)

NetBIOS pro TCP/IP je specifikován v dokumentech RFC 1001 a 1002. Ovladač Netbt.sys je komponenta režimu jádra, která podporuje rozhraní TDI. Služby jako workstation nebo server používají rozhraní TDI přímo, zatímco tradiční aplikace rozhraní NetBIOS mapují svá volání na volání rozhraní TDI prostřednictvím ovladače Netbios.sys. Používání rozhraní TDI k voláním rozhraní NetBIOS je složitější programovací úkol, ale může zvýšit výkon a osvobodit od historických omezení rozhraní NetBIOS. Rozhraní NetBIOS definuje rozhraní softwaru a názvovou konvenci, nikoli protokol. NetBIOS pro TCP/IP poskytuje programovací rozhraní NetBIOS pro protokol TCP/IP s tím, že rozšiřuje dosah klienta NetBIOS a programů serveru na síť IP a umožňuje spolupráci s různými dalšími operačními systémy.

Služba workstation Windows 2000, serverová služba, služby prohlédávání, messenger a NetLogon jsou klienty rozhraní NetBT a ke komunikaci s NetBT používají rozhraní TDI. Operační systém Windows 2000 také zahrnuje emulátor rozhraní NetBIOS. Emulátor přebírá standardní požadavky na rozhraní NetBIOS od aplikací rozhraní NetBIOS a překládá je na odpovídající funkce rozhraní TDI.

Operační systém Windows 2000 používá rozhraní NetBIOS pro TCP/IP ke komunikaci s dřívějšími verzemi operačního systému Windows NT a jinými klienty, například Windows 95. Nicméně služby přeměrovač a server operačního systému Windows 2000 nyní podporují přímé hostitelství komunikace s ostatními počítači běžícími na platformě Windows 2000. U přímého hostitelství se rozhraní NetBIOS pro překlad názvů nepoužívá, ale používá se rozhraní DNS. Síťová komunikace je posílána přímo přes rozhraní TCP bez hlavičky rozhraní NetBIOS. přímé hostitelství přes TCP/IP používá TCP port 445 namísto relačního TCP portu rozhraní NetBIOS 139.

Dle výchozího nastavení je povoleno rozhraní NetBIOS i přímé hostitelství a při vytváření nového připojení jsou zkoušena obě paralelně. První úspěšné rozhraní je pak při připojení používáno dál. Podpora rozhraní NetBIOS pro TCP/IP může být zakázána, takže je veškerý provoz nucen používat přímé hostitelství na protokolu TCP/IP.

► Podporu rozhraní NetBIOS pro TCP/IP zakázete takto:

1. Z ikony Síťové a telefonické připojení v Ovládacích panelech vyberte Lokální připojení a pravým tlačítkem vyvolejte Vlastnosti.
2. Na záložce Obecné klepněte na seznamu komponent na Internetový protokol (TCP/IP) a klepněte na tlačítko Vlastnosti.

3. Klepněte na tlačítko Upřesnit.
4. Klepněte na záložku WINS. Klepněte na Zakázat NetBIOS pro TCP/IP.

Aplikace a služby, které závisí na rozhraní NetBIOS pro TCP/IP po zakázání rozhraní NetBIOS pro TCP/IP nefungují. Je proto vhodné před zakázáním tohoto rozhraní ověřit, že žádní klienti nebo aplikace nepotřebují jeho podporu.

Názvy typu NetBIOS

Obor názvů rozhraní NetBIOS je plochý (nestrukturovaný), což znamená, že všechny názvy v oboru názvů musí být jedinečné. Názvy typu NetBIOS jsou 16 bajtů dlouhé. Prostředky jsou identifikovány pomocí názvů typu NetBIOS, které jsou dynamicky registrovány při spuštění služeb nebo aplikací nebo při přihlášení uživatelů. Názvy mohou být registrovány jako jedinečné názvy (jeden vlastník) nebo jako skupinové názvy (více vlastníků). K lokalizaci prostředku pomocí přiřazení názvu typu NetBIOS adrese IP se používá dotaz NetBIOS Name Query.

Síťové komponenty společnosti Microsoft, například služby workstation nebo server, umožňují uživateli nebo administrátorovi specifikovat prvních 15 znaků názvu typu NetBIOS, ale 16. znak názvu typu NetBIOS rezervují pro určení typu zdroje (00-FF hex). Tabulky 2.2 a 2.3 nabízejí některé příklady názvů typu NetBIOS používaných komponentami společnosti Microsoft:

Tabulka 2.2 Jedinečné názvy typu NetBIOS používané komponentami společnosti Microsoft

Jedinečný název	Služba
<název_počítače>[00] (vyplněný prostor) ¹	Workstation Service
< název_počítače >[03] (vyplněný prostor)	Messenger Service
< název_počítače >[06] (vyplněný prostor)	RAS Server Service
< název_počítače >[1F] (vyplněný prostor)	NetDDE Service
< název_počítače >[20] (vyplněný prostor)	Server Service
< název_počítače >[21] (vyplněný prostor)	RAS Client Service
< název_počítače >[BE] (0xBE vyplněný)	Network Monitor Agent
< název_počítače >[BF] (0xBF vyplněný)	Network Monitor Application
<název_uživatele>[03]	(vyplněný prostor) Messenger Service
<název_domény>[1D] (vyplněný prostor)	Master Browser
<název domény>[1B] (vyplněný prostor)	Domain Master Browser

¹ Číslo v závorkách je šestnáctkové (hexadecimální) číslo. (vyplněný prostor) znamená, že pokud není název počítače nebo domény dlouhý 15 znaků, je zbytek prostoru mezi názvem a posledním rozlišujícím znakem do 15 znaků doplněn mezerami.

Tabulka 2.3 Skupinové názvy typu NetBIOS používané komponentami společnosti Microsoft

Skupinový název	Služba
<název_domény>[00] (vyplněný prostor)	Domain Name
< název_domény >[1C] (vyplněný prostor)	Domain Controllers
< název_domény >[1E] (vyplněný prostor)	Browser Service Elections
[01h][01h]__MSBROWSE__[01h][01h]	Master Browser

Nástroj NBTStat

Nástroj NBTStat je používán k zobrazení a registrování názvů typu NetBIOS na počítači na platformě Windows 2000. Chcete-li vidět, které názvy typu NetBIOS počítač zaregistroval přes NetBT, napište na příkazové řádce následující příkaz:

```
nbtstat -n
```

Operační systém Windows 2000 umožňuje opětovnou registraci názvů typu NetBIOS pomocí názvového serveru i u již spuštěného počítače. Chcete-li opětovně registrovat názvy typu NetBIOS, napište na příkazové řádce následující příkaz:

```
nbtstat -RR
```

Registrace a zjištění názvu typu NetBIOS

Systémy s protokolem Windows 2000 TCP/IP používají pro lokalizaci prostředků typu NetBIOS několik metod:

- Mezipaměť názvů typu NetBIOS.
- Názvový server NetBIOS.
- Všesměrové vysílání v podsítích IP.
- Statický soubor Lmhosts.
- Statický soubor Hosts (volitelný, závisí na položce **EnableDns** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Netbt\Parameters)).
- Server DNS (volitelný, závisí na položce **EnableDns** v registru).

Pořadí zjištění názvů typu NetBIOS závisí na typu uzlu a konfiguraci systému. Podporovány jsou následující typy uzlu:

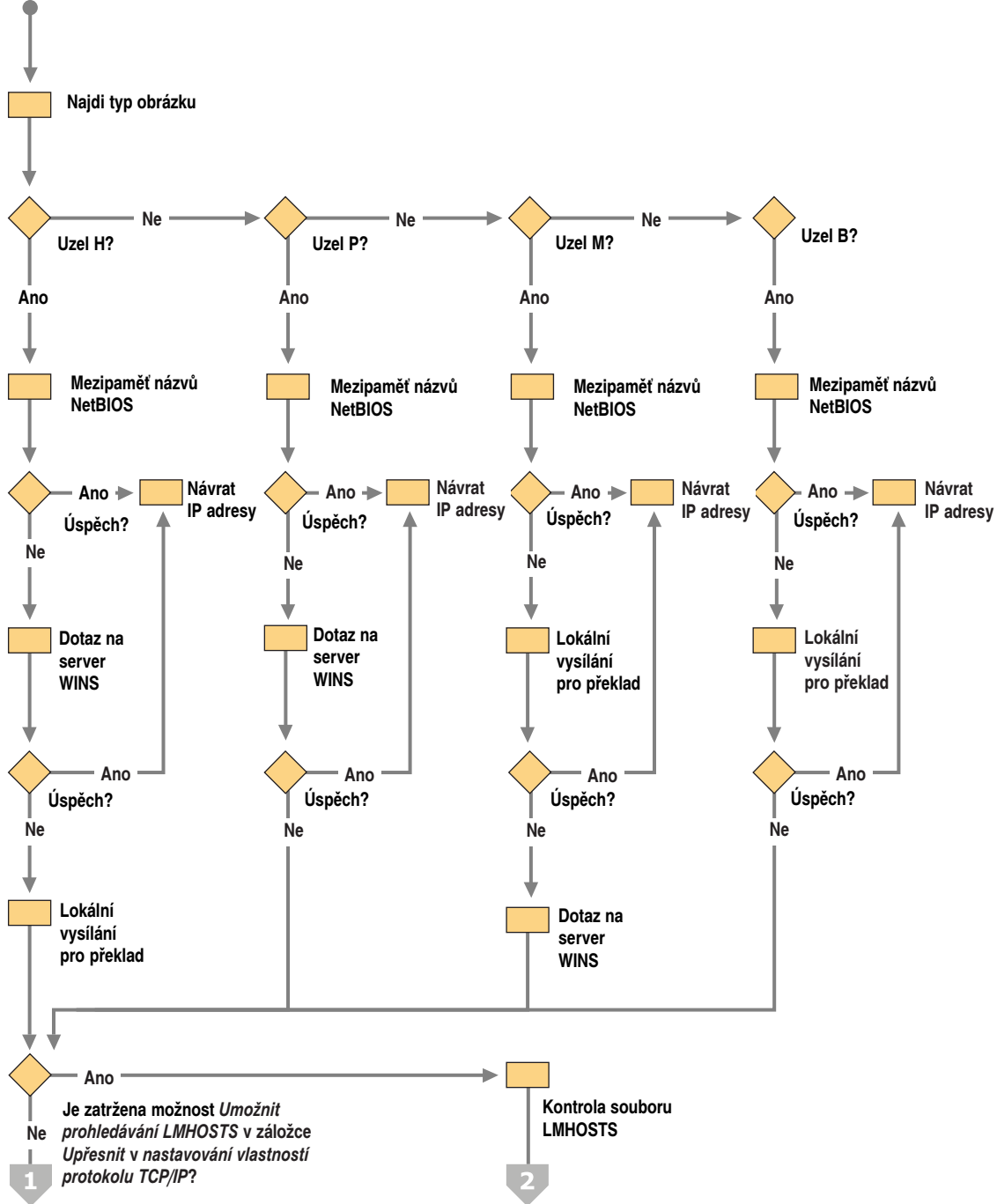
- *Uzel B* – k registraci a zjištění názvu používá všesměrové vysílání.
- *Uzel P* – k registraci a zjištění názvu používá názvový server NetBIOS
- *Uzel M* – k registraci názvu používá všesměrové vysílání. Při zjišťování názvu nejprve zkouší všesměrové vysílání a pokud neobdrží žádnou odpověď, přepne se na režim uzlu p.
- *Uzel H* – k registraci a zjištění názvu používá názvový server NetBIOS. Nicméně pokud žádný názvový server nemůže lokalizovat, přepne se na režim uzlu b. Pokračuje v dotazování se na názvový server a pokud nějaký dostupný nalezne, přepne se zpět na režim uzlu p.
- Microsoft-enhanced (vylepšený) – navíc ke standardním typům uzlů používá lokální soubor Lmhosts nebo WINS proxy plus volání Windows Sockets **gethostbyname()** (za použití standardního DNS a/nebo lokálního souboru Hosts).

Microsoft obsahuje názvový server NetBIOS známý jako služba Windows Internet Name Service (WINS). Většina klientů WINS je nastavena jako uzel h. To znamená, že se nejprve snaží registrovat a zjistit název za pomoci služby WINS a až když tato metoda zklame, vyzkouší všesměrové vysílání na lokálních podsítích. Použití názvového serveru je zpravidla dávana přednost před všesměrovým vysíláním ze dvou důvodů:

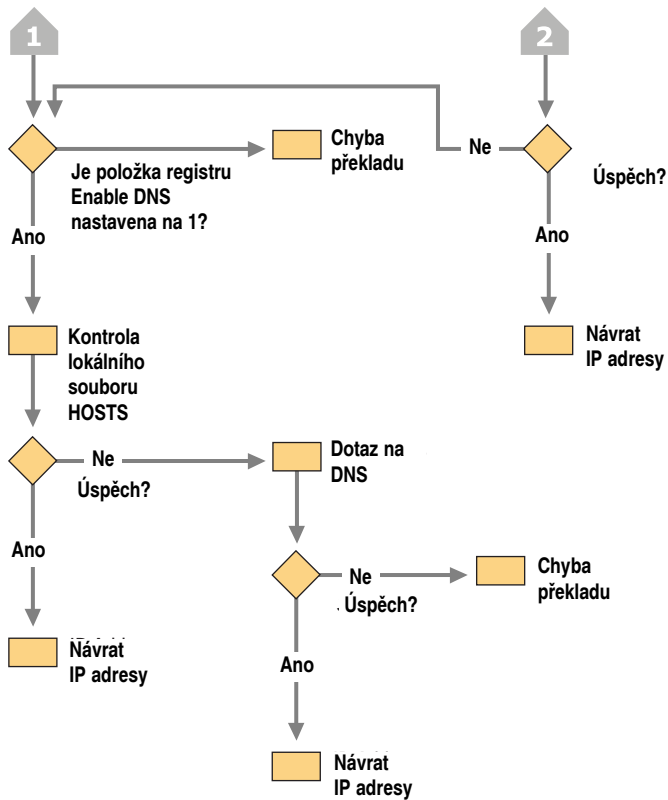
- Všesměrové vysílání není zpravidla směrovači předáváno.
- Rámce všesměrového vysílání jsou zpracovávány všemi počítači na podsíti.

Na obrázcích 2.4. a 2.5 jsou znázorněny metody zjištění názvu typu NetBIOS používané v operačním systému Windows 2000.

Start



Obrázek 2.4 Graf toku zjištění názvu typu NetBIOS (část 1 ze 2)



Obrázek 2.4 Graf toku zjištění názvu typu NetBIOS (část 2 ze 2)

Registrace a zjištění názvu typu NetBIOS u vícedomých počítačů

Rozhraní NetBIOS pro TCP/IP (NetBT) se váže pouze na jednu adresu IP na jedno rozhraní fyzické sítě. Z pohledu rozhraní NetBIOS pro TCP/IP (NetBT) je počítač vícedomý, pouze pokud má instalovaný více než jeden síťový adaptér. Když je z vícedomého počítače odeslán paket s registrací názvu, dostane příznak registrace vícedomého názvu, takže nekoliduje se stejným názvem registrovaným jiným rozhraním stejného počítače.

Když vícedomý počítač obdrží všesměrové vysílání dotazu NetBIOS Name Query, všechny vazby rozhraní, které přijmou dotaz, odpovídají svými adresami a dle výchozího nastavení klient vybere první odpověď a připojí se na adresu dodanou odpovídající protějškem. Po nastavení hodnoty záznamu **RandomAdapter** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Netbt\Parameters) na 1 bude odpovídající protějšek náhodně vybírat adresu IP, na kterou odešle svou odpověď na dotaz NetBIOS Name Query. Toto může použít server se dvěma rozhraními na stejné síti kvůli vyrovnávání zatížení sítě.

Po odeslání směrovaného dotazu NetBIOS Name Query na server WINS server WINS odpovídá seznamem všech adres IP, které jsou registrovány serverem WINS vícedomého počítače.

Klient Windows 2000 používá k výběru nejlepší adresy IP pro připojení na vícedomý počítač následující proces:

1. Pokud je jedna z adres IP v seznamu odpovědi na dotaz NetBIOS Name Query na stejné logické podsíti jako lokální počítač, je vybrána tato adresa. Pokud těmto kritériím vyhovuje více než jedna adresa, je z nich jedna vybrána náhodným výběrem.
2. Pokud je jedna z adres IP v seznamu odpovědi na dotaz NetBIOS Name Query na stejné logické podsíti jako některá z vazeb rozhraní NetBIOS pro TCP/IP (NetBT) na lokálním počítači, je vybrána tato adresa. Pokud těmto kritériím vyhovuje více než jedna adresa, je z nich jedna vybrána náhodným výběrem.
3. Pokud není ani jedna z adres IP v seznamu odpovědi na dotaz NetBIOS Name Query na stejné logické podsíti jako lokální počítač, je adresa vybrána ze seznamu náhodným výběrem.
4. Pokud není ani jedna z adres IP v seznamu odpovědi na dotaz NetBIOS Name Query na stejné logické podsíti jako některá z vazeb rozhraní NetBIOS pro TCP/IP (NetBT) na lokálním počítači, je adresa vybrána ze seznamu náhodným výběrem.

Tento algoritmus poskytuje rozumné vyrovnávání připojení k serveru přes více síťových adaptérů, ale zároveň upřednostňuje lokální připojení (připojení na stejné podsíti), pokud jsou dostupná. Aby byla poskytnuta jistá odolnost proti chybám, je seznam adres IP z odpovědi seřazen do nejlepšího pořadí a rozhraní NetBIOS pro TCP/IP (NetBT) se snaží kontaktovat pomocí utility Ping na každou adresu v seznamu, dokud jedna z nich neodpoví. Rozhraní NetBIOS pro TCP/IP (NetBT) se pak snaží o připojení na tuto adresu. Neodpovídá-li žádná adresa, je učiněn pokus o připojení k první adrese v seznamu, a to v případě, že zde existuje bezpečnostní brána (firewall) nebo jiné zařízení filtrující provoz protokolu ICMP. Operační systém Windows 2000 podporuje mezipaměť názvů rozhraní NetBIOS pro TCP/IP (NetBT) pro každé rozhraní. Obsah mezipaměti názvů lze pro jednotlivá rozhraní zobrazit pomocí příkazu `nbtstat -c`.

Rozšíření rozhraní NetBIOS pro TCP/IP (NetBT) pro Internet/DNS v operačním systému Windows 2000

Je možné připojit se z jednoho počítače na platformě Windows 2000 na jiný za použití rozhraní NetBIOS pro TCP/IP (NetBT) přes Internet. Aby to bylo možné, bylo nutné poskytnout některé způsoby překladu názvu. Dvě obvyklé metody jsou soubor `Lmhosts` a server WINS. V operačním systému Windows NT 4.0 bylo zavedeno několik vylepšení k eliminaci nutnosti zvláštní konfigurace. Tato vylepšení byla ještě rozšířena ve Windows 2000.

Nyní je možné se k rozhraní NetBIOS pro TCP/IP připojit dvěma způsoby:

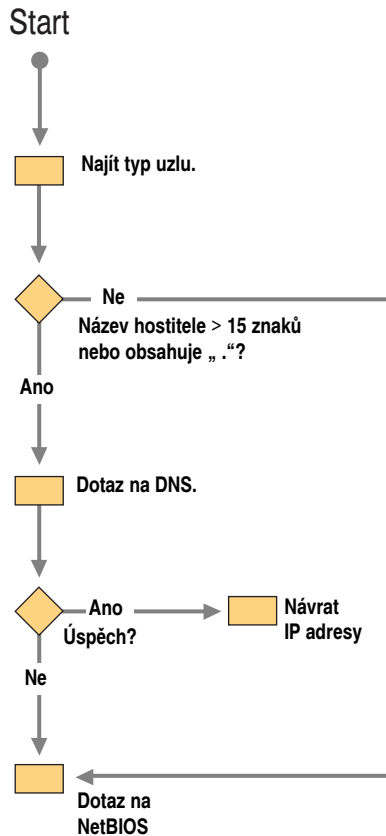
- Za použití příkazu **net use** `\\<ip address>\<share_name>`. To eliminuje potřebu konfigurace překladu názvu typu NetBIOS.
- Za použití příkazu **net use** `\\<FQDN>\<share_name>`. To umožňuje použití serveru DNS k připojení se k počítači používajícímu úplný doménový název (FQDN).

Zde vidíte příklady použití nové funkcionality k mapování jednotky do `ftp.microsoft.com` na adrese IP 198.105.232.1:

- **net use f:** `\\ftp.microsoft.com\data`
- **net use** `\\198.105.232.1\data`
- **net view** `\\198.105.232.1`

■ `dir \\ftp.microsoft.com\bussys\winnt`

Navíc vám různé aplikace umožňují přístup k FQDN nebo adrese IP namísto k názvu počítače. Toto nové chování je znázorněno na obrázku 2.6.



Obrázek 2.6 Chování rozšíření rozhraní NetBIOS pro TCP/IP (NetBT) pro Internet/DNS

V operačním systému Windows 2000 je také možné pro vytvoření připojení přesměrovače nebo serveru mezi počítači na platformě Windows 2000 použít přímé hostitelství bez použití rozhraní NetBIOS. Dle výchozího nastavení se operační systém Windows 2000 snaží vytvořit připojení pomocí obou metod, takže může podporovat připojení k počítačům se starší verzí Windows. Nicméně v prostředích pouze s Windows 2000 můžete rozhraní NetBIOS pro TCP/IP zakázat, viz v části „Relace rozhraní NetBIOS pro TCP/IP“ dále v této kapitole.

Nové rozhraní v operačním systému Windows 2000, které umožňuje operace bez rozhraní NetBIOS, je nazvané zařízení SMB (Server Message Block). Přesměrovači a serveru se jeví spíše jako další rozhraní než jako kombinace samostatného síťového adaptéru a zásobníku protokolu. Nicméně u zásobníku protokolu TCP/IP je zařízení SMB navázáno na ADDR_ANY a používá obor názvů DNS jako aplikace Windows Sockets. Volání umístěné na zařízení SMB ústí ve standardní vyhledávání DNS pro přiřazení do-

ménového názvu adresy IP následované jedinou odchozí žádostí o připojení používající nejlepší zdrojovou adresu IP a rozhraní, jak je určeno ve směrovací tabulce.

Navíc zde není žádné „nastavení relace rozhraní NetBIOS“ na začátku připojení protokolu TCP, jako je u tradičního rozhraní NetBIOS pro TCP/IP: Dle výchozího nastavení přeměrovač umísťuje volání jak na zařízení typu NetBIOS, tak na zařízení SMB a souborový server přijímá volání od obou. Souborový server zařízení SMB naslouchá na portu TCP 445 místo na portu rozhraní NetBIOS pro TCP/IP 139.

Relace rozhraní NetBIOS pro TCP/IP

Relace NetBIOS jsou vytvářeny mezi dvěma názvy. Například, když služba pracovní stanice Windows 2000 vytvoří soubory sdílející připojení ke službě serveru Windows 2000 za pomoci rozhraní NetBIOS pro TCP/IP, události jdou po sobě takto:

1. Název typu NetBIOS pro proces serveru je přiřazen adresy IP.
2. Za použití portu TCP 139 je vytvořeno připojení protokolu TCP z pracovní stanice na server.
3. Pracovní stanice pošle žádost NetBIOS Session Request přes připojení protokolu TCP na název serveru. V případě, že server na tomto názvu naslouchá, potvrdí příjem a vytvoří se připojení.

Jakmile se vytvoří relace NetBIOS, klient a server vyjednávají o připojení sdílejícím soubory s protokolem SMB. Síť společnosti Microsoft používají mezi dvěma názvy v kterémkoli okamžiku pouze jednu relaci NetBIOS. Jakákoli další připojení sdílející soubory nebo tisk vytvořená po prvním připojení jsou znásobena nad stejnou relací NetBIOS.

Na každém připojení se používá aktivita rozhraní NetBIOS Keep-Alive, které ověřují, zda jsou server a pracovní stanice stále schopny udržovat relaci. Takto, pokud dojde k vypnutí pracovní stanice, může server eventuálně zlikvidovat připojení a připojené prostředky a naopak. Aktivita NetBIOS Keep-Alive je řízena záznamem **SessionKeepAlive** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Netbt\Parameters) a dle výchozího nastavení je to jednou za hodinu.

Při použití souboru Lmhosts může dojít ke špatnému zápisu záznamu, přičemž je možné snažit se o připojení k serveru pomocí správné adresy IP, ale nesprávného názvu. V takovém případě je připojení protokolu TCP k serveru stále realizováno. Nicméně žádost relace NetBIOS používající nesprávný název bude serverem odmítnuta. Při pokusu o připojení pomocí příkazu `net use` se vrátí hlášení „Error 51: Remote computer not listening“.

Datagramové služby rozhraní NetBIOS

Datagramy jsou odesílány z jednoho názvu NetBIOS na jiný přes port UDP 138. Datagramová služba poskytuje možnost posílat zprávy (hlášení) na jedinečný název nebo na skupinový název. Skupinové názvy se mohou překládat na seznam adres IP nebo na všesměrové vysílání. Například příkaz **net send /d:mydomain test** posílá datagram obsahující text „test“ na skupinový název MYDOMAIN[03]. Název MYDOMAIN[03] se překládá na všesměrové vysílání podsítě IP, takže datagram je odeslán s následujícími znaky:

- Cílová MAC adresa: Všesměrové vysílání na úrovni MAC (0xFF-FF-FF-FF-FF-FF).
- Zdrojová MAC adresa: MAC adresa lokálního počítače.
- Cílová adresa IP: Adresa všesměrového vysílání lokální podsítě.
- Zdrojová adresa IP: adresa IP lokálního počítače.

- Cílový název: MYDOMAIN[03] (služba SMB na vzdálených počítačích).
- Zdrojový název: USERNAME[03] (služba SMB na lokálním počítači).

Všichni hostitelé na podsíti si vyzvedávají datagramy a zpracovávají je minimálně pro protokol UDP. U hostitelů, kteří mají spuštěnou datagramovou službu NetBIOS, předává protokol UDP datagram rozhraní NetBIOS pro TCP/IP (NetBT) na port 138. Rozhraní NetBIOS pro TCP/IP (NetBT) zkontroluje cílový název, jestli je tento název registrován u některé aplikace. Pokud ano, postoupí datagram. Pokud ne, datagram vyřadí.

Uvedme, že pokud je rozhraní NetBIOS v operačním systému Windows 2000 zakázáno, vyřadí datagram protokol UDP.

Klientské služby a součásti

Tato kapitola je zaměřena na součásti jádra zásobníku protokolu TCP/IP v operačním systému Windows 2000, ne na mnoho dostupných služeb poskytovaných operačním systémem Windows 2000, které je používají. Nicméně zásobník samotný závisí na několika službách potřebných pro informace o konfiguraci a pro překlad názvu a adresy.

Automatická konfigurace klienta

Jednou z nejdůležitějších klientských služeb je klient protokolu DHCP (Dynamic Host Configuration Protocol). Klient používající protokol DHCP má ve Windows 2000 rozšířenou roli. Primárním novým rysem je schopnost konfigurovat adresy IP a masky podsítě, když je klient spuštěn na síti, kde není pro přidělování adres žádný server DHCP. Tato vlastnost umožňuje autokonfiguraci adresy IP a masky podsítě pro malé sítě, například pro domácí síť.

Pokud je klient používající protokol Microsoft TCP/IP nainstalován a nastaven tak, aby dynamicky přijímal informace o konfiguraci protokolu TCP/IP ze serveru DHCP, služby klienta protokolu DHCP se aktivují vždy po restartu počítače. Služba klienta protokolu DHCP nyní používá dvoustupňový postup konfigurace adresy IP a dalších konfiguračních informací klienta:

1. Když je klient nainstalován, snaží se lokalizovat server DHCP a zjistit konfiguraci adresy IP. Většina podnikových a organizačních sítí TCP/IP používá servery DHCP, které jsou nakonfigurovány tak, aby předávaly informace klientům na síti.
2. Selže-li u počítače na platformě Windows 2000 lokalizace serveru DHCP, klient protokolu DHCP sám nakonfiguruje protokol TCP/IP pomocí vybrané adresy IP ze sítě třídy B 169.254.0.0 s maskou podsítě 255.255.0.0 vyhrazené IANA (Internet Assigned Numbers Authority). Klient protokolu DHCP provede detekci duplikované adresy IP, aby se ujistil, že vybraná adresa IP již není používána. Pokud je tato adresa již používána, vybere jinou adresu IP a vybírá je až desetkrát. Poté, co klient protokolu DHCP vybere adresu, která není používána, nakonfiguruje pomocí této adresy rozhraní. Klient na pozadí kontroluje každých pět minut spojení se serverem DHCP; když ho najde, zamítne informace použité k autokonfiguraci a namísto nich použije informace nabídnuté serverem DHCP.

Vlastnost autokonfigurace protokolu Windows 2000 TCP/IP je známá jako *APIPA (Automatic Private IP Addressing)* a umožňuje uživatelům malých sítí (doma nebo v malé firmě) vytvoření funkční sítě TCP/IP na jedné podsíti bez nutnosti manuální konfigurace protokolu TCP/IP nebo nastavování serveru DHCP.

V případě, že klient DHCP již před tím obdržel zapůjčení adresy ze serveru DHCP, nastane tento upravený sled událostí:

1. Jestliže zapůjčení adresy klienta je v době spouštění stále platné (nevypršela dosud doba platnosti), klient se snaží zapůjčení se serverem DHCP obnovit. Pokud se klientovi nepodaří během obnovovacích snah lokalizovat server DHCP, snaží se pomocí nástroje Ping komunikovat s výchozí bránou uvedenou v zapůjčení. Je-li komunikace pomocí nástroje Ping úspěšná, pak klient protokolu DHCP předpokládá, že je stále umístěn na stejné síti, odkud obdržel své aktuální zapůjčení, a pokračuje v jeho používání. Dle výchozího nastavení se klient snaží obnovit své zapůjčení, když uplyne 50 procent jeho předděleného času zapůjčení.
2. Není-li snaha komunikovat s přednastavenou bránou pomocí utility Ping úspěšná, klient předpokládá, že se přesunul na síť, kde momentálně nejsou dostupné žádné služby protokolu DHCP (například domácí síť) a nakonfiguruje se sám, jak bylo uvedeno výše. Po autokonfiguraci se snaží každých pět minut lokalizovat server DHCP.

Rozpoznání média (Media Sense)

Protokol Windows 2000 TCP/IP podporuje rozpoznání média, které může zpříjemnit práci na cestách uživatelům přenosných zařízení. Podpora rozpoznání média, přidaná v NDIS 5.0, poskytuje síťovému adaptéru mechanismus pro vyrozumění zásobníku protokolu o připojení média a odpojení média. Protokol Windows 2000 TCP/IP využívá tato vyrozumění k pomoci při automatické konfiguraci.

Například v operačním systému Windows NT 4.0 neobdržel zásobník protokolu žádné vyrozumění o přesunu, když byl přenosný počítač umístěn a konfigurován pomocí serveru DHCP na podsíti Ethernet a pak bez restartu přesunut na jinou podsít. To znamenalo, že konfigurační parametry zastaraly a neodpovídaly novému segmentu sítě. Navíc, pokud byl počítač vypnut, odnesen domů a restartován, zásobník protokolu si nebyl vědom toho, že síťový adaptér už není připojen do sítě, a zastaralé parametry zůstaly v platnosti. To by mohlo působit problémy, například by podsíťové trasy, výchozí brány a další konfigurační parametry mohly kolidovat s parametry telefonního připojení.

Podpora rozpoznání média umožňuje zásobníku protokolu reagovat na události a odstraňovat zastaralé parametry. Například pokud počítač na platformě Windows 2000 odpojí od sítě (za předpokladu, že síťový adaptér podporuje rozpoznání média), za 20 sekund časového limitu protokol TCP/IP zruší platnost parametrů spojených se sítí, která byla odpojena. adresa IP (adresy) dále neumožní odesílání a všechny trasy spojené s rozhraním ztratí svou platnost.

Je-li aplikace navázána na soket, který používá adresu, jejíž platnost byla zrušena, měl by zvládnout danou situaci a úspěšně se obnovit, například se snažit použít jinou adresu IP systému nebo oznámit uživateli odpojení.

Dynamická aktualizace klienta DNS

Operační systém Windows 2000 obsahuje podporu dynamické aktualizaci rozhraní DNS, jak je popsána v dokumentu RFC 2136. Po každé adresové události, například nové adrese nebo obnovení adresy, pošle klient DHCP parametr (option) 81 a svůj plný doménový název serveru DHCP a požádá server DHCP o registraci záznamu PTR RR (prostředek-ukazatel). Dynamicky aktualizující klient registruje záznam prostředek-ad-

resa (A RR), protože pouze klient ví, které adresy IP na hostiteli se mapují na tento název. Server DHCP nemusí být schopný správně dokončit registraci A RR, protože má neúplné znalosti. Nicméně server DHCP může být nakonfigurován tak, že poskytne klientovi pokyny, které serveru umožní registrovat oba záznamy pomocí DNS. Změna záznamů v registru změní chování dynamicky se aktualizujícího klienta používajícího DNS.

Server DHCP pod Windows 2000 ovládá parametr 81, jak je specifikováno v dokumentu RFC 2136. Pokud klient používající protokol DHCP mluví se serverem DHCP, který tento parametr nepodporuje, registruje si PTR RR sám. Server Windows 2000 DNS je schopen dynamickou aktualizací zvládnout.

Statically konfigurovaní klienti (nepoužívající DHCP) registrují sami na serveru DNS jak A RR, tak PTR RR.

Jestliže se vzdáleně přistupující klient připojí k počítači na platformě Windows 2000, na kterém běží služba Routing and Remote Access, musí klient vykonat registraci DNS sám, protože vzdáleně přistupovaný server nezná název klienta. Jestliže linka vypadne, zapůjčení adresy vyprší, nebo klient neodregistruje své záznamy, vzdáleně přistupovaný server odregistruje záznam PTR za klienta.

Služba DNS Resolver Cache Service

Operační systém Windows 2000 obsahuje službu DNS Resolver Cache Service, která je dle výchozího nastavení povolena. Tuto službu lze za účelem řešení problémů prohlížet, zastavit a spustit jako kteroukoli další službu Windows 2000. Tato služba snižuje provoz na sítích DNS a urychluje některá rozhodnutí tím, že dotazům DNS poskytuje lokální mezipaměť překládání DNS.

Odpovědi na dotaz na název jsou ukládány v mezipaměti po TTL specifikovaný v odpovědi (nepřesahující hodnotu určenou v záznamu **MaxCacheEntryTtlLimit** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters)) a budoucí dotazy jsou, pokud je to možné, zodpovídaný z mezipaměti. Služba DNS Resolver Cache Service podporuje negativní ukládání v mezipaměti. Například je-li učiněn dotaz na DNS na určitý název hostitele a odpověď je negativní, následující dotazy na stejný název budou zodpovídaný (negativně) z mezipaměti po časové období rovné hodnotě v záznamu **NegativeCacheTime** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters) (přednastavená hodnota je 300 sekund). Dalším příkladem negativního ukládání do mezipaměti je situace, kdy všechny servery jsou dotazovány a žádný není dostupný, po časové období rovné hodnotě záznamu **NetFailureCacheTime** v registru (HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters). Všechny následující dotazy na názvy selžou ihned místo postupného vypršení časového limitu. Tato vlastnost šetří čas pro služby, které dotazují DNS během spouštěcího procesu, zvláště při spouštění klienta ze sítě.

Filtrování protokolu TCP/IP

Operační systém Windows 2000 zahrnuje podporu filtrování protokolu TCP/IP, vlastnost známou jako zabezpečení protokolu TCP/IP ve Windows NT 4.0. Filtrování protokolu TCP/IP umožňuje přesně specifikovat, které typy příchozího IP provozu jsou zpracovávány pro které IP rozhraní. Tato vlastnost je navržena tak, aby izolovala provoz zpracováváný Internetovými a intranetovými servery v případě nepřítomnosti dalšího filtrování protokolu TCP/IP poskytovaného službou Routing and Remote Access

nebo dalšími aplikacemi nebo službami protokolu TCP/IP. Filtrování protokolu TCP/IP je dle výchozího nastavení zakázáno.

Filtrování protokolu TCP/IP může být povoleno a zakázáno pro všechny adaptéry prostřednictvím jednoho zaškrtačacího políčka. To může pomoci při řešení problémů s připojením, které mohou být spojeny s filtrováním. Filtry, které jsou příliš restriktivní, nemusí povolit očekávané způsoby připojení. Například, pokud specifikujete seznam portů UDP a nezahrnete do něj port UDP 520, váš počítač nepřijme oznámení protokolu RIP. To může poškodit schopnost počítače být směrovačem RIP nebo tichý hostitel protokolu RIP při využívání služby RIP Listener Service.

Paket je přijat ke zpracování, pokud splňuje jednu z následujících podmínek:

- Cílový port protokolu TCP souhlasí se seznamem portů TCP. Dle výchozího nastavení jsou všechny porty TCP povoleny.
- Cílový port protokolu UDP souhlasí se seznamem portů UDP. Dle výchozího nastavení jsou všechny porty UDP povoleny.
- Protokol IP souhlasí se seznamem protokolů IP. Dle výchozího nastavení jsou všechny protokoly IP povoleny.
- Je to paket protokolu ICMP.

Nemůžete filtrovat provoz protokolu ICMP pomocí filtrování protokolu TCP/IP. Pokud potřebujete filtrování protokolu ICMP, nakonfigurujte filtry pro IP pakety prostřednictvím služby Routing and Remote Access. Více podrobností najdete v části „Jednosměrné IP směrování“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Další informace

Více informací o protokolu TCP/IP najdete v těchto knihách:

- *Internetworking with TCP/IP*, Vol 1, 3rd Edition by Douglas Comer, 1996, Englewood Cliffs, NJ: Prentice Hall.
- *Microsoft Windows 2000 TCP/IP Protocols and Services Technical Reference* by Thomas Lee and Joseph Davies, 1999, Redmond, WA: Microsoft Press.
- *TCP/IP Illustrated*, Volume 1, The Protocols by Richard W. Stevens, 1994, Reading, MA: Addison-Wesley.
- *Improving Round Trip Time Estimates in Reliable Transport Protocols*, by P. Karn & C. Partridge, Aug. 1987, ACM SIGCOMM-87.
- *Congestion Avoidance and Control*, V. Jacobson, Aug. 1988, ACM SIGCOMM-88.

3. KAPITOLA

Řešení problémů protokolu TCP/IP



V operačních systémech Microsoft® Windows® 2000 Server a Microsoft® Windows® 2000 Professional je dostupných mnoho nástrojů pro řešení síťových problémů. Tato kapitola pojednává o nejobvyklejších a nejužitečnějších nástrojích obsažených v operačním systému nebo v sadě *Windows 2000 Resource Kit*.

Řešení problémů vrstvu po vrstvě je často dobrá metoda rychlé izolace problémů. Umožňuje rozlišovat problémy na lokálním hostiteli, vzdáleném hostiteli nebo na směrovači. Úlohy řešení problémů, o kterých se zde bude hovořit, jsou seříděny právě tímto vrstevným způsobem.

V této kapitole najdete:

Přehled nástrojů pro řešení problémů protokolu TCP/IP 104

Přehled řešení problémů 126

Nelze dosáhnout adresy IP 137

Řešení problémů směrování IP 145

Služby pro řešení problémů 150

Související informace v sadě Resource Kit

- Více podrobností o protokolu TCP/IP najdete v této knize v části „Úvod do TCP/IP“ a v části „Windows 2000 TCP/IP“.

Přehled nástrojů pro řešení problémů protokolu TCP/IP

V tabulce 3.1 najdete seznam diagnostických nástrojů obsažených v protokolu Microsoft TCP/IP, které jsou podrobněji popsány na následujících stranách. Všechny jsou při identifikaci a řešení síťových problémů protokolu TCP/IP užitečné.

Tabulka 3.1 Diagnostické utility protokolu TCP/IP

Nástroj	Použití
Arp	Prohlížení mezipaměti ARP na rozhraní lokálního počítače pro vyhledání chybných záznamů.
Hostname	Zobrazení názvu hostitele.
Ipconfig	Zobrazení hodnot aktuální síťové konfigurace protokolu TCP/IP a aktualizace nebo uvolnění zapůjčení alokovaných protokolem DHCP a zobrazení, registrace nebo vyprázdnění názvů systému DNS.
Nbtstat	Kontrola stavu aktuálních připojení rozhraní NetBIOS pro protokol TCP/IP, aktualizace mezipaměti názvů pro NetBIOS a určení registrovaných názvů a Scope ID.
Netstat	Zobrazení statistik aktuálních připojení protokolu TCP/IP.
Netdiag	Kontrola všech aspektů síťového připojení.
Nslookup	Kontrola záznamů, doménových aliasů hostitelů, služeb hostitelů domény a informací o operačním systému pomocí dotazů na názvové servery domén Internetu. Podrobnosti o nástroji Nslookup najdete v této knize části „Služba Windows 2000 DNS“.
Pathping	Sledování cesty ke vzdálenému systému a hlášení ztrát paketů na každém směrovači po cestě.
Ping	Odesílání požadavků ICMP Echo Request pro ověření toho, že protokol TCP/IP je správně nakonfigurován a vzdálený systém s protokolem TCP/IP je dostupný.
Route	Zobrazení směrovací tabulky IP a přidávání nebo odstraňování tras IP.
Tracert	Sledování cesty ke vzdálenému systému.

Stručný odkazový graf těchto nástrojů protokolu TCP/IP, stejně jako vzdálených administrátorských nástrojů najdete v příloze této knihy „Vzdálené nástroje protokolu TCP/IP“.

Kromě nástrojů specifických pro protokol TCP/IP vám při řešení problémů protokolu TCP/IP mohou pomoci také tyto nástroje operačního systému Microsoft® Windows® 2000:

- Služba Microsoft SNMP Service – poskytuje statistické informace systémům správy SNMP.
- Event Viewer – sleduje chyby a události.
- Microsoft Network Monitor – provádí hloubkové sledování sítě. Plná verze je součástí produktu Microsoft® Systems Management Server a omezená verze je obsažena v produktu Windows 2000 Server.
- System Monitor – analyzuje výkon sítě TCP/IP.
- Editor registru – jak Regedit.exe, tak Regedt32.exe umožňují prohlížení a editaci parametrů registru.

Těmto nástrojům jsou v sadě Windows 2000 Resource Kit věnovány samostatné kapitoly.

Arp

Arp umožňuje prohlížení a upravovat mezipaměť ARP. Jestliže se dva hostitelé na stejné podsíti spolu nemohou úspěšně spojit pomocí nástroje Ping, zkuste na obou počítačích spustit příkaz **arp -a** a zkontrolujte s jeho pomocí, zda mají oba počítače navzájem zapsané správné MAC adresy. Správnou MAC adresu hostitele určíte pomocí příkazu Ipconfig.

Arp lze také použít k prohlížení obsahu mezipaměti ARP, a to z příkazové řádky pomocí příkazu **arp -a**. Tento příkaz zobrazí seznam záznamů mezipaměti ARP včetně jejich MAC adres. Zde je příklad seznamu záznamů mezipaměti ARP:

```
C:\>arp -a
```

```
Interface: 172.16.0.142 on Interface 0x2
```

Internet address	Physical Address	Type
172.16.0.1	00-e0-34-c0-a1-40	dynamic
172.16.1.231	00-00-f8-03-6d-65	dynamic
172.16.3.34	08-00-09-dc-82-4a	dynamic
172.16.4.53	00-c0-4f-79-49-2b	dynamic
172.16.5.102	00-00-f8-03-6c-30	dynamic

Jestliže na síti existuje další hostitel se stejnou adresou IP, může mezipaměť ARP MAC adresu počítače přiřadit tomuto hostiteli, což může mít za následek občasné problémy s překladem adres. Když počítač na lokální síti pošle požadavek ARP Request na zjištění adresy, předá jeho data MAC adrese odpovídající první odpovědi ARP Reply, kterou obdrží. Program **arp** může pomoci udržováním seznamu, přidáváním a odebíráním relevantních záznamů.

Pro odstraňování nesprávných záznamů můžete použít příkaz **arp -d** <adresa IP>. Nové statické záznamy přidáte pomocí příkazu **arp -s** <MAC adresa> (kde MAC adresa je ve formátu šestnáctkových bajtů oddělených pomlčkou). Tyto statické záznamy se po vypršení časového limitu z mezipaměti automaticky neodstraňují, nicméně mizí při restartu. Chcete-li, aby statické záznamy v mezipaměti ARP zůstaly i po restaru, musíte vytvořit dávkový soubor spouštěný ze skupiny Po spuštění.

Všechny záznamy ARP pro síťové rozhraní specifikované pomocí kritéria <adresa IP> seřadíte do seznamu pomocí příkazu **arp -N** <adresa IP>. V tabulce 3.2 jsou obsaženy všechny přepínače Arp.

Tabulka 3.2 Přepínače Arp

Přepínač	Název	Účinek
-d <adresa IP>	Delete	Odebírá záznam ze seznamu v mezipaměti ARP
-s <MAC adresa>	Static	Přidává statický záznam do mezipaměti ARP
-N <rozhraní adresy IP>	Interface	Sestavuje seznam všech záznamů mezipaměti ARP pro určené rozhraní
-a	Display	Zobrazuje všechny aktuální záznamy ARP všech rozhraní
-g rozhraní	Display	Zobrazuje všechny aktuální záznamy ARP všech rozhraní

Hostname

Hostname zobrazuje název hostitele, na nějž se příkaz vztahuje. Tento příkaz nemá žádné přepínače nebo parametry. Zobrazený název hostitele odpovídá názvu v kartě Identifikace v síti v **Ovládací panely – Systém**.

Ipsconfig

IPConfig je nástroj příkazového řádku, který zobrazuje aktuální konfiguraci zásobníku protokolu IP instalovaného na počítači v síti.

Při použití s přepínačem **/all** zobrazuje detailní zprávu o konfiguraci všech rozhraní, včetně jakýchkoli konfigurovaných miniportů typu WAN (zpravidla používány pro vzdálený přístup nebo připojení VPN). Výstup může být přesměrován do souboru a vkládán do jiných dokumentů. Zpráva může vypadat například takto:

```
C:>\ipconfig /all
```

```
Windows 2000 IP Configuration
```

```
Host Name . . . . . : TESTPC1
Primary DNS Suffix . . . . . : reskit.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ntcordc1.reskit.com
                                dns.reskit.com
                                reskit.com
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . : dns.reskit.com
Description . . . . . : Acme XL 10/100Mb Ethernet NIC
Physical Address. . . . . : 00-CC-44-79-C3-AA
DHCP Enabled. . . . . : Yes
IP Address. . . . . : 172.16.245.111
Subnet Mask . . . . . : 255.255.248.0
Default Gateway . . . . . : 172.16.240.1
DHCP Server . . . . . : 172.16.248.8
```

```

DNS Servers . . . . . : 172.16.55.85
                        172.16.55.134
                        172.16.55.54

Primary WINS Server . . . . . : 172.16.248.10
Secondary WINS Server . . . . . : 172.16.248.9

Lease Obtained. . . . . : Friday, May 05, 1999 2:21:40 PM
Lease Expires . . . . . : Monday, May 07, 1999 2:21:40 PM

```

V řadě dalších užitečných parametrů nástroje Ipconfig najdete například /flushdns, který maže mezipaměť názvů DNS; /registerdns, který obnovuje všechny zápůjčky serveru DHCP a registruje názvy DNS; /displaydns, který zobrazuje obsah mezipaměti překladače služby DNS.

Možnosti /release <adapter> a /renew <adapter> uvolňují a obnovují adresu IP alokovanou serverem DHCP pro specifický adaptér. Není-li specifikován název žádného adaptéru, jsou pro všechny adaptéry navázané na protokol TCP/IP uvolněny nebo obnoveny zápůjčky DHCP.

U příkazu /setclassid není-li specifikováno žádné třídivé ID, je odebráno. V tabulce 3.3 jsou obsaženy všechny přepínače Ipconfig.

Tabulka 3.3 Přepínače nástroje Ipconfig

Přepínač	Účinek
/all	Vytváří podrobnou zprávu o konfiguraci všech rozhraní.
/flushdns	Odebírá všechny záznamy z mezipaměti názvů DNS.
/registerdns	Obnovuje všechny zápůjčky DHCP a opětovně registruje názvy DNS.
/displaydns	Zobrazí obsah mezipaměti překladače služby DNS.
/release <adaptér>	Uvolní adresu IP pro specifikované rozhraní.
/renew <adaptér>	Obnoví adresu IP pro specifikované rozhraní.
/showclassid <adaptér>	Zobrazí všechna ID tříd DHCP povolená pro specifikovaný adaptér.
/setclassid <adaptér> <třídivé ID k nastavení>	Změní ID tříd DHCP specifikovaného adaptéru.
/?	Zobrazí tento seznam.

Možnosti /showclassid a /setclassid umožňují práci s třídivými ID uživatele z příkazové řádky. Třídivá ID uživatele jsou možnosti (options), které může systémový administrátor nastavit na serveru DHCP, aby nakonfiguroval klientský počítač tak, aby se serveru sám identifikoval. Použitím příkazu **ipconfig /showclassid <adaptér>** se pošle dotaz na server klienta. Tento server odpoví poskytnutím dostupných tříd. Jakmile víte, které třídy jsou dostupné, můžete použít příkaz **ipconfig /setdhcpclassid <adaptér> <třídivé ID pro nastavení na server>**, kterým nastavíte třídivé ID, které od tohoto

okamžiku bude klient používat. Více podrobností o protokolu DHCP a třídivých ID najdete v této knize v části „Protokol DHCP“.

Nbtstat

Nástroj Nbtstat je navržen tak, aby pomáhal s řešením problémů s překladem názvů pro NetBIOS. Když síť funguje normálně, názvy pro NetBIOS adresám IP překládá NetBIOS pro TCP/IP (NetBT). Existuje několik možností, jak název pro NetBIOS přeložit, včetně vyhledávání v lokální mezipaměti, dotazu na server WINS, všesměrového vysílání, vyhledání pomocí LMHOSTS, vyhledání pomocí Hosts a dotazu na server DNS.

Příkaz **nbtstat** odebírá a opravuje přednahráné záznamy za použití řady přepínačů rozlišujících velká a malá písmena. Příkaz **nbtstat -a <název>** provádí stavový příkaz adaptéru NetBIOS na počítači určeném kritériem <název>. Výsledkem stavového příkazu adaptéru je tabulka lokálních názvů pro NetBIOS pro daný počítač, stejně jako MAC adresa karty adaptéru. Příkaz **nbtstat -A <adresa IP>** provádí stejnou funkci za použití cílové adresy IP místo názvu.

Možnost **nbtstat -c** zobrazí obsah mezipaměti názvů pro NetBIOS, který zahrnuje mapování názvů pro NetBIOS na adresy IP.

nbtstat -n zobrazí název, který je registrován lokálně na systému aplikacemi NetBIOS, například serverem nebo přesměrovačem.

Příkaz **nbtstat -r** zobrazí celkový počet názvů pro NetBIOS zjištěných pomocí všesměrového vysílání a pomocí dotazů na server WINS. Příkaz **nbtstat -R** vyčistí mezipaměť názvů a znovu nahraje záznamy #PRE ze souboru LMHOSTS. Záznamy #PRE jsou záznamy názvů souboru LMHOSTS, které jsou přednahráné do mezipaměti. Více podrobností o souboru LMHOSTS najdete v příloze této knihy „LMHOSTS“.

Nbtstat -RR posílá pakety s uvolněním názvů na server WINS a spouští obnovení, čímž se opětovně zaregistrují všechny názvy serveru názvů bez nutnosti restartu. Toto je nová možnost u operačního systému Windows NT 4.0 se Service Pack 4 a u Windows 2000.

Příkaz **nbtstat -S** lze použít k vypsání seznamu aktuálních relací rozhraní NetBIOS a jejich stavu, včetně statistik. Výstup může vypadat například takto:

```
C:\>nbtstat -S
```

```
Local Area Connection:
```

```
Node IpAddress: [172.16.0.142]           Scope Id: []
```

NetBIOS Connection Table

Local Name	State	In/Out	Remote Host	Input	Output
TESTPC1 <00>	Connected	Out	172.16.210.25	6MB	5MB
TESTPC1 <00>	Connected	Out	172.16.3.1	108KB	116KB
TESTPC1 <00>	Connected	Out	172.16.3.20	299KB	19KB
TESTPC1 <00>	Connected	Out	172.16.3.4	324KB	19KB
TESTPC1 <03>	Listening				

A konečně příkaz **nbtstat -s** poskytuje podobnou sadu výpisu relací, ale místo adres IP vzdálených počítačů uvádí jejich názvy.

Poznámka Možnosti příkazu Nbtstat rozlišují velká a malá písmena.

Přepínače Nbtstat najdete v tabulce 3.4.

Tabulka 3.4 Přepínače Nbtstat

Přepínač	Název	Funkce
-a <název>	Adapter status	Vrací tabulku názvů pro NetBIOS a MAC adresu adresové karty daného názvu počítače.
-A <adresa IP>		Adapter status Vypíše stejné informace jako možnost -a, pokud je zadána adresa IP cíle.
-c	cache	Vypíše obsah mezipaměti názvů pro NetBIOS.
[Number]	Interval	Zapsáním číselné hodnoty sdělíte příkazu Nbtstat, v jakém intervalu v sekundách má znovu zobrazit vybrané statistiky s mezerami mezi jednotlivými zobrazeními. Tento cyklus zastavíte stiskem kláves Ctrl+C.
-a	names	Zobrazí názvy registrované lokálně aplikacemi NetBIOS, například serverem a přesměrovačem.
-r	resolved	Zobrazí celkový počet názvů přeložených pomocí všesměrového vysílání a serveru WINS.
-R	Reload	Vyčistí mezipaměť názvů a znovu nahraje všechny záznamy #PRE ze souboru LMHOSTS.
-RR	ReleaseRefresh	Uvolní a znovu u serveru názvů zaregistruje všechny názvy.
-s	sessions	Vypíše seznam relací rozhraní NetBIOS, přičemž zamění cílovou adresu IP na název počítače pro NetBIOS.
-S	Sessions	Vypíše seznam aktuálních relací NetBIOS a jejich stav, včetně adresy IP.
/?	Help	Zobrazí tento seznam.

Netdiag

Netdiag je nástroj, která pomáhá izolovat síťové problémy a problémy s připojením pomocí série testů, v nichž určí stav síťového klienta a jestli je funkční. Tyto testy a klíčové informace o stavu sítě, které zobrazuje, poskytují síťovému administrátorovi a pracovníkům podpory pevnější základ při identifikaci a izolaci síťových problémů. Navíc, vzhledem k tomu, že tento nástroj nepožaduje specifikaci parametrů nebo přepínačů, mohou se síťoví administrátoři a pracovníci podpory soustředit spíše na analýzu výstupů než na poučování uživatelů, jak s tímto nástrojem zacházet.

Nástroj Netdiag diagnostikuje síťové problémy prostřednictvím kontroly všech aspektů síťové konfigurace a připojení hostitelského počítače. Navíc kromě řešení problémů protokolu TCP/IP také na hostitelském počítači prozkoumává konfiguraci IPX (Inter-network Packe Exchange) a NetWare.

Nástroj Netdiag spusíte, kdykoli budou na počítači síťové problémy. Tato nástroj se snaží diagnostikovat problém a může dokonce problémové oblasti označit pro bližší prohlédnutí. Jednoduché problémy s rozhraním DNS může sama vyřešit pomocí přepínače **/fix**.

Více podrobností o utilitě Netdiag najdete ve Windows 2000 Support Tools Help. Informace o instalaci a používání Windows 2000 Support Tools a Support Tools Help najdete v souboru Sreadme.doc v adresáři \Support\Tools na CD operačního systému Windows 2000.

Netdiag provádí své testy prozkoumáváním souborů .dll, výstupů ostatních nástrojů a registru systému, aby našel místa potenciálních problémů. Kontroluje, které síťové služby a funkce jsou povoleny, a pak spouští testy konfigurace sítě uvedené v tabulce 3.5 v uvedeném pořadí. Jestliže na počítači některá s uvedených služeb neběží, test je přeskočen.

Tabulka 3.5 Testy nástroje Netdiag

Název testu	Funkce	Podrobnosti
NDIS	Stav síťového adaptéru	Vypíše podrobnosti konfigurace síťového adaptéru, včetně názvu adaptéru, konfigurace, média, GUID a statistiky. Jestliže tento test prokáže nereagující síťový adaptér, zbývající testy se zruší.
IPConfig	Konfigurace protokolu IP	Tento test poskytuje většinu informací o protokolu TCP/IP normálně získávaných příkazem ipconfig/all, pomocí utility Ping komunikuje se servery DHCP a WINS a kontroluje, že přednastavená brána je na stejné podsíti jako adresa IP.
Member	Členství v doméně	Kontroluje a potvrzuje podrobnosti primární domény, včetně role počítače, názvu domény a GUID domény. Kontroluje, zda je spuštěná služba NetLogon, přidává primární doménu do seznamu domén a dotazuje se na primární SID.
NetBTTransports	Test transportů	Vypíše transporty NetBT spravované přesměrovačem. Nenajde-li žádné transporty NetBT, vytiskne informace o chybách.
APIPA (Automatic Private IP Addressing)	Adresa APIPA	Kontroluje, jestli některé rozhraní používá službu APIPA.
IPLoopBk	Zpětná smyčka IP pomocí utility Ping	Pomocí utility Ping provádí zpětnou smyčku na adresu IP 127.0.0.1.
DefGw	Výchozí brána	Pomocí utility Ping se připojí na všechny výchozí brány každého rozhraní.
NbtNm	Test názvů pro NetBIOS pro TCP/IP (NetBT)	Podobný příkazu nbtstat -n. Kontroluje, že název služby workstation <00> je roven názvu počítače. Kontroluje také, že název služby Messenger <03> a název služby serveru <20> existují na všech rozhraních a že si nekolidují.
WINS	Test služby WINS	Posílá dotazy na název pro NetBIOS pro TCP/IP (NetBT) na všechny konfigurované servery WINS.
Winsock	Test Winsock	Používá funkci Windows Sockets WSAEnumProtocols (), pomocí které získává dostupné transportní protokoly.
DNS	Test rozhraní DNS	Kontroluje, jestli běží služby mezipaměti DNS a jestli je tento počítač správně registrován na konfigurovaných serverech DNS. Jestliže je počítač řadičem domény, test rozhraní DNS kontroluje, zda jsou všechny záznamy DNS v souboru Netlogon.dns registrovány na serveru DNS. Pokud jsou záznamy nesprávné a možnost /fix je zapnutá, zkuste opětovně registrovat záznam řadiče domény na serveru DNS.

Tabulka 3.5 Testy nástroje Netdiag (pokračování)

Název testu	Funkce	Podrobnosti
Browser	Test přesměrovače a prohlížeče	Kontroluje, jestli je služba pracovní stanice spuštěna. Z přesměrovače a prohlížeče získává seznam transportů. Kontroluje, jestli jsou transporty NetBIOS pro TCP/IP (NetBT) na seznamu testu transportů NetBT. Kontroluje, jestli je prohlížeč navázán na všechny transporty NetBT. Kontroluje, jestli může počítač posílat zprávy z poštovní příhrádky. testy probíhají jak na prohlížeči, tak na přesměrovači.
DsGetDc	Test zpřístupnění DC	Nejprve z adresářové služby najde libovolný řadič domény, pak najde primární řadič domény. Potom najde řadič domény Windows 2000 (DC). Je-li testovaná doména primární doménou, kontroluje, jestli je GUID domény uložené v LSA stejné jako GUID domény uložené v DC. Pokud není stejné, test ukáže fatální chybu. Je-li zapnuta možnost /fix, DsGetDC se snaží GUID v LSA opravit.
DcList	Test seznamu DC	Od adresářových služeb na aktivním řadiči domény (DC) získává seznam řadičů domény v doméně. Pokud pro dotčenou doménu nejsou žádné informace o řadičích domény, snaží se získat DC od DS (podobně jako test DsGetDc). Snaží se získat aktivní DC jako cílový DC. Získává seznam DC z cílového DC. Kontroluje stav každého DC. Přidává všechny řadiče domény do seznamu řadičů testované domény. Jestliže výše uvedené sekvence zklame, používá k získání DC prohlížeč. Kontroluje stav všech řadičů domény a přidává je do seznamu řadičů domény. jestliže je možnost položky DcAccountEnum v registru povolena, Netdiag se snaží získat seznam řadičů domény ze Správce zabezpečení účtů zkoumaného počítače.
Trust	Test vztahů důvěryhodnosti	Testuje vztahy důvěryhodnosti k primární doméně pouze v případě, že je počítač členskou pracovní stanicí, členským serverem nebo řadičem domény Backup Domain Controller, který není emulátorem PDC. Kontroluje, že všechny identifikátory bezpečnosti primární domény (SID) jsou správné. Kontaktuje aktivní řadič domény. Připojuje se k serveru SAM na řadiči domény. K otevření domény používá SID domény, aby ověřil, že SID domény je správné. Dotazuje se na informace bezpečnostního kanálu primární domény. Jestliže je počítač BDCDC, přepojí se na emulátor PDC. jestliže je počítač členská pracovní stanice nebo server, ustaví pro každý řadič domény na seznamu řadičů této domény bezpečný kanál.
Kerberos	Test protokolů Kerberos	Testuje protokoly Kerberos pouze v případě, že počítač je členským počítačem nebo řadičem domény a uživatel není přihlášen na lokální účet. testuje protokoly Kerberos pouze v případě, že uživatel je přihlášený na účet domény Windows 2000. Připojuje se k LSA a vyhledává balíček Kerberos. Získává lístkovou mezipaměť balíčku Kerberos. Kontroluje, jestli balíček Kerberos má lístek primární domény a lokálního počítače.

Tabulka 3.5 Testy nástroje Netdiag (pokračování)

Název testu	Funkce	Podrobnosti
LDAP	Test LDAP	Tento test náležející vždy jedné doméně je spuštěn pouze v případě, že na řadiči domény běží DS. Počítač musí být členský počítač nebo řadič domény. NetDiag testuje LDAP na všech aktivních řadičích domény nalezených v doméně. Vytváří blok připojení LDAP k řadiči domény, potom provádí běžné hledání v adresáři LDAP se třemi typy autentifikace: „neautentifikovaný“, NTLM a „Vyjednávat“. Jestliže je zapnutá možnost /v (vypisovat), test LDAP vytiskne podrobnosti každého obdrženého záznamu.
Route	Test trasy	Zobrazí statické a trvalé záznamy ve směrovací tabulce, včetně cílové adresy, masky podsítě, adresy brány, rozhraní a metriky.
NetStat	Test NetStat	Podobný nástroji NetStat. Zobrazí statistiky protokolů a aktuálních síťových připojení protokolu TCP/IP.
Bindings	Test vazeb	Vyoiše seznam všech vazeb, včetně názvu rozhraní, názvu dolního modulu, názvu horního modulu, jestli jsou vazby aktuálně povoleny a vlastníka vazby.
WAN	Test WAN	Zobrazí nastavení a stav aktuálních aktivních připojení vzdáleného přístupu.
Modem	Test modemu	Získá všechna dostupná linková zařízení. Zobrazí konfiguraci každého linkového zařízení.
NetWare	Test NetWare	Určí, jestli NetWare používá adresářový strom nebo vazební postup pro přihlášení, určí přednastavený kontext, jestliže Netware používá stromový postup přihlášení a vyhledá server, ke kterému se hostitel při spuštění připojí.
IPX	Test IPX	Zkoumá konfiguraci IPX sítě, včetně typu rámce, ID sítě, MTU směrovače a jestli je povoleno shlukování paketů (burst) nebo zdrojové směrování.
IPSec	Test bezpečnosti protokolu IP	testuje, jestli je povolena bezpečnost protokolu IP a zobrazí seznam aktivních zásad bezpečnosti IP.

Syntaxe nástroje Netdiag

Syntaxe požadovaná pro Netdiag je jednoduchá. Nástroj lze nakonfigurovat tak, aby prováděl jakoukoli podmnožinu svého vyčerpávajícího seznamu testů pomocí pečlivého použití možností **/test** nebo **/skip**.

Ačkoli není nutno specifikovat žádné parametry nebo syntaxi, je pro Netdiag dostupných několik možností, především ke zvýšení či snížení úrovně podrobností ve zprávě. Tyto přepínače jsou obsaženy v tabulce 3.6. Úplné podrobnosti možností **/test** a **/skip** lze najít pomocí příkazu **netdiag /?** na příkazovém řádku, čímž získáte úplný seznam více než 20 testů, které lze použít jednotlivě nebo úplně přeskočit.

Tabulka 3.6 Přepínače nástroje Netdiag

Přepínač	Název	Funkce
/q	Tichý výstup	Vypíše pouze testy, které vrátí chyby.
/v	Rozepsaný výstup	Rozšířený seznam dat získaných z testování
/l	Protokolový výstup	Ukládá výstupy v aktuálním adresáři do souboru NetDiag.log.
/debug	Nejširší výstup	Úplný seznam dat získaných z testování s uvedenými příčinami úspěchu nebo neúspěchu
/d:<název domény>	Hledání řadiče domény	Ve specifikované doméně vyhledá řadič domény.
/fix	Odstranění problémů DNS	Porovnává hodnoty DNS se souborem hosts.
/DcAccountEnum	Vyjmenuje řadiče domén	Vyjmenuje počítačové účty řadiče domény
/test:<název testu>	Jednotlivý test	Spustí pouze test specifikovaný kritériem <název testu>. Úplný seznam získáte pomocí příkazu netdiag /?.
/skip:<název testu>		Přeskočení testu Přeskočí vyjmenovaný test.

Obecně řečeno Netdiag volá Ipconfig a vrací strukturu, která obsahuje většinu obecných informací vypsaných pomocí příkazu **ipconfig /all**. Tyto informace sbírá z registru a voláním různých ovladačů.

Netdiag vypíše řetězec [FATAL], když detekuje okolnost, kterou je třeba ihned odstranit. Naproti tomu řetězec [WARNING] signalizuje vadnou podmínku, která nemusí být odstraněna neprodleně.

Netstat

Nástroj Netstat zobrazuje statistiky protokolů a aktuální připojení protokolu TCP/IP. Napíšete-li na příkazové řádce **Netstat -a**, zobrazí se všechna připojení a naslouchající porty. Obsah směrovací tabulky a všechny trvalé trasy zobrazíte pomocí příkazu **netstat -r**. Přepínačem **-n** zakážete nástroji Netstat převádění adres a čísel portů na názvy, což urychlí jeho provádění. Možnost **netstat -s** zobrazí statistiky všech protokolů. Možnost **netstat -p <protokol>** lze použít ke zobrazení statistik určitého protokolu nebo dohromady s možností **-s** ke zobrazení připojení pouze určitého protokolu. Přepínač **-e** zobrazí statistiky rozhraní. Výstup příkazu **netstat -e** může vypadat například takto:

```
C:\>netstat -e
Interface Statistics
```

	Received	Sent
Bytes	372959625	123567086
Unicast packets	134302	145204
Non-unicast packets	55937	886
Discards	0	0
Errors	0	0
Unknown protocols	1757381	

Přijaté pakety, které obsahují chyby nebo je nelze zpracovat, jsou vyřazeny. Chyby označují pakety, které jsou poškozené, včetně paketů poslaných lokálním počítačem, které byly poškozeny ve vyrovnávací paměti.

Oba tyto typy chyb by měly být na nule nebo blízko nuly. Pokud ne, chyby ve sloupci Odesláno naznačují, že lokální síť může být přetížena nebo že mezi lokálním hostitelem a sítí může být špatné fyzické spojení. Velký počet chyb a vyřazených paketů značí přetíženou lokální síť, přetíženého lokálního hostitele nebo fyzický problém sítě.

Zpráva vyvolaná příkazem **netstat -a -n** může vypadat například takto:

```
C:\>netstat -a -n
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:42	0.0.0.0:0	LISTENING
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1038	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1041	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1048	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1723	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING
TCP	10.99.99.1:53	0.0.0.0:0	LISTENING
TCP	10.99.99.1:139	0.0.0.0:0	LISTENING
TCP	10.99.99.1:389	10.99.99.1:1092	ESTABLISHED
TCP	10.99.99.1:1092	10.99.99.1:389	ESTABLISHED
TCP	10.99.99.1:3604	10.99.99.1:135	TIME_WAIT
TCP	10.99.99.1:3605	10.99.99.1:1077	TIME_WAIT
UDP	0.0.0.0:135	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:1087	*:*	
UDP	10.99.99.1:53	*:*	
UDP	10.99.99.1:137	*:*	
UDP	10.99.99.1:138	*:*	

Číslo za sloupcem označuje, jaké číslo port používá to které připojení. Úplný seznam portů s odkazy najdete v příloze této knihy „Přiřazení portů TCP a UDP“.

Následující výstup ukazuje statistiky pro protokoly TCP, IP, ICMP a UDP na lokálním hostiteli.

```
D:\>netstat -s
```

IP Statistics

Packets Received	= 3175996
Received Header Errors	= 0
Received Address Errors	= 38054
Datagrams Forwarded	= 0
Unknown Protocols Received	= 0
Received Packets Discarded	= 0
Received Packets Delivered	= 3142564

Output Requests	= 3523906
Routing Discards	= 0
Discarded Output Packets	= 0
Output Packet No Route	= 0
Reassembly Required	= 0
Reassembly Successful	= 0
Reassembly Failures	= 0
Datagrams Successfully Fragmented	= 0
Datagrams Failing Fragmentation	= 0
Fragments Created	= 0

ICMP Statistics

	Received	Sent
Messages	462	33
Errors	0	0
Destination Unreachable	392	4
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenchs	0	0
Redirects	0	0
Echos	1	22
Echo Replies	12	1
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0

TCP Statistics

Active Opens	= 12164
Passive Opens	= 12
Failed Connection Attempts	= 79
Reset Connections	= 11923
Current Connections	= 1
Segments Received	= 2970519
Segments Sent	= 3505992
Segments Retransmitted	= 18

UDP Statistics

Datagrams Received	= 155620
No Ports	= 16578
Receive Errors	= 0
Datagrams Sent	= 17822

Tabulka 3.7 obsahuje přehled přepínačů dostupných v nástroji Netstat.

Tabulka 3.7 Přepínače nástroje Netstat

Přepínač	Funkce
-a	Zobrazí všechna připojení a naslouchající porty.
-r	Zobrazí obsah směrovací tabulky.
-a	Urychlí provádění operací zakázáním převádění adres a čísel portů na názvy.
-s	Zobrazí statistiky pro každý protokol (protokol IP, ICMP, TCP a UDP).
-p <protokol>	Zobrazí informace o připojení specifikovaného protokolu, přičemž se může jednat o protokol TCP, UDP, IP nebo ICMP.
-e	Zobrazí statistiky Ethernetu a lze kombinovat s -s.
interval	Zobrazí novou sadu statistik v zadaném intervalu (v sekundách). Opětovné zobrazování těchto statistik můžete zastavit pomocí CTRL-C. Bez určení intervalu se statistiky zobrazí jednou.

Nslookup

Nslookup je užitečný nástroj pro řešení problémů rozhraní DNS, například překladu názvu hostitele. Po spuštění nástroj Nslookup ukazuje název hostitele a adresu IP serveru DNS, který je nakonfigurován pro lokální systém, a zobrazí také příkazovou řádku pro další dotazy. Napíšete-li otazník (?), zobrazí se všechny dostupné příkazy. program opustíte zapsáním příkazu **exit**.

Pro vyhledání adresy IP hostitele používající rozhraní DNS napište název hostitele a stiskněte Enter. Nástroj Nslookup dle výchozího nastavení používá server DNS nakonfigurovaný pro počítač, na kterém je tento nástroj spuštěn, ale můžete ho zaměřit na jiný server DNS zadáním příkazu **server <název>** (kde <název> je název DNS serveru, který chcete používat pro budoucí vyhledávání). Po specifikaci jiného serveru se cokoliv dalšího vkládaného považuje za název hostitele.

Nástroj Nslookup používá převáděcí metodu doménových názvů. Napíšete-li název hostitele a stisknete ENTER, Nslookup připojí k názvu hostitele příponu domény počítače (například cswatcp.reskit.com) a teprve potom pošle dotaz na server DNS. Není-li název nalezen, je přípona domény o jednu úroveň zkrácena (v tomto případě na reskit.com) a dotaz je zopakován. Počítače na platformě Windows 2000 zkracují názvy pouze na doménu druhé úrovně (například právě reskit.com), takže pokud dotaz není úspěšný, nejsou podniknuty žádné další snahy přeložit název. Jestliže je vepsán úplný doménový název (vyznačený koncovou tečkou), je server DNS dotázán pouze na tento název a žádná převádění se neprovádí. Pro vyhledání názvu hostitele, který je zcela mimo vaši doménu musíte vepsat úplný doménový název.

Režim ladění nástroje Nslookup je užitečnou vlastností při řešení problémů. Lokální počítač nastavíte do tohoto režimu zadáním příkazu **set debug**, případně pro více podrobností **set d2**.

V režimu ladění nástroj Nslookup vypíše seznam kroků, které podnikl ke splnění příkazů, například:

```
C:\>nslookup
(null) testpc1.reskit.com
Address: 172.16.8.190
```

```
> set d2
> rain-city
(null) testpc1.reskit.com
Address: 172.16.8.190
```

```
SendRequest(), len 49
```

```
  HEADER:
```

```
    opcode = QUERY, id = 2, rcode = NOERROR
```

```
    header flags: query, want recursion
```

```
    questions = 1, answers = 0, authority records = 0, additional =
```

```
0
```

```
  QUESTIONS:
```

```
    rain-city.reskit.com, type = A, class = IN
```

```
Got answer (108 bytes):
```

```
  HEADER:
```

```
    opcode = QUERY, id = 2, rcode = NOERROR
```

```
    header flags: response, auth. answer, want recursion, recursion
```

```
avail.
```

```
    questions = 1, answers = 2, authority records = 0, additional =
```

```
0
```

```
  QUESTIONS:
```

```
    rain-city.reskit.com, type = A, class = IN
```

```
  ANSWERS:
```

```
-> rain-city.reskit.com
```

```
    type = CNAME, class = IN, dlen = 31
```

```
    canonical name = seattle.reskit.com
```

```
    ttl = 86400 (1 day)
```

```
-> seattle.reskit.com
```

```
    type = A, class = IN, dlen = 4
```

```
    internet address = 172.16.2.3
```

```
    ttl = 86400 (1 day)
```

```
(null) seattle.reskit.com
```

```
Address: 172.16.2.3
```

```
Aliases: rain-city.reskit.com
```

V tomto případě uživatel zadal pro nastavení nástroje Nslookup na režim ladění příkaz `set d2` a pak zkusil vyhledání adresy názvu hostitele „rain.city“. První dva řádky výstupu ukazují název hostitele a adresu IP serveru DNS, kam bylo vyhledání odesláno. K názvu „rain-city“ byla připojena přípona domény lokálního počítače (reskit.com) a nástroj Nslookup postoupil tento dotaz serveru DNS, viz další odstavec.

Další odstavec příkladu naznačuje, že nástroj Nslookup obdržel od serveru DNS odpověď. Server DNS jako odpověď na jednu otázku poskytl dva záznamy. Dotaz je zopakován společně s oběma odpověďmi. V tomto případě první odpovědní záznam naznačuje, že název „rain-city.reskit.com“ je ve skutečnosti kanonický název (alias) pro ná-

zev hostitele „seattle.reskit.com“. Druhý odpovědní záznam vypsal adresu IP tohoto hostitele jako 172.16.2.3.

Tabulka 3.8 obsahuje všechny přepínače nástroje Nslookup. Identifikátory jsou velkým písmem a volitelné příkazy jsou uvedeny v závorkách.

Tabulka 3.8 Přepínače nástroje Nslookup

Přepínač	Funkce
nslookup	Spustí program nslookup.
set debug	Spustí režim ladění zevnitř nástroje nslookup.
set d2	Spustí rozšířený režim ladění zevnitř nástroje nslookup.
host name	Vrátí adresu IP určeného názvu hostitele.
NAME	Zobrazí informace o názvu hostitele/domény za použití přednastaveného serveru.
NAME1 NAME2	Viz výše, ale jako server používá NAME2.
help or ?	Zobrazí informace o obvyklých příkazech.
set OPTION	Nastaví možnost.
All	Zobrazí možnosti, aktuální server a hostitele.
[no]debug	Zobrazí informace o ladění.
[no]deframe	Připojí ke každému dotazu název domény.
[no]recurse	Žádá o rekurzivní odpověď na dotaz.
[no]search	Používá vyhledávací seznam domény.
[no]yc	Vždy používá virtuální okruh.
domain=NAME	Nastaví přednastavený název domény na NAME.
srchlist=N1[/N2/.../N6/]	Nastaví Doménu na N1 a vyhledávací seznam na N1, N2 atd.
root=NAME	Nastaví kořenový server na NAME.
retry=X	Nastaví počet opakování na X.
timeout=	Nastaví počáteční interval časového limitu na X sekund.
type=X	Nastaví typ dotazu (například A, ANY, CNAME, MX, NS, PTR, SOA, SRV).
querytype=X	Stejně jako type.
class=X	Nastaví třídu dotazu (například IN (Internet), ANY).
[no]msxfr	používá MS rychlý přenos zóny.
ixfrver=X	Aktuální verze pro použití požadavku na přenos IXFR.
server NAME	Nastaví přednastavený server na NAME za použití aktuálního přednastaveného serveru.
lserver NAME	Nastaví přednastavený server na NAME za použití počátečního serveru.
finger[USER]	Označí volitelný název NAME na aktuálním přednastaveném hostiteli.
root	Nastaví aktuální přednastavený server jako kořenový.
ls [opt] DOMAIN [> FILE]	Vypíše seznam adres v doméně DOMAIN (volitelně: výstup do souboru FILE).
-a	Vypíše seznam kanonických názvů a aliasů.
-d	Vypíše seznam všech záznamů.

Přepínač	Funkce
-t TYPE	Vypíše seznam záznamů daného typu (například A, CNAME, MX, NS, PTR atd.).
view FILE	Roztřídí soubor výstupu od možnosti „ls“ popsané dříve a zobrazí ho po stránkách.
exit	Opustí nástroj Nslookup a vrátí se na příkazový řádek.

PathPing

Nástroj PathPing je nástroj pro sledování tras, který kombinuje rysy nástrojů Ping a Tracert s dalšími informacemi, které neposkytuje ani jeden z těchto nástrojů. Nástroj PathPing posílá po určitou dobu pakety na každý směrovač po cestě ke konečnému cíli a pak vypočítá výsledky založené na paketech vrácených z každého předání. Vzhledem k tomu, že nástroj PathPing ukazuje stupeň ztráty paketů na kterémkoli daném směrovači nebo propojení, je možno přesně určit směrovače nebo propojení, které působí síťové problémy. Dostupná je též řada přepínačů, viz tabulka 3.9.

Tabulka 3.9 Přepínače nástroje PathPing

Přepínač	Název	Funkce
-n	Host names	Nepřekládá adresy na názvy hostitele.
-h <Max předání>	Maximum hops	Maximální počet předání při hledání cíle.
-g <cílová adresa>	Router -list	Použití zdrojového směrování spolu se seznamem hostitelů.
<adresa IP směrovače nebo název pro NetBIOS>		
-p <milisekundy>	Period	Počet milisekund čekání mezi jednotlivými opakováními nástroje Ping.
-q <Počet dotazů>	Num_queries	Počet dotazů na jedno předání.
-R	RSVP test	Kontroluje, jestli každý směrovač na cestě podporuje protokol RSVP, který umožňuje hostitelskému počítači vyhradit pro proud dat určitou šířku pásma. Přepínač -R se používá pro testování kvality připojení služby QoS.
-T	Layer 2 tag	Připojuje k paketům příznak priority 2. vrstvy (například IEEE 802.1p) a posílá je na každé síťové zařízení na cestě. To pomáhá při identifikaci síťových zařízení, která nemají správně nakonfigurovanou prioritu 2. vrstvy. Přepínač -T se používá pro testování kvality připojení služby QoS.
-w <milisekundy>	Time-out	Na každou odpověď čeká stanovený počet milisekund.

Dle výchozího nastavení je počet předání 30 a přednastavený časový limit je tři sekundy (3000 milisekund). Přednastavená lhůta je 205 milisekund a přednastavený počet dotazů na každý směrovač po cestě je 100.

Níže je uvedena typická zpráva nástroje PathPing. Všimněte si, že sestavené statistiky, které následují za seznamem předání, označují ztrátu paketů na každém směrovači zvlášť.

```
D:\>pathping -n testpcl
```

```
Tracing route to testpcl [7.54.1.196]
```

```
over a maximum of 30 hops:
```

```
 0  172.16.87.35
 1  172.16.87.218
 2  192.68.52.1
 3  192.68.80.1
 4  7.54.247.14
 5  7.54.1.196
```

```
Computing statistics for 125 seconds...
```

Hop	RTT	Source to Here Lost/Sent = Pct	This Node/Link Lost/Sent = Pct	Address
0				172.16.87.35
1	41ms	0/ 100 = 0%	0/ 100 = 0%	172.16.87.218
2	22ms	16/ 100 = 16%	3/ 100 = 3%	192.68.52.1
3	24ms	13/ 100 = 13%	0/ 100 = 0%	192.68.80.1
4	21ms	14/ 100 = 14%	1/ 100 = 1%	7.54.247.14
5	24ms	13/ 100 = 13%	0/ 100 = 0%	7.54.1.196

```
Trace complete.
```

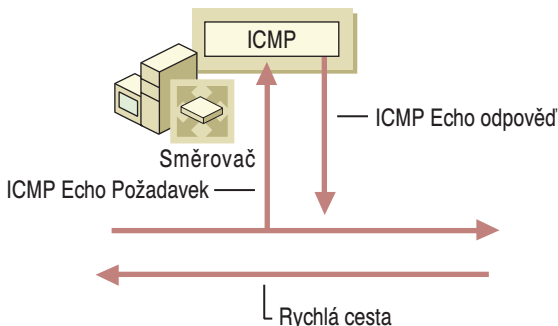
Po spuštění nástroje PathPing jako první výsledek vidíte seznam testování problémů trasy. Je to stejná cesta, jak je zobrazena pomocí nástroje Tracert. Nástroj PathPing poté zobrazí hlášení o obsazení trasy na následujících 125 sekund (tento čas se mění podle počtu předání, přičemž jedno předání potřebuje 25 sekund). Během této doby nástroj PathPing sbírá informace ze všech směrovačů zařazených do seznamu a z propojení mezi nimi. Na konci této lhůty se zobrazí výsledky testů.

Nejužitečnější informace obsahují dva sloupce nejvíce vpravo – „This Node/Link Lost/Sent=%“ a „Address“. Propojení mezi 172.16.87.218 (předání číslo 1) a 192.68.52.1 (předání číslo 2) ztratí 13 procent paketů. všechna ostatní propojení pracují normálně. Směrovače na předáních číslo 2 a 4 také ztratí pakety jim adresované (viz sloupec „This Node/Link“), ale tato ztráta neovlivní jejich předávací cestu.

Hodnoty ztrát zobrazené pro propojení (označené jako „I“ ve sloupci nejvíce vpravo) označují ztráty paketů předávaných na cestě. Tato ztráta značí zahlcení propojení. Hodnoty ztrát zobrazených pro směrovače (označených ve sloupcích nejvíce vpravo jejich adresami IP) značí, že procesorové jednotky směrovačů nebo vyrovnávací paměti paketů mohou být přetíženy. Tyto zahlcené směrovače mohou být také faktorem koncových problémů, zvláště pokud jsou pakety předávány softwarovými směrovači.

Výpočet ztrát

Nezpracovaná data, která nástroj PathPing získá, popisují, kolik odpovědí ICMP Echo Request je ztraceno mezi zdrojem a zprostředkovávajícím směrovačem. Obrázek 3.1 znázorňuje způsob, jakým nástroj PathPing odhaduje statistiky pro každé předání. Ačkoli se tyto výpočty mohou na první pohled zdát triviální, jsou složité rozdíly mezi cestou kódu předání a cestou kódu v odpovědích ICMP Echo Request/Reply.



Obrázek 3.1 Cesty doručení paketů

Horizontální linky označují „rychlou cestu“ směrovače, kterou jdou pakety, které nejsou poslány na lokální počítač nebo z lokálního počítače. To znamená, že rychlá cesta je cesta kódu, kterou jdou přenášené pakety nevyžadující žádné zvláštní zpracování kromě předání, a zároveň cesta, která je pro takové pakety optimalizovaná.

V diagramu vertikální linky označují zvláštní zpracování, které se odehrává při posílání požadavků ICMP Echo Request na lokální počítač. Tím je vyloučena rychlá cesta a pakety jsou doručeny modulu protokolu ICMP (často za použití oddělených front a procesorů). Za předpokladu, že se žádné pakety neztratí kvůli přetečení fronty, modul protokolu ICMP pak vygeneruje odpověď ICMP Echo Reply, která je předána zpět původnímu odesílateli.

Vzhledem k tomu, že se na cestě označené vertikálními linkami mohou objevit ztráty paketů (takové ztráty ovšem nikoli nezbytně neimplikuje ztrátu na horizontální cestě předání samotné), neurčují samotná nezpracovaná data získaná z provedení příkazu Ping koncovou ztrátu paketů. Například provedení příkazu Ping na zprostředkovávajícím směrovači může vytvořit ztrátu 10 procent, ačkoli se nemusí objevit žádná koncová ztráta paketů. Algoritmus nástroje PathPing používá změny v hodnotách od předání k předání a odhaduje podle nich skutečnou ztrátu po jednotlivých předáních spíše, než ztráty v součástech směrovače vyšší úrovně. Tato skutečná ztráta v jednom směrování je výsledkem poskytovaným ve sloupci „This Node/Link“ závěrečné zprávy nástroje PathPing.

Ping

Nástroj Ping je základní nástroj pro řešení problémů s připojením na úrovni protokolu IP. Na příkazovém řádku napište `ping -?` a objeví se úplný seznam dostupných možností příkazu. Příkaz Ping umožňuje specifikovat velikost používaných paketů (dle výchozího nastavení je to 32 bajtů), kolik paketů odesílat, jestli zaznamenávat použité trasy, jakou hodnotu časového limitu `Ttl` použít a jestli nastavit příznak „don't fragment“.

Po zadání příkazu **ping** pošle tento nástroj požadavek ICMP Echo Request na cílovou adresu IP, aby zjistil, jestli odpovídá. Jestliže je toto úspěšné, použijte příkaz Ping tentokrát s názvem hostitele cílového hostitele. Nástroj Ping se nejprve snaží přeložit název na adresu prostřednictvím serveru DNS, pak serveru WINS (je-li nakonfigurován) a potom pomocí lokálního všesměrového vysílání. Je-li pro překlad názvu použit server DNS a není-li vložený název úplným doménovým názvem, přidá DNS překladač název nebo názvy domény počítače tak, aby vygeneroval úplný doménový název.

Jestliže je provedení příkazu ping podle adresy úspěšné, ale provedení příkazu ping podle názvu úspěšné není, problém zpravidla spočívá v překladu názvu a nikoli v připojení sítě. Všimněte si, že překlad názvu může zklamat, jestliže nepoužijete úplný doménový název pro vzdálený název. Tyto požadavky mohou zklamat, protože překladač DNS přidá příponu lokální domény názvu, který se nachází kdekoli v hierarchii domén.

Následující příklad znázorňuje, jak poslat dvě záznamy příkazu ping, každou o velikosti 1450 bajtů, na adresu 172.16.99.2:

```
C:\>ping -n 2 -l 1450 172.16.99.2
```

Pinging 172.16.99.2 with 1450 bytes of data:

```
Reply from 172.16.99.2: bytes=1450 time<10ms TTL=62
```

```
Reply from 172.16.99.2: bytes=1450 time<10ms TTL=62
```

Ping statistics for 172.16.99.2:

Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Dle výchozího nastavení nástroj Ping počká jednu sekundu před každou vrácenou odpovědí a pak vyprší časový limit. Jestliže probíhá provádění příkazu ping na vzdálený systém přes připojení s velkou prodlevou, jako například přes satelitní připojení, vrácení odpovědi může zabrat delší čas. Pro určení delšího časového limitu použijte přepínač -w (wait).

Poznámka Jestliže nástroj Ping označuje vysokou ztrátu paketů nebo pomalou odpověď se zpožděním na síti LAN, může mít vaše síť hardwarový problém. Na síti WAN mohou být tyto výsledky normální a protokol TCP/IP je navržen tak, aby tuto rozdílnost zvládal. Na síti LAN je zpoždění velmi nízké a ztráty paketů jsou malé či vůbec žádné. není-li toto váš případ, zkontrolujte kabely, kabelové koncovky, rozbočovače, přepínače a vysílače.

Tabulka 3.10 obsahuje seznam přepínačů nástroje Ping.

Tabulka 3.10 Přepínače nástroje Ping

Přepínač	Funkce
-t	Provádí příkaz ping na určeného hostitele až do doby, kdy je zastaven. Po stisknutí kláves Control-Break se zobrazí statistiky a pak dál pokračuje. Po stisknutí kláves Control-C se proces zastaví.
-a	překládá adresy k názvům hostitele.

Přepínač	Funkce
-a<počet>	Nastaví počet odesílaných požadavků Echo Request.
-l <velikost>	Posílá pakety příslušné velikosti.
-f	Nastavuje u odchozích paketů příznak „Don't Fragment“.
-i <TTL>	Určuje u odchozích paketů TTL.
-v <TOS>	Určuje typ služby.
-r <počet>	Zaznamenává počet předání na trase.
-s <počet>	Časové razítko pro počítaná předání.
-j <seznam-hostitelů>	Volná zdrojové směrování se seznamem hostitelů.
-k <seznam-hostitelů>	Přísná zdrojové směrování se seznamem hostitelů.
-w	Nastavuje dlouhé čekací lhůty (v milisekundách) pro odpovědi.

Nástroj Route

Nástroj Route se používá k prohlížení a upravování směrovací tabulky IP. Příkaz Route Print zobrazuje seznam aktuálních tras, které hostitel zná. Výstup po provedení příkazu route může vypadat například tak, jak vidíte v části „Řešení problémů směrování IP“ později v této kapitole. Příkaz Route Add přidává trasy do tabulky. Příkaz Route Delete odstraňuje trasy ze směrovací tabulky hostitele.

Poznámka Trasy přidávané do směrovací tabulky nejsou trvalé, pokud není použita volba **-p**. Dočasné trasy vydrží pouze do restartu počítače nebo do deaktivace rozhraní. Rozhraní lze deaktivovat, když je Plug and Play rozhraní odpojeno (například laptop nebo hot-swap PC), když je z karty média odpojen vodič (jestliže adaptér podporuje zjišťování chyb média) nebo když je rozhraní manuálně odpojeno od adaptéru ve složce **Síťová a telefonická připojení**.

Aby si mohli dva hostitelé vyměňovat IP datagramy, musí buď mít oba trasu na toho druhého nebo musí používat přednastavenou bránu, která zná trasu mezi nimi. Normálně si směrovače vyměňují informace za pomoci protokolu, jako je například protokol RIP nebo OSPF. Služba RIP Listening Service je dostupná pro operační systém Microsoft® Windows® 2000 Professional a plné směrovací protokoly jsou podporovány v operačním systému Windows 2000 Server službou Routing and Remote Access Service.

Použití pro nástroj Route je **route [-f] [-p] [příkaz [určení]] [MASK síťová maska] [brána] [metric metrika] [if rozhraní]**.

Příkazy, které jsou použitelné ve výše uvedené syntaxi, jsou Print, Add, Delete a Change. Tabulka 3.11 obsahuje seznam těchto příkazů stejně jako seznam ostatních přepínačů a parametrů nástroje Route.

Tabulka 3.11 Volby nástroje Route

Volba	Funkce
-f	Vyčistí směrovací tabulku od všech záznamů bran. Je-li tato volba použita současně s jedním z dalších příkazů, jsou tabulky před provedením takového příkazu vyčištěny.
-p	Když je použit s příkazem Add, přidává tato volba trasu do směrovací tabulky a do registru ve Windows 2000. Trasa je automaticky přidána do směrovací tabulky při každé inicializaci protokolu TCP/IP. Dle výchozího nastavení jsou trasy přidány bez přepínače -p ukládány pouze ve směrovací tabulce na bázi RAM a nejsou uchovávány po restartu protokolu TCP/IP. Tato možnost je všemi ostatními příkazy ignorována.
Print <určení>	Vytiskne trasu ke specifikovanému hostiteli. Volitelně vytiskne trasy ke specifikovaným místům určení.
Add <určení> Mask <síťová maska> Metric <metrika> if <rozhraní>adresy	Přidává trasu specifikovaného místa určení za použití předávací IP brány. Možnosti metric a if nejsou požadovány.
Delete <určení>	Odstraní trasu ke specifikovanému místu určení.
Change <určení> Mask <síťová maska> <brána> Metric <metrika> if <rozhraní>	Upravuje existující trasu.
Mask <síťová maska>	Určuje, že následující parametr má hodnotu síťové masky. Není-li hodnota síťové masky specifikována, je přednastavena na 255.255.255.255.
Metric <metrika>	Určuje náklady na dosažení místa určení. Přednostně jsou vybírány trasy s nižší metrikou. Typickým požitím hodnoty metriky je označení počtu směrovačů, které musí být pro dosažení místa určení překročeny.
if <rozhraní>	Určuje adresu IP rozhraní, přes které je dosažitelné cílové umístění.

Všechny symbolické názvy používané pro určení jsou vyhledávány v síťovém databázovém souboru NETWORKS. Symbolické názvy bran jsou vyhledávány v databázovém souboru názvů hostitele HOSTS. Jestliže příkaz je **print** nebo **delete**, může být hodnota cílového umístění vyjádřena pomocí zástupného znaku hvězdičkou („*“). Jestliže specifikované cílové umístění obsahuje zástupné znaky * nebo ?, je považován za zápis se zástupnými znaky a jsou vytištěny pouze trasy k odpovídajícím cílům. Znak * odpovídá libovolnému řetězci a znak ? odpovídá jednomu znaku. Příklady: 157.*.1, 157.*,127.*,*224*.

Použití nesprávné kombinace cílového umístění a hodnoty síťové masky vygeneruje chybu „route:bad gateway address netmask“. Tento typ chybového hlášení se objeví například při nerovnosti výsledku logického součinu mezi cílovým umístěním a maskou s hodnotou cílového určení.

Tracert

Tracert je nástrojem pro sledování trasy, který zobrazuje seznam bližší rozhraní směrovačů po cestě mezi zdrojovým hostitelem a cílovým umístěním. Nástroj Tracert použít

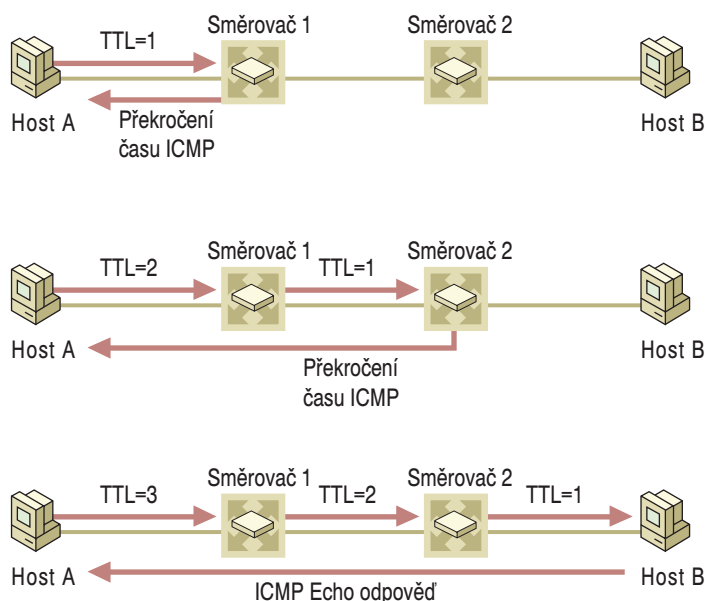
vá k určení cesty ze zdroje na cílové umístění přes síť IP pole TTL protokolu IP v požadavku ICMP Echo Request a hlášení ICMP Time Exceeded Message..

Poznamenejme, že některé směrovače vyřazují pakety s vypršeným TTL bez upozornění. Tyto směrovače se při použití nástroje Tracert nezobrazí.

Jak nástroj Tracert pracuje

Nástroj Tracert pracuje tak, že zvětšuje hodnotu TTL o jednu pro každý požadavek ICMP Echo Request, který odešle, a pak čeká na hlášení ICMP Time Exceeded Message. Hodnoty TTL paketů nástroje Tracert začínají na hodnotě jedna, po každém průchodu se TTL zvětšuje o jednu. Paket odesílaný nástrojem Tracert cestuje na každé další cestě o jedno předání (směrování) dál.

Obrázek 3.2 znázorňuje, jak nástroj Tracert pracuje. Nástroj Tracert byl spuštěn na hostiteli A a prochází cestu k hostiteli B. Na směrovači 1 a 2 se TTL sníží na 0, takže oba směrovače pošlou hlášení ICMP Time Exceeded Message. Když je na hostiteli B zachycen požadavek ICMP Echo Request, pošle zpět odpověď ICMP Echo Reply.



Obrázek 3.2 Činnost nástroje Tracert po jednotlivých krocích

Poznámka Verze nástroje Tracert pro unixové operační systémy vykonává stejné funkce jako verze pro Windows kromě toho, že datová část IP je paketem protokolu UDP adresovaným na (předpokládaně) neznámý cílový port UDP. Předávací směrovače posílají zpět hlášení ICMP Time Expires Message zaznamenávající prošlou trasu a konečné cílové umístění pošle zpět hlášení ICMP Destination Unreachable-Port Unreachable Message.

Datová část UDP z nástroje UNIX Tracert může přecházet směrovače a servery firewall, avšak hlášení ICMP Echo Request Message nemusí odpovídat filtrování protokolu ICMP.

Abyste tomuto problému zabránili v operačním systému Windows 2000, vypněte filtrování paketů tak, jak je popsáno v části „Zkontrolujte filtrování paketů“ později v této kapitole a pak zkuste znovu použít nástroj Tracert.

Výklad výsledků použití nástroje Tracert

Je zde uveden příklad výstupu příkazu tracert. Počínaje prvním záznamem, zobrazuje popořadě každý směrovač objevený na cestě ke konečnému cílovému umístění. Po prvních dvou směrovačích sledování dosáhne svého cíle. Řádky zobrazení nástroje tracert jsou odsazeny kvůli čitelnosti.

```
C:\tracert reskit
Tracing route to reskit.dns.microsoft.com [172.16.180.113] over a maximum
of 30 hops:
 1      <10 ms      <10 ms      <10 ms
        ms28-rtr1-f10-00.network.microsoft.com [157.59.0.1]
 2      <10 ms      <10 ms      <10 ms
        ms42-rtr1-a5-00-1.network.microsoft.com [157.54.247.98]
 1      <10 ms      <10 ms      <10 ms
        RESKIT [172.16.180.113]
```

V případě, že sledování buď nedosáhne cílového určení nebo se nevrátí žádná hlášení ICMP Time Exceeded Message, jsou na výstupu v každém ze tří sloupců, kde je zpravidla zobrazen čas od odeslání požadavku do příchodu odezvy, zobrazeny hvězdičky a v pravém sloupci, kde je zpravidla zobrazen název domény nebo adresa IP, je zobrazeno hlášení Request timed out nebo jiné chybové hlášení.

Tabulka 3.12 obsahuje seznam přepínačů nástroje Tracert.

Tabulka 3.12 Přepínače nástroje Tracert

Přepínač	Funkce
-d	Určuje, že se nemají adresy rozhraní směrovače překládat na názvy hostitele.
-h <maximum_předání>	Určuje maximální počet předání (směrování), ve kterých se má dosáhnout cílového umístění.
-j <seznam_hostitelů>	Určuje volné zdrojové směrování se seznamem hostitelů.
-w <časový_limit>	Označuje, kolik milisekund se má čekat na každou odpověď.

Přehled řešení problémů

Při řešení jakýchkoli problémů se ptejte na následující otázky:

- Která aplikace selhává? Co funguje? Co nefunguje?
- Je to problém základního IP připojení nebo překladu názvu? Je-li to problém s překladem názvu, používá selhávající aplikace názvy typu NetBIOS nebo názvy a názvy hostitele typu DNS?
- Jak jsou spolu souvisí věci, které fungují a nefungují?
- Fungovaly někdy momentálně nefunkční věci na tomto počítači nebo síti?
- Pokud ano, co se změnilo od té doby, co naposledy fungovaly?

V ideálním případě pomůže přehled umístění a načasování problému zúžit rozsah možných problémů. Navíc můžete systematicky prozkoumat selhání protokolu TCP/IP pomocí odkazů na jednotlivé kroky potřebné k úspěšné komunikaci mezi počítači. Tyto kroky jsou popsány v následujících částech, navrhované metody řešení problémů začínají v části „Nelze dosáhnout název hostitele nebo název typu NetBIOS“ v této kapitole.

Komunikace protokolu TCP/IP

Proces protokolu TCP/IP se u dvou počítačů komunikujících přes síť dělí na čtyři zřetelné kroky. Protokol TCP/IP na odesílajícím hostiteli vykoná před odesláním paketu tyto čtyři kroky:

1. Přeloží název hostitele nebo název typu NetBIOS na adresu IP.
2. Za pomoci cílové adresy IP a směrovací tabulky IP protokol TCP/IP určí, které rozhraní a předávací adresa IP se mají použít.
3. U jednosměrového provozu IP na technologiích sdíleného přístupu, například Ethernet, Token Ring a rozhraní FDDI, přeloží protokol ARP předávací adresu IP na MAC adresu.

U vícesměrného provozu IP na technologiích Ethernet a rozhraní FDDI je cílová adresa IP vícesměrového vysílání mapována na odpovídající MAC adresu vícesměrového vysílání. U vícesměrového provozu v IP na technologii Token Ring se používá funkcionální adresa 0xC0-00-00-04-00-00. Pro všesměrové vysílání na technologiích sdíleného přístupu je MAC adresa mapována na 0xFF-FF-FF-FF-FF-FF.

4. IP datagram je odeslán na MAC adresu přiřazenou pomocí protokolu ARP nebo pomocí mapování vícesměrového vysílání.

Následující část popisuje každou část tohoto procesu. Zásobník protokolu TCP/IP vždy při určování, jak dostat paket z jednoho místa na druhé, postupuje podle této posloupnosti. Chcete-li přeskočit přímo k řešení problémů, jděte na část „Nelze dosáhnout název hostitele nebo název typu NetBIOS“ v této kapitole.

Překlad názvu na adresu IP

Jestliže je cílové umístění, kterého má aplikace dosáhnout, ve formátu názvu typu NetBIOS nebo názvu hostitele, je před odesláním prvního paketu protokolem IP třeba nejprve přeložit název. Protokol IP rozumí pouze adresám IP. Název hostitele a název typu NetBIOS se překládá na adresu IP každý jiným způsobem.

Překlad názvu typu NetBIOS na adresu IP

Názvy typu NetBIOS lze přímo přeložit na adresy IP prostřednictvím čtyřech mechanismů: prověření mezipaměti, všesměrové vysílání, kontrole souboru LMHOSTS nebo dotaz na server WINS. Pořadí, ve kterém operační systém Windows 2000 použije tyto mechanismy, závisí na typu uzlu klienta.

Operační systém Windows 2000 vždy začíná kontrolou interní mezipaměti názvů typu NetBIOS hostitelského počítače. Není-li toto úspěšné, lze název typu NetBIOS přeložit na adresu IP za pomoci všesměrového vysílání, souboru LMHOSTS nebo serveru WINS. To, který postup z těchto tří je použit konkrétním počítačem jako první, závisí na jeho typu uzlu. Přednastavený typ uzlu je hybridní čili typ H, který snahu o překlad názvu začíná dotazem na server WINS a pak zkouší lokální všesměrové vysílání. Podrobnosti o typech uzlů najdete v části „Windows 2000 TCP/IP“ v této knize. Po vyčerpání těch-

to mechanismů se klient dotazuje svého souboru Hosts a, neuspěje-li, dotazuje se serveru DNS, je-li k jeho použití nakonfigurován.

Všimněte si, že pokud je jediným problémem překlad názvu typu NetBIOS, počítač by měl být stále schopen dosáhnout vzdáleného zdroje pomocí adresy IP. Nástroje používané k diagnostice překladu názvu typu NetBIOS jsou Ntstat, Nslookup a příkaz net use.

Více podrobností o službě WINS najdete v části „Služba Windows Internet Name Service“ v této knize.

Překlad názvu hostitele nebo doménového názvu na adresu IP

Název hostitele lze přímo přeložit pomocí souboru Hosts nebo serveru DNS. Problémy zde zpravidla působí nesprávně nakonfigurovaný soubor Hosts nebo server DNS, špatně zapsaný záznam souboru Hosts nebo špatně zapsaná adresa IP, nebo více zápisů v souboru Hosts pro jednoho hostitele. Nástroje používané k diagnostice problémů s překladem názvu hostitele nebo doménového názvu jsou Nslookup nebo Netdiag.

Více podrobností o službě DNS najdete v části „Úvod do DNS“ a „Služba Windows 2000 DNS“ v této knize.

Určení, zda adresa je lokální nebo vzdálená

Maska podsítě a adresa IP se používají dohromady k určení, zda je cílová adresa IP lokální nebo vzdálená.

V tomto okamžiku chyby v konfiguraci, například nesprávně nakonfigurovaná maska podsítě, mohou vést k neschopnosti hostitele dosáhnout dalších hostitelů na jiné lokální podsíti, ačkoli stále může komunikovat se vzdálenými hostiteli na vzdálených sítích a hostiteli na vlastní podsíti.

Je-li cílová adresa lokální, protokol IP použije k překladu na MAC adresu protokol ARP

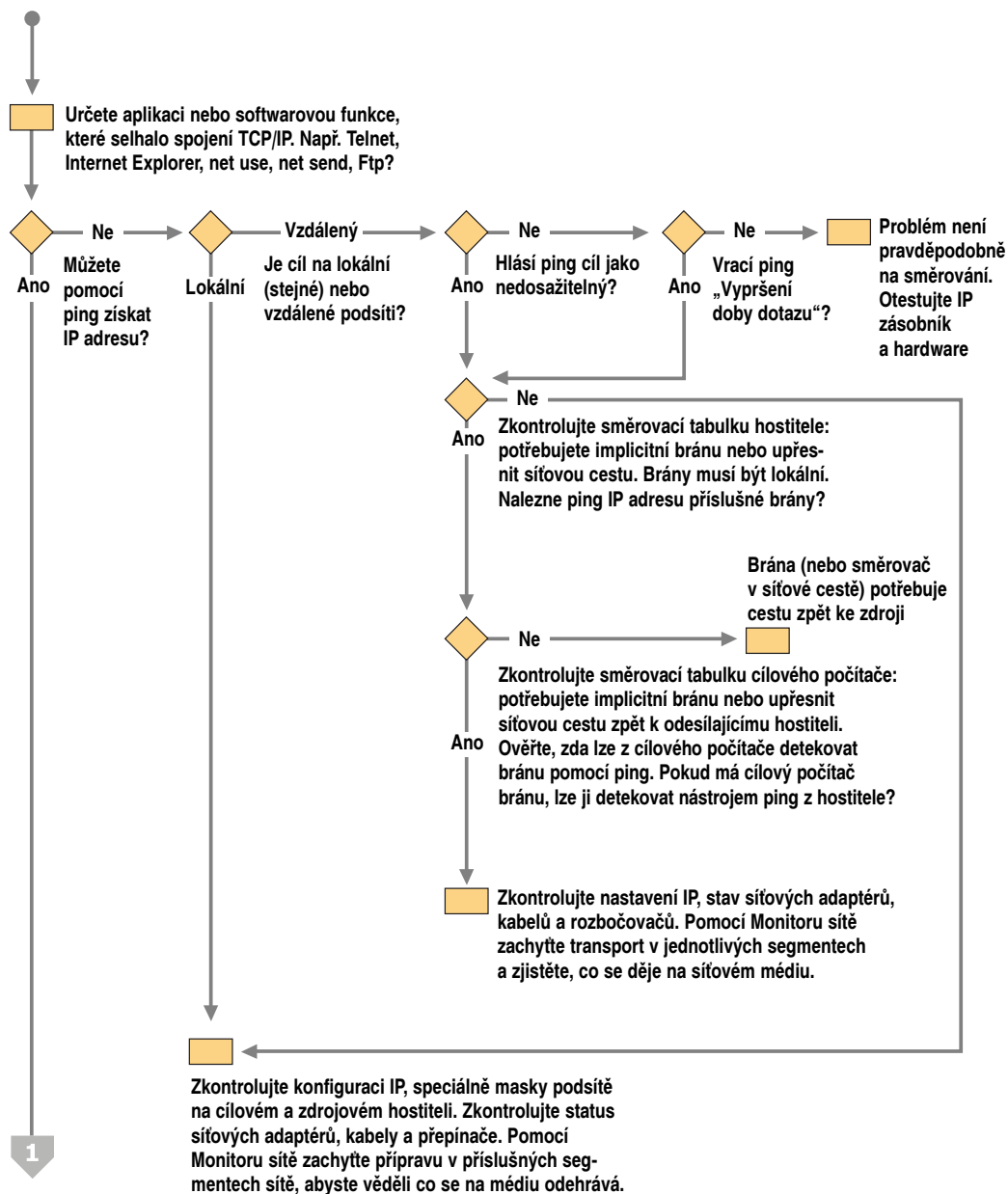
Je-li adresa lokální, vyžaduje doručení přídatnou snahu. Protokol ARP přeloží adresu IP na hardwarovou adresu, typicky MAC adresu (Media Access Control) pro cílové umístění karty Ethernet. Problémy, které se zde vyskytují, jsou zpravidla problémy s mezipamětí ARP (například duplikované adresy) nebo maskou podsítě a lze je vyřešit pomocí nástrojů Arp nebo Ipconfig.

Je-li adresa vzdálená, určí správnou bránu

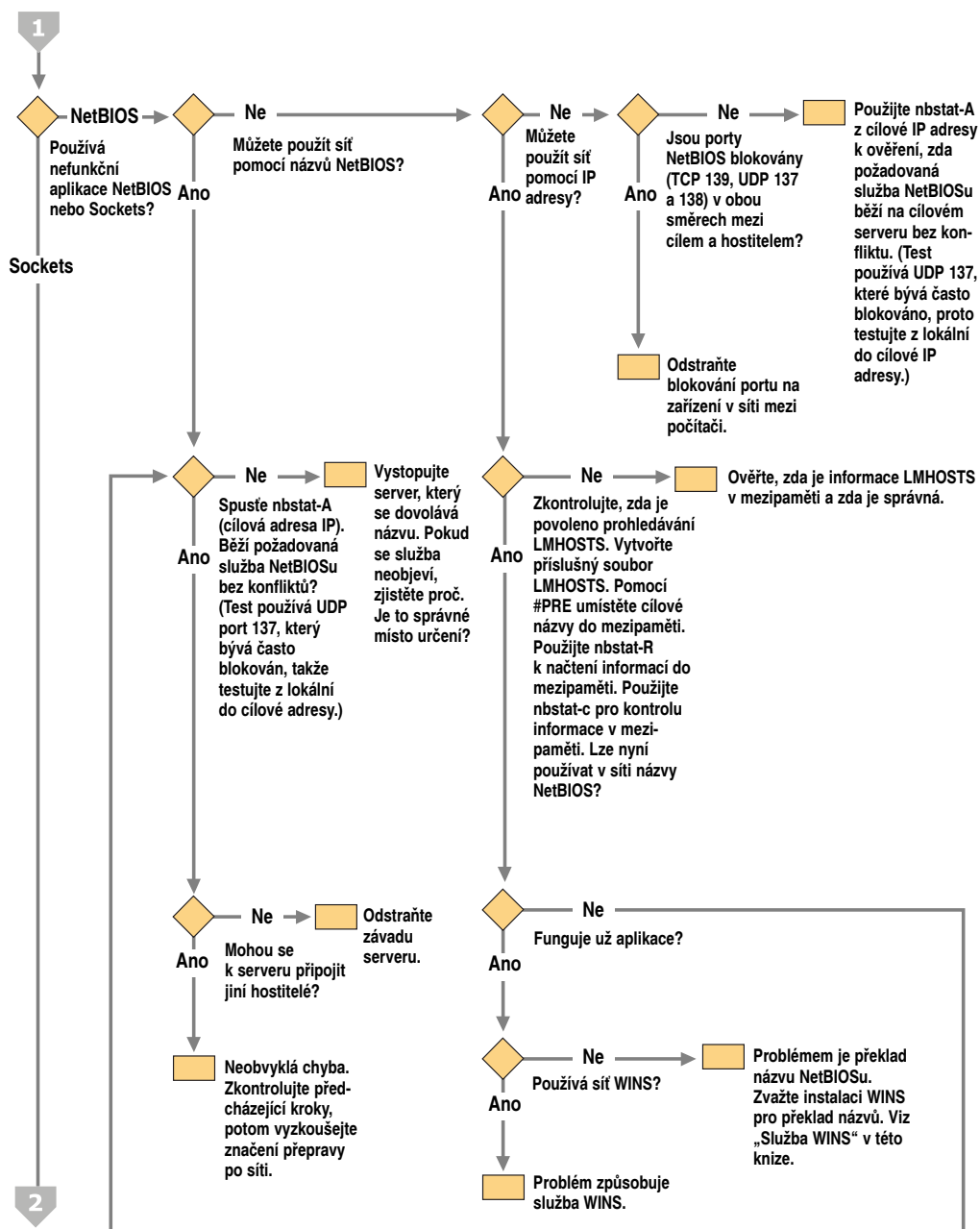
Je-li adresa vzdálená, je dalším krokem určení brány, která bude použita k dosažení této vzdálené adresy. Na síti s pouze jediným směrovačem fungujícím jako externí připojení je problém relativně přímočarý. Nicméně v sítích s více než jedním připojeným směrovačem je určování brány složitější.

Protokol IP řeší tento problém prostřednictvím nahlédnutí do směrovací tabulky. Tato směrovací tabulka slouží jako rozhodovací strom, který umožňuje protokolu IP rozhodnout, které rozhraní a kterou bránu má použít pro odeslání odchozího provozu. Směrovací tabulka obsahuje mnoho jednotlivých tras, přičemž každá trasa sestává z konečného umístění, masky sítě, rozhraní brány a metriky.

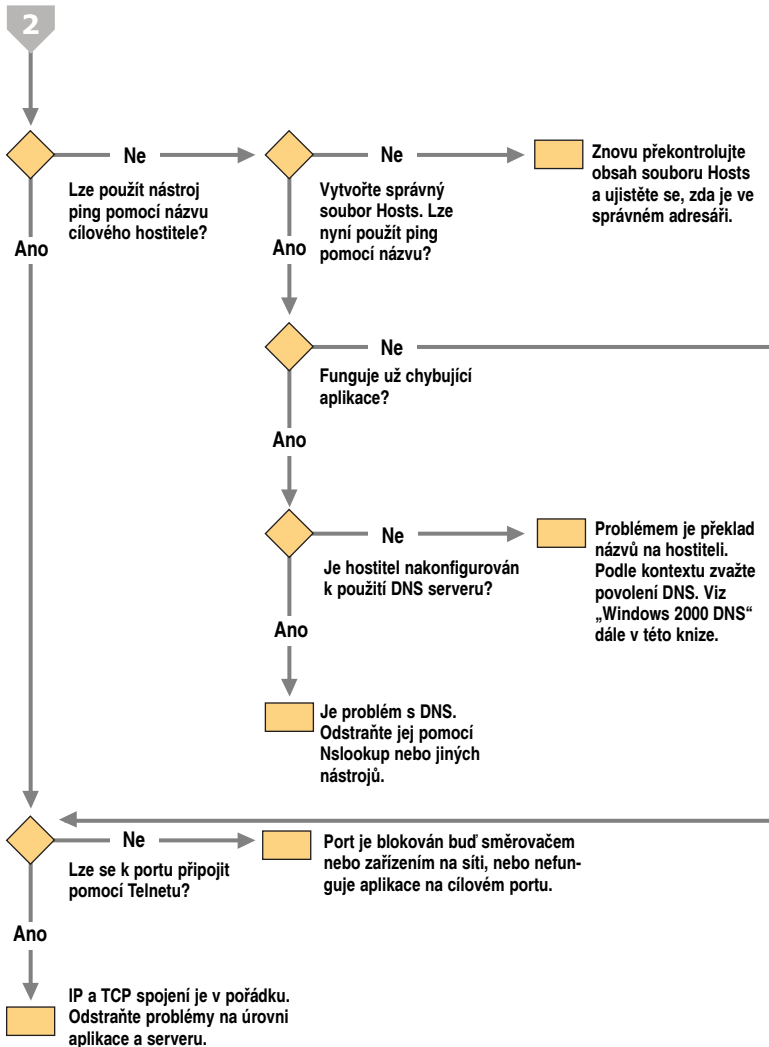
Start



Obrázek 3.3 Graf řešení problémů protokolu TCP/IP (1. část ze 3)



Obrázek 3.4 Graf řešení problémů protokolu TCP/IP (2. část ze 3)



Obrázek 3.5 Graf řešení problémů protokolu TCP/IP (3. část ze 3)

Jsou-li dvě trasy identické, je dána přednost trase s nejnižší metrikou. Všimněte si, že směrovací tabulka je rozdělena od nejurčitějšího k nejobecnějšímu, takže paket je poslán na první bránu, jejíž záznamy směrovací tabulky odpovídají cílovému určení paketu. Při nerozhodném výsledku se vybere způsobem kruhového výběru. Problémy nalezené v této oblasti se řeší pomocí nástroje Route nebo prostřednictvím změn síťové konfigurace.

Protokol ARP pro adresu brány

Poté, co je určena správná brána, proces protokolu ARP proběhne pro adresu brány stejně jako pro kteroukoli jinou lokální adresu. Všesměrové vysílání protokolu ARP vrátí hardwarovou adresu a na bránu je odeslána zpráva, která má být směrována dál.

Nelze dosáhnout název hostitele nebo název typu NetBIOS

Protokol TCP/IP pro Windows 2000 umožňuje aplikaci komunikovat přes síť s jiným počítačem pomocí třech základních typů určení cílového umístění:

- adresa IP
- Název hostitele
- Název typu NetBIOS

Tato část popisuje, jak řešit problémy s překladem názvu hostitele nebo názvu typu NetBIOS. Problémy s IP adresováním najdete v části „Nelze dosáhnout adresu IP“ později v této kapitole. Obě tato témata jsou načrtnuta na obrázcích 3.3 až 3.5, které poskytují zjednodušený graf řešení problémů.

Prvním krokem je určení, která aplikace selhává. Typicky to je Telnet, Internet Explorer, **net use**, správa serveru nebo Ftp. To usnadní další krok, kterým je určení, jestli je problém problémem s překladem názvu hostitele nebo názvu typu NetBIOS.

Nejsnadněji lze rozlišit problémy s překladem názvu hostitele od problémů s překladem názvu typu NetBIOS podle toho, jestli selhávající aplikace používá NetBIOS nebo Sockets. Používá-li Sockets, problém je v rozlišení názvu DNS/názvu hostitele. Mezi nejobvyklejší aplikace patří v rodině NetBIOS různé příkazy NET nebo administrátorské nástroje ve Windows NT 4.0, zatímco v rodině Sockets a WinSockets to jsou Telnet, Ftp a webové prohlížeče.

Následující části popisují postupy nastávající při použití názvu hostitele nebo názvu typu NetBIOS pro připojení k hostitelům na síti protokolu TCP/IP.

Error 53 (Chyba 53)

Nejobvyklejším příznakem problému s překladem názvu typu NetBIOS je vrácení hlášení Error 53 nástrojem Ping. Hlášení Error 53 je obecně vráceno při selhání překladu určitého názvu počítače. Error 53 se může objevit také při vytváření relace NetBIOS. Tyto dva případy můžete rozlišit pomocí následujícího postupu:

► Určení příčiny hlášení Error 53

1. Z menu **Start** otevřete příkazový řádek.
2. Na příkazovém řádku napište:

```
net view * \\<název_hostitele>
```

kde <název_hostitele> je síťový prostředek, o kterém víte, že je aktivní.

Jestliže toto funguje, není překlad názvu pravděpodobně zdrojem problému. K potvrzení proveďte příkaz ping na název hostitele, protože překlad názvu může někdy fungovat správně a přesto síť vrací hlášení Error 53 (jako kdyby například server DNS nebo WINS měl chybný záznam). Jestliže selže i překlad názvu pomocí provedení příkazu ping (vrátí se hlášení Unknown host), zkontrolujte stav relace NetBIOS.

► Kontrola stavu relace NetBIOS

1. Z menu Start otevřete příkazový řádek.
2. Na příkazovém řádku napište:

```
net view * \\< adresa IP>
```

 kde <adresa IP> je stejný síťový prostředek, který jste použili v předchozím postupu. Jestliže toto opět selže, je problém ve vytváření relace.

Jestliže je počítač na lokální podsíti, ověřte si, že název je zapsán správně a že na cílovém počítači běží protokol TCP/IP. Jestliže počítač není na lokální podsíti, ověřte si, že mapování jeho názvu a adresy IP jsou dostupné v databázi DNS, souboru Hosts nebo LMHOSTS nebo v databázi WINS.

Pokud se zdá, že všechny prvky protokolu TCP/IP jsou řádně nainstalovány, proveďte příkaz ping na vzdálený počítač a ujistěte se, že jeho protokol TCP/IP je funkční.

Nelze se připojit na vzdálené systémy používající název hostitele

Jestliže není problémem NetBIOS, ale Sockets, je problém spojený buď se souborem Hosts nebo s chybou konfigurace DNS. K určení, proč pro připojení ke vzdáleným počítačům fungují pouze adresy IP a ne názvy hostitele, se ujistěte, že počítač má nakonfigurovaná příslušná nastavení souboru Hosts a DNS.

► Kontrola konfigurace překladu názvu hostitele

1. Na Ovládacích panelech klepněte na ikonu **Síťová a telefonická připojení**.
2. Klepněte pravým tlačítkem myši na **Připojení k místní síti** a pak vyberte **Vlastnosti**.
3. Klepněte na **Protokol TCP/IP** a pak klepněte **Vlastnosti**.
4. V dialogovém okně **Vlastnosti protokolu Microsoft TCP/IP** klepněte na záložku **Upřesnit**.
5. Klepněte na záložku **DNS**.
6. Ověřte, že DNS je nakonfigurován správně. Jestliže chybí adresa IP serveru DNS, přidejte ji do seznamu adres serverů DNS.

Zkontrolujte si soubor Hosts

Máte-li problémy s připojením ke vzdálenému systému používajícího název hostitele a používáte pro překlad názvu soubor Hosts, může problém působit obsah tohoto souboru. Ověřte si, zda je název vzdáleného počítače v souboru Hosts a v jej používající aplikaci zaznamenán správně.

Soubor Hosts nebo server DNS je používán k překladu názvů hostitele adresám IP, kdykoli použijete nástroje protokolu TCP/IP, například nástroj Ping. Soubor Hosts můžete najít v `%SystemRoot%\System32\Drivers\Etc`.

Tento soubor není dynamický, všechny záznamy jsou vkládány ručně. Formát souboru je následující:

IP Address	Friendly Name
172.16.48.10	testpc1 # Remarks are denoted with a #.

Adresa IP a popisný název hostitele jsou vždy odděleny jednou nebo více mezerami nebo tabulátorem.

Překlad názvu hostitele za použití souboru Hosts

Počítač používající pro překlad názvu soubor Hosts postupuje následujícím způsobem.

1. Počítač A zadá příkaz používající název hostitele počítače B.
2. Počítač A analyzuje svůj soubor Hosts (v `%SystemRoot%\System32\Drivers\Etc`) a hledá název hostitele počítače B. Jakmile tento název najde, přeloží ho na adresu IP.
3. Přiřazená adresa IP je postoupena směrovací součásti protokolu IP. Tato směrovací součást vrátí buď směrovací chybu, protože nebyla nalezena trasa k cílové adrese IP, nebo předávací adresu IP a rozhraní, přes které má být paket odeslán.
4. Protokol ARP přeloží předávací adresu IP hardwarové adrese.

Síťové chyby mohou způsobit následující problémy souboru Hosts:

- Soubor Hosts neobsahuje příslušný název hostitele.
- Název hostitele je v souboru Hosts nebo v příkazu špatně zapsán.
- Adresa IP pro název hostitele v souboru Hosts je vadná nebo nesprávná.
- Soubor Hosts obsahuje více záznamů pro stejného hostitele na samostatných řádcích. Vzhledem k tomu, že soubor Hosts je analyzován od svého začátku, je použit první nalezený záznam.

Zkontrolujte si konfiguraci DNS

Používáte-li DNS, ověřte si, že adresy IP serverů DNS jsou správné a ve správném pořadí. Použijte příkaz Ping na název hostitele vzdáleného počítače a pak na jeho adresu IP, abyste určili, jestli je adresa hostitele správně přeložena. Jestliže provedení příkazu Ping na název hostitele selže a provedení příkazu Ping na adresu IP je úspěšné, je problém v překladu názvu. Pomocí příkazu Ping na jejich adresy IP nebo pomocí otevření relace Telnet na port 53 serveru DNS můžete ověřit, jestli servery DNS běží. Jestliže se připojení vytvoří úspěšně, služba DNS na serveru DNS pracuje. Po ověření toho, že služba DNS běží, můžete vykonávat dotazy nástrojem NSlookup na server DNS, abyste dále ověřili stav záznamů, které hledáte.

Jestliže provedení příkazu Ping na adresu IP a na název selže, je problém v připojení k síti, například základní připojení nebo směrování. Více podrobností o řešení problémů s připojením k síti najdete v této kapitole v části „Řešení problémů směrování IP“.

V této části je poskytnuto stručné shrnutí, jak DNS překládá název hostitele. Více podrobností o DNS najdete v této knize v části „Služba Windows 2000 DNS“.

Překlad názvu hostitele za použití serveru DNS

DNS je distribuovaná databáze, která mapuje doménové názvy datům. Uživatel se může dotázat DNS za použití hierarchických, popisných názvů, aby lokalizoval počítače a jiné prostředky na síti IP. To umožňuje DNS, aby z větší části nahradil funkci vykonávanou souborem Hosts. Přitom přiřazuje popisné názvy adresám IP, a to takto (v nejhorším případě může být odpověď poskytnuta kterýmkoli serverem podél cesty, čímž se zabrání potřebě dalších iterativních dotazů):

1. Klient kontaktuje server názvů DNS s rekurzivním dotazem na `name.reskit.com`. Server nyní musí buď odpovědět, nebo poslat chybové hlášení.
2. Server názvů DNS projde svou mezipaměť a soubory zóny, aby našel odpověď, ale neuspěje. Kontaktuje server na kořeni Internetu (kořenový server DNS) s iterativním dotazem na `name.reskit.com`.

3. Kořenový server odpověď nezná, takže odpoví odkazem na nadřazený server v doméně .com.
4. Server názvů DNS kontaktuje server v doméně .com s iterativním dotazem na name.reskit.com.
5. Server v doméně .com přesnou odpověď nezná, takže odpoví odkazem na nadřazený server v doméně reskit.com.
6. Server názvů DNS kontaktuje server v doméně reskit.com s iterativním dotazem na name.reskit.com.
7. Server v doméně reskit.com odpověď zná, takže odpoví správnou adresou IP.
8. Server názvů DNS reaguje na dotaz klienta adresou IP pro name.reskit.com.

Všimněte si, že tento příklad platí pouze pro Internet. Více podrobností o rozlišení názvů hostitele DNS, rekurzivních dotazech a iterativních dotazech najdete v této knize v části „Úvod do DNS“.

Chybová hlášení DNS

V případě, že záznamy serveru DNS nebo klient nejsou správně nakonfigurováni, že server DNS neběží nebo že je problém s připojením k síti, se mohou objevit chyby v překladu názvu. K určení příčiny jakéhokoli problému s překladem názvu můžete použít nástroj Nslookup.

Neúspěšné dotazy mohou vrátit množství různých hlášení v závislosti na povaze selhání. Například v případě, že server nemůže přeložit název, vrátí hlášení v následujícím formátu:

```
C:\nslookup <cílový_hostitel>
Server: <úplný_název_domény>
Address: <adresa_IP_serveru>
*** <úplný_název_domény> can't find <cílový_hostitel>: Non-existent domain
```

V dalších případech dotazům na službu DNS vyprší časový limit bez odpovědi a vrátí se hlášení v následujícím formátu:

```
C:\nslookup Valid_Host
Server: [IP_Address]
Address: w.x.y.z
DNS request timed out.
        timeout was 2 seconds.
```

Jestliže server neuspěje při odpovědi na dotaz, nástroj Nslookup vrátí chybové hlášení v následujícím formátu:

```
C:\nslookup
*** Can't find server name for address <IP_Address>: No response from
server
*** Default servers are not available.
```

Toto hlášení značí, že server DNS nelze dosáhnout, ale neuvádí důvody, proč ho nelze dosáhnout. Server může být odpojen, hostitelský počítač může mít zakázanou službu DNS nebo mohou být hardwarové nebo směrovací problémy.

Více podrobností o řešení problémů s DNS najdete v části „Úvod do DNS“ v této knize.

Zkontrolujte soubor LMHOSTS

Problém s překladem názvu může být v souboru LMHOSTS, který vyhledává adresy postupně odshora dolů. Jestliže je v seznamu více než jedna adresa pro stejný název hostitele, protokol TCP/IP vrátí první hodnotu, na kterou narazí, bez ohledu na to, jestli je či není správná.

Soubor LMHOSTS můžete najít v `%SystemRoot%\System32\Drivers\Etc`. Všimněte si, že tento soubor dle výchozího nastavení neexistuje, existuje jen vzorový soubor LMHOSTS.SAM, který je nutno před prvním použitím přejmenovat na LMHOSTS.

Poznámka Zatímco `%SystemRoot%\System32\Drivers\Etc` je přednastavený adresář pro tento soubor, to, který soubor LMHOSTS přesně je použit, závisí na hodnotě záznamu v registru `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\databasepath`. Hodnota database path určuje, kde má lokální počítač soubor LMHOSTS hledat.

Dlouhý čas připojení za použití souboru LMHOSTS

Pro určení příčiny dlouhých časů připojení po přidání záznamu do souboru LMHOSTS se podívejte na pořadí záznamů v souboru LMHOSTS.

Dlouhé časy připojení se mohou objevit v případě, že velký soubor LMHOSTS má určitý záznam na konci souboru. Příklad záznamu urychlíte tak, že označíte záznam v souboru LMHOSTS jako přednahráný záznam mapování záložkou `#PRE` (příklad najdete v části týkající se nástroje Nbtstat v této kapitole). Pak použijte příkaz **nbtstat -R**, kterým okamžitě aktualizujete lokální mezipaměť názvů.

Druhou možností je přemístění mapování v souboru LMHOSTS výše. Jak je uvedeno v příloze „Soubor LMHOSTS“ v této knize, při hledání záznamů bez klíče `#PRE` je soubor LMHOSTS procházen od shora dolů. Proto byste vždy měli umísťovat často používané záznamy na začátek souboru a záznamy s příznakem `#PRE` na konec souboru.

Zkontrolujte konfiguraci WINS

Ověřte si, že konfigurace počítače na server WINS je správná. Zvláště pak ověřte správnost adresy na server WINS.

► Kontrola konfigurace serveru WINS

1. Na **Ovládacích panelech** klepněte na ikonu **Síťová a telefonická připojení**.
2. Klepněte pravým tlačítkem myši na **Připojení k místní síti** a pak vyberte **Vlastnosti**.
3. V dialogovém okně **Vlastnosti připojení k místní síti** vyberte **Protokol TCP/IP** a klepněte na **Vlastnosti**.
4. V dialogovém okně **Vlastnosti protokolu TCP/IP** klepněte na **Upřesnit**.
5. V dialogovém okně **Upřesnit nastavení protokolu TCP/IP** klepněte na záložku **WINS**.

V dialogovém okně **Konfigurace serveru WINS** přidejte adresu IP serveru (pokud tam není žádná) a zkontrolujte, zda je povoleno vyhledávání v souboru LMHOSTS. Zkontrolujte také, jestli je NetBIOS pro TCP/IP přebírán ze serveru DHCP, povolen nebo zakázán. Používáte-li pro tento hostiteleksý počítač server DHCP, převezměte hodnotu ze serveru DHCP. V opačném případě povolte NetBIOS pro TCP/IP.

Nelze dosáhnout adresy IP

Jestliže vypadá překlad názvu jako úspěšný, problém může spočívat v něčem jiném. V tomto případě může být problém jednoduše záležitostí opravy konfigurace protokolu IP spíše než přezkoumání procesu překladu názvu.

Při řešení problémů s protokolem TCP/IP obvykle se používá pevný postup. Obecně řečeno, nejprve ověřte, že konfigurace protokolu TCP/IP na problémovém počítači je správná a pak ověřte pomocí provedení příkazu Ping, že existuje připojení a trasa mezi počítačem a cílovým hostitelem, jak je popsáno v části „Zkontrolujte připojení k síti pomocí nástrojů Ping a PathPing“ dále v této kapitole.

Sestavte seznam, co funguje a co nefunguje, a pak ho použijte k izolaci selhání. Jestliže je pochybná spolehlivost propojení, vyzkoušejte velké množství provedení příkazu Ping různých velikostí v různou denní dobu a vyhodnoťte úspěšnost nebo použijte nástroj PathPing. Jestliže zklame všechno ostatní, použijte analyzátor protokolu, například Microsoft Network Monitor.

Zkontrolujte konfiguraci protokolu TCP/IP pomocí nástroje IPConfig

Při řešení síťových problémů s protokolem TCP/IP nejprve proveďte kontrolu konfigurace protokolu TCP/IP na počítači, který problém vykazuje. Použijte příkaz ipconfig a získáte tak informace o konfiguraci hostitelského počítače, včetně adresy IP, masky podsítě a přednastavené brány.

Použijete-li Ipconfig s využitím všech jeho přepínačů, získáte detailní zprávu o konfiguraci všech rozhraní včetně jakýchkoli nakonfigurovaných adaptérů vzdáleného přístupu. Výstup nástroje Ipconfig lze přesměrovat do souboru a vložit do dalších dokumentů pomocí příkazu ipconfig > <adresář\název souboru>, přičemž výstup je umístěn do určeného adresáře pod zadaným názvem souboru.

Výstup nástroje Ipconfig lze prohlížet a najít tak jakýkoli problém v síťové konfiguraci počítače. Například pokud je počítač nakonfigurován na adresu IP, která je duplikátem již existující a v síti detekované adresy IP, maska podsítě bude znázorněna jako 0.0.0.0.

Následující příklad znázorňuje výsledky příkazu ipconfig/all na počítači, který je nakonfigurován k používání serveru DHCP při automatické konfiguraci protokolu TCP/IP a serverů WINS a DNS při překladu názvu:

```
Windows NT IP Configuration
    Host Name . . . . . : testpcl.reskit.com
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:
    Adapter Domain Name . . . . : dns.reskit.com
    DNS Servers . . . . . : 172.16.14.119
    Description . . . . . : ELNK3 Ethernet Adapter.
    Physical Address. . . . . : 00-20-AF-1D-2B-91
    DHCP Enabled. . . . . : Yes
    IP Address. . . . . : 172.16.48.10
    Subnet Mask . . . . . : 255.255.248.0
    Default Gateway . . . . . : 172.16.48.03
    DHCP Server . . . . . : 172.16.48.03
    Primary WINS Server . . . . : 172.16.48.04
```

```
Secondary WINS Server . . . : 172.16.48.05  
Lease Obtained. . . . . : Sunday, May 2, 1999 11:43:01 PM  
Lease Expires . . . . . : Wednesday, May 5, 1999 11:43:01 PM
```

Jestliže se neobjeví žádné problémy s konfigurací protokolu TCP/IP, je následujícím krokem test schopnosti hostitele se připojit k ostatním hostitelským počítačům na síti TCP/IP.

Zkontrolujte připojení k síti pomocí nástrojů Ping a PathPing

Ping je nástroj, který pomáhá ověřit připojení na úrovni protokolu IP. PathPing je nástroj, který detekuje ztrátu paketů při víceném směrování. Při řešení problémů je příkaz ping používán k odesílání žádostí ICMP Echo Request na cílový název hostitele nebo na adresu IP. Příkaz Ping používejte vždy, když chcete ověřit, že hostitelský počítač může odesílat pakety IP na cílového hostitele. Nástroj Ping lze také používat k izolování hardwarových síťových problémů a nekompatibilních konfigurací.

Poznámka Zavoláte-li `ipconfig/all` a obdržíte odpověď, není třeba provádět příkaz ping na zpětnou smyčku a vlastní adresu IP – nástroj `Ipconfig` tak již učinil, aby mohl vygenerovat zprávu.

Použitím příkazu ping a adresy IP síťového hostitele, ke kterému se chcete připojit, je nejlepší ověřit, že existuje trasa mezi lokálním počítačem a tímto síťovým hostitelem. Syntaxe příkazu je:

ping <adresa IP>

Při použití nástroje Ping provádějte následující kroky:

1. Provedte příkaz Ping na adresu zpětné smyčky, abyste ověřili, že protokol TCP/IP je na lokálním počítači nainstalován a nakonfigurován správně.

```
ping 127.0.0.1
```

Jestliže tento krok selže, zásobník protokolu IP nereaguje. To může být kvůli poškození ovladačů protokolu TCP, nefunkčnosti síťového adaptéru nebo konfliktu jiné služby s protokolem IP.

2. Provedte příkaz Ping na adresu lokálního počítače, abyste ověřili, že tato adresa byla do sítě přidána správně. Všimněte si, že v případě správně směrovací tabulky jednoduše předá paket na adresu zpětné smyčky 127.0.0.1.

```
ping <adresa IP lokálního hostitele>
```

3. Provedte příkaz Ping na adresu výchozí brány, abyste ověřili, že tato výchozí brána je funkční a že můžete komunikovat s lokálním hostitelem na lokální síti.

```
ping <adresa IP výchozí brány>
```

4. Provedte příkaz Ping na adresu vzdáleného hostitele, abyste ověřili, že můžete komunikovat přes směrovač.

```
ping <adresa IP vzdáleného hostitele>
```

5. Provedte příkaz Ping na adresu vzdáleného hostitele, abyste ověřili, že můžete přeložit název vzdáleného hostitele.

```
ping <název vzdáleného hostitele>
```

6. Spusíte analýzu nástrojem PathPing pro vzdáleného hostitele, abyste ověřili, že směrovače na cestě k cílovému umístění fungují správně.

```
pathping <adresa IP vzdáleného hostitele>
```

Poznámka Jestliže je vaše lokální adresa vracena jako 139.254.y.z, máte přiřazenu adresu IP pomocí vlastnosti APIPA operačního systému Windows 2000. To znamená, že lokální server DHCP není nakonfigurován správně nebo není z vašeho počítače dosažitelný a adresa IP byla přiřazena automaticky s maskou podsítě 255.255.0.0. Po volte nebo opravte server DHCP, restartujte lokální počítač a podívejte se, jestli síťový problém stále trvá.

Jestliže se vaše lokální adresa vrací jako 0.0.0.0, software Microsoft MediaSense přepsal výchozí, protože síťový adaptér detekuje, že není připojen k síti. Tento problém opravíte tak, že vypnete MediaSense tím, že se ujistíte, že síťový adaptér a síťový kabel jsou připojeny k rozbočovači. Je-li připojení spolehlivé, nainstalujte znovu ovladač síťového adaptéru nebo nový síťový adaptér.

Nástroj Ping používá k překladu názvu počítače na adresu IP překlad názvu hostitele. Z toho vyplývá, že pokud je provedení příkazu ping na adresu úspěšné, ale je neúspěšné na název, problém leží v překladu názvu hostitele, nikoli v připojení k síti. Více informací o řešení problémů s překladem názvu hostitele najdete v části „Nelze dosáhnout název hostitele nebo název typu NetBIOS“ dříve v této kapitole.

Nelze-li použít příkaz Ping úspěšně v žádném z těchto případů, ověřte si následující:

- Adresa IP lokálního počítače je platná a na záložce Adresa IP v dialogovém okně Vlastnosti protokolu TCP/IP nebo při použití nástroje Ipconfig se zobrazuje správně.
- Je nakonfigurována výchozí brána a propojení mezi hostitelem a výchozí bránou je funkční. Kvůli řešení problémů se ujistěte, že je nakonfigurována pouze jedna výchozí brána. Je-li možné nakonfigurovat více než jednu výchozí bránu, brány za první bránou jsou používány pouze v případě, že zásobník protokolu IP vyřadí, že původní brána nefunguje. Vzhledem k tomu, že účelem řešení problémů je určit stav první nakonfigurované brány, všechny ostatní brány odstraňte, zjednodušíte si řešení problému.

Důležité Jestliže vzdálený systém, na který se provádí příkaz ping, je na propojení s velkou prodlevou, například satelitní propojení, může vrácení odpovědi trvat delší dobu. K prodloužení časového limitu lze použít přepínač -w (wait). Následující příklad ukazuje sadu dvou provedení příkazu ping, každý o velikosti 1450 bajtů, které čekají před vypršením časového limitu na odpověď dvě sekundy (2000 milisekund).

```
C:\>ping -w 2000 -n 2 -l 1450 172.16.48.10
Pinging 172.16.48.10 with 1450 bytes of data:
```

```
Reply from 172.16.48.10: bytes=1450 time=1542ms TTL=32
Reply from 172.16.48.10: bytes=1450 time=1787ms TTL=32
```

```
Ping statistics for 172.16.48.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
```


Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 10ms, Average = 1664ms

Vyčistěte mezipaměť ARP

Jestliže můžete provést příkaz Ping jak na adresu zpětné smyčky, tak na vlastní adresu IP, je dalším krokem vyčištění mezipaměti ARP a její opětovné nahrání. To lze provést pomocí nástroje Arp, přičemž nejprve pomocí příkazu **arp -a** nebo **arp -g** zobrazíte záznamy mezipaměti a příkazem **arp -d <adresa IP>** je vymažete.

Ověřte výchozí bránu

Dále zkontrolujte výchozí bránu. Adresa brány musí být na stejné síti jako lokální hostitel. Pokud tomu tak není, nelze předávat z hostitelského počítače žádné zprávy na jakékoli umístění mimo lokální síť. Zkontrolujte také při vkládání adresy, jestli je adresa výchozí brány správná. Nakonec zkontrolujte, že výchozí brána je směrovač, nikoli pouze hostitel a že má povolené předávání datagramů IP.

Provedte příkaz Ping na vzdáleného hostitele

Jestliže výchozí brána odpovídá správně, proveďte příkaz Ping na vzdáleného hostitele, abyste se ujistili, že mezisíťová komunikace funguje tak, jak má. Jestliže toto selže, použijte k prozkoumání cesty k cíli nástroj Tracert. Pro směrovače IP, které jsou počítači na bázi Windows NT nebo Windows 2000, použijte k prozkoumání směrovací tabulky IP nástroj Route nebo administrátorský nástroj Routing and Remote Access. Pro směrovače IP, které nejsou počítači na bázi Windows NT nebo Windows 2000, použijte k prozkoumání směrovací tabulky IP odpovídající nástroj nebo zařízení.

Nástroj Ping běžně při řešení problémů vrací čtyři chybová hlášení:

Hodnota TTL vypršela při přechodu (Hlášení TTL Expired in Transit)

Počet předání (směrování) potřebný k dosažení cílového umístění je větší než hodnota TTL nastavené odesílajícím hostitelem pro předání paketů. Hodnota TTL pro žádosti ICMP Echo Request je dle výchozího nastavení 32. V některých případech to pro dopravu do cílového umístění nestačí. Hodnotu TTL můžete zvýšit pomocí přepínače -i až na 255.

Jestliže ani zvýšení hodnoty TTL problém nevyřeší, pakety jsou předávány ve směrovací smyčce, která vypadá jako opakující se řada stejných adres IP ve zprávě nástroje Tracert. Proveďte příslušné změny ve směrovací tabulce nebo o problému informujte administrátora vzdáleného směrovače.

Cílový hostitel není dostupný

Toto hlášení označuje jeden ze dvou problémů: buď lokální systém nemá žádnou trasu pro žádané cílové umístění, nebo vzdálený směrovač hlásí, že nemá žádnou trasu pro žádané cílové umístění. Tyto dva problémy lze rozlišit podle formátu hlášení. Jestliže hlášení zní pouze jako „Cílový hostitel není dostupný“, není žádná trasa z lokálního systému a odesílané pakety se z lokálního systému nikdy nedostaly. Ke kontrole lokální směrovací tabulky použijte nástroj Route.

Jestliže hlášení zní jako „Odpověď z <adresa IP>: Cílový hostitel není dostupný“, pak se směrovací problém objevil na vzdáleném směrovači, jehož adresa je určena v poli <adresa IP>. Ke kontrole směrovací tabulky IP směrovače, kterému je přiřazena adresa IP <adresa IP>, použijte odpovídající nástroj nebo zařízení.

Jestliže za použití adresy IP provedete příkaz Ping, proveďte ho znovu za pomoci názvu hostitele, abyste se ujistili, že adresa IP, kterou jste použili, je správná.

Časový limit žádosti vypršel

Toto hlášení značí, že v přednastaveném čase 1 sekundy nebyla obdržena žádná hlášení Echo Reply. To může být kvůli mnoha různým příčinám: nejobvyklejší zahrnují zahlcení sítě, selhání žádosti ARP Request, filtrování paketů, chyba směrování nebo vyřazení bez upozornění. Nejčastěji to znamená, že trasa zpět k odesílajícímu hostiteli selhala. To může nastat kvůli tomu, že cílový hostitel nezná trasu zpět k odesílajícímu hostiteli, jeden ze zprostředkovávajících směrovačů nezná trasu zpět nebo dokonce že přednastavená brána cílového hostitele nezná trasu zpět. Zkontrolujte směrovací tabulku cílového hostitele, jestli tam je trasa na odesílajícího hostitele, pak zkontrolujte tabulky na směrovačích.

Jestliže jsou směrovací tabulky správné a obsahují platné trasy zpět na odesílajícího hostitele, zkontrolujte pomocí příkazu arp -a, který vytiskne obsah mezipaměti ARP, jestli odpovídající adresa nechybí v mezipaměti ARP. Zkontrolujte také masku podsítě a ujistěte se, že vzdálená adresa nebyla vyložena jako lokální.

Dále použijte ke sledování trasy na cílové umístění nástroj Tracert. Jestliže nástroj Tracert nezaznamená adresu posledního předání nebo cestu, kterou paket procházel na cestě zpět, může to znamenat, že paket došel do místa určení. V takovém případě je problém pravděpodobně ve směrování na zpáteční cestě. Jestliže sledování nedosáhne až na místo určení, může to být kvůli tomu, že cílový hostitel je chráněn serverem firewall. Když server firewall chrání cílové umístění, filtrování paketů ICMP zabraňuje paketům příkazu Ping – nebo jakýmkoli dalším zprávám ICMP – projít přes server firewall a dosáhnout místa určení.

Kontrolu zahlcení sítě provedete jednoduchým prodloužením povolené čekací doby pomocí přepínače -w, například na 5000 milisekund. Znovu zkuste provést příkaz Ping na cílové umístění. Jestliže žádosti opět vyprší časový limit, není problémem zahlcení, ale mnohem pravděpodobněji jím je překlad adresy nebo chyba směrování.

Neznámý hostitel

Toto chybové hlášení značí, že požadovaný název hostitele nemůže být přeložen na svou adresu IP. Zkontrolujte, že název byl zadán správně a že ho server DNS může přeložit.

Test překladu adresy IP na adresu MAC pomocí protokolu ARP

Protokol Windows 2000 TCP/IP umožňuje aplikacím komunikovat přes síť s jiným počítačem za použití adresy IP, názvu hostitele nebo názvu typu NetBIOS. Nicméně bez ohledu na použitou konvenci názvů musí být pro média sdíleného přístupu, například Ethernet a Token Ring, cílové umístění přiřazeno hardwarové adrese (adresa MAC).

Protokol ARP umožňuje hostiteli po zadání adresy IP uzlu najít adresu MAC uzlu s adresou IP na stejné fyzické síti. Každý počítač ukládá do mezipaměti ARP mapování adres IP na adresy MAC tak, aby eliminoval opakovaná všesměrová vysílání žádostí ARP a zefektivnil používání protokolu ARP:

Nástroj Arp uživateli umožňuje prohlížet a upravovat záznamy tabulky ARP na lokálním počítači. Příkaz **arp** se používá k prohlížení obsahu mezipaměti ARP a řešení problémů s překladem adres.

Do souboru ARP lze přidat statický záznam za pomoci příkazu **arp -s <adresa IP> <adresa MAC>**. Nicméně je třeba takové statické záznamy přidávat do mezipaměti ARP opatrně, protože může snadno dojít k přiřazení nesprávné adresy MAC adrese IP.

Zjišťování duplikovaných adres IP za pomoci protokolu ARP

Při spuštění operační systém Windows provádí bezplatné volání ARP, aby zjistil jakékoliv duplikace vlastních adres IP. Ačkoli tento postup zjistí většinu duplikovaných adres IP, v několika situacích mohou být dva hostitelé s protokolem TCP/IP (ať už na platformě Microsoft nebo jiné) na stejné síti nakonfigurováni na stejnou adresu IP.

Mapování adres MAC a IP provádí modul protokolu ARP, který používá první přijatou odpověď protokolu ARP. Proto někdy přijde zpět odpověď falešného počítače namísto odpovědi zamýšleného počítače.

Je obtížné tyto problémy izolovat a vystopovat. Ke zobrazení mapování v mezipaměti ARP použijte příkaz **arp -a**. Jestliže znáte adresu Ethernet vzdáleného počítače, kterou chcete použít, můžete snadno určit, jestli souhlasí. Pokud nesouhlasí, odstraňte záznam pomocí příkazu **arp -d** a proveďte na stejnou adresu příkaz **Ping** (vynucuje činnost protokolu ARP) a znovu zkontrolujte adresu Ethernet v mezipaměti pomocí příkazu **arp -a**.

Jestliže jsou oba počítače na stejné síti, nakonec dostanete odpověď od falešného počítače. Pokud ne, možná budete muset zachytit provoz z falešného hostitele prostřednictvím nástroje Network Monitor, abyste určili vlastníka nebo umístění takového systému. Více informací o nástroji Network Monitor najdete v knize *Microsoft® Windows® 2000 Professional Resource Kit* v části „Výkon sledování sítě“.

Zjišťování vadných záznamů v mezipaměti ARP

Řešení problémů s mezipamětí ARP může být jedním z nejtěžších úkolů při správě sítě, protože problémy s ní spojené jsou často nesouvislé.

Výjimkou z tohoto pravidla je to, když zjistíte, že na příkaz (například příkaz **Net use** nebo **Telnet**) reaguje nesprávný hostitel. Příznaky vadného záznamu v mezipaměti ARP je těžší rozpoznat a zahrnují nesouvislé problémy, které ovlivňují pouze některé hostitele. Základním problémem jsou dva počítače používající na jedné síti stejnou adresu IP. Problémy se objevují nesouvisle, protože nejaktuálnější záznam v tabulce ARP je vždy od hostitele, který rychleji reagoval na jakoukoli příslušnou žádost ARP Request.

K určení problému si pomocí příkazu **arp -a** zobrazte tabulku ARP. Zde je uveden příklad výstupu příkazu **arp -a**.

```
C:\>arp -a 172.16.0.142
```

```
Interface: 172.16.0.142
```

Internet address	Physical Address	Type
172.16.0.1	00-e0-34-c0-a1-40	dynamic
172.16.1.231	00-00-f8-03-6d-65	dynamic
172.16.3.34	08-00-09-dc-82-4a	dynamic
172.16.4.53	00-c0-4f-79-49-2b	dynamic
157.59.5.102	00-00-f8-03-6c-30	dynamic

Vzhledem k tomu, že adresy přiřazené serverem DHCP nepůsobí konflikty adres jako adresy zde uvedené, hlavním zdrojem těchto konfliktů jsou pravděpodobně statické ad-

resy IP. Budete-li si udržovat seznam přiřazovaných statických adres (a jim odpovídajících adres MAC), může vám to pomoci při sledování konfliktu adres – porovnejte pouze páry adres IP a MAC z tabulky ARP se zaznamenanými hodnotami.

Nemáte-li záznam všech párů adres IP a MAC na vaší síti, použijte bajty výrobce z adresy MAC a hledejte nesoudržnosti. Tato třibajtová čísla jsou označována jako OUI (Organizationally Unique Identifiers) a jsou přiřazována institutem IEEE (Institute of Electrical and Electronics Engineers). První tři bajty každé adresy MAC identifikují výrobce karty. Víte-li, jaké zařízení jste nainstalovali a porovnáte-li hodnoty získané z příkazu **arp -a**, můžete určit, která statická adresa byla vložena chybně.

Nakonec, pokud zdroj problému neodhalí ani záznam párů adres, ani předpony výrobce, Použijte pro další získání dalších záchytných bodů Prohlížeč události. Například, server DHCP zjistil na síti duplikovanou kartu a odmítl proto žádost počítače o připojení. Další hlášení DHCP a jiná hlášení mohou často pomoci rychle izolovat a vyřešit problém.

Ověřte trvalé záznamy směrovací tabulky

Další oblastí, kterou je nutno prověřit, jsou trvalé záznamy ve směrovacích tabulkách, které lze prohlížet pomocí nástroje Route. Trvalé záznamy jsou přidávány pomocí příkazu `route add -p`. K potvrzení správnosti mapování adres IP na hardwarové adresy použijte příkaz `Arp`. Najdete-li chybu, změňte nesprávný záznam pomocí příkazu `route change`. Chcete-li, aby tato změna byla trvalá, použijte příkaz `route add -p`. Více informací o nástroji Route najdete později v této kapitole v části „Prověření směrovací tabulky pomocí nástroje Route“.

Jestliže je lokální směrovací tabulka správná, problém může být mezi hostitelským a cílovým počítačem. Pro vyhledání zdroje problému na úrovni směrovače použijte nástroj Tracert.

Použijte nástroje Tracert a PathPing

Je-li konfigurace směrovací tabulky správná, může být problém na směrovači nebo na propojení kdekoli na trase. Cestu na cílový počítač můžete sledovat pomocí nástroje Tracert a pomocí nástroje PathPing přesně určíte problém. Více informací o používání nástroje Tracert k prověřování směrovacích tras najdete později v této kapitole v části „Prověření cest pomocí nástroje Tracert“.

Nástroj Tracert použijte, když nemáte žádné připojení ke zkoumanému serveru, protože vám sdělí, kde připojení končí. Nástroj PathPing je užitečnější, když jste připojeni k serveru, ale ztrácí se nebo zpožďují některé pakety. V těchto případech vám nástroj PathPing sdělí, kde přesně se pakety ztrácejí.

Ověřte služby serveru na vzdáleném počítači

Někdy systém nakonfigurovaný jako vzdálená brána nebo směrovač nefunguje jako směrovač. K ověření, že vzdálený počítač, který chcete kontaktovat, je nastaven na předávání paketů, ho můžete buď prověřit vzdáleným správcovským nástrojem (za předpokladu, že je to počítač, který spravujete), nebo se můžete pokusit kontaktovat osobu, která tento počítač udržuje.

Správce odpovědného za vzdálenou síť můžete kontaktovat pomocí databází spravovaných organizací InterNIC. Nejjednodušší je použít nástroj Whois, pomocí kterého získáte jméno odpovídající osoby a informace o kontaktech z databáze InterNIC.

Operační systém Windows 2000 nemá lokální nástroj Whois. Více informací o lokálním nástroji Whois najdete na stránce <http://windows.microsoft.com/windows2000/res-kit/webresources>. Server Whois poskytuje stejnou funkcionalitu původně poskytovanou při použití Telnet.

Zkontrolujte zabezpečení protokolu IP na zahajujícím hostiteli

Zabezpečení IPsec může zvýšit ochranu sítě, ale může také ztížit změny konfigurace sítě nebo řešení problémů. V některých případech může zabezpečení IPsec běžící na zahajujícím hostiteli zkoumaného počítače působit komplikace při připojování ke vzdálenému hostiteli. K určení, zda je toto skutečně zdroj problémů, vypněte zabezpečení IPsec a zkuste spustit požadovanou službu nebo funkci sítě.

Jestliže problém při vypnutých zásadách IPsec vymizí, víte, že za problém je zodpovědné dodatečné břemeno zpracovávání IPsec nebo jeho filtrování paketů. Problém vyřešíte podle následujícího postupu:

► Zabránění agentům zásad zabezpečení IPsec prosazovat IPsec

- Ve **Skupině** nebo **Místních zásadách** klepněte pravým tlačítkem myši na zásady a klepněte na **Nepřirazené**.

Jestliže potřebujete zakázat zásady IPsec pouze pro určitý počítač, můžete zakázat službu agenta zásad protokolu IPsec na tomto počítači.

► Zastavení agenta zásad protokolu IPsec

1. Spustíte modul snap-in služeb.
2. V podokně výsledků služeb dvakrát klepněte na **Agenta zásad protokolu IPsec**.
3. Klepněte na **Zastavit** (nebo **Zakázat**, pokud nechcete, aby se agent zásad znovu po restartu systému spustil).

Více informací o problémech zabezpečení IPsec najdete v této knize v části „Zabezpečení protokolu IP“.

Zkontrolujte filtrování paketů

Jakékoli chyby ve filtrování paketů na zásobníku, směrovači, serveru proxy, službě Routing and Remote Access nebo úrovni zabezpečení IPsec mohou způsobit selhání překladu adresy nebo připojení. K určení, zda je filtrování paketů zdrojem síťových problémů, musíte zakázat filtrování paketů protokolu TCP/IP.

► Zákaz filtrování paketů protokolu TCP/IP

1. Klepněte na Ovládací panely a pak dvakrát klepněte na ikonu **Síťová a telefonická připojení**.
2. Klepněte pravým tlačítkem myši na **Připojení k místní síti** a klepněte na **Vlastnosti**.
3. Vyberte **Protokol TCP/IP** a pak klepněte na záložku **Vlastnosti**.
4. Klepněte na **Upřesnit** a pak na **Možnosti**.
5. Klepněte na **Filtrování protokolu TCP/IP** v okně **Volitelná nastavení** a pak klepněte na záložku **Vlastnosti**.
6. Vyčistěte zaškrtnutí políčka **Povolit filtrování protokolu TCP/IP (pro všechny adaptéry)** a pak klepněte na **OK**.

Zkuste provést příkaz Ping na adresu za použití jejího názvu DNS, názvu typu NetBIOS nebo její adresy IP: Je-li pokus úspěšný, mohou být možnosti filtrování paketů špatně nakonfigurovány nebo mohou být příliš omezující. Například filtrování může dovolovat počítači, aby se choval jako server `www`, ale může zakázat takové nástroje jako Ping nebo vzdálenou správu. Obnovte širší rozsah povolených možností filtrování pomocí změny povolených hodnot portů protokolů TCP, UDP a IP.

Jestliže tato snaha stále není úspěšná, se sítí možná koliduje jiná forma filtrování paketů. Více informací o funkcích filtrování služby Routing and Remote Access najdete v knize *Microsoft® Windows® 2000 Server Internetworking* v části „Směrování jednosměrného vysílání IP“. Více informací o filtrování paketů zabezpečení IPSec najdete v této knize v části „Zabezpečení protokolu IP“.

Řešení problémů směrování IP

Operační systém Windows 2000 podporuje směrování jak na jednodomých, tak na vícedomých počítačích se službou i bez služby Routing and Remote Access. Služba Routing and Remote Access obsahuje směrovací protokol RIP a směrovací protokol OSPF. Směrovače mohou protokoly RIP nebo OSPF používat k dynamické výměně směrovacích informací.

Tato část poskytuje informace o směrovací tabulce na platformě Windows 2000 používané na jednodomých i na vícedomých počítačích se službou i bez služby Routing and Remote Access. Tyto podrobné informace vám pomohou s řešením problémů s protokolem TCP/IP. Více informací o směrování TCP/IP najdete v knize *Microsoft® Windows® 2000 Server Internetworking* v části „Směrování IP jednosměrného vysílání“. Více informací o řešení problémů se směrováním IP vícesměrového vysílání najdete v knize *Microsoft® Windows® 2000 Server Internetworking* části „Podpora vícesměrového vysílání IP“.

Nelze se připojit k zadanému serveru

K určení příčiny problémů s připojením k zadanému serveru pomocí připojení na bázi NetBIOS použijte příkaz **nbstat -n**, který určí, jaký název server použil k registraci na síti.

Výstup příkazu **nbstat -n** obsahuje seznam několika názvů, které má počítač zaregistrované. Měl by tam být i název podobný názvu počítače, který je zobrazen na ploše. Pokud není, zkuste jeden z jedinečných názvů zobrazených nástrojem Ntstat.

Nástroj Ntstat může také zobrazit záznamy mezipaměti pro vzdálené počítače jak ze záznamů souboru LMHOSTS označených #PRE, tak z nedávno přeložených názvů. Jestliže název, který vzdálené počítače používají pro server, je stejný, a tyto ostatní počítače jsou na vzdálené podsíti, ujistěte se, že mají tento počítač namapován v souborech LMHOSTS nebo na serverech WINS.

Připojení ke vzdálenému hostiteli visí

K určení, proč připojení TCP/IP ke vzdálenému počítači nefunguje správně, použijte příkaz **netstat -a**, který ukáže veškerou aktivitu na portech TCP a UDP lokálního počítače.

Dobré připojení TCP zpravidla ukazuje 0 bajtů ve frontách Odesláno a Přijato. Jestliže jsou data v kterékoli frontě blokována nebo jestliže je stav nepravdivý, připojení je pravděpodobně vadné. Pokud ne, dochází pravděpodobně k prodloužení sítě nebo aplikace.

Prověření směrovací tabulky pomocí nástroje Route

Aby byli dva hostitelé schopni si vyměňovat IP datagramy, musí mít oba trasu na druhého účastníka nebo používat přednastavené brány, které trasu znají. Normálně si navzájem směrovače vyměňují informace za pomoci směrovacího protokolu, například protokolu RIP.

Povolení směrování IP

Dle výchozího nastavení je směrování IP zakázáno. K povolení směrování IP musíte umožnit počítači předávání přijatých paketů IP. To vyžaduje změnu v registru systému Windows 2000. Povolíte-li pro směrování IP službu Routing and Remote Access, je tento záznam v registru proveden automaticky.

► Povolení směrování IP

1. V menu **Start** klepněte na **Spustit**.
2. Napište **regedt32.exe** nebo **regedit.exe** a pak klepněte na **OK**.
3. V editoru registru přejděte na HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.
4. Vyberte záznam **IPEnableRouter**.
5. K povolení směrování IP pro všechna síťová připojení instalovaná a používaná tímto počítačem přiřadíte hodnotu 1. V souboru regedit.exe tohoto dosáhnete tak, že pravým tlačítkem myši klepnete na záznam a pak klepnete na **Změnit**. V souboru regedt32.exe klepněte na požadovaný záznam, klepněte na Upravit a pak klepněte na příslušný výběr z menu.
6. Zavřete editor registru.

Upozornění Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správcovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. Ke konfiguraci nebo přizpůsobení si Windows 2000 používejte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Jestliže směrovač Windows 2000 nemá na dané podsíti rozhraní, potřebuje na tuto podsít trasu. To lze zařídit pomocí výchozí cesty nebo pomocí přidání statické trasy. Více informací o prostředích dynamického směrování najdete v knize *Microsoft® Windows® 2000 Server Networking* v části „Směrování IP jednosměrného vysílání“.

K přidání statické trasy použijte nástroj Route, viz dále:

```
route add 172.16.41.0 mask 255.255.255.0 172.16.40.1 metric 2
```

V tomto příkladě příkaz route add stanoví, že k dosažení podsítě 172.16.41.0 s maskou 255.255.255.0 se použije brána 172.16.40.1. Také ukazuje, že podsít je vzdálena dvě předání. Možná bude třeba přidat statické trasy na směrovače po proudu toku dat, které by řekly tamním paketům, jak se dostat zpět na podsít 172.16.40.0/24.

Prověření cest pomocí nástroje Tracert

Nástroj Tracert je nástroj určená ke sledování trasy, která používá vzrůstající hodnotu TTL v hlavičce IP, aby určila trasu přes síť od jednoho hostitele k druhému. Činí tak prostřednictvím odesílání žádostí ICMP Echo Request a analýzy chybových hlášení ICMP, která se vrátí. Nástroj Tracert umožňuje sledovat cestu předaného paketu ze směrovače na směrovač až do 30 předání. Jestliže směrovač selže nebo paket je směrován ve smyčce, nástroj Tracert tento problém odhalí. Jakmile je nalezen problémový směrovač, lze kontaktovat jeho správce, je-li to směrovač mimo pracoviště, nebo lze obnovit plnou funkčnost směrovače, je-li to směrovač pod vaší správou.

Řešení problémů s bránami

Jestliže během instalace uvidíte hlášení „Vaše výchozí brána nenáleží ani k jednomu z nakonfigurovaných rozhraní...“, najděte, jestli je výchozí brána umístěna na stejné logické síti jako síťový adaptér počítače. Nejjednodušší je porovnat ID sítě adresy IP výchozí brány s ID sítě síťového adaptéru počítače. Jinak řečeno, zkontrolujte, že logický součin mezi bity adresy IP a masky podsítě se rovná logickému součinu mezi bity výchozí brány a masky podsítě.

Například počítač s jedním síťovým adaptérem nakonfigurovaným na adresu IP 172.16.27.139 a maskou podsítě 255.255.0.0 vyžaduje výchozí bránu ve formátu 172.16.y.z. ID sítě rozhraní IP je 172.16.0.0/16. Za pomoci masky podsítě může protokol TCP/IP určit, že veškerý provoz na této síti je lokální, všechno ostatní musí být odesláno na bránu.

Řešení problémů protokolu ARP

Síťový provoz někdy selže, protože požadavek ARP serveru proxy směrovače vrátí špatnou adresu. Směrovač provádí svůj požadavek ARP Request jménem adresy IP na vlastní podsíti (právě tak jako server vzdáleného přístupu provádí svůj požadavek na lokální síti pro své klienty vzdáleného přístupu). Problém je, že požadavek ARP serveru proxy směrovače vrátí odesílajícímu hostiteli špatnou adresu MAC. Výsledkem je, že odesílající hostitel posílá svůj provoz na špatnou adresu MAC. Jinak řečeno, problém vzniká z odpovědi ARP Reply serveru proxy.

Při určování tohoto problému použijte k zachycení trasování Network Monitor. Trasování může odhalit, že odesílající hostitel posílá požadavek ARP Request na adresu MAC cílové adresy IP a zařízení (zpravidla směrovač) odpoví adresou MAC jinou než je správná adresa MAC cíle.

K určení, jestli se jedná o tento případ, zkontrolujte mezipaměť ARP zdrojového hostitele a ujistěte se, že provádí správně překlad adresy IP adresy MAC. Anebo můžete zaznamenat veškerý provoz pomocí Network Monitor a pak odfiltrovat provoz tak, aby se zobrazily pouze protokoly ARP a RARP. Protokol RARP převádí adresy MAC na adresy IP a je definován v dokumentu RFC 903.

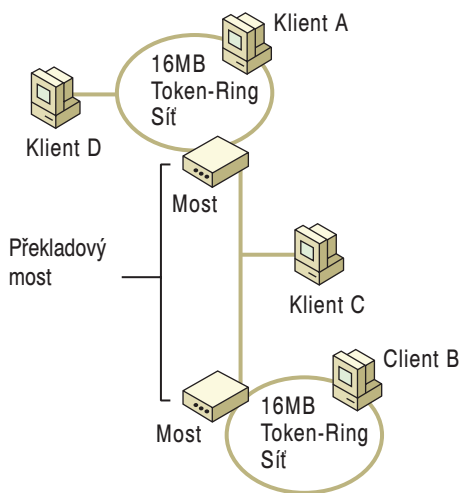
Problémy protokolu ARP můžete spravit zakázáním „Proxy ARP“ na kolidujícím zařízení. Přesný způsob provedení závisí na typu a značce zařízení, použijte dokumentaci dodávanou výrobcem.

Řešení problémů překladového přemostění

Povolení komunikace uzlů ze segmentů Ethernet s uzly na síti Token Ring, představuje řadu problémů. Toto jsou nejobvyklejší problémy spojené s překladovým přemostěním.

Hlavním faktorem odpovědným za problémy jsou odlišné hodnoty MTU mezi segmenty. Hodnoty MTU sítě Token Ring jsou v rozsahu 4464 až 17914 bajtů, zatímco hodnota MTU sítě Ethernet je 1500. Segment rozhraní FDDI má hodnotu MTU 4531 bajtů. Když most nebo přepínač vrstvy 2 spojí dvě z těchto rozdílných technologií, může docházet k vyřazení paketů, protože přepínač vrstvy 2 neumí fragmentovat data a neumí upozornit odesílající uzel na sníženou MTU.

V příkladu znázorněném na obrázku 3.6 spojuje páteř Ethernet dvě sítě Token Ring 16MB. Místo směrovače spojuje segmenty překladový most ve formě přepínače vrstvy 2. V tomto případě používá provoz na síti Token Ring MTU o hodnotě 17914 a není ovlivněn mostem. Nicméně když počítač A musí komunikovat s počítačem B, most vyřazuje velké pakety bez upozornění počítače A na nutnost fragmentace. V této situaci počítač A nemá žádný způsob, jak se dozvědět hodnotu MTU na druhé straně mostu.



Obrázek 3.6 Spojení dvou sítí Token Ring s mostem Ethernet

Další příznaky problémů překladového přemostění mohou zahrnovat schopnost provést příkaz Ping na počítač na vzdálené straně mostu, schopnost vytvořit připojení, ale neschopnost posílat rozměrná data. Důvodem je to, že hlášení Echo Request a segmenty ustavující připojení TCP jsou malé. Při odesílání velkého množství dat jsou ale posílány velké segmenty o velikosti MTU lokálně připojené sítě a jsou vyřazovány přepínačem vrstvy 2. Dalším příkladem je to, že počítač je schopen k vytvoření relace použít protokol FTP, ale není schopen použít příkaz `get <název souboru>`, který je potřeba pro odeslání velkého paketu přes přepínač.

V operačním systému Windows 2000 může být záznam v registru **MTU** upraven tak, aby odpovídal požadavkům MTU segmentu Ethernet spojujícího dva segmenty Token Ring tím, že sníží všechny MTU na nejnižšího obvyklého jmenovatele. Jednotka MTU každého uzlu je snížena na 1500, aby odpovídala požadavkům páteře Ethernet. Nicméně

ně toto řešení požaduje posílání veškerého provozu (dokonce i lokálního provozu na síti Token Ring) se sníženou jednotkou MTU.

Používání nástroje Ping pro určení jednotky MTU

K posílání paketů s definovanou velikostí dat ICMP Echo Request můžete v operačním systému Windows 2000 používat příkaz `ping -l`. Odesláním paketů různých velikostí a sledováním, jak velké pakety přejdou úspěšně přes most, můžete určit jednotku MTU pro jakýkoli daný most. Například na obrázku 3.6 může být z počítače A na počítač C odeslán paket příkazu Ping o velikosti 1472, který generuje paket Echo Reply z počítače C. Nicméně pokud je použit paket o velikosti 1473 bajtů a větší, zprostředkující přepínač tento paket vyřadí. Počítač C žádný požadavek Echo Request neobdrží a žádnou odpověď Echo Reply nevygeneruje.

Přednastavený požadavek ICMP Echo Request obsahuje 32 bajtů dat. K zadání jiné velikosti dat použijte příkaz **ping** *<adresa IP nebo název hostitele> -l <velikost dat>*. Například můžete provést příkaz Ping s maximální velikostí dat pro síť Ethernet pomocí tohoto příkazu:

```
ping 134.56.78.1. -l 1472
```

Velikost dat určená přepínačem `-l` je 1472 namísto jednotka MTU síť Ethernet 1500, protože 20 bajtů je vyhrazených pro hlavičku IP a 8 bajtů musí být přiděleno hlavičce požadavku ICMP Echo Request.

Po určení jednotky MTU můžete nastavit velikost paketu na kterékoli straně mostu prostřednictvím změny hodnoty záznamu registru. Záznam MTU v registru najdete v:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\  
Tcpip\Parameters\Interfaces\Adapter_GUID
```

Více informací o jednotce MTU najdete v této knize v části „Windows 2000 TCP/IP“

Řešení problémů jednotky PMTU směrovačů projevujících se jako černé díry

Některé směrovače neposílají zprávy „Destination Unreachable protokolu ICMP“, když nemohou předat datagram IP. Namísto toho tento datagram ignorují. Typicky, datagram IP nemůže být předán, protože jeho maximální velikost segmentu je pro přijímající server příliš velká a v hlavičce datagramu je nastaven bit Don't Fragment. Směrovače, které ignorují tyto datagramy a neposílají žádné zprávy, se nazývají směrovače projevující se jako černé díry.

K účinné reakci na směrovače projevující se jako černé díry musíte povolit vlastnost Path MTUBH Detect protokolu TCP/IP. Vlastnost Path MTUBH Detect rozpoznává opakované nepotvrzené přenosy a reaguje vypnutím bitu Don't Fragment. Po úspěšném přenosu datagramu se sníží maximální velikost segmentu a znovu se zapne bit Don't Fragment.

Dle výchozího nastavení je vlastnost Path MTUBH Detect zakázána, ale můžete ji povolit přidáním záznamu **EnablePMTUBHDetect** do registru a nastavením jeho hodnoty na 1. Záznam **EnablePMTUBHDetect** je volitelný, který se v registru objeví teprve poté, co ho tam přidáte. Musíte ho umístit do: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`.

Vlastnost Path MTUBH Detect můžete zakázat odstraněním záznamu `EnablePMTUBHDetect` z registru nebo nastavením jeho hodnoty na 0.

Druhý záznam registru, **EnablePMTUDiscovery**, také pomáhá určit problém se směrovači projevujícími se jako černé díry. Tento klíč je dle výchozího nastavení povolen. Záznam **EnablePMTUDiscovery** úplně povoluje nebo zakazuje mechanismus zjištění jednotky PMTU. Je-li zjištění PMTU zakázáno, je pro všechny nelokální cílové adresy použita MSS (Maximum Segment Size) protokolu TCP o velikosti 536 bajtů.

Zjištění jednotky PMTU pomocí provedení příkazu Ping

Jednotku PMTU mezi dvěma hostiteli lze zjistit ručně prostřednictvím příkazu ping - f, viz níže:

```
ping -f -n <number of pings> -l <size> <destination IP address>
```

Následující příklad ukazuje, jak lze měnit parametr velikosti paketu pro provedení příkazu Ping až do nalezení jednotky MTU. Všimněte si, že parametr velikost paketu pro provedení příkazu Ping určuje pouze velikost odesílaných dat požadavku ICMP Echo Request bez hlavičky IP a bez hlavičky požadavku ICMP Echo Request. Hlavička požadavku ICMP Echo Request je 8 bajtů a hlavička IP je normálně 20 bajtů. V případě sítě Ethernet, jak je zde uveden, jednotka MTU vrstvy připojení obsahuje vyrovnávací paměť příkazu Ping maximální velikosti plus 28, takže celkem to je 1500 bajtů při prvním provedení příkazu Ping a 1501 při druhém:

```
C:\>ping -f -n 1 -l 1472 10.99.99.10
Pinging 10.99.99.10 with 1472 bytes of data:
Reply from 10.99.99.10: bytes=1472 time<10ms TTL=128
Ping statistics for 10.99.99.10:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping -f -n 1 -l 1473 10.99.99.10
Pinging 10.99.99.10 with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Ping statistics for 10.99.99.10:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Při druhém provedení příkazu Ping vrstva protokolu IP vrací chybové hlášení ICMP, které příkaz Ping interpretuje. Jestliže je směrovač směrovačem, který se projevuje jako černá díra, jakmile velikost paketu příkazu Ping přesáhne jednotku MTU, kterou je schopen směrovač ovládat, nepřijde žádná odpověď. Příkaz Ping lze tímto způsobem použít k vyhledání takových směrovačů.

Služby pro řešení problémů

Protokol TCP/IP je základní kámen celé řady síťových služeb, například Routing and Remote Access, tisk, zabezpečení protokolu IP a služba prohledávače. Těmto službám jsou podrobně věnovány jiné kapitoly, ale zde je uvedeno několik příkladů základního použití těchto služeb při řešení problémů.

Nelze provést příkaz Ping přes směrovač jako klienta vzdáleného přístupu

Tento problém se objeví, když vyberete **Používat výchozí bránu vzdálené sítě** v záložce **Obecné** v dialogovém okně **Upřesnit vlastnosti protokolu TCP/IP** na stránce **Telefonická přípojení**. Tato vlastnost přidá do směrovací tabulky přednastavenou cestu s metrikou 1 a změní metriku existující přednastavené cesty na 2. Veškerý lokální provoz je nyní předáván na bránu na propojení vzdáleného přístupu. K přístupu na síť Internet musí být tato vlastnost povolena.

Když jste připojeni ke klientovi se vzdáleným přístupem k serveru na bázi Windows se vzdáleným přístupem, použijte k provedení příkazu Ping nebo k jakémukoli připojení k počítačům na vzdálené podsíti přes směrovač příkaz **route add**, kterým přidáte trasu podsítě, kterou chcete použít.

Řešení problémů databázových souborů protokolu TCP/IP

Tabulka 3.13 obsahuje seznam unixových databázových souborů, které jsou při instalaci protokolu Microsoft TCP/IP uloženy v adresáři %SystemRoot%\System32\Drivers\Etc:

Tabulka 3.13 Databázové soubory protokolu TCP/IP

Název souboru	Použití
Hosts	Poskytuje překlad názvů k adresám IP pro aplikace Windows Sockets
LMHOSTS	Poskytuje překlad vzdálených názvů typu NetBIOS k adresám IP pro aplikace typu NetBIOS, například síť na bázi Windows
Networks	Poskytuje překlad názvů sítě k ID sítě pro správu protokolu TCP/IP
Protocols	Poskytuje překlad názvů protokolu k ID protokolu pro aplikace Windows Sockets
Services	Poskytuje překlad názvů služby k ID portu pro aplikace Windows Sockets

Před řešením problémů s kterýmkoli z těchto souborů na lokálním počítači se ujistěte, že formát záznamů v každém souboru odpovídá formátu definovanému ve vzorovém souboru nainstalovaném společně s protokolem TCP/IP. Zkontrolujte chyby v psaní, nesprávné adresy IP a identifikátory.

Odebrání a opětná instalace protokolu TCP/IP

Pokoušíte-li se znovu nainstalovat službu protokolu TCP/IP, můžete obdržet chybové hlášení „Podklíč registru již existuje“ („The registry subkey already exists“). Tento problém opravíte tak, že se ujistíte, že všechny součásti dané služby protokolu TCP/IP jsou řádně odebrány a pak odeberete příslušné podklíče registru.

Upozornění Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správcovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. Ke konfiguraci nebo přizpůsobení si Windows

2000 používejte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Jestliže jste odebrali protokol TCP/IP a s ním spojené služby, musíte také odebrat následující podklíče registru:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpipCU

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dhcp

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LmHosts

Klíče registru služby SNMP

Jestliže jste odebrali součásti služby SNMP, musíte také odebrat následující podklíče registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RFC1156Agent

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Snmp

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Snmp

Klíče registru služby TCP/IP Printing

Jestliže jste odebrali součásti služby TCP/IP Printing, musíte také odebrat následující podklíče registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Lpdsvc

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TcpPrint

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LpdsvcSimple TCP/IP Services

Klíče registru služby Simple TCP/IP Services

Jestliže jste odebrali součásti služby Simple TCP/IP Services, musíte také odebrat následující podklíče registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SimpTcp

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SimpTcp

Klíče registru služby DHCP

Jestliže jste odebrali součásti služby DHCP, musíte také odebrat následující podklíče registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DhcpMibAgent

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DhcpServer

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DhcpServer

Klíče registru služby WINS

Jestliže jste odebrali součásti služby WINS, musíte také odebrat následující podklíče registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wins

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WinsMibAgent

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Wins

Klíče registru služby DNS

Jestliže jste odebrali součásti služby DNS, musíte také odebrat následující podklíče registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dns

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DnsMibAgent

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dns

Další informace

- Více informací o protokolu TCP/IP najdete v knize *Internetworking with TCP/IP: Volume 1 Principles, Protocols, and Architectures* by Douglas E. Comer, 1995, Englewood Cliffs, New Jersey: Prentice Hall a v knize *TCP/IP Illustrated, Vol. 1* by W. Richard Stevens, 1994, Reading, Massachusetts: Addison-Wesley.
- Více informací o řešení problémů protokolu TCP/IP najdete v knize *Windows NT TCP/IP Network Administration* by Craig Hunt and Robert Bruce Thompson, 1998, Sebastopol, California: O'Reilly.

ČÁST II

Přidělování adres a překlad názvu



Protokoly, které umožňují efektivní správu a automatickou konfiguraci síťových hostitelů, jsou nezbytnými nástroji pro správce a administrátory rozsáhlých sítí. Tato část se zabývá vlastnostmi operačního systému Windows 2000, které zajišťují tyto nezbytné funkce.

V této části najdete:

Protokol DHCP 157

Úvod do DNS 239

Služba Windows 2000 DNS 267

Služba Windows Internet Name Service 389

4. KAPITOLA

Protokol DHCP



Protokol DHCP je standardem TCP/IP, který omezuje složitost a nákladnost spravování konfigurace adres IP síťových klientů. Operační systém Microsoft® Windows® 2000 Server poskytuje službu DHCP, která umožňuje počítači, aby fungoval jako server DHCP a aby konfiguroval klientské počítače s povoleným protokolem DHCP na síti. Protokol DHCP běží na serveru, přičemž umožňuje automatickou a centralizovanou správu adres IP a dalších nastavení protokolu TCP/IP pro klientský počítač na síti. Služba Microsoft DHCP Service také poskytuje integraci s adresářovou službou Active Directory™ a službou DNS, vylepšené sledování a statistická hlášení pro servery DHCP, možnosti konkrétního výrobce a podporu uživatelských tříd, přiřazování adres víceměrového vysílání a rozpoznávání nepřátelských serverů DHCP.

V této kapitole najdete:

Co je to protokol DHCP?	158
Proces zápůjčky DHCP	163
Správa oborů	172
Předcházení konfliktům adres	178
Správa možností DHCP	179
Protokol DHCP s víceměrovým vysíláním	187
Databáze DHCP	189
Podpora klientů BOOTP	192
Plánování pro protokol DHCP	195
Scénáře služby DHCP	207
Řešení problémů	221

Další informace v sadě Resource Kit

- Více informací o zavádění protokolu DHCP se službou zabezpečení protokolu IP najdete v této knize v části „Zabezpečení protokolu IP“.
- Více podrobností o možnostech protokolu DHCP najdete v této knize v části „Správa možností DHCP“.
- Více informací o formátech hlášení protokolu DHCP najdete v této knize v části „Zprávy DHCP“.
- Více informací o úpravě nastavení registru protokolu DHCP najdete na příloženém Windows 2000 Resource Kit CD v souboru „Technické odkazy na registr Windows 2000“ (Regentry.chm).

Co je to protokol DHCP?

Protokol DHCP zjednodušuje správu konfigurace adresy IP pomocí automatického konfigurování adres pro síťové klienty. Standard protokolu DHCP zajišťuje používání serverů DHCP, které jsou definovány jako jakýkoli počítač, na němž běží služba DHCP. Server DHCP automaticky přiřazuje adresy IP a podobná nastavení konfigurace protokolu TCP/IP počítačů na síti podporujících protokol DHCP.

Každé zařízení na síti založené na protokolu TCP/IP musí mít jedinečnou adresu IP, aby bylo schopno přistupovat k síti a jejím prostředkům. Bez protokolu DHCP je nutno provést nakonfigurování protokolu IP ručně u nových počítačů, počítačů přesunovaných z jedné podsítě na jinou a počítače odebírané ze sítě.

Po zavedení služby DHCP do sítě probíhá celý tento proces automaticky a je spravován centrálně. Server DHCP spravuje fond adres IP a zapůjčuje adresu jakémukoli klientovi podporujícímu službu DHCP při jeho přihlášení do sítě. Vzhledem k tomu, že adresy IP jsou dynamické (zapůjčované) místo než statických (trvale přiřazené), jsou momentálně nepoužívané adresy automaticky vráceny do fondu adres IP k opětovnému přiřazení.

Služba DHCP pro operační systém Microsoft Windows 2000 Server je založena na standardech IETF (Internet Engineering Task Force). Specifikace služby DHCP jsou definovány v dokumentech RFC vydávaných IETF a dalšími pracovními skupinami. Dokumenty RFC jsou vyvíjející se sadou zpráv, návrhů protokolů a standardů protokolů používanou Internetovou veřejností. Jádro standardů protokolu DHCP podporované službou Microsoft DHCP specifikují tyto dokumenty RFC:

- RFC 2131: Protokol DHCP (ruší dokument RFC 1541)
- RFC 2132: Možnosti protokolu DHCP a rozšíření výrobců BOOTP

Terminologie protokolu DHCP

Tabulka 4.1 obsahuje seznam obvyklých termínů protokolu DHCP, které jsou používány v této kapitole.

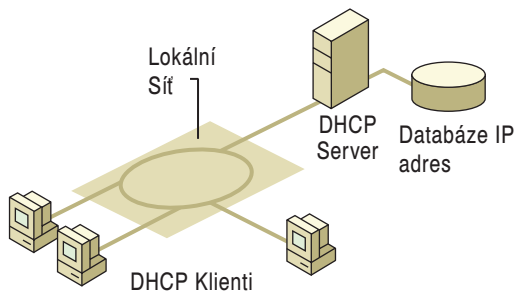
Tabulka 4.1 Terminologie DHCP

Termín	Popis
Server DHCP	Jakýkoli počítač, na kterém je spuštěna služba Windows 2000 DHCP.
Klient DHCP	Jakýkoli počítač, který podporuje nastavení služby DHCP.
Obor	Plný, nepřetržitý rozsah adres IP možných pro síť. Služby DHCP mohou být nabízeny rozsahům, které zpravidla definují jednotlivou fyzickou podsít na síti. Servery DHCP primárně používají obory ke správě distribuce sítě a přiřazování adres IP a jakýchkoli obdobných parametrů konfigurace.
Množina oborů	Administrativní seskupení oborů, které jsou použity k podpoře více logických podsítí IP na stejné fyzické podsíti. Množiny oborů obsahují seznam členských oborů (nebo také podřízených oborů), které mohou být aktivovány jako celek.
Rozsah vyloučení	Zajišťuje, že jakákoli adresa IP zařazená v tomto rozsahu není nabízena službou DHCP jakémukoli klientovi DHCP.

Termín	Popis
Fond adres	Dostupné adresy IP tvoří v rámci oboru fond adres. Adresy ve fondu adres jsou dostupné pro dynamické přiřazování serverem DHCP klientům DHCP.
Zápůjčka	Doba určená serverem DHCP, po kterou může klientský počítač používat dynamicky přiřazenou adresu IP. Po zapůjčení adresy je zápůjčka aktivní. Před vypršením zápůjčky klient obnoví svou zápůjčku u serveru DHCP. Zápůjčka je neaktivní v případě, že vyprší nebo je odebrána serverem. Doba trvání zapůjčení určuje, kdy zápůjčka vyprší a jak často klient potřebuje obnovovat svou zápůjčku od serveru DHCP.
Rezervace	Vytváří trvalé přiřazení zápůjčky adresy od serveru DHCP klientovi. Rezervace zajišťují, že určité hardwarové zařízení na podsíti může vždy používat stejnou adresu IP. To je užitečné pro některé počítače, například brány vzdáleného přístupu nebo servery WINS nebo DNS, které musí mít statickou adresu IP.
Typy možnosti	Další parametry konfigurace klienta, které může přiřazovat server DHCP při nabízení zápůjčky adresy IP klientovi. Typicky jsou tyto typy možnosti povoleny a konfigurovány pro každý obor. Většina možností je předdefinována v dokumentu RFC 2132, ale k definování a přidání upravených typů možnosti můžete použít správce služby DHCP.
Třída možnosti	Způsob, jakým server DHCP dále spravuje typy možnosti poskytnuté klientům. Třídy možnosti jsou přidávány na server, klienti této třídy mohou využívat pro svou konfiguraci typů možnosti specifických pro tuto třídu.

Jak funguje protokol DHCP

Protokol DHCP je založen na modelu klient/server, jak je znázorněno na obrázku 4.1.



Obrázek 4.1 Základní model protokolu DHCP

Správce sítě zakládá jeden nebo více serverů DHCP, které udržují informace o konfiguraci protokolu TCP/IP a poskytují konfiguraci adres klientům podporujícím službu DHCP ve formě nabídky zápůjčky. Server DHCP uchovává informace o konfiguraci v databázi, která zahrnuje:

- Parametry konfigurace protokolu TCP/IP platné pro všechny klienty na síti.

- Platné adresy IP udržované ve fondu adres pro přiřazení klientům, stejně jako adresy vyhrazené pro ruční přiřazení.
- Doba trvání zápůjčky nabízená serverem – doba, po kterou může být adresa IP používána před nutností obnovení zápůjčky.

Klient podporující službu DHCP při přijetí nabídky zápůjčky obdrží:

- Platnou adresu IP pro síť, ke které se připojuje.
- Další parametry konfigurace protokolu TCP/IP, které se označují jako možnosti DHCP.

Výhody protokolu DHCP

Instalací protokolu DHCP na svou rozlehlou síť získáte následující výhody:

- **Bezpečnou a spolehlivou konfiguraci.** Protokol DHCP minimalizuje chyby v konfiguraci způsobené manuální konfigurací adres IP, například chyby v psaní, stejně jako minimalizuje konflikty adres způsobené přiřazením již aktuálně používané adresy IP dalšímu počítači.
- **Sníženou správu sítě.**
 - Konfigurace protokolu TCP/IP je centralizovaná a automatizovaná.
 - Správci sítě mohou centrálně definovat konfigurace protokolu TCP/IP jak obecně, tak pro konkrétní podsítě.
 - Klientům lze automaticky přiřazovat plný rozsah dalších konfiguračních hodnot protokolu TCP/IP pomocí možností DHCP.
 - Změny adres pro konfigurace klienta, které musí být často aktualizovány, například klienti se vzdáleným přístupem, kteří se neustále pohybují, lze provádět efektivně a automaticky při spuštění klienta ze svého nového umístění.
 - Většina směrovačů může předat požadavky na konfiguraci pomocí služby DHCP, čímž se omezují požadavky na nastavení serveru DHCP na každé podsíti, pokud k tomu není důvod.

Nové vlastnosti

Služba Windows 2000 DHCP poskytuje následující nové vlastnosti:

- Do operačního systému Windows 2000 Server byly přidány čítače New System Monitor disponující vylepšeným sledováním výkonu a zprávami o serveru, které speciálně sledují výkon serveru DHCP na vaší síti. Navíc správce služby DHCP nyní poskytuje vylepšené poskytování zpráv prostřednictvím grafického zobrazení aktuálního stavu serverů, oborů a klientů. Například ikony ukazují, jestli je server odpojen, nebo jestli zapůjčil více než 90 procent dostupných adres.
- Rozšířená podpora pro obory a množiny oborů vícesměrového vysílání.

Obory vícesměrového vysílání nyní umožňují aplikacím uvědomovaným vícesměrovým vysíláním zapůjčovat adresy IP třídy D (224.0.0.0 až 239.255.255.255) pro účast ve skupinách vícesměrového vysílání.
- Podpora možností DHCP konkrétního uživatele a konkrétního výrobce

To umožňuje oddělení a rozšíření možností pro klienty s podobnými nebo zvláštními potřebami konfigurace. Například, všem klientům podporujícím službu DHCP na stejném podlaží budovy byste mohli přiřadit stejnou třídu možností. Mohli byste tuto třídu používat (nakonfigurovanou se stejnou hodnotou ID třídy DHCP) k distribuci dalších volitelných dat během procesu zápůjčky, čímž by se převážily všechny možnosti oboru nebo obecného výchozího nastavení.

- **Integrace protokolu DHCP se službou DNS**
Server DHCP může umožnit dynamickou aktualizaci oboru názvů DNS pro jakéhokoli klienta DHCP, který podporuje tuto aktualizaci. Klienti oborů mohou používat službu DNS s dynamickou aktualizací pro aktualizaci jejich informací o mapování názvů adresám IP, jakmile se změní jejich adresa přiřazená serverem DHCP.
- **Rozpoznávání nepřátelských serverů DHCP**
To zabraňuje nepřátelským (neautorizovaným) serverům DHCP připojit se k existující síti DHCP, kde jsou nainstalovány operační systém Windows 2000 Server a Active Directory. Objekt serveru DHCP je vytvořen ve službě Active Directory, která má seznam adres IP serverů oprávněných k poskytování služeb DHCP síti. Když se server DHCP snaží na síti začít fungovat, je poslán dotaz na službu Active Directory a adresa IP serveru je porovnána se seznamem oprávněných serverů DHCP. Jestliže je nalezen odpovídající záznam, je server autorizován jako server DHCP a je mu povoleno dokončit spuštění. Jestliže není nalezen odpovídající záznam, server je identifikován jako nepřátelský a služba DHCP se automaticky vypne.
- **Dynamická podpora klientů BOOTP**
Dynamic BOOTP je rozšíření protokolu BOOTP, který povoluje serveru DHCP konfigurovat klienty BOOTP bez nutnosti použít jednoznačnou konfiguraci pevné adresy. Tato vlastnost redukuje správu rozsáhlých sítí BOOTP umožněním automatické distribuce adres IP v podstatě stejným způsobem jako u DHCP.
- **Přístup do správce služby DHCP přes konzolu pouze pro čtení**
Tato vlastnost poskytuje lokální skupinu se zvláštním určením, skupinu uživatelů služby DHCP, která je automaticky přidávána při instalaci služby DHCP: Přidáním členů do této skupiny můžete poskytnout přístup pouze ke čtení k informacím spojeným se službou DHCP na serveru. Za pomoci správce služby DHCP mohou uživatelé v této skupině prohlížet, ale nikoli měnit, informace a vlastnosti uložené na daném serveru DHCP.

Podpora klienta služby DHCP

Pojem *klient* je použit k popisu počítače připojeného k síti, který posílá požadavky na služby DHCP a používá služby DHCP nabízené serverem DHCP. Jakýkoli počítač na platformě Windows nebo jiné zařízení podporující připojení k síti, které podporuje schopnost komunikovat se serverem DHCP (v souladu s dokumentem RFC 2132), může být nakonfigurován jako klient DHCP.

Podpora klienta DHCP je poskytována počítačům běžícím na platformě některého z následujících operačních systémů společnosti Microsoft:

- Microsoft® Windows NT® Workstation (všechny uvolněné verze)
- Microsoft® Windows NT® Server (všechny uvolněné verze)
- Microsoft® Windows® 98
- Microsoft® Windows® 95
- Microsoft® Windows® for Workgroups verze 3.11 (s nainstalovaným 32bitovým protokolem Microsoft TCP/IP VxD)
- Microsoft® Network Client verze 3.0 pro MS-DOS (s nainstalovaným ovladačem protokolu TCP/IP v reálném režimu)
- LAN Manager verze 2.2c

Autokonfigurace protokolu IP

Klienti na platformě Windows si mohou automaticky nakonfigurovat adresu IP a masku podsítě v případě, že je server DHCP v okamžiku spuštění systému nedostupný. Tato vlastnost nazvaná APIPA (Automatic Private IP Addressing) je užitečná pro klienty na malých soukromých sítích, například doma, v malých kancelářích nebo na klientovi se vzdáleným přístupem.

Při autokonfiguraci klienta Windows 2000 DHCP probíhá následující proces:

1. Klient DHCP se snaží lokalizovat server DHCP a získat adresu a konfiguraci.
2. Jestliže nelze server DHCP nalézt, případně neodpovídá, klient DHCP si sám nakonfiguruje adresu IP a masku podsítě za použití vybrané adresy ze sítě třídy B rezervované pro Microsoft, 169.254.0.0 s maskou podsítě 255.255.0.0. Klient DHCP hledá konflikty adres, aby se ujistil, že vybraná adresa již není na příslušné síti používána. Pokud je nalezen konflikt, klient vybere jinou adresu IP: Klient se pokusí o autokonfiguraci až do 10 adres.
3. Jakmile klient DHCP uspěje při samostatném výběru adresy, nakonfiguruje s touto adresou IP své síťové rozhraní. Klient pak na pozadí pokračuje v intervalech 5 minut v hledání serveru DHCP. Jestliže klient najde server DHCP později, opustí svou autokonfiguraci. Klient DHCP pak použije adresu nabídnutou serverem DHCP (a jakékoli další informace možností DHCP) a zaktualizuje své nastavení konfigurace protokolu IP.

Jestliže již dříve klient DHCP obdržel zápůjčku serveru DHCP:

1. Jestliže je zápůjčka klientovi během spouštění systému stále platná (nevypršela), klient se pokusí obnovit tuto zápůjčku.
2. Jestliže během snahy obnovit zápůjčku klient neuspěje při lokalizaci serveru DHCP, bude se snažit provést příkaz ping na přednastavenou bránu uvedenou v zápůjčce a bude pokračovat jedním z následujících způsobů:
 - Jestliže je provedení příkazu ping úspěšné, klient DHCP předpokládá, že je stále umístěn na stejné síti, odkud získal svou aktuální zápůjčku a pokračuje v jejím užívání. Dle výchozího nastavení se klient bude na pozadí snažit obnovit svou zápůjčku po vypršení 50 procent přiřazeného času zápůjčky.
 - Jestliže je provedení příkazu ping neúspěšné, klient DHCP předpokládá, že byl přesunut na síť, kde nejsou služby DHCP dostupné. Klient pak provede autokonfiguraci své adresy IP, jak je popsáno výše. Klient pak v intervalech 5 minut pokračuje v hledání serveru DHCP a získání zápůjčky.

Místní úložiště

Služba Microsoft DHCP podporuje místní úložiště, které umožňuje klientům ukládat informace o DHCP na vlastní pevné disky. Místní úložiště je užitečné, protože při spuštění systému klienta se nejprve snaží obnovit zápůjčku stejné adresy IP. Místní úložiště také znamená, že klient může být vypnut a zase spuštěn s tím, že používá stále svou předchozí zapůjčenou adresu a konfiguraci i v případě nedosažitelnosti serveru DHCP nebo v případě odpojení od sítě při spouštění klienta. Místní úložiště také umožňuje provádět autokonfiguraci protokolu IP.

Proces zápůjčky DHCP

Klient podporující službu DHCP obdrží od serveru DHCP zápůjčku na adresy IP. Před vypršením časového omezení zápůjčky musí server DHCP tuto zápůjčku klientovi obnovit nebo klient musí získat novou zápůjčku. Zápůjčky jsou v databázi serveru DHCP uchovávány přibližně jeden den po vypršení. Tato poskytnutá lhůta chrání zápůjčku klienta v případě, že klient a server jsou v různých časových pásmech, jejich interní hodiny nejsou synchronizovány nebo klient je v době vypršení zápůjčky mimo síť.

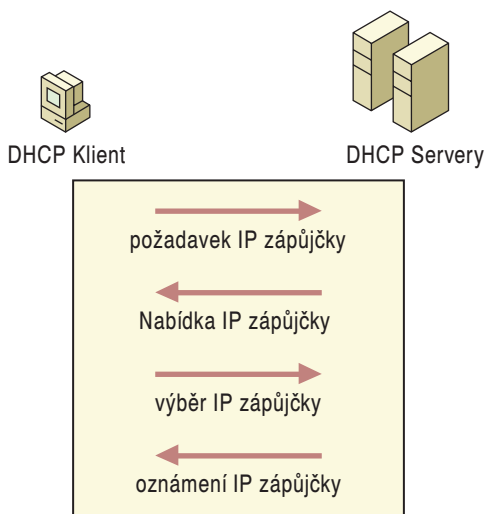
Zprávy DHCP

Tabulka 4.2 popisuje zprávy DHCP vyměňované mezi klientem a serverem. To je nezbytné před pokračováním výkladu o tom, jak proces zápůjček DHCP funguje. Více informací o každé zprávě najdete v této knize v části „Zprávy DHCP“.

Tabulka 4.2 Zprávy DHCP

Typ zprávy	Popis
DHCPDiscover	Když se klient DHCP poprvé snaží přihlásit k síti, žádá o adresu IP ze serveru DHCP prostřednictvím všesměrového vysílání paketu DHCPDiscover. Zdrojová adresa IP v paketu je 0.0.0.0, protože klient dosud nemá žádnou adresu IP. Zpráva je buď 342 nebo 576 bajtů dlouhá – starší verze operačního systému Windows používají delší rámec zprávy.
DHCPOffer	Každý server DHCP, který obdrží paket DHCPDiscover, odpoví pakem DHCPOffer obsahujícím nezapůjčenou adresu IP a další informace o konfiguraci protokolu TCP/IP, například o masce podsítě a přednastavené bráně. Pomocí paketu DHCPOffer může odpovědět více než jeden server DHCP. Klient přijme první paket DHCPOffer, který obdrží. Zpráva je 342 bajtů dlouhá.
DHCPRequest	Jakmile klient DHCP obdrží paket DHCPOffer, odpoví všesměrovým vysláním paketu DHCPRequest, který obsahuje nabízenou adresu IP a ukazuje její přijetí. Zpráva je dlouhá buď 342 nebo 576 bajtů v závislosti na odpovídající zprávě DHCPDiscover.
DHCPAcknowledge (DHCPAck)	Vybraný server DHCP potvrdí klientovi DHCPRequest pro danou adresu IP odesláním paketu DHCPAck. V tomto okamžiku server také předá jakékoli volitelné parametry konfigurace. Po přijetí paketu DHCPAck se může klient účastnit na síti TCP/IP a dokončit spouštění systému. Tato zpráva je 342 dlouhá.
DHCNPak	Jestliže adresa IP nemůže být klientem použita, protože již není platná nebo ji využívá jiný počítač, odpoví server DHCP pakem DHCNPak a klient musí začít proces zápůjčky znovu. Kdykoli server DHCP obdrží požadavek na adresu IP, která je neplatná kvůli oborům, se kterými nakonfigurována, pošle klientovi zprávu DHCNPak.

Typ zprávy	Popis
DHCPDecline	Jestliže klient DHCP určí, že nabízené parametry konfigurace jsou neplatné, pošle serveru paket DHCPDecline. Klient musí začít proces zápůjčky znovu.
DHCPRelease	Klient DHCP pošle paket DHCPRelease serveru, aby uvolnil adresu IP a zrušil jakoukoli zbývající zápůjčku.
DHCPInform	DHCPInform je nový typ zprávy DHCP definovaný v dokumentu RFC 2131 a používaný počítači na síti pro požadování a přijímání informací od serveru DHCP, které použijí v lokální konfiguraci. Když je tento typ zprávy použit, odesílatel již je externě nakonfigurován na svou adresu IP na síti, kterou získal či nezískal pomocí DHCP. Tento typ zprávy není momentálně podporován službou DHCP poskytovanou v dřívějších verzích operačního systému Windows NT Server a nemusí být rozpoznána implementacemi softwaru DHCP třetích stran.

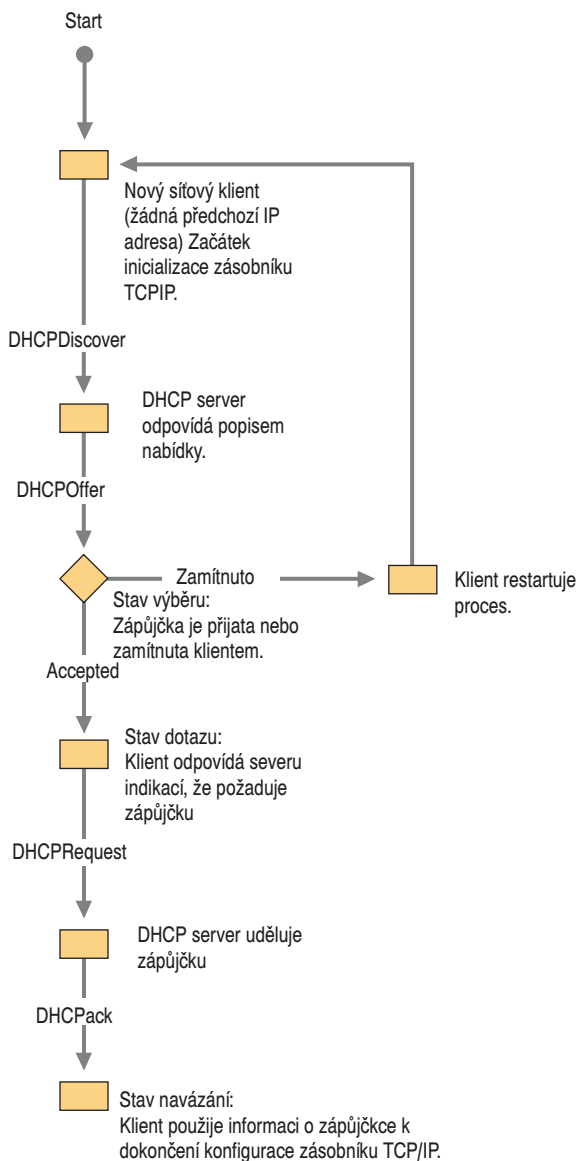


Obrázek 4.2 Proces zápůjčky DHCP

Jak funguje proces zápůjčky

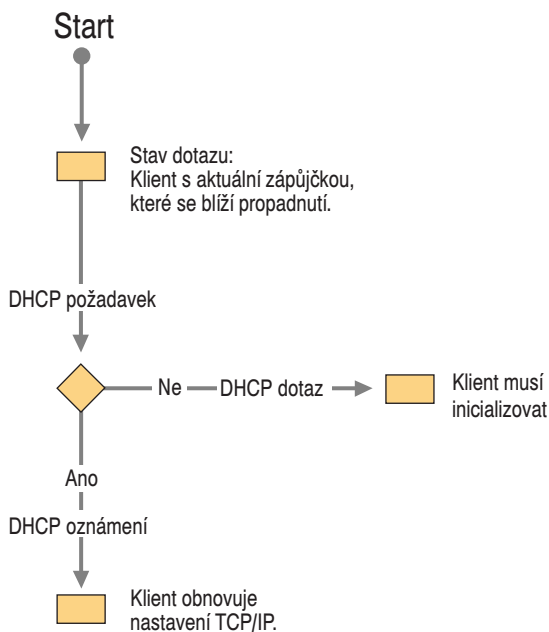
Jakmile se poprvé spustí klient podporující DHCP a pokusí se připojit k síti, automaticky následuje inicializační proces k získání zápůjčky od serveru DHCP. Na obrázku 4.2 je znázorněn proces zápůjčky.

1. Klient DHCP požaduje adresu IP prostřednictvím všesměrového vysílání zprávy DHCPDiscover na lokální podsíti.
2. Klientovi je nabídnuta adresa, když server DHCP reaguje zprávou DHCPOffer obsahující adresu IP a informace o konfiguraci pro zápůjčku. Jestliže na požadavek klienta nereaguje žádný server DHCP, může klient postupovat dvěma způsoby:



Obrázek 4.3 Stavy klienta DHCP během procesu zápůjčky

- Je-li to klient na platformě Windows 2000 a nemá-li zakázánu autokonfiguraci protokolu IP, klient si sám pro své rozhraní nakonfiguruje adresu IP.
- Není-li to klient na platformě Windows 2000, nebo má zakázánu autokonfiguraci protokolu IP, síťová inicializace klienta selže. Klient pokračuje v opakovaném posílání zpráv DHCPDiscover na pozadí (čtyřikrát, vždy po pěti minutách) až do obdržení zprávy DHCPOffer od serveru DHCP.



Obrázek 4.4 Stav klienta DHCP během procesu obnovování zápůjčky

3. Klient sdělí přijetí nabídky výběrem nabízené adresy a odpovídá serveru pomocí zprávy DHCPRequest.
4. Klientovi je přiřazena adresa a server DHCP mu pošle zprávu DHCPACK potvrzující zápůjčku. Ve zprávě mohou být obsaženy i informace o dalších možnostech DHCP.
5. Poté, co klient obdrží potvrzení, nakonfiguruje si vlastnosti protokolu TCP/IP za použití jakékoli informace o možnosti DHCP obsažené v odpovědi a připojí se k síti.

Ve vzácných případech může server DHCP vrátit klientovi negativní potvrzení. To se může stát, jestliže klient žádá neplatnou nebo duplikovanou adresu. Jestliže klient obdrží negativní potvrzení (DHCPNak) musí klient začít celý proces zápůjčky znovu.

Stavy klienta DHCP v procesu zápůjčky

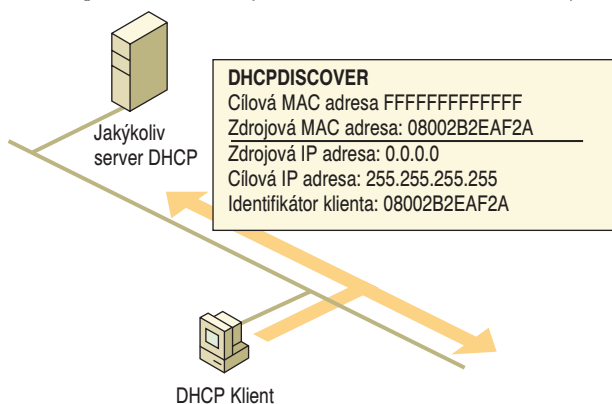
Cyklus klienta DHCP přes šest různých stavů klienta během procesu zápůjčky DHCP je znázorněn na obrázku 4.3 a 4.4. Obrázek 4.4 znázorňuje proces zápůjčky DHCP klientů, kteří obnovují svou zápůjčku.

Když je klient DHCP a server DHCP na stejné podsíti, zprávy DHCPDiscover, DHCPOffer, DHCPRequest a DHCPACK jsou posílány přes všesměrové vysílání na úrovni MAC a IP.

Aby klienti DHCP mohli komunikovat se serverem DHCP na vzdálené síti, musí připojící směrovač nebo směrovače podporovat předávání zpráv DHCP mezi klientem DHCP a serverem DHCP za použití služby BOOTP/DHCP Relay Agent. Více informací najdete později v této kapitole v části „Podpora klientů BOOTP“ a „Správa přenosových agentů“.

Inicializace

Tento stav nastane při první inicializaci zásobníku protokolu TCP/IP na počítači klienta DHCP. Klient ještě nemá od serveru DHCP vyžádanou adresu IP. Tento stav také nastane, pokud je klientovi odepřena adresa IP, kterou požaduje, nebo pokud adresa IP, kterou původně měl, byla uvolněna. Stav inicializace je znázorněn na obrázku 4.5.



Obrázek 4.5 Stav inicializace

Když je klient DHCP v tomto stavu, jeho adresa IP je 0.0.0.0. Při získávání platné adresy klient prostřednictvím všesměrového vysílání pošle zprávu DHCPDiscover z portu UDP 68 na port UDP 67 se zdrojovou adresou 0.0.0.0 a cílovým umístěním 255.255.255.255 (klient dosud nezná adresu serverů DHCP). Zpráva DHCPDiscover obsahuje adresu MAC klienta DHCP a název počítače.

Výběr

Pak se klient přesune do stádia výběru, kdy vybírá odpověď serveru DHCP, DHCPOffer. Všechny servery DHCP, které obdržely zprávu DHCPDiscover a mohou klientovi DHCP nabídnout platné adresy IP, reagují zprávou DHCPOffer odesílanou z portu UDP 68 na port UDP 67. Zpráva DHCPOffer je poslána prostřednictvím všesměrového vysílání MAC a IP, protože klient DHCP ještě nemá platnou adresu IP, kterou lze použít jako cílové umístění. Server DHCP rezervuje adresu IP, aby nebyla nabízena jinému klientovi DHCP:

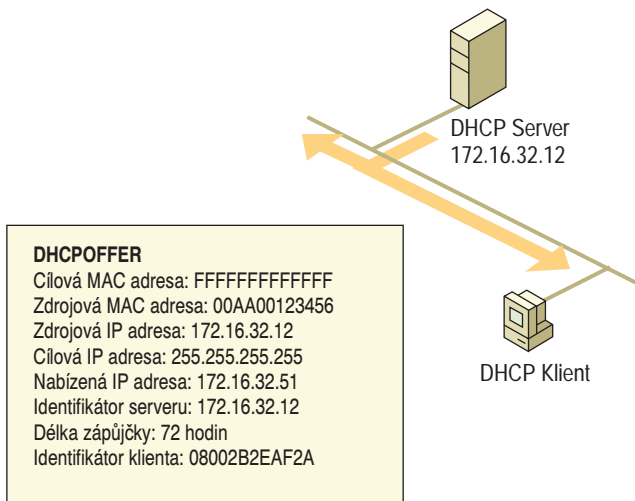
Zpráva DHCPOffer obsahuje adresu IP a odpovídající masku podsítě, identifikátor serveru DHCP (adresu IP nabízejícího serveru DHCP) a dobu trvání zápůjčky. Stav výběru je znázorněn na obrázku 4.6.

Klient DHCP čeká na zprávu DHCPOffer. Neobdrží-li zprávu DHCPOffer od serveru DHCP při spouštění systému, pokusí se o to znovu čtyřikrát (v intervalech 2, 4, 8 a 16 sekund plus náhodný čas mezi 0 a 1000 milisekund). Jestliže klient DHCP neobdrží zprávu DHCPOffer po čtyřech pokusech, počká 5 minut a pak se pokouší znovu, vždy v 5minutových intervalech.

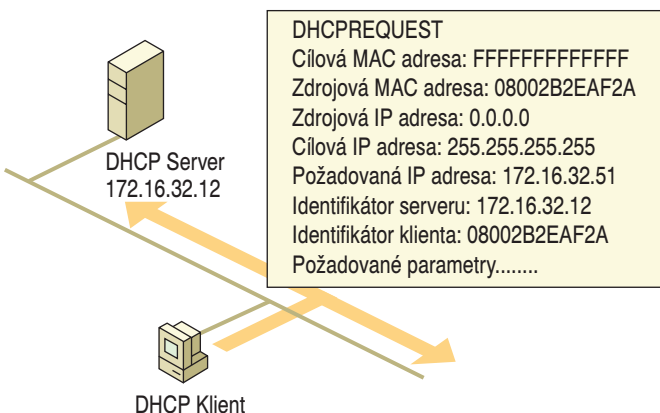
Požadavek

Poté, co klient DHCP obdrží ze serveru zprávu DHCPOffer, klient se přesune do stavu požadavku. Klient DHCP zná adresu IP, kterou chce zapůjčit, takže pošle prostřednictvím všesměrového vysílání zprávu DHCPRequest na všechny servery DHCP. Klient

musí použít všesměrové vysílání, protože stále nemá přiřazenou adresu IP. Stav požadavku je znázorněn na obrázku 4.7.



Obrázek 4.6 Stav výběru



Obrázek 4.7 Stav požadavku

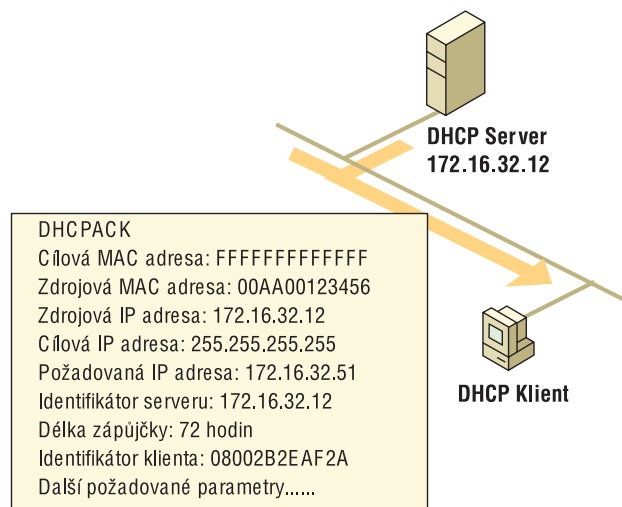
Jestliže byla adresa IP klienta známa (tzn. že počítač byl restartován a snaží se zapůjčit si původní adresu), všesměrové vysílání sledují všechny servery DHCP. Server DHCP, který může zapůjčit požadovanou adresu IP, odpoví buď úspěšným potvrzením (DHCPACK) nebo neúspěšným potvrzením (DHCPNak). Zpráva DHCPNak je použita v případě, že požadovaná adresa IP není dostupná nebo klient se fyzicky přesunul na jinou podsíť, která požaduje jinou adresu IP. Po obdržení zprávy DHCPNak se klient vrací do stavu inicializace a začíná proces zápůjčky znovu.

Jestliže adresa IP klienta byla získána právě při výměně zpráv DHCPDiscover nebo DHCPOffer se serverem DHCP, klient vloží adresu IP tohoto serveru DHCP do zprávy DHCPRequest. Určený server DHCP reaguje na tento požadavek a všechny ostatní servery stáhnou své zprávy DHCPOffer. To zajišťuje, že adresy IP, které byly nabí-

zeny ostatními servery DHCP, se vrací zpět do stavu, kdy jsou dostupné pro další klienty DHCP.

Vazba

Server DHCP reaguje na zprávu DHCPRequest prostřednictvím zprávy DHCPACK. Tato zpráva obsahuje platnou zápůjčku na vyjednanou adresu IP a jakékoli možnosti DHCP nakonfigurované správcem serveru DHCP. Stav vazby je znázorněn na obrázku 4.8.



Obrázek 4.8 Stav vazby

Server DHCP pošle zprávu DHCPACK prostřednictvím všesměrového vysílání IP. Poté, co klient DHCP obdrží zprávu DHCPACK, dokončí inicializaci zásobníku protokolu TCP/IP. Je nyní považován za vázaného klienta DHCP, který může používat protokol TCP/IP ke komunikaci na síti.

Adresa IP zůstává přiřazena klientovi až do ručního uvolnění adresy klientem nebo do vypršení doby zápůjčky a odmítnutí zápůjčky serverem DHCP.

Obnovení

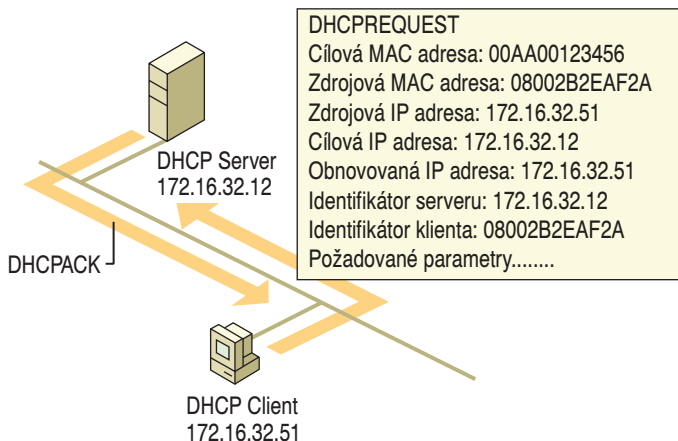
Informace o adresování IP jsou zápůjčeny klientovi a klient je zodpovědný za obnovení zápůjčky. Dle výchozího nastavení se klient DHCP snaží obnovit svou zápůjčku po uplynutí 50 procent doby trvání zápůjčky. Kvůli obnovení zápůjčky posílá klient DHCP zprávu DHCPRequest serveru DHCP, od kterého původně zápůjčku obdržel.

Server DHCP automaticky zápůjčku obnoví prostřednictvím zprávy DHCPACK. Tato zpráva DHCPACK obsahuje novou zápůjčku a parametry možností DHCP. To zajišťuje, že klient DHCP může aktualizovat svá nastavení protokolu TCP/IP v případě, že správce sítě změnil některá nastavení serveru DHCP. Stav obnovení je znázorněn na obrázku 4.9.

Jakmile klient DHCP obnoví zápůjčku, navrátí se do stavu vazby. Zprávy o obnovení (DHCPRequest a DHCPACK) jsou posílány jednosměrným provozem na úrovni IP a MAC.

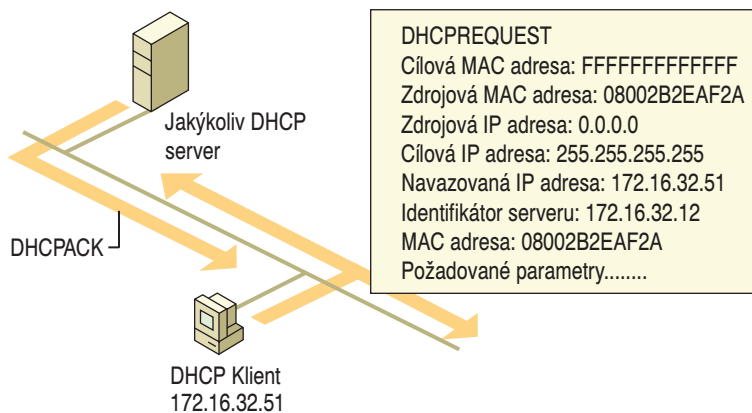
Obnovení vazeb

Jestliže klient DHCP není schopen komunikovat se serverem DHCP, od kterého získal svou zápůjčku a vypršelo již 87,5 procenta doby trvání zápůjčky, bude se snažit kontaktovat jakýkoli dostupný server DHCP pomocí zpráv DHCPRequest odesílaných prostřednictvím všesměrového vysílání. Jakýkoli server DHCP může reagovat zprávou DHCPACK a obnovit zápůjčku, případně zprávou DHCPNak, kterou donutí klienta



Obrázek 4.9 Stav obnovení

DHCP k inicializaci a novému začátku procesu zápůjčky. Stav obnovení vazeb je znázorněn na obrázku 4.10.



Obrázek 4.10 Stav obnovení vazeb

Jestliže doba zápůjčky vyprší, nebo klient obdrží zprávu DHCPNak, musí klient DHCP okamžitě přestat užívat svou aktuální adresu IP. Jakmile k tomuto dojde, je komunikace přes protokol TCP/IP přerušena až do doby, kdy klient získá novou adresu IP.

Restartování klienta DHCP

Když se klient, který před tím měl zapůjčenu adresu IP, restartuje, pošle prostřednictvím všesměrového vysílání namísto zprávy DHCPDiscover zprávu DHCPRequest. Zpráva DHCPRequest obsahuje žádost o původně přiřazenou adresu IP.

Jestliže klient může použít požadovanou adresu IP, server DHCP odpoví zprávou DHCPACK.

Jestliže klient nemůže použít požadovanou adresu IP, protože již není platná, je používána jiným klientem nebo je neplatná, protože klient byl fyzicky přesunut na jinou pod síť, server DHCP odpoví zprávou DHCPNak. Dojde-li k této situaci, klient začne proces zápůjčky znovu.

Jestliže klient neuspěje při lokalizaci serveru DHCP během procesu obnovení, snaží se provést příkaz ping na přednastavenou bránu uvedenou v aktuální zápůjčce s následujícími výsledky:

- Jestliže je provedení příkazu ping na přednastavenou bránu úspěšné, klient DHCP předpokládá, že je stále umístěn na stejné síti, odkud získal svou aktuální zápůjčku a pokračuje v jejím používání. Dle výchozího nastavení se klient na pozadí snaží obnovit svou aktuální zápůjčku po vypršení 50 procent doby trvání zápůjčky.
- Jestliže provedení příkazu ping na přednastavenou bránu selže, klient DHCP předpokládá, že byl přesunut na jinou síť, kde nejsou služby DHCP dostupné (například domácí síť). Dle výchozího nastavení si klient sám nakonfiguruje adresu IP, jak bylo uvedeno výše, a pokračuje na pozadí vždy po pěti minutách ve snáhách lokalizovat server DHCP a získat zápůjčku.

Obnovování zápůjčky

Proces obnovování nastane v případě, že klient již má zápůjčku a potřebuje ji u serveru obnovit. Aby zajistil, že adresy nezůstanou přiřazené, pokud nejsou potřeba, server DHCP adrese přiřadí časový limit zadaný správcem, označovaný jako doba trvání zápůjčky.

Po uplynutí poloviny doby trvání zápůjčky klient DHCP žádá o obnovení zápůjčky a server DHCP ji prodlouží. Jestliže počítač přestane užívat přiřazenou adresu IP (například je přesunut na jiný segment sítě nebo je ze sítě zcela odebrán), zápůjčka vyprší a adresa je opět dostupná pro další přiřazování.

Proces přiřazování probíhá takto:

1. Klient odešle na server DHCP požadavek o obnovení a prodloužení zápůjčky své aktuální adresy. Klient odešle směrovaný požadavek na server DHCP maximálně čtyřikrát, a to s odstupem 4, 8 a 16 sekund.
 - Jestliže lze server DHCP lokalizovat, zpravidla klientovi odešle zprávu DHCPACK. Tím je zápůjčka obnovena.
 - Není-li klient schopen komunikovat se svým původním serverem DHCP, počká až do vypršení 87,5 procent doby trvání zápůjčky. Poté přejde do stavu obnovení vazeb a prostřednictvím všesměrového vysílání odešle (maximálně čtyřikrát, a to s odstupem 4, 8 a 16 sekund) zprávu DHCPDiscover jakémukoli dostupnému serveru DHCP, aby obnovil zápůjčku své aktuální adresy IP.

2. Jestliže server na požadavek o obnovení zápůjčky aktuální adresy odpoví zprávou DHCP Offer, klient obnoví svou zápůjčku u nabízejícího serveru a pokračuje ve fungování.
3. Jestliže doba trvání zápůjčky vyprší a nebyl kontaktován žádný server, klient musí okamžitě přestat používat zapůjčenou adresu IP. Klient pak pokračuje při získávání nové zápůjčky adresy IP stejným způsobem, jako při spouštění systému.

Správa doby trvání zápůjčky

Po vytvoření oboru je dle výchozího nastavení doba trvání zápůjčky nastavena na osm dní, což ve většině případů funguje dobře. Nicméně vzhledem k tomu, že obnovování zápůjčky je pokračující proces, který může ovlivnit výkon klienta DHCP a sítě, může být užitečné změnit dobu trvání zápůjčky. Následující návod vám pomůže se rozhodnout, jak nejlépe upravit nastavení doby trvání zápůjčky, aby se zlepšil výkon služby DHCP na vaší síti:

- Je-li dostupné velké množství adres IP a konfigurace sítě se mění pouze zřídka, zvýšte dobu trvání zápůjčky tak, aby byla snížena frekvence požadavků na obnovení zápůjčky mezi klienty a serverem DHCP. Tím snížíte provoz sítě.
- Je-li dostupné pouze omezené množství adres IP a konfigurace sítě se často mění, případně se klienti na síti často přesunují, snižte dobu trvání zápůjčky. Tím zvýšíte poměr adres vrácených do fondu dostupných adres IP.
- Zvažte poměr mezi připojenými počítači a dostupnými adresami IP. Například, jestliže 40 systémů sdílí adresu třídy C (s 254 dostupnými adresami), je poptávka po znovuvyužití adres malá. Dlouhá doba trvání zápůjčky, například dva měsíce, by byla v takové situaci zcela odpovídající. Nicméně pokud stejný fond adres sdílí 230 počítačů, je poptávka po dostupných adresách větší a více tomu odpovídá doba trvání zápůjčky několik dní či týdnů.
- Použijte neomezenou dobu trvání zápůjčky opatrně. I v relativně stabilním prostředí probíhají mezi klienty určité změny. Minimálně se připojují a odebírají přenosné počítače, kancelářské počítače se přesunují z jedné kanceláře do druhé a mění se síťové adaptéry. Jestliže klient je během neomezené doby trvání zápůjčky odebrán ze sítě, server DHCP není informován a adresu IP nelze znovu využít. Lepší možností je velmi dlouhá doba trvání zápůjčky, například šest měsíců. To zajišťuje, že adresy jsou skutečně obnoveny.

Správa oborů

Před tím, než klient může použít server DHCP k dynamické konfiguraci protokolu TCP/IP, musí být definován a aktivován obor. Obor služby DHCP je administrativní sbírkou adres IP a parametrů konfigurace protokolu TCP/IP, která je dostupná pro zápůjčky klientům DHCP. Správce sítě vytvoří pro každou logickou nebo fyzickou pod síť obor.

Obor má následující vlastnosti:

- Název oboru přiřazený při jeho vytváření.
- Rozsah možných adres IP, ze kterých se vybírají adresy používané při nabídkách zápůjček DHCP.
- Jedinečná maska podsítě, která pro danou adresu IP určuje příslušnou podsít.
- Hodnota doby trvání zápůjčky.

Každá podsít' může mít samostatný obor DHCP se samostatným rozsahem adres IP. Abyste mohli použít v rámci jednoho oboru nebo jedné podsítě několik rozsahů adres, musíte nejdříve definovat obor a pak nastavit rozsahy vyloučení.

Rozsahy vyloučení Vytváříte-li nový obor, adresy stávajících staticky nakonfigurovaných počítačů by měly být okamžitě z tohoto oboru vyloučeny. Použitím rozsahů vyloučení může správce vyloučit z oboru rozsahy adres IP, takže tyto adresy nejsou nabízeny klientům.

Vzhledem k tomu, že operační systém Windows 2000 vyžaduje, aby počítač provozující službu DHCP měl svou adresu IP nakonfigurovanou pevně, ujistěte se, že počítač sloužící jako server má svou adresu IP buď mimo rozsah oboru nebo že je tato adresa z oboru vyloučena.

Vyloučené adresy IP mohou být na síti aktivní, ale pouze po ručním nakonfigurování na počítače, které nepoužívají k získání adresy službu DHCP. Rozsahy vyloučení by měly být používány pro počítače nebo zařízení, které musí mít statickou adresu IP, například tiskové servery, servery firewall nebo směrovače.

Rezervace Správce může určitým počítačům nebo zařízením na síti rezervovat adresy IP pro trvalé přiřazení zápisů. Rezervace zajišťují, že určité hardwarové zařízení na podsíti může vždy používat stejnou adresu IP. Rezervace by měly být prováděny u zařízení podporujících službu DHCP, která musí mít vždy na síti stejnou adresu IP, například tiskové servery, servery firewall nebo směrovače. Více informací najdete později v této kapitole v části „Správa rezervací“.

Odebírání záznamů Může nastat situace, kdy je nutno obor upravit, aby byla odebrána zápisů klienta DHCP. Hlavním důvodem je odebrání zápisů, která koliduje s rozsahem vyloučení adres IP nebo rezervovanou adresou, kterou chcete určit. Odebrání zápisů má stejný účinek jako vypršení doby trvání zápisů – při dalším spuštění počítače musí klient projít celým procesem vyžádání si zápisů. Nicméně nic klientovi nebrání v tom, aby získal zápisů stejné adresy IP.

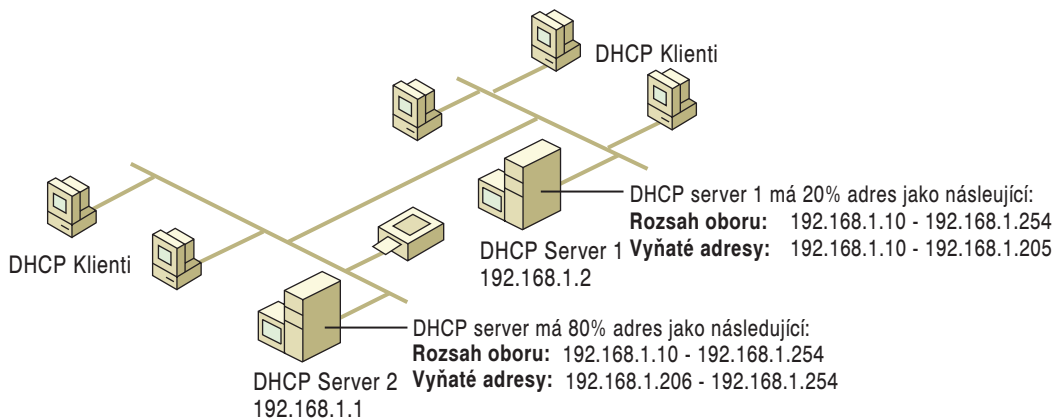
Abyste tomuto zabránili, adresa musí být před tím, než klient požádá o jinou zápisů, nedostupná. Toho dosáhnete tím, že ji odeberete z oboru a nastavíte rezervaci nebo vyloučení. Záznamy oboru odeberte pouze klientům, kteří již nepoužívají přiřazenou zápisů DHCP nebo kteří jsou okamžitě přesunuti na jinou adresu. Odebrání aktivního klienta by mohlo vyústit do duplikace adres IP na síti, protože odebrané adresy jsou automaticky opětovně přiřazovány novým klientům.

Po odebrání zápisů klienta z oboru a nastavení rezervace nebo vyloučení byste vždy měli spustit na příkazové řádce klientského počítače příkaz `ipconfig /release`, abyste klienta donutili uvolnit jeho adresu IP pomocí zprávy DHCPRelease.

Pravidlo 80/20

Aby selhání jakéhokoli samostatného serveru DHCP nezabránilo spuštění klientů DHCP, budete pravděpodobně instalovat více než jeden server DHCP. Nicméně protokol DHCP neposkytuje serverům DHCP žádnou možnost spolupráce, aby byla zajištěna jedinečnost přiřazených adres. Proto musíte pečlivě rozdělit dostupné fondy adres mezi servery DHCP tak, abyste zabránili přiřazování duplikovaných adres.

Kvůli vyváženosti používání serverů DHCP se používá při dělení oborů adres mezi servery DHCP pravidlo 80/20. Příklad pravidla 80/20 je znázorněn na obrázku 4.11.



Obrázek 4.11 Model pravidla 80/20

Server DHCP 1 je nakonfigurován tak, aby zapůjčil většinu (asi 80 procent) dostupných adres. Server DHCP 2 je nakonfigurován tak, aby zapůjčil zbytek adres (asi 20 procent). Tento scénář umožňuje lokálnímu serveru DHCP (server DHCP 1) většinu času reagovat na požadavky lokálních klientů DHCP. Vzdálený nebo záložní server DHCP (server DHCP 2) přiřazuje adresy klientům na jiné podsíti pouze v případě, že lokální server není dostupný nebo již nemá adresy. Stejně pravidlo se používá ve scénáři více podsítí, aby byla zajištěna dostupnost serveru DHCP, když klient požaduje zápůjčku.

Správa rezervací

Za pomoci rezervací můžete pro trvalé používání počítačem nebo zařízením podporujícím službu DHCP rezervovat určité adresy IP. Jestliže je více serverů DHCP nakonfigurováno tak, že jejich obory pokrývají rozsah adres, které musí být rezervovány, musí být rozsah rezervace specifikován na každém serveru DHCP. V opačném případě by tyto adresy mohl vydat jiný server DHCP.

Jestliže chcete změnit rezervovanou adresu klienta, stávající rezervace adresy klienta musí být před přidáním nové rezervace odebrána. Informace o možnostech DHCP lze měnit při zachování rezervované adresy IP.

Rezervování adresy IP z oboru automaticky nenutí klienta používajícího tuto adresu, aby ji okamžitě přestal užívat. Jestliže pro klienta rezervujete novou adresu nebo adresu, která je odlišná od jeho současné adresy, měli byste ověřit, že adresa již nebyla zapůjčena. Jestliže již byla zapůjčena, klient používající adresu ji musí uvolnit prostřednictvím požadavku DHCPRelease. Tohoto dosáhnete, spustíte-li na příkazovém řádku příkaz **ipconfig /release**.

Rezervování adresy nenutí klienta, pro kterého byla rezervována, aby ji začal okamžitě používat. Klient musí kvůli přesunu na novou rezervovanou adresu podat žádost o obnovení. Tohoto dosáhnete, spustíte-li na příkazovém řádku příkaz **ipconfig /renew**.

U klientů na platformě Windows 95 nebo Windows 98 použijte k uvolnění nebo obnovení rezervované adresy program Winipcfg.exe. U klientů na platformě MS-DOS nebo na jiném operačním systému, proveďte restart systému.

Jakmile je uvolnění nebo obnovení dokončeno, klientovi rezervace je k trvalému užívání zapůjčena nově rezervovaná adresa IP.

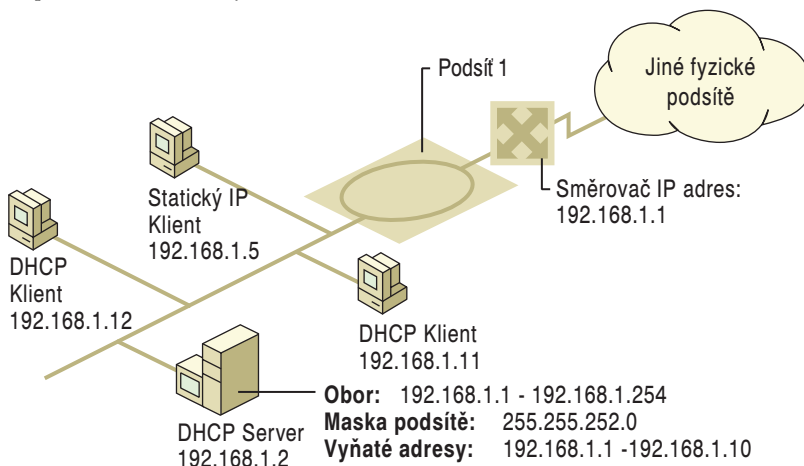
Superobory

Množina oborů umožňuje serveru DHCP poskytovat zápůjčky z více než jednoho oboru na jedné fyzické síti. Před tím, než můžete vytvořit množinu oborů, musíte pomocí správce služby DHCP definovat všechny obory, které mají být zahrnuty do množiny oborů. Obory v množině oborů jsou nazývány členské obory. Množiny oborů mohou řešit záležitosti služby DHCP několika způsoby. Tyto záležitosti zahrnují situace, kdy:

- Je pro klienta DHCP třeba podpora na jednom segmentu fyzické sítě – například jeden segment LAN Ethernet – kde se používá více logických sítí IP. Používá-li se na fyzické síti více než jedna logická síť IP, tato konfigurace se nazývá také multi-net.
- Fond dostupných adres pro aktuálně aktivní obor je téměř vyčerpán a k segmentu fyzické sítě je třeba přidat více počítačů.
- Je třeba přenést klienty do nového oboru.
- Je třeba podpora pro klienty DHCP na opačné straně přenosových agentů BOOTP, kde síť na druhé straně přenosového agenta má na jedné fyzické síti více logických podsítí. Více informací najdete později v této kapitole v části „Podpora klientů BOOTP“.

Verze služby DHCP předcházející operačnímu systému Windows NT 4.0 s aktualizací Service Pack 2 nemohou vytvářet množiny oborů. Jedním řešením této situace je přidání dodatečných síťových adaptérů na server a adresování každého ze síťových adaptérů na danou logickou podsíť IP. To vyžaduje dodatečný a nadbytečný hardware a funguje to pouze na lokálních segmentech serveru DHCP.

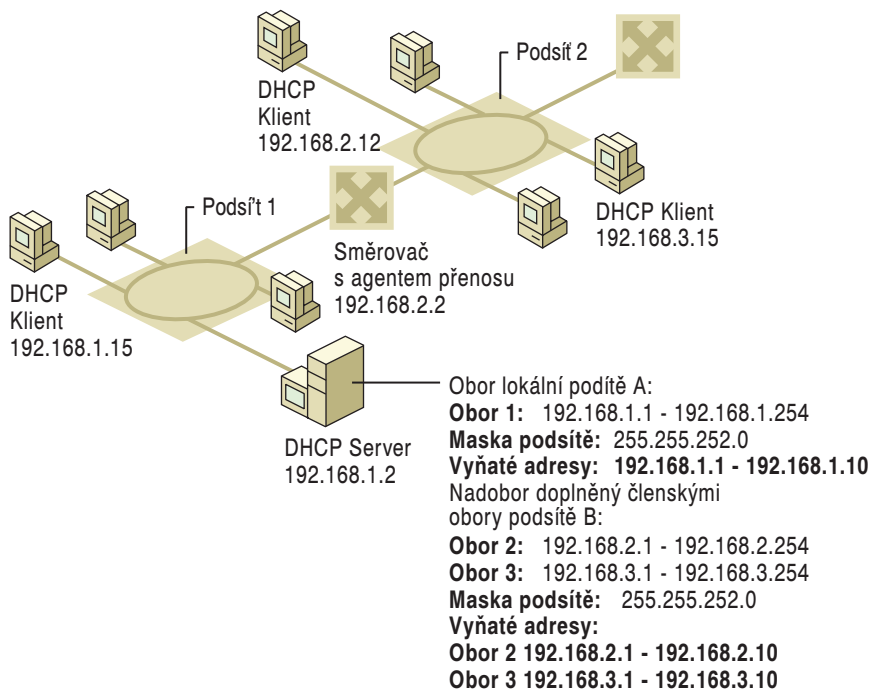
Standardní síť s jedním serverem DHCP na jedné fyzické podsíti je omezena na zapůjčování adres klientům na této fyzické podsíti. Obrázek 4.12 znázorňuje podsíť A před implementací množiny oborů.



Obrázek 4.12 Server DHCP používající jednotlivé obory

K zahrnutí multinetů na podsíti B do rozsahu adres zapůjčených serverem DHCP zobrazeným na obrázku 4.12 můžete vytvořit množinu oborů, které kromě oboru podsítě A zahrnují členy obor 2 a obor 3 podsítě B.

Na obrázku 4.13 je zobrazena konfigurace množiny oborů.



Obrázek 4.13 Server DHCP používající množinu oborů

K zahrnutí multinetů na vzdálených sítích do rozsahu adres zapůjčovaných serverem DHCP můžete nakonfigurovat množinu oborů tak, aby zahrnovala členy obor 1, obor 2 a obor 3.

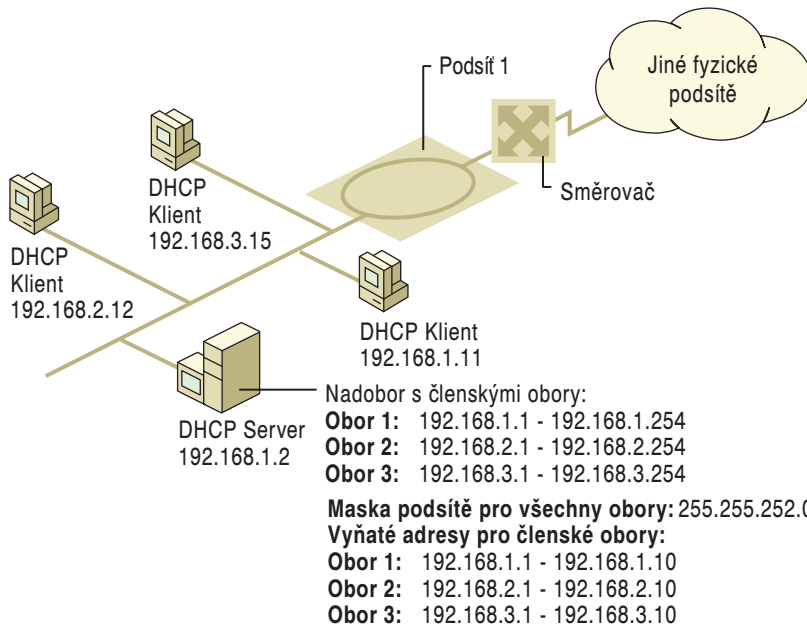
Na obrázku 4.14 je znázorněna konfigurace oboru, který zahrnuje multinetu na vzdálených sítích.

Tabulka 4.3 znázorňuje, jak jsou dva servery DHCP, které jsou umístěny na stejné fyzické podsíti, nakonfigurovány každý s jedním oborem.

Tabulka 4.3 Obor DHCP pro server A a server B

Název serveru DHCP	Počáteční adresa IP oboru	Koncová adresa IP oboru
server DHCP A	211.111.111.1	211.111.111.255
server DHCP B	222.222.222.1	222.222.222.255

Jestliže server DHCP A spravuje jiný obor adres než server DHCP B a ani jeden z nich nemá informace o adresách spravovaných tím druhým, nastávají problémy, pokud klient předtím registrovaný u serveru A, například, během řádného vypnutí uvolní svůj název a později se opět po restartu připojí k síti a snaží se zapůjčit adresu od serveru B.



Obrázek 4.14 Server DHCP používající množiny oborů pro vzdálené sítě

Jestliže server B obdrží od klienta paket DHCPRequest na obnovení adresy před tím, než ho obdrží server A, server B (který neobsahuje žádné adresy serveru A) žádost zamítne a pošle klientovi paket DHCPNak. Klient pak musí znovu vyjednávat o zápůjčce DHCP všesměrovým vysíláním paketu DHCPDiscover na lokální podsít. Server B může poslat paket DHCPOffer nabízející klientovi adresu, kterou může přijmout prostřednictvím paketu DHCPRequest, což server B potvrdí paketem DHCPAck.

V tomto případě klienta nic neochrání před tím, aby každá žádost o obnovení adresy byla po připojení k síti zamítnuta. V procesu zamítání a dostávání zápůjčky adresy může být klientovi nabídnuta adresa, která ho umístí na jinou podsít, pro kterou není klient nakonfigurován. Použitím množiny oborů na obou serverech DHCP se můžete oběma těmito problémům vyhnout a adresy jsou spravovány předvídatelně a efektivně.

Tabulka 4.4 popisuje stejnou situaci, ale používá množinu oborů. Oba servery jsou umístěny na stejné fyzické podsíti a každý je nakonfigurován tak, aby umožňoval více serverům poskytovat adresy pro multinet.

Tabulka 4.4 Množina oborů: servery DHCP A a B

Název serveru DHCP	Počáteční adresa IP oboru	Koncová adresa IP oboru	Vyloučení z oboru
server DHCP A	211.111.111.1	211.111.111.254	
server DHCP A	222.222.222.1	222.222.222.254	222.222.222.1 až 222.222.222.254
server DHCP B	222.222.222.1	222.222.222.254	
server DHCP B	211.111.111.1	211.111.111.254	211.111.111.1 až 211.111.111.254

Po nakonfigurování množin oborů dle tabulky servery A a B rozpoznávají adresy IP přiřazené tím druhým. To zabráňuje negativním potvrzením požadavků klientů DHCP o obnovení adresy IP nebo o získání adresy ze stejného logického rozsahu adres. Funguje to díky tomu, že server DHCP B zná prostřednictvím množiny oborů definované na serveru DHCP B obor serveru DHCP A. Proto pokud se klient DHCP pokusí o obnovení adresy náležející jednomu ze členských oborů v množině oborů serveru DHCP, server B tuto žádost ignoruje.

Varování Jestliže je specifikován rozsah adres IP, který je pro příslušnou masku podsítí příliš velký, správce má možnost pomocí průvodce vytvořením oboru DHCP vytvořit množinu oborů. Nicméně to může omezit prostředky serveru DHCP. Například jestliže nová množina oborů zahrnuje více než 10000 oborů, může server přetížit. V takových případech by množiny oborů měly být vytvářeny ručně s menšími podmnožinami oborů nebo by měl být pomocí průvodce specifikován menší rozsah adres IP.

Odebírání oborů

Obory by měly být odebrány v případě, že se podsítí již nepoužívá nebo pokud potřebujete přechýšlovat síť na používání rozsahu jiné adresy IP.

Před odebráním musíte obor deaktivovat. To umožňuje klientům použít k obnovení jejich zápůjčky jiný obor. V opačném případě klienti ztrácejí své zápůjčky a případně i přístup k síti (pokud nemohou provést autokonfiguraci).

K zajištění hladkého přenesení klientů do jiného oboru byste měli deaktivovat starý obor minimálně na polovinu doby trvání zápůjčky nebo do doby, kdy ručně obnovíte všechny klienty, abyste je odebrali z neaktivního oboru. Více informací o deaktivaci oborů najdete v nápovědě Windows 2000 Server Help.

Předcházení konfliktům adres

Operační systém Windows 2000 disponuje zjišťováním duplikovaných adres IP na síti jak na straně klienta, tak na straně serveru.

Zjišťování konfliktů ze strany serveru

Server DHCP zjišťuje konflikty prostřednictvím provedení příkazu ping na adresu IP před nabídnutím této adresy klientovi. Jestliže je provedení příkazu ping úspěšné (je získána odpověď od počítače), je zaregistrován konflikt a adresa není nabízena klientům žádajícím zápůjčku od serveru. Server DHCP provede příkaz ping pouze na adresy, které nebyly předtím úspěšně zapůjčeny. Jestliže klient obdrží zápůjčku adresy IP, kterou již měl případně žádá o její obnovení, server DHCP příkaz ping neprovede.

Jestliže je povoleno zjišťování konfliktů, je proveden počet příkazů ping definovaný správcem. Server čeká na odpověď 1 sekundu. Vzhledem k tomu, že čas potřebný pro klienta, aby obdržel zápůjčku, je rovný počtu provedení příkazu ping, vybírejte tuto hodnotu opatrně, protože přímo ovlivňuje celkový výkon serveru. Obecně řečeno, jedno provedení příkazu ping by mělo být dostačující.

Server DHCP, který obdrží odpověď na provedení příkazu ping (znamenající konflikt) připojí k této adrese IP v oboru hodnotu BAD_ADDRESS a pokusí se zapůjčit další dostupnou adresu. Jestliže je ze sítě duplikovaná adresa odebrána, může být hodnota

BAD_ADDRESS připojená k této adrese IP odstraněna ze seznamu aktivních zápůjček oboru a adresa se vrátí do fondu adres. Adresy jsou hodnotou BAD_ADDRESS označeny po dobu zápůjčky, pro kterou je obor nakonfigurován.

Jestliže síť zahrnuje starší klienty DHCP, povolte na serveru DHCP zjišťování konfliktů. Dle výchozího nastavení služba DHCP neprovádí žádné zjišťování konfliktů. Obecně řečeno, zjišťování konfliktů by mělo být používáno pouze jako pomůcka při řešení problémů, když existuje podezření, že se na síti nachází duplikované adresy IP. Důvodem toho je, že při každém dalším zjišťování konfliktu, které server DHCP provádí, jsou k době potřebné pro vyjednání zápůjček pro klienty DHCP přidávány další sekundy.

Zjišťování konfliktů ze strany klienta

Klientské počítače na platformě Windows 2000 nebo Windows 98 také před dokončením konfigurace adresy se serverem DHCP kontrolují, zda adresa je či není používána. Jestliže klient zjistí konflikt, pošle serveru DHCP zprávu DHCPDecline. Server DHCP k adrese IP v oboru připojí hodnotu BAD_ADDRESS, jak je uvedeno v odstavci „Zjišťování konfliktů ze strany serveru“. Klient začíná proces zápůjčky znovu a je mu nabídnuta další dostupná adresa v oboru.

U sítí obsahujících klienty, kteří nepoužívají operační systém Windows 2000 nebo Windows 98, by mělo být povoleno zjišťování konfliktů ze strany serveru.

Správa možností DHCP

Možnosti DHCP lze nakonfigurovat na určité hodnoty a povolit jejich přiřazování a distribuci klientům DHCP na základě serveru, oboru, třídy nebo individuální úrovně klienta. Specializované možnosti DHCP mají přednost před obecnými. Ve většině případů jsou hodnoty klienta získány z dialogového okna Vlastnosti možností DHCP na serveru DHCP. Tyto vlastnosti jsou nakonfigurovány a nastaveny pro celý obor nebo pro jednotlivého klienta rezervovaného v oboru.

Ačkoli tyto možnosti nejsou pro použití služby DHCP vyžadovány, přiřazujte a konfiguruje tyto možnosti. Tím zautomatizujete konfiguraci protokolu TCP/IP klienta při velkém počtu aktivních klientských počítačů na bázi Microsoft DHCP. Možnosti DHCP lze také použít pro komunikaci DHCP mezi serverem a klientem.

Možnosti lze spravovat za použití různých úrovní přiřazených každému spravovanému serveru DHCP, a to včetně:

- Přednastavených obecných možností

Tyto možnosti jsou aplikovány obecně pro všechny obory a třídy definované na každém serveru DHCP a na každém klientovi, kterému slouží. Typy aktivních obecných možností se aplikují vždy, pokud nepřeváží jiné nastavení oboru, třídy nebo rezervovaného klienta pro daný typ možnosti.

- Možností oboru

Tyto možnosti jsou aplikovány na klienty, kteří obdrží zápůjčku v rámci určitého oboru. Typy aktivních možností oboru se vždy aplikují na všechny počítače dostávající zápůjčky v daném oboru, pokud nejsou obehity nastavením třídy nebo rezervovaného klienta pro daný typ možnosti.

- Možností třídy

Tyto možnosti jsou aplikovány na klienty, kteří specifikují určitou hodnotu ID třídy DHCP při dostávání zápůjčky v rámci určitého oboru. Typy aktivních možností oboru se vždy aplikují na všechny počítače nakonfigurované jako členové určité třídy možností DHCP, pokud nepřeváží nastavení rezervovaného klienta pro daný typ možnosti.

■ **Možností rezervovaného klienta**

Tyto možnosti jsou aplikovány na jakýkoli příslušný rezervovaný klientský počítač – jakýkoli počítač, který má rezervaci své adresy IP v daném oboru. Když jsou typy možností rezervovaného klienta aktivní, jejich nastavení převáží všechna další možná výchozí nastavení (nastavení možností serveru, oboru nebo třídy pro daný typ možnosti).

Obecně řečeno, možnosti jsou aplikovány na každý server DHCP na úrovni serveru nebo oboru. K přesné správě nebo úpravě nastavení možností specifikujete buď přiřazení buď uživatelské třídy nebo třídy výrobce, které převáží nad širším výchozím nastavením možností serveru nebo oboru. U zvláštních požadavků, například klienti se speciálními funkcemi, zužte toto spektrum ještě více pomocí přiřazení možností rezervovaných klientů.

Možnosti lze také použít k oddělení a distribuci příslušných možností klientům s podobnými nebo zvláštními potřebami konfigurace. Například klientům podporujícím službu DHCP, kteří se nacházejí na stejném podlaží, může být přiřazeno členství ve stejné třídě možností (to znamená, že mohou být nakonfigurováni stejnou hodnotou ID třídy DHCP). Tuto třídu je pak možno použít k distribuci dalších nebo odlišných dat možností během procesu zápůjčky, které převáží nad jakýmkoli přednastavenými obecnými možnostmi nebo možnostmi oboru.

Ve službě Windows 2000 DHCP je předdefinováno mnoho těchto typů možností. Další typy možností standardní služby DHCP lze přidat dle potřeby tak, aby podporovaly jakýkoli software klienta DHCP, který rozpoznává nebo požaduje použití dodatečných typů možností. Všechny možnosti DHCP podporované službou Windows 2000 DHCP jsou definovány v dokumentu RFC 2132, ačkoli většina klientů DHCP používá nebo podporuje pouze malou podmnožinu dostupných typů možností definovaných v dokumentu RFC 2132. Tato vlastnost umožňuje rychlé uvádění přizpůsobených aplikací pro rozsáhlé sítě. Zařízení různých výrobců na síti může také používat různá čísla možností pro různé funkce. Třída výrobce a možnosti výrobce jsou popsány v dokumentu RFC 2132.

Server DHCP na platformě Microsoft zpravidla alokuje 312 bajtů možností DHCP. To je víc než dostatek pro většinu konfigurací možností. Některé servery DHCP a někteří klienti DHCP podporují překrytí možností, ve kterém nevyužitý prostor v hlavičce další standardní zprávy DHCP v paketu DHCP může být překryt, aby uchovával a nesl dodatečné možnosti. Jestliže se snažíte použít více než 312 bajtů, některá nastavení možností se ztratí. V tomto případě byste měli odstranit jakékoli nepoužívané možnosti nebo možnosti s nízkou prioritou. Tabulka 4.5 obsahuje seznam přednastavených možností DHCP používaných klienty DHCP pro Microsoft Windows 2000.

Tabulka 4.5 Přednastavené možnosti DHCP

Kód	Název možnosti	Význam
1	Maska podsítě	Určuje masku podsítě klienta. Tato možnost je definována v dialogovém okně Správce služby DHCP Vytvořit obor nebo Vlastnosti oboru. Nelze ji nastavit přímo v dialogovém okně Možnosti DHCP.
3	Směrovač	Určuje seznam adres IP pro směrovače na podsíti klienta. Více domé počítače mohou mít pouze jeden seznam na počítač, nikoli jeden na síťový adaptér.
6	Servery DNS	Určuje seznam adres IP pro servery názvů DNS dostupných klientovi.
15	Název domény	Určuje název domény DNS, který by klient měl používat pro překlad názvu DNS počítače.
44	Servery WINS/NBNS	Určuje seznam adres IP pro servery názvů typu NetBIOS (NBNS).
46	Typ uzlu WINS/NBT	Umožňuje klientům s konfigurovatelným protokolem NetBIOS pro TCP/IP (NetBT), aby byly nakonfigurovány dle popisu v dokumentu RFC 1001/1002, kde 1 = uzel b, 2 = uzel p, 4 = uzel m a 8 = uzel h. Na vícedomých počítačích je typ uzlu přiřazen celému počítači, ne jednotlivým síťovým adaptérům.
47	ID oboru typu NetBIOS ¹	Určuje řetězec znaků, který je ID oboru typu NetBIOS pro TCP/IP pro klienta, viz dokument RFC 1001/1002.
51	Doba trvání zápůjčky	Určuje čas (v sekundách) od přiřazení adresy do vypršení zápůjčky adresy klienta. Doba trvání zápůjčky je specifikována ve Správci služby DHCP, v dialogovém okně Vytvořit obor nebo Vlastnosti oboru a lze ji nastavit přímo v dialogovém okně Vlastnosti DHCP.
58	Hodnota času obnovení (T1)	Určuje čas (v sekundách) od přiřazení adresy do vstupu klienta do stavu obnovení. Čas obnovení je funkcí možnosti doby zápůjčky, která je specifikována ve Správci služby DHCP, v dialogovém okně Vytvořit obor nebo Vlastnosti oboru a lze ji nastavit přímo v dialogovém okně Vlastnosti DHCP.
59	Hodnota času obnovení vazeb	Určuje čas (v sekundách) od přiřazení adresy do vstupu klienta do stavu obnovení vazeb. Čas obnovení vazeb je funkcí možnosti doby zápůjčky, která je specifikována ve Správci služby DHCP, v dialogovém okně Vytvořit obor nebo Vlastnosti oboru a lze ji nastavit přímo v dialogovém okně Vlastnosti DHCP.

¹): Možnost 47 (ID oboru typu NetBIOS) je poskytována pro zpětnou kompatibilitu. Tuto možnost nepoužívejte, pokud již ve svém prostředí neuplatňujete ID oboru typu NetBIOS.

Poznámka Používáte-li službu Microsoft DHCP Service ke konfiguraci počítačů, které by měly pro překlad názvů využívat služby serveru WINS, ujistěte se, že používáte možnost 44, Servery WINS, a možnost 46, Typ uzlu. Tyto možnosti DHCP automaticky nakonfigurují klienta DHCP jako uzel h, který namísto všesměrového vysílání kontaktuje server WINS kvůli registraci názvu typu NetBIOS a dotazu názvů přímo.

Parametry možností DHCP

Servery DHCP lze nakonfigurovat tak, aby poskytovaly nepovinná data, která plně nakonfiguruje protokol TCP/IP klienta. Některé z nejběžnějších typů možností DHCP nakonfigurovaných a distribuovaných serverem DHCP během zápůjčky zahrnují parametry pro výchozí bránu, směrovač, službu DNS a WINS.

Klienty lze nakonfigurovat takto:

- Možnosti informace. Můžete výslovně nakonfigurovat tyto typy možností a jakékoli s nimi spojené hodnoty poskytované klientům.
- Možnosti protokolu. Můžete výslovně nakonfigurovat tyto typy možností používané službou DHCP založené na nastavení vlastností serveru a oboru.

Ke konfiguraci těchto vlastností můžete použít správce služby DHCP a můžete je nastavit pro celý obor nebo pro jednotlivý rezervovaný obor klienta. Program LAN Manager pro klienta na platformě OS/2 nepodporuje služby DHCP nebo WINS.

Možnosti informace

Tabulka 4.6 obsahuje seznam nejobvyklejších typů možností informace DHCP, které lze nakonfigurovat pro klienty DHCP. Typicky tyto typy možností mohou být povoleny a nakonfigurovány pro každý obor, který nakonfiguruje na serveru DHCP.

Tabulka 4.6 Obvyklé typy možností informace

Kód	Popis
3	Směrovač
6	Server DNS
15	Název domény DNS
44	Server WINS (server názvů typu NetBIOS)
45	Server distribuující datagramy typu NetBIOS (NBDD)
46	Typ uzlu WINS/NetBIOS
47	ID oboru NetBIOS

Klienti mohou obdržet tyto hodnoty pro nastavení konfigurace jejich protokolu TCP/IP během doby trvání zápůjčky.

Vnitřní Možnosti protokolu

Tabulka 4.7 znázorňuje interní typy možností protokolu, které si klienti DHCP mohou nakonfigurovat při komunikaci se serverem DHCP o získání nebo obnovení zápůjčky.

Tabulka 4.7 Obvyklé interní typy možností protokolu

Kód	Popis
51	Doba zápůjčky
52	Typ zprávy DHCP
55	Speciální typ možnosti používaný ke sdělení seznamu požadovaných parametrů serveru DHCP
58	Hodnota času obnovení (T1)
59	Hodnota času obnovení vazeb (T2)

Ve většině případů jsou skutečné hodnoty poskytované klientům pomocí těchto typů možností získány z nastavení vlastností služby DHCP na serveru DHCP.

Možnosti pro klienty se vzdáleným přístupem

Když klient se vzdáleným přístupem získá od serveru se vzdáleným přístupem zápůjčku adresy IP, spusíte program Winipcfg.exe (pro Windows 95) nebo Ipconfig.exe (pro Windows 2000 nebo Windows NT), který zobrazí informace o této zápůjčce.

Když server se vzdáleným přístupem přiřadí adresu IP klientovi se vzdáleným přístupem, ať už s vlastního statického fondu adres nebo z fondu adres DHCP v mezipaměti, přiřadí adresu IP, tato adresa IP nemá žádný efektivní čas zápůjčky, protože je uvolněna v okamžiku odpojení klienta.

Nicméně klienti se vzdáleným přístupem stále mohou od serveru se vzdáleným přístupem získat další informace o konfiguraci protokolu TCP/IP: Přiřazení serveru WINS a přiřazení serveru DNS mohou být delegována klientovi při jeho připojení. Tato nastavení jsou delegována přímo z nastavení serveru se vzdáleným přístupem. Jestliže server se vzdáleným přístupem má jako nakonfigurované záznamy ve vlastnostech telefonického připojení uvedený server WINS nebo server DNS, jsou tato nastavení předána na klienta se vzdáleným přístupem, který podporuje službu DHCP.

Tabulka 4.8 obsahuje seznam typů možností DHCP podporovaných klienty na platformě WINDOWS, které jsou přiřazovány klientům prostřednictvím telefonického připojení k síti se serverem se vzdáleným přístupem.

Tabulka 4.8 Možnosti DHCP používané klienty na platformě Windows se vzdáleným přístupem a podporujícími službu DHCP

Možnost	Popis
Adresa IP	Sever se vzdáleným přístupem získá adresu IP od serveru DHCP a vystaví si v mezipaměti fond zapůjčených adres služby DHCP. Server se vzdáleným přístupem pak na žádost distribuuje adresy IP z mezipaměti klientům se vzdáleným přístupem a spravuje jejich zápůjčky. To je jediná informace, kterou klient se vzdáleným přístupem dostane od serveru DHCP.
Server WINS	Jestliže je server se vzdáleným přístupem nakonfigurován na adresy serveru WINS, hodnoty poskytnuté typem možnosti jsou získány z vlastností telefonického připojení serveru se vzdáleným přístupem. Klient získá seznam serverů WINS, které jsou nakonfigurovány na serveru se vzdáleným přístupem.
Server DNS	Jestliže je server se vzdáleným přístupem nakonfigurován na adresy serveru DNS, hodnoty poskytnuté typem možnosti jsou získány z vlastností telefonického připojení serveru se vzdáleným přístupem. Klient získá adresu prvního serveru DNS uvedeného na seznamu vyhledání serverů DNS serveru se vzdáleným přístupem.
Maska podsítě	Maska podsítě odpovídá přednastavené masce podsítě spojené s typem třídy standardní adresy (třída A, B nebo C) dané adresy IP.
ID oboru NetBIOS	Informace o ID oboru NetBIOS nejsou předávány klientovi. Jestliže potřebujete upravit toto nastavení, musíte ho změnit přímo na klientovi.

Možnost	Popis
Typ uzlu	Typ uzlu není získáván ze zápůjčky DHCP, ale lze ho měnit na klientovi se vzdáleným přístupem v závislosti na informacích WINS. Jestliže server se vzdáleným přístupem nemá lokálně definované servery WINS, klient se vzdáleným přístupem a typem uzlu b zůstává klientem s typem uzlu b. Jestliže server se vzdáleným přístupem má lokálně definované servery WINS, klient se vzdáleným přístupem a typem uzlu b se změní na uzel h po dobu trvání připojení. Klienti na platformě Windows 95 svůj typ uzlu automaticky nezmění, pokud server se vzdáleným přístupem dodá adresy WINS. V tomto případě musíte změnit typ uzlu ručně.

Třídy možností

Tato vlastnost umožňuje rychlé uvedení zakázkových aplikací pro rozsáhlé sítě. Třídy možností DHCP poskytují způsob snadné konfigurace síťových klientů parametry potřebnými ke splnění zvláštních požadavků zakázkových aplikací. Zařízení více dodavatelů na síti také mohou používat různá čísla možností pro různé funkce. Typy možností používané k podpoře tříd dodavatele – identifikátor třídy dodavatele a možnost specifická pro určitého dodavatele – jsou definovány v dokumentu RFC 2132.

U operačního systému Windows 2000 Server jsou dva typy tříd možností: dodavatelem definované a uživatelem definované. Tyto třídy lze nakonfigurovat na vašich serverech tak, aby nabízely speciální podporu klienta následujícími způsoby:

- Přidat a nakonfigurovat třídy definované dodavatelem pro podsprávu možností DHCP přiřazených klientům dle typu dodavatele.
- Přidat a nakonfigurovat třídy definované uživatelem pro podsprávu možností DHCP přiřazených klientům dle obvyklých potřeb na konfiguraci podobných možností DHCP.

Po definování tříd možností na serveru DHCP je třeba nakonfigurovat obory tak, aby přiřazovaly možnosti určitým třídám definovaným dodavatelem a třídám definovaným uživatelem.

Třídy dodavatele

Třídy definované dodavatelem mohou být při získávání zápůjčky použity klienty DHCP ke zjištění typu dodavatele klienta a jeho konfigurace pro DHCP server. Klient identifikuje svou třídu dodavatele během procesu zápůjčky tím, že musí zahrnout možnost ID třídy dodavatele (kód možnosti 60) při žádosti nebo výběru zápůjčky od serveru DHCP.

Identifikátor třídy dodavatele je řetězec znaků interpretovaný servery DHCP. Dodavatelé si mohou vybrat, že budou definovat zvláštní identifikátory třídy dodavatele pro přenášení určité konfigurace nebo jiné identifikační informace o klientovi. Například identifikátor může mít zakódovanou hardwarovou nebo softwarovou konfiguraci klienta. Většina typů dodavatele je odvozena ze standardních rezervovaných zkrácených kódů typů hardwaru a operačních systémů obsažených v dokumentu RFC 1700.

Po specifikaci možnosti dodavatele server provádí následující další kroky, aby poskytl klientovi zápůjčku:

1. Server kontroluje, jestli třída dodavatele obsažená v požadavku klienta je rozpoznanou třídou definovanou na serveru.
Jestliže je třída dodavatele rozpoznána, server zkontroluje, jestli jsou v aktivním oboru pro tuto třídu nakonfigurovány nějaké další možnosti DHCP.
Jestliže třída dodavatele není rozpoznána, server ignoruje třídu dodavatele obsaženou v požadavku klienta a vrátí možnosti přiřazené přednastavené třídě dodavatele (včetně všech standardních možností DHCP).
2. Jestliže obor obsahuje možnosti konfigurované speciálně pro použití u klientů s takovouto třídou definovanou dodavatelem, server vrátí tyto možnosti za použití typu možnosti určitého dodavatele (kód možnosti 43) jako součást potvrzující zprávy.

Ve většině případů přednastavená třída dodavatele – standardní možnosti DHCP – poskytuje přednastavenou třídu dodavatele pro seskupení jakýchkoli klientů podporujících službu Microsoft DHCP nebo dalších klientů podporujících službu DHCP, kteří neurčí ID třídy dodavatele. V některých případech byste mohli definovat další třídy dodavatele pro některé klienty DHCP, například pro tiskárny nebo některé typy klientů na platformě UNIX. Při přidávání dalších tříd dodavatele pro tyto účely si ověřte, že identifikátor třídy dodavatele, který používáte ke konfigurování třídy na serveru, odpovídá identifikátoru použitému klienty daného nezávislého dodavatele.

Třídy uživatele

Třídy uživatele umožňují klientům DHCP, aby se sami rozlišovali pomocí určení typu klienta, například se vzdáleným přístupem nebo kancelářský počítač. U počítačů na platformě Windows 2000 můžete definovat identifikátory určité třídy uživatele, které předají informace o konfiguraci softwaru klienta, jeho fyzickém umístění v budově nebo o předvolbách jeho uživatele. Například identifikátor může určovat, že klienti DHCP jsou členy třídy definované uživatelem nazvané „2. podlaží, západ“, což je třeba pro speciální sadu nastavení směrovače a serverů DNS a WINS. Správce může pak nakonfigurovat server DHCP tak, aby konfiguroval různé typy možností v závislosti na typu klienta získávajícího zápůjčku.

Třídy uživatele pod Windows 2000 lze použít následujícími způsoby:

- Klientské počítače DHCP mohou obsahovat možnost třídy uživatele DHCP při posílání požadavku DHCP na server DHCP. To může zvláště identifikovat klienta jako součást třídy uživatele na serveru.
- Servery DHCP se spuštěnou službou Microsoft DHCP mohou rozpoznat a interpretovat možnost třídy uživatele DHCP od klientů a poskytovat další možnosti (nebo upravenou sadu možností DHCP) založenou na identitě třídy uživatele klienta.

Například klientům se vzdáleným přístupem by měly být přiřazovány kratší zápůjčky. Kancelářské počítače na stejné síti by mohly vyžadovat zvláštní nastavení, například platformy CAD. Tyto varianty mohou také obsahovat nastavení serveru WINS a DNS. Jestliže nejsou specifikovány třídy možnosti definované uživatelem, je přiřazováno výchozí nastavení (například možnosti serveru nebo možnosti oboru).

Třída definovaná uživatelem může být buď přednastavená nebo upravená pro uživatele. Microsoft poskytuje tři přednastavené třídy uživatele, viz tabulka 4.9.

Tabulka 4.9 Přednastavené třídy uživatele poskytované službou Microsoft DHCP

Typ třídy	Řetězec ID třídy	Popis
Přednastavená třída uživatele	Neurčen	<p>Používána službou DHCP ke klasifikaci klientů, kteří neuvádějí další totožnost nebo typ. Tato třída je typicky používána většinou klientů DHCP. Klienti jsou přiřazováni do této třídy za následujících podmínek:</p> <ul style="list-style-type: none"> ■ Klienti DHCP nemají žádný pojem třídy uživatele nebo ID třídy uživatele. Toto platí o většině klientů předcházejících verzí Windows, než jsou Windows 2000. ■ Klienti Windows 2000 s nakonfigurovaným ID třídy, které je pro server DHCP neznámé (například server nemá tuto třídu nadefinovanu).
Přednastavená třída Routing and Remote Access	RRAS.Microsoft	<p>Používaná službou Microsoft DHCP ke klasifikaci klientů připojujících se typem připojení PPP přes server vzdáleného přístupu. Typicky tato třída zahrnuje většinu klientů s telefonickým připojením, kteří používají službu DHCP k získání zápujčky:</p> <ul style="list-style-type: none"> ■ Klienti se vzdáleným přístupem, kteří nemají žádný pojem třídy uživatele Routing and Remote Access nebo ID třídy uživatele Routing and Remote Access. <p>Podrobnosti o interakci mezi serverem s vlastností Routing and Remote Access a serverem DHCP a způsobu, jakým servery identifikují klienty Routing and Remote Access, najdete později v této kapitole v části „DHCP a služba Routing and Remote Access“</p>
Přednastavená třída BOOTP	BOOTP	<p>Používána službou Microsoft DHCP ke klasifikaci jakýchkoli klientů rozpoznaných jako klienti BOOTP.</p>

Používání přednastavených tříd uživatele Microsoft může být užitečné pro izolaci podrobností konfigurace klientů se speciálními potřebami, například u starších klientů nebo klientů, kteří používají BOOTP nebo Routing and Remote Access. Například můžete chtít zahrnout a přiřadit zvláštní typy možnosti BOOTP (například kódy možnosti 66 a 67) klientům typu BOOTP nebo zkrátit dobu trvání zápujčky klientům se vzdáleným přístupem.

Můžete také přidat a nakonfigurovat vlastní třídy uživatele pro klienty DHCP se spuštěným operačním systémem Windows 2000. U vlastních tříd uživatele musíte specifikovat vlastní identifikátor, který musí odpovídat třídě uživatele definované na serveru DHCP.

Momentálně pole možnosti třídy uživatele umožňuje použití pouze jednoho řetězce znakové sady DOS (ASCII) pro identifikaci klienta. To znamená, že každý klientský počítač může být identifikován serverem DHCP pouze jako člen jedné třídy uživatele. Pokud je to potřeba, můžete používat další třídy uživatele a vytvořit nové hybridy z ostat-

ních tříd uživatele. Například, máte-li dvě třídy uživatele, jednu nazvanou „mobilní“ s krátkou dobou trvání zápůjčky a jinou nazvanou „pracovní“ s přiřazenou možností konfigurovat vysokovýkonnostní server pro své klienty, můžete vytvořit novou hybridní třídu nazvanou „mobilní – pracovní“, která bude zapůjčovat adresy klientům, kteří mají specifikovány potřeby konfigurace přesahující danou třídu.

Možnosti konfigurace

Následující postup vám může pomoci při určování úrovně konfigurace a přiřazení možností DHCP klientům na vaší síti:

- Přidejte nebo definujte nové vlastní typy možností pouze v případě, že máte nový software nebo aplikace, které vyžadují nestandardní možnosti DHCP.
- Máte-li rozsáhlou síť, buďte při přiřazování obecných možností vybíraví a konzervativní. Tyto možnosti se budou aplikovat na všechny klienty serveru DHCP.
- Používejte pro většinu možností přiřazovaných klientům možnosti na úrovni oboru. Na většině sítí je při přiřazování možností úroveň oboru upřednostňována.
- Jestliže máte rozsáhlou síť nebo skupiny klientů s odlišnými potřebami, kteří jsou schopni podporovat členství ve třídách možností (například klienti na platformě Windows 2000), používejte možnosti třídy.
- Používejte možnosti rezervovaného klienta pouze pro klienty, kteří mají speciální požadavky, například jestliže intranet má server DNS, který provádí předávání pro překlad názvů Internet DNS, které není na síti autoritativně spravováno. V takovém případě potřebujete přidat adresu IP externího serveru DNS na počítači serveru DNS. Můžete nakonfigurovat svůj server DNS jako rezervovaného klienta služby DHCP a nastavit tuto adresu jako další možnost rezervovaného klienta.

Priorita možností

Služba DHCP používá při určování, kterou možnost prosazovat, vzestupnou hierarchii. To zjednodušuje správu služby DHCP a umožňuje pružnou administraci, která může být od výchozích nastavení serverů až po individualizované nastavení klienta pro zvláštní okolnosti.

Základní pravidla používání možností jsou tato:

- Vždy se aplikují aktivní obecné možnosti, pokud nepřeváží možnosti oboru, třídy nebo rezervovaného klienta.
- Vždy se na všechny počítače získávající zápůjčku z určitého oboru aplikují aktivní možnosti tohoto oboru, pokud nepřeváží možnosti třídy nebo rezervovaného klienta.
- Vždy se na všechny počítače konfigurované jako členy určité třídy aplikují aktivní možnosti této třídy, pokud nepřeváží možnosti rezervovaného klienta.
- Možnosti rezervovaného klienta jsou nadřazeny všem dalším možnostem.
- Staticky nakonfigurované hodnoty na klientovi jsou nadřazené jakýmkoli možnostem DHCP jakékoli úrovně.

Protokol DHCP s vícesměrovým vysíláním

Protokol DHCP s vícesměrovým vysíláním, označovaný jako MADCAP (Multicast Address Dynamic Client Allocation Protocol) je nyní součástí služby DHCP pro Win-

dows 2000 a používá se k podpoře dynamického přiřazování a konfigurace adres IP víceměrového vysílání na sítích na platformě protokolu TCP/IP.

Zpravidla obory DHCP používáte ke konfigurování klientů alokačními rozsahy adres IP tříd A, B nebo C. Prostřednictvím těchto oborů a rozsahů adres jsou klienti nakonfigurováni k používání jednosměrové komunikace point-to-point mezi dvěma počítači na síti.

V operačním systému Windows 2000 Server nabízí služba DHCP podporu služby MADCAP ve formě oborů víceměrového vysílání. Obor víceměrového vysílání se konfiguruje stejně jako obvyklý obor DHCP, ale poskytuje rozsahy oboru víceměrových adres IP třídy D. Tyto adresy jsou rezervovány pro operace víceměrového vysílání používajícího směrového přenosu z jednoho na více bodů.

Pozadí víceměrového vysílání

Skupina počítačů s protokolem TCP/IP může používat adresy IP víceměrového vysílání k posílání směrované komunikace na všechny počítače, se kterými sdílí skupinovou adresu. Adresy víceměrového vysílání sdílí mnohou počítačů.

Když je cílová adresa datagramu IP adresa víceměrového vysílání, paket je předán všem členům skupiny víceměrového vysílání, což je množina žádného či více počítačů identifikovaných touto adresou víceměrového vysílání.

Dynamické členství

Adresy víceměrového vysílání podporují dynamické členství, které umožňuje jednotlivým počítačům se kdykoli přidávat ke skupině víceměrového vysílání a také ji kdykoli opouštět. Členství ve skupině není omezeno velikostí skupiny a počítače se mohou stát členy kterékoli skupiny. Navíc jakýkoli počítač používající protokol TCP/IP může posílat datagramy jakékoli skupině víceměrového vysílání. Adresa skupiny víceměrového vysílání je podobná svým použitím skupinové elektronické adrese. Když je adresa IP víceměrového vysílání použita jako cílová adresa datagramu IP, datagram je předán všem členům skupiny víceměrového vysílání určené touto adresou.

Rozsahy adres víceměrového vysílání

Adresy skupiny víceměrového vysílání můžete trvale rezervovat nebo je přiřazovat a využívat dočasně. Trvalá skupina je tvořena trvale rezervovaným ID adresy IP třídy D (224.0.0.0 až 239.255.255.255) přiřazeným IANA. Rezervovaná adresa se pak stává známou adresou označující určitou skupinu víceměrového vysílání, která existuje nezávisle na tom, jestli členové této skupiny jsou přítomni na síti. Adresy IP víceměrového vysílání, které nejsou trvale rezervovány IANA, mohou být všechny adresy třídy D, které zůstanou nerezervované, použity k dynamickému přiřazování a tvoření dočasných skupin víceměrového vysílání. Tyto dočasné skupiny mohou existovat tak dlouho, dokud je jeden nebo více počítačů na síti nakonfigurováno na adresu skupiny a aktivně se podílí na jejím užívání.

Podpora služby MADCAP

Klienti používající službu MADCAP musí být nakonfigurováni tak, aby mohli používat rozhraní MADCAP API. Více informací o psaní nebo programování aplikací, které užívají toto rozhraní API, najdete v prostředcích vývoje, které jsou dostupné přes síť MSDN.

MADCAP se podílí na zjednodušování a automatizaci konfigurace skupin vícesměrového vysílání na síti, ale není požadován pro operace skupin vícesměrového vysílání nebo pro službu DHCP. Obory vícesměrového vysílání pouze poskytují konfiguraci adres a nepodporují nebo nepoužívají další možnosti přiřaditelné službě DHCP.

Konfigurace MADCAP adresy klientovi by měla být provedena nezávisle na tom, jak jsou klienti nakonfigurováni pro získání své primární adresy IP. Klienty MADCAP mohou být počítače, které používají buď statickou nebo dynamickou konfiguraci prostřednictvím serveru DNS.

Služba DHCP pro Windows 2000 podporuje jak DHCP, tak MADCAP, přestože tyto služby fungují odděleně. Klienti jedné služby nejsou závislí na používání nebo konfiguraci druhé služby.

- Klienti, kteří jsou nakonfigurováni ručně, nebo používají k získání zápůjčky adresy IP jednosměrného vysílání službu DHCP také používají službu MADCAP, a to k získání konfigurace adresy IP vícesměrového vysílání.
- Klienti, kteří nepodporující službu MADCAP nebo se nejsou schopni připojit a získat konfiguraci vícesměrového vysílání od serveru MADCAP, mohou být nakonfigurováni jiným způsobem, takže se mohou účastnit trvalých i dočasných skupin vícesměrového vysílání na síti.
- Ve všech sítích TCP/IP vyžaduje každý počítač jedinečnou primární adresu IP počítače (která není sdílena nebo duplikovaná) z jedné ze standardních adresových tříd používaných pro výstavbu sítí (rozsah třídy A, B, C). Tuto požadovanou primární adresu IP musíte počítači přiřadit ještě před tím, než můžete počítač nakonfigurovat k podpoře a používání sekundární adresy IP, například adres IP vícesměrového vysílání.
- Při používání konfigurace adresy vícesměrového vysílání může server MADCAP dynamicky provádět tuto konfiguraci u klientů, kteří podporují protokol MADCAP.

Databáze DHCP

Servery DHCP pro Windows 2000 používají jádro výkonově vylepšeného úložiště Exchange Server Storage verze 4.0.

Databáze služby DHCP je dynamickou databází, která je aktualizována společně s přiřazováním konfiguračních parametrů protokolu TCP/IP klientům DHCP nebo s jejich uvolňováním. Vzhledem k tomu, že databáze DHCP není distribuovanou databází jako databáze serveru WINS, je udržování databáze služby DHCP jednodušší.

Správa databáze

Následující odstavce popisují administrativní úlohy při správě databáze služby DHCP. Aby se předešlo vysokým nákladům, provádí tyto úlohy automaticky operační systém Windows 2000, ale může je provádět též ručně správce sítě.

Správa záznamů

Neexistuje žádný vestavěný limit počtu záznamů, který server DHCP může uchovávat. Velikost databáze závisí na počtu klientů DHCP na síti. Databáze služby DHCP roste v průběhu času jako důsledek toho, že se klienti připojují k síti a zase se od ní odpo-

jují. Během doby záznamy některých klientů DHCP zastarají a jsou odstraněny, takže zůstane určitý nevyužitý prostor.

Správa úložného prostoru

K obnově nepoužívaného prostoru je třeba databázi DHCP zkomprimovat. Operační systém Windows 2000 dynamicky komprimuje databázi automaticky na pozadí během doby nečinnosti po aktualizaci databáze. Ačkoli dynamické komprimování velice snižuje potřebu provádění komprese v režimu offline, zcela ji nelikviduje. Komprese v režimu offline získá prostor efektivněji a měla by být u velkých sítí s více než 1000 klienty DHCP prováděna minimálně jednou za měsíc. U menších sítí ruční komprese postačí každých několik měsíců.

Vzhledem k tomu, že dynamická komprese databáze se provádí na pozadí, zatímco se databáze používá, nemusíte zastavit server DHCP. Nicméně pro ruční kompresi musí být server DHCP v režimu offline.

Zálohy databáze

Databáze služby DHCP a k ní se vztahující záznamy v registru jsou automaticky zálohovány v určeném intervalu. Tento přednastavený interval můžete upravovat změnou hodnoty záznamu BackupInterval v registru v následujícím podklíči registru: HKEY_LOCAL_COMPUTER\SYSTEM\CurrentControlSet\Services\DHCP\Parameters

Upozornění Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správcovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. Ke konfiguraci nebo přizpůsobení si Windows 2000 používejte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Soubory databáze služby DHCP

Při instalaci služby DHCP jsou v adresáři %SystemRoot%\System32\Dhcp automaticky vytvořeny soubory uvedené v tabulce 4.10.

Tabulka 4.10 Soubory databáze a jejich popis

Soubor	Popis
J50.log a J50xxx.log	Protokol všech transakcí provedených v databázi DHCP. Tento soubor je v případě nutnosti používán službou DHCP ke zotavení dat. Ke zvýšení rychlosti a efektivity ukládání dat databáze zapisuje aplikace Jet aktuální transakce spíše do protokolů než přímo do databáze. Proto je nejaktuálnější pohled na data databáze plus některé transakce v souborech protokolů. Tyto soubory protokolů jsou také používány ke zotavení, když je služba DHCP zastavena nějakým neočekávaným způsobem. Jestliže je služba DHCP zastavena nějakým neočekávaným způsobem, soubory protokolů jsou automaticky použity ke znovuvytvoření správného stavu databáze DHCP.

Soubor	Popis
	<p>Soubory protokolů mají vždy určitou velikost. Nicméně jejich počet na velmi zaneprázdněném serveru DHCP může rychle vzrůst. Je nevyhnutelné, že DHCP bude do protokolu zapisovat více, než jeho velikost může zvládnout. Po naplnění je soubor protokolu přejmenován, aby bylo zřejmé, že se jedná o starší protokol a že se již nepoužívá. Je vytvořen nový protokol o transakcích s názvem souboru Jn.log (kde n je desítkové číslo), například J50.log. Formát názvu předchozího souboru protokolu bude Jetxxxxx.log, kde každé x označuje šestnáctkové číslo od 0 do F. Předcházející soubory protokolu jsou udržovány ve stejné složce jako aktuální soubory protokolu.</p> <p>Soubory protokolu jsou zpracovány (všechny záznamy protokolu jsou zapsány do databáze) a odstraněny, když se provede úspěšně záloha nebo když je server DHCP korektně vypnut. Proto jestliže se nahromadí mnoho souborů Jn.log, měly by být prováděny pravidelně časté zálohy.</p> <p>Pro zpracování záznamů je možné ručně odstranit soubory protokolů. To nicméně zabrání úspěšnému zotavení databáze, pokud by vyvstala jeho potřeba. Je proto důležité, aby soubory protokolů nebyly manuálně odstraňovány nebo odebírány ze systému, dokud neproběhne záloha.</p>
J50.chk	<p>Soubor kontroly, který označuje umístění poslední informace úspěšně zapsané z logů o transakcích do databáze. Používá se také pro účely zotavení – soubor kontroly označuje, kde by mělo začít zotavení nebo znovunahrání dat. Tento soubor kontroly je aktualizován při každém zápisu dat do souboru databáze (DHCP.mdb).</p>
Dhcp.mdb	<p>Soubor databáze DHCP, který obsahuje dvě tabulky: mapovací tabulku adres IP a ID vlastníka a mapovací tabulku názvu a adresy IP.</p>
Dhcptmp.mdb	<p>Dočasný soubor, který je vytvořen serverem DHCP. Tento soubor používá databáze jako odkládací soubor během operací udržujících indexy a může po pádu zůstat v adresáři %SystemRoot%\System32\DHCP.</p>
Resx.log	<p>Toto jsou rezervované soubory protokolu, které jsou udržovány pro případ nouze. Jsou použity v případě, že serveru dojde místo na disku. Pokud se server pokusí vytvořit další soubor protokolu o transakcích a není zde dostatek místa, server přesune všechny významné transakce do těchto rezervovaných souborů protokolu. Služba se pak vypne a zaznamenaná událost do protokolu událostí.</p>

Služba DHCP používá formát databáze aplikace Jet pro ukládání svých dat. Aplikace Jet vytváří ve složce %SystemRoot%\System32\DHCP soubor Jn.log a další soubory, aby zvýšila rychlost a efektivnost ukládání dat.

Upozornění Soubory J50.log, J50xxxxx.log, Dhcp.mdb, Dhcptmp.mdb, a Resx.log by neměly být v žádném případě odebírány ani by se s nimi nemělo žádným způsobem manipulovat.

Podpora klientů BOOTP

Protokol BOOTP (Bootstrap Protocol) je protokol pro konfiguraci počítače vyvinutý před protokolem DHCP. Protokol DHCP vylepšuje protokol BOOTP a řeší zvláštní omezení protokolu BOOTP, které měl jako služba pro konfiguraci počítače. Protokol BOOTP je definován v dokumentu RFC 951.

Protokol BOOTP byl zamýšlen ke konfigurování pracovních stanic bez disků s omezenou možností spuštění, zatímco protokol DHCP byl zamýšlen ke konfigurování často přemísťovaných počítačů v síti (například notebooky), které mají lokální pevné disky a plnou možnost spuštění.

Vzhledem k příbuznosti mezi protokoly BOOTP a DHCP, oba protokoly sdílí některé definiční charakteristiky. Společné prvky zahrnují:

- Struktura formátu použitá k výměně zpráv klienta/serveru.

Protokoly BOOTP a DHCP používají téměř identické požadavky (odesílané klienty) a odpovědi (odesílané servery). Zprávy v obou těchto protokolech používají jeden datagram UDP o velikosti 576 bajtů, který uzavírá každou zprávu protokolu. hlavičky zpráv jsou u obou protokolů stejné s jednou výjimkou: hlavičkou závěrečné zprávy používané k přenosu nepovinných dat. U protokolu BOOTP je toto nepovinné pole nazváno oblastí určenou dodavatelem a je omezeno na 64 oktetů. U protokolu DHCP je tato oblast nazvána možností a může nést až 312 oktetů nepovinných informací protokolu DHCP.

Vzhledem k tomu, že zprávy DHCP i BOOTP používají téměř identický typ formátu a strukturu paketu, typicky používají stejné známé porty služeb, programy přenosového agenta BOOTP nebo DHCP se obvykle ke zprávám BOOTP i DHCP chovají jako ke stejnému typu zpráv bez toho, že by mezi nimi rozlišovaly.

- Použití známých portů UDP pro komunikaci klient/server.

Jak protokol BOOTP, tak protokol DHCP používají pro odesílání a přijímání zpráv mezi servery a klienty stejné rezervované porty protokolu. Servery BOOTP i DHCP používají k naslouchání a přijímání požadavků klientů port UDP 67. Klienti BOOTP a DHCP typicky rezervují port UDP 68 pro přijímání odpovědí ze serveru BOOTP, resp. DHCP.

- Distribuce adres IP jako integrální součást služby konfigurace.

Ačkoli jak protokol BOOTP, tak protokol DHCP přiřazují adresy IP klientům během spouštění, používají různé metody přiřazování. Protokol BOOTP zpravidla poskytuje pevné přiřazení jedné adresy IP pro každého klienta, přičemž tuto adresu trvale rezervuje v databázi serveru BOOTP. Protokol DHCP zpravidla poskytuje dynamické, zapůjčené přiřazení dostupných adres IP, přičemž dočasně rezervuje adresu každého klienta DHCP v databázi serveru DHCP.

- Nahrávání spouštěcího souboru klientem BOOTP je prováděno za použití protokolu TFTP.

Klienti kontaktují servery TFTP, aby provedli přenos souboru své spouštěcí bitové kopie. Vzhledem k tomu, že operační systém Windows 2000 neposkytuje službu protokolu TFTP, potřebujete server TFTP třetí strany, aby podporoval klienty BOOTP, kteří se musí spouštět ze spouštěcí bitové kopie (obvykle pracovní stanice bez disku). Také potřebujete nakonfigurovat server DHCP tak, aby poskytoval podporované možnosti BOOTP/DHCP.

Implementace podpory protokolu BOOTP popsané v této části předpokládá, že služba DHCP je již pro klienty DHCP nainstalovaná a správně nakonfigurovaná.

Více informací o protokolu BOOTP najdete v dokumentech RFC 1532, RFC 2131 a RFC 2132. Podpora protokolu BOOTP je také dostupná u operačního systému Windows NT Server 4.0 s aktualizací Service Pack 2 a pozdější.

Rozdíly mezi BOOTP a DHCP

I přes uvedené podobnosti jsou ve způsobu, jakým protokoly BOOTP a DHCP provádějí konfiguraci klientů, značné rozdíly:

- Protokol BOOTP podporuje omezený počet parametrů pro konfiguraci klienta nazvaný rozšíření dodavatele, zatímco protokol DHCP podporuje rozsáhlejší a rozšiřitelnou sadu parametrů pro konfiguraci klienta nazvanou možností.
- Protokol BOOTP používá dvoufázový samozaváděcí proces konfigurace, ve kterém klienti kontaktují servery BOOTP, aby byla provedeno určení adresy a výběr spouštěcího souboru, a klienti kontaktují servery TFTP, aby prováděly přenos souborů jejich spouštěcí bitové kopie. Protokol DHCP používá jednofázový samozaváděcí proces konfigurace, ve kterém klient DHCP vyjednává se serverem DHCP o určení adresy IP a získání dalších počátečních detailů konfigurace, které potřebuje pro operace na síti.
- Klienti BOOTP neobnovují vazby nebo konfiguraci se serverem BOOTP s výjimkou restartu systému, zatímco klienti DHCP k obnovení vazeb nebo konfigurace se serverem DHCP restart systému nevyžadují. Namísto toho klienti automaticky přecházejí do stavu obnovení vazeb v nastavených časových intervalech, aby obnovili svá zapůjčená umístění adres u serveru DHCP. Tento proces probíhá na pozadí a je pro uživatele zcela transparentní.

Klienti BOOTP požadující pouze informace o adrese IP

Dříve podpora klientů BOOTP prostřednictvím serveru DHCP vyžadovala výslovnou rezervaci klienta pro každého klienta BOOTP.

S novou podporou dynamického protokolu BOOTP může být předem určen fond adres – podobně jako obor u klientů DHCP – k dynamické správě přiřazování adres IP klientům BOOTP: Služba DHCP může později nárokovat adresy použité ve fondu adres dynamického protokolu BOOTP, a to teprve po ověření, že určený čas zápůjčky vypršel a žádná adresa není nadále používána klientem BOOTP.

Prvně musíte na serveru nakonfigurovat fond adres BOOTP v rámci oboru DHCP a teprve poté můžete nakonfigurovat server DHCP tak, aby přiřazoval a distribuoval adresy IP klientům BOOTP.

Další možností fondu adres dynamického protokolu BOOTP je přidání rezervace klienta pro každého klienta BOOTP v rámci oborů DHCP. Rezervace vytvoří asociaci mezi adresou MAC klienta BOOTP (zakódovanou ve fyzickém hardwaru) a jeho zapůjčenou adresou IP. Když rezervovaný klient žádá rezervaci adresy IP, služba DHCP vrátí odpovídající rezervovanou adresu IP v odpovědi založené na adrese MAC klienta zahrnuté v požadavku BOOTP.

Klienti BOOTP požadující informace o spouštěcím souboru

Službu DHCP nakonfigurujete, aby klientům BOOTP poskytovala informace o spouštěcím souboru, takto:

1. Vytvořte rezervaci klienta pro každého klienta BOOTP v rámci aktivního oboru DHCP.

Adresy BOOTP musí být rezervovány rezervací adresy IP, kterou provedete pro každého klienta BOOTP. Po rezervování klientů vložte fyzickou adresu nebo adresu MAC klienta BOOTP, jak je přiřazena LAN adaptéru v dialogovém okně **Přidat rezervaci/Jedinečný identifikátor**. Klienti BOOTP používají tuto adresu při spuštění a odesílání požadavku BOOTP. Ve stejném dialogovém okně pod **Povolené typy klientů** byste při vytváření rezervace každého klienta BOOTP měli klepnout buď na možnost **Pouze BOOTP** nebo na možnost **Oba**.

2. Pro každého klienta v tabulce BOOTP vytvořte na serveru BOOTP záznamy BOOTP.

Informace uložené v tabulce BOOTP jsou vráceny kterémukoli dotazujícímu se klientovi na síti, který všesměrovým vysíláním pošle požadavek BOOTP. Pokud je do tabulky BOOTP přidán alespoň jeden záznam BOOTP, služba DHCP odpoví na požadavek klienta BOOTP. Jestliže nejsou nakonfigurovány žádné záznamy BOOTP, služba DHCP požadavek BOOTP ignoruje.

Odpověď vrácená službou DHCP označuje název a umístění dalšího serveru na síti (server TFTP), který pak může klient kontaktovat a získat od něj spouštěcí bitovou kopii.

Možnosti DHCP podporované pro klienty BOOTP

Klienti BOOTP, kteří nespecifikují kód možnosti DHCP 55 (parametr seznam požadavků možností), mohou i přesto získat od serverů DHCP s operačním systémem Windows NT Server 4.0 nebo pozdějším následující možnosti. Tabulka 4.11 obsahuje seznam možností DHCP dostupných klientům BOOTP.

Tabulka 4.11 Možnosti DHCP pro klienty BOOTP

Kód	Popis
1	Maska podsítě
3	Směrovač
4	Časový server
5	Názvový server
9	Server LPR
12	Název počítače
15	Název domény
17	Kořenová cesta
42	Servery NTP
44	Server WINS
45	Server distribuce datagramů typu NetBIOS pro TCP/IP
46	Typ uzlu typu NetBIOS pro TCP/IP
47	Obor typu NetBIOS pro TCP/IP
48	Server písem pro rozhraní X Windows

Kód	Popis
49	Správce zobrazení systému X Windows
69	Server SMTP
70	Server POP3

Aby získal tyto možnosti, musí klient specifikovat v požadavku BOOTP možnost 55. Servery Windows 2000 DHCP vrátí možnosti v pořadí uvedeném výše a vrátí tolik možností, kolik se jich vejde do jednoho datagramu odpovědi.

Důležité Při konfiguraci rezervací klienta pro klienty BOOTP nezapomeňte, že možnosti DHCP se mohou aplikovat jak na klienty DHCP, tak na klienty BOOTP. Je proto nezbytné správně nakonfigurovat obory.

Konfigurace tabulky BOOTP

Každý záznam v tabulce BOOTP obsahuje tři pole, které obsahují informace vrácení klientovi BOOTP:

- Spouštěcí bitová kopie. Identifikuje generický název souboru (například „unix“) požadovaného spouštěcího souboru v závislosti na typu hardwaru klienta BOOTP.
- Název souboru. Identifikuje plnou cestu spouštěcího souboru (například „/etc/vmunix“) vrácenou klientovi serverem BOOTP za použití protokolu TFTP.
- Název serveru. Identifikuje název serveru TFTP používaného jako zdroj spouštěcího souboru.

K přidání záznamů do tabulky BOOTP použijte Správce služby DHCP.

Plánování pro protokol DHCP

Implementace protokolu DHCP je tak těsně spjata se službou WINS a DNS, že správci sítě získají prospěch z kombinace všech tří při plánování instalací.

Používáte-li servery DHCP pro klienty sítě Microsoft, musíte používat službu překladu názvů. Sítě Windows 2000 používají k podpoře služby Active Directory službu DNS (navíc k obvyklému překladu názvů). Klienti sítě podporující Windows NT 4.0 a dřívější musí používat servery WINS. Klienti sítí podporujících kombinaci Windows 2000 a Windows NT 4.0 by měli implementovat jak službu WINS, tak DNS.

Nejlepší postupy

Před instalací serverů Microsoft DHCP na síti vezměte do úvahy nejlepší postupy:

Používání pravidla 80/20 Používání více než jednoho serveru DHCP na stejné podsíti zvyšuje odolnost proti chybám při obsluhování klientů DHCP umístěných na této podsíti. V případě dvou serverů může při selhání jednoho serveru být takový server nahrazen druhým, který pokračuje v zapůjčování nových adres nebo obnovování existujících klientů. To také pomáhá při vyvažování používání serverů.

Pro prostředí s více servery DHCP používejte množiny oborů Na každé podsíti v prostředí LAN s odlišnými obory pro každý server se doporučuje používat množiny oborů. Po-

užívání množin oborů jako způsob sdílení informací o všech oborech na všech serverech DHCP podsíti řeší problémy, například chybně klientovi zaslané negativní potvrzení.

Po spuštění každý klient DHCP pošle na svou lokální podsít omezeným všesměrovým vysíláním zprávu DHCPDiscover a snaží se najít server DHCP. Vzhledem k tomu, že klienti DHCP používají při počátečním spuštění všesměrové vysílání, nelze v případě více aktivních serverů na stejné podsíti předpovědět, který server bude reagovat na požadavek klienta DHCP.

Například pokud jsou dva servery DHCP – Server 1 a Server 2 nakonfigurovány různými rozsahy oborů dostupných adres, klient DHCP může získat zápůjčku od kteréhokoli z nich v závislosti na tom, který server odpoví jako první na požadavek všesměrového vysílání při počátečním spuštění počítače. Později může být server, který původně klientu DHCP poskytl zápůjčku, dočasně nedostupný během stavu obnovení (dle výchozího nastavení se klient snaží o obnovení po uplynutí 50 procent doby trvání zápůjčky).

Jestliže není obnovení úspěšné, klient odloží jakékoli snahy obnovit svou zápůjčku do doby, kdy vstoupí do stavu obnovení vazeb (dle výchozího nastavení klient vstoupí do stavu obnovení vazeb po uplynutí 87,5 procent doby trvání zápůjčky). Ve stavu obnovení vazeb klient pošle všesměrové vysílání po podsíti, aby získal platnou konfiguraci IP pro pokračování používání na síti. Pokud v tomto okamžiku na všesměrové vysílání klienta odpoví jiný server DHCP (tj. server DHCP odlišný od serveru, který poskytl klientovi první zápůjčku), pošle zprávu DHCPNak (negativní potvrzení). Důvodem je to, že tento server nezná současnou adresu klienta a nerozlišuje ji jako platnou adresu IP pro tuto podsít. Tato situace (DHCPNak) může nastat i v případě, že na síti je dostupný původní server DHCP, který klientovi poskytl zápůjčku.

Těmto problémům zabráníte při používání více než jednoho serveru DHCP na stejné podsíti použitím nové množiny oborů nakonfigurované podobně na všech serverech DHCP. Množina oborů by měla jako členské obory obsahovat všechny platné obory podsítě. Pro konfiguraci členských oborů na každém serveru musí být adresy dostupné pouze na jednom serveru DHCP na podsíti. Všechny ostatní servery na podsíti používají rozsahy vyloučení při konfiguraci odpovídajícího oboru.

Po vytvoření množiny oborů jsou všechny servery DHCP nakonfigurovány členskými obory, které vylučují adresy, které neobsluhují. Když server obdrží požadavek na obnovení, zkontroluje, jestli adresa IP klienta náleží do jednoho oborů, které zná:

- Pokud náleží do jednoho z těchto oborů a adresa spadá do rozsahu, který byl na serveru vyloučen, server tuto žádost o obnovení ignoruje.
- Jestliže server nemůže najít obory, které obsahují tuto adresu IP, server pošle jako odpověď na požadavek zprávu DHCPNak značící, že tato adresa by na této podsíti neměla být používána.
- Jestliže server není dostupný, klientovi vyprší časový limit a čeká na stav obnovení vazeb (T2), zpravidla při uplynutí 87,5 procenta doby trvání zápůjčky. Jestliže je v tomto okamžiku server stále nedostupný, klient používá svou aktuální adresu IP až do vypršení doby zápůjčky. Klient pak pošle zprávu DHCPDiscover všesměrovým vysíláním, aby získal novou zápůjčku. Jestliže původní server DHCP klienta (server, od kterého získal svou zápůjčku) je pořád nedostupný, požadavku klienta vyhoví jiný server DHCP na podsíti a přiřadí mu adresu IP a zápůjčku.

Obory deaktivujte pouze v případě, že obor natrvalo odebíráte ze služby.

Poté, co obor aktivujete a umístíte ho do služby, neměl by být deaktivován, pokud nechcete celý obor a v něm zahrnutý rozsah adres stáhnout z používání na síti. Je to proto, že po deaktivaci oboru server DHCP nadále neakceptuje adresy tohoto oboru jako platné adresy. To může být užitečné, máte-li v úmyslu stáhnout trvale obor z používání. V jiném případě může deaktivace oboru způsobit nežádoucí zprávy DHCPNk posílané servery DHCP klientům se zápůjčkou v tomto oboru.

Máte-li v úmyslu pouze dočasně ovlivnit deaktivaci oboru, upravte obory vyloučení v aktivním oboru, čímž nezpůsobíte nežádoucí problémy se zprávami DHCPNak, které se objeví po deaktivaci oboru.

Zjišťování konfliktů na serverech DHCP používejte pouze za neobvyklých podmínek.

U klientů DHCP na platformě Windows 2000, kteří získávají adresu IP, se používá k provádění zjišťování konfliktů ze strany klienta před dokončením konfigurace a použitím nabídnuté adresy IP nevyžádaný (gratuitous) požadavek ARP Request. Jestliže klient na bázi Windows 2000 je nakonfigurován na používání služby DHCP a zjistí konflikt, pošle serveru DHCP zprávu DHCPDecline. Klienti Microsoft TCP/IP na platformě Windows 95 zpravidla takto zjišťování konfliktů neprovádějí.

Jestliže síť obsahuje klienty DHCP na platformě Windows 95, měli byste používat zjišťování konfliktů ze strany serveru poskytované službou DHCP. Zjišťování konfliktů povolíte tak, že zvýšíte počet provedení příkazu ping, které provádí služba DHCP pro každou adresu přes zapůjčením této adresy klientovi.

Nezapomínejte, že každý další pokus zjistit konflikt, který provede služba DHCP, přidává další sekundu k času potřebnému pro vyjednání zápůjčky pro klienty DHCP.

Na všech serverech DHCP, které mohou potenciálně spravovat rezervované klienty, by měly být vytvořeny rezervace.

K zajištění, že klient DHCP při svém spuštění vždy obdrží zápůjčku stejné adresy IP, můžete používat rezervace klientů. Může-li rezervovaný klient dosáhnout více než jeden server DHCP, přidejte rezervaci na každý další server DHCP. To umožní ostatním serverům ctít rezervaci adresy pro tohoto klienta.

V takové situaci by všechny servery DHCP dosažitelné pro rezervovaného klienta měly být nakonfigurovány tak, jak bylo popsáno výše, tj. za použití množiny oborů s podobnými rozsahy oborů adres. Ačkoli s rezervací klienta bude pracovat pouze server DHCP, kde je rezervovaná adresa dostupná, můžete vytvořit stejnou rezervaci na dalších serverech DHCP, které tuto adresu vylučují.

Výkon serveru – nezapomínejte, že služba DHCP je náročná na prostor na disku a kupte hardware s optimálními vlastnostmi výkonu.

Služba DHCP způsobuje častou a intenzivní aktivitu na pevných discích serveru. K poskytnutí nejlepšího výkonu zvažte při kupování hardwaru pro server řešení RAID, které zlepšuje čas přístupu k disku.

Při hodnocení výkonu serverů DHCP byste měli na službu DHCP pohlížet jako na součást výkonu serveru jako celku. Díky sledování výkonu systémového hardwaru v nevyžadovanějších oblastech využití (CPU, paměť, vstup/výstup disku) získáte nejlepší přehled, kdy je server DHCP přetížen nebo potřebuje inovaci.

Nezapomínejte, že služba DHCP v operačním systému Windows 2000 Server obsahuje několik nových čítačů programu Sledování systému, které mohou být využity ke sledo-

vání služby. Více informací najdete v knize *Microsoft® Windows® 2000 Server Správa systému* v části „Přehled sledování výkonu“.

Nechtejte protokolování auditu povolené pro případ řešení problémů.

Dle výchozího nastavení služba DHCP povoluje protokolování auditu událostí spojených se službou. U operačního systému Windows 2000 Server poskytuje protokolování auditu nástroj dlouhodobého sledování služby, který provádí omezené a bezpečné využití prostředků disku serveru.

Snížte dobu trvání zápůjček pro klienty DHCP, kteří používají pro telefonické připojení k síti službu Routing and Remote Access.

Jestliže je na síti použita k podpoře klientů s telefonickým připojením služba Routing and Remote Access, můžete upravit dobu trvání zápůjčky na oborech, které obsluhují tyto klienty tak, aby používali dobu trvání zápůjčky kratší než je přednastavená doba pro obor, tedy osm dní. U operačního systému Windows 2000 je jedním z doporučených způsobů podpory klientů se vzdáleným přístupem v oboru přidání a konfigurace vestavěných třídy uživatelů Microsoft poskytovaná pro identifikaci klientů se vzdáleným přístupem.

Prodlužte dobu trvání zápůjček oborů pro rozsáhlé, pevné a stabilní sítě, jestliže je dostatek rozsahu adres.

U malých sítí (například jedna fyzická LAN nepoužívající směrovače) je typickou dobou trvání zápůjčky výchozí hodnota osm dní. U rozsáhlejších sítí se směrovači je s ohledem na delší dobu trvání zápůjček oborů tato doba 7 až 21 dní. To může snížit provoz na síti spojený s všesměrovým vysíláním služby DHCP, zvláště jestliže klientské počítače obecně zůstávají na pevném umístění a je dostatek adres oboru (dostupných je ještě minimálně 20 procent adres).

Integrujte službu DHCP mezi ostatní služby, například službu WINS nebo DNS.

Buď služba WINS nebo služba DNS (případně obě) jsou používány na síti pro registraci dynamického mapování názvů k adresám. Pro poskytování služeb překladu názvu musíte počítat se součinností služby DHCP s těmito ostatními službami. Většina správců sítě implementujících službu DHCP také plánuje strategii pro implementaci serverů DNS a WINS.

Používejte buď směrovače, které jsou schopné přenášet provoz zpráv DHCP a BOOTP, nebo používejte přenosové agenty a nastavte příslušné časovače, abyste předešli nežádoucímu předávání a přenosu zpráv BOOTP a DHCP.

Máte-li více fyzických sítí propojených směrovači, směrovače musí být schopné přenášet provoz BOOTP a DHCP. Ve směrovaných sítích, které používají k rozdělení na segmenty sítě podsítě, musí plánování možností služby DHCP zahrnovat některé specifické požadavky, aby služby DHCP plně fungovaly. tyto požadavky zahrnují následující:

- Jeden server DHCP musí být umístěn minimálně na jedné směrované podsíti.
- Aby server DHCP podporoval klienty na dalších vzdálených podsítích oddělených směrovači, musí být použit směrovač nebo vzdálený počítač jako přenosový agent BOOTP a DHCP, který bude podporovat předávání provozu DHCP mezi podsítěmi.

Nemáte-li takové směrovače, můžete nastavit součást služby DHCP, přenosového agenta DHCP, minimálně na jednom počítači se spuštěným operačním systémem Windows 2000 Server (nebo Windows NT Server) v každé směrované podsíti. Přenosový agent přenáší provoz zpráv BOOTP a DHCP mezi klienty podporujícími službu DHCP na lo-

kální fyzické síti a na vzdáleném serveru DHCP umístěném na jiné logické síti. při používání přenosového agenta se ujistěte, že jste nastavili a zvýšili počáteční čas, po kterém přenosový agent čeká před přenosem zpráv DHCP serverům. Více informací najdete později v této kapitole v části „Instalace přenosového agenta“.

Pro službu DNS s dynamickou aktualizací prováděnou serverem DHCP používejte přednastavená nastavení priorit klienta.

U operačního systému Windows 2000 Server provádí služba DHCP dynamickou aktualizaci klientů DHCP založenou na provádění žádostí klientů o aktualizaci. Toto nastavení nabízí nejlepší využití služby DHCP k dynamickým aktualizacím klientů následovně:

- Klientské počítače s operačním systémem Windows 2000 výslovně požadují, aby služba DHCP pouze aktualizovala záznamy prostředků PTR používané ve službě DNS pro zpětný náhled a přiřazení adresy IP klienta jeho názvu. Tito klienti si sami aktualizují záznam své adresy (A).
- Klienti s operačním systémem dřívější verze Windows nemohou výslovně žádat o prioritu dynamické aktualizace. U těchto klientů lze službu DHCP nakonfigurovat tak, že aktualizuje jak záznamy prostředků PTR, tak záznamy prostředků A klienta.

Při přesunu databáze služby DHCP ze starého hardwaru serveru na nový dodržujte doporučený postup.

Informace o přesunu dat služby DHCP na jiný server, například v případě selhání hardwaru nebo obnovení po pádu systému najdete v Microsoft Knowledge Base.

Instalace služby DHCP

Před instalací serveru DHCP zjistěte následující:

- Požadavky na hardware a úložný prostor pro server DHCP.
- Které počítače můžete okamžitě konfigurovat jako klienty DHCP pro dynamickou konfiguraci protokolu TCP/IP a které počítače byste měli nakonfigurovat ručně pomocí statických konfiguračních parametrů TCP/IP.
- Typy možností DHCP a hodnoty možností, které budou klientům DHCP předdefinovány.

Umístění serveru DHCP Použijte fyzické vlastnosti infrastruktury sítě LAN nebo WAN a ne logické seskupení definované doménami Windows 2000 a strukturou služby Active Directory. Pokud jsou podsítě propojeny směrovači, které podporují přenosové agenty BOOTP, nejsou potřeba servery DHCP na každé podsíti. Servery DHCP lze také spravovat vzdáleně z počítače s běžícím operačním systémem Windows 2000 a programem Správce služby DHCP.

Prostředky Sestavte seznam požadavků včetně:

- Počtu a typů počítačů, které je třeba podporovat.
- Spolupráce se stávajícími systémy, včetně vašich požadavků na klíčové účetní, personální a podobné informační systémy.
- Hardwarová podpora a s ní spojená kompatibilita hardwaru, včetně směrovačů, prepínačů a dalších typů serverů.
- Software pro sledování sítě, například Net Monitor (dodávaný s Windows 2000).

Izolace procesu Izolujte oblasti sítě, kde procesy musí běžet bez přerušení a pak se na tyto oblasti zaměřte v posledních stádiích implementace.

Plánování logických podsítí Prohlédněte si zeměpisnou a fyzickou strukturu sítě a určete nejlepší plán pro definování podsítí jako segmentů intranetu.

Fáze testování Určete součásti v novém systému, které vyžadují testování a pak vypracujte rozfázovaný plán pro testování a přidávání součástí. Například plán může určit pořadí typů počítačů, včetně serverů a pracovních stanic na platformě Windows 2000, servery a klienty Microsoft se vzdáleným přístupem, počítače na platformě Windows for Workgroups a klienty MS-DOS.

- Vytvořte hlavní a druhou fázi testu, včetně vyladění konfigurace serveru a klienta DHCP a WINS pro co nejvyšší efektivitu. Tato úloha zahrnuje určení strategií zálohových serverů a rozdělení fondu adres na každém serveru pro lokální a vzdálené klienty.
- Zdokumentujte pro správce sítě celou architekturu a problémy správy.
- Vždy během svých testovacích scénářů používejte odhady běžného zatížení, dostanete tím přesné informace o výkonu.

Podpora dalších podsítí Aby služba DHCP podporovala další podsítě na vaší síti, musíte nejprve určit, jestli jsou směrovače použité k připojení sousedících podsítí schopné podporovat přenos zpráv BOOTP a DHCP. Jestliže směrovače nelze pro přenos zpráv BOOTP a DHCP použít, můžete nastavit některou z následujících možností pro každou podsít:

- Počítač na platformě Windows 2000 Server nebo Windows NT Server 4.0 nakonfigurovaný k používání součásti služby DHCP – přenosového agenta DHCP: Tento počítač jednoduše předává zprávy tam a zpět mezi klienty na lokální podsíti a vzdáleným serverem DHCP za použití adresy IP na vzdáleném serveru. Služba přenosového agenta DHCP je dostupná pouze na počítačích na platformě Windows 2000 Server nebo Windows NT Server 4.0.
- Počítač na platformě Windows 2000 Server nakonfigurovaný jako server DHCP pro lokální podsít. Tento server musí obsahovat a spravovat informace o oborech a další informace o konfiguraci adres pro lokální podsít, které náleží.

Provoz DHCP Provoz DHCP nepoužívá během normálního užívání významnou šířku pásma sítě. Typický provoz DHCP nepřesahuje 1 procento celkového provozu sítě. Nicméně dvě fáze konfigurace klienta DHCP vytvářejí větší množství provozu sítě. Těmito fázemi jsou zápujčka adresy IP a obnovení adresy IP.

Při první inicializaci protokolu TCP/IP klienta, který je nakonfigurován jako klient DHCP, je jeho prvním krokem získání adresy IP za pomoci služby DHCP. Tento proces, jak bylo popsáno výše, vyústí v konverzaci mezi klientem DHCP a serverem skládající se ze čtyřech paketů, z nichž prvním je všesměrové vysílání klienta, kterým odešle paket DHCPDiscover ve snaze lokalizovat server DHCP.

Jak bylo ukázáno v počátečním procesu zápujčky dříve v této kapitole, celý proces získání zápujčky adresy IP prostřednictvím služby DHCP potřebuje celkem čtyři pakety, každý o velikosti 342 až 590 bajtů. Tento proces na čisté síti (šířku pásma nepoužívá žádný další provoz sítě) zabere méně než 1 sekundu (asi 300 milisekund) na médiu 10BaseT. Výsledky závisí na typu používaného média.

Konverzace DHCP se zpravidla objevuje v následujících případech.

- Při první inicializaci klienta DHCP (jsou odeslány všechny čtyři rámce).
- Při automatickém obnovování, které probíhá po uplynutí poloviny doby trvání zá-půjčky (dle výchozího nastavení čtyři dny, tj. 96 hodin). Tato komunikace potře-buje dva pakety (DHCPRequest a DHCPACK) a trvá přibližně 200 milisekund.
- Při přesunu klienta na novou podsít (DHCPRequest, DHCPNak, pak čtyři rámce).
- Při výměně síťového adaptéru klienta DHCP (odeslány jsou všechny čtyři rámce).
- Kdykoli klient ručně obnoví nebo uvolní svou adresu pomocí nástroje Ipconfig.

Pokud chcete snížit množství provozu produkovaného službou DHCP, je možné upra-vit dobu trvání zá-půjčky adresy IP, a to prostřednictvím Správce služby DHCP a úpra-vou Doba trvání zá-půjčky.

Aktualizace databáze DHCP pro Windows 2000

Při aktualizaci operačního systému Windows NT Server verze 3.51 (nebo dřívější) na Windows 2000 musí být databáze DHCP převedena do nového formátu databáze. Da-tabáze Windows 2000 používá vylepšený databázový stroj, který je rychlejší a provádí automatickou komprimaci, čímž předchází fragmentaci a následnému růstu databáze. Proces převedení databáze je prováděn automaticky jako součást instalace aktualizace. Když se služba DHCP spouští po aktualizaci na Windows 2000 poprvé, zjistí, že data-bázi je třeba převést. Pak začne proces převedení spuštěním programu Jetconv.exe. Služba DHCP se zastaví a započne převádění databáze. Program Jetconv.exe najde a převede databáze pro všechny nainstalované služby (DHCP a, pokud je nainstalová-na, WINS) do nového formátu databáze Windows 2000.

Po úspěšném předání databáze se služba DHCP opět automaticky spustí.

Poznámka Před aktualizací na Windows 2000 uveďte všechny databáze Windows NT 3.51 nebo 4.0 pro server DHCP do konzistentního stavu. Toho dosáhnete ukončením služeb, buď prostřednictvím nástroje **Služby** v Ovládacích panelech nebo prostřednic-tvím příkazu **net stop service**. Tento postup je doporučen proto, že brání selhání pře-vádění databáze pomocí programu Jetconv.exe z důvodu nekonzistence databáze Win-dows NT 3.51 nebo 4.0.

Převedení vyžaduje přibližně stejný prostor na disku jako původní databáze a soubory protokolu. Pro soubory protokolu každé databáze byste měli mít alespoň 5 MB volné-ho prostoru na disku.

Převedením se zakonzervuje původní databáze a soubory protokolu v podadresáři na-zvaném 351db (pokud se jedná o Windows NT 3.51) nebo 40db (pokud se jedná o Windows NT 4.0) ve stejném adresáři, kde jsou umístěny původní databáze a soubor-y protokolu. Na serveru DHCP to je adresář `%SystemRoot%\System32\Dhcp\versi-ondb`. Správce může pak později tyto soubory odstranit a uvolnit tak část prostoru na disku.

Převedení databáze může zabrat cokoli od minuty až po hodinu v závislosti na velikos-ti databáze. Uživatel nesmí během převádění databáze spustit tyto služby. Ke kontrole převádění použijte Prohlížeč událostí, kde můžete sledovat protokol událostí procesu programu Jetconv.exe.

V případě, že toto automatické převádění databáze z nějakého důvodu selže (příčinu lze vyhledat v protokolu událostí), databáze, kterou nelze převést automaticky, lze pře-vést ručně pomocí programu `%SystemRoot%\System32\upgversiondb.exe`.

Nový databázový stroj používá soubory protokolu s názvy začínajícími předponou J50.

Varování Nelze převést novou databázi zpět do původního formátu databáze. Převedená databáze nefunguje pod Windows NT 3.51 nebo s dřívějšími verzemi služeb DHCP.

Konfigurování služby DHCP

Hlavní nástroj, který používáte při správě serverů DHCP, je Správce služby DHCP – součást konzoly MMC, která se přidává do menu **Nástroje pro správu** při instalaci služby DHCP.

Po instalaci serveru DHCP můžete Správce služby DHCP používat k:

- Definování oborů, množin oborů a oborů vícesměrového vysílání včetně rozsahů vyloučení a rezervací.
- Aktivaci oborů nebo množin oborů.
- Sledování činnosti zapůjčování oborů.
- Definování vlastních přednastavených typů možností DHCP.
- Konfigurování tříd možností definovaných uživatelem a definovaných dodavatelem.
- Definování dalších vlastností serveru DHCP, například protokolování auditu nebo tabulky BOOTP.

Správce služby DHCP také poskytuje vylepšené sledování výkonu serveru předdefinované typy možností DHCP, podporu dynamické aktualizace u klientů používajících dřívější verze služby DHCP a zjišťování neautorizovaných (nepřátelských) serverů DHCP na síti.

Můžete také definovat:

Vylepšené sledování a poskytování statistik Vylepšené sledování a poskytování statistik upozorní, když je počet adres IP dostupných pro zápůjčku, pod prahem definovaným uživatelem. Například se může spustit výstraha po přiřazení 90 procent adres IP v příslušném oboru. Druhá výstraha se může spustit při vyčerpání fondu adres IP.

Třídy možností definované uživatelem a třídy možností definované dodavatelem Služba DHCP pro Windows 2000 umožňuje definování možností definovaných uživatelem a dodavatelem jako alternativu k potenciálně zdlouhavému procesu získání souhlasu IETF pro novou standardní možnost.

Integrace služby DHCP se službou DNS Servery DHCP mohou umožnit dynamickou aktualizaci v oboru názvů DNS pro kteréhokoli klienta, který podporuje tuto aktualizaci. Tato vlastnost umožňuje klientům oboru používat dynamickou aktualizaci k aktualizaci informací o mapování názvů k adresám (které jsou uloženy na serveru DNS) při změně jejich adresy přiřazené službou DHCP.

Zjišťování nepřátelského serveru DHCP Služba DHCP pro Windows 2000 je navržena tak, aby bránila nepřátelským serverům DHCP ve vytváření konfliktů při přiřazování adres. To řeší problémy, které se objevují kvůli přiřazení nesprávných nebo neúmyslných adres IP klientům neautorizovanými servery DHCP kdekoli na síti.

Předcházení nepřátelským serverům DHCP

Proces autorizace serverů DHCP je užitečný nebo potřebný pro servery DHCP běžící pod operačním systémem Windows 2000 Server. Kde je použito toto schéma, autorizace se použije a není potřeba za následujících podmínek:

- Jestliže servery DHCP běží na dřívějších verzích Windows NT Server, například verze 3.51 nebo 4.0.
- Jestliže servery DHCP běží na jiném softwaru pro servery DHCP.

Aby autorizační proces proběhl správně, předpokládá se a je nezbytné, aby se první server DHCP uvedený na vaší síti podílel na službě Active Directory. To vyžaduje instalaci serveru buď jako řadiče domény nebo členského serveru. Jestliže plánujete nebo aktivně provádíte služby Active Directory, je důležité, abyste nenainstalovali váš první server DHCP jako samostatný server.

Nejobvykleji bude existovat pouze jeden kořen rozsáhlé sítě a tím pádem pouze jedno místo pro adresářovou autorizaci. Nicméně neexistují žádná omezení autorizace serverů DHCP pro více než jeden kořen rozlehlé sítě.

Jestliže jsou správně nakonfigurovány a jsou oprávněny k použití na síti, servery DHCP poskytují užitečnou administrativní službu. Nicméně uvedení nesprávně nakonfigurovaného nebo neautorizovaného serveru DHCP do sítě může způsobit problémy. Například jestliže se spustí nepřátelský server DHCP, může začít klientům zapůjčovat nesprávné adresy IP nebo zasílat negativní potvrzení klientům DHCP, kteří se snaží obnovit svou aktuální zápůjčku adresy.

Jakýkoli z těchto problémů s nesprávnou konfigurací může způsobit další problémy klientům podporujícím DHCP. Například klienti, kteří získají zápůjčku konfigurace od neautorizovaného serveru, mohou selhat při lokalizaci platných řadičů domény, což jim zabrání v úspěšném přihlášení do sítě.

Windows 2000 Server poskytuje určitou integrovanou podporu zabezpečení pro síť, které používají službu Active Directory. To brání většině náhodných poškození způsobených servery DHCP s nesprávnou konfigurací nebo na nesprávných sítích.

Tato podpora používá kromě základního schématu adresáře dodatečné typy objektů (objekt DhcpServer). To poskytuje následující vylepšení:

- Seznam adres IP dostupných počítačům, které autorizujete k fungování na síti jako servery DHCP.
- Zjišťování nepřátelských serverů DHCP a zabránění jejich spuštění nebo používání na vaší síti.

Poznámky Aby adresářový autorizační proces fungoval správně, je nezbytné, aby se první server Windows 2000 DHCP uvedený na vaší síť, podílel na službě Active Directory. To vyžaduje, aby byl server instalován v doméně (buď jako řadič domény nebo členský server) a nikoli v pracovní skupině. Pokud plánujete nebo aktivně provádíte služby Active Directory, neinstalujte svůj první server DHCP jako server pracovní skupiny. K autorizaci serveru DHCP ve službě Active Directory potřebujete práva správce rozsáhlé sítě.

Jak jsou servery DHCP autorizovány

Autorizační proces serverů DHCP pro službu Active Directory závisí na roli serveru na síti. U operačního systému Windows 2000 Server (stejně jako u dřívějších verzí) jsou tři role nebo typy serverů, pro které může být každý server nainstalován:

- **Řadič domény.** Počítač udržuje a spravuje kopii databáze služby Active Directory a poskytuje uživatelům a počítačům členů domény bezpečnou správu účtu.
- **Členský server.** Počítač nefunguje jako řadič domény, ale přidal se k doméně, ve které má členský účet v databázi služby Active Directory.
- **Samostatný server.** Počítač nefunguje jako řadič domény ani jako členský server domény. Namísto toho se server na síti zviditelní prostřednictvím určitého názvu pracovní skupiny, kterou mohou sdílet i další počítače, ale je používána pouze za účelem prohledávání a nikoli poskytování přihlašovacího přístupu ke sdíleným prostředkům domény.

Jestliže si nainstalujete službu Active Directory, musí být všechny počítače fungující jako servery DHCP před možnou autorizací ve službě Active Directory nebo před poskytováním služeb DHCP klientům buď řadiči domény nebo členskými servery domény. Když je server DHCP autorizován, je přidán do seznamu autorizovaných serverů DHCP udržovaném v databázi služby Active Directory.

Jak jsou zjišťovány neautorizované servery

Implementace služby DHCP pod operačním systémem Windows 2000 Server poskytuje zjišťování jak autorizovaných, tak neautorizovaných serverů DHCP dvěma způsoby:

- Použití zaslání zpráv mezi servery DHCP používajícími zprávu DHCPInform.
- Přidání několika nových typů možností definovaných dodavatelem, používaných pro předávání informací o kořeni rozsáhlé adresářové služby.

Služba DHCP pro Windows 2000 používá ke zjišťování dalších serverů DHCP aktuálně běžících na dosažitelné síti a k určení, jestli jsou autorizovány poskytovat službu DHCP, následující proces.

Po svém spuštění služba DHCP pošle zprávu DHCPInform na dosažitelnou síť za použití adresy omezeného lokálního všesměrového vysílání (255.255.255.255), aby lokalizovala kořen adresářové služby, kde jsou nainstalovány a nakonfigurovány další servery DHCP.

Tato zpráva obsahuje několik typů možností definovaných dodavatelem, které jsou známé a podporované dalšími servery DHCP na Windows 2000 Server. Po obdržení dalšími servery DHCP tyto typy možností poskytují dotazování a sběr informací o kořeni rozlehlé adresářové služby.

Jsou-li dotázány, ostatní servery DHCP odpoví zprávou DHCPAck, kterou potvrdí a zodpoví informace o kořeni adresářové služby. Tímto způsobem inicializující server DHCP sbírá a třídí seznam aktuálně aktivních serverů DHCP na dosažitelné síti společně s kořenem adresářové služby používaným každým serverem.

Zpravidla je zjištěn jeden kořen: stejný pro všechny servery DHCP, které jsou dosažitelné a které odpovídají potvrzením inicializujícímu serveru. Nicméně jestliže jsou zjištěny další kořeny rozsáhlé sítě, je každá kořenová síť dotázána, aby se prokázalo, jestli je tento počítač autorizován ke službě DHCP pro tyto další rozsáhlé sítě objevené během této fáze.

Po sestavení seznamu všech serverů DHCP běžících na síti další krok ve zjišťovacím procesu závislý na tom, jestli je adresářová služba dostupná z lokálního počítače.

Jestliže adresářová služba není dostupná (například když je inicializující server DHCP instalován v uzavřeném síťovém prostředí používaném pro testování), inicializace serveru může začít, pokud nejsou na síti objeveny žádné další servery DHCP, které jsou součástí rozsáhlé sítě. Je-li tato podmínka splněna, server se úspěšně inicializuje a začne obsluhovat klienty DHCP.

Nicméně server pokračuje za pomoci zpráv DHCPInform v pětiminutových intervalech ve sběru informací o dalších serverech DHCP běžících na síti jako při spuštění. Pokaždé zkontroluje, jestli je adresářová služba dostupná. Jestliže je adresářová služba nalezena, server se pomocí následujícího postupu v závislosti na tom, jestli je server členským serverem nebo samostatným serverem ujistí, že je autorizován.

- U členských serverů (serverů přiřazených k nějaké doméně, která je součástí rozsáhlé sítě) se server DHCP dotáže adresářové služby na seznam adres serveru DHCP, které jsou autorizovány.
- Jestliže server najde v seznamu autorizací svou adresu IP, inicializuje se a začne poskytovat klientům DHCP služby DHCP: Jestliže svou adresu v seznamu autorizací nenajde, neinicializuje se a přestane poskytovat služby DHCP.
- U samostatných serverů (serverů, které nejsou přiřazené k žádné doméně nebo části existující rozsáhlé sítě) se server DHCP dotáže adresářové služby s kořenem rozsáhlé sítě vráceným každým dalším DHCP serverem, aby zjistil, jestli je na seznamu autorizací pro jakoukoli z uvedených rozsáhlých sítí.

Server se inicializuje a začne poskytovat služby DHCP klientům pouze v případě, že najde svou adresu IP v seznamu autorizací pro každou z kořenových sítí rozsáhlé sítě dle hlášení dalších serverů DHCP. Jestliže svou adresu IP v seznamu autorizací pro každou z kořenových sítí rozsáhlé sítě nenajde, neinicializuje se a služba DHCP se zastaví.

Clustering serverů DHCP

Windows Clustering umožňuje, že dva servery jsou spravovány jako jeden systém. Služba Windows Clustering Service pro Windows 2000 (pouze Advanced Server) může být použita pro servery DHCP, aby poskytovala větší dostupnost, jednodušší spravovatelnost a větší rozšiřitelnost.

Windows Clustering může automaticky zjistit selhání aplikace nebo serveru a rychle ji restartovat na přeživším serveru, zatímco uživatelé zažijí pouze krátkou přestávku v poskytování služeb. S pomocí Windows Clustering mohou správce rychle zkontrolovat stav všech prostředků clusteru a jednoduše přesouvat zatížení na různé servery v rámci clusteru. Toto je užitečné pro ruční vyrovnávání zatížení a pro aktualizace na serverech bez toho, že by důležitá data a aplikace musely být v režimu offline.

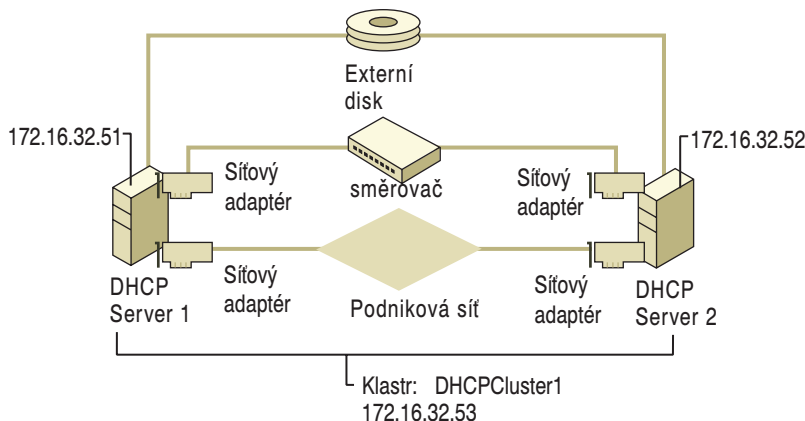
Windows Clustering také umožňuje virtualizaci serverů DHCP, takže pokud jeden z clusterových uzlů selže, obor názvů a všechny služby jsou transparentně předány druhému uzlu. To znamená, že klient nezaznamená žádné změny, jelikož vidí stejnou adresu IP pro všechny clusterované servery DHCP.

Bez clusterování by mohli správci sítě rozdělit obory mezi servery, takže pokud by jeden server selhal, minimálně polovina dostupných adres by zůstala dostupná. Clustering používá adresy IP efektivně díky odstranění nutnosti rozdělovat obory. Databáze uložená na vzdáleném disku sleduje přiřazení adresy a další činnosti, takže pokud ak-

tivní uzel clusteru selže, stane se serverem DHCP druhý uzel, přičemž disponuje plnou znalostí přiřazených adres a přístupem k úplnému oboru adres. Jako server DHCP běží v jednom okamžiku pouze jeden uzel, zatímco clusteringová databáze poskytuje transparentní přenos v případě potřeby.

Příklad seskupených serverů DHCP

Na obrázku 4.15 je znázorněn typický příklad seskupených serverů DHCP. Server DHCP 1 je aktivní server DHCP, zatímco server DHCP 2 je záložní server DHCP.



Obrázek 4.15 Seskupené servery DHCP

Na obrázku 4.15:

- Server DHCP 1 a server DHCP 2 mají nainstalované služby DHCP pro Windows 2000 a Windows Clustering Service.
- Každý server DHCP má jedinečný název serveru a adresu IP.
- Každý server DHCP má dvě síťová rozhraní – jedno pro totožnost clusteru a připojení k rozsáhlé síti a druhé pro komunikaci server – server. To je soukromé propojení pouze pro komunikaci v clusteru, drát běží přímo mezi dvěma servery.
- Oba servery DHCP mají nakonfigurovány stejné obory. Nicméně na serveru DHCP 2 nejsou obory aktivovány, protože server 2 aktuálně nefunguje coby aktivní server DHCP. Server DHCP 2 může fungovat jako rychlý náhradník, který je připraven pro případ, že server DHCP 1 selže.
- Aby mohly provádět clustering a sdílet prostředky, servery DHCP jsou připojeny k systému externích disků, které udržují databázi DHCP a soubory protokolu. To umožňuje serveru DHCP 2 přistupovat k databázovým souborům DHCP, pokud je potřebuje jako aktivní server DHCP převzít. Služba Clustering Service nainstalovaná na každém serveru DHCP zabráňuje tomu, aby se jeden server pokoušel výlučně nárokovat si externí disk a zabránit sdílení systému disků mezi servery DHCP.
- Cluster jako takový má jedinečný název a adresu IP, takže klienti DHCP mohou k připojení k clusteru a požadavkům na služby DHCP používat název clusteru a jeho adresu IP. To zabráňuje zamítání požadavků klientů DHCP v případě vypnutí jednoho serveru DHCP. Například jestliže klient byl nakonfigurován na urči-

tý název serveru DHCP a adresu IP namísto adresy clusteru, neobdrží služby DHCP. Ale po nakonfigurování klientů DHCP na název a adresu IP clusteru je klient schopen komunikovat s aktivní serverem DHCP v clusteru.

Před implementací podobného scénáře zvažte následující doporučení:

- Na každém serveru DHCP v clusteru (ať už hlavním nebo záložním) před instalací služby Clustering Service nainstalujte nejdříve službu DHCP.
- Do doby, než má hlavní server nainstalovány služby Clustering Service a je nakonfigurován na nový název clusteru a jeho adresu, ponechte druhý server DHCP vypnutý. Po zapnutí (a nakonfigurování služeb DHCP a Clustering Service) se přidá k již existujícímu clusteru.
- Název a adresa IP clusteru musí být nakonfigurovány staticky – nelze je konfigurovat dynamicky pomocí jiného serveru DHCP.
- Jestliže cluster DHCP používá k ukládání databázových souborů DHCP systém externích disků, musí být nakonfigurovány záznamy DatabasePath a BackupDatabasePath v registru na obou serverech DHCP v clusteru. Záznamy v registru jsou umístěny v HKLM\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters . Tyto záznamy registru musí specifikovat cestu k systému externích disků.
- Oprávnění: Jakýkoli záložní server DHCP nebude schopen úspěšně převzít úlohy DHCP, pokud nebude mít povolená příslušná bezpečnostní oprávnění. Správci musí vytvořit novou skupinu zabezpečení domény, ke které servery náleží. Tato skupina musí mít plné oprávnění pro objekt zóny DNS ve službě Active Directory, kde mají klienti DHCP registrovány a aktualizovány své záznamy A a PTR. Případně správci mohou přidat druhý server pro doménu do skupiny DNSUpdateProxyGroup. Jinak dojde k selhání překladu názvu.
- Při implementaci seskupených serverů DHCP používejte pravidlo 80/20, kterým poskytnete další vylepšené služby okamžitého náhradníka. Kombinací seskupení serverů DHCP a použití pravidla 80/20 ke správě oborů mezi seskupenými servery umožňuje vylepšené řešení pro okamžitého náhradníka. Podrobnosti určování oborů za pomoci pravidla 80/20 najdete v části „Pravidlo 80/20“ a „Nejlepší postupy“.

Více informací najdete v knize *Microsoft® Windows® 2000 Server Distribuované systémy* v části „Windows Clustering“.

Scénáře služby DHCP

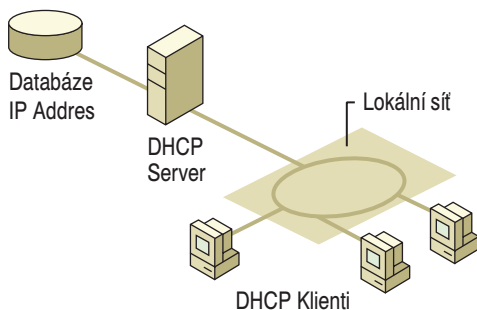
Následující části pojednávají o obvyklých scénářích a problémech instalace DHCP.

DHCP v malých sítích

V malé síti LAN, která neobsahuje směrovače a podsíťování, může být použit jeden server DHCP. Na obrázku 4.16 je zobrazen příklad rozložení malé sítě.

Před instalací serveru DHCP na malou síť potřebujete zjistit následující:

- Požadavky na hardware a na úložný prostor na server DHCP.
- Které počítače lze nakonfigurovat jako klienty DHCP pro dynamickou konfiguraci protokolu TCP/IP a které počítače by měly být nakonfigurovány ručně statickými parametry konfigurace protokolu TCP/IP, včetně statických adres IP.
- Předdefinované typy možností DHCP a jejich hodnoty.



Obrázek 4.16 Samostatná malá síť používající automatickou konfiguraci protokolu TCP/IP pomocí služby DHCP

DHCP ve velkých sítích

U rozsáhlých sítí byste měli:

- Naplánovat fyzické podsítě na síti a relativní umístění serverů DHCP. To zahrnuje naplánování umístění serverů DHCP (a WINS) mezi podsítě tak, aby se snížilo všesměrové vysílání uzlů b přes směrovače.
- Specifikovat typy možností DHCP a jejich hodnoty a předdefinovat je pro jednotlivé obory pro klienty DHCP. To může zahrnovat naplánování oborů založených na potřebě určitých skupin uživatelů. například pro jednotku, kde se často přesunují počítače na jiné umístění, mohou být definovány kratší doby trvání zápůjčky pro spojené obory. Tento přístup shromažďuje adresy IP, které jsou často měněny a zahazovány a vrací je zpět do fondu dostupných adres, které je možno využít pro nové nabídky zápůjček.
- Rozpoznat dopad, který mají na prostředí sítě WAN pomalejší propojení. Umístěte servery DHCP, WINS a DNS tak, aby byl maximalizována prodleva odpovědi a minimalizován pomalý provoz.

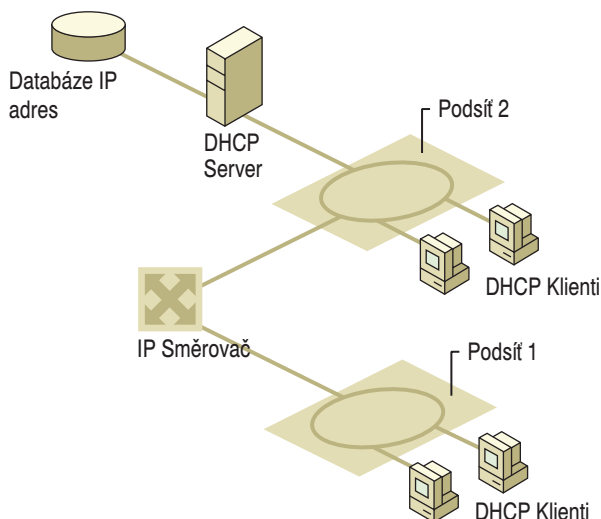
Jeden příklad naplánování rozsáhlé sítě: rozdělení sítě WAN na logické podsítě může odpovídat fyzické struktuře veřejné sítě nebo sítě typu Intranet. Pak jedna podsít IP může sloužit jako páteř a na ni navazující fyzické podsítě disponují vlastní adresou IP podsítě.

DHCP ve směrovaných sítích

Ve směrovaných sítích, které používají k rozdělení segmentů sítě podsítě, musí správci pro plné fungování implementace služeb DHCP dodržet některý ze specifických požadavků. Tyto požadavky zahrnují jeden z následujících:

- Jeden server DHCP musí být umístěn na minimálně jedné podsíti ve směrované síti.
- Aby mohl server DHCP podporovat klienty na dalších vzdálených podsítích oddělených směrovači, musí být směrovač nebo vzdálený počítač použit jako přenosový agent DHCP/BOOTP, který podporuje provoz DHCP mezi podsítěmi.

Na obrázku 4.17 je zobrazen příklad směrované sítě se serverem DHCP a klienty DHCP.



Obrázek 4.17 Veřejná síť nebo síť typu Intranet používající automatickou konfiguraci protokolu TCP/IP pomocí služby DHCP

Jak již bylo popsáno výše, směrovače, které implementují přenosového agenta DHCP/BOOTP, mohou být použity ke směrování provozu mezi servery DHCP a klienty umístěnými na různých podsítích. Přenosový agent na směrovači předává požadavky z lokálních klientů DHCP na vzdálený server DHCP a zároveň předává odpovědi serveru DHCP zpět klientům DHCP.

Instalace přenosového agenta

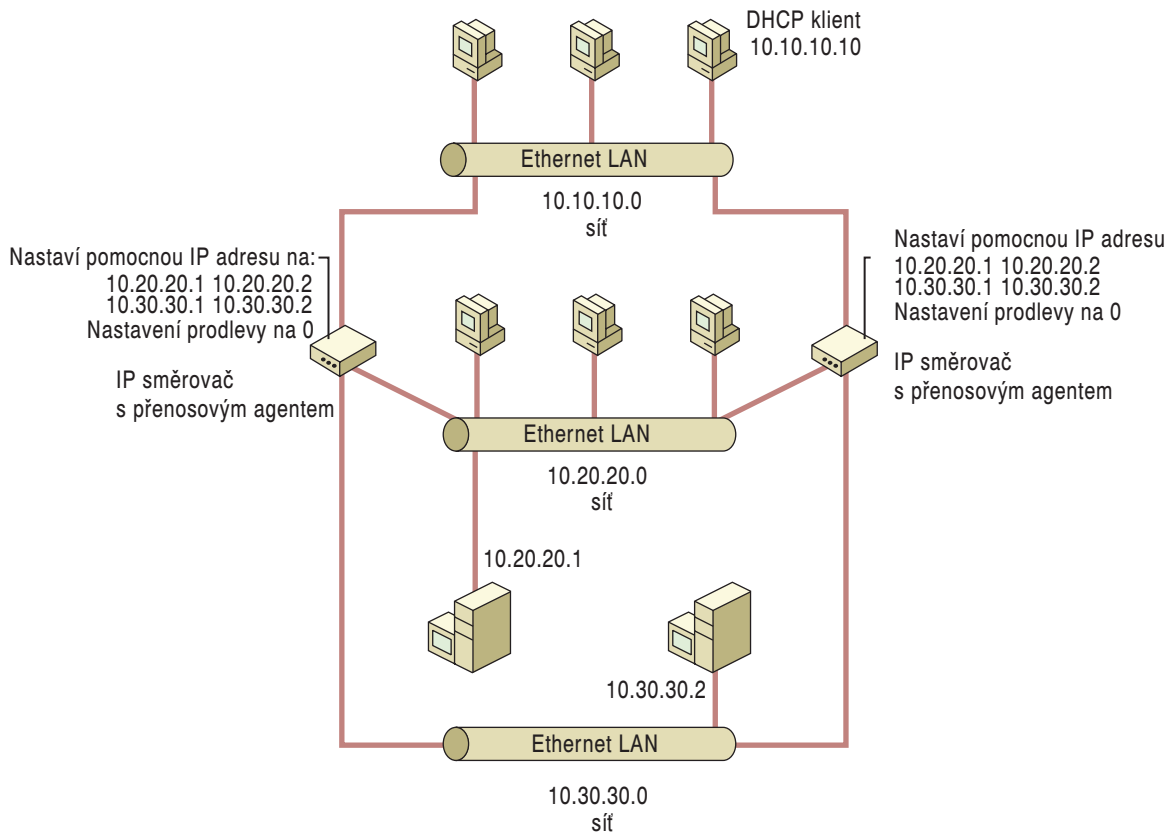
Máte-li více serverů DHCP, společnost Microsoft doporučuje umístit servery DHCP na různé podsítě spíše než umístit všechny servery DHCP na jednu podsít, protože tak dosáhnete větší odolnosti proti chybám. Servery by neměly mít ve svých oborech společné adresy IP (každý server by měl mít jedinečný fond adres).

Jestliže se server DHCP na lokální podsíti vypne, požadavky jsou přenášeny na vzdálenou podsít. Server DHCP na tomto umístění může odpovídat na požadavky DHCP, pokud disponuje oborem adres IP pro požadující podsít. Jestliže vzdálený server nemá pro požadující podsít definován žádný obor, nemůže poskytnout adresy IP, i kdyby měl adresy pro další obory dostupné. Jestliže má každý server DHCP fond adres pro každou podsít, může poskytovat adresy IP pro vzdálené klienty, jejichž vlastní server DHCP je v režimu offline.

Pokud plánujete zabudovat přenosového agenta do sítě podporující DHCP/BOOTP, existuje několik dostupných možností konfigurace přenosových agentů. Ty zahrnují použití směrovačů třetích stran, služby Windows 2000 Routing and Remote Access a přenosového agenta DHCP Relay Agent obsaženého ve Windows NT Server 4.0. Více informací o tom, jak pracuje přenosový agent, najdete později v této kapitole v části „Správa přenosových agentů“.

Doporučená obecná konfigurace

Obrázek 4.18 znázorňuje doporučenou implementaci přenosového agenta, která poskytuje nejlepší výkon sítě.



Obrázek 4.18 Doporučená konfigurace přenosového agenta ve Windows 2000

Tento obrázek zobrazuje obecnou konfiguraci přenosových agentů. Specifické scénáře najdete v následujících částech a obrázcích.

Přenosoví agenti služby Routing and Remote Access pro Windows 2000 Server

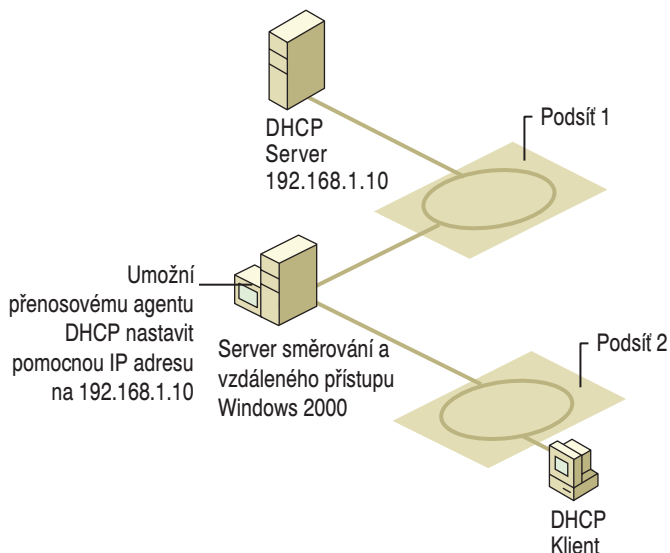
Obrázek 4.19 znázorňuje konfiguraci služby Routing and Remote Access pro Windows 2000 Server. V tomto příkladě server Windows 2000 funguje jako směrovač mezi podsítí 1 a 2 stejně jako přenosový agent mezi serverem DHCP na podsítí 1 a klienty DHCP na podsítí 2.

Přenosový agent DHCP musí být na serveru Windows 2000 nakonfigurován na adresu IP serveru DHCP, aby mohl přenášet požadavky DHCP mezi podsítí 1 a podsítí 2.

Přenosoví agenti pro Windows NT Server 4.0

Obrázek 4.20 znázorňuje standardní konfiguraci směrovače.

Tento příklad ukazuje, jak lze implementovat na síť standardní směrovač IP společně s přenosovým agentem Windows NT Server 4.0 přenášejícím požadavky DHCP mezi podsítí 1 a podsítí 2.



Obrázek 4.19 Služba Routing and Remote Access pro Windows 2000 Server jako přenosový agent

DHCP a služba Routing and Remote Access

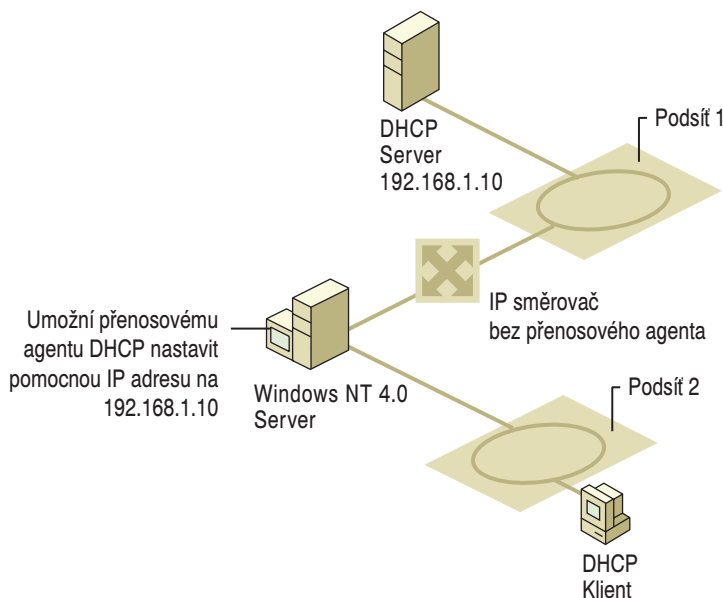
Služba DHCP může být nainstalována společně se službou Routing and Remote Access tak, aby dynamicky poskytovala klientům se vzdáleným přístupem adresy IP během telefonického připojení. Když jsou služby Routing and Remote Access a DHCP používány společně na stejném serveru, jsou během dynamické konfigurace informace poskytnuté odlišně od informací poskytovaných za normální konfigurace DHCP klientů na základě LAN.

Když server se vzdáleným přístupem poskytuje dynamickou konfiguraci klientů s telefonickým připojením, server se vzdáleným přístupem pevně provede před přiřazením záplůjčky klientovi DHCP následující kroky:

- Když se server se vzdáleným přístupem spouští s možností **Použít DHCP k přiřazení adres TCP/IP**, dotáže se dopředu serveru DHCP na adresu klienta DHCP pro klienty s telefonickým připojením a tuto adresu uloží do mezipaměti.
- Počet adres klientů požadovaných dopředu odpovídá počtu portů služby Routing and Remote Access nastaveným k přijímání volání plus jedna adresa navíc.

Například jestliže server se vzdáleným přístupem má dva porty analogového modemu a dva porty adaptéru ISDN, které jsou nastaveny pro přijímání volání, server se vzdáleným přístupem požaduje od serveru DHCP celkem pět adres IP. První čtyři jsou pro přiřazení klientům se vzdáleným přístupem, kteří se přes telefonní linku připojí k por-

tům služby Routing and Remote Access. Pátá adresa je rezervována pro server se vzdáleným přístupem ke konfiguraci a používání vlastní adresy IP při zpracovávání připojení ke klientům s telefonickým připojením.



Obrázek 4.20 Standardní směrovač jako přenosový agent

Když server se vzdáleným přístupem používá tento typ předaktivního ukládání zápůjček adres DHCP pro klienty s telefonickým připojením do mezipaměti, zaznamenává následující informaci pro každou odpověď na požadavek zápůjčky, kterou obdrží od serveru DHCP:

- Adresa IP serveru DHCP.
- Adresa IP zapůjčená klientovi (pro pozdější distribuci klientům se vzdáleným přístupem).
- Čas, kdy byla zápůjčka získána.
- Čas, kdy zápůjčka vyprší.
- Délka doby trvání zápůjčky.

Všechny další informace o možnostech DHCP vrácené serverem DHCP (například možnosti obecné, možnosti oboru nebo rezervovaného klienta) jsou vyřazeny. Když se klient připojí telefonickým připojením k serveru se vzdáleným přístupem a požaduje adresu IP (tj. je vybrána Adresa IP přiřazená serverem), server se vzdáleným přístupem použije jednu ze zápůjček uložených v mezipaměti k poskytnutí dynamické konfigurace adresy IP klientovi se vzdáleným přístupem. Když je adresa IP poskytnuta klientovi se vzdáleným přístupem, klient si není vědom toho, že adresu IP získal prostřednictvím komunikace mezi serverem DHCP a serverem se vzdáleným přístupem. Server se vzdáleným přístupem udržuje zápůjčku na účet klienta. Proto jedinou informací, kterou klient dostane od zápůjčky DHCP, je adresa IP.

Služby DHCP a WINS

Služba WINS je názvová služba používaná k registraci a mapování přiřazení názvů adresám pro klienty typu NetBIOS na sítích TCP/IP.

Vzhledem k tomu, že názvy typu NetBIOS jsou vlastností vyžadovanou u sítí, která je podporována všemi předcházejícími verzemi Windows, nainstalujte a používejte službu WINS, pokud používáte službu Windows 2000 DHCP v síťovém prostředí, které obsahuje klienty běžící pod jedním z následujících dřívějších operačních systémů společnosti Microsoft:

- Windows for Workgroups 3.11
- Windows 95
- Windows NT Advanced Server 3.1
- Windows NT 3.5x
- Windows NT 4.0
- MS-DOS klient pro Microsoft Networks

V mnoha případech není nutné přidávat servery WINS nad počet serverů, které jsou plánovány pro používání serveru DHCP. V mnoha případech stejný server může pracovat efektivně jak jako server WINS, tak jako server DHCP pro jeden internet na síti.

Je-li jeden server nakonfigurován jako server WINS i server DHCP, může:

- Spravovat definovaný obor nebo množinu oborů adres IP pro vaši síť.
- Sloužit jako přednastavená brána k poskytování předávání IP mezi spojenými fyzickými sítěmi.

K nastavení stejné přednastavené brány pro všechny klienty DHCP umístěné na podsítích přiřadte kód 3 možnosti DHCP pomocí adresy IP počítače serveru jako hodnotu do konfigurování možností oborů DHCP.

- Sloužit jako primární server WINS pro spojené fyzické sítě.

K nastavení stejného serveru WINS pro všechny klienty DHCP umístěné na podsítích přiřadte kód 44 možnosti DHCP (seznam adres IP serverů WINS) a jako hodnotu použijte adresu IP počítače serveru .

K zajištění, že server WINS je nejdříve použit všemi klienty DHCP pro překlad názvu typu NetBIOS (před pokusem rozlišit název pomocí všesměrového vysílání), přiřadte kód možnosti 46 (typ uzlu WINS/NBT), který identifikuje typ uzlu WINS jako uzel h (hybridní).

Posílení odolnosti proti chybám služby DHCP/WINS

K vytvoření instalace služeb DHCP a WINS více odolným proti chybám můžete nastavit dva servery s operačním systémem Windows 2000 Server tak, aby se navzájem chovaly jako poskytovatelé záložních služeb. V tabulce 4.12 jsou znázorněny funkce každého serveru (server 1 a server 2) při takovéto konfiguraci.

Tabulka 4.12 Servery DHCP/WINS

Název počítače	Stav serveru WINS	Stav serveru DHCP
Server 1	Primárně server WINS	Sekundárně Server DHCP
Server 2	Sekundárně server WINS	Primárně server DHCP

Jestliže chcete mezi servery DHCP vytvořit vztah primárního a záložního serveru, můžete rozdělit fond adres tak, že každý server poskytuje adresy klientům se vzdáleným přístupem. Jinou doporučovanou zvyklostí je umístění přibližně 75 procent fondu dostupných adres IP pro síť na primární server DHCP a zbývajících 25 procent fondu dostupných adres IP na záložní server DHCP.

Při definování oboru sdíleného dvěma servery DHCP musíte zajistit, že obor je konfigurován tak, aby nebyl spojený (bez přesahování) pro každý server, aby se zabránilo duplikování adres IP v nabídkách zápůjček obou serverů.

Další doporučení

Při současném používání serveru DHCP a WINS na téže síti zvažte následující možnosti vzájemné spolupráce:

Používání dalších možností oboru DHCP. Používejte možnosti DHCP k přiřazení typů uzlů WINS (typ možnosti 46) a k identifikaci serverů WINS pro používání klienty DHCP (typ možnosti 44). V některých případech to může znamenat úpravu těchto typů možností pro každou fyzickou podsíť, kam jsou servery DHCP a WINS implementovány.

Přiřazení doby trvání zápůjčky DHCP srovnatelné s intervaly pro obnovování používanými službou WINS. Dle výchozího nastavení je doba trvání zápůjčky DHCP osm dní a interval obnovování WINS je šest dní. Jestliže se doba zápůjčky DHCP velmi liší od intervalů obnovování WINS, může se jako důsledek na vaší síti zvýšit provoz správy zápůjček a může dojít k registraci WINS obou služeb. Jestliže dobu zápůjčky prodloužíte nebo zkrátíte, upravte odpovídajícím způsobem také interval obnovování WINS.

Nakonfigurujte všechna instalovaná připojení jako směrovatelná rozhraní. Operační systém Windows 2000 nezaručuje závazný pořádek pro NetBIOS, když je přítomno a aktivní více než jedno připojení. Všechny vícedomé servery WINS by měly mít své primární adresy IP přiřazené každému připojení k síti. Při konfigurování partnerů replikace na vícedomém počítači jako partnerských serverů pro nabízenou nebo vyžádanou replikaci se můžete ujistit, že se partner vždy připojuje ke stejnému adaptéru na vícedomém počítači – nakonfigurujte partnera tak, aby se odkazoval na vícedomý server pomocí určité adresy IP, ke které chcete, aby se partner připojoval. Jestliže je partner nakonfigurován tak, že se místo na určitou adresu IP odkazuje na název serveru při tom, když partner replikace přiřazuje název adresy IP, může poslat pakety WINS na vícedomý server na jakoukoli jeho adresu IP.

Servery DHCP a DNS

Servery DNS provádějí pro klienty sítě překlad názvů. Server DNS udržuje (kromě jiného) informace, které propojují úplný doménový název počítače (FDQN) s přiřazenou adresou (adresami) IP.

Zatímco DHCP poskytuje mocný nástroj pro automatickou konfiguraci adresy IP klienta, DHCP až do nedávné doby neuvědomovala službu DNS o aktualizaci záznamů DNS o klientovi, zvláště o aktualizaci mapování názvu klienta adresy IP a adresy IP názvu udržovaném na serveru DNS.

Bez možnosti propojení služby DHCP se službou DNS mohou být informace udržované službou DNS o klientovi DHCP nesprávné. Například klient může obdržet svou ad-

resu IP ze serveru DHCP, ale záznamy DNS nebudou odrážet získanou adresu IP ani poskytovat mapování nové adresy IP na název počítače (FQDN).

V operačním systému Windows 2000 mohou servery DHCP a klienti DHCP registrovat ke službě DNS, aby jí poskytovali tuto aktualizaci – pokud server DNS podporuje DNS s dynamickou aktualizací. Služba DNS pro Windows 2000 dynamickou aktualizací podporuje. Více informací najdete v této knize v kapitole „Služba Windows 2000 DNS“.

Server Windows 2000 DHCP se může hlásit k serveru DNS a aktualizovat záznamy prostředků ukazatele (PTR) a adresy (A) na základě svých klientů podporujících DHCP používajících protokol DNS dynamické aktualizace.

Schopnost registrovat oba záznamy typu A i PTR dovoluje serveru DHCP jednat pro účely registrace DNS jako server proxy pro klienty používající operační systém Microsoft Windows 95 a Windows NT 4.0 a další. Dodatečný kód možnosti DHCP (kód možnosti 81) umožňuje návrat FQDN klienta na server DHCP. Je-li toto implementováno, server DHCP může dynamicky aktualizovat službu DNS, aby upravila záznamy prostředků jednotlivých počítačů pomocí serveru DNS používajícího protokol dynamické aktualizace. Tato možnost DHCP dovoluje serveru DHCP následující možné interakce pro zpracování informací DNS jménem klientů DHCP, které zahrnují kód možnosti 81 ve zprávě DHCPRequest, kterou odesílají na server:

- Server DHCP vždy registruje klienty DHCP pro obě vyhledání DNS – dopředné (záznamy typu A) a zpětné (záznamy typu PTR).
- Server DNS nikdy neregistruje informace o mapování názvu adresy (záznamy typu A) klienta DHCP.
- Server DHCP registruje klienta DHCP pro obě vyhledání DNS – dopředné (záznamy typu A) a zpětné (záznamy typu PTR) pouze na základě požadavku klienta.

Služba DHCP a statická služba DNS nejsou kompatibilní pro udržování synchronizovaných mapování názvu adresy. To může způsobit problémy se současným používáním služby DHCP a DNS na síti, pokud používáte starší, statické servery DNS neschopné dynamické interakce při změně konfigurace klienta DHCP.

K zabránění neúspěšných vyhledávání klientů registrovaných u služby DHCP při spuštěné statické službě DNS proveďte následující kroky:

1. Jestliže jsou na síti používány servery WINS, povolte vyhledávání pro klienty DHCP, kteří používají NetBIOS.
2. Přiřaďte rezervace adres IP s nekonečnou dobou trvání zápůjčky klientů DHCP, kteří používají pouze službu DNS a nepodporují NetBIOS.

Kdykoli je to možné, aktualizujte nebo nahraďte starší servery se statickou službou DNS servery DNS podporujícími aktualizaci. Dynamická aktualizace je podporována službou Microsoft DNS pro Windows 2000.

Další doporučení

Při současném užívání služeb DNS a WINS zvažte následující možnosti spolupráce:

- Jestliže velké procento klientů používá NetBIOS a vy používáte DNS, zvažte vyhledávání WINS na serverech DNS. Jestliže je vyhledávání WINS na službě Microsoft DNS povoleno, Služba WINS je použita pro konečné překlad jakýchkoli názvů, které nebyly vyhledány za pomoci překladu DNS. Záznamy dopředného vyhledání WINS a zpětného vyhledání WINS-R jsou podporovány pouze službou DNS. Používáte-li na své síti servery, které nepodporují DNS, použijte Správce

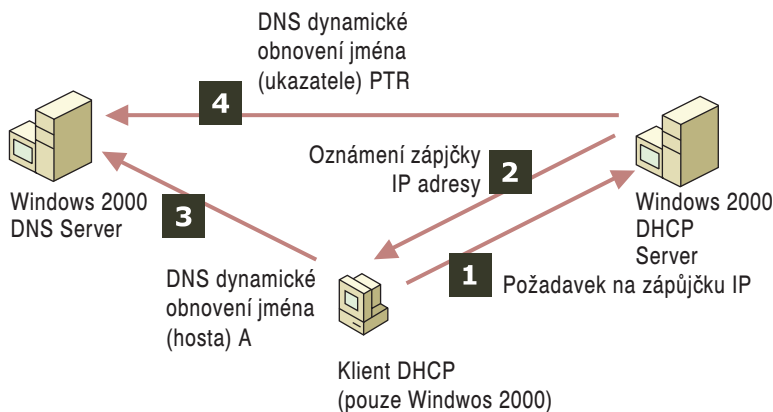
služby DNS a ujistěte se, že tyto záznamy služby WINS nejsou postupovány serverům DNS, které nepodporují vyhledávání WINS.

- Jestliže velké procento klientů na síti používá Windows 2000, zvažte vytvoření prostředí pouze se službou DNS. To zahrnuje vývoj migračního plánu aktualizace starších klientů WINS na Windows 2000. Otázky podpory dotýkající se síťové názvové služby jsou zjednodušeny díky jednotné názvové službě a službě vyhledávání prostředků (například WINS nebo DNS) na síti. Více informací najdete v této knize v části „Služba Windows Internet Name Service“ a „Služba Windows 2000 DNS“..

Klienti Windows DHCP a služba DNS s dynamickou aktualizací

Klienti Windows 2000 DHCP a klienti dřívější verze Windows DHCP se se službou DNS vzájemně různě ovlivňují. Server DHCP může být nakonfigurován tak, aby vždy registroval klienta DHCP pro obojí vyhledávání – dopředné (záznamy typu A) i zpětné (záznamy typu PTR) se službou DNS. Klienti Windows 2000 DHCP aktualizují své názvy dynamického dopředného vyhledávání.

Obrázek 4.21 znázorňuje, jak se klienti Windows 2000 DHCP ovlivňují s dynamickými aktualizacemi:



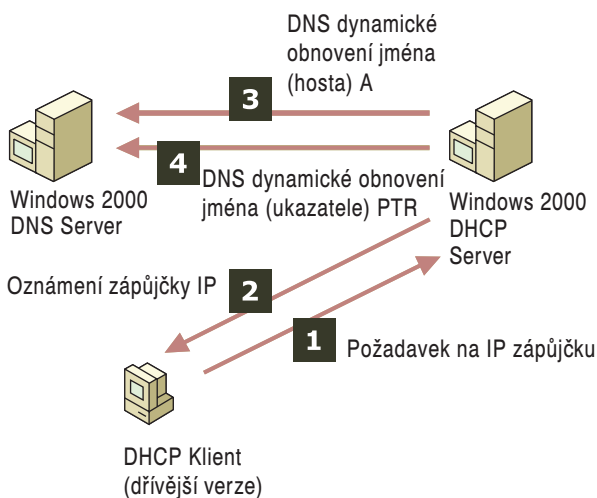
Obrázek 4.21 Klienti Windows 2000 DHCP a dynamické aktualizace

1. Klient Windows 2000 DHCP pošle požadavek o zápůjčku IP.
2. Server DHCP poskytne zápůjčku IP.
3. Klient Windows 2000 DHCP aktualizuje u serveru DNS svůj dopředný název (A).
4. Server DHCP aktualizuje u serveru DNS zpětný název (PTR) klienta používajícího protokol dynamické aktualizace.

Klienti dřívější verze Windows DHCP neinteragují přímo se serverem DNS, který provádí dynamickou aktualizaci. Na obrázku 4.22 je znázorněno, jak jsou názvy dopředného a zpětného předávání aktualizovány serverem DHCP:

1. Klient DHCP pošle požadavek o zápůjčku IP.
2. Server DHCP poskytne zápůjčku IP.
3. Server DHCP automaticky vygeneruje FQDN klienta připojením názvu domény definovaného pro obor k názvu klienta získaného pomocí zprávy DHCPRequest odeslané starším klientem.

4. Za pomoci protokolu dynamické aktualizace server DHCP aktualizuje dopředný (A) název DNS klienta.
5. Za pomoci protokolu dynamické aktualizace server DHCP aktualizuje zpětný (PTR) název DNS klienta.



Obrázek 4.22 Klienti starší služby DHCP a dynamické aktualizace

Služba DHCP a APIPA

Operační systém Windows 2000 a Windows 98 poskytují službu APIPA (Automatic Private IP Addressing), službu pro přiřazování jedinečných adres IP na malých sítích (sítích SOHO) bez instalace služby DHCP. Služba APIPA je určena pro malé sítě s méně než 25 klienty a umožňuje síťování Plug and Play přiřazením jedinečných adres IP počítačům na privátní síti LAN.

Služba APIPA používá rezervovaný rozsah adres IP (169.25.x.x) a algoritmus, který zaručuje, že každá použitá adresa je pro jeden počítač na privátní síti jedinečná.

Služba APIPA pracuje společně se službou DHCP. Je-li na síti nainstalována služba DHCP, služba APIPA se jí podrobí. Server DHCP může být do sítě přidán bez požadavků jakékoli konfigurace na základě služby APIPA. Služba APIPA pravidelně kontroluje přítomnost serveru DHCP a jakmile nějaký zjistí, nahradí adresy privátní sítě adresami IP dynamicky přiřazovanými serverem DHCP.

Vícedomé servery DHCP

Aby byl počítač serveru vícedomý, musí každé síťové připojení připojit počítač na více než jednu fyzickou síť. To znamená, že počítač potřebuje dodatečný hardware (ve formě více instalovaných síťových adaptérů).

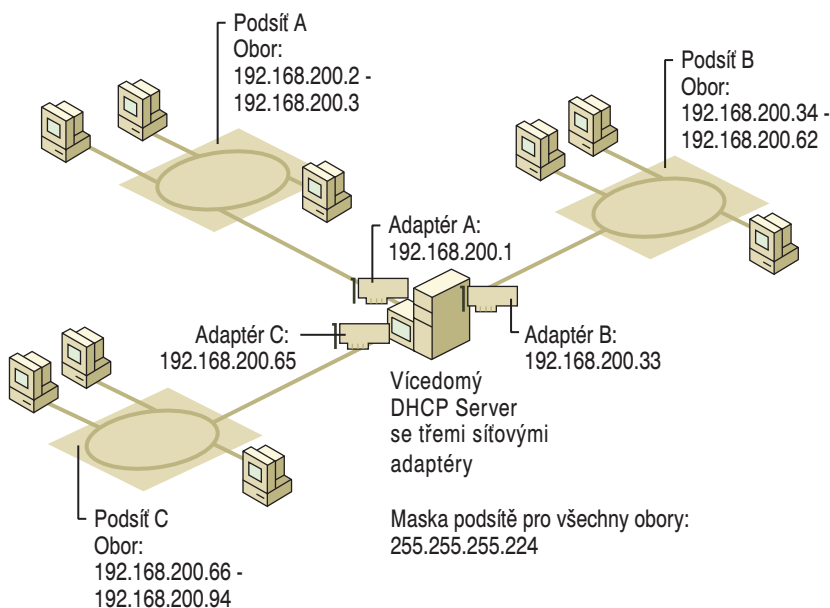
Počítač pod Windows 2000 Server může fungovat jako vícedomý server DHCP. Server DHCP se váže na první adresu IP nakonfigurovanou pro každé síťové připojení (tj. každé rozhraní síťového adaptéru) používané na serveru. Dle výchozího nastavení závisí vazba služeb na tom, jestli je připojení pro TCP/IP konfigurováno dynamicky nebo staticky. Jestliže je konfigurováno staticky, je připojení povoleno ve vazbách služeb pro

naslouchání a poskytování služby klientům DHCP. Jestliže je připojení nakonfigurováno dynamicky, jsou vazby služeb zakázány a neposkytuje službu klientům DHCP. Metody dynamické konfigurace zahrnují používání buď jiného serveru DHCP k získání zapůjčené konfigurace IP nebo autokonfiguraci adresy prostřednictvím vlastnosti APIPA poskytované ve Windows 2000. Více informací najdete dříve v této kapitole v části „Služba DHCP a APIPA“.

Obory serveru používají pro každé z vícedomých síťových připojení ke komunikaci s klienty DHCP primární adresu IP. K ověření primární adresy IP pro každé připojení použité v konfiguraci vícedomého serveru můžete prohlédnout vlastnosti protokolu TCP/IP pro každé připojení zařazené ve složce Síťová a telefonická připojení na serveru.

Konfigurování vícedomého serveru DHCP

Na obrázku 4.23 je znázorněn příklad vícedomého serveru DHCP s nainstalovanými třemi síťovými adaptéry. Každý adaptér je nakonfigurován k zapůjčování adres na oddělených fyzických podsítích.



Obrázek 4.23 Konfigurace vícedomého serveru DHCP

Vícedomý server DHCP má instalované tři adaptéry a je nakonfigurován staticky jednou adresou IP pro každý adaptér. Vzhledem k tomu, že adresování IP serveru DHCP také používá hodnotu upravené nebo vlastní masky podsítě (255.255.255.224), je tato hodnota aplikována pro všechny adresy IP, které jsou nakonfigurovány na serveru, a pro všechny další počítače používané na stejné podsíti. Zde je použit rozsah adres IP třídy C, od 192.168.200.1 do 192.168.200.254.

Každý z těchto tří adaptérů připojuje server k jiné fyzické podsíti (podsít A, B a C). Abyste dosáhli zamýšlených výsledků, tj. aby server DHCP poskytoval službu konfigurace zápisů všem klientům na odpovídající podsíti, musíte v průběhu instalace ověřit dva nezbytně nutné detaily:

1. Server musí používat staticky nakonfigurovanou adresu IP ve stejném rozsahu platných adres IP pro fyzickou síť, na které obsluhuje klienty.
2. Server musí mít každou ze svých platných adres IP podsítě vyloučenou z oboru používaného k nabízení zápůjček klientům.

Například pokud v tomto prostředí nebylo použito žádné zvláštní podsítování, výběr adres IP serveru DHCP není tak klíčový, protože síť IP a podsít IP jsou jedno a samé. Když je přednastavená hodnota masky podsítě (255.255.255.255) této sítě aplikována a používána, všech 254 možných ID počítačů je považováno za součást jedné velké podsítě.

Nicméně pokud je aplikována vlastní maska podsítě 255.255.255.224, ID sítě a ID podsítě nejsou jedno a samé. Když ID podsítě není stejné jako ID sítě, ujistěte se, že server DHCP má adresu IP přiřazenu v rámci stejné podsítě, které má sloužit.

Například u masky nastavené na všech počítačích na 255.255.255.224 jsou první tři bity posledního oktetu (224) brány z plných 8 bitů, které by normálně zahrnovaly celou část ID počítače. Tyto bity jsou používány protokolem IP k identifikaci fyzické podsítě. To umožňuje, aby zbývajících 8 bitů bylo využito jako skutečné neboli redukované pole ID počítače.

Takto síť uvedená v příkladu výše, požaduje na třech používaných podsítích, aby měly maximálně osm (neboli 23) potenciálně různých ID podsítě. Podobně každá z těchto podsítí může podporovat pouze až 32 (neboli 25) potenciálních ID počítače.

Vzhledem k podsítování se podsít A v tomto příkladě skládá z prvních 32 hodnot adres v této síti, od 0 do 31. Protože nelze přiřadit žádné ID počítače sestávající ze samých 0 nebo ze samých 1 v poli ID počítače, užitečný rozsah všech dostupných adres IP pro každou podsít klesne ze 32 na 30.

Ze zbývajících 30 adres potřebuje server DHCP jednu pro sebe. Zbývajících 29 adres může být nakonfigurováno v normálním oboru DHCP a používáno pro přiřazování zápůjček klientům podsítě. Výběr adresy, kterou bude používat server DHCP, závisí na správci, stejně jako rozhodnutí, jestli zahrnout staticky přiřazenou adresu IP serveru DHCP do oboru definovaného pro používání v každé podsíti.

Adresy IP vícedomého serveru (192.169.200.1, 192.168.200.33, 192.168.200.65) jsou za pomoci první dostupné adresy IP nakonfigurovány k používání pro každou ze tří podsítí. U výše uvedené konfigurace jsou tyto adresy vyloučeny z definovaných vazeb každého oboru vytvořeného pro tyto podsítě.

Případně můžete nastavit své obory tak, aby zahrnovaly tyto adresy v rámci definovaných vazeb oboru. Pokud tak učiníte, potřebujete vytvořit vyloučení adres, abyste tyto adresy IP serveru vyloučili z každého z možných oborů.

Jestliže je pro síťové připojení staticky nakonfigurována více než jedna adresa IP, služba Windows 2000 DHCP Server povolí používat pouze první nakonfigurovanou adresu IP v závislosti na povolování nebo zakazování vazeb služeb.

Správa přenosových agentů

Přenosový agent je malý program, který přenáší určitý typ zpráv ostatním hostitelům na síti. V sítích TCP/IP jsou k propojování hardwaru a softwaru na různých podsítích a k předávání paketů IP mezi podsítěmi používány směrovače.

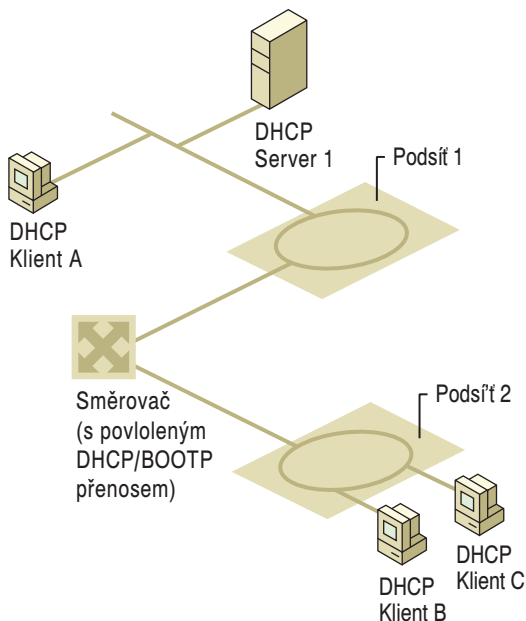
K podpoře a používání služby DHCP přes více podsítí by měly být směrovače připojující každou podsít kompatibilní s vlastnostmi přenosového agenta DHCP/BOOTP po-

psanými v dokumentu RFC 1542. Aby byl kompatibilní s dokumentem RFC 1542 a aby poskytoval podporu přenosového agenta, musí být každý směrovač schopen rozpoznat zprávy protokolu DHCP a BOOTP a zpracovat (přenést) je odpovídajícím způsobem. Vzhledem k tomu, že směrovače interpretují zprávy DHCP jako zprávy BOOTP (například zpráva UDP poslaná přes stejné číslo portu UDP a obsahující strukturu sdílené zprávy), směrovač s vlastnostmi přenosového agenta BOOTP typicky přenesení pakety DHCP a jakékoli pakety BOOTP poslané na síť.

Ve většině případů směrovače podporují přenos DHCP/BOOTP. Pokud vaše směrovače tento přenos nepodporují, kontaktujte svého výrobce nebo dodavatele směrovače, aby zjistil, zda lze tuto vlastnost podporovat pomocí aktualizace softwaru nebo firmwaru.

Případně, pokud směrovač nemůže fungovat jako přenosový agent DHCP/BOOTP, musí mít každá podsít buď svůj server DHCP nebo jiný počítač, který může fungovat na podsíti jako přenosový agent.

V případech, kdy je nepraktické nebo nemožné nakonfigurovat směrovače tak, aby podporovaly přenos DHCP/BOOTP, můžete nakonfigurovat počítač pod Windows 2000 nebo Windows NT Server 4.0, aby se choval jako přenosový agent, pomocí instalace služby přenosového agenta DHCP Relay Agent. Přenosový agent DHCP je hardwarové zařízení nebo softwarový program, který umí postupovat zprávy všesměrového vysílání DHCP/BOOTP z jedné podsítě na jinou podsít podle specifikace pro DHCP v dokumentu RFC 2131. Přenosoví agenti DHCP/BOOTP se chovají jako servery proxy, předávají zprávy z jedné podsítě na další. Dle výchozího nastavení je protokol DHCP protokolem založeným na všesměrovém vysílání, takže bez přenosových agentů a schopnosti postupovat zprávy DHCP a BOOTP přes směrovače by musela mít každá podsít na síti vlastní server DHCP.



Obrázek 4.24 Používání přenosového agenta

Jak pracuje přenosový agent

Na obrázku 4.24 je znázorněno, jak klient C na podsíti 2 získá zápůjčku adresy DHCP od serveru DHCP na podsíti 1.

1. Klient C pošle všesměrovým vysíláním zprávu DHCP/BOOTP DHCPDiscover na podsít 2 jako datagram UDP používající známý port UDP serveru 67 (číslo portu vyhrazené a sdílené pro komunikaci serverů BOOTP a DHCP).
2. Přenosový agent, v tomto případě směrovač podporující přenos DHCP/BOOTP, přezkoumá pole adresy IP brány v hlavičce zprávy DHCP/BOOTP. Jestliže pole má adresu IP 0.0.0.0, agent ho vyplní adresou IP přenosového agenta nebo směrovače a předá zprávu na vzdálenou podsít 1, kde je umístěn server DHCP.
3. Když server DHCP na vzdálené podsíti obdrží zprávu, přezkouší pole adresy IP brány v rámci oboru DHCP, který může být použit serverem DHCP k dodání zápůjčky adresy IP:
4. Jestliže má server DHCP 1 více oborů DHCP, adresa v poli adresy IP brány (giaddr) identifikuje obor DHCP, ze kterého se bude nabízet zápůjčka adresy IP.
Například jestliže v poli giaddr je adresa IP 201.2.45.2, server DHCP zkontroluje svou dostupnou sadu oborů adres pro rozsah oboru adres, které odpovídají síti IP třídy C, která zahrnuje adresu brány počítače. V tomto případě server DHCP zjišťuje, který obor obsahuje adresy mezi 201.2.45.1 a 201.2.45.254. Jestliže existuje obor, který odpovídá těmto kritériím, server DHCP z tohoto oboru vybere dostupnou adresu, kterou použije v nabídce zápůjčky adresy IP klientovi.
5. Když server DHCP 1 obdrží zprávu DHCPDiscover, zpracuje ji a pošle nabídku zápůjčky adresy IP (DHCPOffer) přímo přenosovému agentu identifikovanému v poli adresy IP brány (giaddr).
6. Směrovač přenesení nabídku zápůjčky adresy (DHCPOffer) klientovi DHCP.
Adresa IP klienta je stále neznámá, takže tak musí učinit pomocí všesměrového vysílání na lokální podsíti. Podobně je předána zpráva DHCPRequest od klienta k serveru a zpráva DHCPACK je přenesena ze serveru klientovi, a to podle dokumentu RFC 1542.

Řešení problémů

Tato část obsahuje metody pro určení příčiny komunikačních problémů spojených s DHCP a nástroje, které mohou ověřit statistiky a operace služby DHCP.

Mnoho problémů služby DHCP je způsobeno nesprávnými nebo chybějícími podrobnostmi konfigurace. Prohlédněte si „Nejlepší postupy“ pro instalaci a správu serverů DHCP, pomůže vám to předcházet většině obvyklých typů problémů.

Většina problémů spojených se službou DHCP začíná jako selhání konfigurace IP na klientovi, takže je dobrým zvykem začít právě zde.

Po zjištění, že problémy spojené se službou DHCP nevznikají na klientovi zkontrolujte protokol události systému a protokoly auditu serveru DHCP pro možná vodítka. Pokud se služba DHCP nespustí, tyto protokoly obecně vysvětlují zdroj selhání služby nebo její vypnutí.

Používání nástrojů Ipconfig a Winipcfg

Ipconfig je nástroj protokolu TCP/IP, kterou můžete použít z příkazového řádku. Příkaz **ipconfig** můžete použít k získání informací o parametrech konfigurace TCP/IP na lokálním nebo vzdáleném počítači na síti.

Více informací o tom, jak používat příkaz **ipconfig**, zjistíte po napsání **ipconfig /?** na příkazovém řádku.

Winipcfg je podobná nástroj pro klienty na bázi Windows 95 a Windows 98.

Řešení problémů klientů DHCP

Nejobvyklejším problémem klientů DHCP je selhání získání adresy IP nebo jiných konfiguračních parametrů od serveru DHCP během spouštění. Selže-li získání konfiguračních parametrů klienta, odpovězte si na následující otázky, které vám pomohou rychle zjistit zdroj problému.

Klient DHCP nemá nakonfigurovanou adresu IP nebo má adresu IP nakonfigurovanou jako 0.0.0.0.

Klient se nebyl schopen připojit k serveru DHCP a získat zápůjčku adresy IP, a to buď z důvodu selhání síťového hardwaru nebo z důvodu nedostupnosti serveru DHCP.

Ověřte, že klientský počítač má platné a funkční síťové připojení. Nejprve zkontrolujte, že hardwarová zařízení klienta (kabely a síťové adaptéry) pracují správně.

Klient DHCP má autokonfigurovanou adresu IP, která je pro současnou síť nesprávná.

Klient Windows 2000 DHCP nebo Windows 98 DHCP nemohl najít server DHCP a použil ke konfiguraci adresy IP vlastnost APIPA. V některých rozsáhlých sítích může být pro správu sítě žádoucí tuto vlastnost zakázat.

Nejprve proveďte příkaz **ping**, abyste otestovali připojení z klienta na server. Pak ověřte nebo se ručně pokuste o obnovu zápůjčky klienta. V závislosti na požadavcích sítě může být nezbytné zakázat klientovi vlastnost APIPA.

Dále, pokud se zdá, že hardware klienta funguje správně, zkontrolujte dostupnost serveru DHCP na síti pomocí příkazu ping z jiného počítače na téže síti, kde se nachází defektní klient DHCP.

Také se pokuste o uvolnění nebo obnovu zápůjčky adresy klienta a zkontrolujte nastavení konfigurace protokolu TCP/IP na automatickém adresování.

Klientovi DHCP chybí podrobnosti konfigurace.

Klientovi mohou v zapůjčené konfiguraci chybět možnosti DHCP buď proto, že server DHCP není nakonfigurován k jejich distribuci, nebo klient nepodporuje možnosti DHCP distribuované serverem.

U klientů Microsoft DHCP ověřte, že mají nakonfigurovanou většinu obvykle používaných a podporovaných možností buď na úrovni serveru, oboru, nebo klienta. Zkontrolujte nastavení možností DHCP.

Klient má přiřazenu úplnou a správnou sadu možností DHCP, ale zdá se, že jeho síťová konfigurace nepracuje korektně. Jestliže je server DHCP nakonfigurován nesprávnou možností směrovače DHCP (kód možnosti 3) pro adresu přednastavené brány klienta, klienti používající Windows NT nebo Windows 2000 nepoužívají nesprávnou adresu. Nicméně klienti DHCP s Windows 95 nesprávnou adresu používají.

Změňte seznam adres IP pro možnost směrovače (přednastavená brána) na aplikovatelném oboru a serveru a nastavte správnou hodnotu v záložce Možnosti oboru v dialogovém okně Vlastnosti oboru. Ve vzácných případech budete muset nakonfigurovat klienta DHCP tak, aby používal zvláštní seznam směrovačů odlišný od ostatních klientů oboru. V takových případech můžete přidat rezervaci a nakonfigurovat seznam možností směrovače zvlášť pro rezervovaného klienta.

Klienti DHCP nejsou schopni získat adresy IP od serveru.

Tento problém mohou způsobovat následující věci.

- Adresa IP serveru DHCP se změnila a nyní klienti DHCP nemohou získat adresy IP.

Server DHCP může obsloužit pouze požadavky na obor, který má ID sítě stejné jako ID sítě jeho adresy IP. Ujistěte se, že adresa IP serveru DHCP spadá do stejného síťového rozsahu jako obor, kterému slouží. Například server s adresou IP na síti 192.168.0.0 nemůže přiřazovat adresy z oboru 10.0.0.0, pokud nejsou použity množiny oborů.

- Klienti DHCP jsou umístěni přes směrovač z podsítě, kde sídlí server DHCP a nejsou schopni získat od serveru adresu.

Server DHCP může poskytovat adresy IP klientským počítačům na více vzdálených podsítích pouze v případě, že směrovač, který je odděluje, se může chovat jako přenosový agent DHCP. Postup podle následujících kroků může tento problém opravit:

1. Nakonfigurujte na podsíti klienta (to znamená na stejném segmentu fyzické sítě) přenosového agenta DHCP/BOOTP. přenosový agent může být umístěn na směrovači samém nebo na počítači na platformě Windows 2000 Server podporujícím službu DHCP Relay Service.
2. Na serveru DHCP nakonfigurujte obor, který bude odpovídat adrese sítě na druhé straně směrovače, kde jsou umístěni dotčení klienti.
3. V oboru se ujistěte, že maska podsítě vzdálené sítě je správná.
4. Použijte výchozí bránu na síťovém připojení serveru DHCP tak, že nepoužívá stejnou adresu IP jako směrovač, který podporuje vzdálenou podsít, kde jsou umístěni klienti.
5. Nezahrnujte tento obor (tedy obor pro vzdálenou podsít) do množin oborů nakonfigurovaných k používání na stejné lokální podsíti nebo segmentu, kde sídlí server DHCP.
6. Ujistěte se, že mezi serverem DHCP a klienty na vzdálené podsíti je pouze jediná logická trasa.

- Na stejné síti LAN existuje více serverů DHCP.

Ujistěte se, že nekonfigurujete na stejné síti LAN více serverů DHCP s překrývajícími se obory. Měli byste vyloučit možnost, že jedním z pochybných serverů DHCP je server SBS (Small Business Server). Ze své podstaty se služba DHCP, pokud běží pod serverem SBS, automaticky zastaví, když zjistí další server DHCP na síti LAN.

Řešení problémů serverů DHCP

Nejobvyklejší problémy se servery DHCP jsou neschopnost spustit server na síti v prostředí Windows 2000 nebo prostředí domény Active Directory nebo selhání klientů zís-

skat konfiguraci z funkčního serveru. Selže-li server při poskytování zápůjček klientům, selhání nejčastěji objeví klienti jedním ze tří způsobů:

- Klient je nakonfigurován k používání adresy IP neposkytované serverem.
- Server odešle zpět klientovi negativní odpověď a klient zobrazí chybové hlášení nebo nabídku, že server DHCP nelze nalézt.
- Server zapůjčí klientovi adresu, ale klient vypadá, že má jiné problémy založené na konfiguraci sítě, například neschopnost se registrovat nebo přeložit názvy typu NetBIOS nebo DNS nebo všimnout si počítačů za hranicemi stejné podsítě.

Obvyklé problémy

Následující podmínky chyb naznačují potenciální problémy se serverem DHCP:

- Správce se nemůže připojit k serveru DHCP pomocí Správce služby DHCP. Zpráva, která se objeví, může být „Server RPC není dosažitelný.“
- Klienti DHCP nemohou obnovit zápůjčky svých adres IP. Zpráva, která se objeví na klientském počítači, je „Klient DHCP nemůže obnovit zápůjčku adresy IP.“
- Služba klienta DHCP nebo služba Microsoft DHCP je zastavena a nelze ji opět spustit.

Prvním úkolem při řešení problémů je ujistit se, že služby DHCP jsou spuštěny. To lze ověřit pomocí otevření konzoly služby DHCP, kde je vidět stav služby, nebo pomocí otevření Služeb aplikací pod Správcem počítače. Není-li příslušná služba spuštěna, spusťte ji.

Za vzácných okolností nelze spustit server DHCP nebo se vyskytne chyba Stop. Je-li server DHCP zastaven, opět ho spusťte pomocí následujících kroků:

- Restart zastaveného serveru DHCP
 1. Spusťte Windows 2000 Server a přihlaste se k účtu s administrátorskými právy.
 2. Na příkazové řádce napište `net start dhcpserver` a stiskněte ENTER.

Poznámka: K vyhledání možného zdroje problémů se službami DHCP použijte Prohlížeč událostí ve složce Nástroje pro správu.

Služba Přenosového agenta DHCP je instalována, ale nefunguje

Služba přenosového agenta poskytovaná víceprotokolovým směrováním (MPR) neposkytuje adresu TCP/IP ze vzdáleného serveru DHCP.

Služba přenosového agenta DHCP je spuštěna na stejném počítači jako služba DHCP. Vzhledem k tomu, že obě služby naslouchají a odpovídají zprávám DHCP a BOOTP odeslaným pomocí portů UDP 67 a 68, v případě nainstalování obou služeb na jeden počítač nefunguje ani jedna spolehlivě.

Nainstalujte službu přenosového agenta DHCP a službu DHCP na oddělené počítače.

Konzola DHCP nesprávně hlásí čas vypršení zápůjčky

Když konzola DHCP zobrazuje čas vypršení zápůjčky rezervovaných klientů oboru, označuje jednu z následujících možností:

- Jestliže je doba trvání zápůjčky oboru stanovena na nekonečno, zápůjčka rezervovaného klienta je také zobrazena jako nekonečná.
- Jestliže je doba trvání zápůjčky oboru stanovena jako konečná (například osm dní), zápůjčka rezervovaného klienta používá stejnou dobu trvání zápůjčky.

Doba trvání zápůjčky rezervovaného klienta DHCP je určena dobou trvání zápůjčky přiřazené rezervaci.

K vytvoření rezervovaných klientů s nekonečnou dobou trvání zápůjčky vytvořte obor s nekonečnou dobou trvání zápůjčky a do tohoto oboru přidávejte rezervace.

Server DHCP používá k odpovědím na zprávy všech klientů všesměrové vysílání

Server DHCP používá k odpovědím na požadavky všech klientů o konfiguraci všesměrové vysílání bez ohledu na to, jak má každý klient DHCP nastaven příznak všesměrového vysílání. Klienti DHCP mohou nastavit příznak všesměrového vysílání (první bit v 16bitovém poli příznaku v hlavičce zprávy DHCP) při odesílání zpráv DHCPDiscover, aby serveru naznačili, že by měl při odpovědi pomocí zprávy DHCPOffer použít všesměrové vysílání na omezenou adresu všesměrového vysílání (255.255.255.255).

Dle výchozího nastavení server DHCP s operačním systémem Windows NT Server 3.51 a dřívějšími verzemi ignoroval příznak všesměrového vysílání ve zprávách DHCPDiscover a vysílal všesměrovým vysíláním pouze odpovědi DHCPOffer. Toto chování je implementováno na serveru proto, aby zabránilo problémům, které mohou vznikat u klientů neschopných přijímat nebo zpracovávat jednosměrovou odpověď před nakonfigurováním pro TCP/IP.

Počínaje operačním systémem Windows NT Server 4.0 se služba DHCP stále snaží poslat všechny odpovědi DHCP jako všesměrové vysílání IP na adresu omezeného všesměrového vysílání. Výjimkou jsou případy, kdy je povolena podpora jednosměrovým odpovědím nastavením hodnoty položky **IgnoreBroadcastFlag** v registru na **1**. Záznam je umístěn v:

```
HKEY_LOCAL_MACHINE\CurrentControlSet\Services\DHCPServer\Parameters\IgnoreBroadcastFlag
```

Je-li nastavena hodnota na 1, příznak všesměrového vysílání v požadavcích klienta je ignorován a všechny odpovědi DHCPOffer jsou ze serveru posílány všesměrovým vysíláním. Je-li hodnota nastavena na 0, chování serveru při přenosech (vícesměrové vysílání ano či ne) je určeno nastavením příznakového bitu všesměrového vysílání v požadavku klienta DHCPDiscover. Je-li v požadavku tento příznak nastaven, server posílá svou odpověď všesměrovým vysíláním na adresu omezeného lokálního všesměrového vysílání. Není-li tento příznak v požadavku nastaven, server pošle svou odpověď jednosměrným vysíláním přímo klientovi.

Server DHCP selže při vydávání zápůjčky adresy nového oboru

Za účelem přečíslování existující sítě byl na server DHCP přidán nový obor. Nicméně klienti DHCP nezískávají zápůjčky z nově definovaného oboru. Tato situace je nejčastější při snaze přečíslovat stávající síť IP.

Například pro svou síť můžete získat registrovanou třídu adres IP nebo můžete měnit třídu adres tak, abyste byli schopni uspokojit více počítačů nebo sítí. V těchto situacích chcete, aby klienti získali zápůjčky v novém oboru namísto získávání nebo obnovování zápůjček ze starého oboru. Poté, co všichni klienti aktivně získají zápůjčku z nového oboru, snažte se existující obor odebrat.

Nejsou-li dostupné nebo používané množiny oborů, může být v jednom časovém okamžiku na síti aktivní pouze jeden obor DHCP. Jestliže je na serveru DHCP definováno a aktivováno více oborů než jeden, používá se k poskytování zápůjček klientům pouze jeden obor.

Aktivní obor používaný k distribuci zápůjček je určen tím, jestli rozsah oboru adres obsahuje první adresu IP, která je vázána a přiřazena hardwaru síťovému adaptéru serveru.

ru DHCP. Jsou-li na serveru konfigurovány dodatečné sekundární adresy IP za pomoci záložky **Upřesnit vlastnosti TCP/IP**, nemají tyto adresy žádný vliv na server DHCP při vývěru oboru nebo při odpovídání na požadavky o konfiguraci klientů DHCP na síti.

Tento problém lze vyřešit následujícími způsoby:

- Nakonfigurujte server DHCP tak, aby používal množinu oborů, která zahrnuje starý obor a nový obor.

Pokud nemůžete změnit primární adresu IP přiřazenou kartě síťového adaptéru serveru DHCP, použijte k ovlivnění migrace oborů klientů DHCP na síti množiny oborů. Podpora množin oborů byla přidána do operačního systému Windows NT Server 4.0 v aktualizaci Service Pack 2 a je dostupná i ve Windows 2000 Server. Množiny oborů pomáhají a usnadňují migraci klientů oborů DHCP. Efektivně přesunete klienty ze starého oboru do nového za pomoci množiny oborů takto:

1. Definujete nový obor.
2. Přiřadíte a nakonfigurujete pro nový obor možnosti DHCP.
3. Definujete množinu oborů a přidejte do ní nový i starý obor (tedy obor, který odpovídá primární nebo první adrese IP přiřazené serveru DHCP na záložce **Vlastnosti TCP/IP**).
4. Aktivujete množinu oborů.
5. Ponechte původní obor aktivní a vylučte všechny adresy v rámci tohoto oboru.

Po tomto přechíslování pomocí množin oborů server DHCP po obdržení požadavku na obnovení:

1. Zkontroluje, jestli adresa IP klienta náleží do oboru, který zná. Vzhledem k tomu, že množina oborů zahrnuje i starý obor, server najde obor a zjistí, že tato adresa IP byla označena jako vyloučená.
2. Server zkontroluje, jestli v jeho databázi existuje zápůjčka tohoto klienta. Vzhledem k tomu, že server původně přiřadil zápůjčku tomuto klientovi, pošle mu jako odpověď na požadavek o obnovení zprávu DHCPNack.
3. Server je donucen žádat o novou adresu (klient vyšle všesměrovým vysíláním zprávu DHCPDiscover).
4. Server odpoví na požadavek DHCPDiscover zápůjčkou z nového oboru.

Druhým krokem v tomto procesu (když server zkontroluje existenci zápůjčky v databázi) je to, co odlišuje scénář přechíslování od používání více serverů na stejné podsíti:

- Jestliže server najde zápůjčku v databázi, pošle na požadavek o obnovu zprávu DHCPNack.
- Jestliže server zápůjčku nenajde, ignoruje požadavek o obnovení.

Více informací o používání množin oborů najdete v části „Správa oborů“.

Poznámka: K migraci do nového oboru můžete starý obor buď deaktivovat nebo vyloučit všechny adresy ve starém oboru. Server interpretuje obě metody naprosto stejně.

- Primární adresu IP (adresu přiřazenou v záložce **Vlastnosti TCP/IP**) na síťovém adaptéru serveru DHCP změňte na adresu IP, která je součástí stejné sítě jako nový obor.

V operačním systému Windows NT Server 3.51 není podpora množin oborů dostupná. V tomto případě musíte změnit první adresu IP nakonfigurovanou pro síťový adaptér serveru DHCP na adresu v rozsahu nového oboru adres. Je-li to nezbytné, stále můžete udržovat dřívější adresu, která byla jako první přiřazena jako aktivní adresa IP serveru jejím přemístěním do seznamu více adres IP udržovaném na záložce **Vlastnosti TCP/IP**.

Sledování výkonu serveru

Vzhledem k tomu, že servery DHCP mají v mnoha prostředích klíčovou důležitost, může sledování výkonu serverů pomoci při řešení problémů se snížením výkonu serveru.

V operačním systému Windows 2000 Server služba DHCP zahrnuje i sadu čítačů výkonnosti, které lze použít ke sledování různých typů aktivity serveru. Dle výchozího nastavení jsou tyto čítače dostupné po instalaci služby DHCP. K přístupu k těmto čítačům musíte použít program Sledování systému (dříve Sledování výkonu). Čítače serveru DHCP mohou sledovat:

- Všechny typy zpráv DHCP poslaných a obdržených službou DHCP.
- Průměrné množství procesorového času potřebného k odeslání a přijetí jednoho paketu zprávy.
- Počet paketů zprávy vyhozených kvůli interním zpožděním na serveru DHCP.

Čítače Sledování systému služby DHCP

Tabulka 4.13 obsahuje seznam čítačů sledování systému služby DHCP a jejich význam:

Tabulka 4.13 Čítače sledování systému služby DHCP

Název	Popis
Přijaté pakety/s	Počet paketů zpráv obdržených za sekundu. Velké číslo značí velký provoz zpráv spojený se službou DHCP na serveru.
Vynechané duplikáty/s	Počet duplikovaných paketů za sekundu vyřazených serverem DHCP. Velké číslo značí, že klientům pravděpodobně rychle vyprší časový limit nebo server neodpovídá příliš rychle.
Pakety s vypršelou platností/s	Počet paketů za sekundu, jimž vyprší časový limit a jsou serverem DHCP vyhozeny. Paketům vyprší časový limit, protože jsou ve frontě interních zpráv serveru příliš dlouho. Velké číslo značí, že serveru buď trvá zpracování některých paketů příliš dlouho, takže zbývající pakety se řadí do fronty, nebo je provoz na síti tak velký, že ho server DHCP nezvládne.
Milisekundy na paket (Průměr.)	Průměrný čas v milisekundách, který server DHCP potřebuje ke zpracování každého příchozího paketu. Toto číslo se může měnit v závislosti na hardwaru serveru a jeho podsystému V/V. Náhlý nebo bezdůvodný vzrůst může značit problémy, pravděpodobně se zpomalujícím se podsystémem V/V, nebo kvůli nějakým vnitřním nákladům na zpracování na serveru.

Název	Popis
Délka aktivní fronty	Aktuální délka fronty vnitřních zpráv serveru DHCP. Toto číslo se rovná počtu příchozích nezpracovaných zpráv. Velké číslo může značit velký provoz na serveru.
Délka kontrolní fronty konfliktů	Aktuální délka kontrolní fronty konfliktů serveru DHCP. Tato fronta udržuje zatím nezodpovězené zprávy, když server DHCP provádí zjišťování konfliktu adres. Velké číslo může značit velký provoz zá-půjček na serveru nebo to, že hodnota Pokusy serveru DHCP o zjištění konfliktů je nastavena jako příliš vysoká.
Vyhledání/s	Počet zpráv DHCPDiscover přijatých serverem za sekundu. Náhlý nebo abnormální vzrůst značí, že velké množství klientů se pravdě-podobně snaží o inicializaci a o získání zápůjčky adresy IP ze ser-veru, například při spuštění většího množství počítačů najednou.
Nabídky/s	Počet zpráv DHCPDiscover odeslaných serverem klientům za sekun-du. Náhlý nebo abnormální vzrůst značí velký provoz na serveru.
Požadavky/s	Počet zpráv DHCPRequest přijatých serverem za sekundu. Náhlý nebo abnormální vzrůst značí, že velké množství klientů se pravdě-podobně snaží o obnovu zápůjčky adresy IP ze serveru. To může značit, že doba trvání zápůjčky oboru je příliš krátká.
Informační zprávy/s	Počet zpráv DHCPInform přijatých serverem za sekundu. Zprávy DHCPInform se používají, když se server DHCP dotazuje adresářo-vé služby na kořen rozsáhlé sítě a když probíhá dynamická aktuali-zace serverem DHCP jménem klienta.
Potvrzení/s	Počet zpráv DHCPAck odeslaných serverem za sekundu. Náhlý ne-bo abnormální vzrůst značí, že server pravděpodobně obnovuje zá-půjčku velkému množství klientů. To může značit, že doba trvání zápůjčky oboru je příliš krátká.
Nepotvrzení/s	Počet zpráv DHCPNack odeslaných serverem za sekundu. Velmi vy-soká hodnota může značit potenciální problémy se sítí, buď špat-nou konfiguraci klientů nebo serveru. Při špatné konfiguraci serveru může být jedním z příčin deaktivovaný obor. Co se týče klientů, velmi vysoká hodnota může být způsobena počítači (například no-tebooky nebo jiná přenosná zařízení) přesunujícími se mezi podsí-těmi.
Odmítnutí/s	Počet zpráv DHCPNack přijatých serverem za sekundu. Vysoká hodnota značí, že několik klientů zjistilo, že jejich adresa je v kon-fliktu, tedy že jsou potenciální problémy se sítí. V této situaci může pomoci povolení zjišťování konfliktů na serveru DHCP. Při používá-ní na serveru by mělo být zjišťování konfliktů pouze dočasné. Po návratu situace do normálu by mělo být vypnuto.
Uvolnění/s	Počet zpráv DHCPRelease přijatých serverem za sekundu. Toto číslo je generováno pouze v případě, že klienti ručně uvolní svou adre-su, například při provedení příkazu ipconfig /release na klientském počítači. Vzhledem k tomu, že klienti své adresy uvolňují pouze zřídka, tento čítač by neměl být pro většinu sítí a konfigurací nijak vysoký.

Statistické údaje Správce služby DHCP

Služba DHCP, která podporuje typy objektů protokolu SNMP a MIBs, poskytuje grafické zobrazení statistických údajů. To pomáhá správců sledovat stav systému, například počet dostupných a spotřebovaných adres nebo počet zápůjček zpracovaných za sekundu. Dodatečné statistické informace zahrnují počet spravovaných zpráv a nabídek, stejně jako počet požadavků, potvrzení, odmítnutí, negativních potvrzení a přijatých uvolnění.

Ze Správce služby DHCP lze také získat celkový počet oborů a adres na serveru, počet využitých a dostupných adres. Tyto statistiky mohou být poskytovány pro určitý obor, i pro celý server, což zobrazí souhrn všech oborů spravovaných na tomto serveru.

Protokolování auditu DHCP

Služba Windows 2000 DHCP obsahuje několik nových vlastností protokolování a parametrů serveru, které poskytují vylepšené schopnosti auditu.

Chování protokolování auditu, o kterém pojednává tato část, se týká pouze služby DHCP pro Windows 2000 Server. Nahrazuje předchozí protokolování auditu používané v předchozích verzích operačního systému Windows NT Server, které neprováděly kontroly auditu a používaly pouze jeden soubor protokolu s názvem Dhcpsrv.log pro události služby protokolování.

Formátovaná struktura protokolů služby DHCP a úroveň zpráv udržovaných pro protokolování auditu je stejná jako v dřívějších verzích služby Windows DHCP. Více informací o struktuře protokolů se můžete dozvědět při prohlížení hlavičky každého protokolu v programu na editaci textu, například v programu Notepad.

Nyní můžete specifikovat následující vlastnosti:

- Adresářová cesta, kde služba DHCP ukládá soubory protokol auditu.
- Maximální omezení velikosti (v MB) pro celkový prostor na disku dostupný pro všechny soubory protokolu auditu vytvořené a uchovávané službou DHCP.
- Interval pro kontrolu disku, které je používáno k určení, kolikrát server DHCP zapisal události protokolu auditu do souboru protokolu před kontrolou dostupného prostoru na disku na serveru.
- Požadavek minimální velikosti (v MB) prostoru na disku, který je používán během kontroly disku, aby se zjistilo, jestli na disku existuje dostatek prostoru k pokračování protokolování auditu.

Prostřednictvím dialogových oken okna **Vlastnosti DHCP** můžete specifikovat:

- Adresářovou cestu, kde služba DHCP ukládá soubory protokol auditu.
- Maximální omezení velikosti (v MB) pro celkový prostor na disku dostupný pro všechny soubory protokolu auditu vytvořené a uchovávané službou DHCP.
- Interval pro kontrolu disku, které je používáno k určení, kolikrát server DHCP zapisal události protokolu auditu do souboru protokolu před kontrolou dostupného prostoru na disku na serveru.
- Požadavek minimální velikosti (v MB) prostoru na disku, který je používán během kontroly disku, aby se zjistilo, jestli na disku existuje dostatek prostoru k pokračování protokolování auditu.

Informace o postupu při specifikaci těchto parametrů najdete v dokumentaci online.

Názvy souborů protokolu auditu

Název souboru protokolu auditu je založen na aktuálním dni v týdnu tak, jak je určen aktuálním datem a časem serveru.

Například server DHCP se spustí, když je aktuální datum a čas sobota, 1. ledna 1900, 00:00:00 hodin, pak je soubor protokolu auditu nazván DhcpSrvLog.Sat.

Spuštění protokolu denního auditu

Když se server DHCP spouští nebo když se objeví nový den v týdnu (lokální čas v počítači je 00:00), server zapíše zprávu hlavičky do souboru protokolu auditu označující, že protokolování začalo. V závislosti na tom, jestli je soubor protokolu auditu nový nebo již existující soubor, probíhají následující činnosti:

- Jestliže soubor protokolu auditu již existoval bez úpravy více než 24 hodin, je přepsán.
- Jestliže souboru protokolu auditu existoval, ale byl upraven během předcházejících 24 hodin, není přepsán. Nové protokolování je k existujícímu souboru připojeno.

Kontroly disku

Po spuštění protokolování auditu server DHCP provádí pravidelné kontroly disku, aby se ujistil, že na disku serveru je dostatek dostupného prostoru a že aktuální soubor protokolu auditu není příliš velký nebo neroste příliš rychle.

Server DHCP provádí úplnou kontrolu disku, kdykoli nastaven jedna z následujících podmínek:

- Je zaprotokolován nastavený počet událostí.
- Na serveru se změní datum.

Interval používaný k určení frekvence periodických kontrol disku je nastaven na n počet zaprotokolovaných událostí, kde n je určeno hodnotou záznamu **DhcpLogDiskSpaceCheckInterval** v registru.

Po každém ukončení kontroly disku služba DHCP zkontroluje, jestli je prostor disku serveru plný. Disk se pokládá za plný, když je pravdivá kterákoli z následujících podmínek.

- Prostor na disku serveru je menší než požadované minimální množství pro protokolování auditu DHCP. To je určeno nakonfigurovanou hodnotou záznamu **DhcpLogMinSpaceOnDisk**. Přednastavená hodnota je **20 MB**.
- Aktuální soubor protokolu auditu je větší než jedna sedmina ($1/7$) maximálního přiděleného prostoru pro souhrn všech protokolů auditu aktuálně uložených na serveru. Velikost tohoto prostoru je určena hodnotou získanou podílem hodnoty záznamu **DhcpLogFilesMaxSize** a 7 – maximálního počtu potenciálních souborů protokolu auditu, který může být uložen na serveru. Například jestliže je záznam **DhcpLogFilesMaxSize** nastaven dle výchozího nastavení na 7, největší velikost, které může dosáhnout aktuální soubor auditu, je 1 MB.

Když je disk plný, server DHCP uzavře aktuální soubor a ignoruje další požadavky na protokolování událostí auditu až do 00:00 hodin nebo do zlepšení stavu, kdy disk už není plný.

I když jsou události protokolu auditu ignorovány z důvodu plného disku, server DHCP po počtu n událostí protokolu pokračuje v pravidelných kontrolách stavu prostoru na

disku. Počet *n* je nastaven v záznamu `DhcpLogDiskSpaceCheckInterval`. Jestliže následující kontroly disku určí, že na disku je dostupný požadovaný prostor, služba DHCP znovu otevře soubor protokolu z aktuálního dne a pokračuje v protokolování.

Ukončení protokolu denního auditu

V 00:00 hodin místního času na serveru server DHCP uzavře existující protokol a přesune s na soubor protokolu na následující den v týdnu. Například jestliže se den v týdnu mění v 00:00 hodin ze středy na čtvrtek, soubor protokolu nazvaný `DhcpSrvLog.wed` je uzavřen a je otevřen a pro protokolování událostí je používán soubor protokolu `DhcpSrvLog.thu`.

Obnova dat serveru

Obnova databáze serveru DHCP může být užitečná v případě, že se databáze poškodí nebo ztratí. Když nastane tato situace, poskytuje operační systém Windows 2000 Server progresivní sadu možností obnovení a opravy pro obnovení dat DHCP na serveru. Při řešení problémů poškození dat použijte k zjištění poškození a obnově služby DHCP následující kroky.

- Nejprve si potvrďte, že příčina ztráty nebo poškození dat je na serveru DHCP a proveďte předběžnou diagnostiku nebo opravy, například komprimaci databáze serveru DHCP. Je také dobré ověřit, že poškození není spojeno s dalšími problémy nebo podmínkami hardwarových nebo softwarových změn. Při ztrátě dat ověřte, že diskové jednotky serveru fungují správně. Ve většině případů se poškození databáze nejdříve objeví ve formě chybových hlášení databáze aplikace Jet v protokolu událostí systému.
- Za druhé, při selhání opravy můžete použít jednoduché zotavení serveru DHCP z dostupných možností zálohy databáze. Správce služby DHCP poskytuje možnost jednoduché zálohy, která účinně zálohuje databázi serveru DHCP. Existují také další možnosti získání záložní kopie databáze pro použití během zotavení, například z čerstvé zálohy diskových jednotek na pásku.
- Za třetí, nejsou-li dostupné jednoduché možnosti zotavení dat nebo jsou neúspěšné, můžete také vyzkoušet pokročilé metody zotavení dat nabízené konzolou DHCP a operačním systémem Windows 2000 Server ke zotavení určitých informací spojených s jednotlivými obory v databázi serveru DHCP.

Zjistíte-li, že služba DHCP běží jak na klientovi, tak na serveru, ale chyby pospané výše v části „Řešení problémů serverů DHCP“ přetrvávají, pak není databáze DHCP dostupná nebo je poškozená. Jestliže z jakéhokoli důvodu selže server DHCP, můžete obnovit databázi ze záložní kopie.

► Obnovení databáze DHCP

1. Před tím, než začnete, vytvořte si kopie souborů databáze serveru DHCP.
2. V adresáři `%SystemRoot%\System32\Dhcp` odstráňte soubory `J50.log`, `J50xxxxx.log` a `Dhcp.tmp`.
3. Zkopírujte nepoškozenou záložní verzi souboru `Dhcp.tmp` (z média ruční nebo automatické zálohy databáze) do adresáře `%SystemRoot%\System32\Dhcp`.
4. Restartujte server Microsoft DHCP.

Zjišťování poškození údajů aplikace DHCP Jet

Tabulka 4.14 obsahuje seznam možných zpráv služby DHCP, které se mohou objevit v protokolu událostí systému při poškození databáze serveru DHCP:

Tabulka 4.14 Chybová hlášení o poškození databáze Jet

ID události	Zdroj	Popis
1014	DhcpServer	Databáze Jet vrátila následující chybu: -510.
1014	DhcpServer	Databáze Jet vrátila následující chybu: -1022.
1014	DhcpServer	Databáze Jet vrátila následující chybu: -1850.

Typicky mohou být chyby aplikace Jet vyřešeny ruční komprimací databáze v režimu offline za použití nástroje Jetpack. V případech, kdy nástroj Jetpack selže při opravě databáze, může být k obnovení databáze serveru a zotavení služby DHCP na serveru použita obnova databáze serveru DHCP, jak je popsána v následujících částech.

Ke zotavení poškození databáze DHCP můžete použít následující možnosti určené k obnovení databáze:

- **Jednoduché zotavení.** Obnovte databázi ze záložní kopie souboru databáze, Dhcp.mdb.
Tato metoda je doporučována jako upřednostňovaná metoda zotavení, protože snižuje riziko ztráty informací dříve nakonfigurovaných a uložených na serveru DHCP a její provedení je mnohem jednodušší.
- **Pokročilé zotavení.** Registr lze upravit tak, aby vytvořil nový soubor databáze. Tato metoda může být užitečná jako podpůrná metoda pro zotavení dat, když není možná jednoduchá obnova databáze. Nicméně pokročilé zotavení je nutno provádět s nejvyšší opatrností. Více informací o obnově poškozené databáze DHCP najdete pod odkazem Microsoft Knowledge Base na adrese [WWW](http://windows.microsoft.com/windows2000/reskit/webresources) <http://windows.microsoft.com/windows2000/reskit/webresources>. K prohledání použijte klíčová slova DHCP, databáze a zotavení (resp. *DHCP*, database a recovery).

Jednoduché zotavení: obnova ze zálohy

Jestliže se databáze serveru DHCP poškodí nebo ztratí, je možné jednoduché zotavení nahrazením souboru databáze serveru (Dhcp.mdb) umístěném ve složce `%SystemRoot%\System32\Dhcp` záložní kopií stejného souboru. Pak můžete provést jednoduché zkopírování souboru, kdy přepíšete aktuální poškozenou databázi záložní kopií stejného souboru.

Jestliže byl prvně k povolení zálohy použit Správce služby DHCP, můžete získat záložní kopii souboru databáze serveru ze složky `%SystemRoot%\System32\Dhcp\Backup`. Můžete dát přednost obnovení souboru Dhcp.mdb také ze zálohové pásky nebo z jiného zálohového média.

Před obnovením souboru databáze ze zálohy musíte nejprve službu DHCP zastavit. Po zkopírování záložního souboru do složky `%SystemRoot%\System32\Dhcp` z vybraného zálohového zdroje můžete službu DHCP restartovat.

Službu DHCP zastavíte napsáním následujícího příkazu na příkazové řádce:

net stop dhcpserver

Po zastavení služby DHCP může být použit k bezpečnému obnovení záložní kopie databáze ze zálohového média nebo ze zálohové složky služby DHCP následující postup. Nejprve přesuňte soubory z existující složky DHCP do jiného umístění, například \Olddhcp. Buďte opatrní a nezměňte strukturu složky DHCP. Například napište k provedení tohoto kroku na příkazové řádce následující sadu příkazů:

```
md c:\Olddhcp
```

```
move %SystemRoot%\system32\DHCP\*. * C:\Olddhcp
```

Dále odstraňte poškozený soubor databáze. To lze rovněž provést pomocí příkazu na příkazové řádce:

```
del %SystemRoot%\system32\DHCP\Dhcp.mdb
```

Pak můžete zkopírovat záložní soubor databáze do složky služby DHCP. Cesta, kterou použijete při skutečném kopírování, se mění (viz tabulka 4.15) v závislosti na verzi operačního systému Windows konkrétního počítače, kde se obnovuje soubor databáze DHCP.

Tabulka 4.15 Umístění souborů databáze DHCP

Verze serveru	Použití příkazu copy
Windows NT Server 3.51	copy %SystemRoot%\system32\dhcp\backup\jet\dhcp.mdb %SystemRoot%\system32\dhcp\dhcp.mdb
Windows NT Server 4.0	copy %SystemRoot%\system32\dhcp\backup\jet\new\dhcp.mdb %SystemRoot%\system32\dhcp\dhcp.mdb
Windows 2000 Server	copy %SystemRoot%\system32\dhcp\backup\jet\new\dhcp.mdb %SystemRoot%\system32\dhcp\dhcp.mdb

Po zkopírování souboru databáze do správné složky DHCP na vašem serveru můžete restartovat službu DHCP.

Službu DHCP zastavíte napsáním následujícího příkazu na příkazové řádce:

```
net start dhcpserver
```

Předchozí postup by měl umožnit spuštění služby DHCP, ale pokud chybí informace o oboru, může být nezbytné použít záložní kopii registru k rekonfiguraci hodnot potřebných pro obnovení informací o oboru a o klientských rezervacích.

Znovuvytvoření zastaveného serveru DHCP

Jestliže hardware serveru DHCP funguje nesprávně nebo jiné problémy brání spuštění operačního systému Windows 2000, musíte přesunout databázi DHCP na jiný počítač.

► Přebudování serveru DHCP

1. Můžete-li pomocí příkazu **net start DHCP** spustit původní server DHCP, použijte příkaz **copy** a vytvořte si záložní kopie souborů v adresáři %SystemRoot%\System32\Dhcp. Jestliže nemůžete počítač vůbec spustit, musíte použít poslední verzi zálohy souborů databáze DHCP.
2. Instalujte si operační systém Windows 2000 Server a vytvořte nový server DHCP používající stejné umístění pevných disků a adresář %SystemRoot%. Pokud původ-

ní server ukládal soubory databáze DHCP do adresáře `%SystemRoot%\System32\Dhcp`, musí nový server DHCP k těmto souborům použít stejnou cestu.

3. Ujistěte se, že služba Microsoft DHCP na novém serveru je zastavená a pak použijte editor registru a obnovte ze záložních souborů klíče DHCP.
4. Zkopírujte záložní soubory DHCP do adresáře `%SystemRoot%\System32\Dhcp`.
5. Restartujte nový přestavěný server DHCP.

Přesun databáze serveru DHCP

Pokud potřebujete přesunout databázi DHCP na jiný počítač, použijte následující postup:

► Přesun databáze DHCP

1. Zastavte službu Microsoft DHCP na aktuálním počítači.
2. Zkopírujte adresář `\System32\Dhcp` na nový počítač, který je nakonfigurován jako server DHCP. Ujistěte se, že nový adresář je pod přesně stejným písmenem diskové jednotky a se stejnou cestou jako na starém počítači. Pokud musíte zkopírovat soubory do jiného adresáře, zkopírujte soubor `Dhcp.mdb`, ale nekopírujte soubory `.log` nebo `.chk`.
3. Spusťte službu DHCP na novém počítači. Služba automaticky začne používat soubory `.mdb` a `.log` zkopírované ze starého počítače.

Zkontrolujete-li Správce služby DHCP, obor stále existuje, protože registr udržuje informace o rozsahu adres oboru včetně rastru používaných adres. Ke sloučení databáze potřebujete přidat záznamy databáze pro existující zápůjčky v rastru adres. Jak se klienti obnovují, jsou přiřazováni k těmto zápůjčkám a databáze je nakonec opět úplná.

► Sloučení databáze DHCP

1. Ve Správci služby DHCP v menu Obor klepněte na Aktivní zápůjčky.
2. V dialogovém okně Aktivní zápůjčky klepněte na Sloučit.

I když to není vyžadováno, můžete přimět klienty DHCP k obnovení jejich zápůjček, aby se databáze DHCP aktualizovala co nejrychleji. Toho dosáhnete, zadáte-li na příkazové řádce příkaz **ipconfig/renew**.

Komprimace databáze serveru DHCP

Operační systém Windows 2000 a Windows NT Server 4.0 jsou navrženy tak, že automaticky komprimují databázi serveru DHCP. Nicméně pokud používáte operační systém Windows NT Server verze 3.51 nebo dřívější, budete muset po nějaké době používání služby DHCP databázi zkomprimovat, aby se zlepšil její výkon. Měli byste databázi zkomprimovat vždy, když dosáhne velikosti 30 MB.

Ke komprimaci databáze můžete použít nástroj Jetpack dodávanou s operačním systémem Windows NT Server verze 3.5 a 3.51. Program `Jetpack.exe` je nástroj příkazového řádku, která se spouští v okně příkazového řádku Windows NT. Tuto nástroj najdete v adresáři `%SystemRoot%\System32`.

Syntaxe programu `Jetpack.exe` je:

Jetpack.exe *database_name temp_database_name*

Například:

```
CD %SystemRoot%\SYSTEM32\DHCP
JETPACK DHCP.MDB TMP.MDB
```

V předcházejícím příkladě je Tmp.mdb dočasná databáze používaná programem Jetpack.exe. Dhcp.mdb je soubor databáze serveru DHCP.

Po spuštění programu Jetpack.exe provádí následující úlohy:

1. Zkopíruje informace o databázi do souboru dočasné databáze nazvaného Tmp.mdb.
2. Odstraní původní soubor databáze, Dhcp.mdb.
3. Přejmenuje dočasný soubor databáze na název původního souboru.

► **Komprimace databáze DHCP**

1. Otevřete konzolu Správce služby DHCP.
2. Vyberte aplikovatelný server DHCP.
3. Klepněte na Akce, vyberte položku **Všechny úlohy** a klepněte na **Zastavit**. (Případně napište na příkazové řádce příkaz **net stop DHCP**.)
4. Program Jetpack spustíte na příkazové řádce příkazem **jetpack**.
5. Za pomoci dialogového okna **Služby** restartujete službu DHCP.

Záchrana oborů pomocí vlastnosti Sloučit

Před použitím vlastnosti Sloučit k plnému zotavení informací o klientech oboru DHCP z registru, je nutno na serveru provést následující operace:

- Všechny klíče registru serveru DHCP musí být buď obnoveny nebo existovat a zůstat nedotčené z předcházejících operací služby na serveru.
- Ve složce *%SystemRoot%\System32\Dhcp* na serveru musí být obnovena čerstvá verze souboru databáze DHCP.

Pokud registr a databáze splňují tyto podmínky, můžete restartovat službu DHCP. V tomto okamžiku si při otevírání konzoly DHCP můžete všimnout, že jsou zobrazeny informace o oboru, ale nejsou zobrazeny žádné aktivní zápůjčky. Aktivní zápůjčky pro každý obor získáte pomocí vlastnosti Sloučit. Sloučení a zotavení dat oborů provedete u operačního systému Windows 2000 Server následujícím způsobem:

1. Ve Správci služby DHCP klepněte na obor.
2. Klepněte na složku Aktivní zápůjčky.
3. Klepněte pravým tlačítkem a vyberte **Úlohy** a pak klepněte na **Sloučit**.
4. Po objevení se dialogového okna **Slučování databáze** klepněte na **OK**.

Tento proces lze opakovat pro všechny obory – přidáte tak informace o zápůjčkách klientů a rezervacích klientů z registru zpět do seznamu aktivních zápůjček ke každému oboru původně nakonfigurovánu na serveru DHCP.

Po použití vlastnosti Sloučit si můžete všimnout, že při prohlížení vlastností jednotlivých klientů v seznamu aktivních zápůjček jsou informace o klientech zobrazeny nesprávně. Tyto informace jsou ve Správci služby DHCP opraveny a aktualizovány postupně, jak klienti oborů obnovují své zápůjčky.

Běží-li váš server DHCP pod operačním systémem Windows NT Server 4.0 s aktualizací Service Pack 2 a pozdější, povolte po použití této metody zotavení zjišťování konfliktů adres. Doporučuje se to z toho důvodu, že záloha mohla být provedena na starší databázi nebo mírně zastaralých datech registru systému. Více informací o tom, kdy používat a jak povolovat zjišťování konfliktů, najdete v této kapitole v části „Zjišťování konfliktů ze strany serveru“ a na stránkách WWW Microsoft Knowledge Base.

Ačkoli vlastnost Sloučit lze použít ke zotavení informací oboru v případě zotavení po pádu serveru DHCP, není tato vlastnost určena k nahrazení dalších tradičních zálohových opatření. K dalšímu bezpečnému uložení databáze v režimu offline a duplikování archivů databáze DHCP použijte další metody, například zálohování na pásku.

Analýza souborů protokolu serveru

Vzhledem k tomu, že operační systém Windows 2000 Server používá protokolování auditu při zápisu souborů protokolu serveru DHCP, není protokolování serveru DHCP náročné na prostředky. Lze ho nechat povolené, protože používá omezené množství prostoru na pevných discích serveru.

Formát souboru protokolu serveru DHCP

Protokoly serveru DHCP jsou textové soubory dělené čárkami, kde každý záznam protokolu představuje jeden řádek textu. Pole a jejich pořadí, jak se objevují v každém záznamu souboru protokolu jsou:

Datum ID, čas, popis, adresa IP, název počítače, adresa MAC

Každé z těchto polí je dále podrobně popsáno v tabulce 4.16.

Tabulka 4.16 Pole souboru protokolu

Pole	Popis
ID	Kód ID události serveru DHCP.
Datum	Datum, kdy byl tento záznam na serveru DHCP zaprotokolován.
Čas	Čas, kdy byl tento záznam na serveru DHCP zaprotokolován
Popis	Popis události serveru DHCP.
Adresa IP	Adresa IP klienta DHCP.
Název počítače	Název počítače klienta DHCP.
Adresa MAC	Adresa MAC používaná hardwarem síťového adaptéru klienta.

Kódy události protokolu serveru DHCP

Protokol serveru DHCP také používá zvláštní kódy ID události, jimiž označuje informace o typu protokolované události služby.

V tabulce 4.17 najdete popis těchto kódů ID události.

Tabulka 4.17 Kódy ID události

ID události	Popis
00	Protokol byl zahájen.
01	Protokol byl ukončen.
02	Protokol byl dočasně zastaven kvůli malému prostoru na disku.
10	Klientovi byla zapůjčena nová adresa IP.
11	Klient si obnovil zápůjčku.
12	Klient uvolnil zápůjčku.

ID události	Popis
13	Na síti byla nalezena používaná adresa IP.
14	Nelze uspokojit požadavek zápůjčky, protože fond adres byl vyčerpán.
15	Zápůjčka byla zamítnuta.
20	Klientovi byla zapůjčena adresa BOOTP.

Další informace

Více informací o používání služby DHCP najdete v následujících knihách:

- *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture*, Third Edition: Douglas Comer, 1995, Englewood Cliffs, NJ: Prentice Hall.
- *Managing a Microsoft Windows NT Network*: Microsoft Corporation, 1999, Redmond, WA: Microsoft Press.
- *Mastering TCP/IP For NT Server*: M. Minasi, T. Lammle, and M. Lammle, 1997, Alameda, CA: Sybex.
- *Optimizing Network Traffic*: Microsoft Corporation, 1999, Redmond, WA: Microsoft Press.
- *TCP/IP Unleashed: T. Parker*, 1996, Indianapolis, IN: Sams Publishing.
- *TCP/IP Illustrated, Volume 1: The Protocol*: W.R. Stevens, 1994, Reading, MA: Addison-Wesley.
- *Windows NT TCP/IP Network Administration*: C. Hunt, and R.B. Thompson, 1998, Sebastopol, CA: O'Reilly and Associates.

5. KAPITOLA

Úvod do DNS

Služba DNS (Domain Name System) umožňuje používat hierarchické, popisné názvy ke snadnému vyhledání počítačů a dalších prostředků na síti IP. Následující části popisují základní koncepty služby DNS včetně vlastností vysvětlených v novějších dokumentech RFC, například dynamická aktualizace, podle standardu IETF. Zvláštní implementace služby DNS v operačním systému Microsoft® Windows® 2000 není v rámci této kapitoly projednávána kromě míst, která jsou označena.

Více informací o implementaci služby DNS do operačního systému Windows 2000 najdete v této knize v části „Služba Windows 2000 DNS“.

Služba DNS je distribuovaná databáze, která obsahuje mapování doménových DNS názvů na data. Je to také protokol pro síť TCP/IP definovaný dokumenty RFC, které se vztahují k DNS. Služba DNS definuje následující:

- Mechanismu pro dotazování a aktualizaci databáze.
- Mechanismus pro replikování informací v databázi mezi servery.
- Schéma pro databáze.

V této kapitole najdete

Úvod do služby DNS	240
Servery DNS	245
Překlad názvu	247
Záznamy prostředků a zóny	250
Formát záznamů prostředků	250
Zónový přenos	263
Dynamická aktualizace	263
Standardy služby DNS	264

Další informace v sadě Resource Kit

- Více informací o protokolech TCP/IP najdete v této knize v části „Úvod do TCP/IP“.
- Více informací o implementaci služby DNS do operačního systému Windows 2000 najdete v této knize v části „Služba Windows 2000 DNS“.

Úvod do služby DNS

Přestože protokol TCP/IP používá adresy IP k lokalizaci a připojení k hostitelům (počítačům a dalším zařízením sítě TCP/IP), uživatelé zpravidla dávají přednost popisným názvům. Například uživatelé dávají přednost popisnému názvu namísto adresy IP 172.16.23.55. Služba DNS popsaná v dokumentu RFC 1034 a 1035 se používá na Internetu k poskytování standardní konvence pro názvy pro vyhledávání počítačů na platformě IP.

Před implementací služby DNS bylo na Internetu používání názvů k lokalizaci prostředků na sítích TCP/IP podporováno pomocí souboru nazvaného Hosts. Správci sítě vkládali názvy a adresy IP do souboru Hosts a počítače tento soubor používaly pro překlad názvu.

Jak soubor Hosts, tak služba DNS používají *obor názvů*. Obor názvů je seskupení, ve kterém mohou být názvy použity k symbolické reprezentaci jiného typu informace, například adresy IP, a ve kterém jsou stanovena zvláštní pravidla určující způsob vytváření a používání názvů. Některé obory názvů, například DNS, jsou hierarchicky strukturovány a poskytují pravidla, která umožňují rozdělení oboru názvů do podmnožin názvů pro distribuci a delegování částí oboru názvů. Jiné obory názvů, například obor názvů Hosts, nelze dělit a musí být distribuovány jako celek. Kvůli tomu působilo používání souboru Hosts správcům sítě problémy. Jak počet počítačů a uživatelů Internetu rostl, stala se úloha aktualizace a distribuce souboru Hosts nevládnutelnou.

Služba DNS nahrazuje soubor Hosts distribuovanou databází, která implementuje hierarchický systém zpracování názvů. Tento systém zpracování názvů umožňuje růst Internetu a vytváření názvů, které jsou v síti Internet a v sítích typu intranet na platformě TCP/IP jedinečné.

Obor doménových názvů

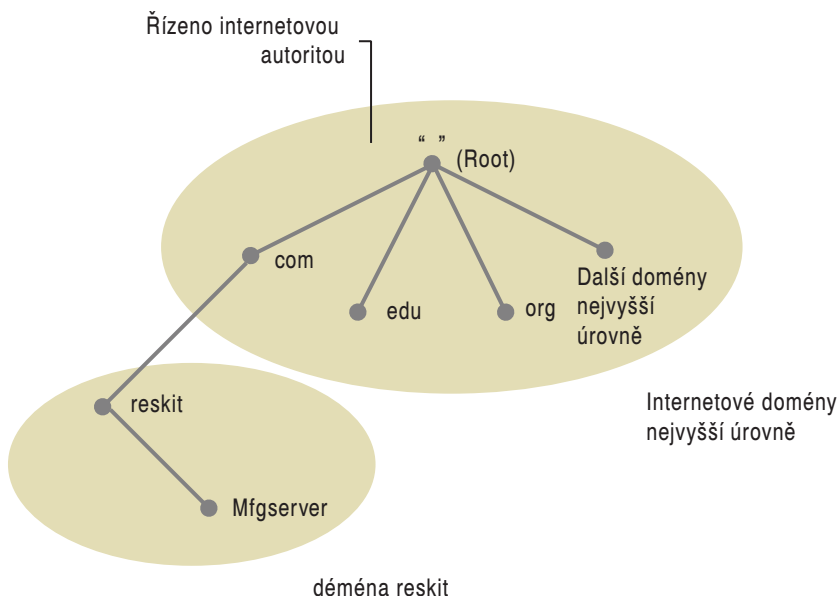
Systém zpracování názvů, na kterém je založena služba DNS, je hierarchická a logická stromová struktura nazvaná *obor doménových názvů*. Organizace mohou také vytvořit privátní síť, které nejsou na Internetu viditelné, za použití vlastních oborů doménových názvů. Obrázek 5.1 znázorňuje část oboru doménových názvů Internetu, od kořenové domény a domén DNS pro Internet nejvyšší úrovně až po fiktivní doménu DNS nazvanou reskit.com, která obsahuje hostitele (počítač) nazvaného Mfgserver.

Každý uzel ve stromu DNS představuje název DNS. Některými příklady názvů DNS jsou domény DNS, počítače a služby. Doména DNS je větev pod uzlem. Například v obrázku 5.1 je reskit.com doména DNS. Domény DNS mohou obsahovat jak hostitele (počítače nebo služby), tak další domény (nazývané též poddomény). Každé organizaci je přiřazeno oprávnění pro část oboru doménových názvů a taková organizace je odpovědná za správu dalšího dělení a zpracování názvů domén DNS a počítačů v rámci této části oboru názvů.

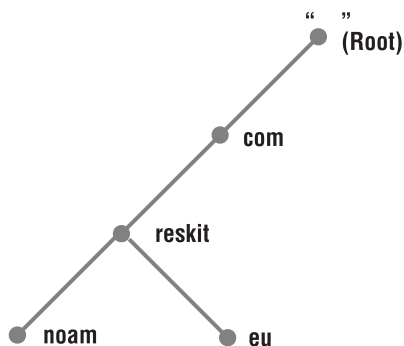
Další dělení je ve službě DNS důležitým konceptem. Vytváření dalšího rozdělení oboru doménových názvů a domén DNS privátních sítí TCP/IP podporuje nový růst Internetu a schopnost bez přerušení rozšiřovat seskupení názvů a administrativních seskupení. Další dělení je obecně vzato založeno na rozdělení tématickém nebo zeměpisném.

Například doména DNS reskit.com může zahrnovat sídla v Severní Americe a Evropě. Správce DNS domény DNS reskit.com může dále rozdělit tuto doménu na dvě poddo-

mény, které odrážejí tato seskupení: noam.reskit.com a eu.reskit.com. Na obrázku 5.2 jsou znázorněny příklady těchto poddomén.



Obrázek 5.1 Systém doménových názvů



Obrázek 5.2 Poddomény

Doménový název

Počítače a domény DNS mají základ názvu závislý na pozici v doménovém stromu. Například protože reskit je poddoménou domény .com, doménový název pro reskit je reskit.com.

Každý uzel v doménovém stromě DNS může být identifikován *úplným doménovým názvem* (fully qualified domain name, FQDN). Název FQDN je doménový název, který byl jednoznačně určen tak, aby s naprostou jistotou označoval jeho umístění vzhledem ke kořeni doménového stromu DNS. To kontrastuje s relativním názvem, což je název relativní vzhledem k jiné doméně DNS, než je doména kořenová.

Poznámka: Obecně řečeno, názvy FQDN mají omezení vytváření názvů, které umožňují používat pouze znaky a – z, A – Z, 0 – 9 a pomlčku nebo minus (-). Použití tečky (.) je povoleno pouze mezi jmenovkami názvů domén (například „reskit.com“) nebo na konci názvu FQDN. Doménové Názvy nerozlišují velká a malá písmena. Můžete nakonfigurovat server Windows 2000 DNS tak, aby preferoval některá nebo všechna omezení znaků dle dokumentu RFC, nebo aby všechna tato omezení znaků ignoroval. Více informací najdete v této knize v části „Služba Windows 2000 DNS“.

Obor doménových názvů Internetu

Kořen (absolutně nejvyšší úroveň) oboru doménových názvů Internetu je spravován úřadem pro registraci názvů Internetu, který deleguje odpovědnost za správu částí oboru doménových názvů organizacím, které se připojují k Internetu.

Pod kořenovou doménou DNS leží domény nejvyšší úrovně také spravované úřadem pro registraci názvů Internetu. Existují tři typy domén nejvyšší úrovně:

- Organizační domény. Tyto domény jsou pojmenovány pomocí tříznakového kódu, který označuje primární funkci nebo činnost organizací zahrnutých v doméně DNS. Organizační domény jsou obecně pouze pro organizace v rámci Spojených států a většina organizací umístěných v USA je obsažena v jedné z těchto organizačních domén.
- Geografické domény. Tyto domény jsou pojmenovány pomocí dvouznakového kódu země/regionu ustaveného organizací ISO 3166.
- Zpětné (reverzní) domény. Toto je zvláštní doména pojmenovaná in-addr.arpa, která je používána pro mapování adres IP na názvy (zvané též *zpětné vyhledání*). Více informací najdete později v této kapitole v části „Překlad názvů“. Existuje také zvláštní doména nazvaná IP6.INT, která se používá ve zpětných vyhledáních protokolu IP verze 6. Více informací najdete v dokumentu RFC 1886.

Nejobvyklejší součásti názvů DNS nejvyšší úrovně pro organizace v USA jsou popsány v tabulce 5.1.

Tabulka 5.1 Součásti názvů nejvyšší úrovně hierarchie DNS

součást názvu nejvyšší úrovně	Popis	Příklad názvu domény DNS
.com	Úřad pro názvy Internetu deleguje část oboru doménových názvů této úrovně komerčním organizacím, například společnosti Microsoft Corporation.	microsoft.com
.edu	Úřad pro názvy Internetu deleguje část oboru doménových názvů této úrovně vzdělávacím institucím, například Massachusetts Institute of Technology (MIT)	mit.edu
.gov	Úřad pro názvy Internetu deleguje část oboru doménových názvů této úrovně vládním organizacím, jako je například Bílý dům ve Washingtonu, D.C.	whitehouse.gov
.int	Úřad pro názvy Internetu deleguje část oboru doménových názvů této úrovně mezinárodním organizacím, například NATO.	nato.int
.mil	Úřad pro názvy Internetu deleguje část oboru doménových názvů této úrovně vojenským operacím, například Defense Data Network (DDN).	ddn.mil

součást názvu nejvyšší úrovně	Popis	Příklad názvu domény DNS
.net	Úřad pro názvy Internetu deleguje část oboru doménových názvů této úrovně síťovým organizacím, například National Science Foundation (NSF).	nsf.net
.org	Úřad pro názvy Internetu deleguje část oboru doménových názvů této úrovně nekomerčním organizacím, například CNIDR.	cnidr.org

Navíc k doménám nejvyšší úrovně uvedeným výše mají jednotlivé země své vlastní domény nejvyšší úrovně. Například doména .ca je doména nejvyšší úrovně Kanady.

Pod doménami nejvyšší úrovně úřad pro názvy Internetu deleguje domény organizacím, které se připojují k Internetu. Organizace, kterým úřad pro názvy Internetu deleguje část oboru doménových názvů je pak odpovědná za vytváření názvů počítačů a síťových zařízení v rámci přiřazené domény a jejích dalších rozdělení. Tyto organizace používají ke správě mapování názvů na adresy IP a adres IP na názvy pro hostitelská zařízení v rámci své části oboru názvů servery DNS.

Základní koncepty DNS

Tato část poskytuje stručné definice dalších konceptů služby DNS, které jsou podrobněji popsány v následujících částech kapitoly.

Servery DNS. Počítače, které provozují programy serveru DNS obsahující informace z databáze DNS o stromové struktuře stromu domén DNS. Servery DNS se také snaží řešit dotazy klientů. Po dotazu mohou servery DNS poskytnout požadované informace, poskytnout odkaz na jiný server, který může pomoci s řešením dotazu nebo odpovědět, že nezná požadované informace nebo že takové informace neexistují.

Překladače služby DNS. Programy, které používají k získání informací ze serverů dotazy DNS. Překladače mohou komunikovat buď se vzdálenými servery DNS, nebo s programem serveru DNS běžícím na lokálním počítači. Překladače jsou zpravidla vestavěny do programů nástrojů, případně jsou dostupné přes funkce knihovny. Překladač může být spuštěn na jakémkoli počítači, a to včetně serveru DNS.

Záznamy prostředků. Množiny informací v databázi DNS, které lze použít ke zpracování dotazů klientů. Každý server DNS obsahuje záznamy prostředků, které potřebuje k zodpovídání dotazů pro tu část oboru názvů DNS, kde je určující (autoritativní). (Server DNS je určující pro část oboru názvů DNS, jestliže obsahuje informace o této části oboru názvů.)

Zóny. Souvislé části oboru názvů DNS, pro které je server určující. Server může být určující pro jednu nebo více zón.

Soubory zón. Soubory, které obsahují záznamy prostředků zón, pro které je server určující. Ve většině implementací služby DNS jsou zóny implementovány jako textové soubory.

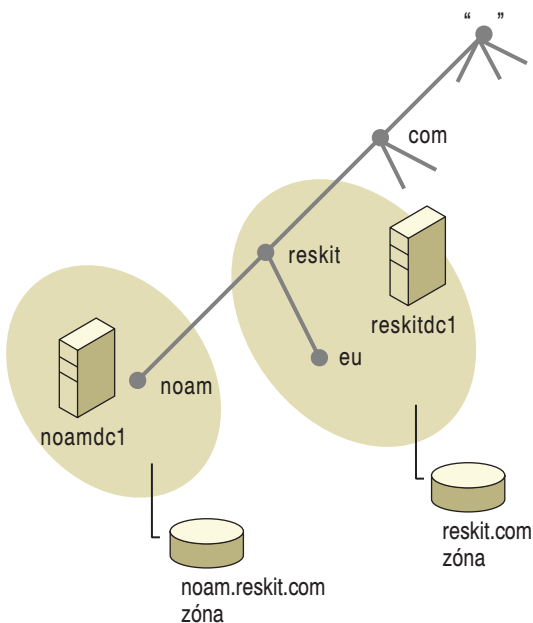
Zóny

Zóna je část oboru názvů DNS. Obsahuje sadu záznamů uložených na serveru DNS. Každá zóna je ukotvená na určitém uzlu domény. Nicméně zóny nejsou domény. *Doména DNS* je větev oboru názvů, zatímco zóna je část oboru názvů DNS obecně ulo-

žená v souboru a může obsahovat více domén. Doména může být dále rozdělena na několik částí a každá část nebo zóna může být řízena samostatným serverem DNS. Za použití zóny server DNS odpovídá na dotazy týkající se hostitelů v této zóně a je pro tuto zónu určující. Zóny mohou být primární nebo sekundární. *Primární zóna* je kopie zóny, kde probíhají aktualizace, zatímco *sekundární zóna* je kopie zóny, která je replikována z nadřazeného serveru.

Zóny lze ukládat různými způsoby. Například mohou být uloženy jako soubory zón. Na serverech Windows 2000 mohou být uloženy též v adresářové službě Active Directory™. Některé sekundární servery je ukládají do paměti a provádějí přenos zón při každém restartu.

Obrázek 5.3 zobrazuje příklad domény DNS, která obsahuje dvě primární zóny. V tomto příkladě obsahuje doména rekit.com dvě poddomény: noam.reskit.com a eu.reskit.com. Autoritu pro poddoménu noam.reskit.com má delegovánu server noamdc1.noam.reskit.com. Proto, jak je znázorněno na obrázku 5.3, jeden server, noamdc1.noam.reskit.com, hostí zónu noam.reskit.com, a druhý server, reskitdc1.reskit.com, hostí zónu reskit.com, která obsahuje poddoménu eu.reskit.com.



Obrázek 5.3 Domény a zóny

Místo delegování zóny noam.reskit.com na server noamdc1.noam.reskit.com může správce také nakonfigurovat reskitdc1, aby hostila zónu noam.reskit.com.

Můžete také nakonfigurovat ke správě stejné zóny dva různé servery. Pouze jeden server může spravovat primární zónu každé domény DNS. Existuje jedna výjimka: více počítačů může spravovat zóny integrované adresářovou službou Windows 2000 Active Directory. Více informací najdete v této knize v části „Služba Windows 2000 DNS“.

Jeden server DNS můžete nakonfigurovat tak, aby spravoval jednu nebo více zón v závislosti na vašich potřebách. K distribuci administrativních úloh na různé skupiny

a k poskytování efektivní distribuce dat můžete vytvořit více zón. Můžete také uložit stejnou zónu na více serverů, čímž zajistíte vyváženost zatížení a odolnost proti chybám. Více informací o tom, co zóny obsahují, najdete později v této kapitole v části „Záznamy prostředků a zóny“.

Servery DNS

Servery DNS uchovávají informace o žádné zóně, o jedné zóně či o více zónách. Když server DNS obdrží dotaz DNS, snaží se najít příslušnou informaci pomocí dat ze svých lokálních zón. Jestliže toto selže kvůli tomu, že není pro požadovanou doménu DNS určující, server může kvůli řešení dotazu zkontrolovat svou mezipaměť, komunikovat s dalšími servery DNS nebo odkázat klienta na jiný server DNS, který by mohl znát odpověď.

Servery DNS mohou hostit primární a sekundární zóny. Servery můžete nakonfigurovat tak, aby hostily tolik různých primárních a sekundárních zón, kolik je praktické, což znamená, že server může hostit primární kopii jedné zóny a sekundární kopii jiné zóny, nebo může hostit pouze primární nebo pouze sekundární kopii zóny. U každé zóny se server, který hostí primární zóny, považuje za *primární server* pro tuto zónu a server, který hostí sekundární zóny, považuje za *sekundární server* pro tuto zónu.

Primární zóny jsou lokálně aktualizované. Pro provedení změny dat zóny, například delegování části zóny jinému serveru DNS nebo přidání záznamů prostředků v zóně, se tyto změny musí provést na primárním serveru DNS této zóny, aby byly nové informace uloženy do lokální zóny.

Naproti tomu sekundární zóny jsou replikovány z jiného serveru. Po definování sekundárního serveru zóny je zóna nakonfigurována na adresu IP serveru, ze kterého má být zóna replikována. Server, ze kterého se soubor zóny replikuje, může být primární nebo sekundární server této zóny a je někdy nazýván nadřazený server sekundární zóny.

Po spuštění se sekundární server zóny kontaktuje nadřazený server zóny a iniciuje přesun zóny. Sekundární server zóny také opakovaně kontaktuje nadřazený server zóny, aby zjistil, jestli se data zóny změnila. Pokud ano, může iniciovat přenos zón, označovaný jako zónový přenos. Více informací o zónových přenosech najdete později v této kapitole v části „Zónový přenos“.

Pro každou zónu musíte mít primární server. Navíc byste měli mít pro každou zónu aspoň jeden sekundární server. V opačném případě, pokud primární server zóny selže, nikdo nebude schopen přeložit názvy v takovéto zóně.

Sekundární server přináší následující výhody:

Odolnost proti chybám Když je pro zónu nakonfigurován sekundární server, klienti mohou stále překládat názvy této zóny i v případě, že primární server zóny selže. Obecně řečeno, naplánujte si instalaci primárního a sekundárního serveru na různých podsítích. Takto, pokud je ztraceno připojení k jedné podsíti, klienti DNS stále mohou směřovat dotazy na server názvů na jiné podsíti.

Snížení provozu na propojení rozsáhlé sítě Sekundární server můžete přidat pro zónu na vzdáleném umístění, která má velké množství klientů, a pak nakonfigurovat klienta tak, aby zkusil nejprve tyto servery. To zabrání klientovi v komunikaci dotazů DNS přes pomalá propojení.

Snížení zatížení na primárním serveru zóny Dotazy zóny může zodpovědět sekundární server, čímž se sníží počet dotazů, které musí zodpovídat primární server zóny. Následující části popisují servery, které se chovají pouze jako servery vyrovnávací paměti, servery pro předávání a podřízené servery.

Servery vyrovnávací paměti

Všechny servery DNS provádějí ukládání do mezipaměti – kdykoli získají informaci od ostatních serverů, uloží si tuto informaci pro určitou dobu. To urychluje výkon překladu DNS, snižuje provoz spojený s dotazy DNS a vylepšuje spolehlivost. Více informací najdete v této kapitole v části „Ukládání do mezipaměti a TTL“.

Určité servery DNS známé jako servery vyrovnávací paměti prostě provádějí dotazy, ukládají odpovědi do mezipaměti a vracejí výsledky. Nejsou určující pro jakoukoli doménu DNS a nehostí žádné zóny. Pouze uchovávají data, která uložily do paměti během zpracovávání dotazů.

Výhodou serverů vyrovnávací paměti je to, že neprodukují provoz zónového přenosu, protože neobsahují žádné zóny. Nicméně mají jednu nevýhodu: když je server spuštěn, nemá v mezipaměti uloženy žádné informace a musí je proto získat během doby, kdy zpracovává dotazy.

Servery pro předávání a podřízené servery

Když server DNS obdrží dotaz, snaží se najít požadovanou informaci v rámci svých lokálních zón a z mezipaměti. Jestliže tuto požadovanou informaci nemůže najít a není pro ni určující, musí kvůli vyřešení dotazu komunikovat s ostatními servery. Nicméně v některých případech správci sítě nechtějí, aby servery přímo komunikovaly mezi sebou. Například jestliže je vaše organizace připojena na Internet přes pomalou linku, asi nebudete chtít, aby se každý server DNS ve vaší organizaci přímo připojoval k serverům DNS na Internetu.

Tento problém řeší servery pro předávání, které služba DNS umožňuje. Servery pro předávání jsou servery DNS určené k předávání dotazů mimo sídlo dalším serverům DNS. Například můžete určit jeden server DNS jako server pro předávání pro názvy počítačů na Internetu a pak nakonfigurovat ostatní servery tak, aby používaly tento server pro předávání k překladu názvů, pro které nejsou určující.

Na počítači určeném jako server pro předávání není třeba provádět zvláštní konfiguraci. Server DNS, který potřebuje předávat dotazy, musíte nakonfigurovat na adresu IP serveru pro předávání.

Server může používat server pro předávání v nevýlučném nebo výlučném režimu. V nevýlučném režimu server po obdržení dotazu DNS, pro který není určující a který nemůže vyřešit pomocí vlastních zón nebo mezipaměti, předá dotaz jednomu z určených serverů pro předávání. Server pro předávání pak obstará veškerou potřebnou komunikaci, vyřeší dotaz a výsledek vrátí dotazujícímu se serveru, který vrátí výsledky původnímu tazateli. Pokud server pro předání nemůže vyřešit dotaz, server, který obdržel původní dotaz, se pokusí dotaz vyřešit samostatně.

Ve výlučném režimu se servery úplně spolehnou na schopnost překladu názvu serverů pro předání. Servery, které používají servery pro předání ve výlučném režimu, se označují jako podřízené. Když podřízený server obdrží dotaz DNS, který není schopen sám vyřešit prostřednictvím svých zón, předá tento dotaz na jeden z určených serverů pro předání. Server pro předání pak obstará veškerou nutnou komunikaci, vyřeší do-

taz a výsledek vrátí podřízenému serveru, který ho vrátí původnímu tazateli. Pokud server pro předání nemůže vyřešit dotaz, podřízený server pošle původnímu tazateli chybové hlášení. Pokud server pro předání dotaz nezodpoví, podřízený server se nesnaží dotaz vyřešit samostatně.

Sdílení zatížení

Servery DNS používají ke sdílení a distribuci zatížení síťových prostředků mechanismu cyklického výběru neboli sdílení zatížení, vysvětlený v dokumentu RFC 1794. Cyklický výběr protačí pořadí dat záznamů prostředků vrácených v odpovědi na dotaz, ve kterém pro názvovou doménu DNS existuje více záznamů prostředků stejného typu.

Například předpokládejte, že máte tři servery WWW se stejným doménovým názvem, WWWServer, které všechny zobrazují webovou stránku, a vy chcete zatížení mezi nimi sdílet. Na serveru názvu vytvořte následující záznamy prostředků:

www.reskit.com.	IN	A	172.16.64.11
www.reskit.com.	IN	A	172.17.64.22
www.reskit.com.	IN	A	172.18.64.33

Server názvů nakonfigurovaný k provádění cyklického výběru při odpovídání na dotazy klientů protačí pořadí záznamů prostředků typu A. V tomto příkladě by server názvů odpověděl na první dotaz klienta pořadí adres 172.16.64.11, 172.17.64.22 a 172.18.64.33. Druhému klientovi by na dotaz odpověděl s adresami řazenými jako 172.17.64.22, 172.18.64.33 a 172.16.64.11. Protáčení pokračuje, dokud nejsou data ze všech typů záznamů prostředků přiřazena názvu, který se protočil až na vrchol seznamu při odpovídání dotazů klientů. Klient pak musí vyzkoušet první zařazenou adresu.

Dle výchozího nastavení server Windows 2000 DNS používá odlišnou metodu řazení záznamů vrácených klientovi. Snaží se najít záznam prostředku obsahující adresu IP klientovi nejbližší, pak vrátí jako první tento záznam prostředku. Nicméně výchozí nastavení můžete změnit tak, aby provádělo tradičního cyklický výběr. Více informací najdete v této knize v části „Služba Windows 2000 DNS“. Verze BIND 4.9.3 a pozdější také provádějí tento způsob sdílení zátěže. Dřívější verze BIND provádějí odlišný typ sdílení zatížení. Více informací najdete v dokumentu RFC 1794.

Překlad názvu

Klienti DNS používají knihovny nazývané překladače, které podávají dotazy DNS na servery jménem klienta. Během následující diskuse nezapomínejte, že server DNS také může být klient jiného serveru.

Poznámka: Počítače běžící pod operačním systémem Microsoft® Windows NT® Workstation nebo Microsoft® Windows NT®Server verze 4.0 používají překlad názvů DNS, když dotaz na název obsahuje název, který obsahuje tečku nebo je delší než 15 bajtů. Počítače běžící pod operačním systémem Windows 2000 se vždy pokusí o překlad názvu. Více informací o překladu názvů DNS a NetBIOS najdete v této knize v částech „Řešení problémů protokolu TCP/IP“ a „Služba Windows 2000 DNS“.

Klienti DNS mohou činit dva typy dotazů: rekurzivní a iterativní.

Rekurzivní a iterativní dotazy

Rekurzivním dotazem na název klient DNS požaduje, aby server DNS odpověděl tomtu klientovi buď požadovaným záznamem prostředku nebo chybovým hlášením oznamujícím, že záznam nebo doménový název neexistují. Server DNS nemůže jen odkázat klienta DNS na jiný server DNS.

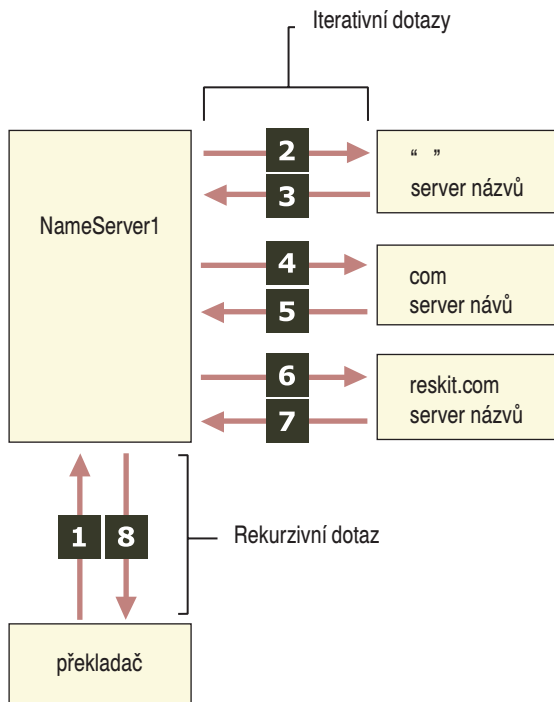
Proto, pokud server DNS nemá požadovanou informaci na dotaz, dotazuje se jiných serverů tak dlouho, dokud informaci nedostane nebo dokud neselže dotaz na název.

Rekurzivní dotazy na název zpravidla činí klient DNS na server DNS nebo server DNS, který je nakonfigurován k postoupení nepřeložených dotazů na název na jiný server DNS, v případě že server DNS je nakonfigurován k použití serveru pro předávání.

Iterativní dotaz na název je dotaz, ve kterém klient DNS umožňuje serveru DNS vrátit nejlepší odpověď, kterou může poskytnout na základě své mezipaměti nebo údajů o zónách. Jestliže dotazovaný server DNS nemá přesný protějšek k dotazovanému názvu, nejlepší možná informace, kterou může vrátit, je odkaz (tj. ukazatel na server DNS určující pro dolní úroveň oboru doménových názvů). Klient DNS se pak může dotázat serveru DNS, na který obdržel odkaz. tento proces pokračuje až do doby nalezení serveru DNS, který je pro dotazovaný název určující nebo dokud nenastane chyba nebo dokud nevyprší časový limit.

Tento proces je někdy označován jako „procházení stromu“ a tento typ dotazu je zpravidla iniciován serverem DNS, který se snaží přeložit pro klienta DNS rekurzivní dotaz na název.

Obrázek 5.4 znázorňuje, příklad iterativních a rekurzivních dotazů. Tento příklad předpokládá, že žádný z dotazovaných serverů nemá požadovanou informaci v mezipaměti.



Obrázek 5.4 Iterativní a rekurzivní dotazy

V příkladu zobrazeném na obrázku 5.4 klient někde na síti Internet potřebuje adresu IP názvu `noam.reskit.com`. Následují tyto události:

1. Klient kontaktuje server názvů 1 s rekurzivním dotazem na název pro `noam.reskit.com`. Server nyní musí vrátit buď odpověď, nebo chybové hlášení.
2. Server názvů 1 zkontroluje svou mezipaměť a zóny, ale odpověď nenajde, takže kontaktuje server určující pro Internet (tj. kořenový server) s iterativním dotazem na `noam.reskit.com`.
3. Kořenový server Internetu odpověď nezná, takže reaguje odkazem na server určující pro doménu `.com`.
4. Server názvů 1 kontaktuje server určující pro doménu `.com` s iterativním dotazem na `noam.reskit.com`.
5. Server určující pro doménu `.com` nezná přesnou odpověď, takže reaguje odkazem na server určující pro doménu `reskit.com`.
6. Server názvů 1 kontaktuje server určující pro doménu `reskit.com` s iterativním dotazem na doménu `noam.reskit.com`.
7. Server určující pro doménu `reskit.com` zná přesnou odpověď. Reaguje požadovanou adresou IP.
8. Server názvů 1 odpoví na dotaz klienta adresou IP pro `noam.reskit.com`.

Ukládání do mezipaměti a TTL

Když server zpracovává rekurzivní dotaz, může být nucen poslat několik dotazů, aby našel definitivní odpověď. Server ukládá do mezipaměti všechny informace, které získá během tohoto procesu na dobu, která je určena ve vrácených údajích. Tato doba se označuje jako *TTL (time to live)* a je specifikována v sekundách. Správce serveru přimární zóny, která obsahuje tyto údaje, rozhodne o délce TTL údajů. Nižší TTL pomáhá zajišťovat, že informace o doméně jsou na síti více konzistentní pro případ, že se často mění. Nicméně také to zvyšuje zatížení serverů názvů, které obsahují tento název a také to zvyšuje provoz na Internetu. Vzhledem k tomu, že data jsou ukládána do mezipaměti, změny provedené v záznamech prostředků nemusí být okamžitě dostupné na celém Internetu.

Jakmile jsou data uložena do mezipaměti, server DNS musí začít snižovat hodnotu TTL z původní hodnoty, takže bude pak vědět, kdy má data ze své mezipaměti odstranit. Když server DNS odpovídá na dotaz pomocí dat uložených v mezipaměti, zahrne do těchto dat i zbývajících TTL. Překladač pak tato data uloží do mezipaměti, přičemž použije TTL zaslané serverem.

Ukládání negativních odpovědí do mezipaměti

Navíc k ukládání vyřešených dotazů do mezipaměti mohou překladače a servery také do mezipaměti ukládat negativní odpovědi, tj. informace o tom, že určitá sada záznamů prostředků (RRset) nebo název domény DNS neexistují. Ukládání negativních odpovědí do mezipaměti může snížit čas potřebný pro negativní odpověď, může také snížit provoz na síti snížením počtu zpráv, které musí projít mezi překladači a servery názvů nebo mezi servery názvů.

Ukládání negativních odpovědí do mezipaměti je specifikováno v dokumentech RFC 1034 a RFC 2308. Dokument RFC 1034 popisuje, jak ukládat negativní odpovědi do mezipaměti, a určuje, že toto ukládání je nepovinné. Dokument RFC 2308 vyžaduje, aby

překladače ukládaly negativní odpovědi do mezipaměti, jakmile ukládají do mezipaměti cokoli dalšího. Také popisuje způsob, jakým servery názvů předávají negativní odpovědi uložené do mezipaměti překladačům. Stejně jako u normálního uložení v mezipaměti, i zde se musí odečítat hodnota TTL.

Více informací o ukládání negativních odpovědí do mezipaměti najdete v této knize v části „Služba Windows 2000 DNS“.

Záznamy prostředků a zóny

K překladu názvů servery konzultují své zóny (také nazývané soubory databáze DNS nebo jednoduše soubory db). Zóny obsahují záznamy prostředků (RR), které vytvářejí informace o prostředcích spojených s doménou DNS. Například některé záznamy prostředků mapují popisné názvy na adresy IP a další mapují adresy IP na popisné názvy.

Určité záznamy prostředků obsahují nejen informace o serverech v doméně DNS, ale také slouží k definování domény prostřednictvím určení, které servery jsou oprávněné pro které zóny. Tyto záznamy prostředků, záznamy prostředků SOA a NS, jsou popsány podrobněji později v této části.

Formát záznamů prostředků

Záznamy prostředků mají následující syntaxi:

```
Owner    TTL      Class   Type      RDATA
```

Tabulka 5.2 popisuje všechna tato pole.

Tabulka 5.2 Typická pole záznamů prostředků

Název	Popis
Vlastník	Název hostitele nebo domény DNS, které náleží tento záznam prostředku.
TTL	32bitové celé číslo, které určuje dobu (v sekundách), po kterou by server DNS nebo překladač měl uchovat v mezipaměti tento záznam před jeho vyhozením. Toto pole je nepovinné a není-li specifikováno, klient použije v záznamu SOA nejmenší TTL.
Třída	Určuje použitou rodinu protokolů. Téměř vždy se u systémů Internetu jedná o třídu IN. Další hodnotou definovanou v dokumentu RFC 1034 je CH pro systém Chaos, který byl experimentálně použit na univerzitě MIT.
Typ	Určuje typ záznamu prostředku.
RDATA	Data záznamu prostředku. To je proměnný typ, který reprezentuje informace popisované typem. například v záznamu A to je 32bitová adresa IP, která reprezentuje hostitele definovaného záznamem prostředku.

Záznamy prostředků jsou v případě vyhledávání a odpovědi reprezentovány ve formě paketů. V souborech databáze jsou reprezentovány záznamy textu o jednom řádku. Většina záznamů prostředků je vyjádřena jednořádkovými textovými záznamy. Jestliže záznam zabere víc než jeden řádek, můžete k zapouzdření informace použít okrouhlé závorky. V mnoha implementacích DNS může být víceřádkový pouze záznam SOA (Start of Authority). Kvůli čitelnosti jsou často do zónových souborů vkládány prázdné řádky a poznámky, které server DNS ignoruje. Poznámky vždy začínají středníkem (;) a končí návratem na začátek řádku.

Typy záznamů prostředků

K poskytování dat založených na DNS o počítačích na síti TCP/IP mohou být použity různé typy záznamů prostředků. Tato část popisuje následující záznamy prostředků:

- SOA
- NS
- A
- PTR
- CNAME
- MX
- SRV

Dále obsahuje další záznamy prostředků specifikované ve standardech RFC. Nakonec zahrnuje také záznamy prostředků specifických pro implementaci Windows 2000 a jeden záznam prostředků specifikovaný organizací ATM Forum.

Záznamy prostředků SOA

Každá zóna na svém začátku obsahuje záznam prostředku SOA (Start of Authority). Záznamy SOA obsahují následující pole:

- Pole Vlastník, TTL, Třída a Typ, jak bylo popsáno dříve v této kapitole v části „Formát záznamů prostředků“.
- Pole určujícího serveru zobrazuje primární určující server DNS zóny.
- Pole odpovědné osoby zobrazuje adresu elektronické pošty správce odpovědného za zónu. Místo symbolu (@) používá tečku (.).
- Pole sériového čísla ukazuje, kolikrát byla zóna aktualizována. Když se sekundární server zóny připojí k nadřazenému serveru takové zóny, aby zjistil, jestli potřebuje iniciovat zónový přenos, sekundární server zóny porovná své sériové číslo se sériovým číslem nadřazeného serveru. Pokud je sériové číslo nadřazeného serveru vyšší, sekundární server iniciuje zónový přenos.
- Pole obnovení ukazuje, jak často sekundární server zóny kontroluje, jestli byly v zóně provedeny změny.
- Pole zopakování ukazuje, jak dlouho se po odeslání požadavku na zónový přenos sekundární server zóny čeká na odpověď od nadřazeného serveru před tím, než svůj pokus zopakuje.
- Pole vypršení časového limitu ukazuje, jak dlouho po předchozím zónovém přenosu sekundární server zóny pokračuje v zodpovídání dotazů na zónu před vyřazením vlastní zóny jako neplatné.
- Pole minimálního TTL se aplikuje na všechny záznamy prostředků v zóně, kdykoli není v záznamu prostředku určena hodnota TTL. Kdykoli se překladač dotazuje serveru, server pošle zpět záznamy prostředků společně s minimální hodnotou TTL. Negativní odpovědi jsou ukládány do mezipaměti s minimální hodnotou TTL záznamu prostředku určující zóny.

Následující příklad ukazuje záznam prostředku SOA:

```
noam.reskit.com. IN SOA (
    noamdc1.noam.reskit.com.      ; authoritative server
                                for the zone
    administrator.noam.reskit.com. ; zone admin e-mail
                                ; (responsible person)
    5099                          ; serial number
    3600                          ; refresh (1 hour)
    600                           ; retry (10 mins)
    86400                         ; expire (1 day)
    60                            ; minimum TTL (1 min)
)
```

Záznamy prostředku NS

Záznam prostředku NS (server názvů) označuje servery určující pro zónu. Označují primární a sekundární servery pro zónu specifikovanou v záznamu SOA a servery pro jakékoli delegované zóny. Každá zóna musí obsahovat minimálně jeden záznam NS na kořeni zóny.

Například když správce domény reskit.com delegoval autoritu pro poddoménu noam.reskit.com na noamdc1.noam.reskit.com, byl k zónám reskit.com a noam.reskit.com přidán následující řádek.

```
noam.reskit.com. IN NS noamdc1.noam.reskit.com.
```

Záznamy prostředků A

Záznamy prostředku adresy (A) mapuje FQDN na adresu IP, takže překladače se mohou dotazovat na adresu IP odpovídající FQDN. například následující záznam prostředků A umístěný v zóně noam.reskit.com mapuje FQDN serveru na jeho adresu IP:

```
noamdc1 IN A 172.16.48.1
```

Záznamy PTR

Záznam prostředku ukazatele (PTR) na rozdíl od záznamu prostředků A mapuje adresu IP na FQDN. například následující záznam prostředku PTR mapuje adresu IP noamdc1.noam.reskit.com na FQDN:

```
1.48.16.172.in-addr.arpa. IN PTR
noamdc1.noam.reskit.com.
```

Záznamy prostředků CNAME

Záznam prostředku kanonický název (CNAME) vytváří alias (synonymní název) pro určité FQDN. Záznamy CNAME můžete používat ke skrytí podrobností implementace vaší sítě před klienty, kteří se k ní připojují. Například předpokládejme, že chcete dát server FTP s názvem na svou poddoménu noam.reskit.com, ale víte, že za šest měsíců jej přesunete na počítač s názvem reskit.com a nechcete, aby vaši uživatelé o této změně věděli. Můžete prostě jen vytvořit alias nazvaný , který ukazuje na a po přesunu na reskit.com musíte pouze změnit záznam CNAME tak, aby ukazoval na .reskit.com. Například následující záznam prostředku CNAME vytváří alias pro .reskit.com.

```
ftp.noam.reskit.com. IN CNAME ftp1.noam.reskit.com.
```

Jakmile se klient DNS dotáže na záznam prostředku A pro , server DNS zjistí záznam prostředku CNAME, přeloží dotaz na záznam prostředku pro a vrátí klientovi jak záznam prostředku A, tak záznam prostředku CNAME.

Poznámka: Na alias může být dle dokumentu RFC 2181 pouze jeden kanonický název.

Záznamy prostředků MX

Záznam prostředku předávání pošty (MX) specifikuje server pro předávání pošty pro název domény DNS. Server pro předávání pošty je hostitel, který bude buď zpracovávat nebo předávat poštu pro název domény DNS. Zpracovávání pošty znamená, že ji buď doručí adresátovi nebo ji postoupí k jinému typu přepravy pošty. Předávání pošty znamená, že ji pošle na server konečného určení, prostřednictvím protokolu SMTP ji pošle na jiný server pro předávání pošty , který je blíž konečnému místu určení nebo ji postaví na určitý čas do fronty.

Poznámka: Záznamy MX používají pouze servery pro předávání pošty.

Chcete-li používat více serverů pro předání pošty v jedné doméně DNS, můžete mít pro tuto doménu více záznamů prostředků MX. Následující příklad ukazuje záznamy prostředků MX pro poštovní servery domény noam.reskit.com.:

*.noam.reskit.com.	IN	MX	0	mailserver1.noam.reskit.com.
*.noam.reskit.com.	IN	MX	10	mailserver2.noam.reskit.com.
*.noam.reskit.com.	IN	MX	10	mailserver3.noam.reskit.com.

První tři pole v tomto záznamu prostředku jsou standardní pole vlastníka, třídy a typu. Čtvrté pole je priorita poštovního serveru nebo hodnota preference. Hodnota preference určuje přednost danou záznamu MX mezi záznamy MX. Jsou upřednostňovány záznamy s nižší prioritou. Proto pokud program pro vedení elektronické pošty potřebuje poslat zprávu elektronické pošty na určitou doménu DNS, prvně kontaktuje server DNS této domény a získá všechny záznamy MX. Poté kontaktuje program pro vedení elektronické pošty s nejnižší hodnotou preference.

Například předpokládejte, že Jana Nováková posílá zprávu elektronické pošty na adresu zrovna ten den, kdy je poštovní server 1 vypnut, ale poštovní server 2 funguje. Janin program pro vedení elektronické pošty se snaží doručit zprávu poštovnímu serveru 1, protože má nejnižší hodnotu preference, ale neuspěje, protože poštovní server 1 je vypnut. V tomto okamžiku si Janin program pro vedení elektronické pošty může vybrat buď poštovní server 2 nebo poštovní server 3, protože jejich hodnoty preference jsou stejné. Úspěšně doručí zprávu na poštovní server 2.

K zabránění smyček pošty, jestliže je program pro vedení elektronické pošty uveden pro cílového hostitele jako MX, může tento program doručovat pouze na MX s nižší hodnotou preference, než má jeho vlastní hostitel.

Poznámka: Program **sendmail** vyžaduje v případě, že v záznamu MX není odkaz na záznam CNAME, zvláštní konfiguraci.

Záznamy SRV

Díky záznamům MX můžete mít v doméně DNS více poštovních serverů. Pokud program pro vedení elektronické pošty potřebuje odeslat zprávu elektronické pošty hostiteli v této doméně, může najít umístění poštovního serveru. Ale co další aplikace, jako jsou například WWW nebo telnet?

Záznam prostředku SRV vám umožňuje určit umístění serverů pro určitou službu, protokol a doménu DNS. Proto pokud máte ve své doméně dva servery WWW, můžete vytvořit záznamy prostředku SRV určující, kteří hostitelé slouží jako servery WWW, a překladače pak mohou získat všechny záznamy prostředků SRV serverů WWW.

Formát záznamu SRV vypadá následovně:

_Služba. _Název.protokolu TTL Třída SRV Priorita Váha Port Cíl

- Pole **_Služba** určuje název služby, například http nebo telnet. Některé služby jsou definovány ve standardech a jiné mohou být definovány lokálně.
- Pole **_Protokol** určuje protokol, například TCP nebo UDP.
- Pole **Název** určuje název domény, ke které se vztahují záznamy prostředku.
- Pole **TTL** a **Třída** jsou stejná jako pole definovaná dříve v této kapitole.
- Pole **Priorita** určuje prioritu hostitele. Klienti se snaží kontaktovat hostitele s nejnižší prioritou.
- Pole **Váha** je mechanismus vyvažující zatížení. Je-li pole priority stejné u dvou nebo více záznamů ve stejné doméně, klienti by měli častěji zkoušet záznamy s vyšší váhou, pokud klienti nepodporují nějaký jiný mechanismus vyvažující zatížení.
- Pole **Port** ukazuje port služby na tomto hostiteli.
- Pole **Cíl** ukazuje úplný doménový název hostitele podporujícího službu.

Následující příklad ukazuje záznamy SRV pro servery WWW:

```
_http._tcp.reskit.com. IN SRV 0 0 80 webserver1.noam.reskit.com.
_http._tcp.reskit.com. IN SRV 10 0 80 webserver2.noam.reskit.com.
```

Poznámka: Tento příklad nespecifikuje hodnotu TTL. Proto překladač použije minimální hodnotu TTL určenou v záznamu prostředku SOA.

Jestliže počítač potřebuje zjistit server WWW v doméně DNS reskit.com, překladač zašle následující dotaz:

```
_http._tcp.www.reskit.com.
```

Server DNS odpoví záznamy SRV, viz výše. Překladač si pak vybere mezi serverem WWW 1 a serverem WWW 2 pomocí porovnání hodnot jejich priority. Vzhledem k tomu, že server WWW 1 má nejnižší hodnotu priority, server DNS vybere server WWW 1.

Poznámka: Jestliže by byla hodnota priority stejná, ale lišily by se hodnoty váhy, klient by si vybral server WWW náhodným výběrem kromě toho, že server s vyšší hodnotou váhy by měl větší pravděpodobnost, že bude vybrán.

Dále překladač žádá o záznam A serveru webserver1.reskit.com a server DNS pošle záznam A. Nakonec se klient snaží kontaktovat server WWW.

Více informací o záznamech SRV najdete na odkazu na IETF na stránkách WWW Web Resources na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>. Operační systém Windows 2000 podporuje koncept Internetu nazvaný „RR služby DNS určující umístění služeb (záznam SRV DNS)“.

Méně časté záznamy prostředků

Tabulka 5.3 obsahuje některé další záznamy prostředků a dokumentů RFC, které je definují. Mnoho z těchto záznamů prostředků je považováno za experimentální.

Tabulka 5.3 Méně časté typy záznamů prostředků

Typ záznamu	RFC	Popis
AAAA	1886	Záznam zvláštní adresy, který mapuje název hostitele (počítače nebo jiného síťového zařízení) na adresu IPv6.
AFSDB	1183	Určuje umístění buď serveru s buňkovou databází AFS nebo ověřený server DCE. Systém AFS používá k mapování doménového názvu DNS na název serveru s buňkovou databází AFS službu DNS. Názvová služba DCE od Open Software Foundation používá službu DNS k podobnému účelu.
HINFO	1035	Záznam prostředků informací o hostiteli určuje typ hardwaru a operačního systému hostitele. Identifikátory typu CPU a operačního systému vycházejí z názvů počítače a názvů systémů zařazených v dokumentu RFC 1700.
	1183	Záznam prostředku ISDN je variací záznamu prostředku A. Spíše než mapování FQDN na adresu IP záznam ISDN mapuje název adresy ISDN. Adresa ISDN je telefonní číslo, která sestává ze směrovacího čísla státu/regionu, směrovacího čísla oblasti nebo státu/regionu, místního telefonního čísla a nepovinně i podadresy. Záznam prostředku ISDN je určen k používání ve spojení s trasou přes záznam prostředku RT.
MB	1035	Záznam prostředku MB (záznam poštovní schránky) je experimentálním záznamem, který určuje hostitele DNS podle určité poštovní schránky. Dalšími příbuznými experimentálními záznamy jsou záznam MG (poštovní skupina), záznam MR (záznam přejmenování poštovní schránky) a záznam MINFO (záznam informací o poštovní schránce nebo seznamu adresátů).
MG	1035	Záznam prostředku MG (záznam poštovní skupiny) je experimentálním záznamem, který určuje poštovní schránku, která je členem poštovní skupiny (seznam adresátů) určeným názvem domény. Dalšími příbuznými experimentálními záznamy jsou záznam MB, záznam MR a záznam MINFO.
MINFO	1035	Záznam prostředku MINFO je experimentálním záznamem, který určuje poštovní schránku, která je odpovědná za určitý seznam adresátů nebo poštovní schránku. Dalšími příbuznými experimentálními záznamy jsou záznam MB a záznam MR.
MR	1035	Záznam prostředku MR je experimentálním záznamem, který určuje poštovní schránku, která je příslušným přejmenování jiné specifikované poštovní schránky. Dalšími příbuznými experimentálními záznamy jsou záznam MG a záznam MINFO.
RP	1183	Určuje osobu odpovědnou (RP) za určitou doménu DNS nebo za určitého hostitele.

Typ záznamu	RFC	Popis
RT	1183	Záznam směrování přes více hostitelů (RT) určuje zprostředkujícího hostitele, který směruje pakety na cílového hostitele. Záznam RT je používán ve spojení se záznamy ISDN a X25. Je syntakticky a sémanticky podobný typu záznamu MX a je používán v podstatě stejným způsobem.
TXT	1035	Záznam prostředku textu spojuje obecné textové informace s položkou v databázi DNS. Typické použití je pro identifikaci umístění hostitele (například Umístění: budova 26S, místnost 2499). Jeden záznam TXT může obsahovat více řetězců, až do 64 kilobajtů (KB).
WKS	1035	Záznam prostředku služby WKS popisuje služby poskytované určitým protokolem na určitém rozhraní. Protokol je zpravidla UDP nebo TCP, ale může jím být kterýkoli záznam v souboru Windows 2000 Protocols umístěném na %SystemRoot%\System32\Drivers\Etc\Protocol. Službami jsou služby pod číslem portu 256 ze souboru Windows 2000 Services umístěném na %SystemRoot%\System32\Drivers\Etc\Services.
X.25	1183	Záznam prostředku X.25 je variací záznamu prostředku A. Spíše než mapování FQDN na adresu IP záznam X.25 mapuje název na adresu X.121. X.121 je standardem ISO, který určuje formát adres používaných v sítích X.25. Záznam prostředku X.25 je určen k použití ve spojení se záznamem prostředku RT.

Záznamy prostředků nedefinované v dokumentech RFC

Navíc k typům záznamů prostředku obsažených v dokumentech RFC používá operační systém Windows 2000 následující typy záznamů prostředků, viz tabulka 5.4.

Tabulka 5.4 Typy záznamů prostředků nedefinované v dokumentech RFC

Název	Popis
WINS	Server Windows 2000 DNS může pro vyhledávání hostitelské části názvu DNS, který neexistuje v zóně DNS určující pro tento název, používat server WINS.
Zpětné vyhledávání WINS (WINS-R)	Tento záznam se používá v zóně zpětného vyhledávání pro hledání hostitelské části názvu DNS, pokud je dána jeho adresa IP. Server DNS vykoná dotaz přes adaptér NetBIOS, jestliže zóna určující pro adresu IP neobsahuje patřičný záznam a obsahuje záznamy prostředku WINS-R.
ATMA	Záznam prostředku ATMA, definovaný organizací ATM Forum, se používá k mapování názvů domén DNS na adresy ATM. Pro více informací kontaktujte ATM Forum a ptejte se na ATM Name System Specification, verze 1.0.

Delegace a společné záznamy

Delegace a společné záznamy jsou záznamy, které přidáváte k zóně za účelem delegace poddomény do oddělené zóny. Delegace je záznam NS v rodičovské zóně, který ob-

sahuje seznam serverů určujících pro delegovanou zónu. Společný záznam je záznam A pro server názvů určující pro delegovanou zónu.

Například předpokládejte, že server názvů pro doménu DNS reskit.com delegoval oprávnění pro zónu noam.reskit.com na server názvů noamNS.noam.reskit.com. Do zóny reskit.com přidáte následující záznamy:

noam.reskit.com.	IN	NS	noamNS.noam.reskit.com
noamNS.noam.reskit.com.	IN	A	172.16.54.1

Delegace jsou nezbytné pro překlad názvů. Společné záznamy jsou také nezbytné, pokud je server názvů delegované zóny také člen této domény. Společný záznam je nezbytný v příkladu uvedeném výše, protože noamNS.noam.reskit.com je člen delegované domény noam.reskit.com. Nicméně pokud by byl členem jiné domény, překladač může provádět standardní překlad názvů k přeložení názvu oprávněného serveru na adresu IP.

Když překladač pošle dotaz na název v dceřinné zóně serveru názvů, který je určující pro rodičovskou zónu, server určující pro rodičovskou zónu zkontroluje svou zónu. Podle delegace se dozví, který server názvů je určující pro dceřinnou zónu. Server určující pro rodičovskou zónu může vrátit odkaz překladači.

Zóny

Stantardy služby DNS neurčují strukturu interních dat, která uchovávají záznamy prostředků, a různé implementace se tak mění. Obecně řečeno, servery používají zóny na nich uložené v prostém textu, ale to není nutná podmínka. U operačního systému Windows 2000 můžete integrovat svou databázi DNS do databáze služby Active Directory. V takovém případě jsou zóny uloženy v databázi Active Directory.

Jedna běžná implementace služby DNS, implementace BIND (Berkeley Internet Name Domain), zpravidla používá soubory uvedené v tabulce 5.5.

Tabulka 5.5 Názvy zón používané v implementaci BIND

Název	Popis
db.doména	Zóna dopředného vyhledávání. Například jestliže vaše doména DNS je reskit.com, pak se tento soubor nazývá db.reskit.com.
db.addr	Zóna zpětného vyhledávání. Například jestliže je vaše adresa sítě třídy C 172.16.32, pak se tento soubor nazývá db.172.16.32.
db. cache	Známý také jako soubor odkazů na kořenové servery. Tento soubor obsahuje názvy a adresy IP serverů názvů, které obsluhují kořenovou doménu DNS. Tento soubor je v podstatě stejný na všech serverech, které používají kořenové servery DNS Internetu. (Kořenový server DNS je server DNS, který je určující pro kořen oboru názvů.)
db.127.0.0.1	Používá se k vyřešení dotazů na adresu zpětné smyčky. Je v podstatě stejný na všech serverech názvů.

Názvy souborů databáze mohou být libovolné a jsou určeny v konfiguraci serveru DNS. Dle výchozího nastavení server Microsoft Windows 2000 DNS nepoužívá stejné názvy souborů jako typický server DNS BIND, ale namísto toho používá _zóna_název.dns. Nicméně přenášíte-li soubory databáze DNS z jiného serveru DNS, můžete nakonfigurovat server Microsoft Windows 2000 DNS tak, aby použil názvy souboru BIND.

Následující část vysvětluje obsah zón a popisuje jeden dodatečný soubor, soubor BOOT, který používají servery BIND, ale který není specifikován ve standardech služby DNS.

Zóna dopředného vyhledávání

Zóny dopředného vyhledávání obsahují informace potřebné k překladu názvů v rámci domény DNS. Musí obsahovat záznamy SOA a NS a mohou zahrnovat jakýkoli typ záznamu prostředku kromě záznamu prostředku PTR.

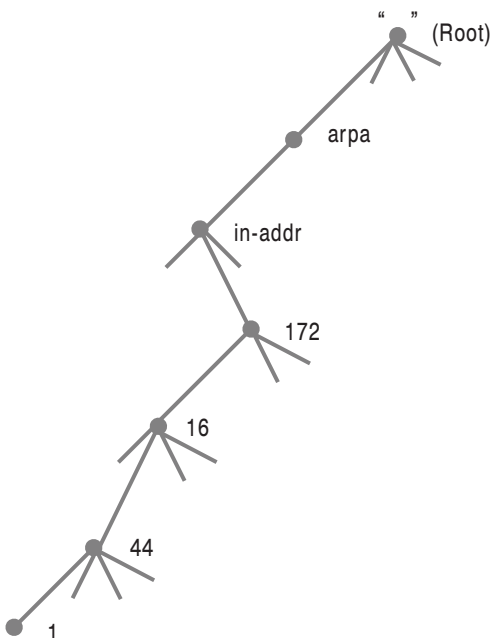
Zóna zpětného vyhledávání

Zóny zpětného vyhledávání obsahují informace potřebné ke zpětnému vyhledávání. Zpravidla obsahují záznamy SOA, NS, PTR a CNAME.

U většiny dotazů klient dodá název a požaduje adresu IP, která tomuto názvu odpovídá. Tento typ dotazu se zpravidla označuje jako dopředné vyhledávání.

Ale co když klient již má adresu IP počítače a chce určit název DNS tohoto počítače? Toto je důležité pro programy, které implementují zabezpečení založené na připojení FQDN připojujícího se, a používá se to také při řešení problémů protokolu TCP/IP. Standard DNS poskytuje tuto možnost prostřednictvím zpětného vyhledávání.

Pokud by jediným způsobem, jak zodpovědět zpětné vyhledávání, bylo provést kompletní prohledání všech domén DNS v oboru názvů DNS, byl by zpětný dotaz k jakémukoli praktickému provedení příliš vyčerpávající.



Obrázek 5.5 Obor názvů in-addr.arpa

K vyřešení tohoto problému byla vytvořena zvláštní doména DNS zvaná in-addr.arpa. Tato doména používá zpětné řazení čísel adres IP v desítkovém formátu s oddělová-

ním tečkou. Díky tomuto uspořádání mohou být nižší odnože správy domény in-addr.arpa delegovány na organizace, jak jsou jim přiřazovány jejich ID sítě IP třídy A, B nebo C. Více informací o vytváření beztřídových zón zpětného vyhledávání najdete v této kapitole v části „Služba Windows 2000 DNS“ a dále v dokumentu RFC 2317 „Beztrídní delegace IN-ADDR.ARPA.“.

Obrázek 5.5 znázorňuje větev oboru názvů in-addr.arpa.

Doménový strom in-addr.arpa požaduje, aby se k ukládání a poskytování zpětných mapování adres IP na odpovídající FQDN používaly záznamy prostředku PTR.

Jestliže klient potřebuje najít FQDN spojené s adresou IP 172.16.44.1, klient se dotazuje na záznam PTR doménového názvu 1.44.16.172.in.addr.arpa.

Inverzní dotaz

Kromě zpětného vyhledávání některé servery DNS podporují to, co je známo jako inverzní dotaz. Stejně jako u zpětného vyhledávání, klient provádějící inverzní dotaz poskytuje adresu IP a požaduje FQDN. Nicméně server nepoužije ke zodpovězení dotazu doménu in-addr.arpa a nedotazuje se dalších serverů. Namísto toho jednoduše hledá odpověď ve vlastních zónách a, pokud nemůže odpověď najít, vrátí chybové hlášení. Neexistuje způsob, jak by se klient nebo server dozvěděli, jestli adresa IP prostě chybí v zónách serveru nebo jestli neexistuje.

Vzhledem k tomu, že podpora inverzních dotazů je nepovinná a servery často nemohou poskytnout definitivní odpověď, inverzní dotazy se příliš nepoužívají. Inverzní dotazy používají pouze některé aplikace, například dřívější verze nástroje **nslookup**.

Server Windows 2000 odpovídá na požadavky o inverzní dotazy opakováním adresy IP specifikované v dotazu uzavřené v hranatých závorkách. Například, jestliže obdrží inverzní dotaz na 172.16.72.1, odpovídá [172.16.72.1].

Více informací o inverzních dotazech najdete v dokumentu RFC 1035.

Soubor odkazů na kořenové servery

Soubor odkazů na kořenové servery také nazývaný soubor odkazů mezipaměti, obsahuje informace o hostitelích, které jsou potřebné pro překlad názvů mimo autoritativní domény DNS. Obsahuje názvy a adresy kořenových serverů DNS.

Jestliže je vaše síť připojena k Internetu, soubor odkazů na kořenové servery by měl obsahovat záznamy pro kořenové servery DNS na Internetu. V operačním systému Windows 2000 je instalován soubor odkazů na kořenové servery s aktuálním mapováním kořenových serverů DNS Internetu jako soubor Cache.dns v adresáři %SystemRoot%\System32\Dns.

Pokud vaše síť není připojena k Internetu, musíte nahradit záznamy NS a A v souboru mezipaměti záznamy NS a A pro servery DNS, které jsou určující pro kořen vaší privátní sítě TC/IP.

Například předpokládejte, že jste vytvořili dva interní kořenové servery DNS (InternalRoot1.reskit.com. a InternalRoot2.reskit.com.). Pak na dalších serverech DNS ve vaší síti vytvoříte soubor odkazů na kořenové servery ukazující na interní kořenové servery DNS. Tímto způsobem, jestliže další servery názvů obdrží dotaz, který nemohou vyřešit, mohou se jednoduše dotázat interních kořenových serverů určených v souboru.

Následující soubor odkazů na kořenové servery domény reskit poskytuje záznamy prostředku NS a mapování názvů na adresy IP pro servery názvů v doméně reskit.com.

```
; Internal root hints file for reskit.com, which is not connected to
; the Internet
.      86400      IN      NS      InternalRoot1.reskit.com.
.      86400      IN      NS      InternalRoot2.reskit.com.

InternalRoot1.reskit.com.      86400      IN      NS      172.16.64.1
InternalRoot2.reskit.com.      86400      IN      NS      172.16.64.2
```

Poznámka: Průvodce konfigurací serveru DNS pro Windows 2000 se snaží určit, jestli síť je připojena k Internetu a pokud není, vytváří vlastní soubor mezipaměti.

Spouštěcí soubor (soubor Boot)

Přestože není spouštěcí soubor v současné době definován v dokumentu RFC a server nemusí být s dokumenty RFC kompatibilní, je zde pro úplnost popsán. Tento soubor je součástí implementace BIND služby DNS.

Dle výchozího nastavení se v implementaci Microsoft DNS nepoužívá. Je-li to prospěšné, můžete přenést existující spouštěcí soubor BIND na server Microsoft DNS. Server Windows 2000 DNS podporuje pouze podmnožinu příkazů spouštěcího souboru BIND a to pouze pro typ souborů používaný servery BIND 4.x.x.

Spouštěcí soubor BIND řídí chování serveru DNS při spouštění. Příkazy musí začínat na začátku řádku, žádné mezery je nemohou předcházet. Tabulka 5.3 obsahuje popis některých příkazů spouštěcího souboru podporovaných operačním systémem Windows 2000.

Tabulka 5.6 Popis příkazů spouštěcího souboru

Příkaz	Popis
Příkaz Directory	Určuje adresář, kde lze nalézt další soubory, na které se odkazuje ve spouštěcím souboru.
Příkaz Cache	Určuje soubor, který napomáhá serveru DNS při kontaktování serverů názvů kořenové domény. Tento příkaz a soubor, na který odkazuje, musí existovat vždy.
Příkaz Primary	Určuje primární zónu, pro kterou je server určující a soubor zóny, který obsahuje záznamy prostředků pro tuto zónu. Ve spouštěcím souboru může být více záznamů příkazů Primary.
Příkaz Secondary	Určuje sekundární zónu, pro kterou je server určující a seznam adres IP nadřazených serverů, od kterých se pokouší o zónový přenos. Také definuje název lokálního souboru pro ukládání této zóny. Ve spouštěcím souboru může být více záznamů příkazů Secondary.

Tabulka 5.7 obsahuje syntaxi některých příkazů spouštěcího souboru podporovaných operačním systémem Windows 2000.

Tabulka 5.7 Syntaxe některých příkazů spouštěcího souboru podporovaných operačním systémem Windows 2000

Syntaxe	Příklad		
directory <adresář>	directory	c:\winnts\system32\dns	
cache <název souboru>	cache	cache	
primary <doména> <název souboru>	primary	reskit.com	reskit.com.dns
	primary	dev.reskit.com	dev.reskit.com.dns
secondary <doména><seznam hostitelů> <lokální název souboru>	secondary	test.reskit.com	157.55.200.100
	test.reskit.com.dns		
forwarders <seznam hostitelů>	forwarders	172.16.64.4	172.16.64.8
slave (následuje po parametru forwarders)	forwarders	172.16.64.4	172.16.64.8 slave

Více informací o spouštěcím souboru BIND najdete na odkazu na stránky WWW Microsoft TechNet na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>. Na těchto stránkách hledejte klíčová slova „struktura“, „systém doménových názvů“ a „spouštěcí soubor“ (resp. „structure“, a „domain name system“ a „boot file“).

Zónový přenos

Pro provedení změn zóny na nadřazeném serveru musí být tyto změny replikovány na všechny sekundární servery této zóny za použití mechanismu nazvaného zónový přenos. V původních specifikacích služby DNS byl dostupný pouze jeden typ zónového přenosu, a to tzv. úplný zónový přenos. Nové dokumenty RFC pojednávají o dalším typu zónového přenosu: přírůstkový zónový přenos. Tato část knihy popisuje oba typy zónového přenosu. Také popisuje mechanismus upozornění DNS (DNS Notify), mechanismus, jehož prostřednictvím nadřazený server zóny může vyrozumět sekundární servery zóny o změnách této zóny.

Úplný zónový přenos

Při úplném zónovém přenosu definovaném v původních specifikacích dokumentů RFC nadřazený server zóny přenesou celou databázi zóny na sekundární server této zóny. Sekundární servery iniciují úplné zónové přenosy pomocí následujícího procesu:

1. Sekundární server zóny čeká po určitou dobu (určenou v poli Obnovit záznamu prostředku SOA) a pak vyzve nadřazený server k poskytnutí jeho záznamu SOA.
2. nadřazený server zóny odpoví záznamem prostředku SOA.
3. Sekundární server zóny porovná získané sériové číslo s vlastním sériovým číslem. Jestliže je sériové číslo odeslané nadřazeným serverem zóny vyšší než vlastní sériové číslo sekundárního serveru, znamená to, že databáze zóny je zastaralá, a sekundární server proto pošle požadavek AXFR Request (požadavek na úplný zónový přenos).
4. nadřazený server zóny pošle sekundárnímu serveru úplnou databázi zóny.

Jestliže nadřazený server zóny nereaguje na výzvu sekundárního serveru, sekundární server opakuje tyto výzvy v intervalu stanoveném v poli Opakovat v záznamu prostřed-

ku SOA. Jestliže od posledního úspěšného zónového přenosu uplyne bez reakce primárního serveru doba delší, než je interval stanovený s poli Vypršení, zónu vyřadí.

Poznámka: Servery názvů s verzemi BIND dřívějšími než 4.9.4 mohou v průběhu úplného zónového přenosu posílat a přijímat pouze jeden záznam prostředku na zprávu. Servery názvů s verzemi BIND 4.9.4 a pozdějšími a servery s Windows 2000 mohou posílat a přijímat více záznamů prostředku ve zprávě. To zlepšuje výkon úplných zónových přenosů.

Nicméně k zajištění zpětné kompatibility servery názvů s Windows 2000 jsou dle výchozího nastavení nastaveny tak, že odesílají pouze jeden záznam prostředků za zprávu, pokud kterýkoli ze sekundárních serverů nakonfigurovaných pro danou zónu neprovozuje operační systém Windows. Máte-li sekundární servery názvů s BIND verze 4.9.4 a pozdější, zlepšuje nakonfigurování operačního systému Windows 2000 na odesílání více záznamů prostředků ve zprávě jejich výkon. Více informací najdete na odkazu na stránky Microsoft TechNet Web na stránkách WWW na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>. Na těchto stránkách hledejte klíčová slova „kompatibilita DNS“ (respektive „DNS Compatibility“), „BIND“ a „4.9.4“.

Přírůstkový zónový přenos

Úplný zónový přenos může spotřebovat velkou část šířky pásma sítě, zvláště pro složité konfigurace DNS. Pro řešení tohoto problému specifikuje dokument RFC 1995 další standard, přírůstkový zónový přenos. U přírůstkového zónového přenosu se musí přenášet pouze upravená část zóny.

Přírůstkový zónový přenos funguje z větší části stejně jako úplný zónový přenos. Sekundární server zóny také používá záznam prostředku SOA k určení, kdy vyzvat nadřazený server k přenosu zóny, kdy opakovat výzvu atd. Nicméně pokud potřebuje provést zónový přenos, pošle namísto požadavku o úplný zónový přenos požadavek IXFR Query, žádající nadřazený server o přírůstkový zónový přenos.

Nadřazený server zóny mezitím udržuje historii posledních verzí zóny, která sleduje jakékoli změny záznamů, které se objevily v posledních verzích aktualizace zóny. Potom, jestliže má nadřazený server zóny novější verzi zóny, může předat pouze tyto změny záznamů, které se objevily mezi dvěma různými verzemi zóny (aktuální verze na nadřazeném a sekundárním serveru), na sekundární server zóny. Nadřazený server odešle jako první starší aktualizace a nejnovější aktualizace jako poslední.

Když sekundární server obdrží přírůstkový zónový přenos, vytvoří novou verzi zóny a začne nahrazovat záznamy prostředků aktualizovanými záznamy, a to počínaje nejstaršími aktualizacemi a konče nejnovějšími. Po provedení všech aktualizací sekundární server nahradí starou verzi zóny její novou verzí.

Nadřazený server zóny nemusí provádět přírůstkový zónový přenos. V případě, že nepodporuje přírůstkový zónový přenos nebo nemá všechny nezbytné údaje k provedení přírůstkového zónového přenosu, anebo přírůstkový zónový přenos zabere víc šířky pásma než úplný zónový přenos, může provádět úplný zónový přenos.

Ačkoli přírůstkový zónový přenos šetří šířku pásma sítě, používá prostor na serveru k zaznamenávání historie verzí. Aby ušetřily prostor, mohou servery historii verzí vyčistit.

Upozornění DNS (DNS Notify)

Upozornění DNS je revize standardu DNS (viz dokument RFC 1996), který navrhuje, že nadřazený server zóny oznamuje určitým sekundárním serverům příslušné zóny změny a sekundární servery mohou zkontrolovat, jestli potřebují iniciovat zónový přenos. Tento proces může pomoci vylepšit soudržnost dat zóny mezi sekundárními servery.

K určení, kterým sekundární serverům zóny posílat změny, nadřazený server zóny obsahuje seznamy upozornění, které obsahují seznam adres IP na tyto sekundární servery. Nadřazený server zóny při změně zóny upozorní pouze servery z tohoto seznamu. Když se aktualizuje lokální zóna na nadřazeném serveru, dochází k následujícím událostem:

1. Aktualizuje se pole Sériové číslo v záznamy SOA, aby signalizovalo, že na disk byla zapsána nová verze zóny.
2. Nadřazený server pak pošle zprávu upozornění na další servery, které jsou součástí seznamu upozornění.
3. Všechny sekundární servery zóny, které obdrží zprávu upozornění, reagují inicializací dotazu na SOA zpět na oznamující nadřazený server, aby určily, jestli je zóna upozorňujícího serveru pozdější verze než jejich aktuálně uložená kopie zóny.
4. Jestliže upozorněný server zjistí, že sériové číslo použité v záznamu SOA zóny upozorňujícího serveru je vyšší (aktuálnější) než sériové číslo použité v záznamu SOA jeho aktuální kopie zóny, požádá o úplný nebo přírůstkový zónový přenos.

Poznámka: Na serverech s operačním systémem Windows 2000 můžete nakonfigurovat nastavení upozornění.

Dynamická aktualizace

Dynamická aktualizace je nový standard specifikovaný v dokumentu RFC 2136, který poskytuje prostředky pro dynamickou aktualizaci údajů zóny na primárním serveru zóny.

Původně byla služba DNS navržena tak, aby podporovala pouze statické změny v databázi zóny. Vzhledem k omezením v návrhu statické služby DNS měl schopnost předávat, odebírat nebo upravovat záznamy prostředků pouze správce systému DNS, a to jen manuálně.

Například správce systému DNS by editoval záznamy na primárním serveru zóny a opravená databáze zóny je pak předávána sekundárním serverům během zónového přenosu. Tento návrh je funkční, jestliže počet změn je malý a aktualizace se neprovádí často, ale jinak se může stát nezvládnutelným.

Na druhou stranu u dynamické aktualizace lze primární server zóny nakonfigurovat také tak, aby podporoval aktualizace, které jsou inicializovány jiným počítačem nebo zařízením, které také podporují dynamickou aktualizaci. Například může obdržet aktualizace z pracovních stanic registrujících záznamy prostředků A a PTR nebo ze serverů DHCP. Aktualizace jsou posílány pomocí standardního formátu zprávy UPDATE a mohou obsahovat přidání nebo odstranění jednotlivých záznamů prostředků (RR) nebo množinu záznamů prostředků (RRset). Více informací o formátu zprávy UPDATE najdete v dokumentu RFC 2136.

Aby mohl proběhnout požadavek o dynamickou aktualizaci, musí být určeno několik výchozích předpokladů. Jsou-li tyto předpoklady nastaveny, před povolením aktualizace musí být všechny požadavky splněny. Zde je několik příkladů takových předpokladů:

- Požadované jednotlivé záznamy prostředku nebo množiny záznamů prostředků již existují nebo se již před aktualizací používají.
- Požadované jednotlivé záznamy prostředku nebo množiny záznamů prostředků neexistují nebo se před aktualizací nepoužívají.
- Požadujícímu serveru je umožněno iniciovat aktualizaci určitého jednotlivého záznamu prostředku nebo množiny záznamů prostředků.

Každá výchozí předpoklad musí být před aktualizací splněna. Po splnění všech výchozích předpokladů může primární server zóny přikročit k aktualizaci vlastních lokálních zón. Více aktualizací lze provádět současně pouze v případě, že jedna aktualizace nezávisí na konečném výsledku další aktualizace.

Standardy služby DNS

Přestože standardy jádra služby DNS (jak byly ustaveny v dokumentech RFC 1034 a 1035) byly před svým přijetím za standardy v roce 1987 dobře propracovány a přijímány, v následujících letech bylo provedeno větší množství revizí. Tyto revize jsou provedeny v dalších dokumentech RFC a návrhy Internetu, které jsou nezávisle autorizovány a postoupeny k dalšímu pojednání IETF před přijetím za standardy v rámci sítě Internet.

Tabulka 5.8 obsahuje seznam přijatých a navržených standardů RFC, které podporuje operační systém Windows 2000.

Tabulka 5.8 Standardy RFC týkající se služby DNS podporované operačním systémem Windows 2000

Číslo	Stav	Název
1034	Standard	Doménové názvy – koncepty a příslušenství
1035	Standard	Doménové názvy – implementace a specifikace
1123	Standard	Požadavky na hostitele sítě Internet – aplikace a podpora
1886	Návrh	Rozšíření služby DNS na podporu protokolu IP verze 6
1995	Návrh	Přírůstkový zónový přenos ve službě DNS
1996	Návrh	Mechanismus okamžitého upozornění na změny zóny
2136	Návrh	Dynamická aktualizace systému doménových názvů (DNS UPDATE)
2181	Navrh. standard	Vyjasnění specifikace DNS
2308	Navrh. standard	Ukládání negativních výsledků dotazů DNS do mezipaměti (DNS NCACHE)

Další informace

- Další informace o koncepčních informacích o službě DNS najdete v knize *DNS and BIND, 3rd Edition* by Paul Albitz and Cricket Liu, 1998, O'Reilly & Associates, Inc..
- Další informace o dokumentech RFC a návrzích Internetu najdete na odkazu na stránku Web Resources na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

6. KAPITOLA

Služba Windows 2000 DNS



Služba Microsoft® Windows® 2000 DNS je kompatibilní se standardní službou DNS (Domain Name System), jak je popsána v dokumentech RFC organizace IETF (Internet Engineering Task Force). Služba DNS je ve skutečnosti systém pro zpracování názvů pro síť na bázi protokolu IP a názvovou službou používanou k lokalizaci počítačů na internetu. Vzhledem k tomu, že služba Windows 2000 DNS je kompatibilní s dokumenty RFC, spolupracuje s většinou implementací jiných serverů DNS, například servery DNS, které používají software BIND (Berkeley Internet Name Domain). Tato kapitola popisuje nové vlastnosti a vylepšení služby Windows 2000 DNS a vysvětluje, jak nastavit některé z těchto vlastností. Více informací o standardech RFC spojených se službou DNS, které jsou podporovány operačním systémem Windows 2000 najdete v kapitole „Úvod do DNS“.

V této kapitole najdete

Úvod do implementace služby DNS v operačním systému Windows 2000	268
Vytváření názvů hostitelů a domén	270
Překladač pro operační systém Windows 2000	275
Nastavení služby DNS pro službu Active Directory	290
Integrace adresářové služby Active Directory a replikace Multimaster	299
Dynamická aktualizace a zabezpečená dynamická aktualizace	309
Zabezpečená dynamická aktualizace	322
Stárnutí a úklid paměti záznamů zastaralých názvů	328
Integrace se službou WINS	332
Spolupráce s dalšími servery DNS	337
Úvahy o přístupu na síť internet	344
Řešení problémů	357

Další informace, které najdete v sadě Resource Kit

- Více informací o protokolu TCP/IP najdete v části „Úvod do TCP/IP“.
- Více informací o službě WINS najdete v části „Služba Windows Internet Name Service“.
- Více informací o konceptech služby DNS najdete v části „Úvod do služby DNS“.
- Více informací o adresářové službě Active Directory najdete v knize *Microsoft® Windows® 2000 Server Distribuované systémy* v části „Logická struktura adresářové služby Active Directory“.

Úvod do implementace služby DNS v operačním systému Windows 2000

Server a překladač DNS pro Windows 2000 mají několik nových vlastností a vylepšení oproti verzi Microsoft® Windows NT® verze 4.0. Tato kapitola popisuje následující vlastnosti:

Podpora služby Active Directory jako vyhledávací služby pro řadiče domén

Služba DNS je vyžadována pro podporu služby Active Directory. K podpoře instalace služby Active Directory můžete také použít jiné implementace serveru DNS.

Integrace se službou Active Directory

Zóny DNS můžete zintegrovat do služby Active Directory, což vám poskytne zvýšenou odolnost proti chybám a zabezpečení. Každá zóna integrovaná do služby Active Directory je replikována mezi všechny řadiče domén v rámci domény služby Active Directory. Všechny servery DNS běžící na těchto řadičích domén mohou jednat jako primární servery takové zóny připouštějící dynamickou aktualizaci. Služba Active Directory replikuje na základě jednotlivých vlastností, a postupuje dále pouze relevantní změny.

Podpora dynamické aktualizace

Služba DNS umožňuje klientským počítačům dynamickou aktualizaci jejich záznamů prostředků ve službě DNS. To zlepšuje správu DNS díky snížení času potřebného k ruční správě záznamů zóny. Vlastnost dynamické aktualizace může být použita ve spojení s protokolem DHCP k dynamické aktualizaci záznamů prostředků při obnově a uvolnění adresy IP počítače. Počítače s operačním systémem Windows 2000 mohou posílat dynamické aktualizace.

Podpora stárnutí a čištění paměti záznamů zastaralých názvů

Služba DNS je schopná sledovat stárnutí názvů a provádět čištění paměti záznamů zastaralých názvů. Když je povolena, tato vlastnost může zabránit zůstávání prošlých záznamů ve službě DNS.

Podpora zabezpečené dynamické aktualizace v zónách integrovaných do služby Active Directory

Zóny integrované do služby Active Directory můžete nastavit k zabezpečené dynamické aktualizaci. Díky zabezpečené dynamické aktualizaci mohou měnit záznamy nebo zóny pouze oprávnění uživatelé.

Zlepšení správy

Konzola DNS nabízí vylepšené grafické uživatelské rozhraní (GUI) pro správu služby DNS. Operační systém Windows 2000 Server také poskytuje několik nových průvodců nastavením a dalších nástrojů usnadňujících správu a podporu serverů DNS a klientů na síti.

Správa z příkazové řádky

K provádění většiny úloh, které lze provádět z konzoly DNS, můžete z příkazového řádku použít nástroj Dnscmd.exe. Například tak můžete vytvářet, odstraňovat a prohlížet zóny a záznamy, vymazat vlastnosti serveru a zón, provádět rutinní operace správy, například aktualizaci zón, opětovné nahrání zón, obnovu zón, zpětné zapsání zón do souboru nebo služby Active Directory, pozastavení a pokračování zóny, vyčištění mezipaměti, zastavení a spuštění služby DNS a prohlížení statistik.

Nástroj Dnscmd.exe můžete také použít k psaní skriptů a pro vzdálenou správu. Více informací o tomto nástroji najdete v nápovědě Windows 2000 Support Tools. Více informací o instalaci a používání nápovědy Windows 2000 Support Tools a Support Tools najdete v souboru Sreadme.doc v adresáři \Support\Tools na CD s operačním systémem Windows 2000.

Vylepšení překladu názvů

Překladač pro Windows 2000 se zpravidla snaží o překlad názvů pomocí služby DNS a teprve poté použije rozhraní NetBIOS. Také se může dotazovat různých serverů v závislosti na adaptérech, kterým jsou přiřazeny.

Vylepšené ukládání do mezipaměti a ukládání negativních odpovědí do mezipaměti

Nyní můžete prohlížet a vyprázdnit mezipaměť překladače z příkazové řádky pomocí nástroje Ipconfig a můžete vyprázdnit mezipaměť serveru z konzoly DNS. Překladač také provádí ukládání negativních odpovědí do mezipaměti, což je ukládání informací o tom, že název nebo typ záznamu neexistuje. Ukládání negativních odpovědí do mezipaměti snižuje čas vyhledávání v případě, že se uživatel dotazuje na název, o kterém už překladač dříve zjistil, že neexistuje. Více informací o ukládání do mezipaměti najdete později v části „Překladač pro operační systém Windows 2000“.

Další vylepšení klientů

Do mezipaměti mohou být přednahrány záznamy ze souboru Hosts. Také lze dynamicky reorganizovat seznam serverů překladače, aby byly upřednostněny reagující servery DNS.

Podpora prostředí pouze s DNS

Jestliže všechny počítače na síti běží pod operačním systémem Windows 2000, nepotřebujete žádné servery WINS. Dokonce i ve smíšeném prostředí nepotřebujete na klientech s operačním systémem Windows 2000 konfigurovat klienta WINS, pokud máte nastaveno vyhledávání pomocí serveru WINS. Prostřednictvím vyhledávání pomocí serveru WINS můžete směřovat službu DNS tak, aby se na překlad názvů dotazovala na server WINS, takže klienti DNS mohou vyhledávat názvy a adresy IP klientů WINS.

Spolupráce s dalšími implementacemi serverů DNS

Vzhledem k tomu, že server DNS pro operační systém Windows 2000 je kompatibilní s dokumenty RFC, spolupracuje s dalšími implementacemi serverů DNS, například BIND.

Integrace s dalšími síťovými službami

Server DNS pro operační systém Windows 2000 je integrován se službou DHCP a WINS.

Přírůstkový zónový přenos

Navíc k provádění úplných zónových přenosů (posílání kopie celé zóny) může nyní server DNS posílat a přijímat přírůstkové zónové přenosy, ve kterých jsou přenášeny pouze změny zóny. To může snížit dobu a šířku pásma potřebnou pro zónový přenos.

Podpora nových typů záznamů prostředku

Operační systém Windows 2000 zahrnuje podporu pro dva nové typy záznamů prostředku: záznam prostředku SRV, který je používán počítači k lokalizaci řadičů domén, a záznam prostředku ATMA.

Vytváření názvů hostitelů a domén

V operačním systému Windows NT 4.0 a dřívějším je počítač identifikován primárně podle názvu typu NetBIOS – tedy podle názvu, pod kterým je počítač znám na síti. Ve Windows 2000 je počítač identifikován primárně podle úplného názvu počítače, což je úplný doménový název (FQDN). Stejný počítač může být určen více než jedním názvem FQDN. Nicméně pouze název FQDN, který je spojením názvu hostitele a primární přípony DNS, je úplným názvem počítače. V této kapitole je první název úplného názvu počítače označován jako název hostitele a zbývající názvy tvoří primární příponu DNS.

Dle výchozího nastavení je primární přípona DNS počítače, který pracuje s operačním systémem Windows 2000, nastavena na název DNS domény Active Directory, ke které počítač patří. Primární přípona DNS může být také určena zásadami skupiny, viz dále v této části.

Poznámka: Názvy FQDN můžete nastavit a prohlížet ze záložky **Identifikace sítě** dialogu **Vlastnosti systému**, které otevřete klepnutím pravým tlačítkem myši na ikonu **Tento počítač** a pak klepnutím na **Vlastnosti**.

Předpokládejte, že máte klienta WINS s názvem client1. Název „client1“ bude název počítače typu NetBIOS. Dále předpokládejte, že na své síti nahrazujete server WINS serverem DNS a z client1 děláte klienta DNS v doméně eu.reskit.com. Název client1 je také názvem počítače jako hostitele a je dle výchozího nastavení spojen s primární příponou DNS eu.reskit.com, aby vytvořil název FQDN client1.eu.reskit.com.

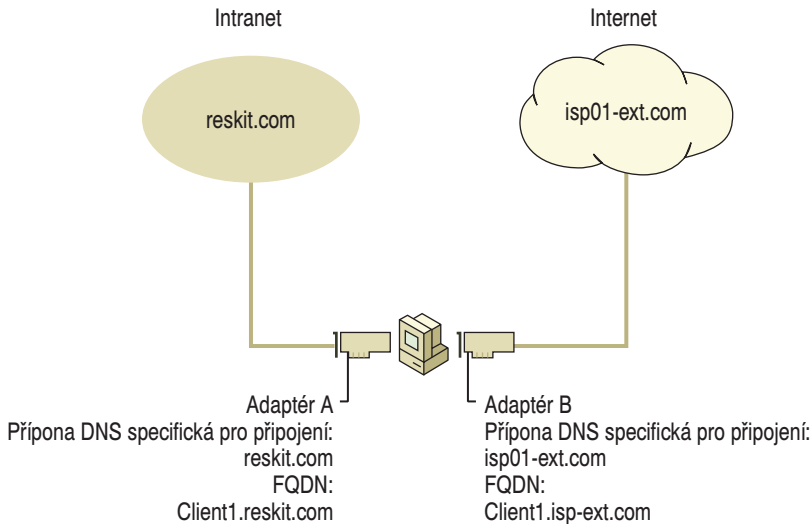
Název typu NetBIOS je odvozen z názvu hostitele, ale tyto názvy nemusí být stejné. Název typu NetBIOS je 16bajtový řetězec, který pro síťovou komunikaci jedinečně určí počítač nebo službu. Používají ho všechny síťové služby Windows 2000, aby získaly jedinečnou identifikaci. Jestliže má název hostitele DNS 15 a méně bajtů, název typu NetBIOS je název hostitele plus tolik mezer, aby vytvořily název o délce 15 bajtů, následován jedinečným identifikátorem, šestnáctým bajtem, který specifikuje síťovou službu. Jestliže je název hostitele delší než 15 bajtů, pak je dle výchozího nastavení název typu NetBIOS tvořen názvem hostitele zkráceným na 15 bajtů a identifikátorem služby. Jestliže se pokusíte vytvořit dva názvy hostitele DNS a prvních 15 bajtů je stejných, jste vyzváni ke vložení nového názvu pro rozhraní NetBIOS.

Poznámka: Vzhledem k tomu, že názvy hostitele jsou zakódovány ve formátu UTF-8, nemají nutně pouze 1 bajt na jeden znak. Znaky ASCII jsou o velikosti 1 bajtu každý, ale velikost rozšířených znaků je větší než 1 bajt.

Operační systém Windows 2000 také umožňuje, aby každý adaptér měl vlastní příponu DNS, která je známá jako zvláštní přípona DNS pro připojení. Tato přípona je zpravidla přiřazována serverem DHCP, který zapůjčuje adresu IP adaptéru. Na počítačích s operačním systémem Windows 2000 mohou správci navíc přiřadit zvláštní příponu DNS pro připojení staticky nastavovaným adaptérům.

V závislosti na nastavení může být zvláštní přípona DNS pro připojení přidána k názvu hostitele, aby vytvořila název FQDN, který je registrován službou DNS. Například předpokládejte, že počítač client1 má primární příponu DNS reskit.com a je připojen jak k síti internet, tak k podnikovému intranetu. Pro každé připojení můžete specifikovat zvláštní příponu DNS pro připojení. Pro připojení k podnikovému intranetu určíte

název reskit.com a název FQDN je potom client1.reskit.com. pro připojení k síti internet určité název isp01-ext.com a název FQDN je potom client1.isp01-ext.com. Toto nastavení je znázorněno na obrázku 6.1.



Obrázek 6.1 Doménové názvy se zvláštní příponou DNS pro připojení

Zvláštní příponu DNS pro připojení můžete specifikovat pro staticky nastavované adaptéry a adaptéry nastavované pomocí služby DHCP na záložce Služba DNS v dialogu Upřesnit nastavení TCP/IP. V tomto dialogu můžete také specifikovat to, jestli klient při registraci svého názvu FQDN používá svou zvláštní příponu DNS pro připojení navíc k primární příponě DNS. Více informací o nastavení klientů DHCP pro službu DNS najdete později v části „Dynamická aktualizace“.

Upozornění: Máte-li vícedomé dynamicky aktualizované klienty a alespoň jeden z adaptérů používá službu DHCP, nastavte server DHCP tak, aby aktualizoval záznamy prostředků podle žádosti klienta. Více informací o tom, jak nastavit servery DHCP, aby prováděly aktualizaci záznamů prostředků najdete později v části „Dynamická aktualizace“. Jestliže je server DHCP nastaven k registrování jak záznamů prostředku A, tak prostředku PTR, server DHCP nahradí všechny záznamy prostředku A u názvů, které se snaží zaregistrovat. Záznamy prostředků odpovídající adresám IP pro jiné adresy počítače mohou být vymazány.

Tabulka 6.1 obsahuje souhrn všech rozdílů mezi oběma druhy názvů s použitím příkladu názvu FQDN client1.reskit.com.

Tabulka 6.1 Názvy DNS a NetBIOS

Typ názvu	Popis
Název NetBIOS	<p>Název typu NetBIOS je používán k identifikaci služeb typu NetBIOS naslouchajícím na první adrese IP, která je navázána na adaptér. Tento jedinečný název typu NetBIOS je přeložen na adresu IP serveru pomocí všesměrového vysílání, serveru WINS nebo souboru LMHosts. Dle výchozího nastavení je stejný jako název hostitele až do délky 15 bajtů plus mezery potřebné k vyplnění celé délky plus identifikátor služby.</p> <p>Název typu NetBIOS je také znám jako název počítače NetBIOS. Například Název typu NetBIOS může být client1.</p>
Název hostitele	<p>Pojem název hostitele může znamenat buď název FQDN nebo první název názvu FQDN. V této kapitole pojem název hostitele odkazuje na první název názvu FQDN.</p> <p>Například první název názvu FQDN client1.reskit.com je client1.</p>
Primární přípona DNS	<p>Každému počítači s operačním systémem Windows 2000 může být přiřazena primární přípona DNS, která se používá při překladu názvu a registraci názvu. Primární přípona DNS je specifikována na záložce Identifikace sítě v dialogu Vlastnosti ikony Tento počítač.</p> <p>Primární přípona DNS je také známá jako primární název domény a název domény.</p> <p>například název FQDN client1.reskit.com má primární příponu DNS reskit.com.</p>
Zvláštní přípona DNS pro připojení	<p>Zvláštní přípona DNS pro připojení je přípona DNS, která je přiřazena adaptéru.</p> <p>Zvláštní přípona DNS pro připojení je známa také jako zvláštní přípona DNS adaptéru.</p> <p>Například zvláštní přípona DNS pro připojení může být acquired01-ext.com.</p>
Úplný název počítače	<p>Úplný název počítače je typu názvu FQDN. Stejný počítač může být identifikován více než jedním názvem FQDN. Nicméně úplným názvem počítače je název, který je spojením názvu hostitele a primární přípony DNS.</p>
Úplný doménový název	<p>Název FQDN je název DNS, který jedinečně identifikuje počítač na síti. Dle výchozího nastavení to je spojení názvu hostitele, primární přípony DNS a tečky.</p> <p>Například název FQDN může být client1.reskit.com.</p>

Dodržování omezení názvů hostitelů a domén

Různé implementace služby DNS používají různá omezení znaků a délky. Tabulka 6.2 obsahuje seznam omezení pro každou implementaci.

Tabulka 6.2 Omezení názvů

Omezení	Standardní služba DNS (včetně Windows NT 4.0)	Služba DNS ve Windows 2000	NetBIOS
Znaky	Podporuje dokument RFC 1123, který umožňuje používání 0 až 9 a pomlčku (-). znaků A až Z, a až z,	Je možno několik různých nastavení, které jsou popsány na konci této části.	Znaky sady Unicode, čísla, bílé mezery, symboly: ! @ # \$ % ^ & ') (. - _ { } ~
Délka úplného doménového názvu	63 bajtů na jeden název a 255 bajtů na název FQDN	63 bajtů na jeden název a 255 bajtů na název FQDN, řadiče domény jsou omezeny na 155 bajtů u názvu FQDN.	15 bajtů

Poznámka: Přestože můžete vytvořit dlouhé, složité názvy DNS, doporučuje se vytváření kratších popisných názvů.

Podle dokumentu RFC 1123 jsou jediné znaky, které je možno použít v názvu DNS, A až Z, a až z, 0 až 9 a pomlčka (-). Tečka (.) je v názvech DNS také používána, ale pouze mezi názvy DNS a na konci názvu FQDN. Mnoho serverů DNS včetně serverů DNS na operačním systému Windows NT 4.0 respektuje dokument RFC 1123.

Nicméně trvání na dokumentu RFC 1123 může představovat problém na sítích Windows 2000, které stále používají názvy typu NetBIOS. Názvy NetBIOS používají další znaky a může být časově velmi nákladné převést všechny názvy typu NetBIOS na standardní názvy DNS.

Ke zjednodušení procesu migrace na operační systém Windows 2000 z Windows NT 4.0 podporuje operační systém Windows 2000 širší znakovou sadu. Dokument RFC 2181 „Výjasnění specifikací služby DNS“ rozšiřuje znakovou sadu povolenou v názvech DNS. Stanoví, že název DNS může být binární řetězec a nemusí být nutně interpretován jako znaky ASCII. Na základě této definice společnost Microsoft navrhla přepracování specifikace názvu DNS tak, aby vyhovoval širší znakové sadě: znakové kódování UTF-8, jak je popsáno v dokumentu RFC 2044. Kódování UTF-8 je nadmnožinou znaků ASCII a překlad kódování USC-2 (známého také jako Unicode). Znaková sada UTF-8 obsahuje znaky z většiny světových psaných jazyků. To umožňuje mnohem větší rozsah možných názvů. Služba DNS pro operační systém Windows 2000 obsahuje i podporu pro kódování UTF-8.

Nicméně před použitím dalších znaků zvažte následující věci:

- Software některých překladačů třetích stran podporuje pouze znaky obsažené v dokumentu RFC 1123. Pokud máte software překladače jakékoli třetí strany, tento software pravděpodobně není schopen vyhledat počítače s názvy obsahujícími nestandardní znaky.
- Server DNS, který nepodporuje kódování UTF-8 může akceptovat zónový přenos zóny obsahující názvy znaků UTF-8, ale nemusí zpět zapsat tyto názvy do souboru zóny nebo opět nahrát tyto názvy ze souboru zóny. Proto nesmíte přenášet zónu, která obsahuje znaky UTF-8 na server DNS, který je nepodporuje.

Server DNS pro operační systém Windows 2000 můžete nastavit tak, aby povoloval nebo zakazoval použití znaků UTF-8 na vašem serveru Windows 2000. Můžete to provést na každém serveru z konzoly DNS. Na záložce *Upřesnit* v okně vlastností serveru nastavte *Kontrola názvů* na jednu z následujících možností:

- *Striktně RFC (ANSI)*. Povoluje A až Z, a až z, pomlčku (-) a hvězdičku (*) jako první název, a podtržítka (_) jako první znak názvu.
- *Jiné než RFC (ANSI)*. Povoluje všechny znaky povolené při režimu **Striktně RFC (ANSI)** a povoluje podtržítka (_) kdekoli v názvu.
- *Vícebajtové (UTF-8)*. Povoluje všechny znaky povolené v režimu **Jiné než RFC (ANSI)** a povoluje znaky UTF-8.
- *Všechny názvy*. Povoluje všechny znaky včetně znaků UTF-8.

Poznámka: Vložíte-li název DNS, který obsahuje znaky UTF nebo podtržítka, které nejsou obsaženy v dokumentu RFC 1123 při úpravách názvu hostitele nebo přípony DNS nebo vytváření domény služby Active Directory, objeví se upozornění vysvětlující, že některé implementace serveru DNS nemusí tyto znaky podporovat.

Používání zásad skupiny ke specifikaci přípony DNS

Když existují zásady skupiny, přípona nastavená v těchto zásadách skupiny je nadřazená lokální primární příponě DNS, která je dle výchozího nastavení stejná jako název domény Active Directory. Uživatelé mohou vkládat příponu do dialogu **Vlastnosti systému**, ale tato přípona je použita pouze v případě, že jsou zásady skupiny zakázány či nespecifikovány.

Nastavíte-li primární příponu DNS počítače odlišné od názvu domény Active Directory, musíte provést dodatečné nastavení, abyste umožnili registraci upraveného úplného názvu počítače v atributu názvu hostitele DNS a atributu hlavního názvu služby (Service Principal Name – SPN) objektu počítače ve službě Active Directory.

Dle výchozího nastavení musí mít název registrovaný v těchto attributech následující syntaxi:

< název typu NetBIOS >. < název domény Active Directory >

kde název typu NetBIOS je název typu NetBIOS počítače a název domény Active Directory je název DNS domény Active Directory. K umožnění registrace upraveného úplného názvu počítače musíte upravit seznam řízení přístupu (ACL) příslušné domény následujícím postupem. Tento postup musíte také provést, pokud jakékoli počítače připojené k doméně mají názvy hostitele delší než 15 bajtů.

► Úprava seznamu řízení přístupu (ACL) z důvodu umožnění registrace úplného názvu počítače

1. Klepněte na nabídku **Start**, vyberte položku **Programy**, dále položku **Nástroje pro správu** a klepněte na položku **Uživatelé a počítače služby Active Directory**.
2. V menu **Zobrazit** klepněte na příkaz **Upřesňující funkce**.
3. Pravým tlačítkem klepněte na doménu, kterou chcete upravit a pak klepněte na **Vlastnosti**.
4. Klepněte na záložku **Zabezpečení**.

5. Klepněte na Přidat, klepněte na **SELF**, klepněte na **PŘIDAT** a pak klepněte na **OK**. To přidá skupinu SELF do seznamu řízení přístupu (ACL).
6. Klepněte na tlačítko **Upřesnit**.
7. Klepněte na **SELF** a pak na **Zobrazit či upravit**.
8. Klepněte na záložku Vlastnosti.
9. V okně **Aplikovat** klepněte na **Objekty počítačů**.
10. V okně **Oprávnění** zaškrtněte **Povolit** u **Zapsat název hostitele DNS** a pak klepněte na **OK**, aby se zavřel dialog **Uživatelé a počítače služby Active Directory**.

Upozornění: Pokud upravíte seznam řízení přístupu (ACL) tak, abyste povolili registraci upraveného úplného názvu počítače, jakýkoli počítač v doméně se může registrovat pod jiným názvem.

Překladač pro operační systém Windows 2000

Operační systém Windows 2000 obsahuje službu překladač s mezipamětí. Překladač s mezipamětí snižuje provoz DNS na síti a urychluje překlad názvů poskytováním lokální mezipaměti pro dotazy DNS. Pro účel řešení problémů lze tuto službu prohlížet, zastavovat a spouštět jako kteroukoli další službu Windows 2000 použitím konzoly **Component Services**. Překladač s mezipamětí je dle výchozího nastavení povolen.

Překladač pro operační systém Windows 2000 provádí následující úlohy:

- Překlad názvů.
- Obecné ukládání dotazů do mezipaměti.
- Ukládání negativních výsledků do mezipaměti.
- Sledování přechodných (Plug and Play) síťových adaptérů a nastavení jejich IP.
- Sledování zvláštních názvů domén pro připojení.
- Když server na dotazy neodpovídá, překladač se ho na určitou dobu přestane dotazovat.
- Když překladač obdrží ze serveru DNS více záznamů prostředku A, určí jejich prioritu na základě jejich adres IP.

Překlad názvů

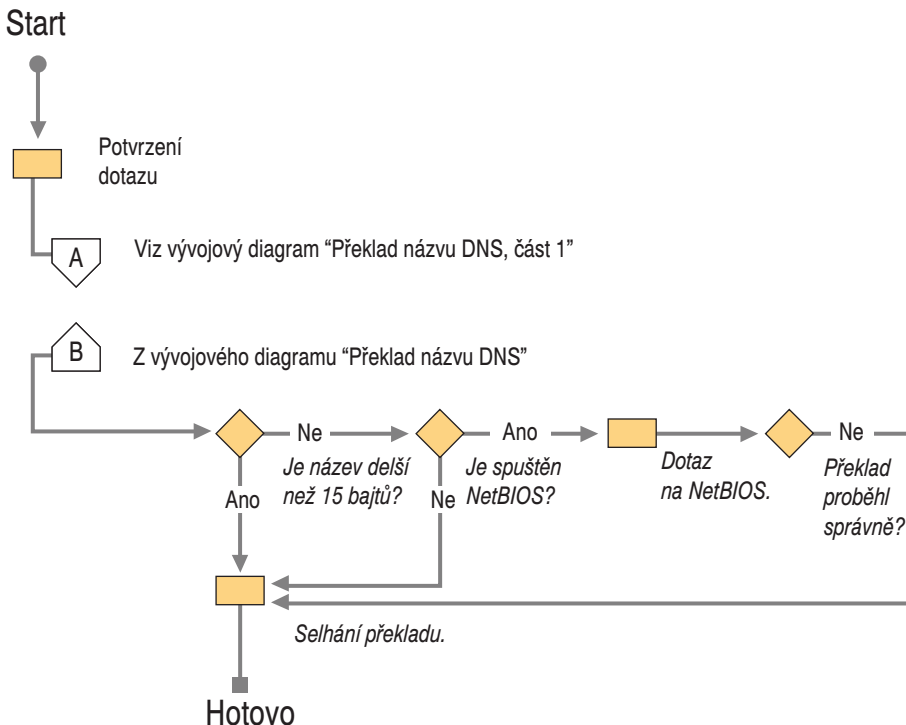
Překlad názvu se v operačním systému Windows 2000 značně liší od překladu názvu v operačním systému Windows NT 4.0. V operačním systému Windows NT 4.0 překladač obecně zkoušel nejprve překlad názvu typu NetBIOS a pak překlad názvu DNS. V operačním systému Windows 2000 ale překladač obecně zkouší nejprve překlad názvu DNS a pak překlad názvu typu NetBIOS. Operační systém Windows 2000 také obsahuje vylepšení pro vícedomé počítače.

Když je použito rozhraní API GetHostByName, překladač Windows 2000 nejprve pošle dotaz na název serveru DNS. Pokud překlad názvu DNS selže, překladač zkontroluje, zda název není delší než 15 bajtů. Pokud je delší, překlad selže. Pokud není delší, překladač zkontroluje, jestli běží rozhraní NetBIOS. Pokud neběží, překlad selže. Pokud běží, překladač zkusí překlad názvu typu NetBIOS. Více informací o překladu názvu ty-

pu NetBIOS a vývojovém diagramu překladu názvu typu NetBIOS najdete v části „Přehled TCP/IP pro Windows 2000“.

Na obrázku 6.2 je znázorněn přehled tohoto procesu.

Poznámka: Vývojový diagram na obrázku 6.2 vás odkazuje na další vývojové diagramy v jiných obrázcích. Správný diagram najdete podle popisu obrázku.



Obrázek 6.2 Přehled překladu názvu

Překlad názvu DNS

Při začátku překladu názvu DNS překladač nejprve zkontroluje, jaký typ názvu byl předložen. Mohou být předloženy tři typy názvů:

- Úplné doménové názvy

Tyto názvy jsou ukončeny tečkou. Například:
host.reskit.com.

- Jednonázvové neúplné doménové názvy

Tyto názvy neobsahují žádné tečky. Například:
host

- Vícenázvové neúplné doménové názvy

Tyto názvy obsahují jednu nebo více teček, ale nejsou ukončeny tečkou. Například:
host.reskit.com

- nebo -
host.reskit

Po vložení názvu FQDN uživatelem, překladač se dotáže služby DNS s použitím tohoto názvu. Podobně když uživatel vloží vícenázvový neúplný (neukončený tečkou) název, překladač DNS přidá ukončující tečku a dotáže se služby DNS na tento název.

Nicméně pokud uživatel vloží vícenázvový neúplný název a jeho překlad jako názvu FQDN je neúspěšný, nebo uživatel vloží jednonázvový neúplný název, překladač systematicky k vloženému názvu přidává různé přípony DNS, přidává tečky, aby z názvu byl název FQDN, a znovu ho předkládá službě DNS.

Pokud uživatel nevložil seznam pro vyhledávání přípon domén, překladač přidá následující názvy:

1. Primární příponu DNS, která je specifikována na záložce **Identifikace sítě** dialogu **Vlastnosti systému** ve vlastnostech ikony **Tento počítač**. Klepněte na tlačítko **Vlastnosti** a pak klepněte na **Další**.
2. Není-li překlad úspěšný, překladač přidá všechny zvláštní přípony DNS pro připojení. Tyto přípony mohou být dynamicky přiřazovány serverem DHCP. Můžete také pro každé připojení specifikovat přípony na záložce **Služba DNS** v dialogu **Upřesnit nastavení TCP/IP**. Dialog **Upřesnit nastavení TCP/IP** otevřete klepnutím pravého tlačítka myši na připojení a pak klepnutím na **Vlastnosti**, čímž otevřete vlastnosti připojení. Pak poklepejte na **Protokol TCP/IP**, tím se dostanete k dialogu **Vlastnosti protokolu TCP/IP** a pak klepněte na **Upřesnit**.

Pokud není překlad stále úspěšný, překladač vytvoří název FQDN přidáním nadřazené přípony názvu primární přípony DNS, potom nadřazené přípony této přípony atd., dokud nezůstanou pouze dva názvy. Například jestliže uživatel vloží název **client** a primární přípona DNS je eu.reskit.com, překladač zkusí client.eu.reskit.com a pak client.reskit.com.

Na druhou stranu, pokud uživatel vloží na záložce **Služba DNS** v dialogu **Upřesnit nastavení TCP/IP** ve vlastnostech síťového připojení seznam přípon domén pro vyhledávání, jsou obě přípony (primární přípona DNS i zvláštní přípona DNS pro připojení) ignorovány a k názvu není před jeho předložením službě DNS připojena žádná z nich. Namísto toho překladač přidá všechny přípony ze seznamu pro vyhledávání ve stejném pořadí a předkládá je serveru DNS tak dlouho, dokud nenajde odpovídající záznam nebo nedosáhne konce seznamu.

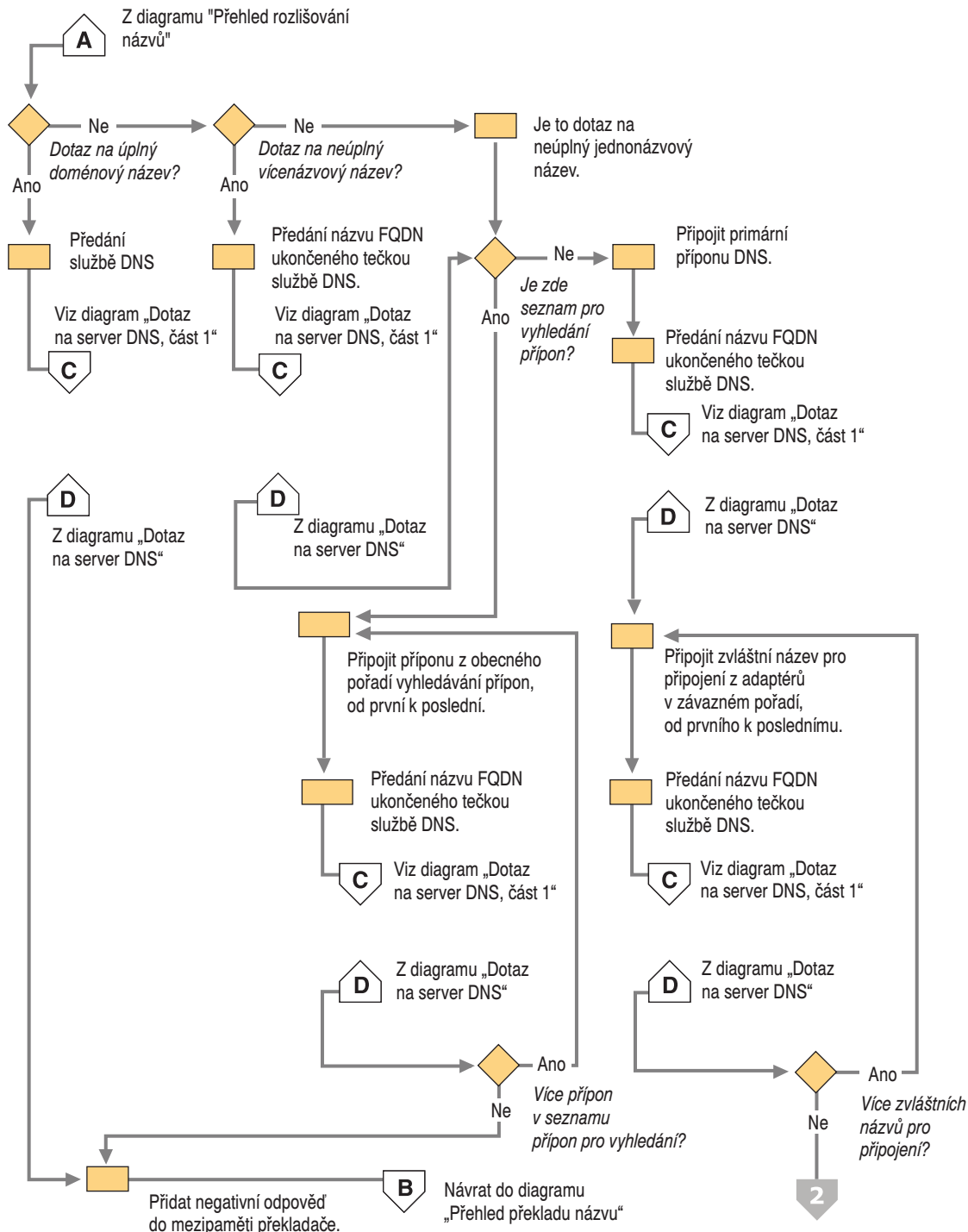
Na obrázcích 6.3 a 6.4 je znázorněno, jak se tvoří názvy FQDN. Obrázek 6.5 znázorňuje, co se stane, když je název předložen serveru DNS.

Poznámka: Vývojové diagramy na obrázcích 6.3 a 6.4 vás odkazují na další diagramy v jiných obrázcích. Správný diagram najdete podle popisu obrázku.

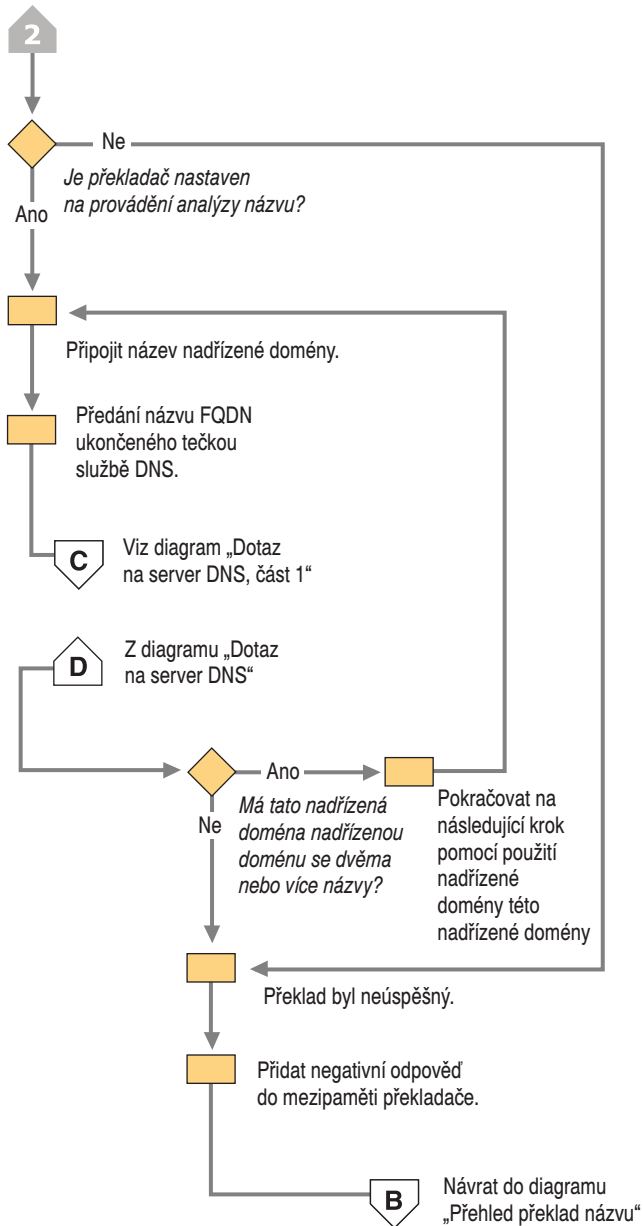
A Z diagramu „Přehled překladu názvu“.

Dotazy DNS

Jestliže překladač ukládá názvy do mezipaměti, překladač zkontroluje po předložení názvu serveru DNS nejdříve mezipaměť. Pokud je název v mezipaměti, vrátí údaje uživateli. Pokud název v mezipaměti není, překladač se dotáže serverů DNS, které jsou obsaženy ve vlastnostech protokolu TCP/IP každého adaptéru.



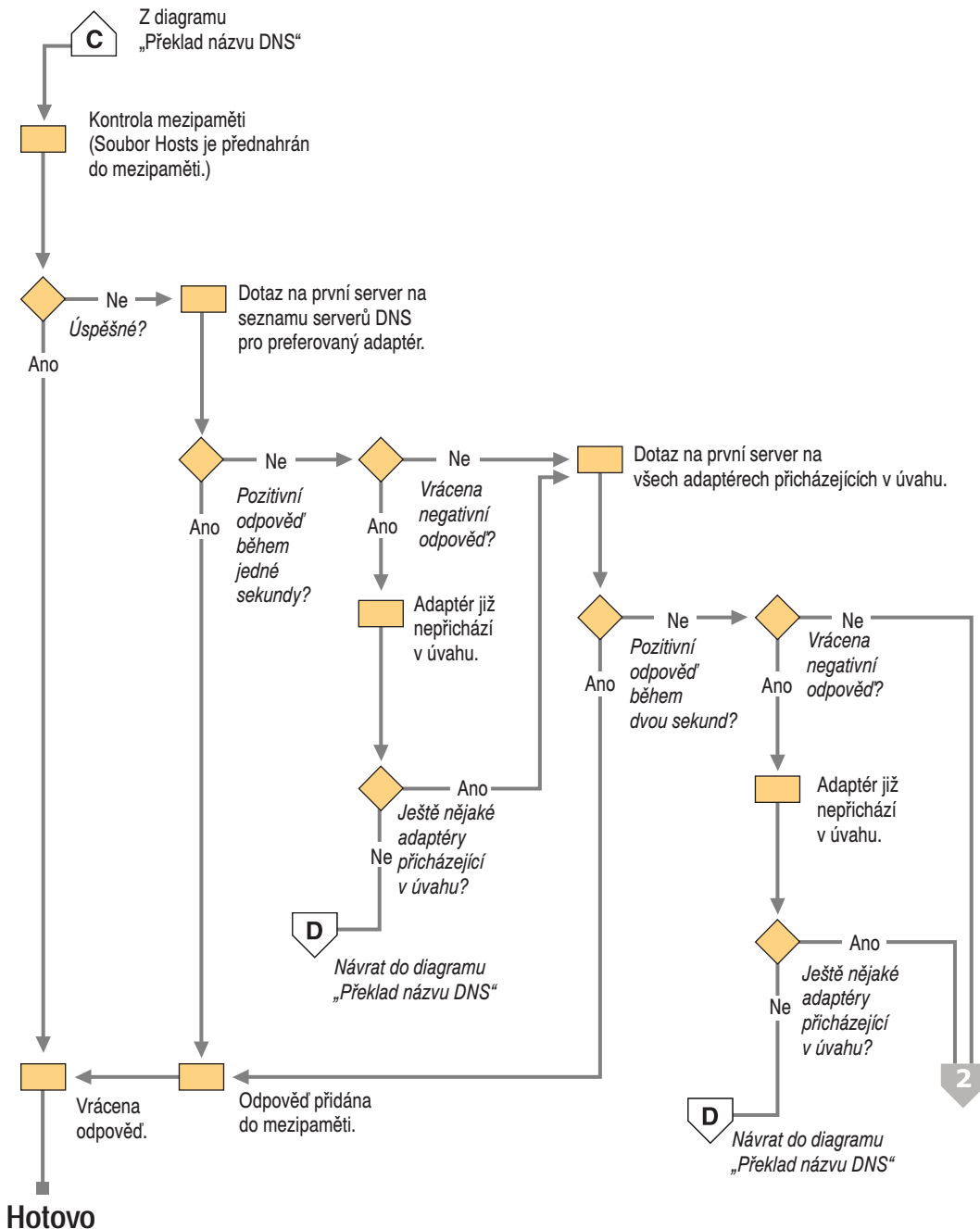
Obrázek 6.3 Překlad názvu DNS, část 1



Obrázek 6.4 Překlad názvu DNS, část 2

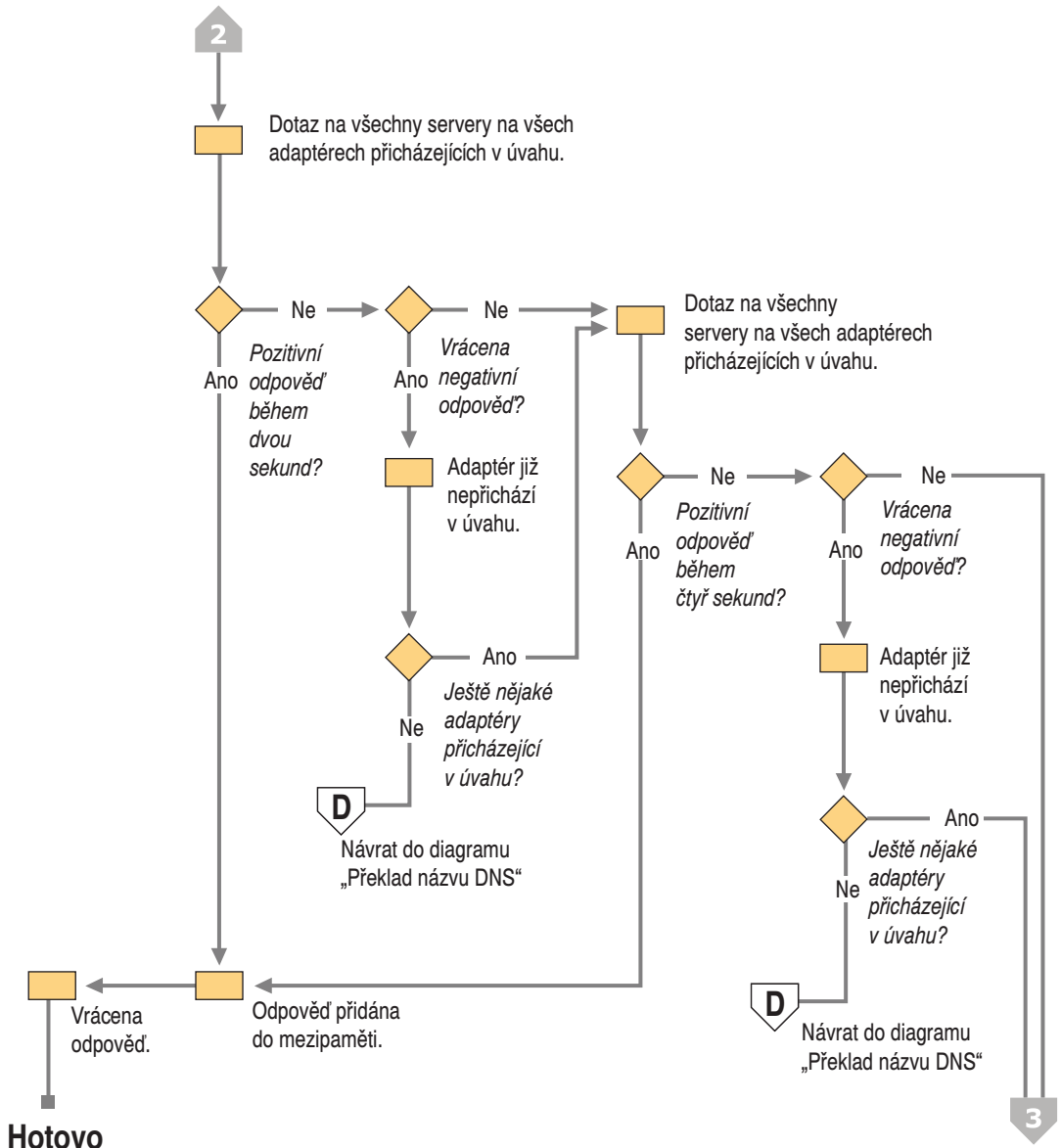
Překladač se může dotázat prostřednictvím adaptérů v počítači, včetně adaptérů vzdáleného přístupu. V operačním systému Windows NT 4.0 se překladač dotazoval serverů DNS prostřednictvím všech adaptérů. V operačním systému Windows 2000 můžete nicméně určit seznam serverů DNS, kterých se má každý adaptér dotazovat.

Obrázky 6.5, 6.6 a 6.7 zobrazují proces, kterým se překladač dotazuje serverů na každém adaptéru.

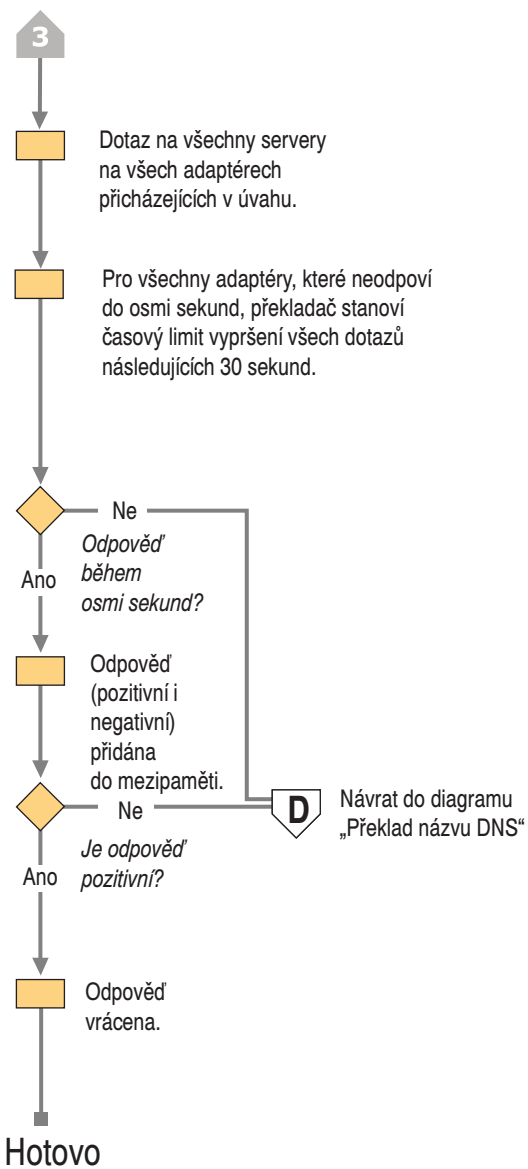


Obrázek 6.5 Dotaz na server DNS, část 1

Poznámka: Vývojové diagramy na obrázcích 6.5, 6.6 a 6.7 vás odkazují na další vývojové diagramy v jiných obrázcích. Správný diagram najdete podle popisu obrázku.



Obrázek 6.6 Dotaz na server DNS, část 2



Obrázek 6.7 Dotaz na server DNS, část 3

Překladač se dotazuje serverů DNS v následujícím pořadí:

1. Překladač pošle dotaz na první server na seznamu serverů DNS umístěném na preferovaném adaptéru a čeká po dobu jedné sekundy na odpověď.
2. Jestliže překladač neobdrží do jedné sekundy odpověď od prvního serveru, pošle dotaz na první servery DNS na všech adaptérech, které připadají v úvahu, a čeká na odpověď dvě sekundy.
3. Jestliže překladač neobdrží od kteréhokoli serveru odpověď do dvou sekund, pošle dotaz na všechny servery DNS na všech adaptérech, které připadají v úvahu, a čeká na odpověď další dvě sekundy.
4. Pokud překladač stále neobdrží odpověď od kteréhokoli serveru, pošle dotaz na všechny servery DNS na všech adaptérech, které připadají v úvahu, a čeká na odpověď čtyři sekundy.
5. Pokud překladač stále neobdrží odpověď od kteréhokoli serveru, pošle dotaz na všechny servery DNS na všech adaptérech, které připadají v úvahu, a čeká na odpověď osm sekund.

Jestliže obdrží pozitivní odpověď, zastaví dotazování na název, přidá odpověď do mezipaměti a vrátí odpověď klientovi.

Jestliže neobdrží žádnou odpověď od kteréhokoli serveru na konci lhůty osmi sekund, odpoví klientovi zprávou o vypršení časového limitu. Jestliže neobdrží odpověď od jakéhokoli serveru na určitém adaptéru, následujících 30 sekund překladač odpovídá na všechny dotazy určené pro servery na tomto adaptéru zprávou o vypršení časového limitu a neposílá na tyto servery žádný dotaz. Tato zpráva o vypršení časového limitu je odesílána pouze počítači s operačním systémem Windows 2000 Professional.

Jestliže v kterémkoli okamžiku překladač obdrží od serveru negativní odpověď, vyloučí všechny servery na tomto adaptéru ze svých úvah během tohoto vyhledávání. Například pokud v kroku č. 2 první server na alternativním adaptéru A vrátil negativní odpověď, překladač by neposlal dotaz na jakýkoli server uvedený na seznamu alternativního adaptéru A.

Překladač sleduje, které servery odpovídají rychleji a může přesunout servery v seznamu nahoru či dolů v závislosti na tom, jak rychle odpovídají na dotazy.

Obrázek 6.8 znázorňuje, jak se překladač dotazuje každého serveru na adaptéru.

Nastavení dotazů

Překladač připojí v dotazu přípony DNS k názvu, který vložíte, pokud je splněna kterákoli z následujících podmínek:

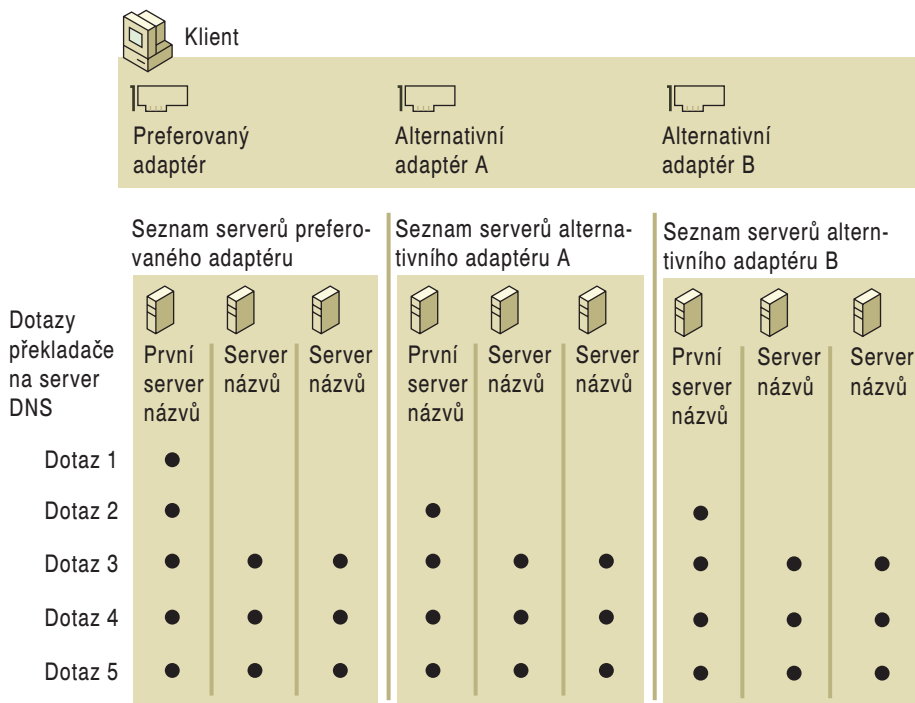
- Název je jednonázvový neúplný název.
- Název je vícenázvový neúplný název a překladač ho nepřeložil jako název FQDN.

Poznámka: Informace o tom, co se stane, když jsou název FQDN a vícenázvové doménové názvy předány serveru DNS, najdete dříve v části „Překlad názvu DNS“.

Přípony, které jsou přidávány k dotazům, můžete nastavit v dialogu **Upřesnit nastavení TCP/IP**.

► Zobrazení dialogu Upřesnit nastavení TCP/IP

1. Klepněte pravým tlačítkem na **Místa v síti** a pak klepněte na **Vlastnosti**.



Obrázek 6.8 Vicedomý překlad názvu

2. Klepněte pravým tlačítkem na připojení, které chcete zobrazit a pak klepněte na **Vlastnosti**.
3. Klepněte na **Protokol TCP/IP** a pak klepněte na **Vlastnosti**.
4. Klepněte na **Upřesnit** a pak klepněte na záložku **Služba DNS**.

Dialog Upřesnit nastavení TCP/IP vidíte na obrázku 6.9.

Okno označené **Připojit tyto přípony DNS (pořadí)** vám umožňuje specifikovat seznam přípon DNS, které má překladač použít, nazvaný seznam vyhledávání přípon DNS. Vložíte-li seznam vyhledávání přípon DNS, překladač přidá tyto přípony do pořadí a nezkouší další názvy domén. Například, pokud okno **Připojit tyto přípony DNS (pořadí)** obsahuje názvy zařazené v obrázku 6.9 a vy předložíte překladači neúplný jednonázvový název „coffee“, překladač se dotazuje na toto pořadí názvů FQDN:

coffee.reskit.com.

coffee.eu.reskit.com.

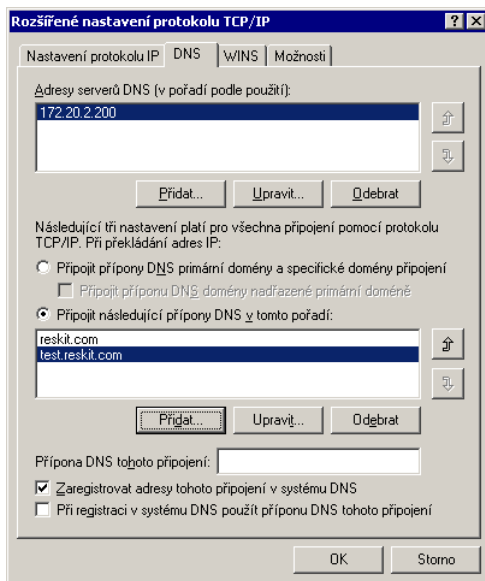
Pokud nevložíte seznam vyhledávání přípon DNS, překladač jako první připojí primární příponu DNS, kterou specifikujete na záložce **Identifikace sítě** v dialogu **Vlastnosti systému**. Například jestliže je primární přípona DNS fareast.isp01-ext.com, překladač se dotáže na následující název FQDN:

coffee.fareast.isp01-ext.com.

Dále, jestliže je tento dotaz neúspěšný, a jestliže je v okně **Přípona DNS pro toto připojení** specifikována zvláštní přípona DNS pro připojení nebo je přiřazena serverem DHCP, překladač připojí tuto příponu. Například jestliže jste vložili do okna **Přípona**

DNS pro toto připojení název noam.reskit.com a pak se dotazovali na neúplný jednonázvový název „coffee“, překladač se dotáže na následující název FQDN:

coffee.noam.reskit.com.



Obrázek 6.9 Záložka Služba DNS v dialogu Upřesnit nastavení TCP/IP

Dále, zaškrtnete-li pole **Připojit příponu nadřazenou primární příponě DNS**, překladač provede analýzu názvu primární přípony DNS. Odebere nejzbytečnější název a zkouší výsledný doménový název, dokud zbývají pouze dva názvy. Například jestliže je primární přípona DNS mfg.fareast.isp01-ext.com a vybrali jste pole **Připojit příponu nadřazenou primární příponě DNS** a dotázali jste se na neúplný jednonázvový název „coffee“, překladač se dotáže na název FQDN v tomto pořadí:

coffee.fareast.isp01-ext.com.

coffee.isp01-ext.com.

Analýzu názvu můžete zakázat odstraněním zaškrtnutí pole **Připojit příponu nadřazenou primární příponě DNS**.

Nastavení ukládání do mezipaměti a ukládání negativních odpovědí do mezipaměti

Když překladač operačního systému Windows 2000 obdrží pozitivní nebo negativní odpověď na dotaz, přidá pozitivní nebo negativní odpovědi do své mezipaměti. Překladač vždy před dotázáním se na jakýkoli server DNS prohledává svou mezipaměť. Je-li název v mezipaměti, překladač místo dotazu na server DNS použije název z mezipaměti. To urychluje dotazy a snižuje provoz dotazů DNS na síti.

K prohlížení a vyprazdňování mezipaměti můžete použít z příkazového řádku nástroj Ipconfig.

► **Prohlížení mezipaměti**

- Na příkazovém řádku napište následující příkaz a stiskněte ENTER:

ipconfig / displaydns

Nástroj Ipconfig zobrazí obsah mezipaměti překladače DNS, a to včetně názvů, které jsou přednahrány ze souboru Hosts a všech nedávno dotazovaných názvů, které byly systémem přeloženy.

Po určité době specifikované hodnotou TTL spojenou s názvem překladač odstraní název z mezipaměti. Hodnoty TTL spojené se záznamem můžete prohlížet a měnit v konzole DNS.

► Prohlížení hodnoty TTL záznamu

1. V konzole DNS vyberte **Zobrazit** a klepněte na **Upřesnit**, čímž se otevře upřesněné zobrazení. tento krok není nutný ke zobrazení hodnot TTL pro záznam Start of Authority (SOA).
2. Klepněte pravým tlačítkem na záznam a klepněte na **Vlastnosti**.

Mezipaměť můžete také vyprázdnit ručně. Po vyprázdnění mezipaměti se počítač musí dotazovat serverů DNS.

► Ruční vyprázdnění mezipaměti pomocí nástroje Ipconfig

- Na příkazovém řádku napište následující příkaz a pak stiskněte ENTER:

ipconfig / flushdns

Lokální soubor Hosts je přednahrán do mezipaměti překladače a opětovně do mezipaměti nahrán při každé aktualizaci lokálního souboru Hosts.

Poznámka: Mezipaměť překladače a mezipaměť serveru jsou udržovány odděleně. Informace o mezipaměti serveru najdete v nápovědě Windows 2000 Server.

Délka doby, po kterou jsou pozitivní a negativní odpovědi udržovány v mezipaměti klienta DNS, závisí na hodnotách následujícího klíče registru:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\\DNSCache\Parameters

Upozornění: Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správčovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. K nastavení nebo přizpůsobení si Windows 2000 používejte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Pozitivní odpovědi jsou ukládány do mezipaměti na počet sekund specifikovaný v odpovědi na dotaz, kterou překladač obdržel, ale nikdy ne na déle než je hodnota záznamu **MaxCacheEntryTtlLimit** (DWORD) v registru. Přednastavená hodnota je 86 400 sekund.

Operační systém Windows 2000 podporuje ukládání negativních odpovědí do mezipaměti, jak je specifikováno v dokumentu RFC 2308, s některými úpravami mezipaměti překladače. V mezipaměti překladače jsou ukládány negativní odpovědi po dobu spe-

cifikovanou hodnotou záznamu **NegativeCacheTime** value (DWORD) v registru. Přednastavená hodnota je 30 sekund. Nechcete-li negativní odpovědi vůbec ukládat do mezipaměti, nastavte hodnotu záznamu **NegativeCacheTime** na 0.

Poznámka: Server DNS pro operační systém Windows 2000 ukládá negativní odpovědi do mezipaměti s ohledem na minimální hodnotu TTL v záznamu SOA. Nicméně nemůže to být méně než jedna minuta a více než 15 minut. Proto je-li minimální hodnota TTL v záznamu SOA 20 minut, negativní odpověď je uložena pouze 15 minut. Změnu minimální hodnoty TTL můžete provést prostřednictvím konzoly DNS nebo programu Dnscmd.exe.

Jestliže jsou všechny servery DNS na adaptéru dotázány a žádný z nich neodpovídá, ať už pozitivně či negativně, všechny následující dotazy na názvy na jakýkoli server zařazený na tomto adaptéru okamžitě selžou a selhávají po přednastavenou dobu 30 sekund. Tato vlastnost snižuje provoz sítě a je dostupná pouze na operačním systému Windows 2000 Professional.

Nastavení priorit podsítě

Jestliže překladač obdrží od serveru DNS více záznamů prostředku A a některé mají adresy IP ze sítě, na které je překladač přímo připojený, překladač zařadí tyto záznamy prostředku jako první. To snižuje provoz sítě přes podsítě díky přinucení počítačů, aby se připojovaly k prostředkům sítě, jež jsou jim nejbližší.

Například předpokládejte, že máte tři servery WWW, které všechny hostí stránku WWW pro a jsou všechny umístěny na různých podsítích. Na serveru názvů můžete vytvořit následující záznamy prostředku:

www.reskit.com.	IN	A	172.16.64.11
www.reskit.com.	IN	A	172.17.64.22
www.reskit.com.	IN	A	172.18.64.33

Když se uživatelé dotazují na , překladač vezme první ze seznamu adres IP ze sítě, ke kterým je počítač přímo připojen. Například pokud se uživatel s adresou IP 172.17.64.93 dotazuje na www.reskit.com, překladač vrátí záznamy prostředku v následujícím pořadí:

www.reskit.com.	IN	A	172.17.64.11
www.reskit.com.	IN	A	172.16.64.22
www.reskit.com.	IN	A	172.18.64.33

Stanovení priorit podsítě zabraňuje překladači použít vlastnost cyklického výběru definovanou v dokumentu RFC 1794. Při použití této vlastnosti server „protáčí“ pořadí záznamů prostředku vrácené v odpovědi na dotaz, ve které je více záznamů prostředku stejného typu pro dotazovaný doménový název DNS. Proto pokud se v příkladu uvedeném výše uživatel dotazuje na doménu , server názvů odpovídá na požadavek prvního klienta následujícím pořadím adres:

```
172.16.64.11
172.17.64.22
172.18.64.33
```

Na požadavek druhého klienta odpovídá následujícím pořadím adres:

```
172.17.64.22
```

172.18.64.33

172.16.64.11

Pokud jsou klienti nastaveni k používání první adresy IP v seznamu, který dostanou, používají různí klienti různé adresy, takže zatížení mezi více prostředky sítě, které mají stejný název, je lépe vyváženo. Nicméně pokud jsou překladače nastaveny pro stanovení priorit podsítě, překladače reorganizují seznam tak, aby upřednostňoval adresy IP ze sítí, na které jsou přímo připojeni, čímž je snížena efektivita vlastnosti cyklického výběru.

Ačkoli stanovení priorit podsítě snižuje provoz sítě přes podsítě, v některých případech je lepší dát přednost vlastnosti cyklického výběru, jak je popsána v dokumentu RFC 1794. Pokud tomu tak je, můžete zakázat stanovení priorit podsítě na klientech přidáním záznamu `PrioritizeRecordData` do registru s hodnotou 0 (`REG_DWORD`) do následujícího podklíče registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\DnsCache\Parameters
```

Upozornění: Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správcovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. K nastavení nebo přizpůsobení si Windows 2000 použijte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Nastavení priorit podsítě na serveru

Navíc k nastavení překladače k provádění stanovení priorit podsítě pro záznamy, které obdrží, můžete nastavit server tak, aby prováděl totéž u záznamů, které odesílá. Chování serveru závisí na nastavení možnosti **Umožnit techniku round robin** na záložce **Upřesnit** v dialogu **Vlastnosti** modulu snap-in služby DNS a hodnotě záznamu **LocalNetPriority** (`REG_DWORD`) v registru v následujícím podklíči registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\DNS\Parameters\
```

Můžete také změnit nastavení možnosti cyklického výběru v registru, ale udělejte to namísto toho v modulu snap-in služby DNS.

Je-li vybrána možnost **Umožnit techniku round robin** (dle výchozího nastavení) a hodnota záznamu **LocalNetPriority** je 1, server protáčí záznamy prostředku A, které vrací v pořadí dle jejich podobnosti adrese IP dotazujícího se klienta. Je-li zrušeno vybraní možnosti **Umožnit techniku round robin**, server vrací záznamy v pořadí dle priority lokální sítě. Neprotáčí dostupné adresy.

Je-li vybrána možnost **Umožnit techniku round robin** a hodnota záznamu **LocalNetPriority** je 0 (dle výchozího nastavení), server protáčí dostupné záznamy v pořadí, ve kterém byly přidány do databáze. Je-li zrušeno vybraní možnosti **Umožnit techniku round robin** a hodnota záznamu **LocalNetPriority** je 0 (dle výchozího nastavení), server vrací záznamy v pořadí, ve kterém byly přidány do databáze. Server se vracené záznamy nesnaží třídit nebo protáčet.

Upozornění: Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správcovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. K nastavení nebo přizpůsobení si Windows 2000 použijte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Zabránění překladači v přijímání odpovědí od nedotázaných serverů

Dle výchozího nastavení překladače přijímají odpovědi i od serverů, které nebyly dotázány. Tato vlastnost zrychluje výkon, ale může představovat ohrožení zabezpečení. Chcete-li tuto vlastnost zakázat, přidejte záznam QueryIpMatching registru s hodnotou 1 (REG_DWORD) do následujícího podklíče registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
\DnsCache\Parameters
```

Upozornění: Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správcovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. K nastavení nebo přizpůsobení si Windows 2000 použijte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Nastavení služby DNS pro službu Active Directory

Základní koncepty služby DNS a Active Directory

Služba Active Directory je adresářová služba operačním systémem Windows 2000. Adresářová služba sestává z následujících součástí:

- Úložiště informací používané k ukládání informací o objektech.
- Služby, které zpřístupňují tyto uložené informace uživatelům a aplikacím.

Stejně jako služba DNS, i služba Active Directory je distribuovaná databáze, která může být členěna a replikována. Domény služby Active Directory jsou určeny názvy DNS. Služba Active Directory používá službu DNS jako svou *lokalizační službu*, která umožňuje počítačům najít umístění (lokalizovat) řadičů domén. K vyhledání řadiče domény v určité doméně klient dotazuje server DNS na záznam prostředků SRV a A, které poskytují názvy a adresy IP serverů protokolu LDAP domény. Protokol LDAP je protokol používaný k dotazování a aktualizaci služby Active Directory a všech řadičů domén běžících jako server LDAP. Více informací o záznamech prostředku A a SRV najdete v části „Úvod do služby DNS“. Více informací o lokalizační službě domén najdete v knize *Microsoft® Windows® 2000 Server Distribuované systémy* v části „Logická struktura služby Active Directory“.

Více informací o tom, jak nastavit službu DNS k podpoře služby Active Directory najdete později v části „Nastavení služby DNS pro službu Active Directory“.

Službu Active Directory nemůžete instalovat bez služby DNS na síti, protože služba Active Directory používá DNS jako svou lokalizační službu. Nicméně můžete odděleně, bez služby Active Directory, instalovat službu DNS. Instalujete-li službu DNS na řadiči domény, můžete také vybrat, jestli k poskytování uložení a replikací používat nebo nepoužívat službu Active Directory. Používání služby Active Directory pro ukládání a replikace poskytuje následující výhody:

- Zvýšená odolnost proti chybám
- Zabezpečení
- Jednodušší správa
- Efektivnější replikace rozsáhlých zón

Pro fungování služby DNS jako lokalizační služby pro službu Active Directory musíte mít server DNS, který bude hostit záznamy lokátoru (záznamy A, SRV a CNAME). Více informací o lokátoru najdete v knize *Microsoft® Windows® 2000 Server Distribuované systémy* v části „Logická struktura služby Active Directory“.

Server DNS pro operační systém Windows 2000 můžete nastavit automaticky pomocí průvodce instalací služby Active Directory, dodávaného v operačním systému Windows 2000, který instaluje a nastavuje službu Active Directory. Průvodce instalací služby Active Directory může provádět veškerou instalaci a nastavení potřebné pro službu DNS a nezbytné záznamy lokátoru přidá služba Netlogon. Více informací o průvodci instalací služby Active Directory najdete dále v části „Používání průvodce instalací služby Active Directory“.

Pokud nepoužíváte server DNS pro jiný operační systém než Windows 2000, nebo pokud nechcete provádět zvláštní nastavení, nepotřebujete nastavovat službu DNS ručně, aby podporovala službu Active Directory. Nicméně pokud chcete změnit přednastave-

né nastavení, které vytváří průvodce instalací služby Active Directory, můžete službu DNS nastavit ručně. V operačním systému Windows 2000 můžete nastavit službu DNS použitím konzoly DNS. Informace o konzole DNS a jejím použití najdete dále v části „Používání průvodce nastavením serveru DNS“.

Pokud používáte server DNS třetích stran, musíte také provést ruční nastavení. Informace o problémech spojených s nastavením služby DNS při používání serveru DNS třetích stran najdete dále v části „Nastavení serverů DNS s jiným operačním systémem než Windows 2000 k podpoře služby Active Directory“.

Používání průvodce instalací služby Active Directory

Průvodce instalací služby Active Directory povyšuje počítač do role řadiče domény, instaluje službu Active Directory a může instalovat a nastavit server DNS. Více informací o průvodci instalací služby Active Directory najdete v knize *Microsoft® Windows® 2000 Server Distribuované systémy* v části „Ukládání dat službou Active Directory“.

Když spustíte průvodce instalací služby Active Directory a rozhodnete se vytvořit novou doménu, průvodce najde server DNS, který je určující pro název nové domény Active Directory, a pak zkontroluje, jestli server bude přijímat dynamickou aktualizaci. Je-li test pozitivní, průvodce neinstaluje a nanastavuje lokální server DNS.

Pokud průvodce instalací služby Active Directory nemůže najít server DNS, který je určující pro název nové domény Active Directory, nebo pokud server, který průvodce najde, nepodporuje dynamickou aktualizaci nebo není na dynamickou konfiguraci nastaven, průvodce instalací služby Active Directory se vás zeptá, jestli chcete, aby průvodce automaticky nainstaloval a nastavil lokální server DNS. Odpovíte-li, že ano, průvodce automaticky nainstaluje a nastaví službu DNS Server.

Během automatického nastavení průvodce instalací služby Active Directory přidá do serveru DNS zónu pro dopředné vyhledávání, která bude hostit záznamy lokátoru, a nastaví server DNS k přijímání dynamické aktualizace. (Zóna s dopředným vyhledáváním je zóna, která obsahuje informace potřebné k překladu názvů v rámci domény DNS.) V některých případech také upřednostní kořenové odkazy s názvy kořenových serverů. Průvodce používá k určení, zda upřednostnit odkazy na kořenové servery, následující proces:

Průvodce instalací služby Active Directory prozkoumá nastavení protokolu TCP/IP počítače a zkontroluje, jestli je počítač nastaven k používání jakýchkoli serverů DNS. Pokud ano, průvodce instalací služby Active Directory se dotáže na kořenové servery. Jestliže najde kořenové servery DNS, upřednostní odkazy na kořen s názvy kořenových serverů DNS.

Pokud překladáč není nastaven k použití jakýchkoli serverů DNS, průvodce instalací služby Active Directory se dotáže na kořenové servery DNS specifikované v souboru *Cache.dns*. Dle výchozího nastavení jsou jimi kořenové servery internetu. Pokud najde kořenové servery DNS, upřednostní odkazy na kořeny s názvy kořenových serverů DNS. Pokud žádné kořenové servery nenajde, vytvoří kořenovou zónu na serveru DNS, kterou se tím stane kořenovým serverem.

Po skončení průvodce instalací služby Active Directory jste vyzváni k restartu počítače. Po restartu počítače se komponenta Netlogon snaží přidat záznamy prostředků lokátoru do serveru DNS pomocí posílání požadavku na dynamickou aktualizaci určujícímu serveru DNS. Záznamy prostředků lokátoru jsou nezbytné proto, aby ostatní počítače mohly lokalizovat tento řadič domény.

Poznámka: Průvodce instalací služby Active Directory můžete vyvolat také provedením souboru odpovědí pro bezobslužnou instalaci, který obsahuje všechna potřebná nastavení. Soubor odpovědí pro bezobslužnou instalaci je soubor, který průvodce používá k poskytování odpovědí na otázky. Více informací o souboru odpovědí pro bezobslužnou instalaci pro průvodce instalací služby Active Directory najdete v knize *Microsoft® Windows® 2000 Server Distribuované systémy* v části „Uložení dat služby Active Directory“.

K instalaci a nastavení služby DNS a Active Directory postupujte dle následujících kroků. Více informací o instalaci a nastavení služby Active Directory najdete v knize *Microsoft® Windows® 2000 Server Distribuované systémy* v části „Uložení dat služby Active Directory“.

► **Nastavení služby DNS a služby Active Directory**

1. Přihlaste se jako administrátor.
2. Zkontrolujte nastavení protokolu TCP/IP na vašem počítači, abyste se ujistili, že je nastaven k používání serveru DNS. Pokud je váš počítač první server DNS na síti, můžete nastavit svůj počítač, aby používal sám sebe jako server DNS.
3. Jestliže zatím není spuštěn průvodce Nastavení serveru Windows 2000, klepněte na Start, vyberte Programy a Nástroje pro správu a pak klepněte na Nastavení serveru.
4. K instalaci a nastavení služby Active Directory použijte průvodce Nastavení serveru Windows 2000. Průvodce Nastavení serveru Windows 2000 se vás zeptá na vlastní nastavení a pak spustí průvodce instalací služby Active Directory, který nainstaluje a nastaví službu Active Directory. Pokud je to nezbytné, průvodce instalací služby Active Directory vás také provede instalací a nastavením komponent serveru DNS.
5. Na požádání restartujte počítač.

Po spuštění průvodce instalací služby Active Directory budete možná potřebovat přidat delegaci v nadřazené zóně zóny, kterou jste vytvořili. Jestliže tento server je kořenový server DNS, není zde žádná nadřazená zóna, takže nemusíte přidávat žádnou delegaci. Nicméně pokud na síti jsou další servery DNS, delegaci přidat musíte.

► **Přidání delegace**

1. Lokalizujte zónu, kterou vytvořil průvodce instalací služby Active Directory. Tento průvodce automaticky vytvoří zónu se stejným názvem jako má doména Active Directory, kterou jste vytvořili.
2. Lokalizujte nadřazenou zónu této zóně.
3. Na nadřazené zóně přidejte delegaci.

Používání průvodce nastavením serveru DNS

Ve většině případů nepotřebujete ručně nastavovat službu DNS, aby podporovala službu Active Directory, ale můžete nechat službu DNS nainstalovat a nastavit službou Active Directory. Nicméně průvodce nastavením služby serveru DNS můžete použít k nastavení služby DNS, pokud chcete nastavit jiné než výchozí nastavení, které nastaví průvodce instalací služby Active Directory. Například můžete požadovat, aby server DNS byl odlišný od řadiče domény.

Zamýšlíte-li nastavit svůj server DNS pomocí průvodce nastavením serveru DNS, před jeho spuštěním proveďte následující:

- Není-li server DNS ještě instalován, nainstalujte ho.
- Pokud server nebude kořenovým serverem DNS, nastavte jeho síťová připojení tak, aby ukazovala na jeden nebo více serverů DNS na síti.

Po spuštění nebo po dokončení průvodce musíte vytvořit zónu dopředného vyhledávání, která je určující pro záznamy lokátoru, které přidá služba Netlogon.

Po dokončení nastavení serveru DNS pomocí průvodce musíte provést následující:

- Povolit dynamickou aktualizaci této zóny.
- Pokud toto není kořenová zóna, přidejte v nadřazené zóně delegaci nové zóně dopředného vyhledávání.
- Ujistěte se, že server, který bude řádit domény, má síťové připojení na tento server.

K nastavení serveru DNS, který neběží na řadiči domény, musíte být členem skupiny správců tohoto počítače.

K nastavení serveru DNS, který běží na řadiči domény, musíte být členem alespoň jedné skupiny zařazené v seznamu řízení přístupu (ACL) kontejneru Microsoft DNS ve službě Active Directory. Tato skupina musí mít také oprávnění plného řízení. Dle výchozího nastavení jsou v seznamu řízení přístupu (ACL) zařazeny následující skupiny:

- Správci DNS
- Správci domény
- Správci podnikové sítě

Před nastavením služby DNS ověřte, zda jsou nastavení klienta DNS správná.

► Ověření nastavení klientů DNS

1. Pravým tlačítkem klepněte na **Místa v síti** a pak klepněte na **Vlastnosti**.
2. Klepněte pravým tlačítkem na připojení, pro která chcete nastavit server DNS a pak klepněte na **Vlastnosti**.
3. Klepněte na **Protokol TC/IP** a pak klepněte na **Vlastnosti**.
4. Klepněte na stranu **Vlastnosti protokolu TCP/IP** a v poli **Preferovaný server DNS** vložte adresu IP existujícího serveru DNS. Můžete také do pole **Alternativní server DNS** přidat adresu IP alternativního serveru DNS.
5. Potřebujete-li specifikovat více než jeden alternativní server DNS, klepněte na příkaz **Upřesnit**, klepněte na záložku **Služba DNS** a vložte servery do okna **Adresy serverů DNS**.

Průvodce nastavením serveru DNS používá informace o klientovi DNS, aby určil, jestli na síti existují nějaké kořenové servery DNS. Více informací o nastavení adresy IP serveru DNS najdete v nápovědě Windows 2000 Server.

Před nastavením serveru musí být server DNS nainstalován. Server DNS nainstalujete a nastavíte následujícím postupem:

► Instalace serveru DNS

1. V Ovládacích panelech poklepejte na **Přidat nebo odebrat programy** a pak klepněte na **Přidat nebo odebrat součásti systému Windows**.
2. Klepněte na **Součásti** a pak klepněte na **Další**.

3. Klepněte na **Síťové služby** a pak klepněte na **Podrobnosti**.
4. Pokud není zatím vybráno pole **Služba DNS**, zaškrtněte ho a pak stiskněte **OK**.
5. Klepněte **Další**. Operační systém Windows 2000 nainstaluje službu DNS.
6. Klepněte **Dokončit**.

► **Nastavení serveru DNS**

1. V Ovládacích panelech poklepejte na **Nástroje pro správu** a pak klepněte na **Služba DNS**.
2. Pro rozšíření klepněte na server DNS.
3. Klepněte pravým tlačítkem na název serveru a z kontextového menu vyberte **Nastavení serveru**. Průvodce nastavením serveru DNS se spustí a provede vás procesem nastavení serveru DNS. V některých případech toto zahrnuje vytvoření zóny zpětného vyhledávání. Více informací o vytváření zóny zpětného vyhledávání najdete v části „Přidání zóny zpětného vyhledávání“.
4. Pokud již byla služba Active Directory nainstalována, můžete integrovat zónu do služby Active Directory. Informace o integraci zóny do služby Active Directory najdete v části „Integrace adresářové služby Active Directory a replikace Multimaster“.

Průvodce nastavením serveru DNS vás vyzve k zadání všech informací potřebných k vytvoření příslušných zón dopředného a zpětného vyhledávání.

Průvodce nastavením serveru DNS také upřednostní odkazy na kořenové servery a v případě potřeby vytvoří kořenovou zónu, stejně jako průvodce instalací služby Active Directory. Nicméně nevytvoří zónu zpětného vyhledávání, to musíte udělat později. Více informací o vytváření zón zpětného vyhledávání najdete v části „Přidání zóny zpětného vyhledávání“.

Vytváříte-li doménu Active Directory, musíte provést některá další nastavení.

► **Nastavení serveru DNS k podpoře služby Active Directory**

1. Ujistěte se, že máte zónu dopředného vyhledávání, která je určující pro záznamy prostředků registrované službou Netlogon.
2. Nastavte zónu dopředného vyhledávání tak, aby umožňovala dynamickou aktualizaci.
3. Pokud server DNS není kořenový server DNS, delegujte z nadřazené zóny zónu dopředného vyhledávání tomuto serveru.

Přidání zóny zpětného vyhledávání

Průvodce instalací služby Active Directory automaticky nepřidává zónu zpětného vyhledávání a záznamy prostředku PTR, protože je možné, že zónu zpětného vyhledávání řídí jiný server, například nadřazený server. Můžete chtít přidat na svůj server zónu zpětného vyhledávání, když žádné další servery neřídí zónu zpětného vyhledávání pro hostitele uvedené ve vaší zóně dopředného vyhledávání. Zóny zpětného vyhledávání a záznamy prostředku PTR nejsou pro fungování služby Active Directory nezbytné, ale potřebujete je, pokud chcete, aby klienti byli schopni přeložit názvy FQDN z adres IP. Záznamy prostředku PTR jsou také běžně používány některými aplikacemi k ověření totožnosti klientů.

Následující části vysvětlují, kam umístit zóny zpětného vyhledávání a jak je vytvářet, nastavovat a delegovat. Informace o jakýchkoli konceptech adresování IP projednávaných v následujících částech najdete v části „Úvod do TCP/IP“.

Plánování zón zpětného vyhledávání

K určení umístění zón zpětného vyhledávání nejprve sestavte seznam všech podsítí na síti a pak u každé podsítě proveďte třídu (A, B, C) a typ (třídivý nebo podsítový).

Ke zjednodušení správy vytvořte co nejméně zón zpětného vyhledání. Například máte-li pouze jeden identifikátor sítě třídy C (i když je vaše síť rozdělena do podsítí), je nejjednodušší umístit zóny zpětného vyhledávání podél hranic třídy C. Zónu zpětného vyhledávání a všechny záznamy prostředku PTR můžete přidat na existující server DNS na síti.

Poddomény nevyžadují vlastní zóny zpětného vyhledávání. Máte-li více identifikátorů sítě třídy C, můžete pro každý z nich nastavit na primárním serveru názvu nejbližším podsíti s identifikátorem sítě zónu zpětného vyhledávání a záznamy prostředků PTR.

Nicméně umístění zón zpětného vyhledávání podél hranic třídy C nemusí být vždy možné. Například pokud má vaše organizace malou síť, můžete obdržet od svého poskytovatele připojení k síti internet pouze část adresy třídy C. Tabulka 6.3 zobrazuje nastavení sítě s každým typem podsítě.

Tabulka 6.3 Plánování zón zpětného vyhledávání

Typ sítě	Doporučená akce	Najdete v části
Síť třídy A	Nastavte zónu zpětného vyhledávání na primárním serveru názvu domény nejvyšší úrovně.	„Nastavení standardní zóny zpětného vyhledávání“
Síť třídy B	Nastavte zónu zpětného vyhledávání na primárním serveru názvu domény nejvyšší úrovně.	„Nastavení standardní zóny zpětného vyhledávání“
Síť třídy C	Nastavte zónu zpětného vyhledávání na primárním serveru názvu domény nejvyšší úrovně.	„Nastavení standardní zóny zpětného vyhledávání“
Síť třídy A s podsítěmi	Rozdělte svou síť na síť třídy B nebo C.	„Nastavení standardní zóny zpětného vyhledávání“
Síť třídy B s podsítěmi	Rozdělte svou síť na síť třídy C.	„Nastavení standardní zóny zpětného vyhledávání“
Síť třídy C s podsítěmi, vlastník sítě třídy C spravuje zónu zpětného vyhledávání	Spolehněte se na to, že vlastník sítě třídy C bude spravovat zónu zpětného vyhledávání.	Neaplikovatelné.
Síť třídy C s podsítěmi, vlastník sítě třídy C delegoval zónu zpětného vyhledávání na vás	Nastavte beztřídovou zónu zpětného vyhledávání In-addr.arpa.	„Nastavení a delegace beztřídové zóny zpětného vyhledávání In-addr.arpa.“

Nastavení standardní zóny zpětného vyhledávání

Následující postupy popisují jak přidat zónu zpětného vyhledávání pro IP síť třídy C.

► Přidání zóny zpětného vyhledávání

1. V Ovládacích panelech poklepejte na **Nástroje pro správu** a pak poklepejte na příkaz **Služba DNS**.
2. Nepovinné – pokud server, kterému chcete přidat zónu zpětného vyhledávání, se neobjeví na seznamu, klepněte pravým tlačítkem na **Služba DNS**, klepněte na **Připojit se k počítači** a pak se řiďte pokyny k přidání požadovaného serveru.
3. Ke zobrazení zón klepněte na název serveru.
4. Klepněte pravým tlačítkem na složku **Zóny zpětného vyhledávání** a klepněte na **Nová zóna**. Objeví se průvodce nastavením zóny.

Klienti na platformě operačního systému Windows 2000 a servery DHCP pro Windows 2000 mohou automaticky přidávat záznamy prostředku PTR, nebo můžete nastavit záznamy prostředku PTR souběžně při vytváření záznamů prostředku A. Záznamy prostředku lze také přidat ručně.

► Přidání záznamů prostředku PTR

1. V Ovládacích panelech poklepejte na **Nástroje pro správu** a pak poklepejte na **Služba DNS**.
2. Ke zobrazení zón klepněte na název serveru.
3. Klepněte pravým tlačítkem na složku **Zóny zpětného vyhledávání**, vyberte **Nová** a vyberte **Ukazatel**.
4. K vytvoření záznamu prostředku PTR se řiďte zobrazeným návodem.

Poznámka: Nemůžete-li vybrat pole **Ukazatel**, protože je zašedlé, poklepejte na zónu.

Nastavení a delegace beztrídové zóny zpětného vyhledávání in-addr.arpa

Mnoho organizací dělí síť třídy C na menší části. Tento proces se označuje jako „vytváření podsítí“. Pokud jste vytvořili podsítě, můžete vytvořit odpovídající zóny zpětného vyhledávání podsítí, jak jsou specifikovány v dokumentu RFC 2317. Ačkoli je vaše síť rozdělena, nemusíte vytvářet odpovídající zóny zpětného vyhledávání podsítí, záleží to pouze na rozhodnutí správce. Servery DNS a zóny jsou nezávislé na podřízené infrastruktuře podsítí.

Nicméně v určitých situacích můžete chtít vytvořit a delegovat beztrídové zóny zpětného vyhledávání. Vlastníte-li adresu třídy C a chcete distribuovat adresy v rozsahu do několika různých skupin (například kanceláře poboček), ale nechcete spravovat zóny zpětného vyhledávání pro tyto adresy, vytvoříte beztrídové zóny zpětného vyhledávání a delegujete je těmto skupinám. Například předpokládejte, že poskytovatel připojení k síti internet má adresu třídy C a dal organizaci Reskit 62 adres. Poskytovatel připojení k síti internet může obsahovat záznamy v této zóně označující, že server názvů v organizaci Reskit má informace o této části oboru názvů. Reskit může spravovat tuto část oboru zahrnutím záznamů prostředků s přiřazením adresy IP k hostiteli, známé také jako beztrídová zóna zpětného vyhledávání in-addr.arpa.

Následující části vysvětlují syntaxi beztrídových zón zpětného vyhledávání a pomocí předcházejícího příkladu popisují, jak zóny zpětného vyhledávání delegovat a nastavovat.

vat. Více informací o delegování zón zpětného vyhledávání najdete na odkazu dokumentů RFC na stránce WWW Web Resources na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>. Hledejte dokument RFC 2317 „Classless in-addr.arpa delegation“.

Poznámka: Dynamická aktualizace u beztržidových zón in-addr.arpa nefunguje. Potřebujete-li dynamicky aktualizovat záznamy prostředku PTR, nepoužívejte beztržidové zóny.

Syntaxe beztržidové zóny zpětného vyhledávání in-addr.arpa

Ke specifikaci názvu beztržidové zóny zpětného vyhledávání in-addr.arpa můžete použít následující zápis:

<název podsítě>.<oktet>.<oktet>.<oktet>.in-addr.arpa

kde oktet určuje oktet rozsahu adresy IP. Oktety jsou určeny v opačném pořadí, než jak se objevují v adrese IP.

Přestože se název podsítě může skládat z jakýchkoli znaků povolených určujícím serverem DNS, nejobvykleji používané formáty zahrnují následující:

- *<minimální bodnota rozsahu podsítě><maximální bodnota rozsahu podsítě>*
- *<podsít'>/<počet bitů masky podsítě>*
- *<ID podsítě>*

Podsít' specifikuje segment adresy IP třídy C, který tato síť používá. Počet bitů masky podsítě specifikuje, kolik bitů používá síť pro svou masku podsítě. Identifikátor podsítě specifikuje název, který správce vybral pro tuto podsít'.

Například předpokládáte, že poskytovatel připojení k síti internet má adresu třídy C 192.168.100.0 a rozdělil tuto adresu na čtyři podsítě po 62 hostitelích na jednu síť, s maskou podsítě 255.255.255.192 a dal prvních 62 adres hostitelů společnosti s názvem DNS Reskit.com. Název beztržidové zóny zpětného vyhledávání může používat následující syntaxi:

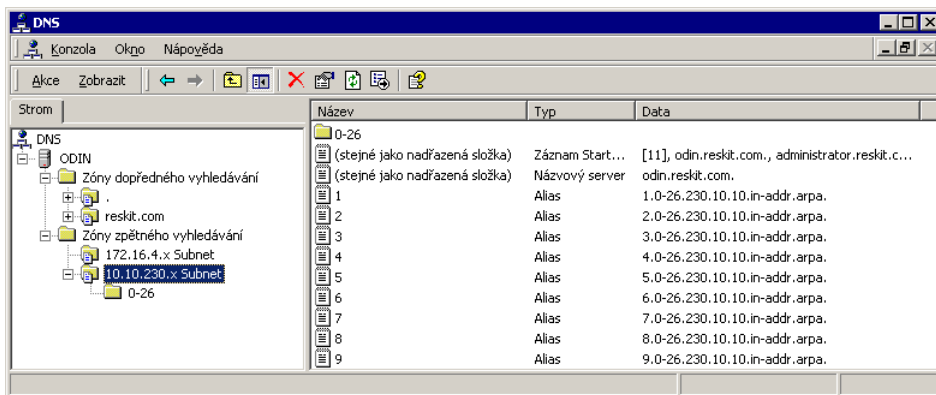
- 0-26.100.168.192.in-addr.arpa
- 0/26.100.168.192.in-addr.arpa
- Subnet1.100.168.192.in-addr.arpa

Ve službě DNS pro operační systém Windows 2000 můžete použít kteroukoli syntaxi vložením zón do textového souboru. Více informací o vytváření a delegaci zón zpětného vyhledávání v podsítích přes textové soubory najdete na stránce WWW Web Resource na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>. Hledejte fráze „zóna zpětného vyhledávání v podsítích“ a „Windows NT“ (resp. „subnetted reverse lookup zone“ a „Windows NT“).

Delegace beztržidové zóny zpětného vyhledávání

Nikdy není nutné delegovat beztržidovou zónu zpětného vyhledávání, a to ani v případě sítě s podsítěmi. Nicméně existuje několik případů, kdy možná budete chtít delegovat beztržidovou zónu zpětného vyhledávání. Například dáte-li spojené organizaci část své adresy třídy C, nebo máte-li vzdálenou síť s podsítěmi a chcete se vyhnout provozu posílání replikací nebo zónového přenosu přes rozsáhlou síť.

Obrázek 6.10 ukazuje, jak správce zóny zpětného vyhledávání třídy C by pak nastavoval server DNS.



Obrázek 6.10 Delegation zpětného vyhledávání

Beztržidové zóny zpětného vyhledávání můžete delegovat a vytvářet z konzoly DNS.

► Delegation beztržidové zóny zpětného vyhledávání

1. Na serveru DNS vaši domény vytvořte zónu zpětného vyhledávání.

U předcházejícího příkladu vytvořte zónu zpětného vyhledávání 100.168.192.in-addr.arpa. Zóna zpětného vyhledávání se přidá na serveru na doménu poskytovatel_připojení.com ne Reskit.com.

2. Klepněte pravým tlačítkem na zónu zpětného vyhledávání, kterou jste vytvořili, vyberte Nová delegace.
3. V průvodci novou delegací vložte název delegované domény a název a adresu IP delegovaného serveru názvů. V předcházejícím příkladě je delegovaná doména 0-26.
4. Klepněte pravým tlačítkem na zónu zpětného vyhledávání a klepněte na Nový alias.
5. Přidejte pro všechny delegované adresy záznamy CNAME.

Například pro adresu IP 192.168.100.5 vytvořte název CNAME 5, který ukazuje na 5.0-26.100.168.192.in-addr.arpa.

6. Vytvořte beztržidovou zónu zpětného vyhledávání v poddoméně pomocí postupu v následující části.

Nastavení beztržidové zóny zpětného vyhledávání In-addr.arpa

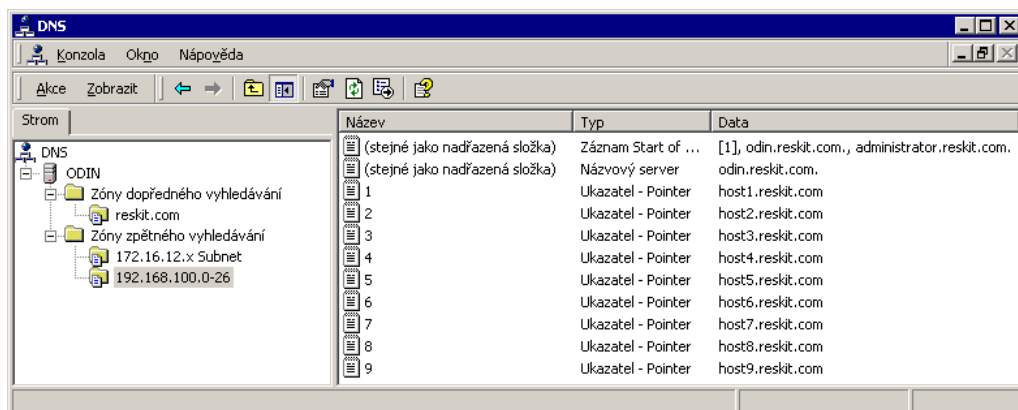
Pokud vám byla delegována nějaká beztržidová zóna zpětného vyhledávání, musíte ji nastavit. V předcházejícím příkladě správce poskytovatele připojení k síti internet delegoval zónu zpětného vyhledávání doméně Reskit.com a správce domény Reskit.com musí proto nastavit beztržidovou zónu zpětného vyhledávání. Obrázek 6.11 zobrazuje, jak by Reskit.com nastavila svou beztržidovou zónu zpětného vyhledávání.

► Vytváření beztržidové zóny zpětného vyhledávání

1. V konzole DNS klepněte na název serveru, tím zobrazíte podrobnosti o nastavení, klepněte pravým tlačítkem na složku **Zóny zpětného vyhledávání** a pak klepněte na **Vytvořit novou zónu**. Objeví se průvodce přidáním nové zóny.
2. Když dosáhnete stránky **Identifikátor sítě**, v poli nazvaném **Přímo vložit název zóny** vložte název beztržidové zóny zpětného vyhledávání.

Například napište **0-26.100.168.192.in-addr.arpa**.

Přidejte pak do této zóny všechny nezbytné záznamy prostředku PTR.



Obrázek 6.11 Beztřídová zóna zpětného vyhledávání

Integrace adresářové služby Active Directory a replikace Multimaster

Navíc k ukládání souborů zón na servery DNS můžete ukládat primární zónu do služby Active Directory. Je-li zóna uložena v Active Directory, údaje o zóně jsou uloženy jako objekty služby Active Directory a jsou replikovány jako součást replikace Active Directory.

Replikace služby Active Directory poskytuje výhodu oproti standardní službě DNS jako takové. Se standardní službou DNS může zónu upravit pouze primární server této zóny. S replikací Active Directory mohou zónu upravovat všechny řadiče domén a pak změny replikovat dalším řadičům domén. Tento replikační proces se nazývá replikace multimaster, protože zónu může aktualizovat více řadičů nebo hlavních serverů.

Přestože zóny integrované se službou Active Directory jsou přenášeny pomocí replikací Active Directory, můžete také provádět standardní přenosy na sekundární servery jako u standardních zón DNS.

Ukládání integrované se službou Active Directory poskytuje následující výhody:

Odolnost proti chybám Přestože stále můžete se zónami integrovanými se službou Active Directory provádět standardní přenosy, poskytuje replikace multimaster služby Active Directory vyšší odolnost proti chybám než používání samotných standardních zónových přenosů. Standardní zónové přenosy a aktualizace závisí na jednom primárním serveru DNS, který aktualizuje všechny sekundární servery. U replikací služby Active Directory není pouze jeden bod, na kterém závisí všechny aktualizace zón.

Zabezpečení Můžete omezit přístup k aktualizacím jakékoli zóny nebo záznamu a zabránit tak nezabezpečeným dynamickým aktualizacím. Více informací o nastavení za-

bezpečné dynamické aktualizace najdete v části „Dynamická aktualizace a zabezpečená dynamická aktualizace“.

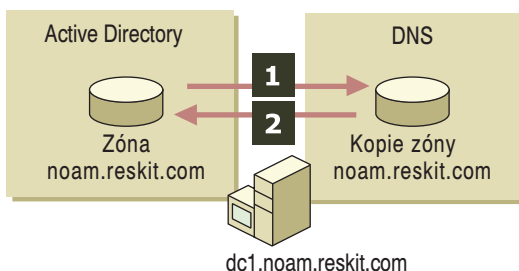
Jednodušší správa Vzhledem k tomu, že replikace provádí služba Active Directory, nepotřebujete pro servery DNS nastavovat a udržovat oddělenou topologii replikací (tedy zónových přenosů).

Efektivnější replikace rozsáhlých zón Služba Active Directory replikuje na základě vlastností, přičemž prosazuje pouze relevantní změny. To je efektivnější než úplný zónový přenos.

Integrované ukládání

Při nastavení primární zóny na zónu integrovanou se službou Active Directory je zóna uložena v Active Directory.

Obrázek 6.12 znázorňuje toto nastavení.



Obrázek 6.12 Zóna integrovaná se službou Active Directory

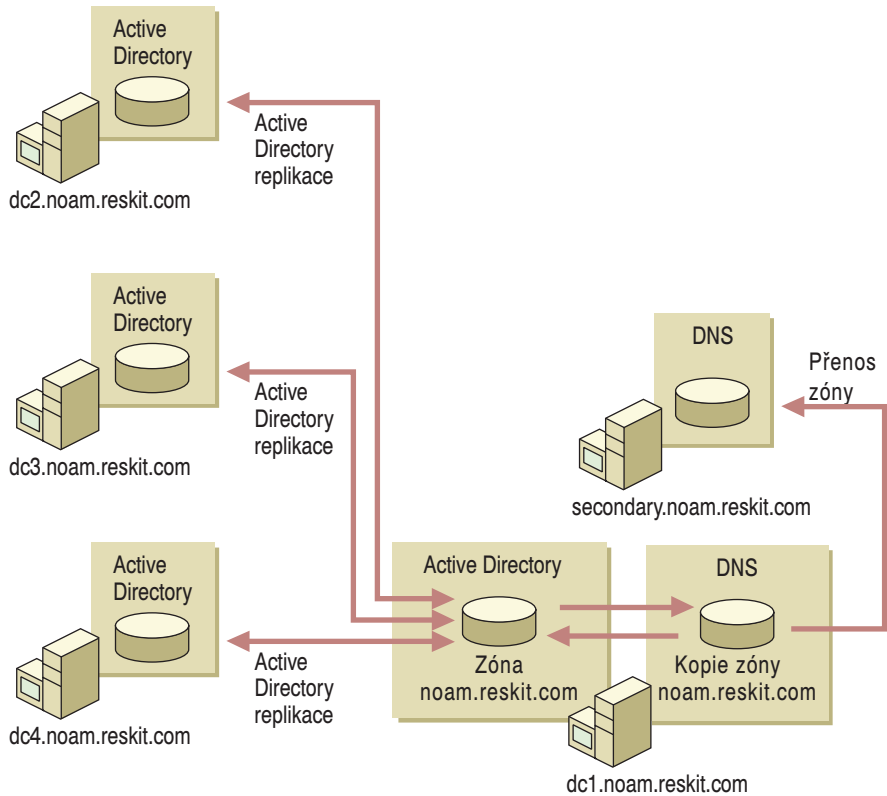
Součástí serveru DNS obsahuje pouze kopii zóny. Při spuštění načte kopii zóny ze služby Active Directory (krok 1). Pak, když server DNS obdrží nějakou změnu, zapíše tu to změnu do služby Active Directory (krok 2).

Prostřednictvím replikací služby Active Directory je zóna replikována na další řadiče domén. Také prostřednictvím standardního zónového přenosu může server DNS poslat svou kopii zóny na kterýkoli sekundární server DNS, který o to požádá. Server DNS může provádět jak přírůstkové, tak úplné zónové přenosy. Obrázek 6.13 zobrazuje, jak může být zóna replikována pomocí jak replikace služby Active Directory, tak standardního zónového přenosu.

Dle výchozího nastavení při spouštění server integrovaný se službou Active Directory kontroluje, jestli je dostupná služba Active Directory a jestli obsahuje nějaké zóny DNS. Pokud má služba Active Directory nějaké zóny, server DNS nahraje zóny z umístění specifikovaného nastavením hodnoty **Při spuštění nahrát data** na stránce vlastností serveru v rámci konzoly DNS. Server DNS může nahrát zóny z následujících umístění:

- Je-li hodnota **Při spuštění nahrát data** nastavena na **Z registru**, server DNS nahraje všechny soubory lokálních standardních zón a zón integrovaných se službou Active Directory specifikované v následujícím podklíči registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\DNS\Zones
```



Obrázek 6.13 Replikace a zónový přenos

- Je-li hodnota **Při spuštění nahrát data** nastavena na **Spustit ze souboru**, server DNS použije spouštěcí soubor stylu BIND k určení umístění souborů zóny.

Poznámka: Server DNS automaticky zapisuje v pravidelných intervalech zpět do spouštěcího souboru. Spouštěcí soubor můžete také aktualizovat klepnutím na server v konzole DNS a pak poklepáním na menu Akce a vybráním příkazu Aktualizovat datové soubory serveru. Případně můžete server zastavit a opět spustit, abyste aktualizovali spouštěcí soubor klepnutím pravého tlačítka na server v konzole DNS, vybráním Všechny úlohy v kontextovém menu a pak klepnutím na Restartovat.

- Je-li **Při spuštění nahrát data** nastaveno na **Ze služby Active Directory a registru** (dle výchozího nastavení), server DNS nahraje všechny zóny integrované se službou Active Directory i adresáři a všechny soubory lokálních standardních zón specifikovaných v registru. (Server DNS musí nahrát všechny soubory v adresáři, nemůžete nastavit server DNS tak, aby nahrál pouze některé zóny.)

Server DNS také nahraje soubory s odkazy na kořenové servery a s parametry serveru a zóny z různých umístění v závislosti na nastavení **Při spuštění nahrát data**. Tabulka 6.4 ukazuje umístění, ze kterých server DNS nahrává a do kterých zapisuje zóny, odkazy na kořenové servery a parametry serveru a zóny v závislosti na nastavení **Při spuštění nahrát data**.

Tabulka 6.4 Jak server DNS nahrává zóny, odkazy na kořenové servery a parametry serveru

	Při spuštění nahrát data: Spustit ze souboru	Při spuštění nahrát data: Spustit z registru	Při spuštění nahrát data: Spustit ze služby Active Directory a registru
Odkazy na kořenové servery načti z:	Ze souboru odkazů na kořenové servery	Je-li dostupný, ze souboru odkazů na kořenové servery. Jinak, pokud je dostupná služba Directory, která obsahuje odkazy na kořenové servery, z této služby.	Je-li dostupná adresářová služba, která obsahuje odkazy na kořenové servery, z adresářové služby. Jinak ze souboru odkazů na kořenové servery.
Odkazy na kořenové servery zapiš do:	Souboru odkazů na kořenové servery	Souboru odkazů na kořenové servery	Je-li dostupná adresářová služba, do adresářové služby
Zóny načti z:	Spouštěcího souboru	Registru	Adresářové služby (u zón integrovaných se službou Active Directory) a registru
Zóny zapiš do:	Spouštěcího souboru a registru	Registru a, je-li to zóna integrovaná se službou Active Directory, do adresářové služby	Registru a, je-li to zóna integrovaná se službou Active Directory, do adresářové služby
Parametry serveru a zóny načti z:	Spouštěcího souboru a registru	Registru a (u zón integrovaných se službou Active Directory) adresářové služby	Registru a (u zón integrovaných se službou Active Directory) adresářové služby
Parametry servery a zón zapiš do:	Spouštěcího souboru a registru	Registru (u všech zón) a (u zón integrovaných se službou Active Directory) adresářové služby	Registru (u všech zón) a (u zón integrovaných se službou Active Directory) adresářové služby

Změníte-li nastavení **Při spuštění nahrát data**, server DNS nejprve zapiše soubor odkazů na kořenové servery, zóny a parametry do umístění specifikovaných v původním nastavení **Při spuštění nahrát data** a pak je načte z nového nastavení.

Pokud server nahrál zóny integrované se službou Active Directory, pravidelně vyzývá službu Active Directory k poskytnutí změn těchto zón. Server také kontroluje přidání nových zón nebo odstranění zón existujících.

Server DNS může upravit službu Active Directory, jestliže správce provede změnu zóny nebo server je nastaven k přijímání dynamických aktualizací a dynamická aktualizace nastane. (Dynamická aktualizace je popsána dále v části „Dynamická aktualizace a zabezpečená dynamická aktualizace“.)

Servery DNS aktualizují službu Active Directory za použití následujícího postupu:

1. Když se objeví aktualizace, server DNS vyzve službu Active Directory k tomu, aby se ujistila, že kopie zóny uložená v paměti serveru DNS je aktuální. Pokud není, server DNS vyzve k předání všech změn a zapracuje tyto změny do kopie v paměti.

2. Dále server ověří, že všechny nutné podmínky jsou splněny. Nutné podmínky jsou podmínky, které musí být splněny před tím, než lze aktualizovat záznamy.
3. Nakonec pro přijetí změn aktualizuje data primární zóny ve službě Active Directory.

Umístění úložiště

Adresářová služba Active Directory je objektově orientovaná databáze, která organizuje prostředky sítě v hierarchické struktuře. Každý prostředek je reprezentován objektem.

Každý objekt má atributy, které definují jeho charakter.

Třídy objektů a atributy každého objektu jsou definovány ve schématu služby Active Directory.

Tabulka 6.5 zobrazuje objekty DNS ve službě Active Directory.

Tabulka 6.5 Objekty DNS ve službě Active Directory

Objekt	Popis
dnsZone	Kontejner vytvořený při uložení zóny ve službě Active Directory
dnsNode	List stromové struktury používaný k přiřazení a asociaci názvu v zóně k údajům o prostředku
dnsRecord	Vícehodnotový atribut objektu dnsNode používaný k ukládání záznamů prostředku asociovaných s objektem pojmenovaného uzlu
dnsProperty	Vícehodnotový atribut objektu dnsZone používaný k ukládání informací o nastavení zóny

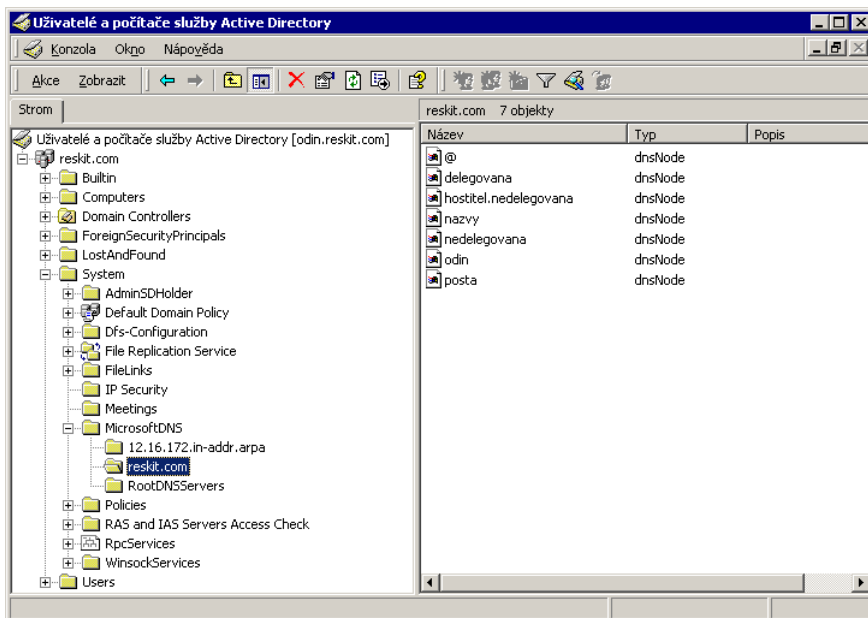
Obrázek 6.14 zobrazuje, jak jsou objekty DNS reprezentovány ve službě Active Directory.

V rámci kontejneru Microsoft DNS jsou umístěny objekty kontejneru dnsZone. Na obrázku 6.14 obsahuje Microsoft DNS následující objekty dnsZone:

- Zónu zpětného vyhledávání 72.16.172.in-addr.arpa
- Zónu dopředného vyhledávání reskit.com
- odkazy na kořenové servery RootDNSServers

Objekt kontejneru dnsZone obsahuje list stromové struktury dnsNode pro každý jedinečný název v zóně. Obrázek 6.14 zobrazuje následující objekty dnsNode v rámci objektu kontejneru dnsZone pro reskit.com:

- **@**, který označuje, že uzel má stejný název jako objekt dnsZone.
- **delegated**, delegovaná poddoména
- **host.notdelegated**, hostitel v doméně notdelegated.reskit.com, doméně, která je řízena zónou na reskit.com.
- **host1**, hostitel v doméně reskit.com.
- **mailserver**, poštovní server v doméně reskit.com.



Obrázek 6.14 Objekty DNS ve službě Active Directory

- **nameserver**, server názvů v doméně reskit.com.
- **nordelegated**, doména notdelgated.reskit.com, která je řízena zónou reskit.com.

List stromové struktury dnsNode má vícehodnotový atribut nazvaný dnsRecord s instancí hodnoty pro každý záznam spojený s názvem objektu. V tomto příkladě list stromové struktury dnsNode mailserver.reskit.com má atribut „A“ obsahující adresu IP.

Objekty DNS můžete prohlížet v rámci konzoly Uživatelé a počítače služby Active Directory.

► Prohlížení zón uložených ve službě Active Directory

1. Klepněte na **Start**, vyberte **Programy a Nástroje pro správu** a pak klepněte na položku **Uživatelé a počítače služby Active Directory**.
2. V menu **Prohlížet** klepněte na **Upřesnit vlastnosti**.
3. Ke zobrazení objektů dnsZone poklepejte na objekt Doména, objekt Systém a pak na objekt MicrosoftDNS.
4. Poklepejte na zónu, kterou si chcete prohlédnout.

Ačkoli si můžete objekty zón v součásti Uživatelé a počítače služby Active Directory prohlédnout, nemůže tato součást interpretovat hodnotu atributu dnsRecord. Chcete-li si prohlédnout hierarchii domén DNS a spojené záznamy, musíte tak učinit z konzoly DNS. Informace o konzole DNS najdete dříve v části „Nastavení služby DNS pro službu Active Directory“. Podobně, pokud chcete prohlížet zóny, můžete tak učinit pomocí nástroje Nslookup. Více informací o nástroji Nslookup najdete dále v části „Řešení problémů“.

Vytváření, převádění a odstraňování zón

Ve službě Active Directory můžete uchovávat jakékoli množství zón. Zóny uložené ve službě Active Directory se chovají jako zóny primární: může je upravit jakýkoli server DNS běžící na řadiči domény v doméně.

K uložení zóny ve službě Active Directory můžete buď vytvořit zónu integrovanou se službou Active Directory nebo převést primární nebo sekundární zónu na zónu integrovanou se službou Active Directory. Zóny integrované se službou Active Directory můžete také převést zpět na standardní primární nebo sekundární zóny. Tato část vysvětluje problémy, které je nutno zvážit při vytváření, převádění a odstraňování zón. Informace o vytváření, převádění a odstraňování zón najdete v nápovědě Windows 2000 Server.

Vytváření zóny integrované se službou Active Directory

Jakákoli zóna, kterou vytvoříte, je automaticky replikována na všechny řadiče domén v zóně. Z tohoto důvodu nevytvářejte stejnou zónu na více než jednom řadiči domény.

Upozornění: Vytvoříte-li zónu na jednom řadiči domény a pak vytvoříte stejnou zónu na jiném řadiči domény před tím, než služba Active Directory zónu zreplikovala, služba Active Directory zónu na prvním řadiči domény odstraní. Výsledkem je to, že ztratíte některé změny, které jste provedli na verzi zóny vytvořené na prvním řadiči domény.

Převedení standardní zóny na zónu integrovanou se službou Active Directory

Na zónu integrovanou se službou Active Directory můžete převést buď standardní primární nebo sekundární zónu. Integrujete-li zónu se službou Active Directory, zvažte následující problémy:

- Aby server DNS používal zónu integrovanou se službou Active Directory, musí tento server běžet na řadiči domény.
- Namůžete nahrát zóny integrované se službou Active Directory z jiných domén. Chcete-li, aby byl váš server DNS určující pro zónu integrovanou se službou Active Directory z jiné domény, může být pro takovou zónu pouze serverem sekundárním.
- Neexistuje nic takového jako sekundární zóna integrovaná se službou Active Directory. Uložíte-li zónu ve službě Active Directory, mohou tuto zónu aktualizovat všechny řadiče domén.
- Nemůžete mít najednou jak zónu integrovanou se službou Active Directory a standardní primární kopii stejné zóny.

Převádění zóny integrované se službou Active Directory na standardní zónu

Zónu integrovanou se službou Active Directory můžete převést buď na standardní primární nebo standardní sekundární zónu.

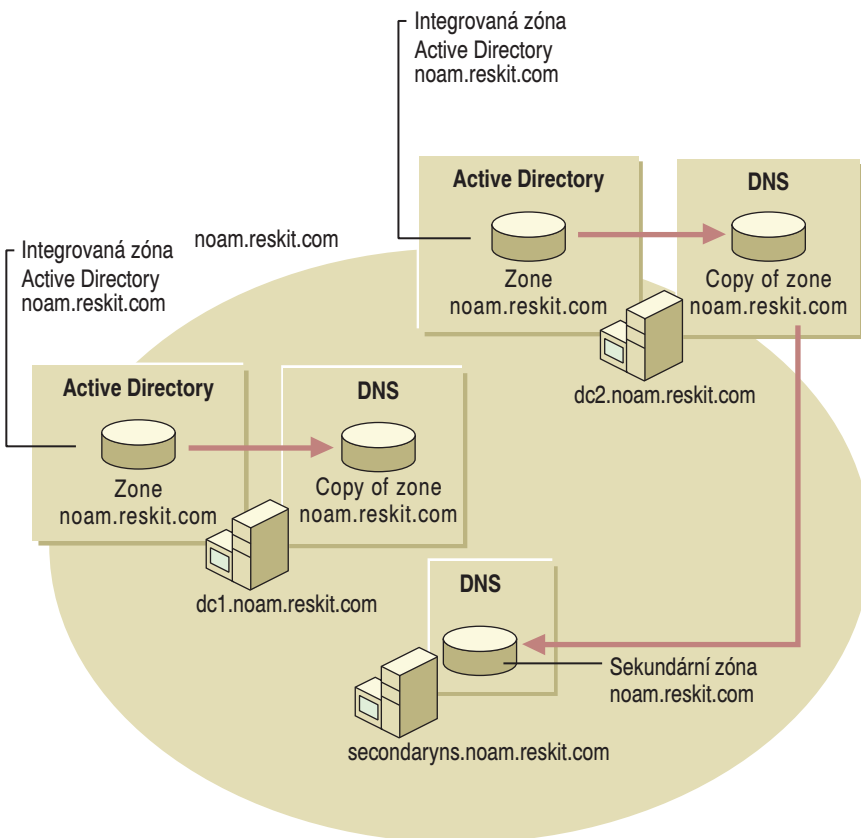
Převedete-li zónu integrovanou se službou Active Directory na standardní sekundární zónu, zóna se zkopíruje na server názvů, na kterém jste ji převáděli. Tento server nadále nenahrává zónu ze služby Active Directory, ale má vlastní sekundární kopi-

i této zóny. Požaduje zónové přenosy od kteréhokoli serveru určeného jako primární server zóny.

Převedete-li zónu integrovanou se službou Active Directory na standardní primární zónu, zóna se zkopíruje do standardního souboru na takovém serveru a odstraní se ze služby Active Directory. Zóna se nadále neobjevuje na dalších serverech DNS integrovaných se službou Active Directory.

Odstraňování zón

Odstraní-li zónu integrovanou se službou Active Directory z řadiče domény a **Při spuštění nahrát data** je nastaveno na **Registr**, konzole DNS se dotáže, jestli také chcete odstranit zónu ze služby Active Directory. Pokud klepnete na **Ano**, zóna se úplně odstraní ze služby Active Directory a není dostupná na žádném řadiči domény. Jestliže klepnete na **Ne**, zóna je odstraněna z registru, ale zůstává ve službě Active Directory. Je-li **Při spuštění nahrát data** na záložce **Upřesnit** na stránce vlastností serveru DNS v konzole DNS nastaveno na **Ze služby Active Directory a registru**, při příští výzvě adresáři o sdělení změn se zóna opět objeví. Pokud je **Při spuštění nahrát data** nastaveno na **Registr**, zóna se již znovu neobjeví.



Obrázek 6.15 Ukázka struktury domény

Odstraníte-li standardní sekundární zónu z řadiče domény, je obecně odstraněna z tohoto řadiče domény. Nicméně pokud existuje odpovídající zóna integrovaná se službou Active Directory, a máte server DNS nastaven na nahrávání dat při spuštění ze služby Active Directory a registru, zóna se znovu objeví jako primární zóna integrovaná se službou Active Directory. Zónu integrovanou se službou Active Directory pak můžete odstranit z počítače nebo ze služby Active Directory.

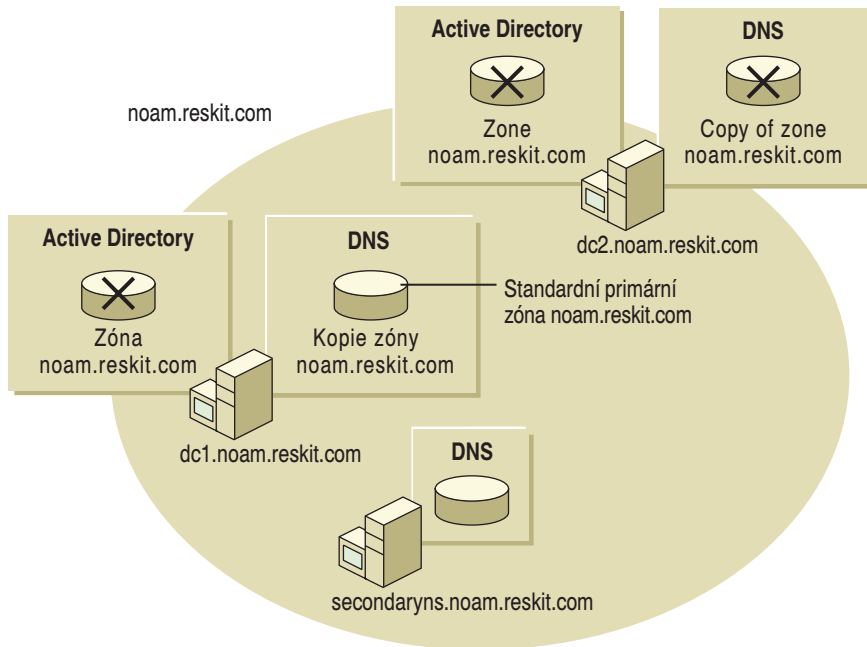
Vytváření sekundární kopie zóny integrované se službou Active Directory

Je možné zónu integrovat do služby Active Directory a pak přidat sekundární kopii této zóny na jiný server DNS. O vytvoření sekundární kopie zóny integrované se službou Active Directory můžete mít zájem například v případě, že máte vzdálené sídlo, ze kterého musí být vaši uživatelé schopni překládat názvy, ale nechcete zvýšit provoz na síti přidáním řadiče domény. Řešením je vytvoření sekundární kopie zóny.

Předcházení problémům při převádění nebo odstraňování zón

Při odstraňování zóny nebo převádění zóny integrované se službou Active Directory na standardní sekundární zónu můžete způsobit chyby nastavení. Například pokud odstraníte kopii zóny ze serveru a sekundární server je nastaven tak, že přebírá zónové přenosy z tohoto serveru, sekundární server nadále nebude schopen zónové přenosy převzít.

Jiný příklad – převádíte-li zónu integrovanou se službou Active Directory na standardní primární zónu, server DNS nahrávající novou primární zónu se stane jediným hlavním serverem této zóny. Proto služba Active Directory odebírá převedené zóny ze služby Active Directory, což znamená, že zóna je odstraněna ze všech řadičů domén.



Obrázek 6.16 Sekundární server bez synchronní kopie

To může způsobit problémy v některých nastaveních sekundárním serverům. Například předpokládejte, že doména noam.reskit.com má dva servery integrované se službou Active Directory – DC1.noam.reskit.com a DC2.noam.reskit.com. Doména má jeden sekundární server názvů, SecondaryNS.noam.reskit.com, který je sekundární kopií zóny pro noam.reskit.com a který ukazuje na DC2.noam.reskit.com jako na hlavní server zóny. Toto nastavení je znázorněno na obrázku 6.15.

Nyní předpokládejte, že se uživatel s odpovídajícími oprávněními přihlásí na server DC1.noam.reskit.com a převede zónu ze zóny integrované se službou Active Directory na standardní primární zónu. Jak je znázorněno na obrázku 6.16, server DC1.noam.reskit.com bude mít standardní primární zónu a server DC2.reskit.com nebude mít kopii této zóny. Přestože je zóna ze serveru DC2.noam.reskit.com odstraněna, server SecondaryNS.reskit.com stále ukazuje na server DC2.noam.reskit.com jako na hlavní server zóny a server SecondaryNS.reskit.com nemá žádnou šanci, jak pomocí zónových přenosů získat kopii zóny.

Abyste předešli tomuto problému, ujistěte se, že aktualizujete všechny sekundární servery zóny převáděné ze zóny integrované se službou Active Directory na standardní primární zónu.

Tento problém se objevuje pouze tehdy, když odstraňujete zónu ze serveru nebo převádíte zónu integrovanou se službou Active Directory na standardní primární zónu a sekundární server ukazuje na server, ze kterého byla zóna odstraněna. Problém se neobjeví, když převádíte zónu integrovanou se službou Active Directory na standardní sekundární zónu, protože převedení zóny integrované se službou Active Directory na standardní sekundární zónu neodstraňuje zónu z jakéhokoli serveru.

Replikace multimaster

Služba Active Directory podporuje *replikace multimaster*, což jsou replikace, v rámci kterých kterýkoli řadič domény může posílat nebo přijímat aktualizace informací uložených ve službě Active Directory. Zpracování replikací probíhá na základě jednotlivých vlastností, což znamená, že jsou šířeny pouze relevantní změny. Zpracování replikací se liší od úplných zónových přenosů DNS, ve kterých jsou šířeny celé zóny. Zpracování replikací se liší také od přírůstkových zónových přenosů DNS, ve kterých jsou šířeny všechny změny od poslední změny. U replikací služby Active Directory je posílán pouze konečný výsledek všech změn záznamu.

Uchovávejte-li primární zónu ve službě Active Directory, informace o zóně jsou replikovány všem řadičům domén v rámci domény Active Directory. Každý server DNS běžící na řadiči domény je pak určující pro tuto zónu a může ji aktualizovat.

Kolize názvů

Vzhledem k tomu, že všechny řadiče domén mohou provádět změny na stejné zóně, je možné, aby někdo aktualizoval vlastnost objektu služby Active Directory na jednom řadiči domény, zatímco někdo jiný bude současně (nebo takřka současně) aktualizovat stejnou vlastnost na jiném řadiči domény, čímž dojde k nekonzistenci vlastnosti jednoho řadiče domény se stejnou vlastností druhého řadiče. Nastane-li změna na druhém řadiči domény před rozšířením změny z repliky prvního serveru, nastane *kolize replikací*.

Kolize replikací může ovlivnit zóny integrované se službou Active Directory. Předpokládejte, že v rámci jedné domény a na dvou řadičích domény je souběžně vytvořen stejný název. Změny se replikují a služba Active Directory zjistí, že existují dva objekty dnsNode, které mají stejný název. Aby tento problém vyřešil, podsystém replikací

služby Active Directory změni název objektu, který byl vytvořen jako první, přidáním zvláštního znaku a globálně jedinečného identifikátoru (GUID) k názvu. Identifikátor GUID je jedinečné 128bitové číslo, které služba Active Directory spojí s objektem, aby byl objekt jedinečný. To odliší název objektu, takže ony dva objekty mají různé názvy. Při příštím převzetí změn serverem DNS ze služby Active Directory server DNS odstraní kopii objektu hostitele s identifikátorem GUID, takže služba DNS akceptuje poslední vytvořený název.

Pokud souběžně upravujete objekt názvu na dvou různých replikách serverů, musí služba Active Directory rozhodnout, která ze změn (hodnota atributu) bude přijata a která bude zahozena. Služba Active Directory proto vybírá hodnotu atributu, která má nejvyšší číslo verze. Jsou-li čísla verze stejná, služba Active Directory vybere hodnotu atributu, která má nejnovější časové razítko. Takže služba Active Directory přijme druhou změnu. Více informací o kolizích replikací najdete v knize *Microsoft® Windows® 2000 Server Distribuované systémy* v části „Replikace služby Active Directory“.

Vyvolání okamžité replikace

Při nastavování služby DNS nebo řešení problémů s replikami nemusíte chtít čekat na normální replikační cyklus. V takovém případě můžete vyvolat okamžitou replikaci. Nezapomínejte na to, že výkon vaší sítě ovlivňuje to, jak dlouho trvá aktualizace cílového řadiče domény.

► Způsobení okamžité replikace

1. Klepněte na **Start**, vyberte **Programy**, vyberte **Nástroje pro správu** a pak klepněte na **Správce sídel a služeb Active Directory**.
2. Poklepejte na ikonu **Sídla** a rozšířte ji.
Zobrazí se všechny sídla, včetně prvního sídla označeného **Výchozí název prvního sídla**, a všech dalších sídel, která byla nastavena ručně.
3. Poklepejte na vybrané sídlo.
4. U vybraného sídla poklepejte na ikonu **Servery** a pak rozšířte ikonu počítače.
Zobrazí se ikona **Nastavení NTDS**.
5. Klepněte na ikonu **Nastavení NTDS**.
V pravé polovině je jeden nebo více objektů. Jedním z těchto objektů je připojení na řadič domény, na kterém chcete vyvolat okamžitou replikaci.
6. Klepněte pravým tlačítkem na objekt, který se připojuje na řadič domény, na kterém chcete vyvolat okamžitou replikaci, a pak klepněte na **Replikovat**.

Dynamická aktualizace a zabezpečená dynamická aktualizace

Operační systém Windows 2000 podporuje jak dynamickou aktualizaci, definovanou v dokumentu RFC 2136, tak zabezpečenou dynamickou aktualizaci, definovanou v dokumentu návrhu internetu IETF „Algoritmus GSS pro TSIG (GSS-TSIG)“.

U dynamické aktualizace mohou klienti automaticky posílat aktualizace na server názvů, který je určující pro záznam, jež klienti zamýšlejí změnit. Oprávněný server názvů pak zkontroluje, že jsou splněny určité nezbytně nutné podmínky. Nutné podmínky jsou záznamy prostředků, které musí nebo naopak nesmí být přítomny před aktualizací záznamů. Více informací o nutných podmínkách najdete v části „Úvod do služby

DNS“. Jsou-li nutné podmínky splněny, určující server názvů provede změnu. Změnou může být přidávání záznamů, odstraňování záznamů nebo upravování záznamů.

Poznámka: Dynamickou aktualizaci mohou zasílat jak klienti, tak servery.

Dynamická aktualizace poskytuje následující výhody:

- Umožňuje klientům, včetně klientů DHCP, dynamicky registrovat záznamy prostředků na primárním serveru. To snižuje prostředky správy potřebné k ruční správě těchto záznamů.
- Umožňuje serverům DHCP registrovat jménem klientů DHCP záznamy prostředku A a PTR. To snižuje čas potřebný k ruční správě těchto záznamů a poskytuje podporu klientům DHCP, kteří nemohou provádět dynamickou aktualizaci.
- Zjednodušuje nastavení služby Active Directory umožněním dynamické registrace řadičů domén pomocí záznamů SRV.

Zabezpečená dynamická aktualizace funguje jako dynamická aktualizace s následující výjimkou: oprávněný server názvů přijímá aktualizace jen od klientů a serverů, které jsou oprávněné provádět dynamickou aktualizaci objektů `dnsZone` a `dnsNode`.

Zabezpečená dynamická aktualizace poskytuje následující výhody:

- Chrání zóny a záznamy prostředků od úpravy uživateli bez oprávnění.
- Umožňuje specifikovat přesně uživatele a skupiny, kteří mohou upravovat zóny a záznamy prostředků.

Poznámka: Pro dynamickou aktualizaci lze nastavit jakoukoli primární zónu. Nicméně pro zabezpečenou dynamickou aktualizaci lze nastavit pouze zóny integrované se službou Active Directory.

Dle výchozího nastavení klient s dynamickou aktualizací se snaží nejdříve o dynamickou aktualizaci a v případě, že ta selže, vyjednává zabezpečenou dynamickou aktualizaci. Nicméně klienta můžete nastavit tak, aby se vždy pokoušel o nezabezpečenou dynamickou aktualizaci nebo vždy o zabezpečenou dynamickou aktualizaci, přidáním záznamu `UpdateSecurityLevel` do registru do podklíče:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\Tcpip\Parameters
```

Hodnota podklíče **UpdateSecurityLevel** může být nastavena na desítkové hodnoty 0, 16 nebo 256, které nastavují zabezpečení následujícím způsobem:

- 256. Určuje použití pouze zabezpečené dynamické aktualizace.
- 16. Určuje použití pouze nezabezpečené dynamické aktualizace.
- 0. Určuje použití zabezpečené dynamické aktualizace, když je zamítnuta nezabezpečená dynamická aktualizace. Toto je přednastavená hodnota.

Upozornění: Zakázete-li zabezpečenou dynamickou aktualizaci, klient nemůže provádět aktualizace na zónách, které jsou nastaveny pro zabezpečenou dynamickou aktualizaci. Také, pokud nastavujete zónu pro používání zabezpečené dynamické aktualizace, Ujistěte se, že servery DHCP aktualizující záznamy v dané zóně nejsou nainstalovány na řadičích domény. Jinak server DHCP, který provádí registraci záznamů prostředku A jménem svých klientů, může převzít vlastnictví názvů, které náležejí počítačům registrujícím vlastní záznamy.

Dynamická aktualizace

Tato část popisuje implementaci dynamické aktualizace do operačního systému Windows 2000. Informace o standardu dynamické aktualizace specifikované v dokumentu RFC 2136 najdete v části „Úvod do služby DNS“.

Poznámka: Dynamická aktualizace může být posílána jménem různých služeb, například klienta DHCP, serveru DHCP, Netlogon a clusterových služeb. Následující části popisují pouze dynamické aktualizace prováděné klientem a serverem DHCP.

V operačním systému Windows 2000 mohou klienti posílat dynamické aktualizace na tři různé typy síťových adaptérů: adaptéry DHCP, staticky nastavované adaptéry a adaptéry vzdáleného přístupu. Nezávisle na tom, který adaptér je použit, posílá služba klienta DHCP dynamické aktualizace na určující server DNS. Služba klienta DHCP běží na všech počítačích nezávisle na tom, jestli jsou nastaveny jako klienti DHCP.

Dle výchozího nastavení klient s dynamickou aktualizací dynamicky registruje své záznamy prostředku A a případně všechny své záznamy prostředku PTR každých 24 hodin nebo kdykoli nastane jakákoli z následujících událostí:

- Změní se nastavení protokolu TCP/IP.
- Obnoví se adresa DHCP nebo je získána nová zápůjčka adresy DHCP.
- Nastane událost Plug and Play.
- Počítači je přidána nebo odebrána adresa IP, když uživatel mění nebo přidává adresu IP statickému adaptéru. (Uživatel nepotřebuje restartovat počítač klienta s dynamickou aktualizací kvůli registraci přiřazení názvu na adresu IP.)

Dle výchozího nastavení klient s dynamickou aktualizací automaticky odregistruje přiřazení názvu adresy IP při každém vypršení doby zápůjčky DHCP. Můžete klienta nastavit tak, aby neregistroval svůj název a adresu IP ve službě DNS. Nastavíte-li klienta tak, že automaticky neregistruje přiřazení názvu adresy IP a server DHCP běží pod operačním systémem Windows 2000 a je nastaven k registraci záznamů prostředku DNS jménem klientů, kteří běží pod dřívějšími verzemi operačního systému než Windows 2000, server DHCP se snaží namísto toho aktualizovat přiřazení.

► Zabránění klientovi v registraci přiřazení názvu adresy IP

1. V Ovládacích panelech poklepejte na ikonu **Sít**.
2. Klepněte pravým tlačítkem na ikonu pro připojení, na kterém chcete zakázat registraci přiřazení názvu adresy IP a pak klepněte na **Vlastnosti**.
3. Klepněte na **Protokol TCP/IP** a pak klepněte na **Vlastnosti**.
4. Klepněte na **Upřesnit** a pak klepněte na záložku **Služba DNS**.
5. Odstraňte zaškrtnutí v poli **Registrovat adresu tohoto připojení v DNS**.

Můžete prosadit opětovnou registraci pomocí nástroje z příkazové řádky Ipconfig. U klientů na platformě operačního systému Windows 2000 napište na příkazové řádce následující příkaz:

ipconfig /registerdns

U klientů na platformě operačního systému Windows NT 4.0 napište na příkazové řádce následující příkaz:

ipconfig /release
ipconfig /renew

U klientů na platformě operačního systému Microsoft® Windows® 98 a Microsoft® Windows® 95 napište na příkazové řádce následující příkaz:

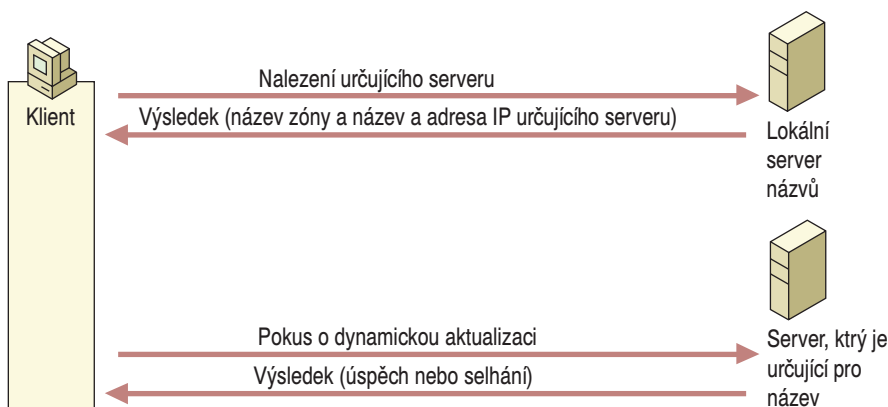
winipcfg /renew

Proces dynamické aktualizace

Při dynamické aktualizaci nastávají tyto události:

1. Klient žádá svůj lokální server názvů (za použití procesu popsaného dříve v části „Dotazy DNS“) o nalezení primárního serveru názvů a zóny, které jsou určující pro název, který je aktualizován. Lokální server názvů pak provádí standardní proces překladu názvu k objevení primárního serveru názvů, který je určující pro název. (Lokální server názvů může být také serverem, který je určující pro tento název.) Pak odpoví názvem určujícího serveru a zóny.
2. Klient pošle požadavek na dynamickou aktualizaci primárnímu serveru, který je určující pro danou zónu. Požadavek o dynamickou aktualizaci může zahrnovat seznam nutných podmínek, které musí být před aktualizací splněny. Určující server pak zahájí proces dynamické aktualizace. (Informace o tom, co se stane, je-li zóna nastavena na zabezpečenou dynamickou aktualizaci, najdete dále v části „Dynamická aktualizace a zabezpečená dynamická aktualizace“.) Určující server pak zkontroluje, jestli jsou splněny nutné podmínky. Pokud ano, server provede aktualizaci a pak odpoví klientovi.

Obrázek 6.17 znázorňuje typický proces dynamické aktualizace.



Obrázek 6.17 Proces dynamické aktualizace

Aktualizace může být neúspěšná z následujících důvodů:

- Primární server, který je určující pro daný název, neodpovídá.

Primární server nemusí odpovídat, pokud je mimo provoz nebo pokud lokální server názvů má ve svých záznamech prostředku SOA nesprávný nebo zastaralý server názvů. Servery DNS se standardními zónami (včetně sekundárních serverů pro zóny integrované se službou Active Directory) mohou působit problémy odesláním nesprávných nebo zastaralých záznamů SOA, když klienti s dynamickou aktualizací o záznamy SOA žádají. Nicméně servery DNS se zónami integrovanými se službou Active Directory vždy zahrnují své názvy do záznamů SOA, takže servery DNS se zónami integrovanými se službou Active Directory nepošílají nesprávné nebo zastaralé záznamy SOA.

Pokud primární server neodpovídá, ale zóna je replikována prostřednictvím replikace multimaster, klient se snaží o registraci názvu u jiných primárních serverů DNS, které jsou pro daný název určující.

Pokud aktualizace selže kvůli nedostupnosti serveru, klient zaprotokoluje zápis do protokolu událostí, který si můžete prohlédnout pomocí Prohlížeče událostí. Můžete také nastavit protokol serveru, Dns.log, tak, aby zobrazil případná selhání. Více informací o Prohlížeči událostí najdete dále v části „Řešení problémů“.

- Server nepřijímá dynamické aktualizace, protože zóna je právě přenášena.
- Server přijímá pouze zabezpečené dynamické aktualizace a nezabezpečená dynamická aktualizace selhala.

Více informací o zabezpečené dynamické aktualizaci najdete dále v části „Dynamická aktualizace a zabezpečená dynamická aktualizace“.

- Nebyly splněny nutné podmínky. Například klient s dynamickou aktualizací se může pokoušet o aktualizaci názvu, pro který momentálně neexistuje žádný záznam.

Následující části popisují proces dynamické aktualizace pro adaptéry nastavované službou DHCP, staticky nastavované adaptéry (adaptéry, jejichž adresy IP ručně vložili uživatelé nebo správci) a adaptéry vzdáleného přístupu.

Klienti a servery DHCP

Klienti služby DHCP na platformě Windows 2000 respektují dynamickou aktualizaci a mohou iniciovat proces dynamické aktualizace. Klient DHCP vyjednává o procesu dynamické aktualizace se serverem DHCP, když klient si zapůjčí adresu IP nebo obnoví svou zápůjčku, přičemž určí, který počítač bude aktualizovat záznamy prostředku A a PTR klienta u názvů FQDN (které mohou obsahovat zvláštní příponu DNS pro připojení). V závislosti na procesu vyjednávání klient DHCP, server DHCP nebo oba, aktualizují záznamy odesláním požadavku na dynamickou aktualizaci primárnímu serveru DNS, který je určující pro daný název, který má být aktualizován.

Klienti a servery, které mají dřívější verze operačního systému Windows než Windows 2000, dynamickou aktualizaci nepodporují. Nicméně servery DHCP na platformě Windows 2000 mohou provádět dynamickou aktualizaci jménem klientů, kteří nepodporují možnost názvu FQDN (která je popsána v následující části). například klienti s operačním systémem Windows 95, Windows 98 a Windows NT nepodporují možnost názvu FQDN. K povolení této funkcionality vyberte na záložce **Služba DNS** vlastnostech serveru pro konzolu DNS možnost **Povolit aktualizaci pro klienty DNS nepodporující dynamickou aktualizaci**. Server DHCP nejdříve obdrží název původních klientů z paketu DHCPRequest. Pak připojí název domény daný pro tento obor a zaregistruje záznamy prostředku A a PTR.

Informace o tom, jak je implementováno zabezpečení pro klienty nepodporující možnost názvu FQDN prostřednictvím zabezpečené dynamické aktualizace, najdete dále v části „Dynamická aktualizace a zabezpečená dynamická aktualizace“.

V některých případech se mohou po vypršení zápůjčky klienta DHCP na serverech DNS objevit zastaralé záznamy prostředku A nebo PTR. Například když se klient DHCP v operačním systému Windows 2000 pokouší o vyjednání procesu dynamické aktualizace se serverem DHCP v operačním systému Windows NT 4.0, klient DHCP v operačním systému Windows 2000 musí zaregistrovat jak záznamy prostředku A, tak záznamy prostředku PTR. Později, pokud je klient DHCP v operačním systému Windows 2000

nesprávně odejmut ze sítě, klient nemůže odregistrovat své záznamy prostředku A a PTR, proto zastarají.

Pokud se v zóně, která umožňuje pouze dynamickou aktualizaci, objeví zastaralý záznam prostředku A, žádná osoba nebo počítač nemůže použít název v tomto záznamu prostředku A.

K zabránění problémům se zastaralými záznamy prostředku PTR a A můžete povolit vlastnost stárnutí a čištění paměti záznamů zastaralých názvů. Více informací o vlastnosti stárnutí a čištění paměti záznamů zastaralých názvů najdete dále v části „Stárnutí a úklid paměti záznamů zastaralých názvů“.

K poskytnutí odolnosti proti chybám zvažte integraci se službou Active Directory u těch zón, které akceptují dynamické aktualizace od klientů na platformě Windows 2000. Chcete-li zrychlit zjišťování určujících serverů, můžete nastavit u každého klienta seznam preferovaných a alternativních serverů, které jsou určující pro takovou zónu integrovanou se službou Active Directory. Pokud selže aktualizace klienta z preferovaného serveru kvůli jeho nedostupnosti, může klient vyzkoušet alternativní server. Když se preferovaný server zpřístupní, nahraje aktualizovanou zónu integrovanou se službou Active Directory, která zahrnuje aktualizaci od klienta.

Proces dynamické aktualizace u adaptérů nastavovaných službou DHCP

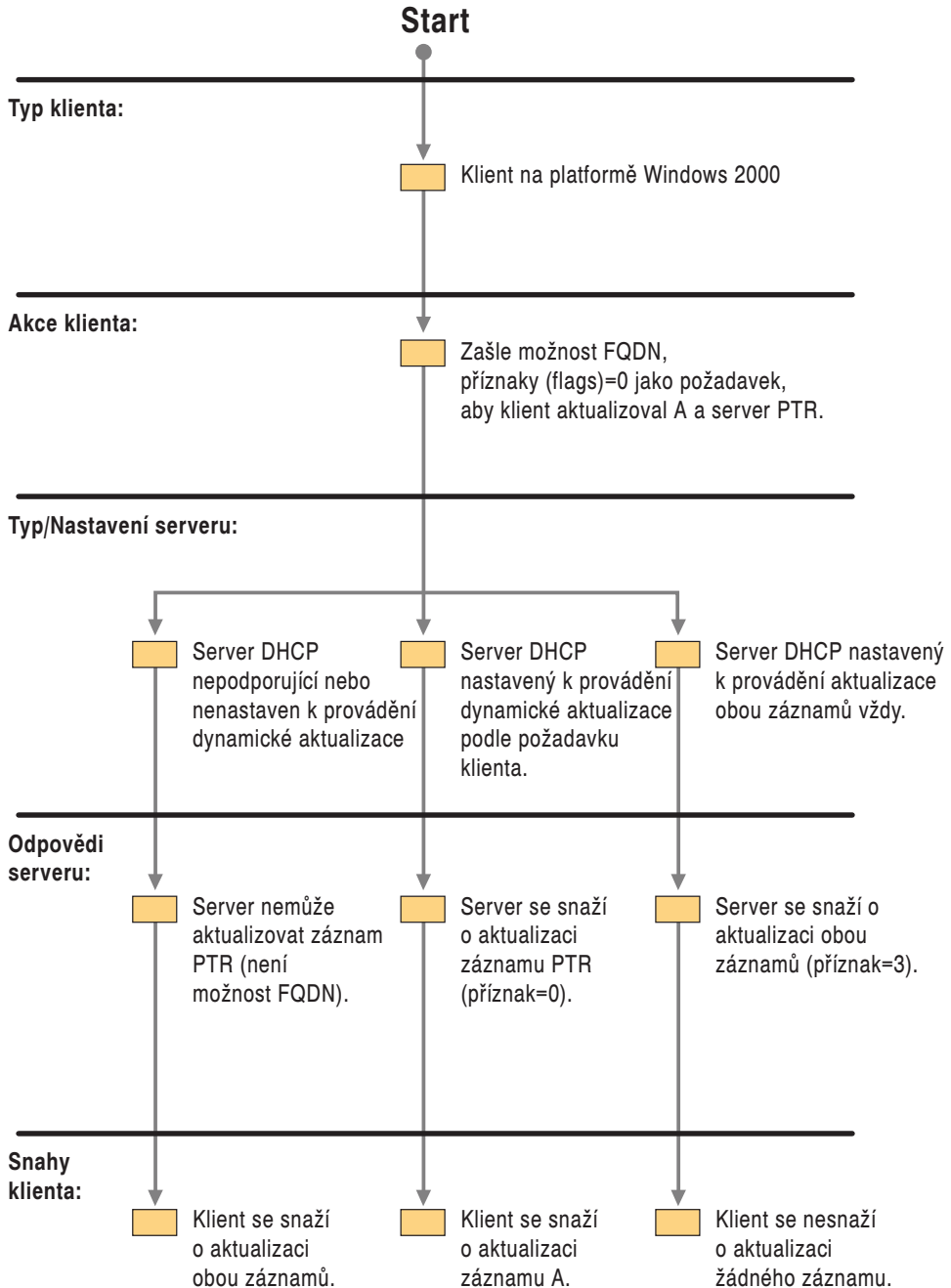
K vyjednání procesu dynamické aktualizace posílá klient DHCP název FQDN na server DHCP v paketu požadavku DHCPRequest za použití možnosti FQDN. Server pak odpoví klientovi DHCP odesláním zprávy DHCPACK za použití možnosti FQDN.

Tabulka 6.6 obsahuje pole možnosti FQDN paketu DHCPRequest.

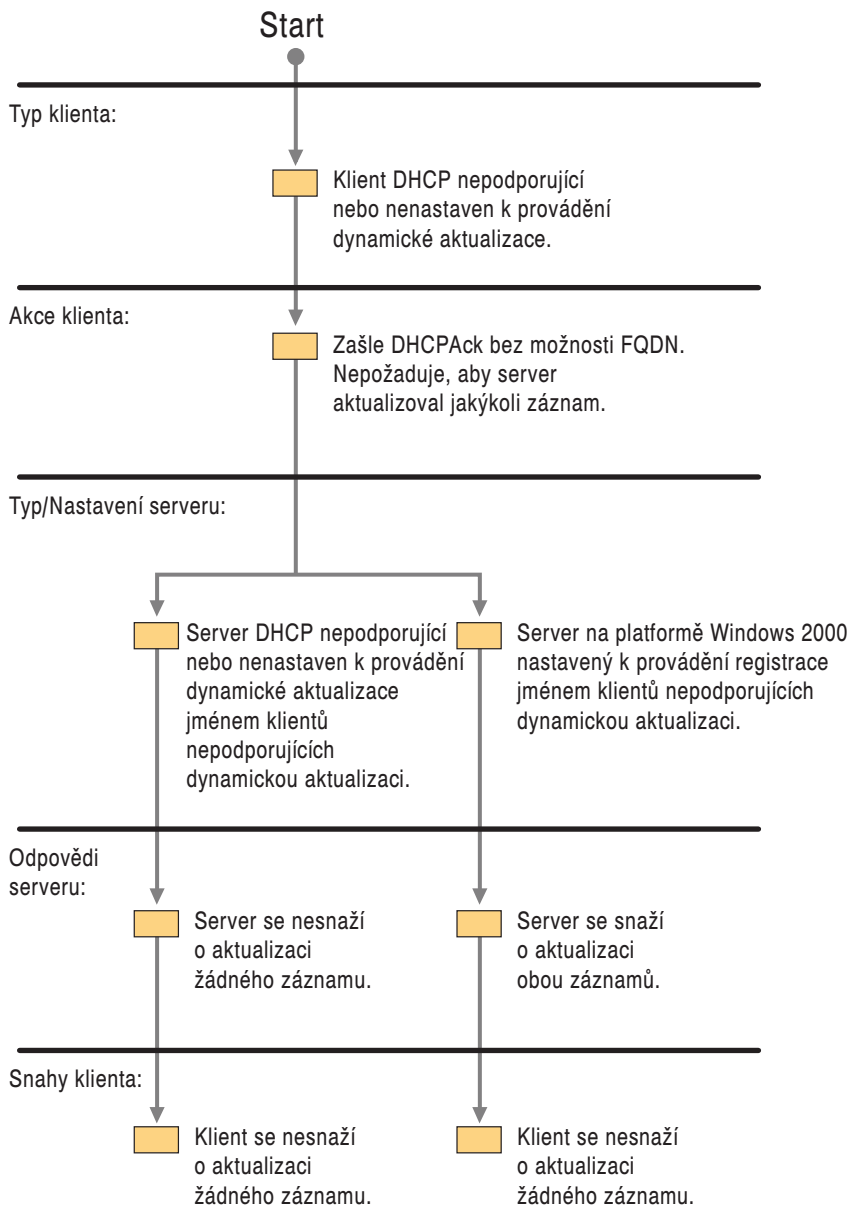
Tabulka 6.6 Pole možnosti FQDN paketu DHCPRequest

Pole	Význam
Kód	Určuje kód této možnosti (81).
Délka	Určuje délku této možnosti (minimálně 4).
Příznak	Může být jednou z následujících hodnot: <ul style="list-style-type: none"> 0. Klient chce zaregistrovat záznam prostředku A a požaduje aktualizaci záznamu prostředku PTR serverem. 1. Klient chce, aby server zaregistroval záznamy prostředku A a PTR. 3. Server DHCP registruje záznamy prostředku A a PTR bez závislosti na požadavku klienta.
RCODE1 a RCODE2	Server DHCP používá tato pole k určení kódu odpovědi z registrace záznamu prostředku A prováděného jménem klienta a k označení, jestli se pokusil o aktualizaci před odesláním paketu DHCPACK.
Název domény	Určuje název FQDN klienta.

Jak vidíte na obrázcích 6.18 a 6.19, podmínky, za kterých klienti DHCP posílají možnost FQDN a akce vykonané servery DHCP závisí na operačním systému klienta a serveru a na jejich nastavení.



Obrázek 6.18 Klient na platformě Windows 2000



Obrázek 6.19 Klient, který neprovádí dynamické aktualizace

To, jestli klient požaduje dynamickou aktualizaci, závisí na tom, zda pracuje pod operačním systémem Windows 2000 nebo jinou verzí operačního systému Windows a na tom, jestli a jak je klient nastaven. Klienti mohou provádět následující akce:

1. Dle výchozího nastavení klienti na platformě Windows 2000 zasílají možnost FQDN s polem příznaku nastaveným na 0 – tím požadují, aby klient aktualizoval záznam prostředku A a server DHCP záznamy prostředku PTR. PO požadavku

o aktualizaci čeká klient na odpověď od serveru DHCP. Pokud server DHCP nenastaví pole příznaku na 3, klient se pokusí o registraci záznamů prostředku A a PTR.

2. Klienti DHCP na dřívějších verzích operačního systému Windows než je Windows 2000 a klienti DHCP pro operační systém Windows 2000, kteří jsou nastaveni k neregistrování záznamů prostředku DNS nepošílají možnost FQDN. V tomto případě se klient nepokouší aktualizovat jakýkoli záznam.

V závislosti na požadavku klienta server může provádět různé akce. Pokud klient DHCP pošle zprávu DHCPRequest bez možnosti FQDN, závisí následující události na typu serveru a na jeho nastavení. Server může nicméně aktualizovat oba záznamy. Server tak učiní, pokud je nastaven k aktualizování záznamů jménem klientů, kteří nepodporují možnost FQDN.

Případně server nemusí udělat nic. Server nic neudělá v následujících případech:

1. Server nepodporuje dynamickou aktualizaci (například server s operačním systémem Windows NT 4.0).
2. Server běží pod operačním systémem Windows 2000 a je nastaven tak, aby dynamickou aktualizaci neprováděl u klientů, kteří možnost FQDN nepodporují.
3. Server běží pod operačním systémem Windows 2000 a je nastaven tak, aby neregistroval záznamy prostředku DNS.

Jestliže klient DHCP na platformě operačního systému Windows 2000 požaduje, aby server aktualizoval záznamy prostředku PTR, ale nikoli záznamy prostředku A, závisí následující události na typu serveru a jeho nastavení. Server může provést kteroukoli z následujících akcí:

1. Jestliže server běží buď pod operačním systémem Windows NT 4.0 nebo Windows 2000 a je nastaven tak, aby neprováděl dynamickou aktualizaci, server neodpoví pomocí možnosti FQDN a neaktualizuje žádný záznam. Když nastane tato situace, klient DHCP se snaží aktualizovat jak záznamy prostředku A, tak záznamy prostředku PTR.
2. Jestliže server běží pod operačním systémem Windows 2000 a je nastaven tak, aby prováděl dynamickou aktualizaci na základě žádosti klienta, server se snaží aktualizovat záznamy prostředku PTR. Server odešle klientovi zprávu DHCPACK a klient se poté pokusí o aktualizaci záznamu prostředku A.
3. Jestliže server běží pod operačním systémem Windows 2000 a je nastaven tak, aby prováděl dynamickou aktualizaci vždy, server se snaží aktualizovat jak záznamy prostředku A, tak záznamy prostředku PTR. Klientovi odešle zprávu DHCPACK. Pokud klient požadoval, aby server aktualizoval záznamy prostředku PTR, ale nikoli záznamy prostředku A, nastaví server také pole příznaku na hodnotu 3. V tomto případě se klient nesnaží o aktualizaci žádného záznamu prostředku.

Nastavení dynamické aktualizace u klientů a serverů DHCP

Dle výchozího nastavení jsou klienti DHCP pro operační systém Windows 2000 nastaveni tak, že odesílají možnost FQDN s polem příznaku nastaveným na 0, který požaduje, aby klient registroval záznam prostředku A a server registroval záznam prostředku PTR. Název používaný v registraci DNS je spojením názvu hostitele a primární přípony DNS počítače. Toto výchozí nastavení můžete změnit ve vlastnostech protokolu TCP/IP připojení k síti.

Poznámka: Z této stránky můžete určit, jestli se má vůbec použít při registraci DNS zvláštní přípona DNS pro připojení a jestli vůbec registrovat adresu IP připojení.

► **Změna výchozího nastavení dynamické aktualizace na klientovi s dynamickou aktualizací**

1. Klepněte pravým tlačítkem na **Místa v síti** a pak klepněte na **Vlastnosti**.
2. Klepněte pravým tlačítkem na připojení, které chcete nastavit a pak klepněte na **Vlastnosti**.
3. Vyberte **Protokol TCP/IP**, klepněte na **Vlastnosti** a **Upřesnit** a vyberte záložku **Služba DNS**.
4. Dle výchozího nastavení je vybrána možnost **Registrovat adresu tohoto připojení v DNS** a není vybrána možnost **Použít příponu DNS tohoto připojení při registraci DNS**, které způsobují, že server aktualizuje záznam prostředku PTR a klient aktualizuje záznam prostředku A za použití primární přípony DNS.

K nastavení klienta, aby registroval jak zvláštní příponu DNS pro připojení, tak primární příponu DNS, vyberte **Použít příponu DNS tohoto připojení při registraci DNS**.

K nastavení klienta, aby neregistroval svou adresu IP v DNS, odeberte **Registrovat adresu tohoto připojení v DNS**.

Můžete server DNS pro operační systém Windows 2000 nastavit tak, aby prováděl jednu z následujících akcí: aktualizovat jakýkoli záznam dle požadavku klienta, vždy aktualizovat záznamy prostředku jak A, tak PTR nezávisle na požadavku klienta, neaktualizovat jakýkoli záznam DNS.

► **Nastavení dynamické aktualizace serveru DHCP pro operační systém Windows 2000**

1. Klepněte na **Start**, vyberte **Programy a Nástroje pro správu** a pak klepněte na **Služba DHCP**.
2. Rozviňte stromovou strukturu u názvu serveru.
3. Klepněte pravým tlačítkem na obor, který nastavujete a pak klepněte na **Vlastnosti**.
4. Klepněte na záložku **Služba DNS**.
5. Pokud není tato možnost dosud vybrána, vyberte **Automaticky aktualizovat informace o klientovi DHCP v DNS**.
6. Chcete-li, aby server registroval jakýkoli záznam, o jehož registraci klient požádá, vyberte možnost **Aktualizovat pouze na požadavek klienta DNS**.
7. Chcete-li, aby server vždy registroval záznam prostředku A i PTR, vyberte možnost **Vždy aktualizovat DNS**.
8. Chcete-li, aby server vždy registroval záznam prostředku A i PTR jménem klienta, který nepodporuje možnost FQDN, vyberte možnost **Povolit aktualizaci u klientů DNS, kteří nepodporují dynamickou aktualizaci**.

Upozornění: Máte-li nějaké vícedomé klienty s dynamickou aktualizací a alespoň jeden adaptér používá službu DHCP, vyberte možnost Aktualizovat pouze na požadavek klienta DNS (přednastavená hodnota). Pokud je server DHCP nastaven tak, že registruje záznam prostředku A i PTR, server DHCP nahrazuje všechny záznamy prostředku A názvu, který se snaží registrovat.

K aktualizaci záznamů prostředku A nebo PTR server DHCP posílá požadavek na dynamickou aktualizaci na server DNS. Jestliže server DHCP aktualizoval záznam prostředku A nebo PTR, odebere tento záznam při vypršení zápůjčky klienta. Můžete také nastavit server tak, aby odebíral záznam prostředku A klienta při vypršení zápůjčky klienta i v případě, že záznam prostředku A zaregistroval klient DHCP a ne server. Po obnovení zápůjčky DHCP klient DHCP opětovně zaregistruje záznamy prostředku.

► **Nastavení serveru DHCP pro operační systém Windows 2000 k odstranění záznamu prostředku A při vypršení zápůjčky**

1. Klepněte na **Start**, vyberte **Programy a Nástroje pro správu** a pak klepněte na **Služba DHCP**.
2. Rozviňte stromovou strukturu u názvu serveru.
3. Klepněte pravým tlačítkem na obor, který nastavujete a pak klepněte na **Vlastnosti**.
4. Klepněte na záložku **Služba DNS**.
5. Vyberte možnost **Při vypršení zápůjčky vyřadit dopředné vyhledávání (název na adresu)**.

Více informací o možnosti FQDN a integraci mezi službami DNS a DHCP najdete na odkazu IETF na adrese <http://windows.microsoft.com/windows2000/reskit/webresource>. Vyhledávejte „spolupráce mezi službami DHCP a DNS“ (respektive „Interaction Between DHCP and DNS“).

Klienti se statickým nastavením a vzdáleným přístupem

Klienti se statickým nastavením a klienti se vzdáleným přístupem nespolehají při registraci na server DHCP. Klienti se statickým nastavením dynamicky aktualizují své záznamy prostředků A a PTR při každém spuštění nebo každých 24 hodin, pokud je počítač zapnut delší dobu než jeden den, v případě poškození záznamů nebo nutnosti jejich obnovení v databázi. Klienti s dynamickou aktualizací dynamicky aktualizují záznamy prostředku A a PTR při telefonickém připojení. Také se při ukončení připojení uživatelem snaží odregistrovat záznamy prostředku A a PTR. Nicméně pokud klient se vzdáleným přístupem neuspěje při odregistrování záznamu prostředku během čtyř sekund, ukončí připojení a databáze DNS bude obsahovat zastaralý záznam. Pokud klient se vzdáleným přístupem neuspěje při odregistrování záznamu prostředku, odešle zprávu protokolu událostí, který můžete prohlížet pomocí Prohlížeče událostí. Klient se vzdáleným přístupem nikdy neodstraňuje zastaralé záznamy. Nicméně server RRAS se snaží při odpojení klienta odregistrovat záznam prostředku PTR.

Vícedomí klienti

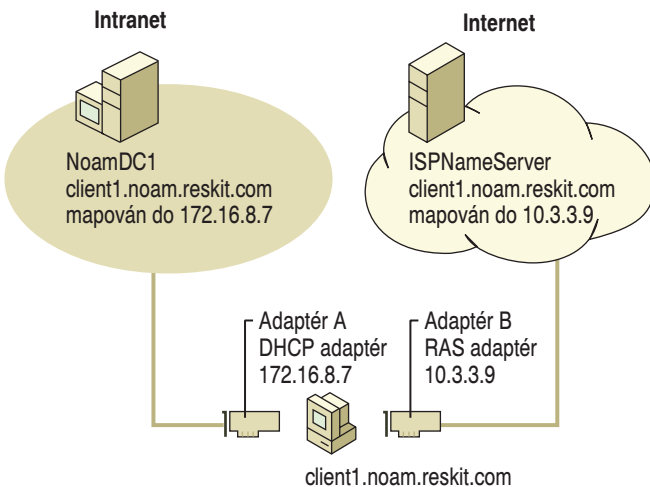
Pokud je klient s dynamickou aktualizací vícedomý (má více než jeden adaptér a s ním spojenou adresu IP), dle výchozího nastavení registruje adresu IP pro každý adaptér. Pokud nechcete, aby registroval tyto adresy, můžete ho na stránce vlastností připojení k síti nastavit tak, že nebude registrovat adresy IP pro jeden nebo více adaptérů.

► **Zabránění počítači v registraci adresy IP adaptéru**

1. Klepněte na **Místa v síti** a pak klepněte na **Vlastnosti**.
2. Vyberte připojení, které chcete nastavit a pak klepněte na **Vlastnosti**.
3. Vyberte **Protokol TCP/IP**, klepněte na **Vlastnosti**, klepněte na **Upřesnit** a pak vyberte záložku **Služba DNS**.

4. Odstraňte zaškrtnutí v poli **Registrovat adresu tohoto připojení v DNS**.

Klient s dynamickou aktualizací neregistruje všechny adresy IP u všech serverů DNS. Například obrázek 6.20 zobrazuje vícedomý počítač, client1.noam.reskit.com, který je připojen jak k internetu, tak k podnikovému intranetu. Tento počítač je k intranetu připojen adaptérem A, což je adaptér DHCP s adresou IP 172.16.8.7. Je také připojen k internetu adaptérem B, adaptérem se vzdáleným přístupem s adresou IP 10.3.3.9. Počítač Client1 překládá názvy intranetu pomocí serveru názvů na intranetu (NoamDC1) a názvy internetu překládá pomocí serveru názvů internetu (ISPName Server).



Obrázek 6.20 Dynamická aktualizace u vícedomých počítačů

Všimněte si, že ačkoli počítač Client1 je připojen k oběma sítím, adresa IP 172.16.8.7 je dostupná pouze prostřednictvím adaptéru A a adresa IP 10.3.3.9 je dostupná pouze prostřednictvím adaptéru B. Proto když klient s dynamickou aktualizací registruje adresy IP počítače Client1, neregistruje obě adresy IP na oba servery názvů. Namísto toho registruje přiřazení názvu na adresu IP pro adaptér A na server NoamDC1 a přiřazení názvu na adresu IP pro adaptér B na server ISPNameServer.

Dle výchozího nastavení počítač registruje spojení názvu hostitele a primární přípony DNS. Můžete počítač také nastavit tak, aby registroval doménový název, který je spojením názvu hostitele a zvláštní přípony DNS pro připojení. Například máte-li klienta, který je připojen ke dvěma různým sítím, a chcete, aby měl jiný doménový název pro každou síť, můžete to také nastavit. Více informací o nastavení názvů více domén najdete dříve v části „Vytváření názvů hostitelů a domén“.

Hodnota TTL

Kdykoli se klient s dynamickou aktualizací registruje ve službě DNS, s ním spojené záznamy prostředku A a PTR obsahují hodnotu TTL, která je dle výchozího nastavení nastavena na 20 minut. Přednastavenou hodnotu můžete změnit upravením záznamu **DefaultRegistrationTTL** v registru v následujícím podklíči registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Tcpip\Parameters
```

Záznam má hodnotu DWORD a obsahuje TTL v sekundách. Malá hodnota způsobuje dřívější vypršení záznamů uložených v mezipaměti, což zvyšuje provoz DNS, ale snižuje riziko zastarání záznamů. Dřívější vypršení záznamů je užitečné pro počítače, které často obnovují své zápůjčky DHCP. Velká hodnota způsobuje delší udržování záznamů uložených v mezipaměti, což snižuje provoz DNS, ale zvyšuje riziko zastarání záznamů. Dlouhé udržovací doby jsou vhodné pro počítače, které obnovují své zápůjčky DHCP zřídka.

Upozornění: Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správčovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. K nastavení nebo přizpůsobení si Windows 2000 použijte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Řešení konfliktů názvů

Pokud během registrace dynamické aktualizace klient zjistí, že jeho název už je u služby DNS zaregistrován s adresou IP, která náleží jinému počítači, dle výchozího nastavení se klient snaží nahradit registraci adresy IP dalšího počítače novou adresou IP. To znamená, že u zón, které nejsou nastaveny pro zabezpečenou dynamickou aktualizaci, může měnit registraci adresy IP jakéhokoli klientského počítače kterýkoli uživatel. U zón nastavených pro zabezpečenou dynamickou aktualizaci jsou schopni záznamy prostředku měnit pouze oprávnění uživatelé.

Výchozí nastavení lze změnit, takže namísto nahrazení adresy IP klient „vycouvá“ z procesu registrace a zaprotokoluje chybu do Prohlížeče událostí. K tomuto nastavení přidejte záznam **DisableReplaceAddressesInConflicts** s hodnotou 1 (DWORD) do následujícího podklíče registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
  \Tcpip\Parameters
```

Záznam může být buď 1 nebo 0, což určuje jednu z následujících možností:

- 1. Pokud název, který se klient snaží vytvořit, již existuje, klient se ho nesnaží přepsat.
- 0. Pokud název, který se klient snaží vytvořit, již existuje, klient se ho snaží přepsat. Toto je přednastavená hodnota.

Upozornění: Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správčovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. K nastavení nebo přizpůsobení si Windows 2000 použijte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Zabezpečená dynamická aktualizace

Jakoukoli zónu integrovanou se službou Active Directory můžete nastavit pro zabezpečenou dynamickou aktualizaci a pak použít seznam řízení přístupu (ACL), ve kterém se specifikují uživatelé a skupiny, kteří mají oprávnění upravovat zónu a záznamy v zóně. Následující části popisují standardy, které zahrnují zabezpečenou dynamickou aktualizaci, popisují proces zabezpečené dynamické aktualizace a vysvětlují, jak nastavit zabezpečenou dynamickou aktualizaci.

Poznámka: Zabezpečená dynamická aktualizace je dostupná pouze pro zóny integrované se službou Active Directory.

Nastavení zabezpečené dynamické aktualizace

Po vytvoření zóny integrované se službou Active Directory je nastavena dle výchozího nastavení tak, že umožňuje pouze zabezpečené dynamické aktualizace. Vytvoříte-li zónu jako standardní primární zónu a pak ji převedete na zónu integrovanou se službou Active Directory, je nastavena pro nezabezpečené dynamické aktualizace nebo zabezpečené dynamické aktualizace v závislosti na tom, jak byla nastavena původní primární zóna.

► Nastavení zabezpečené dynamické aktualizace

1. V konzole DNS klepněte pravým tlačítkem na zónu, pro kterou chcete nastavit zabezpečenou dynamickou aktualizaci a pak klepněte na **Vlastnosti**.
2. V okně **Povolit dynamickou aktualizaci?** vyberte **Pouze zabezpečené aktualizace**.

Řízení přístupu aktualizace k zónám

U zabezpečené dynamické aktualizace mohou pouze počítače a uživatelé specifikovaní v seznamu řízení přístupu (ACL) v rámci zóny vytvářet nebo upravovat objekty dnsNode. Dle výchozího nastavení seznam řízení přístupu dává oprávnění Create všem členům skupiny Ověření uživatelé, skupině všech oprávněných počítačů a uživatelů ve stromu služby Active Directory. To znamená, že jakýkoli oprávněný uživatel nebo počítač může vytvořit nový objekt v zóně. Také dle výchozího nastavení tvůrce vlastní nový objekt a náleží mu jeho úplné řízení.

U všech objektů DNS můžete prohlížet a měnit oprávnění na záložce Zabezpečení objektu z konzoly Uživatelé a počítače Active Directory nebo prostřednictvím vlastností zóny a záznamu prostředku na konzole DNS.

► Prohlížení seznamu řízení přístupu (ACL) pro objekt dnsZonev nebo dnsNode

1. V konzole DNS klepněte pravým tlačítkem na zónu nebo záznam, který si chcete prohlédnout a pak klepněte na **Vlastnosti**.
2. Klepněte na záložku **Zabezpečení**.

Poznámka: Seznamy řízení přístupu (ACL) jsou přiřazovány na základě názvu. Proto pokud máte dva různé záznamy pro stejný název FQDN, namapují se na stejný objekt ve službě Active Directory a mají stejný seznam řízení přístupu (ACL). Například stejné seznamy řízení přístupu (ACL) mají následující záznamy:

host1.reskit.com	A	172.16.15.9
host1.reskit.com	MX	mailer.reskit.com

Rezervace názvů

Názvy FQDN můžete rezervovat, takže je mohou používat pouze určití uživatelé. K tomu vytvoříte v konzole DNS název FQDN a pak upravíte jeho seznam řízení přístupu (ACL) tak, že množinu záznamů spojenou s názvem FQDN může měnit pouze určitý počítač, uživatel nebo uživatelé.

Standardy DNS pro zabezpečenou dynamickou aktualizaci

Operační systém Windows 2000 podporuje zabezpečené dynamické aktualizace spíše prostřednictvím rozhraní GSS-API (specifikováno v dokumentu RFC 2078) než prostřednictvím rozšíření zabezpečení služby DNS (RFC 2535) nebo zabezpečené dynamické aktualizace DNS (RFC 2137). Rozhraní GSS-API poskytuje služby zabezpečení nezávisle na podřízeném mechanismu zabezpečení.

Rozhraní GSS-API specifikuje způsob vytvoření zabezpečovacího kontextu pomocí bezpečnostních tokenů. Klient vygeneruje počáteční token a pošle ho na server. Server token zpracuje a v případě nutnosti vrátí následující token klientovi. Proces se opakuje až do ukončení vyjednávání a vytvoření zabezpečovacího kontextu. Po vytvoření má zabezpečovací kontext omezenou dobu existence, během které může být použit k vytváření a ověřování podpisu transakce na zprávách mezi dvěma stranami.

Operační systém Windows 2000 implementuje rozhraní GSS-API za použití algoritmu specifikovaného v dokumentu IETF „Algoritmus GSS pro TSIG (GSS-TSIG)“. Tento algoritmus používá ověřovací protokol Kerberos verze 5 jako svůj podřízený mechanismus zabezpečení. Další zabezpečení, například karty Smart Card nebo certifikáty, nebyly testovány. Algoritmus používá k poskytování služeb zabezpečení následující záznamy prostředku:

TKEY. Záznam prostředku specifikovaný v dokumentu IETF „Vytvoření tajného klíče pro DNS (TKEY RR)“ jako nosič k přenosu tokenů zabezpečení mezi klientem a serverem a k vytvoření tajných klíčů, používá se se záznamy prostředku TSIG.

TSIG. Záznam prostředku specifikovaný v dokumentu IETF „Podpisy transakce tajného klíče pro DNS (TSIG)“ k posílání a ověřování zpráv chráněných podpisem.

Ke sledování předávání záznamů TKEY a TSIG přes síť můžete použít Sledování sítě. Verze 6.12 a pozdější dekodují záznamy prostředku.

Záznam prostředku TKEY

Tabulka 6.7 popisuje strukturu záznamu prostředku TKEY, jak je popsán v dokumentu IETF „Vytvoření tajného klíče pro DNS (TKEY RR)“.

Tabulka 6.7 Záznamy prostředku TKEY

Pole	Typ dat	Poznámka
NAME	Název domény	Liší se podle režimu a kontextu
TTYPE	u_int16_t	TKEY
CLAS	u_int16_t	Ignorován, měl by být 0.
TTL	u_int32_t	Měl by být 0
RDLEN	u_int16_t	Délka pole RDATA
RDATA		

Pole	Typ dat	Poznámka
Algoritmus	název domény	Určuje, jak je použit materiál o tajných klíčích vyměněný za použití záznamu prostředku TKEY k odvození zvláštního klíče.
Začátek	u_int	V počtu sekund od 1.1.1970 GMT.
Vypršení	u_int32_t	V počtu sekund od 1.1.1970 GMT.
Režim	u_int16_t	Schéma pro souhlas klíče
Chyba	u_int16_t	Kód chyby
Velikost klíče	u_int16_t	Velikost pole Data klíče v oktetech.
Data klíče	datový proud oktětů	Liší se podle režimu
Další velikost	u_int16_t	Nepoužívá se
Další data	datový proud oktětů	Nepoužívá se

Záznam prostředku TSIG

Tabulka 6.8 popisuje strukturu záznamu prostředku TSIG, jak je popsán v dokumentu IETF „Podpisy transakce tajného klíče pro DNS (TSIG“ k posílání a ověřování zpráv chráněných podpisem.

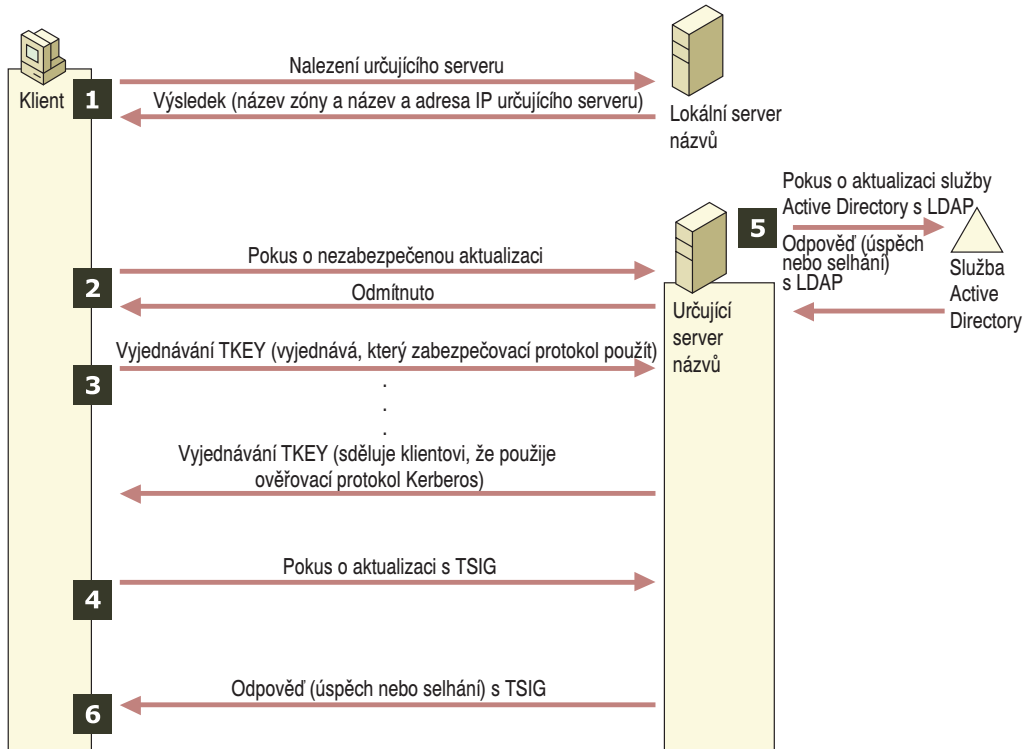
Tabulka 6.8 Struktura záznamu prostředku TSIG

Pole	Typ dat	Poznámka
Název algoritmu	Název domény	Název algoritmu vyjádřený jako název domény
Vyznačený čas	u_int48_t	Sekundy od 1.1.1970 UTC
Odchyłka	u_int16_t	Sekundy odchylky povolené v poli Vyznačený čas
Velikost podpisu	u_int16_t	Počet oktětů v poli Podpis
Podpis	datový proud oktětů	Definován v poli Název algoritmu
Chyba	u_int16_t	Rozšířené zpracování podpisu pokrývajícího RCODE
Další délka	u_int16_t	Délka pole Další data v oktetech
Další data	datový proud oktětů	Nedefinováno

Proces zabezpečené dynamické aktualizace

K inicializaci zabezpečené dynamické aktualizace klient prvně inicializuje vyjednávací proces TKEY, aby určil podřízený zabezpečovací mechanismus a vyměnil klíče. Dále klient pošle požadavek na zabezpečenou dynamickou aktualizaci obsahující záznamy prostředků k přidání, odstranění nebo úpravě serveru podepsaný záznamem prostředku TSIG, přičemž server pošle potvrzení. Nakonec se server pokusí o aktualizaci Active Directory jménem klienta.

Obrázek 6.21 znázorňuje proces dynamické aktualizace, která se koná mezi klientem na bázi Windows 2000 a serverem, pokud jsou oba nastaveni přednastavenými parametry.



Obrázek 6.21 Proces zabezpečené dynamické aktualizace

Během prvního kroku klient žádá lokální server názvů o zjištění, který server je určující pro název, který se snaží aktualizovat (za použití procesu popsaného dříve v části „Dotazy DNS“). Lokální server názvů odpovídá názvem zóny a určujícího primárního serveru této zóny.

Během druhého kroku se klient snaží o nezabezpečenou aktualizaci a server ji zamítne. Pokud by byla zóna nastavena pro nezabezpečenou dynamickou aktualizaci namísto zabezpečené dynamické aktualizace, server by se místo toho snažil přidat, odstranit nebo upravit záznamy prostředku ve službě Active Directory.

Během třetího kroku je započato vyjednávání TKEY mezi klientem a serverem. Nejprve klient a server vyjednávají o podřízeném zabezpečovacím mechanismu. Klienti a servery na platformě Windows 2000 s dynamickou aktualizací oba navrhují protokol Kerberos, takže se jej rozhodnou ho použít. Dále pomocí zabezpečovacího mechanismu ověří navzájem svou totožnost a vytvoří zabezpečovací kontext.

Během čtvrtého kroku klient pošle serveru požadavek na dynamickou aktualizaci podepsanou klíčem TSIG, který byl vygenerován pomocí zabezpečovacího kontextu vytvořeného ve třetím kroku. Server DNS ověří původ paketu dynamické aktualizace pomocí zabezpečovacího kontextu a klíče TSIG.

V pátém kroku se server snaží přidat, odstranit nebo upravit záznamy prostředku ve službě Active Directory. To, jestli může nebo nemůže provést aktualizaci, závisí na tom, jestli má klient odpovídající oprávnění provést aktualizaci a jestli jsou splněny všechny nutné podmínky.

Během šestého kroku server odešle odpověď klientovi, ve které stanoví, jestli byl nebo nebyl schopen provést aktualizaci, podepsanou klíčem TSIG. Pokud klient obdrží podvodnou odpověď, zahodí ji a počká na podepsanou odpověď.

Zabezpečení klientů DHCP nepodporujících možnost FQDN

Klienti DHCP, kteří nepodporují možnost FQDN, nejsou schopni provádět dynamickou aktualizaci. Proto pokud chcete mít jejich záznamy prostředku A a PTR dynamicky registrované ve službě DNS, musíte k provádění dynamické aktualizace jejich jménem nastavit server DHCP.

Nicméně nechcete, aby server DHCP prováděl zabezpečenou dynamickou aktualizaci jménem klientů DHCP, kteří nepodporují možnost FQDN. Když server DHCP provádí zabezpečenou dynamickou aktualizaci názvu, stane se vlastníkem názvu server DHCP a může ho nadále aktualizovat pouze tento server. To může působit problémy v několika rozdílných okolnostech. Například předpokládejte, že server DHCP DHCP1 vytvořil objekt pro název nt4host1.reskit.com a pak přestal odpovídat, načež se záložní server DHCP, DHCP2 pokoušel o aktualizaci názvu. Server DHCP2 není schopen aktualizovat tento název, protože ho nevlastní. V jiném příkladě předpokládejte, že server DHCP1 přidal názvu nt4host1.reskit.com objekt a pak správce inovoval název nt4host1.reskit.com na počítač na platformě Windows 2000. Vzhledem k tomu, že počítač na platformě Windows 2000 nevlastnil svůj název, nebyl by schopen aktualizovat ho.

Proto máte-li povolenu zabezpečenou dynamickou aktualizaci, můžete chtít nastavit každý server, který bude provádět dynamickou aktualizaci, zvláštním způsobem. Umístěte server do zvláštní bezpečnostní skupiny nazvané DNSUpdateProxy. Objekty vytvořené členy skupiny DNSUpdateProxy nemají žádné zabezpečení, proto může jejich vlastnictví převzít jakýkoli oprávněný uživatel.

► Přidání serveru DHCP do skupiny DNSUpdateProxy

1. Klepněte na **Start**, vyberte **Programy, Nástroje pro správu** a pak klepněte na **Uživatele a počítače Active Directory**.
2. Ve stromě konzole poklepejte na uzel domény.
3. Poklepejte na složku **Uživatelé**.
4. V detailním pohledu klepněte pravým tlačítkem na skupinu a klepněte na **Vlastnosti**.
5. Klepněte na záložku **Členové** a pak klepněte na **Přidat**.
6. Klepněte na **Náhled** a zobrazte si seznam domén, jejichž uživatelé a počítače mohou být přidány do skupiny, a klepněte na doménu obsahující server, který chcete přidat.
7. Klepněte na žádaný server a pak klepněte na **Přidat**.

Upozornění: Pokud jste instalovali službu DHCP na řadič domény, buďte si úplně jistí, že server není členem skupiny DNS Update Proxy. Pokud by byl členem této skupiny, kterýkoli uživatel nebo počítač by měl úplnou kontrolu nad záznamy DNS, které odpovídají řadičům domén, tedy pokud ručně neupravíte odpovídající seznam řízení pří-

stupu (ACL). Navíc, pokud je server DHCP běžící na řadiči domény nastaven k provádění dynamických aktualizací jménem svých klientů, tento server DHCP může převzít vlastnictví kteréhokoli záznamu. A to i v případě zón, které jsou nastaveny tak, že umožňují zabezpečenou dynamickou aktualizaci. To je kvůli tomu, že server DHCP běží pod účtem počítače, takže pokud je nainstalován na řadiči domény, má plnou kontrolu nad objekty DNS uloženými ve službě Active Directory.

Klienti DHCP na platformě Windows 2000 registrují vlastní záznamy prostředku A. Proto vložení serveru DHCP do skupiny DNSUpdateProxy nijak neovlivní zabezpečení záznamů prostředku A klientů DHCP pro operační systém Windows 2000.

Poznámka: Záznam prostředku A odpovídající serveru DHCP nemá žádné zabezpečení, jestliže je server umístěn do skupiny DNSUpdateProxy. Nicméně můžete ručně upravit prostřednictvím konzoly DNS seznam řízení přístupu (ACL).

Více informací o spolupráci mezi službami DNS a DHCP najdete v nápovědě Windows 2000 Server.

Stárnutí a úklid paměti záznamů zastaralých názvů

U dynamické aktualizace jsou záznamy automaticky přidávány do zóny společně s přidáním počítačů a řadičů domén. Nicméně v některých případech nejsou automaticky odstraněny. Například pokud počítač zaregistruje vlastní záznam prostředku A a je nesprávně odpojen od sítě, záznam prostředku A nemusí být odstraněn. Pokud jsou ve vaší síti mobilní uživatelé, bude s e toto stávat často.

Mnoho zastaralých záznamů představuje několik různých problémů. Zastaralé záznamy prostředku zabírají místo na serveru a server může použít k odpovědi na dotaz zastaralý záznam. Výsledkem je pokles výkonu serveru DNS.

K vyřešení tohoto problému může server DHCP na platformě Windows 2000 čistit paměť záznamů zastaralých názvů, tedy může procházet databází a hledat záznamy, které zestárlý, a odstraňovat je. Stárnutí záznamů a úklid paměti záznamů zastaralých názvů mohou řídit správce pomocí specifikace následujících věcí:

- Které servery mohou čistit paměť záznamů zastaralých názvů zón
- Které zóny mohou být takto čištěny
- Které záznamy je nutno po jejich zastarání odstranit

Server DNS používá algoritmus, který zajišťuje, že omylem neodstraní záznam, který musí zůstat, tedy za předpokladu, že všechny parametry nastavíte správně. Dle výchozího nastavení je úklid paměti záznamů zastaralých názvů vypnutý.

Upozornění: Dle výchozího nastavení je mechanismus úklidu paměti záznamů zastaralých názvů zakázán. Nepovolujte ho, pokud si nejste absolutně jisti, že rozumíte všem parametrům. Jinak můžete omylem nastavit server tak, že odstraní záznamy, které musí zůstat nedotčené. Pokud dojde k náhodnému odstranění názvu, uživatelé jsou neúspěšní při řešení dotazů na tento název a jakýkoli uživatel může tento název vytvořit a převzít jeho vlastnictví, dokonce i v zónách se zabezpečenou dynamickou aktualizací.

Stárnutí a úklid paměti záznamů zastaralých názvů můžete povolovat a zakazovat na úrovni serveru, zóny nebo záznamu. Můžete také povolit stárnutí pro množiny záznamů za pomoci nástroje Dnscmd.exe z příkazové řádky. (Informace o nástroji Dnscmd.exe najdete v nápovědě Windows 2000 Support Tools. Informace o instalaci a používání nápovědy Windows 2000 Support Tools a Support Tools najdete v souboru Sreadme.doc v adresáři \Support\Tools na CD operačního systému Windows 2000.) Nezapomínejte, že když povolíte úklid paměti záznamů zastaralých názvů na záznam, který není dynamicky aktualizovaný, záznam bude odstraněn a vy ho v případě nutnosti musíte znovu vytvořit.

jestliže je na standardní zóně úklid paměti záznamů zastaralých názvů zakázán a vy ho povolíte, server nevyhodí záznamy, které existovaly před povolením úklidu paměti záznamů zastaralých názvů. Server tyto záznamy nezlíkuje ani v případě, že převedete zónu nejprve na zónu integrovanou se službou Active Directory. Úklid paměti záznamů zastaralých názvů povolíte pomocí příkazu AgeAllRecords v nástroji Dnscmd.exe.

Parametry stárnutí a úklidu paměti záznamů zastaralých názvů

Server DNS pro operační systém Windows 2000 používá pro určení doby, kdy záznamy vyhodit, časové razítko, které dodává každému záznamu společně s parametry nastavení.

Tabulka 6.9 obsahuje seznam parametrů zóny, které ovlivňují dobu likvidace záznamu. Tyto vlastnosti se nastavují v zóně.

Tabulka 6.9 Parametry stárnutí a úklidu paměti záznamů zastaralých názvů pro zóny

Parametr zóny	Popis	Nástroj nastavení	Poznámky
Minimální interval mezi aktualizacemi	Doba, během které server nepřijímá žádosti o obnovu záznamu. (Nicméně stále přijímá změny.) Tato hodnota je interval mezi posledním okamžikem obnovy záznamu a nejbližším okamžikem, kdy může být znovu obnoven.	Konzola DNS a nástroj Dnscmd.exe.	Když je vytvořena zóna integrovaná se službou Active Directory, je tento parametr nastaven na parametr serveru DNS Přednastavený minimální interval mezi aktualizacemi . Tento parametr se replikuje přes replikaci služby Active Directory.
Interval aktualizace	Interval aktualizace následuje po minimálním intervalu mezi aktualizacemi. Na začátku intervalu aktualizace server začíná přijímat obnovy. Po jeho vypršení server DNS může uklidit záznamy, které nebyly obnoveny během nebo po intervalu aktualizace.	Konzola DNS a nástroj Dnscmd.exe	Když je vytvořena zóna integrovaná se službou Active Directory, je tento parametr nastaven na parametr serveru DNS Přednastavený interval aktualizace . Tento parametr se replikuje přes replikaci služby Active Directory.

Parametr zóny	Popis	Nástroj nastavení	Poznámky
Povolit úklid	Tento příznak značí, jestli je povoleno stárnutí a úklid zastaralých záznamů v zóně.	Konzola DNS a nástroj Dnscmd.exe	Když je vytvořena zóna integrovaná se službou Active Directory, je tento parametr nastaven na parametr serveru DNS Výchozí povolení úklidu . Tento parametr se replikuje přes replikaci služba Active Directory.
Server pro úklid	Tento parametr určuje, které servery mohou uklidit záznamy v této zóně.	Pouze nástroj Dnscmd.exe	Tento parametr je replikován službou Active Directory.
Zahájit úklid	Tento parametr určuje, zda může server zahájit úklid této zóny	Nelze nastavit	Tento parametr není replikován službou Active Directory.

Tabulka 6.10 obsahuje seznam parametrů serveru, které ovlivňují okamžik, kdy jsou záznamy uklizeny. Tyto parametry nastavíte na serveru.

Tabulka 6.10 Parametry stárnutí a úklidu paměti záznamů zastaralých názvů pro servery

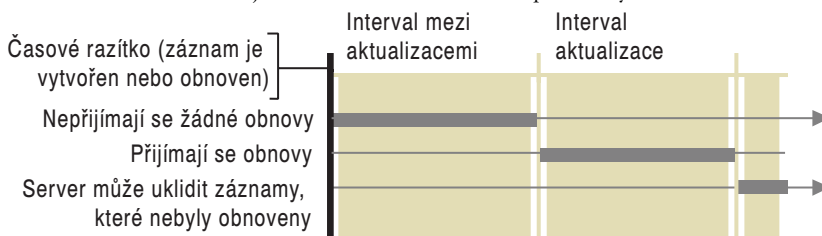
Parametr serveru	Popis	Nástroj nastavení	Poznámky
Přednastavený interval mezi aktualizacemi	Tato hodnota určuje interval mezi aktualizacemi, který se používá dle výchozího nastavení pro zónu integrovanou se službou Active Directory.	Konzola DNS (viz Interval mezi aktualizacemi) a nástroj Dnscmd.exe	Dle výchozího nastavení je to 7 dní.
Přednastavený interval aktualizace	Tato hodnota určuje interval aktualizace, který se používá dle výchozího nastavení pro zónu integrovanou se službou Active Directory.	Konzola DNS (viz Interval aktualizace) a nástroj Dnscmd.exe	Dle výchozího nastavení je to 7 dní.
Přednastavené povolení úklidu	Tato hodnota určuje parametr Povolit úklid, který se používá dle výchozího nastavení pro zónu integrovanou se službou Active Directory.	Konzola DNS (viz Povolit úklid) a nástroj Dnscmd.exe	Dle výchozího nastavení je zakázáno.

Parametr serveru	Popis	Nástroj nastavení	Poznámky
Povolit úklid	Tento příznak určuje, jestli server DNS může provádět úklid zastaralých záznamů. Pokud je úklid na serveru povolen, automaticky ho opakuje v intervalu specifikovaném v parametru Interval úklidu.	Konzola DNS, rozšířené zobrazení (viz Povolit automatický úklid zastaralých záznamů) a nástroj Dnscmd.exe.	Dle výchozího nastavení je úklid zakázán.
Interval úklidu	Tento interval určuje, jak často server DNS s povoleným úklidem může odebírat zastaralé záznamy.	Konzola DNS, rozšířené zobrazení (viz Interval úklidu) a nástroj Dnscmd.exe	Dle výchozího nastavení to je 7 dní.

Délka života záznamu

Průvodce instalací služby Active Directory můžete také vyvolat provedením souboru odpovědí pro bezobslužnou instalaci, který obsahuje všechna nastavení, která je třeba nastavit. Soubor odpovědí pro bezobslužnou instalaci je soubor, který používá průvodce k poskytování odpovědí na otázky. Více informací o souboru odpovědí pro bezobslužnou instalaci pro průvodce instalací služby Active Directory najdete v knize *Microsoft® Windows® 2000 Server Distribuované systémy* v části „Ukládání dat služby Active Directory“.

Obrázek 6.22 znázorňuje délku života záznamu s povoleným úklidem.



Obrázek 6.22 Délka života záznamu s povoleným úklidem

Po vytvoření nebo znovunačtení záznamu v zóně integrované se službou Active Directory nebo standardní primární zóně, pro kterou je povolen úklid, je zapsáno časové razítko.

Upozornění: Vzhledem k přidání časového razítka, má soubor standardní primární zóny, pro kterou je povolen úklid, mírně odlišný formát než standardní zóna DNS. To nepůsobí žádné problémy se standardním zónovým přenosem. Nicméně nemůžete kopírovat soubor standardní zóny s povoleným úklidem na server DNS, který není na platformě Windows 2000.

Hodnota časového razítka je doba, kdy byl záznam vytvořen nebo byl naposledy obnoven. Dle výchozího nastavení, pokud není záznam dynamicky aktualizován, časové razítko se rovná nule a záznam nelze uklízet. Také se časové razítko nikdy nemění, pokud obsahuje hodnotu nula. Pokud záznam náleží zóně integrované se službou Active Directory, pak je při každém obnovení časového razítka záznam replikován na další řadiče domén v doméně.

Dle výchozího nastavení jsou časová razítka záznamů vytvořených jinak než dynamickou aktualizací nastavena na nulu. Nulová hodnota značí, že časové razítko nesmí být obnovováno a záznam nesmí být uklizen.

Po obnovení záznamu nemůže být znovu obnoven po dobu specifikovanou v intervalu mezi aktualizacemi. Interval mezi aktualizacemi, parametr zóny, zabráňuje nikoli nezbytnému provozu replikací služby Active Directory.

Nicméně záznam může být během intervalu mezi aktualizacemi stále měněn (aktualizován). Pokud požadavek o dynamickou aktualizaci žádá o úpravu záznamu, považuje se tato žádost za aktualizaci. Nepožaduje-li žádné úpravy, považuje se za obnovení. Proto jsou považovány aktualizace nutných podmínek, tedy aktualizace obsahující seznam nutných podmínek ale žádné změny zóny, jsou také považovány za obnovení.

Interval mezi aktualizacemi je následován intervalem aktualizace. Po vypršení intervalu mezi aktualizacemi server začne přijímat obnovení a pokračuje v jejich přijímání po dobu délky života záznamu. Záznam lze obnovit, když je aktuální čas větší než hodnota časového razítka plus interval mezi aktualizacemi. Když server přijme obnovení nebo aktualizaci, časové razítko se změní na aktuální čas.

Dále po vypršení intervalu aktualizace server může záznam, pokud nebyl obnoven, uklidit. Záznam může být uklizen, pokud je aktuální čas větší než hodnota časového razítka plus hodnota intervalu mezi aktualizacemi plus hodnota intervalu obnovení. Nicméně server nemusí nutně v tento okamžik záznam uklidit. Okamžik, kdy dojde k uklizení záznamu, závisí na několika parametrech serveru.

Chování serveru

Server můžete nastavit tak, aby prováděl úklid záznamů automaticky v pravidelných intervalech. Navíc můžete úklid spustit na serveru ručně, takže proběhne okamžitý úklid. Po začátku úklidu se server snaží uklidit všechny primární zóny a je úspěšný, pokud jsou splněny následující podmínky:

- Parametr **Povolit úklid** je na serveru nastaven na 1.
- Parametr **Povolit úklid** je na zóně nastaven na 1.
- Je povolena dynamická aktualizace zóny.
- Parametr zóny **Servery pro úklid** není specifikován nebo obsahuje adresu IP serveru.
- Aktuální čas je větší než hodnota parametru zóny **Zahájit úklid**.

Poznámka: Parametr zóny **Servery pro úklid** je nastavitelný pouze pomocí nástroje Dnscmd.exe. Více informací o nástroji Dnscmd.exe najdete v nápovědě Windows 2000.

Server nastaví parametr **Zahájit úklid**, když se objeví jedna z následujících událostí:

- Je zapnutá dynamická aktualizace.
- Parametr **Povolit úklid** je v zóně nastaven z 0 na 1.

- Zóna je zavedena.
- Zóna je obnovena.

Parametr **Zahájit úklid** se rovná času, kdy se objeví jedna z výše uvedených událostí plus množství času specifikované v intervalu obnovy zóny. To brání problému, který se může objevit, pokud klient není schopen obnovit záznamy, protože zóna není dostupná. Například pokud je zóna pozastavena nebo server nefunguje. Pokud toto nastane a server nepoužije parametr **Zahájit úklid**, server může uklidit zónu předtím, než má klient vůbec šanci záznam aktualizovat.

Když je server připraven k úklidu záznamů, zkontroluje všechny záznamy v zóně jeden po druhém. Pokud časové razítko není nula a aktuální čas je větší než čas specifikovaný v časovém razítku záznamu plus interval mezi aktualizacemi plus interval obnovy zóny, záznam odstraní.

Nastavení parametrů úklidu

Tato část pojednává o problémech, které musíte vzít v úvahu při nastavování parametrů úklidu.

Abyste zajistili, že nedojde k odstranění žádných záznamů před tím, než má klient s dynamickou aktualizací čas je obnovit, ujistěte se, že interval obnovy je větší než perioda obnovy každého záznamu v zóně. Mnoho různých služeb může obnovovat záznamy v různých intervalech. Například Netlogon obnovuje záznamy jednou za hodinu, clusterové servery zpravidla jednou za 15 až 20 minut, servery DHCP obnovují záznamy při obnově zápůjček adres IP a počítače na platformě Windows 2000 obnovují své záznamy prostředku A a PTR každých 24 hodin.

Služba DHCP zpravidla vyžaduje nejdelší interval obnovy ze všech služeb. Pokud používáte službu DHCP pro operační systém Windows 2000, můžete použít přednastavené hodnoty stárnutí a úklidu zastaralých záznamů. Pokud používáte jiný server DHCP, možná budete muset přednastavené hodnoty upravit.

Čím delší jsou intervaly mezi aktualizacemi a aktualizace, tím déle zůstávají zastaralé záznamy. Proto můžete zkrátit tyto intervaly na nejmenší rozumnou míru. Nicméně pokud bude interval mezi aktualizacemi příliš krátký, můžete způsobit nepotřebnou replikaci službou Active Directory.

Integrace se službou WINS

Služba WINS poskytuje překlad dynamických názvů pro obor názvů typu NetBIOS. Před operačním systémem Windows 2000 byla služba WINS vyžadována na všech klientech a serverech. Server DNS s operačním systémem Windows NT 4.0 poskytoval vlastnost nazvanou vyhledávání WINS. S vyhledáváním WINS můžete nasměrovat službu DNS tak, aby se ptala na překlad názvů služby WINS, takže klienti DNS mohou vyhledávat názvy a adresy IP klientů služby WINS. Operační systém Windows 2000 stále podporuje vyhledávání WINS, i když pro klienty DHCP za předpokladu, že server DHCP používá operační systém Windows 2000, můžete použít místo toho dynamickou aktualizaci.

Více informací o dynamické aktualizaci najdete dříve v části „Dynamická aktualizace a zabezpečená dynamická aktualizace“, Více informací o službě WINS najdete v části „Služba Windows Internet Name Service“.

Poznámka: Služba WINS není vyžadována v prostředí vystavěném výhradně na operačním systému Windows 2000.

K použití integrace vyhledávání WINS přidejte dva zvláštní záznamy – záznamy prostředku WINS a WINS-R – do zón zpětného vyhledávání a dopředného vyhledávání. Když je server DNS určující pro tuto zónu dotazován na název, který nenašel v určující zóně, a zóna je nastavena k používání překladu WINS, server DNS se dotáže serveru WINS. Pokud je název registrován u služby WINS, server WINS vrátí asociované záznamy serveru DNS.

Zpětné vyhledávání funguje trochu odlišně. Když je určující server DNS dotázán na neexistující záznam PTR a určující zóna obsahuje záznam WINS-R, server DNS použije vyhledávání stavu adaptéru uzlu NetBIOS.

Nakonec server DNS vrátí název nebo adresu IP v odpovědi na původní požadavek DNS. Proto klienti DNS nemusí vědět, jestli je klient registrován u služby WINS nebo DNS, a stejně tak se nemusí dotazovat serveru WINS.

Poznámka: Kvůli odolnosti proti chybám můžete určit více serverů WINS. Server, který používá službu DNS pro operační systém Windows 2000, se pokouší lokalizovat název prohledáváním serverů WINS v pořadí stanoveném v seznamu.

Formát záznamů prostředku WINS a WINS-R

Záznamy prostředku WINS se používá pro dopředné vyhledávání. Když překladač pošle dotaz na server DNS, ve kterém požaduje odpovídající záznamy prostředku A, a server DNS nenalezne název v zóně dopředného vyhledávání, použije záznam WINS, pomocí kterého lokalizuje server WINS, který může být určující pro název nejvíce vlevo v názvu FQDN. Pokud je přítomen, záznam WINS se aplikuje pouze na nejvyšší úroveň zóny a nikoli na poddomény použité v zóně. Záznamy prostředku WINS má následující syntaxi:

*<doména> <třída> WINS [<TTL>] <lokální> <časový limit vyhledávání>
<časový limit mezipaměti> <adresa IP serveru WINS>*

kde jednotlivé členy mají následující význam:

doména. Název domény, kde je nalezen záznam WINS. Je to vždy @.

třída. Třída je pro záznamy WINS vždy IN.

TTL. Doba, po kterou může být záznam před vyhozením uložen v mezipaměti.

lokální. Určuje, jestli záznam musí být zahrnut v replikaci zóny.

časový limit vyhledávání. Doba v sekundách, po kterou server DNS používající vyhledávání WINS čeká před tím, než to vzdá.

časový limit mezipaměti. Doba v sekundách, po kterou server DNS používající vyhledávání WINS může uchovávat v mezipaměti odpověď od serveru WINS.

adresy IP serverů WINS. Adresy IP serverů WINS, které se mají použít.

Zde je uveden příklad záznamu prostředku WINS:

```
@      IN      WINS LOCAL 5 3600 172.16.72.3
```

Záznam prostředku WINS-R se používá pro zpětné vyhledávání. Když překladač pošle dotaz na server DNS, ve kterém požaduje odpovídající záznamy prostředku PTR, a ser-

ver DNS nenalezne název v zóně zpětného vyhledávání, použije dotaz na stav uzlu adaptéru typu NetBIOS pro dotazovanou adresu IP. Záznam prostředku WINS má následující syntaxi:

*<doména> <třída> WINSR [<TTL>] <lokální> <časový limit vyhledávání>
<časový limit mezipaměti> <výsledná doména názvu>*

kde jednotlivé členy mají následující význam:

doména. Název domény, kde je nalezen záznam WINS. Je to vždy @.

třída. Třída je pro záznamy WINS vždy IN.

TTL. Doba, po kterou může být záznam WINS před vyhozením uložen v mezipaměti.

lokální. Určuje, jestli záznam musí být zahrnut v replikaci zóny.

časový limit vyhledávání. Doba v sekundách, po kterou server DNS používající vyhledávání WINS čeká před tím, než to vzdá.

časový limit mezipaměti. Doba v sekundách, po kterou server DNS používající vyhledávání WINS může uchovávat v mezipaměti odpověď od serveru WINS.

výsledná doména názvu. Doména, která se připojuje k vráceným názvům typu NetBIOS.

Zde je uveden příklad záznamu prostředku WINS-R:

```
@      IN  WINS-R LOCAL 5 3600 reskit.com.
```

Příklad vyhledávání WINS

Předpokládejte, že klientská pracovní stanice zadá následující příkaz:

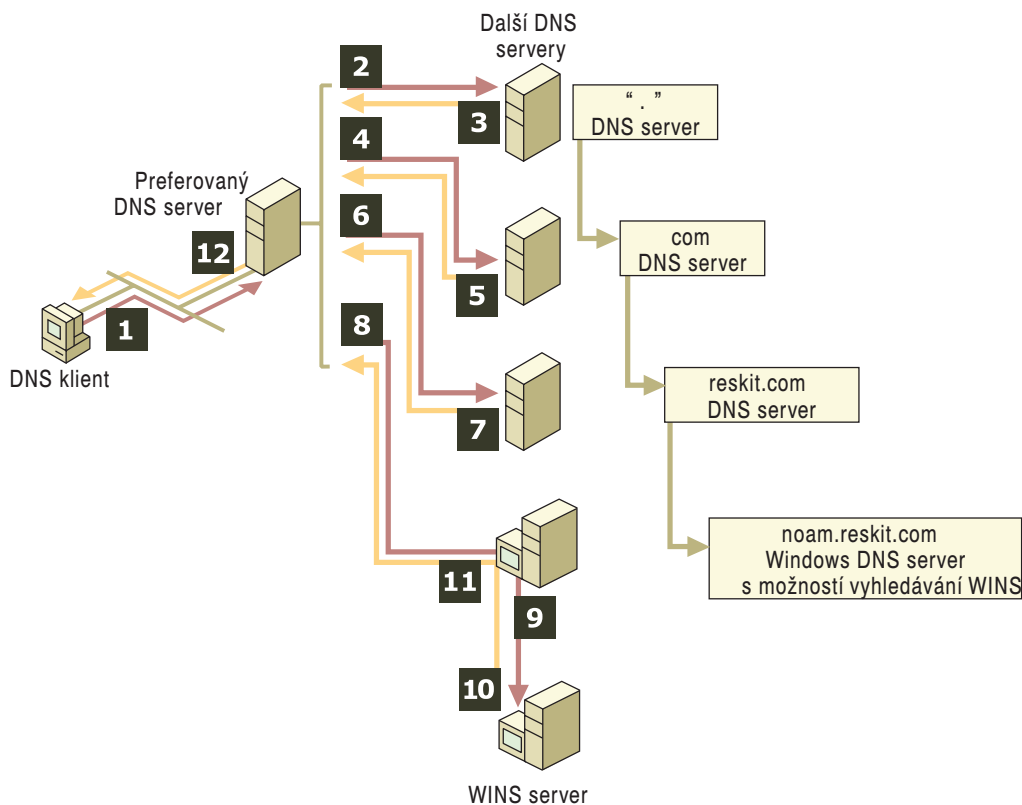
```
net use \\host-a.noam.reskit.com.\public
```

Tento příkaz vytvoří připojení mezi klientskou pracovní stanicí a službou Public na počítači host-a.noam.reskit.com, který je klientem provozujícím operační systém Windows NT 4.0. Nicméně před vytvořením připojení musí být službou DNS, nebo v tomto případě službou WINS, přeložen název FQDN host-a.noam.reskit.com na adresu IP. Obrázek 6.23 ukazuje, jak je tento název přeložen za předpokladu, že žádný server nemá údaje uloženy v mezipaměti a žádný server nepředává dotazy.

1. Klient se dotáže svého preferovaného serveru DNS.
2. Servery DNS provedou normální proces rekurze, jak se preferovaný server DNS postupně dotazuje dalších serverů DNS jménem klienta. Tento proces končí v osmém kroku, když je server DNS pro zónu noam.reskit.com lokalizován prostřednictvím řetězce odkazujících odpovědí. V tomto okamžiku procesu server, který je kontaktován, je serverem DNS pro operační systém Windows buď Windows NT Server 4.0 nebo Windows 2000 Server.

Když server DNS pro operační systém Windows určující pro zónu noam.reskit.com obdrží dotaz na „host-a“, prohlédne svou konfigurovanou zónu, jestli nenajde odpovídající záznamy prostředku A. Pokud záznam prostředku A nenajde a zóna je nastavena k použití vyhledávání WINS, server provede následující:

3. Server DNS oddělí hostitelskou část názvu (host-a) od názvu FQDN obsaženého v dotazu DNS.
Hostitelská část názvu je první název v názvu FQDN.
4. Server pak pošle požadavek na název typu NetBIOS serveru WINS za použití hostitelského názvu host-a.



Obrázek 6.23 Příklad vyhledávání WINS

5. Pokud server WINS může přeložit název, vrátí adresu IP serveru DNS.
6. Server DNS pro operační systém Windows pak vrátí tuto adresu IP původnímu preferovanému serveru DNS, který byl dotázán požadujícím klientem.
7. Preferovaný server DNS pak postoupí odpověď na dotaz zpět požadujícími klientovi.

Klientská pracovní stanice vytvoří relaci s host-a.noam.reskit.com a připojí se ke složce Public.

V tomto příkladě znal službu WINS pouze poslední server názvů v řetězci odkazů. Pro překladače klienta a všechny ostatní servery názvů to vypadá, že za celý proces překladače názvu je odpovědná služba DNS. Navíc, pokud se adresa IP pro host-a.noam.reskit.com změní, služba WINS je automaticky zaznamenaná. Ve službě DNS se nemusí nic měnit.

Zpětné vyhledávání s integrací služby WINS funguje trochu jinak než předchozí příklad. Vzhledem k tomu, že databáze služby WINS není indexována podle adresy IP, server DNS nemůže poslat na server WINS požadavek na zpětné vyhledávání názvu, aby získal název počítače podle jeho adresy IP. Server DNS namísto toho odešle požadavek na stav adaptéru uzlu přímo na adresu IP obsaženou ve zpětném dotazu DNS. Když server DNS obdrží v odpovědi na požadavek na stav adaptéru uzlu název typu

NetBIOS, připojí název domény DNS specifikovaný v záznamu WINS-R k názvu typu NetBIOS poskytnutému v odpovědi a předá výsledek požadujícímu klientovi.

Nastavení vyhledávání WINS

Vyhledávání WINS můžete nastavit na primárním i sekundárním serveru. K nastavení vyhledávání WINS na serveru DNS postupujte takto:

► Nastavení vyhledávání WINS

1. V konzole DNS klepněte pravým tlačítkem na zónu, u které chcete povolit vyhledávání WINS, a pak klepněte na **Vlastnosti**.
2. V dialogu **Vlastnosti** klepněte na záložku **Služba WINS**.
3. Vyberte **Použít dopředné vyhledávání WINS**.
4. V poli **Adresa IP** napište adresu IP serveru WINS, který bude použit pro překlad a klepněte **Přidat**.

Opakujte postup pro další žádané servery WINS. Vyhledávání WINS lze nastavit na primárním i sekundárním serveru. Můžete chtít nastavit vyhledávání WINS na sekundárním serveru, například pokud jsou vaše primární i sekundární servery umístěny na různých sídlech a chcete, aby sekundární server používal lokální servery WINS. Pokud tak učiníte, musíte nicméně zakázat replikace z primárního serveru prostřednictvím zaškrtnutí pole **Nereplikovat tento záznam** na záložce **Služba WINS** na stránce vlastností dané zóny.

Upozornění: Záznamy prostředku WINS a WINS-R jsou vlastní službě DNS poskytované operačním systémem Windows 2000 Server a dřívějšími verzemi operačního systému Windows NT Server. Nejlepší je ujistit se, že všechny servery DNS, které jsou určující pro zónu, běží na platformě operačního systému Windows 2000 nebo jakékoli verze Windows NT. V opačném případě mohou překladače vyhledávat záznamy WINS a WINS-R pouze přerušovaně. Pokud máte server s jinou implementací služby DNS oprávněné pro danou zónu, musíte zabránit zahrnutí těchto záznamů do zónových přenosů na jiné implementace služby DNS pomocí zaškrtnutí pole **Nereplikovat tento záznam** na záložce **Služba WINS** ve vlastnostech zóny. Více informací o zakázání replikací služby WINS najdete dále v části „Úvahy o spolupráci vyhledávání WINS“.

Upřesňující parametry vyhledávání WINS

Pro záznamy prostředku WINS a WINS-R můžete použít následující upřesňující časové parametry:

Časový limit mezipaměti Určuje serveru DNS, jak má dlouho uchovávat v mezipaměti jakékoli informace získané vyhledáváním WINS. Dle výchozího nastavení je tato hodnota nastavena na 15 minut.

Časový limit vyhledávání Určuje, jak dlouho má čekat na odpověď od serveru WINS před vypršením časového limitu a dotázáním dalšího serveru WINS uvedeného v záznamu WINS. Dle výchozího nastavení je tato hodnota 2 sekundy.

Tyto parametry nastavíte pomocí tlačítka **Upřesnit** v dialogu **Vlastnosti zóny**. Toto tlačítko se objeví buď na záložce WINS nebo WINS-R podle toho, jestli se zóna, kterou nastavujete, používá k dopřednému vyhledávání a nebo zpětnému vyhledávání.

Spolupráce s dalšími servery DNS

Služba DNS pro operační systém Windows 2000 je kompatibilní s dokumentem RFC a spolupracuje s dalšími implementacemi služby DNS. Byla testována a funguje s implementacemi pro Windows NT 4.0, BIND 8.2, BIND 8.1.2 a BIND 4.9.7. Nicméně operační systém Windows 2000 podporuje některé vlastnosti, které ostatní implementace služby DNS nepodporují. Tabulka 6.11 porovnává implementaci Windows 2000 s implementacemi Windows NT 4.0, BIND 8.2, BIND 8.1.2 a BIND 4.9.7.

Tabulka 6.11 Porovnání vlastností

Vlastnost	Windows 2000	Windows NT 4.0	BIND 8.2	BIND 8.1.2	BIND 4.9.7
Podpora dokumentu IETF „Záznam RR DNS pro určení umístění služeb (DNS SRV)“ (záznamy SRV)	Ano	Ano (s aktualizací Service Pack 4)	Ano	Ano	Ano
Podpora dynamické aktualizace	Ano	Ne	Ano	Ano	Ne
Podpora zabezpečené dynamické aktualizace založené na algoritmu GSS-TSIG	Ano	Ne	Ne	Ne	Ne
Podpora záznamů WINS a WINS-R	Ano	Ano	Ne	Ne	Ne
Podpora rychlých zónových přenosů	Ano	Ano	Ano	Ano	Ano
Podpora přírůstkových zónových přenosů	Ano	Ne	Ano	Ne	Ne
Podpora kódování znaků UTF-8	Ano	Ne	Ne	Ne	Ne

Následující části popisují problémy, které je nutné vzít do úvahy při implementaci vlastností, které další servery DNS nepodporují. Popisují také jak nastavit službu DNS, aby podporovala službu Active Directory při používání serverů DNS třetích stran.

Úvahy o dynamické aktualizaci a zabezpečené dynamické aktualizaci

Klienti a servery s operačním systémem Windows dřívějších verzí než Windows 2000 nepodporují dynamickou aktualizaci. Nicméně servery DHCP pro Windows 2000 mohou provádět dynamickou aktualizaci jménem klientů, kteří nepodporují možnost FQDN. Jestliže server DHCP pro Windows 2000 musí provádět zabezpečenou dynamickou aktualizaci jménem klientů, kteří provozují operační systém Windows dřívějších verzí než Windows 2000, umístíte tento server DHCP do zvláštní zabezpečovací skupiny nazvané DNS Update Proxy. Objekty vytvořené skupinou DNS Update Proxy nemají žádné zabezpečení, takže mohou být aktualizovány jakýmkoli počítačem na síti.

Více informací o tomto tématu najdete dříve v části „Dynamická aktualizace a zabezpečená dynamická aktualizace“.

Úvahy o spolupráci vyhledávání WINS

U zóny nastavené pro vyhledávání WINS pracuje vyhledávání WINS nejlépe, pokud všechny určující servery běží na operačním systému Windows 2000 nebo Windows NT 4.0. Vyhledávání WINS vyžaduje použití záznamů prostředku WINS a/nebo WINS-R, tedy zvláštních záznamů prostředku specifických právě pro operační systém Windows. Počítače s implementacemi služby DNS třetích stran nepodporují záznamy WINS

a WINS-R. Pokud se pokusíte pro jednu zónu použít směs serverů DNS společnosti Microsoft a třetích stran, může jejich kombinace způsobit chyby dat nebo selhání zónových přenosů na serverech DNS třetích stran, pokud nenastavíte servery s operačním systémem Windows 2000 na zakázání replikací záznamů WINS a WINS-R.

► **Zakázání replikací záznamů WINS a WINS-R**

1. V konzole DNS poklepejte na server a zobrazte si jeho zóny.
2. Chcete-li zakázat replikace v zóně dopředného vyhledávání, poklepejte na složku **Zóna dopředného vyhledávání**.
-nebo-
Chcete-li zakázat replikace v zóně zpětného vyhledávání, poklepejte na složku **Zóna zpětného vyhledávání**.
3. Klepněte pravým tlačítkem na zónu, u níž chcete zakázat replikace záznamů WINS a WINS-R a pak klepněte na **Vlastnosti**.
4. Klepněte na záložku **Služba WINS**.
5. Zaškrtněte pole **Nereplikovat tento záznam**.

Pokud zakážete replikace záznamů WINS a WINS-R, dotazy směřované na primární a sekundární servery vrátí různé výsledky. Když je určující primární server dotazován na název klienta WINS, dotáže se služby WINS a pak vrátí výsledek klientovi. Když je nicméně dotazován oprávněný sekundární server, odpoví klientovi, že název nebyl nalezen.

Tomuto problému zabráníte nejlépe pomocí nastavení serveru DNS na používání odkazu WINS popsaného v následující části.

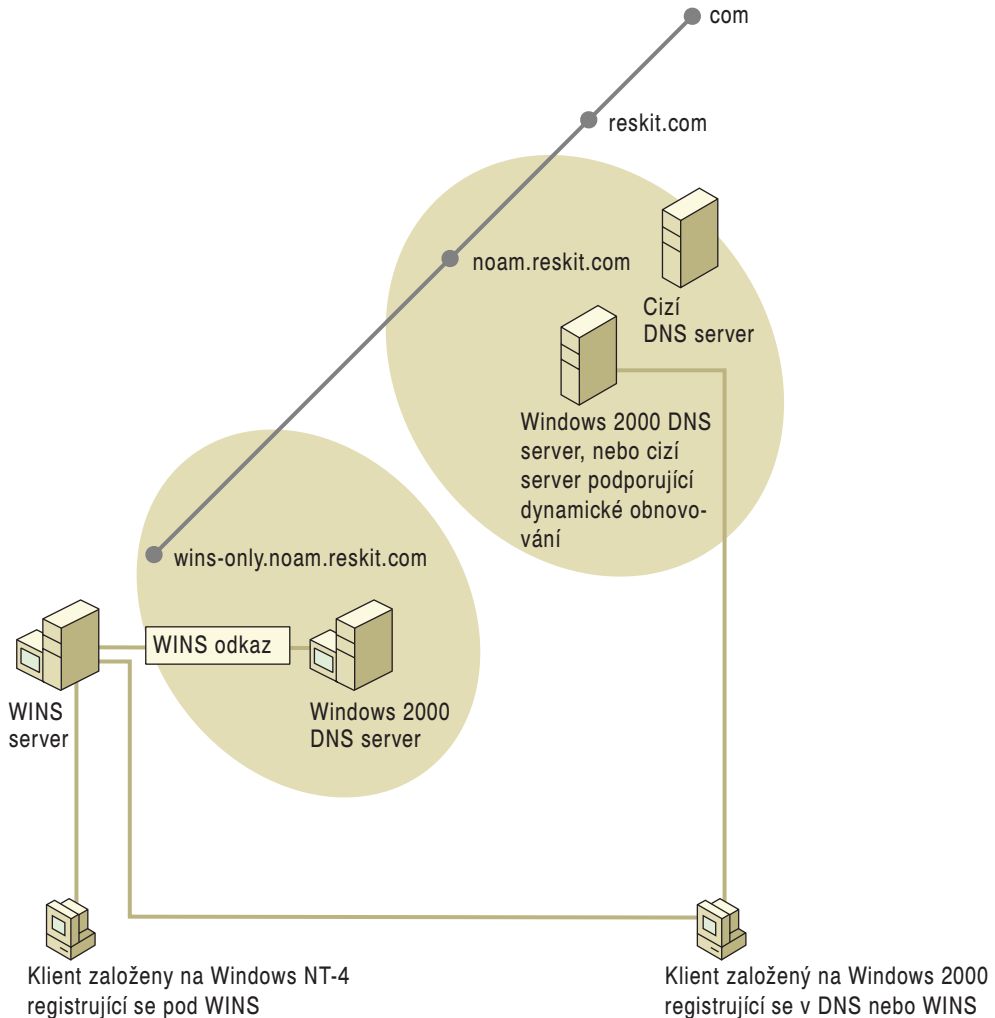
Používání odkazu WINS

Máte-li doménu, která musí obsahovat záznamy prostředku vyhledávání WINS, ale některé určující servery názvu této domény používají implementace služby DNS třetích stran, můžete zabránit problémům se spoluprací zakázáním replikací WINS. Případně můžete zabránit problémům se spoluprací vytvořením a delegováním zóny odkazů WINS. Tato zóna neprovádí nějaké registrace nebo aktualizace, ale pouze odkazuje vyhledávání DNS na službu WINS.

Po vytvoření zóny odkazů WINS nastavte klienty DNS, aby připojovali název zóny odkazů WINS k neúplným dotazům. Nejjednodušší je nastavit server DHCP, aby přiřazoval zvláštní příponu DNS pro připojení ke všem adaptérům DHCP na všech počítačích v síti. Tato přípona se připojuje k neúplným dotazům.

Případně můžete na každém počítači specifikovat seznam pro vyhledávání přípon domén, jak je popsáno dříve v části „Překladač pro operační systém Windows 2000“. Nezapomínejte, že když specifikujete seznam pro vyhledávání přípon domén, že se vaše primární přípony DNS a zvláštní přípony DNS pro připojení nepoužijí, pokud je speciálně nepřidáte do tohoto seznamu.

Obrázek 6.24 ukazuje příklad odkazu WINS v síti, která obsahuje servery s implementací služby DNS třetích stran a klienty s operačním systémem Windows 2000 i Windows NT 4.0.

**Obrázek 6.24 Odkaz WINS**

V tomto příkladě je zóna **noam.reskit.com** uložena a replikována mezi servery s operačním systémem Windows 2000 a servery s dalšími implementacemi služby DNS. K podpoře vyhledávání WINS správce sítě vytvořil novou zónu nazvanou **wins-only.noam.reskit.com**, která je určena k poskytování integrovaného vyhledávání DNS-WINS pro klienty WINS. Správce sítě povolil vyhledávání WINS pouze na této zóně a nepřidal žádné další záznamy prostředků kromě záznamů prostředku WINS.

Aby se registrovali ve službě DNS, klienti na platformě operačního systému Windows 2000 posílají požadavky na dynamickou aktualizaci serveru DNS, který je určující pro doménu **noam.reskit.com**. Klienti s operačním systémem Windows 2000 a Windows NT 4.0 se registrují zároveň ve službě WINS.

V tomto příkladě když klient DNS s operačním systémem Windows 2000 vyhledá počítač pomocí jeho zkráceného názvu, připojí všechny přípony domén, které má nasta-

veny pro připojování, včetně přípony domény wins-only.noam.reskit.com, aby vytvořil název FQDN. Například pokud je požadovaný hostitel WINS host-a, klient použije dotaz DNS pro host-a.wins-only.noam.reskit.com.

Mít pouze jednu zónu integrovanou se službou WINS poskytuje další výhody. Když dopředné vyhledávání WINS názvu hostitele počítače používá vyhledávání WINS, název DNS specifikovaný a používaný v dotazu výslovně označuje, že prostředek použitý k překladu názvu byl server DNS používající integraci vyhledávání WINS. Toto integrované řešení může také předejít zmatku v tom případě, když dotazy DNS na různé názvy FQDN přiřazují název stejného klienta WINS a adresu IP. Tento výsledek se může lehce objevit, pokud přidáte a nastavíte více zón a povolíte jim všem používat integraci vyhledávání WINS.

Například předpokládejte, že máte dvě zóny, obě nastavené k používání vyhledávání WINS. Zóny mají kořeny pocházející z následujících názvů domén DNS:

- noam.reskit.com
- eu.reskit.com

S tímto nastavením dotaz na klienta WINS s názvem host-a může být přeložen pomocí jednoho z těchto názvů FQDN:

- host-a.noam.reskit.com
- host-a.eu.reskit.com

Úvahy o zónovém přenosu

Operační systém Windows 2000 podporuje metodu zónového přenosu nazvanou rychlý zónový přenos. Pomocí rychlého zónového přenosu může server DNS pro Windows 2000 poslat více než jeden záznam prostředku na zprávu. To je efektivnější než odesílání pouze jednoho záznamu prostředku ve zprávě. Nicméně některé servery DNS třetích stran včetně serverů s verzemi BIND dřívějšími než 4.9.5 rychlý zónový přenos nepodporují. Použijete-li sekundární server, který nepodporuje rychlý zónový přenos, zakažte rychlý přenos na hlavním serveru zaškrtnutím pole **Navázat sekundární servery** na záložce Upřesnit ve vlastnostech serveru přístupných z konzole DNS.

Mnoho serverů DNS včetně serverů s verzemi BIND dřívějšími než 8.2 nepodporuje přírůstkový zónový přenos, další metodu zónového přenosu. U přírůstkového zónového přenosu může server DNS místo přenosu celé zóny přenést jen ty části zóny, které se změnily od posledního dotazu sekundárního serveru. Nicméně to nepůsobí problémy se spoluprací, protože operační systém Windows 2000 může stále používat úplný zónový přenos, pokud některý ze sekundárních serverů přírůstkový zónový přenos nepodporuje.

Operační systém Windows 2000 také podporuje typy záznamů prostředku, které další servery nemusí podporovat, například záznam WINS a WINS-R. Máte-li primární kopii zóny na serveru DNS pro Windows 2000 a sekundární kopii zóny na serveru DNS třetích stran, a primární zóna obsahuje záznamy prostředku, které server třetích stran nepodporuje, sekundární server může tyto záznamy vyhodit nebo nemusí být schopen přenést zónu. Informace o záznamech WINS najdete dříve v části „Úvahy o spolupráci vyhledávání WINS“.

Je také možné, že server DNS třetích stran bude podporovat typ záznamu prostředku, který nepodporuje operační systém Windows 2000, například záznamy prostředku nezapsané v dokumentech RFC. Máte-li primární kopii zóny na serveru DNS třetích stran a sekundární kopii na serveru pro Windows 2000 a primární zóna obsahuje záznamy

prostředku, které server DNS pro operační systém Windows 2000 nepodporuje, sekundární server tyto záznamy vyhodí. Pokud obdrží nějaké záznamy CNAME, vyhodí je také. Server DNS lze nastavit také tak, že zastaví zónový přenos, jakmile obdrží záznam prostředku, který nepodporuje.

Informace o problémech se zónovým přenosem najdete později v části „Diagnostika problémů s překladem názvu“.

Úvahy o znakové sadě Unicode

Operační systém Windows 2000 podporuje dokument RFC 2044, který rozšiřuje znakovou sadu povolenou v názvech DNS, že obsahuje i kódování znaků UTF-8. Nicméně mnoho serverů DNS včetně serverů s operačním systémem Windows NT 4.0 respektuje dokument RFC 1123, který povoluje menší znakovou sadu. Provádíte-li zónový přenos ze zóny obsahující znaky UTF-8 na sekundární server třetích stran, který znaky UTF-8 nepodporuje, sekundární server může záznamy prostředku „vyhodit“ nebo může zónový přenos selhat. Proto pokud plánujete používání nějakých znaků ze znakové sady UTF-8, zvažte problémy popsané dříve v části „Dodržování omezení názvů hostitelů a domén“.

Nastavení serverů DNS s jiným operačním systémem než Windows 2000 k podpoře služby Active Directory

Aby lokátor řadiče domény fungoval správně, primární server DNS určující pro názvy registrované službou Netlogon na řadiči domény musí podporovat záznam prostředku umístění služby (SRV RR). Záznam SRV je specifikován v dokumentu IETF „Záznam prostředku DNS pro určení umístění služeb (DNS SRV)“. Další servery DNS, které jsou určující pro doménu, musí také podporovat záznamy SRV.

Navíc můžete zjednodušit správu tím, že se ujistíte, že servery DNS určující pro názvy registrované službou Netlogon podporují protokol dynamické aktualizace, jak je popsáno v dokumentu RFC 2136. Můžete jako primární hlavní server pro název domény použít server DNS, který nepodporuje dynamickou aktualizaci. Nicméně toto se nedoporučuje, protože budete muset ručně aktualizovat primární zónu při konfiguraci služby Active Directory. Informace o nastavení a ověřování záznamů DNS používaných k podpoře služby Active Directory najdete dále v části „Ověření základního nastavení služby DNS“.

Používáte-li server DNS, který nepodporuje dokument IETF „Záznam prostředku DNS pro určení umístění služeb (DNS SRV)“, musíte inovovat server DNS nebo přidat server DNS, který podporuje tyto standardy. Server podporující tyto standardy musí být primárním serverem DNS určujícím pro názvy DNS, které budou registrovány službou Netlogon na řadiči domény. Pak musíte provést zvláštní nastavení na obou serverech DNS. Tato část vysvětluje, které servery DNS mohou být použity k podpoře služby Active Directory a jak nastavit služby DNS a Active Directory, když používáte server nepodporující službu Active Directory.

Používáte-li službu DNS jinou než pro operační systém Windows 2000, je vhodné otestovat její kompatibilitu se službou Active Directory a DHCP.

Podpora služby Active Directory pomocí jiných serverů DNS než společnosti Microsoft

Záznamy SRV jsou podporovány těmito servery:

- Windows 2000
- Windows NT 4.0 s aktualizací Service Pack 4 a pozdější
- BIND 4.9.6 a pozdější

Dynamickou aktualizaci podporují následující servery:

- Windows 2000
- BIND 8

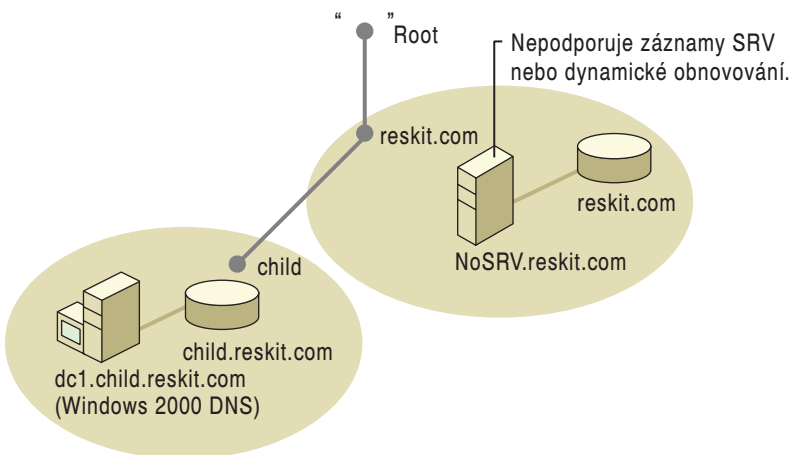
Používáte-li server třetích stran, nemůžete nicméně použít konzolu DNS nebo nástroj Dnscmd.exe, integraci služby Active Directory, zabezpečenou dynamickou aktualizaci, stárnutí a úklid zastaralých záznamů nebo vzdálenou správu.

Je také vhodné ověřit nastavení služby DNS po instalaci služby Active Directory.

Databáze služby DNS musí obsahovat záznamy prostředku lokátoru (SRV, CNAME a A) tak, aby podporovala všechny řadiče domén.

Používání názvu delegované zóny jako domény služby Active Directory

Pokud již má vaše organizace doménu DNS (například reskit.com) a primární server DNS určující pro tuto doménu nepodporuje dokument RFC 2136 a IETF „Záznam prostředku DNS pro určení umístění služeb (DNS SRV)“, přičemž nemůžete tento server inovovat, můžete stále vytvořit doménu služby Active Directory. K poskytnutí podpory služby DNS pro doménu služby Active Directory v takovéto situaci delegujete poddoménu (například child.reskit.com) z prvního serveru DNS na druhý server DNS, který podporuje tyto standardy. Dále nastavte tento druhý server DNS jako určující pro poddoménu a vytvořte doménu služby Active Directory, která má stejný název jako poddoména DNS. Na obrázku 6.25 je znázorněn příklad implementace serveru DNS pro operační systém Windows 2000 a jeho určení pro delegovanou poddoménu.



Obrázek 6.25 Implementace serveru DNS pro operační systém Windows 2000 k podpoře delegované poddomény

V tomto příkladě primární server názvů pro doménu reskit.com, NoSRV.reskit.com, nepodporuje záznamy SRV a proto nemůže být použit k podpoře služby Active Directory. Vzhledem k tomu správce NoSRV.reskit.com delegoval poddoménu child.reskit.com na server DNS pro operační systém Windows 2000. Server DNS pro operační systém Windows 2000 poskytuje této zóně stejné možnosti jako jakékoli jiné zóně. Například může být ukládána ve službě Active Directory, jak je popsáno dříve v části „Integrace adresářové služby Active Directory a replikace Multimaster“.

Používání názvu existující zóny jako názvu domény služby Active Directory

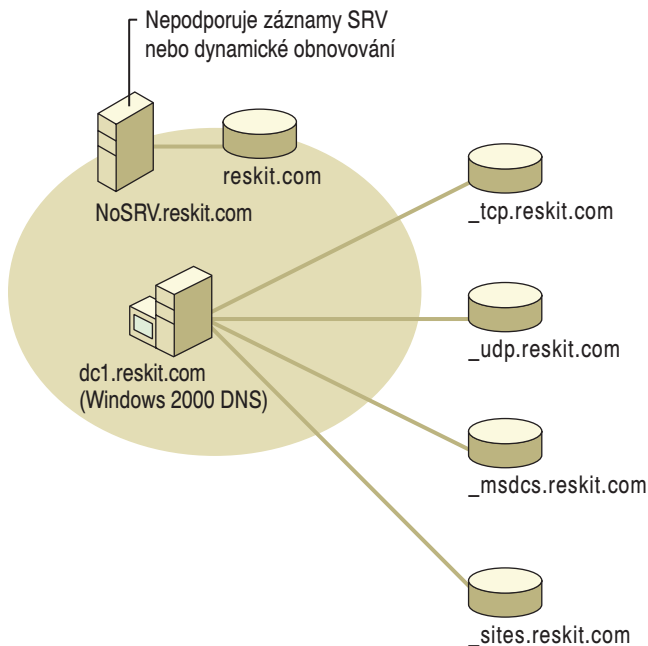
Pokud již má vaše organizace doménu DNS (například reskit.com) a primární server DNS určující pro tuto doménu nepodporuje dokument RFC 2136 a IETF „Záznam prostředku DNS pro určení umístění služeb (DNS SRV)“, přičemž nemůžete tento server inovovat, můžete stále implementovat službu Active Directory s názvem existující zóny DNS. K implementaci služby Active Directory přidejte další server DNS, který podporuje tyto standardy a delegujte na tento server určité zóny.

Na serveru DNS, který nepodporuje záznamy SRV a dynamickou aktualizaci, delegujte následující zóny na serveru, který je podporuje:

- `_tcp.< název domény služby Active Directory >`
- `_udp.< název domény služby Active Directory >`
- `_msdcs.< název domény služby Active Directory >`
- `_sites.< název domény služby Active Directory >`

Na serveru DNS, který podporuje tyto vlastnosti, vytvořte a povolte dynamickou aktualizaci pro zóny uvedené v předchozím seznamu. Řadiče domén dynamicky aktualizují příslušné záznamy v těchto zónách.

Obrázek 6.26 znázorňuje toto nastavení pro příklad domény reskit.com:



Obrázek 6.26 Delegování zón na server DNS podporující službu Active Directory

Služba Netlogon zasílá delegovaným zónám dynamické aktualizace. Dle výchozího nastavení se služba Netlogon snaží o dynamickou aktualizaci záznamu prostředku A, který obsahuje název vlastníka, který je stejný název jako název domény služby Active Directory. Název vlastníka je název uzlu, kterému náleží záznam prostředku. V tomto příkladě selže dynamická aktualizace prováděná službou Netlogon. To způsobí chybové hlášení v Prohlížeči událostí, které oznamuje, že dynamická aktualizace selhala. Abyste zabránili službě Netlogon registrovat záznamy prostředku A, přidejte záznam DnsRegisterARecords do registru do následujícího podklíče registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\NetLogon\Parameters
```

Hodnotu záznamu DnsRegisterARecords nastavte na 0x0 (DWORD).

Upozornění: Nepoužívejte editor registru k přímým úpravám, pokud máte ještě jinou možnost. Editory registru obcházejí standardní zabezpečení poskytované správcovskými nástroji. Toto zabezpečení brání vložení kolidujícího nastavení nebo nastavení, která by snížila výkon nebo poškodila systém. Přímá editace registru může mít vážné a nepředvídatelné následky, které mohou bránit spuštění systému a vyžadovat reinstalaci operačního systému Windows 2000. K nastavení nebo přizpůsobení si Windows 2000 používejte, je-li to možné, programy v Ovládacích panelech nebo na konzole Microsoft Management Console.

Úvahy o přístupu na síť internet

Aby byla vaše organizace viditelná na síti internet, musíte mít vnější obor názvů, veřejný obor názvů, do kterého může přistupovat kdokoli na síti internet. Úřad pro názvy v síti internet musí přiřadit název vaší doméně DNS a ujistit se, že nadřazená zóna zahrnuje delegaci na server DNS určující pro tuto doménu DNS. Nicméně jako pomoc při zabránění neúmyslným přístupům k síti můžete používat vnitřní obor názvů, privátní obor názvů, který mohou vidět pouze uživatelé uvnitř organizace, což brání neoprávněným osobám ve zjištění názvů a adres IP počítačů na síti.

Plánujete-li, že budete mít jak vnější, tak vnitřní obor názvů, musíte nastavit své servery DNS tak, aby umožňovaly vnitřním klientům překládat názvy v obou oborech názvů. To, jak plánujete svůj obor názvů, závisí na typu klientů.

Plánování oboru názvů

Při plánování oboru názvů se musíte rozhodnout, jestli budete používat privátní kořenovou doménu a jestli chcete, aby vnější a vnitřní obory názvů měly stejný název domény.

To, jestli můžete použít privátní kořen, závisí na typu klientů, které máte. Privátní kořen můžete použít pouze v tom případě, že každý z klientů má jednu z následujících vlastností:

- *Seznam vyloučených názvů.* Seznam vnitřních přípon DNS.
- *Soubor automatického nastavení proxy.* Seznam přípon DNS a přesných názvů, které jsou vnitřní nebo vnější.

Máte-li klienty, kteří postrádají obě z těchto vlastností, server DNS hostící vnitřní doménu nejvyšší úrovně ve vaší organizaci musí předávat dotazy na síť internet.

Tabulka 6.12 ukazuje, v závislosti na proxy možnostech klienta, jestli můžete použít privátní kořen. (Všimněte si, že tabulka lokálních adres (tabulka LAT) je seznam adres IP, které jsou vnitřní i vnější.)

Tabulka 6.12 Nastavení vnitřních a vnějších oborů názvů v závislosti na možnostech proxy

	Bez proxy	Tabulka LAT	Seznam vyloučených názvů	Soubor pro automatické nastavení (PAC)
Software společnosti Microsoft s odpovídajícími možnostmi proxy	Obecný Telnet	Proxy Windows Sockets (WSP) 1.x, 2.x	WSP 1.x, WSP 2.x a všechny verze prohlížeče Microsoft® a pozdější Internet Explorer	WSP 2.x, prohlížeč Internet Explorer 3.01
Můžete předávat dotazy?	Musí předávat dotazy.	Musí předávat dotazy.	Možné.	Možné.
Můžete používat privátní kořen?	Není možné.	Není možné.	Možné.	Možné.

Kvůli zjednodušení překladu názvů vnitřních klientů použijte odlišný název domény pro vnitřní a vnější obor názvů. Například můžete použít název reskit01-ext.com pro vnější obor názvů a reskit.com pro vnitřní obor názvů. Nicméně nevytvořte vnější obor názvů jako poddoménu vnitřní domény, tedy v kontextu příkladu, nepoužívejte reskit.com pro vnitřní obor názvů a noam.reskit.com pro vnější obor názvů.

Můžete použít stejný název vnitřně i navenek, ale působíte tím problémy s nastavením a obecně zvyšujete náklady na správu. Pokud chcete používat stejný název domény vnitřně i navenek, musíte provést jednu z následujících akcí:

- Zduplikujte vnitřně veřejnou zónu DNS vaší organizace.
- Zduplikujte vnitřně veřejnou zónu DNS a všechny veřejné servery (například servery WWW), které přísluší vaší organizaci.
- V souboru PAC každého z vašich klientů udržujte seznam veřejných serverů, které náleží vaší organizaci.

Upozornění: Ujistěte se, že název domény vašeho vnitřního oboru názvů není používán někde na síti internet. Pokud by byl používán, měli byste problémy s nejednoznačností při procesu překladu názvů

Akce, kterou je nutno provést k používání stejné domény vnitřně i navenek, se různí. Tabulka 6.13 ukazuje, jestli můžete používat stejný název domény pro vnitřní i vnější obor názvů, a pokud ano, kterou metodu musíte použít v závislosti na proxy možnostech softwaru klienta.

Tabulka 6.13 Používání stejného názvu domény pro vnitřní i vnější obor názvů v závislosti na možnostech proxy

	Bez proxy	Tabulka LAT	Seznam vyloučených názvů	Soubor pro automatické nastavení (PAC)
Použití různých názvů domén.	Možné.	Možné.	Možné.	Možné (s použitím jednoduchého vyloučení).

	Bez proxy	Tabulka LAT	Seznam vyloučených názvů	Soubor pro automatické nastavení (PAC)
Použití stejných názvů domén; vnitřní duplikace veřejných oborů názvů DNS organizace (záznamy).	Možné	Možné (pomocí zveřejnění tabulky LAT).	Není možné.	Možné. Při použití souboru PAC se nepoužijí zduplikované vnější záznamy.
Použití stejných názvů domén; vnitřní duplikace veřejných oborů názvů DNS organizace a veřejných serverů.	Možné.	Možné.	Možné.	Možné.
Použití stejných názvů domén; udržování seznamu veřejných serverů v souborech PAC.	Není možné.	Není možné.	Není možné.	Možné.

Příklad plánování oboru názvů

Následující části vysvětlují některé problémy, které musíte zvážit při plánování oboru názvů, pomocí popisu nastavení dvou fiktivních organizací. První organizace, která má rezervované názvy domén DNS reskit.com a reskit01-ext.com má pouze klienty proxy, kteří podporují buď seznam vyloučení nebo soubor PAC. Na druhou stranu, druhá organizace, která má rezervované názvy domén acquired01-int.com a acquired01-ext.com, nemá žádné takové klienty proxy. Obě organizace používají různý název domény pro vnitřní a vnější obor názvů.

Domény reskit.com a acquired01-int.com obě potřebují nastavení, které provádí následující:

- Pro síť internet odhaluje pouze veřejnou část oboru názvů organizace.
- Umožňuje jakémukoli počítači v organizaci přeložit jakýkoli název vnitřní nebo vnější.
- Umožňuje jakémukoli počítači v organizaci přeložit jakýkoli název ze sítě internet.

Navíc, obě organizace se spojily a všechny počítače z jednoho privátního oboru názvů musí být schopné přeložit jakýkoli název z druhého oboru názvů.

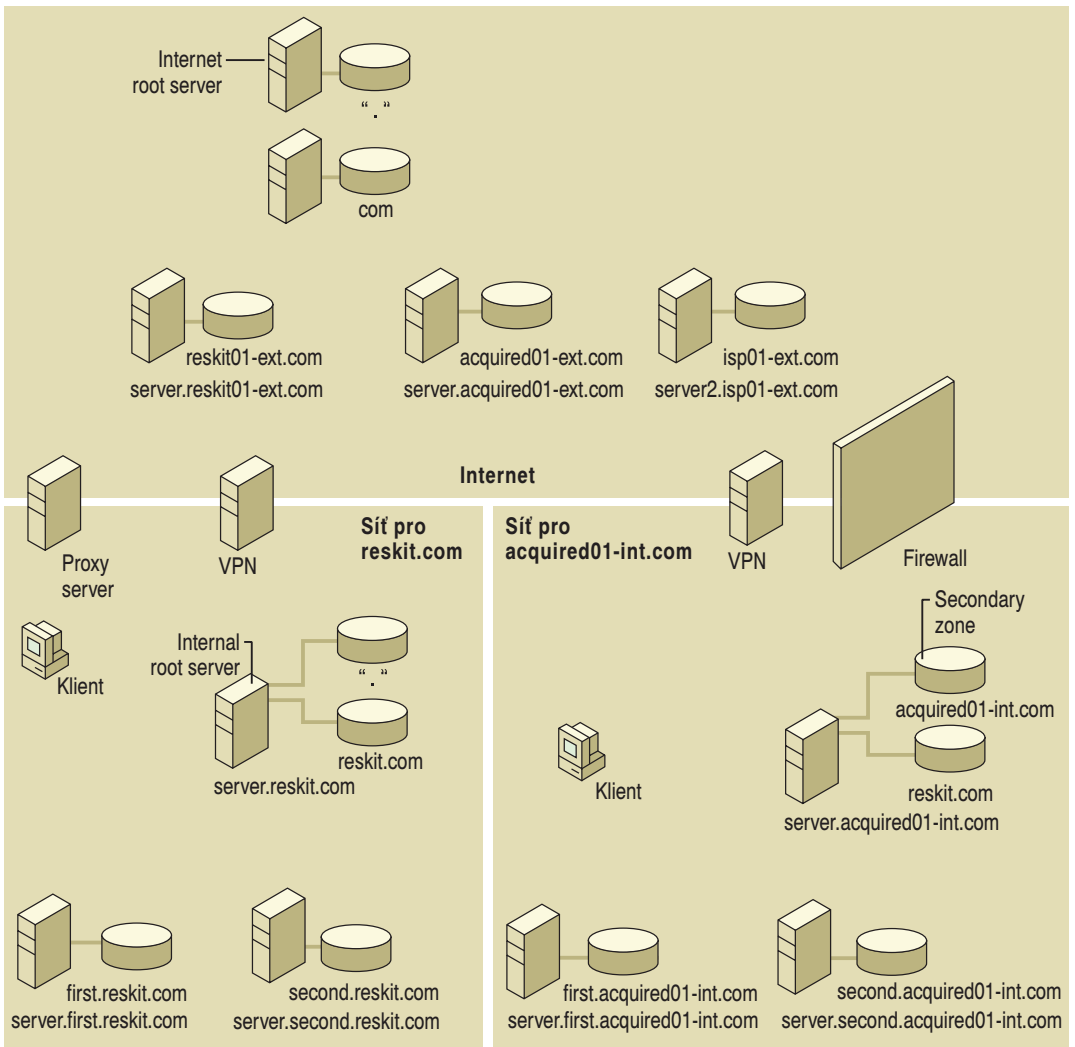
Následující části popisují, jak obě organizace nastavily své vnitřní a vnější obory názvů, aby vyhověly těmto požadavkům. Toto nastavení je znázorněno na obrázku 6.27.

Nastavení vnějšího oboru názvů

Ve vnějším oboru názvů existují dvě zóny: reskit01-ext.com a acquired01-ext.com. Zóny obsahují pouze záznamy (názvy a delegace), které mají být viditelné zvnějšku. Server server.reskit01-ext.com hostí zónu reskit01-ext.com a server server.acquired01-ext.com zónu acquired01-ext.com. Názvy reskit01-ext.com a acquired01-ext.com musí být zaregistrovány u úřadu pro názvy sítě internet.

Nastavení vnitřního oboru názvů

Vnitřní obor názvů organizace, která navenek hostí reskit01-ext.com, je reskit.com. Podobně vnitřní obor názvů organizace, která hostí navenek acquired01-ext.com, je acquired01-int.com. Server server.reskit.com hostí zónu reskit.com a server server.acquired01-int.com hostí zónu acquired01-int.com. Názvy reskit.com a acquired01-int.com musí být registrovány u úřadu pro názvy sítě internet.



Obrázek 6.27 Příklad nastavení domény DNS reskit.com a acquired01-int.com

Všechny počítače v doméně reskit.com podporují buď seznam vyloučení nebo soubor PAC a žádný z počítačů v doméně acquired01-int.com nepodporuje ani seznam vyloučení, ani soubor PAC.

Obor názvů bez klientů proxy podporujících seznam vyloučení nebo soubor PAC

Pro obor názvů, v němž žádný z počítačů není klient proxy, který podporuje buď seznam vyloučení nebo soubor PAC (v tomto příkladě obor názvů acquired01-int.com), musí organizace určit jeden nebo více serverů DNS, který bude udržovat zóny obsahující všechny názvy z vnitřního oboru názvů. Každý klient DNS musí posílat dotazy DNS na jeden nebo více z těchto serverů DNS. Pokud server DNS obsahuje zónu nejvyšší

úrovně oboru názvů organizace (například acquired01-int.com), musí předat tyto dotazy přes server firewall na jeden nebo více serverů DNS v oboru názvů sítě internet. Všechny další servery DNS musí předávat dotazy jednomu nebo více serverům DNS, které obsahují zónu nejvyšší úrovně oboru názvů organizace.

K zajištění toho, aby každý klient v organizaci mohl přeložit jakýkoli název z připojené organizace, musí každý server DNS obsahující zónu nejvyšší úrovně oboru názvů organizace zahrnovat také zóny obsahující všechny vnitřní a vnější názvy připojené organizace.

Toto řešení klade značné zatížení na vnitřní servery DNS, které obsahují vnitřní zóny nejvyšší úrovně organizace. Většina z dotazů generovaných v organizaci je předávána těmto serverům, a to včetně dotazů na počítače ve vnějším oboru názvů a v privátním oboru názvů připojené organizace. Servery také musí obsahovat sekundární kopie zón připojené organizace.

Obor názvů s klienty proxy podporujícími seznam vyloučení nebo soubor PAC

V oboru názvů, ve kterém jsou všechny počítače klienty proxy, kteří podporují buď seznam vyloučení nebo soubor PAC (například obor názvů reskit.com), může privátní obor názvů obsahovat privátní kořen. Ve vnitřním oboru názvů může být jeden nebo více kořenových serverů a všechny ostatní servery DNS musí ve svých souborech odkazů na kořenové servery obsahovat název a adresu IP kořenového serveru.

K překladu vnitřních a vnějších názvů musí každý klient DNS postoupit všechny dotazy buď vnitřním serverům DNS nebo serveru proxy na základě seznamu vyloučení nebo souboru PAC.

Aby opravdu každý klient v organizaci mohl přeložit každý název z připojené organizace, musí privátní kořenová zóna obsahovat delegaci na zónu nejvyšší úrovně připojené organizace.

Používání klientů proxy a privátního kořene zjednodušuje nastavení DNS, protože žádný ze serverů DNS nemusí obsahovat sekundární kopii zóny. Nicméně toto nastavení vyžaduje, abyste vytvořili a spravovali seznamy vyloučení nebo soubory PAC, které je nutno přidat na každého klienta proxy v síti.

Příklady dotazů

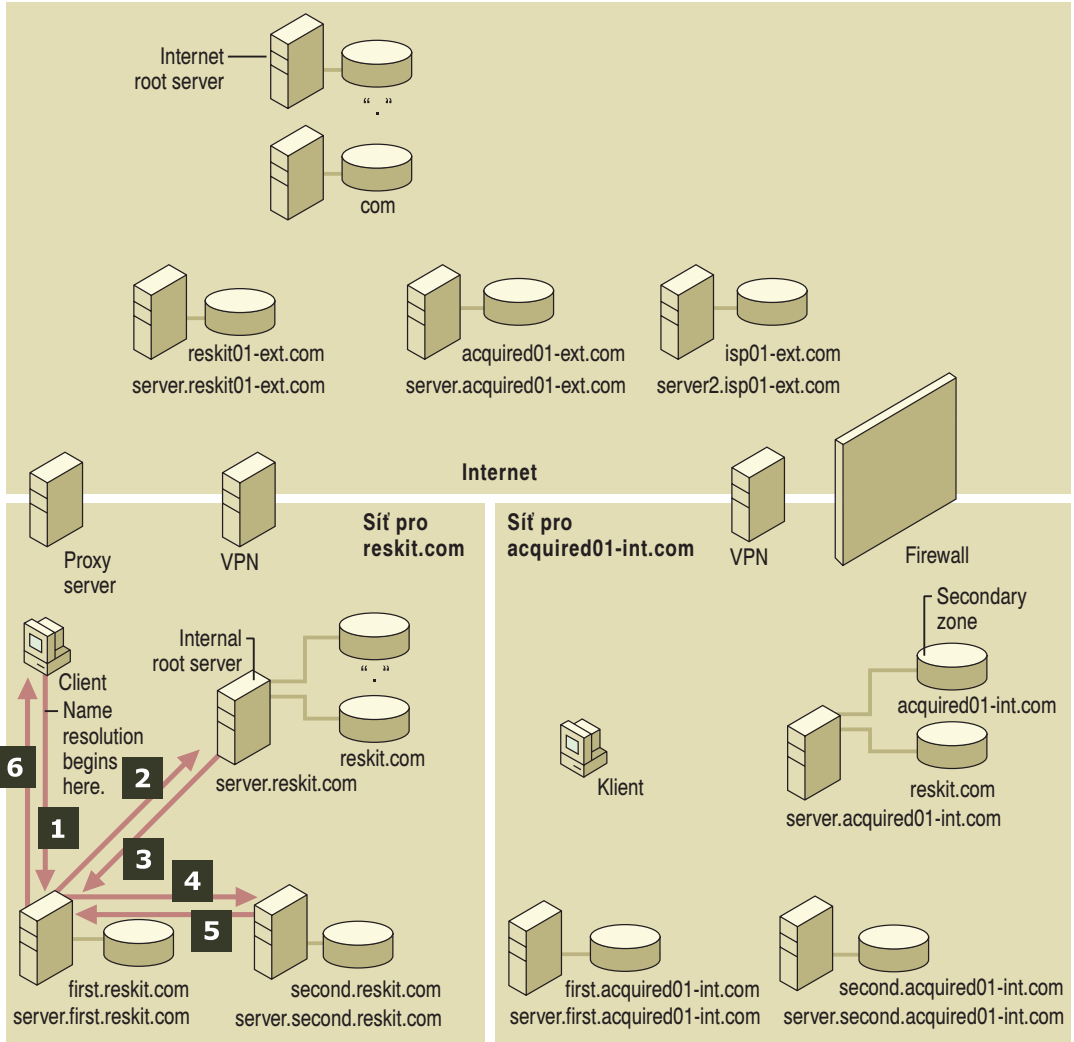
Následující příklady ukazují, jak jsou přeloženy tyto názvy:

- Vnitřní název
- Název na síti internet
- Název ve vnějším oboru názvů organizace
- Název ve vnitřním oboru názvů připojené organizace

Poznámka: Ve všech těchto příkladech nemá žádný server DNS uložený název, na který se klient dotazuje, v mezipaměti. Skutečný dotaz se může zpracovávat jinak, protože název může být uložen v paměti.

Dotaz na název ve vnitřním oboru názvů

Předpokládejte, že počítač v doméně reskit.com potřebuje vyřešit dotaz DNS na název host.second.reskit.com. Nejprve počítač projde svůj seznam vyloučení nebo soubor PAC a zjistí, že název host.second.reskit.com je ve vnitřním oboru názvů. Proto postoupí dotaz lokálnímu serveru DNS. Na obrázku 6.28 je znázorněn postup zpracování tohoto dotazu.



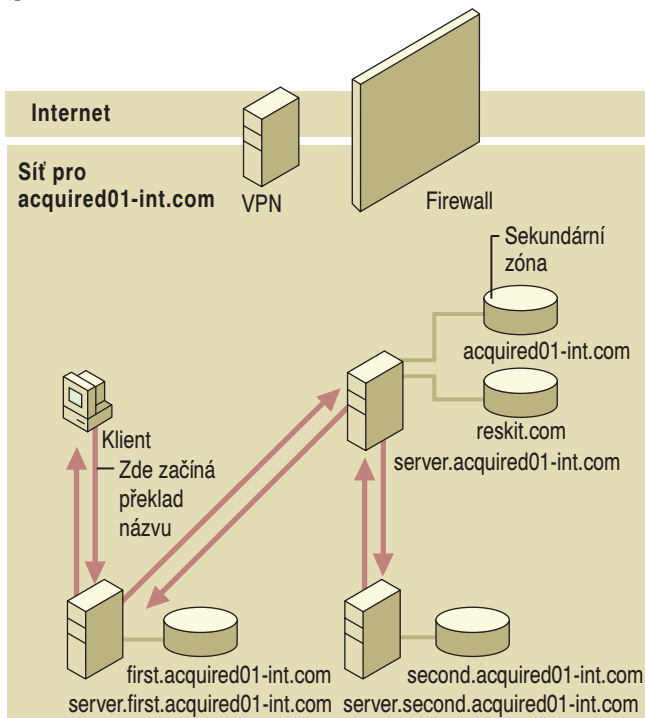
Obrázek 6.28 Dotaz na vnitřní název v doméně reskit.com

Dotaz je zpracováván následujícím způsobem:

1. Počítač postoupí dotaz lokálnímu serveru DNS, server.first.reskit.com.
2. Jestliže lokální server není pro název host.second.reskit.com určující, dotáže se kořenového serveru.

3. Kořenový server vrátí odkaz na určující server, server.second.reskit.com.
4. Lokální server server.first.reskit.com se dotáže serveru server.second.reskit.com.
5. Server.second.reskit.com vyřeší dotaz a vrátí odpověď lokálnímu serveru.
6. Server server.first.reskit.com předá odpověď klientovi.

Nyní předpokládejte, že počítač v doméně acquired01-int.com potřebuje vyřešit dotaz DNS pro název host.second.acquired01-int.com. Na obrázku 6.29 je znázorněn postup zpracování tohoto dotazu.



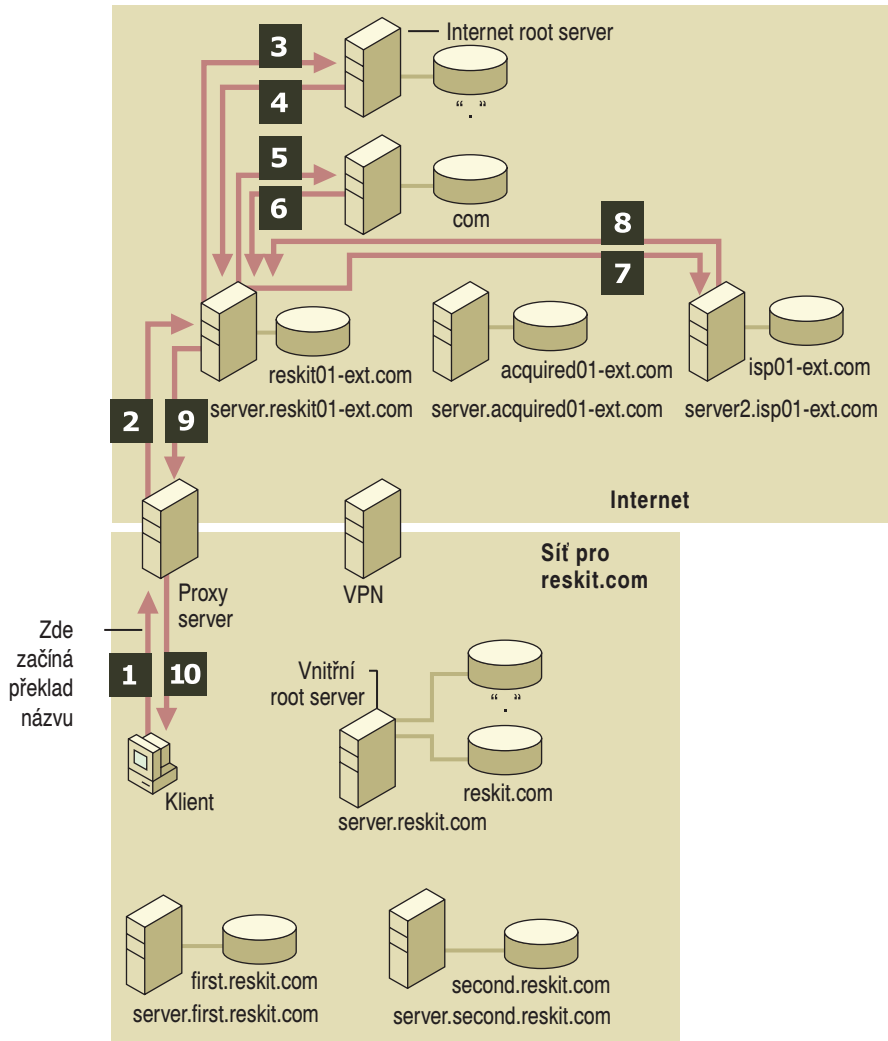
Obrázek 6.29 Dotaz na vnitřní název v doméně `acquired01-int.com`

Dotaz je zpracováván následujícím způsobem:

1. Počítač postoupí dotaz lokálnímu serveru DNS, `server.first.acquired-01.int.com`.
2. Jestliže lokální server není pro název `host.second.acquired01-int.com` určující, předá dotaz serveru DNS, který je určující pro zónu `acquired-01.int.com`.
3. Server DNS určující pro zónu `acquired-01.int.com` najde delegaci na server `server.second.acquired01-int.com` a dotáže se tohoto serveru.
4. Server `server.second.acquired01-int.com` vyřeší dotaz a vrátí název serveru DNS určujícímu pro zónu `acquired-01.int.com`.
5. Server DNS určující pro zónu `acquired-01.int.com` vrátí název lokálnímu serveru DNS.
6. Server `server.first.acquired-01.int.com` vrátí název klientovi.

Dotaz na název ve vnějším oboru názvů

Předpokládejte, že počítač v doméně reskit.com potřebuje přistoupit na stránku www na počítači host.isp01-ext.com. Na obrázku 6.30 je znázorněn postup zpracování tohoto dotazu.

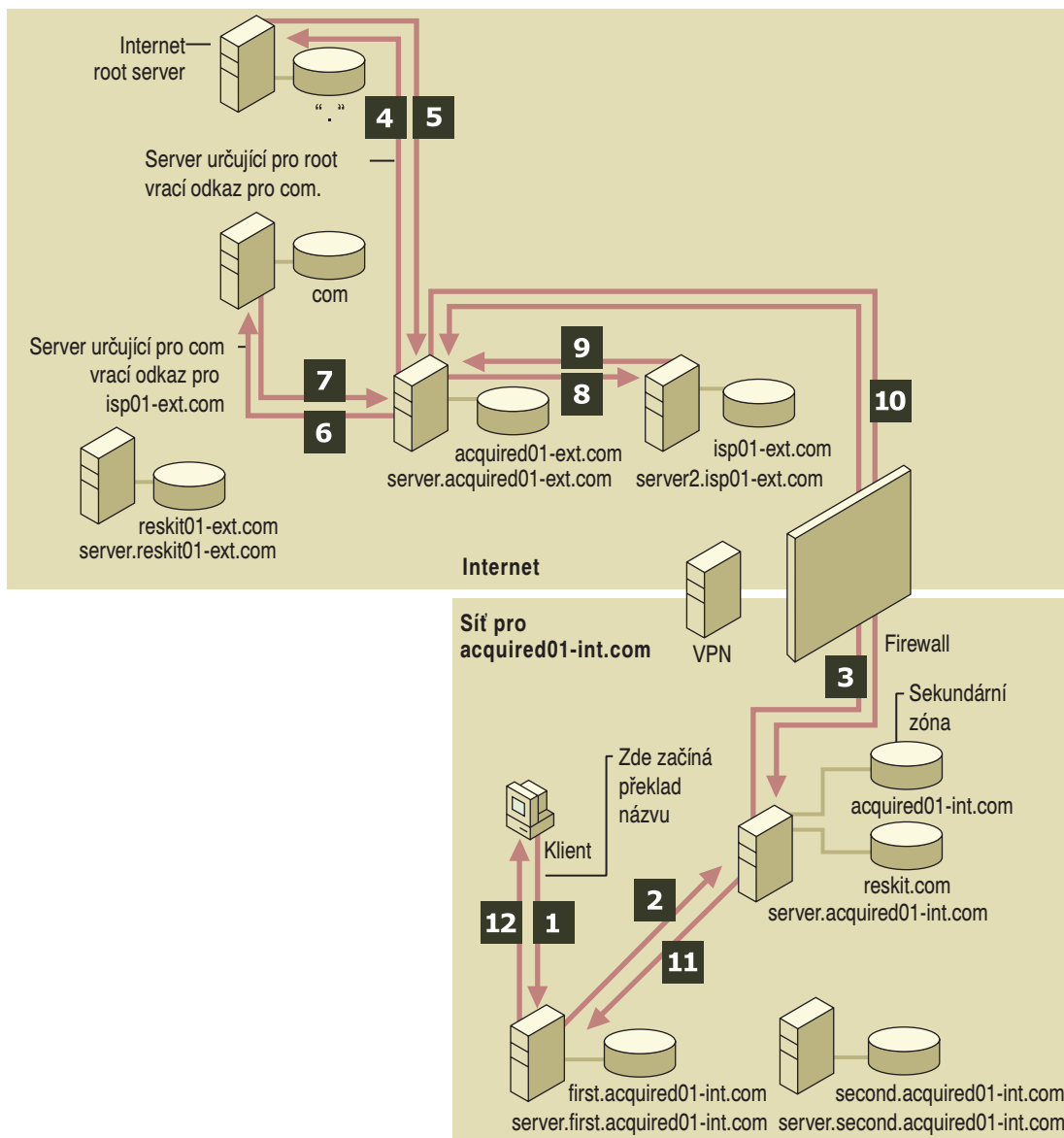


Obrázek 6.30 Dotaz v doméně reskit.com na název v síti internet

Dotaz je zpracováván následujícím způsobem:

1. Vzhledem k tomu, že klient využívá proxy, projde svůj seznam vyloučení nebo soubor PAC a zjistí, že daný název není ve vnitřním oboru názvů. Proto klient pošle požadavek na server proxy.
2. Server proxy pošle dotaz na server DNS, na který je nastaven posílat dotazy. V tomto případě je to server server.reskit01-ext.com.

3. Server server.reskit01-ext.com pošle dotaz na kořenový server sítě internet.
4. Kořenový server sítě internet vrátí odkaz na server, který je určující pro zónu internetu com.
5. Server server.reskit01-ext.com se dotáže serveru určujícího pro zónu com.
6. Server oprávněný pro zónu com vrátí odkaz na server, který je určující pro zónu isp01-ext.com.



Obrázek 6.31 Dotaz v doméně `acquired01-int.com` na název v síti internet

7. Server server.reskit01-ext.com se dotáže serveru určujícího pro zónu isp01-ext.com.
8. Server, který je určující pro zónu isp01-ext.com vrátí adresu IP, která odpovídá názvu host.isp01-ext.com.
9. Server server.reskit01-ext.com vrátí odpověď serveru proxy.
10. Server proxy použije adresu IP k připojení k hostiteli host.isp01-ext.com a poskytne potřebné informace klientovi.

Nyní předpokládejte, že počítač v doméně acquired01-int.com potřebuje vyřešit dotaz DNS na host.isp01-ext.com. Na obrázku 6.31 je znázorněn postup zpracování tohoto dotazu.

Dotaz je zpracováván následujícím způsobem:

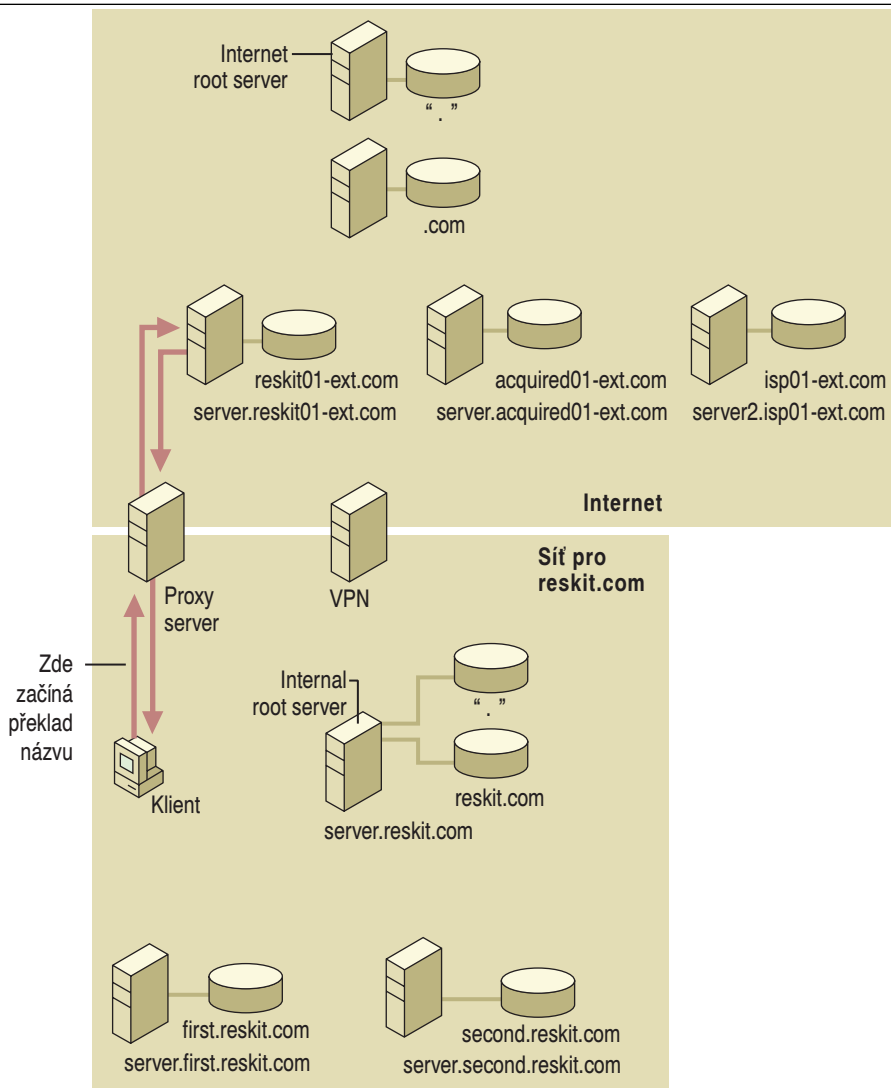
1. Počítač se dotáže svého lokálního serveru DNS, server.first.acquired01-int.com.
2. Pokud mezipaměť serveru neobsahuje požadovaná data, lokální server DNS předá dotaz na server DNS určující pro zónu acquired01-int.com, server.acquired01-int.com.
3. Server server.acquired01-int.com předá dotaz vnějšímu serveru server.acquired01-ext.com přes server firewall.
4. Server server.acquired01-ext.com pošle dotaz kořenovému serveru sítě internet.
5. Kořenový server sítě internet vrátí odkaz na server, který je určující pro zónu internetu com.
6. Server server.acquired01-ext.com se dotáže serveru, který je určující pro zónu com.
7. Server, který je oprávněný pro zónu com, vrátí odkaz na server, který je určující pro zónu isp01-ext.com.
8. Server server.acquired01-ext.com se dotáže serveru určujícího pro zónu isp01-ext.com.
9. Server, který je určující pro zónu isp01-ext.com, vrátí adresu IP odpovídající názvu host.isp01-ext.com.
10. Server server.acquired01-ext.com vrátí adresu IP serveru server.acquired01-int.com přes server firewall.
11. Server.acquired01-int.com vrátí adresu IP lokálnímu serveru DNS server.first.acquired01-int.com.
12. Server server.first.acquired01-int.com vrátí adresu IP klientovi. Klient se může k hostiteli připojit přes server firewall a stáhnout žádanou stránku WWW.

Dotaz na název ve vnějším oboru názvů organizace

Předpokládejte, že počítač v doméně reskit.com potřebuje přistoupit ke stránce WWW ve vnější zóně. Na obrázku 6.32 je znázorněn postup zpracování tohoto dotazu.

Dotaz je zpracováván následujícím způsobem:

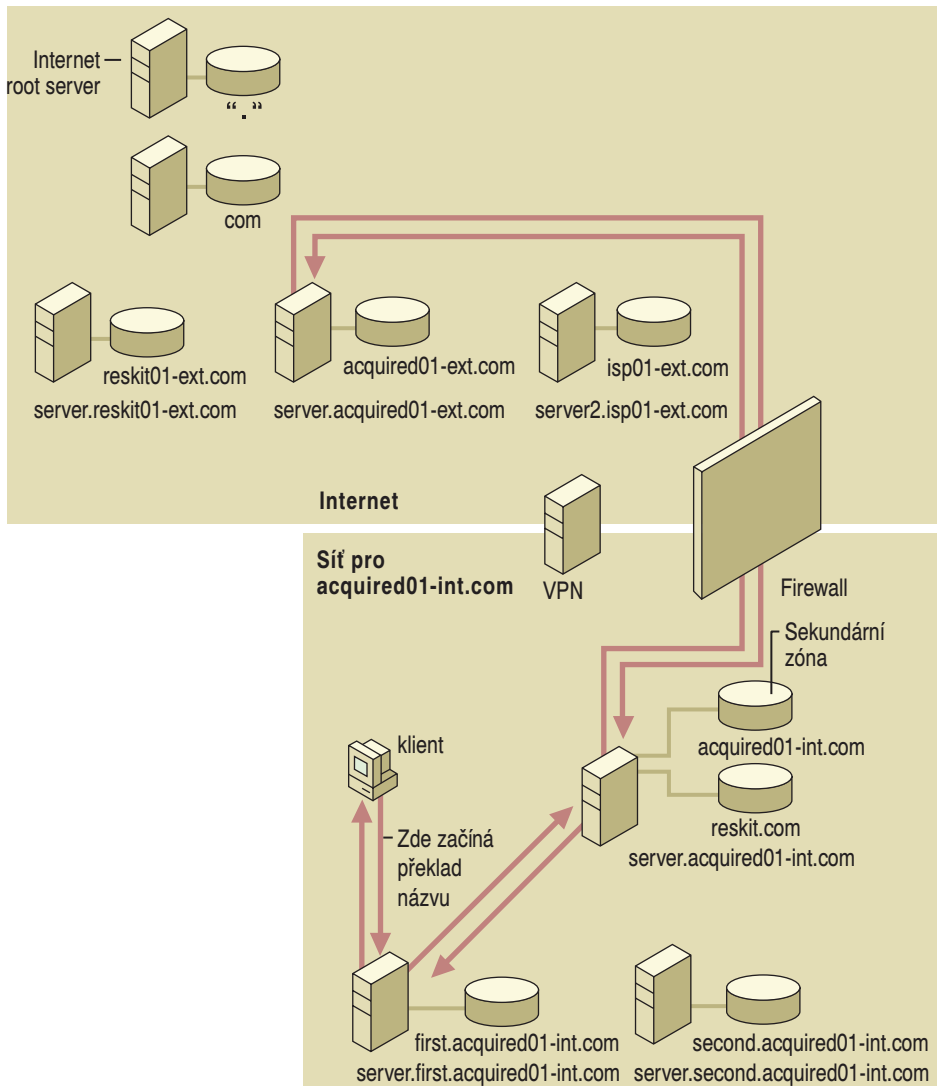
1. Vzhledem k tomu, že klient využívá proxy, projde svůj seznam vyloučení nebo soubor PAC. Když nenajde daný název, pošle požadavek na server proxy.
2. Server proxy předloží dotaz serveru DNS, který je nastaven používat, server.reskit01-ext.com. V tomto příkladě je server.reskit01-ext.com také určující pro .
3. Server server.reskit01-ext.com vyřeší dotaz a vrátí odpověď serveru proxy.



Obrázek 6.32 Dotaz na název ve vnější zóně `reskit01-ext.com`

4. Server proxy použije výslednou adresu IP a připojí se k serveru `server.reskit.com` a poskytne klientovi potřebné informace.

Nyní předpokládejte, že počítač v zóně `acquired01-int.com` potřebuje otevřít stránku WWW ve vnější zóně. Na obrázku 6.33 je znázorněn postup zpracování tohoto dotazu.



Obrázek 6.33 Dotaz na název ve vnější zóně acquired01-ext.com

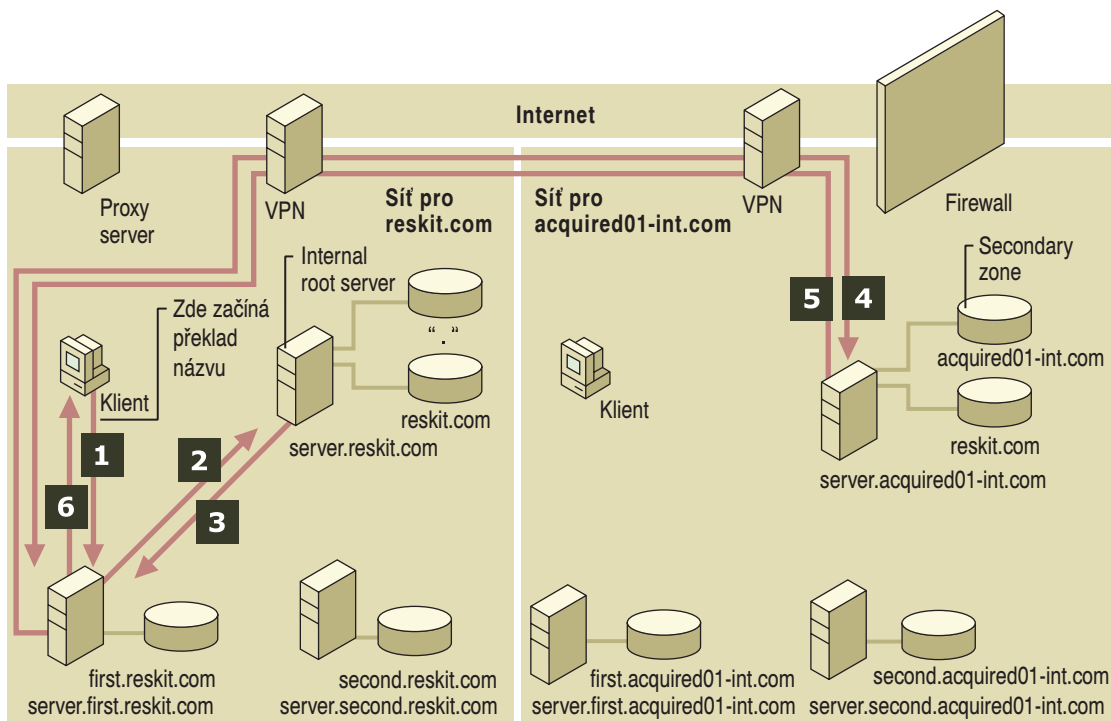
Dotaz je zpracováván následujícím způsobem:

1. Počítač se dotáže svého lokálního serveru DNS, server.first.acquired01-int.com.
2. Pokud mezipaměť serveru neobsahuje požadovaná data, server server.first.acquired01-int.com předá dotaz na server DNS určující pro zónu acquired01-int.com.
3. Server určující pro zónu acquired01-int.com předá požadavek přes server firewall na server server.acquired01-ext.com.
4. Server server.acquired01-ext.com přeloží název a vrátí odpověď serveru server.acquired01-int.com přes server firewall.

5. Server.first.acquired01-int.com vrátí odpověď serveru DNS server.first.acquired01-int.com.
6. Server server.first.acquired01-int.com vrátí odpověď klientovi. Klient pak použije adresu IP k připojení přes server firewall na stránku WWW, která je umístěna na síti internet.

Dotaz na název v oboru názvů připojené organizace

Předpokládejte, že se počítač v doméně reskit.com potřebuje připojit k hostiteli host.acquired01-int.com. Na obrázku 6.34 je znázorněn postup zpracování tohoto dotazu.



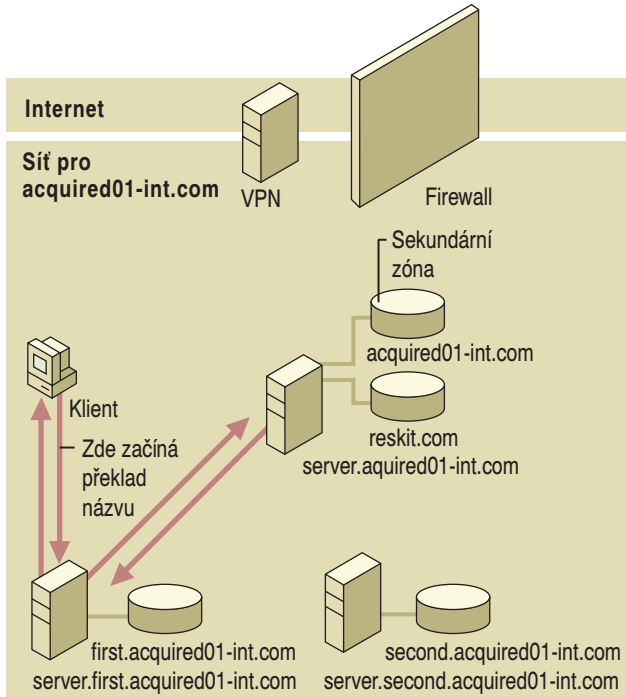
Obrázek 6.34 Dotaz na název v oboru názvů zóny acquired01-int.com

Dotaz je zpracováván následujícím způsobem:

1. Vzhledem k tomu, že klient využívá proxy, projde svůj seznam vyloučení nebo soubor PAC a předloží dotaz na název host.acquired01-int.com lokálnímu serveru DNS, server.first.reskit.com.
2. Jestliže mezipaměť neobsahuje požadovaná data, server se dotáže vnitřního kořenového serveru.
3. Kořenový server najde delegaci na zónu acquired01-int.com a vrátí adresu IP serveru, který je určující pro zónu acquired01-int.com lokálnímu serveru DNS.
4. Lokální server DNS předloží dotaz serveru, který je určující pro zónu acquired01-int.com.

5. Vzhledem k tomu, že tento server je určující pro zónu acquired01-int.com, vyřeší dotaz a vrátí lokálnímu serveru DNS odpověď.
6. Lokální server server.first.reskit.com vrátí odpověď klientovi.

Nyní předpokládejte, že se počítač v zóně acquired01-int.com potřebuje připojit k počítači host.reskit.com. Na obrázku 6.35 je znázorněn postup zpracování tohoto dotazu.



Obrázek 6.35 Dotaz na název v oboru názvů reskit.com

Dotaz je zpracováván následujícím způsobem:

1. Počítač předloží dotaz svému lokálnímu serveru DNS, server.first.acquired01-int.com.
2. Pokud mezipaměť neobsahuje požadovaná data, server předá dotaz na server DNS, který je určující pro zónu acquired01-int.com.
3. Vzhledem k tomu, že server DNS, který je určující pro zónu acquired01-int.com, obsahuje sekundární kopii zóny reskit.com, vyřeší dotaz a vrátí odpověď lokálnímu serveru server.first.acquired01-int.com.
4. Server server.first.acquired01-int.com vrátí odpověď klientovi.

Řešení problémů

Následující části popisují užitečné nástroje pro řešení problémů, poskytují nejlepší postupy pro vyvarování se chyb, obsahují seznam postupů, které vám pomohou při ověřování správnosti nastavení serverů názvů, a vysvětlují, jak diagnostikovat a vyřešit běžné problémy služby DNS.

Nástroje pro řešení problémů

Operační systém Windows 2000 poskytuje mnoho nástrojů, které vám mohou pomoci diagnostikovat a vyřešit problémy se službou DNS. Tato část se věnuje následujícím nástrojům:

Nslookup Nástroj Nslookup můžete používat k provádění dotazů DNS a kontrole obsahu souborů zón na lokálních i vzdálených serverech.

Ipconfig Nástroj Ipconfig můžete používat k prohlížení nastavení klienta DNS, zobrazení a vyprázdnění mezipaměti překladače a donucení klienta s dynamickou aktualizací k registraci svých záznamů DNS.

Prohlížeč událostí Prohlížeč událostí můžete používat k prohlížení chybových hlášení klienta DNS a serveru DNS.

Protokol služby DNS Server DNS můžete nastavit tak, aby sledoval určité události a protokoloval je do protokolu DNS pro další zkoumání.

Příkaz přesměrovače sítě U klienta DNS lze zastavit ukládání do mezipaměti a vyprázdnit mezipaměť pomocí příkazů přesměrovače sítě **net start** a **net stop**.

Sledování v konzole DNS Pomocí možností na záložce **Sledování** v konzole DNS lze provádět testovací dotazy.

Pomocí nástroje Sledování sítě můžete zkoumat oktety odesílané a přijímané servery DNS na vaší síti. Více informací o tomto nástroji najdete v knize *Microsoft® Windows® 2000 Server Správa systému* v části „Sledování výkonu sítě“.

K rychlé identifikaci problémů s nastavením služby DNS můžete použít také nástroj Netdiag. Více informací o tomto nástroji najdete v části „Řešení problémů protokolu TCP/IP“.

Nástroj Nslookup

Nslookup je standardní nástroj příkazové řádky poskytovaný ve většině implementací služby DNS včetně operačního systému Windows 2000. Nástroj Nslookup poskytuje možnost provádět testování dotazů serverů DNS a získat podrobné odpovědi na příkazovém řádku. Tyto informace mohou být užitečné při diagnostice a řešení problémů s překladem názvu, při ověření přidání záznamů prostředku do zóny nebo jejich správné aktualizace v zóně a při odstraňování dalších problémů spojených se serverem. Tato část popisuje, jak provádět řešení problémů a obsahuje seznam a vysvětlení chybových hlášení nástroje Nslookup.

Informace o přesné syntaxi nástroje Nslookup najdete v nápovědě Windows 2000 Server nebo v nástroji Nslookup po zadání příkazu `help` na příkazové řádce.

Provádění jednoduchých úloh pomocí nástroje Nslookup

Tato část popisuje, jak provádět následující jednoduché úlohy řešení problémů:

- Pro vyhledání jednoduchých údajů použijte nástroj Nslookup v neinteraktivním režimu
- Zapněte interaktivní režim a použijte vlastnost ladění
- Proveďte z interaktivního režimu následující úlohy:
 - Nastavte možnosti dotazu
 - Vyhledejte název

- Vyhledejte v zóně záznam
- Proveďte zónový přenos
- Opusťte nástroj Nslookup

Poznámka: Při vkládání dotazů je zpravidla vhodné vkládat názvy FQDN, takže můžete kontrolovat, jaký název je serveru předán. Nicméně pokud chcete vědět, jaké přípony jsou připojovány k neúplným názvům před jejich předáním serveru, můžete přepnout nástroj Nslookup do ladicího režimu a pak vložit neúplný název.

► Používání nástroje Nslookup v neinteraktivním režimu

- Napište následující příkaz a stiskněte ENTER:

nslookup <název> <server>

kde *název* je vlastník záznamu, který hledáte, a *server* je *server*, který chcete dotázat.

V interaktivním režimu můžete vyhledávat více než jeden údaj. Spuštění nástroje Nslookup s parametrem na příkazové řádce -d2 přepne nástroj Nslookup do interaktivního režimu s povoleným ladicím režimem výstupu. Ladicí režim výstupu umožňuje zkoumat pakety dotazů a odpovědí mezi překladačem a serverem.

► Spuštění nástroje Nslookup v interaktivním režimu

- Napište následující příkaz a stiskněte ENTER:

nslookup [-d2]

► Vypnutí interaktivního režimu

- Napište následující příkaz a stiskněte ENTER:

exit

V interaktivním režimu můžete použít příkaz **set**, kterým nastavíte, jak bude překladač provádět dotazy. Tabulka 6.14 obsahuje několik možností dostupných s příkazem **set**:

Tabulka 6.14 Možnosti příkazového řádku dostupné s příkazem **set**

Možnost	Účel
set all	Zobrazí všechny možnosti dostupné s příkazem set .
set d2	Přepne nástroj Nslookup do ladicího režimu, takže můžete zkoumat pakety dotazů a odpovědí mezi překladačem a serverem.
set domain=<název domény>	Určuje překladači, který název domény připojit k neúplným dotazům.
set timeout=<časový limit>	Určuje překladači, jaký časový limit použít. tato možnost je užitečná pro pomalá připojení, kde dotazy často vyprší a je nutno prodloužit čekací dobu.
set type=<typ záznamu> -nebo-	Určuje překladači, jaký typ záznamu prostředku hledat (například A, PTR nebo SRV). Chcete-li, aby se překladač ptal na všechny typy záznamů prostředku, napište set type=all .
set querytype=<typ záznamu> -nebo-	
set q=<typ záznamu>	

Můžete vyhledat jeden název.

► Vyhledávání názvů v interaktivním režimu

- Napište následující příkaz a stiskněte ENTER:

<název> [server]

kde název je vlastník záznamu, který hledáte, a server je server, který chcete dotázat.

V dotazu můžete použít zástupný znak (*). Například pokud chcete vyhledat všechny záznamy prostředku, které mají jako první písmeno „K“, můžete napsat následující:

K*

S nástrojem Nslookup lze také prohlížet obsah domén.

► Prohlížení obsahu domény

- Napište následující příkaz a stiskněte ENTER:

set type=*<typ záznamu>*

ls -t *<název domény>*

kde typ záznamu je typ záznamu (pokud chcete prohlédnout všechny záznamy, použijte příkaz any) a název domény je název domény, kterou chcete prohlížet.

Přidáním přepínače **-d** můžete simulovat a testovat zónový přenos. To může pomoci při určení, jestli dotazovaný server umožňuje nebo neumožňuje zónové přenosy na váš počítač.

► Simulace zónového přenosu

- Napište následující příkaz a stiskněte ENTER:

ls -d *<název domény>*

Nástroj Nslookup poskytuje nápovědu na příkazové řádce.

► Získání nápovědy v interaktivním režimu

- Napište následující příkaz a stiskněte ENTER:

help nebo **?**

Chyby nástroje Nslookup

Úspěšná odpověď nástroje Nslookup vypadá takto:

Server: *<název serveru DNS>*

Address: *<adresa IP serveru DNS>*

<Data odpovědi>

Nástroj Nslookup může vrátit také jednu z následujících chyb. Následující zprávy znamenají, že překladatel nelokalizoval záznam prostředku PTR (obsahující název hostitele) pro adresu IP serveru. Nástroj Nslookup může posílat dotazy na server DNS a server DNS může tyto dotazy zodpovídat. Více informací o používání nástroje Nslookup k ověření nastavení služby DNS najdete v části „Ověření základního nastavení služby DNS“.

Časový limit dotazu DNS vypršel.

Časový limit byl *<x>* sekund.

*** Nelze najít název serveru pro adresu *<adresa IP>*: Časový limit vypršel

*** Přednastavené servery nejsou dostupné

Přednastavený server: Neznámý

Adresa: <adresa IP serveru DNS>

Následující zprávy znamenají, že časový limit dotazu vypršel. To se může stát, například, když služba DNS nebyla spuštěna na serveru DNS, který je určující pro daný název.

*** Požadavek na <Server> vypršel

Následující zpráva znamená, že server nedostává odpovědi na portu UDP 53. Více informací o řešení problémů se serverem najdete v části „Servery DNS“.

*** <Server> nelze najít <dotazovaný název nebo dotazovaná adresa IP>: Žádná odpověď od serveru

Následující zpráva znamená, že server DNS nebyl schopen najít název nebo adresu IP v určující doméně. Určující doména může být na tomto serveru DNS nebo na jiném serveru DNS, kam je tento server DNS schopen dosáhnout.

*** <Server> nelze najít <dotazovaný název nebo dotazovaná adresa IP>: Neexistující doména

Následující zpráva zpravidla znamená, že server DNS běží, ale nefunguje správně. Například může obsahovat poškozený paket nebo zóna, ve které se dotazujete na záznam, může být pozastavena. Nicméně tato zpráva může být také vrácena, jestliže se klient dotazuje na hostitele v doméně, pro kterou není server DNS určující a server DNS se nemůže připojit ke svým kořenovým serverům, nebo není připojen k síti internet nebo nemá odkazy na kořenové servery.

*** <Server> nelze najít <dotazovaný název nebo dotazovaná adresa IP>: Selhání serveru

Používání nástroje IPConfig

Nástroj příkazové řádky Ipconfig můžete používat k prohlížení nastavení klientů DNS, prohlížení a mazání informací uložených v mezipaměti a používaných lokálně pro řešení dotazů na názvy DNS a k registrování záznamů prostředků klientů s dynamickou aktualizací.

Použijete-li nástroj Ipconfig bez nastavení nějakých parametrů, zobrazí informace DNS pro každý adaptér, a to včetně názvu domény a serverů DNS pro něj používaných.

Tabulka 6.15 obsahuje některé možnosti dostupné pro nástroj Ipconfig z příkazové řádky.

Tabulka 6.15 Příklady příkazů Ipconfig

Příkaz	Akce
ipconfig /all	Zobrazí další informace o službě DNS včetně názvů FQDN a seznamu pro vyhledávání přípon DNS.
ipconfig /flushdns	Vyprázdní a resetuje mezipaměť překladače DNS. Více informací o této možnosti najdete v části „Zastavení a vyprázdnění mezipaměti“.
ipconfig /displaydns	Zobrazí obsah mezipaměti překladače DNS. Více informací o této možnosti najdete v části „Zastavení a vyprázdnění mezipaměti“.

Příkaz	Akce
ipconfig /registerdns	Obnoví všechny zápůjčky DHCP a zaregistruje všechny spojené názvy DNS. Tato možnost je dostupná pouze pro počítače na platformě operačního systému Windows 2000, kde běží služba DHCP Client Service.
ipconfig /release [adapter]	Uvolní všechny zápůjčky DHCP.
ipconfig /renew [adapter]	Obnoví všechny zápůjčky DHCP a dynamicky aktualizuje názvy DNS. Tato možnost je dostupná pouze pro počítače, kde běží služba DHCP Client Service.

Prohlížeč událostí

Prohlížeč událostí protokoluje chyby operačního systému Windows 2000 a služeb, jako je například DNS server. Máte-li problémy se službou DNS, můžete zkontrolovat prohlížeč událostí, jestli tam nenajdete události spojené se službou DNS.

► Otevření prohlížeče událostí

- Klepněte na **Start**, vyberte **Programy**, vyberte **Nástroje pro správu** a pak klepněte na **Prohlížeč událostí**.

K prohlížení zpráv o serveru DNS klepněte na **Server DNS**.

-nebo-

K prohlížení zpráv o klientovi DNS klepněte na **Protokol systému**.

Více informací o Prohlížeči událostí najdete v nápovědě Windows 2000.

Protokol DNS

Server DNS lze nastavit tak, aby vytvářel soubor protokolu, který zaznamenává následující typy událostí:

- Dotazy
- Zprávy upozornění od ostatních serverů
- Dynamické aktualizace
- Obsah otázkové části dotazu DNS
- Obsah odpovědní části dotazu DNS
- Počet dotazů odeslaných tímto serverem
- Počet dotazů přijatých tímto serverem
- Počet požadavků DNS přijatých přes port UDP
- Počet požadavků DNS přijatých přes port TCP
- Počet úplných paketů odeslaných serverem
- Počet paketů zapisovaných přes server zpět do zóny

Protokol DNS je umístěn v adresáři % Systemroot%\System32\dns\Dns.log. Vzhledem k tomu, že protokol je ve formátu RTF, musíte k jeho prohlížení použít například WordPad.

Adresář a název souboru, ve kterém se protokol DNS nachází, můžete změnit přidáním následujícího záznamu do registru s typem dat REG_SZ:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS
\Parameters**LogFilePath**

Hodnotu záznamu LogFilePath nastavte tak, aby byla rovna cestě souboru a názvu souboru, kde chcete umístit protokol DNS.

Dle výchozího nastavení je maximální velikost souboru Dns.log 4 MB. Chcete-li tuto velikost změnit, přidejte do registru následující záznam s typem dat REG_DWORD:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS
\Parameters**LogFileMaxSize**

Hodnotu záznamu LogFileMaxSize nastavte tak, aby byla rovna požadované velikosti souboru v bajtech. Minimální velikost je 64 KB.

Jakmile soubor protokolu dosáhne maximální velikosti, operační systém Windows 2000 přepíše začátek souboru. Zvýšíte-li hodnotu LogFileMaxSize data se uchovají delší dobu, ale protokol spotřebuje více prostoru na disku. Snížíte-li hodnotu LogFileMaxSize, soubor protokolu spotřebuje méně prostoru na disku, ale data se uchovají kratší dobu.

Upozornění: Nespouštějte protokolování DNS během normálních operací, protože zabírá prostředky jak procesoru, tak pevného disku. Povolte ho pouze při diagnostice a řešení problémů se službou DNS.

► **Nastavení serveru, aby zapisoval události do protokolu DNS**

1. V konzole DNS klepněte na pole serveru, klepněte pravým tlačítkem na server a vyberte Vlastnosti.
2. Klepněte na záložku **Protokolování** a pak vyberte možnosti, které chcete protokolovat.

Zastavení a vyprázdnění mezipaměti

Kromě vyprazdňování mezipaměti pomocí nástroje Ipconfig můžete mezipaměť zastavit a vyprázdnit pomocí zastavení a spuštění klienta.

► **Zastavení klienta**

- Na příkazové řádce napište následující příkaz:

net stop „dns client“

► **Spuštění klienta**

- Na příkazové řádce napište následující příkaz:

net start „dns client“

Sledování v konzole DNS

K provádění testovacích dotazů, pomocí kterých zjistíte, jestli server pracuje nebo nepracuje správně, můžete použít konzolu DNS.

► **Provedení testovacích dotazů z konzoly DNS**

1. V konzole DNS poklepejte na název serveru a rozviňte tak informace o serveru.
2. Klepněte pravým tlačítkem na server a pak klepněte na **Vlastnosti**.
3. Klepněte na záložku **Sledování**.
4. Vyberte test, který chcete provést a pak klepněte na příkaz **Testovat nyní**.

Pokud jednoduchý dotaz selže, zkontrolujte, jestli lokální server obsahuje zónu 1.0.0.127.in-addr.arpa. Jestliže selže rekurzivní dotaz, zkontrolujte, jestli jsou odkazy na

kořenové servery správné a jestli jsou kořenové servery spuštěné. Více informací o jednoduchých dotazech a rekurzivních dotazech najdete v části „Úvod do služby DNS“.

Více informací o řešení problémů s rekurzí najdete v části „Diagnostika problémů s rekurzí“.

Rady pro nastavení a správu služby DNS

Projďte si následující návrhy, zabráníte tím běžným chybám v nastavení:

- Vložte správnou adresu elektronické pošty odpovědné osoby pro každou zónu, kterou přidáváte na server DNS, nebo kterou tam spravujete.

Toto pole se používá k vyrozumění správců DNS o mnoha věcech. Například toto pole lze použít k hlášení chyb dotazů, nesprávných dat vrácených v dotazu a problémů se zabezpečením. Přestože většina adres elektronické pošty obsahuje při použití v aplikacích elektronické pošty znak @, musíte ho v tomto poli nahradit tečkou (.). Například místo napíšete administrator.reskit.com.

- Při navrhování sítě DNS používejte standardní směrnice a kdykoli je to možné, dodržujte při správě infrastruktury DNS preferovanou praxi.
- Zajistěte, aby každou zónu hostily minimálně dva servery. Mohou hostit buď primární a sekundární kopii zóny nebo dvě kopie každé zóny integrované s adresářovou službou.
- Používáte-li služby Active Directory, používejte pro zóny ukládání integrované s adresářovou službou.

V integrované zóně odpovídají řadiče domén každé domény služby Active Directory v přímém mapování jeden na jeden serverům DNS. Při řešení problémů se službou DNS a replikacemi služby Active Directory se používají stejné servery v obou topologiích, což zjednodušuje plánování, instalaci a řešení problémů.

Používání ukládání integrovaného s adresářovou službou také zjednodušuje aktualizace u klientů DNS s operačním systémem Windows 2000. Nastavíte-li seznam preferovaných a alternativních serverů DNS pro každého klienta, můžete specifikovat servery odpovídající řadičům domén umístěným blízko každého klienta. Pokud selže aktualizace klienta s jeho preferovaným serverem, protože tento server není dostupný, klient zkusí alternativní server. Jakmile je preferovaný server dostupný, nahraje aktualizovanou zónu integrovanou s adresářovou službou, která obsahuje aktualizace již klientem provedené.

- Nepoužíváte-li integraci se službou Active Directory, nastavte správně klienty a uvědomte si, že se standardní primární zóna stane jediným selhávajícím článkem dynamických aktualizací a replikací zón.

Standardní primární zóny jsou nutné pro vytváření a správu zón ve vašem oboru názvů DNS, pokud nepoužíváte službu Active Directory. V tomto případě se aplikuje model aktualizace jediného hlavního serveru s jedním serverem DNS určeným jako primární server zóny. Jak je určeno ve vlastnostech záznamu SOA zóny, pouze primární server může provést aktualizaci takové zóny.

Z tohoto důvodu zajistěte, aby byl tento server DNS spolehlivý a dostupný. V opačném případě klienti nemohou aktualizovat své záznamy prostředku A a PTR.

- Zvažte používání sekundárních serverů a serverů vyrovnávací paměti pro zóny, abyste snížili provoz dotazů DNS.

Sekundární servery lze použít jako zálohu pro klienty DNS, ale lze je použít také jako preferované servery DNS pro původní klienty DNS. Ve smíšených prostředích vám toto umožní vyrovnat zatížení provozu dotazů DNS na síti. Rezervujte proto primární servery DNS pro klienty na platformě operačního systému Windows 2000, kteří potřebují primární servery k provádění dynamické registrace a aktualizace záznamů prostředku A a PTR.

Organizace IETF vydala několik dokumentů RFC, které shrnují rady a zkušenosti týkající se služby DNS, jak byly doporučeny návrháři služby DNS a projektanty sítě internet. Tyto dokumenty RFC se vám možná budou hodit, zvláště pokud projektujete návrh rozsáhlé služby DNS:

- RFC 1912, „Běžné chyby při práci se službou DNS a jejím nastavením“
- RFC 2182, „Výběr a fungování sekundárních serverů DNS“
- RFC 2219, „Používání aliasů DNS pro síťové služby“.

Ověření základního nastavení služby DNS

Použijete-li k podpoře služby Active Directory server DNS třetích stran, musíte provést nastavení ručně. Při tom můžete způsobit běžné chyby v nastavení, které zabrání v řádném fungování služby DNS a Active Directory. Následující části popisují testy, které můžete provést k ověření správného fungování serveru DNS, správného nastavení zón zpětného vyhledávání a dopředného vyhledávání a podpory služby Active Directory.

Použijete-li k instalaci serveru DNS na platformě operačního systému Windows 2000 průvodce nastavením serveru DNS nebo průvodce instalací služby Active Directory, většina nastavení je provedena automaticky a můžete se tak vyhnout mnoha chybám v nastavení. Nicméně to vám nijak nebrání v provedení testů z této části.

Před kontrolováním čehokoli zkontrolujte nejdříve protokol událostí, jestli v něm nejsou zaznamenány chyby. Více informací o Prohlížeči událostí najdete v části „Nástroje pro řešení problémů“.

Ověření, že server DNS může odpovídat na dotazy

K ověření, že server DNS je spuštěn a může odpovídat na dotazy, proveďte následující postup.

- Ujistěte se, že server má základní připojení k síti. Více informací o ověřování základního připojení k síti najdete v části „Hledání problémů se serverem DNS“.
- Ujistěte se v záložce Sledování v konzole DNS, že server může odpovídat jak na jednoduché, tak na rekurzivní dotazy. Více informací o záložce Sledování najdete v části „Nástroje pro řešení problémů“.
- Z klienta použijte nástroj Nslookup k vyhledání názvu domény a názvu hostitele v doméně. Více informací o používání nástroje Nslookup najdete v části „Nástroje pro řešení problémů“.
- Na serveru spusťte nástroj netdiag a ujistěte se, že server funguje správně a že záznamy prostředku, které potřebuje služba Netlogon, jsou registrovány na serveru. Více informací o službě Netdiag najdete v části „Nástroje pro řešení problémů“.
- Ujistěte se, že server může dosáhnout na kořenový server pomocí následujícího příkazu:

nslookup

server <adresa IP serveru>

set querytype=NS

.

- Ujistěte se, že pro server je nastaven záznamy prostředku A a PTR. Informace o záznamech prostředku PTR najdete v části „Testování zón zpětného vyhledávání a záznamů prostředku PTR“.

Ověření správného nastavení zóny dopředného vyhledávání

Po vytvoření zóny dopředného vyhledávání můžete použít nástroj Nslookup k ujištění, že je správně nastavena a k otestování její integrity se službou Active Directory. Nástroj Nslookup spustíte takto:

Nslookup

server < adresa IP serveru, na kterém je zóna vytvořena>

set querytype=any

Nástroj Nslookup se spustí. Pokud překladač nemůže lokalizovat záznam prostředku PTR pro server, uvidíte chybové hlášení, ale stále budete schopni provést testy této části.

K ověření, že zóna reaguje správně, simulujte zónový přenos pomocí následujícího příkazu:

ls -d <název domény>

Pokud je server nastaven tak, že omezuje zónové přenosy, můžete v Prohlížeči událostí vidět chybové hlášení. (Více informací o Prohlížeči událostí najdete v části „Nástroje pro řešení problémů“.) V opačném případě se zobrazí seznam všech záznamů v doméně.

Dále dotazte se na záznam SOA pomocí následujícího příkazu:

<název domény>

Jestliže je server nastaven správně, zobrazí se záznam SOA. Záznam SOA obsahuje pole „primární server názvů“. K ověření, že primární server názvů zaregistroval záznam NS napište následující příkaz:

set type=ns

<název domény>

Jestliže je server nastaven správně, zobrazí se záznam NS serveru názvů.

Ujistěte se, že se lze připojit k oprávněnému serveru názvů uvedenému v záznamu SOA, aby odpovídal na dotazy, pomocí následujícího příkazu:

server <název serveru nebo adresa IP serveru>

Dále se serveru dotazte na kterýkoli název, pro který je určující.

Jestliže tyto testy proběhly úspěšně, záznam NS vybere správný název hostitele a název hostitele má k sobě připojenou správnou adresu IP.

Testování zón zpětného vyhledávání a záznamů prostředku PTR

Fungování zón zpětného vyhledávání a záznamů prostředku PTR není pro službu Active Directory nutné. Nicméně je potřebujete, jestliže chcete, aby klienti byli schopni přeložit názvy FQDN z adres IP. Záznamy PTR jsou také běžně používány některými aplikacemi pro účely zabezpečení, k ověření totožnosti klienta.

Nepotřebujete mít zóny zpětného vyhledávání a záznamy prostředku PTR na vlastních serverech. Namísto toho může tyto zóny obsahovat jiný server DNS.

Po nastavení zón zpětného vyhledávání a záznamů prostředku PTR je ručně zkontrolujte v konzole DNS. Zóna zpětného vyhledávání musí existovat pro každou podsít a nadřazená zóna zpětného vyhledávání musí mít delegaci na vaši zónu zpětného vyhledávání. Například máte-li privátní kořen a podsítě 172.32.16.x a 172.32.17.x, privátní kořen může hostit všechny zóny zpětného vyhledávání, nebo může obsahovat zónu zpětného vyhledávání 172.32.x a delegovat zóny zpětného vyhledávání 172.32.16.x a 172.32.17.x na další servery. Záznamy prostředku PTR musí také existovat pro všechny počítače v síti. Více informací o přidávání zóny zpětného vyhledávání najdete v části „Přidání zóny zpětného vyhledávání“.

K ověření správnosti nastavení zón zpětného vyhledávání a záznamů prostředku PTR můžete použít také nástroj Nslookup.

► Ujistění se o správnosti nastavení zón zpětného vyhledávání a záznamů prostředku PTR

1. Spusíte nástroj Nslookup pomocí příkazu **Nslookup** na příkazové řádce.
2. Pomocí následujícího příkazu se přepnete na server, kterého se chcete dotázat:

server <adresa IP serveru>

3. Vložte adresu IP počítače, jehož záznamy prostředku PTR chcete ověřit a pak stiskněte ENTER.

Jestliže je zóna zpětného vyhledávání a záznam prostředku PTR nastaven správně, nástroj Nslookup vrátí název počítače.

4. Nástroj Nslookup opustíte pomocí příkazu exit a stiskem klávesy ENTER.

Ověření nastavení služby DNS po instalaci služby Active Directory

Používáte-li k podpoře služby Active Directory servery DNS třetích stran, můžete ověřit registraci záznamů prostředku lokátoru řadiče domény. Pokud server nepodporuje dynamickou aktualizaci, musíte přidat tyto záznamy ručně.

Služba Netlogon vytváří soubor protokolu, který obsahuje všechny záznamy prostředku lokátoru a umísťuje soubor protokolu na následující místo:

%SystemRoot%\System32\Config\Netlogon.dns

Můžete zkontrolovat tento soubor a zjistit, které záznamy prostředku lokátoru se pro řadič domény vytvořily.

Záznamy prostředku lokátoru jsou uloženy v textovém souboru kompatibilním se specifikacemi v dokumentech RFC. Pokud je váš server nastaven správně, zobrazí se záznam LDAP SRV řadiče domény:

```
_ldap._tcp.<Active Directory domain name>      IN      SRV      <priority>
<weight> 389 <domain controller name>
```

Například:

```
_ldap._tcp.reskit.com.  IN  SRV  0  0  389  dc1.reskit.com
```

Dále použijte nástroj Nslookup k ověření registrace záznamů prostředku SRV řadiče domény, které byly uvedeny ve službě Netlogon.dns.

Poznámka: Pokud jste nenastavili zónu zpětného vyhledávání a záznam PTR pro server DNS, kterého se dotazujete, během následujícího testu se může zobrazit několik vypršený časového limitu. To však není problém.

► Ověření registrace záznamů prostředku SRV řadiče domény

1. Na příkazovém řádku napište **nslookup** a stiskněte ENTER.
2. K nastavení typu dotazu DNS tak, aby filtroval pouze záznamy SRV, napište **set type=SRV** a stiskněte ENTER.
3. Dotaz na registrované záznamy prostředku SRV řadiče domény v doméně služby Active Directory odešlete tak, že napíšete **_ldap.tcp.<název domény služby Active Directory>** a stisknete ENTER.
4. Měli byste vidět záznamy SRV uvedené ve souboru Netlogon.dns. Pokud je nevidíte, záznamy SRV nemusí být pro tento řadič domény registrovány.

Následující příklad ukazuje úplnou relaci Nslookup používanou k ověření záznamů prostředku SRV, které jsou registrovány pro lokalizaci dvou řadičů domén na síti. V tomto příkladě jsou pro doménu noam.reskit.com registrovány dva řadiče domén (DC1 a DC2).

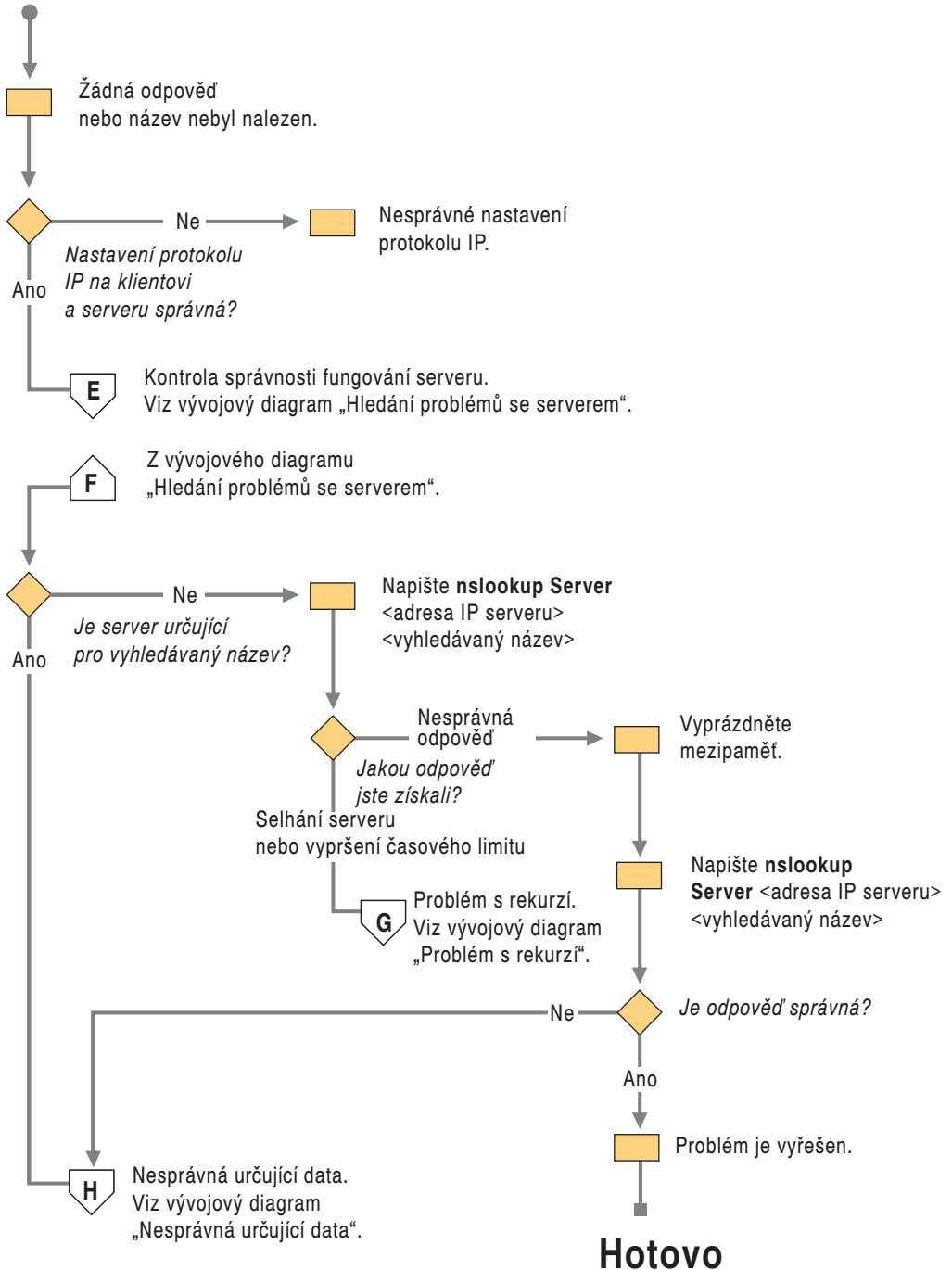
```
C:\>nslookup
Default Server:  dc1.noam.reskit.com
Address:  10.0.0.14
> set type=SRV
> _ldap._tcp.noam.reskit.com
Server:  dc1.noam.reskit.com
Address:  10.0.0.14
_ldap._tcp.noam.reskit.com  SRV service location:
        priority      = 0
        weight         = 0
        port           = 389
        svr hostname   = dc1.noam.reskit.com
_ldap._tcp.noam.reskit.com  SRV service location:
        priority      = 0
        weight         = 0
        port           = 389
        svr hostname   = dc2.noam.reskit.com
dc1.noam.reskit.com  internet address = 10.0.0.14
dc2.noam.reskit.com  internet address = 10.0.0.15
```

Diagnostika problémů s překladem názvu

Většina neúspěšných pokusů o překlad názvu selže jedním ze dvou obecných způsobů:

- Uživatel obdrží při snaze přeložit název negativní odpověď, například chybové hlášení „název nelze najít“.
- Uživatel obdrží při snaze přeložit název pozitivní odpověď, ale informace není správná.

Start



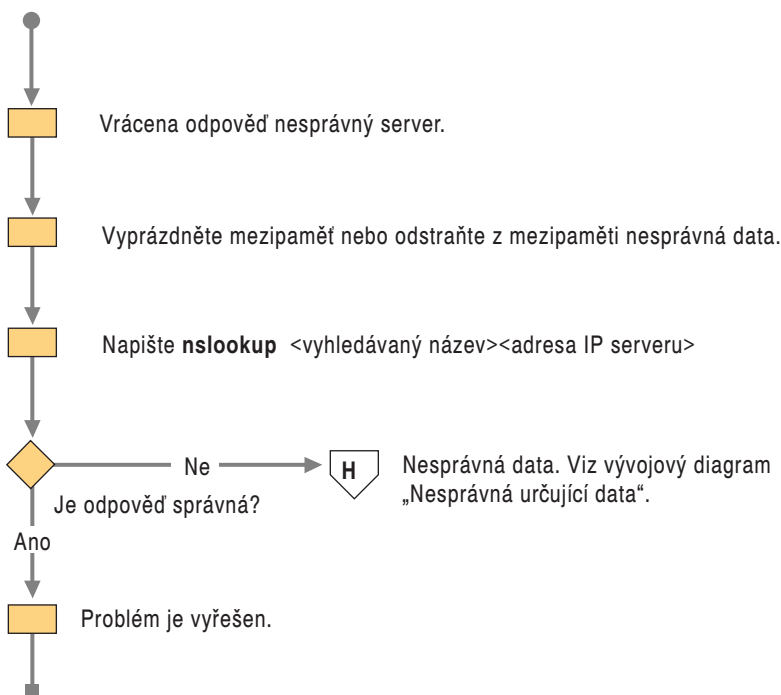
Obrázek 6.36 Žádná odpověď nebo název nebyl nalezen

Důležité: Při řešení problémů s překladem názvu používejte vždy název FQDN. Tím se ujistíte, že problém není způsoben nesprávnou příponou domény připojenou k dotazovanému názvu.

Následující vývojové diagramy a připojené texty na obrázcích 6.36 – 6.41 vysvětlují, jak diagnostikovat každý z těchto problémů. Dalším dobrým zdrojem informací o diagnostice běžných problémů je dokument RFC 1912 „Běžné chyby fungování a nastavení služby DNS“.

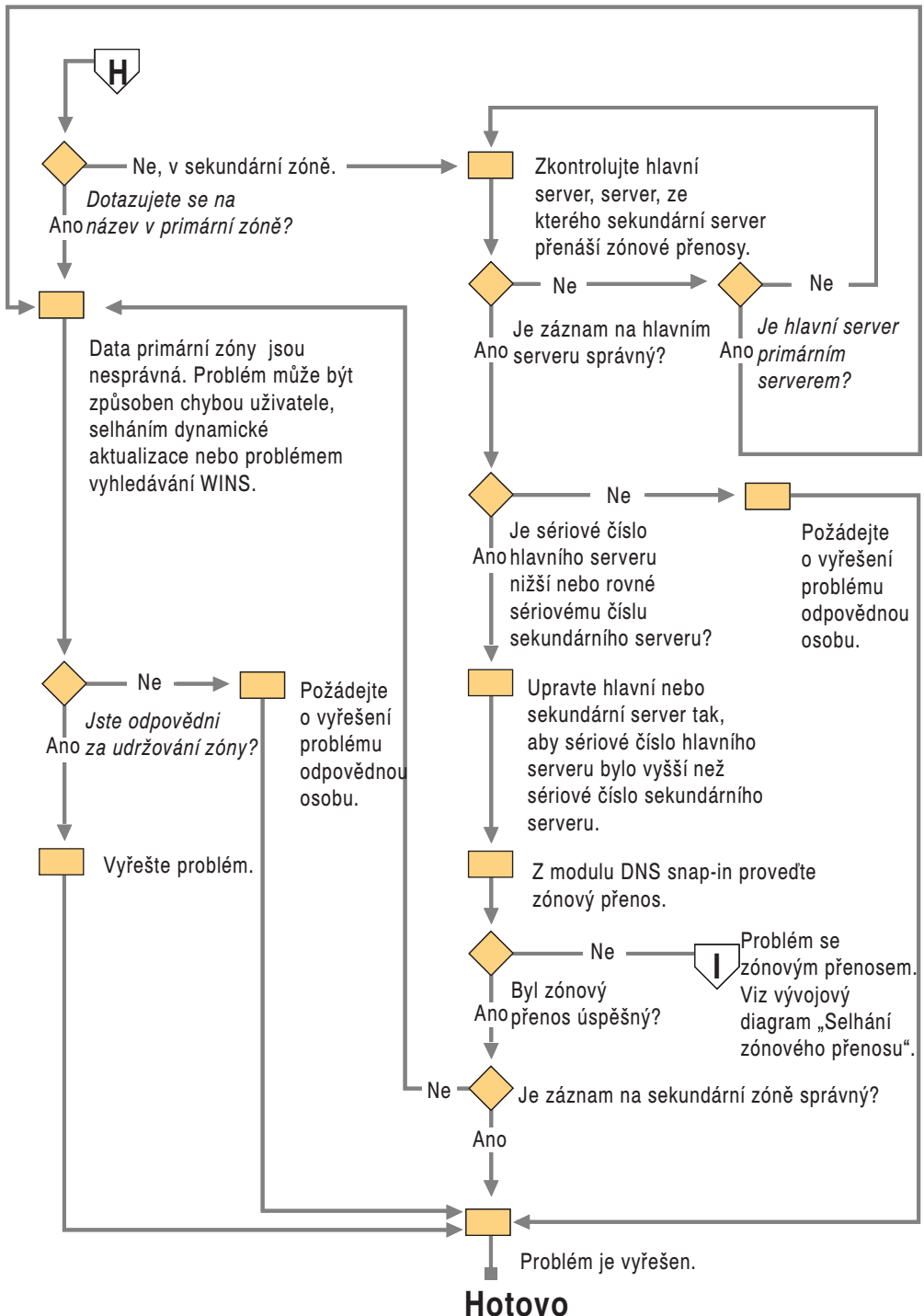
Poznámka: Vývojové diagramy na obrázcích 6.36 – 6.41 vás směřují na další vývojové diagramy v dalších obrázcích. K lokalizaci správného vývojového diagramu používejte legendu.

Start

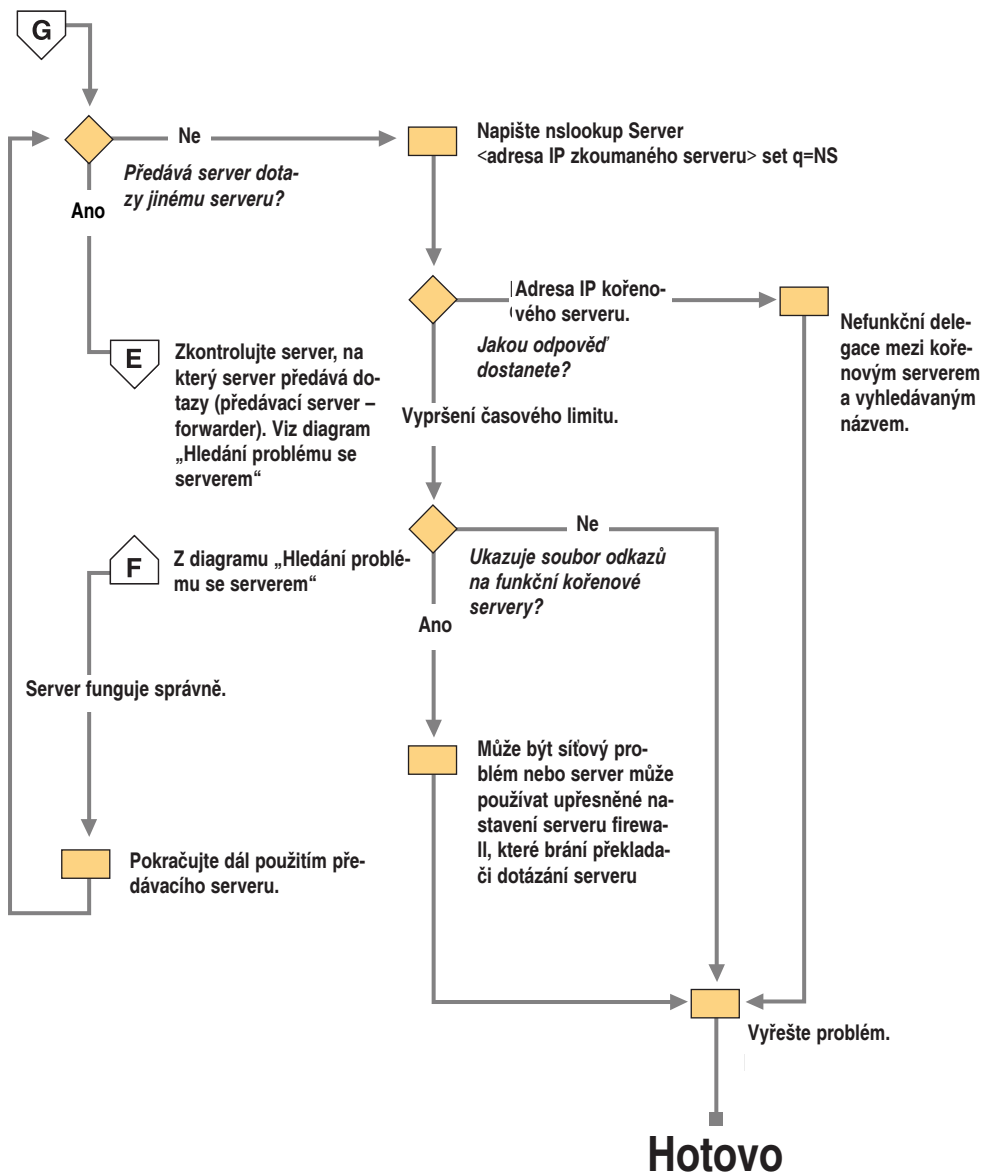


Hotovo

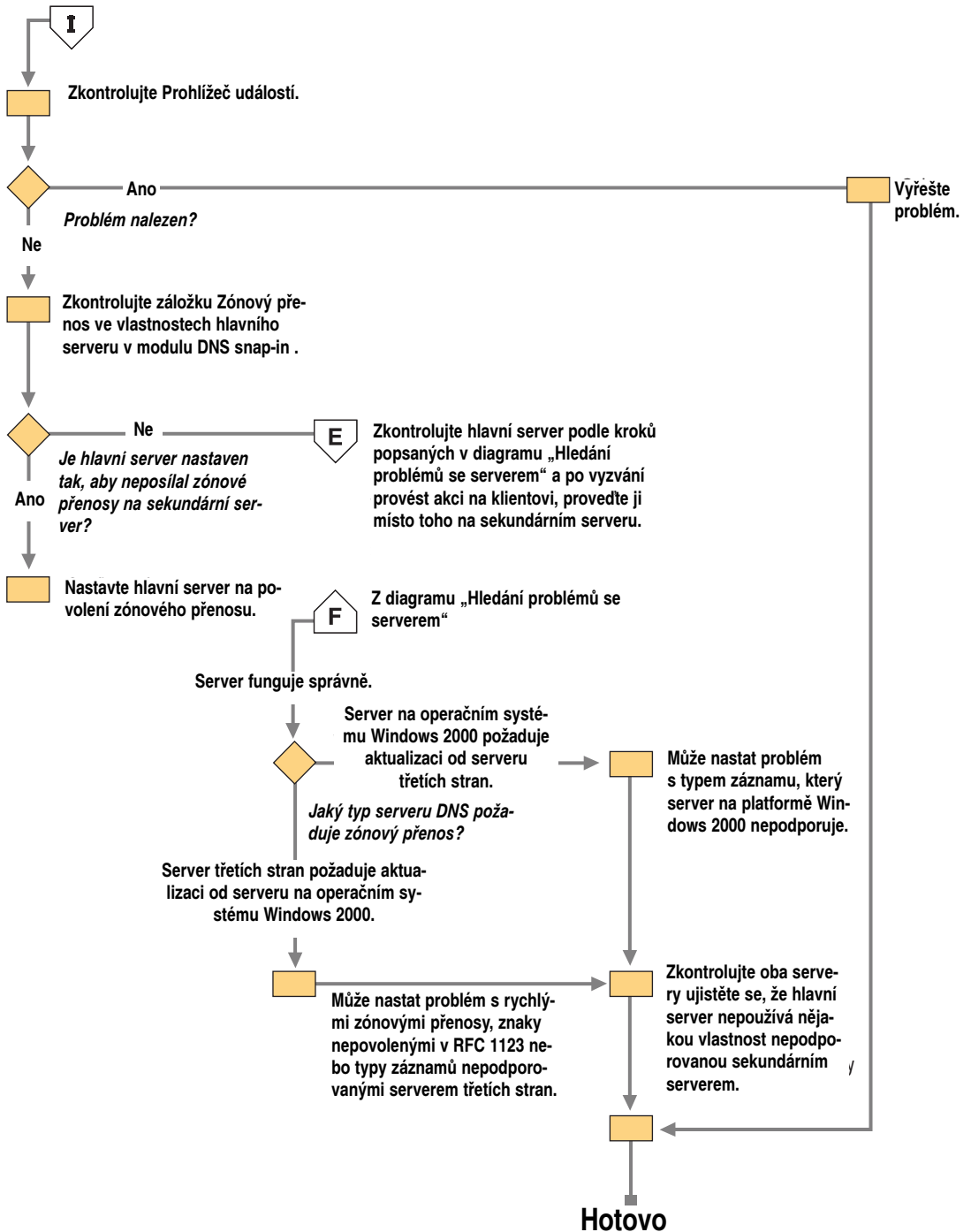
Obrázek 6.37 Nesprávná odpověď



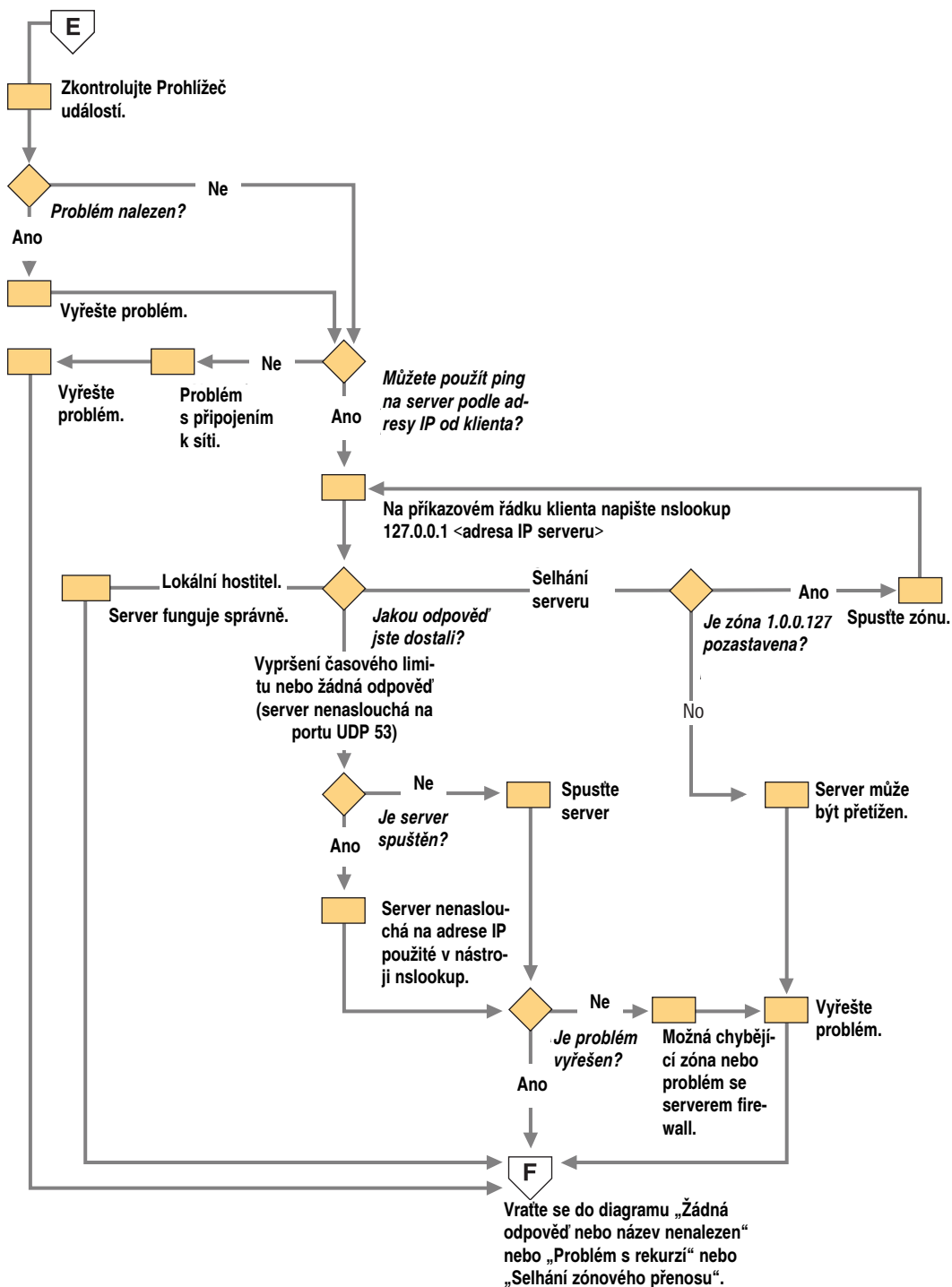
Obrázek 6.38 Nesprávná určující data



Obrázek 6.39 Problém s rekurzí



Obrázek 6.40 Selhání zónového přenosu



Obrázek 6.41 Hledání problémů se serverem

Nelze najít název nebo adresu IP

Pokud dotaz selže, protože dostanete od nástroje Nslookup odpověď **Neexistující doména** nebo od nástroje Ping **Neznámý hostitel**, server DNS nenalezl vyhledávaný název nebo vyhledávanou adresu IP. K řešení problému použijte následující postup znázorněný na obrázku 6.36:

1. Zkontrolujte, že počítače klienta a serveru mají platně nastavenou adresu IP.
Ke kontrole nastavení adresy IP použijte příkaz **ipconfig /all** na příkazovém řádku. V řádkovém výstupu ověřte adresu IP, masku podsítě a přednastavenou bránu.
2. Zkontrolujte, že server funguje správně. Více informací o ověření správného fungování serveru najdete v části „Hledání problémů se serverem DNS“.
3. Zkontrolujte, jestli je server DNS určující pro vyhledávaný název.

Pokud je server DNS určující pro vyhledávaný název, problém je pravděpodobně v určujících datech. Více informací o hledání problémů s určujícími daty najdete v části „Diagnostika problémů s nesprávnými určujícími daty“.

-Nebo-

Není-li server DNS určující pro vyhledávaný název, pokračujte dalším krokem.

4. Pomocí nástroje Nslookup pošle dotaz na daný název. Na příkazovém řádku napište následující:

Nslookup <dotazovaná adresa> <adresa IP serveru>

kde adresa IP serveru je adresa IP serveru, kterého jste se dotázali původně a je dotazovaná adresa název nebo adresa IP, které se snažíte přeložit. Dostanete-li zprávu „Selhání serveru“ nebo „Vypršel časový limit požadavku na server“, je problém pravděpodobně v nefunkční delegaci. Více informací o problémech s nefunkční delegací najdete v části „Diagnostika problémů s rekurzí“.

-Nebo-

Dostanete-li nesprávnou odpověď nebo zprávu „Neexistující doména“, pokračujte dalším krokem.

5. Vyprázdněte mezipaměť překladače. Na příkazovém řádku napište následující příkaz:

Nslookup <dotazovaná adresa> <adresa IP serveru>

kde adresa IP serveru je adresa IP serveru, kterého jste se dotázali původně a dotazovaná adresa je název nebo adresa IP, které se snažíte přeložit. Je-li odpověď správná, problém byl v zastaralém záznamu uloženém v mezipaměti a váš problém je vyřešen.

-Nebo-

Pokud odpověď není správná, problém je pravděpodobně v určujících datech. Více informací o hledání problémů s určujícími daty najdete v části „Diagnostika problémů s nesprávnými určujícími daty“.

Nesprávná odpověď

Jestliže pošlete serveru DNS dotaz a obdržíte nesprávnou odpověď, použijte následující postup znázorněný na obrázku 6.37:

1. Vyprázdněte mezipaměť překladače.

2. Na příkazovém řádku napište následující:

Nslookup <dotazovaná adresa> <adresa IP serveru>

kde adresa IP serveru je adresa IP serveru, kterého jste se dotázali původně a dotazovaná adresa je název nebo adresa IP, které se snažíte přeložit. Je-li odpověď správná, problém byl v zastaralém záznamu uloženém v mezipaměti a váš problém je vyřešen.

-Nebo-

Pokud odpověď není správná, problém je pravděpodobně v určujících datech. Více informací o hledání problémů s určujícími daty najdete v části „Diagnostika problémů s nesprávnými určujícími daty“.

Hledání problémů se serverem DNS

K vyhledání problémů se serverem DNS použijte následující postup znázorněný na obrázku 6.41:

1. Zkontrolujte Prohlížeč událostí, jestli se v něm nacházejí chybová hlášení. Informace o Prohlížeči událostí najdete v části „Nástroje pro řešení problémů“.
2. Zkontrolujte základní připojení mezi počítačem klienta a serverem DNS, který jste použili pro původní dotaz, pomocí příkazu ping na adresu IP serveru.
Pokud server DNS neodpovídá na přímý příkaz ping na svou adresu IP, problém je pravděpodobně v síťovém připojení mezi klientem a serverem DNS.
3. Na příkazovém řádku klienta napište následující příkaz:

nslookup 127.0.0.1 <IP address of server>

Pokud překladač vrátí název lokálního hostitele, na serveru není žádný problém.

-Nebo-

Pokud překladač vrátí odpověď „Selhání serveru“, pokračujte krokem 4.

-Nebo-

Pokud překladač vrátí odpověď „Časový limit požadavku na server vypršel“ nebo „Žádná odpověď od serveru“, pokračujte krokem 5.

4. Pokud překladač vrátí odpověď „Selhání serveru“, zóna 1.0.0.127.in-addr.arpa je pravděpodobně pozastavena nebo je přetížen server. Pozastavení zóny můžete zjistit po kontrole záložky **Obecné** u vlastností zóny z konzole DNS.
5. Pokud překladač vrátí odpověď „Časový limit požadavku na server vypršel“ nebo „Žádná odpověď od serveru“, server DNS je pravděpodobně vypnut. Zkuste restartovat server pomocí následujícího příkazu na příkazové řádce serveru:

net start DNS

-Nebo-

Pokud běží, server nemusí naslouchat na adrese IP použité v dotazu Nslookup. Ze záložky **Rozhraní** na stránce vlastnosti serveru z konzole DNS mohou správci omezit naslouchání serveru DNS pouze na vybrané adresy. Jestliže je server DNS nastaven tak, že omezuje služby na určitý seznam nastavených adres IP, je možné, že adresa IP použitá v dotazu není obsažena v takovém seznamu. Můžete vyzkoušet jinou adresu IP uvedenou v seznamu nebo přidat adresu IP do seznamu. Více informací o omezení serveru DNS na naslouchání pouze vybraným adresám najdete v nápovědě Windows 2000.

-Nebo-

V řídkých případech může mít server DNS nastaven zákaz používání automaticky vytvořených přednastavených zón. Dle výchozího nastavení služba DNS automaticky vytváří standardní zóny zpětného vyhledávání na základě doporučení v dokumentech RFC:

- 0.in-addr.arpa
- 127.in-addr.arpa
- 255.in-addr.arpa

Automatické vytváření těchto zón lze zakázat pouze v registru, takže je nepravděpodobné, že k něčemu takovému došlo. Nicméně pokud se domníváte, že automatické vytváření zón bylo zakázáno, můžete k ujištění o existenci zóny použít konzolu DNS.

-Nebo-

V řídkých případech může mít server DNS upřesněné nastavení zabezpečení nebo serveru firewall. Je-li server umístěn v jiné síti, která je dostupná pouze prostřednictvím zprostředkujícího hostitele (například směrovač filtrující pakety nebo server proxy), server DNS může použít k naslouchání a dostávání požadavků klientů nestandardní port. Dle výchozího nastavení nástroj Nslookup pošle dotazy na servery DNS na port UDP 53, takže pokud server DNS používá jiný port, dotaz Nslookup selže. Domníváte-li se, že problém může být v tomto, zkontrolujte, jestli je k blokování provozu na známých portech DNS úmyslně použit zprostředkující filtr. Pokud není, snažte se upravit filtry paketů nebo zásady portů na serveru firewall tak, aby povolily provoz na portu UDP/TCP 53.

Diagnostika problémů s nesprávnými určujícími daty

Pokud jste zjistili, že server obsahuje nesprávná určující (neuložená v mezipaměti) data, použijte při řešení tohoto problému následující postup:

1. Zjistěte, jestli server, který vrací nesprávnou odpověď, je primární nebo sekundární server zóny.

Pokud je primární server zóny, ať už standardní primární server zóny nebo server používající k nahrávání zóny integraci se službou Active Directory, data jsou nesprávná v primární zóně. Pokračujte krokem 5.

-Nebo-

Pokud server hostí sekundární kopii zóny, pokračujte následujícím krokem.

2. Prozkoumejte zónu na hlavním serveru (serveru, ze kterého tento server přetahuje zónové přenosy). Hlavní server můžete určit prozkoumáním vlastností sekundární zóny v konzole DNS. Je na hlavním serveru správný název?

Pokud na hlavním serveru není správný název, vraťte se na krok 1. Po vyzvání k prozkoumání serveru prozkoumejte server, ze kterého tento server přetahuje zónové přenosy.

-Nebo-

Pokud na hlavním serveru je správný název, pokračujte následujícím krokem.

3. Zkontrolujte, jestli sériové číslo hlavního serveru je nižší nebo rovné sériovému číslu sekundárního serveru. Pokud ne, pokračujte následujícím krokem.

-Nebo-

Pokud je sériové číslo hlavního serveru nižší nebo rovné sériovému číslu sekundárního serveru, upravte buď hlavní nebo sekundární server tak, aby bylo sériové číslo hlavního serveru vyšší než sériové číslo sekundárního serveru. Pak pokračujte následujícím krokem.

4. Proveďte nucený zónový přenos z konzoly DNS. (Informace o tom, jak provést nucený zónový přenos, najdete v nápovědě Windows 2000 Server.) Dále opět prozkoumejte sekundární server, jestli byla zóna přenesena správně. Pokud ne, problém je pravděpodobně v zónovém přenosu. Viz část „Diagnostika problémů se zónovým přenosem“.

-Nebo-

Pokud byla zóna přenesena správně, zkontrolujte, jestli jsou data nyní správná. Pokud ne, data jsou nesprávná v primární zóně. Pokračujte následujícím krokem.

5. Pokud jsou data nesprávná v primární zóně, problém mohl být způsoben chybou uživatele při vkládání dat do zóny, problémem s replikací Active Directory, s dynamickou aktualizací nebo problémem vyhledávání WINS. Informace o problémech s chybou uživatele a replikací Active Directory najdete v části „Řešení dalších běžných problémů služby DNS“. Informace o problémech s dynamickou aktualizací najdete v části „Řešení problémů s dynamickou aktualizací“. Informace o problémech s vyhledáváním WINS najdete v části „Řešení dalších běžných problémů služby DNS“.

Pokud jste odpovědní za udržování zóny, můžete problém vyřešit. V opačném případě požádejte o vyřešení problému osobu odpovědnou za udržování zóny.

Diagnostika problémů s rekurzí

Aby rekurze fungovala úspěšně, musí být všechny servery DNS používané na cestě rekurzivního dotazu schopné odpovídat a předávat správná data. Pokud toho nejsou schopny, může rekurzivní dotaz selhat z jakéhokoli z následujících důvodů:

- Časový limit dotazu vyprší před jeho dokončením.
- Server použitý během dotazu neodpověděl.
- Server použitý během dotazu odpověděl nesprávnými údaji.

Pokud jste zjistili, že máte problém s rekurzí, použijte k řešení tohoto problému následující postup znázorněný na obrázku 6.39. Začněte serverem použitým pro původní dotaz:

1. Zkontrolujte, jestli tento server předává dotazy dalšímu serveru, a to pomocí záložky **Servery pro předávání** ve vlastnostech serveru přístupných z konzoly DNS. Je-li vybráno pole **Povolit servery pro předávání** a je tam zařazen jeden nebo více serverů, tento server předává dotazy.

Jestliže tento server předává dotazy jinému serveru, zkontrolujte také server, kterému byl dotaz předán. Postupujte podle části „Hledání problémů se servery DNS“. Úlohy stanovené v této části pro klienty provádějte namísto toho na serveru.

Pokud je server zdravý a může předávat dotazy, opakujte tento krok při zkoumání serveru, kterému byl dotaz předán.

-Nebo-

Pokud server nepředává dotazy jinému serveru, proveďte následující krok.

2. Otestujte, jestli se tento server může dotázat kořenového serveru pomocí následujícího příkazu:

nslookup**server** <adresa IP zkoumaného serveru>**set querytype=NS**

.

Když překladač vrátí adresu IP kořenového serveru, je pravděpodobně mezi kořenovým serverem a názvem nebo adresou IP, kterou se snažíte přeložit, nefunkční delegace. K určení kde je tato delegace nefunkční použijte postup „Testování nefunkční delegace“.

-Nebo-

Když překladač vrátí odpověď „Časový limit požadavku na server vypršel“, zkontrolujte, jestli odkazy na kořenové servery ukazují na funkční kořenové servery pomocí postupu „Náhled na aktuální odkazy na kořenové servery“. Jestliže odkazy na kořenové servery ukazují na funkční kořenové servery, můžete mít problém se sítí, nebo server může používat upřesněné nastavení serveru firewall, který brání překladači v dotázání se na server, jak je popsáno v části „Hledání problémů se serverem DNS“. Je také možné, že přednastavený časový limit rekurze je příliš krátký (15 sekund). Informace o tom, jak změnit tento časový limit naleznete v nápovědě Windows 2000 Server. Hledejte „ladění upřesňujících parametrů“.

Poznámka: Testy v následujícím postupu začněte dotazy na platný kořenový server. Testy vás provedou postupným dotazováním všech serverů DNS z kořenových serverů dolů až na server, který testujete kvůli nefunkční delegaci.

► **Testování nefunkční delegace**

1. Na příkazovém řádku testovaného serveru napište následující příkaz:

nslookup**server** <adresa IP serveru>**set norecursion****set querytype=<typ záznamu prostředku>**

<název FQDN >

kde *typ záznamu prostředku* je typ záznamu prostředku, na který se dotazujete v původním dotazu, a *název FQDN* je název FQDN, na který se dotazujete (ukončený tečkou).

2. Pokud odpověď obsahuje seznam záznamů prostředků A a NS pro delegované servery, opakujte krok 1 pro všechny servery a použijte adresu IP ze záznamu prostředku A jako adresu IP serveru.

-Nebo-

Pokud odpověď neobsahuje seznam záznamů prostředků A a NS pro delegované servery, delegace je nefunkční.

-nebo-

Pokud odpověď obsahuje seznam záznamů prostředků NS pro delegované servery, ale žádné záznamy prostředku A, napište **set recursion** a dotazujte se na jednotlivé záznamy prostředku A serverů obsažených v záznamech NS. Pokud jste pro každý záznam prostředku NS v zóně nenašli alespoň jednu platnou adresu IP záznamu prostředku A, delegace je nefunkční.

Zjistíte-li nefunkční delegaci, opravte ji přidáním nebo aktualizací záznamu prostředku A v nadřazené zóně platnou adresou IP pro správný server DNS delegované zóny.

► **Prohlížení aktuálních odkazů na kořenové servery**

1. Spusťte konzolu DNS.
2. Přidejte nebo připojte se k serveru DNS, u něhož selhal rekurzivní dotaz.
3. Klepněte pravým tlačítkem na server a vyberte **Vlastnosti**.
4. Klepněte na **Odkazy na kořenové servery**.
5. Zkontrolujte základní připojení ke kořenovým serverům.
6. Jestliže se zdá, že odkazy na kořenové servery jsou nastaveny správně, ověřte, že server DNS použitý v neúspěšném překlad názvu může provést příkaz ping pomocí adresy IP na kořenové servery.

Jestliže kořenové servery neodpovídají na příkaz ping pomocí adresy IP, mohlo dojít ke změně adres IP kořenových serverů. Nicméně přenastavování kořenových serverů není běžnou záležitostí.

Diagnostika problémů se zónovým přenosem

Pokud jste zjistili, že sekundární server nemůže zajišťovat zónový přenos z hlavního serveru, použijte k diagnostikování a vyřešení tohoto problému následující postup znázorněný na obrázku 6.40.

1. Zkontrolujte Prohlížeč událostí na primárním i sekundárním serveru DNS. Informace o Prohlížeči událostí najdete v části „Nástroje pro řešení problémů“.
2. Zkontrolujte hlavní server, jestli odmítá zaslat přenos z důvodů zabezpečení. Zkontrolujte záložku **Zónové přenosy** na stránce vlastností serveru v konzole DNS. Jestliže server omezuje posílání zónových přenosů na seznam serverů, například uvedených v záložce **Servery názvů** vlastností zóny, ujistěte se, že sekundární server je na takovémto seznamu. Ujistěte se, že server je nastaven na zasílání zónových přenosů.
3. Zkontrolujte hlavní server pomocí postupu v části „Hledání problémů se serverem DNS“. Po výzvě provést úlohu na klientovi, proveďte ji namísto toho na sekundárním serveru.
4. Zkontrolujte, jestli sekundární server nepoužívá jinou implementaci služby DNS, například BIND. Pokud ano, problém může mít několik příčin:
 - Hlavní server s operačním systémem Windows 2000 může být nastaven k posílání rychlých zónových přenosů, ale sekundární server třetích stran tyto rychlé zónové přenosy nepodporuje. Pokud ano, zakažte rychlé zónové přenosy na hlavním serveru zaškrtnutím pole **Navázat sekundární servery** na záložce **Upřesnit** na stránce vlastností serveru z konzoly DNS.
 - Pokud zóna dopředného vyhledávání na serveru s operačním systémem Windows 2000 obsahuje záznam vyhledávání WINS nebo zóna zpětného vyhledávání záznam WINS-R, server BIND nemusí být schopen přenést zónu. Informace o diagnostice problémů, při kterých server BIND nemůže přenést zónu, najdete v části „Řešení dalších běžných problémů služby DNS“.
 - Pokud zóna dopředného vyhledávání na serveru s operačním systémem Windows 2000 obsahuje typ záznamu (například záznamy SRV), který sekundární server nepodporuje, sekundární server může mít problémy s přetažením zóny.

5. Zkontrolujte, jestli hlavní server používá jinou implementaci služby DNS server, například BIND.

Pokud ano, je možné, že zóna na hlavním serveru obsahuje nekompatibilní záznamy prostředků, které operační systém Windows 2000 nerozpozná. Úplný seznam všech záznamů prostředků kompatibilních s dokumenty RFC, které jsou podporovány servery DNS běžícími pod operačním systémem Windows 2000 Server, najdete v nápovědě Windows 2000 Server.

6. Pokud hlavní nebo sekundární server používá jinou implementaci služby DNS server, zkontrolujte oba servery a ujistěte se, že podporují stejné vlastnosti. Server s operačním systémem Windows 2000 můžete zkontrolovat ze záložky **Upřesnit** na stránce vlastností serveru z konzole DNS. Kromě pole **Navázat sekundární servery** tato stránka obsahuje také seznam **Kontrola názvů**, který umožňuje vybírat posílení střídme kompatibility dokumentů RFC znaků v názvech DNS.

Řešení dalších běžných problémů služby DNS

Tato část obsahuje několik běžných problémů služby DNS a vysvětluje, jak je řešit.

V protokolu událostí se objeví identifikátor události 7062.

Objeví-li se protokolu událostí identifikátor události 7062, server DNS poslal paket sám sobě. To je zpravidla způsobeno chybou nastavení. Zkontrolujte následující:

- Ujistěte se, že pro tento server neexistuje žádná neúčinná delegace. Neúčinná delegace se objeví v případě, že server deleguje zónu serveru, který pro ni není určený.
- Zkontrolujte seznam serverů pro předávání a ujistěte se, že server nevede sám sebe jako server pro předávání.
- Pokud tento server obsahuje sekundární zóny, ujistěte se, že nevede sám sebe jako hlavní server pro tyto zóny.
- Pokud tento server obsahuje primární zóny, ujistěte se, že nevede sám sebe v seznamu vyrozumění.

Zónové přenosy na sekundární servery používající BIND jsou pomalé.

Dle výchozího nastavení server DNS S operačním systémem Windows 2000 vždy používá rychlý zónový přenos. Tato metoda používá komprimaci a obsahuje více záznamů prostředků v jedné zprávě, čímž se značně zvyšuje rychlost zónových přenosů. Většina serverů DNS podporuje rychlé zónové přenosy. Nicméně BIND 4.9.4 a dřívější rychlé zónové přenosy nepodporují. To však není problém, protože po instalaci služby DNS Server pro operační systém Windows 2000 je dle výchozího nastavení rychlý zónový přenos zakázán. Nicméně pokud používáte BIND 4.9.4 nebo dřívější a povolili jste rychlý zónový přenos, musíte ho znovu zakázat.

► Zakázání rychlého zónového přenosu

1. V konzole DNS klepněte pravým tlačítkem na server DNS a pak klepněte na **Vlastnosti**.
2. Klepněte na záložku **Upřesnit**.
3. V seznamu **Možnosti** serveru vyberte pole **Navázat sekundární servery** a pak klepněte **OK**.

Vidíte chybové hlášení „Přednastavené servery nejsou dostupné“

Po spuštění nástroje Nslookup můžete vidět následující chybové hlášení:

*** Nelze nalézt název serveru pro adresu <adresa>. Neexistující doména

*** Přednastavené servery nejsou dostupné

Přednastavený server: Neznámý

Adresa:127.0.0.1

Uvidíte-li tuto zprávu, server DNS je stále schopen odpovídat na dotazy a podporovat službu Active Directory. Překladač nemůže lokalizovat záznamy prostředku pro server názvů, který je nastaven používat. Vlastnosti síťového připojení musí specifikovat adresu IP minimálně jednoho serveru názvů a po spuštění nástroje Nslookup překladač použije tuto adresu IP k vyhledání názvu serveru. Pokud překladač nemůže najít název serveru, zobrazí chybové hlášení. Nicméně stále můžete nástroj Nslookup používat k dotazům na server.

Problém vyřešíte následujícím způsobem:

- Ujistěte se, že zóna zpětného vyhledávání, která je určující pro záznam prostředku PTR, existuje. Více informací o přidávání zóny zpětného vyhledávání najdete v části „Přidání zóny zpětného vyhledávání“.
- Ujistěte se, že zóna zpětného vyhledávání obsahuje záznam prostředku serveru názvů.
- Ujistěte se, že server názvů, který používáte pro vyhledávání, se může dotazovat na server obsahující záznam prostředku PTR a zónu zpětného vyhledávání buď iterativně nebo rekurzivně.

Nesprávná data vložená do zóny uživatelem.

Informace o přidávání a aktualizaci záznamů pomocí konzole DNS najdete v nápovědě Windows 2000 Server. Více informací o používání záznamů prostředků v zónách najdete pomocí vyhledání klíčových slov „správa“ a „záznamy prostředku“ v nápovědě Windows 2000 Server.

Zóny integrované se službou Active Directory obsahují nekonzistentní data.

U zón integrovaných se službou Active Directory je také možné, že příslušné záznamy dotazu byly aktualizovány ve službě Active Directory, ale nebyly replikovány na všechny servery DNS, které zónu zavádějí. Dle výchozího nastavení všechny servery DNS zavádějící zóny ze služby Active Directory vyzývají službu Active Directory v nastaveném intervalu (zpravidla každých 15 minut) a aktualizují zónu přírůstkovými změnami. Ve většině případů službě DNS netrvá replikace na všechny servery DNS používané v prostředí domény služby Active Directory, které používá přednastavené nastavení replikace a vysokorychlostní připojení, více než 20 minut.

Uživatel nemůže přeložit název existující na správně nastaveném serveru DNS.

Nejprve ověřte, že název nebyl uživatelem vložen omylem. Ověřte přesnou sadu znaků vloženou uživatelem při původním dotazu DNS. Pokud název použitý v původním dotazu nebyl úplný a nebyl to název FQDN, použijte v klientské aplikaci název FQDN a zopakujte dotaz. Ujistěte se, že název FQDN skutečně obsahuje na konci názvu tečku, která značí, že se jedná o název FQDN.

Jestliže bude název FQDN úspěšný a vrátí v odpovědi správná data, nejpravděpodobnější příčinou problému je špatně nastavený seznam pro vyhledávání přípon domén, který se používá v nastavení překladače klienta.

Překlad názvu na síť internet je pomalé, nesouvislé nebo selhává.

Jestliže jsou dotazy určené na síť internet pomalé, nesouvislé nebo název na internetu nelze přeložit, ale překlad názvů lokálního intranetu probíhá úspěšně, může být soubor mezipaměti na serveru na platformě Windows 2000 poškozený, chybějící nebo neaktuální. Soubor mezipaměti můžete buď nahradit původní verzí souboru mezipaměti nebo do něj z konzole DNS ručně vložit správné odkazy na kořenové servery. Pokud je server DNS nastaven tak, že při spuštění nahrává data ze služby Active Directory a registru, musíte k vložení odkazů na kořenové servery použít konzolu DNS.

► Vložení odkazů na kořenové servery v konzole DNS

1. V konzole DNS poklepejte na server a rozvíňte jej.
2. Klepněte pravým tlačítkem na server a pak klepněte na **Vlastnosti**.
3. Klepněte na záložku **Odkazy na kořenové servery**.
4. Vložte odkazy na kořenové servery a pak klepněte na OK.

► Nahrazení souboru mezipaměti

1. Zastavte službu DNS pomocí následujícího příkazu:

net stop dns

2. Napište následující příkaz:

cd %Systemroot%\System32\DNS

3. Přejmenujte soubor mezipaměti:

ren cache.dns cache.old

4. Pomocí následujícího příkazu zkopírujte původní verzi souboru mezipaměti, kterou lze nalézt na jednom nebo dvou místech:

copy backup\cache.dns

-Nebo-

copy samples\cache.dns

5. Spustíte službu DNS pomocí následujícího příkazu:

net start dns

Pokud překlad názvů na internetu stále selhává, opakujte postup a zkopírujte soubor mezipaměti ze zdrojového média operačního systému Windows 2000.

► Kopírování souboru mezipaměti ze zdrojového média operačního systému Windows 2000

- Na příkazovém řádku napište následující příkaz:

**expand <jednotka>:\i386\cache.dn_
%Systemroot%\system32\dns\cache.dns**

kde jednotka je jednotka, která obsahuje zdrojové médium operačního systému Windows 2000.

Překladač nevyužívá výhod vlastností cyklického výběru

Operační systém Windows 2000 zahrnuje upřednostňování podsítí, novou vlastnost, která snižuje provoz přes podsítě. Nicméně to brání překladači v používání vlastností cyklického výběru, jak je definována v dokumentu RFC 1794. Pomocí vlastností cyklického výběru server protáčí pořadí záznamů prostředku A vrácených v odpovědi na dotaz, kde je více záznamů prostředku stejného typu pro dotazovaný název domény DNS. Nicméně pokud je překladač nastaven pro upřednostňování podsítí, přeorganizuje po-

řadí v seznamu tak, aby byly upřednostněny adresy IP ze sítě, ke kterým je přímo připojen.

Pokud byste chtěli dát přednost vlastnosti cyklického výběru před upřednostňováním podsítí, můžete tak učinit změnou hodnoty záznamu v registru. Více informací o nastavení vlastnosti upřednostňování podsítí najdete v části „Nastavení priorit podsítí“.

Záznam vyhledávání WINS způsobuje selhání zónového přenosu na server DNS třetích stran

Jestliže zónový přenos ze serveru na platformě Windows 2000 na server DNS třetích stran selhává, zkontrolujte, jestli zóna obsahuje nějaké záznamy WINS nebo WINS-R. Pokud ano, můžete zakázat přenos těchto záznamů na sekundární server DNS.

► **Zákaz přenášení záznamů vyhledávání WINS na sekundární server DNS**

1. V konzole DNS poklepejte na server DNS, klepněte pravým tlačítkem na název zóny, která obsahuje záznam WINS a pak klepněte na **Vlastnosti**.
2. V dialogu **Vlastnosti** zóny klepněte na záložku **WINS** a zaškrtněte pole **Nereplikovat tento záznam**.

► **Zákaz přenášení záznamů WINS-R na sekundární server DNS**

1. V konzole DNS poklepejte na server DNS, klepněte pravým tlačítkem na název zóny, která obsahuje záznam WINS a pak klepněte na **Vlastnosti**.
2. V dialogu **Vlastnosti** zóny klepněte na záložku **WINS-R** a zaškrtněte pole **Nereplikovat tento záznam**.

Záznam vyhledávání WINS způsobuje problémy s určujícími daty

Máte-li problémy s nesprávnými určujícími daty v zóně, pro kterou je povolena integrace vyhledávání WINS, chybná data mohou být způsobena službou WINS vracející nesprávná data. To, jestli je služba WINS zdrojem problémů, můžete zjistit pomocí kontroly hodnoty TTL dat v dotazu Nslookup. Normálně služba DNS odpovídá názvy uloženými v datech určující zóny pomocí nastavené hodnoty TTL zóny nebo záznamu prostředku. Obecně odpovídá pouze se sníženou hodnotou TTL při poskytování odpovědi na základě neurčujících dat uložených v mezipaměti získaných od ostatních serverů DNS během rekurzivního vyhledávání.

Nicméně vyhledávání WINS je výjimka. Server DNS prezentuje data ze serveru WINS jako určující, ale ukládá je pouze v mezipaměti serveru a ne v zónách a snižuje hodnotu TTL dat.

► **Určení, zda data pocházejí ze serveru WINS**

1. Na příkazovém řádku napište následující příkaz:

```
nslookup -d2  
server <server>
```

kde <server> je server určující pro testovaný název.

Tím se spustí nástroj Nslookup v interaktivním ladicím režimu a zajišťuje, že se dotazujete správného serveru. Pokud se dotážete serveru, který není pro testovaný název určující, není možno říci, jestli data pocházejí ze serveru WINS.

2. K otestování dopředného vyhledávání WINS napište následující příkaz:

```
set querytype=a
```

-Nebo-

K otestování zpětného vyhledávání WINS napište následující příkaz:

set querytype=ptr

3. Vložte dopředný nebo zpětný název domény DNS, který chcete otestovat.
4. V odpovědi si všimněte, jestli server odpověděl jako určující nebo neurčující, a všimněte si hodnoty TTL.
5. Pokud server neodpověděl jako určující, zdrojem dat není server WINS. Nicméně pokud odpověděl jako určující, zopakujte dotaz na název ještě jednou.
6. V odpovědi si všimněte, jestli hodnota TTL klesla. Pokud ano, zdrojem dat je server WINS.

Pokud jste zjistili, že data pocházejí ze serveru WINS, zkontrolujte server WINS. Více informací o hledání problémů na serveru WINS najdete v části „Služba Windows Internet Name Service“.

Zóna se po odstranění opět objeví

V některých případech se zóna po svém odstranění může opět objevit. Zóna se opět objeví, odstraníte-li sekundární kopii zóny, když existuje kopie zóny integrované se službou Active Directory ve službě Active Directory, a server, ze kterého jste odstranili sekundární kopii zóny je nastaven tak, že při spuštění nahrává data ze služby Active Directory a registru.

Chcete-li odstranit sekundární kopii zóny, která existuje ve službě Active Directory, nastavte server DNS tak, aby při spuštění nahrával data z registru, a pak odstraňte zónu ze serveru DNS hostičího sekundární kopii zóny. Případně můžete zónu úplně odstranit ze služby Active Directory, když jste přihlášení na řadič domény, který má kopii zóny.

Vidíte chybová hlášení o tom, že nelze registrovat záznamy PTR

Když server DNS určující pro zónu zpětného vyhledávání nemůže provádět dynamickou aktualizaci nebo je nastaven tak, že ji neprovádí, systém zaznamená chyby do protokolu událostí uvádějící, že nelze zaregistrovat záznamy PTR. Chybám v protokolu událostí můžete zabránit zakázáním registrace záznamů PTR dynamickou aktualizací na klientovi DNS. Registraci dynamickou aktualizací zakážete přidáním záznamu **DisableReverseAddressRegistrations** s hodnotou 1 a typem dat REG_DWORD do registru do následujícího podklíče:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Tcpip\Parameters\Interfaces\<název rozhraní>
```

kde *název rozhraní* je GUID síťového adaptéru.

Řešení problémů s dynamickou aktualizací a zabezpečenou dynamickou aktualizací

Máte-li problémy s dynamickou aktualizací, použijte pro jejich diagnostikování a vyřešení následující postup.

Řešení problémů s dynamickou aktualizací

Pokud dynamická aktualizace neregistruje správně název nebo adresu IP, použijte k odhalení a vyřešení tohoto problému následující postup.

- Příkazem `ipconfig /registerdns` donuťte klienta k obnovení registrace.
- Zkontrolujte, je-li povolena dynamická aktualizace zóny určující pro název, který se klient snaží obnovit.

Více informací o dynamické aktualizaci a zabezpečené dynamické aktualizaci najdete v části „Dynamická aktualizace a zabezpečená dynamická aktualizace“.

- K vyloučení dalších problémů zkontrolujte, jestli klient s dynamickou aktualizací má server DNS zóny jako svůj preferovaný server DNS.

To není pro fungování dynamické aktualizace nutné. Nicméně má-li klient uveden jako preferovaný server jiný server než primární server DNS zóny, může se objevit mnoho dalších problémů, například problém se síťovým připojením mezi dvěma servery nebo prodloužené zpětné vyhledávání primárního serveru zóny. Abyste zajistili pro klienta preferovaný server DNS, zkontrolujte adresu IP nastavenou ve vlastnostech protokolu TCP/IP na síťovém připojení klienta, nebo použijte příkaz `ipconfig /all`.

Je-li zóna integrovaná se službou Active Directory, může provádět aktualizaci kterýkoli server DNS, který hostí kopii zóny integrovanou se službou Active Directory.

- Zkontrolujte, jestli je zóna nastavena pro zabezpečenou dynamickou aktualizaci.

Pokud je zóna nastavena pro zabezpečenou dynamickou aktualizaci, aktualizace může selhat, pokud zabezpečení zóny nebo záznamu nedovoluje klientovi provádět změny zóny nebo záznamu. Aktualizace může selhat také tehdy, pokud klient není vlastníkem názvu, který se snaží aktualizovat. To, jestli došlo k selhání z jednoho z těchto důvodů, zjistíte v Prohlížeči událostí. Více informací o Prohlížeči událostí najdete v části „Nástroje pro řešení problémů“.

Informace o tom, co dělat, pokud aktualizace selhala kvůli tomu, že zóna je nastavena pro zabezpečenou dynamickou aktualizaci, najdete v části „Řešení problémů se zabezpečenou dynamickou aktualizací“.

Řešení problémů se zabezpečenou dynamickou aktualizací

Zabezpečená dynamická aktualizace může zabránit klientovi ve vytváření, úpravě nebo odstraňování záznamů v závislosti na seznamu řízení přístupu (ACL) k zóně a názvu. Dle výchozího nastavení zabezpečená dynamická aktualizace brání klientovi ve vytváření, úpravě nebo odstraňování záznamu, pokud klient není původním tvůrcem tohoto záznamu. například pokud dva počítače mají stejný název a oba se snaží zaregistrovat svůj název ve službě DNS, dynamická aktualizace selže u toho klienta, který se zaregistroval jako druhý.

Pokud klient selhal při aktualizaci názvu v zóně, která je nastavena pro zabezpečenou dynamickou aktualizaci, může být selhání způsobeno jednou z následujících podmínek:

- Systémový čas klienta a systémový čas serveru DNS nejsou synchronizovány.
- Upravili jste záznam **UpdateSecurityLevel** v registru tak, aby zakazoval použití zabezpečené dynamické aktualizace na klientovi. Více informací o dynamické aktualizaci a zabezpečené dynamické aktualizaci najdete v části „Dynamická aktualizace a zabezpečená dynamická aktualizace“.
- Klient nemá odpovídající oprávnění k aktualizaci záznamu prostředku. Toto můžete potvrdit zaškrtnutím seznamu řízení přístupu u názvu, který má být aktualizován.

Pokud klient nemá odpovídající oprávnění k aktualizaci záznamu prostředku, zkontrolujte, jestli server DHCP zaregistroval název klienta a jestli je vlastníkem odpovídajícího objektu `dnsNode`. Pokud ano, uvažujte o umístění serveru DHCP do zabezpečovací

skupiny DNSUpdateProxy. Jakýkoli objekt vytvořený členem této skupiny nemá žádné zabezpečení.

Více informací o zabezpečovací skupině DNSUpdateProxy najdete v části „Úvahy o dynamické aktualizaci a zabezpečené dynamické aktualizaci“.

Další informace

- Více informací o službě DNS najdete v knize *DNS and BIND*, 3. vydání, autor Paul Albitz and Cricket Liu, 1998, Sebastopol, CA: O'Reilly & Associates.
- Více informací o dokumentech RFC (Request for Comments) a IETF (IETF Internet-Drafts) najdete na stránce WWW Web Resources s adresou <http://windows.microsoft.com/windows2000/reskit/webresources>.

KAPITOLA 7

Služba Windows Internet Name Service



Přestože systém Windows 2000 používá pro mapování adres IP na názvy hostitelů v první řadě protokol a systém DNS (Domain Name System), pracuje v tom směru také se službou WINS (Windows Internet Name Service). Služba WINS je systém pro překlad jednoduchých názvů, využívaný ve Windows NT Server 4.0 a v dřívějších operačních systémech.

Služba DNS pro Windows 2000 nabízí místo názvových konvencí rozhraní NetBIOS, podporovaných službou WINS, hierarchickou službu úplných názvů hostitelů s protokolem TCP/IP nazývanou FQDN (fully qualified domain names). Služba WINS však poskytuje neocenitelnou službu administrátorům spravujícím heterogenní síť, které pracují s klienty se staršími operačními systémy jako Windows 95 nebo Windows NT verze 4.0. Tyto starší systémy mohou s protokolem DNS pracovat pouze částečně. Využívají sice službu překlad názvů služby DNS, ale nepodporují dynamické aktualizace jejich záznamů.

Obsah této kapitoly:

Celkový pohled na službu WINS	390
Původ služby WINS	391
Klienti služby Microsoft WINS	395
Servery služby Microsoft WINS	405
Databáze WINS	417
Replikace WINS	430
Správa serverů WINS	445
Zavádění služby Microsoft WINS	453
Vyřazení služby WINS z provozu	466
Interoperabilita	468
Odstraňování problémů spojených se službou WINS	470
Prostředky	476

Související informace v dokumentaci k soupravě prostředků (Resource Kit)

Podrobnější informace týkající se protokolu a systému DNS naleznete v kapitole „Úvod do DNS“.

Podrobnější informace o implementaci protokolu a systému DNS v rámci operačního systému Windows 2000, najdete v kapitole „Služba Windows 2000 DNS“.

Celkový pohled na službu WINS

Ačkoliv sítě, sestavené výhradně z počítačů s nainstalovaným operačním systémem Windows 2000, nevyžadují přítomnost serverů WINS, jsou tyto servery naprosto klíčovým prvkem všech sítí, sestavených z počítačů se starší architekturou operačních systémů Windows NT verze 4.0, Windows 98 nebo Windows 95. Tato podkapitola obsahuje jednak celkový popis této výkonné architektury, jednak popis jejích nových vlastností. V krátkosti se také zabývá důležitými základními údaji o pozadí vzniku služby WINS ze svého předchůdce, systému NetBIOS, vyvinutého v roce 1980.

Inovace pro systém Windows 2000

Nová implementace služby WINS v systému Windows 2000 obsahuje následující rozšíření:

Trvalá spojení Nyní lze nakonfigurovat každý server WINS tak, aby udržoval trvalá spojení s jedním nebo několika partnerskými servery pro replikace. Toto rozšíření podstatně zvyšuje rychlost replikací a odstraňuje zatížení systému, k němuž dochází při otevírání a uzavírání spojení.

Ruční označování záznamů za neplatné Je možné ručně určit záznamy, které budou označeny k odstranění. Stav takto označených záznamů je pak replikován na všechny servery WINS, čímž se zabraňuje propagaci aktivních záznamů a jejich dalšímu šíření.

Zdokonalený nástroj systémového řízení Konzola systémového řízení WINS je plně integrovaná s programem Microsoft Management Console (MMC) a obsahuje jednoduché, ale přesto velmi výkonné prostředí, které můžete upravovat a dále tak zvyšovat efektivitu své práce. Vzhledem k tomu, že všechny administrativní nástroje, začleněné do operačního systému Windows 2000 Server, jsou součástí aplikace MMC, používají se všechny nástroje konzoly MMC mnohem snáze a lze si je osvojit podstatně rychleji. Činnost těchto nástrojů je transparentnější a vychází z návrhu společného pro celý operační systém.

Rozšířené filtrování a vyhledávání záznamů Zdokonalené možnosti filtrování a nové funkce vyhledávání záznamů vám umožní nalézat požadované záznamy pouhým zobrazením podmnožiny záznamů shodných se zadanou vyhledávací podmínkou. Zmíněné funkce jsou užitečné zejména při analyzování velmi rozsáhlých databází WINS.

Dynamické mazání záznamů a vícenásobný výběr Správu databáze WINS podstatně usnadňuje dynamické mazání záznamů a možnost vícenásobného výběru. Díky konzole správy počítače můžete ukázat na jednu nebo více statických či dynamických položek databáze WINS, označit je a vymazat. (Tato funkce nebyla v předchozích verzích nástrojů příkazového řádku, určených pro správu služby WINS (jako například programu Winscl, dostupná.). Nyní lze mazat dokonce i záznamy, které obsahují v názvech jiné než alfanumerické znaky.

Ověření správnosti záznamů a ověření platnosti verze Ověření správnosti záznamu je založeno na srovnání s adresami IP, získanými dotazem na název rozhraní NetBIOS různých serverů WINS. Ověření platnosti testuje číslo verze tabulky mapování vlastního. Tyto vlastnosti rychle a efektivně ověřují shodnost uložených názvů s názvy replikovanými na vlastních serverech WINS.

Funkce Export Data služby WINS lze exportovat do textového souboru s oddělovači, které lze importovat do aplikací Microsoft Excel, do programu Zásílání zpráv o chybách systému Windows, skriptovacích programů nebo do dalších analytických či ohlašovacích programů.

Zvýšená odolnost proti chybám na straně klienta Klienti se spuštěným operačním systémem Windows 2000 nebo Windows 98 mohou určit maximálně 12 serverů WINS pro každé rozhraní (oproti dřívějším dvěma). Dodatečné adresy serverů WINS jsou použity pouze v případech, kdy dojde k selhání odezvy jak primárního, tak i sekundárního serveru WINS.

Dynamická obnova klientů Klient služby WINS nemusí po obnovení registrace místních názvů rozhraní NetBIOS restartovat počítač. Příkaz Nbtstat nyní obsahuje novou volbu – je to parametr RR, jenž poskytuje možnost uvolnit a následně obnovit registraci názvů tohoto rozhraní. Zmíněnou vlastnost příkazu Nbtstat lze využívat také u klientů s operačním systémem Windows NT verze 4.0, aktualizovaným pomocí aktualizáčního balíčku Service Pack verze 4 nebo vyšší.

Nastavení přístupu ke konzole systémového řízení WINS jen pro čtení Instalační program služby WINS přidává do seznamu skupin uživatelů speciální místní skupinu, skupinu WINS Users. Uživatelům této skupiny můžete prostřednictvím konzoly systémového řízení WINS poskytovat omezený přístup k informacím služby WINS uloženým na počítači serveru. Tento přístup nastavuje uživatelům, kteří nemají zároveň administrátorská práva, oprávnění jen pro čtení. Členství v této skupině tedy umožňuje uživatelům prohlížet – ale nikoliv upravovat – informace a vlastnosti uložené na určitém serveru WINS.

Díky všem těmto vlastnostem je systém Windows 2000 ideální volbou pro překlad názvů rozhraní NetBIOS. Služba WINS usnadňuje práci správcům směrovaných sítí a řeší problém překládání adres IP ve veřejných rozlehlých sítích (WAN).

Původ služby WINS

Jeden z důležitých bodů správy počítačové sítě spočívá v tom, zda síť využívá službu DNS nebo WINS. Překlad názvů umožňuje prohledávat síť a připojovat se ke prostředkům pomocí jednoduchých názvů jako „mojetiskarna01“ či „nassouborovyserver01“. Není tedy třeba pamatovat si adresy IP příslušných hostitelských počítačů. Památování si jednotlivých adres IP může být navíc nepraktické, neboť budete-li k přiřazení adres používat protokol DHCP (Dynamic Host Configuration Protocol), může se stát, že nastavené adresy budou zakrátko neplatné.

Služby DHCP obsahují vestavěnou podporu protokolu WINS. Kdykoli je počítači, nazvanému například „souborovyserver01“, automaticky přiřazena nová adresa IP, je změna zcela transparentní. Když se k počítači souborovyserver01 připojíte z jiného uzlu, můžete místo nové adresy IP použít jednoduchý název souborovyserver01. Služba WINS totiž obsahuje všechny informace o změnách adres IP, přiřazených k danému názvu.

Služba WINS byla vytvořena jako řešení problémů s překlady názvů pomocí všesměrového vysílání a jako odlehčení správy souborů LMHOSTS. Informace o překladu adres IP jsou v souborech LMHOSTS uloženy ve statickém formátu. Správa rozhraní je tak podstatně spolehlivější. V systémech, založených na překladu názvů pomocí všesměro-

vého vysílání (např. rozhraní NetBIOS), dochází v rozlehlých sítích po připojení klientů a všesměrovému vysílání zpráv všem ostatním uzlům, pro přeložení adres IP, k velkému zatížení. Všeměrová vysílání navíc nemohou překračovat hranice směrovače, což v praxi znamená, že názvy mohou být překládány pouze místně.

WINS je postaven na protokolu, definovaném standardem IETF (Internet Engineering Task Force) specifikace RFC (Request for Comments), který zajišťuje registraci názvů, překlad a uvolnění pomocí jednosměrového vysílání datagramů názvovým serverům NetBIOS. Umožňuje, aby systém pracoval i přes směrovače a odstraňuje tak potřebu vytváření souborů LMHOSTS. Obnovuje dynamickou povahu překladu názvů rozhraní NetBIOS a umožňuje dokonalou spolupráci systému se protokolem DHCP. Vytvoří-li například dynamické adresování pomocí protokolu DHCP pro počítače, které se pohybují mezi jednotlivými podsítěmi, nové adresy IP, promítnou se tyto změny ihned také do databáze WINS.

Součástmi kompletního systému Windows 2000 WINS jsou server WINS, klienti, agenti proxy, databáze WINS a konzola systémové správy WINS. Tyto součásti budou později v této kapitole popsány.

Služba WINS je slučitelná s protokoly definovanými ve specifikacích RFC 1001 a RFC 1002 pro názvové servery rozhraní NetBIOS (NBNS), takže je provozuschopná také s ostatními implementacemi standardu RFC. Další implementace klienta, vyhovující specifikacím RFC, mohou komunikovat se serverem WINS, stejně jako může klient protokolu Microsoft TCP/IP komunikovat s dalšími implementacemi názvových serverů rozhraní NetBIOS. Ale vzhledem k tomu, že protokol replikace WINS typu server/server není specifikován žádným standardem, nepracuje server WINS s ostatními implementacemi serverů NBNS. Data nemohou být replikována mezi serverem WINS a Non-WINS názvovým serverem NetBIOS. Bez replikace nelze zaručit správný překlad názvů na adresy IP.

Dědictví rozhraní NetBIOS obsažené WINS

Pochopit skutečnou nezbytnost přítomnosti služby WINS znamená porozumět historii rozhraní NetBIOS. Ta se začala psát před více než 10 lety, když se toto rozhraní objevilo jako rozhraní, určené vyšším programovacím jazykům pro tvorbu aplikací v systému PC-DOS, určeným pro širokopásmové sítě osobních počítačů typu IBM. Společnost Microsoft toto rozhraní využívala při návrzích svých síťových součástí. Rozhraní NetBIOS je rozhraním na úrovni relace, které používají aplikace ke vzájemné komunikaci prostřednictvím přenosů kompatibilních se standardem NetBIOS. Ten vytváří v rámci sítě logické názvy, nastavuje mezi nimi příslušné relace a podporuje spolehlivý přenos dat mezi počítači, jež jsou součástí vytvořené relace. Protokoly, implementované díky síťovým součástem společnosti Microsoft, včetně TCP/IP, zahrnují rozhraní NetBIOS neboli vrstvu mapování. Posledně jmenovaná vrstva umožňuje užití i jiných než přirozených součástí rozhraní NetBIOS, které se díky ní mohou snadno sloučit s okolním prostředím NetBIOS. Komunikace typu NetBIOS používají názvové konvence NetBIOS k jedinečné identifikaci prostředků či jiných uzlů sítě.

Délka všech názvů rozhraní NetBIOS je shodně 16 bajtů. Názvový obor NetBIOS je rovinný, což znamená, že názvy lze v rámci sítě použít pouze jednou. (Na druhé straně používá služba DNS názvy FQDN (úplné doménové názvy), které kombinují jednotlivé názvy ze názvu hostitele a názvu domény. Název rozhraní NetBIOS, jako například „WINserver01“ by mohl podle standardu FQDN vypadat následovně: „WINserver01.itreskit.com“.) Podrobnější informace, týkající se názvů NetBIOS, uvedeme později v této kapitole v oddíle „Názvy systému NetBIOS“.

Názvy rozhraní NetBIOS jsou registrovány dynamicky při spuštění počítače nebo po přihlášení uživatele do systému. Název rozhraní NetBIOS lze zaregistrovat buď jako jedinečný název, jenž reprezentuje jednu adresu, anebo jako název skupiny, který je namapovaný na více různých adres. Oběma zmíněnými typy názvů se budeme podrobněji zabývat později v oddíle „Správa serverů WINS“.

Překlad názvů NetBIOS

Překlad názvů NetBIOS je proces úspěšného převádění názvu rozhraní NetBIOS na adresu IP. Název rozhraní NetBIOS je 16bajtovou adresou, používanou k identifikaci prostředku NetBIOS v příslušné síti. Název rozhraní NetBIOS může být jednak jedinečný název, exkluzivní pro samostatný proces na jednom počítači, nebo také název skupiny, jenž může obsahovat adresy většího počtu procesů na několika počítačích.

Příkladem procesu, jenž využívá název rozhraní NetBIOS, je služba Sdílení souborů a tiskáren v sítích Microsoft, dostupná na počítači se spuštěným operačním systémem Windows 2000. Po spuštění počítače zaregistruje tato služba jedinečný název rozhraní NetBIOS, založený na názvu počítače. Zaregistrovaný název je 15místný znakový název počítače plus znak 0x20, umístěný na 16. místě. Pokud je název počítače kratší než 15 písmen, je doplněn mezerami tak, aby vytvořil požadovaný 15místný řetězec.

Když na základě názvu navážete spojení s počítačem, používajícím systém Windows 2000, jenž zajišťuje sdílení souborů, použije připojení automaticky službu Sdílení souborů a tiskáren v sítích Microsoft, umístěnou na zadaném serveru. Sdílení souborů a tiskáren vždy odpovídá určitému názvu rozhraní NetBIOS. Když se například pokusíte připojit k počítači nazvanému CORPSEVER, bude název služby Sdílení souborů a tiskáren v sítích Microsoft tohoto počítače vypadat takto:

CORPSEVER [20]

Všimněte si používání mezer k doplnění délky názvu počítače. Před navázáním spojení pro sdílení souborů a tiskáren musí být vytvořeno spojení TCP. Aby k tomu došlo, musí být název rozhraní NetBIOS, CORPSEVER [20], nejprve přeložen na adresu IP.

Přesný mechanismus překládání názvů NetBIOS na adresy IP závisí na typu uzlu rozhraní NetBIOS konfigurovaném na počítači provádějícím překlad názvu. Příslušné typy uzlů NetBIOS definuje specifikace RFC 1001 a všechny jsou uvedeny v tabulce 7.1.

Tabulka 7.1: Typy uzlů rozhraní NetBIOS

Režim překladu názvů NetBIOS	Popis
Uzel B	Využívá všesměrové vysílání zpráv IP pro registraci a překlad názvů rozhraní NetBIOS na adresy IP. Počítače se systémem Windows 2000 mohou používat upravené překlad názvu uzlu typu uzel B
Uzel P	Při registrování a překládání názvů počítačů na adresy IP využívá dvoubodové komunikace s názvovým serverem NetBIOS (v sítích systému Windows 2000 se jedná o server WINS).

Režim překladu Popis
názvů NetBIOS

Uzel M	Při registrování a překládání názvů NetBIOS používá jak komunikace typu uzel B, tak komunikace typu uzel P. Uzel M nejprve použije překlad pomocí všesměrového vysílání a teprve pak, je-li to nezbytné, použije dotaz serveru.
Uzel H	Používá hybridní metodu, založenou na metodě typu uzel B spojenou s metodou typu uzel P. Počítače typu uzel H se vždy pokoušejí nejprve spustit dotaz serveru a všesměrové vysílání používají teprve po selhání přímého dotazu. počítače se systémem Windows 2000 jsou standardně nakonfigurovány jako počítače typu uzel H. V zájmu omezení všesměrového vysílání IP používají tyto počítače soubor LMHOSTS, v nichž ještě před použitím všesměrového vysílání IP typu uzel B vyhledávají údaje, mapující název počítače na příslušnou adresu IP.

Počítače se systémem Windows 2000 používají standardně překlad názvu typu uzel B, zatímco překlad typu uzel H používají, jsou-li nakonfigurovány pomocí serveru WINS.

K tomu, aby bylo možné překládat vzdálené názvy rozhraní NetBIOS, je třeba nakonfigurovat počítač se systémem Windows 2000 pomocí adresy IP serveru WINS. Má-li počítač se spuštěnou službou Active Directory v systému Windows 2000 komunikovat s počítači s nainstalovaným operačním systémem Windows NT, Windows 2000, Windows 95 nebo Windows 98, ale bez služby Active Directory, musí být nakonfigurován pomocí adresy IP serveru WINS.

Všesměrové Vysílání v překladu názvů NetBIOS

Překlad názvů NetBIOS v malé a samostatné počítačové síti je založen na všesměrovém vysílání. Požadavek na registraci názvu může být vyslán do lokální sítě a vyslyšen všemi počítači typu uzel B, uzel H a uzel M. Nevyskytnou-li se žádné námitky, předpokládá vysílající aplikace, že má oprávnění k používání daného názvu, a uveřejní požadavek na přepsání názvu. Je-li požadovaný název právě používán, obdrží aplikace při registraci názvu zápornou odezvu právě od uzlu, jenž daný název aktuálně používá. V tomto případě nemá žádající aplikace oprávnění k používání zvoleného názvu.

V rozlehlejších propojených skupinách podsítí vytváří překlad názvu, založené na všesměrovém vysílání, určité problémy. Za prvé, jednotlivé uzly na sebe mohou působit v rámci jedné oblasti všesměrového vysílání, nemohou však mezi sebou komunikovat napříč směrovači ve směrovaných sítích. Za druhé, překlad názvu pomocí všesměrového vysílání vyvolává v síti značný provoz. Za třetí, každý uzel v rámci vysílací oblasti musí ověřit každý datagram všesměrového vysílání, čímž spotřebovává určitou část prostředků každého uzlu. Překlad názvu na bázi všesměrového vysílání funguje skvěle v malých sítích LAN, ale postupně, když se lokální síť zvětšuje a přerůstá v rozlehlou síť, se tato metoda stává neefektivní. Rozsáhlé síť LAN pocítují problémy týkající se šířky pásma a po zavedení směrovačů je tento způsob překladu názvu zcela neúčinný.

Služba WINS zamezuje těmto problémům zavedením dynamické správy databáze pro registraci názvů a jejich překlad. Snižuje také provoz všesměrového vysílání, neboť umožňuje klientům snadno vyhledávat vzdálené systémy napříč jak lokálními, tak rozlehlými počítačovými sítěmi.

Soubory LMHOSTS

Soubor LMHOSTS byl zaveden jako podpora pro překlad vzdálených názvů rozhraní NetBIOS. Soubor LMHOSTS je statický lokální databázový soubor, jenž mapuje názvy rozhraní NetBIOS na adresy IP. Tento přístup je velmi podobný funkci souboru Hosts, používaného službou DNS, nicméně ten je používán k mapování adres IP názvům hostitelů v hierarchickém názvovém oboru DNS, nikoliv názvům rozhraní NetBIOS. Vložení záznamu o názvu v rozhraní NetBIOS spolu s jeho adresou IP do souboru LMHOSTS umožňuje, aby uzel, který nemůže zareagovat na dotaz na název, mohl získat adresu IP, odpovídající příslušnému názvu rozhraní NetBIOS.

Používá-li systém Windows 2000 k překladu vzdálených názvů NetBIOS soubor LMHOSTS, prohledává soubor LMHOSTS uložený ve složce %SystemRoot%\System32\Drivers\Etc.

Jak již bylo uvedeno dříve, počítač v síti typu Microsoft může překládat názvy NetBIOS hned několika způsoby. Pokud některá z metod překladu selže, pokusí se počítač použít další metodu, uvedenou v pevném pořadí. V síti, založené na bázi vysílání, ověřuje uzel nejprve, zda se ve vyrovnávací paměti vzdálený název už nenachází, a teprve pak vysílá dotaz na název (pokud byl daný název používán při posledním připojení nebo je uložen v souboru LMHOSTS, bude uložen ve vyrovnávací paměti). Posledním pokusem je použití souboru LMHOSTS k získání adresy IP, přiřazené názvu rozhraní NetBIOS, jenž se aplikace pokouší přeložit (například k získání adresy IP pro název počítače, jenž se nachází za směrovačem v síti založené na vysílání).

Podrobnosti týkající se souborů LMHOSTS vyhledejte v části „Soubor LMHOSTS“.

Navzdory mnoha možnostem jeho využití má soubor LMHOSTS jistá omezení. Největším z nich je to, že se jedná o statický soubor, což znamená, že údaje musí být aktualizovány ručně po každé změně názvu nebo adresy IP daného počítače (například když je počítač přesunut do jiné podsítě nebo když zavolá vzdálený uživatel a připojí se pomocí modulu Směrování a vzdálený přístup). Toto omezení souboru LMHOSTS se ještě více projevilo po uvedení protokolu DHCP. Server DHCP přiřazuje adresy IP uzlům dynamicky – to v podstatě znemožňuje udržovat stále aktuální soubor LMHOSTS.

Proč je služba WINS stále potřebná

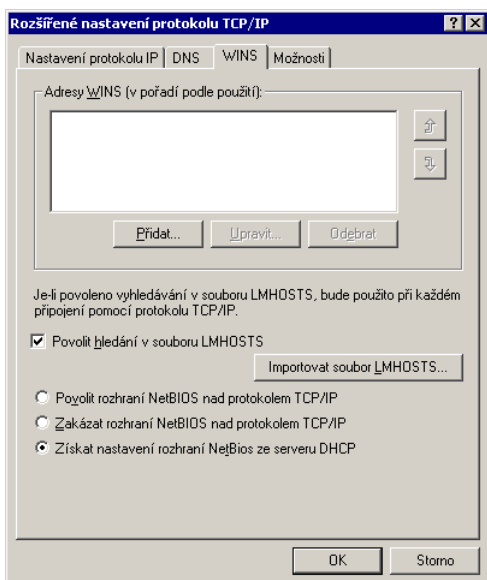
Jsou-li v počítačové síti pouze počítače se systémem Windows 2000 nebo jiným systémem, založeným na protokolu TCP/IP, jenž nevyžaduje používání názvů NetBIOS (jak je tomu například ve většině verzí operačního systému UNIX), bude služba WINS v síti zbytečná. V tomto případě byste měli k překládání adres IP používat raději službu Microsoft DNS.

Přesto však mnoho sítí ještě dnes obsahuje počítače s operačním systémem Windows NT, Windows 98 a Windows 95. V těchto sítích bude služba WINS nezbytná, dokud na všech počítačích v síti nebude nainstalován operační systém Windows 2000.

Klienti služby Microsoft WINS

Chcete-li konfigurovat klienty služby WINS pomocí adresy IP jednoho ze serverů WINS, otevřete dialogové okno **Síťová a telefonická připojení sítě**, označte položku **Připojení místní počítačové sítě**. Klepněte na tlačítko **Vlastnosti**, vyberte ze seznamu položku **Vlastnosti nastavení protokolu TCP/IP** a zadejte příkaz **Vlastnosti**. Potom

klepněte na tlačítko **Upřesnit**. V dialogovém okně Upřesnit nastavení protokolu TCP/IP se přesuňte na kartu **WINS**. Na obrázku 7.1 vidíte právě tuto konfigurační kartu.



Obrázek 7.1: Služba WINS na klientovi systému Windows 2000.

Názvy NetBIOS jsou propojeny s různými službami počítačové sítě, kdy lze každý z klientských počítačů používat spolu s ostatními počítači v síti.

Microsoft umožňuje používání klientů služby WINS na následujících platformách:

- Windows 2000
- Windows NT Server
- Windows NT Workstation
- Windows 98
- Windows 95
- Windows for Workgroups
- LAN Manager 2.x

Klient, který podporuje službu WINS, komunikuje se serverem WINS za účelem:

- Registrace v databázi WINS všech názvů procesů, probíhajících na klientovi, jako názvy rozhraní NetBIOS,
- uvolnění z databáze WINS všech názvů NetBIOS procesů, které už nejsou na klientovi spuštěny,
- obnovení názvů klienta v databázi WINS,
- přeložení názvů tím, že z databáze WINS získá mapování uživatelských jmen, názvů NetBIOS, názvů DNS a adres IP.

Klienti, kteří nejsou konfigurováni k používání služby WINS, se mohou do těchto procesů zapojit v omezené míře, ale musí používat agenta serveru proxy služby WINS, aby provedl konfiguraci za ně. Více informací o agentech serverů proxy najdete v oddíle „Server proxy služby Microsoft WINS“ později v této kapitole. Každý z dalších úkolů vykonávaných klientem WINS je popsán v následujícím oddílu.

Jak registrují klienti WINS své názvy

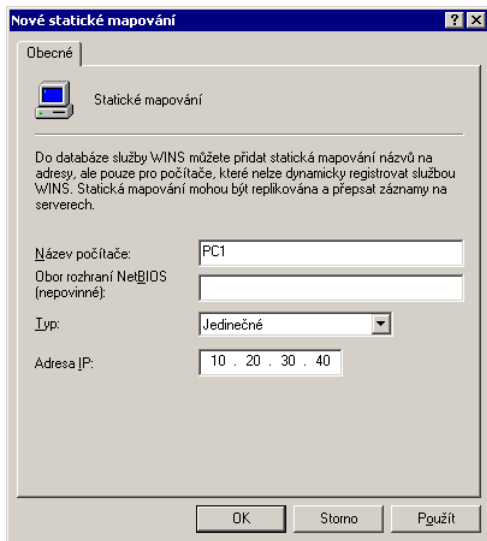
Počítač s podporou služby WINS se po spuštění pokusí zaregistrovat svoje názvy NetBIOS spolu se souvisejícími adresami IP přímo pomocí serveru WINS. V případě, že se registrace nezdaří, bude se klient WINS opakovaně pokoušet o zaregistrování v 10minutových intervalech, dokud nebude registrace úspěšná. Zpráva, kterou klient odešle, se nazývá požadavkem na zaregistrování názvu. Klient WINS odešle po jednom požadavku na registraci názvu (jenž obsahuje mimo jiné také adresu IP žádajícího počítače) pro každou službu typu NetBIOS, která je momentálně na počítači spuštěna.

Poznamenejme, že klient s nakonfigurovaným využitím služby DHCP má adresu IP přiřazenu dynamicky serverem DHCP. Jestliže klient nepoužívá DHCP, jeho adresa IP je staticky přiřazené číslo, které je nutné získat od administrátora sítě a manuálně nakonfigurovat na počítači.

► Vytvoření statického mapování pomocí služby WINS

1. V konzole správy počítače WINS klepněte ve stromu konzoly na položku **Aktivní registrace** a vyberte příslušný aktivní server WINS.
2. Z nabídky **Akce** zadejte příkaz **Nová statická**.
3. V dialogovém okně **Vytvořit statické mapování** zadejte v poli **Adresa IP** statickou adresu.

Na obrázku 7.2 vidíte dialogové okno Vytvořit statické mapování.



Obrázek 7.2 Statické mapování pomocí služby WINS.

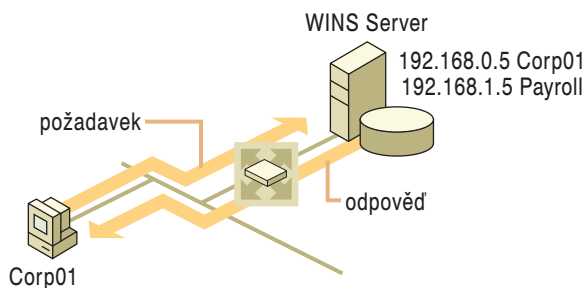
Když server WINS přijme požadavek na registraci jedinečného názvu rozhraní NetBIOS, ověří nejprve, zda už tento název v jeho databázi WINS neexistuje. Server WINS odešle kladnou nebo zápornou odpověď. Tabulka 7.2 obsahuje popis všech možných typů odezvy serveru WINS na požadavek registrace názvu.

Tabulka 7.2: Odezvy serveru WINS

Odezva serveru	Popis
Žádná odezva	Klient WINS odešle další požadavek na registraci stejného názvu.
Kladná odezva	Server WINS nenašel v databázi WINS žádný duplicitní název a proto odesílá žádajícímu klientovi kladnou odezvu. Odezva zahrnuje hodnotu TTL (time-to-live), která nastavuje dobu zapůjčení adresy IP zaregistrovanou v databázi na serveru aktivní (životnost). Klient musí svoji registraci obnovit ještě před vypršením zapůjčení.
Záporná odezva	Server WINS našel ve své databázi existující registraci požadovaného názvu. Server odešle klientovi paket WACK (čekat na potvrzení) a následně odešle výzvu zaregistrovanému vlastníkovvi názvu. Jakmile obdrží odpověď, odešle žádajícímu klientovi zápornou zprávu.

Když obdrží server WINS požadavek na registraci názvu, který už v databázi existuje, odešle vlastníkovvi názvu výzvu, zvanou dotaz na název. Server pak mezi jednotlivými výzvami čeká na odpověď 500 milisekund. Je-li klient vícedomým klientem, testuje server WINS každou z adres IP, vlastněných daným počítačem, a to tak dlouho, dokud neobdrží odpověď, nebo dokud neověří všechny adresy IP.

Na obrázku 7.3 vidíte tok zpráv mezi klientem, serverem a vyzývaným klientem. První zprávou je požadavek na registraci názvu; poslední je odezva dotaz na název.

**Obrázek 7.3: Registrace názvu klienta WINS.**

V prvním kroku, znázorněném na obrázku 7.3, odešle počítač CORP01 zprávu svému serveru WINS, která obsahuje požadavek na registraci jeho adresy. Tento požadavek je ve tvaru zprávy pro registraci názvu NetBIOS. Server odešle odpověď s potvrzením adresy, kterou doprovází odezva na zaregistrování názvu NetBIOS. Na vzdálené straně směrovače existuje ještě jeden server WINS. Tento server se dozví adresu počítače CORP01 v okamžiku replikace databáze serveru WINS.

Jak obnovují klienti WINS svoje názvy

Klienti WINS musí svoji registraci obnovovat před uplynutím nastaveného intervalu jejího zapůjčení. Interval obnovení určuje, jak dlouho bude server udržovat registrovaný název jako aktivní záznam v databázi WINS.

Když klient WINS obnovuje registraci svého názvu, odesílá serveru WINS požadavek na obnovení názvu. Požadavek na obnovení názvu obsahuje adresu IP a název

NetBIOS obnovovaného záznamu. Server WINS na tento požadavek odpoví a v odpovědi odešle také novou dobu životnosti registrovaného názvu.

Klient WINS při obnovování registrace svého názvu postupuje následujícím způsobem:

1. Když dosáhne klient $\frac{1}{2}$ životnosti registrace svého názvu, odešle serveru WINS automaticky požadavek na obnovení jeho registrace.
2. Pokud primární server WINS registraci neobnoví, bude klient po dobu 1 hodiny odesílat další požadavky na obnovení názvu vždy v 10minutových intervalech.
3. Klient WINS se po 1 hodině neúspěšných pokusů na primárním serveru WINS pokusí o obnovení registrace názvu pomocí sekundárního serveru WINS.
4. Pokud nebude název obnoven ani v databázi sekundárního serveru WINS, budou požadavky na obnovení názvu odesílány po dobu 1 hodiny, a to stejně jako u primárního serveru v 10minutových intervalech.
5. Klient WINS se po 1 hodině neúspěšných pokusů na sekundárním serveru WINS opět pokusí o obnovení registrace názvu pomocí primárního serveru WINS.
6. Tento proces pokusů o obnovení názvu v databázích střídavě primárního a střídavě sekundárního serveru WINS trvá tak dlouho, dokud nedojde k překročení životnosti záznamu v databázi nebo k jeho obnovení.
7. Po úspěšném obnovení názvu klienta WINS je nastaven také interval životnosti záznamu v databázi serveru WINS.
8. Pokud však nedojde k obnovení názvu během nastaveného intervalu, je záznam o názvu klienta z databáze uvolněn.

Jak klienti uvolňují své názvy

Názvy NetBIOS lze uvolňovat výslovně i mlčky. Výslovně jsou názvy NetBIOS uvolněny, je-li činnost klienta ukončena standardním způsobem. Tiché uvolnění názvu proběhne po selhání klienta nebo po jeho vypnutí. Toto nepřímé uvolnění názvu je serverem zaznamenáno, není-li po překročení životnosti záznamu v databázi WINS název obnoven.

Po uvolnění názvu je záznam v databázi označen jako uvolněný s časovým razítkem, jenž je součtem aktuálního času uvolnění a intervalu zániku. Interval zániku je doba mezi časem označení záznamu za uvolněný a časem, kdy je záznam označen jako neplatný. Časový limit zániku určuje interval mezi okamžikem, kdy byl záznam označen jako neplatný, a jeho skutečným odstraněním z databáze. Tato informace není přenášena na partnerské servery WINS. Je-li záznam uvolněn výslovně, převede server WINS vlastnická práva záznamu na sebe (pokud tomu již tak není).

V systému Windows 2000 je uvolnění položky z databáze WINS obslouženo jinak, pokud se ID vlastníka položky liší od identifikátoru serveru, jenž název zaregistroval. Dojde-li k tomu, je údaj označen jako neplatný a je k němu přiřazeno časové razítko, jež je součtem intervalu zániku a časového limitu zániku. Tato hodnota je nastavena proto, aby nedocházelo k nesrovnalostem mezi sekundárními a primárními servery WINS. Vzhledem k tomu, že uvolněný záznam už není dále replikován, mohl by být po jedné replikaci jeho název na jednom serveru WINS uvolněn, ale na jiném by mohl být aktivní ještě velmi dlouhou dobu, což je nežádoucí.

Změnou stavu uvolněného záznamu na neplatný se tento údaj přenesení do replikačního procesu a umožní rychlou synchronizaci databází WINS. Bez označení zániku záznamu by se mohly nesrovnalosti protahovat. Ukázková situace může nastat v okamžiku

ku, kdy je primární server WINS při ukončení činnosti daného klienta nedostupný. Uvolnění názvu by bylo v takovém případě nasměrováno na sekundární server WINS. Kdyby byl v okamžiku opětovného spuštění klienta aktivní opět primární server WINS, klient by se mohl zaregistrovat na tomto serveru a obnovit svůj název, jenž by se po celou dobu nezměnil, neboť server nezaznamenal žádnou změnu stavu klienta, přestože sekundární server WINS by neustále vyjadřoval skutečný stav klientského záznamu (uvolněný).

Jak klienti WINS překládají názvy

Díky protokolu NetBIOS rozlišují klienti WINS mapování názvů NetBIOS na adresy IP, vestavěné do součásti TCP/IP (NetBT). Počítače se systémem Windows NT jsou automaticky konfigurovány tak, aby používaly jeden ze čtyř různých režimů překladu názvů NetBT (metod překladu názvů), založených na způsobu nakonfigurování protokolu TCP/IP na daném počítači. Tabulka 7.1 obsahuje seznam režimů NetBIOS, včetně způsobů, kterými získávají adresy IP z názvů NetBIOS.

Chcete-li zobrazit konfiguraci TCP/IP svého počítače, zapište do příkazového řádku příkaz **ipconfig /all**. Pokud je počítač nakonfigurován jako klient WINS, zobrazí se po zadání příkazu **ipconfig /all** jako typ uzlu „Hybridní“.

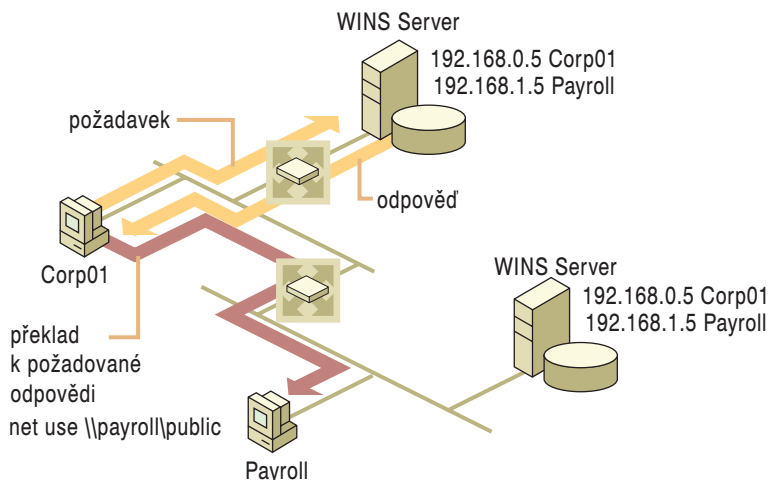
Proces překladu názvů mezi klientem WINS typu uzlu H a serverem WINS postupuje podle následujících kroků:

1. Když zadá uživatel na příkazovém řádku síťový příkaz, jako například **net use**, ověří klientský počítač, zda se ve vyrovnávací paměti nenachází název NetBIOS a adresa IP hostitele. Je-li údaj nalezen, je název hostitele přeložen bez vyvolávání jakékoli síťové aktivity.
2. Nenajde-li však klientský počítač název hostitele ve vyrovnávací paměti, pokusí se třemi pokusy spojit s prvním serverem WINS (je-li nakonfigurován). Pokud první server WINS neodpoví, pokusí se klient kontaktovat další server WINS. Takto bude postupovat se všemi servery WINS v síti. Po úspěšném přeložení názvu hostitele některým ze serverů WINS je klientovi vrácena příslušná adresa IP.
3. V případě, že není požadovaný název hostitele přeložen žádným z dostupných serverů WINS, vygeneruje klient vysílání uzlu B v lokální síti. Je-li požadovaný název NetBIOS v lokální síti nalezen, je přeložen na adresu IP.
4. Pokud nelze název NetBIOS získat vysláním uzlu B, ale je povoleno prohledávání souboru LMHOSTS, analyzuje klient místní soubor LMHOSTS. Je-li název nalezen v tomto souboru, je přeložen na adresu IP.
5. Jestliže aplikace nenalezla název ani v souboru LMHOSTS, pokusí se klientský počítač přeložit název pomocí dalších technik překladu názvu hostitele. Je-li zaškrtnuto políčko **Překlad systému Windows** používá DNS na kartě **Adresa WINS** v dialogovém okně **Vlastnosti TCP/IP**, pokusí se přeložit název pomocí místního souboru Hosts nebo serveru DNS.

Při překládání názvu hostitele ověřuje služba WINS místní soubor Hosts, kde se pokouší nalézt položku shodnou s názvem hostitele. Pokud je tato položka nalezena, je automaticky přeložena na související adresu IP. Soubor Hosts musí být ovšem umístěn na lokálním počítači.

6. Není-li název hostitele nalezen ani v souboru Hosts, vyšle klient požadavek nakonfigurovanému serveru DNS. Pokud název hostitele nalezne server DNS, přeloží jej také na příslušnou adresu IP.

V případě, že ani jedna z uvedených metod nepovede k úspěšnému přeložení názvu NetBIOS, vrátí příkaz **net use** chybu, která ukazuje, že počítač nelze najít.



Obrázek 7.4: řeklad názvu prostřednictvím služby WINS.

Z obrázku 7.4 je patrné, že první zprávou je požadavek na překlad názvu, odeslaný klientem jeho primárnímu serveru WINS. Tento požadavek je následován odezvou serveru WINS, který vrací požadovanou adresu IP. Klient ihned po přijetí této odezvy použije tuto adresu k vytvoření připojení k požadovanému zdroji.

Konflikty klientů zjištěné během registrace

Během registrace klientského uzlu nebo při obnovování názvu hostitele se může stát, že vyžadovaný název už v databázi WINS existuje. Následná akce, kterou vykoná server WINS, je závislá na stavu registrovaného názvu. Údaj s tímto názvem může být aktivní, uvolněný nebo neplatný. (Neplatným názvům se také říká zaniklé.) Název může být jednak jedinečným názvem počítače nebo procesu, ale také názvem skupiny, může být vlastněn serverem nebo replikou, může to být databázový údaj, zkopírovaný z jiného serveru WINS, se staticky nebo dynamicky přiřazovanou adresou IP. Adresa IP může být navíc stejná jako adresa určená v požadavku registrace názvu klienta nebo od ní odlišná.

Dva z těchto případů jsou za každých okolností obsluhovány stejně: nikdy nejsou přepisovány údaje o normální skupině ani statické záznamy. Pokud se jedná o název skupiny nebo statický název, vrátí server WINS zápornou odpověď vždy, když je ve své databázi najde. Skupiny Internet získávají další členy prostřednictvím datagramu Registrace skupiny Internet. Skupiny Internet nebo „speciální skupiny“ (jak se jim také občas říká) jsou používány pro speciální, uživatelsky definované administrativní skupiny. Jsou občas používány k seskupování prostředků, jako jsou souborové servery nebo tiskárny. V takových případech, je-li požadavek na registraci názvu v konfliktu s již uvolněným nebo zaniklým údajem, je tento požadavek považován za registraci nového názvu.

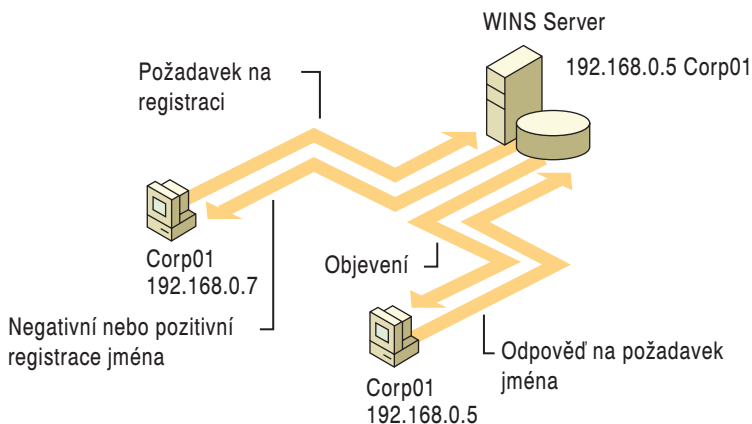
V případě jedinečných dynamických názvů, tzn. jsou-li adresy IP shodné, vrátí server WINS kladnou odpověď a chová se tak, jak je uvedeno v tabulce č. 7.3.

Tabulka 7.3: Odezvy na požadavek na registraci názvu

Stav názvu	Akce serveru
Vlastněn a aktivní	Aktualizace označení aktuálním časem
Replika a aktivní	Aktualizace označení aktuálním časem, převzetí vlastnictví, zvýšení ID verze.
Uvolněn	Aktualizace označení aktuálním časem, zaktivnění záznamu, zvýšení ID verze.
Vlastněn zaniklý	Aktualizace označení aktuálním časem, zaktivnění záznamu, zvýšení ID verze.
Replika označená jako neplatná	Aktualizace označení aktuálním časem, převzetí vlastnictví, zaktivnění záznamu, zvýšení ID verze.

Je-li adresa IP v požadavku registrace názvu odlišná od adresy IP uložené spolu s příslušným záznamem v databázi na serveru WINS, a je-li zároveň existující databázový záznam uvolněn nebo zaniklý, je požadavek považován za registraci nového názvu. Server odešle klientovi na tento požadavek kladnou odpověď a zaktualizuje údaj v databázi, aby ten odrážel nový čas, vlastnictví, identifikátor verze a aktivní stav.

Pokud je však existující databázový údaj aktivní a adresa IP v požadavku na registraci názvu je odlišná od adresy IP uložené spolu s příslušným záznamem, musí server WINS určit, zda je registrovaný název s adresou IP stále používán. Server WINS tedy odešle klientskému počítači s příslušnou adresou IP dotaz na název. Na obrázku 7.5 je znázorněn první krok požadavku registrace názvu, odeslaného klientem na příslušný server, za nímž následuje výzva serveru, ověřující starou adresu IP.

**Obrázek 7.5: Výzvy serveru WINS ověřující staré adresy.**

Pokud server obdrží na svůj dotaz kladnou odezvu, zamítne novou registraci a odešle žádajícímu klientovi zápornou odpověď. Jestliže však klient na staré adrese na dotaz serveru nezareaguje, bude server předpokládat, že k této adrese není přidružen žádný počítač a přijme novou registraci. V tomto případě vyjadřuje poslední šipka kladnou odezvu serveru na požadavek registrace nového názvu.

Chování klienta WINS

V tomto oddíle se zaměříme na reakce klientů WINS na různé základní scénáře, včetně:

- denního spouštění klienta WINS,
- zapojování klienta do jiné podsítě,
- prodloužených vypnutí,
- propojení dvou systémů WINS.

Denní spouštění

Aktivní registrace názvu klienta WINS v databázi serveru WINS je replikována na všechny partnerské servery tohoto serveru pro nabízenou replikaci (server WINS uvedený pod jménem Push). Partnerským serverem pro nabízenou replikaci je server WINS, jenž odesílá data jiným serverům a spouští tak replikaci. Po nějaké době je aktivní registrace názvu replikována na všechny servery WINS v síti.

Po vypnutí klienta WINS na konci dne je automaticky uvolněn také zaregistrovaný název. Při výchozím nastavení intervalu zániku se stav záznamu během následující noci nezmění na zaniklý, a proto není během této noci replikován. Po opětovném spuštění počítače následující den si klient WINS opět zaregistruje svůj název na serveru WINS a je mu přidělen nový identifikátor verze. Tento nový údaj aktivní registrace názvu je replikován na všechny partnerské servery pro vyžádanou replikaci serveru pro nabízenou replikaci stejně jako předchozího dne. Partnerský server pro vyžádanou replikaci je server WINS, jenž vyžaduje data, která pak budou odeslána z jiných serverů.

Počet každodenně replikovaných údajů o registraci názvu je zhruba stejný jako počet každodenně spuštěných počítačů krát počet názvů NetBIOS zaregistrovaných každým z těchto počítačů.

V rozlehlých sítích (50 000 a více počítačů) dochází k největšímu zatížení při odesílání požadavků na registraci názvu, generovaných při spouštění klientů WINS. Rozdíly v časových pásmech, jež se v takto rozlehlých sítích vyskytují, však naštěstí umožňují toto ohromné zatížení částečně rozložit.

Zapojování klienta do jiné podsítě

Uživatel na cestách, jenž vypne počítač a přesune se do jiné podsítě s jiným primárním serverem WINS, generuje výzvy na název. Typickou odezvou serveru při požadavku na registraci názvu je zpráva WACK (čekat na potvrzení). Potom, za předpokladu, že byl aktivní záznam replikován, vygeneruje nový server WINS paket s dotazem na název, obsahující výzvu na adresu IP, přiřazenou k existujícímu názvu v databázi. Vzhledem k tomu, že počítač, který tuto adresu v databázi zaregistroval, už není v původní podsíti aktivní (a tím pádem nepoužívá dříve přiřazenou adresu IP), neobdrží server na svůj dotaz žádnou odezvu. Aby bylo zajištěno, že chybějící odezva není pouze souhrou náhod, opakuje server WINS svůj dotaz třikrát po sobě.

Výzva na ověření názvu zpravidla nikdy neputuje do podsítě, kterou počítač opustil, neboť v takovém případě selže dotaz ARP. Přesto však zpráva o výzvě putuje do podsítě nového serveru WINS a propojení směrovačů. Server WINS přiřadí novému údaji nový identifikátor verze, takže nový záznam může být replikován z nového vlastníka na všechny ostatní servery WINS.

Prodloužená vypnutí

Některé počítače nejsou spouštěny po dobu delší než interval ověřování. Tento interval neboli četnost ověřování je doba, za kterou musí server WINS ověřit, zda jsou stále aktivní všechny staré názvy, které nevlastní a jsou v jeho databázi. Server WINS neodstraňuje údaje replik, týkající se těchto počítačů, neboť nevlastněné údaje nikdy nezanikají a zůstávají v databázi aktivní. Počítač, jenž je příležitostně spuštěn, obnoví všechny repliky příslušných údajů, kterým se přiřadí nový identifikátor verze. Tento ID verze vyzve k replikaci všech replik v ostatních databázích WINS v síti.

Občas se stane, že je počítač vypnutý delší dobu. Jeho replikované záznamy se neobnovují po dobu delší, než je nastavení intervalu ověřování. Zjistí-li server WINS takovou repliku, pokusí se ověřit její platnost prostřednictvím vlastnického serveru WINS. Pokud server-vlastník tento údaj nenalezne, bude související záznam z databáze ověřujícího serveru odstraněn. Dojde-li však k úspěšnému ověření platnosti záznamu, bude do databáze přenesen nový stav.

Vzájemné spojení dvou systémů WINS

Po sloučení dvou organizací musí dojít také ke sloučení jejich počítačových systémů, nevyjímaje z toho ani systémy WINS. Při slučování dvou systémů WINS může způsobit určité problémy jednak prvotní zatížení replikace, ale také možnost konfliktů názvů NetBIOS. Po připojení serveru WINS jednoho ze systémů k serveru WINS druhého systému dojde ke vzájemné replikaci záznamů na obou těchto serverech, neboť jejich databáze nemají žádné sdílené záznamy. Proto je třeba nejprve replikovat databáze obou systémů. Potom už partnerské servery replikace kopírují pouze záznamy nové, dokud se obě databáze nespojí v jednu.

Aby při tomto procesu nedocházelo k žádným dalším problémům, je třeba jednotlivé systémy slučovat a vynutit si replikaci v době, kdy jsou jednotlivá připojení příslušných propojení WAN víceméně nečinná. Bude-li databáze obsahovat konfliktní názvy, pokusí se systém tyto konflikty vyřešit, což může zvýšit momentální zatížení sítě. Tento proces byl popsán dříve v této kapitole v oddíle „Konflikty klientů zjištěné během registrace“.

Poznámka: Uživatelé počítačů s konfliktními názvy budou poté, co obdrží hlášení „duplicitní název“, hledat pomoc pravděpodobně u pracovníků odborné pomoci a jejich počítače budou odmítat otevírat nové relace.

Doporučené postupy pro klienty WINS

Správná konfigurace a správa klientů vyžadují určitou pozornost. Následující oddíly obsahují výčet nejvhodnějších postupů.

Konfigurace klientů pomocí plného seznamu serverů WINS

V předchozích verzích systému Windows NT byli klienti schopni využívat služby pouze primárního a sekundárního serveru WINS. V systému Windows 2000 lze klienty WINS nakonfigurovat pro využívání až 12 serverů WINS. Tyto servery lze navíc nakonfigurovat jako statické – v dialogovém okně Konfigurace TCP/IP – nebo dynamicky, prostřednictvím protokolu DHCP (nastavit možnost 44). Bude-li v systému nakonfigurováno více serverů WINS, klient získá větší odolnost proti chybám.

Používání příkazu Nbtstat –RR při správě propojitelnosti klienta

Nástroj příkazového řádku Nbtstat (novinka v systému Windows 2000) umožňuje odstranit z místní vyrovnávací paměti všechny názvy NetBIOS přiřazené vzdáleným názvům a vynutit si okamžité obnovení a novou registraci všech místních názvů klienta. Je to vhodné zejména jako první pomoc při potížích s propojitelností klienta WINS. Použití je vhodné k opětovnému zaplnění databáze klientskými údaji a k jejich replikaci na partnerský server WINS, aniž byste byli nuceni restartovat klientské počítače.

Postupy při konfiguraci klienta

Služba WINS je systém typu klient/server, jenž vyžaduje software na obou stranách procesu, tedy jak na straně klienta, tak na straně serveru. Jen tak může dojít ke správnému průběhu překladu a převodu názvů NetBIOS na adresy IP. Získání správné konfigurace klienta může odvrátit mnoho potenciálních problémů.

Klienti se systémem Windows NT, kteří se podílejí na službě WINS, si musí názvy NetBIOS zaregistrovat. Tyto názvy jsou nakonfigurovávány pomocí nástroje Systém v Ovládacích panelech a lze je libovolně měnit. Problémy mohou nastat, když uživatel změní název NetBIOS svého počítače na název počítače se systémem Windows 2000 nebo existující doménou systému Windows NT. Klient zde napodobí server a v podstatě se ve službě WINS zaregistruje jako počítač se systémem Windows 2000. To se může stát pouze tehdy, když není dostupný server nebo řadič domény, jenž by mohl zabránit přiřazení názvu WINS. Aby k tomuto problému nedocházelo:

- První, ale méně žádoucí metodou vypořádání se s problémem napodobování v systému Windows 2000, je umístění statických údajů v databázi WINS. Tím zajistíte, že žádný z uživatelů nebude moci nakonfigurovat svůj počítač tak, aby dynamicky napodobil server. Tato metoda, stejně jako všechny statické procesy, je pro správu náročnější než dynamická registrace názvu NetBIOS žádajícího počítače.
- Druhou metodou je nastavení konfigurací klientských počítačů tak, aby jejich uživatelé nemohli jejich názvy NetBIOS upravovat. Tato metoda zatěžuje proces registrace názvů NetBIOS ve službě WINS zcela minimálně a poskytuje navíc prostředí pro řízenou správu klientů. Pomocí nástroje pro správu systémových zásad, v němž můžete nastavit úroveň oprávnění uživatelů pro změny vlastností jejich pracovních stanic, tak můžete snadno řídit nastavení pracovních stanic se systémy Windows 95 a Windows NT.

Všechny klientské počítače by měly být inovovány na nejnovější klientskou platformu. Teprve pak bude možné získat plnou kontrolu nad všemi parametry přístupu ke konfiguraci pracovní plochy počítače. Pro zamezení přístupu uživatelů k nástrojům pro změnu názvů NetBIOS jejich počítačů používejte systémové zásady, implementované v konzole správy počítače. Tento nástroj spustíte poklepáním na ikonu Tento počítač a zadáním příkazu Správa, který najdete v rozevírací nabídce.

Servery služby Microsoft WINS

Na systém WINS, určený pro překlad názvů, lze nahlížet jako na ucelenou sadu komponent.

- **Server WINS** Jedná se o počítač, jenž poskytuje službu WINS a replikuje databázi WINS na jiné servery WINS tak, aby ucelená informace o překladu názvu na adre-

su IP byla dostupná vždy, a to bez ohledu na to, jaký server WINS daný klient WINS momentálně používá.

- **Klient WINS** Jsou to všechny počítače, které pracují se službou WINS a používají ji k registrování nebo obnovování svých názvů NetBIOS a svých adres IP.
- **Server proxy WINS** Je to počítač s podporou služby WINS, jenž je ve směrovacích sítích intranet typu TCP/IP prostředníkem při převádění dotazů na název počítačů, které se službou WINS nepracují.
- **Databáze WINS** Jedná se o dynamicky aktualizovaný seznam názvů NetBIOS a k nim přidružených adres IP, včetně adres IP přiřazených názvům prostřednictvím protokolu DHCP. V sítích s více servery WINS se databáze na jednotlivých serverech aktualizují pomocí mechanismu replikace.
- **Konzola systémového řízení WINS** Je to doplněk nástroje Microsoft Management Console, který poskytuje celou řadu řídicích nástrojů.

V následujících oddílech se některým z nich budeme věnovat podrobněji a začneme servery WINS a servery proxy, jež tvoří pomyslnou páteř celého systému.

Celkový pohled na servery WINS

Servery WINS předcházejí vzniku možných administrativních potíží, neodmyslitelně spjatých s dotazy na názvy NetBIOS a se staticky mapovanými soubory jako například soubory LMHOSTS. Služba Microsoft WINS odstraňuje potřebu vysílání dotazů na název NetBIOS, čímž šetří cennou šířku síťového pásma při současné možnosti dynamického mapování databází s údaji o přiřazení názvů NetBIOS k příslušným adresám IP.

Databáze replikované mezi jednotlivými servery WINS obsahují názvy NetBIOS a přidružené adresy IP. Když se do sítě přihlásí počítač s operačním systémem Windows, jsou jeho názvy NetBIOS, spolu s příslušnými adresami IP, automaticky zaregistrovány a přidány do databáze na serveru WINS (za předpokladu, že server pracuje s dynamickým aktualizací záznamů v databázi). Databáze serveru WINS je pak synchronizována s ostatními replikami na všech serverech WINS v síti LAN nebo WAN. Replikace databáze zabraňuje uživatelům ve vícenásobné registraci názvů NetBIOS pro různé počítače v jedné počítačové síti.

Server Microsoft WINS jednak řeší problémy, související s překládáním názvů prostřednictvím všesměrového vysílání IP, ale navíc také zprošťuje správce sítí povinnosti neustále aktualizovat statické soubory mapování. Služba WINS aktualizuje databázi WINS automaticky, jakmile je název NetBIOS dynamicky přiřazena nová adresa IP prostřednictvím protokolu DHCP (k čemuž dochází, když se počítač přesune do jiné podsítě).

Servery WINS poskytují kromě toho následující výhody:

- Dynamické databáze, které obsahují podporu pro registraci a překlad názvů NetBIOS v prostředí, v němž lze klientům, používajícím protokol DHCP, přiřazovat adresy TCP/IP dynamicky.
- Centralizovanou správu databáze názvů NetBIOS a její synchronizaci s jejími replikami na ostatních serverech WINS.
- Snížení počtu všesměrového vysílání dotazů na název NetBIOS.
- Podporu klientským počítačům se systémy Windows NT Server, Windows NT Workstation, Windows 95, Windows 98, Windows for Workgroups a LAN Manager 2.x.

- Podporu transparentního prohledávání sítě přes směrovače pro klientské počítače se systémy Windows NT Server, Windows NT Workstation, Windows 95, Windows 98 a Windows for Workgroups.

Servery Microsoft WINS komunikují s ostatními servery Microsoft WINS a synchronizují navzájem repliky svých databází. Tento proces zaručuje, že název zaregistrovaný na jednom serveru WINS bude replikován na všechny ostatní servery Microsoft WINS v rámci intranetu, ale pouze za předpokladu, že celý podnikový systém používá jednu databázi. Pokud podniková síť využívá více serverů WINS, je každý server WINS nakonfigurován jako partnerský server pro nabízenou nebo vyžádanou replikaci alespoň jednoho dalšího serveru WINS.

Partnerský server WINS pro vyžádanou replikaci je server, který od svého partnera žádá nové záznamy v databázi WINS, kterým se říká repliky. K přenosu dat dochází ve stanovených intervalech, definovaných replikačním intervalem, nebo jako odezva na zprávu o aktualizaci, odeslanou partnerským serverem pro nabízenou replikaci.

Partnerský server WINS pro nabízenou replikaci je server, jenž odesílá zprávy o aktualizaci vždy, když počet nových nebo zaktualizovaných záznamů v databázi překročí mez stanoveného počtu aktualizací, nebo je odesílá okamžitě. K tomu dochází pouze tehdy, je-li server nakonfigurován tak, aby odesílal zprávy ihned po změně adresy (tuto volbu lze vybrat zaškrtnutím políčka **Po změně adresy** v dialogovém okně **Partnerské servery pro replikaci** konzoly služby WINS). Pokud je váš server nakonfigurován právě takto, přenáší na partnerské servery po změně v databázi WINS aktivacíní procedury. Partnerské servery potom tyto změněné údaje vyžadují na serveru WINS, na němž je uložena aktualizovaná databáze.

Registrace názvů skupin

Kromě registrace jedinečných názvů, již se týkal předchozí popis rozhraní NetBIOS, umožňuje služba WINS také registrování názvů skupin. Služba WINS rozlišuje dva typy skupin: běžné a speciální.

Běžné názvy skupin

Běžný název skupiny se od běžného jedinečného názvu liší hned v několika klíčových ohledech. Nejdůležitějším z nich je absence přidružené adresy. Předpokládá se, že tento název je platný v rámci všech podsítí. Stejnou skupinu lze zaregistrovat dokonce na několika serverech WINS. Pro celou skupinu je k názvu přidruženo jedno časové razítko, jež sděluje poslední registraci nebo obnovení uzlu v libovolné podsíti. Když přijme služba WINS dotaz na název skupiny, vrátí omezenou vysílací adresu (255.255.255.255). Klient WINS potom tuto adresu vyšle do své podsítě, aby zjistil příslušný název.

Při synchronizaci názvů skupin mezi jednotlivými servery WINS je název přidáván do všech databází, v nichž se ještě nevyskytuje. Server WINS odpoví na dotaz na název uvolněných a zaniklých skupin. Konfliktní registrace jedinečných názvů vygenerují zápornou odezvu. V případě údajů o skupinách lze stavy jako uvolněný nebo zaniklý považovat za určitý typ pseudostavů (pseudouvolněný a pseudozaniklý). Tyto dva stavy se mění na konci intervalu zániku, což je hodnota určující délku prodlevy mezi uvolněním záznamu a jeho skutečným odstraněním. Po uplynutí této doby dochází ke zvýšení identifikátoru verze. Tato změna v podstatě znamená, že informace o stavu bude synchronizována s ostatními servery WINS.

Speciální názvy skupin

Po přijetí registrace názvu speciální skupiny uloží služba WINS aktuální adresu místo omezené vysílací adresy. Časové razítko, vyjadřující čas poslední registrace nebo obnovení záznamu, a identifikátor vlastníka jsou ukládány spolu s každou adresou, jež patří k dané skupině. Server WINS po přijetí dotazu na název takové skupiny vrací všechny adresy IP, jejichž platnost doposud nevypršela. Záznamy o těchto skupinách jsou, stejně jako běžné skupiny, replikovány ze serveru WINS, na němž byly poprvé zaregistrovány, na všechny partnerské servery v síti.

Tabulka 7.4 obsahuje seznam všech typů statického mapování názvů NetBIOS.

Tabulka 7.4: Statické mapování názvů NetBIOS

Volba typu	Popis
Jedinečný	Jedinečný název, k němuž je přidružena jedna adresa IP.
Skupina	Tomuto typu se také říká normální nebo „běžná“ skupina. Když skupinu rozšiřujete o další záznam pomocí modulu snap-in WINS, musíte zadat také název počítače a jeho adresu IP. Adresy IP jednotlivých členů skupiny nejsou ukládány v databázi WINS. Vzhledem k tomu, že adresy členů nejsou ukládány, neexistuje ve skutečnosti žádné omezení počtu členů dané skupiny. Všesměrová Vysílání paketů s názvem jsou používána ke komunikaci s jednotlivými členy skupiny.
Doména	Mapování názvu NetBIOS na adresu IP, které má na místě 16. bajtu zapsanou hodnotu 0x1C. Skupina domény uchovává až 25 adres pro členy skupiny. Při registraci dalších adres přepisuje adresu repliky nebo, pokud žádná neexistuje, přepisuje starší registraci. Názvy domény jsou používány k přidávání statických údajů pro počítač, určený názvem ve statickém mapování, do seznamu řadičů domén, používaných v dané počítačové síti.
Skupina Internet	Skupiny Internet jsou uživatelsky definovanými skupinami, které umožňují přístup ke prostředkům skupiny, jako jsou například sdílené tiskárny pro snadné odkazy a procházení. Standardně je 16. bajt názvu nastaven na hodnotu 0x20. Skupina síť Internet může uchovávat maximálně 25 adres svých členů. Po zaregistrování skupiny Internet, budou automaticky do databáze přidány tři jedinečné záznamy: InternetGroupName<0x20> se používá pro registrování souborů, InternetGroupName<0x0> se používá pro registrování pracovní skupiny a InternetGroupName<0x3> je používána službou Messenger. (Služba Messenger se využívá pro zobrazení zpráv v místních oknech na obrazovce počítače. Zprávy tiskárny například sdělují, že tisk byl úspěšně dokončen.) Je to velmi podobné přidávání členů do skupiny domény. Nové členy skupiny Internet lze přidávat prostřednictvím dynamické registrace skupiny. Dynamicky přidáný člen však nemůže nahradit člen statický, přidáný pomocí konzoly systémového řízení WINS nebo importováním souboru LMHOSTS.
Vícedomý	Je to jedinečný název, jenž může obsahovat více než jednu adresu a který se používá pro vícedomé počítače. V databázi může být nadefinováno maximálně 25 adres vícedomých počítačů. V případě všech dalších adres těchto počítačů přepisuje služba WINS adresu repliky nebo, pokud v databázi není žádná replika, přepisuje starší registraci.

Sekundární servery WINS

Klientské počítače by měly mít nastaveny jak primární, tak sekundární server WINS. Ne-li možné spojit se s primárním serverem WINS a použít některou z jeho funkcí (jako například registrace, obnovení, uvolnění, dotaz), může klient vyžadovat stejnou službu na sekundárním serveru. Klient se však pravidelně pokouší o obnovení spojení s primárním serverem.

Poznámka: Přestože systém Windows 2000 Advanced Server podporuje clustering pro servery WINS, je tato služba ve většině případů postradatelná. Konfigurací sekundárního serveru WINS dosáhnete stejného efektu. Správa sekundárního serveru WINS je kromě toho podstatně snazší a navíc může být sekundární server WINS umístěn na jiném místě. Další podrobnosti, týkající se clusteringu serverů WINS najdete v oddílu „Clustering – seskupování“ později v této kapitole nebo v kapitole „Windows Clustering“ v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.

V sítích s primárními a sekundárními servery WINS se doporučuje, aby polovina klientů používala jeden server jako primární server WINS a druhý server jako sekundární, zatímco druhá polovina klientů bude využívat opačné nastavení. Tímto způsobem se jednak sníží zatížení serveru na polovinu, ale bude také zaručeno, že sekundární server nebude čekat nečinně, zatímco primární server je neustále zahlcován dalšími a dalšími požadavky.

Server proxy služby Microsoft WINS

Ve specifikaci RFC 1001 se doporučuje nepoužívat překlad názvů typu uzel B ve směrovaných sítích – což znamená nespolehat se na všesměrové vysílání dotazů na název. V praxi jsou však uzly B užitečné i ve směrovaných sítích a někdy je dokonce nejde ani odstranit či aktualizovat. Z tohoto důvodu uvedla společnost Microsoft na trh servery proxy WINS. Server proxy WINS je počítač s podporou služby WINS, jenž pomáhá v překládání dotazů na název, vysílaných počítači, které ve směrovaných sítích typu TCP/IP nepracují se službou WINS.

Počítače, které nejsou pro spolupráci se službou WINS nakonfigurovány, používají k překladu názvů uzel typu B. Server proxy WINS sleduje místní podsít' a odposlouchává všesměrová vysílání názvových služeb uzlu B (jako například registrace, obnovení, uvolnění či dotazu) a reaguje na ty názvy, které nejsou součástí místní sítě. Server proxy WINS komunikuje s ostatními servery WINS pomocí jednosměrových datagramů, jejichž pomocí získává informace nezbytné k vytvoření odezvy požadované přijatým vysláním.

Server proxy WINS překládá názvy klientů s nenainstalovanou službou WINS následujícím způsobem:

1. Když takový klient odešle dotaz na název, server proxy WINS jej přijme a ověří, zda se v jeho vyrovnávací paměti nenachází údaj, jenž by vytvářel vazbu mezi požadovaným názvem NetBIOS a adresou IP.
2. Je-li tento údaj ve vyrovnávací paměti, odešle nalezenou informaci žádajícímu počítači jako odezvu na dotaz na název NetBIOS.
3. Není-li název ve vyrovnávací paměti, odešle serveru WINS dotaz na adresu IP přidruženou k požadovanému názvu.
4. Pokud v dané podsíti není dostupný žádný server WINS, může server proxy WINS odeslat dotaz jinému serveru WINS, umístěnému za směrovačem, zatímco

požadované názvy NetBIOS a adresy IP uchovává ve vyrovnávací paměti pro pozdější dotazy.

Význam serveru proxy WINS lze přirovnat k významu protokolu DHCP a agentům přenosů BOOTP, kteří předávají požadavky klientů DHCP napříč směrovači. Vzhledem k tomu, že server WINS neodpovídá na všesměrové vysílání, měl by být v každé podsíti, obsahující počítače bez podpory služby WINS, nastaven jeden počítač jako server proxy WINS.

Server proxy WINS ověřuje všesměrově vysílanou registraci názvu v databázi WINS, neboť odesílá požadavek s dotazem na název. Tím zaručuje, že názvy nebudou v konfliktu s jinými názvy v databázi. V případě, že požadovaný název už v databázi WINS existuje, vygeneruje obvykle server proxy WINS na registraci názvu žádajícího počítače zápornou odezvu. Jako odpověď na požadavek uvolnění názvu server proxy WINS jednoduše odstraní záznam, uložený ve vyrovnávací paměti.

Když server proxy WINS přijme dotaz na název, ověří, zda se název nenachází v jeho tabulce vzdálených názvů. Server vždy rozlišuje mezi dotazy na název pocházející z místní podsítě a dotazy na název přicházející z jiných částí sítě. Pomocí masky podsítě porovnává adresy jednotlivých názvů s vlastními adresami a jsou-li tyto hodnoty shodné, na přichází dotaz nereaguje.

Pokud server proxy WINS nenajde název ve své tabulce vzdálených názvů, odešle dotaz na server WINS. Potom vloží název do tabulky vzdálených názvů a nový záznam označí příznakem „určuje se“. Jestliže server proxy WINS obdrží dotaz na stejný název ještě dříve, než mu stačí odpovědět server WINS, nebude už odesílat další dotazy. Pokud server proxy WINS obdrží odpověď serveru WINS, zaktualizuje údaj v tabulce vzdálených názvů, v němž nastaví správnou adresu a změní příznak záznamu na „určeno“. V případě, že server proxy WINS už obsahuje odpověď ve své vyrovnávací paměti, pouze ji odešle jako odezvu na požadavek klienta WINS.

Chování klienta uzlu B se po přidání serveru proxy WINS do místní podsítě nezmění. Po překročení časového limitu prvního dotazu na přeložení adresy IP se b klient pokusí zjistit adresu následujícím dotazem. Pokud server proxy WINS má odpověď na dotaz uloženu ve své mezipaměti, odešle ji okamžitě žádajícímu klientovi.

Poznámka: V každé podsíti by měl být jako server proxy WINS nastaven pouze jeden počítač. Vzhledem k tomu, že každý server proxy WINS v síti přenáší všechna zachycená vysílání, mohlo by nastavení více počítačů v podsíti jako serverů proxy WINS neúměrně zatížit vlastní servery WINS.

Když server proxy WINS zachytí další dotaz na stejný název, odešle klientovi vyžadovanou odpověď znova. Rozhraní NetBIOS neobsahuje žádné opatření, pro „doručení“ přeložené adresy IP názvovým serverem klientovi. Název je vždy přeložen jako odezva na dotaz. Proto tedy musí být počítače, využívající službu WINS Proxy pro uzly B, nakonfigurovány tak, aby vytvářely stejný dotaz opakovaně. A aby nedocházelo ke zdvojení provozu, měl by být v každé podsíti v daném okamžiku aktivní pouze jeden server proxy WINS.

Mapování názvu na adresu IP, přijaté serverem proxy WINS od serveru proxy WINS, je po určitou dobu ukládáno v jeho vyrovnávací paměti. Standardně je tato hodnota nastavena na 10 minut. Minimální povolenou hodnotou je 1 minuta.

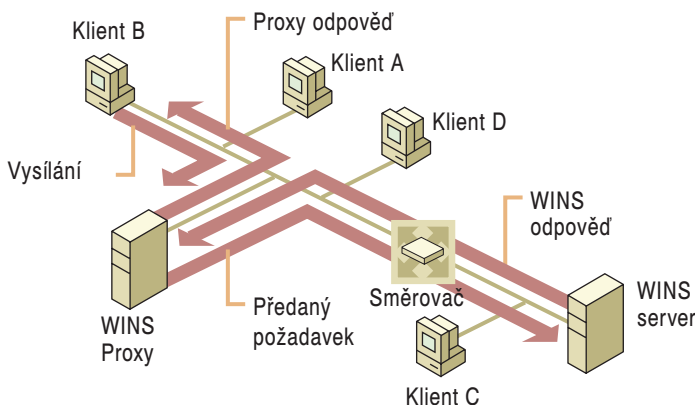
Má-li být počítač serverem proxy WINS, je třeba upravit odpovídajícím způsobem také jeho systémovou registrační databázi. Hodnota klíče EnableProxy musí být nastavena na 1 (REG_DWORD). Tento údaj je uložen v následujícím podklíči registru:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netbt\Parameters

Upozornění: K přímé editaci registru se uchylujte skutečně až tehdy, nezbyvá-li žádná jiná možnost jeho úpravy. Editory registru obcházejí standardní bezpečnostní opatření, poskytovaná správnými nástroji. Tato bezpečnostní opatření zajišťují prevenci proti zadávání konfliktních nastavení nebo nastavení, která by mohla snížit výkon systému nebo dokonce systém poškodit. Přímá editace registru může mít vážné a nepředpokládané následky, jež mohou ve svém důsledku zabránit spuštění systému. Takové poškození lze řešit jedině opětovnou instalací systému Windows 2000. Chcete-li konfigurovat nebo přizpůsobit nastavení systému Windows 2000, používejte k tomu účelu program Microsoft Management Console (MMC) nebo jiné nástroje Ovládacích panelů.

Dotazy pomocí serveru proxy WINS

Na obrázku 7.6 je znázorněna malá síť typu LAN založená na všesměrovém vysílání, skládající se ze dvou klientů (A a B), pomocí směrovače připojená k rozlehlejší síti. Aplikace rozhraní NetBIOS na klientském počítači B vyžaduje komunikaci s klientem C. Za normálních okolností by to nebylo možné, neboť klient C je na jiné straně směrovače. Klienti B a C spolu ale mohou komunikovat, neboť počítač s nainstalovaným operačním systémem Windows 2000 Professional v síti LAN se chová jako server proxy WINS.



Obrázek 7.6: Činnost serveru proxy WINS.

Klient B všesměrově vysílá dotaz na název s požadavkem na získání adresy IP klienta C. Klient C tento požadavek nezachytí, neboť se všesměrové vysílání zastaví na směrovači. Server proxy WINS však toto všesměrové vysílání pro uzel v jiné podsíti zachytí a odešle serveru WINS požadavek s dotazem na název v podobě jednosměrového datagramu. Server WINS vrátí serveru proxy WINS kladnou odpověď, obsahující adresu IP klienta C. Zde bude tento údaj uložen do vyrovnávací paměti pro pozdější použití. Server proxy WINS navíc tuto informaci předá klientovi B.

Řízení shlukového přenosu

Díky implementaci řízení shlukového přenosu v systému Windows 2000 mohou nyní servery WINS pracovat s rozsáhlým (neboli výbojovým) zatížením serveru. Tyto situace se vyskytují vždy, když o zaregistrování svých názvů usiluje právě v jednom okamžiku velký počet klientů WINS. V režimu shlukového přenosu odešle server WINS kladnou odezvu klientům ještě předtím, než ve své databázi zpracuje a skutečně uloží všechny příslušné aktualizace.

Režim shlukového přenosu používá hodnotu velikosti fronty shlukového zpracování k nastavení mezního počtu požadavků na registraci či obnovení, které může zpracovat běžným způsobem do doby, než server WINS přejde do režimu shlukového přenosu. Standardně umožňuje fronta shlukového zpracování vyřízení 500 požadavků, než server WINS použije shlukové zpracování. Další podrobnosti, týkající se změny nastavení fronty shlukového zpracování vyhledejte v oddílu „Konfigurace podpory režimu shlukového zpracování“ dále v této kapitole.

Fronta shlukového zpracování umožňuje serveru WINS řídit střídavě vyřizování požadavků na registraci či obnovení například po prvním spuštění serveru WINS nebo po jeho spuštění s prázdnou databází, či v situacích, kdy se do systému najednou přihlásí velký počet nových klientů WINS. Všechny tyto stavy vytvářejí velký počet požadavků na registraci či obnovení názvů.

Funkce řízení shlukového přenosu je určena pro zběžné vyřizování požadavků (s kladnou odezvou), a tím pádem pro snížení zatížení sítě. Řízení shlukového přenosu také rozšiřuje a obměňuje interval zpoždění tak, aby bylo zatížení sítě rozloženo na větší časové úseky.

Řízení shlukového přenosu je povoleno všem serverům WINS se systémem Windows NT Server 4.0 se stávající aktualizací Service Pack či se systémem Windows 2000. Server WINS, jenž umožňuje řízení shlukového přenosu, použije shlukové zpracování, jakmile počet požadavků na registraci názvu překročí nastavenou hodnotu velikosti fronty shlukového zpracování.

Jak funguje shlukové zpracování

Pomocí funkce shlukového zpracování lze neprodleně vyřídit dodatečné požadavky klientů, které překročily mezní hodnotu velikosti fronty, a kladně na ně zareagovat. Odezva serveru WINS také obsahuje proměnlivý interval zpoždění nebo interval zapůjčení adresy, jenž pomáhá regulovat zatížení při registraci klienta, stejně tak jako řízení požadavků, přijatých v jednom intervalu shlukového zpracování.

Zahrnutí intervalu zpoždění do následujících odpovědí snižuje stupeň zatížení, způsobený novými či opakovanými pokusy klientů o obnovení nebo registraci názvu, a reguluje výbojové přenosy klientů WINS.

Pro každých dalších přibližně 100 klientských požadavků bude server WINS zvětšovat interval zpoždění o dalších 5 minut, dokud tento interval nedosáhne souhrnné hodnoty 50 minut. Přicházejí-li klientské požadavky i nadále ve shlukových přenosech, i když interval zpoždění dosáhl svého maxima, odpoví server WINS následujícím 100 klientským požadavkům s výchozím intervalem zpoždění, rovným 5 minut. Přírůstkový proces se tak spustí znova.

Pokud je například výchozí velikost fronty shlukového zpracování nastavena na 500 údajů, zpracuje server WINS běžným způsobem prvních 500 požadavků. Dalším 100 klientům odpoví také okamžitě tím, že jim odešle časnou odezvu o úspěšné registraci. Tyto časné odezvy používají výchozí interval zpoždění, nastavený na hodnotu 5 minut.

Server WINS pak tímto způsobem pokračuje ve zpracovávání shlukových přenosů, dokud příjem dotazů na registraci či obnovení názvu nedosáhne maximální hodnoty 25 000. Od tohoto okamžiku začne server WINS nové dotazy rušit.

Konfigurace podpory režimu shlukového zpracování

Změnu v nastavení stupně podpory režimu shlukového zpracování můžete provést v dialogovém okně **Vlastnosti služeb WINS** serveru WINS. Chcete-li otevřít toto dialogové okno, musíte otevřít složku **Ovládacích panelů**, kde poklepejte na ikonu **Systémové nástroje**. Ze zobrazeného seznamu vyberte ikonu **Správa počítače** a otevřete skupinu **Služby a aplikace**. V této skupině klepněte na položku **WINS** a potom z nabídky **Akce** zadejte příkaz **Vlastnosti**. Chcete-li nastavit bližší údaje nebo dokonce zakázat používání shlukového zpracování, klepněte na tlačítko **Upřesnit**.

Pro konfiguraci režimu shlukového zpracování jsou určeny čtyři tlačítka: **Nízká**, **Střední**, **Vysoká** a **Vlastní**. Tlačítko **Vlastní** umožňuje nastavit počet dotazů v rozmezí od 50 do 5 000. tlačítka **Nízká**, **Střední** a **Vysoká** nastavují velikost fronty shlukového zpracování na 300, 500 a 1 000 dotazů.

Režim shlukového zpracování je ve výchozím nastavení povolen a velikost fronty je nastavena na hodnotu Střední.

► Úprava řízení shlukového přenosu

1. Ve stromu konzoly MMC klepněte na název serveru WINS, jehož vlastnosti chcete upravovat.
2. Z nabídky **Akce** zadejte příkaz **Vlastnosti**.
3. Klepněte na tlačítko **Upřesnit**.
4. V seznamu **Povolit řízení shlukového přenosu** upravte výchozí nastavení podle vlastních potřeb.
5. Chcete-li získat nápovědu, týkající se jednotlivých položek dialogového okna, klepněte na požadované položce pravým tlačítkem myši a z místní nabídky zadejte příkaz **Co je to?**

Clustering – seskupování

Systém Windows 2000 umožňuje seskupování serverů WINS. Přesto se však před přidáním serveru WINS do skupiny seskupených serverů ujistěte, zda znáte všechny výhody, ale i nevýhody tohoto kroku. V mnoha případech, kdy je celkový počet serverů WINS nízký, je seskupování serverů WINS jednoduše zbytečné – díky replikaci je služba WINS odolná proti poruchám. V takových případech byste měli na klientských počítačích nakonfigurovat také sekundární server WINS, abyste zaručili nepřerušovaný provoz služby.

► Přidání služby WINS skupině serverů

1. Ujistěte se, že je služba WINS nainstalována a spuštěna na obou serverech.
2. Klepněte pravým tlačítkem myši uvnitř dialogového okna a z místní nabídky zadejte příkaz **Nový prostředek**.
3. Potom klepněte na tlačítko **Další** a vyberte skupinu serverů, kterou chcete přidat.
4. Nyní zadejte všechny možné vlastníky – tzn. jiné členy skupiny.
5. Nastavte závislosti prostředku: jednotku, adresu IP a síťový název.
6. Zadejte cestu k záložní databázi a klepněte na tlačítko **Dokončit**.

Ujistěte se, že vlastník, k němuž chcete službu WINS přidat, má disk, adresu IP a síťový název. Cesta k databázi musí být ukončena zpětným lomítkem (\) a musí určovat umístění na vybrané závislé jednotce. Je-li touto závislou jednotkou například jednotka G, musíte nastavit cestu k databázi na této jednotce .

Správnou funkci seskupení ověřte připojením závislé jednotky (na počátku je ve stavu offline). Potom klepněte pravým tlačítkem myši uvnitř okna a tažením přemístěte skupinu na jiný uzel. Skupiny zobrazí jednotku jako přemístitelný prostředek. Jednotka pak bude přesunuta v rámci příslušné skupiny z jednoho uzlu na jiný. Při přesouvání prostředku byste měli pozorovat změnu údaje v seznamu Vlastník.

Podrobnější informace o seskupování serverů WINS můžete najít v kapitole „Seskupování v systému Windows“, která je součástí dokumentace *Microsoft® Windows® 2000 Server Distribuované systémy*.

Poznámka: Rozhodnete-li se pro seskupování serverů WINS, uvědomte si, že byste měli tyto servery vybavit pevnými disky s rychlým rozhraním vstup/výstup, vyčleněnými pro práci se službou WINS. Tento krok umožní zrychlení odezvy databáze a zaručí vysokou efektivitu seskupených serverů.

Doporučené postupy při práci se servery WINS

Udržováním serverů WINS a jejich chodu můžete předejít přechodu klientů WINS k překládání názvů v režimu uzlu B a následnému zaplavení sítě všesměrovým vysíláním jejich požadavků. Následující odstavce přinášejí několik návrhů, směřujících k efektivní správě činnosti serverů.

Používání výchozí konfigurace

Výchozí nastavení služby WINS, vytvořené při první instalaci služby, poskytuje optimální konfiguraci pro většinu možných okolností a mělo by být používáno ve většině síťových instalací služby WINS. Pokud se rozhodnete tato nastavení změnit, ujistěte se, že je to skutečně zapotřebí a že chápete všechny možné důsledky tohoto kroku.

Minimalizace počtu serverů WINS

Používání příliš velkého počtu serverů WINS může znásobit problémy příslušné sítě, takže při přidávání nových serverů WINS buďte spíše opatrní. Při zajišťování služeb všech klientů WINS se pokuste používat minimální počet serverů tak, aby toto množství neovlivňovalo přijatelný výkon celého systému.

Při plánování činnosti serverů pamatujte na to, že každý server WINS může simultánně zpracovávat stovky registrací a dotazů za sekundu. Částečně je to dáno malým objemem dat, přenášeným mezi servery WINS a jejich klienty. Průměrná velikost záznamu WINS se pohybuje okolo 40 bajtů.

Přenosy v síti WINS mohou být během registrace klienta přibližně stejné jako v případě služby DHCP, která využívá k nalezení serverů klientské vysílání. Většina klientů WINS standardně nejprve odesílá svému primárnímu serveru WINS jednosměrové směrované datagramy.

Obecně platí, že byste se měli vyhýbat rozmísťování velkého počtu serverů WINS. To však samozřejmě neplatí, existuje-li k takovému postupu skutečně vážný důvod. Omezením počtu serverů WINS minimalizujete počet přenosů v síti WAN, jež jsou zapotřebí k zajištění synchronizace replik na jednotlivých serverech WINS. Menší počet těchto

serverů také zajišťuje solidní vlastnosti při překladu adres IP a navíc snižuje problémy spojené se správou systému, aniž by bylo třeba obětovat něco z funkčnosti systému. Při návrhu instalace služby WINS, která zahrnuje více než 20 serverů WINS, se doporučuje požádat o pomoc pracovníky odborné pomoci společnosti Microsoft.

Servery WINS přijímají požadavky v podobě jednosměrových směrovaných datagramů, což znamená, že jsou tyto požadavky směrovány. Proto tedy jeden server WINS postačuje pro zajištění služeb pro síť o 10 000 uzlech, ačkoli pro zajištění odolnosti systému proti poruchám se doporučuje začlenit do systému alespoň servery dva. Vzhledem k tomu, že výměna dat mezi servery WINS a jejich klienty probíhá ve zprávách o velikosti přibližně 40 bajtů a služba WINS navíc používá ke vzájemné komunikaci směrované datagramy, postačuje pro správu velmi malých sítí i jeden server WINS.

Na základě počtu procesorů určuje služba WINS, kolik podprocesů je třeba vytvořit, aby bylo možné dotazy klientů zpracovat. Služba vytvoří jeden podproces pro každý procesor. Každá registrace názvu trvá při povolení protokolování přibližně 40 milisekund. Je-li protokolování zakázáno, probíhá registrace mnohem rychleji. tato konfigurace však hrozí v případě poruchy ztrátou posledních několika aktualizací databáze WINS.

Používání výkonného diskového hardwaru

Služba WINS vyžaduje opakovanou a intenzivní činnost pevných disků serveru. Aby byl zajištěn jejich nejlepší výkon, doporučuje se při koupi hardwaru pro server WINS také pořídit řešení založených na technologii RAID, která podstatně snižují přístupovou dobu k jednotkám. Při hodnocení výkonu serveru byste měli vzít v úvahu také činnost služby WINS. Nejlepší odhad požadavků na hardwarové vybavení serveru získáte monitorováním výkonu systémového hardwaru v nejdůležitějších oblastech využití (procesor, paměť a rozhraní vstup/výstup diskových jednotek). Jedině tak můžete zjistit, zda je váš server přetěžován a zda by měl být inovován.

Hardware pro síťové rozhraní přidávejte s rozvahou

Při rozšiřování počítače se systémem Windows 2000 o další síťové adaptéry postupujte opatrně. Budete-li přidávat nový hardware do počítače, na kterém jsou spuštěny procesy kritické pro chod celého systému, můžete spolehlivost systému zvýšit tím, že dočasně snížíte počet služeb, provozovaných na inovovaném počítači. Velkou část těchto služeb (jako například řadič domény) lze dočasně přenést na jiný počítač a vrátit je zpět až po dokončení inovace počítače.

Nastavení serveru tak, aby registroval sám sebe

Každý server WINS nainstalovaný v systému musí ve službě WINS zaregistrovat také sebe a nastavit si vlastní jedinečné názvy NetBIOS. Je-li registrace a vlastnictví záznamu WINS rozděleno, mohlo by ve službě WINS docházet k nežádoucím problémům. Je to proto, že by mohlo dojít k situaci, kdy by názvy, registrované pro určitý server WINS vlastnil jiný server WINS. Aby k tomu nemohlo dojít, je nezbytné nakonfigurovat každý server WINS tak, aby byl svým primárním i sekundárním serverem WINS.

Odolnost serveru WINS proti chybám

Chcete-li se vyhnout jakýmkoli potížím, jež by mohly vyplynout ze selhání při komunikaci v rámci služby WINS, prozkoumejte možnost využití statického souboru LMHOSTS, jenž by poskytoval sekundární prostředek pro překlad adres IP v situaci, kdy by došlo k selhání služby WINS. Přestože tyto soubory nejsou považovány za nej-

lepší řešení, mohou v takových výjimečných situacích poskytovat efektivní prozatímní náhradu. Soubory LMHOSTS je však třeba pečlivě spravovat, neboť změny v prostředí NetBIOS neaktualizují statické názvové soubory.

Abyste mohli využívat překlad adres IP pomocí souborů LMHOSTS, musíte mít správně nakonfigurovaný soubor LMHOSTS, schopný vyhledávat počítače se systémem Windows 2000 i po selhání služby WINS. Hlavní soubor LMHOSTS by měl obsahovat statické mapování adres IP počítačů se systémem Windows 2000. Tento soubor by také měl být rozeslán do všech domén systému Windows prostřednictvím jedné z následujících tří možností:

- Typický soubor LMHOSTS v systému Windows 2000 obsahuje cestu k centrálnímu souboru ve tvaru UNC (universal naming convention). V případě, že cesta ukazuje na jeden soubor, stačí, když budete udržovat pouze jednu kopii souboru LMHOSTS.
- V případě počítačů bez systému Windows 2000 můžete rozvrhnout úlohu pomocí plánovací služby. Tato služba automaticky rozešle hlavní soubor LMHOSTS na všechny určené servery. Příkaz winat, jenž je součástí soupravy prostředků Windows 2000 Resource Kit, tuto úlohu usnadní ještě více. Odešlete soubor jak na primární řadič domény (PDC), tak na záložní řadiče všech domén (BDC).
- Nejméně efektivní možností je ruční kopírování souboru na všechny servery a klienty, kteří by jeho služby mohli vyžadovat. Stejně neproduktivní je také ruční aktualizace souboru LMHOSTS. Přesto se i tato metoda může vyplatit například v sítích s jedním serverem WINS.

Jakmile je soubor LMHOSTS připraven a rozeslán, bude v případě selhání některého serveru obsahovat odkaz na hlavní soubor LMHOSTS ve sdíleném adresáři na PDC. Pokud navíc použijete direktivu #INCLUDE, bude centrální soubor LMHOSTS dostupný také z alternativních serverů.

Nepoužívejte znaky rozšířených znakových sad

V názvech NetBIOS nepoužívejte znaky rozšířených znakových sad, obzvláště pak podtržítka (_) a tečku (.). Znak podtržítka je v názvech DNS hostitelských počítačů převáděn na pomlčku. Přiblížíme-li si to na příkladu, pak se z názvu NTServer_1 stane NTServer-1, což samozřejmě povede k selhání při pokusu o překlad názvu na adresu IP, neboť tento název ve skutečnosti může být uložen v souborech DNS.

Srovnejte intervaly zapůjčení a obnovení názvů ve službách DHCP a WINS

Při konfigurování sítě pro používání protokolu DHCP i protokolu WINS nastavte dobu zapůjčení názvu DHCP tak, aby se zhruba shodovala s intervalem obnovení služby WINS nebo byla ještě větší. Tímto krokem předejdete situaci, v níž se může stát, že server WINS nezareaguje na to, že klient DHCP uvolnil adresu IP, přiřazenou službou DHCP. Klient nemůže odeslat požadavek na obnovení názvu, pokud neobnoví registraci přidělené adresy IP. Dojde-li k tomu, že je nový počítač k dané adrese IP přiřazen ještě předtím, než se o tom dozví server WINS, může se stát, že server chybně nasměruje požadavek na adresu novému klientu.

Databáze WINS

V případě, že klient vyžaduje kontakt na jiný hostitelský počítač v síti, spojí se nejprve se serverem WINS, jemuž odešle dotaz na název. Ten přeloží název pomocí mapovací informace, uložené ve své databázi. Relační databázový stroj serveru WINS se k databázi připojuje metodou indexsekvenčního přístupu (ISAM). Databáze ISAM je replikovanou databází, která obsahuje názvy NetBIOS počítačů se souvisejícími adresami IP.

Aby se mohl klient WINS k síti přihlásit, musí nejprve na serveru WINS zaregistrovat svůj název a adresu IP. Tím v databázi WINS zajistí vytvoření jednoho údaje o klientovi. Vzhledem k tomu, že tyto údaje jsou aktualizovány při každém přihlášení se klienta do sítě, je informace uložená v databázi serveru WINS neustále aktuální.

Správa databáze serveru WINS

Databáze WINS v systému Windows 2000 využívá zdokonalený nástroj Rozšiřitelné jádro úložiště, což je vylepšená verze obecně použitelného jádra úložiště, používaného jak servery Microsoft Exchange 5.5, tak servery Windows 2000. Tato databáze nezávisí žádná omezení, týkající se počtu ukládaných či replikovaných záznamů. Velikost databáze je závislá na počtu klientů WINS v síti, ale není přímo úměrná počtu aktivních klientských údajů. S narůstajícím počtem neaktivních údajů také narůstá samotná databáze WINS a mnoho údajů o klientech WINS se stává zastaralými. Nakonec tyto údaje přeplní celou databázi.

K obnovení nevyužitého prostoru je databáze WINS komprimována. V systému Windows 2000 probíhá komprimace jako automatický proces spuštěný na pozadí a probíhající v době nečinnosti databáze po vykonání všech aktualizací. Vzhledem k tomu, že je komprimace databáze také dynamická, není třeba k tomuto účelu server WINS zastavovat. Tomuto procesu se také říká komprimace online. I když služba WINS pravidelně komprimace online provádí, je občas třeba využít také komprimace offline, i když v podstatně omezené míře. Proto musí být služba WINS čas od času přerušována, aby bylo možné právě komprimaci offline provést. Více informací na toto téma budete mít k dispozici v oddíle „Správa databáze serveru WINS“ dále v této kapitole.

Tabulka 7.5 obsahuje databázové soubory, uložené v adresáři %SystemRoot%\System32\Wins.

Tabulka 7.5: databázové soubory serveru WINS

Soubor	Popis
J50.log a J50xxxxx.log	Protokol o všech transakcích provedených v databázi. Tento soubor je používán službou WINS k případnému obnovení dat.
J50.chk	Kontrolní soubor, používaný při spuštění databáze WINS. Tento soubor slouží ke zjištění, zda poslední ukončení systému proběhlo standardním způsobem a zda jsou všechny databáze v nepoškozeném stavu. Pokud tomu tak není, lze pomocí souboru protokolu zjistit, k čemu došlo a případně obnovit chybějící záznamy.

Soubor	Popis
Wins.mdb	Databázový soubor serveru WINS, jenž se skládá ze dvou tabulek – tabulky s adresami IP přidruženými k identifikátoru vlastníka, a tabulky s názvy přidruženými k adresám IP.
Winstmp.mdb	Dočasný soubor, vytvořený službou WINS. Databáze tento soubor používá jako odkládací při správě indexů. Po vzniku chyby lze tento soubor najít v adresáři %SystemRoot%\System32\Wins.

Upozornění: Za žádných okolností nesmí dojít k odstranění, ani jinému poškození souborů J50.log, J50xxxxx.log, Wins.mdb a Winstmp.mdb.

Konzola systémového řízení WINS poskytuje všechny nástroje, které můžete potřebovat při správě, prohlížení, zálohování či obnovování databáze serveru WINS. Konzolu systémového řízení WINS můžete používat například k zálohování všech databázových souborů serveru WINS.

Zálohování databáze serveru WINS

Konzola systémového řízení WINS poskytuje všechny nástroje nezbytné pro vytvoření záložní kopie databáze WINS. Po určení adresáře, v němž bude uložena záloha databáze, bude služba WINS pravidelně zálohovat celou databázi ve tříhodinových intervalech, což je výchozí nastavení systému. Podrobné instrukce, týkající se vlastního zálohování a obnovování databáze WINS vyhledejte v nápovědě online k systému Windows 2000 Server. Kromě toho byste měli pravidelně zálohovat také položky registru pro server WINS.

Oprava databáze WINS

Dojde-li k narušení databáze, můžete při obnovení její integrity využít některé z řady nabízených možností. Týká-li se poškození pouze určité skupiny záznamů, můžete poškozené záznamy opravit výběrovým zvyšováním nebo snižováním počátečního čísla verze, používaného serverem WINS, jenž vlastní dotyčné záznamy. Budete-li používat právě tuto metodu, můžete přizpůsobit počáteční číslo verze, používané serverem, tak, abyste si vynutili replikaci nepoškozených záznamů WINS. Takto synchronizace odstraní poškozené záznamy také z ostatních serverů WINS.

V případě, že poškození databáze nelze napravit výše uvedeným postupem, můžete vymazat celou databázi WINS a zcela ji obnovit ze zálohy (za předpokladu, že taková existuje). K tomuto účelu můžete využít jednu z vlastností zálohování pomocí konzoly systémového řízení WINS, která umožňuje vytvořit kopii databáze WINS.

Občas můžete poškození databáze WINS odstranit pouhým zvýšením nejvyššího čísla verze lokální databáze serveru WINS. Dosáhnete toho zvýšením hodnoty v dialogovém okně **Počáteční číslo verze**, jež můžete vyvolat z nabídky Předvolby serveru WINS. Po následném opakovaném spuštění služby WINS aktualizuje určený server WINS svoje místní číslo verze pro všechny jím vlastněné záznamy.

Zvýšení hodnoty počátečního čísla verze vlastnického serveru WINS si vynutí v nejbližším replikačním cyklu synchronizaci všech záznamů, vlastněných určeným serverem WINS, se záznamy na ostatních partnerských serverech WINS.

Počáteční číslo verze však můžete nastavit pouze na hodnotu vyšší než je existující číslo verze lokálně udržovaných záznamů daného serveru. Pokud žádné lokálně udržované záznamy vybraného serveru neexistují, můžete počáteční číslo verze nastavit na hodnotu vyšší než je aktuální počáteční číslo verze. Po nastavení hodnoty není možné snížit hodnotu bez předchozího vymazání místní databáze WINS a přeinstalování služby WINS na tomto serveru.

Hodnoty zadané a dále používané vlastností **Počáteční číslo verze** jsou analyzovány jako hexadecimální čísla. Služba WINS je schopna upravit vámi zadanou hodnotu na vyšší, aby tímto krokem zajistila urychlenou replikaci záznamů databáze také na ostatní servery WINS. Nejvyšší přípustnou hodnotou, kterou je schopen akceptovat program Konzola systémové správy WINS, je platné číslo, rovnající se hexadecimální hodnotě **FFFFFFFF**.

Obnovení dat pomocí replikace

Pokud sjednocení záznamů služby WINS trvá krátce (tzn. změny jsou mezi servery WINS replikovány rychle), doporučuje se po narušení integrity obnovovat databázi lokálního serveru WINS pomocí metody synchronizace dat s partnerským serverem pro replikaci. Tato metoda je neefektivnější v případě, kdy jsou data služby WINS na partnerském serveru aktuální.

Nejsnadnější cestou k obnovení databáze na lokálním serveru je replikovat data zpět z partnerského serveru pro replikaci. Tuto vlastnost řídí dva údaje v systémové registraci databázi: **InitTimeReplication** a **InitTimePause**. Údaj **InitTimeReplication** je umístěn v následujícím podklíči:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services  
Wins\Partners\Pull and Push
```

Jeho hodnota se standardně rovna 1 a vyvolá replikaci databáze WINS ihned po spuštění systému. Údaj **InitTimePause** je umístěn v podklíči WINS Parameters, jenž sděluje, že služba WINS bude po dobu replikace dočasně pozastavena. Popis těchto dvou údajů je obsahem následujícího oddílu.

Název: InitTimeReplication

Datový typ: REG_WORD

Popis: Je-li hodnota **InitTimeReplication** nastavena na výchozí hodnotu 1, vyžádá si server WINS replikaci nových databázových údajů od svých partnerů ihned po inicializaci systému nebo po změně parametrů replikace. Pokud se jeho hodnota rovná 0, dojde k replikaci pouze v intervalech určených hodnotou vlastnosti Interval replikace, jejíž hodnotu lze upravit v dialogovém okně Vlastnosti partnerského serveru pro replikaci (viz obrázek 7.10).

Název: InitTimePause

Datový typ: REG_WORD

Popis: Zde nastavená hodnota určuje, zda bude služba WINS spuštěna jako pozastavená. V tomto stavu setrvá až do doby, kdy bude dokončena její první replikace. Rovná-li se hodnota tohoto klíče 1, bude služba WINS spuštěna v režimu pozastavení. Bude-li však hodnotou 0 (výchozí nastavení), bude služba WINS spuštěna normálně. V režimu pozastavení nemůže služba WINS přijímat žádosti o registraci či uvolnění názvů, ba

ani dotazy. Služba WINS v tomto režimu zůstane až do té doby, kdy bude dokončena replikace s partnerskými servery nebo do té doby, kdy selže pokus o první replikaci. Je-li hodnota klíče **InitTimePause** nastavena na 1, měl by klíč **InitTimeReplication** (v podklíči partnerských serverů pro vyžádanou replikaci) obsahovat buď hodnotu 1 nebo by měl být z registru zcela odstraněn.

Komprimování databáze WINS

V systému Windows 2000 Server komprimuje služba WINS svou databázi pomocí databázového stroje Jet v režimu online. Tento způsob komprimace snižuje potřebu používání nástroje Jetpack.exe, používaného pro komprimaci offline. Proto tedy tato procedura nemusí být až tak důležitá, jako tomu bylo v minulých verzích serverů WINS a DHCP, pracujících v systému Windows NT Server.

Systém Windows 2000 Server také obsahuje nástroj Jetpack.exe, takže i v tomto systému lze komprimovat jak databázi WINS, tak i jiné databáze Jet (jako například DHCP) v režimu offline. Microsoft doporučuje používání nástroje Jetpack.exe k pravidelné komprimaci databází Jet, jakmile velikost databáze překročí hodnotu 30 megabajtů.

Jetpack.exe je nástroj příkazového řádku pro komprimaci databází v režimu offline. Následující příkaz ukazuje jeho správnou syntaxi:

```
jetpack <název databáze> <název dočasné databáze>
```

Dejme tomu, že máte dočasnou databázi, uloženou v souboru Tmp.mdb. Databáze WINS je uložena v souboru Wins.mdb. V takovém případě můžete databázi komprimovat pomocí následujících příkazů:

```
cd %SystemRoot%\System32\Wins
```

```
net stop wins
```

```
jetpack wins.mdb tmp.mdb
```

```
net start wins
```

Jetpack zkomprimuje databázi WINS následujícím způsobem: Nejprve zkopíruje informace o databázi do dočasného databázového souboru Tmp.mdb, potom odstraní původní databázový soubor Wins.mdb. Nakonec přejmenuje dočasný databázový soubor na původní název databáze, tedy na Wins.mdb.

Čištění databáze

Stejně, jako je tomu i v ostatních databázích, zaplní se i databáze WINS po nějaké době celou řadou neplatných nebo zaniklých záznamů. Z tohoto důvodu je nezbytné databázi pravidelně uklízet a zálohovat. Čištěním databáze zajistíte obojí. Čištění obvykle probíhá ve stejných intervalech jako zálohování.

Čištění databáze aktualizuje stav názvu všech údajů a uklidí z databáze lokálního serveru WINS všechny uvolněné záznamy. Kromě toho z databáze odstraní také všechny repliky vzdálených serverů WINS, jež nebyly z databáze lokálního serveru odstraněny v okamžiku jejich odstranění ze vzdálených databází. Proces čištění se opakuje automaticky po uplynutí času nastaveného relací mezi intervaly obnovení a zániku. Obě tyto hodnoty můžete nastavit v dialogovém okně Konfigurace. Toto dialogové okno lze zobrazit jednak ze záložky Záznam o názvu na kartě Vlastnosti serveru, ale také z karty konfigurace (viz obrázek 7.8).

Tabulka 7.6 obsahuje popis účinků procesu čištění na údaje v databázi WINS.

Tabulka 7.6: Stav údajů v databázi WINS před a po vyčištění databáze

Stav před vyčištěním	Stav po vyčištění
Vlastněný záznam o názvu, jemuž ještě nevypršela doba platnosti.	Nezměněn.
Vlastněný záznam o názvu, jemuž už vypršela doba platnosti.	Označen jako uvolněný.
Vlastněný uvolněný záznam o názvu, pro nějž ještě neuplynul interval zániku	Nezměněn.
Vlastněný uvolněný záznam o názvu, pro nějž uplynul interval zániku	Označen jako zaniklý.
Vlastněný zaniklý záznam o názvu, pro nějž ještě neuplynul časový limit zániku	Nezměněn.
Vlastněný zaniklý záznam o názvu, pro nějž uplynul časový limit zániku	Vymazán.
Replika vlastněného uvolněného záznamu o názvu, pro nějž uplynul časový limit zániku	Vymazán.
Replika aktivního názvu, pro nějž dosud neuplynul interval ověření.	Nezměněn.
Replika aktivního názvu s vypršeným intervalem ověření.	Opětovně ověřen.
Replika zaniklého nebo vymazaného názvu.	Vymazán.

Čištěním se udržuje správný stav informací uložených v databázi, a to díky ověřování každého serverem vlastněného záznamu, přičemž se nejprve porovnává časové razítko a aktuální čas a potom se změní stav všech záznamů, jejichž interval uplynul (například změna stavu z aktivního na uvolněný).

Čištění se opakuje podle nastaveného plánu. Časovač čištění se spustí ihned po spuštění serveru a je nastaven na polovinu intervalu obnovení. Z tohoto důvodu by neměl být server WINS zastaven nebo restartován před uplynutím poloviny intervalu obnovení, neboť by nemohlo dojít k vyčištění databáze. První čištění je totiž spuštěno po uplynutí poloviny nastaveného intervalu obnovení. Během prvního čištění jsou vykonány všechny akce s výjimkou jedné. Tou je odstranění zaniklých záznamů. Zaniklé záznamy jsou odstraňovány až po uplynutí nejméně tří dnů od spuštění serveru, aby služba měla dostatek času na jejich replikaci. Čištění se opakuje buď po uplynutí poloviny intervalu obnovení, nebo je lze spustit ručně.

Čištění probíhá podle algoritmu, zobrazeného ve výpisu 7.7.

```

Zjistit informace o všech vlastněných záznamech
Pokud Aktuální čas > časové razítko
    Změnit stav
        Aktivní -> Uvolněný
        Uvolněný -> Zaniklý
        Zaniklý -> Vymazat z databáze
Zjistit informace o zaniklých replikách
Pokud Aktuální čas > Časové razítko
    Vymazat záznam z databáze
Zjistit informace o aktivních replikách
Pokud Aktuální čas > Časové razítko
    Ověřit u vlastníka, zda záznam stále existuje
    Pokud Existuje
        Časové razítko = Aktuální čas + Interval ověření
    Jinak
        Vymazat záznam z databáze

```

Výpis 7.7: Algoritmus čištění databáze WINS.

Výsledek této operace je podrobně popsán v tabulce 7.6.

Kontrola konzistence

Kontrola konzistence databáze pomáhá při udržování integrity mezi jednotlivými servery WINS v rámci rozlehlé sítě. Po spuštění kontroly konzistence pomocí konzoly systémového řízení WINS si služba WINS bezprostředně vyžádá všechny záznamy od všech vlastnických serverů, včetně těch, kteří mají záznamy v lokální databázi, i když nepatří mezi partnerské servery pro replikaci.

Všechny záznamy vyžádané na vzdálených databázích jsou pak porovnány se záznamy v lokální databázi, přičemž se jejich konzistence porovnává v následujících krocích:

- Je-li záznam v lokální databázi stejný jako záznam vyžádaný na vlastnické databázi, je aktualizováno jeho časové razítko.
- V případě, že záznam v lokální databázi obsahuje nižší identifikátor verze, je záznam vyžádaný na vlastnické databázi přidán do lokální databáze jako nový, zatímco původní záznam je označen pro smazání.
- Mají-li záznamy stejný identifikátor verze, ale odlišné názvy, bude lokální záznam označen pro smazání a na jeho místo bude umístěn vyžádaný záznam.

Musíte si však uvědomit, že kontrola konzistence ve velmi rozsáhlých databázích WINS může velmi zatížit chod celé sítě. V systému Windows 2000 lze kontrolu konzistence provádět pomocí konzoly systémového řízení WINS. Stačí, když zaškrtnete políčko před položkou **Povolit periodickou kontrolu konzistence databáze** na kartě **Záznam o názvu** v dialogovém okně vlastností serveru.

Databázové soubory služby WINS

Formát databáze služby WINS zrychluje a zefektivňuje uchovávání dat, neboť nezapišuje aktuální transakci přímo do databáze, ale do souborů protokolu. Proto vyžaduje pohled na aktuální stav databáze také ověření záznamů o transakcích, uložených v souborech protokolu. Tyto soubory slouží také jako velmi účinný nástroj při zotavení po chybě (například po výpadku elektrického proudu). Díky souborům protokolu lze pohodově stav databáze WINS opravit.

Velikost souborů protokolu se pohybuje vždy okolo 1 megabajtu. Přesto se však při velkém zatížení serveru WINS může jejich velikost podstatně zvětšit. Když server WINS dosáhne maximální velikosti svého souboru protokolu, automaticky vytvoří další takový soubor.

Efektivní velikost databáze každého připojeného serveru WINS je zhruba stejná. Každá databáze obsahuje stejný počet záznamů (když nepočítáme záznamy čekající ve vyrovnávací paměti), přičemž je velikost databáze úměrná počtu uložených záznamů. Jediné údaje zpravidla obsazují 42 bajtů (nevyžadují ID oboru). Údaje o skupině Internet mohou zaujímat až 25 adres a tím pádem také odpovídající počet bajtů. Skutečná velikost může být ještě o něco větší z důvodu nevyužitého prostoru, jenž lze komprimací databáze získat zpět.

Tabulka pro údaje mapování názvů na adresy IP uchovává názvy rozhraní NetBIOS a k nim přiřazené adresy IP. Údaje v této tabulce jsou vytvářeny při přijetí požadavku na registraci názvu NetBIOS, odeslaného uzlem TCP/IP nebo na základě replik přijatých z ostatních serverů WINS. Seskupený (clustered) index, připojený k poli názvu, umožňuje rychlé vyhledání záznamů, požadovaných dotazy na název. Seskupený index je index, v němž je logické nebo indexové řazení klíčových hodnot stejné jako fyzické řazení odpovídajících řádků

v tabulce. Primární index je vytvořen na základě zřetězení hodnoty v polích ID vlastníka a ID verze. Tento způsob vytváření indexů umožňuje rychlý přístup k záznamům, spadajícím do rozsahu ID verze daného vlastníka.

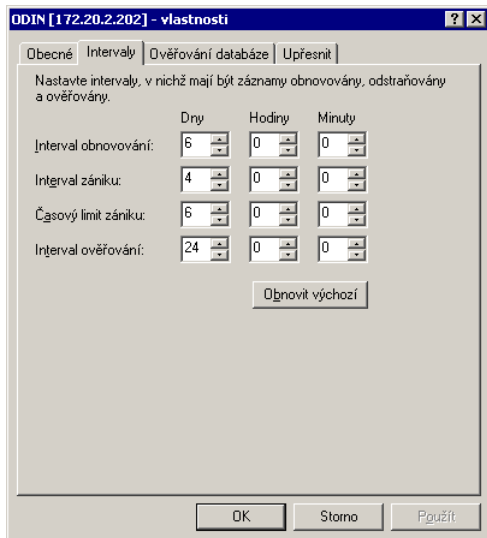
Tabulka pro údaje mapování adres IP na ID vlastníka obsahuje po jednom řádku pro každý server WINS, jenž obsahuje jakékoli údaje v tabulce mapování názvů na adresy IP. Tyto řádky obsahují adresu IP příslušných serverů WINS spolu s jejich identifikátorem, jež jsou spolu ukládány jako ID vlastníka všech údajů, vlastněných daným serverem.

Časovače

Záznamy v databázi WINS jsou spravovány čtyřmi konfigurovatelnými hodnotami časovače:

- Interval obnovy,
- interval zániku,
- časový limit zániku,
- interval ověření.

Společnost Microsoft se rozhodla pro takové výchozí nastavení těchto čtyř hodnot, které zpravidla není třeba měnit. Tyto hodnoty udržují přijatelný stupeň přenosů a umožňují minimální zatížení serverů WINS. Jsou tím ideálním kompromisem mezi zajištěním všech služeb a minimalizací doby, po kterou může být databáze neaktuální. Tohoto kompromisu bylo dosaženo testováním mnoha konfigurací, v nichž mohou být servery WINS zaváděny. Do úvah promluvily navíc i takové aspekty provozu, jako jsou dlouhé víkendy, vyhýbání se zbytečným přenosům během replikací, schopnost rychle zpracovat značný počet klientů i při těch nejhorších okolnostech, stejně tak jako kompromisy mezi rychlým úklidem databáze a uchováním údajů pro zajištění jejich replikace. To všechno byly okolnosti, jež určovaly nastavení výchozích hodnot těchto intervalů.



Obrázek 7.8: Dialogové okno Konfigurace záznamu o názvu.

Čtyřmi hodnotami, uvedenými v tabulce 7.7 se budeme zabývat podrobně ještě v následujícím oddílu. Jejich hodnoty můžete změnit v dialogovém okně, znázorněném na obrázku 7.8.

Tabulka 7.7: Časovače serveru WINS

Položka konfigurace	Popis
Interval obnovení	Určuje to, jak často bude muset klient obnovovat registraci svého názvu. Výchozí hodnotou je šest dnů.
Interval zániku	Určuje interval mezi označením záznamu za uvolněný a označením záznamu za zaniklý. Výchozí hodnota této položky závisí na velikosti intervalu obnovení a, to pokud server WINS má své partnerské servery pro replikaci, na maximální velikost časového intervalu replikace. Maximální povolenou hodnotou je šest dnů.
Časový limit zániku	Určuje časový interval mezi označením položky za zaniklý a jejím skutečným vymazáním z databáze. Výchozí nastavení závisí na velikosti časového intervalu obnovení a, to pokud server WINS má své partnerské servery pro replikaci, na maximální velikost časového intervalu replikace. Výchozí hodnotou je šest dnů.
Interval ověření	Určuje časový interval, po jehož uplynutí musí server WINS ověřit, zda jsou jím nevlastněné starší záznamy pořád aktuální. Výchozí nastavení závisí na časovém limitu zániku. Maximální povolenou hodnotou je v tomto případě 24 dnů.

Interval obnovení

Intervalu obnovení se říká také časový limit obnovení názvu nebo také hodnota jeho životnosti. Databázový údaj je po zaregistrování na serveru WINS označen časovým razítkem, sestávajícím se ze součtu aktuálního času a intervalu obnovení. Pokud se klientovi nepodaří v tomto nastaveném časovém intervalu svoji registraci obnovit, bude mu jeho registrace odebrána. Je-li název uvolněn po uplynutí stanovené doby nebo na základě výslovného požadavku klienta, změní server pouze stav z aktivního na uvolněný a označí záznam novým časovým razítkem, které bude v tomto případě součtem aktuálního času a intervalu zániku. Tato změna není replikována na ostatní servery WINS. Je-li záznam o názvu označen jako RELEASED neboli uvolněný a server přijme požadavek na jeho registraci s jinou adresou IP, může být název okamžitě přidělen novému klientu, aniž by bylo nutné odesílat jakoukoli ověřovací výzvu, neboť se ví, že původní klient už tento název nepoužívá. Výchozí hodnota časového intervalu obnovení je šest dnů.

Interval zániku

Intervalu zániku se říká také časový limit stárí názvu nebo interval pro označování záznamů za neplatné. Tento interval určuje dobu, po jejímž uplynutí bude stav příslušných záznamů změněn z uvolněný na neplatný. V tomto okamžiku je záznam označen časovým razítkem, které je nyní součtem aktuálního času a časového limitu zániku. Současně je aktualizována také hodnota ID verze, což zajistí, že tato informace bude při následující replikaci přenesena také na všechny ostatní servery WINS.

Záznamům označeným za neplatné je po vytvoření připojeno časové razítko, sestávající se ze součtu aktuálního času a časového limitu zániku, nastaveného na partnerském serveru pro vyžádanou replikaci. Výchozí interval zániku je založen na hodnotách intervalů obnovení a replikace. V systému Windows 2000 je jeho hodnota zpravidla šest dnů.

Časový limit zániku

Časovému limitu zániku se také občas říká časový limit označení záznamu za neplatný. Záznamy označené za neplatné, které jsou starší než je časový limit zániku, jsou z databáze vymazány. Jak již bylo uvedeno dříve, v systému Windows 2000 je povoleno také jejich ruční vymazání, a to díky konzole systémového řízení WINS. Výchozí nastavení tohoto intervalu je šest dnů.

Interval ověření

Replikace by měla zajistit synchronizaci všech databází. Přesto se však v některých případech stává, že mohou některé nepoužívané názvy v databázi přetrvávat a vytvářet tak v ní nevyužitý prostor. Pokud je například záznam označený za neplatný z databáze odstraněn ještě před provedením replikace, stav záznamů v ostatních databázích zůstane nadále aktivní. K tomu může dojít například tehdy, nelze-li během časového limitu zániku dosáhnout spojení s partnerským serverem.

Po provedení synchronizace je aktivní záznam na žádajícím serveru WINS označen časovým razítkem, skládajícím se ze součtu aktuálního času a intervalu ověření. Pokud server WINS najde v době úklidu záznamy starší než interval obnovení, odešle dotaz na server WINS, který vlastní jejich názvy, a pokusí se ověřit, zda jsou identifikátory verzí pořád platné. Je-li odpověď vlastnického serveru záporná (neplatný záznam), bude záznam odstraněn. Jestliže však příslušný server WINS odešle kladnou odpověď (platný záznam), bude záznam opatřen novým časovým razítkem. V případě, že s příslušným serverem WINS nelze navázat spojení, budou záznamy ponechány v původním stavu až do uplynutí následujícího intervalu ověření nebo dokud správce nespustí funkci uklidit databázi. Záznamy nelze odstranit, dokud se nelze s příslušným serverem spojit. Výchozí hodnota intervalu ověření je 24 dnů.

Hodiny serveru

Algoritmy replikace a čištění se opírají o přiměřeně konzistentní systémové hodiny. Samozřejmě, že tyto algoritmy lze ovlivnit posunutím hodin dopředu nebo dozadu. Přesto však servery WINS nemusí být synchronizovány v určitém čase, neboť časové značky jsou vkládány na základě místního času serveru. Pokud je tedy čas na příslušných serverech, konzistentní budou nastavené intervaly fungovat zcela spolehlivě.

Mazání záznamů z databáze WINS

Konzola systémové správy WINS poskytuje zdokonalený systém správy databází, neboť využívá následující operace mazání:

- Jednoduché mazání záznamů v databázi WINS bez podpory replikace,
- odstranění záznamů označených za neplatné, jež byly replikovány do databází na ostatních serverech WINS,
- schopnost výběru většího počtu skupin zobrazených databázových záznamů s následným jednoduchým vymazáním nebo vymazáním neplatných záznamů.

Konzola systémové správy WINS poskytuje kromě toho ještě jednodušší a pohodlnější nástroj pro administrativní odstraňování dynamicky registrovaných záznamů. V předchozích verzích služby WINS umožňovaly nástroje konzoly systémové správy WINS odstranění pouze staticky registrovaných mapování.

Záznamy WINS lze z databáze odstranit dvěma způsoby: buď běžným vymazáním, nebo vymazáním záznamů označených za neplatné. Ve zbývajících částech tohoto oddílu se budeme zabývat možnostmi jejich využití při správě databáze WINS.

Budete-li používat běžné vymazání záznamu, budou všechny záznamy, vybrané pomocí konzoly WINS, odstraněny z aktuální lokální databáze WINS.

V případě, že takto odstraněné záznamy byly předtím replikovány na jiné servery WINS, budou odstraněny i tyto dodatečné záznamy. Pokud pomocí konzoly systémové správy WINS neurčíte, že mají být najednou odstraněny také záznamy v databázích umístěných na ostatních serverech WINS, zůstanou záznamy na těchto serverech nedotčeny. Navíc se může klidně stát, že se takto odstraněné záznamy v databázi opět objeví po dokončení hned následující synchronizace databází s některým z partnerských serverů pro replikaci.

Budete-li však používat techniku mazání záznamů označených za neplatné, jejímž vlastníkem je navíc vámi vybraný server, budou vybrané záznamy odstraněny ze všech serverů, které se na replikaci podílejí.

Příslušný server WINS (vlastník) změní ve své databázi status vybraných záznamů z aktivního na neplatný. Služba WINS pak bude tyto záznamy považovat za neaktivní a přestane je používat. Jakmile jsou tyto záznamy označeny v místní databázi za neplatné, nebude příslušný server ani odpovídat na požadavky s dotazy na tyto názvy, jež budou přicházet jak od klientů služby WINS, tak od ostatních serverů WINS. Tento stav potrvá do té doby, dokud je některý z klientů WINS nezaregistruje znovu. Server WINS, jenž tyto záznamy vlastní, je bude během následujících replikačních cyklů předávat ostatním serverům jako neplatné.

Přesto tyto záznamy nejsou z databáze odstraněny ani násilně, ani okamžitě. Jsou pouze označeny pro pozdější vymazání. Interval replikačního cyklu je konfigurován na základě vlastnosti Záznam o názvu v nastavení serveru v konzole systémové správy WINS. Záznamy zůstanou v databázi až do vypršení intervalu zániku. Tento postup umožňuje ostatním serverům WINS zjistit, že tyto záznamy již nejsou používány, a na základě této informace aktualizovat repliky ve svých vlastních databázích a dále pak tuto informaci předávat dalším partnerským serverům. Tímto způsobem budou vybrané záznamy označené za neplatné na všech serverech WINS, které se na replikaci podílejí.

Jakmile je cyklus replikace dokončen na všech serverech WINS a když vyprší interval zániku neplatných záznamů, budou tyto záznamy z databází na všech serverech WINS při následujícím cyklu čištění odstraněny. Po dokončení úklidu všech databází se záznamy přestanou zobrazovat v konzole systémové správy WINS a ani nebudou fyzicky v databázích přítomny.

I po ručním označení záznamů za neplatné (nebo po jejich označení službou WINS za uvolněné) zůstanou tyto uvolněné záznamy v databázi až do spuštění následných čistících operací. Přesná doba jejich pobytu v databázi závisí na tom, za jak dlouho bude spuštěn proces úklidu. Zpravidla se tato doba rovná součtu intervalu zániku, časového limitu zániku a intervalu ověření.

Příklad registrace záznamu a jeho označení za neplatný

Pokusme se vše přiblížit na praktickém příkladu. Dejme tomu, že klient WINS registruje svůj název TESTPC1 na serveru WINS, nazvaném WINS1. Tento server má interval obnovení nastaven na tři dny. Po zaregistrování názvu jej bude server WINS1 replikovat na všechny partnerské servery, například na server WINS2 atd. Po uplynutí intervalu ověření server WINS2 ověří platnost záznamu v databázi WINS1. WINS1 s uloženým záznamem už neprovádí žádné změny. Pouze čeká, až si klient obnoví svůj název nebo jej znova zaregistruje.

V případě, že klient registraci svého názvu během nastaveného intervalu obnovení neobnoví, nastaví server WINS1 příznak názvu TESTPC1 jako „uvolněný“. Pokud klient neobnoví název během následného intervalu zániku, bude záznam označen za neplatný. V této chvíli je opět replikován na server WINS2 (neboť se zvýšila hodnota ID verze záznamu TESTPC1).

Po provedení synchronizace záznamu zkopíruje WINS2 zneplatněný údaj ze serveru WINS1 a označí jej časovým razítkem s aktuálním časem plus interval ověření. Server WINS2 počká s odesláním dotazu na server WINS1 až do vypršení intervalu ověření. Na druhé straně celou tu dobu plus interval zániku čeká také server WINS1, a to pouze na to, zda si klient neobnoví nebo opět nezaregistruje svůj název. Pokud tak klient do té doby neučiní, server WINS1 tento záznam z databáze odstraní. Potom, po vypršení intervalu ověření, odešle server WINS2 dotaz na server WINS1. Nebude-li záznam uložen na serveru WINS1, odstraní jej server WINS2 ze své databáze také.

Stane-li se však, že server WINS2 odešle dotaz na server WINS1, ale ten nebude odpovídat (například z důvodu poruchy, provádění údržby nebo pomalého spojení), ponechá si jej server WINS2 ve své databázi. V takovém případě bude interval ověření znova nastaven a po jeho uplynutí se server WINS2 pokusí opět spojit se serverem WINS1.

Ruční označování záznamů za neplatné

V předchozích verzích služby WINS nebyly záznamy odstraňovány na všech serverech simultánně. Mezi jednotlivými replikačními cykly existovaly časové díry, jež mohly způsobovat nekonzistentnost záznamů. Znamená to, že odstraněné záznamy se mohly klidně zobrazit i tam, odkud byly před časem odstraněny.

Možnost ručního označování záznamů za neplatné, implementovaná v systému Windows 2000, tomuto problému předchází. Doba trvání neplatného záznamu je větší než zpoždění při předávání, způsobené nutností synchronizace záznamů v celé síti. Po dosažení nebo překročení nastavené hodnoty budou neplatné záznamy odstraněny během běžného úklidu databáze.

Ruční označení záznamů za neplatné poskytuje také prvotřídní nástroj pro práci se statickými záznamy.

Po synchronizaci záznamů označených za neplatné je jejich statut zneplatnění aktualizován a použit také ostatními servery, které uchovávají jejich repliky ve svých databázích. Všechny partnerské servery pro replikaci tyto záznamy zaktualizují a individuálně je označí za neplatné. Jakmile jsou tyto repliky zaktualizovány na všech serverech WINS, mohou být odstraněny po uplynutí intervalu ověření, nastaveného na každém serveru WINS individuálně.

Ruční označování záznamů za neplatné je dostupné jak z grafického uživatelského rozhraní, tak z příkazového řádku. Chcete-li tuto funkci používat, otevřete dialogové okno WINS, označte v něm server (vlastníka) a zobrazte jeho všechny záznamy. Označte

záznamy, které chcete z databáze odstranit a potom je vymažete zadáním příslušného příkazu z nabídky Akce. V tomto okamžiku můžete záznam vymazat nebo označit za neplatný. I když možnost ručního označení záznamu za neplatný vyžaduje instalaci serverů Windows 2000 WINS, lze takto označené záznamy úspěšně replikovat na servery se systémy Windows NT 3.51 a Windows NT verze 4.0.

Doporučené postupy při práci s databázemi služby WINS

Díky dynamické komprimaci a konzole systémového řízení WINS lze databáze WINS v systému Windows 2000 udržovat podstatně snadněji. Přesto však je i zde třeba dodržovat určité zavedené administrativní postupy či pravidelnou údržbu.

Provádění pravidelných kontrol konzistence V systému Windows 2000 lze kontrolu konzistence provádět prostřednictvím konzoly systémového řízení WINS. Tuto funkci použijete k pravidelným kontrolám konzistence databáze WINS.

Kontrola konzistence velmi zatěžuje jak síťové zdroje, tak i systémové prostředky samotného počítače, neboť server WINS se musí replikovat pro každého vlastníka, jehož záznamy jsou ověřovány na konzistenci. Z tohoto důvodu se doporučuje provádět kontrolu konzistence záznamů databáze WINS během nízkého provozu sítě (například v noci nebo o víkendech).

Pravidelné komprimování v režimu offline Dynamické komprimování databáze probíhá na serverech WINS jako automatický proces spouštěný na pozadí v době nečinnosti databáze nebo po její aktualizaci. Tento proces probíhá během používání databáze. K dokončení dynamické komprese databáze tedy nemusíte službu serveru WINS zastavovat. Přestože možnost dynamického komprimování potřebu komprimace offline podstatně snižuje, přece ji docela nenahrazuje. Komprimace offline pomocí nástroje JETPACK obnoví podstatně více nepoužívaného prostoru než dynamická komprese a měla by být v sítích s 1 000 nebo více klienty spouštěna alespoň jednou měsíčně. V případě menších sítí stačí, když ruční komprimaci provedete jednou za několik měsíců.

I když není ruční komprimace databáze serveru WINS v systému Windows 2000 Server až tak důležitá, jako tomu bylo v předchozích verzích systému, je pořád velmi užitečná. Komprimaci offline byste měli spouštět týdně nebo měsíčně kvůli defragmentaci a zvýšení výkonu disku. Sledujte všechny změny velikosti databázového souboru Wins.mdb, uloženého ve složce `%SystemRoot%\System32\Wins`.

Budete-li ověřovat velikost souboru Wins.mdb před komprimací offline i po ní, zjistíte jednak jeho velikost, ale také jeho zmenšení. Tato informace vám zcela jistě pomůže při zjišťování výhod komprimace offline. Na základě těchto informací můžete také stanovit četnost provádění komprimací offline, aby byly jejich výsledky skutečně změnitelné.

Pravidelné zálohování za účelem snadného obnovení Kromě toho, že můžete data počítače s instalací serveru WINS zálohovat na páskovou jednotku, umožňuje konzola systémového řízení WINS také obnovení poškozené nebo ztracené databáze WINS. Další informace o obnovování dat z databáze WINS po jejich poškození nebo ztrátě najdete v podkapitole „Odstraňování problémů spojených se službou WINS“ dále v této kapitole.

Databázi můžete také obnovit pomocí partnerského serveru pro replikace. V případě, že jsou aktuální data uložena také na partnerském serveru pro replikaci, můžete je použít po selhání serveru k obnovení vlastní databáze. Tuto funkci řídí dva údaje sy-

stémové registrační databáze, **InitTimeReplication** a **InitTimePause**. První z nich je umístěn v následujícím podklíči:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
\Wins\Partners\Pull and Push
```

Jeho hodnota se standardně rovná 1 a vyvolá replikaci databáze WINS ihned po spuštění systému. Údaj **InitTimePause** je umístěn v následujícím podklíči:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
\Wins\Parameters
```

Tento údaj systému sděluje, že služba WINS bude po dobu replikace dočasně pozastavena.

Používání funkce Uklidit Funkce **Uklidit** je automatickou funkcí služby Windows 2000 WINS. Uvolňuje zastaralé záznamy, odstraňuje záznamy zaniklé a ověřuje stav záznamů, jejichž stáří dosáhlo nebo překročilo limit nastavený intervalem ověření.

Budete-li používat výchozí konfiguraci služby WINS v systému Windows 2000, bude funkce **Uklidit** spouštěna každých 72 hodin neboli každou polovinu intervalu obnovy. V případě, že bude služba WINS zastavena a následně obnovena po uplynutí 72 hodin, bude také doba spuštění této funkce o 72 hodin posunuta. Budete-li zastavovat službu WINS denně, ke spuštění funkce **Uklidit** nedojde nikdy.

Chcete-li zjistit, zda ke spuštění této funkce vůbec dochází, otevřete dialogové okno vlastností serveru WINS. Potom se přesuňte na kartu **Upřesnit** a zaškrtněte políčko před položkou **Protokolovat podrobně události do protokolu událostí**. Tato vlastnost ještě více zatěžuje celý proces a měli byste ji používat pouze při ověřování procesu úklidu. Pokud ke spuštění této funkce vůbec nedochází, nastavte příslušnou zásadu úklidu jako součást údržby databáze WINS.

Předcházíte používání statických údajů WINS Aby bylo možné statické údaje WINS zdárně používat, vyžadují se ze strany správce určité akce. Přesto však mohou být tyto údaje v určitých situacích užitečné. Jako příklad nám může posloužit ochranná registrace názvů, používaných kritickými systémovými servery.

Můžete například přidat do databáze statický údaj, jenž zabrání ostatním počítačům v registraci názvu kritického serveru v době jeho nečinnosti. Rezervování názvů touto metodou účinně předchází možnosti zmocnění se názvu serveru (prostřednictvím protokolu DHCP) během registrace názvu jiným počítačem. Kdyby v daném okamžiku server neodpověděl na výzvu, mohl by server WINS předpokládat, že je název nepoužíván. Na základě tohoto předpokladu by postoupil název novému počítači.

Největší nevýhodou používání statických údajů WINS je to, že značně komplikují správu změn názvů a síťových adres. Změní-li se například název počítače nebo statický údaj, budete muset aktualizovat také další konfigurace jako například servery DHCP, servery DNS, koncové systémy, soubory LMHOSTS atd.

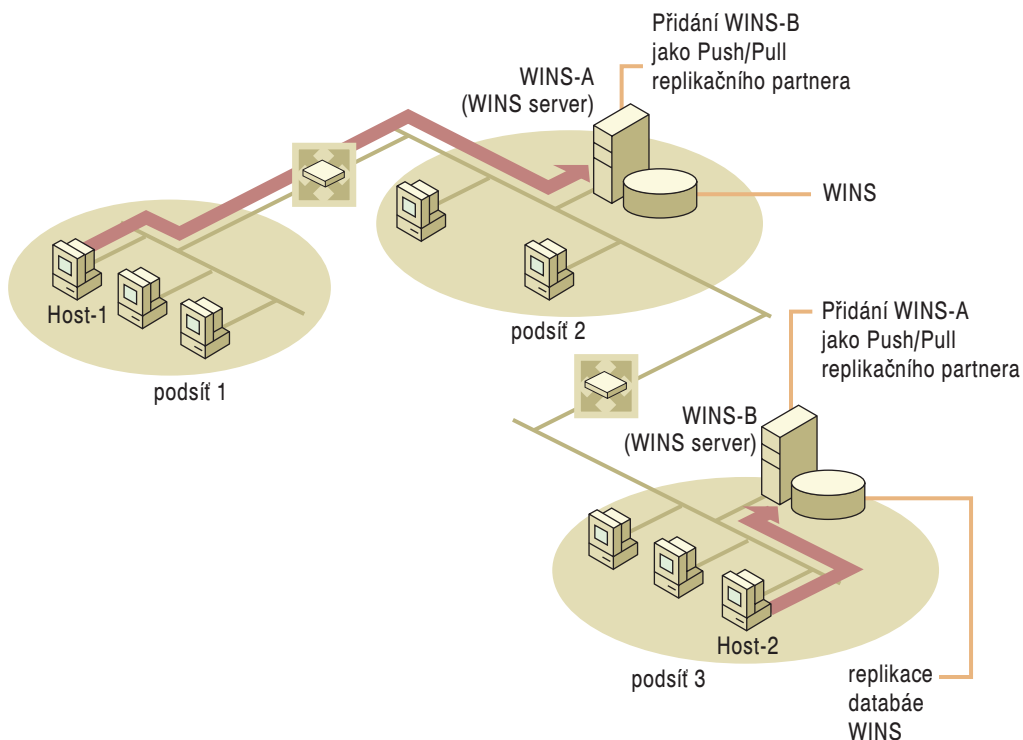
Budete-li využívat statické údaje WINS, využívejte také rezervace, aby byl dopad na DHCP co nejmenší. Každá adresa, použitá ve statickém mapování WINS, by měla mít odpovídající rezervaci klientské adresy, která by umožnila vyhradit tomuto názvu adresu IP i na serveru DHCP. V takových případech je také nezbytné pečlivě monitorovat a sledovat stav a chování serverů, do jejichž databází byly tyto údaje přidány (vlastníci). V ideálním případě by měly být všechny statické údaje zadávány na jednom serveru. To by značně usnadnilo jejich pozdější odstranění. Další informace o rezervacích adres najdete v kapitole „Protokol DHCP“.

Replikace WINS

Všechny servery WINS v rámci počítačové sítě lze nakonfigurovat tak, aby replikovaly záznamy ze svých databází na všechny ostatní servery WINS. Takový typ replikace zaručuje to, že název, zaregistrovaný na jednom serveru WINS, bude nakonec zaregistrován také na všech zbývajících serverech WINS. V této podkapitole se budeme podrobně věnovat právě procesu synchronizace záznamů.

Celkový pohled na proces replikace

Replikování databází mezi servery WINS udržuje konzistentní sadu informací WINS v rámci celé sítě. Příklad replikace databáze WINS si můžete prohlédnout na obrázku 7.9. Dva servery WINS, WINS-A a WINS-B, jsou konfigurovány tak, aby mezi sebou vzájemně replikovaly všechny své záznamy.

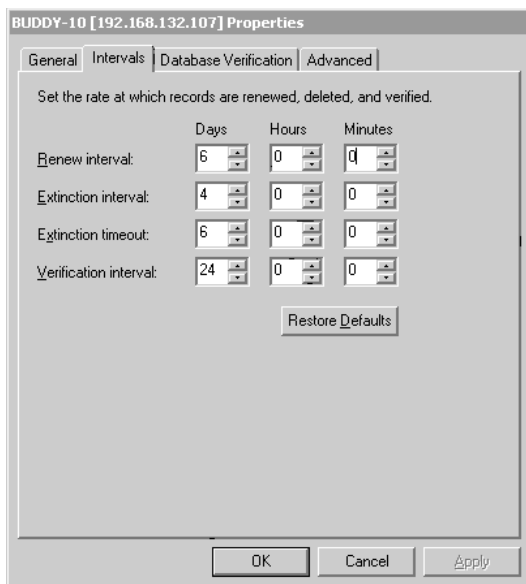


Obrázek 7.9: Celkový pohled na replikaci WINS.

Na obrázku 7.9 je znázorněn klient služby WINS, HOST-1 v podsíti 1, jenž registruje svůj název na svém primárním serveru WINS, jímž je server WINS-A. Jiný klient, HOST-2 v podsíti 3, registruje svůj název na svém primárním serveru WINS, tedy na serveru WINS-B. Jestliže se kterýkoli z těchto klientských počítačů pokusí vyhledat svůj protějšek pomocí služby WINS (když například HOST-1 odešle dotaz na adresu IP počítače HOST-2), bude tento požadavek splněn právě díky tomu, že si servery WINS mezi sebou replikovaly své záznamy.

Poznámka: Replikace WINS je vždy přírůstková, což znamená, že během následných replikací jsou v databázi synchronizovány pouze změny, nikoli celá databáze.

Replikace může fungovat pouze v případě, kdy je na každém serveru WINS konfigurován alespoň jeden další server WINS jako partnerský server pro replikaci. Toto nastavení zaručuje, že název zaregistrovaný na jednom serveru WINS bude nakonec replikován na všechny ostatní servery WINS v rámci počítačové sítě. Partnerský server pro replikaci může být nastaven buď jako partnerský server pro nabízenou replikaci, jako partnerský server pro vyžádanou replikaci či jako partnerský server pro nabízenou i vyžádanou replikaci. Posledně uvedená možnost umožňuje využití obou metod replikace. Po přidání partnerského serveru pro replikaci je nový server automaticky konfigurován jako partnerský server pro nabízenou i vyžádanou replikaci. Tento typ partnerského serveru je ve většině případů doporučeným nastavením.



Obrázek 7.10: Dialogové okno Vlastností partnerských serverů pro replikaci.

Během replikace serverů WINS dochází k fázi zpoždění. Tato fáze nastává mezi počátkem a koncem přenosu informace o mapování názvu klienta na adresu IP, a to z libovolného serveru na všechny ostatní servery WINS. Tomuto zpoždění se říká také doba konvergence systému WINS. Například požadavek na uvolnění názvu klienta se nepřenáší stejně rychle jako požadavek na jeho registraci. Děje se to proto, že názvy jsou sice běžně uvolňovány, ale následně opětovně používány se stejným mapováním, jako je tomu například při restartování počítače nebo když je počítač večer vypnut a ráno znovu zapnut. Replikování všech těch názvů by proto neúměrně zatížilo provoz celé sítě.

Navíc když dojde například k nesprávnému vypnutí klientského počítače (k čemuž může dojít třeba po výpadku napájení z elektrické sítě), není registrovaný název uvolněn standardně pomocí dotazu klienta na server. Z tohoto důvodu neznamena přítomnost záznamu v databázi WINS, že jej klient stále používá nebo že je k němu i nadále při-

družená související adresa IP. Jeho přítomnost znamená pouze to, že některý z počítačů tento název zaregistroval a je k němu přidružená nějaká adresa IP.

Poznámka: Primární a sekundární servery WINS přiřazené ke kterémukoli klientu musí mít mezi sebou relaci typu vyžádaná/nabízená replikace. Během přiřazování serverů ke klientům je vhodné mít u sebe seznam dvojic partnerských serverů pro vyžádanou/nabízenou replikaci.

Aby bylo možné replikovat záznamy v databázi, musí být každý server WINS v rámci příslušné počítačové sítě konfigurován buď jako partnerský server pro nabízenou replikaci, nebo jako partnerský server pro vyžádanou replikaci alespoň pro jeden další server WINS.

Partnerské servery pro nabízenou a vyžádanou replikaci

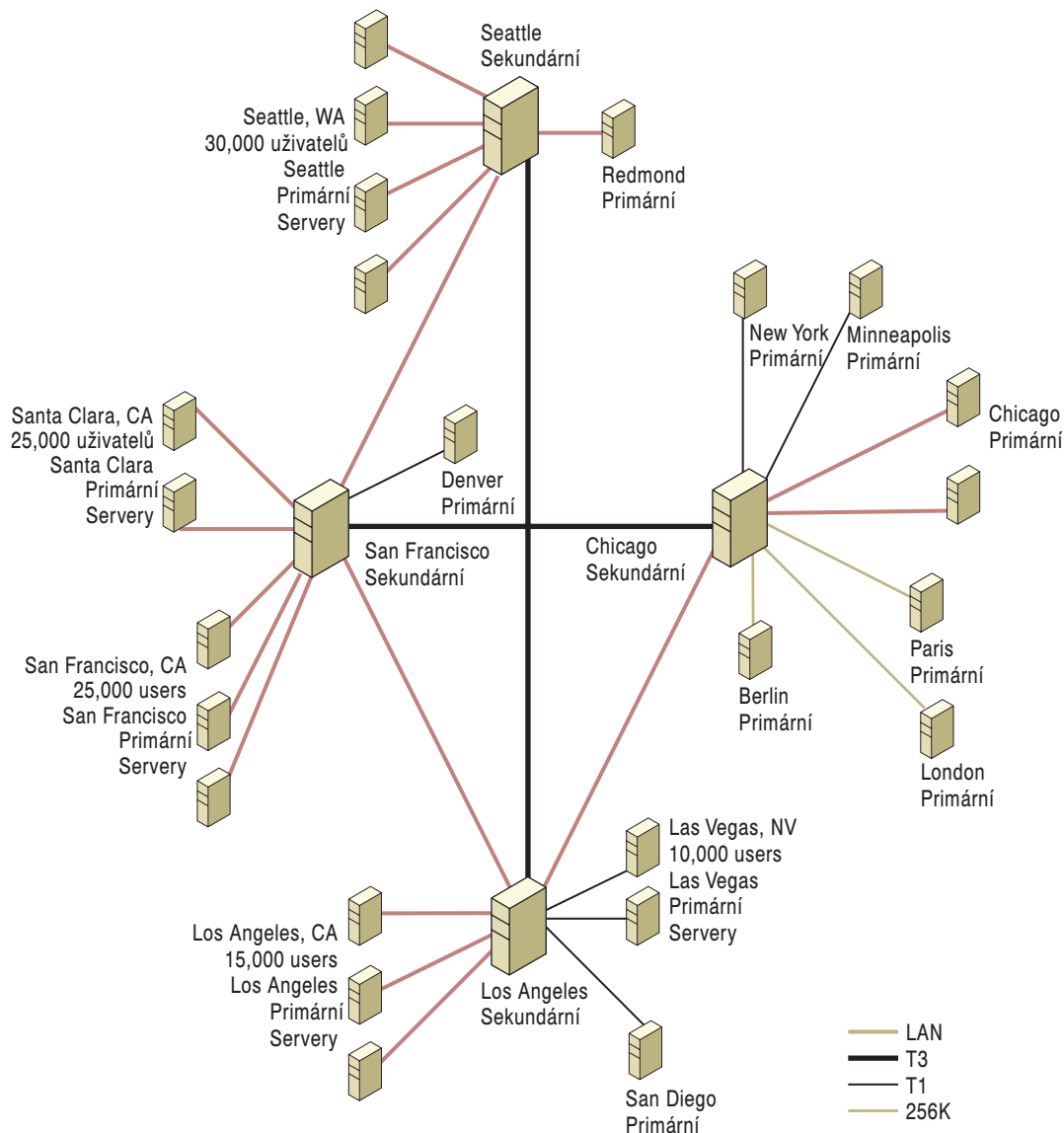
Databáze WINS je řízena společně všemi servery WINS, na nichž je uložena její kopie. Aby byly záznamy v těchto kopiích konzistentní, servery své záznamy mezi sebou synchronizují. Každý server WINS je konfigurován tak, aby obsahoval odkazy na jeden nebo více partnerských serverů pro replikaci. Když se k síti připojí nový nebo náhradní počítač, musí samozřejmě zaregistrovat také svůj název adresy IP na jiném serveru, jenž na oplátku odesílá nové záznamy na všechny servery příslušného podniku. Výsledek je uložení záznamu, týkajícího se nového počítače, na všech serverech počítačové sítě.

Podrobná analýza příkladu replikace

Na následujícím obrázku je znázorněna neobyčejně rozlehlá implementace služby WINS, která zde slouží pro uspokojení požadavků více než 100 000 uzlů. V konfiguraci s tolika uzly byste mohli podlehnout pokušení vytvořit hodně nadbytečných vztahů typu vyžádaná/nabízená replikace. To by samozřejmě způsobilo značné znepráhlednění systému s následnými potížemi při odstraňování vzniklých problémů.

Struktura rozbočovačů zanáší do příkladu konfigurace na obrázku 7.11 určitý pořádek. Čtyři hlavní rozbočovače jsou umístěny v Seattlu, San Franciscu, Chicagu a Los Angeles. Tyto rozbočovače slouží zároveň jako sekundární servery WINS pro příslušné zeměpisné oblasti. Všechny primární servery WINS jsou konfigurovány jako partnerské pro nabízenou a vyžádanou replikaci s rozbočovači. Rozbočovače jsou zároveň partnerskými servery pro nabízenou/vyžádanou replikaci jiných rozbočovačů.

Dejme tomu, že primární servery WINS z obrázku 7.11 budou své záznamy synchronizovat s rozbočovači každých 15 minut, zatímco replikační interval pro synchronizaci mezi jednotlivými rozbočovači je nastaven na 30 minut. Doba konvergence systému WINS je dobou, která uplyne od zaregistrování příslušného uzlu po jeho replikování na všechny servery WINS. V tomto případě by mohla nejdelší prodleva nastat mezi přenosem dat z primárního serveru v Seattlu na primární server v Chicagu. Dobu konvergence lze snadno vypočítat, když k ní přidáte maximální dobu synchronizace záznamu mezi primárním serverem v Seattlu a sekundárním serverem v Seattlu, dále pak dobu synchronizace mezi sekundárním serverem v Seattlu a sekundárním serverem v San Franciscu, dobu synchronizace záznamů mezi sekundárním serverem v San Franciscu a sekundárním serverem v Chicagu a nakonec také dobu synchronizace záznamů mezi sekundárním serverem v Chicagu a primárním serverem v tomtéž městě. To nám dohromady dá $15 + 30 + 30 + 15$, čili 1,5 hodiny.



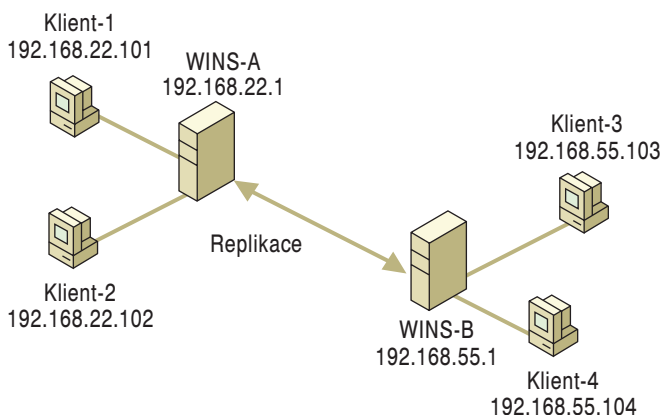
Obrázek 7.11: Rozlehlá implementace služby WINS pomocí topologie rozbočovače.

Přesto však může být tato doba o něco delší, neboť některé z těchto serverů mohou být propojeny prostřednictvím pomalých připojení. Pravděpodobně není zapotřebí, aby servery například v Paříži a Berlíně synchronizovaly své záznamy každých 15 minut. Tyto servery lze nakonfigurovat tak, aby replikovaly databáze například každé dvě hodiny nebo dokonce každých 24 hodin. Toto nastavení závisí zejména na povaze a citlivosti názvů systému WINS.

Příklad rozmístění sítě obsahuje některé přebytečné prvky, ale není jich mnoho. Nelze-li z nějakých důvodů používat například spojení mezi servery v Seattlu a Los Angeles, může replikace nerušeně pokračovat prostřednictvím serveru v San Franciscu. Co se však stane, když dojde k výpadku rozbočovače v Seattlu? Záznamy z oblasti Seattlu nebude možné nadále synchronizovat se zbytkem databáze WINS. Funkce překladu názvu však budou fungovat normálně. V takové situaci budou ztraceny pouze změny, k nimž došlo po výpadku serveru v Seattlu. Uživatelé v Seattlu nebudou schopni přeložit název souborového serveru v Chicagu, jenž byl do systému začleněn až po výpadku serveru v Seattlu. Po obnovení činnosti příslušného rozbočovače však budou všechny repliky databáze WINS přeneseny tak, jako by se nic nebylo stalo.

Příklad replikace v malém měřítku

I když jsme si už na obrázku 7.11 ukázali rozmístění rozlehlé implementace, bude asi přínosem, když si přiblížíme také příklad replikace podstatně menší. Nejjednodušší případ zahrnuje pouze dva servery (viz obrázek 7.12).



Obrázek 7.12: Replikace databáze mezi dvěma servery WINS.

Tabulky 7.8 a 7.9 obsahují záznamy z databází serveru WINS-A a WINS-B z 1. ledna 2000. Všichni klienti spouštějí počítače mezi 8.00 a 8.15. Jediným vypnutým počítačem je Klient2. Servery WINS-A a WINS-B mají nastaveny tyto parametry:

- Oba jsou si navzájem partnerskými servery pro nabízenou/vyžádanou replikaci,
- interval replikace je nastaven na 30 minut,
- interval obnovení je stanoven na 4 dny,
- hodnota intervalu zániku je 4 dny,
- časový limit zániku je 1 den,
- interval ověření je nastaven na 24 dnů.

Před spuštěním replikace jsou v databázi serveru WINS-A zapsány dva údaje. Jsou jimi záznamy počítačů Klient1 a Klient2 (viz tabulka 7.8).

Tabulka 7.8: Databáze serveru WINS-A před replikací

Název	Adresa	Příznaky	Vlastník	ID verze	Časové razítko
Klient1	192.168.22.101	jedinečný, aktivní, uzel H, dynamický	WINS-A	4B3	1/5/00 8:05:32
Klient2	192.168.22.102	jedinečný, uvolněný uzel H, dynamický	WINS-A	4C2	1/5/00 8:23:43

Před provedením replikace jsou v databázi serveru WINS-B také dva záznamy (viz tabulka 7.9). Tyto záznamy však patří klientům Klient3 a Klient4.

Tabulka 7.9: Databáze serveru WINS-B před replikací

Název	Adresa	Příznaky	Vlastník	ID verze	Časové razítko
Klient3	192.168.55.103	jedinečný, aktivní, uzel H, dynamický	WINS-B	78F	1/5/00 8:11:12
Klient4	192.168.55.104	jedinečný, aktivní, uzel H, dynamický	WINS-B	79C	1/5/00 8:12:21

Záznamy Klient1, Klient3 a Klient4 byly při spuštění opatřeny časovými razítky, jež jsou součtem aktuálního času a intervalu obnovení, zatímco Klient2 byl v okamžiku uvolnění opatřen časovým razítkem, které je součtem aktuálního času a intervalu zániku. Číslo ID verze indikuje hodnotu čítače registrace v okamžiku zaregistrování. Čítač registrace při každém vygenerování nového čísla ID verze v databázi automaticky narůstá o hodnotu 1 (hexadecimální). Každý server WINS má vlastní čítač registrace. Číslo ID verze je v případě Klienta1 4B3. Jak sami vidíte, u záznamu Klient2 se už tato hodnota rovná 4C2. Znamená to, že mezi těmito dvěma záznamy proběhlo 14 registrací (nebo zániků či uvolnění aktivních transakcí).

K synchronizaci záznamů dochází vždy v 8.30 (měřeno podle systémových hodin serveru WINS-A). V tomto okamžiku je na serveru WINS-B ukazují systémové hodiny čas 8.31:15. Je jasné, že replikace neproběhne ve stejné vteřině, ale servery používají systémové hodiny k opatření záznamů časovými razítky. Uvědomte si, že replikace neznamená, že by k vyžádání replikace mělo na obou serverech dojít souběžně – každý ze serverů si vyžádá synchronizaci podle vlastního plánu. Po dokončení replikace bude tabulka v databázi serveru WINS-A obsahovat záznamy, uvedené v tabulce 7.10.

Tabulka 7.10: Databáze serveru WINS-A po dokončení replikace

Název	Adresa	Příznaky	Vlastník	ID verze	Časové razítko
Klient1	192.168.22.101	jedinečný, aktivní, uzel H, dynamický	WINS-A	4B3	1/5/00 8:05:32
Klient2	192.168.22.102	jedinečný, uvolněný, uzel H, dynamický	WINS-A	4C2	1/5/00 8:23:43
Klient3	192.168.55.103	jedinečný, aktivní, uzel H, dynamický	WINS-B	78F	1/5/00 8:30:45
Klient4	192.168.55.104	jedinečný, aktivní, uzel H, dynamický	WINS-B	79C	1/5/00 8:30:45

Stejně tak po dokončení replikace bude tabulka v databázi serveru WINS-B obsahovat záznamy, uvedené v tabulce 7.11.

Tabulka 7.11: Databáze serveru WINS-B po dokončení replikace

Název	Adresa	Příznaky	Vlastník	ID verze	Časové razítko
Klient1	192.168.22.101	jedinečný, aktivní, uzel H, dynamický	WINS-A	4B3	1/5/00 8:31:15
Klient3	192.168.55.103	jedinečný, aktivní, uzel H, dynamický	WINS-B	78F	1/5/00 8:11:12
Klient4	192.168.55.104	jedinečný, aktivní, uzel H, dynamický	WINS-B	79C	1/5/00 8:12:21

V průběhu synchronizace byl na server WINS-B replikován záznam Klient1 a na server WINS-A byly replikovány záznamy Klient3 a Klient4. Těmto replikám byla ponecháno číslo ID verze, ale byly označeny novým časovým razítkem, které je v tomto případě součtem aktuálního času a intervalu ověření. Záznam Klient2 nebyl replikován, neboť je momentálně uložen s příznakem uvolněný. Je to poněkud neobvyklé (ale možné), neboť počítač Klient2 byl vypnut ještě před provedením replikace. Kdyby byl tento počítač vypnut až po jejím dokončení, byl by jeho záznam přenesen na server WINS-N jako aktivní. Tato replika by na tomto serveru zůstala aktivní, i kdyby se Klient2 poté ze sítě odpojil. Důvod je jasný – tato změna by nebyla na další servery replikována.

Pokud Klient2 zůstane odpojen po celou dobu trvání intervalu zániku, převede server záznam do stavu označen za neplatný. Při prvním spuštění funkce Uklidit po 8.23:43 5. ledna 2000 (za předpokladu, že interval zániku je nastaven na čtyři dny), bude databáze na serveru WINS-A obsahovat údaje, zobrazené v tabulce 7.12.

Tabulka 7.12: Databáze na serveru WINS-A po dokončení funkce Uklidit

Název	Adresa	Příznaky	Vlastník	ID verze	Časové razítko
Klient1	192.168.22.101	jedinečný, aktivní, uzel H, dynamický	WINS-A	4B3	1/9/00 6:35:26
Klient2	192.168.22.102	jedinečný, neplatný, uzel H, dynamický	WINS-A	657	1/6/00 9:50:53
Klient3	192.168.55.103	jedinečný, aktivní, uzel H, dynamický	WINS-B	78F	1/25/00 8:30:45
Klient4	192.168.55.104	jedinečný, aktivní, uzel H, dynamický	WINS-B	79C	1/25/00 8:30:45

Záznam Klient2 byl označen za neplatný, a proto se změnila jak hodnota jeho identifikátoru verze, tak i časové razítko. Časové razítko je nyní součtem aktuálního času a časového limitu zániku a nové číslo ID verze znamená, že bude tento údaj synchronizován hned při následné replikaci. Všimněte si také, že Klient1 má také nové časové razítko, ale jeho číslo ID verze se nezměnilo. Znamená to, že jeho registrace byla v předchozích čtyřech dnech obnovena. Interval obnovy závisí na klientském zásobníku.

Po následné replikaci, která proběhne v 10.00.23, bude databáze na serveru WINS-B obsahovat údaje zobrazené v tabulce 7.13 (povšimněte si také, že záznamy Klient3 a Klient4 byly obnoveny).

Tabulka 7.13: Databáze na serveru WINS-B po dokončení replikace

Název	Adresa	Příznaky	Vlastník	ID verze	Časové razítko
Klient1	192.168.22.101	jedinečný, aktivní, uzel H, dynamický	WINS-A	4B3	1/25/00 8:31:15
Klient2	192.168.22.102	jedinečný, neplatný, uzel H, dynamický	WINS-A	657	1/6/00 10:00:23
Klient3	192.168.55.103	jedinečný, aktivní, uzel H, dynamický	WINS-B	78F	1/9/00 8:11:12
Klient4	192.168.55.104	jedinečný, aktivní, uzel H, dynamický	WINS-B	79C	1/9/00 8:12:21

V případě, že Klient2 zůstane nečinný déle, než stanovuje časový limit zániku, bude při následném vyčištění databáze.

Po odstranění záznamu Klient2 bude databáze serveru WINS-A obsahovat záznamy, uvedené v tabulce 7.14.

Tabulka 7.14: Databáze na serveru WINS-A po odstranění záznamu Klient2

Název	Adresa	Příznaky	Vlastník	ID verze	Časové razítko
Klient1	192.168.22.101	jedinečný, aktivní, uzel H, dynamický	WINS-A	4B3	1/11/00 9:45:56
Klient3	192.168.55.103	jedinečný, aktivní, uzel H, dynamický	WINS-B	78F	1/25/00 8:30:45
Klient4	192.168.55.104	jedinečný, aktivní, uzel H, dynamický	WINS-B	79C	1/25/00 8:30:45

Po odstranění záznamu Klient2 bude databáze serveru WINS-B obsahovat záznamy, uvedené v tabulce 7.15.

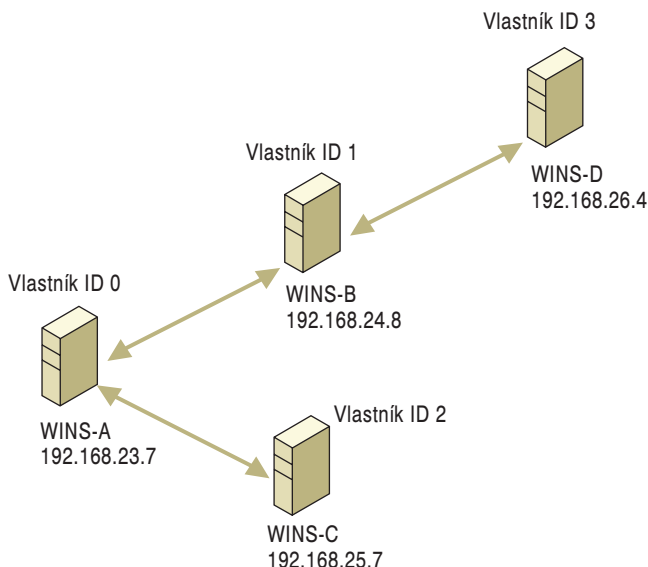
Tabulka 7.15: Databáze na serveru WINS-B po odstranění záznamu Klient2

Název	Adresa	Příznaky	Vlastník	ID verze	Časové razítko
Klient1	192.168.22.101	jedinečný, aktivní, uzel H, dynamický	WINS-A	4B3	1/25/00 8:31:15
Klient3	192.168.55.103	jedinečný, aktivní, uzel H, dynamický	WINS-B	78F	1/11/00 9:44:27
Klient4	192.168.55.104	jedinečný, aktivní, uzel H, dynamický	WINS-B	79C	1/11/00 9:46:44

Při prvním čištění databáze 25. ledna 2000 v 8.30 ověří server WINS-A na serveru WINS-B, zda počítače Klient3 a Klient4 jsou i nadále platným názvy. Stejný úkon vykoná také server WINS-B a odešle dotaz na server WINS-A pro ověření záznamu Klient1.

Vyžádání údajů z databáze WINS na základě čísla verze

Databáze serveru WINS udržuje tabulku, v níž uchovává adresy IP a ID vlastníka vzdáleného serveru WINS, který vlastní údaje v lokální databázi.



Obrázek 7.13: Vzorový replikační model.

Podle vzorového modelu replikací, znázorněného na obrázku 7.13, může tabulka mapování adres IP na ID vlastníka vzorového serveru (opět zde můžeme použít server WINS-A) obsahovat údaje, podobné těm v tabulce 7.16.

Tabulka 7.16: Příklad adres IP vzdáleného serveru WINS a čísel ID vlastníka

Adresa IP	ID vlastníka
192.168.23.7	0
192.168.24.8	1
192.168.25.7	2
192.168.26.4	3

Během inicializace služby WINS prochází příslušný server tabulku mapování název-adresa a vyhledává v ní nejvyšší číslo verze, odpovídající každému vlastníkovi, registrovanému v databázi. Po zjištění těchto informací je server spuštěn a vytváří v paměti novou tabulku, v níž páruje identifikátory partnerských serverů pro replikace se zjištěnými čísly verzí. Tato tabulka není nikdy uložena do databáze. Vzorový server WINS-A vytvoří tabulku s hodnotami zobrazenými v tabulce 7.16. Ostatní servery si vytvoří jiné tabulky.

Jak jste jistě očekávali, bude tabulka typu partner-číslo verze obsahovat jeden údaj pro každý partnerský server. Tyto údaje budou obsahovat nejvyšší číslo ID verze všech vlastníků nalezené v lokální databázi partnerského serveru. Pokud je například číslo ID

vlastníka místního serveru rovno 0, potom by podle předchozího příkladu tabulky mapování adres na ID vlastníka mohla tabulka mapování partnerských serverů na číslo verze vypadat tak, jako tabulka na obrázku 7.14.

	0	1	2
0	100	900	630
1			
2			

Obrázek 7.14: Příklad tabulky mapování partnerského serveru na číslo verze.

Obrázek 7.14 ukazuje, že lokální databáze na serveru WINS, identifikovaná pomocí identifikátoru vlastníka rovného 0, obsahuje údaje, vlastněné třemi servery WINS, jejichž čísla ID vlastníka jsou 0, 1 a 2. Nejvyššími čísla verze těchto údajů jsou 100, 900 a 630.

Server WINS-A je nyní připraven určit, zda potřebuje aktualizovat svoji databázi. Odešle zprávu všem partnerským serverům pro replikace a vyžádá si odezvu s nejvyššími čísly verze, náležejícími k souvisejícím adresám IP, uloženým v lokální databázi. Po odpovědích partnerských serverů pro nabízenou replikaci doplní server WINS svoji tabulku. Tabulka se může rozšířit o další sloupce, z nichž každý je určen pro další server.

Pokud například server WINS-B na adrese IP 192.168.24.8 (ID vlastníka rovné 1) odešle požadovaný záznam o serveru WINS-D na adrese IP 192.168.26.4, přidá žádající server WINS-A do lokální tabulky mapování partnerský server pro nabízenou replikaci-číslo verze nový sloupec. Ten bude obsahovat údaje o nepřímém partnerském serveru pro nabízenou replikaci WINS-D s číslem ID vlastníka rovným 3. Ve stejné době bude do tabulky mapování adresa-ID vlastníka přidán záznam s adresou IP a číslem ID vlastníka serveru WINS-D. Při jeho vložení jsou automaticky inicializovány buňky v nové tabulce. Pokud server WINS-B na adrese 192.168.24.8 odešle jako odpověď následující tři záznamy, přidá server WINS do tabulky mapování vlastníků-adresa nový záznam, obsahující adresu IP 192.168.26.4 a číslo ID vlastníka 3.

```
192.168.24.8    999
192.168.26.4    700
192.168.23.7    89
```

Současně také aktualizuje místní tabulku mapování partnerský server pro nabízenou replikaci-číslo verze. Tato tabulka by mohla vypadat asi jako ta na obrázku 7.15.

	0	1	2	3
0	100	900	630	0
1	89	999	0	700
2				

Obrázek 7.15: Příklad tabulky mapování partnerský server pro nabízenou replikaci-číslo verze po přijetí odezvy serveru WINS-B.

Jakmile na dotaz odpoví všechny partnerské servery pro nabízenou replikaci, bude tabulka adresa-verze obsahovat informace, znázorněné na obrázku 7.16.

	0	1	2	3
0	100	900	630	0
1	89	999	0	700
2	93	879	820	0

Obrázek 7.16: Příklad tabulky mapování partnerský server pro nabízenou replikaci-číslo verze po přijetí všech odpovědí.

Server WINS ověřuje stav této tabulky, aby mohl určit, který z partnerských serverů pro nabízenou replikaci má nejnovější data příslušných vlastníků. Server WINS má vždy nejvyšší číslo ID verze pro jím vlastněné údaje. V příkladu na obrázku 7.16 byl záznam s identifikátorem 0 zaznamenán ve třech databázích: 0, 1 a 2. Vzhledem k tomu, že je tento údaj vlastněn serverem WINS-A (údaje s identifikátorem 0), bude nejvyšší číslo ID verze (100) tohoto údaje obsahovat záznam 0,0.

Přesto však některé servery nemusí být partnery žádajícího serveru pro vyžádanou replikaci. Server WINS určuje počáteční číslo ID verze k synchronizaci lokální databáze a požaduje, aby mu partnerský server pro nabízenou replikaci odeslal všechny databázové záznamy se stejným nebo vyšším číslem ID verze. V případě, že tento server obsahuje nejnovější data více než jednoho vlastníka, může vyslat jeden dotaz na získání všech záznamů najednou. Samozřejmě, že v tomto jednoduchém příkladu se změny neprojeví na serveru WINS s nejnovějšími daty. Když si server WINS-A vyžádá data, bude server WINS-B obsahovat svoje nejnovější data a nejnovější data serveru WINS-D. Server WINS-C obsahuje pouze svoje nejnovější data. Ve složitějším příkladu by mohla cesta replikace vytvářet cykly a replikace by probíhala v rozdílných intervalech.

Jakmile přijme partnerský server pro nabízenou replikaci požadavek z jiného serveru WINS (partnerského serveru pro vyžádanou replikaci), vyhledá ve své databázi vyžádané záznamy a odešle je žádajícímu serveru. Partnerský server pro nabízenou replikaci vyhledává vyžádané záznamy tak, že nastaví příslušný interval a sekvenčně v něm prochází všechny záznamy, dokud z něj nevyzvedne poslední vyžádaný záznam. Při přijetí těchto záznamů partnerský server pro vyžádanou replikaci automaticky aktualizuje svoji databázi.

V cílové databázi budou nahrazeny všechny údaje s větším číslem ID verze. Každá změna v databázi ovšem ještě neznamená, že se musí zvýšit také číslo ID verze ovlivněných záznamů.

Jak dochází ke změnám a aktualizacím záznamů

Server WINS zadává do své databáze vždy údaje o registraci názvů jako aktivní a automaticky je označuje časovým razítkem, rovným součtu aktuálního času a intervalu obnovení. Číslo ID verze je převzato z čítače čísla ID verze. Čítač čísla ID verze je pak zvýšen.

V případě, že byl název výslovně zrušen nebo v případě, kdy nebyl obnoven ve stanoveném intervalu, bude záznam označen za uvolněný. Server WINS k němu připojí časové razítko, k jehož vytvoření použije součet aktuálního času a intervalu zániku. Číslo ID verze ponechá beze změny. Díky tomu záznam nespádá do množiny záznamů, které budou synchronizovány při následných replikacích. Pokud záznam v tomto stavu přetrvá i po dobu vyznačenou intervalem zániku, bude označen za neplatný a server WINS k němu připojí časovou značku, vytvořenou ze součtu aktuálního systémového času a časového limitu zániku. Kromě toho zvýší jeho číslo ID verze, takže od té-

to chvíle se tento záznam stane součástí množiny replikovaných záznamů. Jestliže záznam v tomto stavu zůstane i po vypršení časového limitu zániku, bude z databáze fyzicky odstraněn.

Služba WINS replikuje pouze záznamy označené jako aktivní nebo neplatné. V partnerských databázích pak tyto záznamy vkládá pomocí polí, získaných z vlastnické databáze. Výjimkou jsou ID vlastníka a časová značka. (ID vlastníka pochází z místní tabulky mapování vlastníka-adresa, neboť místně použitá hodnota může být na každém serveru jiná. Například WINS-D může být na serveru WINS-B zastoupen hodnotou 2, zatímco na serveru WINS-A jej označuje hodnota 3.) Služba WINS připojí k aktivnímu záznamu vlastní časové razítko, vytvořené ze součtu aktuálního systémového času a intervalu ověření. K záznamu označenému za neplatný připojí časové razítko vytvořené na základě součtu místního systémového času a časového limitu zániku.

Konflikty zjištěné během replikace

Přestože jsou konflikty názvu zpravidla obslouženy už v okamžiku registrace (viz „Konflikty zjištěné během registrace“ dříve v této kapitole), je možné, že dojde k registraci stejného názvu na dvou různých serverech WINS. To se může stát, když klient WINS zaregistruje stejný název na druhém serveru WINS ještě předtím, než dojde k replikaci databáze z prvního serveru WINS. V takových případech služba WINS řeší konflikty v době replikace.

Konflikty, objevené během replikace, mohou nastat mezi dvěma jedinečnými názvy, mezi jedinečným názvem a názvem skupiny nebo mezi záznamy o dvou skupinách.

Konflikt mezi jedinečnými údaji Služba WINS řeší všechny konflikty mezi jedinečnými údaji podle následujících tří okolností:

- **Aktuální označení záznamů** Údaje v databázi mohou být označeny jako aktivní, uvolněné nebo neplatné. Replika může být označena buď za aktivní nebo za neplatnou.
- **Vlastnictví údajů** Server WINS může, ale také nemusí být vlastníkem těchto databázových položek.
- **Adresy položek** Adresy položek se mohou, ale také nemusí shodovat.

Konflikt mezi dvěma replikami Dojde-li ke konfliktu dvou replik, přepíše novější replika starší záznam bez ohledu na to, zda se jejich adresy shodují či nikoliv. Jediná výjimka tohoto pravidla nastane, když je starší replika aktivní, zatímco novější záznam je označen za neplatný. Je-li nová replika označená za neplatnou, ponechá původní záznam beze změny, pokud samozřejmě není vlastníkem obou záznamů jeden a tentýž server WINS.

Konflikt mezi vlastněným záznamem a replikou se stejnou adresou IP Replika nahradí záznam v databázi vždy kromě případů, kdy je záznam v databázi aktivní a příchozí replika je označená za neplatnou. V tomto případě služba WINS pouze zvýší číslo ID verze databázového záznamu, aby byl synchronizován při nejbližší následné replikaci.

Konflikt mezi vlastněným záznamem a replikou s jinou adresou IP Replika nahradí záznam v databázi vždy kromě případů, kdy je záznam v databázi aktivní. Pokud je záznam aktivní a příchozí replika je označená za neplatnou, zvýší služba WINS číslo ID verze databázového záznamu, aby byl synchronizován při nejbližší následné replikaci. V případě, že je příchozí replika také aktivní, vyzve server klienta (vlastníka názvu v lokální databázi), aby určil, zda je záznam i nadále používán. Po kladné odezvě odešle klientovi příchozí repli-

ky výzvu ke změně do konfliktního názvu, tedy zprávu, která tohoto klienta zařadí na do konfliktního stavu. Přířímým důsledkem existence záznamu v tomto seznamu je označení názvu uzlu na konfliktní. Takto označené názvy dále nelze používat.

Konflikt mezi jedinečným záznamem a záznamem skupiny Jsou-li v konfliktu jedinečný záznam a záznam skupiny, zachová služba WINS v databázi záznam skupiny. V případě, že je příslušný server vlastníkem záznamu a záznam není označen za uvolněný nebo neplatný, požádá klienta jedinečného záznamu, aby název neprodleně uvolnil.

Konflikt mezi dvěma záznamy speciální skupiny Replika nenahradí databázovou položku jedinečnou tehdy, je-li tato aktivní. V tomto případě služba WINS zvýší číslo ID verze, aby mohl být záznam synchronizován s ostatními databázemi ihned při následné replikaci. Pokud je aktivní také přichodí replika, server WINS provede aktualizaci seznamu členů tohoto databázového záznamu, a to pomocí nových členů, určených přichodí replikou. Přesahují-li počet nových členů mezní hranici 25, bude do seznamu přidán pouze maximální povolený počet a zbývající členové budou tiše odstraněni.

Konflikt s vícedomým záznamem Dojde-li ke konfliktu vícedomé přichodí repliky se záznamem označeným za uvolněný nebo neplatný, přepíše služba WINS tento záznam hodnotami přichodí repliky. K výjimce z tohoto pravidla dojde v případě, kdy je databázový záznam údajem běžné skupiny označeným za uvolněný. Tato skutečnost však nijak nevybočuje z ostatních scénářů, v nichž dojde ke konfliktu uvolněného záznamu běžné skupiny se záznamem s jedinečnou adresou.

V případě konfliktu přichodí vícedomé repliky označené za neplatnou s aktivním databázovým záznamem, jehož vlastník je také vlastníkem přichodí vícedomé repliky, je databázový záznam nahrazen přichodí replikou. Je-li aktivní databázový záznam replikou, vlastněnou jiným serverem, služba WINS ponechá záznam v původním stavu. Pokud je aktivní záznam vlastněn místním serverem WINS a jedná-li se o jedinečný záznam, zvýší služba WINS jeho číslo ID verze a vynutí tak jeho replikaci.

Pokud je aktivní vícedomá replika v konfliktu s aktivní jedinečnou vícedomou replikou v lokální databázi stejného vlastníka, bude původní databázový záznam přepsán. Je-li její vlastníkem jiný server, zůstane původní záznam neporušen. Pokud je vlastníkem záznamu v databázi lokální server WINS a jsou-li členové záznamu (v případě jedinečného záznamu to bude jeden člen) zároveň podmnožinou členů repliky, změní služba WINS jeho časové razítko a zvýší jeho identifikátor verze. Díky tomu bude tento záznam v příští replikaci propagován do ostatních databází. Jestliže nejsou členové repliky takovou podmnožinou, bude odeslána výzva adresám v databázovém záznamu. Bude-li tato výzva úspěšná (tzn. pokud oslovený klient na žádnou výzvu nezareaguje), bude záznam v databázi nahrazen novým záznamem. V případě, že klient zareaguje alespoň na jednu z odeslaných výzev, upozorní jej služba WINS, aby uvolnil název ze všech registrovaných. Poté WINS server provede nahrazení záznamu replikou. Je-li vícedomá přichodí replika v konfliktu s aktivním záznamem skupiny, zvýší služba WINS identifikátor verze aktivního záznamu a tím zajistí jeho replikaci.

V případě, že se přichodí jednoadresová replika dostane do konfliktu s vícedomým neaktivním záznamem v databázi, nahradí služba WINS záznam replikou. Je-li tato replika v konfliktu s aktivním vícedomým záznamem, vlastněným stejným serverem, nahradí služba WINS záznam replikou také. Jestliže je vícedomý záznam v databázi replikou, vlastněnou jiným serverem, ponechá WINS původní záznam beze změny. Pokud je však vícedomý záznam vlastněn lokálním serverem WINS, zatímco přichodí replika je

jedinečným záznamem, vyzve služba WINS k uvolnění adres právě klienta vícedomého záznamu. Bude-li výzva úspěšná, může být záznam přepsán příchozí replikou. V případě, že klient zareaguje alespoň na jednu z odeslaných výzev, služba WINS jej upozorní, aby před nahrazením mapování názvu uvolnil název ze všech registrovaných adres v rámci celé databáze, a teprve pak záznam přepíše. Adresa v jedinečné replice (pokud se nachází v seznamu členů) je v předchozí situaci přeskočena.

Trvalá připojení

Služba Windows 2000 WINS zavádí trvalá připojení mezi partnerskými servery pro replikace. V dřívějších verzích bylo vyžadováno, aby servery vytvářely nové připojení při každé replikaci databáze. Vzhledem k tomu, že vytvoření a ukončení každého připojení vyžadovalo kromě odesílání síťových paketů také poměrně značnou část času procesoru, nastavovali správci sítě své systémy tak, aby se před každou takovou operací nastrádal určitý počet záznamů. Čekání na nastrádání nastaveného počtu záznamu vytvářelo zpoždování při aktualizaci celé databáze (aktualizace se často zpožďovaly i o desítky minut), což způsobovalo vznik časových oken. Zde byl samozřejmě původ nekonzistence lokální databáze s databázemi partnerských serverů.

Server služby Windows 2000 WINS lze pomocí konzoly systémové správy WINS konfigurovat tak, aby vyžadoval trvalé připojení s jedním nebo více partnerskými servery pro replikace. Toto nastavení odstraní zbytečné přetěžování sítě opakovaným otevíráním a zavíráním připojení. Trvalá připojení zvyšují rychlost replikace, neboť server odesílá záznamy svým partnerům okamžitě, aniž by předtím musel vytvářet dočasné připojení. Tyto okamžité aktualizace každého záznamu logicky zvyšují soudržnost záznamů. Šířka vyžadovaného frekvenčního pásma je však minimální, neboť připojení je po většinu času nečinné.

Stejně tak je možné konfigurovat trvalá připojení za účelem replikování záznamů pouze po dosažení určitého počtu změn. Za normálních okolností je tento počet nastaven na 20 záznamů. Je-li používáno trvalé připojení, je tato mezní hodnota ignorována.

Automatické zjišťování partnerských serverů pro replikace

Funkce automatického vyhledávání umožňuje serverům WINS vyhledávat partnerské servery bez vnějšího zásahu. Není tedy zapotřebí zdlouhavého předběžného nastavování partnerských serverů pro replikace. Tuto funkci lze spustit z prostředí konzoly Microsoft Management Console na kartě Vlastnosti partnerských serverů pro replikace. Zde zaškrtněte políčko Povolit automatickou konfiguraci partnerského serveru.

Server WINS potom bude v pravidelných intervalech ohlašovat svou přítomnost v síti. Tato oznámení WINS jsou odesílána metodou vícesměrového vysílání na adresu, rezervovanou pro službu WINS (224.0.1.24). Servery WINS s povolenou funkcí automatického zjišťování partnerských serverů pro replikace budou toto vysílání sledovat a tímto způsobem se dozví o všech přítomných serverech v příslušné počítačové síti. Všechny takto nalezené servery WINS budou automaticky přidány do seznamu partnerských serverů jako partnerské servery pro nabízenou i vyžádanou replikaci. Tuto funkci byste však měli využívat pouze tehdy, jste-li si jisti, že do vaší sítě neproniknou žádné neautorizované servery WINS. Jinak by mohlo dojít k tomu, že by se tyto servery staly vašími partnery proti vaší vůli.

Doporučené postupy při replikování databáze WINS

Správným nakonfigurováním funkce replikace se můžete vyvarovat mnoha nepříjemností a navíc tím umožníte skupině serverů WINS fungovat podstatně efektivněji.

Konfigurace partnerských serverů pro nabízenou a vyžádanou replikaci

Obecně platí, že nabízená a vyžádaná replikace je nejjednodušším a přitom nejefektivnějším způsobem zajištění plné synchronizace záznamů mezi jednotlivými servery WINS. Toto nastavení také zaručuje to, že primární a sekundární servery libovolného klienta služby WINS jsou zároveň partnerskými servery pro nabízenou a vyžádanou replikaci proti sobě navzájem, což je v podstatě požadavek správné funkce služby WINS v případě selhání primárního serveru klienta.

Ve většině instalací služby WINS se vyhýbejte používání omezeného partnerství při replikacích (pouze pro vyžádanou nebo pouze pro nabízenou replikaci). V rozsáhlých podnikových sítích může omezení partnerství pro replikace umožnit také replikace prostřednictvím pomalých připojení. Když však máte v úmyslu používat pro replikace pouze omezené partnerství, věnujte zvýšenou pozornost návrhu sítě a její konfiguraci. Každý server musí mít i tak nastaven alespoň jeden partnerský server pro replikace a každé pomalé připojení, které zaměstnává jednosměrnou vazbu, by mělo být vyváжено jinou jednosměrnou vazbou, která zajišťuje přenesení vyžádaných aktualizací v opačném směru.

Návrh replikace a konvergence WINS v paprskovitě rozmístěné síti s centrálním rozbočovačem

Konvergence je kritickou částí plánování služby WINS. Hlavním otázkou doby konvergence zůstává: „Jak dlouho bude trvat synchronizace změny v datech jednoho serveru WINS s daty uloženými na partnerských serverech WINS?“ Odpověď je součet časových intervalů mezi jednotlivými servery na nejdelší replikační cestě. Více informací o otázkách konvergence najdete v jiném oddíle této kapitoly, „Celkový pohled na proces replikace“.

Ve většině případů poskytuje model paprskovitě rozmístěné sítě s centrálním rozbočovačem jednoduchou a zároveň efektivní metodu plánování rozvržení, vyžadovaného pro plnou a rychlou konvergenci s minimálními administrativními prodlevami. Tento model bude například skvěle fungovat v organizacích s centrálním řízením nebo se společným datovým úložištěm (rozbočovač) s několika pobočkami (ramena sítě). Druhý záložní rozbočovač (druhý server WINS s centrálním umístěním) může zvýšit odolnost služby WINS proti chybám.

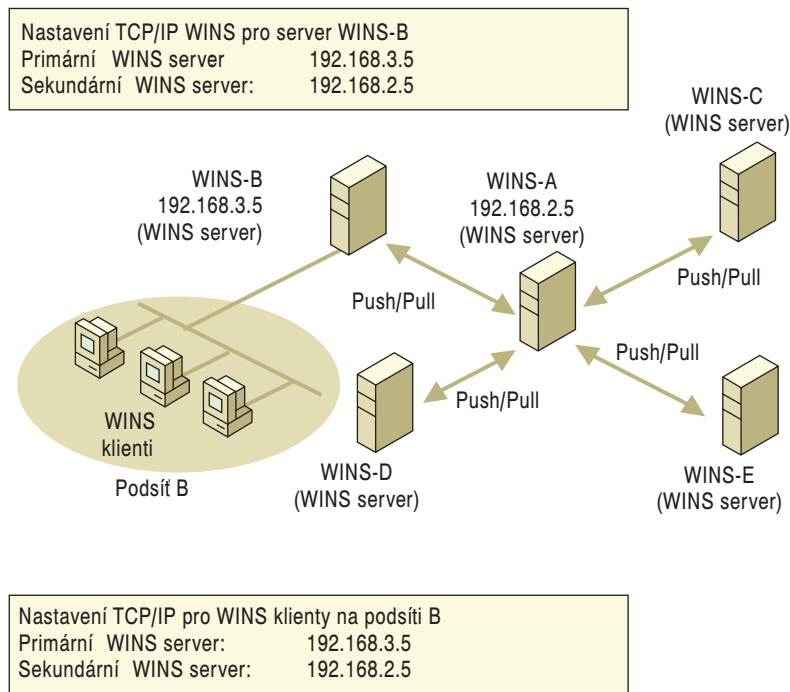
Podívejte se na jednoduchý model paprskovitě rozmístěné sítě s centrálním rozbočovačem, zobrazený na obrázku 7.17.

Doba konvergence systému znázorněného na obrázku 7.17 je součtem dvou nejdelších intervalů konvergence rozbočovače. Pokud například servery WINS-B a WINS-D synchronizují svá data se serverem WINS-A ve 30minutových intervalech a servery WINS-S a WINS-E synchronizují svá data každé 4 hodiny, činí doba konvergence 8 hodin.

Replikace napříč bezpečností bránou (firewall)

V některých rozlehlých sítích je třeba synchronizovat data také napříč bezpečnostní bránou. Replikace WINS probíhá prostřednictvím portu TCP 42. Z toho vyplývá, že ten-

to port nesmí být (v případě nastavení replikace napříč bezpečností bránou) zablokovan na žádném ze zprostředkujících síťových zařízení, umístěných mezi dvěma partnerskými servery pro replikace.



Obrázek 7.17: Model paprskovitě rozmístěné sítě s centrálním rozbočovačem.

Správa serverů WINS

Systém Windows 2000 poskytuje inovovanou verzi programu Správce WINS, což je administrativní nástroj grafického uživatelského rozhraní, který můžete používat při správě služby WINS v rámci vlastní počítačové sítě. Inovovaná verze tohoto nástroje je umístěna v konzole Microsoft Management Console (MMC) a umožňuje vlastní správu serverových aplikací.

Konzola systémového řízení WINS obsahuje ve srovnání s předchozími verzemi podstatná rozšíření, z nichž mnoho bylo navrženo samotnými správci sítí. Mezi tyto nové funkce patří:

- Trvalé připojení,
- ruční označování záznamů za neplatné,
- vylepšené nástroje pro správu serverových aplikací,
- rozšířené možnosti filtrování a vyhledávání záznamů,
- dynamické mazání záznamů a možnost jejich vícenásobného výběru,
- ověřování platnosti samotného záznamu, ale i čísla jeho verze,
- funkce Export,

- zvětšená odolnost proti chybám,
- dynamické obnovení klientů.

Konzola systémového řízení WINS poskytuje nástroje pro snadnou údržbu, prohlížení, zálohování a obnovu databáze serveru WINS. Slouží také jako ideální prostředek pro prohlížení a změny parametrů serverů WINS. Více informací o specifických úlohách správy a konfigurace najdete v nápovědě online k programu konzola systémového řízení WINS.

Program Sledování systému a agent služby SNMP jsou nezdědka velmi cennými nástroji při správě serverových aplikací služby WINS. Program Sledování systému můžete používat například k monitorování výkonu serveru WINS.

Službu SNMP lze použít ke sledování a konfiguraci serverů WINS pomocí nástrojů správce SNMP od jiných dodavatelů. Budete-li takové nástroje používat, mohou některé dotazy WINS překračovat časové limity. Proto byste měli zvýšit časový limit ve svém nástroji SNMP. Služba Windows 2000 SNMP Service využívá objekty Microsoft Information Base. Tyto objekty jsou obecně označovány jako objekty, které poskytují podporu pro službu SNMP, aby ta mohla sledovat takové procesy jako počet chyb, stavové záznamy nebo obsah tabulky směrování adres IP daného počítače. Více informací o typech objektů Microsoft Information Base najdete v kapitole „Typy objektů databáze MIB“, další informace o programu Sledování systému a agent služby SNMP najdete v jiné kapitole této knihy, „Simple Network Management Protocol“, nebo v kapitole „Monitoring Network Performance“ (Sledování výkonu sítě) v dokumentaci *Microsoft® Windows® 2000 Server Správa systému*.

Prohlížení operačního stavu serveru WINS

Konzola systémového řízení WINS zobrazuje administrativní a operační informace o serverech WINS. Chcete-li zobrazit základní statistiku určitého serveru WINS, otevřete okno konzoly systémového řízení WINS, označte příslušný server a z rozevřací nabídky zadejte příkaz **Akce**. Potom klepněte na tlačítko **Zobrazit statistiku serveru**. Na obrazovce se zobrazí podobné informace, jak si můžete prohlédnout na obrázku 7.18. Tabulka 7.17 obsahuje popis základních statistických údajů, znázorněných také na obrázku 7.18. Tyto údaje zahrnují jak základní, tak i podrobné statistické údaje systému Windows NT verze 4.0.

Tabulka 7.17: Statistické údaje o serveru WINS

Statistický údaj	Popis
Databáze inicializována	Doba posledního importu statického mapování do databáze WINS.
Statistika naposledy vynulována	Doba posledního vymazání statistických údajů o příslušném serveru WINS pomocí příkazu Vymazat statistiku v nabídce Zobrazit.
Poslední časy replikace	Zaznamenané časy replikování databáze WINS.
Poslední pravidelná replikace	Poslední zaznamenaná replikace, založená na intervalu replikace určeném v dialogovém okně Předvolby.
Poslední replikace spuštěná administrátorem	Poslední zaznamenaná replikace databáze WINS, vyvolaná po klepnutí na tlačítko Replikovat, umístěném v dialogovém okně Partnerské servery pro replikace.

Statistika serveru WINS ODIN		
Popis	Podrobnosti	
Čas spuštění serveru	11.8.2000 3:24:48	
Databáze inicializována	...	
Statistika naposledy vynulována	11.8.2000 3:37:22	
Poslední periodická replikace	11.8.2000 4:08:42	
Poslední ruční replikace	11.8.2000 3:40:34	
Poslední replikace sítovou aktualizací	...	
Poslední replikace změny adres	...	
Celkem požadavků	77	
nalezených záznamů	31	
Záznamy nebyly nalezeny.	46	
Celkem uvolnění	8	
nalezených záznamů	8	
Záznamy nebyly nalezeny.	0	
Jedinečné registrace	16	
Konflikty	21	
Obnovení	25	
Registrace skupin	0	
Konflikty	4	
Obnovení	17	
Celkem přijatých registrací	16	
Poslední pravidelné čištění	...	
Poslední ruční čištění	...	
Poslední čištění záznamů	...	
Poslední čištění ověření	...	
Partner WINS 172.20.11.250	Počet replikací 4	Počet selhání komunikace 0
<input type="button" value="Obnovit"/> <input type="button" value="Aktualizovat"/> <input type="button" value="Zavřít"/>		

Obrázek 7.18: Statistiky serveru WINS

Statistický údaj**Popis**

Poslední replikace sítovou aktualizací

Poslední zaznamenaná replikace databáze WINS, spuštěná jako výsledek síťového požadavku, jímž byla zpráva s vyžádáním o přenos aktualizovaných záznamů.

Celkem požadavků

Celkový počet zpráv s dotazy na název, přijatých příslušným serverem WINS. Položka „Nalezeno záznamů“ určuje počet názvů, odpovídajících zadané podmínce, zatímco položka „Nenalezeno záznamů“ určuje počet názvů, které server nemohl přeložit.

Celkem uvolnění

Celkový počet přijatých zpráv popisujících zastavení programu NetBIOS. Položka „Nalezeno záznamů“ určuje počet uvolněných názvů, zatímco položka „Nenalezeno záznamů“ určuje počet názvů, které se serveru nepodařilo uvolnit.

Celkem přijatých registrací

Celkový počet přijatých zpráv s požadavkem na registraci názvu.

Poslední replikace změny adres

Popisuje, kdy byla replikována poslední změna databáze WINS.

Poslední časy úklidu

Popisuje poslední časy, kdy byly z databáze uklizeny údaje určitého typu.

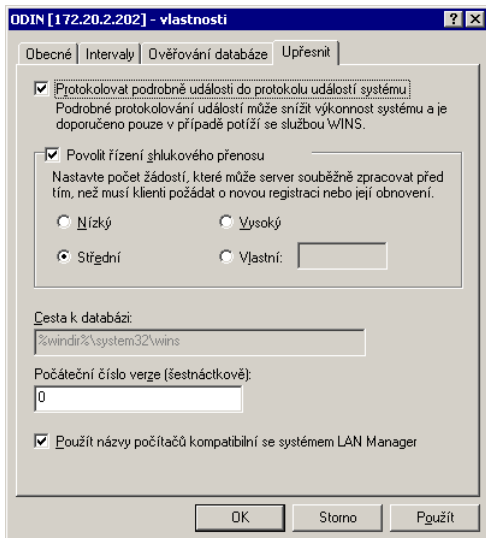
Poslední pravidelný úklid

Poslední zaznamenaný úklid, založený na intervalu obnovení určeném v dialogovém okně Vlastnosti serveru WINS na kartě Záznam o názvu.

Statistický údaj	Popis
Poslední úklid spouštěný administrátorem	Popisuje dobu posledního úklidu databáze, vyvolaného zadáním příkazu Zahájit úklid databáze.
Poslední čištění zániků	Popisuje dobu posledního úklidu databáze vyvolaného po uplynutí zadaného intervalu zániku.
Poslední čištění ověření	Popisuje dobu posledního úklidu databáze vyvolaného po uplynutí zadaného intervalu ověření.
Jedinečné registrace	Popisuje počet požadavků na registraci názvů, které byly daným serverem WINS akceptovány.
Jedinečné konflikty	Počet konfliktů zjištěných během registrace jedinečných názvů, vlastněných daným serverem WINS.
Jedinečná obnovení	Počet přijatých požadavků na obnovení jedinečných názvů.
Registrace skupin	Počet požadavků na registraci názvů skupin přijatých daným serverem WINS.
Konflikty skupin	Počet konfliktů zjištěných během registrace názvů skupin.

Konfigurace chování serveru a klienta

Konfigurační volby, poskytované konzolou systémového řízení WINS, můžete používat ke změně správy mapování klientských záznamů v databázi WINS.



Obrázek 7.19: Možnosti konfigurace serveru WINS na kartě Upřesnit.

Volby pro konfiguraci časovače lze najít na kartě **Záznam o názvu** dialogového okna **Vlastnosti serveru WINS**, znázorněného na obrázku 7.8. Díky těmto volbám můžete určit různé časové intervaly, které budou následně řídit chování klienta služby WINS. Zde můžete nastavit interval obnovení, interval zániku, časový limit zániku a interval

ověření. Podrobnosti o nastavení těchto hodnot najdete v oddíle „Časovače“ dříve v této kapitole.

Kromě toho se dá nastavit také četnost obnovování statistických údajů. Můžete změnit i cestu pro ukládání záložního souboru databáze. Tuto vlastnost lze změnit na kartě **Obecné** dialogového okna **Vlastnosti** serveru WINS. Nakonec můžete změnit také upřesňující vlastnosti serveru, znázorněné na obrázku 7.19.

Chcete-li jemně doladit chod serveru WINS, použijte možnosti znázorněné na obrázku 7.19. Patří mezi ně Upřesnit přihlášení a Ovládání shlukového přenosu. Změny parametrů, uvedených v tabulce 7.18, umožňují změnit většinu pokročilých vlastností serveru WINS.

Tabulka 7.18: Upřesňující volby konfigurace serveru WINS

Možnosti konfigurace	Popis
Protokolovat změny v databázi	Určuje, zda změny v databázi budou ukládány do souborů protokolu J50.log.
Protokolovat podrobně události do protokolu událostí	Určuje, zda budou události protokolovány v režimu s podrobným výstupem, používaným zpravidla při odstraňování potíží. Tento režim vyžaduje značné systémové prostředky počítače a proto by měl být zakázán, chcete-li dosáhnout lepšího výkonu systému.
Replikovat pouze s partnerskými servery	Určuje, že k replikaci bude docházet pouze s nakonfigurovanými partnerskými servery pro nabízenou či vyžádanou replikaci. Není-li tato možnost nastavena, může správce požádat server, aby si vyžádal replikaci, nebo ji naopak poskytl serveru, jenž není na seznamu partnerských serverů pro replikace. Standardně je tato možnost zapnutá.
Zálohovat při ukončení	Automaticky zálohuje databázi WINS při ukončení činnosti konzoly systémového řízení WINS. Výjimkou je vypnutí počítače.
Přenést	Jedinečné statické a vícedomé statické záznamy jsou při konfliktu s novou registrací nebo replikou považovány za dynamické záznamy. Není-li ověřena jejich další platnost, jsou novou registrací či replikou přepsány. Pokud přenášíte nastavení na jiný systém než systém typu Windows NT, zaškrtněte toto políčko. Standardně je prázdné.
Číslo počáteční verze	Určuje nejvyšší číslo Id verze příslušné databáze. Zpravidla nebudete potřebovat tuto hodnotu měnit, ale vše se může změnit, dojde-li k narušení databáze. V takovém případě zvýšte číslo Id verze své databáze na všech partnerských serverech pro replikace, které už dříve synchronizovaly svá data s příslušným serverem. Díky službě WINS lze tuto hodnotu zvýšit a zajistit tak rychlou replikaci dat na ostatní servery WINS. Maximální povolená hodnota je 231 –1. Tuto hodnotu můžete najít v dialogovém okně Zobrazit databázi v konzole systémového řízení WINS.

Možnosti konfigurace	Popis
Cesta k záložní kopii databáze	Určuje adresář pro uložení záložní kopie databáze. Určí-li cestu k záložní kopii databáze, bude služba WINS automaticky každých 24 hodin zálohovat všechna data. Služba WINS používá tento adresář k automatickému obnovení záznamu, zjistí-li při spuštění, že došlo k narušení databáze. Cesta k záložní kopii by neměla ukazovat na síťovou složku.

Správa mapování statických adres

Statickým mapováním se označují ty nedynamické položky v databázi, které obsahují názvy počítačů rozhraní NetBIOS a adresy IP, jež jsou rezervovány pro síťové počítače, které nespolupracují se službou WINS, nebo jež jsou rezervovány pro speciální skupiny síťových zařízení.

Chcete-li prohlížet, přidávat, editovat, importovat nebo odstraňovat statická mapování v konzole systémového řízení WINS, zadejte z nabídky **Mapování** příkaz **Statické mapování**.

Jakmile je statické mapování název-adresa vloženo do databáze, nelze je ani ověřovat, ani odstranit. Výjimkou je akce správce, jenž může tyto záznamy z databáze odstranit prostřednictvím konzoly systémového řízení WINS. Všechny změny v databázi WINS provedené pomocí tohoto nástroje se projeví okamžitě. Statické adresy IP neboli adresy rezervované pro službu DHCP mapované na jedinečné názvy na vícedomém počítači přepisují zastaralá statická mapování, jestliže je volba **Přesun zapnout/vypnout** zapnuta.

Správa vícedomých serverů

U všech počítačů, které používají službu WINS nebo NetBIOS spolu s protokolem TCP/IP (NetBT), je k názvu připojena jedna adresa IP, která je následně s tímto názvem používána. Ve výchozím nastavení je adresa IP, používaná k vytvoření vazby NetBT, primární adresou IP, konfigurovanou pro první síťový nainstalovaný adaptér rozpoznáný systémem Windows 2000.

Pořadí vytváření vazeb s nalezenými adaptéry však lze změnit. Nejprve poklepejte v Ovládacích panelech na ikonu **Síťová a telefonická připojení**. Potom z nabídky zadejte příkaz **Upřesnit**. V zobrazeném dialogovém okně zadejte příkaz **Upřesnit nastavení...** a následně se přesuňte na kartu **Adaptéry a vazby**.

Pořadí vytvoření vazeb můžete nastavit také na kartě **Adaptéry a vazby** dialogového okna **Upřesnit nastavení**, zobrazeného ze složky **Síťová a telefonická připojení**. Toto dialogové okno je umístěno mimo nabídku **Upřesnit**. Pořadí vytváření vazeb změňte přesunutím pomocí šipek nahoru a dolů u položek v seznamu **Seznam připojení**.

Vzhledem k tomu, že činnost rozhraní NetBIOS závisí na prvním instalovaném adaptéru, musíte si při používání vícedomého serveru WINS ověřit platnost adresy IP příslušného adaptéru. Jakmile budete tuto adresu znát, stačí, že ji přiřadíte klientům WINS (ať už dynamicky pomocí serveru služby DHCP, nebo ručním nakonfigurováním klientů).

Všechny partnerské servery pro nabízenou a vyžádanou replikaci by kromě toho měly být konfigurovány i na používání této vázané adresy IP, je nutné ověřit její použití na dalších partnerských serverech WINS.

Správa služby WINS napříč bezpečnostní bránou (firewall)

Budete-li spravovat službu WINS ze vzdáleného počítače, musíte nejprve vytvořit připojení prostřednictvím portu TCP č. 135. Tato relace pokračuje další relací na náhodně vybraný port nad mezní hodnotou 1024. Tyto dvě relace na určité porty jsou vytvořeny proto, že program Správce WINS používá tyto dynamické koncové body při práci s protokolem RPC (vzdálené volání procedur). Bezpečnostní brány sítě Internet nelze nakonfigurovat tak, aby propouštěly přenosy při správě služby WINS, zatímco je příslušný port v nekonzistentním stavu. V systému Windows 2000 je tento problém vyřešen výchozím systémovým nastavením, které umožňuje v registru změnit dynamické přidělení portu na přidělení pevné.

Upozornění: K přímé editaci registru se uchylujte skutečně až tehdy, nezbývá-li žádná jiná možnost jeho úpravy. Editory registru obcházejí standardní bezpečnostní opatření, poskytována správnými nástroji. Tato bezpečnostní opatření zajišťují prevenci proti zadávání konfliktních nastavení nebo nastavení, která by mohla snížit výkon systému nebo dokonce systém poškodit. Přímá editace registru může mít vážné a nepředpokladané následky, jež mohou ve svém důsledku zabránit spuštění systému. Takové poškození lze řešit jedině opětovnou instalací systému Windows 2000. Chcete-li konfigurovat nebo přizpůsobit nastavení systému Windows 2000, používejte k tomu účelu konzolu Microsoft Management Console (MMC) nebo jiné nástroje Ovládacích panelů.

Správa služby WINS prostřednictvím bezpečnostní brány sítě Internet bude možná až po konfigurování seznamu všech portů, které jsou k dispozici (nebo které nejsou) z Internetu. Nastavené hodnoty budou v registru uloženy pod následujícím klíčem:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Internet

Třemi uloženými údaji jsou Ports, PortsInternetAvailable a UseInternetPorts. Podívejme se tedy na jejich podrobnější popis.

Název: Ports

Datový typ: REG_MULTI_SZ – sada rozsahy portů IP.

Popis: Určuje sadu rozsahů portů IP, které se skládají buď ze všech portů dostupných v síti Internet nebo ze všech portů v síti nedostupných. Každý z řetězců reprezentuje jeden port nebo rozsah portů (například „1000 – 1050“ nebo „1984“). Pokud jsou některé údaje mimo rozsah od nuly do 65 535 nebo pokud nelze řetězec správně interpretovat, bude služba RPC runtime považovat tuto konfiguraci za neplatnou.

Název: PortsInternetAvailable

Datový typ: REG_SZ – Y nebo N (nerozlišují se malá a velká písmena).

Popis: Je-li nastavena na Y, budou porty uvedeny v seznamu všech portů, považovány za dostupné v síti Internet. Je-li touto hodnotou N, budou v seznamu uvedené porty, které za dostupné v síti Internet považovány nejsou.

Název: UseInternetPorts

Datový typ: REG_SZ – Y nebo N (nerozlišují se malá a velká písmena).

Popis: Určuje výchozí systémovou zásadu. Je-li tato hodnota nastavena na Y, budou procesům, používajícím výchozí nastavení, přiřazeny porty ze seznamu dostupných portů v síti Internet (viz výše). Je-li však touto hodnotou N, budou procesům, používajícím výchozí nastavení, přiřazeny porty ze seznamu portů dostupných pouze v podnikové síti intranet.

Doporučené postupy při práci s konzolou systémového řízení WINS

Konzola systémového řízení WINS umožňuje pružné řízení sítě WINS. Přesto však v mnoha případech bude nejlepší pracovat s výchozím nastavením. Protokolování a přenosy, to jsou dva nejčastější zdroje obtíží.

Používejte výchozí konfigurační nastavení Výchozí nastavení služby WINS poskytuje ve většině případů optimální konfiguraci a mělo by být využíváno ve většině síťových instalacích služby WINS. Pokud se rozhodnete tuto nastavení změnit, ujistěte se, že je to skutečně zapotřebí a že chápete všechny možné důsledky tohoto kroku.

Neupravuje nastavení Přenos Používáte-li statické údaje pouze jako podporu dočasných síťových změn, ponechte v konzole systémového řízení WINS výchozí nastavení položky **Přenos (Přepsat jedinečný statický záznam dynamickým záznamem)**.

Bude-li zaškrtnuto políčko **Přenos (Přepsat jedinečný statický záznam dynamickým záznamem)**, budou klienti moci ověřovat a dynamicky aktualizovat všechny dočasné statické záznamy, ať už jedinečné nebo vícedomé. Všechny pozdější pokusy klientů WINS o dynamickou registraci existujícího názvu, jedinečného nebo vícedomého, budou mít za následek výzvu.

Ve výzvě ověření bude server WINS porovnávat adresu IP ve statickém mapování s libovolnou adresou IP, kterou se klient pokouší dynamicky registrovat v databázi WINS. Pokud se tyto dvě adresy liší a statická adresa IP už není aktivní, lze mapování adresy změnit ze statického na dynamické a potom aktualizovat adresu IP v databázi WINS.

Jestliže však používáte statické údaje trvale, měli byste zaškrtnutí políčka **Přenos (Přepsat jedinečný statický záznam dynamickým záznamem)** zrušit. Tímto krokem předejdete eventuálnímu přepsání statického záznamu dynamickou položkou WINS. Statický záznam totiž může mapovat název na adresu IP kritického serveru. Toto zabezpečení je nezbytné v první řadě v prostředích s více počítači se systémy UNIX, které se neregistrují pomocí služby WINS.

Možnost protokolování databáze WINS by měla být zapnuta Bude-li možnost protokolování databáze zapnuta, bude služba WINS dočasně protokolovat všechny aktivity, spojené s aktualizací záznamů, do souboru protokolu a teprve pak bude provádět vlastní změny v databázi. Povolením protokolování bude služba WINS schopna hromadně zpracovávat zaprotokolované změny a tyto změny pak zapisovat do databáze v předem stanovených intervalech. Zakážete-li funkci protokolování, bude služba WINS zapisovat do databáze každou nahlášenou změnu ihned po jejím přijetí.

Zpracovávání požadavků na registraci bude rychlejší, jestliže bude protokolování zakázáno, ale při tomto nastavení riskujete, že při výskytu nepředvídatelných potíží můžete ztratit záznamy o posledních několika aktualizacích.

Zaškrtnutí políčka **Protokolovat podrobně události do protokolu událostí** zapíná činnost služby v režimu podrobného výstupu a zpravidla se používá při výskytu problémů. Užití této funkce vyžaduje, aby příslušný počítač měl dostatek systémových prostředků. Chcete-li zlepšit výkon služby, měli byste tuto funkci vypnout.

Zavádění služby Microsoft WINS

Před zavedením služby Microsoft WINS ve vaší síti byste měli zvážit následující otázky. Každou z nich se budeme zabývat podrobněji v následujícím oddílu.

Určení optimálního počtu serverů služby WINS Jeden server může obsluhovat požadavky přeložení názvů v systému NetBIOS až pro 10 000 počítačů. Při rozhodování však musíte uvážit, jak budou umístěny směrovače a jaké bude rozmístění klientů v jednotlivých podsítích. Více informací na toto téma najdete v oddílu „Kolik serverů je zapotřebí“.

Návrh partnerských serverů WINS pro replikace Plánování replikace databáze WINS zahrnuje také rozhodnutí, zda budou servery WINS nakonfigurovány jako partnerské servery pro vyžádanou replikaci nebo jako partnerské servery pro nabízenou replikaci. Toto nastavení pak musíte přiřadit ke konfiguraci každého serveru. Více informací o rozhodování mezi vyžádanými nebo nabízenými replikacemi najdete v oddílu „Konfigurační nastavení replikace“.

Dopad přenosů WINS na pomalá připojení Přestože služba WINS podstatně omezuje všesměrové přenosy v a mezi jednotlivými místními podsítěmi, dochází zde k přenosům mezi jednotlivými servery a jejich klienty. Pokuste se odhadnout jejich počet, a to obzvláště ve směrovaných sítích TCP/IP. Kromě směrovaných přenosů musíte při konfiguraci replikačních přenosů mezi servery WINS a přenosů při registraci a obnovování názvů klientů v systému NetBIOS vzít v potaz také pomalá připojení (jako například připojení, vyskytující se v rozlehlých sítích). Více informací o tomto tématu najdete v oddílu „Přístup k síťovým přenosům“.

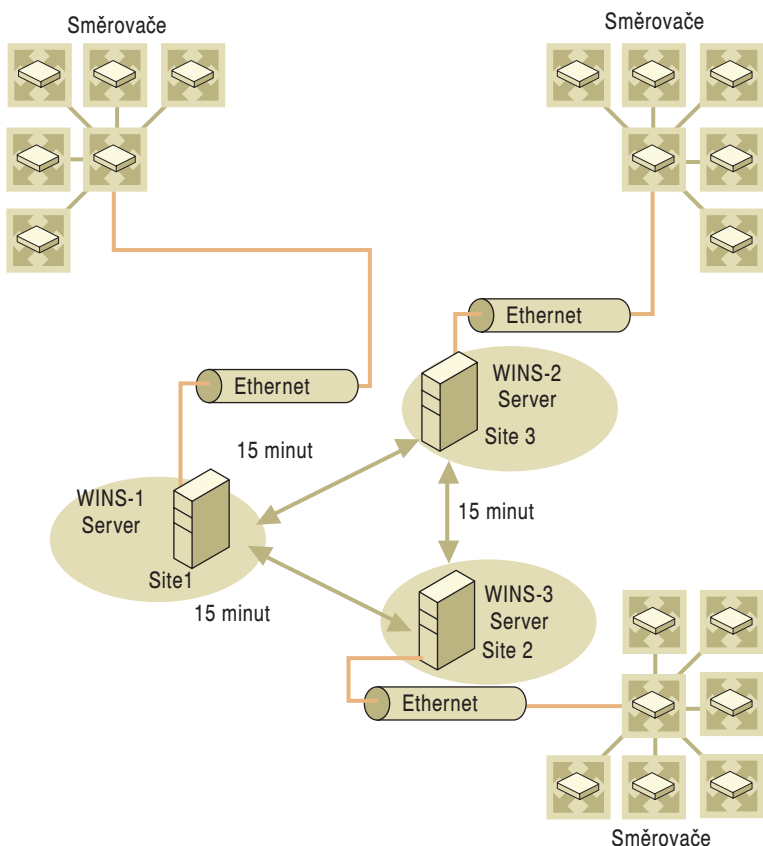
Nastavení funkce Odolnost proti chybám služby WINS v síti Aby byla instalace služby WINS úspěšná, musíte také vzít v úvahu důsledky vypnutí serveru WINS nebo jeho dočasného odpojení ze síťového provozu. K zotavení služby, k zálohování a redundanci použijte dodatečné servery WINS. Více informací o plánování instalace WINS odolné proti chybám najdete v oddílu „Odolnost serveru WINS proti chybám“.

Testování a úpravy naplánované instalace služby WINS Testováním výkonu vaší instalace služby WINS můžete snáze určit zdroj potenciálních problémů ještě dříve, než k nim vůbec dojde.

Příklady konfiguračního nastavení služby WINS

V příkladu na obrázku 7.20 je znázorněna středně velká společnost se dvěmi hlavními sídly (označené jako Site1 a Site3). Každé z nich obsluhuje 500 počítačů, a jsou spojeny pomocí relativně rychlých připojení. Tato společnost má kromě toho také více než 160 menších poboček. Z úsporných důvodů jsou některé z poboček konfigurovány jako koncentrátoři pro příslušnou oblast (jako například Site2).

Jednotlivé pobočky mohou mít svoje místní servery WINS, ale ve většině případů tomu tak nebude – jednoduše proto, že není potřeba samostatný server pro každou pobočku. Zmíněná společnost však zavedla do sítě oblastní servery WINS tam, kde náklady na přenosy registrací a dotazů překročily náklady na zavedení dalšího serveru. Po případném selhání oblastního serveru WINS lze místní názvy i nadále překládat pomocí mechanismu všesměrového vysílání.

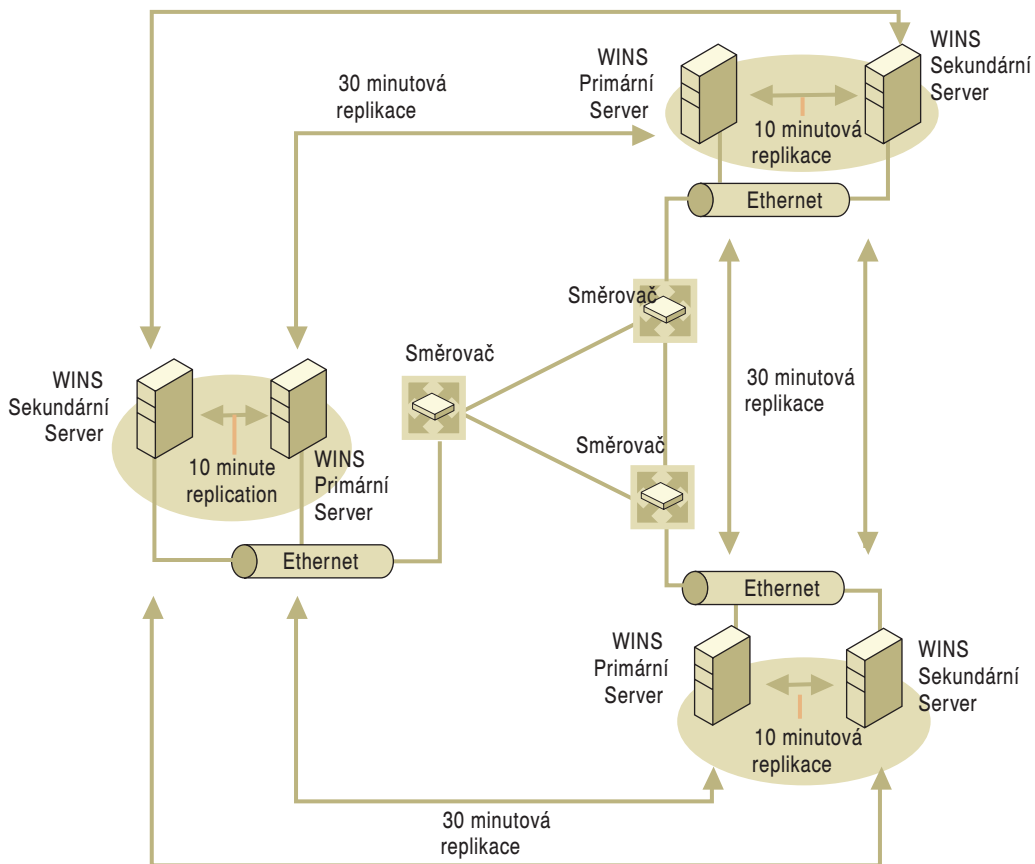


Obrázek 7.20: Typické rozmístění služby WINS.

K tomu, aby tato konfigurace fungovala bezchybně, nejsou oblastní servery WINS nezbytné. Poskytují však možnost optimalizace nákladů. Z pohledu efektivního využití sítě by se měli správci sítě vyvarovat zavádění oblastních serverů, kde to jen situace dovoluje, neboť tyto servery zvyšují dobu konvergence. Správci konfiguruji na všech hlavních síťových serverech (Server1 a Server3) oblastní servery WINS (například v Site2) jako partnerské servery pro replikace serverů WINS v hlavních sídlech (Site1 a Site3). Klienti v hlavním sídle mají jako primární server WINS konfigurovanou adresu IP místního serveru WINS a jako sekundární server WINS mají konfigurovanou adresu IP serveru WINS druhého hlavního sídla. Klienti v oblastních větvích mají jako primární server WINS adresu oblastního serveru WINS a jako sekundární server WINS adresu serveru WINS nejbližšího hlavního sídla.

Na obrázku 7.21 je znázorněno konfigurační nastavení sítě jiné vzorové společnosti. Jistě si povšimnete, že se od předchozí konfigurace liší zcela zásadně. Jedná se o rozsáhlejší podnikovou síť se třemi sídly, z nichž každé zahrnuje 5 000 klientů. Servery jsou připojeny pomocí několika spojení T1. Počet uživatelů ospravedlňuje existenci primárního i sekundárního serveru WINS v každém sídle. Klienti mají konfigurovány jak primární, tak sekundární servery WINS lokální. Polovina klientů má jako primární server konfigurován jeden místní server WINS a druhý server používá jako sekundární server

WINS. Druhá polovina klientů je konfigurována opačně. Toto nastavení zaručuje vyváženost zatížení při příjmu požadavků na registraci nebo při přijímání dotazů. Navíc je zde k okamžité dispozici možnost rychlého obnovení narušených dat.



Obrázek 7.21: Trojúhelníkové rozmístění služby WINS.

Místní servery WINS využívají velmi krátké 10minutové intervaly pro vyžádanou replikaci, takže všechny počítače ve stejné budově jsou dostupné už po 10 minutách od zaregistrování názvu nebo po jeho změně. Interval replikace mezi sídly může být delší – přibližně 30 minut – neboť většina uživatelů používá prostředky místních serverů.

Přístup k síťovým přenosům

Výkon celého systému WINS závisí na jiných síťových přenosech. Není-li server WINS umístěn v místní podsíti, ale někde v síti WAN, musí procházet všechny požadavky a jejich odpovědi frontami směrovačů, což způsobuje zejména ve špičkách značná zpoždění. Podstatná část šířky síťového pásma je také spotřebována při přenosu replikací.

V následujícím oddílu se budeme věnovat podrobně zprávám protokolu UDP/TCP. Tyto zprávy mohou být odesílány až po určení adresy MAC (Media Access Control) neboli adresy fyzického hardwaru. Je-li adresa IP uložena ve vyrovnávací paměti ARP, ne-

vygeneruje zpráva WINS novou zprávu ARP (protokol převodu adres). V opačném případě klient vyšle paket ARP pro překlad cílové adresy IP na adresu fyzickou, jestliže cíl je na stejné místní podsíti, nebo pro překlad adresy IP směrovače, jestliže cíl leží na vzdálené podsíti. Registrace probíhají zpravidla ve skupinách. Pro každou skupinu je vyžadována jedná zpráva ARP. Tato zpráva nezpůsobuje žádné přenosy v síti WAN.

Velikosti všech zpráv, jimiž se zabýváme v tomto oddíle, jsou udávány bez čísla ID oboru a vztahují se na síť Ethernet. Záhlaví zprávy (a tím pádem také celková délka) může být v sítích Token Ring, FDDI, WAN atd. jiná.

Klienti WINS generují čtyři následující základní zprávy:

- Registrace názvu,
- obnovení názvu,
- uvolnění názvu,
- dotaz na název.

Těmito čtyřmi zprávami se budeme podrobně zabývat v podkapitole „Klienti služby Microsoft WINS“.

Klient systému Windows 2000 WINS si proti klientům služby WINS zpravidla registruje více názvů rozhraní NetBIOS než jiní klienti. Požadavky registrace názvu, vygenerované počítačem se systémem Windows 2000, zahrnují následující:

- Součást Workstation,
- součást Server,
- název služby Messenger,
- název nebo názvy domény,
- název služby Replicator,
- název služby Browser,
- další názvy síťových programů nebo služeb.

Po připojení klienta služby WINS je odeslán požadavek registrace názvů služby Workstation, služby Server, služby Messenger a všech dalších služeb sítě Microsoft spuštěných na příslušném počítači. Znamená to, že když se klient služby WINS přihlásí k síti, vygenerují se nejméně tři požadavky registrace názvu a nejméně tři položky v databázi WINS.

Typické síťové přenosy

Požadavek registrace názvu je odeslán pro každý název systému NetBIOS, který daná aplikace používá. Aplikace vznesе požadavek ihned po spuštění (aplikace je zpravidla implementována jako služba). K tomu dochází obvykle po spuštění počítače. Klient může mít nejméně dva názvy počítače (jeden pro součást Workstation s posledním bajtem rovným hodnotě <00> a jeden pro službu Messenger s posledním bajtem rovným hodnotě <03>); název domény a uživatelský jméno (názevMessenger, poslední bajt <03>).

Server má zpravidla ještě další názvy, včetně názvu služby Server (stejný jako název počítače, ale s posledním bajtem rovným hodnotě <20>). Má také několik variant názvu domény (<1B> a <1D> pro prohlédávání a <1C> pro řadiče domény). Dále pak má účet služby Replicator, účet služby Systems Management Server atd. Požadavek registrace názvu obsahuje 110 bajtů. Kladná odpověď registrace názvu obsahuje 104 bajty.

Požadavek uvolnění názvu je odesílán v okamžiku zastavení služby, která si jej zaregistrovala. Zpravidla k tomu dochází při vypnutí počítače. Požadavek uvolnění názvu obsahuje 110 bajtů, zatímco odpověď registrace uvolnění názvu obsahuje 104 bajty.

Požadavek obnovení názvu (nazývaný také požadavkem aktualizace názvu) je po zaregistrování názvu odesílán v pravidelných intervalech. Požadavek obsahuje 110 bajtů, zatímco odpověď 104 bajty. Časový interval mezi odesláním jednotlivých požadavků závisí na implementaci klienta a na intervalu obnovení. Implementace služby WINS v systému Windows 2000 zajišťuje odesílání požadavků obnovení názvu v intervalech, rovných polovině intervalu obnovení, nastaveného na primárním serveru WINS. Po zastavení primárního serveru jsou požadavky obnovení názvu odesílány v intervalech určených sekundárním serverem WINS. Sekundární server ve skutečnosti zpracuje pouze polovinu pokusů o obnovení názvu. Druhá polovina je vždy odeslána na primární server. Je-li služba WINS na primárním serveru zastavena, pokus o obnovení názvu se nezdaří. Přesto však každý pokus generuje tři pakety.

Provoz dotazů na název závisí na aplikaci i na serveru. Aplikace se může od serveru odpojovat pravidelně a uvolňovat tak relace systému NetBIOS. Souborový server může kromě toho odpojovat nečinné relace. Různé aplikace se mohou připojovat k různým serverům. To s sebou přináší také přenosy dotazů na název. Požadavek s dotazem na název obsahuje 92 bajtů, odpověď obsahuje 104 bajtů.

Zatížení sítě replikací a ověřováním

Problém se zatížením sítě replikací a ověřováním je o něco složitější než běžné zatížení sítě, neboť servery služby WINS z důvodu odlehčení zátěže provádějí replikace a ověření dávkově. Kromě toho tyto procesy občas spouštějí dodatečné přenosy s výzvami ověření. Dochází k tomu, když jsou položky ověřovány u svých vlastníků.

Implementace replikace a ověření také vyžaduje základní zatížení při vytváření nebo rušení připojení pomocí protokolu TCP. Každý jedinečný název vyžaduje, aby server služby WINS odeslal a přijal data v rozsahu 12 až 50 bajtů. Jiné typy údajů o názvu jako například názvy skupin, které vytvářejí zátěž úměrně počtu svých klientů, mohou na serverech požadovat výměnu větších datových objemů. Vhodným konfigurováním intervalu replikace můžete snížit zatížení sítě při připojování. Budete-li však využívat trvalé připojení, sníží se zatížení na nulu.

Klientské přenosy ve směrovaných sítích

Při plánování přenosů klienty WINS v rozlehlých směrovaných sítích zvažte všechny důsledky zatížení sítě přenosy dotazů na název, požadavků registrace názvu a odpovědí mezi jednotlivými podsítěmi. Požadavky registrace názvu a odpovědi musí při každodenním spouštění počítačů procházet frontami přenosů přes směrovače a ve špičce mohou způsobit značné časové prodlevy.

Přenosy a topologie

Četnost přenosů byste měli na základě předchozího popisu chování klientů WINS být schopni předvídat. Přesto však při tomto odhadu musíte také mít na zřeteli topologii sítě a návrh nebo konfiguraci jejích směrovačů. V této situaci se může stát, že bude nemožné předpovědět zatížení sítě, neboť směrovače mohou být navrženy nebo konfigurovány tak, aby autonomně směrovaly přenosy i na základě jiných podmínek než zatížení sítě.

Kolik serverů je zapotřebí

Počet potřebných serverů služby WINS využívaných v podnikové síti systému Windows NT závisí na dvou okolnostech: na počtu klientů WINS na jeden server a na topologii sítě. Počet uživatelů, které může server obsloužit, závisí na modelu využití, na ukládání dat a na schopnosti zpracování dat serverem. Je možné, že za účelem využívání služby WINS budete muset inovovat hardware serveru.

Počet klientů na jeden server

Jeden server služby WINS může obsluhovat požadavky na přeložení názvu systému NetBIOS až 10 000 klientů, což je počet, jenž může uspokojit požadavky menší sítě. Chcete-li však zajistit vyšší odolnost proti chybám, měli byste ve své síti konfigurovat ještě alespoň jeden server se systémem Windows 2000, jenž bude využíván jako sekundární (nebo záložní) server služby WINS.

Budou-li v síti využívány dva servery WINS, měly by být také konfigurovány jako partnerské servery pro replikace. V případě běžné replikace mezi dvěma servery byste měli konfigurovat jeden server jako partnerský server pro vyžádanou replikaci a druhý server jako partnerský server pro nabízenou replikaci. Replikace můžete konfigurovat ručně nebo je můžete konfigurovat automaticky. K tomu stačí zaškrtnout políčko **Povolit automatickou konfiguraci partnerského serveru** na kartě **Upřesnit** v dialogovém okně **Partnerský server pro replikaci**.

Výkon serveru WINS

Server služby WINS by měl být vždy vyhrazeným zařízením. Neměl by být současně řadičem domény, poštovním serverem nebo ještě něčím jiným. Měl by mít výkonný diskový subsystém jako diskové pole RAID. Obecně se dá říci, že, není-li to nezbytné, neměly by se rozmísťovat služby WINS na řadiče domény nebo na servery, které plní v síti jiné úlohy.

Server WINS může zpravidla zaregistrovat 1 500 názvů za minutu nebo odpovědět na 4 500 dotazů za minutu. Konzervativně se doporučuje, aby byl v síti každý jeden server WINS konfigurován pro 10 000 počítačů. Uvedený údaj vychází právě z těchto statistických údajů. Při návrhu implementace služby WINS byste měli vycházet z kritického scénáře, kdy by mohlo dojít k tomu, že všechny počítače po výpadku napájení pokusí o registraci v jednom okamžiku (budou spuštěny najednou).

Výkon serveru služby WINS zlepšují dvě okolnosti:

1. Server WINS, osazený dvěma procesory, zaručuje zvýšení výkonu skoro o 25 procent.
2. Vyhrazená disková jednotka podstatně zkracuje dobu, nezbytnou pro vytvoření odpovědi na replikaci.

Po vytvoření serveru WINS v podnikové síti intranet můžete upravit i délku intervalu obnovení. Prodloužením tohoto intervalu můžete také zrychlit odezvu serveru na přichozí požadavky. Interval obnovení můžete nastavit hned při první konfiguraci serveru, ale změnit jej můžete také na kartě vlastností **Partnerský server pro replikace**.

Konfigurační nastavení replikace

Správné konfigurování replikací je podstatou efektivního využívání služby WINS. Nej důležitější vlastnosti vhodného nastavení jsou uvedeny v následujících oddílech.

Automatická konfigurace partnerských serverů pro replikaci

Server WINS lze konfigurovat tak, aby automaticky uznával ostatní servery WINS jako své partnerské servery pro replikaci. V případě, že server využívá funkci automatické konfigurace partnerských serverů pro replikaci, zjistí jejich existenci ihned po jejich připojení k síti a automaticky je přidá do seznamu partnerských serverů pro replikaci.

Automatická konfigurace je možná díky tomu, že po připojení k síti se každý server služby WINS ohlašuje pomocí opakovaného vícesměrového vysílání. Tyto zprávy jsou odeslány v podobě zpráv IGMP na adresu skupiny výběrového vysílání 224.0.1.24 (obvyklá adresa IP výběrového vysílání, rezervovaná pro servery služby WINS).

Používá-li služba WINS automatickou konfiguraci partnerských serverů pro replikaci, monitoruje právě přenosy těchto vícesměrových vysílání. V případě, že zjistí existenci nového serveru, vykoná automaticky následující kroky:

- Přidá adresy IP objevených serverů do svého seznamu partnerských serverů pro replikaci,
- konfiguruje všechny objevené servery jako partnerské servery pro nabízenou a vyžádanou replikaci,
- konfiguruje server tak, aby vyžádaná replikace s novými servery probíhala každé dvě hodiny.

Je-li vzdálený server objeven na základě odběru vícesměrového vysílání a takto přidán do seznamu jako partnerský server pro replikaci, bude z tohoto seznamu automaticky odebrán, bude-li služba WINS zastavena správně. Chcete-li, aby informace o automaticky přidávaných partnerských serverech pro replikaci zůstala v seznamu natrvalo, musíte partnerský server konfigurovat ručně.

Ručně můžete konfigurovat replikaci s ostatními servery služby WINS v prostředí konzoly systémového řízení WINS.

Automatická konfigurace partnerských serverů pro replikaci je nejužitečnější v prostředí s jedinou podsítí. Může však být vhodná i v situacích, kdy je dosažitelnost přenosu vícesměrového vysílání WINS rozšířena příslušným konfigurováním směrovačů mezi jednotlivými podsítěmi.

Vzhledem k tomu, že vícesměrové vysílání mezi servery služby WINS zatěžuje síťový provoz, doporučuje se používat funkci automatické konfigurace partnerských serverů pro replikaci pouze v těch případech, kdy jsou v dosažitelné síti konfigurovány maximálně tři servery služby WINS.

Replikace mezi nedůvěryhodnými doménami

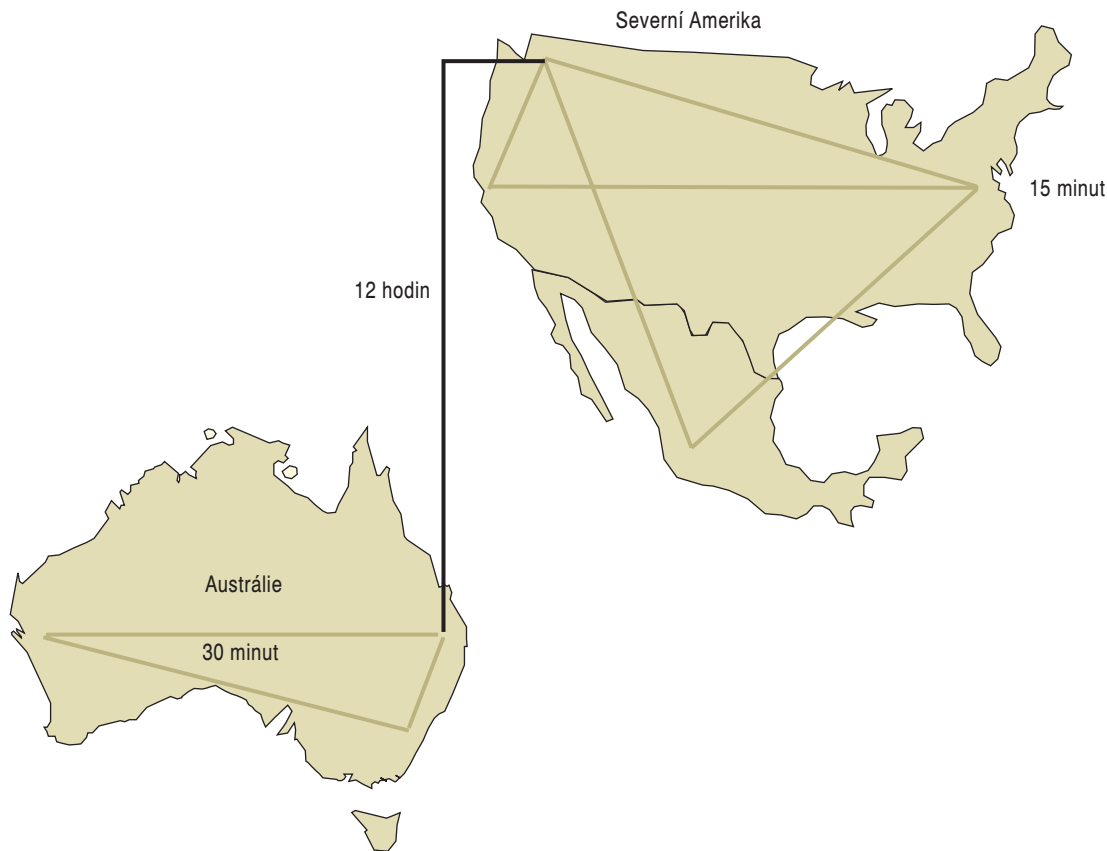
Replikaci WINS lze mezi servery umístěnými v nedůvěryhodných doménách provádět bez požadavku na platný uživatelský účet v nedůvěřující doméně. Při konfiguraci takového typu replikace musí správci obou serverů pomocí konzoly systémového řízení WINS konfigurovat opačný server WINS pro umožnění replikace se vzdálenou doménou.

Replikace v rámci sítě WAN

Nastavení vhodného intervalu replikace vyžaduje určitou rozvahu. Databáze serveru WINS by měla být replikována dostatečně často, aby zastavení jednoho serveru služby WINS neovlivnilo spolehlivost mapovacích informací v databázích příslušných serverů WINS. Samozřejmě že také nebudete chtít, aby nastavený interval narušil propustnost sítě, k čemuž by mohlo dojít, kdyby byl nastaven jako příliš krátký.

Musíte vzít v úvahu také topologii své sítě. Pokud síť obsahuje větší počet rozbočovačů, připojených prostřednictvím relativně pomalých propojení sítě WAN, je třeba interval replikace konfigurovat tak, aby po těchto připojeních probíhaly replikace méně často než v případě rychlých propojení. Tím podstatně omezíte zatížení pomalých připojení a zamezíte vzniku sporů mezi přenosem replik a přenosem klientských dotazů na název.

Prohlédněte si příklad sítě, ve které servery služby WINS v ústřední síti LAN replikují své záznamy každých 15 minut, zatímco servery WINS na odlišných rozbočovačích sítě WAN replikují své záznamy každých 30 minut. Servery na rozdílných světadílech replikují své záznamy dokonce pouze dvakrát za den. Obrázek 7.22 názorně ukazuje rozdíly v četnosti provádění replikací.

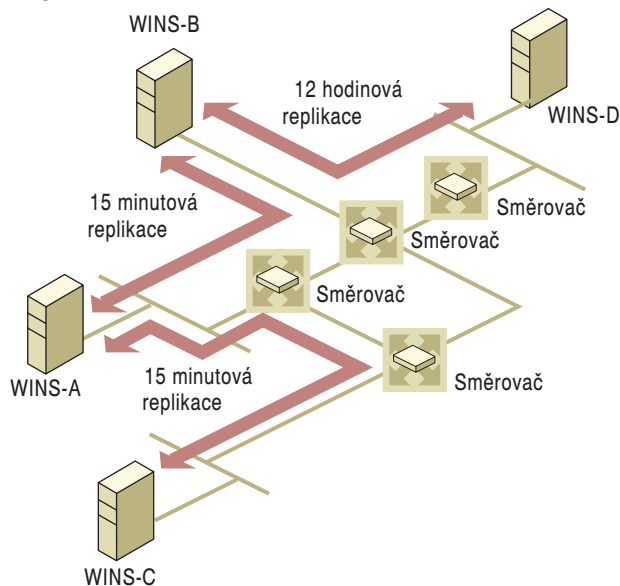


Obrázek 7.22: Replikace záznamů v rozsáhlé podnikové síti.

Konfigurace jiných podnikových sítí mohou zahrnovat ještě více zón, v nichž interní replikace probíhají na konstantní bázi trvalých připojení nebo v krátkých časových intervalech (každých 10-30 minut). Tím je doba konvergence udržována na spodní hranici. Servery, které propojují dvě z těchto zón, mohou synchronizovat své záznamy v hodinových nebo jednodenních intervalech.

Doba konvergence replikace

Při rozmístění serverů služby WINS musíte zvolit dobu konvergence, přijatelnou pro provoz své sítě. Na obrázku 7.23 je znázorněna síť se servery služby WINS a s nastaveným intervalem replikace jejich databází. Tato vzorová konfigurace sítě ukazuje, jakým způsobem může interval replikace mezi jednotlivými servery WINS ovlivnit dobu konvergence.



Obrázek 7.23: Intervaly replikace ve směrované síti TCP/IP.

Pokud klient WINS zaregistruje svůj název na serveru WINS-C, mohou se ostatní klienti dotázat na jeho název serveru WINS-C, jenž jim poskytne mapování název-adresa. Klienti WINS, dotazující se kteréhokoli jiného serveru WINS, budou dostávat zápornou odpověď do té doby, dokud nebude údaj ze serveru WINS-C replikován na servery WINS-A, WINS-B a WINS-D.

Server WINS-C je konfigurován tak, aby spouštěl replikaci poté, co počet aktualizací přesáhne mezní hodnotu nabízené replikace nebo po vypršení intervalu replikace partnerského serveru pro vyžádanou replikaci, serveru WINS-A. Počet aktualizací je souhrnem změn položek v databázi a je nastaven jako spouštěcí mechanismus nabízené replikace. (V tomto případě je server WINS-A konfigurován jako partnerský server pro vyžádanou replikaci s 15minutovým intervalem. Nepoužívá tedy pro spuštění replikace nějaký konkrétní počet aktualizací, jako je tomu u serveru WINS-C.)

V našem příkladu je údaj replikován pouze v případě, že dojde k vypršení intervalu vyžádané replikace, ale i po této synchronizaci nebudou dotazy na servery WINS-B a WINS-D vyřízeny kladně. Interval replikace, nastavený na serveru WINS-B, se rovná 15 minut. Interval replikace serveru WINS-D je 12 hodin. Nyní si vypočítejte dobu konvergence:

$$12 \text{ hodin} + (2 \cdot 15 \text{ minut}) = 12,5 \text{ hodiny}$$

Přesto však může dojít také k tomu, že požadavek přeložení názvů uspěje i před uplynutím doby konvergence. V našem příkladu k tomu dojde tehdy, jsou-li záznamy replikovány kratší cestou než kritickou. Může k tomu dojít, dosáhne-li počet aktualizací mezní hodnoty ještě před vypršením intervalu replikace. Příným důsledkem této situace je časnější replikace nových záznamů. Čím delší je cesta replikace, tím delší je také doba konvergence.

Příklad odolnosti serveru WINS proti chybám

Databáze serveru WINS poskytuje služby odolné proti chybám, neboť je replikována mezi větším počtem serverů WINS v sítích LAN nebo WAN. Tento návrh replikované databáze zabraňuje uživatelům jedné sítě v registraci duplicitních názvů počítačů v systému NetBIOS. Obecně se dá říci, že i malé sítě mohou obsahovat víc než jeden server WINS, aby bylo možné rozdělit zatížení při zpracování dotazů na název nebo požadavku registrace názvu. Samozřejmě, že více serverů poskytuje také možnost pro kontrolu, zálohování nebo zotavení databáze po chybě.

Chyba serveru služby WINS může mít podobu dvou následujících selhání:

- **Selhání serveru** Na serveru se může vyskytnout chyba nebo může být dočasně zastaven kvůli údržbě.
- **Selhání sítě** Může dojít k zastavení činnosti směrovačů nebo propojených stanic.

Selhání jednoho serveru v rámci jedné sítě ovlivňuje chod více serverů WINS. Vzorová směrovaná síť, kterou si můžete ještě jednou prohlédnout na obrázku 7.23, obsahuje čtyři samostatné fyzické segmenty, oddělené směrovači a čtyři servery WINS. Každý segment má svůj server WINS, který poskytuje služby primárně místním klientům tohoto segmentu. Tři ze serverů (WINS-A, WINS-B a WINS-C) jsou propojeny pomocí směrovačů, které jsou součástí samostatné topologie vysokorychlostního propojení sítě LAN. Čtvrtý server, WINS-D, je umístěn ve vzdáleném segmentu, využívajícím pomalé připojení sítě WAN.

V tomto příkladu by selhání serveru WINS-A nebo WINS-B mohlo ovlivnit distribuci názvů systému NetBIOS. Údaje by už dále nebyly replikovány ze serveru WINS-C na WINS-D, ani naopak. Protože pro aktualizované klienty nemusí dále souhlasit adresa IP a název, další klienti nemusí být schopni se k aktualizovaným klientům připojit. Rozšíříte-li možnost replikace také mezi servery WINS-B a WINS-C, můžete konfiguraci vylepšit pro případ selhání serveru WINS-A. Když přidáte navíc možnost replikace mezi servery WINS-D a WINS-C, zvýšíte odolnost proti chybám i pro případ, že by došlo k selhání serveru WINS-B.

Selhání samostatného vedení mezi servery A, B a C nemůže chod sítě WINS ohrozit, neboť příslušné směrovače by v tomto případě přenosy přesměrovaly. I když toto řešení není příliš efektivní, porovnáme-li jej s plně funkčním síťovým řešením, bude služba WINS fungovat relativně spolehlivě. Přesto však k rozdělení sítě dojde po selhání vedení mezi servery WINS-B a WINS-D. Vzhledem k tomu, že takové selhání by znemožnilo další síťové přenosy, potřebuje tato konfigurace ještě navíc vyžádané záložní propojení mezi servery WINS-D a WINS-C. Toto propojení by mělo umožnit infrastrukturu směrovačů přesměrovat replikační přenosy WINS.

Na obrázku 7.23 jsou všechny směrovače potenciálními body selhání. Stane-li se to, bude celá síť rozdělená na nespolupracující samostatné články.

Segmentová konfigurace

Dojde-li k selhání propojení nebo směrovače mezi dvěma podsítěmi, může dojít jak k přerušení probíhající replikace, tak k jejímu zamezení v budoucnu. Segmentová konfigurace služby WINS je však schopna zajistit celou řadu služeb plně funkčního systému. Klienti mohou tak jako obvykle překládat adresy podle názvu. Místní servery WINS nebo všesměrové vysílání zaručují přeložení většiny dotazů na název. V takových podmínkách nelze přeložit pouze nově zaregistrované názvy, a to ještě v případech, kdy se jedná o vzdáleně registrované názvy. Údaje nejsou při čištění databáze odstraněny, neboť služba se nemůže spojit s jejich vlastníkem. Chcete-li rychle obnovit činnost rozdělené sítě, instalujte službu WINS na jiném počítači, když hardware obvyklého serveru WINS selže, a obnovte databázi vynucením replikace od replikačního partnera.

Zvýšení odolnosti proti chybám

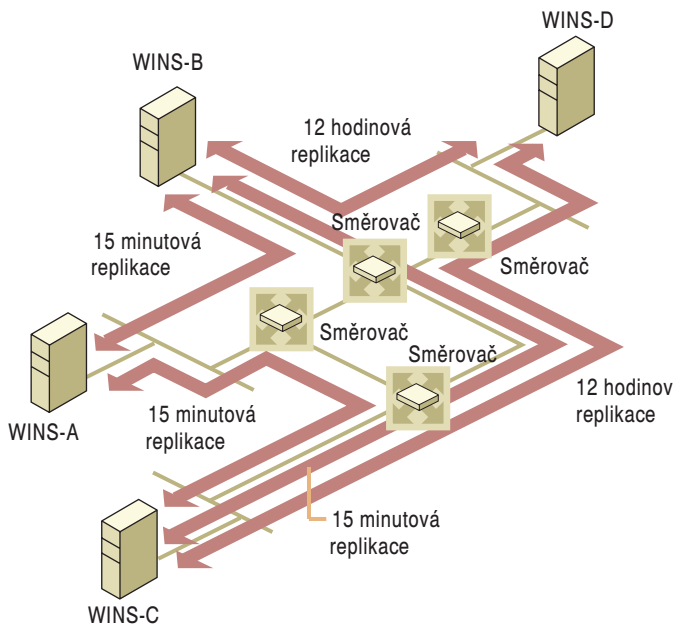
Systémy Windows 2000 a Windows 98 poskytují dodatečné prostředky pro zvýšení stupně odolnosti proti chybám. Umožňují totiž, aby si klient mohl nastavit více než dva servery WINS (až 12) pro každé rozhraní buď prostřednictvím služby **DHCP** nebo nastavením **WINS**, dostupného v Systémových nástrojích. Dodatečné servery služby WINS překládají názvy pouze v případě, že nereaguje ani primární, ani sekundární server WINS. Pokud na dotaz odpoví některý z dodatečných názvových serverů, uloží si klient do vyrovnávací paměti adresu serveru, který mu na dotaz odpověděl a napříště jej bude používat vždy, když selže spojení s primárním a sekundárním serverem. Tato vlastnost je ve výchozím nastavení povolena v systému NetBT. Je-li tato funkce spuštěna na mnoha počítačích, dochází k nadměrnému vytváření duplicitních názvů dotazů, což velmi snižuje výkon.

Při nastavování odolnosti proti chybám musíte určit maximální časový interval, o němž předpokládáte, že bude dostatečně dlouhý, aby jej nepřekročil žádný plánovaný výpadek serveru WINS. Přizpůsobte svůj odhad délce plánovaných i neplánovaných zastavení. Zvažte také, jaké důsledky bude mít pro klienty WINS dočasné zastavení služby názvového serveru. Vhodnou údržbou a nastavením sekundárního názvového serveru můžete také minimalizovat dopad výpadku jednoho ze serverů, i když důsledky nelze odstranit zcela. Kromě toho lze odolnost proti chybám zvýšit také clusteringem – shlukováním. Více informací o tomto tématu najdete v jednom z předchozích oddílů, „Clustering – seskupování“.

Zatížení sítě duplicitními replikacemi

Jemné doladění intervalů replikace může v případě sítě WAN ušetřit část šířky síťového pásma. Zkvalitněním příkladu síťového řešení z obrázku 7.23 lze dosáhnout řešení, patrného z obrázku 7.24. Toto nové řešení není pouze odolnější proti chybám, ale také zkracuje dobu konvergence. Na obrázku 7.23 byla nejdelší cesta replikace mezi servery WINS-C přes WINS-A a WINS-B na WINS-D. Nyní nejdelší cesta replikace prochází ze serveru WINS-A nebo WINS-C přes server WINS-B na WINS-D, což zaručuje dobu konvergence 12 hodin a 15 minut.

Budou-li nastaveny intervaly vyžádaných replikací mezi servery WINS-C a WINS-B na 15 minut, bude synchronizace serverů WINS-A, WINS-B a WINS-C vždy na přiměřené úrovni. Repliky nebudou nikdy vyžádány víc než dvakrát a mezi servery bude vždy zkopírována pouze replika s vyšším číslem ID verze. Když si server WINS-B vyžádá replikaci přímo na serveru WINS-C, nebude už vyžadovat přímou synchronizaci této repliky ze serveru WINS-A.



Obrázek 7.24: Zkvalitněné řešení otázky replikace.

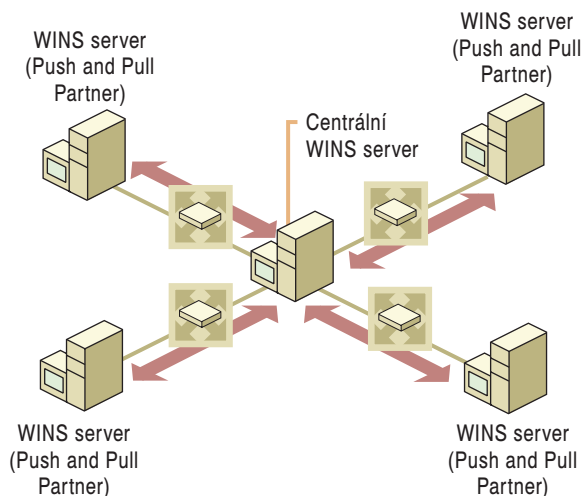
Servery WINS-D a WINS-B mohou vyžadovat repliky na serveru WINS-C prostřednictvím propojení mezi servery WINS-B a WINS-C za předpokladu, že server WINS-B bude vyžadovat repliku na serveru WINS-C, a server WINS-D bude potom vyžadovat repliku na serveru WINS-C. Toto řešení zvyšuje zátěž propojení mezi servery WINS-B a WINS-C. Abychom se tomuto problému vyhnuli, je třeba konfigurovat server WINS-D tak, aby vyžadoval repliku nejprve na serveru WINS-B a teprve pak ověřoval nové záznamy na serveru WINS-C. Interval vyžádané replikace mezi servery WINS-D a WINS-C zůstává stále 12 hodin.

Aby bylo zaručeno, že bude replikace spuštěna vypršením intervalu replikace a nikoli dosažením mezního počtu aktualizací, musíte konfigurovat počet nabízených aktualizací na serverech WINS-D a WINS-C tak, aby tato hodnota podstatně překračovala 12hodinový interval vyžádané replikace. Budou-li tyto hodnoty příliš nízké, může mezní počet aktualizací spustit neočekávanou replikaci.

Partnerské servery pro replikace a konfigurace sítě

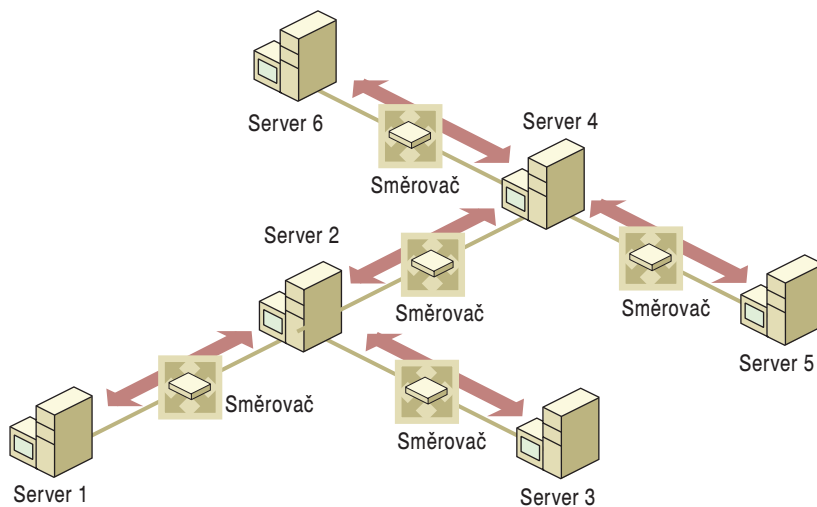
To, zda konfiguruje další názvový server služby WINS jako partnerský server pro nabízenou replikaci nebo partnerský server pro replikaci vyžádanou, závisí na několika okolnostech včetně specifické konfigurace názvových serverů na příslušném síťovém serveru nebo toho, zda je partnerský server součástí rozsáhlé sítě (WAN) či toho, jak je důležitá okamžitá distribuce změn do dostupné sítě.

V paprskovitém rozmístění sítě s centrálním rozbočovačem můžete konfigurovat jeden názvový server WINS jako centrální, zatímco všechny ostatní servery budou buď partnerskými servery pro nabízenou replikaci a současně partnerskými servery pro vyžádanou replikaci tohoto centrálního serveru. Řešení zaručuje to, že bude databáze WINS na všech serverech obsahovat adresy všech uzlů rozlehlé sítě.



Obrázek 7.25: Replikace zajišťovaná pomocí centrálního serveru služby WINS.

Partnerské servery pro replikace můžete konfigurovat také jinak, a to tak, aby splňovaly specifické požadavky vaší sítě. Podívejte se na příklad: Na obrázku 7.26 má Server1 jako jediného partnera nastaven Server2, ale Server2 má tři partnery. Díky tomu Server1 získá všechny repliky přímo ze Serveru2, ale Server2 získává potřebné informace ze Serveru1, Serveru3 a ze Serveru4.



Obrázek 7.26: Replikace v síti modelu T.

Pokud bude například Server2 odebírat vyžádané repliky ze Serveru3, musíte zajistit, aby byl Server3 partnerským serverem pro nabízenou replikaci. V případě, že bude vyžadovat repliky na Server3, musíte zajistit, aby byl Server3 partnerským serverem pro vyžádanou replikaci.

Vyřazení služby WINS z provozu

Může se stát, že budete chtít v prostředí systému Windows 2000 omezit nebo dokonce zcela vyřadit službu WINS ze své sítě. Procesu odstranění instalovaných serverů WINS ze síťového prostředí se obecně říká vyřazení z provozu. Aby mohl být tento proces úspěšný, je třeba nejprve zjistit odpověď na následující otázky.

- Pracují ještě v síti některé počítače se staršími verzemi operačních systémů Windows nebo Windows NT?
- Jsou na některém z podnikových počítačů spouštěny aplikace starších verzí operačního systému Windows nebo dokonce aplikace systému MS-DOS (jako například síťové nástroje příkazového řádku), které stále vyžadují existenci služby WINS?

Dostanete-li na některou z těchto otázek kladnou odpověď, musíte ve své síti servery služby WINS ponechat i nadále, neboť budou zajišťovat zpětnou kompatibilitu se staršími verzemi klientů a aplikací. V případě záporných odpovědí můžete spustit proces návrhu a implementace vyřazení služby WINS ze své sítě.

Současně s vyřazením služby WINS ze sítě musíte jako primární názvové servery všech počítačů se systémem Windows implementovat servery DNS systému Windows 2000. Více informací o implementaci názvových serverů DNS najdete v kapitole „Servery DNS“. Jakmile nastavíte servery DNS, můžete službu WINS vyřadit ze sítě. Postupujte podle následujících kroků.

Změňte konfiguraci služby WINS klientských počítačů

Rozhodnete-li se odstranit ze své sítě servery WINS, musíte nejprve změnit konfigurace jejich klientů tak, aby přestali registrovat a obnovovat svoje názvy pomocí serverů služby WINS. Klienti registrují v databázi služby WINS své názvy na základě nastavení protokolu TCP/IP. Změnu konfigurace lze v tomto případě vykonat dvěma způsoby:

- V případě klientů konfigurovaných ručně na používání protokolu TCP/IP odeberte adresy všech serverů WINS ze seznamu nastavení TCP/IP všech jeho síťových připojení.
- V případě klientů dynamicky konfigurovaných pomocí služby DHCP změňte konfiguraci na příslušném serveru DHCP (včetně všech možností konfigurace serveru, oboru nebo klienta) tak, aby klientům nedistribuoval nastavení možnosti 44. Toto nastavení poskytuje klientům seznam adres IP serverů WINS.

Ověřte konfiguraci serverů DNS

Během odebírání serverů WINS z konfigurace klientských počítačů ověřte, zda jsou tyto počítače konfigurovány tak, aby mohly k překladu názvu používat servery DNS. Jakmile zjistíte, že všechny počítače používají server DNS, můžete ze sítě odebrat servery WINS.

Klienti registrují názvy pomocí služby DNS na základě individuální konfigurace protokolu TCP/IP. Tuto konfiguraci zabezpečit dvěma způsoby:

- V případě klientů konfigurovaných ručně na používání protokolu TCP/IP přidejte adresy pro primární a sekundární servery DNS v dialogovém okně Nastavení TCP/IP každého síťového připojení klienta.

- V případě klientů dynamicky konfigurovaných pomocí služby DHCP změňte konfiguraci na příslušném serveru DHCP (včetně všech možností konfigurace serveru, oboru nebo klienta) tak, aby klientům distribuoval nastavení možnosti 6. Toto nastavení předává klientům seznam adres IP serverů DNS.

Vyřazení serverů WINS

Po změně nastavení klientů, kteří nyní používají názvové servery služby DNS, můžete postupně vyřadit všechny servery WINS.

Pomocí konzoly systémového řízení WINS označte všechny záznamy vyřazovaného serveru (vlastníka) za uvolnění. Tato informace o zneplatnění záznamů je při další replikaci přenesena na ostatní servery WINS, které provedou aktualizace svých databází. Jakmile je informace o zneplatnění přenesena na ostatní servery, budou takto označené záznamy po vypršení časového limitu zániku ze všech databází automaticky vyjmuty.

Nyní přichází čas k vlastnímu vyřazení serveru. Klepněte na tlačítko **Start**, přesuňte ukazatel nad nabídku **Programy** a potom nad nabídku **Systémové nástroje** kde klepněte na příkaz **WINS**. Jestliže se požadovaný server nezobrazuje ve stromu konzoly, můžete jej tam přidat.

Ve stromu konzoly označte server WINS, který chcete vyřadit, klepněte na tlačítko **Aktivní registrace**. Z nabídky **Akce** zadejte příkaz **Odstranit vlastníka**. V dialogovém okně **Odstranit vlastníka** klepněte v seznamu **Odstranit následujícího vlastníka:** na adresu IP toho serveru WINS, který chcete vyřadit. Pokud není požadovaný server spuštěn místně na daném počítači, může načtení záznamu vybraného serveru nějakou dobu trvat.

Ve skupinovém rámečku **Způsob odstranění vybraného vlastníka a jeho záznamů:** klepněte na položku **Replikovat odstranění záznamu na ostatní servery (označit záznam jako neplatný)** a stiskněte tlačítko **OK**. Po zobrazení výzvy o potvrzení označení záznamu za neplatný klepněte na tlačítko **Ano**.

Ve stromu konzoly klepněte na příkaz **Partnerské servery pro replikace**. Z nabídky **Akce** zadejte příkaz **Replikovat**. Jakmile ověříte, že byly všechny záznamy, označené v předchozím kroku za neplatné, replikovány na ostatní partnerské servery, zastavte server WINS a odeberte jej ze seznamu.

Upozornění: Před vyřazením serveru WINS se ujistěte, že byla všem počítačům, které byly dříve nakonfigurovány jako klienti, změněna konfigurace primárních a sekundárních serverů. Tato změna je nezbytná pouze v případě, že tito klienti používají k registraci a překladu názvu právě servery služby WINS.

Označení záznamů za neplatné zaručuje, že servery označené jako partnerské servery pro replikace budou správně aktualizovány tak, aby mohly odpovídajícím způsobem uvolnit příslušné záznamy. Kdyby nebyl status zneplatnění odpovídajícím způsobem odeslán, museli byste na ostatních serverech ručně označit všechny záznamy, u nichž k replikaci stavu zneplatnění nedošlo.

Služba WINS umožňuje vzdálené mazání záznamů také na počítačích s operačním systémem Windows NT verze 4.0, s aktualizací Service Pack 4 (SP4) nebo novější.

Omezení a přesměrování přenosů WINS

Většina sítí musí používat službu WINS i po zavedení systému Windows 2000 do většiny počítačů. Jakmile jste jednou přistoupili k vyřazování serverů WINS, může několik dalších úprav v konfiguraci snížit počet potřebných serverů WINS, stejně tak jako omezit přenosy WINS.

Jednou z doporučených možností na straně serveru je povolit na všech zónách DNS, kde jsou používány servery DNS standardu Microsoft, prohledávání WINS. Tato metoda umožňuje serverům DNS používat službu WINS k vyhledávání názvů klientů a k ukládání často vyžadovaných názvů WINS do mezipaměti. Více informací o konfiguraci vyhledávání WINS v zónách DNS najdete v oddíle „Příklad vyhledávání WINS“.

Posledním krokem při vyřazování služby WINS z provozu jsou změny na straně klienta, které lze provést na počítačích se systémem Windows 2000. Změny spočívají v zákazu rozhraní NetBIOS nad protokolem standardu TCP/IP. Tuto vlastnost budete využívat pouze v případech, kdy budete chtít zabránit přenosům dotazů na názvy systému NetBIOS nebo požadavkům registrace na jejich zdroji, tzn. na klientském počítači. Přesto však ve většině sítí zůstává potřeba alespoň omezeného využívání služby WINS. Přinejmenším v nejbližší budoucnosti. Proto se tedy ve většině případů nedoporučuje zakazovat rozhraní NetBIOS nad protokolem TCP/IP.

Interoperabilita

Služba WINS může sdílet informace a funkce se systémy DHCP a DNS. Nejdůležitější otázky této spolupráce jsou obsahem této podkapitoly.

Používání serverů DHCP se servery WINS

Budete-li používat současně servery DHCP i WINS, uvažujte také o využití dodatečných možností oboru DHCP, používaných jednak pro přiřazování typu uzlu služby WINS, ale i pro identifikaci primárních a sekundárních serverů WINS pro klienty služby DHCP. Upravte tyto možnosti pro každou fyzickou podsít, v níž jsou služby DHCP a WINS společně implementovány.

Určete srovnatelnou dobu trvání zapůjčení jak pro službu DHCP, tak pro službu WINS. Budou-li se tyto hodnoty u obou služeb podstatně lišit, může to výrazně zvýšit zatížení sítě, neboť zde bude probíhat zvýšený počet přenosů zapůjčení mezi oběma službami. Toto zatížení se může výrazně projevit pouze v případech, kdy nevyužíváte výchozího nastavení obou zmíněných služeb, ale rozhodli jste se nastavit dobu trvání zapůjčení pro každou službu samostatně.

Vytvořte rezervace DHCP pro hostitelské počítače systému Windows 2000

Staticky mapované počítače se systémem Windows 2000 mohou způsobovat určité problémy, pokud nejsou pravidelně vypínány a spouštěny a náhodou dojde k poškození jejich počátečního registračního záznamu v databázi WINS. Když vytvoříte pro počítače se systémem Windows 2000 rezervace DHCP, budete spravovat mnohem spolehlivější a mnohem ovladatelnější síť. Konfigurujte řadiče domény se systémem Windows 2000 a členské servery domény jako klienty služby DHCP s rezervovanými adresami protokolu TCP/IP.

Rezervaci DHCP můžete na serveru DHCP zajistit pomocí adresy MAC (Media Access Control) neboli adresy fyzického síťového hardwaru. Tato rezervace zajišťuje to, že bude počítačům se systémem Windows 2000 po přihlášení do systému přidělena serverem DHCP vždy stejná adresa IP. Registraci WINS pro klienta služby DHCP můžete obnovit zadáním příkazu `ipconfig /renew` na příkazovém řádku nebo restartováním počítače. Obě tyto procedury zaručují opravu porušeného záznamu registrace WINS.

Nastavení odolnosti proti chybám na počítačích využívajících službu WINS

Chcete-li zvýšit odolnost proti chybám, vzniklým na základě selhání spojení, upravte konfiguraci počítačů, závislých na službě WINS, umístěných v jiné podsíti. Postupujte přitom podle následujících kroků. Primárním serverem WINS těchto počítačů by měl být vždy místní server služby WINS. Nastavení sekundárního serveru by mělo ukazovat na sekundární rozbočovač WINS. Počítače se systémem Windows 95 nebo Windows NT Workstation odesílají jednosměrové zprávy na sekundární server WINS vždy, když primární server WINS neobsahuje požadovaný název systému NetBIOS. V ideálním případě bude sekundární server WINS umístěn v odlišné budově a bude připojen k odlišné napájecí síti než primární server WINS.

Používání služby DNS spolu se službou WINS

Služba WINS spolupracuje v systému Windows 2000 s implementací služby DNS. Služba DNS (Domain Name System) je protokolem sítě Internet a TCP/IP, jenž poskytuje škálovatelnou a dynamickou databázovou službu. DNS v systému Windows 2000 registruje a překládá názvy domény DNS, používané jak v soukromých sítích, tak v síti Internet. Díky tomu lze poskytovat službu názvových serverů DNS síťovým klientům tak, jak to popisuje standard DNS. Více informací o službě DNS najdete v kapitolách „Úvod do DNS“ a „Služba Windows 2000 DNS“.

V systému Windows 2000 tvoří, stejně jako v systému Windows NT verze 4.0, implementace služby DNS se službou WINS nedílný celek. Toto provedení umožňuje klientům, nespolupracujícím se službou WINS, překládat názvy systému NetBIOS dotazováním se na serverech DNS. Správci sítě nyní mohou odebírat statické údaje o klientech standardu Microsoft také ve starších zónách serverů DNS, a to ve prospěch dynamické integrace služeb WINS a DNS. Pokud například klientský produkt od jiného dodavatele bude chtít získat přístup ke stránce WWW na serveru WWW, jenž využívá služby DHCP a WINS, stačí, že odešle dotaz na server DNS. Server DNS odešle dotaz na server služby WINS a přeložený název bude neprodleně vrácen klientovi. Dokud nebyly tyto dvě služby sjednoceny, bylo zcela nemožné, aby byly při dynamickém přidělování adres IP spolehlivě překládány názvy i v těchto situacích.

Možnosti nastavení spolupráce WINS se službou DNS

Pokud většina vašich klientů používá názvy systému NetBIOS a vy používáte službu DNS v systému Windows 2000, přemýšlejte o povolení funkce vyhledávání WINS na serverech DNS. Povolíte-li vyhledávání WINS na serverech DNS, přeloží služba WINS všechny názvy, které překlad DNS není schopen vyhledat. Záznamy vyhledávání WINS a obrácené vyhledávání WINS-R lze používat výhradně se službou DNS v systému Windows 2000. Používáte-li servery DNS jiných dodavatelů, použijte program Správce DNS a zakažte přenášení záznamů WINS na tyto DNS servery, neboť ty nepodporují vyhledávání WINS.

Pokud má většina počítačů v síti nainstalovaný systém Windows 2000, uvažujte o inovaci také zbývajících starších klientů WINS na systém Windows 2000 a o nastavení služby DNS jako jediné metody překladu názvů. Budete-li používat jednotnou službu lokátoru názvů a prostředků, bude činnost podpůrných nástrojů, včetně síťové názvové služby, velmi zjednodušena. Více informací o přechodu z prostředí zkombinovaných služeb WINS a DNS na prostředí využívající výhradně systém Windows 2000 DNS najdete v jednom z předchozích oddílů „Vyřazení služby WINS z provozu“.

Doporučené postupy

Udržení různých služeb, dobře fungujících společně, je ve většině případů také otázkou vypořádání se s jejich vnitřními problémy (nikoli s jejich sdílenými prvky). V tomto oddíle se seznámíte se základními postupy, které by měly usnadnit jejich vzájemnou spolupráci.

Konsolidujte podsítě

Jestliže máte více podsítí v malých vzdálených pobočkách, uvažujte o sjednocení poboček na jednu adresu podsítě. Tuto změnu můžete provést přepnutím na asynchronní režimu přenosu (ATM) nebo změnou konfigurace sítě VPN (Virtual Private Network). Po konsolidaci podsítí pod jednu adresu podsítě můžete používat k překladu názvu místní všesměrové vysílání a teprve pak bude hledání přecházet do sítě WAN, kde se spojí se serverem WINS.

Změna klienta na uzel M povoluje všesměrově vysílat místně požadavky na prostředky ještě dříve, než se pokusí za účelem překladu názvu systému NetBIOS spojit se serverem WINS. Toto nastavení může pomoci ke snížení celkového počtu přenosů zpráv služby WINS, obzvláště pak přenosů v síti WAN.

Aktualizace starších klientů

U klientů se systémem Windows for Workgroups, kteří používají zásobník protokolu TCP/IP-32 standardu Microsoft, aktualizujte soubory Vredir a Vserver na poslední verze. Tyto soubory jsou umístěny na kompaktním disku Windows NT Server 4.0 (revize 3.11b).

Odstraňování problémů spojených se službou WINS

V této podkapitole se budeme věnovat některým základním krokům spojeným s odstraňováním základních problémů. Najdete zde také popis postupu při obnově a opětovném sestavení databáze WINS.

Některé základní problémy lze zjistit po výskytu následujících okolností:

- Správce se nemůže připojit k serveru WINS pomocí konzoly systémového řízení WINS. Za obrazovce se zobrazí zpráva „Server RPC není k dispozici“.
- Pomocná služba TCP/IP NetBIOS na klientském počítači WINS je vypnuta a nelze ji opětovně spustit.
- Služba WINS je vypnuta a nelze ji spustit.

Nejprve musíte zajistit chod příslušných služeb. Následující kroky proto vykonajte jak na serveru WINS, tak na klientu WINS:

1. Ověřte, zda jsou spuštěny služby WINS.

2. Pokud některá ze služeb na daném počítači není spuštěna, spusťte ji.

Nelze-li služby správně spustit, použijte panel **Správa počítače**, dostupný z ikony **Nástroje pro správu**, umístěné ve složce Panel nástrojů. Pomocí tohoto nástroje ověřte sloupec stavu služeb a pokuste se je restartovat ručně. Nelze-li službu spustit ani tímto způsobem, pokuste se pomocí programu Prohlížeč událostí prohlédnout protokol událostí a určit příčinu selhání.

Na klientských počítačích by se ve sloupci **TCP/IP NetBIOS Helper Service** měl zobrazit řetězec „Spuštěno“. Na serverech WINS by se řetězec „Spuštěno“ měl zobrazit ve sloupci **Služba Windows Internet Name Service (WINS)**.

Běžné problémy

V tomto oddíle se seznámíte s běžnými problémy služby WINS a se způsoby, jak se s nimi vypořádat.

Kde mohu najít příčinu chybových zpráv „duplicitní název“? Ověřte, zda se v databázi tento název už nevyskytuje. Najdete-li statický název, odstraňte jej z databáze primárního serveru daného klienta.

Alternativně zaškrtněte políčko **Přenášet (Přepíše jedinečný statický záznam záznamem dynamickým)** v dialogovém okně **Vlastnosti partnerských serverů pro replikace** serveru WINS. Nyní lze aktualizovat statické záznamy dynamickými registracemi (poté, co služba WINS úspěšně vyzve klienta k uvolnění adresy).

Kde mohu najít příčinu chybových zpráv „Síťová cesta nenalezena“, zobrazovaných na počítači klienta? Ověřte, zda je název uložen v databázi. Není-li přítomen, ověřte, zda počítač používá typ uzlu B. Je-li tomu tak, přidejte do databáze záznam se statickým mapovacím názvem počítače.

Je-li počítač nakonfigurován jako uzel P, uzel M nebo uzel H a je-li jeho adresa IP jiná než ta v databázi WINS, mohlo dojít k nedávné změně adresy, ale tato změna se ještě neprojevila v replikovaných databázích partnerských serverů. Chcete-li zjistit nejnovější změny, spusťte replikaci na serveru, na němž byl klient zaregistrován. Tím vyvoláte nabízenou replikaci s okamžitým přenosem záznamů z místní databáze WINS.

Proč nelze spouštět vyžádané ani nabízené replikace serveru s jiným serverem WINS? Jsou-li servery umístěny za směrovači, ujistěte se, že problémem není ztráta připojení k síti, selhání směrovače nebo zprostředkovatelského propojení.

Zajistěte, aby byly všechny servery správně konfigurovány buď jako partnerské servery pro vyžádanou replikaci, nebo partnerské servery pro nabízenou replikaci.

Dejme tomu, že se dva servery WINS jmenují WINS-A a WINS-B. Pokud server WINS-A vyžaduje replikaci záznamů na serveru WINS-B, přesvědčte se, že váš server je partnerským serverem pro nabízenou replikaci s serverem WINS-B. Stejně tak je tomu v případě, kdy váš server nabízí replikaci serveru WINS-B. V tomto případě musí být partnerským serverem serveru WINS-B pro vyžádanou replikaci.

Při určování stávající konfigurace partnerských serverů pro replikace používejte konzolu systémového řízení WINS, jejíž pomocí můžete ověřit sloupec Typ v seznamu partnerských serverů pro replikace. Bude-li to zapotřebí, můžete změnit typ partnerského serveru. Ujistěte se také, zda není na některých zprostředkovatelských zařízeních jako směrovač či bezpečnostní brána zablokován port TCP 42.

Proč se trvale nedaří vytvořit záložní kopie databáze WINS? Ujistěte se, že je cesta k záložní kopii databáze nastavena na místní diskovou jednotku serveru WINS. Služba WINS nemůže zálohovat databázové soubory na vzdálené diskové jednotky.

Odstraňování problémů s klienty WINS

Nejběžnějším problémem, souvisejícím s klienty WINS, je nezdar při překladu názvu. Nezdaří-li se překlad názvu u klienta, pokuste se odpovědět na následující otázky a určit tak zdroj problému.

Je požadovaný název názvem systému NetBIOS nebo DNS? Názvy systému NetBIOS obsahují maximálně 15 znaků a jejich struktura je jiná než v případě názvů systému DNS. Názvy systému DNS jsou zpravidla delší a k oddělení každého stupně domény používají tečky. Například název systému NetBIOS „PRINT-SRV1“ a delší název systému DNS „print-srv1.example.microsoft.com“ mohou obsahovat odkaz na stejný prostředek počítače se systémem Windows 2000, síťový tiskový server, jenž je nakonfigurován tak, aby mohl používat oba tyto názvy.

Kdyby byl v předchozím příkladu klientem použit krátký název, mohl by systém Windows 2000 nejprve použít názvové služby systému NetBIOS, jako je WINS nebo všesměrové vysílání NetBT. Pokud k chybě došlo proto, že klient použil delší název (jako v příkladu názvu s tečkami), selhání při překladu názvu způsobuje pravděpodobně server služby DNS.

Používá klient vhodnou aplikaci nebo verzi systému Windows, která je vyžadována pro správný překlad názvu službou WINS? Službu WINS nebo NetBIOS nad protokolem TCP/IP (NetBT) nevyžadují všechny počítače, ba ani všechny aplikace. Kdyby název, který se nepodařilo přeložit, byl adresou URL, zadanou v prohlížeči sítě WWW nebo v klientovi FTP, nebo kdyby tento název byl součástí adresy zadané v programu elektronické pošty v síti Internet, byl by pravděpodobným původcem problémů server DNS.

V ryzím prostředí systému Windows 2000 může DNS nahradit službu WINS. Ryzí prostředí existuje pouze v případě, že na počítači klienta, ale také na serveru, poskytujícím prostředek (tedy na počítači, který klient hledá pomocí názvu), je spuštěn operační systém Windows 2000. Musí být také spuštěna služba Active Directory. Ve všech ostatních případech, včetně těch, kdy klient i server používají dřívější verze operačního systému Windows nebo MS-DOS, se jedná o smíšené prostředí.

Ve smíšeném prostředí může docházet k selhání překladu názvu, když klienti potřebují získat přístup ke sdíleným prostředkům, nepublikovaným prostřednictvím služby Active Directory, jako jsou starší souborové nebo tiskové servery, nebo pro dokončení přihlášení a prohledávání domén Windows NT. Jako příklady aplikací, které mohou klienti používat a které potřebují asistenci služby WINS při překladech názvů, mohou posloužit například složka Místa v síti, funkce programu Průzkumník Připojit síťovou jednotku, příkaz net (Net.exe) spolu s četnými parametry příkazového řádku jako net use či net view.

Lze na klientském počítači používat službu WINS a je tento počítač správně nakonfigurován?

Nejprve ověřte, zda konfigurace klienta umožňuje používání jak protokolu TCP/IP, tak protokolu WINS. Konfiguraci klientských nastavení služby WINS lze upravit ručně pomocí administrátorského nastavení konfigurace protokolu TCP/IP klienta nebo dynamicky pomocí serveru DHCP, jenž poskytuje klientovi jeho konfigurační nastavení TCP/IP automaticky.

Ve většině případů lze službu WINS na počítačích se staršími verzemi operačních systémů společnosti Microsoft používat po nainstalování a konfigurování protokolu TCP/IP. V operačním systému Windows 2000 lze volitelně zakázat používání systému NetBIOS nad protokolem standardu TCP/IP (NetBT). Zakážete-li používání NetBT, nebude moci klient využívat ani službu WINS.

Ověřte také, zda má klientský počítač nastavené platné adresy IP. K ověření konfigurace adres IP klienta použijte nástroj příkazového řádku s parametrem **ipconfig /all**. (Výstup programu můžete na obrazovce stránkovat modifikovaným příkazem **ipconfig /all | more**.)

Ve výstupním okně příkazového řádku zkontrolujte, zda má klient platnou adresu IP, platnou masku podsítě, výchozí bránu a primární a sekundární server WINS.

Vyskytne-li se v konfiguraci klienta nějaký chybný údaj, můžete použít příkaz **ipconfig /renew**, který si vynutí obnovení konfigurace IP klienta pomocí serveru DHCP (nebo můžete upravit konfiguraci TCP/IP klienta ručně).

Funguje spojení mezi klientem a nastavenými servery WINS? Chcete-li si ověřit, zda klient má k serveru WINS přístup TCP/IP na základní úrovni, pokuste se nejprve použít příkaz PING s adresou serveru WINS.

Přibližme si to na konkrétním příkladu. Pokud klient používá primární server WINS na adrese 10.0.0.1, запиšte na příkazovém řádku příkaz **ping 10.0.0.1**. Nejste-li si jistí adresou IP příslušného serveru, stačí, když jej zjistíte po zadání příkazu **ipconfig /all | more**.

Jestliže server WINS odpovídá na přímý příkaz PING s adresou IP, použijte jiný nástroj příkazového řádku, **nbtstat -RR**, a to jak na klientském počítači, tak na vyžadovaném serveru. Tento příkaz zajistí, že klientské služby WINS na obou počítačích odešlou serveru WINS požadavky uvolnění a obnovení názvu a zaregistrují si tak svoje názvy.

Pokud server WINS nereaguje na příkaz PING, bude zdrojem problémů pravděpodobně síťové spojení mezi klientem a serverem WINS. V takových případech postupujte podle standardních kroků při odstraňování potíží. Více informací najdete v kapitole „Řešení problémů protokolu TCP/IP“.

Je primární nebo sekundární server WINS schopen poskytovat svoje služby klientům WINS? Na primárním nebo sekundárním serveru klienta spusťte Prohlížeč událostí nebo konzolu systémového řízení WINS a ověřte, zda je server WINS spuštěn. V případě, že je, vyhledejte název posledního požadavku klienta a ověřte, zda se v databázi vůbec nachází.

Pokud příslušný záznam v databázi chybí, zjistěte, zda je správně nastavena replikace a zda tato funkce mezi servery funguje správně. Více informací najdete v oddílu „Odstraňování potíží s replikací WINS“.

Odstraňování potíží se servery WINS

Nečastějším problémem serverů WINS je nemožnost překladu názvu pro klienty. Nepodaří-li se serveru název pro klienty přeložit, zjistí se to jedním ze dvou způsobů:

- Server odešle zápornou odpověď na dotaz klienta jako například „Název nenalezen“.
- Server odešle klientovi kladnou odpověď, ale odpověď obsažená ve zprávě je chybná.

Příčinou většiny problémů se službou WINS jsou nesprávné nebo chybějící položky v odpovědích na dotazy. Aby k těmto nejběžnějším problémům nedocházelo, prohlédněte si doporučené postupy při zavádění a správě serverů WINS.

Budete-li postupovat přesně podle instrukcí poradce při potížích, bude ve většině případů problém rychle vyřešen. Většina problémů služby WINS začíná selháním dotazu klienta, takže byste měli s odstraňováním potíží začínat právě u něj. Více informací najdete v oddíle „Odstraňování problémů s klienty WINS“.

Zjistíte-li, že problém nevznikl na počítači klienta, pokuste se odpovědět na následující otázky, které by v další fázi mohly vést k odstranění zdroje problému.

Je server WINS schopen poskytovat svoje služby klientům WINS? Na primárním nebo sekundárním serveru klienta, který nemůže vyhledat název, spusťte Prohlížeč událostí nebo konzolu systémového řízení WINS a ověřte, zda je server WINS spuštěn. V případě, že je spuštěn, vyhledejte název posledního požadavku klienta a ověřte, zda se v databázi vůbec nachází.

V případě opakovaného selhání serveru WINS nebo při výskytu chyb v záznamech o registraci, můžete použít technik zotavení databáze WINS, které napomohou při obnovení operací WINS. Více informací najdete v podkapitole „Odstraňování problémů spojených se službou WINS“.

Pokud příslušný záznam v databázi chybí, zjistěte, zda je správně nastavena replikace a zda tato funkce mezi servery funguje správně. Více informací najdete v oddílu „Odstraňování potíží s replikací WINS“.

Mohou problémy se statickým mapováním ovlivnit záznam o názvu? Obecně se nedoporučuje používat statická mapování u klientů, kteří mohou využívat funkci systému WINS dynamické aktualizace informací o názvu a adrese. V případě, že získaná informace je chybná nebo zastaralá, ověřte, zda záznam náhodou není statickou položkou. Je-li tomu tak, můžete jej aktualizovat následujícím způsobem:

1. V dialogovém okně **Vlastnosti partnerských serverů pro replikace** zaškrtněte políčko **Povolit přenesení** (viz obrázek 7.10). To umožní službě WINS přepsat statický záznam záznamem dynamickým.
2. Editujte statické mapování a upravte přidruženou adresu.
3. Odstraňte statický záznam z databáze WINS.

Probíhá replikace skutečně mezi všemi servery? V některých implementacích se používá pouze jednosměrné replikace, kde jsou příslušné servery konfigurovány buď jako partnerský server pro nabízenou replikaci, anebo jako partnerský server pro vyžádanou replikaci. V takových situacích pak může docházet k případům, kdy názvy nejsou replikovány na všechny servery stejnoměrně. Více informací najdete v oddíle „Odstraňování potíží s replikací WINS“.

Potíže se serverem WINS mohou indikovat například následující chybové stavy:

- Správce se nemůže připojit k serveru WINS pomocí konzoly systémového řízení WINS a při každém pokusu se zobrazí chybové hlášení.
- Služba klienta WINS nebo serveru WINS je vypnuta a nelze ji znova spustit.

Odstraňování potíží s replikací WINS

Mnoho problémů se službou WINS lze opravit odstraněním potíží replikací WINS, kdy k chybě překladu názvu dochází mezi klientem a servery. V některých případech, jako

například v rozlehlých podnikových sítích se složitým návrhem replikací a s velkým počtem používaných serverů WINS, mohou být problémy s přesností nebo dostupností názvů spojeny s dodržением včasné replikace databáze WINS v rámci celé sítě.

Po prozkoumání běžných možných příčin problémů, spojených s klienty a servery WINS, se pokuste odpovědět na následující otázky. Tyto odpovědi vám mohou pomoci v dalším vyhledávání zdroje potíží v replikované síti WINS.

Je model replikace ve vaší síti nastaven správně? Obecně se vůbec nedoporučuje, aby bylo v jedné síti použito více než 20 serverů WINS. Lepších výsledků a také snazší správy dosáhnete, když přejdete na model topologie paprskovitého rozmístění sítě s centrálním rozbočovačem, kdy můžete navrhnout replikovanou síť WINS, která využívá služeb partnerských serverů pro nabízenou a vyžádanou replikaci mezi každým rozbočovačem a k němu paprskovitě připojenými členskými servery.

Pokud samostatné řešení typu paprskovitě rozmístění sítě s centrálním rozbočovačem přesáhne maximální doporučený počet serverů WINS, měli byste se spojit s pracovníky odborné pomoci společnosti Microsoft a pokusit se společně najít řešení, jak snížit počet aktuálně využívaných instalací služby WINS. V případě rozsáhlejších podnikových instalací bývá efektivním řešením zpravidla přechod na model více sítí s centrálními rozbočovači.

Velmi zřídka se může stát, že budete muset nastavit vztahy typu partnerský server jen pro nabízenou replikaci a partnerský server jen pro vyžádanou replikaci. Při zavádění těchto konfigurací byste měli pečlivě zvážit jejich všechny možné důsledky. Minimálně byste měli vytvořit spolehlivé podpůrné procedury pro případ, kdy by bylo zapotřebí ručně spustit replikaci mezi servery konfigurovanými pro omezené partnerství při replikacích.

Zvyšuje se číslo ID verze položek WINS při replikaci na všechny servery? Číslo ID verze je zvyšováno v databázi WINS každým serverem, který vlastní a registruje záznam o názvu. Číslo ID verze je hexadecimální hodnotou, uloženou v databázi s každým záznamem o názvu, a služba WINS ji používá při sledování verze při synchronizaci záznamů s databázemi ostatních serverů.

Číslo ID verze jsou zvyšována pouze při určitých typech změn. Například při obnovení záznamu služba WINS zpravidla tuto hodnotu nezvyšuje. V případě jiných změn jako změna adresy IP, je tato hodnota naopak zvyšována téměř vždy.

Kdyby došlo k tomu, že číslo ID verze není u některého záznamu o názvu zvyšováno systematicky, použijte k ručnímu zvýšení této hodnoty konzolu systémového řízení WINS nebo některý z nástrojů příkazového řádku. Tím by měl být problém odstraněn.

Nástroje pro odstraňování potíží se serverem

Při odstraňování potíží se serverem jsou užitečné zejména dva nástroje: Hotfix.exe a Srvinfo.exe. Program Hotfix.exe poskytuje specifické informace o tom, které rychlé opravy jsou momentálně na serveru nainstalovány. Tento program je umístěn na serveru FTP společnosti Microsoft a je obsažen v rychlých opravách. Program Srvinfo.exe podává podrobné informace o daném serveru, například to, které služby nebo ovladače jsou momentálně používány. Podává také informace o disku vzdáleného serveru. Tento nástroj je součástí Soupravy prostředků systému Windows 2000 (Windows 2000 Resource Kit).

Při přípravách k odstranění potíží se dále doporučuje ověřit si, zda mají oddíly serveru dostatek místa pro soubor výpisu chyb, konfigurovat kritické servery tak, aby používaly symboly při procedurách odstraňování potíží – ladění a výpisu paměti do souboru.

Odstraňování potíží se serverem WINS

Databáze WINS je pro překlad názvu v systému WINS zcela nepostradatelná. Dojde-li k porušení této databáze, nahlédněte do oddílu „Obnovení dat pomocí replikace“ (dříve v této kapitole).

Prostředky

V této podkapitole najdete referenční materiály o názvech systému NetBIOS, včetně specifikací všech jedinečných a skupinových přípon. Dále zde najdete příkazy modulů Netshell, RFC a další dokumentaci WINS.

Názvy systému NetBIOS

Síťové součásti standardu Microsoft, jako například Workstation nebo služba Server, povolují zadání 15místného názvu systému NetBIOS. Šestnáctý znak názvu (00-FF hex) je rezervován pro určení typu prostředku. V následujícím oddílu najdete některé příklady používání názvů systému NetBIOS součástmi standardu Microsoft.

Odkazy na názvy systému NetBIOS

Uživatel může ve všech operačních systémech společnosti Microsoft, které využívají názvy systému NetBIOS, určit prvních 15 znaků názvu. 16. znak názvu (00-FF hex) je však vždy rezervován pro určení typu prostředku.

Tabulky 7.19 a 7.20 obsahují dodatečné podrobnosti o názvech NetBIOS, používaných síťovými součástmi Microsoft při registrování jedinečných nebo skupinových názvů.

Tabulka 7.19: Jedinečné názvy systému NetBIOS

Formát	Popis
název_počítače[00h]	Registrován službou Workstation na klientském počítači WINS. Obecně se tomuto názvu říká název počítače systému NetBIOS.
název_počítače[03h]	Registrován službou Messenger na klientském počítači WINS. Klient používá tuto službu při odesílání a příjmu zpráv. Tento název je při odesílání zpráv v síti zpravidla připojen k názvu počítače NetBIOS klientského počítače WINS a k názvu uživatele přihlášeného k tomuto počítači.
název_počítače[06h]	Registrován službou směrování a vzdáleného přístupu na klientském počítači WINS (po spuštění služby Směrování a vzdálený přístup).

Formát	Popis
Název_domény[1Bh]	Registrován všemi řadiči domény systému Windows 2000 Server, spuštěnými jako hlavní prohlížeč domény. Tento název je používán k umožnění vzdáleného prohlédávání domén. Po odeslání dotazu na server WINS na tento název vrátí WINS server adresu IP počítače, jenž má registrován tento název.
název_počítače[1Fh]	Registrován službami NetDDE (Network Dynamic Data Exchange). Zobrazí se pouze tehdy, je-li na počítači spuštěna služba NetDDE.
název_počítače[20h]	Registrován službou Server na klientském počítači WINS. Tato služba se využívá k poskytování servisních bodů proto, aby klient WINS mohl sdílet soubory v síti.
název_počítače[21h]	Registrován službou Klient směrování a vzdáleného přístupu na klientském počítači WINS (po spuštění služby Klient směrování a vzdáleného přístupu).
název_počítače[BEh]	Registrován službou Agent monitorování sítě a zobrazí se pouze po spuštění této služby na klientském počítači služby WINS. Je-li název počítače kratší než 15 znaků, doplní existující název symboly plus (+) které prodlouží název na požadovaných 15 znaků.
název_počítače[BFh]	Registrován službou monitorování sítě (zahrnutou v Microsoft® Systems Management Server). Jestliže je název počítače kratší než 15 znaků, budou k němu přidány symboly plus (+) které prodlouží název na požadovaných 15 znaků.
jméno_uživatele[03h]	Uživatelská jména aktuálně přihlášených uživatelů jsou registrována v databázi WINS. Každé uživatelské jméno je registrováno službou Server tak, aby uživatel mohl přijímat všechny příkazy net send odeslané na jeho jméno. V případě, že se přihlásí více uživatelů se stejným jménem, pouze první počítač přihlášený s tímto jménem uživatele toto jméno registruje.

Tabulka 7.20: Názvy skupin systému NetBIOS

Formát	Popis
název_domény[00h]	Registrován službou Workstation, aby bylo možné přijímat všesměrová vysílání prohlížeče z počítačů se systémem LAN Manager.
název_domény[1Ch]	Registrován pro použití řadiči domény v doméně, může obsahovat nejvýše 25 adres IP
název_domény[1Dh]	Název název_domény[1Dh] je registrován, aby jej mohl používat hlavní prohlížeč. V podsíti je pouze jeden hlavní prohlížeč. Záložní prohlížeče používají tento název při komunikaci s hlavním prohlížečem při získávání seznamu dostupných serverů. Servery WINS vždy vracejí kladnou odpověď na požadavek registrace názvu název_domény[1D], i když tento název nezaregistrují ve své databázi. Proto tedy, když je server WINS dotazován na název_domény[1D], obsahuje jeho odpověď vždy adresu všesměrového vysílání, která přinutí klienta přeložit název pomocí všesměrového vysílání.

Formát	Popis
název_skupiny[1Eh]	Název normální skupiny. Všechny počítače, nakonfigurované jako prohlížeče sítě mohou pro výběr hlavního prohlížeče všesměrově vysílat na tento název a sledovat vysílání směrované na tento název. Staticky mapované názvy skupiny používají tento název k vlastní registraci v síti. Když server WINS přijme dotaz na název zakončený znakem [1E], vrátí vždy adresu všesměrového vysílání, platnou v místní síti žádajícího klienta. Klient pak může tuto adresu použít k všesměrovému vysílání členům skupiny. Tyto všesměrové zprávy jsou určeny pro místní podsít a neměly by být přenášeny za směrovače.
název_skupiny[20h]	Název speciální skupiny, zvané skupina Internet, je registrován servery WINS k identifikaci skupin počítačů, vytvořených ke správním účelům. Například název "tiskskup" by mohl být registrován jako název, určující správní skupinu tiskových serverů.
[01h][01h] __MSBROWSE__ [01h][01h]	Registrován hlavním prohlížečem každé podsítě. Když server WINS přijme dotaz na tento název, vrátí vždy síťovou adresu všesměrového vysílání, platnou v místní síti žádajícího klienta.

Příkazy modulu NetShell

Příkazy modulu NetShell pro službu WINS jsou alternativním způsobem správy ke správě pomocí konzoly a v některých specifických situacích jsou velmi užitečné. Nabízejí plně funkční nástroj příkazového řádku pro správu serverů WINS.

Při správě serverů WINS v síti WAN můžete příkazy NetShell používat například v interaktivním režimu pomocí příkazové výzvy nástroje NetShell pro lepší správu serverů WINS přes pomalá síťová spojení.

Tabulka 7.21 obsahuje seznam příkazů, které můžete použít na příkazovém řádku modulu NetShell při správě serverů WINS. Příkazový řádek tohoto modulu se liší od příkazového řádku systému Windows 2000. Všechny příkazy jsou opatřeny poznámkami o přepínačích a použití. Tyto poznámky můžete zobrazit po zadání příslušného názvu následovaného přepínačem /?.

Tabulka 7.21: Příkazy modulu NetShell

Příkaz	Popis
list	Zobrazí seznam všech dostupných příkazů WINS.
dump	Vypíše konfiguraci serveru WINS do výstupního okna.
add name	Registruje název na serveru.
add partner	Přidává k serveru další partnerský server pro replikace.
add pngserver	Přidává seznam nežádoucích serverů aktuálního serveru.
check database	Ověřuje konzistentnost databáze.
check name	Ověřuje seznam záznamů o názvu a porovnává jej se sadou serverů WINS.

Příkaz	Popis
check version	Ověřuje konzistentnost čísla ID verze.
delete name	Odstraní z databáze serveru registrovaný název.
delete partner	Odstraní ze seznamu partnerských serverů pro replikace zadaný partnerský server.
delete records	Vymaže nebo označí za neplatné všechny nebo některé záznamy v databázi na serveru.
delete owner	Vymaže seznam vlastníků a jejich záznamů.
delete pngserver	Vymaže ze seznamu všechny nebo vybrané nežádoucí servery (PNG). Repliky z PNG serverů nejsou v průběhu replikace akceptovány.
init backup	Iniciuje zálohování databáze WINS.
init import	Zahájí import záznamů ze souboru LMHOSTS.
init pull	Zahájí replikaci a odešle aktivaci vyžádání do jiného serveru WINS.
init pullrange	Iniciuje replikaci a vyžádá si rozsah záznamů z jiného serveru WINS.
init push	Zahájí replikaci a odešle aktivaci nabídky do jiného serveru WINS.
init replicate	Zahájí replikaci databáze s partnerskými servery pro replikaci.
init restore	Zahájí obnovení databáze ze souboru.
init scavenge	Zahájí úklid databáze WINS pro daný server.
init search	Zahájí vyhledávání zadaného záznamu v databázi serveru WINS.
reset counter	Vynuluje statistické údaje serveru.
set autoperpartnerconfig	Nastaví informace o automatické konfiguraci partnerského serveru pro replikaci pro daný server.
set backuppath	Nastaví parametry zálohování pro daný server.
set burstparam	Nastaví parametry ovládání shlukového přenosu pro daný server.
set logparam	Nastaví možnosti databáze a protokolování události.
set migrateflag	Nastaví příznak přenesení pro daný server.
set namerecord	Nastaví hodnoty intervalů a časových limitů registrace pro daný server, které určují četnost obnovy, mazání a ověřování záznamů
set periodicdbchecking	Nastaví parametry periodické kontroly databáze pro daný server.
set pullpartnerconfig	Nastaví konfigurační parametry pro zadaný server pro vyžádanou replikaci.
set pushpartnerconfig	Nastaví konfigurační parametry pro zadaný server pro nabízenou replikaci.
set pullparam	Nastaví výchozí parametry serveru pro vyžádanou replikaci pro daný server.

Příkaz	Popis
set pushparam	Nastaví výchozí parametry serveru pro nabízenou replikaci pro daný server.
set replicateflag	Nastaví replikační příznak pro daný server.
set startversion	Nastaví ID počáteční verze dané databáze.
show browser	Zobrazí všechny záznamy [1Bh] hlavních prohlédávačů domény.
show database	Zobrazí záznamy pro určený server
show info	Zobrazí konfigurační informace serveru.
show name	Zobrazí podrobné informace pro konkrétní záznam na serveru.
show partner	Zobrazí servery pro vyžádanou nebo nabízenou repliku nebo všechny tyto servery pro daný server.
show partnerproperties	Zobrazí výchozí konfiguraci partnera.
show pullpartnerconfig	Zobrazí konfigurační informace pro server pro vyžádanou replikaci.
show pushpartnerconfig	Zobrazí konfigurační informace pro server pro nabízenou replikaci.
show reccount	Zobrazí počet záznamů vlastněných zadaným vlastnickým serverem.
show rechyversion	Zobrazí záznamy vlastněné zadaným serverem.
show server	Zobrazí aktuálně vybraný server.
show statistics	Zobrazí statistiku pro server WINS.
show version	Zobrazí aktuální hodnotu čítače verzí pro server WINS.
show versionmap	Zobrazí mapování Id vlastníka na nejvyšší čísla verze.

Specifikace služby WINS (RFC)

Požadavky komentářů (RFC) jsou řadou vyvíjejících se zpráv, návrhů protokolů a standardů protokolů, používaných uživateli sítě Internet. Specifikace služby WINS (Windows Internet Name Service) jsou založeny na schválených specifikacích RFC, publikovaných Komisí techniky sítě Internet (IETF) a dalšími pracovními skupinami.

Následující specifikace RFC obsahují hlavní specifikace použité při návrhu WINS:

RFC 1001: Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Koncep-
ty a metody

RFC 1002: Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Podrob-
né specifikace

Poznámka: Specifikace 1001 a 1002 definují standardní protokol pro podporu systému NetBIOS v prostředí TCP/IP. Tyto specifikace popisují obecné používání systému NetBIOS nad protokolem standardu TCP/IP (NetBT) se zdůrazněním základních pojmů a technik, používaných ve všech implementacích NetBT.

Služba WINS těmto specifikacím vyhovuje a poskytuje otevřenou, na standardech založenou a interoperabilní názvovou službu NetBIOS. Vzhledem k tomu, že společnost Microsoft značně rozšířila protokol určený ve specifikacích RFC, lze servery WINS přesněji označit jako rozšířené názvové servery NetBIOS.

ČÁST III

Řízení a bezpečnost sítě



Bezpečnost a automatizace řízení sítě jsou nutné vlastnosti pro vedoucí pracovníky a správce velkých sítí. V této sekci vyzkoušíme další vlastnosti Windows 2000, které umožňují zabezpečení sítě, řízení šířky pásma a automatické řízení klientů

V této části najdete

Zabezpečení protokolu IP 485

Technologie Quality of Service 529

Simple Network Management Protocol 587

KAPITOLA 8

Zabezpečení protokolu IP



Zabezpečení protokolu IP (IPSec) je aplikační rámec otevřených standardů, který díky šifrovacím službám zabezpečuje soukromá zabezpečená spojení prostřednictvím sítí protokolu IP. Implementace zabezpečení protokolu v systému Microsoft® Windows® 2000 je založena na standardech, vyvinutých pracovní slupinou organizace IETF.

Obsah této kapitoly

Otázky zabezpečení protokolu IP	486
Představení zabezpečovacího protokolu IPSec	488
Služby	492
Typy protokolu IPSec	497
Součásti protokolu IPSec	500
Tunelová propojení	508
Struktura zásad IPSec	510
Plánování zabezpečení protokolem IPSec	514
Obecně použitelný příklad zabezpečení IPSec	519
Odstraňování problémů	521

Související informace v Soupravě nástrojů (Resource Kit)

- Obecné informace o protokolu IP (Internet Protocol) najdete v kapitole „Úvod do TCP/IP“.
- Další informace o pojmech sítí VPN najdete v tématu „Virtuální privátní síť“ v dokumentaci *Microsoft® Windows® 2000 Server Internetworking*
- Obecné informace o zabezpečení najdete v kapitolách části „Distribuívané zabezpečení“ v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.

Otázky zabezpečení protokolu IP

Bez zabezpečení by jak soukromé, tak veřejné sítě umožňovaly neautorizované sledování a neautorizovaný přístup. V důsledku minimálního nebo dokonce vůbec žádného zabezpečení může v podnikových sítích intranet docházet k nežádoucím vnitřním útokům. Riziko vnějších útoků představuje připojení k síti Internet a k sítím extranet. Ani přístup k síti, zabezpečený uživatelským heslem, však nechrání přenášaná data.

Běžné typy síťových útoků

Bez příslušné míry zabezpečení se mohou vaše data stát snadným terčem vnějšího útoku. Některé útoky jsou pasivní, což znamená, že jsou vaše data pouze sledována, jiné útoky jsou však aktivní – zde může docházet k záměně informací nebo k pokusům o narušení nebo zničení dat v síti.

Vaše síť a data v ní jsou zranitelné a pokud neučiníte patřičná opatření, mohou podlehnout některému z následujících typů útoku.

Tajné sledování

Obecně je většina síťových spojení nechráněná a vyskytuje se v podobě „obyčejného textu“, což umožňuje útočníkovi, který získal přístup k datovým cestám ve vaší síti, aby „sledoval“ nebo interpretoval (četl) sledované přenosy. Jsou-li vaše data útočníkem tajně sledována, říká se také, že jsou odchyťována nebo špiclována. Schopnost slídila sledovat vaši síť je zpravidla jedním z velkých problémů zabezpečení, s nimž se správci velkých podnikových sítí často setkávají. Bez výkonné šifrovací služby, založené na kryptografii, lze při síťových přenosech vaše data snadno číst.

Záměna informací

Když si útočník vaše data v klidu přečte, lze se domnívat, že jeho následujícím krokem bude jejich záměna. Útočník může upravit data v paketu, aniž by se o tom dozvěděl jak odesílatel, tak příjemce. I když nevyžadujete důvěrnost na všech komunikačních spojeních, určitě nebudete souhlasit s tím, že vám někdo bude data upravovat. Když například odesíláte objednávku zboží, nechcete, aby někdo změnil počet objednaných kusů, jejich typ nebo informace o provedení platby.

Záměna identity (Padělání adresy IP)

Většina sítí a operačních systémů používá adresy IP svých počítačů k identifikaci platného subjektu. V některých případech je možné, že bude adresa IP falzifikována (padělání adresy IP). Útočník může použít speciální programy, které vytvoří zvláštní pakety IP, které se k nerozeznání podobají platným adresám uvnitř podnikové sítě.

Po získání přístupu k síti pomocí platné adresy IP může útočník nerušeně upravit, přesměrovat nebo vymazat vaše data. Může kromě toho útočit i jiným způsobem, o čemž se dozvíte v následujících oddílech.

Útok na zabezpečení heslem

Společným jmenovatelem plánu zabezpečení operačního systému nebo sítě je přístup založený na ověření totožnosti. Znamená to, že vaše přístupová práva k počítači nebo k síťovým prostředkům jsou určena na základě toho, kdo jste, tedy, jaké je vaše uživatelské jméno a heslo.

Starší aplikace identitu uživatele při přenosech v síti nechránily. Díky tomu mohla celá řada slídlů získat přístup k síti vytvářením dojmu, že jsou řádnými uživateli.

Když útočník našel platný uživatelský účet, získal tím stejná práva jako skutečný uživatel. Proto tedy, když měl napadený uživatel práva administrátora, mohl si útočník snadno vytvořit vlastní účet pro pozdější snadný přístup.

Jakmile má útočník přístup k vaší síti, může udělat následující :

- Získat seznam platných jmen uživatelů a názvů počítačů včetně všech podstatných síťových informací.
- upravit konfiguraci serveru a celé sítě včetně změn v přístupových právech a v tabulkách směrování.
- Upravit, přesměrovat nebo vymazat vaše data.

Odmítnutí služby

Útok typu odmítnutí služby, na rozdíl od útoku na zabezpečení heslem, zamezuje běžnému používání počítačů nebo sítě oprávněnými uživateli.

Jakmile má útočník přístup k vaší síti, může udělat následující:

- Příkazem pro vytvoření náhodného jména může oklamat pozornost vnitřních informačních systémů, takže ty nezjistí vetřelce ihned. Takto nezjištěný vetřelec může během své invaze provést ještě mnoho jiných typů útoků.
- Může odeslat neplatná data aplikacím nebo síťovým službám, což může způsobit předčasné ukončení nebo chybný chod těchto programů.
- Může zaplavit počítač nebo celou síť svými přenosy, což může ve svém důsledku způsobit zhroucení se systému z důvodů přetížení.
- Může zablokovat datové přenosy, což zase způsobí ztrátu přístupu autorizovaných uživatelů k síťovým zdrojům.

Prostředník

Jak už napovídá sám název, k tomuto typu útoku dochází, když někdo mezi vámi a osobou na druhé straně aktivně sleduje průběh spojení a neviditelnou rukou zachycuje a řídí datové přenosy. Takový útočník může v jednom okamžiku třeba přesměrovat výměnu dat. Pokud spolu počítače komunikují pomocí nízkoúrovňových spojení, nejsou pak schopny zjistit, s kým si vlastně svá data vyměňují.

Takový prostředník útočí stejně, jako někdo, kdo se za vás vydává, aby mohl zjistit obsah vašich zpráv. Osoba na druhém konci si může být jista, že komunikuje s vámi, neboť útočník může klidně během relace s vaším partnerem aktivně komunikovat, jako byste to byli vy, a díky tomu získá informací ještě více. Tento útok může způsobit stejné škody jako útok na vrstvu aplikace, o němž se dozvíte později.

Ohrožení bezpečnosti klíče

Klíč je důvěrným kódem neboli číslem, nezbytným k tomu, abyste byli schopni přečíst důvěrnou informaci. Přestože získání takového klíče útočníkem není zdaleka snadnou záležitostí, je náročné na použité prostředky a může trvat dlouhou dobu, je možné. Jakmile se něco takového podaří, je klíč označován jako klíč s ohroženou bezpečností.

Útočník tento klíč používá k získání přístupu k zabezpečeným spojení, aniž by o tom odesílatel nebo příjemce měli sebemenší tušení. S tímto klíčem může dekódovat nebo

upravit data, může se s jeho pomocí pokusit o výpočet dalších klíčů, což ve svém důsledku může umožnit tomuto útočníkovi přístup k dalším důvěrným informacím.

Štěnice

Štěnice je aplikace nebo zařízení, které je schopno číst, sledovat nebo zachytit síťovou výměnu dat nebo číst síťové pakety. V případě, že nejsou tyto pakety nijak zašifrovány, má štěnice plný přístup ke všem datům uvnitř paketu. Nejsou-li zašifrovány, může útočník tímto způsobem prolomit také pakety odesílané tunelovým propojením (zapouzdřené).

Útočník může pomocí štěnice ve vašem systému napáchat například tyto škody:

- Analyzovat vaši síť a získat takové informace, které mu nakonec umožní tuto síť rozbít nebo narušit.
- Číst přenášené zprávy.

Útok na aplikační vrstvu

Útok na vrstvu aplikací zpravidla cíleně způsobuje chyby v operačním systému serveru nebo v jeho aplikacích. Výsledkem je schopnost útočníka obejít běžnou kontrolu přístupu. Útočník z toho těží a převezme kontrolu nad vašimi aplikacemi, systémem a sítí a nakonec vám může způsobit například tyto škody:

- Číst, přidávat, mazat nebo upravovat data nebo operační systém.
- Spustit v systému virus, který bude používat vaše počítače a aplikace ke svému opakovanému kopírování po celé vaší síti.
- Může spustit štěnici, která bude vaši síť analyzovat a získávat informace, které může útočník nakonec použít k rozbíjení nebo narušení sítě a systému.
- Vyvolávat nesprávné ukončování aplikačních programů nebo operačních systémů.
- Zakázat další ochranné mechanismy, aby si usnadnil cestu pro následné útoky.

Představení zabezpečovacího protokolu IPSec

IPSec představuje výsledek dlouhodobého úsilí o zabezpečení síťového provozu. Poskytuje klíčovou obrannou linii proti útokům vedeným proti soukromým sítím a celosvětové síti Internet. Jeho účinnost navíc je vyvážena se snadností použití.

Zavedení tohoto protokolu do praxe mělo a má dva cíle:

- Zabezpečovat pakety IP,
- poskytovat ochranu proti útokům vedeným proti síťovému provozu.

Obou těchto cílů se podařilo dosáhnout prostřednictvím služeb zabezpečujících zprávy na bázi kryptografie, prostřednictvím zabezpečovacích protokolů a správce dynamických klíčů. Tento základ poskytuje jak sílu, tak potřebnou pružnost při zabezpečování spojení mezi počítači soukromých sítí, doménami, síťovými servery, vzdálenými servery, sítěmi extranet a klienty služeb telefonického připojení sítí. Lze jej také použít k zablokování odběru nebo přenášení specifických typů zpráv.

Protokol IPSec je založen na modelu zabezpečení koncových uživatelů, což znamená, že jedinými počítači, které vědí o zabezpečených přenosech jsou ty, které odesílají nebo přijímají zabezpečené zprávy. Každý z nich zajišťuje ochranu na svém konci přenosu, kdy se předpokládá, že prostředí, v němž jsou zprávy přenášeny, není zabezpečeno. Není přitom nutné, aby všechny počítače, které směřují svá data ze zdroje k cíli,

tento protokol využívaly. Model umožňuje protokol IPSec začlenit také do vašich stávajících podnikových řešení:

- místní síť (LAN): klient/server, peer to peer (rovnocenná síťová komunikace),
- rozlehlá síť (WAN): směrovač/směrovač (rovnocenná síťová komunikace), brána/brána (rovnocenná síťová komunikace),
- vzdálený přístup: klienti služby telefonického připojení sítě, přístup k síti Internet z soukromých sítí.

Implementace protokolu IPSec, použitá v systému Windows 2000, je založená na průmyslových standardech, v současné době používaných pracovní skupinou organizace IETF (Organizace zaměřená na vývoj a návrh protokolů pro síť Internet). Protokol IPSec a s ním související služby v systému Windows 2000, byly vyvíjeny společnými silami společností Microsoft a Cisco Systems, Inc.

Důsledná ochrana

Data je třeba chránit před zachycením, úpravami nebo neautorizovaným přístupem. Síťové útoky mohou vést k nežádoucím prostojům a ke zveřejňování důvěrných informací.

Strategie ochrany sítě se obecně zaměřuje pouze na obranu proti útokům vedeným zvenčí. Proto běžně používá bezpečnostní brány, zabezpečovací směrovače (zabezpečovací brány) a přístup pomocí telefonického připojení sítě s ověřením totožnosti. Tomuto typu zabezpečení se říká zónové zabezpečení. Tento způsob zabezpečení však nevytváří dostatečnou ochranu proti útokům vedený zvnitř.

Metody zabezpečení řízeného přístupu uživatelů (karty Smart Card, ověření totožnosti pomocí protokolu Kerberos v5) nemohou dostatečným způsobem chránit proti většině útoků vedených na úrovni síťového protokolu, neboť se spoléhají toliko na uživatelská jména a hesla. Mnoho počítačů je sdíleno více uživateli. Výsledkem je stav, kdy počítač často zůstává zapnutý s přihlášeným uživatelem, což jej činí nezajištěným. Pokud někdo ukradl uživatelské jméno a heslo, nelze útočníkovi pomocí metod zabezpečení řízeného přístupu uživatelů v jeho útoku na síťové prostředky zabránit.

Strategie zabezpečení na fyzické úrovni, která se běžně nepoužívá, chrání síťová vedení před neoprávněným přístupem a síťové přístupové body před neoprávněným používáním. I to však zřídka zaručuje ochranu celé cesty, kterou musí data při své cestě za cílem překonat.

Nejlepší ochranou je protokol IPSec, založený na modelu zabezpečení koncových uživatelů: odesílatel zabezpečuje data před odesláním (ještě dříve, než data dosáhnou síťových vedení) a příjemce tato data dešifruje až po jejich přijetí. Z tohoto důvodu by měl být protokol IPSec jednou z hlavic součástí rozvrstveného řešení podnikové sítě. Chrání soukromá data ve veřejném prostředí, když poskytuje výkonnou ochranu, založenou na kryptografii. Celá síť je tak chráněna samostatným zabezpečováním každého odesílaného paketu. Ve spojení s přísným řízením uživatelského přístupu, zónovým zabezpečením a možná dokonce i zabezpečením na fyzické úrovni, zaručuje protokol IPSec skutečně důslednou ochranu vašich dat.

Agresivní zabezpečení proti útokům

Protokol IPSec chrání data, takže útočníka, který pronikne do systému, čeká ještě velmi nelehký úkol analýzy zakódovaných dat. Úroveň zabezpečení je navíc určována úrovní obecného zabezpečení, nastaveného v zásadách struktury zabezpečení protokolem IPSec.

Protokol IPSec má celou řadu vlastností, které významně snižují riziko dříve uvedených typů útoku nebo jej dokonce vylučují:

Štěnice, ztráta soukromí Protokol ESP (zabezpečení integrity dat šifrováním) zajišťuje důvěrnost zašifrovaných paketů IP.

Úprava dat protokol IPSec používá klíče vytvářené na bázi kryptografie. Tyto klíče jsou sdíleny pouze odesílatelem a odběratelem zprávy. Pomocí obou rozdělených částí tohoto klíče je vytvářen digitální kontrolní součet paketu IP. Všechny úpravy paketu narušují konzistenci tohoto součtu, což znamená, že lze poznat, zda byl během přenosu paket upravován.

Záměna identity, zabezpečení heslem, aplikační vrstva a odmítnutí služby Protokol IPSec umožňuje výměnu a ověření informací o identitách, aniž by se tato skutečnost dostala k potenciálnímu útočníkovi. Oboustranné ověření (ověřování totožnosti) se používá k vytvoření důvěryhodného propojení mezi komunikačními systémy. Vzájemná komunikace může probíhat pouze mezi dvěma důvěryhodnými systémy.

Prostředník Protokol IPSec kombinuje model oboustranného ověření totožnosti se sdílenými zašifrovanými klíči.

Odmítnutí služby Protokol IPSec využívá metodiku filtrování paketů IP jako základ pro určování, která spojení jsou povolena a která zabezpečena nebo zablokována. Tyto údaje získává na základě rozsahů adres IP, protokolů nebo dokonce specifických protokolů jednotlivých portů.

Zabezpečení vrstvy 3

Zabezpečení protokolem IPSec zpravidla vyžaduje určité úpravy systému. Strategická implementace protokolu IPSec však na úrovni přenosů IP (síťová vrstva 3) umožňuje vyšší úroveň zabezpečení, transparentního vůči většině aplikací, služeb a protokolů vyšších vrstev. Přitom zatížení sítě zůstává minimální. Zavedení protokolu IPSec nevyžaduje žádné změny ve stávajících aplikacích nebo v operačním systému. Zásady lze definovat centrálně v rámci služby Active Directory™ nebo je spravovat místně na každém počítači zvlášť.

Implementace zabezpečení vrstvy 3 poskytuje ochranu protokolu IP, stejně jako všech protokolů vyšších vrstev TCP/IP, jako jsou TCP, UDP, ICMP, Raw (protokol 255) a dokonce i uživatelské protokoly, které posílají data prostřednictvím vrstvy IP. (Více informací o modelu síťové vrstvy najdete v kapitole „Úvod do TCP/IP“.) Primární výhodou zabezpečení informací v nižší vrstvě je to, že všechny aplikace a služby, které používají protokol IP pro přenos dat, mohou být chráněny protokolem IPSec bez nutnosti jejich předběžných úprav.

Jiné zabezpečovací mechanismy, které fungují nad vrstvou 3 jako například vrstva SSL (Secure Sockets Layer), zabezpečují pouze aplikace, které vědí, jak je třeba mechanismu SSL využívat (jako příklad uveďme například prohlížeče sítě WWW). Abyste mohli chránit aplikace na všech svých počítačích pomocí SSL, museli byste všechny tyto aplikace nejprve odpovídajícím způsobem upravit. Zabezpečovací mechanismus, který působí pod vrstvou 3, jako například šifrování linkové vrstvy, chrání pouze propojení, nikoliv všechna propojení cesty, kterou musí data překonat. Díky tomu je tato vrstva pro zabezpečení koncových uživatelů v síti Internet nebo ve směrovaných sítích intranet nevhodná.

Zabezpečení metodou zásad

Přestože se výkonnější metody zabezpečení (např. šifrování) staly při plném zabezpečování spojení nutností, zpravidla podstatně ztěžují práci správců. Protokol IPSec předchází i tomu a využívá správu zabezpečení metodou zásad.

Zásady protokolu IPSec se používají ke konfiguraci zabezpečovacích služeb IPSec, nikoli k úpravám rozhraní aplikačních programů nebo operačního systému. Tyto zásady poskytují proměnlivé hladiny zabezpečení pro většinu typů přenosů ve většině existujících sítí,

Protokol IPSec poskytuje možnost řízení přístupu, když umožňuje správci v zásadách IPSec navrhnout specifické filtry a jejich akce. Protokol využívá dva typy řízení přístupu: jednoduché filtrování paketů IP a úspěšné ověření totožnosti. Kromě toho povoluje zablokovat určité akce (viz „Akce filtrů“ dále v této kapitole), umožňuje kontrolu odesílání a přijímání určitých typů paketů IP nebo kontrolu adres, s nimiž může daný počítač komunikovat.

Správce zabezpečení vaší sítě může nakonfigurovat zásady protokolu IPSec tak, aby splňovaly jak požadavky jednoho uživatele, tak skupiny, aplikace, domény, serveru nebo celého podniku. Operační systém Windows 2000 obsahuje prostředí pro správu – službu Agent zásad IPSec. Díky tomuto nástroji lze definovat zásady protokolu IPSec pro počítače na úrovni služby Active Directory nebo pro místní počítače, které nespádají do žádné domény.

Zjednodušené zavedení

Aby bylo možné dosáhnout zabezpečení spojení s nejmenšími náklady, zjednodušuje systém Windows 2000 zavedení protokolu IPSec následujícími funkcemi:

Integrace s soustavou zabezpečení systému Windows 2000 Protokol IPSec využívá bezpečné domény systému Windows 2000 jako důvěryhodný model. Zásady IPSec při určování důvěryhodnosti komunikujících počítačů standardně využívají výchozí ověření totožnosti systému Windows 2000 (protokolu Kerberos v5). Počítače, jež jsou členy domény systému Windows 2000, a bezpečné domény mohou snadno vytvořit zabezpečené komunikační připojení s protokolem IPSec.

Centralizace správy zásad IPSec na úrovni služby Active Directory Zásady IPSec lze nastavit pomocí funkce Zásady skupiny, implementované službou Active Directory. Tato funkce umožňuje přiřazení zásad IPSec na úrovni domény nebo organizační jednotky. Není už tedy nutné zatěžovat správu konfigurováním každého počítače zvlášť.

Transparentnost protokolu IPSec z pohledu uživatelů a aplikací Těsná integrace na úrovni vrstvy IP (vrstva 3) poskytuje ochranu všech protokolů sady TCP/IP. V žádném z protokolů sady TCP/IP nebudete muset vytvářet zvláštní zabezpečovací balíčky, neboť všechny aplikace, které používají k přenosu svých dat protokol TCP/IP, budou zabezpečeny.

Pružná konfigurace zabezpečení Služby zabezpečení v rámci každé zásady ze podle potřeby dynamicky upravovat, aby vyhovovaly většině požadavků pro zabezpečení sítě i přenosu dat.

Automatická správa klíčů Služba IKE (Internet Key Exchange) umožňuje dynamickou výměnu klíčů v síti Internet a správu šifrování klíčů mezi komunikujícími počítači.

Automatické vyjednávání o výměně klíčů Služba IKE (Internet Key Exchange) umožňuje dynamicky vyjednávat o výměně klíčů (neboli sadě zabezpečovacích požadavků) mezi komunikujícími počítači. Není už tedy nutné, aby oba počítače měly stejné zásady.

Podpora infrastruktury veřejných klíčů Systém obsahuje podporu použití certifikátů veřejných klíčů pro ověřování. Díky tomu lze zdůvěřhodnit a zabezpečit spojení mezi počítači, které nenáleží do důvěryhodné domény systému Windows 2000, mezi systémy s jiným operačním systémem než Windows 2000, mezi počítači, které mohou být členy nedůvěryhodné domény, nebo v případě, kdy je třeba přístup počítače omezit na menší skupinu nebo kdy se povoluje ověření totožnosti v doméně.

Podpora předběžných sdílení klíčů V případě, že nelze ověřit totožnost pomocí protokolu Kerberos v5 a nelze použít ani certifikát veřejného klíče, lze povolit ověření předběžného sdílení klíče. Více informací najdete v oddílech „Ověřování“ a „Doporučené postupy“ později v této kapitole.

Služby

Protokol IPSec umožňuje vysoký stupeň zabezpečení díky užití šifrovacích mechanismů. Šifrování umožňuje bezpečný přenos informací pomocí transformačních (integrita) a šifrovacích (důvěrnost) algoritmů.

K zabezpečení informace se používá kombinace algoritmů s klíčem:

- *Algoritmus* je matematický proces, jehož prostřednictvím je informace zabezpečena.
- *Klíč* je důvěrný kód nebo číslo, vyžadované pro čtení, úpravy nebo ověřování zabezpečených dat.

Protokol IPSec v systému Windows 2000 využívá následující služby.

Vlastnosti zabezpečení

Protokol IPSec obsahuje tyto vlastnosti pro zabezpečenou komunikaci:

Neodvolatelnost Ověřuje, zda je odesílatel zprávou jedinou osobou, která ji mohla odeslat. Odesílatel nemůže popřít odeslání zprávy. Neodvolatelnost je vlastností zpráv, obsahujících digitální podpis zadaný pomocí technologie veřejného klíče. Pomocí této technologie je soukromý klíč použit k vytvoření digitálního podpisu, který je odeslán s danou zprávou. Příjemce používá veřejný klíč odesílatele, jehož pomocí ověřuje pravost digitálního podpisu. Vzhledem k tomu, že pouze odesílatel vlastní soukromý klíč, mohl také pouze on tento digitální podpis vygenerovat. Neodvolatelnost není vlastností kódů ověření zprávy nebo transformací zpráv, používajících technologie důvěrných klíčů, neboť důvěrný klíč mají jak odesílatel, tak příjemce.

Neopakovatelnost Také nazývána *zamezení opakování*. Zajišťuje jedinečnost každého paketu IP. Neopakovatelnost zaručuje, že data zachycené útočníkem nelze opětovně

použít nebo „přehrát“ za účelem vytvoření relace nebo nelegálního získání informací. Tak se data chrání před pokusy odposlouchávat zprávu a potom ji používat k nelegálnímu získání přístupu k prostředkům (i kdyby to mělo být mnohem později).

Integrita Chrání data před neautorizovanými úpravami při přenosu, když zaručuje, že přijatá data jsou přesně taková, jaká byla data odeslaná. Transformační funkce označí pomocí sdílených klíčů každý paket zašifrovaným kontrolním součtem. Tuto hodnotu ověřuje příjemce ihned po přijetí zprávy a to ještě před jejím otevřením. Klíč, nezbytný k výpočtu kontrolního součtu, mají k dispozici pouze odesílatel a příjemce. V případě, že dojde ke změně paketu, a tím pádem také ke změně podpisu, bude paket ignorován.

Důvěrnost (Šifrování) Zaručuje, že budou data zpřístupněna pouze zamýšleným příjemcům. To je zajištěno šifrováním dat před odesláním.

Tento postup dává jistotu, že data nelze přečíst během přenosu, i kdyby byl paket sledován nebo dokonce zachycen. Pouze strana se sdíleným důvěrným klíčem je schopna tato data přečíst (po dekodování). Používání této vlastnosti je volitelné a závisí na nastavení zásad IPSec.

Ověřování Ověřuje původ zprávy pomocí procesu jednosměrného odesílání pověření a následného ověření pravosti tohoto pověření příjemcem. Protokol IPSec v systému Windows 2000 poskytuje celou řadu metod ověřování, díky nimž zaručuje kompatibilitu se staršími systémy, systémy jiného typu než Windows a se vzdálenými počítači. Více informací o ověřování najdete v kapitolách části „Distribuované zabezpečení“ v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.

Ověřování na bázi certifikátu veřejného klíče

Vhodným způsobem implementovaná infrastruktura veřejných klíčů, v níž lze vykazovat pověření bez ohrožení těchto pověření během přenosu, řeší mnoho problémů zabezpečení. Protokol IPSec využívá vaši infrastrukturu veřejných klíčů k ověřování počítačů na základě certifikátu veřejného klíče.

Certifikát veřejného klíče (PKC) zaručuje, že se *kdo tvrdíš, že jsi* neliší od *kdo jsi opravdu*. Standard PKC je jedním z typů spolehlivého ověřování.

Certifikát veřejného klíče je něco jako digitální pas. Tyto certifikáty jsou používány k ověření totožnosti počítačů s jiným systémem než Windows 2000, samostatných počítačů, klientů, kteří nejsou členy důvěryhodné domény nebo počítačů, které nevyužívají protokol ověření totožnosti Kerberos v5 (výchozí metoda ověřování v systému Windows 2000).

Více informací o implementaci infrastruktury veřejných klíčů najdete v kapitole „Volba zabezpečovacích řešení, která využívají technologie veřejných klíčů“ v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.

Ověřování s předběžným sdílením klíče

Protokol IPSec lze používat také k ověřování s předběžným sdílením klíče. Předběžné sdílení klíče znamená, že musí obě strany souhlasit s používáním sdíleného důvěrného klíče, jež se stává součástí zásady IPSec. Během vyjednávání o výměně klíče je informace zašifrována ještě před přenosem pomocí sdíleného klíče a na straně příjemce je stejným klíčem dekodována. Podaří-li se příjemci dekodovat přijatou informaci, považuje se tato identita za ověřenou.

Společnost Microsoft časté používání metody ověřování s předběžným sdílením klíče nedoporučuje, neboť ověřovací klíč je uložen a nechráněn v zásadě IPSec. Metodologie předběžného sdílení klíče je zahrnuta pouze z důvodů spolupráce s jinými systémy a za účelem dodržení standardů IPSec zveřejněných komisí IETF. Aby bylo možné tuto metodu ověřování používat bezpečně, musí být vyhrazena pouze pro správce a při komunikaci mezi řadičem domény a členskými počítači domény musí být z důvodů důvěrnosti zašifrována. Navíc musí být vyhrazena pouze pro čtení systémem.

Šifrování veřejných klíčů

Protokol IPSec implementuje metody šifrování veřejných klíčů pro ověřování (podpis certifikátu) a výměnu klíče (Diffie-Hellmanův algoritmus). Šifrování veřejných klíčů obsahuje všechny přednosti šifrování důvěrných klíčů, ale je zpravidla bezpečnější, neboť k ověření vyžaduje klíče dva – jeden pro vygenerování podpisu a zašifrování dat a druhý pro ověření podpisu a dekodování dat. Tento způsob šifrování je označován jako asymetrické šifrování, což znamená, že k úspěšnému dokončení procesu je zapotřebí dvou klíčů.

Každý uživatel vlastní svůj soukromý klíč, který zná jenom on sám. Vlastní také veřejný klíč, který je veřejně distribuován. Pokud chce například Katka odeslat Bogdanovi zabezpečenou zprávu, použije k zašifrování zprávy Bogdanův veřejný klíč. Tuto zprávu může dekodovat pouze Bogdan, neboť k přečtení zprávy je nezbytný jeho klíč soukromý. Přestože tyto dva klíče spolu souvisí, je z matematického hlediska nemožné vygenerovat jeden klíč pomocí druhého. Z tohoto prostého důvodu lze veřejný klíč bezpečně distribuovat. Soukromý klíč, označovaný také jako důvěrný klíč, musí být pečlivě střežen.

Integrita pomocí transformačních funkcí

Algoritmy *HMAC* (*Hash message authentication codes*) „podepisují“ pakety za účelem pozdějšího ověření toho, zda je přijatá informace přesně tatáž, jako informace odeslána odesílatelem (integrita). Tato funkce je klíčová při přenosech přes nezabezpečené oblasti nebo média.

Algoritmy HMAC zajišťují integritu přenášených informací pomocí transformačních neboli přepočtových funkcí (algoritmus), kombinovaných se sdíleným důvěrným klíčem. Tento přepočet je častěji označován jako podpis paketu. Je to poněkud nepřesné označení, neboť přepočet se od digitálního podpisu přece jen liší: přepočtové funkce používají sdílený důvěrný kód, zatímco digitální podpis využívá technologii veřejného klíče a posílání klíče počítače. Transformační funkce jsou také nesprávně označovány za jakýsi zhuštěný obsah zprávy nebo jednosměrný přenos. Jednosměrné přenosy nebo funkce mají jeden společný jmenovatel: každá ze stran musí provést výpočet na svém konci přenosu a, i když je poměrně snadné vytvořit zhuštěný obsah zprávy, je matematicky nemožné převést zhuštěný obsah zpět do původní podoby. A obráceně. Obousměrné funkce mohou pracovat oběma směry. Příkladem těchto funkcí je například šifrování.

Podpis HMAC je ve skutečnosti zašifrovaným kontrolním součtem neboli kódem MIC (*Message Integrity Code*), který musí každá ze stran vypočítat, aby autenticitu zprávy ověřila. Přiblížme si to na praktickém příkladu. Počítač odesílatele používá při výpočtu kontrolního součtu zprávy algoritmus HMAC a sdílený klíč a výslednou hodnotu pak přidá k odesílané zprávě. Příjemce musí vypočítat hodnotu HMAC přijaté zprávy a výslednou hodnotu porovnat s originálem (včetně paketu odesílatele). V případě, že bě-

hem přenosu došlo ke změně zprávy, budou se obě hodnoty lišit a paket bude zamítnut.

Při zajišťování integrity a nastavení zásady můžete vybírat ze dvou transformačních funkcí:

- **HMAC-MD5** Kontrolní součet MD5 (Message Digest 5) je založen na standardu RFC 1321. Byl vytvořen jako odpověď na slabiny kontrolního součtu MD4, což byl produkt předchozí etapy vývoje původního kontrolního součtu MD. MD5 je sice o něco pomalejší, je za to mnohem výkonnější.

Kontrolní součet MD5 prochází každý blok dat čtyřikrát (zatímco algoritmus kontrolního součtu pouze třikrát) a při každém průchodu používá pro každé slovo zprávy jinou konstantu. Při výpočtu hodnoty MD5 je tedy použito 64 32bitových konstant.

Nakonec je vygenerován 128bitový klíč, který je pak používán pro ověření integrity.

- **HMAC-SHA** Algoritmus SHA (Secure Hash Algorithm) byl vyvinut ve Národním institutu pro vývoj standardů a technologie (National Institute of Standards and Technology), jak popisuje standard FIPS PUB 180-1. Algoritmus SHA je velmi podobný modelu algoritmu MD5.

Tento algoritmus používá během výpočtu 79 32bitových konstant. Výsledkem je 160bitový klíč, používaný pro ověření integrity. Větší délka klíče poskytuje vyšší úroveň zabezpečení, takže algoritmus SHA je považován za výkonnější.

V další části kapitoly bude při pojednání o způsobech zajišťování integrity pomocí transformačních funkcí používán pojem „podpis“.

Šifrování dat: Důvěrnost

Protokol IPSec v systému Windows 2000 pracuje při zabezpečování důvěrnosti dat (šifrování dat) se standard šifrování DES (US Data Encryption Standard), používaným ve Spojených státech.

Standard šifrování DES

Algoritmus DES byl poprvé zveřejněn v roce 1977 v Národním úřadu pro vytváření standardů ve Spojených státech. Protokol IPSec umožňuje časté přegenerování klíče i během spojení. Tato funkce brání ohrožení celé datové sady při prolomení klíče DES. Více informací najdete v oddílu „Životnost klíče“.

Algoritmus DES používá 56bitový klíč a mapuje 64bitové vstupní bloky na 64bitové výstupní bloky. Klíč se jeví jako 64bitová hodnota, ale jeden bit v každém z 8 bajtů je používán pro ověření liché parity, což ve svém důsledku umožňuje používat při generování klíče pouze 56 bitů.

Vstupní blok je zpočátku zpracován tak, aby vytvořil 64bitový výstupní blok. Zpracování je jako zamíchání balíčku karet – je to náhodně vykonávaný proces, který zajišťuje, že pokaždé budou vytvořena jiná čísla. Tento klíč se používá ke generování 16 48bitových hodnot na každý zpracovaný klíč. Každé zpracování přebírá jako svůj vstup výstup předchozího zpracování (klíč), ke kterému se přičte 48bitový klíč a nakonec je vytvořen 56bitový klíč. Po šestnáctém zpracování je klíč obměněn obrácením původní permutace.

40bitový šifrovací algoritmus DES *CBC* (*Cipher Block Chaining*) se používá k ukrytí vzorů stejných bloků dat uvnitř paketu. Vektor inicializace (počáteční náhodné číslo) se používá jako první náhodný blok šifrovaných dat. V tomto spojení se různé náhodně vybrané bloky používají s důvěrným klíčem a spolu šifrují každý blok. Tato metoda zaručuje, že budou přetvořena stejná data v podobě prostého textu (nezabezpečená data) na jedinečné zašifrované bloky dat. Opakování by mohlo ohrozit zabezpečení klíče, neboť by mohl být vytvořen vzor, na jehož základě by mohl útočník prolomit vaše šifrování. Vzhledem k tomu, že se žádný blok neopakuje, nelze data během šifrování porovnávat.

Protokol IPSec v systému Windows 2000 využívá následující šifrovací algoritmy:

- **3DES** Tento šifrovací algoritmus je velmi účinný, ale právě proto je o něco pomalejší. Zpracovává každý blok dat třikrát a používá pokaždé jiný jedinečný klíč:

1. šifrování bloku pomocí klíče č. 1,
2. šifrování bloku pomocí klíče č. 2,
3. šifrování bloku pomocí klíče č. 3.

Při dekódování hodnoty funguje tento proces obráceně. Protokol IPSec v systému Windows 2000 používá šifrování 3DES z důvodů zachování důvěrnosti přenášených informací.

- **DES** Toto šifrování je používáno v případech, kdy není vyžadováno vysoké zabezpečení a není třeba používat šifrování 3DES.

Správa klíčů

Klíč je důvěrným kódem neboli číslem, nezbytným k tomu, abyste byli schopni důvěrnou informaci přečíst. Klíč se k zabezpečení dat používá ve spojitosti s příslušným algoritmem (matematický proces). Systém Windows 2000 automaticky popisuje generování klíčů a implementuje následující vlastnosti pro jejich správu, které maximalizují zabezpečení:

Dynamické překlíčování

Zásada protokolu IPSec řídí četnost generování klíče během spojení. K tomuto účelu využívá funkci dynamického překlíčování. Komunikace probíhá tak, že jsou data z jednoho počítače na druhý odesílána v blocích, kdy je každý blok dat zabezpečen jiným klíčem. Tento postup nedovolí útočníkovi, jenž získal část přenášených dat a klíčů probíhající korespondence, aby získal i zbývající část zprávy. Toto vyžádané vyjednávání, stejně jako správa automatických klíčů, je poskytováno pomocí zásad výměny klíčů v síti Internet (IKE), definovaných organizací IETF ve specifikaci RFC 2409.

Zásada IPSec umožňuje zkušeným uživatelům řídit způsob vygenerování nového klíče. Pokud nenakonfigurujete žádné hodnoty, budou se klíče generovat automaticky v předem stanovených časových intervalech.

Délky klíčů

Pokaždé, když se délka klíče zvětší o jeden bit, zdvojnásobí se automaticky počet možných hodnot, což exponenciálně křivkou ztěžuje prolomení klíče. Zásada protokolu IPSec poskytuje více algoritmů, které povolují generovat dlouhé nebo krátké klíče.

Klíčové místo generování klíče: Diffie-Hellmanův algoritmus

Chcete-li umožnit zabezpečení spojení mezi dvěma počítači, musí obě tyto stanice získat stejný sdílený klíč (klíč relace), bez nutnosti jeho odeslání, neboť posílání klíče síťovou cestou by mohlo velmi významně narušit důvěrnost sdělení.

Algoritmus DH (*Diffie-Hellmanův algoritmus*) časově předchází šifrování RSA (Rivest-Shamir-Adleman) a je navíc výkonnější. Je jedním z nejstarších a nejbezpečnějších algoritmů, používaných při výměně klíče.

Dvě komunikující strany si spolu veřejně vyměňují klíče. Tuto operaci systém Windows 2000 navíc chrání pomocí podpisu transformačních funkcí. Ani jedna ze stran ve skutečnosti nikdy nevyměňuje skutečný klíč. Přesto je po jejich výměně každá ze stran schopna vygenerovat stejný sdílený klíč. Strany si nikdy skutečný klíč nevyměňují.

Klíčování DH, vyměňovaného mezi dvěma stranami, lze založit na 96 nebo 128 bajtech materiálu, označovaného jako skupiny DH. Síla těchto skupin přímo souvisí se silou klíče. Silné skupiny DH zkombinované s delšími klíči ještě zvyšují stupeň složitosti pro počtů, nezbytných k prolomení klíče.

Protokol IPSec používá algoritmus DH k poskytování materiálu klíčování pro všechny další klíče šifrování. Algoritmus DH sám žádnou možnost ověřování neposkytuje. V implementaci protokolu IPSec v systému Windows 2000 probíhá totožnost ověřování až po výměně DH.

Více informací o procesu generování klíčů najdete v oddílu „Výměna klíčů v síti Internet“.

Typy protokolu IPSec

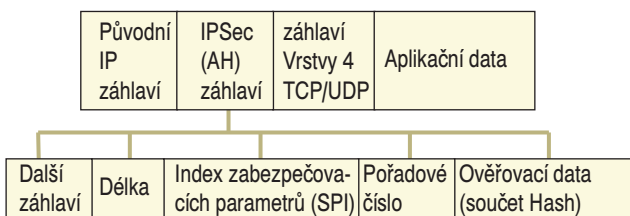
Protokoly IPSec zajišťují ochranu dat a možnost využívání služeb pro ověřování pravosti u všech paketů IP, kdy ke každému paketu přidávají vlastní zabezpečovací záhlaví.

Ověřovací záhlaví

Ověřovací záhlaví (AH) umožňuje ověřování, kontrolu integrity a neopakovatelnost každého paketu (jak záhlaví IP, tak data paketu jsou přenášeny uvnitř paketu). Neposkytuje však žádné zabezpečení důvěrností, což znamená, že nešifruje data. Data tak lze přecíst, přestože jsou chráněna před neoprávněným zásahem. Ověřovací záhlaví používá algoritmus HMAC, popsany dříve, jehož pomoci podepisuje paket za účelem zajištění integrity obsažených dat.

Uvedme si názorný příklad. Katka u počítače A odesílá data Bogdanovi u počítače B. Záhlaví IP, záhlaví AH a data jsou chráněna proti narušení integrity. Znamená to, že si Bogdan může být jist, že data skutečně odeslala Katka a že je cestou nikdo neupravoval.

Zabezpečení integrity a ověření pravosti je zajištěno umístěním záhlaví AH mezi záhlaví IP a přenosovou vrstvou (vrstva 4) záhlaví protokolu, což je na obrázku 8.1 znázorněno jako TCP/UDP. Záhlaví AH využívá k vlastní identifikaci v záhlaví IP identifikátor protokolu IP rovný 51.



Obrázek 8.1: Ověřovací záhlaví.

Záhlaví AH lze používat samostatně nebo ve spojení s protokolem ESP (Encapsulating Security Payload).

Záhlaví AH obsahuje tato následující pole:

Další záhlaví Identifikuje další záhlaví, které používá identifikátor protokolu IP. Například hodnota „6“ označuje TCP.

Délka Udává délku záhlaví AH.

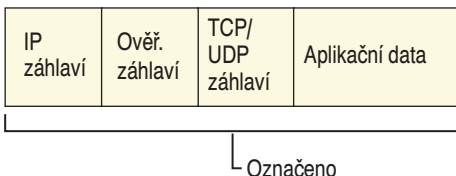
Číslo SPI (Security Parameters Index) Používá se v kombinaci s cílovou adresou a protokolem zabezpečení (AH nebo ESP). Určuje přiřazení zabezpečení pro dané spojení. (Více informací najdete v oddílu „Výměna klíčů v síti Internet“.) Příjemce tuto hodnotu používá ke stanovení definice přiřazení zabezpečení.

Číslo sekvence Zajišťuje zabezpečení neopakovatelnosti SA. Je to 32bitové neustále se zvyšující číslo (s počáteční hodnotou 1), které se nikdy nemůže zacyklit a které současně určuje číslo paketu, odeslaného nad přiřazením zabezpečení pro dané spojení. Příjemce toto pole ověřuje, aby zjistil, zda přidružení zabezpečení tohoto paketu už nebylo přečteno. Pokud tato hodnota již byla jednou přijata, je paket automaticky zamítnut.

Ověřování dat Obsahuje hodnotu ICV (Integrity Check Value), která slouží k ověřování integrity zprávy. Příjemce počítá přepočtovou hodnotu, kterou později porovná s touto hodnotou (vypočtenou odesílatelem). Takto je zajištěna kontrola integrity.

Podpis paketu

Záhlaví AH je vloženo mezi záhlaví IP a horní vrstvu protokolu jako TCP, UDP nebo ICMP. Pokud je kromě záhlaví AH používán ještě další zabezpečovací protokol, je záhlaví AH vkládáno před všechna další záhlaví IPSec. Podpis paketu je znázorněn na obrázku 8.2.



Obrázek 8.2: Podpis zabezpečení integrity AH.

AH podpisuje celý paket a zajišťuje jeho integritu kromě určitých polí v záhlaví IP, které se mohou v průběhu přenosu změnit. Těmito poli jsou Životnost a Typ služby.

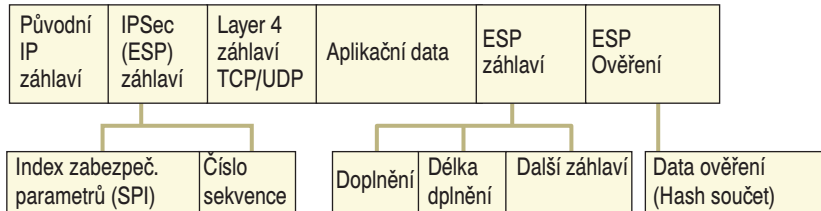
Zabezpečení datové části zprávy zapouzdřením (ESP)

Zabezpečení *ESP (Encapsulating Security Payload)* zajišťuje kromě ověřování, integrity a neopakovatelnosti také důvěrnost sdělení. Zabezpečení ESP lze používat samostatně nebo ve spojení se záhlavím AH.

ESP zpravidla nepodepisuje celý paket. K výjimkám dochází v případech, kdy je k přenosu používáno tunelového propojení. Chráněna je obvykle pouze datová část zprávy IP, nikoli záhlaví.

Uvedme si příklad. Katka u počítače A odesílá data Bogdanovi na počítači B. Datová část je zašifrovaná a obsahuje podpis integrity. Po přijetí zprávy a po ověření její integrity je datová část dekodována. Bogdan si nyní může být jist, že zprávu odeslala právě Katka, že při přenosu nedošlo k žádným změnám dat a že nikdo jiný tuto zprávu nemohl přečíst.

ESP se identifikuje v záhlaví IP pomocí identifikátoru protokolu IP rovného hodnotě 50. Jak vidíte na obrázku 8.3, je záhlaví ESP umístěno před záhlavím vrstvy přenosu (TCP nebo UDP) nebo před datovou částí paketu IP nebo před jinými typy protokolu IP.



Obrázek 8.3: ESP.

Záhlaví ESP obsahuje tato pole:

Číslo SPI (Security Parameters Index) Používá se v kombinaci s cílovou adresou a protokolem zabezpečení (AH nebo ESP). Určuje přiřazení zabezpečení pro dané spojení. (Více informací najdete v oddílu „Výměna klíčů v síti Internet“.) Příjemce používá tuto hodnotu ke stanovení definice přiřazení zabezpečení.

Číslo sekvence Zajišťuje zabezpečení neopakovatelnosti SA. Je to 32bitové neustále se zvyšující číslo (s počáteční hodnotou 1), které se nikdy nemůže zacyklit a které současně určuje číslo paketu, odeslaného nad přiřazením zabezpečení pro dané spojení. Příjemce toto pole ověřuje, aby zjistil, zda přiřazení zabezpečení tohoto paketu už nebylo přečteno. Pokud tato hodnota již byla jednou přijata, je paket automaticky zamítnut.

Koncová část ESP obsahuje tato pole:

Doplnění (Padding) K 32bitovému zarovnání na velikost bloku se pro jeho šifrování používá 0 až 255 bajtů.

Délka doplnění Stanovuje délku pole Doplnění v bajtech. Používá se příjemcem k odložení pole Doplnění.

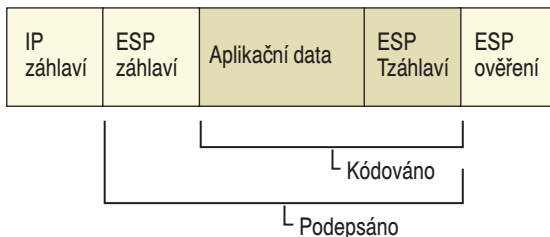
Další záhlaví Určuje povahu datové části jako například TCP nebo UDP.

Koncová část ověřování ESP obsahuje tato pole:

Data ověření Obsahuje hodnotu ICV a ověřovací kód zprávy, použitý k ověření totožnosti odesílatele a k ověření integrity zprávy. Hodnota ICV je vypočtena na základě záhlaví ESP, datové části a koncové části ESP.

Podpis paketu a kódování

Jak je patrné z obrázku 8.4, zabezpečuje ESP horní vrstvy protokolu. Podepsaná oblast stanovuje, kde bylo ověření integrity paketu podepsáno. Zakódovaná oblast určuje, o zabezpečení jaké informace se jedná.



Obrázek 8.4: ESP: Podpis a kódování.

ESP je vloženo mezi záhlaví IP a horní vrstvy protokolu jako TCP, UDP, ICMP nebo jakékoli další záhlaví protokolu IPSec. Všechno, co následuje za záhlavím ESP (horní vrstva protokolu, datová část nebo koncová část ESP) je podepsáno. Záhlaví IP podepsáno není, a proto není také nezbytně chráněno před úpravami. Informace v horní vrstvě protokolu, datová část a koncová část ESP jsou zakódovány.

Součásti protokolu IPSec

Následující oddíly obsahují popis součástí protokolu IPSec instalované v systému Windows 2000.

Služba Agent zásad IPSec

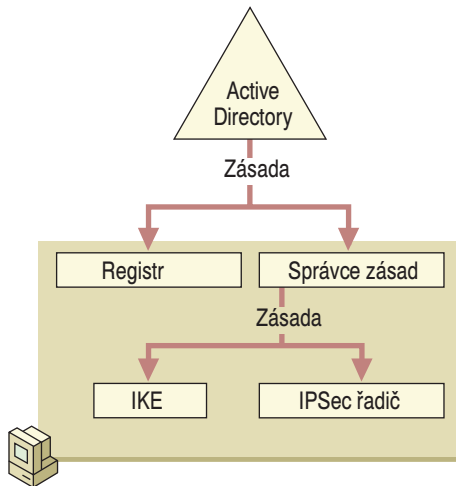
Účelem této služby je vyhledávat informace o zásadách IPSec a předávat je jiným mechanismům protokolu IPSec, které tuto informaci vyžadují k vykonávání zabezpečovacích funkcí (viz obrázek 8.5).

Agent zásad IPSec je službou spuštěnou na všech počítačích se systémem Windows 2000 a zobrazuje se v seznamu systémových služeb. Agent zásad IPSec zajišťuje plnění následujících úloh:

- Je-li počítač členem domény, vyhledá odpovídající zásadu IPSec (byla-li taková přiřazena) ve službě Active Directory. V opačném případě tuto informaci vyhledá v místním registru.
- Odešle ovladači IPSec informaci o aktivní zásadě IPSec.

Ke zpřístupnění zásady dochází buď při spuštění systému, v pravidelných časových intervalech určených zásadou IPSec (je-li počítač připojen k doméně) nebo ve standardních intervalech dotazování Winlogon (je-li připojen k doméně):

- Je-li informace zásady IPSec nakonfigurována centrálně pro všechny počítače, jež jsou členy domény, je tato informace uložena ve službě Active Directory a dočasně také v místním registru počítačů, na něž se vztahuje.



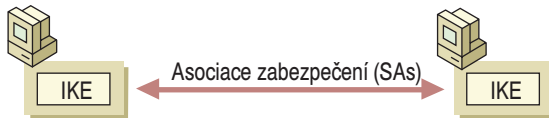
Obrázek 8.5: Agent zásad IPsec.

- V případě, že je počítač dočasně odpojen od domény a existují zásady v mezipaměti, tyto budou po jeho opětovném připojení k doméně přepsány všemi novými informacemi zásady.
- Jestliže je počítač samostatnou jednotkou nebo je členem domény, která nevyužívá službu Active Directory pro ukládání zásad, bude zásada IPsec uložena v jeho místním registru.

Agent zásad IPsec se aktivuje automaticky při spuštění systému. Pokud ve adresářové službě nebo v registru nejsou určeny žádné zásady IPsec, nebo pokud se agent nemůže připojit ke službě Active Directory, bude čekat, dokud nebude přiřazena nebo aktivována zásada.

Výměna klíčů v síti Internet

Ještě dříve, než může dojít k výměně zabezpečených dat, musí být vytvořena smlouva příslušných dvou počítačů. V této smlouvě, označované také jako přidružení zabezpečení (SA), musí oba účastníci souhlasit s výměnou a zabezpečením informací (viz obrázek 8.6).



Obrázek 8.6: Výměna klíče v síti Internet.

Aby bylo možné smlouvu mezi dvěma počítači vytvořit, zavedla organizace IETF standardní metodu přidružení zabezpečení a rozlišení výměny klíčů, označovanou jako Výměna klíče v síti Internet. Tato metoda:

- Centralizuje správu přidružení zabezpečení a tím pádem zkracuje dobu připojení,
- Generuje a spravuje ověřovací klíče, používané k zabezpečení informací.

Tento proces zabezpečuje nejen přímou komunikaci mezi dvěma počítači, ale také vzdálené počítače, u nichž je vyžadován zabezpečený přístup k podnikové síti. Je

uplatňován také v jakékoli situaci, v níž je vyjednávání cílového počítače (koncový bod) zabezpečováno směrovačem zabezpečení nebo jiným serverem proxy.

Co je to SA?

Přidružení zabezpečení (SA Security Association) je kombinace vzájemně sjednaného klíče, zabezpečovacího protokolu a čísla SPI, která definuje použité zabezpečení spojení mezi odesílatelem a příjemcem. Číslo SPI je jedinečná popisující hodnota, používána v SA k rozlišení mezi větším počtem přidružení zabezpečení existujících na počítači příjemce. Na cílovém počítači může existovat více přidružení zabezpečení, pokud tento počítač komunikuje pomocí zabezpečeného protokolu také s dalšími počítači. K této situaci dochází většinou tehdy, je-li počítač souborovým serverem nebo serverem pro vzdálený přístup mnoha klientů. V takových případech používá počítač příjemce číslo SPI, s jehož pomocí určuje, které přidružení zabezpečení bude použito ke zpracování příchozích paketů.

SA typu Phase I

K úspěšnému zajištění zabezpečené komunikace používá služba IKE dvoufázovou operaci. Důvěrnost a ověřování během obou těchto fází jsou zajištěny díky algoritmům kódování a ověřování, s jejichž používáním souhlasily oba počítače během vyjednávání. Rozdělením služby do dvou fází dochází k podstatnému zrychlení kódování.

Během první fáze vytvoří dva počítače zabezpečený a ověřený kanál – fáze I SA. Toto pojmenování vycházelo z potřeby rozlišování mezi přidružením jednotlivých zabezpečení pro každou fázi. Služba IKE během výměny automaticky zajišťuje nezbytnou ochranu totožnosti. Zaručuje, že nedojde k odeslání žádné informace, určující totožnost, aniž by byla předem zašifrována. Tímto je zajištěna dokonalá důvěrnost spojení.

Vyjednávání typu Phase I

Následující kroky probíhají během vyjednávání typu Phase I.

1. Vyjednávání zásad

Tyto čtyři povinné parametry jsou při vyjednávání nastavovány jako součást fáze I SA:

- Algoritmus kódování (DES, 3DES),
- transformační algoritmus (MD5 nebo SHA),
- ověřovací metoda (certifikát, předběžné sdílení klíčů, ověření pomocí protokolu Kerberos v5),
- skupina Diffie–Hellmanna (DH), která bude použit jako materiál pro klíčování.

Budou-li k ověření pravosti používány certifikáty nebo předběžné sdílení klíčů, bude totožnost počítače chráněna. Bude-li však použito ověřování pomocí protokolu Kerberos v5, nebude totožnost počítače zakódována, pokud nebude během ověřování zakódována také datová část zprávy.

2. Výměna DH (neboli veřejné hodnoty)

Účastníci spojení si nikdy nevyměňují skutečné klíče. K vygenerování sdíleného důvěrného klíče pomocí algoritmu DH je třeba pouze základních informací. Po provedení této výměny vygeneruje služba IKE na obou počítačích hlavní klíč, který bude použit v posledním kole: při ověření.

3. Ověření

Počítače se pokoušejí ověřovat výměnu DH. Bez úspěšného ověření pravosti nemůže komunikace pokračovat. K ověření totožnosti je ve spojení s algoritmy a metodami vyjednávání používán hlavní klíč. Celá datová část totožnosti – včetně typu, portu a protokolu – je transformována a zakódována pomocí klíčů, vygenerovaných na základě výměny DH ve druhém kole. Datová část identity je pak, bez ohledu na použitou metodu ověření, zabezpečena jak proti úpravám, tak proti analýze.

Odesílatel představuje příjemci nabídku možného přidružení zabezpečení. Reagující počítač tuto nabídku nemůže změnit. Bude-li tato nabídka změněna, zamítne iniciátor spojení zprávu reagujícího počítače. Reagující počítač odešle buď odpověď s potvrzením nabídky, nebo odpověď s možnými alternativami.

Zprávy se během této fáze opakují v pravidelných intervalech pětkrát za sebou. Po krátkém intervalu je opakování zastaveno (povoluje-li to zásada IPSec). Bude-li odpověď přijata v nastaveném intervalu, začne standardní vyjednávání o přidružení SA.

Žádný limit počtu výměn neexistuje. Počet vytvořených přidružení zabezpečení je omezen pouze dostupnými systémovými prostředky.

SA typu Phase II

V této fázi je vyjednáváno přidružení zabezpečení pro službu IPSec.

Vyjednávání typu Phase II

Následující kroky probíhají během vyjednávání typu Phase I.

1. Vyjednávání zásad

Počítače využívající protokol IPSec si vyměňují své požadavky na zabezpečení datového přenosu:

- Protokol IPSec (AH nebo ESP),
- transformační algoritmus pro ověření integrity (MD5 nebo SHA),
- algoritmus kódování, je-li vyžadován: DES, 3DES.

Je dosaženo společné dohody a jsou vytvořeny dvě přidružení zabezpečení: jedno pro vstupní a druhé pro výstupní spojení.

2. Obnovení nebo výměna materiálu klíče relace

IKE obnovuje materiál klíčování a k ověřování totožnosti a kódování (je-li vyjednané) paketů jsou generovány nové sdílené nebo důvěrné klíče. Je-li vyžadován obnovený klíč, dochází k druhé výměně algoritmu DH (viz „Vyjednávání typu Phase I“) nebo použit jeho obnovený originál.

3. Přidružení zabezpečení a klíče jsou spolu s číslem SPI předávány řadiči protokolu IPSec.

Během druhého vyjednávání sdílené zásady a materiálu klíčování (tentokrát za účelem zabezpečení datového přenosu) jsou informace chráněny přidružením zabezpečení Fáze I SA.

Vzhledem k tomu, že první fáze zajistila ochranu totožnosti, zajišťuje druhá fáze ochranu obnovením materiálu klíčování, aby nedošlo k pokusu o nápodobu přidružení zabezpečení. Proces výměny klíčů v síti Internet může zahrnovat datovou část výměny klíče, určenou pro další výměny algoritmu DH, pokud by bylo zapotřebí obnovit klíč (je povolena metoda PFS pro hlavní klíč). V opačném případě obnoví služba IKE nejprve materiál klíčování z výměny DH z první fáze.

Výsledkem fáze Phase II je dvojice přidružení zabezpečení: jedno pro příchozí spojení a druhé pro odchozí. Každé vlastní svoje číslo SPI a klíč.

Algoritmus opakování zprávy je zde téměř stejný jako v procesu „Vyjednávání typu Phase I“. Existuje pouze jeden rozdíl: Dojde-li během druhého nebo některého z následujících vyjednávání k překročení časového limitu, pokusí se počítače o obnovení vyjednávání typu Phase I SA. Kdyby byla zpráva přijata, ale nebylo by vytvořeno přidružení zabezpečení typu Phase I SA, bude zpráva zamítnuta.

Díky použití jednoho SA typu Phase I pro větší počet vyjednávání SA typu Phase II je celý proces neobyčejně rychlý. Dokud nedojde k vypršení SA typu Phase I, není třeba obnovovat vyjednávání ani ověřování. Počet možných vyjednávání přidružení zabezpečení typu Phase II je určen pomocí atributů zásady IPSec. Kdyby docházelo k častějšímu obnovování stejného klíčování typu Phase I, mohlo by dojít k ohrožení zabezpečení sdíleného důvěrného klíče.

Životnost přidružení zabezpečení

Přidružení zabezpečení typu Phase I je uloženo v mezipaměti, což umožňuje vícenásobná vyjednávání přidružení zabezpečení typu Phase II (pokud ovšem není povolena metoda PFS pro hlavní klíč nebo nebyla překročena životnost zásady klíče relace). Dojde-li k překročení životnosti hlavního klíče nebo klíče relace, bude kromě obnovení a nového vygenerování klíče vyjednáváno také nové přidružení zabezpečení.

Po překročení výchozí životnosti přidružení zabezpečení typu Phase I, respektive životnosti hlavního klíče nebo klíče relace, bude odpovídajícímu počítači odeslána odstraňovací zpráva. Odstraňovací zpráva IKE sděluje reagujícímu počítači, aby ukončil platnost přidružení zabezpečení typu Phase I. Tím se předchází možnosti nápodoby přidružení zabezpečení typu Phase II, neboť životnost přidružení zabezpečení typu Phase II je ukončována ovladačem IPSec nezávisle na životnosti přidružení zabezpečení typu Phase I. Služba IKE neukončuje přidružení zabezpečení typu Phase II, neboť počet bajtů nebo sekund, které zbývají do vypršení platnosti SA zná pouze ovladač IPSec.

Nastavování životnosti klíčů věnujte zvýšenou pozornost, aby nedocházelo ke stanovení neslučitelných hodnot. Životnost klíče určuje totiž také životnost přidružení zabezpečení. Nastavíte-li například životnost hlavního klíče na osm hodin a životnost klíče relace na dvě hodiny, může dojít k tomu, že budete mít nastaveno přidružení zabezpečení typu Phase II ještě dvě hodiny poté, co vyprší platnost přidružení zabezpečení typu Phase I. K tomu bude docházet vždy, když je přidružení zabezpečení typu Phase II generováno bezprostředně po vypršení platnosti přidružení zabezpečení typu Phase I.

Ochrana klíče

Základní prvočísla (materiál klíčování) a délka hlavního klíče a klíče relace jsou doplněny o následující funkce. Všechny funkce, s nimiž se seznámíte v tomto oddíle, jsou platné pro oba typy klíčů.

Životnost klíče

Životnost klíče určuje to, kdy bude vygenerován nový klíč (nikoli to, jak bude vygenerován). Životnost klíče, označovaná také jako dynamické obnovování klíče nebo opakované generování klíče, umožňuje vynutit si opětovné vygenerování klíče po uplynutí určeného časového intervalu. Pokud například určité spojení trvá 10 000 sekund, zatímco vy jste nastavili životnost klíče na 1 000 sekund, bude během tohoto spojení vygenerováno 10 klíčů. Tímto postupem zajistíte to, že i kdyby útočník během spojení

získal část přenášených dat, nebude schopen získat celý obsah spojení. Automatické přegenerování klíčů je nedílnou součástí protokolu. Jeho konfigurace je však volitelná. Životnost klíčů se pro hlavní klíče a pro klíče relace může lišit. Kdykoli, kdy bude dosažen konec životnosti klíče, bude také znova zahájeno vyjednávání přidružení zabezpečení. Množství zpracovaných dat pomocí jednoho klíče by nemělo překračovat 100 megabajtů. Správci by si měli ve stávajících metodických pokynech ověřit, jak by měli zajišťovat odpovídající ochranu pro všechny typy přenášených dat.

Limit obnovení klíče relace

Opakované používání stejného klíčování může ohrozit sdílený důvěrný Diffie-Hellmanův algoritmus. Z tohoto důvodu je implementován limit obnovení klíče.

Uvedme si příklad. Katka u počítače A odešle zprávu Bogdanovi u počítače B a za několik minut mu odešle další zprávu. Jako materiál klíčování lze použít stejný klíč relace, neboť mezi oběma počítači bylo v poslední době úspěšně vytvořeno přidružení zabezpečení. Chcete-li však omezit počet takových případů, snižte limit obnovení klíče relace.

Limit obnovení klíče relace bude ignorován, pokud jste pro hlavní klíč povolili metodu Perfect Forward Secrecy (PFS). Tato metoda si totiž vynucuje opětovné vygenerování klíče. Nastavení limitu obnovení klíče relace na hodnotu 1 se rovná povolení metody PFS. V případě, že jste nastavili životnost hlavního klíče i limit obnovení klíče relace, bude následující přegenerování klíče vyvoláno při výskytu první z těchto událostí. Ve výchozím nastavení protokol IPSec nemá určen žádný limit obnovení klíče relace.

Skupiny typu Diffie-Hellman

Skupiny typu Diffie-Hellman (DH) se používají k určení délky základních prvočísel (materiál klíče) pro výměnu DH. Úroveň libovolného klíče, odvozeného z výměny DH, závisí částečně na úrovni skupiny DH, na jejímž základě jsou prvočísla postavena.

Každá skupina DH definuje délku použitého materiálu klíče. Skupina 2 (střední) stojí na vyšší úrovni než Skupina 1 (nízká). Skupina 1 chrání 758 bitů materiálu klíče, Skupina 2 chrání 1024 bitů. Větší skupina označuje vyšší entropii, a tím pádem ji lze hůře prolomit.

Služba IKE obstarává vyjednávání o tom, která skupina bude použita. Tím je zajištěno, že nebude docházet ke zbytečným neúspěchům při vyjednávání, pokud by příčinou neúspěchů mělo být nesprávné přiřazení skupin DH při spojení rovnocenných partnerů.

Je-li pro danou relaci povolena metoda PFS, bude Diffie-Hellmanův algoritmus spolu s klíčem předán cílovému počítači při přenosu první zprávy vyjednávání přidružení zabezpečení typu Phase II. Toto nastavení si vynutí obnovení Diffie-Hellmanův algoritmu, což z počáteční výměny DH odstraní materiál klíčování relace.

Příjemce nemusí používat pro klíč relace metodu PFS, i když ji používá odesílatel. Pokud však tuto metodu používá pouze příjemce, skončí vyjednávání nezdarem.

Skupina DH používá stejný název jak při vyjednávání přidružení zabezpečení typu Phase I, tak při vyjednávání přidružení zabezpečení typu Phase II. Znamená to, že, bude-li použita metoda PFS, ovlivní během vytváření relace všechna obnovení klíčů, i kdyby byla skupina DH nastavena jako součást vyjednávání přidružení zabezpečení typu Phase I.

Perfect Forward Secrecy

Na rozdíl od životnosti neurčuje *metoda Perfect Forward Secrecy*, kdy má být nový klíč vygenerován, ale jak. Přesněji, metoda Perfect Forward Secrecy zaručuje, že jakékoli ohrožení zabezpečení jednoho klíče umožní přístup jen k datům chráněným právě tímto jediným klíčem – nikoli tedy k celému spojení. Aby to bylo vůbec možné, zaručuje metoda PFS, že klíč, použitý k zabezpečení přenosu v jakékoli fázi, nelze opakovaně použít k vygenerování jakýchkoli dalších klíčů. Ba co víc, pokud byl k vytvoření klíče použit určitý materiál klíčování, nelze ke generování dalších klíčů použít ani ten.

Metoda PFS pro hlavní klíč vyžaduje opakované ověření totožnosti, takže ji využívejte s rozvahou. Je-li povolena, musí služba IKE opakovaně ověřovat totožnost komunikujících počítačů, což bude způsobovat dodatečné zatížení všech radičů domény. Nastavení metody PFS také si vynucuje obnovení vyjednávání typu Phase I pro každé následné vyjednávání typu Phase II.

Metodu PFS lze pro klíč relace používat i bez opakovaného ověřování identity, proto lze také omezit zatížení použitých prostředků. Metoda PFS pro klíč relace vyvolává výměnu DH, což si vynutí vygenerování nového materiálu klíčování. Takový způsob vyžaduje přenos pouze čtyř zpráv a není v něm zapotřebí nového ověření totožnosti.

Není nutné, aby byla metoda PFS povolena na obou rovnocenných partnerských počítačích, není to totiž vlastnost, spadající do oblasti vyjednávání. Pokud příjemce vyžaduje metodu PFS a přitom dojde k vypršení platnosti přidružení zabezpečení typu Phase II odesílatele, bude jednoduše zpráva odesílatele ignorována a bude zahájeno nové vyjednávání. Odesílatel ukončí přidružení zabezpečení typu Phase I a obnoví vyjednávání. Metodu PFS lze nastavit nezávisle jak pro hlavní klíč, tak pro klíč relace.

Řadič IPsec

Řadič IPsec, s použitím seznamu filtrů IP v aktivní zásadě IPsec, hlídá odchozí pakety IP, které musí být zabezpečeny, a příchozí pakety IP, které je třeba ověřit a dekodovat.

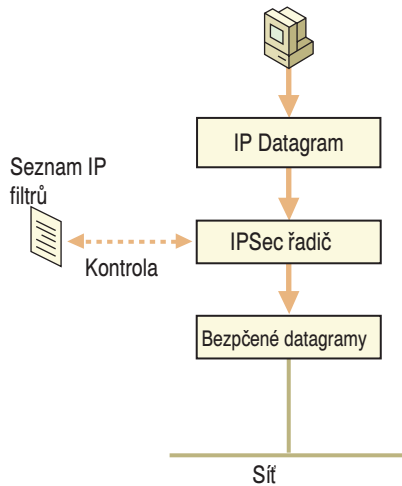
Jak je patrné z obrázku 8.7, přijímá řadič IPsec od služby Agent zásad IPsec seznam filtrů IP. Řadič IPsec hlídá, aby se všechny pakety IP odesílané z počítače shodovaly s filtrem nastaveným v uloženém seznamu filtrů IP. Odchozí zprávy inicializují vyjednávání o zabezpečení až poté, co je ověřena jejich shoda se seznamem filtrů IP. Řadič IPsec oznámí službě IKE, že může zahájit vyjednávání o zabezpečení.

Po úspěšném dokončení vyjednávání řadič IPsec na počítači odesílatele:

1. Přijme od služby IKE přidružení zabezpečení, obsahující klíč relace.
2. Vyhledá odchozí přidružení zabezpečení ve své databázi a do záhlaví IPsec vloží číslo SPI z nalezeného přidružení zabezpečení.
3. Podepíše, a vyžaduje-li to důvěrnost sdělení, také zašifruje pakety.
4. Odešle pakety s číslem SPI do vrstvy IP, aby byly předány cílovému počítači.

Řadič IPsec na počítači příjemce:

1. Přijme od služby IKE klíč relace, přidružení zabezpečení a číslo SPI.
2. Ve své databázi vyhledá příchozí přidružení zabezpečení na základě cílové adresy a čísla SPI.
3. Ověří podpis a dekoduje pakety (je-li to zapotřebí).
4. Odešle pakety řadiči TCP/IP, aby je předal přijímací aplikaci.

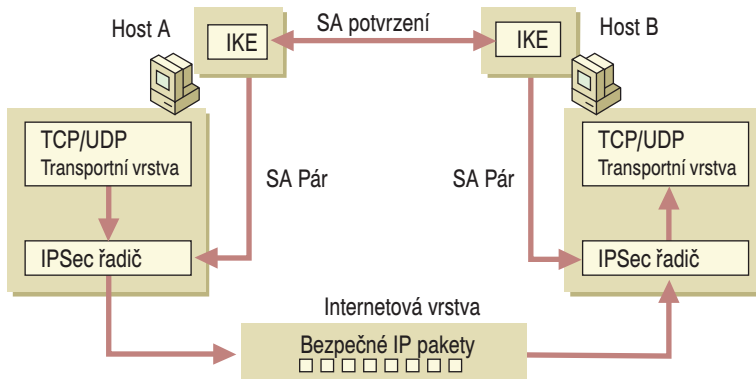


Obrázek 8.7: Služby řadiče IPSec.

Řadič IPSec ukládá v databázi všechna aktuální přidružení zabezpečení. V případě, že je v databázi těchto přidružení více, použije k určení správného přidružení zabezpečení číslo SPI, připojené k paketu.

Model IPSec

Nyní, kdy jste se postupně a podrobně seznámili s funkcemi všech součástí, je třeba přistoupit k souhrnnému pohledu. Pouze tak můžete zcela pochopit celou architekturu modelu IPSec (viz obrázek 8.8).



Obrázek 8.8: Celkový pohled: Proces IPSec.

Pro zjednodušení uvádíme, že se jedná o příklad řešení místní počítačové sítě intranet. Každý počítač zde má vlastní aktivní zásadu IPSec.

1. Katka, používající data aplikace na počítači, označeném jako HOST A, odesílá zprávu Bogdanovi, který pracuje s počítačem HOST B.
2. Řadič IPSec na počítači HOST A ověřuje uložený seznam filtrů IP, aby zjistil, zda je nutné pakety zabezpečit.

3. Řadič uvědomí službu IKE, aby zahájila vyjednávání.
4. Služba IKE na počítači HOST B přijme zprávu s požadavkem vyjednání zabezpečení.
5. Počítače spolu vytvoří přidružení zabezpečení typu Phase I i sdílený hlavní klíč.

Poznámka: Pokud hostitelské počítače A i B spolu vytvořily přidružení zabezpečení typu Phase I už v některém z předchozích spojení (kdy není zároveň povolena metoda PFS pro fázi I, ani nedošlo k vypršení životnosti klíčů), mohou okamžitě přejít k vytvoření přidružení zabezpečení typu Phase II.

6. Probíhá vyjednávání dvojice přidružení zabezpečení typu Phase II. jedno pro příchozí přidružení zabezpečení, druhé pro odchozí. Tato přidružení zahrnují klíče, použité k zabezpečení přenášných informací, a čísla SPI.
7. Řadič IPSec na hostitelském počítači A použije k vytvoření podpisu a k zakódování paketů odchozí přidružení zabezpečení.
8. Řadič předá pakety vrstvě IP, která je nasměruje směrem k počítači B.
9. Řadič síťového adaptéru hostitelského počítače B přijme zakódované pakety a předá je řadiči IPSec.
10. Řadič IPSec na hostitelském počítači B pomocí příchozího přidružení zabezpečení ověří integritu podpisu a dekoduje pakety.
11. Řadič předá dekodované pakety řadiči TCP/IP, který je předá cílové aplikaci na hostitelském počítači B.

Přestože se celý postup může na první pohled jevit jako dlouhá řada časově náročných a složitých operací, probíhá vše ve skutečnosti velmi rychle a z pohledu všech uživatelů také transparentně.

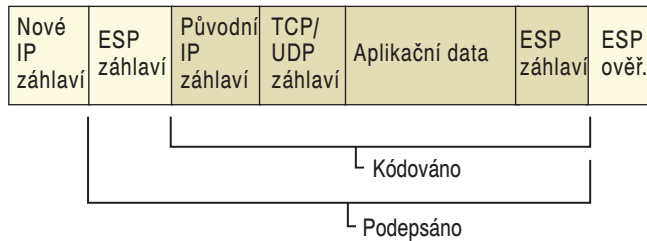
Všechny směrovače nebo přepínače, stojící na cestě mezi komunikujícími počítači, jednoduše předávají zakódované pakety IP dále, směrem k jejich cíli. Pokud se však na této cestě vyskytne bezpečnostní brána, zabezpečovací směrovač nebo server proxy, musí mít povolenou funkci předávání paketů IP, jinak by byly přenosy protokolů IPSec a IKE zamítnuty. Vyjednávání o zabezpečení nelze používat v sítích s převaděčem adres (NAT). Vyjednávání IKE obsahuje adresy IP v zakódované zprávě, které NAT nesmí měnit, jinak by došlo k narušení integrity převáděcích algoritmů či dekodování paketů.

Tunelová propojení

Tunelová propojení jsou označována také jako zapouzdření, neboť původní pakety jsou ukryty neboli zapouzdřeny uvnitř nového paketu. Tunelové propojení je logickou datovou cestou, jejímž prostřednictvím putují zapouzdřené pakety ke svému cíli. Více informací o pojmech spojených s tunelovými propojeními nebo o sjednocení protokolů L2TP a IPSec najdete v kapitole „Virtuální privátní síť“ v dokumentaci *Microsoft® Windows® 2000 Server Internetworking*. Následující oddíly se vztahují pouze na IPSec v tunelových propojeních.

Režim tunelového propojení ESP

Zatímco režim tunelového propojení obsahuje ve vnitřním záhlaví IP (původní záhlaví paketu) původní zdrojovou a cílovou adresu, vnější záhlaví IP může obsahovat pouze adresy bezpečnostních bran (viz obrázek 8.10).



Obrázek 8.10: Režim tunelového propojení ESP.

Podepsaná oblast popisuje, kde byl paket za účelem zabezpečení integrity a ověření totožnosti podepsán. Zašifrovaná oblast popisuje, jaká informace je zabezpečena pro důvěrnost.

Vzhledem k tomu, že je nové záhlaví pro tunelové propojení umístěno uvnitř paketu je vše, co následuje za podpisem záhlaví ESP (kromě koncové části ESP), nyní zapouzdřeno v paketu tunelového propojení. Původní záhlaví je přesunuto až za záhlaví ESP.

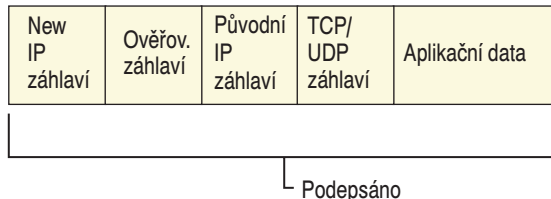
Celý paket je pak připojen pomocí koncové části ESP k předchozímu šifrování. Vše, co se nachází za záhlavím ESP, kromě koncové ověřovací části ESP, je zašifrováno, a to včetně původního záhlaví, neboť nyní je i to považováno za součást datové části.

Celá datová část ESP je tedy zašifrována uvnitř nového záhlaví tunelového propojení. To však zašifrováno není. Informace umístěné v novém záhlaví tunelového propojení je použita pouze k nasměrování paketu z místa odeslání do místa určení.

Bude-li paket procházet veřejnou sítí, bude přenesen na adresu IP serveru tunelového propojení cílové sítě intranet. Samotný paket pak bude s největší pravděpodobností určen některému z počítačů sítě intranet. Server tunelového propojení dekoduje paket, odstraní záhlaví ESP a ke konečnému nasměrování paketu použije původní záhlaví IP.

Režim tunelového propojení AH

Jediným rozdílem mezi režimy tunelového propojení AH a ESP je způsob zpracování paketu. V režimu AH je podepsán celý paket, včetně nového záhlaví tunelového propojení (v režimu ESP není zašifrováno záhlaví tunelového propojení), ale šifrování není poskytováno záhlavím AH (viz obrázek 8.11).



Obrázek 8.11: Režim tunelového propojení AH.

Režimy tunelového propojení ESP a AH lze kombinovat, čímž můžete dosáhnout tunelového propojení se zajištěním integrity celého paketu, ale také uchování důvěrnosti původního paketu IP, který obsahuje skutečně odesílaná data.

Struktura zásad IPSec

Zásady IPSec lze uplatňovat v jednotlivých počítačích, sítích, doménách nebo jakýchkoli organizačních jednotkách, které vytvoříte v rámci služby Active Directory.

Zásady protokolu IPSec by měly být založeny na metodických pokynech příslušné organizace pro zabezpečené operace. Budou-li dodržovány zásady zabezpečeného provozu, označované jako pravidla, lze tutéž zásadu uplatňovat v různorodých skupinách počítačů nebo organizačních jednotek. Více informací o používání metodických pokynů pro zabezpečené operace najdete v oddíl „Doporučené postupy“.

V zásadách IPSec lze používat pouze dvojí umístění úložiště:

1. Službu Active Directory,
2. úložiště definované v místním registru samostatného počítače nebo počítačů, které nejsou připojeny k doméně (když je počítač odpojen od důvěryhodné domény systému Windows 2000, je informace příslušné zásady dočasně uložena v registru počítače). Více informací najdete v jedné z podkapitol předchozí kapitoly, „Služba Agent zásad IPSec“.

Každá nová zásada by se měla být aplikována na scénář, přijatý při vytvoření plánu zabezpečení. Speciální konfigurační nastavení lze uplatnit při určování zásad pro server DHCP, službu DNS (Domain Name System), službu WINS (Windows Internet Name Service), protokol SNMP (Simple Network Management Protocol) nebo v případě serveru pro vzdálený přístup. Více informací najdete v oddílu „Úvahy o specifických vlastnostech zabezpečení IPSec“

Dědičnost zásad

Přednost používání zásad vychází z modelu zásad skupiny. Zásady skupiny jsou uplatňovány v hierarchickém modelu, nejméně omezeným objektem počínaje (sítí) a objektem s nejvíce omezeným přístupem konče (organizační jednotka). Více informací o službách Active Directory a Zásady skupiny najdete v kapitolách, spadajících do částí „Active Directory“ a „Správa konfigurace plochy“ v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.

Při nastavování zásad IPSec byste se měli řídit následujícími okolnostmi:

- Zásady IPSec, přiřazené k zásadě domény, přepisují místní zásady IPSec všech počítačů, jež jsou členy dané domény.
- Priorita Zásad skupiny. Zásada IPSec připojená k organizační jednotce potlačuje zásadu IPSec domény, vztahující se k účtu tohoto počítače. Zásada IPSec připojená k dceřině organizační jednotce může potlačit zásadu IPSec také pro nadřazený počítač a to podle nastavení konfigurace oprávnění pro zásady skupiny.

Pravidla

Pravidla řídí, jak a kdy bude zásada IPSec zabezpečovat probíhající komunikaci. Pravidlo poskytuje možnost spouštět a řídit zabezpečenou komunikaci, založenou na zdroji, cíli a typu přenosu IP.

Každé pravidlo obsahuje seznam filtrů IP a kolekci zabezpečovacích akcí, které budou spuštěny, dojde-li ke shodě s některou z položek seznamu filtrů:

- Akce filtrů,
- metody ověřování,
- nastavení tunelového propojení IP,
- typy připojení.

Každá zásada může obsahovat jedno nebo více pravidel. Aktivní může být jedno nebo také všechna pravidla, a to nezávisle na sobě. Můžete například vyžadovat, aby jedna zásada platila pro směrovač sítě, ale pro komunikaci v sítích intranet a Internet budete chtít používat jiné zabezpečovací akce. Pro směrovač můžete nastavit jednu zásadu, která bude obsahovat více pravidel: po jednom pro každý možný typ spojení.

Protokol IPSec obsahuje sadu výchozích pravidel, která zahrnují zpracování celé řady spojení, založených na klientech nebo serverech. Tato pravidla lze používat v existující podobě nebo je lze přizpůsobit vlastním požadavkům.

Filtrování paketů IP

Adresa IP identifikuje umístění systému počítače v síti. Každá adresa IP je vnitřně rozdělena na dvě části: identifikátor sítě a identifikátor počítače.

- Identifikátor sítě popisuje samostatnou síť v rámci větší sítě TCP/IP (tzn. v síti sítí). Tento identifikátor kromě toho slouží k jednoznačnému určení sítě v rámci rozlehlější sítě.
- Identifikátor počítače pro každé zařízení (například pracovní stanice nebo směrovač) popisuje systém uvnitř jeho vlastní sítě.

Více domé počítače mají také přiděleno více adres IP: po jedné pro každé síťové zařízení.

Filtry

Pravidlo dává možnost spouštět vyjednávání o zabezpečení spojení založených na zdroji, cíli a typu přenosu IP. Celému tomuto procesu se říká filtrování paketů IP. Díky němu má správce sítě možnost přesně definovat, jaké spouštěče budou použity pro zabezpečené, zablokované nebo předávané (nezabezpečené) přenosy IP.

Každý seznam filtrů IP obsahuje seznam filtrů. Každý filtr v seznamu filtrů IP popisuje určitou podmnožinu síťových přenosů, které budou zabezpečovány jako příchozí spojení či jako odchozí spojení.

- Filtry příchozích přenosů Vztahují se na přijímané přenosy. Umožňují cílovému počítači, aby porovnal přenos s položkami ve svém seznamu filtrů IP. Filtry příchozích spojení odpovídají na požadavky zabezpečené komunikace nebo naleznou shodu s existujícím přidružením zabezpečení a zpracují zabezpečené pakety.
- Filtry odchozích přenosů Vztahují se na přenosy, směřující z příslušného počítače směrem k určitému cíli. Spouštějí vyjednávání o zabezpečení, které musí proběhnout ještě před odesláním přenosu.

Filtr musí pokrývat celou oblast přenosů, pro něž byl vytvořen. Pokud například počítač A bude vždy vyžadovat zabezpečené přenosy na počítač B, tak je zapotřebí zajistit následující:

- Aby počítač A mohl odesílat na počítač B pouze zabezpečená data, musí mít pravidlo IPSec příslušný filtr pro odchozí pakety směřující na počítač B.
- Aby mohl počítač B přijímat pouze zabezpečená data z počítače A, musí mít obsahovat zásadu IPSec s filtrem pro všechny příchozí pakety z počítače A.

Filtr obsahuje následující parametry:

- Adresy zdroje a cíle paketu IP. Tyto hodnoty lze nakonfigurovat na libovolném stupni seskupení, tedy i jako jedinečnou adresu IP, nebo také jako globální adresu, sdružující členy celé podsítě nebo sítě.
- Protokol použitý pro přenos paketů. Výchozí hodnota pokrývá všechny protokoly sady TCP/IP. Přesto však lze tuto hodnotu nakonfigurovat na jakoukoli úroveň protokolu tak, aby to vyhovovalo vlastním specifickým požadavkům (včetně čísel protokolů).
- Port zdroje a cíle protokolů TCP a UDP. Tato hodnota ve výchozím nastavení také pokrývá všechny porty, ale lze ji nakonfigurovat tak, aby byla uplatňována pouze na pakety odesílané nebo přijímané prostřednictvím určitého portu daného protokolu.

Akce filtrů

Akce filtrů nastavuje požadavky zabezpečení pro určitý typ spojení. Tyto požadavky jsou určeny v seznamu zabezpečovacích metod, obsaženém v akci filtru. Zde jsou zahrnuty algoritmy, zabezpečovací protokoly a vlastnosti klíčů.

Akci filtru lze nakonfigurovat jako:

- Zásadu předávání Tato zásada nepovoluje zabezpečené spojení. Protokol IPSec v tomto případě jednoduše přenos ignoruje. Zásada je vhodná zejména v případech, kdy přenos nelze zabezpečit, neboť vzdálený počítač nevyužívá zabezpečení protokolem IPSec, nebo v případech, kdy přenos neobsahuje takové informace, které by bylo nutné zabezpečovat. Do této skupiny spadají také přenosy s vlastním zabezpečením (například protokoly Kerberos, SSL či PPTP).
- Zásadu blokování Přeruší spojení s nepřátelským počítačem.
- Zásadu, která vyjednává o zabezpečení, ale i přesto povoluje přenosy i na počítače bez podpory protokolu IPSec. Akci filtru lze konfigurovat tak, aby se postupně vytrácela. Chcete-li konfigurovat takový typ akce, nastavte v seznamu filtrů IP minimální obor platnosti. Takové nastavení byste však měli používat velmi opatrně. U všech spojení, ovlivněných touto zásadou může totiž docházet k tomu, že po neúspěšném vyjednávání o zabezpečení se přenos přece jen uskuteční. Pokud iniciátor vyjednávání IKS přijme odpověď příjemce, vyjednávání nedovolí zánik akce.

Typy připojení

Připojením se rozumí vše, co vytvoříte v konzole **Síťová připojení** systému Windows 2000.

Výběrem typu připojení pro každé pravidlo je možné určovat, která připojení počítače (rozhraní) budou ovlivněna příslušnou zásadou IPSec – adaptér telefonického připojení sítě či síťová karta. Každé pravidlo má vlastnost Připojení, která určuje, zda bude pravidlo uplatňováno pro více připojení nebo pouze pro jedno z nich. Můžete mít napří-

klad pravidlo, které bude vyžadovat velmi vysoké zabezpečení pro telefonické připojení sítě, zatímco v případě místní sítě (LAN) nebude vyžadovat zabezpečení žádné.

Ověřování

Pomocí pravidel lze určit vícenásobné metody ověřování a tím zajistit, aby jednotlivé počítače v síti používaly společnou metodu.

Zabezpečení IPSec využívá následující metody ověřování:

- Ověření totožnosti pomocí protokolu Kerberos v5 je výchozí technologií v systému Windows 2000. Tuto metodu ověřování lze používat u všech klientů s protokolem Kerberos v5 (ať už jsou, nebo nejsou klienty systému Windows 2000), kteří jsou členy důvěryhodné domény. Více informací o protokolu ověřování Kerberos v5 najdete v kapitole „Ověřování“ v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.
- Používání certifikátu veřejného klíče v případech, kdy je zapotřebí využít přístupu přes síť Internet, nebo pro vzdálené společné prostředky, při komunikaci s externími obchodními partnery, u volání protokolem L2TP nebo při komunikaci s počítači bez protokolu Kerberos v5. Tento způsob ověřování totožnosti vyžaduje konfiguraci alespoň jednoho certifikačního úřadu. Více informací o infrastruktuře certifikátů a veřejných klíčů v systému Windows 2000 najdete v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.

Služba IKE v systému Windows 2000 je slučitelná s několika certifikačními systémy, včetně systémů, poskytovaných společnostmi Microsoft, Entrust, VeriSign a Netscape. Služba IKE využívá při zpracovávání certifikátů v systému Windows 2000 funkce rozhraní Cryptographic API verze 2.0 (CAPIv2). IKE nevyžaduje žádný specifický typ certifikátu, pouze ten, jenž je uložen na účtu počítače a který má platný podpis, je v kořenovém úložišti důvěryhodných certifikátů a je používán před vypršením doby platnosti.

Certifikáty, získané pomocí služby Microsoft Certificate Services a s upřesněním **Povolit silnou ochranu soukromého klíče**, nebudou při ověřování pomocí služby IKE fungovat. Musíte vybrat certifikační úřad, jenž příslušný certifikát vašemu počítači vystavil, nebo kořenové úložiště důvěryhodných certifikátů (certifikační úřad – CA).

Při ujednání certifikátu je zapotřebí spolupráce se správcem vzdáleného počítače, jinak by nemuselo být vyjednávání o výměně klíčů v síti Internet úspěšné. Více informací o certifikátech, konfiguraci certifikačního úřadu a odvolání najdete v kapitole „Distribuované zabezpečení“ v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.

- Podporu předběžného sdílení klíčů. Jedná se o sdílený důvěrný klíč, na němž se v předchozí fázi vyjednávání shodli oba účastníci spojení. Používání tohoto typu klíče je velmi rychlé a nevyžaduje, aby klient používal protokol Kerberos v5 nebo měl certifikát veřejného klíče. Obě strany musí ručně nakonfigurovat své zásady zabezpečení IPSec, v nichž budou mechanismu předběžného sdílení klíčů využívat. Tento způsob zabezpečeného spojení lze v omezené míře používat tam, kde nelze využít metody ověření podle protokolu Kerberos v5 nebo na základě vystaveného certifikátu. Tento typ ověření totožnosti je určen pouze pro účely zabezpečení a nelze jej využít pro zašifrování dat. Viz oddíl „Doporučené postupy“ dále v této kapitole.

Společnost Microsoft nedoporučuje časté používání tohoto typu ověřování, neboť ověřovací klíč je uložen v nechráněné podobě v zásadě zabezpečení IPSec. Metodologie používání předběžně sdíleného klíče poskytuje možnost spolupráce s jinými standardy, zavedenými komisí IETF. Tuto metodu lze bezpečně používat až tehdy, bude-li přístup k příslušné zásadě umožněn pouze správci, bude-li při spojení mezi řadičem domény a členskými počítači domény zásada zašifrována na každém počítači a bude-li k ní na těchto počítačích povolen pouze systémový přístup.

Při používání metody předběžného sdílení klíčů se doporučuje používat ověření podle protokolu Kerberos v5 nebo na základě vystaveného certifikátu a tím zvyšovat také jejich zabezpečení.

Plánování zabezpečení protokolem IPSec

Následující oddíly lze považovat za jakési metodické pokyny při plánování zabezpečení IPSec.

Doporučené postupy

Modul Správa zásad zabezpečení protokolu IP v systému Windows 2000, umístěný v konzole Microsoft Management Console (MMC), zavedení zásad ve velké míře zjednodušuje. Chcete-li využít jeho možností a předejít problematickým implementacím, měli byste dodržovat následující principy.

- Zhodnotit typ přenášené informace – zda se jedná o choulostivá finanční data, zákonem chráněné informace nebo elektronickou poštu. Některá oddělení mohou vyžadovat vyšší stupeň zabezpečení než zbytek podniku už ze samotné povahy jejich funkce.
- Určit, kde jsou informace uloženy, jak jsou v síti směrovány a ze kterých počítačů lze k těmto informacím získat přístup. Takto zjistíte potřebné informace o rychlosti, kapacitě a využití sítě ještě před zavedením protokolu IPSec, což vám pomůže při optimalizaci výkonu.
- Zhodnotit možnosti zranitelnosti sítě ze strany útoků, popisovaných v úvodu kapitoly.
- Navrhnout a zdokumentovat plán zabezpečení celé podnikové sítě. Přitom je třeba zohlednit:
 - Obecný aplikační rámec zabezpečení systému Windows 2000, včetně modelu Active Directory, a způsob, jakým je zabezpečení uplatňováno na objekty zásad skupiny,
 - pravděpodobné scénáře probíhajících komunikací: intranet, vzdálený přístup, síť extranet s obchodními partnery, komunikace mezi sítěmi (směrovač-směrovač),
 - stupeň zabezpečení každého scénáře. Můžete se například rozhodnout, že budou zabezpečena pouze spojení se sítí Internet.
- Navrhnout, vytvořit a otestovat zásady zabezpečení IPSec pro všechny scénáře vašeho plánu. To umožňuje uspořádat a upřesnit to, které zásady a jaké jejich struktury jsou pro váš záměr zapotřebí.

Vytvoření plánu zabezpečení IPSec

Implementace zabezpečení IPSec, ať už v rámci velké domény nebo malé pracovní skupiny, znamená nalezení rovnováhy mezi snadným přístupem k informacím ze strany velkého počtu uživatelů a zabezpečením choulostivých informací před neoprávněným přístupem.

Nalezení takové rovnováhy vyžaduje:

- Vyhodnocení rizika a určení vhodného stupně zabezpečení celé organizace,
- určení cenných informací,
- definici zásad zabezpečení, která využívají kritéria správy nebezpečí a zabezpečují určené informace,
- stanovení nejlepších způsobů implementace zásad v existující správě dané organizace,
- zajištění vhodné technologie a její správy,
- poskytnutí zabezpečeného, ale zároveň efektivního přístupu ke všem prostředkům, které uživatelé potřebují ke své práci.

Tyto úvahy o zabezpečení jsou ovlivněny okolnostmi provozu, v němž je počítač používán. Požadavky na zabezpečení se mohou například lišit podle toho, zda je počítač řadičem domény, serverem WWW, serverem pro vzdálený přístup, souborovým serverem, databázovým serverem, serverem sítě intranet nebo například vzdáleným klientem.

Aplikační rámec zabezpečení v systému Windows 2000 splňuje i ta nejpřísnější měřítka. Přesto však bude samotný software bez pečlivého naplánování a vyhodnocení úkolů, bez efektivně navržených metodických pokynů, vykonání, revizí a navržení a zavedení zásad zabezpečení choulostivých informací méně efektivní.

K definici standardního zabezpečení neexistují žádné přesné definice nebo měřítka. Standardní stupeň zabezpečení se může lišit od implementaci k implementaci, a to v závislosti na zásadách organizace a její infrastruktuře. Následující stupně zabezpečení lze považovat za obecný základ pro plánování a zavádění zabezpečovacího protokolu IPSec.

Minimální zabezpečení

Počítače si mezi sebou žádná citlivá data nevyměňují. Zabezpečení IPSec je ve výchozím nastavení vypnuto. K vypnutí tohoto zabezpečení není zapotřebí žádného zásahu správce.

Standardní zabezpečení

Počítače, zejména souborové systémy, se používají k uchovávání cenných dat. Zde je třeba nastavit vyvážené zabezpečení, aby se ono samo nestalo překážkou pro oprávněné uživatele, kteří budou chtít s uloženými daty vykonávat požadované operace. Systém Windows 2000 poskytuje předdefinované zásady IPSec. Tyto zásady jsou určeny pro data, která by měla být zabezpečena, ale přesto nevyžadují nejvyšší stupeň zabezpečení: Klient (Jen odpovědět) a Server (Vyžaduje zabezpečení). Tato (nebo podobná vlastní) zabezpečení, optimalizují efektivitu, aniž by byla ohrožena bezpečnost dat.

Vysoký stupeň zabezpečení

Počítače, které obsahují vysoce choulostivá data, mohou být cílem krádeže s cílem náhodného či úmyslného poškození systému. Takové nebezpečí hrozí zejména při telefonickém připojení sítě nebo u všech spojení ve veřejné síti. Předdefinovaná zásada Zabezpečený server (vyžaduje zabezpečení) vyžaduje zabezpečení IPSec pro všechny odslané nebo přijaté přenosy. Zabezpečený server (vyžaduje zabezpečení) zahrnuje silný algoritmus pro zajištění důvěrnosti a integrity, metodu Perfect Forward Secrecy, životnost klíče, jejich limity a skupiny Diffie-Hellman.

Úvahy o specifických vlastnostech zabezpečení IPSec

Následující úvahy vám mohou pomoci při zjednodušení správy zásad IPSec:

Seznamy filtrů IP

Tento výčet obsahuje seznam doporučení pro práci se seznamy filtrů IP:

- Chcete-li pokrýt správu skupiny počítačů pouze jedním filtrem, používejte filtry obecné. Například v dialogovém okně Vlastnosti filtru používejte možnost Žádná adresa nebo adresu IP podsítě, nikoli adresu IP určitého zdroje či cíle daného počítače.
- Definujte filtry, které vám umožní seskupovat a zabezpečovat přenosy z logický přidružených sektorů sítě.
- Pořadí používání filtrů souvisí s pořadím jejich zobrazení při prohlížení zásady IPSec. Služba Agent zásad IPSec přijímá nezávisle všechna data ihned při spuštění systému a setřídí je od nespecifičtějších až po nejobecnější. Neexistují žádné záruky, že bude určitý specifický filtr použit ještě před uplatněním obecnějšího filtru, a to až do doby jejich zpracování. To může v určitém smyslu ovlivnit některá spojení při spuštění systému.

Akce filtrů

Následující výčet obsahuje seznam doporučení pro práci se akcemi filtrů:

- Budete-li chtít zamezit komunikaci s nepřátelskými cílovými počítači, zajistěte, aby nedocházelo k vyjednávání o zabezpečení přenosu nepodstatných dat nebo k přenosu dat mezi počítači, nepoužívajícími protokol IPSec. V takových případech použijte Akce filtru jako zásadu blokovacího nebo předávacího mechanismu.
- Při konfiguraci vlastních metod zabezpečení nastavte důvěrnost zabezpečení datové části zprávy zapouzdřením, pokud příslušné kódování zajišťuje vyšší vrstva, na hodnotu Žádné.
- V případě scénářů, počítajících s počítači se vzdáleným přístupem (včetně tunelového propojení), uvažujte o seznamu zabezpečovacích metod, jež určí vyšší stupeň zabezpečení, jako například 3DES, dále pak o krátkých intervalech životnosti klíčů (menší než 50 MB) a o metodě Perfect Forward Secrecy pro hlavní klíč a klíč relace. Tím můžete předejít útokům vedeným na základě znalosti klíče.

Spojení se vzdáleným přístupem

Následující výčet obsahuje seznam doporučení pro zpracování vzdálených přístupů:

- Seznam ověřovacích metod musí zahrnovat certifikáty. Pro spojení musí být alespoň na jednom z počítačů definován certifikát veřejného klíče (vzdálený klient

nebo server pro vzdálený přístup). Řadiče domény v systému Windows 2000 lze konfigurovat jako členy, automaticky se zapisující na certifikačním úřadu.

- Vyžadujete-li v podniku možnost vzdálené správy počítačů, musíte k aktivní zásadě zabezpečení IPSec připojit pravidlo, které zakáže blokování přenosů RPC TCP, pokud přicházejí z vnitřní sítě. (Tento typ přenosů používají v systému Windows 2000 nástroje konfigurace se vzdáleným přístupem.) Uvedme si příklad.
 - Seznam filtrů IP v pravidle by měl určovat výstupní adresu společné podsítě (umístění konzoly systémového řízení) a přichází adresu IP spravovaného počítače. Nastaveným protokolem by měl být TCP.
 - Akce filtru tohoto pravidla by měla mít nastavené tyto parametry: **Přijímat nezabezpečenou komunikaci** a **Povolit komunikaci s počítači, které nepodporují protokol IPSec**.

SNMP

Pokud počítač využívá službu SNMP, musíte k zásadě přidat pravidlo, které zamezí za-blokování zpráv SNMP:

- Seznam filtrů IP by měl obsahovat určení zdrojové a cílové adresy systému správy služby SNMP a příslušných agentů. Vlastnost Typ protokolu by měla být nastave-na na UDP a komunikace by měla probíhat mezi porty 161 a 162. To vyžaduje nastavení dvou filtrů: jednoho pro přichodí a odchozí komunikaci portu UDP 161 a druhého pro přichodí a odchozí komunikaci portu UDP 162.
- Nastavte akci filtru na Povoleno, což zajistí blokaci vyjednávání o zabezpečení a předá dál všechny přenosy, které odpovídají příslušnému seznamu filtrů IP.

Zabezpečovací brány

Na zabezpečovací bráně, bezpečnostní bráně, serveru proxy, směrovači nebo jiném ser-veru, jenž je styčným bodem mezi místní sítí intranet a vnějším světem, je zapotřebí specifického způsobu filtrování, aby pakety, zabezpečené pomocí protokolu IPSec, ne-byly zamítnuty. Na těchto počítačích je třeba definovat alespoň filtry rozhraní sítě Inter-net.

Vstupní filtry

- Protokol IP s identifikátorem 51 (0x33) pro přichodí přenosy se záhlavím pro ově-ření IPSec,
- protokol IP s identifikátorem 50 (0x32) pro přichodí přenosy s protokolem zabez-pečení datové části zprávy zapouzdřením,
- port UDP 500 (0x1F4) pro přichodí přenosy s vyjednáváním výměny klíčů v síti Internet.

Výstupní filtry

- Protokol IP s identifikátorem 51 (0x33) pro odchozí přenosy se záhlavím pro ově-ření IPSec,
- protokol IP s identifikátorem 50 (0x32) pro odchozí přenosy s protokolem zabez-pečení datové části zprávy zapouzdřením,
- port UDP 500 (0x1F4) pro odchozí přenosy s vyjednáváním výměny klíčů v síti Internet.

Služby DHCP, DNS a WINS; řadiče domény

Před zavedením protokolu IPSec na počítačích, které fungují jako servery služby DHCP, DNS WINS nebo jako řadiče domény, určete, zda všichni klienti také spolupracují se standardem tohoto protokolu. Není-li tomu tak, nebude zásada IPSec nakonfigurována způsobem, který by umožňoval uvolnění zásady nebo povoloval nezabezpečené přenosy se staršími klienty. Vyjednávání o zabezpečení může neočekávaně selhávat a přístup k těmto síťovým prostředkům může být následně zablokován.

Předdefinované konfigurace

Systém Windows 2000 obsahuje sadu předdefinovaných konfigurací protokolu IPSec. Standardně jsou všechny předdefinované zásady navrženy pro počítače, jež jsou členy domény systému Windows 2000. Předdefinované zásady, seznamy filtrů a jejich akcí nejsou určeny k okamžitému použití. Jsou určeny spíše k testovacím účelům při zavádění služby. Při různých nastaveních těchto zásad lze také očekávat jiné chování systému.

Následující oddíly obsahují popis předdefinovaných zásad IPSec v systému Windows 2000.

Klient (Jen odpověď)

Tato zásada je určena pro počítače, jež (ve většině případů) nezabezpečují svá spojení. Například klienti v síti intranet nemusí vyžadovat zabezpečení protokolem IPSec, odpovídají-li na požadavek jiného počítače. Uvedená zásada umožňuje takto nastaveným počítačům vhodně reagovat na požadavky zabezpečených spojení. Obsahuje pravidlo Výchozí reakce, které povoluje vyjednávání s počítači, vyžadujícími IPSec. V těchto případech je zabezpečen pouze požadovaný protokol a přenos přes port.

Server (Vyžaduje zabezpečení)

Tato zásada je určena pro počítače, které (ve většině případů) svá spojení zabezpečují, jako například pro servery, jež přenášejí choulostivá data. Tato zásada povoluje počítači přijmout nezabezpečené přenosy, ale vždy se pokusí zabezpečit dodatečná spojení, požadavkem zabezpečení na odesílateli. Umožňuje také průběh zcela nezabezpečených komunikací, pokud počítač na druhém konci spojení nepracuje s protokolem IPSec.

Zabezpečený server (Vyžaduje zabezpečení)

Tato zásada je určena pro počítače, jež zabezpečená spojení vyžadují vždy. Příkladem může být server, který přenáší velmi choulostivá data. Zásada umožňuje zpracování nezabezpečených příchozích přenosů, ale vždy zabezpečuje odchozí komunikaci.

Předdefinovaná pravidla

Stejně jako je tomu v případě předdefinovaných zásad, lze pravidlo Výchozí reakce uplatnit bez dalších úprav jako šablonu při definování vlastních pravidel. Toto pravidlo je automaticky přidáno ke každé nové zásadě, ale neaktivuje se automaticky. Je určeno pro všechny počítače, jež nevyžadují zabezpečení, ale musí být schopny příslušným způsobem odpovědět, když jiný počítač zabezpečenou komunikaci vyžaduje.

Předdefinované akce filtru

Stejně jako v předchozích dvou případech lze i předdefinované akce filtrů okamžitě použít, upravit nebo dále používat jako šablonu při definování vlastních akcí filtrů. Lze je použít v libovolném existujícím nebo novém pravidle:

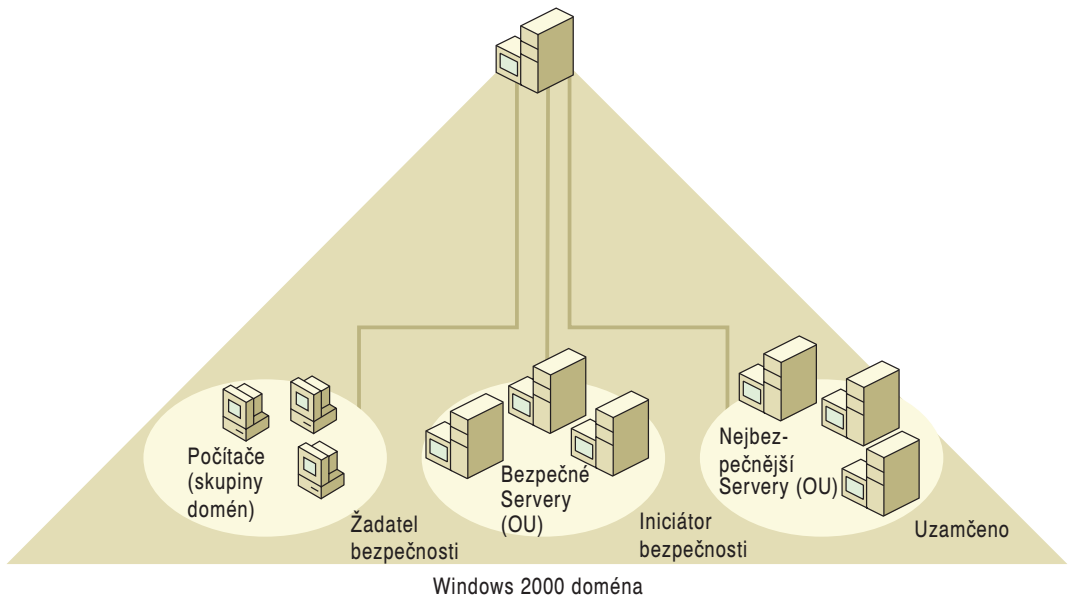
- Vyžaduje zabezpečení Vysoký stupeň zabezpečení. Není povolen žádný nezabezpečený přenos.
- Požadované zabezpečení (nepovinné) Střední nebo nízký stupeň zabezpečení. Je povoleno přenášet nezabezpečená data, aby bylo možné navázat spojení mezi počítači, jež z nějakých důvodů nemohou vyjednávat o zabezpečení IPSec.

Obecně použitelný příklad zabezpečení IPSec

Tento příklad popisuje příklad zavedení obecně použitelné konfigurace zabezpečení IPSec. I když se může základní konfigurace vaší sítě lišit, základní principy zůstávají stejné.

Zabezpečení skupin počítačů, které si mezi sebou běžně vyměňují důvěrné informace, zpravidla vyžaduje segmentaci podnikové sítě. Skupiny počítačů v samostatných fyzických sektorech účinně předcházejí narušení zabezpečení. Protokol IPSec zajišťuje ochranu, přičemž umožňuje skupinám zabezpečených počítačů být součástí stejné fyzické podnikové sítě intranet.

Na obrázku 8.14 je znázorněna doména, zahrnující počítače finančního oddělení. Většina klientů sítě intranet nemusí mezi sebou komunikovat zabezpečenými spoji. Přesto však určitá skupina serverů obsahuje velmi důvěrná data, k nimž někteří klienti nemusí mít přístup. Všechny počítače mají ve službě Active Directory vlastní účet.



Obrázek 8.14: Doména sítě intranet s modelem zabezpečení koncových uživatelů.

Účty počítačů jsou z bezpečnostních důvodů seskupeny v organizačních jednotkách služby Active Directory. Tento způsob uspořádání umožňuje vhodné nastavení zásad IPSec, založených na funkci příslušných počítačů:

- Servery, které uchovávají a vyměňují velmi důvěrná data, patří do organizační jednotky Servery s nejvyšší úrovní zabezpečení.
- Servery, jež mohou používat nezabezpečená spojení k tomu, aby si mohly vyměňovat data s počítači bez systému Windows 2000 v doméně organizační jednotky Zabezpečené servery.
- Klienti, jež vyžadují schopnost odpovídajícím způsobem odpovídat na požadavky zabezpečeného spojení. Tito klienti patří do výchozí skupiny Počítače.

Seskupování počítačů do organizačních jednotek umožňuje přiřazovat zásady IPSec pouze těm počítačům, které to skutečně vyžadují. Lze tím pádem nastavit příslušný stupeň zabezpečení a vyhnout se nadměrnému zatížení systému zabezpečovacími pravidly. V tomto scénáři jsou ve službě Active Directory uloženy zásady IPSec všech počítačů.

Je zbytečné nastavovat vysoký stupeň zabezpečení přenosů mezi klienty a řadiči domény: výměny dat, chráněných protokolem Kerberos, mezi těmito počítači jsou již standardně zašifrované a přenos zásad IPSec ze služby Active Directory na členské počítače je v systému Windows 2000 chráněn protokolem LDAP.

V tomto příkladu by měl být protokol IPSec zkombinován se zabezpečeným řízením přístupu. Oprávnění jednotlivých uživatelů jsou i nadále nedílnou součástí řízení přístupu ke sdíleným souborům, dostupným ve skupině serverů s nejvyšší nebo vysokou úrovní zabezpečení. Protokol IPSec zabezpečuje přenosy na úrovni sítě, takže útočníci nejsou schopni analyzovat, ani upravovat data. Více informací o nastavování uživatelských práv najdete v nápovědě online k operačnímu systému Windows 2000.

Vyžadovaná zabezpečení

Při zavádění zabezpečení protokolem IPSec byste měli vzít v úvahu následující zásady.

Počítače: Klient (Jen odpovědět)

Počítače, jež jsou členy domény, přijímají zásady IPSec, připojené k zásadě zabezpečení domény. Předdefinovaná zásada Klient (Jen odpovědět) je připojena k zabezpečovací zásadě domény pro skupinu a zabezpečuje tyto počítače podle aktuálních potřeb pro zabezpečené komunikace.

Zabezpečené servery: Server (Vyžaduje zabezpečení)

Účty počítačů v této organizační jednotce komunikují mezi sebou zpravidla prostřednictvím zabezpečených spojů, mohou však komunikovat také s počítači, jež nemohou odpovědět na požadavek zabezpečení. Přiřazením této předdefinované zásady umožňujete podle potřeby inicializaci zabezpečeného spojení, ale také spojení s počítači se staršími operačními systémy, které mohou být součástí domény.

Servery s nejvyšší úrovní zabezpečení: Zabezpečený server (Požaduje zabezpečení)

Účty počítačů v této organizační jednotce nekomunikují s žádnými počítači, které nemohou vyjednávat o zabezpečení. Tyto servery ukládají a přenášejí mezi sebou vysoce choulostivá data. Tato předdefinovaná zásada je skupině přiřazována k zajištění toho,

aby se odchozí komunikace nikdy neuchýlila k nezabezpečenému přenosu, když selže zahájené vyjednávání nebo počítač na druhé straně spojení nepoužívá protokol IPSec. Zabezpečené jsou po předchozím vyjednávání také přenosy mezi počítači této skupiny a řadičem domény. Díky přísnosti této zásady budete možná nuceni k rozšíření zásady o výjimky, vztahující se například na přenosy SNMP. Více informací o úpravách zásady IPSec „Úvahy o specifických vlastnostech zabezpečení IPSec“.

Odstraňování problémů

Tato podkapitola obsahuje popis metod, používaných pro snazší určení příčin problémů, vzniklých při komunikaci prostřednictvím protokolu IPSec, stejně jako nástrojů, které mohou ověřovat komunikace, zabezpečené protokolem IPSec.

Poznámka: Selhání v jádru síťových služeb jako DHCP, DNS a WINS může způsobit nepředvídané chyby v protokolu IPSec.

Odstraňování obecných problémů

V následujících odstavcích se můžete seznámit s možnými příčinami chyb zabezpečených komunikací a s navrhanými řešeními těchto nenadálých situací.

Selhání komunikace se vzdáleným počítačem

Jste-li uživatelem vzdáleného klienta, jenž selhává pouze při pokusu o navázání zabezpečeného připojení, vraťte se k oddílu „Doporučené postupy“, uvedenému dříve v této kapitole. V něm se můžete dočíst o možných scénářích komunikace se vzdálenými počítači. Podle těchto informací tak můžete zkontrolovat, zda vámi používaná metoda ověřování je správná a zda používáte metody slučitelné s metodami zabezpečení, používanými na serveru pro vzdálený přístup.

Selhání komunikace uvnitř sítě intranet

Jestliže dva počítače spolu po nějakou dobu komunikovaly a najednou došlo k neočekávanému přerušení spojení, postupujte podle následujících kroků:

1. Pomocí příkazu PING ověřte, zda je počítač i nadále registrován v síti. Měli byste dostat zprávu, že momentálně probíhá vyjednávání o zabezpečení IPSec. Nedostanete-li tuto zprávu, ověřte, zda se seznam použitelných zabezpečovacích metod vaší akce filtru o posledního připojení nějak nezměnil. V seznamu mohou být aktivní některá starší přiřazení zabezpečení, která byla definována ještě v předchozích metodách zabezpečení. Je-li tomu tak, pokračujte dalším krokem. Pamatujte si, že používáte-li výchozí neupravené zásady, budou příkazy ping protokolem IPSec zablokovány. Ale i když jste si vytvořili vlastní zásady a nevyňali přitom protokol ICMP, používaný nástrojem Ping, může spojení dojít k chybě a následnému ukončení.
2. Restartujte službu Agent zásad. Tento krok zajistí vymazání všech starších přiřazení zabezpečení. Více informací o restartování služby Agent zásad najdete v oddíle „Selhávají pouze spojená zabezpečení protokolem IPSec“.

Jiné příčiny selhání

- Ověřte integritu zásad, abyste zjistili, zda se změny v nastaveních zásad přenesly do služby Active Directory nebo do registru. Více informací o testování integrity zásad najdete v nápovědě online k operačnímu systému Windows 2000.
- Pokud jste příslušný počítač vyňali z domény nebo jste změnili jeho nastavení tak, aby používal místo zásady Active Directory zásadu místní, budete asi muset znova spustit službu Agent zásad. Jinak by agent zásad pokračoval v pokusech spojit se se službou Active Directory a nepoužíval by zásadu, uloženou v registru místního počítače.
- Vícedomé počítače mají více výchozích spojení, což také může způsobovat problémy.

► Při určování výchozího spojení

1. V příkazovém řádku запиšte následující příkaz a stiskněte klávesu Enter:

```
route print
```

2. Ověřte, zda se adresa 0.0.0.0 objeví jako cíl v jednom nebo více řádcích a zda se s nejnižší metrickou hodnotou (obvykle 1) zobrazí jeden nebo více řádků spojení.
3. Je-li splněna některá z těchto podmínek, vymažte jedno z výchozích spojení nebo ověřte, zda má jedno z nich menší metrickou hodnotu než ostatní.

Řešení základních problémů, spojených s protokolem IPSec

V následujících oddílech se budeme věnovat některým metodám, používaných při řešení základních problémů, spojených s protokolem IPSec.

Chyba vyvolaná nesprávným přiřazením zásady IPSec

Selhání vyjednávání o zabezpečení může být důsledkem nekompatibilních nastavení zásad IPSec. Pokuste se tuto nekonzistenci odstranit pomocí následujících kroků:

1. Spusťte nástroj Prohlížeč událostí a prohlédněte si protokol zabezpečení. Zápis o posledně vyvolaných událostech zahrnuje také pokusy o vyjednávání IKE s popisem úspěchu operace nebo příčin nezdaru.
2. Projděte protokol zabezpečení na počítači, určeném adresou IP v zprávě protokolu.
3. Určete příčinu nesprávného přiřazení zásady a:
 - ověřte, zda jsou slučitelné metody ověřování,
 - ověřte, zda existuje mezi oběma počítači alespoň jedna slučitelná zabezpečovací metoda.

Zprávy „Chybné pakety SPI“ v Prohlížeči událostí

K této chybě může dojít, je-li životnost klíče příliš krátká nebo interval přidružení zabezpečení vypršel, ale odesílatel pokračuje v odesílání dat příjemci. Tato chyba nemá vliv na přenášené informace a měla by přitáhnout vaši pozornost pouze v případě svého nadměrného výskytu. Chcete-li určit její příčinu a opravit problém, postupujte podle následujících kroků:

1. Spusťte program IPSecMon.
2. Prozkoumejte počet překlíčování.

Je-li jejich počet příliš vysoký ve srovnání s aktivní dobou trvání spojení, prodlužte životnost klíče v zásadě. Při velkém provozu u připojení v sítích Ethernet se doporučuje nastavit hodnoty větší než 50 MB a delší než pět minut.

Takové nastavení sice nevylučuje následné výskyty chybných paketů SPI, ale přinejmenším podstatnou měrou snižuje jejich počet.

Ověřování spojení zabezpečených protokolem IPSec

V tomto oddílu se budeme zabývat nástroji a procedurami, které lze používat k určování, zda je protokol IPSec aktivní, a k zajištění úspěšných přenosů informací, zabezpečených právě tímto protokolem.

Používání příkazu PING k ověření platnosti síťového připojení

Následující procedura určuje, zda lze vytvořit standardní, nezabezpečené spojení. Díky ní lze snadno oddělit problémy způsobené sítí od problémů vyvolaných používáním protokolu IPSec.

1. Otevřete okno příkazového řádku.
2. Zapište následující příkaz:

```
ping <adresa IP>
```

V tomto příkazu zastupuje proměnná *<adresa IP>* skutečnou adresu IP počítače, s nímž se pokoušíte spojit.

Na tento příkaz byste měli dostat odpověď. Přijatá odpověď znamená, že můžete se svým partnerem komunikovat. Budete-li používat přednastavené a neupravené zásady, nebude příkaz ping zablokován. Pokud jste však vytvořili vlastní zásady a neuvolnili v nich protokol ICMP, používaný nástrojem PING, bude volání tímto příkazem neúspěšné.

V případě, že na volání příkazu **ping** nedostanete žádnou odpověď, projděte si kapitulu „Řešení problémů protokolu TCP/IP“ a pokuste se určit příčinu nezdaru.

Ověření, zda byla zásada vůbec přidělena

Následující procedury můžete používat k ověření, zda je přiřazená zásada aktivní.

Sledování IPSec

1. Klepněte na tlačítko **Start** a potom vyberte položku **Spustit**.
2. V příkazovém řádku zapište tento příkaz:

```
ipsecmon <název počítače>
```

Po otevření okna programu Sledování IPSec se v pravém spodním rohu zobrazí zpráva, zda je na tomto počítači povoleno používat protokol IPSec. Chcete-li, aby bylo možné tento protokol na daném počítači používat, musíte nejprve nastavit příslušnou zásadu. Není-li aktivní žádné přidružení zabezpečení s jiným počítačem, nezobrazí se v seznamu Přidružení zabezpečení v programu Sledování IPSec žádné zásady.

Prohlížeč událostí

Agent zásad IPSec vkládá záznamy do souboru protokolu systému Windows a určuje zdroj zásady. Indikuje také interval dotazování tak, jak je určen v aktivní zásadě. Slouží to k určení změn zásady ve službě Active Directory. Změny aktivní zásady IPSec na místním počítači, které provedou správci, se projeví okamžitě.

Můžete také zjistit, zda počítač používá místní zásadu nebo zásadu služby Active Directory. Tato informace je uložena v protokolu událostí. Projděte tedy pomocí programu Agent zásad IPsec protokol systému Windows.

Vlastnosti protokolu TCP/IP

Když zobrazíte okno vlastností protokolu IP (TCP/IP), můžete si prohlédnout aktivní zásadu IPsec. V případě, že počítač pracuje s místní zásadou IPsec, je název zobrazen v editovatelném formuláři. Jestliže však počítač používá zásadu, přiřazenou službou Active Directory, bude název a dialogové okno vystínované a příslušné hodnoty nebude možné měnit. Více informací o zobrazení dialogového okna vlastností protokolu IP najdete v nápovědě online k systému Windows 2000.

Nástroj Sledování IPsec

Program Sledování IPsec může potvrdit, zda jsou vaše zabezpečená spojení úspěšná. Zobrazí totiž všechna přidružení zabezpečení, jež jsou aktivní na místním počítači nebo na vzdálených počítačích.

Tento nástroj můžete například použít k určení, zda existuje nějaký model pro jednotlivá selhání ověřování nebo přidružení zabezpečení, jenž by naznačoval neslučitelná nastavení v zásadě zabezpečení.

Nástroj Sledování IPsec lze spouštět na místním počítači nebo, je-li počítač připojen prostřednictvím sítě k vzdálenému počítači, také vzdáleně.

► Spuštění programu Sledování IPsec

1. Klepněte na tlačítko **Start** a potom vyberte položku **Spustit**.
2. V příkazovém řádku zapište tento příkaz:

```
ipsecmon <název počítače>
```

3. Klepnutím na tlačítko **Možnosti** můžete změnit interval obnovování.

Ke každému přidružení zabezpečení se vztahuje jeden zobrazený záznam. Informace, uložená v každém záznamu, zahrnuje název aktivní zásady IPsec, aktivní akci filtru se seznamem filtrů IP (včetně podrobností o aktivním filtru) a koncový bod tunelového propojení (pokud bylo určeno).

Díky tomuto programu můžete vytvářet statistiky, jež vám budou nápomocny při ladění výkonu a odstraňování problémů. Mezi tyto statistiky patří následující sestavy:

- Počet a typ aktivních přidružení zabezpečení,
- celkový počet hlavních klíčů a klíčů relace (Úspěšná přidružení zabezpečení IPsec iniciují vytvoření jednoho hlavního klíče a jednoho klíče relace. Následná generování klíčů jsou zobrazena jako dodatečné klíče relace.),
- celkový počet důvěrných zabezpečení datové části zprávy zapouzdřením (ESP) nebo ověřených odeslaných nebo přijatých bajtů (ESP nebo AH)-

Poznámka: Vzhledem k tomu, že ESP poskytuje jak možnost ověřování, tak i zajištění důvěrnosti sdělení, jsou zvyšovány oba čítače.

- Celkový počet měkkých přidružení.

Obnovovací frekvence je jedinou možností, kterou lze konfigurovat. Standardně se statistické údaje obnovují každých 15 sekund. Statistické údaje jsou střádány při každém spojení, vytvořeném pomocí protokolu IPSec.

Selhávají pouze spojení zabezpečená protokolem IPSec

Tento oddíl obsahuje procedury, určené ke stanovení a odstranění možných příčin selhávání spojení zabezpečených protokolem IPSec.

Porušené odkazy v součástech zásady

Vzhledem k tomu, že služba Active Directory považuje poslední uloženou informaci za aktuální, je možné, že pokud zásadu upravuje více správců, může dojít k porušení některých odkazů mezi jednotlivými součástmi zásady. Uvedme si příklad.

- Zásada A používá filtr A.
- Zásada B používá filtr B.

Znamená to, že filtr A obsahuje odkaz na zásadu A, zatímco filtr B obsahuje odkaz na zásadu B.

- Robert upravuje zásadu A a přidává pravidlo, které používá filtr C.
- Ve stejné chvíli Alice z jiného místa upravuje zásadu B a přidává pravidlo, které také používá filtr C.

Budou-li obě zásady ukládány současně, vznikne možná odkaz mezi filtrem C a oběma zásadami A a B. Vzhledem k tomu, že je to nepravděpodobné, přepíše zásada A odkaz z filtru C do zásady B, bude-li uložena jako poslední. Filtr C bude tedy obsahovat odkaz pouze na zásadu A a to způsobí problémy při úpravách filtru C. Změna se projeví pouze v zásadě A, zásada B se o nich nedozví.

Kontrola integrity zásady tyto problémy odstraňuje, neboť ověřuje odkazy ve všech zásadách IPSec. Doporučuje se spouštět kontrolu integrity po každé úpravě zásady.

► Kontrola integrity zásad

1. Spusťte program **Správa zabezpečení protokolu IP**.
2. Klepněte na tlačítko **Akce**.
3. Přesuňte ukazatel myši nad seznam **Úloha** a klepněte na tlačítko **Ověřit integritu zásady**.

Tato akce si vynutí ověření integrity všech zásad IPSec, uvedených v seznamu konzoly. Budou-li některé odkazy neplatné, zobrazí se chybové hlášení.

Restart služby Agent zásad

Chcete-li vymazat starší přidružení zabezpečení, je možné, že budete muset restartovat službu Agent zásad. Jinou možností je vynutit si stažení zásady ze služby Active Directory na všechny klientské počítače domény. Službu lze správně spustit znovu jediné restartováním daného počítače.

Samotný restart služby Agent zásad si vynutí také restart ovladače IPSec.

Pokud se služba Agent zásad nespustí, pokuste se možnou příčinu zjistit pomocí programu Prohlížeč událostí.

Opakovaná instalace součástí IPSec

V případě, že systém nemůže najít některé soubory součástí protokolu IPSec jako IKE, Agent zásad IPSec nebo ovladač IPSec, můžete obnovit instalaci odstraněním původních souborů z disku a opakovanou instalací protokolu TCP/IP. Příslušné součásti IPSec jsou přeinstalovány jako součást instalace protokolu IP. Více informací o způsobu odstranění a instalaci protokolu IP najdete v nápovědě online systému Windows 2000.

Další zdroje

- Informace týkající se zdrojů RFC pro IPSec, konceptů sítě Internet či dalších odkazů, vztahujících se k protokolu IPSec, najdete pod odkazem International Engineering Task Force (IETF) na stránce WWW „Web Resources“, kterou najdete na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Další informace o IPSec najdete v následujících specifikacích:

- RFC 2085: *HMAC-MD5 IP Authentication with Replay Prevention*
- RFC 2104: *HMAC: Keyed Hashing for Message Authentication*
- RFC 2401: *Security Architecture for the Internet Protocol*
- RFC 2402: *IP Authentication Header (AH)*
- RFC 2403: *The Use of HMAC-MD5-96 within ESP and AH*
- RFC 2404: *The Use of HMAC-SHA-1-96 within ESP and AH*
- RFC 2405: *The ESP DES-CBC Cipher Algorithm with Explicit IV*
- RFC 2406: *IP Encapsulating Security Payload (ESP)*
- RFC 2407: *The Internet IP Security Domain of Interpretation for IKE*
- RFC 2410: *The NULL Encryption Algorithm and Its Use with IPSec*
- RFC 2411: *IP Security Document Roadmap*
- RFC 2451: *The ESP CBC-Mode Cipher Algorithms*

Tyto specifikace se neustále vyvíjejí a postupně zahrnují další skupiny dokumentů. Všechny informace, týkající se nejnovějších specifikací RFC a konceptů sítě Internet najdete na stránkách WWW organizace IETF.

- Více informací o zavádění zabezpečení systému Windows 2000 najdete pod odkazem Microsoft Security Advisor na stránce WWW Web Resources, kterou najdete na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.
- Více informací o vytváření sítě a spojení v systému Windows 2000 najdete pod odkazem Microsoft Networking and Communication na stránce WWW Web Resources, kterou najdete na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.
- Více informací o standardech a technologii protokolu IPSec, stejně jako o exportních pravidlech, najdete pod odkazem National Institute of Standards and Technology Computer Security Resource Clearinghouse na stránce WWW Web Resources, kterou najdete na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

KAPITOLA 9

Technologie Quality of Service



Technologie Quality of Service (QoS) usnadňuje zavádění multimediálních aplikací, jako jsou vytváření videokonferencí nebo telefonování v síti Internet, aniž by to mělo nějaký vliv na průchodnost sítě. Technologie Quality of Service, implementovaná v systému Microsoft® Windows® 2000, zdokonaluje také výkon kritických aplikací typu Enterprise Resource Planning (ERP). Systém Windows 2000 využívá službu QoS Admission Control Service, což je mechanismus, jenž umožňuje navrhovat centrálně, jak, kdy a kým budou užívány síťové prostředky na úrovni podsítí. Quality of Service je rozvíjející se technologie postavená na standardech, vyvíjených a ověřovaných názory zákazníků a spoluprací v rámci celého průmyslového odvětví.

Tato kapitola se zaměřuje na zavádění technologie Quality of Service a služby QoS Admission Control Service v systému Windows 2000. Tyto technologie jsou postaveny na standardech vytvořených organizací Internet Engineering Task Force (IETF).

Obsah této kapitoly

Co je to Quality of Service?	530
Spuštění služby QoS	534
Řízení přenosů	535
Resource Reservation Protocol	539
Podpora QoS v systému Windows 2000	552
Služba řízení podsítě QoS v systému Windows 2000	557
Zásady služby řízení podsítě QoS	562
Definování zásad služby řízení podsítě QoS	564
Odstraňování potíží	566

Další informace v Soupravě prostředků (Resource Kit)

Více informací o protokolu Kerberos najdete v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.

Další informace o zásadách služby Active Directory najdete v dokumentaci *Microsoft® Windows® 2000 Server Distribuované systémy*.

Podrobnější informace o obecných pojmech při vytváření sítí najdete v kapitolách této publikace „Úvod do TCP/IP“ a „Windows 2000 TCP/IP“.

Co je to Quality of Service?

Obecně je technologie QoS kolekcí metod a procesů, které organizace na bázi služeb implementuje k zajištění určité úrovně kvality. V kontextu sítě je kolekcí součástí, které ve vzájemné spolupráci zajišťují specifickou úroveň kvality pro přenosy dat aplikací, které procházejí napříč sítí nebo nestejnými sítěmi. Implementace technologie QoS je syntézou kolekce technologií definovaných organizací IETF a určených ke zmírnění problémů, způsobených sdílenými síťovými prostředky a omezenou šířkou pásma.

QoS poskytuje dvě rozdílné výhody:

- Mechanismus, jenž umožňuje aplikacím vyžadovat parametry kvality služeb, např. malé zpoždění přenášených dat,
- vyšší stupně řízení přepínaných prostředků šířky pásma podsítě.

Zavedení technologie QoS umožňuje správcům využívat šířku pásma podsítě nanejvýš efektivně, a to zejména při zavádění aplikací s vyšším podílem zatížení prostředků. Síť, využívající tuto technologii, vždy zaručuje existenci dostatečného množství požadovaných prostředků, když přepínaným sektorům sítě nastaví takovou úroveň služeb, že se jeví jako privátní síť. Rozdílné třídy aplikací mají při průchodu sítí různé stupně tolerance zpoždění. Technologie QoS zaručuje schopnost aplikace přenášet data vhodnými spoji a v přijatelném časovém rámci, takže se přenos nezpozdí, není deformován ani ztracen.

Udržení takových záruk však vyžaduje, aby s technologií QoS spolupracovaly jak odesílatel, tak příjemce (koncové uzly), zařízení (přepínače) vrstvy propojení (vrstva 2 modelu OSI), zařízení (směrovače) síťové vrstvy (vrstva 3 modelu OSI) a všechna propojení rozlehlých sítí (WAN) mezi těmito uzly. Bez technologie QoS by všechna tato síťová zařízení posuzovala všechna data jako rovnocenná a poskytovala by služby metodou první příchozí je první obsloužen. Aby však aplikace mohla QoS využívat, musí mít určitou úroveň znalosti QoS, aby si mohla na síti vyžádat šířku pásma a další prostředky.

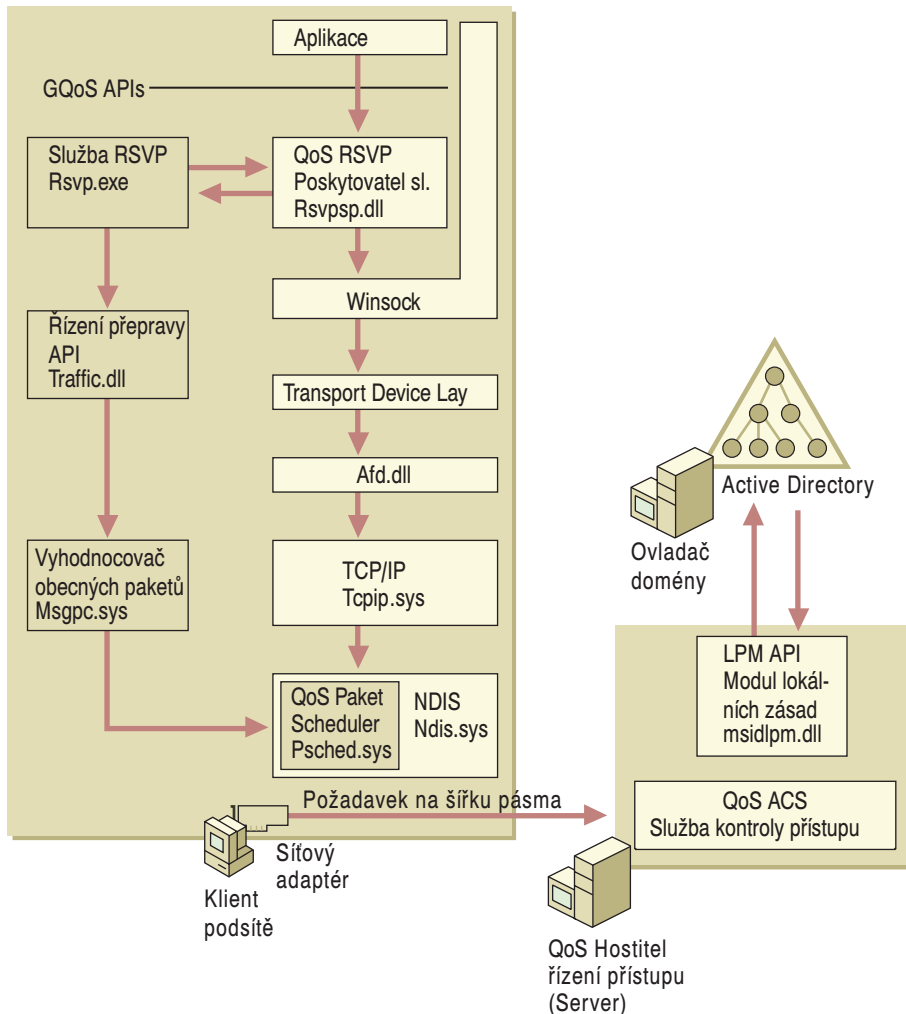
Efektivní přidělování šířky pásma je klíčovou úlohou, rozhodující pro výkonnost. Aplikace, pracující v reálném čase, multimediální aplikace a aplikace pro plánování využití podnikových prostředků vyžadují pro úspěšný přenos široké nepřerušované pásmo, což může existující síťové prostředky značně zatížit. Při velkém provozu se celkový výkon sítě sníží. Výsledkem je zpoždění (jako reakční čas a kolísání) a ztráta paketů. Snížení výkonu způsobuje celou řadu dalších problémů s přenášením videokonferencí, s přenosem zvuku v reálném čase, stejně tak jako s interaktivní komunikací, což vyúsťuje ve zkreslení zvuků a obrazů. Vzhledem k tomu, že multimediální aplikace využívají podstatnou část šířky pásma, trpí tradiční kritické aplikace značným nedostatkem dostupných prostředků. Technologie QoS poskytuje systém doručování síťových přenosů, jenž zaručuje minimální zpoždění a minimální ztráty dat.

Je třeba si uvědomit, že technologie QoS nemůže vytvořit šířku pásma, může ji pouze na bázi různých parametrů efektivně rozdělit.

Součásti technologie QoS v systému Windows 2000

Architektura technologie QoS v systému Windows 2000 je postavena na integrálně propojené kolekci protokolů průmyslových standardů, služeb a mechanismů, které řídí přístup k síťovým prostředkům, třídí a plánují síťové přenosy, a protokolů, jež vysílají signály síťovým zařízením. Ta mají uplatňovat technologii QoS při upřednostňování

přenosů určitých datových podsad. Na obrázku 9.1 je znázorněna architektura technologie QoS v systému Windows 2000.



Obrázek 9.1: Součásti technologie QoS v systému Windows 2000.

Všechny tyto součásti spolu velmi těsně spolupracují – umožňují tím využití této technologie v síťovém prostředí. Šrafované obdélníky na obrázku 9.1 znázorňují součásti technologie QoS v systému Windows 2000. Nezakreslené jsou prvky síťového infrastruktury, vyžadované k záruce kvality služeb od jednoho konce přenosu na druhý. Zařízení vrstvy 2 a 3 modelu OSI mezi koncovými uzly (tzn. mezi odesílatelem a příjemcem) musí také využívat technologii QoS. V opačném případě budou přenosy v tomto sektoru považovány za standardní (doručení s největším úsilím, ale bez záruky).

Obecné rozhraní API (část služby Winsock verze 2.0) v technologii QoS (GQoS) Technologie QoS v systému Windows 2000 je navržena pomocí obecného rozhraní QoS API, což je abstraktní rozhraní technologií QoS v systému Windows 2000. Programátoři apli-

kačních programů mohou používat GQoS k určení nebo k vyžádání šířky pásma pro rozlišení médií, jako jsou Ethernet nebo IP v režimu ATM (Asynchronous Transfer Mode).

Zprostředkovatel služby RSVP (Rsvpsp.dll) Je-li požadováno použití technologie QoS, zavolá rozhraní GQoS služby zprostředkovatele služby QoS, Resource Reservation Protocol Service Provider (RSVP SP). Zprostředkovatel služby QoS spustí službu RSVP a odešle signál o požadavcích na šířku pásma, řízení přenosu a podpoře služby řízení podsítě QoS všem síťovým zařízením na cestě uvedené pro data.

Služba RSVP (Rsvp.exe) Protokol Resource Reservation Protocol (RSVP) je signalizačním protokolem, definovaným organizací IETF, jenž přenáší požadavky QoS na přidělení priority šířky pásma v dané síti. Protokol RSVP překonává všechny rozpory mezi aplikací, operačním systémem a mechanismy QoS, zaměřenými na určitý typ média. Protokol RSVP odesílá zprávy ve formátu na médium nezávislém, díky čemuž je možný přenos QoS mezi koncovými uživateli i prostřednictvím sítí, které v sobě kombinují různé typy zařízení, pracujících v nižších hladinách.

Řízení provozu (Traffic.dll) Řízení provozu vytváří a reguluje tok dat používáním parametrů systému QoS. Umožňuje také vytváření filtrů, s jejichž pomocí lze třídit pakety uvnitř toku dat. Povolené operace řízení provozu lze využívat prostřednictvím rozhraní Traffic Control API.

Obecný klasifikátor paketů (Msgpc.sys) Obecný klasifikátor paketů určuje třídu služby, ke které jednotlivé pakety patří. Pakety jsou zařazovány do fronty podle úrovně služby. Fronty jsou spravovány pomocí nástroje Plánovač paketů služby QoS.

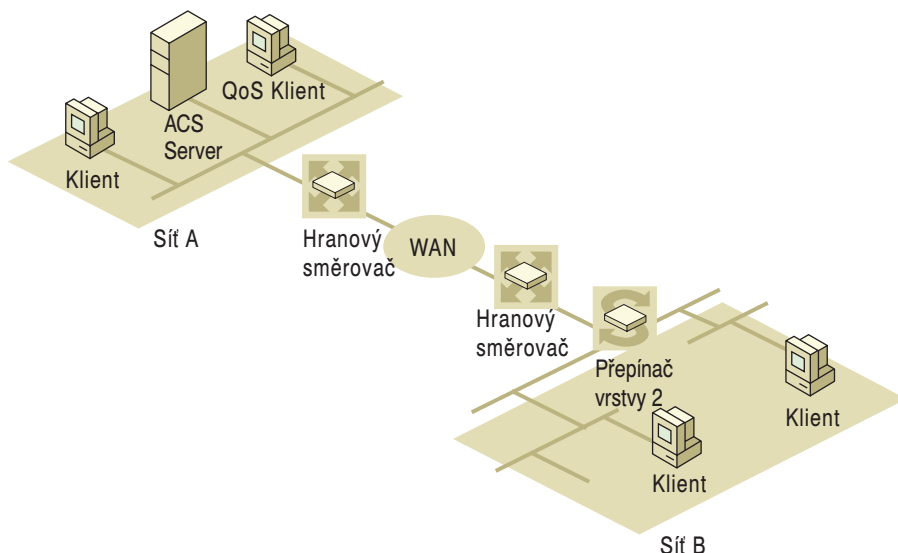
Plánovač paketů QoS (Psched.sys) Plánovač paketů QoS vynucuje užití parametrů QoS pro daný tok dat a přiděluje přenosu určitou prioritu. Plánovač paketů QoS potom určuje plán doručení každé fronty paketů a řídí soutěžení mezi pakety ve frontách, jež vyžadují simultánní přístup k síti. Paketům je stanovena priorita 802.1p pro zařízení ve vrstvě 2 a pro zařízení vrstvy 3 je stanovena priorita Odlišná třída služby.

Služba řízení podsítě QoS (QoS ACS) Služba řízení podsítě QoS spravuje síťové prostředky v přepínaných segmentech sdílené sítě (podsítích). Tuto službu není nutné v každé podsíti implementovat. Maximální přínos služby řízení podsítě QoS se projeví zejména v přepínaných segmentech. Služba řízení podsítě QoS poskytuje řídicí bod pro požadavky na šířku pásma a určuje, zda jsou požadované síťové prostředky v současné době dostupné a zda má uživatel potřebná oprávnění k tomu, aby mohl takový požadavek vznést.

Modul místních zásad (Msidlp.m.dll) Modul místních zásad (LPM) je součástí služby QoS ACS, která poskytuje bod provádění zásady (PEP) a bod rozhodování o zásadách (PDP). Modul LPM, implementovaný v systému Windows 2000, rozšiřuje službu QoS ACS o prostředky k vyhledávání informací o zásadách služby Active Directory™. Služba QoS ACS volá dynamickou knihovnu modulu LPM (Msidlp.m.dll) ihned po přijetí zprávy RSVP s tiketem protokolu Kerberos. Modul LPM potom z této zprávy získá jméno uživatele a vyhledá v adresáři služby Active Directory zásadu služby řízení pro tohoto uživatele. Součástí tohoto procesu je také rozhraní API modulu LPM.

Na jakých principech technologie Quality of Service funguje

V tomto oddíle se dozvíte, jak všechny součásti této technologie podle společného scénáře QoS fungují. Na obrázku 9.2 je obecně znázorněno zavedení technologie QoS.



Obrázek 9.2: Na jakých principech funguje technologie QoS.

1. Klient sítě A požaduje užití technologie QoS. Aplikace používaná k přenosu dat umožňuje využívat technologii QoS. Aplikace požaduje zpřístupnění této technologie na zprostředkovateli služby QoS.
2. Zprostředkovatel služby QoS vyžaduje tuto službu k odeslání signálu s požadavkem nezbytné šířky pásma a upozorní řízení provozu, že pro daný tok dat byla vyžádána služba QoS. Přenos je aktuálně odeslán se zaručením normálního zpracování při průchodu sítí.
3. Na server QoS ACS je odeslána zpráva RSVP s požadavkem na rezervaci. Službě QoS ACS jsou předávány zprávy RSVP, nikoli datové pakety, které jsou nakonec předmětem výměny informací mezi koncovými klienty.
4. Server služby QoS ACS ověří, zda je v daném okamžiku k dispozici dostatek potřebných síťových prostředků, jež by mohly požadavky úrovně QoS splnit. Mimo to ověří, zda má uživatel potřebná oprávnění ke vznesení požadavku na tuto šířku pásma. Modul místních zásad používá tiket protokolu Kerberos, uložený v požadavku RSVP, jehož pomocí ověřuje totožnost uživatele a potom vyhledá jeho zásadu v adresáři služby Active Directory. Služba QoS ACS může ověřovat prostředky pro odesílatele, příjemce nebo pro oba zároveň.
5. Po ověření totožnosti potvrdí server QoS ACS daný požadavek a logicky mu přidělí nezbytnou šířku pásma. Server QoS ACS předá požadavek směrem k příjemci (klient) v síti B.
6. Když požadavek RSVP překročí hranice směrovače v síti A, sleduje tento směrovač vyžádané prostředky (šířka pásma). Šířka pásma není doposud přidělena fy-

zicky (RSVP je protokol inicializovaný příjemcem a šířku pásma tedy může rezervovat pouze příjemce). Stejný proces se opakuje na hranici sítě B.

7. Požadavek nyní na cestě uvedené pro data překročí zařízení obou sítí. Příjemce (klient) potvrdí, že chce data přijmout a vrátí zprávu RSVP s vyžádáním příslušné rezervace.
8. Když požadavek příjemce na šířku pásma překročí hranice směrovače v síti B, má tento směrovač už v danou chvíli ve své mezipaměti požadavek odesílatele. Směrovač porovná oba tyto požadavky a provede rezervaci fyzickým přidělením šířky pásma. Stejný proces se pak bude opakovat na směrovači síti A.
9. Rezervace je odeslána zpět odesílateli. Síťová zařízení 3. vrstvy (krajní směrovače) jsou schopna potvrdit a přidělit fyzickou šířku pásma. Rezervace pak jednoduše prochází přepínačem vrstvy 2.
10. Během tohoto procesu je přenos odeslán modulem řízení provozu jako normální přenos. Po přijetí rezervace spustí řízení provozu na hostitelském počítači odesílatele proces klasifikace, označování a plánování odesílání paketů podle požadované úrovně QoS. Plánovač paketů QoS označí prioritu paketů RSVP, 802.1p pro zařízení 2. vrstvy (na obrázku jako přepínač) a Odlišná třída služby pro zařízení 3. vrstvy (na obrázku jako krajní směrovače).
11. Plánovač paketů QoS spustí přenos podle důležitosti. Data jsou všemi zařízeními po cestě stanovené pro data zpracována jako prioritní. Tím je zaručena vyšší rychlost při průchodu sítí a přenos dat klientu v síti B je úspěšnější.

Příklad jsme zde uvedli pouze jako ukázkou. Model totiž umožňuje rozličné úpravy, závislé na topologii sítě, ale také na přítomnosti různých síťových zařízení.

Spuštění služby QoS

Obecné rozhraní QoS API a zprostředkovatel služeb QoS zjednodušují rozmístění technologie QoS, neboť poskytují rozhraní pro aplikační programy a podporu pro aplikace, které na síti službu QoS vyžadují.

Obecné rozhraní QoS API

Obecné rozhraní QoS API poskytuje vývojářům standardní rozhraní pro vytváření aplikačních programů, stejně tak jako účinné mechanismy pro přidávání nových součástí QoS, aniž by bylo zapotřebí měnit celkový návrh stávajících aplikací, tuto technologii užívajících. Obecné rozhraní QoS API je součástí knihovny Windows Sockets 2.0 (Winsock2), implementovanou v rozhraní API. Existence tohoto rozhraní umožňuje aplikacím spouštět službu QoS bez nutnosti plné znalosti všech aktuálně dostupných mechanismů QoS, nebo dokonce bez specifických znalostí základních síťových médií.

Programátoři aplikací mohou používat obecné rozhraní QoS API k určování nebo vyžadování nezbytné šíře pásma, kdy je třeba zaručit, aby nedocházelo ke zpoždování paketů (například u proudu zvukových dat). Programátoři mohou toto rozhraní používat také k stanovení priorit přenosů, generovaných aplikací s kritickým posláním. Obecné rozhraní QoS API je abstraktní množinou a vyžaduje pouze velmi jednoduché direktivy z aplikace. Rozšíření rozhraní API poskytují další možnosti řízení. Aplikace, jež odesílají požadavky na službu QoS, by měly používat právě obecné rozhraní QoS API.

Dokumentace Windows 2000 Software Development Kit obsahuje všechny koncepční a referenční materiály, nezbytné k využívání obecného rozhraní QoS API.

Zprostředkovatel služby QoS (RSVP SP, služba RSVP)

Po vyžádání služby QoS budou obecným rozhraním QoS API spuštěny služby zprostředkovatele služeb QoS (RSVP SP). Ten zprostředkovává následující služby:

- RSVP (vysílání signálů)

Zprostředkovatel služby QoS inicializuje a končí signalizaci RSVP ve prospěch aplikací v rámci služby RSVP (Rsvp.exe). Poskytuje zainteresovaným aplikacím informace o stavu s ohledem na rezervaci. Služba řízení podsítě QoS minimalizuje nutnost toho, aby aplikace znala podrobnosti signalizace RSVP.

- Podpora zásad

Služba RSVP komunikuje s Kerberos řadičem domény a generuje prvky zásad, jež jsou pak zahrnuty do signálních zpráv RSVP. Tyto prvky identifikují uživatele, takže při zpřístupňování síťových prostředků lze uplatňovat zásady řízení přístupu podle uživatele nebo podle podsítě.

- Řízení přenosů

Služba RSVP používá API řízení přenosů pro vyvolání řízení přenosu na vyžádání aplikací podporujících QoS jako odpověď na volání GQoS nebo na signální zprávy RSVP. Služba RSVP ukrývá složitost rozhraní Traffic Control API pomocí obecného rozhraní GQoS API, takže pro použití této funkce není třeba aplikace předkládat.

- Podpora Služby řízení podsítě QoS

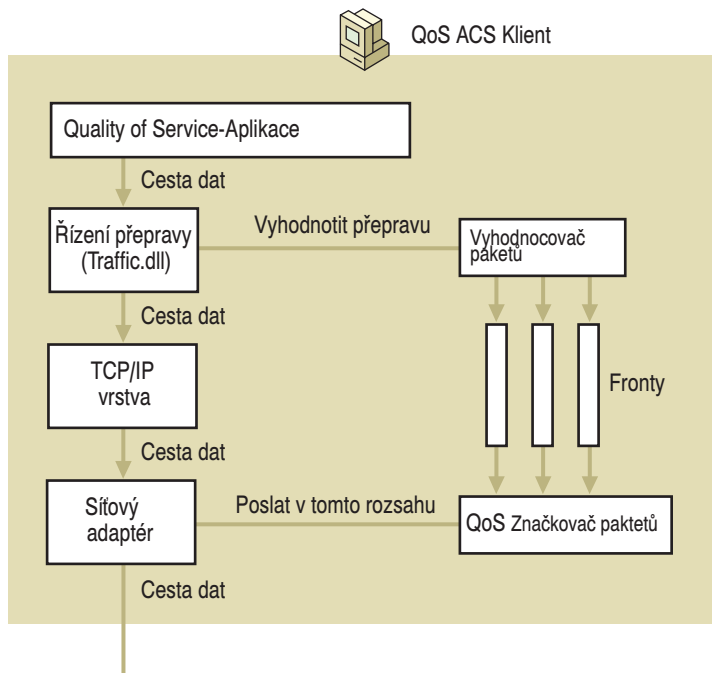
Služba RSVP komunikuje se serverem řízení podsítě stejným způsobem jako se serverem QoS ACS v systému Windows 2000. Předchází tím vytváření příliš velkého množství vazeb na šířku pásma ve sdílených segmentech.

Řízení přenosů

Služba RSVP používá řízení přenosů ve prospěch příslušných aplikací vždy, když je vyžádáno použití technologie QoS. Řízení přenosů odkazuje na kolekci mechanismů, jež po vytvoření rezervace QoS řídí a chrání specifické toky dat. Řízení přenosů se používá k rozdělení přenosů do samostatných tříd služeb a k usměrňování jejich doručení v síti. Na obrázku 9.3 jsou znázorněny jednotlivé součásti řízení přenosů.

Klíčovým prvkem řízení přenosů je ustanovení parametrů obsluhy pro posloupnost paketů (označovanou také jako specifikace toku dat) s následným považováním všech členských paketů za jeden tok. Řízení toku využívá informace ze specifikace toku dat s definovanými parametry QoS, na jejichž základě vytvoří filtry pro přímý výběr paketů do daného toku (specifikace filtru).

Řízení přenosů spolupracuje se službami řízení podsítě QoS RSVP, s jejichž pomocí plní úroveň služby a priority, vyžadovanou požadavkem šířky pásma. Řízení přenosů je v některých případech dostupné také pomocí určitých nástrojů, určených pro klienty podsítě, kteří systém QoS nepoužívají a řídí tok dat prostřednictvím síťových zařízení, neodpovídajících specifikacím RSVP, tím, že označují pakety jako 802.1p (zařízení vrstvy 2) nebo jako Odlišnou třídu služby (zařízení vrstvy 3).



Obrázek 9.3: Součásti řízení přenosů.

Rozhraní Traffic Control API (TC API) Traffic Control API je programovacím rozhraním komponent řízení provozu, které regulují síťový provoz na. Rozhraní TC API umožňuje seskupování přenosů z různých zdrojů (na tomtéž hostitelském počítači odesílatele) do jednoho řízeného toku dat. Například přenosy dat na cílovou síťovou adresu 1.2.3.0 lze umístit do stejného toku, bez ohledu na adresy zdrojového a cílového portu. Jen pro srovnání lze říci, že obecné rozhraní QoS API omezuje použití řízeného toku dat k přenosům pouze z jedné „konverzace“ (konverzace je definována adresami zdrojového a cílového portu).

TC API také spolu s obecným rozhraním QoS API umožňuje použití aplikací pro řízení přenosů, dodávaných jinými dodavateli, jež mohou požadovat uplatnění systému QoS ve prospěch aplikací, které tento požadavek nemohou vznést samy. Dále v situacích, kdy chtějí správci sítě získat lepší kontrolu nad QoS, poskytovaným aplikacím. Více informací o využívání rozhraní Traffic Control API najdete na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Součásti řízení přenosů

Na každém hostitelském počítači jsou přenosy označovány a předávány jako upřednostněné přenosy QoS díky klasifikaci a plánování.

Obecný klasifikátor paketů (Msgpc.sys)

Mechanismus klasifikace paketů poskytuje prostředky, s jejichž pomocí jsou pakety, generované v aplikacích, klasifikovány a před odesláním do sítě je stanovena jejich priorita. Služba Obecný klasifikátor paketů je mechanismem, jehož pomocí řízení přenosů

určuje tok libovolného paketu, tzn. také zacházení s paketem při jeho přijetí. Po klasifikaci paketu jako součásti příslušného datového toku je Plánovač paketů QoS schopen zajistit příslušné zacházení s paketem podle nastavených parametrů datového toku.

Plánovač paketů QoS (Psched.sys)

Plánování paketů je prostředek, s jehož pomocí lze řídit přenos dat (paketů), což je klíčová funkce technologie Quality of Service. Plánovač paketů QoS vynucuje nastavení parametrů QoS pro příslušný datový tok. Tvarování přenosů (vyhlazování shlukových přenosů a špiček v přenosu každého datového toku) se opírá o funkci klasifikátoru paketů a na základě parametrů QoS zařazuje jednotlivé pakety do front. Plánovač paketů QoS vyhledává pakety ve frontách a přenáší je na základě parametrů QoS. Mezi tyto parametry zpravidla patří plánovaná rychlost a určité označení priority. Parametr plánovaná rychlost se používá při určování rychlosti přenosu paketů v síti. Tato priorita se hodí k určení pořadí, v němž je třeba pakety přenášet, je-li daný segment přetížen. Tato technika umožňuje vyhlazovat shlukové přenosy a špičky při provozu v určitých časových intervalech a to dále zefektivňuje rovnoměrnější využívání sítě a správu integrity prostředků.

Plánovač paketů QoS lze nainstalovat na libovolný počítač, na němž chcete mít nainstalované služby řízení přenosů. Program Plánovač paketů QoS je třeba instalovat na všechny koncové systémy, které rezervují potřebné prostředky v podsítích, v nichž je spuštěna Služba řízení podsítě QoS, a na všechny hostitelské počítače, jež odesílají data na jiné hostitelské počítače (například multimediální server nebo server pro řízení zásob).

Označování paketů

K zajištění správné funkce technologického řešení Quality of Service musejí být pakety označeny takovým způsobem, aby jim mohla všechna síťová zařízení na jejich cestě poskytnout požadovanou úroveň služby, anebo, to v případě, že by nespolupracovaly s protokolem RSVP se o to alespoň mohla pokusit. Plánovač paketů QoS zajišťuje označení paketů jako 802.1p, zatímco označení paketů jako Odlišná třída služby (Differentiated Class of Service) zajišťuje protokol TCP/IP. Plánovač paketů QoS nelze instalovat na počítače se systémem Microsoft® Windows® 98. Znamená to, že na těchto počítačích nelze využívat výhody označení paketů podle standardu 802.1p. Na takových počítačích je možné pomocí zprostředkovatele služby QoS označovat pakety kódem DSCP (Diff-serv Code Point). Systém Windows 2000 definuje v registru výchozí mapování na standard 802.1p a standard Odlišná třída služby. O tomto mapování pojednává jeden z oddílů dále v této kapitole. Síťová zařízení mohou potlačit výchozí mapování tím, že budou do signálních zpráv RSVP vkládat speciální objekt. Rozhodovací proces probíhá na serveru zásady QoS, jenž může mapovat uživatelské přenosy na nižší nebo vyšší prioritu, než určuje výchozí mapování v registru. Server zásady může vložit objekt třídy přenosu (T class), jímž potlačí třídu 802.1p, a objekt třídy D může použít k potlačení třídy Diff-serv.

Úroveň služeb přenosu

Modely přenosů lze rozdělit do dvou základních skupin:

- Pružné přenosy

Pružné přenosy se snadno přizpůsobují změnám. Je-li dostupné pouze úzké pásmo, bude doručení pružných přenosů pomalé. Rychlejší bude, jakmile se zvětší šířka

pásma. Odesílatel dat je automaticky nastaven na rychlost sítě. Pružné přenosy jsou zpravidla generovány pomocí transakčně orientovaných aplikací, například při přenosech objemných dat.

- Přenosy v reálném čase

Přenosy v reálném čase jsou generovány zejména aplikacemi, jež v reálném čase pracují a vyžadují vyhrazenou šířku pásma. Do této skupiny patří například videokonference. Přenosy v reálném čase mají omezenou schopnost přizpůsobovat se změnám podmínek v síti a různá zpoždění mohou významně snížit srozumitelnost a použitelnost přenášených dat.

Řízení přenosů využívá čtyř úrovní služeb, což umožňuje vyhovět potřebám dvou primárních skupin modelu přenosů:

- Nejlepší snaha

Nejlepší snaha je standardní úroveň služeb, používaná v mnoha sítích, založených na komunikačním protokolu IP. Je to bezspořádaný model doručování, jenž je vhodný zejména pro pružné přenosy. Pakety jsou odesílány bez záruky pro malé zpoždění nebo odpovídající šířku pásma.

Následující dvě úrovně jsou vhodné pro aplikace, pracující v reálném čase, které poskytují přednostní služby:

- Kontrolované zatížení

Kontrolované zatížení přibližuje chování služby typu nejlepší snaha v podmínkách nezatížených (středně zatížených nebo zaplněných) podsítí. Služba kontrolovaného zatížení na síťovém zařízení, přijímající tok dat, zaznamená pouze malé nebo vůbec žádné zpoždění nebo přetížení. Nerezervovaná šířka pásma nebo rezervované šířky pásma, které nejsou momentálně používány, jsou dostupné pro všechny ostatní přenosy. Více informací o úrovni služby najdete ve specifikaci RFC 2211 Request for Comment organizace IETF.

- Zaručená služba

Zaručená služba garantuje maximální limit zpoždění. Nejužitečnější je situace, kdy všechny hostitelské počítače na cestě datového toku poskytují právě tuto úroveň služby, a to včetně směrovačů či prepínačů, které jsou slučitelné s QoS a RSVP. Dopad na zatížení sítě zaručenou službou je však značný, proto se nedoporučuje používat tuto úroveň služby u aplikací, jež generují pružné přenosy nebo přenosy typu nejlepší snaha.

- Jakostní služba

Jakostní služba je navržena pro aplikace, které vyžadují zpracování upřednostněných přenosů, ale nemohou své požadavky QoS kvantitativně určit ve smyslu konkrétní specifikace datového toku. Tyto aplikace zpravidla odesílají data v přerušovaných nebo shlukových přenosech. V případě jakostní služby je to právě síť, kdo určuje způsob nakládání s datovými toky jakostní služby. Tento typ přenosů je generován aplikacemi s klíčovým posláním ERP. Více o této úrovni služby najdete pod odkazem IETF na stránce Web Resources na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>. Podrobné informace o této službě najdete v konceptu sítě Internet definovaném organizací IETF a nazvaném „Specification of the Qualitative Service Type“.

Zásada služby řízení podsítí QoS určuje výběr úrovně služby použité při doručování přenosu.

Resource Reservation Protocol

Resource Reservation Protocol (RSVP) je signálním protokolem (RFC 2205) definovaným organizací Internet Engineering Task Force, jež k přepravě požadavků QoS po síti využívá Integrované služby (Intserv). Architektura Intserv určuje rozšíření modelu nejlepší snaha – standardní model doručování, používaný ve většině sítí s protokolem IP a v síti Internet. Služba Intserv poskytuje možnost speciálního zpracování dat podle nastavené priority. Kromě toho má k dispozici mechanismus, jehož pomocí si mohou aplikace s podporou technologie QoS samy volit úroveň doručení přenosu: kontrolované zatížení nebo zaručená služba. Systém Windows 2000 poskytuje možnosti rozšíření typů služby Intserv v podobě jakostní služby. Jakostní služba je navržena pro aplikace, jež vyžadují podporu technologie QoS, ale samy nemohou kvantitativně určit požadavky QoS vinou svých přerušovaných nebo shlukových přenosů. Integrované služby mimoto definují signalizaci QoS (RSVP) pro zajišťování rezervací prostřednictvím sítě.

RSVP je protokol vrstvy 3, jež tuto vrstvu činí nezávislou na základních síťových médiích. Klientské sítě obsahují zpravidla různorodá média, včetně adaptérů Ethernet nebo médií místních sítí (LAN) s uzly zapojenými do okruhu, sítí WAN přizpůsobených pro používání pomalých i rychlých pronajatých spojů, modemových propojení nebo sítí ATM. RSVP překlene rozdíly mezi aplikacemi, operačními systémy a mechanismy, specifickými pro určitý typ média. To umožňuje odesílat službě RSVP zprávy QoS prostřednictvím sítí, jež kombinují v nižších vrstvách různé typy médií. Například koncové uzly si mohou mezi sebou vyměňovat zprávy RSVP prostřednictvím sítí, jež se skládají z místních sítí typu 802, směrovačů, oblastí ATM a WAN, kdy každé z těchto médií má vlastní službu řízení podsítě QoS.

Protokol RSVP je vhodný pro aplikace s kritickým posláním (například software plánování podnikových zdrojů, relačně orientované aplikace jako telefonování IP nebo videokonference). Oba typy aplikací vyměňují data QoS mezi pevnými koncovými uzly na určitém stupni trvalosti. Směřují k vytváření datových toků. Propojení QoS jsou jednostranná. Pokud chcete povolit propojení hostitelských počítačů pro odesílání i přijímání dat, je zapotřebí dvou připojení typu QoS.

Protokol RSVP je v první řadě určen pro přenosy IP a operuje nad protokoly IPv4 nebo IPv6, zatímco transportní protokol se nachází v zásobníku protokolu. Přesto je to pouze signalizační, nikoli směrovací protokol. Směrovací protokoly určují místo předávání paketů. Protokol RSVP konfiguruje rezervace pro toky dat spolu s jejich předurčenou cestou pomocí síťového směrovacího protokolu.

Protokol RSVP je instalován na počítač jako součást instalace knihovny Windows Sockets 2.0 v systému Windows 2000. Řeší následující otázky:

- Funguje se všemi současnými směrovacími protokoly a využívá celou řadu protokolů síťové vrstvy, včetně TCP/IP.
- Využívá přenosy vícesměrových a jednosměrových vysílání.
- Přenáší požadavky rezervace šířky pásma na všechna síťová zařízení nebo cíl směrování (směrovače, přepínače nebo servery proxy), zodpovědná za správu prostředků na předurčené cestě datového toku mezi odesílatelem a příjemcem (koncové uzly).
- Udržuje rezervace na každém cíli směrování, když ukládá informace do mezipaměti tohoto počítače a vytváří logické rezervace neboli rezervace stavu.

- Předává data transparentně prostřednictvím zařízení, která nepracují s protokolem RSVP.

V případě, že síťové zařízení nepracuje s protokolem RSVP, není v tomto segmentu sítě používání technologie QoS plně zaručeno. Zprávy jsou jednoduše předávány prostřednictvím následných cílů směrování, aniž by byla datovému toku přidělena šířka pásma upřednostněných přenosů. Těmito segmenty je informace předávána pomocí mechanismu „nejlepší snaha“, což znamená, že u dané úrovně služby nelze garantovat spojení obou koncových uzlů, stejně jako malé zpoždění zprávy. Tato situace může nastat v oblastech, kde je k dispozici dostatečná šířka pásma nebo kde si síťové prvky samy omezují přiděl prostředků. V současné době pracuje s protokolem RSVP několik výkonných směrovačů a přepínačů.

Zprostředkovatel služby QoS (RSVP SP), jenž volá a usnadňuje signalizaci QoS a RSVP, umožňuje vývojářům aplikací pomocí protokolu RSVP přímo komunikovat. Více informací o zprostředkovateli služby QoS najdete pod odkazem Software Development Kit na stránce Web Resources na adrese <http://windows.microsoft.com/windows2000/res-kit/webresources>.

Přímá interakce s aplikací nebo serverem pomocí protokolu RSVP umožňuje jemné doladění služby nebo odesílání požadavků na služby speciální. Přesto většina programátorů aplikací zjišťuje, že použití zprostředkovatele služby QoS, jenž volá a spravuje signalizaci RSVP, pro aplikace a servery je postačující k tomu, aby tyto aplikace nebo servery využívaly všechny výhody technologie QoS.

Obecné rozhraní QoS API je programátorským rozhraním pro zprostředkovatele služby QoS. Ve většině okolností je to jediné rozhraní, které mohou programátoři při vytváření aplikací podporujících technologii QoS požadovat.

Zprávy protokolu RSVP

Zprávy protokolu RSVP identifikují to, co aplikace a uživatel na službě QoS požadují, dále identifikují úroveň služby požadované na síti, požadovanou šířku pásma a koncové uzly (adresy zdroje a cíle). Podle správcem definovaných zásad služby řízení podsítě QoS a dostupnosti síťového prostředku je požadavek QoS počítačem vykonávajícím službu řízení podsítě QoS buď schválen, nebo zamítnut. V případě, že je požadavek přijat, je zavolán mechanismus QoS, jenž klasifikuje a plánuje přenos datového toku, logicky přiděluje šířku pásma a oznamuje žádajícímu hostitelskému počítači schválení požadavku. Na základě této zprávy začne žádající počítač odesílat přenos se stanovenou úrovní priority. Až do tohoto okamžiku je tento přenos považován za standardní.

Informace ukryté ve zprávách RSVP jsou rozděleny na jednotlivé toky dat (tok je datový proud mezi dvěma koncovými uzly). Zprávy RSVP přenášejí následující informace:

- *Informace o klasifikaci přenosu* Adresy IP a porty zdroje a cíle identifikují přenášený tok (specifikace filtru).
- *Parametry přenosu* Parametry, vyjádřené pomocí bloku řídících zpráv služby Intserv, identifikují rychlost datového přenosu (specifikace toku dat).
- *Informace o úrovni služby* Na základě typu služby definované službou Intserv odesílá nároky na datový proud v požadavku RSVP.
- *Informace o zásadě* Umožňuje systému ověřit, zda požadavek na příslušné prostředky a jejich množství je oprávněný.

Protokol RSVP používá k vytvoření a údržbě rezervované šíře pásma typy zpráv, uvedené v tabulce 9.1.

Table 9.1: Typy zpráv RSVP

Typ zprávy	Funkce
PATH	Přenáší informace o datovém proudu od odesílatele k příjemci. Zpráva PATH určí cestu, kterou musí vyžádaná data urazit směrem k příjemci. Zprávy PATH obsahují požadavky na šířku pásma, charakteristiku přenosu a informace o adresách jako jsou adresa IP zdroje a adresa IP cíle. Tyto zprávy jsou určeny pouze pro danou relaci, což je určeno cílovou adresou a portem datového toku. Je zapotřebí, aby relace měla jedinečný identifikátor, neboť odesílatel může nabídnout více přenosů a přijímat zprávy RESV od více příjemců. Jedinečný identifikátor relace umožňuje správně sdružovat zprávy PATH s odpovídajícími zprávami RESV.
RESV	Nese požadavek příjemce na rezervaci. Zprávy RESV obsahují rezervaci skutečné šíře pásma, požadované úrovně služby a adresu IP zdroje. Tato zpráva aktivuje rezervaci.
PATH-ERR	Indikuje chybu v odpovědi na zprávu PATH.
RESV-ERR	Indikuje chybu v odpovědi na zprávu RESV.
PATH-TEAR	Ruší stav PATH z celé trasy.
RESV-TEAR	Ruší rezervaci na celé délce trasy dat.
RESV-CONF	Nepovinná. Pokud příjemce vyžaduje potvrzení, odešle ji odesílatel příjemci.

Když aplikace na koncovém uzlu vyžaduje QoS, sestaví protokol RSVP zprávy PATH, jež vyjadřují požadavky QoS odesílající aplikace. Jsou vyjádřeny v abstraktních pojmech vrstvy 3, to znamená, že je může interpretovat každé síťové zařízení na trase. Koncový uzel příjemce odešle zpátky zprávu RESV, která vytvoří rezervaci požadovaných prostředků po celé délce předdefinované trasy přenášených dat. Aby bylo možné rezervaci garantovat, musí každé směrování tuto rezervaci povolit a fyzicky přidělit požadované prostředky. Povolením rezervace směrování potvrdí poskytnutí přiměřených zdrojů. Zařízení mohou požadavky na prostředky zamítnout například z důvodu nedostatečných oprávnění žádajícího uživatele nebo nedostatku síťových prostředků v okamžiku vznesení požadavku.

V případě zamítnutí rezervace obdrží aplikace okamžitou odpověď, obsahující sdělení, že daná podsít' nemůže v daném okamžiku zajistit požadovanou šířku pásma nebo požadovanou úroveň služby. Nyní záleží na aplikaci, která musí určit, zda odešle data ještě jednou, přijme službu na úrovni nejlepší snaha či nějakou dobu počká a zopakuje požadavek na šířku pásma později. Koncové uzly musí pravidelně obnovovat rezervaci opakovaným odesíláním zpráv PATH a RESV každých několik sekund (zpravidla jsou to 30sekundové intervaly).

Specifikace toku dat a specifikace filtru

Zprávy RSVP přenášejí velmi specifické informace o klasifikaci, které umožňují zařízením, podporujícím protokol RSVP, aby rozdělila přenos do proudů, přidružených s příslušnou konverzací a zajistila to, že s každým z těchto proudů bude zacházeno podle předchozích požadavků RSVP. Jemná klasifikace poskytuje lepší garanci služby.

Zprávy RESV obsahují specifikace toku dat a specifikace filtru, jež společně poskytují potřebné informace o přenášeném proudu. Zkombinované specifikace toku dat a filtru jsou označovány jako popisovač toku.

Specifikace filtru

Klasifikace přenosu je založena na adresách IP a portech zdroje a cíle, uložených v paketu. Tato skupina parametrů se nazývá specifikace filtru. Zařízení, která podporují technologii QoS, zakládají zpracování paketu na základě shody se specifikací filtru.

Tato specifikace, spolu se specifikací relace, definuje kolekci datových paketů, jež budou součástí příslušného toku. Specifikace filtru je využívána k nastavení parametrů v Klasifikátoru paketů. Datové pakety, adresované do určité relace, jež se ale neshodují se specifikací filtru dané relace, jsou zpracovávány jako přenosy typu nejlepší snaha.

Styly filtru

Rezervace zahrnuje možnosti, označované také jako styl rezervace. Tento styl určuje způsob, jakým je rezervace z pohledu odesílatele zpracovávána.

Rezervace může být buď odlišná pro každého odesílatele, nebo sdílená určitou skupinou odesílatelů. Může se také jednat o výslovný seznam všech vybraných odesílatelů nebo o specifikaci pomocí zástupných znaků, která jednoduše vybere všechny odesílatele v rámci dané relace.

Styl filtru se zástupnými znaky

Rezervace pomocí filtru se zástupnými znaky obsahuje výběr odesílatele, určeného pomocí zástupných znaků, a sdílenou rezervaci. Styl filtru se zástupnými znaky vytváří jednu nebo více rezervací pro všechny toky odesílatele. Množství prostředků rezervovaných sdílenými rezervacemi je určeno největším ze požadavků, které byly sloučeny. Rezervace filtru se zástupnými znaky je automaticky nabízena všem novým odesílatelům. Není zapotřebí dalších specifikací filtrů.

Styl filtru s pevnými znaky

Na rozdíl od předchozího typu rezervace obsahuje styl filtru s pevnými znaky formát výslovného výběru odesílatele s jedinečnými parametry (v protikladu k sloučeným parametrům). Rezervace pomocí filtru s pevnými znaky je pro pakety každého odesílatele jedinečná. Větší počet rezervací ve stylu filtru s pevnými znaky v jednom celku je zpracováván pomocí popisovačů toku. Specifikace filtru se musí přesně shodovat pouze s jedním odesílatelům.

Sdílený výslovný styl rezervace

Sdílený výslovný styl rezervace zahrnuje jedinou rezervaci, jež je sdílená v rámci výslovného seznamu odesílatelů. Sdílený výslovný styl rezervace je určen jednou specifikací toku dat a seznamem specifikací filtrů.

Specifikace toku dat

Prostřednictvím sémantiky protokolu RSVP a Intserv umožňuje obecné rozhraní QoS API aplikacím popisovat kvalitu služeb vyžadovaných pro přenos dat. Parametry technologie QoS jsou nesené v obecné specifikaci toku dat Intserv.

Tato specifikace určuje typ požadované služby QoS a používá se k nastavení parametrů v plánovači paketů QoS. Tato informace je součástí požadavku rezervace a zahrnuje následující položky:

- *Rspec* Definuje úroveň požadované služby QoS.
- *Tspec* Popisuje tok dat.

Struktura specifikace toku dat poskytuje protokolu RSVP následující parametry QoS. Díky tomu mohou aplikace využívající technologii QoS volat, upravovat nebo odstraňovat nastavení QoS pro daný tok dat.

TokenRate Tento parametr výslovně určuje rychlost, s níž mají být data prostřednictvím sítě po celou dobu přenosu přenášena. TokenRate je podobný ostatním modelům bloků řídicích zpráv, známým také z technologií sítí WAN, jako je například rozhraní Frame Relay, v němž je řídicí zpráva analogická s úvěrem. Nejsou-li tyto řídicí zprávy používány okamžitě, nahromadí se, aby umožnily přenosy dat až do stanoveného množství (velikost bloku řídicích zpráv). Toky jsou také limitovány počtem shlukových přenosů (stanovená špička šířky pásma). Tímto se předchází situacím, v nichž neaktivní toky najednou zaplaví dostupnou šířku pásma nahromaděnými řídicími zprávami. Řízení přenosů je udržováno, neboť toky nemohou odesílat příliš mnoho dat najednou. Integrita síťových prostředků je udržována proto, neboť tato zařízení jsou ušetřena velkých provozních shlukových přenosů.

TokenRate je vyjádřen jako počet bajtů na sekundu. Důležité je zejména to, že aplikace stavějí své požadavky TokenRate na přijatelných očekávaních zatížení při přenosu. Například v případě aplikací pro přenos videa je TokenRate zpravidla nastavován na průměrnou rychlost bitu od špičky po špičku. Je-li člen parametru TokenRate nastaven na hodnotu -1 , nebudou žádná omezení přenosové rychlosti uplatněna.

TokenBucketSize Tento parametr vyjadřuje maximální počet kreditů, jež lze nahromadit pro daný směr datového toku bez ohledu na čas. V aplikacích, určených pro přenos videa, obsahuje TokenBucketSize předpokládanou největší průměrnou velikost rámce. V aplikacích s konstantní rychlostí musí být parametr TokenBucketSize nastaven tak, aby umožňoval zanášení malých korekcí. Hodnota tohoto parametru je vyjádřena v bajtech.

PeakBandwidth Tento parametr určuje horní limit oprávnění toků, v přenosech založených na časovém intervalu, označovaných občas jako limit shlukového přenosu. Parametr PeakBandwidth omezuje toky tak, aby nepřetěžovaly síťové prostředky jednorázovými nebo cyklickými shlukovými přenosy rozdělováním přenosu dat na jednosekundová maxima. Některé mezilehlé systémy mohou tuto informaci využít. Výsledkem je pak ještě efektivnější přidělování prostředků. Hodnota parametru PeakBandwidth je vyjádřena v B/s.

Latency Tento parametr určuje maximální přijatelné zpoždění mezi odesláním bitu odesílatelem a jeho přijetím na straně jednoho nebo více zamýšlených příjemců. Přesná interpretace tohoto čísla závisí na stupni záruky, určeném v požadavku QoS. Hodnota parametru Latency je vyjádřena v mikrosekundách.

DelayVariation Parametr DelayVariation stanovuje rozdíl mezi maximálním a minimálním zpožděním paketu, jež lze ještě akceptovat. Aplikace používají tento parametr k určení prostoru pro mezipaměť, nezbytného na druhém konci přenosu, aby bylo možné ob-

novit původní data podle přenosového vzoru. Hodnota tohoto parametru je vyjádřena v mikrosekundách.

ServiceType Tento parametr určuje úroveň služby pro daný tok:

- *NoTraffic* Indikuje, že v daném směru nejsou přenášena žádná data. Tato hodnota sděluje základnímu softwaru, aby na oboustranných médiích vytvářel pouze jednosměrná spojení.
- *BestEffort* Stanovuje, že síťová zařízení musí vynaložit přiměřené úsilí, aby udržela požadovanou úroveň služby, aniž by převzala jakoukoli záruku za doručení. Toto je standardní úroveň síťové služby.
- *ControlledLoad* Poskytuje koncovou službu QoS, která velmi věrně vyznačuje úroveň kvality přenášovaných dat, která odráží podmínky nezatížené sítě (slabý provoz) na přidružených síťových zařízeních po celé délce trasy přenosu. Ztráta paketů se blíží počtu základních chyb paketů na přenosovém médiu. Zpoždění přenosu v drtivé většině případů nepřesáhne minimální zpoždění, zaznamenané všemi úspěšně doručenými pakety.
- *Guaranteed* Indikuje algoritmus řazení do front v rámci zprostředkovatele služby QoS. Ten izoluje daný tok, jak jen je to možné tak, aby nebyl ovlivněn děním v jiných tocích. Tento algoritmus zaručuje schopnost přenášet data s rychlostí nastavenou parametrem TokenRate po celou dobu přenosu. Přesto když příslušný koncový uzel přenáší data rychleji než stanovuje hodnota parametru TokenRate, může síť nadbytečné přenosy zpozdít nebo ignorovat. Pokud je TokenRate po celou dobu překročen, je zaručeno také požadované zpoždění.
- *Qualitative* Jakostní služba je určena pro aplikace, jež nemohou kvantitativně určit své požadavky na QoS. Aplikace, která vyžaduje jakostní službu, ve skutečnosti žádá síť, aby zjistila, jak je třeba s daty nakládat. Požadavek jakostní služby je zpravidla doprovázen číslem ID aplikace, takže síťový server zásad může způsob nakládání s daty dané aplikace vyřešit. Server zásad může odeslat systému Windows 2000 instrukce, v nichž žádá, aby systém označil přenos jako jakostní tok s určitým kódem DSCP (Differentiated Services Code Point).

Jak funguje protokol RSVP

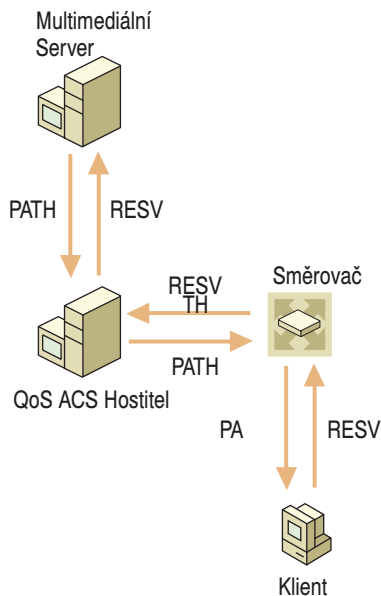
Protokol RSVP je založen na signalizačních zprávách, jež putují napříč sítí a na své cestě alokují příslušné prostředky. Protokol RSVP je iniciován příjemcem, neboť inicializace odesílatelem není dostatečně vhodná pro rozsáhlé scénáře, založené na vícesměrovém vysílání, v nichž se předpokládá existence různorodých příjemců. V těchto scénářích odesílá aplikační server příjemcům pouze zprávy PATH, což výrazně šetří síťovou šířku pásma. V případě přenosů vícesměrového vysílání jsou zprávy RESV od více příjemců slučovány a přijímají maximální požadované hodnoty.

RSVP je protokol typu soft-state, což znamená, že rezervaci je zapotřebí neustále obnovovat, jinak vyprší. Informace o rezervaci neboli stavu je uložena v mezipaměti každého směrování, obsahujícího požadované prostředky. V případě, že síťový protokol směrování změní datovou trasu, pokusí se RSVP přeinstalovat stav rezervace po celé délce předpokládané trasy. Neobdrží-li RSVP zprávu obnovy registrace, časový interval rezervace vyprší a rezervovaná šířka pásma bude uvolněna. Odesílatel obnovuje zprávy PATH a příjemce obnovuje zprávy RESV. Vzhledem k tomu, že služba RSVP odesílá tyto zprávy jako datagramy IP typu best-effort (nejlepší snaha) bez dalšího stupňování spolehlivosti, některé zprávy se mohou cestou ztratit, ale pravidelně se opaku-

jící přenosy obnovovacích zpráv z hostitelských počítačů a směrovačů občasné ztráty zpráv RSVP vyvažují. K zajištění příjmu a obnovení zpráv musí být síťový mechanismus řízení přenosů konfigurován staticky, neboť musí přidělovat určitou minimální šířku pásma zprávám RSVP, které tím chrání před nadbytečným nahromaděním a následnými ztrátami informací. Odesílatel, příjemce nebo jiné síťové zařízení, poskytující QoS, může kdykoli ukončit relaci odesláním zprávy PATH-TEAR nebo RESV-TEAR.

Směrovače protokolu RSVP a přepínače po celé datové trase příslušnou zásadu ověřují. Některá zařízení mohou požadavky přidělení prostředků v důsledku výsledků těchto testů zamítnout. Je-li rezervace zamítnuta vinou nedostatku zdrojů, bude žádající aplikace informována, že síť v daném okamžiku nemusí podpořit vyžádanou kapacitu a typ šířky pásma nebo požadovanou úroveň služby. Aplikace pak určí, zda počká a zopakuje požadavek později, nebo odešle data neprodleně, používajíc doručení typu best-effort (nejlepší snaha). Aplikace, které využívají technologii QoS, jako například programy řízení přenosů vícesměrového vysílání, zpravidla po přijetí této zprávy spustí přenos ihned, a to na bázi typu best-effort. Typ přenosu je inovován na QoS ihned po přijetí rezervace.

Na obrázku 9.4 je znázorněn příklad přenášení zpráv RSVP mezi odesílatelem a příjemcem, prostřednictvím služby řízení podsítě QoS a mezilehlých směrování.



Obrázek 9.4: Jak funguje protokol RSVP.

1. Multimedialní server odesílá zprávu PATH, v níž požaduje přidělení upřednostňované šířky pásma hostitelskému počítači QoS ACS (server Windows 2000 se službou řízení podsítě QoS). Zpráva nakonec zamíří k příjemci dat. V případě vícesměrového vysílání (více příjemců) je zpráva PATH odeslána na adresu vícesměrového vysílání a následně odebírána všemi hostitelskými počítači, jež jsou členy dané skupiny vícesměrového vysílání. Je to právě zpráva RSVP, která je předávána službě řízení podsítě QoS, nikoli datové pakety, které jsou nakonec přenášeny od odesílatele k příjemci.

Až do přijetí rezervace ve zprávě RESV jsou data tohoto připojení odesílána na úrovni služby best-effort. Tento typ služby dává zprostředkovateli QoS instrukce, aby používal parametry aplikace nebo služby QoS jako vodítko pro nastavení požadavků na kvalitu služby a přitom použil odpovídající mechanismy, jejichž pomocí by požadovaný stupeň služby mohl udržet. Neposkytuje však žádné záruky, že tyto parametry budou implementovány nebo vynuceny.

2. V případě, že v dané místní podsíti je přítomen server služby řízení podsítě QoS, bude zpráva PATH směrována právě jím. V tomto případě hostitel služby řízení podsítě QoS potvrdí požadavek a předá jej příjemci (klient). Zpráva PATH putuje prostřednictvím sítě k příjemci po trase, vytyčené síťovým protokolem směrování.
3. Stav PATH je udržován na každém bodu směrování. Každý stav PATH obsahuje kopii zprávy PATH a adresu IP předchozího bodu směrování.
4. Po příchodu zprávy PATH na zamýšlený počítač odpovídá hostitel příjemce (zainteresovaný přijetím dat) odesláním zprávy RESV, která rezervuje prostředky po datové trase vyznačené zprávou PATH.

Nyní příjemce vytváří zprávu RESV, která indikuje, že chce přijmout data z multimediálního serveru.

5. Zpráva RESV putuje obráceným směrem než zpráva PATH, dokud nedorazí na multimediální server. K nalezení správné cesty využije informaci, uloženou ve stavu PATH na každém bodu směrování.
6. Zatímco zpráva RESV putuje k multimediálnímu serveru, každý bod směrování se rozhoduje, zda může přijmout příslušnou rezervaci a přidělit přenosu požadované prostředky. V případě kladné odpovědi bude očekávanému přenosu přidělena fyzická šířka pásma a zprávy RESV jsou předány k následujícímu směrování. V případě, že daný bod směrování není schopen požadavek rezervace přijmout, odešle hostitelskému počítači příjemce zprávu RESV-ERR.

Když na směrovač dorazí zpráva RESV, je přenosu přidělena fyzická šířka pásma. Bod směrování udržuje stav RESV (stav rezervace) a sděluje službě řízení, že data mají být odeslána.

Rezervace je nastavena tak, že k jejímu nainstalování dojde při přijetí první zprávy RESV jako odpovědi na zprávu PATH, vyslanou odesílatelem pro nastavení příslušné relace. Rezervace bude platná, dokud nebude relace ukončena buď hostitelským počítačem, nebo síťovým zařízením. Dokud je však platná, může odesílatel přenášet svá data na cílový počítač.

7. Multimediální server spolu s klientem během přenosu dat pravidelně vysílají také zprávy PATH a RESV, čímž udržují platnost rezervace.

Protokol RSVP nemusí podporovat libovolný bod směrování, obzvláště jsou-li data přenášena prostřednictvím sítě Internet. Zároveň směrovače s podporou protokolu RSVP, jakož i směrovače bez ní, předávají zprávy PATH směrem k jejímu cíli pomocí svých místních tabulek jednosměrového nebo vícesměrového vysílání. Znamená to, že směrování zpráv PATH není směrovači, nevyužívajícími protokol RSVP, nijak ovlivněno. I když skupina směrovačů, nevyužívajících protokol RSVP, nemůže vykonávat analýzy prostředků, ani poskytovat rezervace, může, za předpokladu, že k tomu má dostačující prostředky, poskytovat služby na určité úrovni, použitelné také pro aplikace pracující v reálném čase.

Protokol RSVP během přenosu datového proudu upravuje dynamicky nové trasy. Po změně trasy (například když směrovač nebo přepínač nemohou déle poskytovat vyžá-

dané prostředky) inicializují následující zprávy PATH stav PATH na nové trase a odpoví na tyto zprávy vytvoří fyzickou rezervaci prostředků na nové trase.

Možná dojde k situaci, v níž budete muset aktivovat speciální filtr, jenž umožní zprávám RSVP průchod přes zabezpečovací brány, bezpečnostní brány typu firewall nebo servery proxy, aniž by došlo k vygenerování zprávy PATH-ERR. Zabezpečení protokolu IP v systému Windows 2000 (IPSec) neruší interpretaci žádné ze zpráv RSVP.

Struktura zprávy RSVP

Každá zpráva RSVP se skládá z obecného záhlaví. Jednotlivá pole tohoto záhlaví jsou uvedena v tabulce 9.2.

Tabulka 9.2: Pole obecného záhlaví

Pole	Velikost	Popis
Vers	4 bity	Číslo verze RSVP (tato implementace obsahuje číslo verze 1.)
Flags	4 bity	Rezervováno. V současné implementaci nebyly definovány žádné příznaky.
Message Type	8 bitů	1 = PATH 2 = RESV 3 = PATH-ERR 4 = RESV-ERR 5 = PATH-TEAR 6 = RESV-TEAR 7 = RESV-CONF
RSVP Checksum	16 bitů	Kontrolní součet k zajištění integrity zprávy. Pouze nulové hodnoty znamenají, že nebyl přenesen žádný kontrolní součet.
Send TTL	8 bitů	Zpřístupňuje dobu životnosti (TTL), obsaženou ve zprávě. V případě běžného předávání IP může RSVP zjistit bod směrování bez podpory protokolu RSVP tím, že porovná životnost adresy IP při odeslání zprávy PATH s hodnotou TTL při přijetí zprávy. Tato hodnota je uváděna v záhlaví právě z tohoto důvodu.
RSVP Length	16 bitů	Celková délka zprávy RSVP vyjádřená v bajtech, a to včetně společného záhlaví a následných objektů s proměnlivou délkou.

Každý objekt se skládá z jednoho nebo více 32bitových slov s jednoslovným záhlavím. Tabulka 9.3 obsahuje seznam polí, jež jsou uvedeny v záhlaví objektu.

Tabulka 9.3: Formáty objektů

Pole	Velikost	Popis
Length	16 bitů	Obsahuje celkovou délku všech objektů vyjádřenou v bajtech. Musí to být násobek hodnoty 4, přičemž nejnižší povolenou hodnotou jsou 4.

Class-Num	Třída objektu. Implementace protokolu RSVP musí rozeznávat určité třídy. Seznam tříd, které musí RSVP rozeznávat, je uveden v tabulce 9.3a.
C-Type	Typ objektu. Je jedinečný v rámci třídy objektu. Pole Class-Num a C-Type lze používat spolu jako 16bitové číslo, které jedinečným způsobem definuje typ každého objektu. Hodnoty C-Type jsou definovány pro dvě rodiny adres v síti Internet, IPv4 a IPv6 (zde je uvedena pouze IPv4). Všechna nepoužívaná pole musí být odeslána jako nuly a při přijetí budou ignorována. Seznam hodnot C-Type je uveden v tabulce 9.3b.

Tabulka 9.3a: Pole Class-Num

Pole	Popis
NULL	Délka této hodnoty musí být násobkem hodnoty 4, přičemž nejnižší povolenou hodnotou jsou 4. Může se objevit na každém místě v sekvenci objektů. Obsah je příjemcem ignorován.
Session	Obsahuje adresu IP cíle, hodnotu ID protokolu a port na cílovém počítači. Definuje specifickou relaci pro všechny následující objekty. Vyžadováno.
RSVP_Hop	Je to adresa IP uzlu standardu RSVP, jenž vyslal zprávu, a zároveň je to logický manipulátor výstupního rozhraní.
Time_Values	Interval obnovení. Vyžadován ve zprávách PATH i RESV.
Style	Styl rezervace a k němu se vztahující informace, která není obsažena ani v poli FLOWSPEC, ani v poli FILTER_SPEC. Vyžadováno ve zprávách RESV.
Flowspec	Vyžádané parametry QoS. Část zprávy RESV.
Filter_Spec	Definuje, pro které datové pakety v dané relaci musí být uplatněna vyžádána úroveň služby QoS. Část zprávy RESV.
Sender_Template	Adresa IP odesílatele a pravděpodobně také informace demultiplexoru, která identifikuje odesílatele. Vyžadováno ve zprávách PATH.
Sender_Tspec	Charakteristika přenosu datového toku odesílatele. Vyžadováno ve zprávách PATH.
Adspec	Nese data OPWA ve zprávách PATH. OPWA je zkratkou anglického sousloví „One Pass With Advertising“ (jeden oznamovací průchod) a identifikuje nastavení modelu rezervace, v němž zprávy PATH shromažďují informace (ohlášení), které příjemci mohou používat při odhadu koncové služby.
Error_Spec	Skutečná chyba ve zprávě PATH-ERR, RESV-ERR nebo potvrzení zprávy RESV-CONF.
Policy_Data	Nese informaci, kterou místní modul zásad používá k určení, zda je rezervace správcem povolena. Objevuje se ve zprávách PATH, RESV, PATH-ERR nebo RESV-ERR. Tento objekt není v současnosti plně specifikován.
Integrity	Obsahuje kryptografická data, jež ověřují totožnost uzlu odesílatele, stejně tak jako ověřují obsah zprávy RSVP.
Scope	Výslovný seznam uzlů odesílatelů, jimž je zapotřebí předat informaci. Objevuje se ve zprávách RESV, ResvErr nebo ResvTear.

RESV_Confirm	Adresa IP uzlu příjemce, jenž si vyžádal potvrzení. Objevuje se ve zprávách RESV nebo ResvConf.
--------------	---

Tabulka 9.3b: Pole C-Type

Název objektu	C-Type	Třída	Obsahuje	Další informace
Objekt IPv4/UDP SESSION	1	1	IPv4 DestAddress (4 bajty), Protocol ID, Flags, DestPort	Používá se ve zprávách PATH a určuje hranice sítě, čímž kontroluje uplatňování zásad přenosů. Není-li odesílatel schopen používat zásady, nastaví tento bit ve všech zprávách PATH, které odesílá. Tím sděluje prvnímu bodu směrování standardu RSVP, aby uplatnil svoje zásady (a vypnul příznak).
Objekt IPv4 RSVP_HOP	1	3	IPv4 adresa dalšího/předchozího směrování, manipulátor logického rozhraní (LIH)	LIH charakterizuje logická externí rozhraní. Neexistuje-li manipulátor logického rozhraní, musí toto pole obsahovat nulu.
Time_Values	1	5	Interval obnovení	Časový limit obnovení R, používaný k vygenerování této zprávy RSVP. Vyjádřeno v milisekundách.

Název objektu	C-Type	Třída	Obsahuje	Další informace
IPv4 Error_Spec	1	6	IPv4 Error Node Address (4 bajty), Flags, Error Code, Error Value, Error Node Address	Pole Error Node Address je adresou IP uzlu, na němž byla chyba zaznamenána. Flags: 0x01 = InPlace. Tento příznak se používá pouze pro objekt ERROR_SPEC ve zprávě RESV-ERR. Je-li nastaven, sděluje, že v místě selhání byla a stále existuje rezervace. 0x02 = NotGuilty. Tento příznak se používá pouze pro objekt ERROR_SPEC ve zprávě RESV-ERR. Je nastaven pouze v rozhraní přijímací aplikace. Je-li nastaven, znamená to, že neúspěšná specifikace datového toku FLOWSPEC byla zcela jasně vyšší než specifikace FLOWSPEC požadovaná příjemcem. Error Code je jednobajtovým popisem chyby. Error Value je dvoubajtovým polem, obsahujícím další informace o vzniklé chybě. Jeho obsah závisí na poli Error Type. Více informací najdete v tabulce 9.12.
Scope		7	Tento objekt obsahuje seznam adres IP, používaných pro směrování zpráv pomocí oboru zástupných znaků bez použití cyklů.	Adresy musí být uvedeny v numerickém vzestupném pořadí.
IPv4 Scope_List	1	7	IPv4 Source Address (4 bajty)	

Název objektu	C-Type	Třída	Obsahuje	Další informace
Style	1	8	Flags (8 bitů), Option Vector (24 bitů)	<p>Kolekce bitových polí s hodnotami pro nastavení možností rezervace. Bude-li tato kolekce v budoucnu rozšířena o další členy, budou příslušná pole připojována od nejnižšího platného bitu. Pokud uzel nerozezná identifikátor stylu, může interpretovat tolik vektorů možností, kolik chce, přičemž bude ignorovat všechna nová pole, která mohou být v budoucnu definována.</p> <p>Flags: doposud nepřirazeno.</p> <p>Option Vector, přiřazeno (zleva):</p> <p>19 bitů: rezervováno</p> <p>2 bity: řízení sdílení</p> <p>00b: rezervováno</p> <p>01b: jednotlivé rezervace</p> <p>10b: sdílené rezervace</p> <p>11b: rezervováno</p> <p>3 bity: řízení výběru odesílatele</p> <p>000b: rezervováno</p> <p>001b: zástupný znak</p> <p>010b: výslovné</p> <p>011b – 111b: rezervováno Bity nižšího stupně v poli Vektor možností jsou určený hodnotou pole</p> <p>Style:</p> <p>WF 10001b</p> <p>FF 01010b</p> <p>SE 10010b</p>
Flowspec	1	9	Reserved (zastaralé), objekt Flowspec	
Intserv Flowspec	2	9	Obsah a pravidla kódování tohoto objektu jsou určeny v dokumentech, připravených pracovní skupinou Intserv (jak je uvedeno ve specifikaci RFC 2210).	
IPv4 Filter_Spec	1	10	IPv4 SourceAddress (4 bajty), SourcePort	
IPv4 Sender_Template	1	11	IPv4 SourceAddress (4 bajty), SourcePort	
Intserv Sender_Tspec	2	12	Obsah a pravidla kódování tohoto objektu jsou určena v dokumentech, připravených pracovní skupinou Intserv.	

Název objektu	C-Type	Třída	Obsahuje	Další informace
Intserv Adspec	2	13	Obsah a pravidla kódování tohoto objektu jsou určena v dokumentech, připravených pracovní skupinou Intserv.	
Type 1 Policy_Data	1	14	Obsah tohoto objektu je odložen k dalšímu rozboru.	
IPv4 RESV_Confirm	1	15	IPv4 Receiver Address (4 bajty)	

Podpora QoS v systému Windows 2000

Tato podkapitola obsahuje popis standardů a technologií podporovaných službou QoS v systému Windows 2000.

Architektura signalizované služby QoS

Signalizovaná služba QoS používá signální protokoly jako RSVP k upozornění sítě, aby přizpůsobila zpracování přenosu, jakmile dojde k požadavku upřednostnění. To je v rozporu v porovnání s konfigurovanou službou QoS, jejíž pomocí je síť připojena.

Systém Windows 2000 zavádí architekturu signalizované služby QoS, aby ta mohla poskytovat služby podle aktuální potřeby a uvolňovala šířku pásma pro ostatní typy přenosů. Dělá to tehdy, není-li využívána k přednostním přenosům. Takto může spolu současně existovat více různých typů síťových přenosů. Konfigurovaná služba QoS rezervuje šířku pásma, ať už je to zapotřebí, nebo ne, a plýtvá síťovými prostředky, jež by jinak mohly být využívány pro jiné typy přenosů.

Užití architektury signalizované služby QoS poskytuje také možnost zpětné vazby v reálném čase, založené na aktuálních podmínkách v síti, podpoře pro službu řízení pod-sítě QoS a topologii. Využívá se zde zprávy RSVP, které proudí od zařízení k zařízení a koordinují přidělování prostředků a vytváření rezervací QoS po celé délce datové trasy.

Jakostní aplikace

Správci podnikových sítí se v první řadě soustřeďují na zajištění kvality služeb pro aplikace s klíčovým posláním, jako jsou například aplikace pro plánování prostředků v podnikové síti (ERP), a teprve pak na zajišťování kvality služeb pro multimediální aplikace.

Společnost Microsoft podporuje jak kvantitativní, tak jakostní služby QoS. Díky tomu lze zajistit podporu pro aplikace ERP, ale také pro další aplikace s klíčovým posláním, jež jsou jakostní už svou povahou. Tradiční signalizace protokolu RSVP využívá pro vyjadřování požadavků na kapacitu síťových prostředků právě model integrovaných služeb (Intserv). Zatímco je tento model vhodný pro multimediální aplikace (telefonování IP nebo videokonference), není vhodný pro jakostní aplikace, které nemohou snadno vyjádřit požadavky na nezbytné prostředky v mnohostní podobě tak, jak to vyžaduje model Intserv.

Díky rozšířením signalizačních mechanismů protokolu RSVP poskytuje společnost Microsoft jakostním aplikacím nezbytnou podporu. Vznikla tak nová služba, nazvaná Ja-

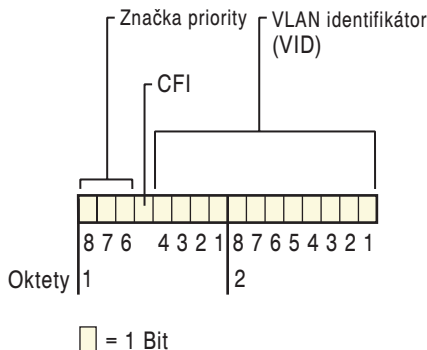
kostní typ služby. Aplikace musí být navrženy tak, aby v základních parametrech QoS zahrnovaly požadovaný typ služby. Tyto aplikace musí být také naprogramovány tak, aby mohly vytvářet prvek zásady, jenž obsahuje názvy aplikace a podaplikace. Tento prvek zásady je porovnáván s databází zásad při výběru zásady pro přenosy právě této konkrétní aplikace. Všechny ostatní funkce služby QoS zpracovává operační systém. Více informací o této úrovni služby najdete v konceptu organizace Internet Engineering Task Force nazvaném „Specification of the Qualitative Service Type“ (Specifikace jakostního typu služby).

Názvy aplikace a podaplikace jsou zahrnuty do signalizační zprávy spolu s typem služby. Po vyžádání tohoto typu služby interpretují síťová zařízení požadavek jako datový tok, jenž vyžaduje specifické zacházení, i když tato zařízení neví, o jaký způsob zacházení se bude jednat. Síťová zařízení vyhledají v databázi aplikací, typ podsady aplikace a žádajícího uživatele. Na základě nalezených informací určí nejvhodnější zásadu upřednostnění daného přenosu. Znamená to, že síťová zařízení ve skutečnosti nepřizpůsobují danému přenosu žádné určité množství prostředků, ale přiřadí tento přenos k příslušné Odlišné třídě služby. Správce sítě musí kromě toho určit (pomocí zásady nebo nastavení registru), jakým způsobem budou mapovány datové toky z různých aplikací do menší skupiny tříd seskupených služeb. Tento model umožňuje seřadit přenosy dané jakostní aplikace podle důležitosti.

Integrace vrstvy 2

Služba QoS v systému Windows 2000 mapuje signály RSVP na signály vrstvy 2 pomocí označení priority IEEE 802.1p. Tím umožňuje seřadit přenosy podle důležitosti pomocí zařízení vrstvy 2, jako jsou například přepínače, na síťové segmenty. Standard označování paketů IEEE 802 se vztahuje na technologii vrstvy 2, včetně vrstvy datového spojení (Data Link) i vrstvy řízení přístupu k médiím (Media Access Control – MAC). Standard IEEE 802.1p definuje způsob, jakým zařízení vrstvy 2 zpracovávají přenosy, označené prioritou 802.1p. Plánovač paketů QoS označuje prioritou 802.1p pakety všech aplikací, které vyžadují službu QoS prostřednictvím obecného rozhraní QoS API nebo Traffic Control API.

V síti Ethernet je priorita 802.1p přenášena ve značkách virtuální místní sítě (VLAN), definovaných standardem IEEE 802.1q/p (802.1p). Pole ve značce 802.1q nese jednu z osmi hodnot priority (o délce 3 bitů), kterou v daném segmentu sítě rozeznávají všechna zařízení 2. vrstvy. Tento způsob označování určuje úroveň služby pro pakety, přenášené přes segment sítě, podporující prioritu standardu 802.1p. Na obrázku 9.5 je znázorněno umístění bitů priority 802.1p uvnitř značky 802.1q.



Obrázek 9.5: Značka 802.1p.

Značka 802.1p je umístěna uvnitř záhlaví Ethernet, mezi záhlavím řízení přístupu k médiím a datovou částí. Mapování ze služebního typu, používaného protokolem RSVP, je zajištěno díky jedné hodnotě priority 802.1p. Výchozí mapování je definováno na hostitelském počítači, avšak důmyslné přepínače mohou usměrnit jako hostitelské počítače, tak směrovače, aby používaly jiné než výchozí mapování. Výchozí označování úrovně upřednostňovaných služeb, uvedené v tabulce 9.4, jsou pevně zapsána v programu Plánovač paketů QoS, implementovaným v systému Windows 2000, a lze je upravit pouze pomocí změn v registru hostitelského počítače.

Tabulka 9.4: Výchozí úrovně priority 802.1p v systému Windows 2000

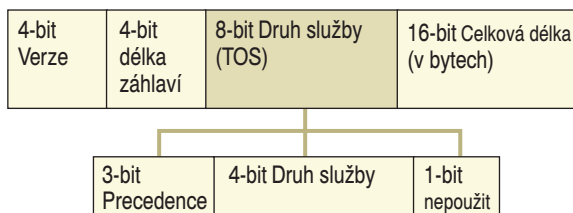
Označení priority	Úroveň služby
0	Nejlepší snaha
1	< Nejlepší snaha
2	Rezervováno
3	Rezervováno
4	Řízené zatížení
5	Zaručená služba s hranicí 100ms
6	Zaručená služba s hranicí 10ms
7	Rezervováno

Odlišná třída služby

Služba QoS v systému Windows 2000 podporuje Odlišné služby (Diff-serv), označované také jako Třída služby (Class of Service – CoS). Diff-serv rozšiřuje QoS na všechny sítě, které doposud s protokolem RSVP nepracují, třeba na velké přepravní sítě, jež tvoří základ sítě Internet.

Plánovač paketů QoS označuje prioritou Diff-serv pakety všech aplikací, které vyžadují označení obecného rozhraní QoS API nebo Traffic Control API. Záhlaví IP daného paketu je označeno hodnotou priority v polích Type of Service (ToS), nazývaných také body kódu Diff-serv (DSCP). Toto označení určuje úroveň služby, poskytované paketu při přenosu přes segment Diff-serv.

Pole Type of Service a DSCP Hodnota DSCP je vytvořena nastavením prvních šesti bitů pole ToS. Na obrázku 9.6 je znázorněno záhlaví IP s ohraničeným polem ToS.



Obrázek 9.6: Záhlaví IP s polem ToS.

Výchozí mapování hodnoty DSCP v desítkové soustavě je uvedeno v tabulce 9.5. Tyto 6bitové hodnoty se zobrazují v horních 6 bitech pole ToS tak, jak je určeno ve specifikaci RFC 2474.

Tabulka 9.5: Označení výchozí priority DSCP

Označení priority	Úroveň služby
0	Nejlepší snaha
24	Řízené zatížení
40	Zaručeno
48	Řízení sítě
0	jakostní

Hodnota DSCP zahrnuje pole IP Precedence, a je proto slučitelná s polem IP Precedence. Pole IP Precedence obsahuje 3 horní bity pole DSCP. Tyto hodnoty jsou uvedeny v tabulce 9.6.

Tabulka 9.6: Označení pole IP Precedence

Označení priority	Úroveň služby
0	Nejlepší snaha
3	Řízené zatížení
5	Zaručeno
6	Řízení sítě
0	jakostní

Plánovač paketů QoS musí být nainstalován na libovolný hostitelský počítač, jenž vytváří nebo interpretuje označení Diff-serv. Pokud zařízení 3. vrstvy mezi koncovými uzly nepodporují Diff-serv, nelze v daném sektoru zaručit udržení úrovně služby QoS.

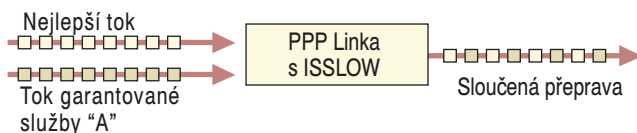
Integrované služby nad pomalým připojením

K profilování přenosů na pomalých připojeních, jako například připojení modemu 28,8 kB/s, slouží speciální mechanismus. V případě těchto připojení může přenos rozsáhlých paketů zaneprázdnit připojení na dlouhou dobu a tím pádem bude docházet ke zpoždění přenosu malých zvukových paketů, které musí být posílány stejnou cestou. To samozřejmě vyvolá problémy s kvalitou zvuku. Aby k tomu nedocházelo, fragmentuje služba řízení provozu objemné pakety v linkové vrstvě a odesílá na zařízení najednou pouze jeden fragment. Zvukové pakety, citlivé na zpoždění, mohou být tím pádem vkládány mezi fragmenty objemnějších paketů. Zmenšuje se tím riziko vzniku zpoždění a zvyšuje se naopak kvalita přijímaného zvuku.

Integrované služby nad pomalým připojením ISLOW je mechanismus pro shromažďování zpráv ve frontách, jenž se používá k optimalizaci pomalých (nizkokapacitních) síťových rozhraní tím, že snižuje zpoždění při doručování. Přesněji je to mechanismus, navržený pro ta rozhraní, která předávají přenosy modemovým přípojkám, kanálům B na přípojkách ISDN a subpřípojkám T1.

Typický paket zaneprázdní modemovou přípojku přibližně na půl sekundy. Příjem dalších paketů, jež se shromažďují ve frontě, se zpožďuje. Pakety, které jsou delší než maximální povolená délka zpoždění, jsou fragmentovány ještě před odesláním prostřednictvím přípojky. To zaručuje, že se mezi jednotlivé fragmenty mohou vklínit také pakety s vysokou prioritou, což ve svém důsledku umožňuje vyhovět vyžadovaným

parametrům QoS pro rychlost přenosu. Na obrázku 9.7 je znázorněna přípojka protokolu PPP (Point-to-Point), využívající mechanismus ISSLOW.



Obrázek 9.7: Přípojka PPP s mechanismem ISSLOW.

Přípojka protokolu PPP například nese data na úrovni služby best-effort (nejlepší snaha) se zaručenou úrovní služby „A“. Kapacita přípojky PPP však je 100 kB/s a průměrné zpoždění je 100 milisekund. Přenos best-effort spotřebuje většinu dostupné šířky pásma přípojky, již se nedostává požadovaných prostředků pro přenos typu A. V tomto příkladu úroveň služby A nemůže tolerovat zpoždění větší než 145 milisekund. Přenos best-effort naplňuje frontu a postupně přicházející pakety z toku A. První paket typu best-effort (10 kilobitů) je fragmentován na 2kilobitové pakety. 8kilobitové pakety z toku A jsou nyní také fragmentovány na 2kilobitové fragmenty, které jsou poté vkládány mezi pakety best-effort tak, aby splnily požadavky na zpoždění toku A.

ATM

ATM je pružný protokol, který přenáší pakety v 53bajtových buňkách. Asynchronní přenos (ATM) se ukázal jako velmi populární páteřní technologie, z důvodu své škálovatelnosti a schopnosti integrovat různé typy síťových přenosů. Rozhraní standardu ATM nevyžaduje služby typu ISSLOW, neboť samotná služba ATM už rozděluje pakety na malé buňky, významně tím omezuje zpoždění a velmi přesně plánuje přenosy. V tom se značně odlišuje od úrovně služby best-effort. Služba ATM vyjedná smlouvu o přenosu mezi koncovým systémem a přístupovým přepínačem ATM ještě před vytvořením připojení, což vyžaduje také kolekci parametrů QoS. Signalizace zahrnuje smlouvu o přenosu, jež stanovuje třídu služby ATM. V tabulce 9.7 jsou uvedena přidružení funkcí služby ATM k funkcím služby QoS.

Tabulka 9.7: Mapování služby ATM na QoS

Třída integrovaných služeb	Třída služby ATM
Zaručená služba	Constant Bit Rate (CBR) nebo Real-Time Variable Bit Rate (rtVBR).
Řízené zatížení	Non-Real-Time Variable Bit Rate (nrtVBR) nebo Available Bit Rate (ABR) s minimální rychlostí buňky.
Best-effort (nejlepší snaha)	Unspecified Bit Rate (UBR) nebo Available Bit Rate (ABR).

Dohody o úrovni služby

Když data procházejí sítí WAN, bývá velmi těžké zaručit požadovanou úroveň služby. Pokud přenos dat probíhá mezi koncovými uživateli, dejme tomu mezi vzdálenými podniky, procházejí data velkým počtem domén (včetně sítě Internet). Na hranici každé domény je přenos předán dalšímu poskytovateli. Různí poskytovatelé musí vyjednávat nové dohody o způsobu nesení a zpracování dat tak, aby zajistily potřebnou úroveň služby. Tyto dohody se označují jako dohody o úrovni služby (SLA).

Dohody SLA stanovují rychlost, s níž musí být informace předávána mezi jednotlivými poskytovateli, jimiž jsou zpravidla ISP. Správce každé domény musí zajistit dostatečný objem síťových prostředků, které budou naplnění dohody SLA, nabízené danou doménou, zajišťovat. Dohody SLA mohou určovat třídy a pravidla označování paketů. Kromě toho, že se musí poskytovatelé dohodnout na přenosu uživatelských dat, musí se také dohodnout na spotřebě zdrojů ve vlastních sítích, které by v jiném případě mohly být nabídnuty jinému uživateli. Určitý datový tok spotřebovává více zdrojů. Tím se jeho přenos prodražuje. Následkem toho poskytovatelé objem upřednostněných přenosů omezují. Tomuto omezení se říká vytváření zásad. Zásady jsou sjednány v dohodě SLA. V případě, že přenos paketů překročí sjednanou mez, může poskytovatel přenos skartovat nebo snížit jeho prioritu na úroveň sjednanou v dohodě SLA.

Zdrojová doména obvykle označuje prioritu paketů ještě před překročením svých hranic. Určení vhodného označení paketů je snadnější, děje-li se blíže zdrojové aplikace, a to ještě předtím, než bude sjednána jakákoliv dohoda o přenosu paketů s jiným poskytovatelem. Přesto musí poskytovatel občas označit pakety místo zákazníka, obzvláště v případech, kdy je uživatel zákazníkem starší sítě. V takových případech označuje poskytovatel pakety pouze tak, aby nepřekročily úroveň služby, sjednanou s dalšími poskytovateli v dohodě SLA.

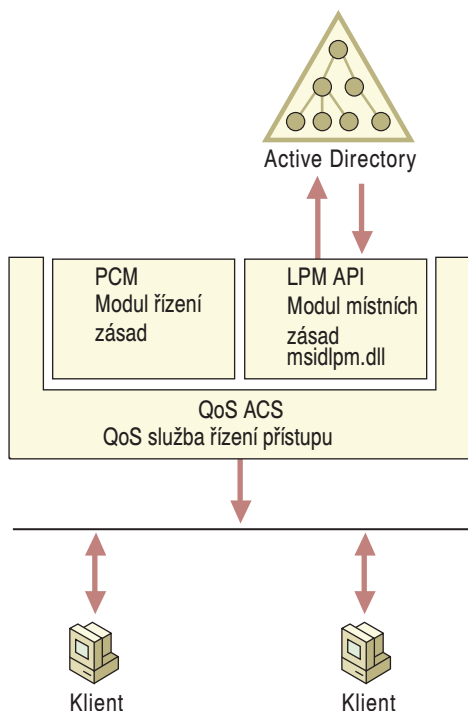
Služba řízení podsítě QoS v systému Windows 2000

Telefonie IP poskytuje znamenitý příklad nezbytnosti služby řízení podsítě QoS. Když uživatel volá pomocí telefonního subsystému IP jinému uživateli, závisí úspěch této operace na dostupné prioritní šíři pásma. Jakékoli další telefonní relace IP mohou teoreticky snížit kvalitu prvního volání, jež je stále aktivní, neboť všechna volání musí sdílet stejnou šířku pásma. K zabezpečení síťových prostředků a zaručení požadované úrovně služby po celou dobu původního volání je nutná Služba řízení podsítě QoS.

Po zavedení služby řízení podsítě QoS nebudou povolena žádná nová volání, dokud nebude dostupná taková šířka pásma, která by zaručila požadovanou úroveň služby. K ověření toho, kdo má v jaké podsíti přístup k širší pásma s vysokou prioritou, slouží ověřovací zásady. Uživatel může mít například právo požadovat videozáznam z místního multimediálního serveru, ale může mít nastavena omezení, která říkají, že mu není dovoleno žádat žádné videozáznamy, jež procházení páteří sítě a překračují její nastavenou mezní hodnotu.

Služba řízení podsítě QoS (QoS ACS) je součástí systému Windows 2000, určenou pro správu síťových prostředků ve sdíleném segmentu sítě (podsít). Tato služba vytváří řídicí bod pro správu požadavků na šířku pásma, pocházejících ze serverů. Tyto požadavky už tedy nemohou zaplavovat síť souběžně. Ve všech podsítích není třeba službu řízení podsítě QoS instalovat. Nejeefektivnější je implementace služby v přepínlých segmentech.

Jak je patrné z obrázku 9.8, uplatňuje služba řízení podsítě QoS svůj vliv tím, že se umístí do fronty zprávy RSVP, zachycuje zprávy PATH a RESV a předává uživatelskou informaci do modulu místních zásad (LPM), kde dochází k vyhledání zásady a ověření totožnosti.



Obrázek 9.8: Služba řízení podsítě QoS.

Služba řízení podsítě QoS zjednodušuje správu podsítě díky implementaci:

- Centralizované konfigurace zásad pro šířku pásma podsítě na bázi konkrétních uživatelů, jednotlivých podsítí nebo podsítě prostřednictvím modulu Služba řízení podsítě QoS,
- transparentnosti vzhledem k uživatelům,
- schopnosti rozdělit prostředky podsítě mezi přenosy s nízkou a vysokou prioritou,
- služeb pro přenosy mezi koncovými klienty s nízkým intervalem zpoždění,
- interoperability s konfiguracemi sítí LAN, WAN, ATM, Ethernet a Token Ring,
- podpory pro přenosy vícesměrových vysílání zpráv s požadavky rezervace šířky pásma.

Jak funguje služba řízení podsítě QoS

Aby bylo možné zavádět multimediální aplikace, pracující v reálném čase, nebo jiné aplikace s klíčovým posláním, jež také vyžadují přijatelnou rychlost přenosu, musí síť zajistit určitý stupeň dostupnosti zaručených prostředků. Služba správy podsítě musí kromě toho najít nějaké řešení, v němž mohou tyto prioritní přenosy existovat souběžně s běžnými přenosy. Jednou z možností je samostatná fyzická podsít pro každý typ přenosu: řešení veskrze nákladné a náročné na údržbu.

Služba řízení podsítě QoS tento problém řeší. Dává správcům sítě nástroj, jehož pomocí mohou centrálně navrhovat jak, kým a kdy budou používány sdílené síťové prostřed-

ky. Služba řízení podsítě QoS uplatňuje logické přidělování síťových prostředků díky spoluúčasti na signálním protokolu. Nemůže však přidělovat nikomu prostředky fyzicky (například síťovou šířku pásma nebo síťové fronty). Jsou to právě zprávy RSVP, jež jsou předávány službě řízení podsítě QoS, a nikoli pakety datové, přenášené mezi odesílatelem a příjemcem.

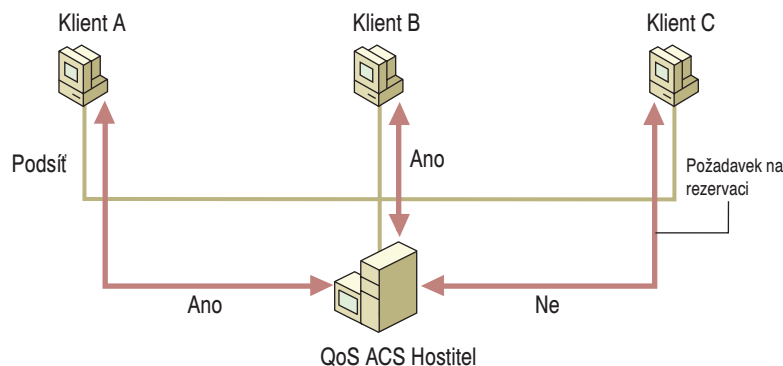
Hostitelská aplikace může i nadále odesílat data, která nejsou přidružená k požadavku RSVP a mohla by teoreticky přetížít danou síť. Služba řízení podsítě QoS však tomu může předejít. Například v sítích Ethernet s podporou správy priorit IEEE 802.1p může tato služba řídit přístup k pásmu přenosů s vysokou prioritou, zatímco mechanismus priority 802.1p zabraňuje tomu, aby přenosům s vysokou prioritou zamezovaly cestu přenosy úrovně best-effort.

Server služby řízení podsítě QoS (QoS ACS) řídí přístup k šířce pásma v podsíti, k níž je připojen. Všechna zařízení v rámci této podsítě (klienti podsítě) podřizují své požadavky na šířku pásma priority požadavkům serveru QoS ACS.

Na obrázku 9.9 je znázorněn server služby řízení podsítě QoS, konfigurovaný tak, že povoluje rezervaci šířky pásma v maximálním objemu 20 megabajtů (MB). Klienti reprezentují zařízení v rámci spravované podsítě.

Po přijetí požadavku na serveru QoS ACS je iniciován následující sled událostí:

- Služba řízení podsítě QoS ověřuje, zda je stupeň síťových prostředků odpovídající. Služba ACS může tuto informaci ověřovat pro odesílatele, příjemce nebo pro oba.
- Pomocí protokolu standardu Kerberos je ověřena totožnost žádajícího uživatele (protokol Kerberos je výchozí službou pro ověřování totožnosti, používanou v systému Windows 2000).
- V adresáři služby Active Directory je vyhledána zásada QoS ACS pro tohoto uživatele (může však být uložena také v mezipaměti serveru QoS ACS).
- Server QoS ACS prověřuje zásadu, aby zjistil, zda má uživatel k přijatému požadavku příslušné oprávnění.
- Služba řízení podsítě QoS požadavek potvrdí nebo zamítne.



Obrázek 9.9: Jak funguje služba řízení podsítě QoS.

1. Aplikace typu videokonference na počítači Klient A požaduje přidělení 10 MB rezervované šířky pásma. Server služby řízení podsítě QoS stanoví, zda v podsíti jsou takové prostředky momentálně dostupné a logicky tuto rezervaci potvrdí. Po přijetí rezervace zůstává v podsíti ještě 10 z dostupných 20 MB rezervované šířky pásma.

2. Aplikace typu videokonference na počítači Klient B požaduje přidělení 10 MB rezervované šířky pásma. Vzhledem k tomu, že v podsíti je i nadále dostatek volných prostředků, server QoS ACS logicky tuto rezervaci potvrdí. Po přijetí rezervace není žádná dostupná šířka pásma.
3. Aplikace typu videokonference na počítači Klient C požaduje přidělení 10 MB rezervované šířky pásma. Vzhledem k tomu, že v dané podsíti už není žádná volná šířka pásma, kterou by mohla tato aplikace použít, je požadavek rezervace zamítnut. Aplikace na počítači Klient C nyní může rozhodnout, zda odešle data na úrovni služby best-effort nebo počká na uvolnění požadované šířky pásma priority.

Klienti a servery se systémy Microsoft® Windows® 98 nebo Windows 2000 či klienti s nainstalovaným softwarem pro správu šířky pásma klienta, jsou automaticky konfigurováni tak, aby při požadavcích na přidělení pásma priority využívali služeb serveru QoS ACS. Tento server odesílá signály IP, tedy zprávy, jež upozorňují klienty podsítě, že server QoS ACS je připraven přijmout další požadavky rezervace šířky pásma. Klient se nepokouší odesílat tyto požadavky, dokud server QoS ACS nevysílá signály IP. Signalizační protokol je popsán v konceptu Subnet Bandwidth Manager (SBM), vypracovaném pracovní skupinou organizace IETF pro RSVP. Klient, připojený k podsíti se sdíleným médiem, sleduje signalizaci serveru služby řízení podsítě QoS. Když ji zachytí, odesílá zprávy RSVP a PATH. Není-li klient součástí sítě spravované serverem QoS ACS nebo pokud v dané podsíti momentálně není aktivní žádný takový server, jsou zprávy RSVP předávány podle metodologie směrování standardu IP. Směrovače a můstky s podporou klientů služby SBM, připojených ke sdíleným médiím jako Ethernet, musí nejprve službu QoS ACS v daném segmentu rozpoznat a předat zprávy RSVP příslušnému serveru QoS ACS.

Server služby řízení podsítě QoS potvrzuje nebo zamítá požadavky rezervace šířky pásma na základě oprávnění, definovaných v zásadě QoS ACS žadajícího uživatele. Po potvrzení požadavku je šířka pásma priority danému uživateli přidělena logicky (každé směrování musí potom šířku pásma ještě přidělit fyzicky) a požadavek je předán příjemci. Server QoS ACS však požadavek zamítne, pokud nemá uživatel oprávnění, nezbytná buď k rezervaci prioritní šířky pásma v dané podsíti, nebo k rezervaci požadované kapacity anebo pokud podsít nemůže v daném okamžiku tyto prostředky poskytnout.

Jestliže však žádost nemůže být potvrzena, nelze přenos zablokovat. Žadající aplikace je o daném stavu okamžitě informována a je na ní, aby se rozhodla, zda odešle data na úrovni služby best-effort, anebo počká a znova odešle svůj požadavek na prioritní šířku pásma později. V případě, že se aplikace rozhodne data odeslat, bude přenos uskutečněn na úrovni služby best-effort.

Povšimněte si, že služba QoS ACS zajišťuje řízení přístupu jak pro zprávy PATH (odesílatel), tak pro zprávy RESV (příjemce).

Implementace služby QoS ACS

Služba QoS ACS je implementací společnosti Microsoft. Služba SBM, která definuje užívání standardizovaných signalizačních protokolů při uplatňování pravidel řízení přístupu typu 802 pro datové toky RSVP v sítích LAN, je standardní technologií, definovanou organizací IETF a implementovanou do služby Microsoft QoS ACS. Služba QoS ACS v systémech Windows 2000 začleňuje technologii SBM pro plnění funkcí řízení přístupu.

V různorodých sítích může v podsíti spolu teoreticky existovat více služeb SBM. Volitelnými zařízeními jsou (ve vzestupném pořadí podle nadřazenosti):

- Přepínače, které umožňují využívat službu SBM a jsou součástí sdílené sítě,
- připojené směrovače, které umožňují využívat službu SBM,
- připojené hostitelské počítače, které umožňují využívat službu SBM (včetně serverů služby QoS ACS systému Windows 2000).

Tato zařízení se podílejí na volbě, založené na vícesměrovém vysílání IP, která určuje Stanovenou službu SBM (DSBM) pro danou podsít. Všichni klienti služby QoS ACS (SBM) v dané podsíti budou předávat všechny zprávy RSVP službě DSBM. Zbývající eventuální služby SBM jsou určeny jako záložní pro případ, kdyby přestala fungovat služba DSBM.

Při správě integrity rezervací RSVP ve sdílené podsíti je důležité, aby byly všechny směrovače a hostitelské počítače, které odesílají zprávy do podsítě (a tím také spotřebovávají její zdroje), klienty služby QoS ACS (SBM). Ve spravované podsíti mohou klienti se systémem Windows 2000 nebo se softwarem klienta služby SBM používat k rezervaci šířky pásma službu QoS ACS. Příslušné aplikace musí podporovat službu QoS.

Službu řízení podsítě QoS lze nainstalovat na libovolný počítač se systémem Windows 2000 Server. Tato služba působí v síťové vrstvě IP a obsluhuje nejběžnější protokoly aplikací včetně všech přenosových protokolů v sadě TCP/IP (TCP, UDP a RTP). Aplikace, které technologii QoS nepodporují, nemohou se serverem QoS ACS komunikovat, ani využívat úroveň síťové služby best-effort.

Jeden server služby řízení podsítě QoS lze konfigurovat tak, aby spravoval více podsítí nebo nesdílených médií, jako je telefonické připojení sítě na vyžádání (najdete například v konfiguraci služby Směrování a vzdálený přístup). Jediným omezením je skutečnost, že služba řízení podsítě QoS nemůže spravovat dva různé typy médií souběžně. Znamená to, že nemůže spravovat zároveň sdílený segment sítě Ethernet a telefonické připojení sítě na vyžádání.

Před nastavením serverů pro řízení přístupu se ujistěte, že váš hardware, konfigurace systému Windows a zásad služby QoS ACS vyhovují nezbytným požadavkům nastíněným v tomto oddílu.

Hardware Síťové adaptéry musí být slučitelné se standardem IEEE 802.1p. Tento standard poskytuje mechanismy nezbytné pro řízení přenosů.

Konfigurace systému Windows Služba řízení podsítě QoS musí být nainstalována na počítači se systémem Windows 2000. Tento počítač musí být členem domény, jež zahrnuje také podsít, kterou máte v úmyslu spravovat. Server služby QoS ACS nesmí být zároveň serverem služby RSVP (s podporou QoS). Může však být také souborovým nebo tiskovým serverem.

Plánovač paketů QoS Musí být nainstalován na všech klientech podsítě, kteří uplatňují rezervace prostřednictvím serveru služby QoS ACS. Kromě toho se doporučuje nainstalovat Plánovač paketů QoS také na server QoS ACS. Jinak by se mohlo stát, že budou některé zprávy RSVP při velkém zatížení serveru QoS ACS vynechány.

Protokoly řízení přístupu Správci se navíc mohou rozhodnout pro vytvoření souboru protokolu služby QoS ACS, jenž může být nápomocen při odstraňování problémů. Tento soubor vznikne protokolováním všech odeslaných a přijatých zpráv RSVP. Takto vzniknou cyklicky přepisované soubory protokolu, podléhající správnému řízení ve

smyslu své velikosti, umístění a celkového počtu. Více informací najdete v oddílu „Odstraňování potíží“ později v této kapitole.

Zásady služby řízení podsítě QoS

Zásada je specifikace limitu daného prostředku. Je nejdůležitějším prvkem implementace služby QoS. Musí být uplatněna při každém rozhodování o oprávněnosti nároku na přenos datového toku v upřednostněném režimu. Z toho vyplývá, že každá instalace QoS musí zahrnovat následující součásti zásad:

- *Úložiště dat* Obsahuje parametry zásady – jména uživatele a síťové zdroje, jež je daný uživatel oprávněn využívat. V případě služby QoS ACS systému Windows 2000 je úložištěm dat zásady adresář služby Active Directory.
- *Rozhodovací body zásady* (PDP) Dohlíží na požadavky přidělení zdrojů a potvrzuje je nebo zamítá na základě příslušné zásady. V případě služby QoS ACS systému Windows 2000 je tímto bodem Modul místních zásad.
- *Body vynucení zásady* (PEP) Jednají na základě rozhodnutí PDP. Síťová zařízení, která fyzicky nebo logicky přidělují prostředky přenášeným tokům. V případě služby QoS ACS systému Windows 2000 jsou to směrovače, přepínače nebo D Správci DSBM (Designated Subnet Bandwidth Manager).

Modul místních zásad

Modul místních zásad (LPM) je součástí serveru služby QoS ACS. Jeho úkolem je vyhledat a zpřístupnit informace ze zásad, uložených v adresáři služby Active Directory. Modul místních zásad je obecný pojem, používaný k označení implementace kurýrní služby, sloužící k vybavení služby QoS ACS prostředky pro vyhledávání informací o zásadách v konkrétním úložišti zásad. Moduly místních zásad jsou integrální součástí služby QoS ACS. Výchozí modul místních zásad v systému Windows 2000 (Msidlpm.dll) popisuje ověření totožnosti porovnáním informací o uživateli na tiketu standardu Kerberos, obsaženém ve zprávě RSVP, s informací v zásadě, uložené v adresáři služby Active Directory. Rozhodování zásady QoS ACS o logickém přidělení šířky pásma je povoleno díky přístupu modulu místních zásad do úložiště zásad služby Windows 2000 Active Directory. Server služby řízení podsítě QoS zavolá Modul místních zásad ihned po zjištění existence objektu s tiketem Kerberos standardu Windows 2000. Modul místních zásad zjistí na základě objektu zásady zprávy RSVP jméno uživatele a potom vyhledá příslušnou zásadu v úložišti zásad služby Active Directory. Modul místních zásad pak může udělat jedno z následujících:

- zamítnout (zamítne na základě zásady),
- přijmout (požadavek může být i přesto zamítnut Modulem místních zásad od jiného dodavatele),
- ignorovat (vyžaduje souhlas).

Požadavek je přijat, pokud alespoň jeden Modul místních zásad souhlasí a žádný není proti (veto). Server QoS ACS potom rozhodne o logickém přidělení šířky pásma.

Modul místních zásad je umístěn na serveru služby řízení podsítě QoS a poskytuje službu pro ověřování totožnosti. Služba QoS ACS poskytuje také rozhraní LPM API, které umožňuje nezávislým dodavatelům vytvářet vlastní řešení modulů místních zásad. V budoucnu se předpokládá také vývoj jak modulů místních zásad (LPM), tak prvků zásad (PE) i u jiných dodavatelů.

Zabezpečení

Při využívání služby řízení podsítě QoS musí také existovat způsob, jímž by bylo možné dokázat serveru QoS ACS, že zpráva RSVP pochází od oprávněného uživatele z důvěryhodné domény Windows 2000. Zpráva tedy musí obsahovat jméno uživatele. Tato informace musí být navíc zašifrována jednotkou, důvěryhodnou z pohledu služby řízení podsítě QoS. Z tohoto důvodu jsou do zpráv vkládány také tikety protokolu Kerberos.

Zprostředkovatel služby QoS na hostitelském počítači, jenž používá službu Středisko distribuce klíčů modulu Kerberos (KDC) domény, může vygenerovat obyčejný tiket protokolu Kerberos, který identifikuje totožnost uživatele, klíč relace pro službu QoS ACS a interval životnosti tiketu. Tiket je zašifrován pomocí sdíleného klíče, známému jak službě KDC, tak službě QoS ACS. Server poslední zmiňované služby používá sdílený klíč k dešifrování tiketu a k získání klíče relace, přičemž postupně ověřuje transformaci šifrování, aby se ujistil, že objekt zásady RSVP je skutečně pravý a že nebyl nikým upraven. Tato metoda také chrání tiket před metodou vyjmout a vložit.

Neplatný tiket protokolu Kerberos vloží do souboru protokolu údaj o chybě a původci zprávy bude odeslána zpráva PATH-ERR nebo RESV-ERR. Servery QoS ACS lze nakonfigurovat tak, aby v takových případech generovaly varování správy sítě (depeše SNMP). Více informací o protokolu SNMP najdete v kapitole „Simple Network Management Protocol“.

Úložiště zásad

Úložištěm zásad služby QoS ACS je adresář služby Windows 2000 Active Directory. Tato služba poskytuje zabezpečené, replikované a trvalé úložiště informací o zásadách služby řízení podsítě QoS. Všechny informace služby QoS ACS vlastní pouze služba QoS ACS a lze je upravovat pouze prostřednictvím programů s oprávněním správy služby QoS ACS. Objekty QoS ACS v úložišti služby Active Directory jsou chráněny zabezpečovacím nastavením, takže server QoS ACS k nim musí mít nastaveno oprávnění alespoň ke čtení. Vytváření a úpravy těchto objektů vyžadují oprávnění správce.

Služba QoS ACS může získat přístup k datům zásady v okamžiku, kdy bude znát název podsítě, pro níž plní úkoly služby řízení přístupu QoS. Název podsítě je konfigurován při instalaci služby QoS ACS na serveru se systémem Windows 2000. Konfigurace musí obsahovat názvy všech podsítí, takže jak konfigurace, tak zásada mohou být uloženy v úložišti Active Directory. V případě konfigurace sítě LAN Ethernet může být názvem podsítě předpona IP, například 192.1.1.0/24. Pokud na jednu logickou podsít' IP připadá více než jedna sdílená podsít', může správce sítě vybrat i jiné názvy než předpony IP.

Každá služba QoS ACS vyhledává svou konfiguraci pomocí názvu podsítě. Tak se může při startu přesunout do správného kontejneru v úložišti Active Directory a následně přechází a uložit v mezipaměti data zásady. V úložišti Active Directory existuje mimo jiné také uzel služby QoS ACS, jenž je kontejnerem všech informací, týkajících se jejich zásad a konfigurace. Server QoS ACS si na službě Active Directory vyžádá konfigurační informace a je-li tato informace přiměřeně malá, může ji uložit ve své mezipaměti.

Definování zásad služby řízení podsítě QoS

Následující oddíly obsahují některé úvahy, jež mohou být užitečné zejména při definování zásady QoS ACS. Informace o procedurálním postupu při samotné konfiguraci jednotlivých parametrů zásady najdete v nápovědě online pro systém Windows 2000 Server.

Hierarchie zásady

Zásady služby QoS ACS jsou uspořádány hierarchicky od nejkonkrétnější (jednotliví uživatelé v příslušné podsíti) po nejobecnější (uživatelská zásada pro všechny podsítě spravované službou řízení přístupu QoS).

Když uživatel vyše žádost o přidělení požadované šířky pásma, bude služba QoS ACS v úložišti Active Directory vyhledávat hodnoty zásady v následujícím pořadí:

- V uživatelské zásadě na úrovni podsítě, v níž se žádající uživatel nachází,
- v uživatelské zásadě na úrovni podnikové sítě.

V případě, že uživatel má kromě vlastní zásady definovanou také zásadu skupiny, má přednost následující pořadí:

- Uživatelská zásada pro aktuální podsít,
- zásada skupiny pro aktuální podsít,
- uživatel s ověřenou totožností pro aktuální podsít,
- uživatel v kontejneru rozlehlé (podnikové) sítě,
- uživatel s ověřenou totožností v kontejneru rozlehlé (podnikové) sítě.

Má-li uživatel definovány zásady v obou umístěních a v obou zásadách jsou konfigurovány stejné hodnoty, budou hodnoty zásady s vyšší prioritou vždy potlačovat hodnoty zásady s nižší prioritou.

Zásady na úrovni rozlehlé (podnikové) sítě

Zásady na úrovni podnikové sítě jsou zásadami platnými v rozsahu celé sítě a vztahují se na přenosy zasílané prostřednictvím libovolné podsítě, spravované službou QoS ACS. Tento kontejner obsahuje dvě předdefinované zásady:

1. *Všichni ověření uživatelé* Tato zásada je uplatňována na všechny ověřené uživatele domény. Ověřeným uživatelem je každý uživatel, řádně přihlášený k účtu domény pomocí jména uživatele a doménového hesla. Doporučuje se upravit parametry QoS této zásady pro potřeby svého podniku tak, aby definovala další zásady na úrovni podnikové sítě pouze v případech, kdy mají jednotliví uživatelé specifické požadavky. Tyto zásady výjimkou musí specifikovat atributy, jež se musí lišit od výchozí zásady. Zásada výjimky a výchozí zásada jsou agregovány při vznesení žádosti uživatele o přidělení šířky pásma.
2. *Neověření uživatelé* Tato zásada je uplatňována v okamžiku, kdy se šířku pásma pokusí rezervovat neověřený uživatel. Je užitečná při řízení přenosů uživatelů, jež mají přístup k síti, ale nejsou ověření důvěryhodnou doménou systému Windows 2000. Pojmem neověřený uživatel se označují všichni uživatelé, kteří nejsou přihlášení k účtu domény, ale jsou zároveň připojeni k síti. Přihlásíte-li se k počítači jako místní uživatel bude vás služba QoS ACS považovat za neověřeného uživatele, neboť jste se nepřihlásili k doméně.

Hodnoty parametrů v předdefinovaných podnikových zásadách jsou uvedeny v tabulce 9.8.

Tabulka 9.8: Výchozí hodnoty zásad na úrovni rozlehlé (podnikové) sítě

Vlastnost přenosu	Všichni ověření uživatelé	Neověřený uživatel
Rychlost přenosu	500 kilobitů za sekundu	64 kilobitů za sekundu
Rychlost přenosu ve špičce	500 kilobitů za sekundu	64 kilobitů za sekundu
Počet toků	Dva (2)	Jeden (1)

Zásady na úrovni podnikové sítě se vztahují na všechny podsítě. Výjimkou jsou pouze případy, kdy má uživatel definovanu pouze zásadu podsítě. Pokud má uživatel A jednu zásadu v kontejneru podnikové sítě a druhou v kontejneru podsítě A, bude zásada definovaná v kontejneru podnikové sítě platit ve všech případech s výjimkou přenosů v rámci podsítě A. Tehdy bude platit zásada podsítě.

Zásady na úrovni podsítě

Pod objektem podsítě můžete vytvářet zásady pro úroveň podsítě. Jednotliví uživatelé mohou mít na určité podsítě vlastní a nezřídka specifické požadavky. Aby bylo možné jejich požadavky splnit, musíte vytvořit uživatelskou zásadu právě pod objektem příslušné podsítě. Můžete konfigurovat pouze ty atributy, jež se liší od hodnot nastavených v zásadách na úrovni celé sítě.

Doporučuje se, aby v kontejneru podsítě byly nejprve změněny zásady pro neověřeného a ověřeného uživatele. Tyto změny mohou uspokojit požadavky většiny uživatelů, kteří odesílají data do dané podsítě. Pokud má uživatel i přesto na přidělování prostředků specifické požadavky, lze vytvořit zásady výjimek. Chcete-li například pro určitého uživatele potlačit agregování šířky pásma, můžete tomuto uživateli vytvořit zásadu podsítě, v níž bude definována pouze hodnota agregované šířky pásma. Všechny ostatní hodnoty, nezbytné pro rezervaci šířky pásma, budou pocházet ze zásady uložené v kontejneru rozlehlé sítě.

Objekty podsítě v konzole QoS ACS

V každé spravované podsíti musíte vytvořit objekt podsítě. Vlastnosti tohoto objektu jsou pak použity při konfiguraci všech vlastností serveru QoS ACS v dané podsíti. Takové uspořádání zaručuje, že všechny servery služby řízení podsítě QoS budou zpracovávat požadavky klientů stejným způsobem.

Objekt podsítě je propojen s fyzickou podsítí a serverem služby QoS ACS pomocí adresy IP podsítě. Vlastnosti objektu podsítě určují:

- Limity přenosů a úroveň služby poskytované danou podsítí,
- vlastnosti přihlašování a tvorby účtů na serveru služby QoS ACS,
- vlastnosti služby QoS ACS na všech serverech QoS ACS.

Musíte nejprve vytvořit objekt podsítě, a teprve pak k němu můžete připojovat uživatelské zásady, vztahující se k dané podsíti.

Vlastnosti podsítě nesmějí být zaměňovány se zásadami uživatele na úrovni podsítě. Objekt podsítě je vytvářen k nastavení limitů přenosů v dané podsíti a k nastavení vlastností serveru QoS ACS, které budou platné pro všechny servery QoS ACS spravující

příslušnou podsít. Zásady na úrovni podsítě, umístěné v kontejneru podsítě (Subnet) modulu QoS ACS, určují uživatelské zásady pro vyžadování šířky pásma dané podsítě.

Odstraňování potíží

V této podkapitole najdete jednak některé metody, vhodné pro určování příčin problémů, vztahujících se ke komunikaci QoS ACS nebo QoS, jednak také popis nástrojů, které mohou opravit jak statistiku, tak chod těchto služeb.

Odstraňování základních problémů

Tabulka 9.9 vytváří jakousi stručnou referenční příručku k odstraňování základních problémů. Najdete v ní návody, jak postupovat v případě nezdařeného zavedení služby QoS.

Tabulka 9.9: Odstraňování základních problémů se službou QoS

Příznak	Doporučený postup/zjištění
Není spojení.	<ul style="list-style-type: none"> ■ Standard 802.1p je povolen u odesílatele, nikoliv však u příjemce. ■ Mezi odesílatelem a příjemcem je zařízení, které neumožňuje používat standard 802.1p. ■ Předčasně ukončena instalace řízení přístupu. Odstraňte předchozí instalaci a pokuste se znovu nainstalovat službu Plánovač paketů QoS. ■ Údaj v registru MaxOutstandingSends v klíči \Psched\Parameters je nastaven na příliš nízkou hodnotu.
Nelze detekovat službu QoS.	<ul style="list-style-type: none"> ■ Selhala signalizace mezi koncovými klienty nebo řízení přístupu. Více informací o sledování zdroje potíží najdete v oddíle „Obecné postupy při odstraňování problémů“ dále v této kapitole. ■ Síť není přeplněna. ■ V této části sítě nejsou aktivní žádné prvky QoS nebo síť není přeplněna. ■ Pakety nejsou správně označeny podle standardu 802.1p. ■ Pakety nejsou správně označeny podle standardu DSCP.
Nefunkční zásada QoS ACS.	<ul style="list-style-type: none"> ■ Zásada konfigurovaná ve službě QoS ACS, která však není správcem Designated Subnet Bandwidth Manager v příslušném segmentu sítě (použijte nástroj Wdsbm, jenž vám pomůže zjistit, která služba QoS ACS je správcem DSBM). ■ Ověřte, zda je služba QoS ACS spuštěna pod názvem účtu QoS ACSService. Více informací o procedurálním postupu najdete v nápovědě online pro systém Windows 2000 Server.

Příznak	Doporučený postup/zjištění
Zprávy RSVP jsou v síti vynechávány.	<ul style="list-style-type: none"> ■ Směrovač na trase datového toku vynechává zprávy RSVP. Integritu cesty RSVP ověřte pomocí nástroje Rsping. ■ Zprávy RSVP jsou vynechány z důvodu přetížení. Ověřte, zda je tok označen jako 802.1p a DSCP.
Požadavek rezervace RSVP byl zamítnut.	<ul style="list-style-type: none"> ■ Nedostatek prostředků, zajištěných některým ze směrovačů nebo serverů QoS ACS. Zamítnutí zásady službou QoS ACS.
Pakety nejsou označeny podle standardu 802.1p.	<ul style="list-style-type: none"> ■ Řízení přenosů není instalováno. ■ Protokol 802.1p není v tomto rozhraní zpřístupněn. ■ Požadavek QoS pro přenos datového toku zamítnut. ■ Rozhraní, které nepodporuje standard 802.1p.
Pakety označené neočekávanou značkou 802.1p.	<ul style="list-style-type: none"> ■ Správce potlačil změnou nastavení hodnot v registru. ■ Přepis nastavení TCLASS. ■ Nekonformní pakety.
Pakety označené neočekávanou značkou DSCP.	<ul style="list-style-type: none"> ■ Přepis nastavení v registru. ■ Přepis nastavení DCLASS.

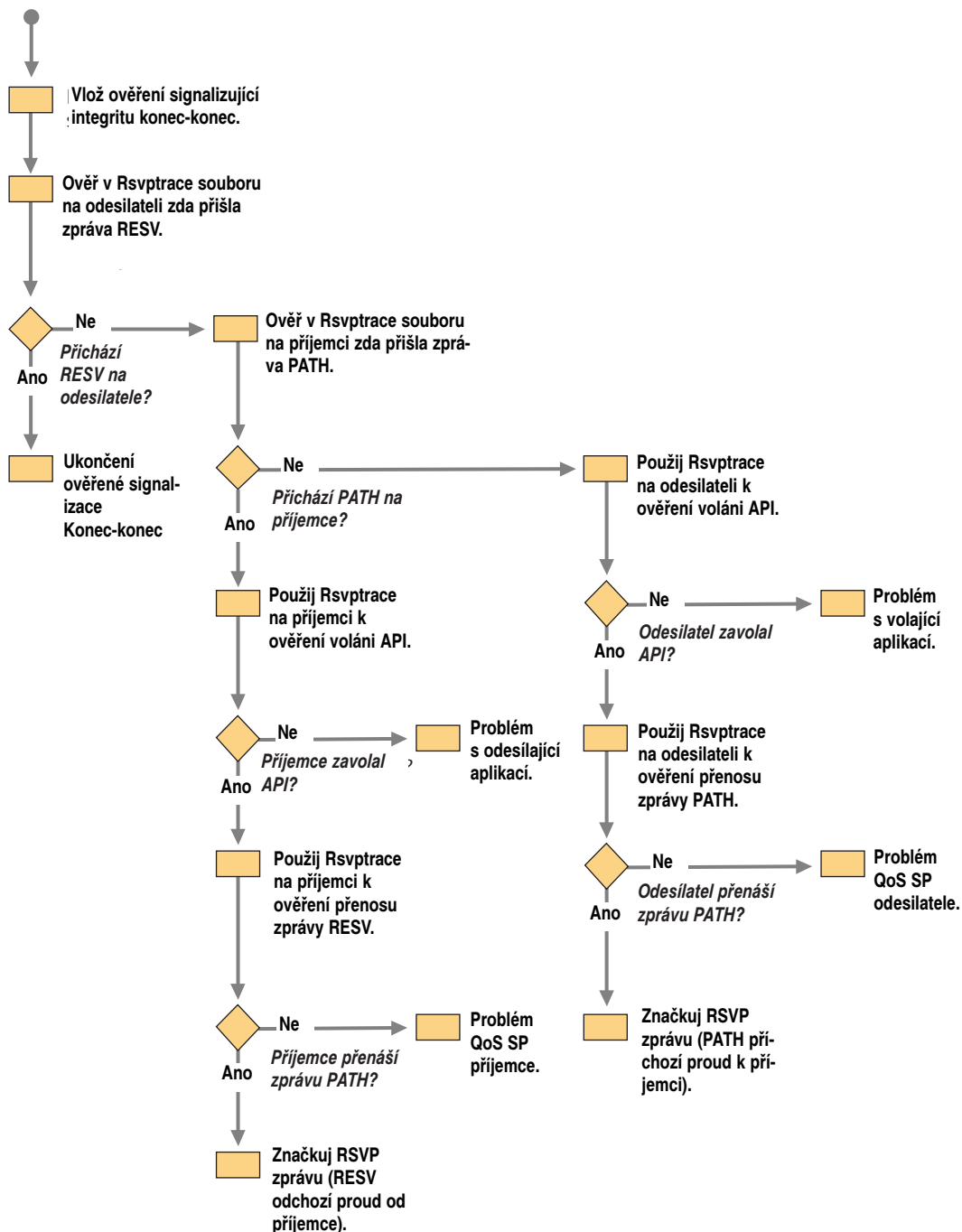
Obecné postupy při odstraňování problémů

Klíčem k odstranění problémů se službou QoS je ověření, zda signalizační zprávy procházejí sítí podle výchozích předpokladů nebo jsou z nějakého důvodu vynechávány či blokovány. Jakmile to zjistíte, bude vaším následujícím krokem ověření toho, zda je řízení přenosů pro řízené zatížení a zaručené úrovně služby voláno efektivně a správně.

Praktickým prvním krokem je návrh topologie sítě, jenž usnadní identifikaci všech síťových zařízení na trase mezi odesílatelem a příjemcem. Usnadní také zjištění všech zařízení, která se na signalizaci RSVP podílejí. Zjištění těchto zařízení je velmi důležité, neboť zachycují zprávy RSVP, přenášené sdílenými segmenty. Užitečnými nástroji při určování topologie sítě jsou Tracert a Wdsbm.

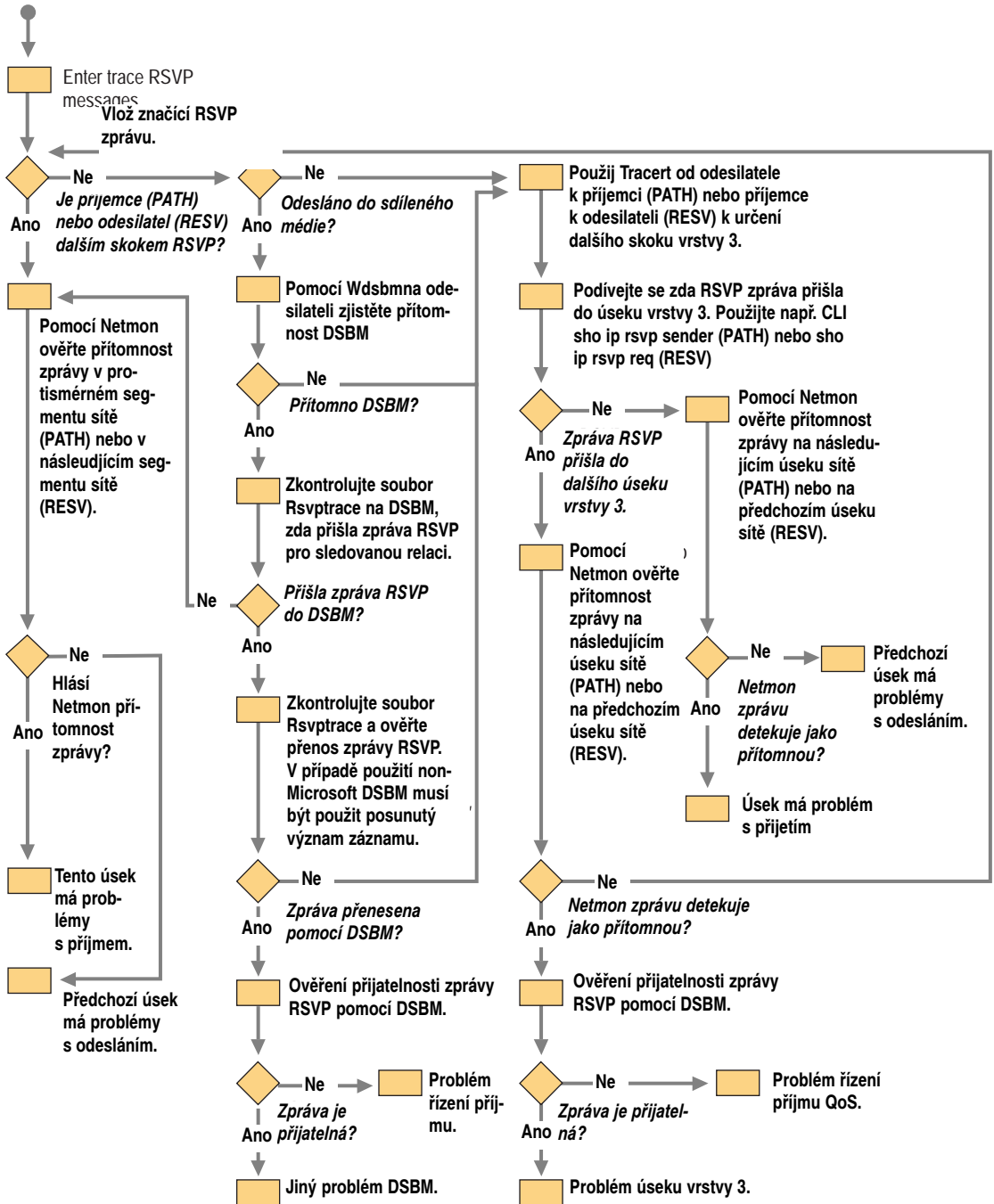
Sledování zpráv RSVP od zdroje k cíli Na obrázku 9.10 je znázorněn postup ověření signalizace mezi koncovými uzly. Na obrázku 9.11 je pak uveden postup sledování jednotlivých úseků trasy zpráv RSVP.

Start



Obrázek 9.10: Ověření signalizace mezi koncovými uzly.

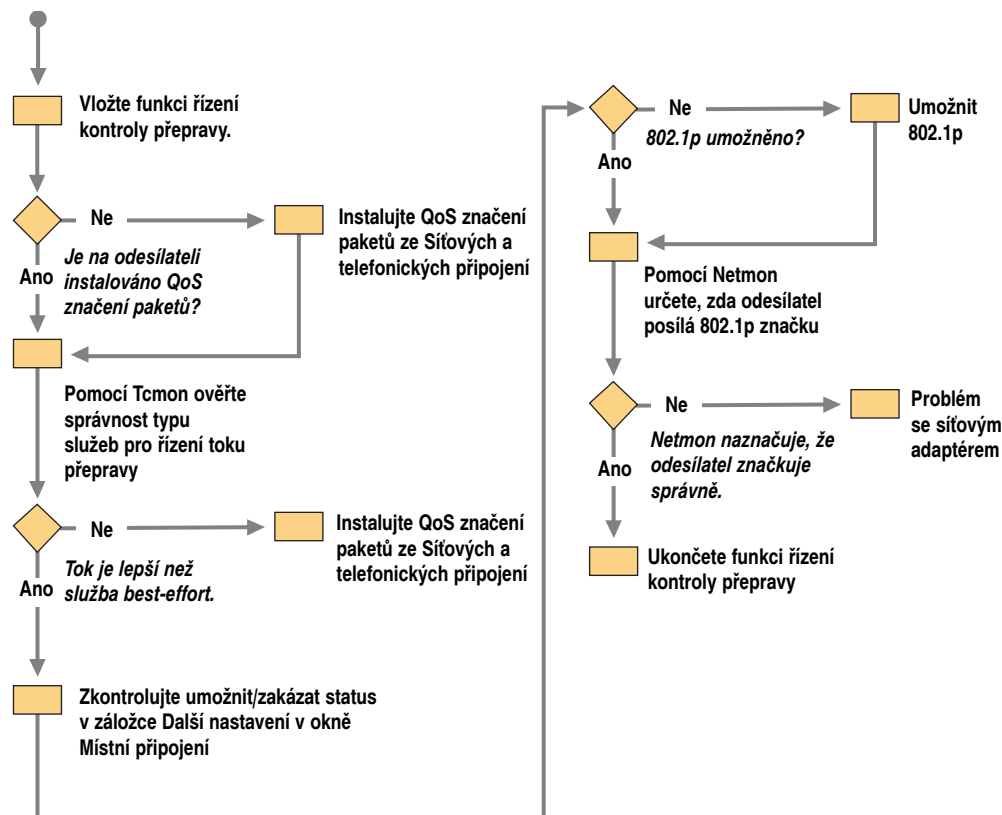
Start



Obrázek 9.11: Sledování stopy zpráv RSVP.

Na obrázku 9.12 je popsána metoda ověření funkčnosti řízení přenosů.

Start



Obrázek 9.12: Metoda ověření funkčnosti řízení přenosů (802.1p).

Soubory protokolu služby QoS ACS

Transakce QoS ACS (zprávy RSVP) lze shromažďovat. Stačí konfigurovat soubory protokolu služby QoS ACS. Zprávy protokolu účtování služby řízení přístupu a služby protokolování RSVP lze prohlížet v programu Prohlížeč událostí systému Windows 2000 Server. Zprávy protokolu jsou velmi podrobné a jsou ukládány jako pevný (nepřízpůsobitelný) soubor ve formátu ASCII, jenž lze prohlížet v textovém editoru nebo převést na databázi rozhraní ODBC (Open Database Connectivity). Nepleťte si soubory protokolu služby QoS ACS s výchozími soubory protokolu systému Windows 2000 Server (které lze prohlížet pomocí Prohlížeče událostí).

Při vytváření všech typů souborů protokolu můžete nastavit celou řadu možností včetně složky, v níž budou soubory vytvořeny, a toho, zda bude vytvořen jeden nebo více souborů. Soubory protokolu jsou cyklické. Když nastavíte maximální velikost souboru, dojde po dosažení této hodnoty k jedné ze dvou událostí:

- Bude vytvořen další soubor protokolu. Nové soubory protokolu budou vytvářeny tak dlouho, dokud nebude dosaženo jejich maximálního povoleného počtu. Ten-

to způsob reakce na dosažení povolené velikosti souboru je vhodný zejména pro prohlížení historie transakcí, ale také pro prohlížení pouze posledních informací.

- První soubor je jednoduše přepsán vždy, jakmile dosáhne svého maxima. Toto nastavení však nedovoluje zpětné prohlížení historie.

K tomu, abyste si mohli prohlédnout obsah souborů protokolu, není třeba služby QoS ACS zastavovat. Po každém požadavku na přidělení šířky pásma je vygenerován nový záznam. To způsobuje soustavné narůstání velikosti souborů nebo jejich počtu. Proto může nastat potřeba vyvážení mezi shromažďováním podrobných dat a potřebou omezení souborů na snadno ovladatelnou velikost nebo snadno zvládnutelný počet. Mimořádně velké soubory protokolu mohou ovlivnit výkon služby, neboť každý soubor obsahuje přibližně 500 zpráv na jeden megabajt. Správci kromě toho mohou požadovanou informaci snáze najít v menších souborech. Při určování velikosti souborů protokolu mějte na paměti volné místo na disku a i pak nepřestávejte sledovat volný prostor při všech operacích spojených s protokolováním událostí.

Účtovací protokoly

Informace uložené v souboru účtovacího protokolu jsou užitečné pro:

- Plánování počtu uživatelů, kteří si pravidelně rezervují síťové prostředky,
- odhad aktuálních a budoucích požadavků na šířku síťového pásma,
- odstraňování problémů po vzniku chyb při síťové komunikaci, zabezpečené službou řízení podsítě QoS.

Informace v souboru účtovacího protokolu zahrnuje následující údaje:

- Kdo aktuálně síťový prostředek používá,
- datum a čas individuálních relací,
- informace o adresování individuálních relací.

Všechna pole v souboru protokolu jsou ukončena středníkem (;). Následující ukázka je příkladem záznamu ze souboru účtovacího protokolu:

```
1998/11/18 13:58:00:0578;192.168.3.5:4000[17];Start
Sender;ENGR\Vincent;192.168.3.4:4000;New; 250000,1500,300000,10,1500
```

Pro účtování má největší význam viditelnost informace o tom, že hostitelský počítač řízení podsítě QoS potvrdil požadavek na šířku pásma 18. listopadu 1998 (1998/11/18) ve 13.58 (13:58:00:0578), což spustilo relaci (StartSender) s identifikátorem 192.168.3.4, načež začalo odesílání dat z hostitelského počítače v doméně Řízení (ENGR), jehož uživatelem je Vincent.

Tabulka 9.10 obsahuje popis všech polí v souboru protokolu.

Tabulka 9.10: Všechna pole souboru protokolu

Pole	Popis
Datum/čas	Datum a čas zprávy ve formátu GTM (Greenwich Mean Time).
Informace o adrese IP relace.	Adresa IP příjemce, číslo portu, na něž jsou data posílána (za dvojtečkou) a desítkové číslo ID použitého protokolu uzavřené v hranatých závorkách ([]). Chcete-li vyhledat názvy protokolů podle čísel ID, podívejte se do specifikace RFC 1700.
Typ záznamu	Jeden z následujících typů: Start Sender, Start Receiver, Stop Sender, Stop Receiver, Reject Sender nebo Reject Receiver.

Pole	Popis
Číslo ID uživatele	Doména a jméno uživatele, kterému předchází zpětné lomítko (\), jenž je buď odesílatelem nebo příjemcem.
Informace o adrese IP posledního směrování	Adresa IP posledního směrování a také číslo portu, na nějž jsou data posílána (za dvojtečkou) nebo hexadecimální adresa síťového adaptéru (je-li hostitel dávající zprávu vícedomým zařízením). Například 192.168.2-2.106:0x00000000.
Stav zprávy	Jedna z následujících hodnot: New, Modify, Stop Sender důvod, Reject Sender nebo adresa IP zdroje datového toku.
Podrobnosti zprávy	Informace odesílatele o přenosu, informace příjemce o přenosu, Stop Receiver důvod a Reject Receiver důvod.

Účtování

Informaci vygenerovanou službou QoS ACS můžete používat k účtování. Z hlediska správy sítě vám funkce účtování umožňují celkový pohled na způsob využívání prostředků QoS. Účtování QoS ACS vám přesně ukáže, kde se jaký prostředek používá a navíc jak dlouho. Neúspěšné požadavky jsou zaznamenávány také, což poskytuje pohled na to, kdo se pokoušel používat služby QoS, aniž by k tomu měl patřičné oprávnění.

Tyto informace máte k dispozici, neboť servery QoS ACS protokolují zprávy RSVP a zaznamenávají v nich počátek a konec přenosu, dále pak vyžádaný prostředek a uživatele, jenž o přidělení prostředku požádal. Tyto záznamy lze shromažďovat z údajů serveru QoS ACS a používat k vygenerování různých hlášení o využívání služby pro správce sítě. Jak je také zřejmé, je možné tyto záznamy použít k vygenerování účtu za používání sítě.

Protokoly RSVP

Další možností je konfigurace protokolování zpráv RSVP. Protokol zpráv RSVP poskytuje podobné informace jako program Sledování sítě (NetMon). Pomocí protokolu můžete sledovat, kdo odesílá a přijímá zprávy RSVP a zda jsou tyto zprávy přijímány nebo zamítány. Tyto informace můžete využít při odstraňování problémů po vzniku chyb, spojených se síťovou komunikací řízenou službou QoS ACS.

Informace v souboru protokolu RSVP vám pomůže při odstraňování potíží tím, že vám zprostředkuje následující informace:

- Datum a čas vygenerování zprávy RSVP,
- informace o adresách odesílatele a příjemce zprávy.

V souboru protokolu RSVP je každé pole ukončeno čárkou (.). Svislá čárka (!) indikuje konec skupiny informací o daném přenosu. Následující ukázka je příkladem záznamu v souboru protokolu RSVP:

```
1998/02/06 15:35:05, PATH,192.168.3.6,4000,17,!,
192.168.3.5,0x00000000,!,30000,!,
192.168.3.4,4000,!,3.000E+004,1.50E+003,3.300E+004,10,1500,!,
0,0.000E+000,1500,1.#IOE+000
```

Nejdůležitější údaje v tomto záznamu říkají, že 6. února 1998 v 15.35 byla z hostitelského počítače 192.168.3.4 na počítač 192.168.3.6 odeslána zpráva PATH.

Tabulka 9.11 obsahuje popis všech položek v souboru protokolu, přičemž zobrazuje také parametry, jež musí každá zpráva v protokolu RSVP mít.

Tabulka 9.11: Všechna pole souboru protokolu RSVP

Pole	Popis
Datum/čas	Datum a čas zprávy ve formátu GTM (Greenwich Mean Time).
Typ zprávy	PATH, RESV, PATH-ERR, RESV-ERR, PATH-TEAR nebo RESV-TEAR s dalšími parametry: <i>Požadavek potvrzení:</i> RESV-CONF nebo No RESV-CONF, jenž určuje, zda příjemce chce nebo nechce potvrdit rezervaci. <i>Obor:</i> Výslovný seznam hostitelských počítačů odesílatelů (ve formátu rezervace se zástupnými znaky), jimž bude informace ve zprávě předána. <i>Styl rezervace:</i> Stanoví, zda budou prostředky rezervovány pomocí pevného filtru, výslovného sdílení nebo pomocí zástupných znaků. Více informací o těchto stylech najdete ve specifikacích RFC 2205, 2210, 2215 a 2216. Podrobné informace o těchto parametrech najdete ve specifikaci RFC 2205.
Informace o adrese IP relace.	Adresa IP příjemce, číslo portu, na něž jsou data posílána a desítkové číslo ID použitého protokolu, za nímž následuje svislá čárka (). Chcete-li vyhledat názvy protokolů podle čísel ID, podívejte se do specifikace RFC 1700.
Informace o adrese IP posledního směrování	Adresa IP posledního směrování a také číslo portu, na něž jsou data posílána (za dvojtečkou), nebo hexadecimální adresa síťového adaptéru (je-li hostitel překládací zprávu vícedomým zařízením). Následuje svislá čárka ().
Interval obnovení	Četnost odesílání zpráv v milisekundách.
Informace o adrese IP odesílatele	Adresa IP odesílatele, číslo portu, na něž jsou data posílána, a desítkové číslo ID použitého protokolu, za nímž následuje svislá čárka ().
Rychlost bloku	Rychlost bloku dat.
Velikost bloku	Velikost bloku, v němž jsou data za účelem přenosu seskupena. Více informací o blocích paketů najdete ve specifikacích RFC 2210, 2215 a 2216.
Maximální rychlost	Shluková rychlost paketů.
Velikost paketu	Minimální velikost paketu určeného pro přenos.
Velikost jednotky MTU	Maximální velikost paketu určeného pro přenos, za níž následuje svislá čárka (). Toto pole spolu s předchozími čtyřmi poli vytváří hodnotu Tspec (parametry přenosu datového toku). Více informací o parametrech přenosu datového toku najdete ve specifikacích RFC 2205, 2210, 2215 a 2216.
Adspec	Zbývající pole v záznamu indikují parametry přenosu určené pro příjemce.

Chybové kódy RSVP

Tabulka 9.12 obsahuje chybové kódy, jež se vyskytují ve zprávách RESV-ERR.

Tabulka 9.12: Chybové kódy a jejich hodnoty

Chybový kód	Popis
00	Potvrzení. Rezervováno pro použití objektu ERROR_SPEC ve zprávě RESV-CONF. Hodnota chyby bude vždy nulová.
01	Selhání řízení přístupu. Požadavek přidělení rezervace byl zamítnut službou řízení přístupu, neboť služba neměla v daném okamžiku dostatek volných prostředků. 16 bitů pole chybové hodnoty jsou ssur, cccc cccc a cccc, kde se jednotlivé bity dělí na: ss = 00: Dolních 12 bitů obsahuje globálně definovaný druhotný kód (hodnoty uvedené dále). ss = 10: Dolních 12 bitů obsahuje druhotný kód organizace. RSVP může tento kód interpretovat pouze jako numerickou hodnotu. ss = 11: Dolních 12 bitů obsahuje druhotný kód služby. RSVP může tento kód interpretovat pouze jako numerickou hodnotu. Vzhledem k tomu, že řídicí mechanismus může různé služby nahradit, může toto kódování obsahovat určitou reprezentaci používané služby. u = 0: Služba RSVP zamítne zprávu, aniž by aktualizovala místní stav. u = 1: RSVP může použít zprávu k aktualizaci místního stavu a potom zprávu předá dál. Znamená to, že zpráva je informačního charakteru. r: Rezervovaný bit, musí obsahovat nulu. cccc cccc cccc: 12bitový kód. Následující globálně definované druhotné kódy se mohou vyskytovat v dolních 12 bitech, kdy ssur = 0000: Druhотný kód = 1: Nelze splnit požadavek mezního zpoždění. Druhотný kód = 2: Požadovaná šířka pásma je nedostupná. Druhотný kód = 3: jednotka MTU ve specifikaci toku dat je větší než rozhraní MTU.
02	Selhání řízení zásad. Rezervace nebo zpráva PATH byly zamítnuty z administrativních důvodů (nebylo například doručeno vyžadované doporučení, nedostatečné penzum nebo vyrovnání nebo nucené přerušení správcem). Tento chybový kód se může vyskytnout ve zprávě PATH-ERR nebo RESV-ERR. Obsah pole chybová hodnota bude určen v budoucnu.
03	Není určena cesta této zprávy RESV. Není nastaven stav cesty pro danou relaci. Zprávu RESV nelze předat dál.
04	Tato zpráva RESV neobsahuje údaje o odesílateli. Existuje sice informace o stavu cesty, ale ta neobsahuje žádný popisovač odesílatele, jež by se shodoval s obsahem zprávy RESV. Zprávu RESV nelze předat dál.
05	Konflikt stylu rezervace. Styl rezervace je v konfliktu s existujícími styly rezervace. Pole chybová hodnota obsahuje dolních 16 bitů pole Option Vector existujícího stylu, s nímž je nový styl v konfliktu. Zprávu RESV nelze předat dál.
06	Neznámý styl rezervace. Zprávu RESV nelze předat dál.
07	Neslučitelné porty cíle. V relaci pro danou adresu a protokol se vyskytly jak nulová, tak nenulová pole portů cíle. Tento chybový kód se vyskytuje ve zprávách PATH-ERR nebo RESV-ERR.
08	Neslučitelné porty odesílatele. Ve zprávách PATH dané relace se vyskytují jak nulové, tak nenulové porty odesílatele. Tento chybový kód se vyskytuje pouze ve zprávě PATH-ERR.
09, 10, 11	(rezervováno)
12	Nucené přerušení služby. Požadavek služby, definovaný objektem STYLE, a popisovač toku byly přerušeny správcem. V případě tohoto chybového kódu je 16 bitů chybové hodnoty takovýchto: ssur cccc cccc cccc Horní bity ssur jsou definované v chybovém kódu 01. Globálně definované druhotné kódy, jež se mohou vyskytnout v dolních 12 bitech, když se ssur = 0000, budou definovány v budoucnu.

Chybový kód	Popis
13	Neznámá třída objektu. Chybová hodnota obsahuje 16bitovou hodnotu, složenou z polí Class-Num a C-Type neznámého objektu. Tato chyba může být vyslána pouze v případě, že RSVP zamítne zprávu, což určují horní bity pole Class-Num. Tento chybový kód se vyskytuje ve zprávě PATH-ERR nebo RESV-ERR.
14	Neznámý objekt C-Type. Chybová hodnota obsahuje 16bitovou hodnotu, složenou z polí Class-Num nebo C-Type daného objektu.
15-19	(rezervováno)
20	Rezervováno pro rozhraní API. Pole chybová hodnota obsahuje chybový kód rozhraní API, neboť byla asynchronně zjištěna chyba rozhraní API, kterou je třeba ohlásit prostřednictvím volání upcall.
21	Chyba řízení přenosů. Volání řízení přenosů selhalo vinou formátu nebo obsahu parametrů požadavku. Zprávu RESV nebo PATH, která způsobila volání, nelze předat dál a opakování volání je zbytečné. V případě tohoto chybového kódu se chybová hodnota skládá ze 16 následujících bitů: ss00 cccc cccc cccc Horní bity ss jsou definovány v chybovém kódu 01. Globálně definované druhotné kódy, jež se mohou vyskytnout v dolních 12 bitech (cccc cccc cccc), když ss = 00: Druhotný kód = 01: Konflikt služby. Pokus o sloučení dvou neslučitelných požadavků na službu. Druhotný kód = 02: Nepodporovaná služba. Řízení přenosů nemůže poskytnout ani vyžádanou službu, ani žádnou přijatelnou náhradu. Druhotný kód = 03: Chybná hodnota specifikace toku dat. Deformovaný nebo neopodstatněný požadavek. Druhotný kód = 04: Chybná hodnota parametrů přenosu datového toku. Deformovaný nebo neopodstatněný požadavek. Druhotný kód = 05: Chybná hodnota objektu Adspec. Deformovaný nebo neopodstatněný požadavek.
22	Systémová chyba řízení přenosů. Systémová chyba byla zjištěna a ohlášena jedním z modulů řízení přenosů. Chybová hodnota obsahuje systémovou hodnotu, která blíže popisuje vzniklou chybu. Nepředpokládá se, že by služba RSVP byla schopna tuto hodnotu interpretovat.
23	Systémová chyba RSVP. Pole Chybová hodnota poskytuje informace závislé na implementaci. RSVP není schopna tuto hodnotu interpretovat.

Každá zpráva RSVP je obvykle znovu sestavena na každém bodu směřování a uzel, jenž zprávu RSVP vytvoří, je zodpovědný ze její korektní sestavení. Podobně musí každý uzel ověřovat korektnost sestavení všech přijímaných zpráv. Kdyby programátorská chyba umožnila službě RSVP vytvořit deformovanou zprávu, nebyla by chyba koncovému systému ohlášena v podobě objektu ERROR_SPEC, ale zobrazila by se místně a pravděpodobně by byla ohlášena pomocí mechanismu správy sítě.

Jedinými chybami, jež vytvářejí zprávy odesílané koncovým systémům, jsou chyby, které odrážejí nesoulad verzí a které lze v koncových systémech obejít (například uchýlením se k předchozímu parametru C-Type pro daný objekt, viz kód 13 a 14 v předchozí tabulce).

Volba chyb generujících zprávy, které lze detekovat pomocí služby RSVP a místně pak protokolovat, je závislá na dané implementaci. Přesto zpravidla obsahuje následující údaje:

- Zpráva s chybnou délkou: Hodnota pole Délka RSVP neodpovídá délce zprávy,
- neznámá nebo nepodporovaná verze RSVP,
- chybný kontrolní součet RSVP,
- selhání integrity,

- nepřípustný typ zprávy RSVP,
- nepřípustná délka objektu: hodnota není násobkem hodnoty 4 nebo je menší než hodnota 4,
- adresa IP pro předchozí nebo následující směrování, uložená v objektu HOP, je nepřípustná,
- chybný port zdroje: port na zdrojovém počítači je nenulový, zatímco ve specifikaci filtru nebo v šabloně odesílatele pro danou relaci je určen nulový port,
- chybí třída vyžadovaného objektu (určit),
- v typu zprávy je určena třída neplatného objektu (určit),
- narušení požadovaného pořadí objektů,
- chybná hodnota čítače popisovače toku pro daný styl nebo typ zprávy,
- neplatný manipulátor logického rozhraní,
- neznámý objekt Class-Num,
- adresa cíle zprávy RESV-CONF neodpovídá adrese příjemce, uvedené v objektu RESV_CONFIRM, který tato zpráva obsahuje.

Nástroje

Tento oddíl obsahuje popis různých nástrojů a jejich význam při odstraňování problémů s implementací služby QoS. Část nástrojů je popsána pouze stručně. Více informací o najdete v nápovědě pro Nástroje soupravy prostředků Microsoft® Windows® 2000.

PathPing

Tento nástroj protokolu TCP/IP má několik zajímavých funkcí, vztahujících se k QoS.

-t

Jsou-li pakety s označením 802.1p odesílány ze sítě s podporou standardu 802.1p do sítě bez podpory tohoto standardu, může být přepínač spojující obě tyto sítě konfigurován tak, aby toto označení paketů rušil ještě předtím, než odešle takto označené pakety do sítě, která nepracuje se standardem 802.1p. Kdyby to neudělal, mohla by některá zařízení, nevyužívající protokol 802.1p, pakety zamítnout, chybně se domnívající, že jsou poškozené. Aktivací tohoto parametru umožníte odesílat pakety s označením, které identifikuje síťové prvky, jež odmítají označené pakety.

-r

Tento přepínač testuje, zda všechny uzly na předpokládané trase datového toku podporují protokol RSVP. Odpoví-li uzel na zprávu protokolu 46 (nebo vyprší-li časový interval), je považován za slučitelný se standardem RSVP. Pokud však odešle chybové hlášení protokolu ICMP „nedostupný“, předpokládá se, že nepodporuje RSVP. Není-li v daném okamžiku na příslušném uzlu spuštěna služba RSVP, vrátí uzel chybové hlášení protokolu ICMP „nedostupný“.

Více informací o nástroji PathPing najdete v kapitole „Řešení problémů protokolu TCP/IP“.

Wdsbm

Tento nástroj identifikuje službu QoS ACS, která spravuje segment sítě, k němuž je příslušný hostitelský počítač připojen.

```
wdsbm -i < adresa IP místního rozhraní >
```

Program Wdsbm vytiskne informaci (včetně adresy IP), jež se vztahuje na službu QoS ACS, která zachycuje příchozí i odchozí zprávy RSVP určeného rozhraní. Vzhledem k tomu, že služba QoS ACS může zprávy RSVP blokovat, je dobré znát adresu IP serveru služby QoS ACS. Takto můžete snáze izolovat místo, v němž dochází k zadržování zpráv RSVP.

Rsvptrace

Nástroj příkazového řádku Rsvptrace generuje protokol zpráv RSVP, které jsou odesílány a přijímány zprostředkovatelem služby QoS na hostitelském počítači. Tento nástroj zobrazuje volání funkcí API aplikací jak odesílajících, tak přijímajících zprávy zprostředkovatele služby QoS. Spustíte-li program Rsvptrace na odesílateli a příjemci, bude snadné ověřit, zda aplikace skutečně požadované funkce API volá, zda zprostředkovatel služby QoS generuje zprávy RSVP a zda zprávy přicházejí ze sítě. Program Rsvptrace můžete spustit také na serveru QoS ACS a prohlédnout si přijaté a odeslané zprávy RSVP. Vzhledem k tomu, že servery QoS ACS žádné multimediální aplikace nehostí, nezobrazí se v protokolu žádné údaje API.

Chcete-li povolit sledování RSVP na hostitelském počítači, přidejte do následujícího podklíče registru údaj EnableTracing:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RSVP \Parameters
```

Tento údaj musí být datového typu REG_WORD. Jeho hodnotu nastavte na 0x1.

Změny se projeví až po restartu služby RSVP. Restartujte tedy tuto službu prostřednictvím konzoly Správa počítače.

Upozornění: K přímé editaci registru se uchylujte skutečně až tehdy, nezbyvá-li žádná jiná možnost jeho úpravy. Editory registru obcházejí standardní bezpečnostní opatření, poskytovaná správnými nástroji. Tato bezpečnostní opatření zajišťují prevenci proti zadávání konfliktních nastavení nebo nastavení, která by mohla snížit výkon systému nebo dokonce systém poškodit. Přímá editace registru může mít vážné a nepředpokladané následky, jež mohou ve svém důsledku zabránit spuštění systému. Takové poškození lze řešit jedině opětovnou instalací systému Windows 2000. Chcete-li konfigurovat nebo přizpůsobit nastavení systému Windows 2000, používejte k tomu účelu program Microsoft Management Console (MMC) nebo jiné nástroje Ovládacích panelů.

Po přidání nové hodnoty do registru musíte restartovat službu RSVP. Restartujte tedy tuto službu prostřednictvím konzoly Správa počítače.

Zprostředkovatel služby QoS začne generovat soubor protokolu Rsvptrace ve složce %windir%\system32\logfiles.

Soubory protokolu jsou pojmenovány RsvpTraceXX.txt, kde „XX“ jsou zástupné znaky pro čísla od 00 do 09. Všechny soubory protokolu mají omezenou velikost. Dosáhne-li velikost souboru maximální povolené hodnoty, bude vytvořen nový soubor s vyšší hodnotou v části „XX“. Jakmile je v sekvenci souborů protokolu použito poslední dvojčíslí, bude první soubor protokolu vymazán. Uživatel by měl sám kontrolovat seznam těchto souborů, stejně jako data jejich vytvoření. Zjistí tak, které soubory budou v nejbližší době vymazány.

Uživatel si může záznamy v těchto souborech prohlížet v reálném čase, zadáním následujícího příkazu:

```
tail -f RsvpTraceXX.TXT
```

„XX“ jsou zástupné znaky pro čísla od 00 do 09.

Následující ukázka je vzorkem protokolu Rsvptrace odesílatele:

```
1999/04/20 17:53:42:0679; From API; PATH
;172.31.8.159,5003,17;0.0.0.0,0x00000000;30000;172.31.3.21,3128;1.028E+0
1999/04/20 17:53:42:0679; 172.31.8.159 <= 172.31.3.21; PATH
;172.31.8.159,5003,17;172.31.3.21,0x00000000;1500;172
1999/04/20 17:53:44:0679; 172.31.8.159 <= 172.31.3.21; PATH
;172.31.8.159,5003,17;172.31.3.21,0x00000000;3000;172
1999/04/20 17:53:46:0773; 172.31.8.159 <= 172.31.3.21; PATH
;172.31.8.159,5003,17;172.31.3.21,0x00000000;6000;172
1999/04/20 17:53:54:0617; 172.31.8.159 <= 172.31.3.21; PATH
;172.31.8.159,5003,17;172.31.3.21,0x00000000;12000;17
1999/04/20 17:54:07:0664; 172.31.8.159 <= 172.31.3.21; PATH
;172.31.8.159,5003,17;172.31.3.21,0x00000000;24000;17
1999/04/20 17:54:12:0601; 172.31.3.1 => 172.31.3.21; RESV
;172.31.8.159,5003,17;172.31.3.1,0x00000000;30000;No Re
1999/04/20 17:54:12:0679; From API; PATH
;172.31.8.159,5003,17;0.0.0.0,0x00000000;30000;172.31.3.21,3128;1.028E+0
```

1. První údaj ukazuje, že v 17:53:42:0679 zavolala odesílající aplikace funkci QoS API, která odeslala zprávu PATH.
2. Následující údaj ukazuje zprávu PATH, přenášenou sítí. Doposud neexistují žádné záruky, že zpráva byla do sítě skutečně odeslána, ale v tomto místě můžeme říci, že zprostředkovatel služby QoS předal zprávu do zásobníku TCP/IP, odkud bude předána do sítě.
3. Do sítě je odeslána další zpráva PATH. Zprávy jsou obnovovány ve 30sekundových intervalech.
4. V 17:54:12:0601 přichází zpráva RESV pro danou relaci. Tato zpráva dokončuje proces rezervace. Znamená to, že zpráva PATH dorazila k cílovému uzlu (příjemce) a příjemce odpověděl zprávou RESV.
5. V 17:54:12:0679 je zaprotokolována další zpráva API PATH. Znamená to, že server proxy této aplikace (na počítači zprostředkovatele služby QoS) obnovuje stav RSVP jménem této aplikace.

Adresy IP v zaprotokolovaných údajích zprávy PATH ukazují, že relace RSVP má adresu 172.31.8.159 a odesílatel 172.31.3.21. V případě jednosměrného přenosu je adresa relace ekvivalentem adresy příjemce, kdežto v případě vícesměrného přenosu je tato adresa ekvivalentem adresy vícesměrné relace.

Adresy IP v údajích zprávy RESV ukazují, že tato zpráva byla vyslána odesílateli na adresu IP 172.31.3.21. Ukazuje se však také, že zpráva přichází z adresy předchozího směrování – 172.31.3.1 – což je adresa IP směrovače, který odeslal zprávu odesílateli.

NetMon

Sledování sítě (NetMon) dohlíží na síťové přenosy. Novější verze tohoto nástroje (verze 2 a vyšší) obsahují funkce analyzátoru RSVP. Pomocí tohoto programu Sledování sítě můžete monitorovat značky 802.1p.

Sledování sítě můžete spouštět na hostitelském počítači odesílatele, na hostitelském počítači příjemce, na serverech QoS ACS nebo na mezilehlých bodech směrování. Tento

program však musíte nejprve nainstalovat. Více informací o instalaci nástroje NetMon najdete v nápovědě online pro systém Windows 2000 Server.

Spouštění nástroje NetMon na hostitelských počítačích

Program NetMon by se měl zpravidla spouštět pouze na počítači, jenž je určen jako monitorovací počítač sítě. Nikoli tedy na koncových uzlech nebo serverech QoS ACS (všech hostitelích, jež generují zprávy RSVP). Je také velmi důležité, aby daný počítač nebyl k síti připojen pomocí vyhrazeného portu na učitím můstku typu přepínač (většina moderních skříňových přepínačů). V opačném případě by mohl přepínač bránit monitorovacímu počítači ve sledování přenosů, které nejsou určeny přímo jemu. Menší levnější rozbočovače se zpravidla nechovají jako učití můstky a propouštějí přenosy mezi všemi porty. Používejte tento typ rozbočovače k připojení monitorovacího počítače ke stejnému přepínacímu portu jako následující nebo předchozí bod směrování.

Doporučuje se instalovat program NetMon jak na počítač odesílatele, tak na počítač příjemce.

Filtry pro zachycování a zobrazení

Nastavte filtr pro zachycování pro všechny příchozí i odchozí zprávy příslušného koncového uzlu. Zachycování vyžaduje, aby byla tato služba spuštěna na všech uzlech ještě před spuštěním odesílající aplikace. Zprávy RSVP jsou zpravidla obnovovány každých 30 sekund. Tuto hodnotu byste měli vzít v úvahu při rozhodování o době, po kterou budete pakety zachycovat.

Jakmile je proces zachycování ukončen, použijte filtr zobrazení, aby se na obrazovce zobrazily pouze zprávy RSVP pocházející ze zachycených dat. Sledování zpráv RSVP by mělo označit zprávy PATH vyslané odesílatelem, které o něco později dorazí k příjemci. Příjemce odpoví zprávou RESV, která dorazí k odesílateli první zprávy. V případě, že sledování toto chování nepotvrdí, byly pravděpodobně zprávy (jedna nebo obě) během přenosu odhozeny nebo nebyly vygenerovány koncovým uzlem. Po celou dobu relace příslušné aplikace se ve sledovaném rozsahu nezobrazí ani jedna zpráva PATH-TEAR nebo RESV-TEAR. Tyto zprávy by mohly naznačovat, že jedna z partnerských aplikací byla ukončena nebo že uzel sítě s podporou protokolu RSVP žádost zamítl.

Sledování značek 802.1p

Abyste mohli značky 802.1p sledovat, zkopírujte soubor Parser.dll ze složky nástrojů Microsoft® Windows® 2000 Resource Kit Tools Help do kořenové složky instalace programu Sledování sítě (NetMon). Potom ze stejné složky zkopírujte do složky Parsers, vnořeně do instalační složky programu Sledování sítě, také soubor Mac.dll. Po zkopírování těchto souborů restartujte program Sledování sítě.

Program Sledování sítě zobrazuje značky 802.1p pouze tehdy, je-li spuštěn na hostitelském počítači, který nemá instalovány ovladače standardu 802.1p (nebo na počítači, na kterém je funkce 802.1p zakázána). Ovladače standardu 802.1p odstraňují značky 802.1p ještě dříve, než předají paket programu Sledování sítě.

Rsping

Program Rsping určuje, zda specifická síťová cesta neblokuje signalizační zprávy RSVP. Máte-li podezření, že některé zprávy RSVP nedospívají ke svým cílům, můžete pomocí tohoto nástroje rozpoznat, zda je vinna síť. Na rozdíl od programu Rsvptrace, jenž umožňuje uživateli sledovat příchozí a odchozí zprávy RSVP na určitém uzlu, program

Rsping umožňuje uživateli generovat specifický styl zpráv RSVP přenášených na partnerský uzel.

Po spuštění nástroje Rsping jsou generovány jak zprávy PATH, tak zprávy RESV. Můžete kromě toho určit:

- To, zda jsou tyto zprávy jednosměrové nebo vícesměrové,
- typ služby Intserv,
- rychlost datového toku.

Vícesměrové zprávy RESV, generované pomocí nástroje Rsping, používají styl filtru se zástupnými znaky (WF), zatímco jednosměrné zprávy používají styl filtru se znaky pevnými (FF). Maximální požadovaná rychlost je vždy dvakrát větší než určená rychlost datového toku.

Spusťte nástroj Rsping pomocí parametrů, které nejvíce napodobují zprávy RSVP, generované skutečnými aplikacemi. Tyto zprávy lze pak prohlížet v souboru protokolu Rsvptrace na hostitelském počítači odesílatele.

Tcmon

Nástroj Tcmon je monitorovacím programem řízení provozu. Můžete jej používat k následujícím úkonům:

- Ověřování tvorby vysílání datových proudů jádrem,
- identifikace charakteristiky a statistiky přidružené k danému rozhraní (například zda je či není povolen standard 802.1p),
- identifikace charakteristiky a statistiky přidružené ke každému proudu (například typu služby, skutečné označování, přenos bajtů uvnitř proudu atd.)

Videokonference programu Microsoft® NetMeeting® vytváří například jeden proud pro zvukové přenosy a druhý proud pro obrazová data. Oba tyto proudy by měly být zachyceny pomocí programu Tcmon (spusťte Tcmon pro požadované přenosové rozhraní a nastavte jej do režimu automatického obnovování (Auto Refresh). Tcmon indikuje kromě toho ještě třetí proud pro typ služby řízení přístupu (Network Control). Tento proud je určen pro přenosy signálních zpráv RSVP a je aktivní po celou dobu činnosti služby RSVP.

Na počátku Tcmon oznámí, že byly pro aplikací vytvořeny dva proudy a že jsou typu best-effort. Tento typ služby zůstane aktivní, dokud síť nepotvrdí požadavek RSVP odesílatele. V tom okamžiku bude spuštěno řízení přenosů a změní se typ služby na řízené zatížení nebo zaručený přenos. Nestane-li se tak, znamená to, že buď síť nepotvrdila požadavek QoS, nebo vznikl problém při řízení přenosu, respektive u zprostředkovatele služby QoS.

Instalaci aplikace Tcmon spustíte souborem Setup.exe z instalační složky Tcmon na disku Resource Kit Tool Help.

Samotný program pak spustíte z příkazového řádku zadáním následujícího příkazu:

```
tcmom
```

Na obrazovce se zobrazí dialogové okno Tcmon. Vyberte si požadované rozhraní, v němž chcete řízení přenosů sledovat. Budete-li hledat změny v parametrech proudu (například změny typu služby), doporučuje se aktivovat režim automatického obnovování (v nabídce Obnovit).

Sledování systému

Program Sledování systému (Sysmon) monitoruje součásti služby řízení přenosů, služby RSVP a služby QoS ACS. Je to standardní součást systému Windows 2000. Více informací o spuštění programu Sledování systému najdete v nápovědě pro systém Windows 2000 Server.

Po spuštění Sledování systému můžete v dialogovém okně Přidat čítač:

- Vybrat položku Kanál plánovače paketů, což vám umožní sledovat parametry řízení přenosů jako počet instalovaných proudů nebo počet paketů ve frontách různých součástí Plánovače paketů QoS.
- Vybrat položku Služba QoS ACS/RSVP, což umožní sledovat takové parametry jako volání API nebo zprávy RSVP.

Qtcp

Program Qtcp měří integritu koncových síťových uzlů a kvalitu služby pro ověření QoS. Qtcp odesílá sekvenci testovacích paketů a podává hlášení o zpoždění všech paketů. Pakety, které nedorazí do místa určení, jsou považovány za ztracené.

Qtcp poskytuje následující funkce:

1. Podává hlášení o změnách zpoždění v mikrosekundách,
2. volá standardně síťovou službu QoS a je užitečný při hodnocení užitečnosti mechanismu QoS,
3. může napodobovat proudy dat pro uživatelem definované velikosti paketů,
4. může napodobovat proudy dat, vytvarované podle nastavených parametrů bloku řídících zpráv,
5. může být používán v izolovaných, řízených sítích nebo ve výrobní síti,
6. generuje podrobné protokoly o zjištěných výsledcích.

Relace programu Qtcp je spuštěna jak na odesílajícím, tak na přijímacím počítači. Qtcp používá obecné rozhraní QoS API k volání služby QoS z místního modulu řízení přenosů nebo ze sítě. Odesílatel Qtcp odešle zprávy RSVP PATH směrem k příjemci a čeká na odpověď. Příjemce Qtcp čeká na zprávu RSVP PATH od odesílatele a odpovídá zprávou RSVP RESV.

Přijetí zprávy RESV na počítači odesílatele inicializuje fázi měření. V této fázi vystaví odesílatel mezipaměť působení přenosů jádrem. Jádro bude čekat na přenos definovaný pomocí parametrů bloku řídících zpráv a typu služby, nastaveného uživatelem. Při přenosu paketů je v každém paketu zaznamenáno číslo sekvence a aktuální místní čas (s přesností na 100 nanosekund).

Po přijetí paketů příjemcem je na cílovém počítači k paketům připojen záznam o místním čase a řízení provozu předá pakety partnerskému příjemci Qtcp. Příjemce Qtcp zpracovává seznam všech přijatých paketů včetně paketu s číslem sekvence, dobou odeslání a době přijetí.

Odesílací část testu je ukončena, jakmile vysílač odesílatel odešle požadovaný počet paketů (lze přepsat výchozí hodnotu 2 048 paketů). Odesílatel odešle za posledním paketem ukončovací sekvenci 10 paketů. Text bude na straně příjemce ukončen po přijetí ukončovacího paketu nebo po přijetí požadovaného počtu paketů. Na zvláště přetížených linkách se může stát, že příjemce nikdy požadovaný počet paketů neobdrží, neboť ukončovací pakety se cestou ztratí. V tomto případě lze test na straně příjemce ukončit ručně, zadáním následujícího příkazu:

q

V okamžiku ukončení příjemce analyzuje a zpracuje protokol přijatých paketů. Náš program vygeneruje tři soubory protokolů:

- *<Název_souboru>.sta* obsahuje celkovou statistiku. Podává zprávu o celkovém počtu přijatých paketů a určuje číslo sekvence každého ztraceného paketu.
- *<Název_souboru>.raw* obsahuje podrobný protokol, zobrazující normalizovaný čas odeslání a přijetí každého paketu, zpoždění (rozdíl mezi časem odeslání a časem přijetí), velikost paketu a číslo sekvence.
- *<Název_souboru>.log* je výsledkem normalizace výsledků uložených v druhém souboru, kdy se započítávají všechny nesrovnalosti hodin mezi oběma hostitelskými počítači. Zpravidla jsou tyto hodnoty zanedbatelné, ale v neúměrně zatížené a vysokorychlostní síti LAN mohou značně narůst.

Program Qtcp spustíte na počítači odesílatele následujícím příkazem:

```
qtcp -l 64 -t <Adresa IP>
```

Parametr 64 je velikost mezipaměti v bajtech, zatímco <Adresa IP> je adresou IP příjemce. Na obrazovce se zobrazí následující hlášení:

Initiated QoS connection. Waiting for receiver.

Na počítači příjemce spustíte program Qtcp následovně:

```
qtcp -f <názevsouboru> -r
```

Na obrazovce se zobrazí následující zpráva:

Waiting for QoS sender to initiate QoS connection.

Příjemce a odesílatel čekají na požadovanou výměnu zpráv RSVP, která se musí uskutečnit před skutečným spuštěním datového přenosu. Standardně jsou datové proudy vysílané jádrem rychlostí 100 kB/s (kilobajtů za sekundu).

Qtcp zobrazuje na konzolách uzlu řadu teček. Každá tečka odpovídá 100 odeslaným nebo přijatým paketům. Na straně příjemce je první vytištěna jedna tečka a teprve pak se začnou zobrazovat tečky, znázorňující prvních 100 paketů. Tečky označují, že Qtcp funguje.

Po odeslání určeného počtu paketů ukončí odesílatel operaci pomocí zprávy, a to bez ohledu na rychlost přenosu. Potom, po přijetí vyžadovaného počtu paketů (nebo ukončovacích paketů), ukončí činnost také příjemce a vyšle následující zprávu:

Received 2048 buffers.

Za touto zprávou následují statistické údaje. Přesto však tato statistika nemusí být přesná. Přesné statistické údaje této relace si ale můžete prohlédnout v souborech protokolu *název_souboru.sta*, *název_souboru.raw* a *název_souboru.log*.

Chcete-li generovat zprávy, stiskněte po ukončení relace klávesu Enter na konzole příjemce.

Readpol

Readpol zobrazuje zásady QoS ACS, uložené v rámci konkrétní domény. Tento nástroj poskytuje metody pro identifikaci zásad, které platí pouze pro individuálního uživatele, aniž by tento uživatel měl oprávnění správce nebo používal konzolu QoS ACS. Je

užitečný při sledování šíření zpráv PATH a RESV v všech případech, v nichž podezříváte službu QoS ACS z blokování zpráv vinou příliš restriktivního nastavení zásad.

Rsvpsm

Rsvpsm je interaktivní nástroj, jenž umožňuje uživateli odesílat dotazy na status relace RSVP na vzdáleném počítači. Informace, poskytovaná uživateli pomocí nástroje Rsvpsm, zahrnuje všechny bloky stavu PATH, bloky stavu RESV a bloky stavu služby Traffic Control. Všechny bloky jsou udržovány vzdáleným hostitelským počítačem.

Tento nástroj lze s úspěchem používat k vysledování problémů RSVP obepínajících více hostitelských počítačů.

Qossp.aid, Rapilib.aid

Knihovny Qossp.aid a Rapilib.aid budou generovat diagnostický výstup na základě informací zprostředkovatele služby QoS. Tyto nástroje jsou užitečné zejména při sledování problémů, vzniklých používáním rozhraní QoS API, nebo potíží, které způsobil samotný zprostředkovatel služby QoS.

Chcete-li povolit protokolování RSVP SP, vložte údaj **EnableDebugAid** datového typu REG_DWORD do následujícího podklíče systémové registrační databáze:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RSVP\Parameters

Má-li se ladění zprostředkovatele služby QoS vztahovat na použití rozhraní API, nastavte nejnižší platný bit na hodnotu 1 (bit 0).

Pokud chcete zobrazit diagnostický výstup bez ohledu na funkčnost zprostředkovatele služby QoS, nastavte 2. nejnižší platný bit na hodnotu 1 (bit 1).

K restartování služby RSVP použijte konzolu Správa počítače. Pouze tak můžete protokolování zprostředkovatele služby QoS aktivovat.

Soubory protokolu zprostředkovatele služby QoS jsou uloženy ve složce %windir%\system32\logfiles. Tyto soubory jsou generovány pro každou aplikaci zvlášť. Soubory QoSsp.aid <XXXX> jsou generovány v okamžiku, kdy je hodnota v registru rovna 1 (bit 0). Soubory protokolu nazvané rapilib.aid <XXXX> jsou generovány, když je bit 1 nastaven na hodnotu 1. V takovém případě zastupuje hodnota <XXXX> číslo ID aplikace.

Ttcp

Ttcp je nástroj pro generování šumů. Účinky služby QoS se násobí, je-li v síti nedostatek prostředků (některá část sítě je přetížená). Při testování rozmístění služby QoS je vhodné uměle přetížit síť (plánovitě) generováním násobných souběžných konverzací a přenosů paketů, jež napodobují model fungování sítě.

Ttcp generuje mezi dvěma hostitelskými počítači samostatné relace UDP nebo TCP. Při této operaci lze nastavit a řídit velikost mezipaměti, počet vyrovnávacích pamětí, použité porty a celou řadu dalších různých parametrů. Není však možné kontrolovat rychlost jednotlivých přenosů (jinak než vytvořit určitý proud pomocí Plánovače paketů QoS nebo programu Tcmon, který později použijete pro přenosy Ttcp). V každé instanci aplikace Ttcp je vytvořena samostatná konverzace. Větší počet konverzací lze vytvořit vytvořením většího počtu instancí programu Ttcp.

Chcete-li přimět program Ttcp, aby využíval síť agresivněji, spusťte jej s parametry **-a** a **-c**.

Tracert

Tento nástroj určuje trasu k cíli tím, že odešle pakety Echo protokolu ICMP (Internet Control Message Protocol) s různými hodnotami TTL (životnost). Na každém směrovači po trase datového toku se požaduje, aby snížil tuto hodnotu minimálně o 1 a teprve pak odeslal dál. Když spadne životnost paketu na nulu, odešle směrovač zpět do zdrojového systému zprávu ICMP Time Exceeded (překročený limit). Program Tracert můžete používat následovně:

```
tracert [-d] [-h <max_směrování>] [-j <seznam_počítačů>] [-w <časový_limit>]  
<název_cíle> <adresa IP příjemce>
```

Parametry příkazu Tracert

-d

Určuje, že adresy IP nebudou překládány na názvy počítačů.

-h <max_směrování>

Určuje maximální počet bodů směrování na cestě k předpokládanému cíli.

-j <seznam_počítačů>

Určuje nespojitou trasu podél <seznam_počítačů>.

-w <časový_limit>

Čeká na odpověď určitý časový interval určený v milisekundách.

<název_cíle>

Název cílového počítače.

<adresa IP příjemce>

způsobí, že odesílající hostitelský počítač vytiskne adresy IP pro každé rozhraní všech směrovačů, které existují podél trasy od odesílatele po příjemce. Tento seznam může být užitečný při určování uzlů, na nichž se mohou zprávy RSVP (či data) ztrácet anebo být blokovány.

Další zdroje

Informace týkající se zdrojů RFC pro QoS, konceptů sítě Internet či dalších odkazů, vztahujících se ke službě QoS, najdete pod odkazem International Engineering Task Force (IETF) na stránce WWW „Web Resources“, kterou najdete na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Následující koncepty sítě Internet pojednávají o službě QoS:

- *Providing Integrated Services Over Low-Bit-Rate Links*
- *SBM (Subnet Bandwidth Manager): A Proposal for Admission Control Over IEEE 802-Style Networks*
- *A Framework for Providing Integrated Services Over Shared and Switched IEEE 802 LAN Technologies*
- *Integrated Services over IEEE 802.1D/802.1p Networks*
- *Integrated Service Mappings on IEEE 802 Networks*
- *RSVP Cryptographic Authentication*
- *RSVP Extensions for Policy Control*

- *Partial Service Deployment in the Integrated Services Architecture*

Další informace o QoS najdete v následujících specifikacích:

- RFC 2205: *Resource Reservation Protocol (RSVP) Version 1 Functional Specification*
- RFC 2207: *RSVP Extensions for IPSEC Data Flows*
- RFC 2208: *Resource Reservation Protocol (RSVP) Version 1: Applicability Statement: Some Guidelines on Deployment*
- RFC 2209: *Resource Reservation Protocol (RSVP) Version 1: Message Processing Rules*
- RFC 2210: *The Use of RSVP with IETF Integrated Services*
- RFC 2211: *Specification of the Controlled-Load Network Element Service*
- RFC 2212: *Specification of Guaranteed Quality of Service*

KAPITOLA 10

Simple Network Management Protocol



Aby bylo možné odpovědět na výzvy k návrhům efektivních platforem pro správu různorodých sítí, založených na protokolu TCP/IP (Transmission Control Protocol/Internet Protocol), byl v roce 1988 definován protokol SNMP (Simple Network Management Protocol), jenž byl v roce 1990 schválen Výborem pro aktivity v síti Internet (IAB) jako standard pro síť Internet. Služba SNMP umožňuje sledovat a oznamovat stav informací mezi různými hostitelskými počítači. Tato kapitola obsahuje podkladové a konceptuální materiály pro správce, nezbytné k porozumění službě SNMP a její implementaci v kontextu systému Microsoft® Windows® 2000.

Obsah této kapitoly

Co je to SNMP? 588

Celkový pohled na SNMP 590

Vlastnosti služby Agent SNMP systému Windows 2000 593

Zabezpečení 594

Architektura protokolu SNMP v systému Windows 2000 597

Specifické otázky při implementaci protokolu SNMP 599

Nastavení položek registru 601

Odstraňování problémů s protokolem SNMP 602

Související informace v Soupravě prostředků (Resource Kit)

Více informací o zabezpečení zpráv SNMP najdete v kapitole „Možnosti konfigurace zabezpečení protokolu SNMP“

Více informací o typech objektů Microsoft Information Base najdete v kapitole „Typy objektů databáze MIB“.

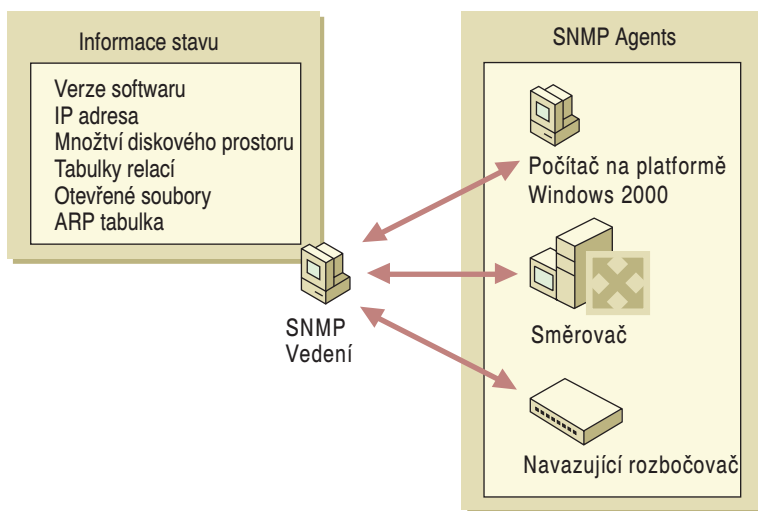
Další informace o instalaci a konfiguraci služby Microsoft SNMP najdete v nápovědě online pro systém Windows 2000 Server.

Co je to SNMP?

SNMP je standard pro správu sítě, obecně používaný v sítích TCP/IP a v poslední době také v sítích IPX (Internetwork Packet Exchange). Standard SNMP zahrnuje následující součásti standardu RFC (Request for Comment):

- Informace o správě II (MIB II), RFC 1213. Je to kolekce ovladatelných objektů, reprezentujících různé typy informací o konfiguraci sítě (seznam síťových rozhraní, směrovací tabulka, tabulka ARP, seznam otevřených připojení TCP nebo statistika ICMP).
- Struktury informací o správě (SMI), RFC 1902. Jedná se o samostatnou specifikaci RFC sítě Internet, která popisuje syntaxi objektů při určování způsobu odkazování na data MIB a jejich ukládání.
- Protokol SNMP (Simple Network Management Protocol), RFC 1157. Standard definující, jak dochází ke komunikaci mezi zařízeními standardu SNMP a jaké typy zpráv mohou být těmito spojeními přenášeny.

SNMP poskytuje snadnou metodu správy síťových uzlů (serverů, pracovních stanic, směrovačů, můstků a rozbočovačů) z centrálně umístěného hostitelského počítače. SNMP vykonává svoje administrátorské služby pomocí distribuované architektury správních systémů a agentů. Jak je patrné také z obrázku 10.1, je centrální hostitelský počítač se spuštěným softwarem pro správu sítě označen jako systém správy SNMP nebo Správce SNMP. Řízené uzly sítě jsou označeny jako Agenti SNMP.



Obrázek 10.1: Distribuovaná architektura SNMP.

Správa sítě je klíčová zejména z pohledu správy prostředků a revizí. Službu SNMP lze využívat několika způsoby:

Konfigurace vzdálených zařízení Lze konfigurovat informace, které je možné posílat ze systému správy na každý hostitelský počítač v síti.

Sledování výkonu sítě Můžete sledovat rychlost zpracování a propustnost sítě a navíc shromažďovat údaje o úspěšnosti datových přenosů.

Detekce chyb v síti nebo neoprávněného přístupu Na síťových zařízeních lze konfigurovat spouštěcí procedury upozornění. Tyto procedury po výskytu určitých událostí automaticky vygenerují příslušná hlášení a odešlou je do systému správy sítě. Mezi běžné typy události, pro něž lze konfigurovat aktivační procedura, patří:

- Vypnutí nebo restartování zařízení,
- rozpoznání chyby připojení na směrovači,
- nevhodný přístup.

Používání revize sítě Sledujte celkové využití sítě. Díky tomu můžete identifikovat přístupy uživatele nebo skupiny uživatelů a určovat typ využití síťových zařízení nebo služeb. Tato informace bude užitečná při generování přímého individuálního nebo skupinového účtování a při obhajobě aktuálních nákladů na síť, respektive plánovaných výdajů.

Implementace SNMP v systému Windows 2000 je 32bitovou službou, která podporuje všechny počítače s instalovanými protokoly TCP/IP a IPX. V systému Microsoft® Windows® 2000 Professional je to nepovinná součást a lze ji nainstalovat po úspěšném dokončení konfigurace protokolů TCP/IP a IPX. Systém Windows 2000 implementuje službu SNMP ve verzi 1 a 2C. Tyto verze jsou postaveny na průmyslových standardech, jež definují jednak strukturu a ukládání informací o systému správy sítě, ale i způsoby komunikace mezi agenty a systémy správy sítí postavených na standardu TCP/IP.

Služba SNMP v systému Windows 2000 poskytuje agenty, kteří umožňují centralizovanou vzdálenou správu všech počítačů s následujícím softwarem:

- Microsoft® Windows® 2000 Server,
- Microsoft® Windows® 2000 Professional,
- službou WINS (Windows Internet Name Service) založenou na systémech Windows 2000 a Microsoft® Windows® NT,
- službou DHCP (Dynamic Host Configuration Protocol) založenou na systémech Windows 2000 a Microsoft® Windows® NT,
- službou IIS (Microsoft® Internet Information Service) založenou na systémech Windows 2000 a Microsoft® Windows® NT,
- službou Microsoft® LAN Manager,
- službou řízení přístupu k QoS v systému Windows 2000,
- službou Směrování a vzdálený přístup v systému Windows 2000,
- službou Windows 2000 Internet Authentication Service.

Abyste mohli využívat informace poskytované službou SNMP v systému Windows 2000, musíte mít v síti centrálně umístěn alespoň jeden hostitelský počítač se spuštěným softwarem správy sítě SNMP. Služba SNMP v systému Windows 2000 poskytuje pouze Agentu SNMP; nezahrnuje však software správy sítě SNMP. Chcete-li, aby se hostitelský počítač choval jako systém správy sítě, musíte použít některou z aplikací správy sítě SNMP od jiného dodavatele. Můžete také pomoci dvou rozhraní pro vytváření

aplikací (API), zabudovaných do systému Windows 2000, vytvořit vlastní aplikaci tohoto typu. Zmíněnými rozhraními jsou:

- Rozhraní WinSNMP API (WinSNMP.dll), jež poskytuje kolekci funkcí pro šifrování, dešifrování, odesílání a příjem zpráv SNMP.
- Rozhraní Management API (Mgmtapi.dll), které poskytuje kolekci základních funkcí pro rychlou a snadnou tvorbu systémů správy SNMP.

Nástroj SNMPUtil.exe, jež je umístěn na instalačním disku systému Microsoft® Windows® 2000, je jakousi ukázkou či příkladem aplikačního softwaru, vytvořeného pomocí funkcí rozhraní Management API. Více informací o rozhraní Management API najdete v oddílu „Architektura protokolu SNMP v systému Windows 2000“ později v této kapitole. Služba SNMP v systému Windows 2000 podporuje také programy pro správu sítě od jiných dodavatelů.

Celkový pohled na SNMP

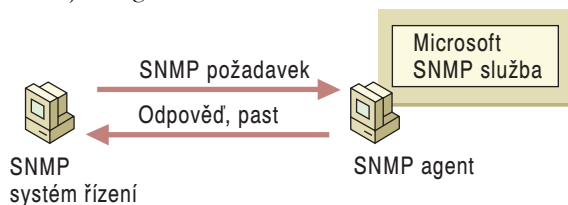
Služba SNMP využívá distribuovanou architekturu agentů a systémů pro správu sítě. V následujících oddílech se budeme zabývat úlohou jednotlivých součástí včetně objektů a zprávy, používaných k ukládání a vyhledávání informací o správě sítě.

Správa a agenti

Využívání služby SNMP vyžaduje přítomnost dvou součástí (viz obrázek 10.2).

- Systém správy SNMP,
- Agent SNMP.

Aplikační software pro správu služby SNMP nemusí být nutně spuštěn na stejném počítači jako agenti SNMP.



Obrázek 10.2: Systém správy a agent SNMP.

Systém správy SNMP, označovaný také jako Správní konzola SNMP může na řízených počítačích (agenti SNMP) požadovat následující informace:

- Identifikaci a statistiku síťového protokolu,
- dynamickou identifikaci zařízení připojených k síti (proces označovaný jako vyhledávání),
- konfigurační data softwaru a hardwaru,
- statistiku používání a výkonu zařízení,
- zprávy o chybách a událostech zařízení,
- statistiku o užívání programů a aplikací.

Správní systém může také odesílat požadavky na konfiguraci agenta, v němž může specifikovat změny místních parametrů. Stává se to však pouze ojediněle, neboť většina klientských parametrů je určena jen pro čtení.

Na doprovodném CD Windows 2000 Resource Kit je umístěno několik nástrojů pro správu SNMP. Více informací o nástrojích pro správu systému najdete v oddílu „Architektura protokolu SNMP v systému Windows 2000“ později v kapitole.

Agenti SNMP zásobují systémy správy SNMP informacemi o všech aktivitách, k nimž v síťové vrstvě protokolu IP (Internet Protocol) dochází, a odpovídají na žádosti o informace, vysílané správním systémem. Všechny počítače se softwarem agenta SNMP, jako je Windows 2000 SNMP Service, jsou agenti SNMP. Službu agenta SNMP lze konfigurovat a tím také podrobně určit, jaké statistiky budou sledovány a jaké systémy správy jsou oprávněny tyto informace vyžadovat.

Agenti zpravidla nejsou původci zpráv – pouze na příchozí zprávy odpovídají. Výjimkou je však výstražná zpráva, spuštěná jako reakce na určitou událost. Výstražná zpráva je označována také jako depeše. Zachycovač je událost, která na počítači agenta aktivuje událost varování. Touto událostí může být restart počítače nebo nepovolený přístup. Zachycovače a depeše utvářejí základní podobu zabezpečení, neboť oznamují správnímu systému výskyt každé sledované události.

Více informací o požadavcích SNMP a depeších najdete v oddílu „Zprávy SNMP“ později v této kapitole.

Management Information Base

Management Information Base (MIB) je kontejner objektů, z nichž každý reprezentuje jiný typ informace. Tato kolekce objektů obsahuje informace vyžadované systémem správy. Uvedme si příklad. Jeden objekt MIB reprezentuje počet aktivních relací na počítači agenta, zatímco druhý objekt volné místo na disku tohoto počítače. Všechny informace, které by systém správy mohl na agentu požadovat, jsou uloženy v objektech MIB.

MIB definuje pro své objekty následující hodnoty:

- Název a identifikátor,
- definovaný datový typ,
- textový popis objektu,
- metoda indexování, používaná pro objekty s komplexními datovými typy (zpravidla popisovanými jako vícerozměrná pole nebo tabulková data).

Mezi příklady komplexních dat lze zařadit seznam všech síťových rozhraní konfigurovaných v systému, směrovací tabulku nebo tabulku protokolu převodu adres (ARP).

- Oprávnění ke čtení/zápisu.

Každý objekt v databázi MIB má svůj jedinečný identifikátor, jenž obsahuje následující informace:

- Typ (čítač, řetězec, míra nebo adresa),
- úroveň přístupu (čtení nebo čtení/zápis),
- omezení velikosti,
- informace o rozsahu.

Služba SNMP v systému Windows 2000 podporuje databáze Internet MIB II, LAN Manager MIB II, Host Resources MIB a značkovou MIB společnosti Microsoft.

Více informací o databázích MIB standardu Windows 2000 a o popisu objektů těchto databází najdete v kapitole „Typy objektů databáze MIB“.

Zprávy SNMP

Jak agenti, tak systémy správy používají zprávy SNMP ke zkoumání a předávání informací o spravovaných objektech. Zprávy SNMP jsou posílány prostřednictvím protokolu UDP (User Datagram Protocol). Protokol IP je zde používán ke směrování zpráv mezi systémem správy a hostitelským počítačem.

Požadavky na síťová zařízení, vysílané programy pro správu sítě SNMP, jsou na těchto zařízeních přijímány programy agentů SNMP. Potom je požadovaná informace vyhledána v databázích MIB. Po jejím nalezení je vyžádaná informace odeslána zpět programu správy SNMP. Agent SNMP odesílá informace:

- Když odpovídá na žádost správy o zpřístupnění informace,
- když zachytí sledovanou událost.

K zajištění této funkce používají programy správy a agentů následující zprávy:

- GET

Základní zpráva požadavku SNMP. Odeslaná systémem správy žádá o zpřístupnění informace o jednom údaji MIB na počítači agenta – například informace o volném místě na disku.

- GET-NEXT

Rozšířený typ zprávy požadavku, který lze používat k procházení celé hierarchie objektů správy. V okamžiku, kdy agent zpracovává požadavek GET-NEXT pro příslušný objekt, vrací identitu a hodnotu objektu, který logicky následuje po předchozí odeslané informaci. Požadavek GET-NEXT je užitečný zejména při práci s dynamickými tabulkami jako například s vnitřní směrovací tabulkou IP.

- SET

Tuto zprávu můžete používat k odesílání a přiřazování aktualizované hodnoty MIB, povoluje-li agent přístup i pro zápis.

- GET-BULK

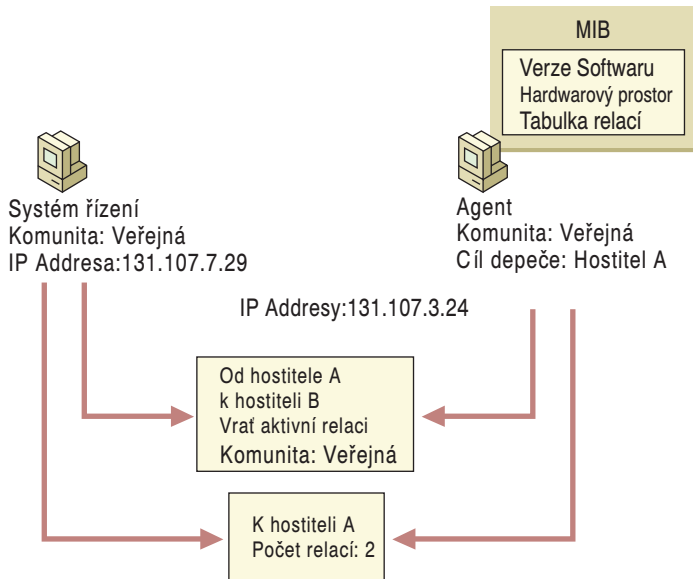
Požadavek, aby rozsah dat agenta v rámci nastavených omezení velikosti zpráv byl co největší. Tento způsob předávání zpráv minimalizuje počet výměn protokolu, nezbytných při přijímání velkého množství správních informací.

- NOTIFY

Označovaná také jako depeše. Je to nevyžádaná zpráva, odesílána agentem správním systému v okamžiku rozpoznání určitého typu události. Depeše může být odeslána v okamžiku restartu počítače. Systém správy, který tuto zprávu obdrží, je označován jako cíl depeše.

Služba standardně používá ke sledování zpráv SNMP port UDP č. 161, zatímco port 162 se používá ke sledování depeší SNMP. Nastavení těchto portů však můžete upravit změnou konfigurace místního souboru Services. Více informací o vykonávání úprav najdete v oddílu „Změna nastavení portů SNMP“ později v této kapitole.

Příklad na obrázku 10.3 znázorňuje způsob předávání informací mezi systémem správy a agenty.



Obrázek 10.3: Předávání informací mezi systémem správy a agenty.

Komunikace mezi oběma počítači probíhá takto:

1. Systém správy vytvoří zprávu SNMP, obsahující požadavek zpřístupnění informace (GET), název komunity, k níž systém správy patří, a cíl zprávy – adresu IP agenta (131.107.3.24).
2. Zpráva SNMP je odeslána agentovi.
3. Agent přijímá pakety a dešifruje je. Název komunity (Public) je uznán.
4. Služba SNMP volá příslušného podagenta, který vyhledá v databázi MIB vyžádanou informaci dané relace.
5. Služba SNMP tuto informaci převeze a vytvoří návratovou zprávu SNMP, která bude obsahovat počet aktivních relací a cíl – adresu IP systému správy (131.107.7.29).
6. Zpráva SNMP je odeslána zpět systému správy.

Vlastnosti služby Agent SNMP systému Windows 2000

Tabulka 10.1 obsahuje popis všech typů služby, které lze konfigurovat za účelem správy počítačů vašeho systému.

Tabulka 10.1: Služba Agent SNMP

Typ služby agenta	Podmínky při výběru služby agenta
Fyzická	Počítač řídí fyzická zařízení jako oddíly na disku jednotky.
Správa logických zařízení	Počítač používá aplikace, které odesílají data pomocí protokolu TCP/IP. Tato služba by měla být povolena vždy.
Datová linka a podsít	Počítač řídí můstek.
Internet	Počítač vykonává funkci brány IP (směrovač).
Koncová	Počítač funguje jako hostitel IP. Tato služba by měla být povolena vždy.

Konfigurace služby SNMP obsahuje také následující informace:

- Jméno osoby, na kterou se můžete obrátit v případě potíží (například správce sítě),
- sídlo kontaktní osoby.

Tyto vlastnosti služby můžete konfigurovat na kartě **Agent** v dialogovém okně **Vlastnosti služby Microsoft SNMP**. Můžete je však zjistit také pomocí vzdálených požadavků SNMP. Více informací o konfiguraci vlastností agenta najdete v nápovědě pro systém Windows 2000.

Zabezpečení

Služba SNMP poskytuje základní zabezpečení prostřednictvím užívání názvů komunit a ověřovacích depeší. Komunikace SNMP můžete omezit například tak, že určitému agentu umožníte komunikovat pouze se skupinou systémů správy SNMP.

Depeše

Depeše lze používat k omezenému ověření zabezpečení. Nastavíte-li na počítači agenta příslušné depeše, bude je služba SNMP generovat po rozpoznání výskytu sledovaných událostí. Agent může být nastaven tak, aby inicioval odeslání ověřovací depeše v případech, kdy přijme informaci ze systému správy, který nemůže rozpoznat. Zpráva z tohoto systému je odeslána cíli depeše, přesně určeném v konfiguraci služby SNMP. Depeše lze mimoto generovat také pro takové události, jako jsou spuštění systému, vypnutí systému nebo narušení hesla.

Cíl depeše je určen pomocí názvu hostitelského počítače a adresy IP nebo IPX systému správy. Cílem depeše musí být hostitelský počítač s přístupem k síti a se spuštěným softwarem pro správu SNMP. Přestože jsou depeše konfigurovány správcem, jsou události (jako například restart systému), generující tyto zprávy, definovány agentem.

Cíle depeší můžete konfigurovat na kartě **Depeše** v dialogovém okně **Vlastnosti služby Microsoft SNMP**. Více informací o konfiguraci cílů depeší najdete v nápovědě pro systém Windows 2000.

Komunity

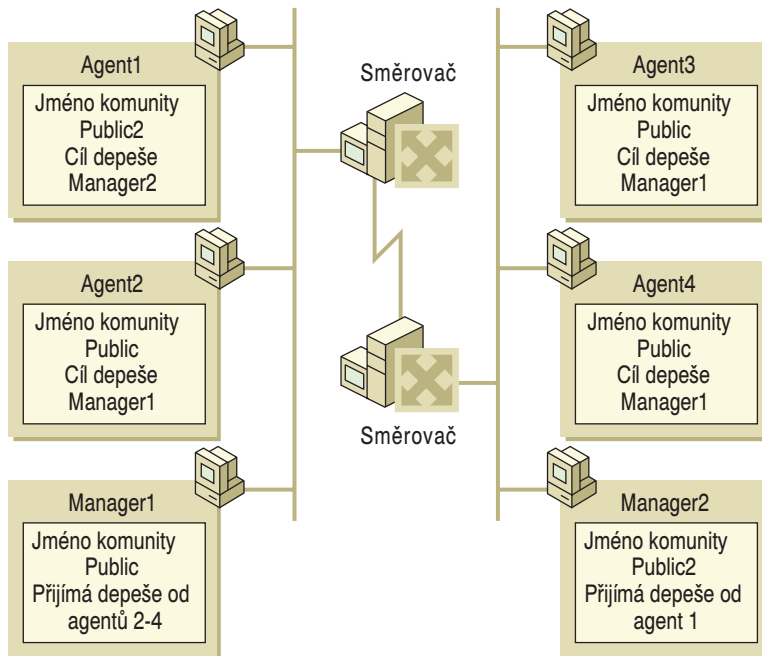
Každý hostitelský počítač se softwarem správy SNMP patří ke komunitě SNMP. Komunita SNMP je kolekce hostitelských počítačů, seskupených ze správních důvodů. Rozhodování o tom, které počítače by se měly stát členy téže komunity, je zpravidla (ni-

koli však vždy) určováno fyzickou blízkostí počítačů. Komunity jsou definovány podle názvů, které jim přiřadíte.

Názvy komunit lze používat k ověřování zpráv SNMP a tím také vytvořit základní zabezpečovací schéma služby SNMP. Přestože může jeden hostitelský počítač patřit k několika různým komunitám zároveň, nebude agent SNMP nikdy přijímat požadavky ze systému správy, jenž není na seznamu uznaných názvů komunit.

Mezi názvy komunit a názvy domén nebo pracovních skupin neexistuje žádná souvislost. Název komunity lze považovat za sdílené heslo správních konzol SNMP a řízených počítačů. Přiřazení těžko odhadnutelných názvů jednotlivým komunitám při instalaci služby SNMP leží už na bedrech správců sítí.

V příkladu (viz obrázek 10.4) jsou znázorněny dvě komunity – Public a Public2. Agent1 může odpovídat na požadavky služby SNMP z počítače Manager2, na který může také odesílat depeše, neboť oba tyto počítače jsou členy komunity Public2. Agent2, Agent3 a Agent4 mohou odpovídat na požadavky počítače Manager1, na nějž mohou také odesílat depeše, neboť všechny tyto počítače jsou členy komunity Public (výchozí).



Obrázek 10.4: Příklad komunit SNMP.

Názvy komunit jsou spravovány pomocí konfigurace vlastností zabezpečení SNMP. Více informací o konfiguraci vlastností zabezpečení najdete v nápovědě pro systém Windows 2000 Server.

Jakmile přijme agent SNMP zprávu, bude název komunity, obsažený v paketu, okamžitě porovnán s položkami seznamu uznaných názvů komunit. Je-li v tomto seznamu nalezen shodný údaj, přijde řada na porovnání názvu s položkami seznamu přístupových práv dané komunity. Libovolné komunitě můžete přiřadit následující typy oprávnění:

- **Žádné**
- **Agent SNMP požadavek nezpracuje.** Když přijme zprávu SNMP ze systému správy takové komunity, vyřadí jej a vygeneruje ověřovací depeši.
- **Upozornění**
V současné době je toto oprávnění shodné s oprávněním **Žádné**.
- **Jen pro čtení**
Agent nezpracovává požadavky SET žádající komunity. Zpracovává pouze její požadavky GET, GET-NEXT a GET-BULK. Agent zamítne všechny požadavky SET, odeslané systémy správy této komunity a vygeneruje ověřovací depeši.
- **Pro čtení a vytvoření**
Agent SNMP zpracuje nebo vytvoří všechny požadavky dané komunity. Zpracuje všechny její požadavky SET, GET, GET-NEXT a GET-BULK včetně požadavků SET, které vyžadují přidání nového objektu do databáze MIB.
- **Pro čtení i zápis**
V současné době shodné s oprávněním **Pro čtení a vytvoření**

Oprávnění komunity jsou konfigurována na kartě **Zabezpečení SNMP** v dialogovém okně **Vlastnosti služby Microsoft SNMP**.

Názvy komunit jsou přenášeny v síti jako prostý text, tzn. bez šifrování. Vzhledem k tomu, že je tento typ přenosu je zranitelný ze strany počítačových pirátů, kteří analyzují software, představuje používání názvů komunit SNMP potenciální riziko ohrožení zabezpečení. K zabezpečení zprávy SNMP však můžete použít zabezpečení protokolu IP systému Windows 2000. Více informací o konfiguraci zabezpečení protokolu IP najdete v oddílu „Ochrana zpráv SNMP pomocí zabezpečení protokolu IP“ později v této kapitole.

Možnosti konfigurace zabezpečení protokolu SNMP

Ochranu přenosů SNMP můžete zvýšit nastavením některých nebo všech níže uvedených možností:

- **Uznané názvy komunit** Služba SNMP vyžaduje konfiguraci alespoň jednoho názvu komunity. Název Public se používá obecně jako název komunity, neboť se jedná o běžný název, jenž je vesměs uznáván ve všech implementacích služby SNMP. Výchozí název komunity můžete také vymazat nebo změnit, případně přidat nové názvy. V případě, že agent SNMP přijme požadavek komunity, která není uvedena v příslušném seznamu, generuje automaticky ověřovací depeši. Nebude-li v seznamu definován alespoň jeden název komunity, agent SNMP zamítne všechny příchozí požadavky SNMP.
- **Oprávnění** Pomocí úrovně oprávnění můžete určit, jakým způsobem bude agent zpracovávat požadavky SNMP různých komunit. Lze například určit takový stupeň oprávnění, který zabráni zpracování všech zpráv přicházejících z určené komunity.
- **Přijímat pakety SNMP od všech hostitelů** V tomto kontextu se zdrojový hostitelský počítač a seznam hostitelských počítačů odkazují na systém správy SNMP a seznam ostatních uznaných systémů správy. Je-li tato možnost povolena, nebudou žádné pakety SNMP zamítnuty ani na základě názvu nebo adresy zdrojového hostitelského počítače, ani na základě seznamu uznaných hostitelských počítačů. Tato možnost je ve výchozím nastavení povolena.

- **Přijímat pakety SNMP pouze od těchto hostitelů** Nastavení této volby poskytuje zajištění omezeného stupně zabezpečení. Je-li tato možnost povolena, budou přijímány pouze pakety SNMP, přijaté od hostitelů uvedených na seznamu uznaných hostitelů. Agent SNMP zamítne všechny zprávy, pocházející z jiných zdrojů a v takových případech vždy generuje ověřovací depeši. Omezením přístupu pouze na vybrané hostitele poskytuje vyšší stupeň zabezpečení než omezení přístupu k určité komunitě, neboť název komunity může skrývat rozsáhlou skupinu hostitelů.
- **Odesílat ověřovací depeše** Bude-li přijat požadavek bez uvedení platného názvu komunity nebo když odesílatel přijaté zprávy není na seznamu uznaných hostitelů, může agent odeslat ověřovací depeši na jeden nebo více cílů depeše (systémové zprávy). Depeše indikuje, že oprávnění požadavku SNMP nebylo možné ověřit. To je výchozí nastavení.

Zabezpečení SNMP je konfigurováno na kartě **Zabezpečení** v dialogovém okně **Vlastností služby Microsoft SNMP**. Více informací o konfiguraci služby SNMP najdete v nápovědě pro systém Windows 2000 Server.

Překladač událostí SNMP

Tato funkce umožňuje správci stanovit události SNMP, které budou překládány na depeše. Četnost překladů těchto událostí lze určit také. Kromě toho můžete nastavit také možnosti souboru protokolu.

Ke konfiguraci lze použít nástroj příkazového řádku `Evntcmd.exe` nebo aplikace grafického rozhraní `Evntwin.exe`. Oba tyto soubory, spolu s knihovnou `Evntagnt.dll`, jsou při instalaci služby SNMP vytvořeny ve složce `%SystemRoot%\system32`. Lze je spouštět z příkazového řádku systému Windows 2000.

Překladač událostí používá službu SNMP ke generování depeše. Standardně nejsou překládány žádné události. Více informací o používání a konfiguraci tohoto nástroje najdete v dokumentaci online ke službě SNMP.

Architektura protokolu SNMP v systému Windows 2000

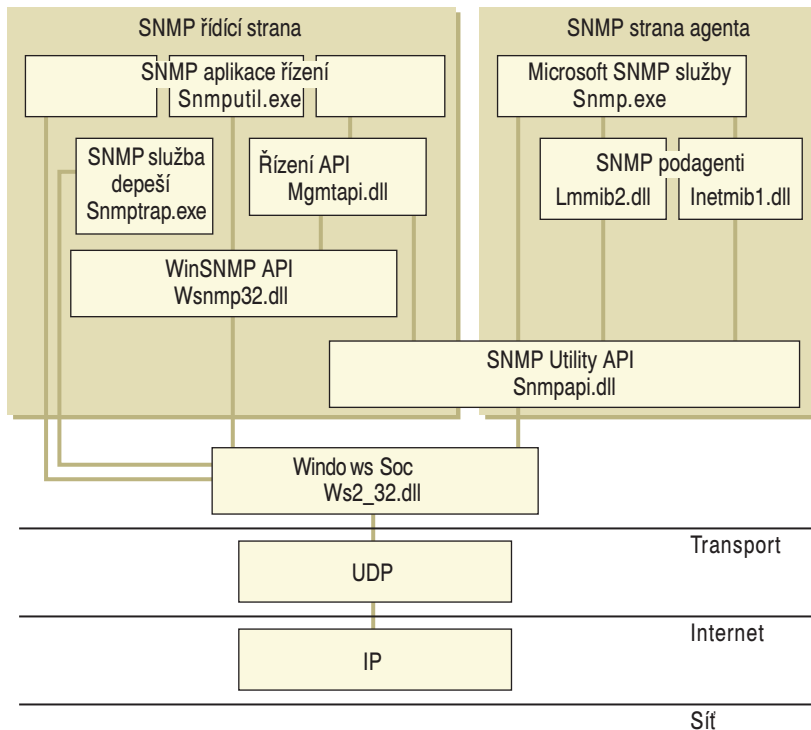
Vnitřní architektura protokolu SNMP v systému Windows 2000 je rozdělena na funkce správy a agentů. V některých případech se však tyto funkce překrývají (viz obrázek 10.5).

Vnitřní součásti, které se bezprostředně zapojují do plnění následujících funkcí SNMP:

Služba Microsoft SNMP Service (`Snmp.exe`) Služba Microsoft SNMP Service (`Snmp.exe`) přijímá ze sítě pakety SNMP, dešifruje je a potom je předává příslušným podagentům. Služba SNMP je také označována jako Hlavní agent SNMP nebo Rozšiřitelný agent SNMP. Tato služba je také zodpovědná za zachycování událostí jednotlivých podagentů SNMP a předávání depeší příslušným systémům správy.

Podagenti SNMP Tato služba je také označována jako Rozšiřující agenti SNMP (jako například `Inetmib1.dll`, `Hostmib.dll`, `Lmmib2.dll`). Podagenti jsou v podstatě dynamickými knihovnami, exportujícími kolekce vstupních bodů. Po přijetí zprávy SNMP dešifruje služba SNMP její obsah a předá jej příslušným podagentům voláním jednoho

ze vstupních bodů. Po zpracování zprávy předá podagent informaci zpět službě SNMP. Ta zase uspořádá získaná data do zprávy SNMP, kterou odešle zpět systému správy. Služba SNMP a podagenti se opírají o rozhraní SNMP Utility API.



Obrázek 10.5: Architektura protokolu SNMP v systému Windows 2000.

SNMP Utility API (Snmpapi.dll) Tato podmnožina rozhraní API poskytuje kolekci funkcí, vyžadovaných agentem i správcem pro zpracovávání zpráv SNMP. Služba SNMP používá tuto knihovnu pro operace spojené se správou paměti, pro rutiny dešifrování adres, v rutinách zpracování identifikátoru objektu atd. Kolekce funkcí je určena také podagentům ke zpracovávání a řízení objektů SNMP. Přestože není její používání nijak vynucováno, její aplikační rámec významně usnadňuje vývoj dalších podagentů SNMP.

WinSNMP API (Wsnmp32.dll) a Management API (Mgmtapi.dll) Tyto podmnožiny rozhraní API slouží k usnadnění vývoje softwaru pro správu SNMP. Knihovna WinSNMP API obsahuje kolekci funkcí pro šifrování, dešifrování, odesílání a přijímání zpráv SNMP. Knihovna Management API je jednoduchou limitovanou knihovnou vytvořenou nad rozhraními WinSNMP a SNMP Utility API. Obsahuje skutečně pouze ty nejzákladnější funkce, které lze používat k rychlému vytváření nových aplikací pro správu SNMP.

Služba SNMP Trap Service (Snmptrap.exe) Služba vytváření depeší SNMP je samostatnou součástí protokolu SNMP, jež umožňuje aplikacím pro správu systému přijímat depeše vysílané agenty SNMP. Služba přijímá příchozí depeše ze sítě a předává je funkcím rozhraní WinSNMP API (Wsnmp32.dll) příslušného systému správy.

Aplikace služby Správce SNMP (Snmputil.exe) Tento nástroj, dodávaný na disku s operačním systémem Windows 2000, má sloužit jako příklad aplikačního softwaru pro správu SNMP, vytvořeného na bázi rozhraní Management API. K vytváření vlastních aplikací můžete používat jak rozhraní Management API, tak WinSNMP API anebo obě zároveň. Aplikace lze vytvářet také bezprostředně nad rozhraním knihovny Microsoft Windows Sockets API. Více informací o vytváření vlastních aplikací pro správu SNMP najdete v dokumentaci Microsoft® Windows® 2000 Platform SDK.

Specifické otázky při implementaci protokolu SNMP

Následující řádky jsou určeny vám, kteří chcete službu SNMP využívat co nejeefektivněji, a vám, kteří se chcete vyhnout problematickým implementacím.

Změna nastavení portů SNMP

Protokol SNMP standardně používá ke sledování zpráv SNMP port UDP č. 161, zatímco port 162 se používá ke sledování depeší SNMP. Pokud jsou tyto porty užívány jiným protokolem nebo službou, můžete nastavení změnit příslušnými úpravami místního souboru Services. Soubor Services je umístěn ve složce `%SystemRoot%\System32\Drivers\Etc`.

Tento soubor nemá žádnou příponu. K jeho úpravám můžete použít libovolný textový editor. Systém správy musí být také konfigurován tak, aby zachycoval a odesílal zprávy na nové porty.

Upozornění: Pokud jste už dříve používali zabezpečení protokolu IP k ochraně a šifrování zpráv SNMP na výchozích portech, musíte nyní aktualizovat také zásadu zabezpečení IP. Kdybyste tak neučinili, byla by komunikace na nově nastavených portech chybně zablokována, nebo by komunikace SNMP probíhala bez zabezpečení.

Ochrana zpráv SNMP pomocí zabezpečení protokolu IP

Chcete-li používat k zabezpečení zpráv SNMP protokol IPSec, musíte konfigurovat všechny systémy podporující protokol SNMP tak, aby používaly také IPSec. V opačném případě komunikace selže. Nemůžete-li konfigurovat všechny systémy podporující protokol SNMP tak, aby používaly také IPSec, musíte alespoň konfigurovat zásady IPSec pro všechny systémy s podporou protokolu SNMP. A to tak, aby mohly odesílat zprávy v podobě prostého textu (nešifrované informace). To však značnou měrou maří myšlenku zabezpečení zpráv, neboť tak budou všechny komunikace nechráněny.

Zabezpečení protokolu IP neznamena automatické šifrování protokolu SNMP. Musíte nejprve v příslušném seznamu filtrů IP vytvořit specifikace filtru pro přenosy mezi systémy správy a agenty SNMP. Specifikace filtru zahrnuje dvě sady nastavení.

První sada specifikací filtru je určena pro běžné přenosy SNMP (zprávy SNMP) mezi systémy správy a agenty SNMP:

- Zrcadleno: povoleno,
- Typ protokolu: TCP,
- Zdrojový a cílový port: 161,
- Zrcadleno: povoleno,

- Typ protokolu: UDP,
- Zdrojový a cílový port: 161,

Druhá sada specifikací filtru je určena pro depeše odesílané agenty SNMP systémům správy:

- Zrcadleno: povoleno,
- Typ protokolu: TCP,
- Zdrojový a cílový port: 162,
- Zrcadleno: povoleno,
- Typ protokolu: UDP,
- Zdrojový a cílový port: 162,

Více informací o vytváření specifikací filtru najdete v nápovědě systému Windows 2000.

Správa služeb DHCP, Windows Internet Name Service a Internet Authentication Service

Správce sítě může používat službu SNMP jako pomocníka při následujících úkonech:

- Při prohlížení a úpravě parametrů databází MIB LAN Manager a MIB-II,
- při sledování a konfiguraci parametrů všech serverů WINS v dané síti,
- při sledování serverů DHCP,
- při používání programu Sledování systému za účelem monitorování výkonu čítačů TCP/IP (čítačů výkonu protokolů ICMP (Internet Control Message Protocol), IP, Network Interface, TCP, UDP, DHCP, FTP, WINS a IIS).

Více informací o programu Sledování systému najdete v dokumentaci k Microsoft® Windows® 2000 Professional Resource Kit.

K zajištění jednoduchých funkcí správy SNMP se doporučuje používat nástroje, dodávané na doprovodném CD Windows 2000 Resource Kit.

Používání programu Sledování systému

Pomocí služby SNMP lze prohlížet všechny nainstalované čítače programu Sledování systému. Služba SNMP k tomuto účelu poskytuje nástroj Perf2MIB, umístěný na doprovodném CD Windows 2000 Resource Kit. Více informací o používání tohoto nástroje najdete v nápovědě Tools Help na stejném CD.

Správa služby DHCP

Pomocí služby SNMP lze sledovat, nikoli však konfigurovat, také objekty serveru DHCP i objekty serveru IIS, které jsou založeny na standardu Windows 2000.

Správa služby WINS

Pomocí služby SNMP lze monitorovat i konfigurovat téměř všechny objekty serveru WINS. Více informací o tom, jaké parametry WINS lze konfigurovat pomocí SNMP, najdete v kapitole „Typy objektů databáze MIB“. Konfigurovat lze všechny objekty WINS, jež jsou definovány pro čtení i zápis.

Správa služby IAS

Služba Internet Authentication Server (IAS) implementuje mechanismus ověřování RADIUS a mechanismus účtování MIB, což umožňuje jejich monitorování i konfiguraci pomocí služby SNMP. Konfigurovat lze všechny objekty IAS, jež jsou definovány pro čtení i zápis.

Nástroje služby SNMP

Tabulka 10.2 obsahuje popisy nástrojů, souvisejících s činností služby SNMP, a souborů, dodávaných na doprovodném CD Windows 2000 Resource Kit. Více informací o používání tohoto nástroje najdete v nápovědě Tools Help na stejném CD.

Informace o nástroji Snpmputil.exe najdete v nápovědě Nástroje pro podporu systému Windows 2000. Informace o instalaci a používání těchto nástrojů a související nápovědy najdete v souboru Sreadme.doc uloženém ve složce \Support\Tools na instalačním CD operačního systému Windows 2000.

Tabulka 10.2: Nástroje služby SNMP

Název souboru	Popis
Mibcc.exe	Převádí popis ASN.1 MIB do binárního souboru MIB.bin.
Snpmputil.exe	Vzorový aplikační program pro správu, vytvořený pomocí rozhraní Management API. Více informací o rozhraní Management API najdete v oddílu „Architektura protokolu SNMP v systému Windows 2000“.

Nastavení položek registru

Služba SNMP převádí informace uložené v registru do formátu, jenž lze používat také v programech správy sítě SNMP od jiných dodavatelů. Uživatelské rozhraní Služby SNMP systému Windows 2000 se při změnách nastavení položek registru doporučuje používat vždy, když je to možné. Změníte-li některou z vlastností služby SNMP prostřednictvím uživatelského rozhraní, budou automaticky upraveny také hodnoty souvisejících položek registru. Výjimku tvoří pouze následující položka registru, která definuje seznam konfigurovaných doplňujících agentů (podagentů):

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SNMP\Parameters\
ExtensionAgents
```

Služba SNMP rozpozná všechny změny nastavení položek registru při spuštění službě. Změny parametrů služby SNMP budou uplatněny bez nutnosti tuto službu restartovat.

Upozornění: K přímé editaci registru se uchylujte skutečně až tehdy, nezbyvá-li žádná jiná možnost jeho úpravy. Editory registru obcházejí standardní bezpečnostní opatření, poskytovaná správnými nástroji. Tato bezpečnostní opatření zajišťují prevenci proti zadávání konfliktních nastavení nebo nastavení, která by mohla snížit výkon systému nebo dokonce systém poškodit. Přímá editace registru může mít vážné a nepředpokladané následky, jež mohou ve svém důsledku zabránit spuštění systému. Takové poškození lze řešit jedině opětovnou instalací systému Windows 2000. Chcete-li konfigurovat nebo přizpůsobit nastavení systému Windows 2000, používejte k tomu účelu program Microsoft Management Console (MMC) nebo jiné nástroje Ovládacích panelů.

Odstraňování problémů s protokolem SNMP

Tato podkapitola obsahuje popis některých metod, jež mohou být užitečné při řešení problémů spojených s činností služby SNMP. Při testování mějte službu spuštěnou při normálním zatížení. Jedině tak můžete získat skutečně reálné informace.

Prohlížeč událostí

Správa výjimek služby SNMP byla v systémech Windows 2000 Server a Windows 2000 Professional značně vylepšena. Ruční konfigurace parametrů protokolování chyb služby SNMP byla nahrazena zdokonaleným mechanismem řízení výjimek, integrovaným navíc s programem Prohlížeč událostí. Máte-li podezření, že služba SNMP nefunguje tak, jak má, spusťte program Prohlížeč událostí. Více informací o postupech při odstraňování problémů najdete v nápovědě systému Windows 2000.

► Použití Prohlížeče událostí

1. Klepněte na tlačítko **Start**, přesuňte ukazatel nad položku **Nastavení**, klepněte na položku **Ovládací panely** a v okně Ovládacích panelů poklepejte na ikonu **Nástroje pro správu**. V zobrazené složce poklepejte na ikonu **Prohlížeč událostí**.
2. Zadejte příkaz **Systémový protokol**.
3. V podokně **Obor** poklepejte na událost služby SNMP. Zobrazí se podrobnosti vybrané události.

Pomocí filtru **Zobrazit** můžete zobrazit pouze kolekci událostí služby SNMP. Více informací o používání služby Prohlížeč událostí najdete v nápovědě systému Windows 2000.

Služba WINS

Při dotazování na server WINS se může stát, že budete muset v systému správy SNMP zvýšit interval časového limitu SNMP. Pokud některé dotazy WINS fungují, a jiné ne, zvýšte hodnotu v nastavení časového limitu SNMP.

Adresy IPX

V případě, že při instalaci služby SNMP uvedete jako cíl depeše adresu IPX, může se po restartu počítače zobrazit následující chybové hlášení:

Error 3

K zobrazení této zprávy dochází v případech, kdy byla adresa IPX zadána nesprávně (k oddělení čísla sítě od adresy řízení přístupu k médiím (MAC) byla použita čárka nebo pomlčka). Software správy SNMP by mělo adresu 00008022,0002C0-F7AABD rozpoznat zcela normálně. Služba SNMP systému Windows 2000 však nerozpoznává správně adresy s čárkou nebo pomlčkou mezi číslem sítě a adresou MAC.

Adresa, použitá jako cíl depeše IPX, musí dodržovat formát 8.12 pro čísla sítí a adresy MAC, definovaný organizací IETF. Následující formát je správný:

xxxxxxxx.yyyyyyyyyyyy

xxxxxxxx je číslo sítě, zatímco yyyyyyyyyyyy je adresa MAC.

Soubory služby SNMP

Tabulka 10.3 obsahuje seznam souborů, které jsou součástí služby Microsoft Windows 2000 SNMP. Tento seznam můžete použít jako pomoc při odstraňování potíží.

Tabulka 10.3: Soubory služby SNMP

Název souboru	Popis
Wsnmp32.dll, Mgmtapi.dll	Správce SNMP standardu Windows 2000 pro správu knihoven API. Sleduje požadavky správce a odesílá požadavky agentům SNMP a přijímá jejich odpovědi.
Mib.bin	Instalován spolu se službou SNMP a používán knihovnou Management API (Mgmtapi.dll). mapuje textové názvy objektů na numerické identifikátory objektů.
Snmpp.exe	Služba Agent SNMP. Hlavní agent (proxy). Přijímá požadavky programu správy a předává požadavky ke zpracování příslušným knihovnám doplňujících agentů (podagentů).
Snmpttrap.exe	Proces spuštěný na pozadí. Přijímá depeše SNMP od agentů SNMP a předává je příslušným funkcím knihovny Management API v konzole pro správu. Je spouštěn pouze tehdy, když Správce SNMP funkcí API přijme požadavek správce na přijetí depeše.

Další zdroje

Více informací o službě SNMP najdete v následujících knihách:

- J. D. Murray: *Windows NT SNMP*, 1998, Sebastopol: O'Reilly & Associates.
- D. Perkins a E. McGinnis: *Understanding SNMP MIBs*, 1997, New York: Prentice Hall PTR.
- M. T. Rose: *The Simple Book: An Introduction to Management of TCP/IP-based Internets*, 1994, New York: Prentice-Hall, Inc.
- M. Hein a D. Griffiths: *SNMP Versions 1 & 2: Simple Network Management Protocol Theory and Practice*, 1995, New York: International Thomson Computer Press.
- W. Stallings: *SNMP, SNMPv2 and CMIP: The Practical Guide to Network-Management Standards*, 1993, Addison-Wesley Publishing Company.
- Více informací o implementaci služby SNMP v systému Windows 2000 najdete pod odkazem Microsoft TechNet na stránce WWW Web Resources na <http://windows.microsoft.com/windows2000/reskit/webresources>.

Následující specifikace RFC se vztahují na verzi 1 služby SNMP:

- RFC 1155: *Structure and Identification of Management Information for TCP/IP-based Internets*.
- RFC 1157: *Simple Network Management Protocol (SNMP)*.
- RFC 1213: *Management Information Base for Network Management of TCP/IP-based Internets. MIB-II*.
- RFC 1573: *Evolution of the Interfaces Group of MIB-II*.

Následující specifikace RFC se vztahují na verzi 2 služby SNMP:

- RFC 1902: *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2).*
- RFC 1904: *Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2).*
- RFC 1905: *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2).*
- RFC 1906: *Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2).*
- RFC 1907: *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2).*
- RFC 1908: *Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework.*

ČÁST IV

Dodatky



PŘÍLOHA A

Model OSI

V počátečních letech počítačových sítí bylo odesílání a přijímání dat po síti zmatečné, protože velké společnosti jako IBM, Honeywell, a Digital Equipment Corporation měly své vlastní standardy pro propojování počítačů. Nebylo pravděpodobné, že by aplikace, pracující s různým vybavením od různých dodavatelů, spolu mohly komunikovat. Dodavatelé, uživatelé a standardizační orgány se museli dohodnout a realizovat standardní architekturu, která by umožňovala výměnu informací mezi počítačovými systémy i v případě, že by používaly software a vybavení různých dodavatelů.

V roce 1978 předložila organizace International Standards Organization (ISO) první síťový model, nazvaný Open Systems Interconnection (OSI) jako první krok ke standardizaci datových komunikací, která by podporovala univerzálnost sítí různých dodavatelů.

Model OSI se skládá z vrstev, z nichž má každá přesně stanovenou sadu funkcí. Model určuje sadu protokolů a rozhraní, které musí být v každé vrstvě implementovány a poskytuje směrnice pro implementaci rozhraní mezi vrstvami.

V této příloze

Vrstvy modelu OSI 608

Tok dat v modelu OSI 612

Terminologie vertikálního rozhraní v modelu OSI 613

Související informace v Resource Kitu

- Více informací o síťové architektuře systému Windows 2000 naleznete v části „Síťová architektura systému Windows 2000“ v této knize.

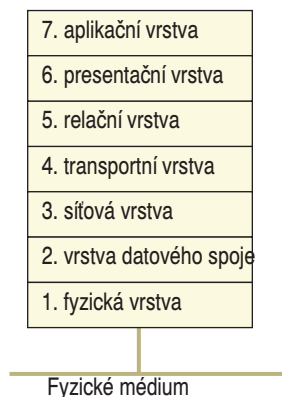
Vrstvy modelu OSI

Každá vrstva modelu OSI existuje jako nezávislý modul. Teoreticky tedy můžete v libovolné dané vrstvě nahradit jeden protokol jiným bez toho, že by to mělo vliv na činnost vyšších nebo nižších vrstev.

Návrh modelu OSI vychází z následujících zásad:

- Vrstva by měla být vytvořena jen tehdy, když je vyžadována další úroveň abstrakce.
- Každá vrstva by měla vykonávat dobře definovanou funkci.
- Funkce každé vrstvy by měla být zvolena s cílem definovat mezinárodně standardizované protokoly.
- Hranice vrstvy by měly být vybrány tak, aby se minimalizoval tok informací přes rozhraní.
- Počet vrstev by měl být dost velký, aby umožňoval oddělení rozdílných funkcí, ale dost malý, aby se architektura nestala těžkopádnou.

Obrázek A.1 ukazuje vrstvy v modelu OSI, počínajíc fyzickou vrstvou, která je nejbližší síťovému médium.



Obrázek A.1 Vrstvy modelu OSI

Fyzická vrstva

Fyzická vrstva je nejnižší vrstvou modelu OSI. Tato vrstva řídí způsob, jakým je po fyzickém médium poslán a přijímán bitový proud nestrukturovaných hrubých dat. Skládá se z elektrických, optických a fyzických součástí sítě. Fyzická vrstva přenáší signály pro všechny vyšší vrstvy.

Kódování dat modifikuje jednoduchý digitální formát signálu (jedničky a nuly), používaný počítačem, pro lepší přizpůsobení charakteristikám fyzického média a na podporu synchronizace bitů a rámců.

Kódování dat určuje:

- Jaký vzor signálu představuje binární 0 a binární 1.
- Jak přijímající stanice rozpoznává, kdy začíná zakódovaný bit.
- Jak přijímací stanice odděluje rámec.

Fyzické součásti (elektroinstalace, konektory, vývody) určují:

- Zda se pro připojení k médiu používá externí vysílač-přijímač.
- Kolik kolíků mají konektory a jaká je jejich úloha.

Technika přenosu určuje, zda se zakódované bity přenášejí signály v základním pásmu (digitálně) nebo širokopásmově (analogově).

Fyzické prostředky přenosu (síťový adaptér, adaptér přenosu optickými vlákny apod.) určují, zda je vhodné přenášet bity jako elektrické nebo optické signály.

Linková vrstva

Linková vrstva poskytuje bezchybný přenos datových rámců z jednoho počítače do druhého přes fyzickou vrstvu. Vrstvy nad touto vrstvou mohou předpokládat virtuálně bezchybný přenos dat po síti.

Linková vrstva obstarává následující funkce:

- Zřízení a ukončení logických spojů (propojení virtuálního okruhu) mezi dvěma počítači, identifikovanými svými jedinečnými adresami síťových adaptérů.
- Řízení toku rámců instruováním vysílajícího počítače, aby nepřepřeládal vyrovnávací paměť rámců.
- Sekvenční přenos a příjem rámců.
- Poskytuje a přijímá potvrzení příjmu rámců a zajišťuje detekci a opravu chyb, které se vyskytnou ve fyzické vrstvě, opětovným vysláním nepotvrzených rámců a ošetřením duplicitních příjmů rámců.
- Řízení přístupu k médiu pro určení, kdy je počítači povoleno použití fyzického média.
- Ohraničování rámců k vytvoření a rozpoznávání jejich hranic.
- Kontrolu chyb rámců pro potvrzení integrity přijatého rámce.
- Prozkoumávání cílových adres každého přijatého rámce a určování, zda má být rámec směrován vyšší vrstvě.

Poznámka: Zatímco služby linkové vrstvy zajišťují spolehlivé doručení dat, mnoho směrovatelných sad protokolů jako TCP/IP a IPX/SPX je ani nezajišťují, ani nepoužívají služby linkové vrstvy pro spolehlivé doručení. Místo toho je spolehlivé doručení dat poskytováno protokoly, pracujícími na transportní vrstvě.

Síťová vrstva

Síťová vrstva řídí činnost podsítě. Určuje, jakou fyzickou cestou půjdou data podle podmínek v síti, priority služby a dalších faktorů..

Síťová vrstva obstarává následující funkce:

- Přenos rámců ke směrovači, pokud síťová adresa doručení neudává síť, ke které je počítač připojen.
- Řízení provozu podsítě, aby umožnila zprostředkujícím systémům dávat vysílajícím stanicím pokyny k zastavení přenosu, když se zaplní vyrovnávací paměť směrovače. Pokud je směrovač zaměstnán, síťová vrstva může dát vysílající stanici pokyn k použití náhradního směrovače.

- Fragmentaci rámců směrovačem, pokud velikost spoje ve směru k dalšímu směrovači (největší přenosová jednotka – MTU) je menší než velikost rámce. Fragmenty rámců jsou znovu složeny v cílové stanici.
- Překlad logické adresy počítače (v síťové vrstvě) na fyzickou adresu síťového adaptéru (v linkové vrstvě), pokud je to zapotřebí.

Síťová vrstva musí v přenášejícím počítači vytvořit svou hlavičku způsobem, který rozpoznávají síťové vrstvy zprostředkujících systémů podsíti, aby ji mohly použít ke směrování dat do cílové adresy.

V síťové vrstvě a ve vrstvách pod ní existují protokoly protějšků (peer protocols) mezi počítačem a jeho bezprostředním sousedem, který často nebývá definitivním cílem. Zdrojový a cílový počítač může být často oddělen mnoha zprostředkujícími systémy.

Síťová vrstva odstraňuje u vyšších vrstev potřebu vědět cokoliv o přenosech dat nebo o technologiích zprostředkujícího přepínání pro propojení systémů. Síťová vrstva odpovídá za navázání, údržbu a ukončení spojení se zprostředkujícími systémy v komunikační podsíti.

Transportní vrstva

Transportní vrstva zajišťuje, aby zprávy byly doručeny v takovém pořadí, v jakém byly odeslány a aby nedocházelo ke ztrátám nebo duplicitám.

Velikost a složitost transportního protokolu závisí na typu služeb, dostupných ze síťové a linkové vrstvy. Pro spolehlivou síťovou vrstvu nebo linkovou vrstvu se schopností vytvářet virtuální okruhy (například vrstva LLC v protokolu NetBEUI) je transportní vrstva vyžadována pouze pro předávání dat do další vrstvy. Pokud je síťová nebo linková vrstva nespolehlivá nebo pokud podporuje pouze datagramy, jak je tomu u vrstvy IP v protokolu TCP/IP a u vrstvy IPX protokolu IPX/SPX, zahrnuje transportní vrstva řazení a potvrzování a s tím spojenou detekci chyb a jejich odstraňování.

Mezi funkce transportní vrstvy patří:

- Přijímání zpráv z vyšších vrstev a jejich rozdělení do segmentů v případě potřeby.
- Zajišťování spolehlivého doručování zpráv s potvrzením z jednoho konce na druhý.
- Vydání pokynu přenášejícímu počítači, aby nepokračoval v přenosu, když nejsou k dispozici vyrovnávací paměti pro příjem.
- Multiplexování relací nebo proudů zpráv mezi procesy v jednom logickém spojení a sledování, které relaci patří která zpráva.

Transportní vrstva může přijímat velké zprávy, ale síťová a nižší vrstvy vynucují přísná omezení velikosti. Proto musí transportní vrstva rozdělovat zprávy do menších jednotek, zvaných segmenty, a ke každému rámcu připojovat hlavičku.

Pokud nižší vrstvy nespravují řazení, musí obsahovat transportní hlavička informace o řazení, které umožní transportní vrstvě na straně příjemce odevzdat nejbližší vyšší vrstvě data ve správném pořadí.

Na rozdíl od nižších vrstev, které mají protokoly, týkající se připojení k bezprostředně sousedícím uzlům nebo počítačům, transportní vrstva a vrstvy nad ní jsou skutečnými vrstvami přenosu od zdroje do cíle, kterým se také říká vrstvy na úrovni koncových zařízení (end-to-end). Tyto vyšší vrstvy se nezabývají podrobnostmi dílčích komunikačních služeb nižších úrovní. Software pro tyto vrstvy komunikuje s podobným softwarem cílových počítačů použitím hlaviček zpráv a řídicích zpráv.

Relační vrstva

Relační vrstva navazuje komunikační relaci mezi dvěma procesy, spuštěnými na různých počítačích, a může podporovat přenos dat v režimu zpráv.

Funkce relační vrstvy zahrnují následující úkoly:

- Povoluje aplikačním procesům registrovat jedinečné adresy procesů, jakými jsou názvy systému NetBIOS. Relační vrstva používá tyto uložené adresy pro pomoc při překladu adres procesů na adresy síťových adaptérů.
- Navazování, sledování a ukončování relace na bázi virtuálního okruhu mezi dvěma procesy, určenými svými jedinečnými adresami. Relace na bázi virtuálního okruhu je přímé spojení, existující mezi vysílačem a přijímačem.
- Odděluje zprávy přidáním informací, určujících začátek a konec zprávy, do hlavičky. Přijímající relační vrstva pak nemusí oznamovat přítomnost zprávy aplikaci vyšší úrovně, dokud není přijata celá zpráva.
- Provádí synchronizaci zpráv. Synchronizace zpráv je koordinace přenosu dat mezi vysílající relační vrstvou a přijímající relační vrstvou. Synchronizace chrání přijímající relační vrstvu před přetečením dat. Tento přenos je koordinován s potvrzovacími zprávami (ACK). Zprávy ACK se posílají tam a zpět mezi oběma konci přenosu a ohlašují stav přijímací vyrovnávací paměti pro příjem dalších dat.
- Provádí další podpůrné funkce, které umožňují procesům komunikovat po síti, jako je ověřování uživatelů a zabezpečení přístupu k prostředkům.

Prezentační vrstva

Prezentační vrstva slouží jako překladatč dat pro síť. Tato vrstva u odesílajícího počítače překládá data, odeslaná aplikační vrstvou, do společného formátu. V přijímajícím počítači překládá prezentační vrstva společný formát na formát, známý aplikační vrstvě.

Prezentační vrstva obstarává následující funkce:

- Překlad kódování znaků, například z kódování ASCII do kódování EBCDIC.
- Konverzi dat, jako například obrácení pořadí bitů, náhradu znaků CR znaky CR/LF, převod celých čísel na čísla v pohyblivé řádové čárce.
- Kompresi dat, která snižuje množství bitů, které se musí přenášet.
- Šifrování a dešifrování dat, které zabezpečuje data pro přenos potenciálně nechráněnou sítí. Jedním z použití šifrování je přenos hesla do přijímajícího počítače.

Aplikační vrstva

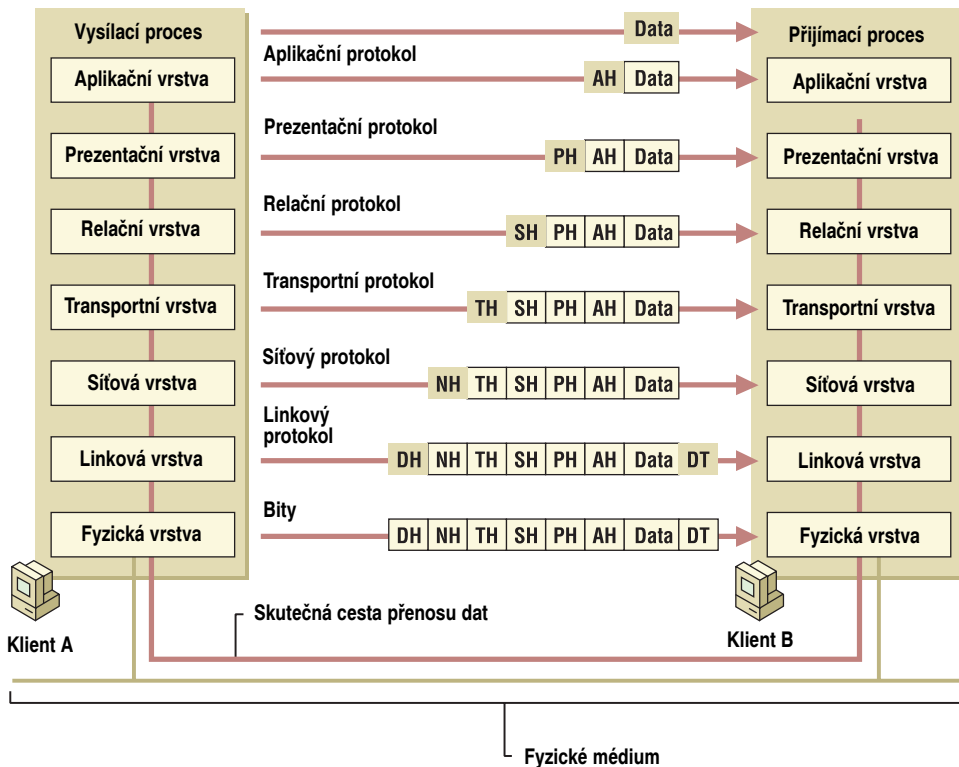
Aplikační vrstva slouží jako přístupové okno k síťovým službám pro uživatele a aplikační procesy. Aplikační vrstva zajišťuje následující funkce:

- Sdílení prostředků a přesměrování zařízení
- Přístup ke vzdáleným souborům
- Přístup ke vzdáleným tiskárnám
- Podporu komunikace mezi procesy
- Podporu vzdáleného volání procedur
- Správu sítě

- Adresářové služby
- Předávání elektronických zpráv včetně elektronické pošty (e-mail)
- Simulaci virtuálních terminálů

Tok dat v modelu OSI

Model OSI představuje standardní architekturu toku dat s protokoly, specifikovanými takovým způsobem, že přijímající vrstva na cílovém počítači přijímá přesně stejný objekt, jaký byl odeslán shodnou vrstvou zdrojového počítače. Obrázek A.2 ukazuje tok dat modelu OSI.



Obrázek A.2 Tok dat modelu OSI

Vysílající proces předává data aplikační vrstvě. Aplikační vrstva připojuje aplikační hlavičku a pak předává rámec prezentační vrstvě.

Prezentační vrstva může data různým způsobem transformovat, pokud je to nezbytné, například překládáním nebo přidáním hlavičky. Dává výsledek relační vrstvě. Prezentační vrstva se nezabývá tím, zda vůbec se v datech, přijatých od aplikační vrstvy, nachází hlavička aplikační vrstvy, která část dat je aplikační hlavičkou a kterou část tvoří uživatelská data, protože tato informace je pro úlohu prezentační vrstvy nepodstatná.

Proces přidávání hlaviček se opakuje od vrstvy k vrstvě dokud rámec nedosáhne linkovou vrstvu. Zde je kromě linkové hlavičky přidáno i zakončení (trailer). Zakončení

linkové vrstvy obsahuje kontrolní součet a v případě potřeby i výplň. To pomáhá synchronizaci rámců. Rámec je předán dolů fyzické vrstvě, kde je přenesen k přijímajícímu počítači.

V přijímajícím počítači jsou různé hlavičky i zakončení jedna po druhé odstraněny tak, jak rámec stoupá mezi vrstvami a nakonec dospěje k přijímajícímu procesu.

Ačkoliv skutečný přenos dat je vertikální, je každá vrstva naprogramována tak, jakoby byl přenos horizontální. Například když vysílající transportní vrstva dostane zprávu od relační vrstvy, připojí transportní hlavičku a odešle zprávu přijímající transportní vrstvě. Skutečnost, že zpráva vlastně prochází síťovými vrstvami ve vlastním počítači, není důležitá.

Terminologie vertikálního rozhraní v modelu OSI

Kromě definice ideální síťové architektury a síťových funkcí, rozdělených mezi vrstvy, definuje model OSI standardní sadu pravidel, která řídí rozhraní mezi vrstvami.

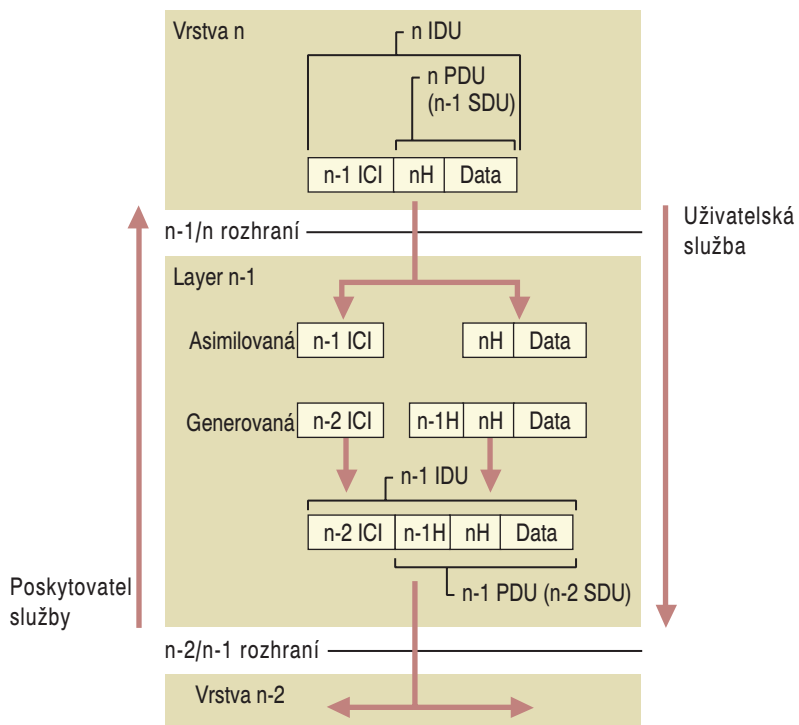
Aktivní prvky protokolu v každé vrstvě se nazývají entity a jsou obvykle implementovány pomocí softwarových procesů. Entity ve stejné vrstvě různých počítačů se nazývají stejnovrstvové entity (*peer entities*). Například sada protokolů TCP/IP obsahuje dvě entity uvnitř své transportní vrstvy: Transmission Control Protocol (TCP) a User Datagram Protocol (UDP).

Vrstva $n-1$, tedy vrstva přímo pod entitami vrstvy n , zavádí služby, které jsou používány vrstvou n .

Pro služby přenosu dat definuje model OSI terminologii pro oddělené součásti dat, předávané přes rozhraní a mezi stejnovrstvovými entitami. Obrázek A.3 ilustruje entity vertikálního rozhraní.

- Entita vrstvy n předává datovou jednotku rozhraní (interface data unit – IDU) entitě vrstvy $n-1$.
- Jednotka IDU se skládá z datové jednotky protokolu (protocol data unit – PDU) a nějaké řídicí informace rozhraní (interface control information – ICI). Řídicími informacemi rozhraní jsou například délka jednotky SDU a adresovací informace, které potřebuje nižší vrstva k vykonávání svých funkcí.
- Jednotka PDU obsahuje data, která chce entita vrstvy n předat po síti své stejnovrstvové entitě. Obsahuje hlavičku vrstvy n a data, která vrstva n přijala od vrstvy $(n+1)$.
- Jednotka PDU vrstvy n se stává služební jednotkou dat (service data unit – SDU) vrstvy $n-1$, protože je tou jednotkou dat, která bude obsloužena vrstvou n .
- Když vrstva $n-1$ přijme jednotku IDU vrstvy n , odstraní a „vezme v úvahu“ řídicí informace ICI, přidá informace do hlavičky pro svou stejnovrstvovou entitu v síti, přidá informace ICI pro nižší vrstvu a předá výslednou jednotku IDU entitě vrstvy $n-2$.

Na datové cestě mezi dvěma síťovými stanicemi se mohou vyskytnout problémy včetně chybné, zkrácené nebo dokonce zastavené komunikace.



Obrázek A.3 Entity vertikálního rozhraní

PŘÍLOHA B

Síťová architektura systému Windows 2000



Síťová architektura systému Microsoft® Windows® 2000 se skládá ze softwarových součástí, které zabezpečují síťové schopnosti operačního systému Windows 2000. Tato příloha popisuje součásti, protokoly a rozhraní uvnitř systému Windows 2000. Navíc zavádí síťové pojmy, které poskytují základ, na kterém stavějí jiné kapitoly v této knize.

V této příloze

Přehled síťové architektury systému Windows 2000 616

Specifikace rozhraní síťového ovladače 618

Síťové protokoly 626

Vrstva rozhraní transportního ovladače 634

Síťová aplikační programová rozhraní 634

Komunikace mezi procesy 646

Základní síťové služby 654

Související informace v Resource Kitu

- Více informací o protokolech SNA naleznete v části „Spolupráce s hostitelskými systémy IBM“ v *Microsoft® Windows® 2000 Server Plánování a implementace sítě*.

Přehled síťové architektury systému Windows 2000

Tato kapitola popisuje softwarové a hardwarové součásti a spojení mezi nimi, jež umožňují počítačům fungovat jako síť. Síťové komponenty systému Windows 2000 jsou uspořádány do vrstev. Každá vrstva vykonává určité úkoly a uvnitř každé vrstvy může podobný úkol vykonávat více součástí.

V následujících odstavcích jsou popsány síťové vrstvy systému Windows 2000 směrem zdola nahoru v modelu síťové architektury. Vrstvy jsou:

Vrstva specifikace rozhraní síťového ovladače (NDIS) Vrstva NDIS je vrstvou, která zajišťuje komunikační cestu ze síťového přenosu k fyzickému zařízení, jakým je například síťový adaptér. Vrstva NDIS vystupuje jako hraniční vrstva mezi síťovým adaptérem a síťovým protokolem a řídí vazby mezi těmito součástmi. Vrstva NDIS přidává podporu pro síťová média orientovaná na spojení, jakými jsou například síť ATM a Integrated Services Digital Network (ISDN) a dále podporuje tradiční síťová média bez spojení, jakými jsou síť Ethernet, Token Ring, a síť s optickými vlákny (Fiber Distributed Data Interface – FDDI). Tato vrstva obsahuje ovladače miniportu, které připojují přímo síťový adaptér.

Vrstva síťového protokolu Síťové protokoly poskytují služby klientům. Tyto služby umožňují aplikacím nebo klientům posílání dat po síti. Síťovými protokoly jsou například TCP/IP, ATM, NWLink, Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), NetBEUI, Infrared Data Association (IrDA), AppleTalk a Data Link Control (DLC). Přidáním serveru Microsoft® SNA Server jsou k dispozici protokoly síťové architektury systému (Systems Network Architecture – SNA).

Vrstva rozhraní transportního ovladače Vrstva rozhraní transportního ovladače (TDI) poskytuje standardní rozhraní mezi síťovými protokoly a klienty těchto protokolů (jako jsou aplikace, síťové přesměrovače nebo síťová aplikační programová rozhraní (API).

Vrstva síťového aplikačního rozhraní Síťové aplikační programové rozhraní (API) obstarává standardní programová rozhraní pro síťové aplikace a služby. Podporují služby Winsock, NetBIOS, rozhraní telefonního subsystému (Telephony API – TAPI), rozhraní zpracování zpráv (Messaging API – MAPI), rozhraní WNet API a další služby.

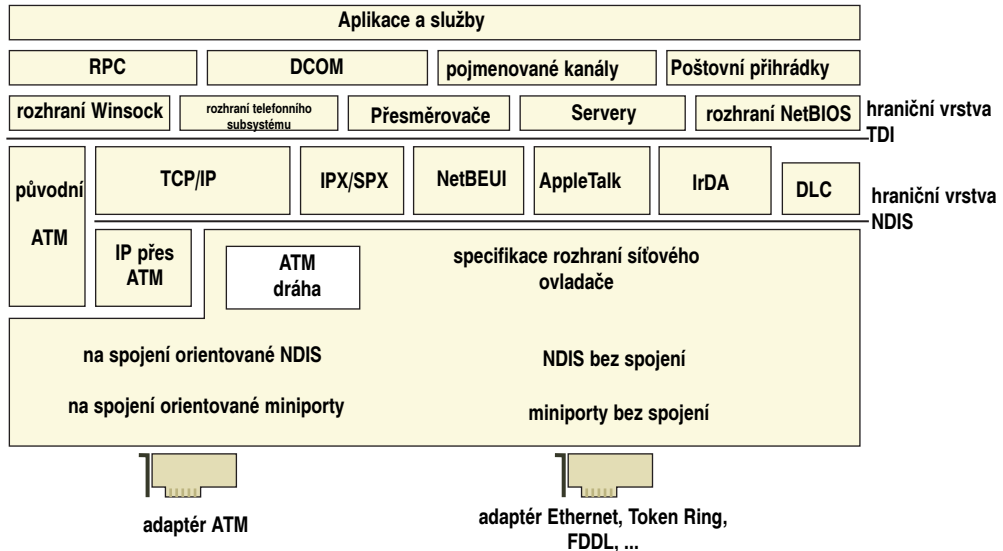
Vrstva komunikace mezi procesy Komunikace mezi procesy (IPC) podporuje výpočty a distribuované zpracování typu klient-server. Některými ze služeb, které podporuje jsou vzdálená volání procedur (RPC), model Distributed Component Object Model (DCOM), pojmenované kanály, poštovní přihrádky a služby protokolu Common Internet File System (CIFS).

Vrstva základních síťových služeb Základní síťové služby podporují uživatelské aplikace zajišťováním služeb. Mezi ně patří správa síťových adres, názvové služby, souborové služby a vyspělé síťové služby jako zabezpečovací služby protokolu Internet Protocol Security (IPSec) a služby Quality of Service (QoS).

Mezinárodní organizace pro standardizaci (ISO) má model pro počítačové sítě, nazvaný referenční model Open Systems Interconnection (OSI). Tento model je užitečný pro popis síťových vrstev. Model OSI definuje modulární přístup k sítím s každou vrstvou zodpovídající za jistý oddělený aspekt síťového procesu. Model OSI se s většinou existujících síťových architektur neshoduje přesně. Nicméně modely pomáhají v pochopení toho, jak sítě fungují tím, že poskytují strukturu, která slouží pro srovnání. Více informací o modelu OSI najdete v příloze Model OSI v této knize.

Síťová komunikace začíná, když se aplikační program pokouší přistupovat k prostředkům na jiném počítači. Data a požadavky se pohybují z vrstvy do vrstvy uvnitř počítače. Každá vrstva je schopná komunikovat s vrstvami bezprostředně nad sebou a bezprostředně pod sebou. Pokud není paket určen pro použití aktuální vrstvou, je předán následující vrstvě. Pakety se pohybují dolů po zásobníku protokolu prvního počítače. Pokud je cíl na jiném počítači v síti, jsou vyslány datové pakety po fyzickém médiu (jakým jsou například vodiče, vláknová optika nebo satelit). Data jsou pak předána směrem nahoru spodními vrstvami druhého počítače stejné vrstvě, která zahájila výměnu dat.

Obrázek B.1 představuje model síťové architektury systému Windows 2000.



Obrázek B.1 Síťová architektura systému Windows 2000

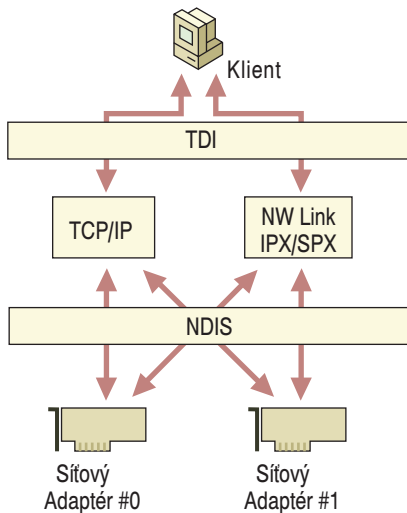
Softwarové součásti jsou znázorněny jako obdélníky. Tyto součásti jsou v horizontálních vrstvách. Součásti, které jsou ve stejné horizontální vrstvě, zajišťují podobnou funkčnost. Nejvyšší vrstva diagramu je místem, kde sídlí uživatelské aplikace. Aby bylo možné komunikovat s jinými počítači v síti, je potřebná další softwarová a hardwarová podpora. Každá vrstva pod aplikační vrstvou poskytuje služby, které jsou nezbytné pro vytváření paketů dat, zařízení jejich doručení a jejich zaslání po fyzickém médiu jinému počítači.

Hraniční vrstvy jsou rozhraními mezi funkčními vrstvami v síťovém modelu systému Windows 2000. Vytvoření hraničních vrstev jako bodů přerušení v síťových vrstvách pomáhá standardizovat programování pro vývojáře. Protože funkčnost mezi vrstvami je dobře definována, stačí, když vývojáři programují pouze k hraniční vrstvě namísto toho, aby museli kódovat vše odshora (aplikační program) dolů v zásobníku protokolu (síťový adaptér). Pokud je software korektně napsán k hraniční vrstvě, existuje již podpora na opačné straně této vrstvy a není třeba ji znovu psát. Hraničními vrstvami jsou rozhraní transportního ovladače (TDI) a vrstva specifikace rozhraní síťového ovladače (NDIS). V diagramu je mezera mezi horní hranou DLC a Native ATM a vrstvou TDI, protože se nepřipojují přes vrstvu TDI.

Vazba je spojení síťových komponent v sousedících vrstvách zásobníku protokolu. Vazby se vyskytují v hraničních vrstvách a jiných sousedících vrstvách. Vazby umožňují komunikaci mezi různými vrstvami.

Součástí jsou části softwaru, které vykonávají určité úkoly. Síťové součásti se mohou vázat k jedné nebo více síťovým součástem nad sebou nebo pod sebou. Při přidávání síťového softwaru svazuje systém Windows 2000 všechny potřebné spojené součásti dohromady. Během svazování obsahuje informační soubor (.inf) instrukce, nezbytné pro sestavení požadovaných vazebních vztahů.

Obrázek B.2 ukazuje vazbu dvou protokolů ke dvěma síťovým adaptérům uvnitř jednoho počítače.



Obrázek B.2 Vazba

Specifikace rozhraní síťového ovladače

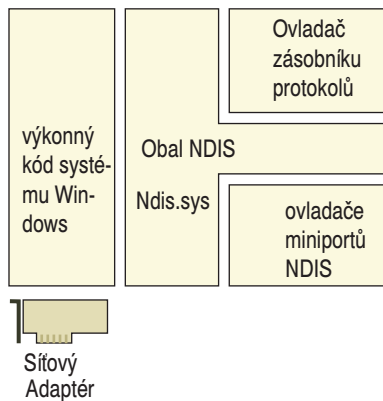
Specifikace rozhraní síťového ovladače (NDIS) je specifikací architektury síťového ovladače, která umožňuje transportním protokolům, jako jsou TCP/IP, Native ATM, IPX, a NetBEUI, komunikovat se síťovými adaptéry dalším hardwarovým zařízením v nižší vrstvě. Síťový adaptér pak může odesílat nebo přijímat data po síti. Vrstva NDIS dovolu je součástí protokolů vyšších úrovní být nezávislé na síťovém adaptéru, protože poskytuje síťovým protokolům standardní rozhraní. Protože síťová architektura systému Windows 2000 podporuje specifikaci NDIS, vyžaduje, aby ovladače síťových adaptérů byly napsány podle specifikace NDIS.

Vrstva NDIS v systému Windows 2000 poskytuje standardní rozhraní bez spojení a definuje i rozhraní orientované na spojení. Síťová architektura systému Microsoft® Windows NT® verze 4.0 podporovala tradiční síťové standardy bez spojení, jako například Ethernet, Token Ring, a FDDI. Síť bez spojení neprovádějí sjednání, správu a údržbu spojení před přenosem dat. Síť bez spojení, rovněž známé jako datagramová služba, jsou doručovací službou s „nejlepší snahou“ (best-effort). Není zde žádná záruka, že se zprávy nebudou ztraceny, duplikovány nebo doručeny v nesprávném pořadí. Tyto služby jsou obvykle poskytovány na vyžádání síťovým protokolem.

Systém Windows 2000 dále podporuje tradiční síť bez spojení, ale navíc přidává podporu pro média, orientovaná na spojení, jako například asynchronní režim přenosu (ATM) a síť Integrated Services Digital Network (ISDN). V sítích orientovaných na spojení je vytvořeno spojení a všechna data jsou odeslána po virtuálním okruhu. Systém Windows 2000 sjednává spojení použitím správce volání. Správce volání je softwarová součást, která dokáže vytvořit a udržovat spojení vytvářením virtuálních okruhů (VC) mezi dvěma koncovými body sítě. Virtuální okruh vystupuje jako cesta pro přenos dat, umožňující větší ovládání šířky pásma, zpoždění, střídání prodlev a řazení. Tyto služby dávají větší podporu pro distribuované hlasové, datové a obrazové aplikace.

Vrstva NDIS je v systému Windows 2000 implementována souborem, nazvaným Ndis.sys, který je označován jako „obal NDIS“. Obal NDIS je kód, který obklopuje všechny ovladače zařízení NDIS. Obal NDIS poskytuje jednotné rozhraní mezi ovladači protokolu a ovladači zařízení NDIS, a obsahuje podpůrné rutiny, které usnadňují vývoj ovladačů NDIS. Specifikace NDIS povoluje neomezené množství síťových adaptérů v počítači a neomezené množství protokolů, svázaných s jedním nebo více síťovými adaptéry.

Obrázek B.3 ukazuje architekturu obalu NDIS.



Obrázek B.3 Obal NDIS (Ndis.sys)

Obal NDIS definuje způsob, kterým protokoly komunikují se síťovými adaptéry. Protokoly komunikují s obalem NDIS místo komunikace se síťovým adaptérem. Toto je příkladem modulární struktury vrstveného síťového modelu. Síťový adaptér je nezávislý na transportních protokolech.

Nové vlastnosti specifikace NDIS

Specifikace NDIS v systému Windows 2000 obsahuje mnoho nových vlastností, jako například podporu sítí orientovaných na spojení a novou podporu zprostředkujících ovladačů a ovladačů miniportu. K dalším vlastnostem specifikace NDIS v systému 2000 patří:

- Na spojení orientovaná specifikace NDIS
- Režim Wake-On-LAN
- Detekce média
- Síť k okamžitému použití
- Snižování zátěže sítě TCP/IP

Na spojení orientovaná specifikace NDIS

Na spojení orientovaná specifikace NDIS (CoNDIS) je část specifikace NDIS, která podporuje média, orientovaná na spojení, jako například síť s vytáčenou linkou, síť ATM a síťové toky médií orientovanými na spojení. Na spojení orientovaná specifikace NDIS poskytuje podporu pro zřízení, údržbu a ukončení spojení.

Režim Wake-On-LAN

Režim Wake-On-LAN ovládání zapínání počítačů podle událostí v síti. Je to podmnožina systému řízení spotřeby OnNow Power Options Initiative. Aby mohl režim Wake-On-LAN fungovat, musí síťové adaptéry umožňovat provoz v tomto režimu a ovladače zařízení musí tento režim podporovat. Síťový adaptér může být uveden do režimu nízké spotřeby, když systém vyžaduje změnu energetické úrovně. Tento požadavek může spustit uživatel nebo systém. Například uživatel může chtít uvést systém do úsporného režimu nebo může úsporný režim vyžádat systém na základě aktivit myši a klávesnice.

Pokud je zahájen uživatelem, musí nejdříve s požadavkem souhlasit všechny síťové součásti ve vyšších vrstvách, než může být vypnut síťový adaptér. Pokud jsou v síti nějaké aktivní relace nebo otevřené soubory, může být požadavek na vypnutí odmítnut některou nebo všemi zúčastněnými součástmi.

Mnoho událostí umožňuje systému, aby se probudil z úsporného režimu bez zásahu uživatele. Systém může být schopen probouzet se z úsporného režimu podle síťových událostí, určených síťovým softwarem. Tato schopnost znamená, že každý standardní přístup k síti v systému Windows (například připojení ke sdíleným složkám, aplikace poskytující služby a správu) může probudit systém z úsporného režimu. To se stane při:

- příjmu dříve zaregistrovaného paketu.
- příjmu paketu Magic. Paket Magic je paket, který obsahuje 16 souvislých kopií adresy přijímajícího adaptéru Ethernet.
- události spojení, jakou je například zapojení síťového kabelu.

Síťové adaptéry a hardware, které nepodporují režim Wake-On-LAN, mohou být v systému Windows 2000 nadále používány. Systémy, mající adaptéry bez podpory režimu Wake-On-LAN mohou být pozastaveny nebo obnoveny podle uživatelské aktivity, ale nemohou být obnoveny podle síťových událostí.

Detekce média

Detekce média je schopnost síťového adaptéru oznamovat, kdy má nebo nemá spojení s fyzickým síťovým médiem. Většina síťových technologií systému Windows 2000 podporuje detekci média. Protokoly a aplikace mohou přijímat tato oznámení a podle toho se chovat. Například může být zobrazena ikona, označující, že médium je odpojeno, může být zaznamenána událost a protokol TCP/IP může spravovat adresy se znalostí stavu sítě.

Sít' k okamžitému použití

Sít' k okamžitému použití je kombinací hardwarové a softwarové podpory, která umožňuje počítačovému systému rozpoznat a přizpůsobit změny nastavení hardware s malými nebo žádnými zásahy uživatele. Uživatel může přidávat nebo odebírat zařízení k okamžitému použití dynamicky. Není nutná znalost spletností počítačového hardwaru. Například může uživatel umístit přenosný počítač do doku a použít adaptér Ether-

net doku k připojení k síti beze změny nastavení. Později může uživatel též počítač vyjmout z doku a použít k síťovému připojení modem, opět bez nutnosti provádět manuální změny nastavení.

Snižování zátěže sítě TCP/IP

Snižování zátěže sítě TCP/IP umožňuje úkolům, normálně prováděným transportní vrstvou, aby byly zpracovávány síťovým adaptérem. To snižuje režii systémové jednotky CPU, požadovanou pro tyto úkoly. To umožňuje systémové jednotce CPU vykonat více práce, eventuálně zvýšit propustnost sítě. Transportní ovladač pokládá zvláštní dotaz, kterým zjišťuje, zda síťový adaptér podporuje snižování zátěže výpočtů kontrolních součtů TCP/IP, segmentace TCP/IP, služby Fast Packet Forwarding a snižování zátěže zabezpečení IPSec. Pokud je zjištěna některá z těchto podmínek, může transport požádat síťový adaptér o zařazení těchto služeb.

Snižování zátěže výpočtů kontrolních součtů TCP/IP

Kontrolní součty TCP/IP ověřují integritu datového paketu. Protokol TCP/IP pokládá dotaz miniportu, aby zjistil jeho schopnost provádět výpočty kontrolních součtů. Pokud je miniport schopen zpracovávat snižování zátěže, provádí tyto výpočty. Tyto výpočty mohou spotřebovávat mnoho cyklů jednotky CPU. Mohou zahrnovat vysílání a příjem výpočtů kontrolních součtů pro protokoly TCP, User Datagram Protocol (UDP) a IP. Ovladač miniportu vyžaduje, aby tyto výpočty prováděl síťový adaptér místo vyžadování zpracování těchto požadavků jednotkou CPU. Výsledkem může být zlepšení výkonu.

Snižování zátěže segmentace TCP/IP

Segmentace TCP/IP (zasílání rozsáhlých dat) je vytváření paketů TCP z dat, která jsou příliš objemná pro přenos síťovým médiem. Protokol TCP/IP rozděluje data do malých segmentů, přidává hlavičky IP a TCP a vytváří pakety TCP. Segmentace TCP/IP může být nyní provedena miniporty NDIS a způsobilým síťovým adaptérem. Adaptér musí být schopen vypočítat kontrolní součty IP a TCP pro odesílané pakety a mít příslušný ovladač miniportu. Snižování zátěže jednotky CPU těmito výpočty má za následek větší výkon systému.

Služba Fast Packet Forwarding

Služba Fast Packet Forwarding umožňuje multiportovým síťovým adaptéřům (FastEthernet, FDDI nebo podobné jednoportové síťové adaptéry) používat systém Windows 2000 ke směrování paketů z jednoho portu do druhého bez předávání paketu hostitelskému procesoru. To zvyšuje průchodnost sítě a snižuje práci pro jednotku CPU.

Snižování zátěže zabezpečení IPSec

Zabezpečení Internet Protocol Security (IPSec) je standardem společenství Internet Engineering Task Force (IETF) pro zabezpečení ve vrstvách zpracování paketů v sítích IP. Zabezpečení IPSec zajišťuje dvě zabezpečovací služby:

- Ověřovací hlavička. Umožňuje ověřování odesílatele.
- Protokol Encapsulating Security Payload. Podporuje ověřování odesílatele i šifrování dat.

Informace protokolu IPSec, přiřazené každou z těchto služeb, jsou vloženy do paketu v hlavičce, která následuje za řádnou hlavičkou IP. V těchto informacích je zahrnut i in-

dex parametrů zabezpečení, což je 32bitová hodnota používaná k rozlišení mezi různými přidruženími zabezpečení, končícími ve stejném místě určení a používajícími stejný protokol IPSec.

Práce se šifrováním a dešifrováním každého paketu může být přiřazena síťovému adaptéru použitým vrstvy NDIS a přiřazených ovladačů miniportu. Správným nastavením zásad zabezpečení systému Windows 2000 jsou odcházející pakety IP ověřovány a šifrovány před přenosem do sítě a přicházející pakety IP jsou uznány a dešifrovány.

Pro více informací o nových vlastnostech vrstvy NDIS viz Platform Software Development Kit (SDK). Pro více informací o zabezpečení IPSec viz „Zabezpečení protokolu IPI“ v této knize.

Typy ovladačů rozhraní NDIS

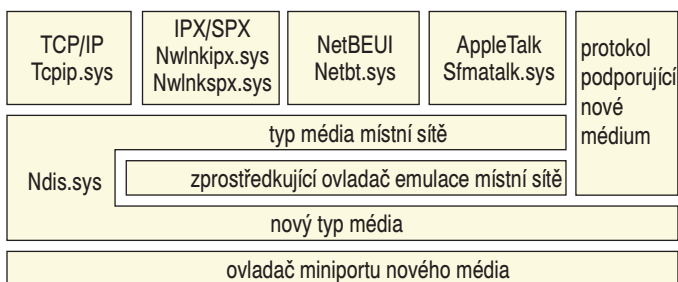
Ovladače rozhraní NDIS umožňují transportním protokolům komunikovat s hardwarovou vrstvou. Tyto ovladače mohou být zavedeny v různých nastaveních, popsaných v následujících odstavcích.

Zprostředkující ovladače

Zprostředkující ovladače se nacházejí přímo pod transportním protokolem a nad ovladači miniportů v zásobníku protokolů sítě. Existují dva typy používaných zprostředkujících ovladačů: zprostředkující ovladač emulace místní sítě a ovladač filtru.

Zprostředkující ovladač emulace místní sítě

Zprostředkující ovladač emulace místní sítě překládá pakety z formátu přenosu bez spojení místní sítě ve vyšších vrstvách do formátu orientovaného na spojení (jakým je například ATM) v nižších vrstvách. Proto se zdá, že transportní protokoly komunikují se síťovým adaptérem místní sítě (LAN), ale ve skutečnosti komunikují s jiným hardwarovým zařízením. Zprostředkující ovladač emulace místní sítě překládá přicházející a odcházející pakety pro protokolovou vrstvu výše. Převádí tyto pakety na pakety, které mohou být poslány jiným médiem. Obrázek B.4 ilustruje architekturu zprostředkujícího ovladače emulace místní sítě.



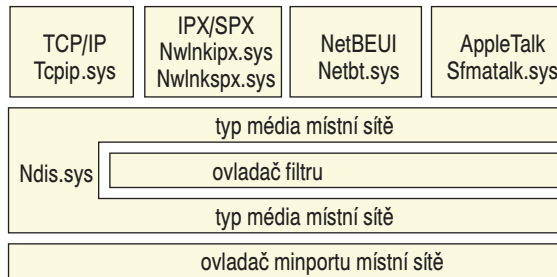
Obrázek B.4 Zprostředkující ovladač emulace místní sítě

V současné době je jedinou podporovanou aplikací pro tento ovladač emulace místní sítě pro ATM. Tato konfigurace ovladačů však může být v budoucnosti použita pro jiné typy nových médií.

Pro více informací o rozhraní NDIS viz Platform Software Development Kit (SDK).

Ovladač filtru

Ovladače filtrů provádějí zvláštní operace (jako například komprimace, šifrování a sledování) s pakety, které jsou přes ně transportovány. Obrázek B.5 ukazuje architekturu ovladače filtru.



Obrázek B.5 Ovladač filtru

Při transportu paketu ovladačem filtru může být provedena komprimace a šifrování. Tohoto typu zprostředkujícího ovladače využívá několik služeb, například plánovač paketů ve službě Quality of Service (QoS) a vyvažování zatížení sítě.

Ovladače miniportů

Ovladač miniportu je ovladač, který připojuje hardwarová zařízení k zásobníku protokolů. Ovladač miniportu je připojen ke zprostředkujícímu ovladači nebo ovladači protokolu a k hardwarovému zařízení. Ovladač miniportu zpracovává operace, specifické pro hardware, které jsou nezbytné pro řízení síťového adaptéru nebo jiného hardwarového zařízení. Uskutečňují odesílání a příjem dat v síťovém adaptéru. Společnost Microsoft přináší několik zprostředkujících ovladačů pro systém Windows 2000. To pomáhá výrobcům hardwaru, protože není nezbytné zavádět přídavnou funkčnost. Pro přidání další funkčnosti mohou dodavatelé hardwaru rovněž vytvářet zprostředkující ovladače. V této kapitole jsou ovladače miniportů označovány také jako miniporty.

Model Windows Driver Model (WDM) je specifikací pro ovladače zařízení. Model WDM činí kompatibilními ovladače zařízení systémů Windows 2000 a Microsoft® Windows® 98. Aby pomohl snížit námahu, nezbytně vynaloženou dodavateli hardwaru pro podporu všech platform Windows, umožňuje model WDM, aby zařízení navržená pro jeden ze systémů Windows 2000 nebo Windows 98 byla instalována a používána v počítačích s druhým z těchto systémů. Návrháři, používající model WDM, vytvářejí malé části kódu (miniporty), které hovoří přímo s jejich hardwarem a volají příslušné ovladače třídy pro většinu obecných úkolů.

Ovladače miniportů mohou být serializované nebo deserializované. Serializované ovladače spoléhají na rozhraní NDIS při řazení volání funkcí miniportu a při správě jejich front. Deserializované ovladače miniportů v systémech s více procesory mohou pracovat rychleji serializací přístupů ke svým vnitřním datovým strukturám místo toho, aby umožnily tuto funkci provádět rozhraním NDIS. Zařazují rovněž všechny příchozí pa-

kety pro odeslání do front místo využívání rozhraní NDIS. To může mít za následek lepší výkon plného duplexu. Deserializované ovladače miniportů jsou však obtížnější při návrhu a vyžadují více testování a ladění.

Obvyklé ovladače miniportů

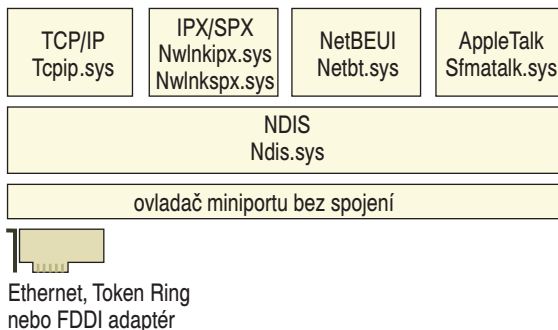
Nejběžnějšími ovladači miniportů jsou:

- Ovladače miniportů bez spojení
- Ovladače miniportů rozhraní NDISWAN
- Ovladače miniportů nižších rozhraní mimo NDIS
- Ovladače miniportů orientované na spojení

Ovladače miniportů bez spojení

Ovladače miniportů bez spojení řídí síťové adaptéry pro média bez spojení, jakými jsou síť Ethernet, FDDI a Token Ring.

Obrázek B.6 ukazuje architekturu ovladačů miniportů bez spojení.



Obrázek B.6 Architektura ovladače miniportu bez spojení

Nejobvyklejší využití miniportů bez spojení je u síťových adaptérů místních sítí (LAN). Síťová média jako Ethernet, Token Ring a FDDI nepodporují komunikace orientované na spojení. Pakety jsou přijímány a odesílány na místo určení bez existujícího spojení.

Ovladače miniportů rozhraní NDISWAN

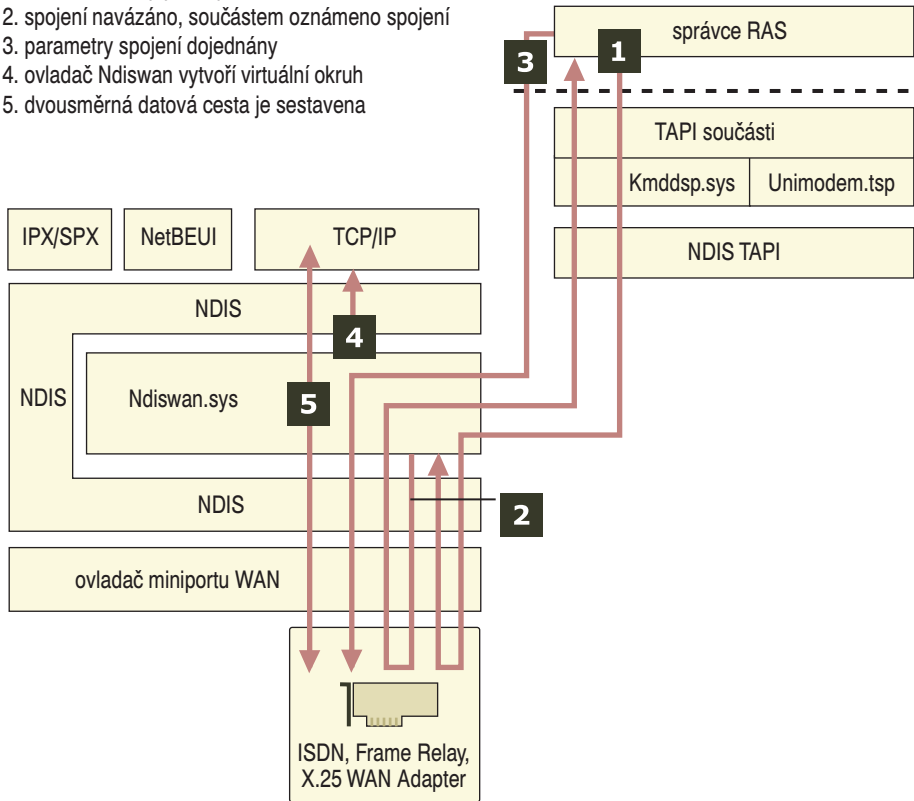
Existuje mnoho typů miniportů rozhraní NDISWAN. Miniporty rozhraní NDISWAN se používají u linek ISDN, Frame Relay a X.25 k vytvoření sítí s vytáčenou linkou. Soubor Ndiswan.sys je ovladač společnosti Microsoft, který zajišťuje protokol Point-to-Point Protocol (zapouzdření PPP), kompresi a šifrování. Ovladač Ndiswan.sys komunikuje se službou Routing and Remote Access.

Obrázek B.7 ilustruje architekturu a použití ovladače miniportu rozhraní NDISWAN.

Obrázek B.7 ukazuje příklad použití rozhraní NDISWAN. Očíslované šipky ukazují kroky, kterými služba Routing and Remote Access nastavuje relaci PPP použitím ovladače miniportu rozhraní NDISWAN.

1. Služba Routing and Remote Access zahajuje spojení předáním informací dolů přes součásti rozhraní TAPI, (kmddsp.tsp, NDIS TAPI) ovladači miniportu rozhraní WAN (NDISWAN).

1. API RAS zahajuje spojení
2. spojení navázáno, součástíem oznámeno spojení
3. parametry spojení dojednány
4. ovladač Ndiswan vytvoří virtuální okruh
5. dvousměrná datová cesta je sestavena

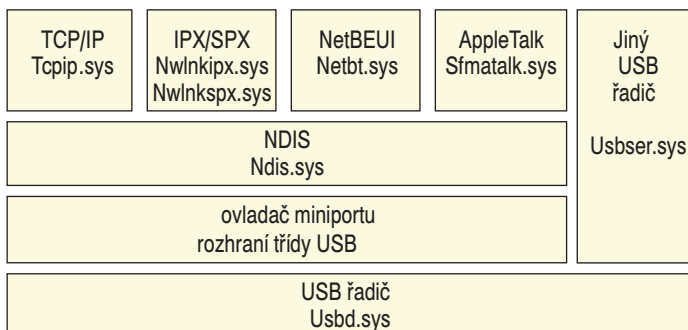


Obrázek B.7 Architektura a použití ovladače miniportu rozhraní NDISWAN

2. Stejnou cestou je předána zpět službě Routing and Remote Access odpověď, aby ji informovala že bylo sestaveno spojení. Všechny součásti jsou upozorněny, že byl dokončen pokus o volání.
3. Správce služby vzdáleného přístupu (RAS Manager) dojedná parametry spojení PPP. Ty zahrnují kompresní protokoly a typy rámců.
4. Ovladač Ndiswan.sys vytvoří virtuální okruh pro příslušný protokol.
5. Data jsou poslána a přijata spojením, které bylo sestaveno ovladačem Ndiswan.sys.

Ovladač miniportů nižších rozhraní mimo NDIS

Ovladač miniportů nižších rozhraní mimo NDIS je ovladač miniportu orientovaný na spojení, který propojuje síťové protokoly nahoře, ale dole může propojovat zařízení, jako například zařízení sběrnice Universal Serial Bus (USB) a zařízení IEEE 1394. Obrázek B.8 ukazuje architekturu ovladače miniportů mimo NDIS.



Obrázek B.8 Architektura ovladače miniportů mimo NDIS

Miniporty orientované na spojení

Miniporty orientované na spojení přenášejí data po určitém spojení a nikoliv do určitého cíle. Je to nová architektura ovladačů vrstvy NDIS. Miniporty orientované na spojení se liší od miniportů bez spojení tím, že před výměnou dat musí být ustaveno spojení mezi dvěma body. Miniporty orientované na spojení podporují média jako je síť ATM.

Některé aplikace se spoléhají na komunikaci orientovanou na spojení. Protože data jsou posílána po spojení, zůstávají ve správném pořadí a všechna data sledují stejnou cestu. Protože jdou všechna data po stejné cestě, mohou být parametry QoS ovládány snáze než u přenosu dat bez spojení. Správce volání sjedná požadavky kvality služby (QoS) pro spojení, pokud médium podporuje QoS. Správci volání vytvářejí a udržují spojení. Existují dva typy správců volání:

- Samostatný správce volání je samostatná softwarová entita, oddělená od ovladače miniportu.
- Kód integrovaného správců volání je integrální částí ovladače miniportu orientovaného na spojení.

Miniporty orientované na spojení podporují mnoho typů přenosu dat. Ovladače miniportů orientované na spojení umožňují datové přenosy, hlasové přenosy a videokonference, používající proudy dat. Rozhraní NDIS může snížit zátěž ovladače miniportu při synchronizaci a řízení front. Ovladače miniportů orientované na spojení mohou vystavovat spojení pro síťové protokoly. Diagram a další informace o ovladačích miniportů orientovaných na spojení, podporujících síť ATM naleznete v části „Protokol ATM“ dále v této kapitole.

Síťové protokoly

Protokoly jsou specifikace pro standardizované pakety dat, které sítím umožňují sdílení informací. Systém Windows 2000 podporuje mnoho různých protokolů. Pakety informací jsou přesouvány nahoru a dolů po zásobníku protokolů a napříč přenosovým médiem. Mezi síťové protokoly patří:

- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Asynchronous Transfer Mode (ATM)
- NetWare Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

- NetBIOS Enhanced User Interface (NetBEUI)
- AppleTalk
- Data Link Control (DLC)
- Infrared Data Association (IrDA)

Poznámka: Protokoly síťové architektury systému (SNA) nejsou zahrnuty do systému Windows 2000. Protokoly SNA jsou dostupné po přidání serveru Microsoft SNA Server. Microsoft SNA Server je samostatný produkt, který podporuje spolupráci s minipočítači a sálóvými počítači IBM. Více informací o protokolech SNA najdete v části „Spolupráce s hostitelskými systémy IBM“ v knize *Microsoft® Windows® 2000 Server Inter-networking*.

TCP/IP

Protokol Transmission Control Protocol/Internet Protocol (TCP/IP) byl přijat společností Microsoft jako strategický podnikový transportní protokol pro systém Windows 2000. Sada protokolů TCP/IP systému Windows 2000 je navržena pro usnadnění integrace podnikových sítí Microsoft do velkých sítí společností, vládních sítí a veřejných sítí a pro poskytnutí schopnosti provozovat tyto sítě bezpečným způsobem.

Několik faktorů vedlo k úspěchu protokolu TCP/IP. Tento Protokol je směrovatelný, což znamená, že datové pakety mohou být přepínány (směřovány do jiné podsítě) použitím cílové adresy paketu. Schopnost být směrován umožňuje protokolu TCP/IP větší odolnost proti chybám. Pokud dojde k chybě sítě, pakety jsou transportovány jinou trasou. Jiný faktor, který přispívá k úspěchu protokolu TCP/IP je masivní zájem o Internet. Protokol TCP/IP je standardem pro vzájemné propojování počítačů.

Protokol TCP/IP systému Windows 2000 obsahuje několik vylepšení výkonu pro vytváření sítí v prostředí místních sítí se širokým přenosovým pásmem a v prostředích rozlehlých sítí (WAN). K těmto znakům patří:

Podpora velkých oken

Podpora velkých oken zlepšuje výkon protokolu TCP/IP, když jsou mezi dvěma spoji velké objemy dat na cestě nebo nepotvrzeny. V komunikaci založené na protokolu TCP je velikost okna maximálním počtem paketů, které mohou být odeslány v řadě v proudě dat předtím, než musí být první paket potvrzen. Podpora velkých oken umožňuje, aby bylo na cestě v síti více datových paketů najednou a zvyšuje efektivní šířku pásma.

Selektivní potvrzování

Selektivní potvrzování je možnost protokolu TCP, která umožňuje příjemci selektivně oznamovat a vyžadovat od vysílače jen ty pakety, které chyběly nebo byly porušeny během prvního doručení. Selektivní potvrzování umožňuje sítím rychlé zotavení ze stavu přetížení nebo dočasné poruchy vyžadováním opětovného vyslání pouze ztracených paketů. Pokud v předchozích implementacích protokolu TCP/IP nepřijal příjemce hostitelský počítač jediný paket, nemohl vysílač poslat znovu pouze porušený nebo chybějící paket, ale všechny následující pakety. Se selektivním potvrzováním se posílá méně paketů což vede k lepšímu využití sítě..

Odhad času okružní cesty

Odhad času okružní cesty (RTT) je technika odhadu časů přenosu paketu a přizpůsobení pro optimální časy opakovaných přenosů paketů. Čas okružní cesty je doba, kterou trvá okružní komunikace mezi vysílačem a přijímačem po spojení, založeném na protokolu TCP. Protože výkon závisí na znalosti, jak dlouho se má čekat na scházející paket, zlepšení přesnosti odhadu RTT vede k lepšímu nastavení hodnot časových prodlev opakovaných přenosů pro každý hostitelský počítač. Lepší časování mimofradně zlepšuje výkon u dlouhých okružních síťových spojení, jakými jsou síť WAN, které se rozpínají na velké vzdálenosti (mezikontinentální) nebo používají buď bezdrátových nebo satelitních spojů.

Zabezpečení protokolu IP

Zabezpečení protokolu IP (IPSec) je šifrovací proces, který umožňuje zakódování dat tak, že je prakticky nemožné prohlížet jejich obsah. Zabezpečení IPSec používá kryptografické zabezpečení k zajištění integrity, ověření původu dat, ochranu proti znovupřehrávání, důvěrnost a omezenou důvěrnost toku provozu. Protože zabezpečení IPSec je poskytováno vrstvou IP, jeho služby jsou dostupné protokolům ve vyšších úrovních zásobníku a jsou transparentně dostupné existujícím aplikacím.

Zabezpečení IPSec umožňuje systému vybírat zabezpečovací protokoly, určovat, které algoritmy budou použity pro službu a nastavit a spravovat kryptografické klíče pro každý zabezpečený vztah. Zabezpečení IPSec může chránit cesty mezi hostitelskými počítači, mezi bezpečnostními branami nebo mezi hostitelskými počítači a bezpečnostními branami. Zásady zabezpečení IPSec mohou být nastaveny místně v počítači nebo mohou být přiřazeny prostřednictvím mechanismu zásad skupiny systému Windows 2000 použitím adresářové služby Active Directory™.

Když je použito zabezpečení IPSec k šifrování dat, dochází obecně ke snížení výkonu sítě zvýšením režie na šifrování. Jednou z metod snížení režie je snižování zatížení přenosem zpracování na hardwarové zařízení. Protože rozhraní NDIS podporuje snižování zátěže, je možné zahrnout šifrovací hardware do síťových adaptérů.

Více informací o zabezpečení IPSec najdete v části „Zabezpečení protokolu IP“ v této knize.

Více informací o protokolu TCP/IP najdete v části „Úvod do TCP/IP“ a „Windows 2000 TCP/IP“ v této knize.

Obecná kvalita služby

Obecná kvalita služby (Generic Quality of Service – GQoS) je implementována v rozhraní Winsock, takže obecná kvalita služby systému Windows 2000 může být spuštěna na každé síti, která podporuje protokol TCP/IP. Služba GQoS zajišťuje kvalitu spojení a umožňuje vývojářům rozmístit aplikace pracující v reálném čase po sítích IP, když poskytují přijatelnou úroveň šířky pásma, zpoždění a kolísání. Služba GQoS umožňuje protokolu TCP/IP poskytovat výhody sítí ATM v prostředí TCP/IP.

Více informací o službě QoS najdete v části „Obecná kvalita služby“ v této knize.

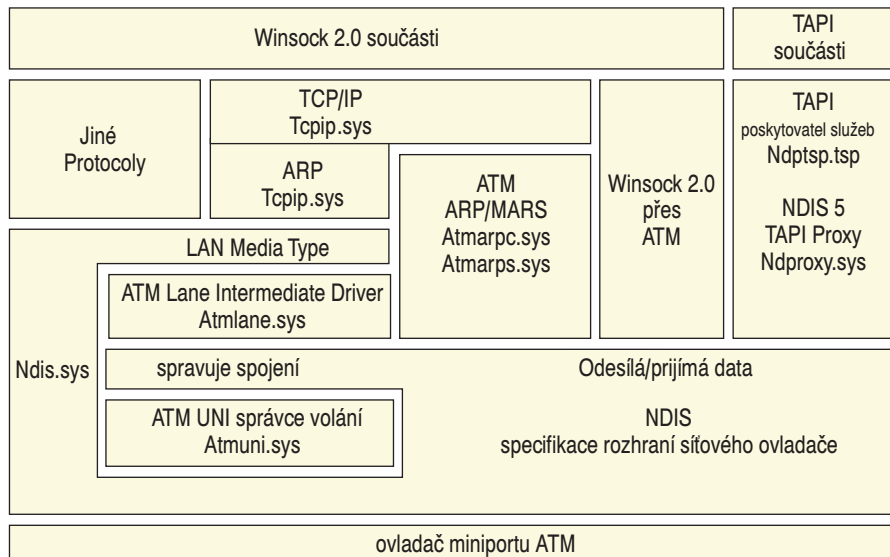
Protokol ATM

Protokol asynchronního režimu přenosu (ATM) je protokol orientovaný na spojení, který je ideální pro hlasové, obrazové a datové komunikace. Protokol ATM je vysokorychlostní síťová technologie, která přenáší data v buňkách pevné délky. Protokol ATM je

přirozený transportní protokol orientovaný na spojení. Je složen z množství příbuzných technologií včetně softwaru, hardwaru a média, orientovaného na spojení. Buňka je paket pevné délky, obsahující 53 bajtů informací. Protože počet bajtů buňky – a v důsledku toho i čas přenosu – je konstantní, mohou být buňky přepínány v konstantním intervalu.

Koncový bod v protokolu ATM sestavuje spojení nebo virtuální okruh před odesláním jakýchkoli dat do sítě. Poté posílá buňky po této cestě k cíli. Tento virtuální okruh je přímou cestou z jednoho koncového bodu do jiného. Zatímco sestavuje spojení, dohaduje koncový bod ATM také smlouvu o kvalitě služby pro přenos. Tato smlouva detailně popisuje šířku pásma, maximální zpoždění, přijatelnou odchylku a další parametry virtuálního okruhu a tato smlouva se šíří od jednoho koncového bodu do druhého. Protože virtuální okruh je orientovaný na spojení, data dorazí do přijímajícího konce ve správném pořadí a se specifikovanou úrovní služeb. Protokol ATM je skvělým kompromisem pro přenos hlasu a dat po síti. Protokol ATM poskytuje zaručenou kvalitu služby v místních sítích LAN, rozlehlých sítích WAN a ve veřejných propojených sítích.

Obrázek B.9 ilustruje architekturu ovladače miniportu orientovaného na spojení, jak je implementován v protokolu ATM.



Obrázek B.9 Použití miniportů orientovaných na spojení v protokolu ATM

Protokol ATM je podporován architekturou systému Windows 2000 následujícími součástmi. Tento diagram je použit pro:

- LANE (emulace místní síť LAN)
- protokol IP over ATM
- protokol PPP over ATM
- původní protokol ATM prostřednictvím rozhraní Winsock 2.0

Více informací o protokolu ATM naleznete v části „Asynchronní režim přenosu“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Emulace místní sítě Lan (LANE) Emulace místní sítě Lan (LANE) je metoda, kterou ostatní protokoly (nejen TCP/IP), které si rozumí jen s médii bez spojení, mohou komunikovat přes protokol ATM. Umožňuje protokolu ATM používat starší verze sítí i aplikací. Tradiční aplikace a protokoly místních sítí LAN mohou komunikovat přes síť ATM bez modifikací.

Emulace LANE se skládá ze dvou primárních součástí: klienta LANE (Atmlane.sys) a služeb LANE. Klient LANE umožňuje protokolům a aplikacím místních sítí LAN fungovat tak, jako by komunikovaly s tradiční místní sítí LAN. Klient LANE předává příkazy místní sítě LAN síťovým protokolům a původní příkazy ATM vrstvě protokolu ATM. Služby LANE jsou skupinou součástí protokolu ATM, obvykle na přepínači, který podporuje emulaci místní sítě LAN.

Protokol IP Over ATM Protokol IP over ATM je nástrojem přenosu paketů IP přes síť ATM. Protokol IP over ATM používá vlastnosti orientované na spojení protokolu ATM, aby překonal povahu bez spojení protokolu IP. Funguje podobným způsobem jako emulace LANE. Centrální server IP (zvaný server ATMARP) spravuje databázi adres IP a adres ATM a poskytuje konfigurační a vysílací služby. Protokol IP over ATM je skupinou součástí, které nesídlí v jednom místě. Služby nejsou obvykle na přepínači ATM. Služby serveru protokolu IP over ATM jsou poskytovány systémem Windows 2000 a mohou sídlit na systémovém serveru Windows 2000.

Protokol IP over ATM je malou vrstvou mezi protokolem ATM a protokoly TCP/IP. Klient emuluje standardní protokol IP protokolu TCP/IP nad sebou a používá původní příkazy ATM pro nižší vrstvy protokolu ATM.

Protokol IP over ATM je ovládán dvěma primárními součástmi: serverem protokolu IP over ATM (Atmarps.sys) a klientem protokolu IP over ATM (Atmarpc.sys). Server protokolu IP over ATM je složen ze serveru ATMARP a služby překládání adres vícesměrového vysílání (Multicast Address Resolution Service – MARS). Server ATMARP poskytuje služby, které emulují standardní funkce protokolu IP, zatímco služby MARS poskytují služby všesměrového a vícesměrového vysílání. Obě služby udržují databáze adres IP.

Protokol ATM Over xDSL Technologie digitální účastnické linky (Digital Subscriber Line – xDSL) je prostředek, pomocí něhož může být použita jednoduchá stará telefonní služba (POTS) k posílání buněk protokolu ATM párem měděných vodičů do ústředny telefonní společnosti. Protokol ATM over xDSL nabízí vysokorychlostní přístup k síti z domova a z prostředí malé kanceláře. V těchto oblastech bylo vyvinuto několik standardů, včetně asymetrické digitální účastnické linky (ADSL) a univerzální linky ADSL (UADSL). Tyto technologie používají lokální smyčku, měděné vodiče, které spojují místní ústřednu v sousedství uživatele a telefonní přípojku zákazníka. V mnoha oblastech je tato smyčka připojen přímo k jádru ATM sítě, provozované telefonní společností.

Služby protokolu ATM over xDSL zachovávají vysokorychlostní charakteristiky a záruky QoS, dostupné v jádru sítě ATM beze změny protokolů. To vytváří potenciál pro síť ATM typu end-to-end pro obydli a malé kanceláře.

Protokol Point-to-Point Protocol (PPP) nad touto architekturou typu end-to-end přidává funkčnost a užitečnost. Protokol PPP umožňuje nezbytné hlavní rysy, jako jsou ověření, šifrování a komprese. Pro podporu těchto architektur (jako například residential broadband, PPP over ATM) má systém Windows 2000 další součásti. Modul Ndtsp.sys je poskytovatelem služby TAPI, který umožňuje NDIS proxy spojení s voláním prostřednictvím služby TAPI. Modul Ndproxy.sys poskytuje řízení volání po médiích orientovaných na spojení.

Přístup k původnímu protokolu přes rozhraní Winsock 2.0 Aplikace mohou přímo používat rozhraní Winsock 2.0 pro zabezpečení přirozeného přístupu k protokolům ATM. Aplikace, které používají původní protokol ATM mohou přistupovat k zárukám QoS, jako je šířka pásma a zpoždění.

Více informací o protokolu ATM naleznete v části „Asynchronní režim přenosu“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Protokol NWLink

Protokol je kompatibilní protokol IPX/SPX pro systém Windows 2000. Protokol NWLink neumožňuje počítači se systémem Windows 2000 přistupovat k souborům nebo tiskárnám, sdíleným na serveru NetWare nebo vystupovat jako souborový nebo tiskový server pro klienta NetWare, musí být použit přeměrovač, jakým je například Client Service for NetWare v systému Microsoft® Windows® 2000 Professional nebo Gateway Service for NetWare v systému Microsoft® Windows® 2000 Server.

Protokol NWLink je užitečný u aplikací NetWare typu klient-server, které používají rozhraní Winsock nebo NetBIOS nad protokoly IPX/SPX. Klient NWLink může být spuštěn na počítačích se systémy Windows 2000 Server nebo Windows 2000 Professional jako klient NetWare kompatibilní se sítí Microsoft a přistupovat k serverové části na serveru NetWare.

Součástí NetWare NetBIOS Link (NWNBLink) obsahuje vylepšení pro systém NetBIOS od vývojářů společnosti Microsoft. Součástí NWNBLink se používá k formátování požadavků na úrovni rozhraní NetBIOS a jejich předávání součásti protokolu NWLink pro přenos po síti.

Více informací o protokolu NetWare IPX/SPX najdete v části „Spolupráce s protokoly NetWare“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Protokol NetBEUI

Protokol NetBEUI (NetBIOS Extended User Interface) byl původně vyvinut jako protokol pro malé lokální síť LAN s 20 až 200 počítači. Protokol NetBEUI není směrovatelný, protože nemá síťovou vrstvu. Protokol NetBEUI je obsažen v systémech Windows 2000 Server a Windows 2000 Professional. Je to hlavně protokol pro podporu starších existujících pracovních stanic, které nebyly aktualizovány na systém Windows 2000.

Více informací o protokolu NetBEUI naleznete v části „Protokol NetBEUI“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Protokol AppleTalk

AppleTalk je sada protokolů, vyvinutá společností Apple Computer Corporation pro komunikaci mezi počítači Macintosh. Systém Windows 2000 zahrnuje podporu pro protokol AppleTalk, která umožňuje být systému Windows 2000 směrovačem a serverem vytáčeného spojení. Podpora je přirozeně poskytována jako služba pro sdílení souborů a tiskáren.

Více informací o protokolu AppleTalk naleznete v části „Služby pro počítače Macintosh“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

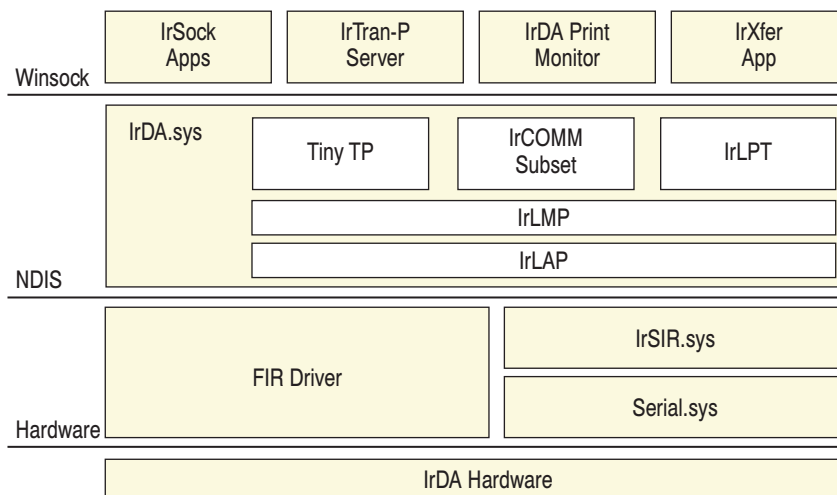
Protokol DLC

Protokol Data Link Control (DLC) byl původně vyvinut pro komunikace centrálních počítačů IBM. Protokol nebyl navržen jako primární protokol pro síťové použití mezi osobními počítači. Další využití protokolu DLC je tisk na tiskárnách Hewlett-Packard, připojených přímo k sítím. Tiskárny připojené k síti používají protokol DLC, protože přijaté rámce se snadno rozkládají a protože funkčnost protokolu DLC může být snadno zakódována do paměti ROM. Užitečnost protokolu DLC je omezená, protože se nepoužívá přímo s vrstvou rozhraní transportních ovladačů. Protokol DLC je potřeba instalovat pouze na těch síťových strojích, které vykonávají tyto dva úkoly, jako je tiskový server, posílající data na síťovou tiskárnu Hewlett Packard. Klienti, odesílající tiskové úlohy na síťovou tiskárnu, nepotřebují protokol DLC. Pouze tiskový server, komunikující přímo s tiskárnou, musí mít nainstalován protokol DLC.

Více informací o protokolu DLC najdete v části „Protokol Data Link Control“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Protokoly IrDA

Asociace Infrared Data Association (IrDA) definovala skupinu vysokorychlostních dvousměrných bezdrátových infračervených protokolů krátkého dosahu, všeobecně označovaných jako protokoly IrDA. Protokoly IrDA umožňují vzájemnou komunikaci mnoha různých zařízení. Kamery, tiskárny, přenosné počítače, stolní počítače a osobní digitální asistenti (PDA) mohou použitím této technologie komunikovat s kompatibilními zařízeními. Zásobník protokolů IrDA je přístupný použitím ovladačů bez spojení vrstvy NDIS. Obrázek B.10 ilustruje architekturu protokolu IrDA.



Obrázek B.10 Architektura protokolu IrDA

Součástmi protokolu IrDA jsou:

Rozhraní Winsock Winsock je aplikační programové rozhraní (API), které umožňuje aplikacím, systému Windows přistupovat k transportním protokolům. Zásobník protokolů IrDA je zpřístupněn aplikacím pomocí rozhraní Winsock.

Protokol IrTran-P Protokol IrTran-P je obousměrný protokol pro přenos obrazu. V systému Windows 2000 přijímá protokol IrTran-P pouze data a používá se u kamer s infračerveným připojením. Mnoho kamer má digitální porty a dokáže vyzařovat infračervená data do přijímajícího počítače. Tato data jsou pak umístěna do adresáře, určeného uživatelem (nebo do výchozího adresáře).

Součást IrDA Print Monitor IrDA Print Monitor je softwarová součást, která se spojuje s tiskárnou, připojenou rozhraním IrDA tak, aby se tato tiskárna jevila uživatelům systému Windows 2000 jako každá jiná tiskárna.

Modul IrXfer Modul IrXfer je aplikace přenosu dat v protokolech IrDA. Soubory mohou být přetahovány a upuštěny z pracovní plochy na jiný počítač. Implementace modulu IrXfer v systému Windows 2000 umožňuje obousměrný přenos.

Modul Tiny TP Služba Tiny TP je mechanismus řízení toku pro protokoly IrDA. Modul Tiny TP vystupuje jako regulátor pro řízení rychlosti vstupu nebo výstupu dat. To zahrnuje výskytům chyb a přetečení dat.

Modul IrDA.sys Modul IrDA.sys je zásobník transportních protokolů, který podporuje protokoly IrDA. Poskytuje podporu aplikacím prostřednictvím rozhraní Winsock do vrstvy NDIS.

Modul IrCOMM Modul IrCOMM je softwarová součást, která podporuje protokol IrTran-P. Modul IrCOMM používá rozhraní Winsock a je v počátečním nastavení připojena k serveru IrTran-P. Pokud potřebují jiné aplikace používat port IrCOMM, musí být server IrTran-P zablokován.

Modul IrLPT Modul IrLPT je podpora protokolu, používaná součástí IrDA Print Monitor. Modul IrLPT umožňuje tisk přímo ze zařízení IrDA na tiskárnách IrDA.

Protokol IrLMP Protokol Infrared Link Management Protocol se používá u několika různých spojení přes jeden spoj IrDA. Multiplexování je technika rozdělování dat z různých zdrojů na časová kvanta a zasílání těchto kvant v řadě do cíle.

Protokol IrLAP Protokol Infrared Link Access Protocol je softwarová součást pro řízení přístupu k médiu, jež určuje, která komponenta může přistupovat k médiu během každého časového kvanta.

Ovladač FIR Ovladač Fast Infrared (FIR) je ovladač miniportu, poskytnutý dodavatelem hardwaru k propojení hardwarových zařízení na spodní straně zásobníku protokolů k transportním protokolům výše, jakým je například protokol TCP/IP nebo protokol IPX/SPX. Zařízení FIR si mohou vyměňovat data rychlostí až 4 megabajtů za sekundu. U všech zařízení FIR je také vyžadována podpora přenosu použitím ovladače Serial Infrared (SIR).

Ovladač IrSIR.sys Ovladač Serial Infrared je ovladač miniportu dodávaný společností Microsoft. Je to také alternativní ovladač k ovladači Fast Infrared a může být použit pouze v kombinaci s ovladačem Serial.sys. Maximální přenosová rychlost je 115,2 kilobajtů za sekundu (Kbps). V kombinaci s ovladačem Serial.sys, poskytuje ovladač IrSIR.sys podporu pro sériové porty.

Ovladač Serial.sys Ovladač se používá pro připojení infračervených zařízení k ovladači IrSIR.sys výše v zásobníku protokolů a k hardwarovému zařízení níže. Jde o softwarový ovladač, který posílá a přijímá data z hardwarového zařízení a předkládá je ovladači IrSIR.sys ve formátu, který odpovídá požadavkům ovladače IrSIR.sys.

Vrstva rozhraní transportního ovladače

Vrstva rozhraní transportního ovladače (Transport Driver Interface – TDI) je obecným rozhraním pro ovladače (jako jsou přeměrovač a server systému Windows 2000), používané pro komunikaci s různými síťovými transportními protokoly. To umožňuje, aby služby zůstaly nezávislé na transportních protokolech. Na rozdíl od rozhraní NDIS neexistuje ovladač pro TDI, které je specifikací pro předávání zpráv mezi dvěma vrstvami v síťové architektuře.

Společnost Microsoft vyvinula rozhraní TDI, aby poskytla větší flexibilitu a funkčnost, než je poskytována existujícími rozhraními (jako jsou rozhraní Winsock a NetBIOS). Všechny součásti systému Windows 2000, poskytující transportní služby, jsou napojeny přímo na rozhraní TDI. To umožňuje, aby rozhraní TDI poskytovalo konzistentní rozhraní pro transportní protokoly. Specifikace rozhraní TDI popisuje sadu funkcí a mechanismů volání, kterými komunikují transportní ovladače a klienti TDI. Dodržování specifikace TDI poskytuje naplnění zvláštních požadavků softwaru na obou stranách. Některé aplikace, jako například NetBEUI se nepřipojují přímo na vrstvu TDI.

Moduly emulátorů

Moduly emulátorů poskytuje jednotné společné rozhraní všem transportním ovladačům systému Windows 2000. To zjednodušuje práci při vývoji transportních ovladačů, protože stačí kódovat pouze rozhraní. Transportní ovladače poskytuje vrstva rozhraní transportního ovladače. Z tohoto důvodu mohou být používány pouze aplikacemi, které mohou používat vrstvu TDI. Některé starší aplikace jsou napsány pro použití starších existujících rozhraní. Systém Windows 2000 obsahuje moduly emulátorů pro většinu oblíbených existujících síťových rozhraní (jako je NetBIOS). Moduly emulátorů poskytují mapovací vrstvu mezi síťovým rozhraním a protokoly vyhovujícími specifikaci TDI.

Síťová aplikační programová rozhraní

Aplikační programové rozhraní (API) je sada rutin, které používá aplikační program pro vyžádání a provádění služeb nižší úrovně, jež vykonává operační systém. Mezi síťová aplikační programová rozhraní systému Windows 2000 patří:

- rozhraní Winsock API
- rozhraní NetBIOS API
- rozhraní telefonního subsystému
- rozhraní zpracování zpráv
- rozhraní WNet API

Rozhraní Winsock API

Rozhraní Winsock je aplikační programové rozhraní, které umožňuje aplikacím systému Windows přistupovat k transportním protokolům. Rozhraní Winsock v systému Windows 2000 síťové API nezávislé na protokolu. Rozhraní Winsock je implementací široce používaného rozhraní Sockets API v systému Windows 2000, standardem pro přístup k službám datagramů a relací nad protokoly TCP/IP, NWLink, IPX/SPX, NetBIOS a AppleTalk. Mezi aplikace, napsané pro rozhraní Winsock, patří protokoly

File Transfer Protocol (FTP) a Simple Network Management Protocol (SNMP). Rozhraní Winsock vykonává následující funkce:

- Poskytuje známé síťové API pro programátory, používající Windows nebo UNIX.
- Nabízí binární slučitelnost mezi různorodými dodavateli nástrojů a protokolů zásobníku TCP/IP systému Windows.
- Podporuje jak protokoly orientované na spojení, tak protokoly bez spojení.

Systém Windows 2000 obsahuje podporu rozhraní Winsock 1.1. Rozhraní Winsock 2.0 rozšiřuje rozhraní Winsock 1.1, aby poskytovalo přístup k sítím, které používají jiné protokoly než TCP/IP, jako jsou sítě NetWare a AppleTalk. Rozhraní Winsock 2.0 Poskytuje následující vylepšení nad rozhraní Winsock 1.1:

- Registrace a překlad názvů.
Rozhraní Winsock 2.0 může být použito aplikacemi pro přístup k mnoha různým oborům názvů, jako jsou Domain Name System (DNS), Novell Directory Services (NDS) a X.500.
- Podpora multimediální komunikace v reálném čase.
Rozhraní Winsock podporuje několik multimediálních vylepšení, včetně služby Quality of Service (QoS)
- Na protokolu nezávislé vícesměrové vysílání a vysílání typu multipoint.
Rozhraní Winsock 2.0 umožňuje aplikacím využít výhody možností vysílání více příjemcům a vícesměrového vysílání transportních zásobníků.

Architektura rozhraní Winsock

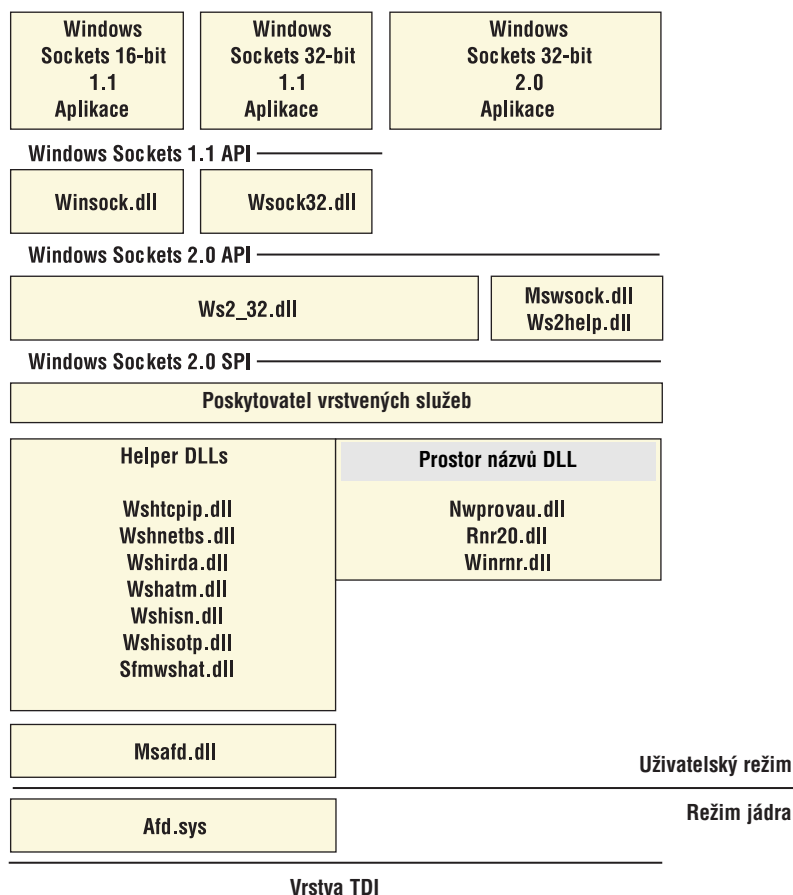
Rozhraní Winsock 2.0 je rozhraní, vyhovující specifikaci Windows Open Systems Architecture (WOSA), které umožňuje komunikovat aplikacím typu front-end se službami typu back-end. Rozhraní Winsock 2.0 obsahuje následující součásti:

- Aplikační programové rozhraní Winsock 1.1
- Aplikační programové rozhraní Winsock 2.0
- Poskytovatele transportních služeb rozhraní Winsock 2.0
- Poskytovatele služeb vrstev

Obrázek B.11 ukazuje architekturu rozhraní Winsock 2.0.

Soubory rozhraní Winsock

Tabulka B.1 obsahuje seznam souborů, které používá rozhraní Winsock při vykonávání svých funkcí. Tabulka uvádí soubory v pořadí vrstev, které podporují a udává stručný popis jejich funkcí.



Obrázek B.11 Architektura rozhraní Winsock 2.0

Table B.1 Winsock Files

Knihovny DLL rozhraní Winsock	Popis
Winsock.dll	16bitové rozhraní Winsock 1.1
Wsock32.dll	32bitové rozhraní Winsock 1.1
Ws2_32.dll	Hlavní rozhraní Winsock 2.0
Mswsock.dll	Rozšíření rozhraní Winsock společnosti Microsoft. Knihovna Mswsock.dll je aplikační programové rozhraní, které dodává služby, jež nejsou součástí rozhraní Winsock.
Ws2help.dll	Nástroje závislé na platformě. knihovna Ws2help.dll dodává kód, specifický pro operační systém, který není částí rozhraní Winsock.
Wshtcpip.dll	Pomocné moduly pro TCP
Wshnetbs.dll	Pomocné moduly pro NetBT

Knihovny DLL rozhraní Winsock	Popis
Wshirda.dll	Pomocné moduly pro IrDA
Wshatm.dll	Pomocné moduly pro ATM
Wshisn.dll	Pomocné moduly pro Netware
Wshisotp.dll	Pomocné moduly pro transporty OSI
Sfmwshat.dll	Pomocné moduly pro Macintosh
Nwprovau.dll	Poskytovatel překladu názvů pro IPX
Rnr20.dll	Hlavní překlad názvů
Winrnr.dll	Překlad názvů LDAP
Msafd.dll	Spojení rozhraní Winsock s jádrem
Afd.sys	Spojení jádra rozhraní Winsock s transportními protokoly TDI

Aplikační programové rozhraní Winsock 1.1

Aplikační programové rozhraní Winsock 1.1 je přepínací vrstva. Překládá výstup ze součásti do tvaru, který dokáže používat jiná součást. Příkazy vrstvy rozhraní Winsock 1.1 jsou převáděny na příkazy vrstvy rozhraní Winsock 2.0, aby umožňovaly zpětnou kompatibilitu pro starší aplikace.

Aplikační programové rozhraní Winsock 2.0

Aplikační programové rozhraní Winsock 2.0 je rozhraní pro Winsock 2.0. Například pomáhá přidávat nová aplikační programová rozhraní do rozhraní Winsock 2.0 (jako například rozhraní Generic Quality of Service). Aplikační programové rozhraní Winsock 2.0 je umístěno mezi dynamicky připojovanou knihovnou (DLL) rozhraní Winsock 2.0 a aplikací Winsock 2.0.

Poskytovatelé transportních služeb rozhraní Winsock 2.0 SPI

Poskytovatelé transportních služeb dávají aplikacím konzistentní rozhraní pro přístup k více transportním protokolům. Dynamické knihovny rozhraní Winsock 2.0, umístěné nad poskytovatelem transportní služby, berou požadavky aplikací a odesílají tyto požadavky poskytovateli transportní služby. Dynamické knihovny rozhraní Winsock 2.0 také zabezpečují řízení provozu. Poskytovatel transportní služby může podporovat jeden nebo více transportních protokolů.

Vrstva poskytovatelů služeb vrstev

Volitelná vrstva poskytovatelů služeb vrstev může být vložena mezi dynamické knihovny rozhraní Winsock 2.0 a zásobník protokolů v nižších vrstvách, pokud je to požadováno aplikací. Může rozšiřovat zásobník protokolů v nižších vrstvách poskytováním dodatečných služeb, jako jsou ověřování, šifrování nebo služby serverů proxy.

Knihovny pomocných modulů rozhraní Winsock

Knihovny pomocných modulů rozhraní Winsock poskytují zvláštní softwarové součásti na pomoc rozhraní Winsock 2.0. Transportní protokoly, jako TCP, ATM a IrDA mají knihovny DLL, které dodávají nezbytný programový kód pro podporu rozhraní Winsock.

Poskytovatelé překladů názvů rozhraní Winsock 2.0

Poskytovatelé překladů názvů umožňují aplikacím serverů a klientů používat konzistentní rozhraní pro více názvových služeb. Služby se registrují v knihovnách DLL rozhraní Winsock, aplikace klientů posílají požadavky na názvy těchto služeb knihovně DLL rozhraní Winsock. Knihovna DLL rozhraní Winsock řídí registraci a zavádění poskytovatelů překladů názvů a odesílá operace překladu názvů správnému poskytovateli. Poskytovatel nakonec implementuje rozhraní s existujícími názvovými službami, jako je služba DNS.

Obecná kvalita služby a protokol rezervace prostředků

Sítě bez připojení (jako jsou síť Ethernet) činí pouze nejlepší snahu pro doručení paketů do jejich cíle. Není zde žádná záruka, že pakety dorazí nebo že dorazí ve správném pořádku. Místo toho protokoly jako TCP/IP byly vyvinuty pro zajištění opakovaného přenosu ztracených paketů a zajištění, že pakety v nesprávném pořadí mohou být znovu poskládány ve správném pořadí. To postačuje pro většinu aplikací jako je elektronická pošta. Nicméně pro novější aplikace, jako je zvuk a obraz v reálném čase, musí pakety dorazit včas a v pořádku nebo může být přenos zkomolen.

Sítě orientované na spojení umožňují aplikacím vyžadovat pro určitá spojení určité úrovně služeb, jako jsou šířka pásma a spolehlivost. Navíc umožňují počítačům sestavovat několik různých spojení s několika různými kvalitami služby. Například v síti orientované na spojení mohou dvě souběžná spojení podporovat jak spojení s velkým zpožděním a malou šířkou pásma pro posílání elektronické pošty, tak spojení s velkou šířkou pásma a malým zpožděním pro videokonference.

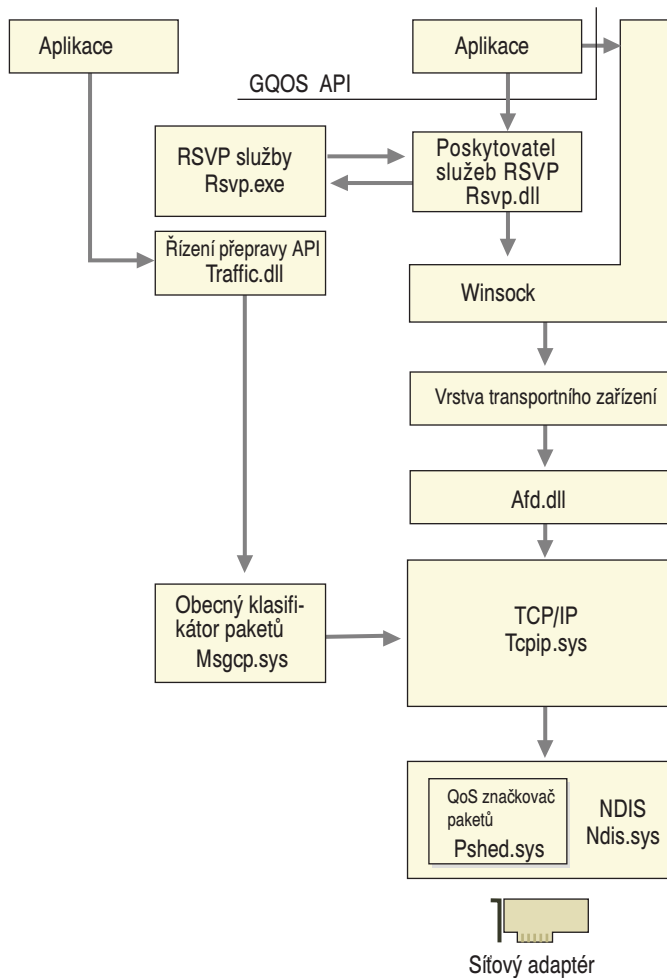
Systém Windows 2000 umožňuje různé úrovně služeb prostřednictvím svého programového rozhraní Generic Quality of Service (GQoS) a jeho podpory pro protokol rezervace a oznamování prostředků Resource Reservation Signaling Protocol (RSVP). Aplikace mohou pro spojení požadovat různé síťové charakteristiky. Protokol RSVP pak zpracovává tyto požadavky a pokouší se provést rezervaci šířky pásma pro toto spojení.

Obecná kvalita služby

Aplikační programové rozhraní obecné kvality služby (GqoS) v rozhraní Winsock 2.0 poskytuje přístup k většině úrovní služby QoS. Poskytovatelé služby QoS v nižších vrstvách umožňují používat tyto úrovně služby přímo z programových rozhraní GQoS. Aplikace mohou provádět volání rozhraní GQoS a vyžadovat atributy jako:

- Špičková šířka pásma (průměrná nebo vrcholová hodnota přenosové rychlosti).
- Zpoždění (maximální přípustná prodleva mezi přenosem bitu a jeho příjmem příjemcem).
- Odchyłka zpoždění (rozdíl mezi minimálním a maximálním zpožděním paketu).

Obrázek B.12 ukazuje architekturu rozhraní GQoS.



Obrázek B.12 Architektura rozhraní GQoS

Součástmi rozhraní GQoS jsou:

- Poskytovatel služby RSVP

Součástí služby QoS která vyvolává skoro všechny funkce a služby QoS. Poskytovatel služby RSVP (moduly rsvpsp.dll a rsvp.exe) spouští řízení provozu a zavádí, spravuje a obstarává signalizaci RSVP pro všechny funkce služby QoS v systému Windows 2000.

- Aplikační programové rozhraní řízení provozu

Programové rozhraní pro součásti řízení provozu, které regulují síťový provoz na místních hostitelských počítačích. Ovládá provoz vnitřně (uvnitř jádra) a v síti. (Přiděluje rovněž priority a zařazuje pakety do front podle priorit přenosu).

- Obecný klasifikátor paketu (GPC)

Klasifikuje pakety a přiděluje jim priority, dokáže poskytovat vyhledávací tabulky a klasifikační služby uvnitř zásobníku sítě.

- Modul Afd.sys

Rozhraní jádra Winsock poskytuje přístup k přenosům TDI.

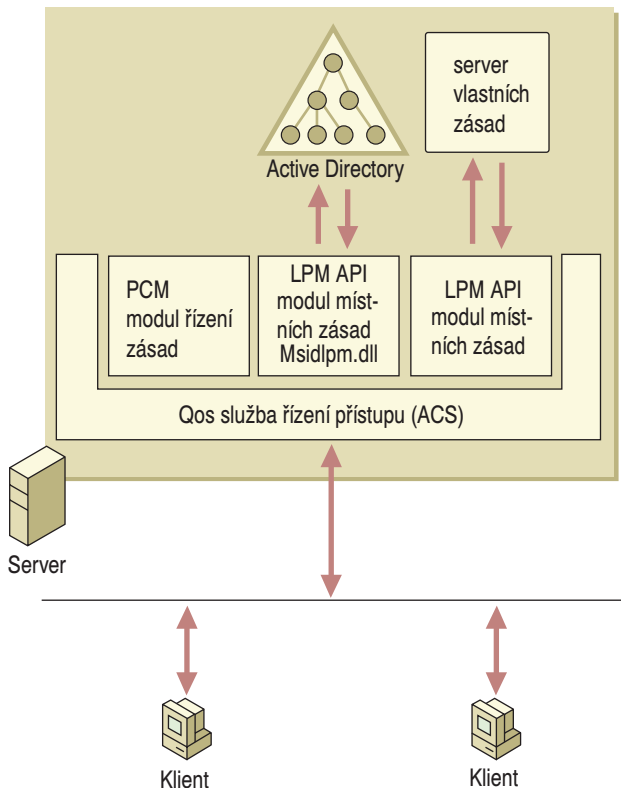
- Plánovač paketů QoS

Tento modul řízení provozu ovládá množství dat, které smí aplikace přenést najednou, čímž vynucuje nastavení parametrů QoS pro určitý tok.

Služba řízení přístupu Quality of Service Admission Control Service

Služba QoS Admission Control Service je zodpovědná za ovládání využití podsítě pro součásti otevřené službě QoS.

Obrázek B.13 ilustruje architekturu služby QoS Admission Control Service.



Obrázek B.13 Služba QoS Admission Control Service

Služba QoS ACS spravuje prostředky šířky pásma podsítě, které jsou nezbytné pro zajištění přenosu dat službou QoS. Služba QoS ACS pracuje v systému Windows 2000 Server a sídlí v podsíti. Ve sdílených segmentech jsou směrovány všechny rezervační zprávy služby QoS přes službu QoS ACS, takže klienti podsítě mohou sdílet šířku pásma a správa přidělování šířky pásma může být centralizována. Služba QoS ACS posílá zprávy, zvané signalizace, aby uvědomila ostatní klienty v síti, že je přítomna a připravena přijímat požadavky na rezervace šířky pásma podsítě. Součástí služby QoS Admission Control Service ovládají aplikace, podporující QoS. Služba QoS ACS musí být instalována na serveru, na kterém nejsou přítomny součásti QoS.

Součástí služby QoS ACS jsou:

- Součást Quality of Service Admission Control Service (QoS ACS)

Součást služby QoS, která ovládá využití podsítě pro aplikace přístupné službě QoS. Služba QoS ACS vykonává své řízení nad aplikacemi a klienty tím, že se umístí do cesty zpráv protokolu RSVP. Služba QoS ACS zachycuje zprávy protokolů Resource Reservation Protocol (RSVP) a Reservation (RESV) a předává tyto zprávy s informacemi o uživateli modulům místních zásad k ověření. Zprávy RSVP jsou zasílány pro vyžádání přenosových charakteristik a zprávy RESV potvrzují že tyto přenosové charakteristiky mohou být poskytnuty.

- Modul řízení zásad (PCM)

Zprostředkovává interakce mezi službou QoS ACS a moduly LPM. Moduly PCM posílají uživatelské informace každému modulu LPM a sbírají všechny odpovědi, pak provádějí logické kontroly informací. Modul PCM sbírá informace a posílá je jako jednu odpověď službě QoS ACS.

- Modul místních zásad (LPM)

Aplikační programové rozhraní, které komunikuje se službou QoS Admission Control Service. Rozhraní LPM rovněž specifikuje, jak jsou moduly LPM zaznamenávány a inicializovány uvnitř konceptu služby QoS ACS.

- Služba Active Directory

Poskytuje jediné místo pro správu zásad, uživatelských účtů, klientů, serverů a aplikací systému Windows. Ve službě QoS ukládá služba Active Directory informace o úrovních služeb, které používá rozhraní GQoS.

- Vlastní Server zásad

Součást dodaná třetí stranou, která může být použita k ukládání zásad pro úroveň služby rozhraní GQoS.

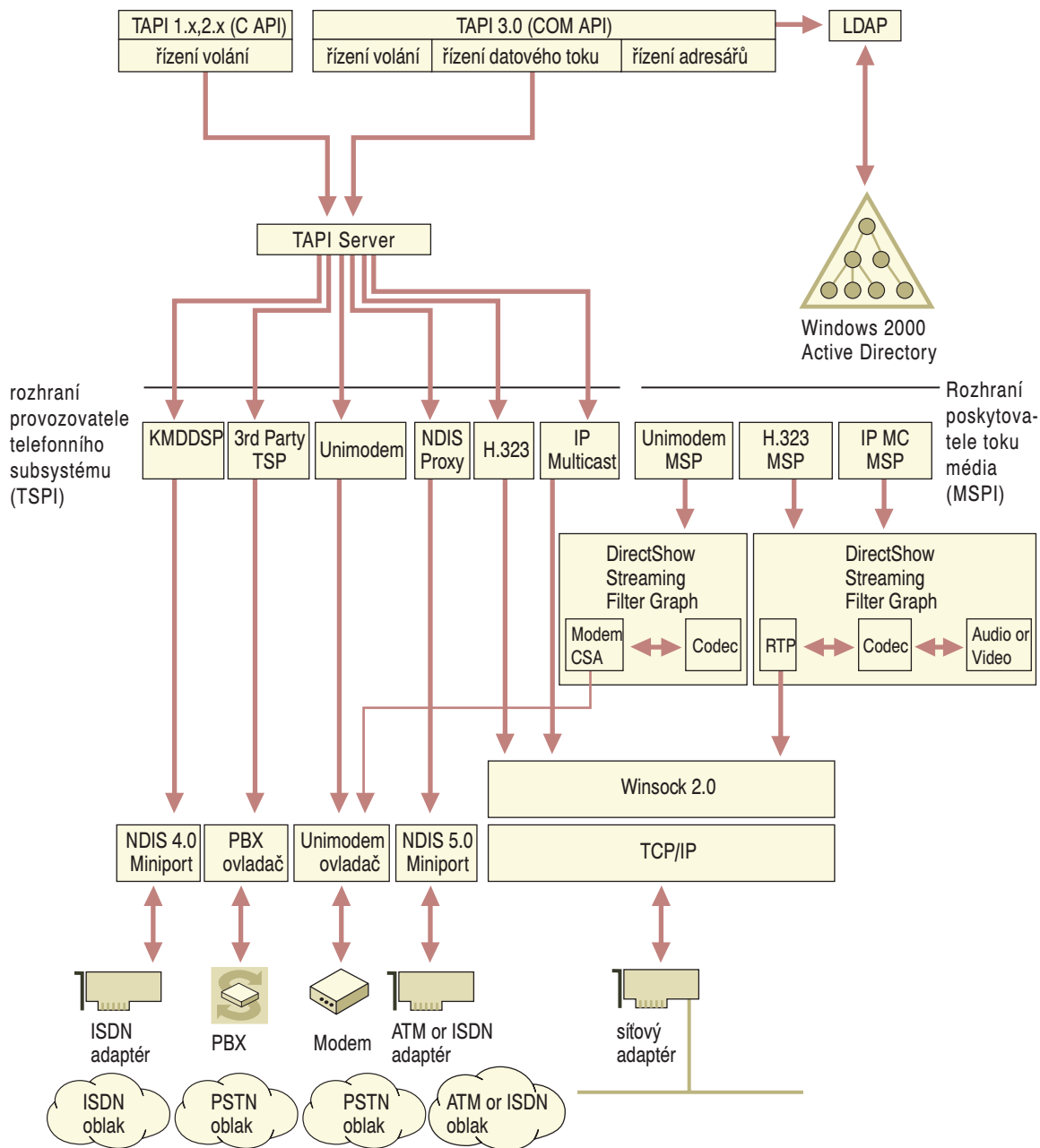
Aplikace vyžadují úroveň služeb QoS. Poskytovatel signalizace protokolu RSVP dohodne se sítí požadované úrovně služeb. Klasifikátor a plánovač paketů určí, kdy mají být poslány pakety a s jakou prioritou. Směrovač sledující službu QoS nakonec předá pakety jak je požadováno.

Více informací o službě QoS a protokolu RSVP najdete v části „Obecná kvalita služby“ v této knize.

Rozhraní telefonního subsystému

Telefonní subsystém je technologie, která integruje počítače s telefonními sítěmi. S telefonním subsystémem mohou lidé využívat svých počítačů pro využití výhod širokého rozsahu služeb po telefonní lince.

Rozhraní telefonního subsystému (TAPI) umožňuje programátorům vytvářet aplikace, které poskytují osobní telefonní služby uživatelům. Rozhraní TAPI podporuje přenos řeči i dat a počítá s řadou koncových zařízení. Podporuje složité typy spojení a techniky řízení volání jakými jsou konferenční volání, čekání volání a hlasová pošta. Rozhraní TAPI umožňuje všem prvkům použití telefonu, od jednoduchých volání typu vytoč a mluv po mezinárodní elektronickou poštu, aby byly řízeny uvnitř aplikací vyvinutých pro aplikační programová rozhraní Microsoft® Win32®.



Obrázek B.14 Architektura rozhraní TAPI

Telefonní subsystém může využívat mnoho aplikací:

- Vícesměrové multimediální konference v sítích IP.
- Hlasová volání po síti Internet.
- Aplikace center volání schopné sledovat více agentů.
- Základní hlasová volání v síti Public Switched Telephone Network (PSTN).
- Řízení systému Private Branch Exchange (PBX).
- Interaktivní systémy hlasové odezvy (IVR).
- Hlasová pošta.

Obrázek B.14 ukazuje hlavní součásti architektury rozhraní TAPI.

Rozhraní TAPI 3.0 COM API Rozhraní TAPI 3.0 API je implementováno jako sada rozhraní modelu Component Object Model (COM). To umožňuje vývojářům psát aplikace zpřístupňující rozhraní TAPI v libovolném jazyce, který podporuje model COM, jakým je například Java, Microsoft® Visual Basic nebo Microsoft® Visual C++®. Rozhraní TAPI 3.0 podporuje dvě třídy poskytovatelů služeb: telefonní subsystém a médium.

Rozhraní TAPI 2.1 COM API Rozhraní TAPI 2.1 COM API zabezpečuje kompatibilitu s rozhraním TAPI 3.0. Rozhraní TAPI 2.1 je překládací vrstvou, která mapuje 16bitové adresy na 32bitové adresy a postupuje požadavky dál dynamické knihovně Tapi32.dll.

Knihovna Tapi32.dll Knihovna Tapi32.dll je tenká seřadovací vrstva, která přenáší požadavky funkcí pro server Tapisrv.exe. Když je třeba, zavádí a volá knihovny DLL rozhraní poskytovatele služby.

Server TAPI Server TAPI je implementován modulem Tapisrv.exe, hlavní součástí rozhraní TAPI. Server TAPI je spuštěn jako samostatný služební proces, ve kterém jsou spuštěni všichni poskytovatelé služeb telefonního subsystému. Funkce aplikačního programového rozhraní komunikují se serverem TAPI při zasílání požadavků služeb poskytovatelům služeb telefonního subsystému.

Poskytovatelé služeb telefonního subsystému Poskytovatelé služeb telefonního subsystému jsou dynamicky připojované knihovny, které vykonávají akce nižších úrovní specifických pro zařízení pro dokončení úkolů telefonního subsystému hardwarovými zařízeními, jako jsou faxové adaptéry, adaptéry ISDN, telefony a modemy. Aplikace připojují a volají funkce pouze v dynamicky připojované knihovně TAPI; nikdy nevolají poskytovatele služeb přímo.

Poskytovatelé služeb média Poskytovatel služeb telefonního subsystému (Microsoft H.323 Telephony Service Provider) a s ním spojený poskytovatel média (Media Service Provider – MSP) umožňují aplikacím, používajícím služeb TAPI, zapojit se do multimediálních zvukově-obrazových relací s libovolným koncovým zařízením, vyhovujícím specifikaci H.323, v místní síti (LAN) nebo v síti Internet. K příkladům patří:

- Poskytovatel služby vícesměrových konferencí. Používá vícesměrové techniky protokolu IP k zajištění efektivního zvukového a obrazového konferenčního spojení v sítích IP, intranetech a v síti Internet.
- Poskytovatel služby proxy v rozhraní NDIS. Nabízí rozhraní TAPI zařízením rozlehlých sítí (WAN), jakými jsou síť ISDN nebo ATM.
- Rozhraní TAPI, které má vzdálený poskytovatel služby pro podporu telefonního subsystému typu klient-server. Vzdálený poskytovatel služby zajišťuje rozšíření

služeb telefonního subsystému TAPISRV pro přístupy klientů k zařízením TAPI, která sídlí na serverech v síti.

- Poskytovatel služby režimu jádra rozhraní TAPI. Komunikuje se součástmi NDIS, aby poskytl rozhraní TAPI ovladačům NDISWAN.
- Unimodem 5. Poskytovatel služeb telefonního subsystému, který zajišťuje abstrakci pro modemová zařízení, takže aplikace mohou operovat transparentně s širokou paletou modemů.
- Jiní dodavatelé software a hardware. Mohou vytvářet poskytovatele služeb telefonního subsystému, kompatibilní s rozhraním TAPI, pro další aplikace.

Více informací o rozhraní TAPI najdete v části „Integrace telefonního subsystému“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Rozhraní NetBIOS API

Rozhraní NetBIOS je standardní aplikační programové rozhraní v prostředí osobních počítačů. Rozhraní NetBIOS se používá pro vývoj aplikací typu klient-server. Rozhraní NetBIOS se používalo jako mechanismus komunikace mezi procesy (IPC) od svého zavedení. Je obsaženo v systému Windows 2000 pro podporu starších aplikací.

Aplikace rozhraní NetBIOS typu klient-server může komunikovat různými protokoly:

- Protokol NetBEUI Frame (NBF)
Protokol NetBEUI je transportní protokol kompatibilní s rozhraním NetBIOS. Protokol NBF byl navržen pro malé sítě s 50 až 200 počítači. Protože protokol NetBEUI nemá síťovou vrstvu, není směrovatelný. Je obsažen v systému Windows 2000 pro podporu starších verzí sítí.
- protokol NetBIOS over TCP/IP (NetBT)
Protože protokol NetBEUI není směrovatelný, byly vytvořeny alternativní prostředky pro jeho transport přes směrovače. Specifikace RFC 1001 a 1002 definovaly metody, kterými může být protokol NetBEUI transportován v paketech IP. S touto technikou lze spojit sítě NetBEUI.
- Protokol NWLink NetBIOS (NWNBLink)
Protokol NetWare NetBIOS Link (NWNBLink) obsahuje vylepšení rozhraní NetBIOS od společnosti Microsoft. Součást NWNBLink se používá k formátování požadavků na úrovni rozhraní NetBIOS a jejich postupování součástí protokolu NWLink pro přenos sítí.

Rozhraní NetBIOS používá následující součásti:

- Knihovna Netapi32.dll. Spojená s emulátorem rozhraní NetBIOS pro umožnění komunikace s protokoly TCP/IP, NetBEUI a NWLink. Sdílí obor adres uživatelských aplikací rozhraní NetBIOS.
- Emulátor rozhraní NetBIOS. Zajišťuje mapovací vrstvu rozhraní NetBIOS mezi aplikacemi NetBIOS a protokoly vyhovujícími rozhraní TDI.

Aplikační programové rozhraní Winsock může být rovněž použito pro přístup k protokolům rozhraní NetBIOS.

Více informací o rozhraní NetBIOS najdete v části „Protokol NetBEUI“ v knize *Microsoft® Windows® 2000 Server Internetworking*.

Rozhraní zpracování zpráv

Aplikační programové rozhraní zpracování zpráv (MAPI) je standardem, který umožňuje aplikacím spolupracovat s mnoha různými službami zpracování zpráv použitím jediného rozhraní. Rozhraní MAPI je sada funkcí aplikačního programového rozhraní, které umožňují klientům služeb zpracování zpráv, jako je například Microsoft Exchange, spolupracovat s různými poskytovateli služeb zpracování zpráv, jako jsou například Microsoft Mail a Microsoft Fax.

Více informací o rozhraní MAPI naleznete v popisu Platform Software Development Kit (SDK).

Rozhraní WNet API

Aplikační programová rozhraní WNet zajišťují síťové funkce systému Windows (WNet), které poskytují síťové možnosti aplikacím. Jak je známo u aplikačních programových rozhraní Win32, aplikace vytvořené s použitím aplikačních programových rozhraní WNet fungují nezávisle na síti, ve které pracují. Použitím aplikačních programových rozhraní WNet lze vyvíjet aplikace, které lze úspěšně spouštět na všech platformách, přičemž jsou ještě schopny využívat výhody jedinečných vlastností a schopností každé konkrétní platformy.

Síťové služby jsou jednou z mnoha kategorií služeb, které mohou poskytovat aplikační programová rozhraní Win32. Požadavky na síťové služby jsou zajišťovány směrovačem hromadného zprostředkovatele (MPR). Směrovač hromadného zprostředkovatele přijímá příkazy rozhraní Wnet, určuje odpovídající přesměrovač a předává příkazy tomuto přesměrovači. Směrování hromadného zprostředkovatele pak směruje požadavky na síťové služby příslušnému zprostředkovateli pro přenos v síti.

Více informací o rozhraních WNet najdete v popisu Platform Software Development Kit (SDK).

Další síťová aplikační programová rozhraní

Systém Windows 2000 používá mnoho aplikačních programových rozhraní navíc k těm, která byla popsána:

- Rozhraní zabezpečení systému proti průniku zvenčí je programové rozhraní nízké úrovně, které umožňuje větší a složitější filtrování než rozhraní ovladačů filtrů.
- Aplikační programové rozhraní Dynamic Host Configuration Protocol (DHCP) umožňuje aplikacím požadovat možnosti protokolu DHCP.
- Aplikační programové rozhraní Multicast Address Dynamic Client Allocation Protocol (MADCAP) umožňuje aplikacím požadovat adresy vícesměrového vysílání.
- Aplikační programové rozhraní volání serveru DHCP umožňuje uživatelská rozšíření serveru DHCP.
- Aplikační programové rozhraní pomocníka IP (IPHLP API) je veřejné aplikační programové rozhraní, které poskytuje informace protokolu TCP/IP aplikacím Win32.
- Aplikační programové rozhraní směrovače hromadného zprostředkovatele (MPR API) se používá pro nastavování a správu směrovačů.
- Aplikační programové rozhraní ovladačů filtrů umožňuje nastavení filtrování paketů pro provoz sítě IP.

- Aplikační programové rozhraní front zpráv zajišťuje spolehlivé volně spojené komunikace. Řazení zpráv do front může být použito pro zpracování transakcí ke komunikaci o stavu transakce.

Více informací o síťových aplikačních programových rozhraních najdete v popisu Platform Software Development Kit (SDK).

Komunikace mezi procesy

Komunikace mezi procesy (IPC) umožňuje dvousměrnou komunikaci mezi klienty a servery používající distribuované aplikace. IPC je mechanismus používaný programy a víceuživatelskými procesy. Komunikace IPC umožňují současně spuštěným úkolům spolu komunikovat na místním počítači nebo mezi místním a vzdáleným počítačem.

Mechanismus IPC je používán pro podporu distribuovaného zpracování. Aplikace, které rozdělují zpracování mezi počítače v síti, se nazývají distribuované aplikace. Rozdělené části distribuované aplikace mohou být umístěny na stejném počítači nebo na oddělených počítačích. Aplikace typu klient-server používá distribuované zpracování, ve které je zpracování rozděleno mezi pracovní stanici (klient) a výkonnější server. Uživatelské části se někdy říká přední část (front end) a serverové části zadní část (back end). Klientská část aplikace typu klient-server se může skládat pouze z uživatelského rozhraní aplikace. Distribuovaná aplikace však může být rozdělena v různých místech. Je spuštěna na pracovní stanici klienta a spotřebovává menší množství výpočetního výkonu. Klientská část může například obsluhovat pouze grafiku obrazovky, pohyb myši a stisknutí kláves.

Vícesložkové aplikace jsou rozšířením základního modelu klient-server. Tento obecný distribuovaný model činnosti je někdy označován jako tříložkový model. Je složen ze tří částí: složky klienta, složky součástí a složky serveru.

Například mzdová účtárna vaší společnosti používá aplikaci pro tisk výplat. Když spustí zaměstnanec mzdové účtárny aplikaci klienta, aplikace spustí server pravidel činnosti ve složce součástí. Složka součástí se skládá z různých součástí, jako jsou například pravidla činnosti, správa transakcí a další součásti logiky činnosti.

Server pravidel činnosti organizuje příslušné součásti pro úkol. Aplikace serveru se spojí s databázovým serverem v databázové složce a vyhledá záznamy zaměstnance, jako například informace o platu. Server pravidel činnosti převede mzdové informace do výsledného výstupu a vrátí ho klientovi.

Aplikační server může zpracovávat informace, které by normálně zpracovával klient v modelu klient-server. Aplikační server řeší logiku činnosti nebo aplikace a komunikuje s databází na zadní části, obvykle strukturovaným dotazovacím jazykem (SQL). Server nebo databáze na zadní části (back-end) často používá velké množství uložených dat, výpočetní výkon a specializovaný hardware. Části součástí usnadňují správu, rozmístění a aktualizace těchto objektů.

Cílem distribuovaného zpracování je přesunout skutečné zpracování aplikace od klienta k serverům, které mají výkon pro velké aplikace. Klientská část formátuje požadavky a posílá je na zpracování serveru. Servery zpracovávají požadavky a předávají výsledky zpět klientovi.

Je řada způsobů navazování takového spojení. Operační systém Windows 2000 poskytuje mnoho různých mechanismů komunikace mezi procesy (IPC).

Distribuovaný model Component Object Model

Navíc k podpoře modelu Component Object Model (COM) pro komunikaci mezi procesy v místním počítači podporuje systém Windows 2000 distribuovaný model (DCOM). Model DCOM je systém softwarových objektů navržených tak, aby byly opakovaně použitelné a zaměnitelné. Objekty jsou softwarové součásti, které mohou provádět a podporovat aplikace. Objekty podporují sady příbuzných funkcí, jako například třídění, generování náhodných čísel a prohledávání databází. Každé sadě funkcí se říká rozhraní a každý objekt modelu DCOM má více rozhraní. Když aplikace přistupují k objektu, dostávají nepřímý odkaz na funkce rozhraní. Odkaz obsahuje informaci o umístění objektu. Po obdržení tohoto odkazu nepotřebuje volající aplikace vědět, kde je objekt nebo jak vykonává svou práci, protože tento odkaz na něj volající aplikaci směřuje.

Model DCOM umožňuje procesům, aby byly efektivně distribuovány více počítačům, takže klientské a serverové součásti aplikace mohou být umístěny v optimálních místech sítě. Zpracování probíhá transparentně pro uživatele, protože tuto funkci obstarává model DCOM. Uživatel tak může přistupovat k informacím a sdílet informace bez potřeby vědět, kde jsou umístěny součásti aplikace. Pokud jsou klientské a serverové součásti aplikace umístěny na stejném počítači, může být model DCOM použit pro přenos informací mezi procesy. Model DCOM je nezávislý na platformě a podporuje každou 32bitovou aplikaci, která využívá model DCOM.

Výhody používání modelu DCOM

Model DCOM je vývojáři upřednostňovanou metodou pro vytváření aplikací typu klient-server pro systém Windows 2000. S modelem DCOM lze k softwarovým objektům přidávat nebo aktualizovat rozhraní, takže nejsou vynucovány aktualizace aplikací při každé změně softwarového objektu. Objekty jsou softwarové entity, které zajišťují určité funkce. Tyto funkce jsou implementovány jako dynamicky připojované knihovny, takže změny v těchto funkcích včetně nových rozhraní a způsobů vykonávání funkcí, lze provádět bez přepisování a nového překládání aplikací, které je používají.

Systém Windows 2000 podporuje model DCOM zprůhledněním implementace aplikačních odkazů pro aplikaci i pro objekt. Pouze operační systém musí vědět, jestli volaná funkce je zpracována ve stejném procesu nebo někde v síti. To zbavuje aplikace starosti o místní nebo vzdálená volání procedur. Správci mohou vybrat, zda spustí aplikace modelu DCOM na místních nebo vzdálených počítačích a mohou měnit nastavení pro efektivní vyrovnávání zátěže.

Vaše aplikace může podporovat svou vlastní sadu vlastností modelu DCOM. Více informací o nastavení vaší aplikace pro použití modelu DCOM naleznete v dokumentaci k vaší aplikaci..

Model DCOM staví na technologii vzdáleného volání procedur poskytnutím snadno použitelného mechanismu pro začlenění distribuovaných aplikací do sítě. Distribuovaná aplikace se skládá z více procesů, které spolupracují, aby provedly jeden úkol. Na rozdíl od jiných mechanismů komunikace mezi procesy (IPC) vám poskytuje model DCOM vysoký stupeň ovládnutí bezpečnostních rysů, jakými jsou povolování a ověřování domén. Může být rovněž použit pro spouštění aplikací na jiných počítačích a k začlenění aplikací webových prohlížečů, které běží na platformě Microsoft® ActiveX®.

Vzdálené volání procedury

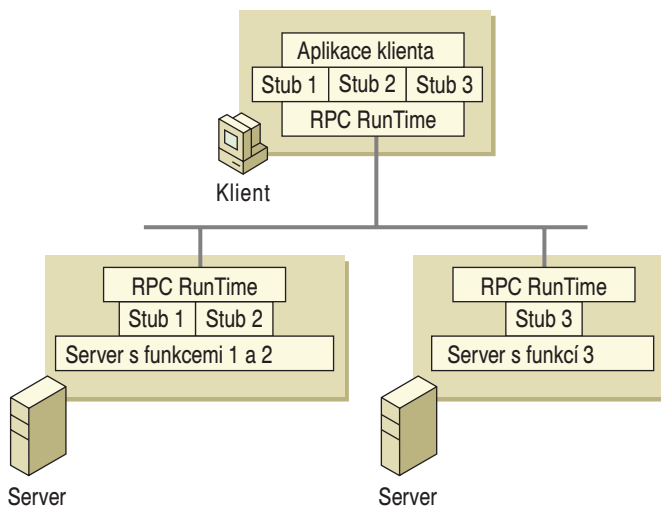
Vzdálené volání procedury (RPC) je technika komunikace mezi procesy, která umožňuje komunikovat softwaru klienta se softwarem serveru. Prostředek Microsoft RPC je kompatibilní se specifikací Open Group's Distributed Computing Environment (DCE) pro vzdálená volání procedur a může spolupracovat s jinými systémy RPC, založenými na specifikaci DCE, jako jsou systémy založené na operačních systémech HP-UX a IBM AIX UNIX. Prostředek RPC je kompatibilní se specifikací Open Group.

Mechanismus vzdáleného volání procedur Microsoft RPC je jedinečný v tom, že používá další mechanismy IPC, jako jsou pojmenované kanály, rozhraní NetBIOS nebo Winsock, k navázání komunikace mezi klientem a serverem. S prostředkem RPC mohou být části logiky programu a příbuzné kódy procedur na různých počítačích, což je důležité pro distribuované aplikace.

Volání RPC je založeno na pojmech, používaných pro tvorbu strukturovaných programů, které lze vidět jako páteř, ke které mohou být připojeny řady žebířů. Páteř je hlavní logika programu, které se mění zřídka. Žebíř jsou procedury, které volá páteř k vykonání práce nebo funkcí. V tradičních programech jsou tato žebířa staticky připojena k páteři a uložena ve stejném spustitelném souboru. Prostředky RPC umísťují páteř a žebířa na různých počítačích.

Systém Windows 2000 používá dynamicky připojované knihovny (DLL) k zajištění kódu procedur i kódu páteře. To umožňuje modifikace nebo aktualizace knihoven DLL beze změny nebo redistribuce páteřní části.

Aplikace klientů jsou vyvinuty se zvlášť kompilovanými stub knihovnami, poskytnutými aplikačním programem. Moduly těchto stub knihoven ve skutečnosti přenášejí data a funkce běžícímu modulu (run-time) volání RPC. Tento modul je zodpovědný za nalezení serveru, který dokáže vyhovět příkazu RPC. Když je nalezen, jsou funkce a data poslány tomuto serveru, kde jsou vyzvednuty běžící součástí tohoto serveru. Server vybuduje příslušnou datovou strukturu a zavolá funkci.

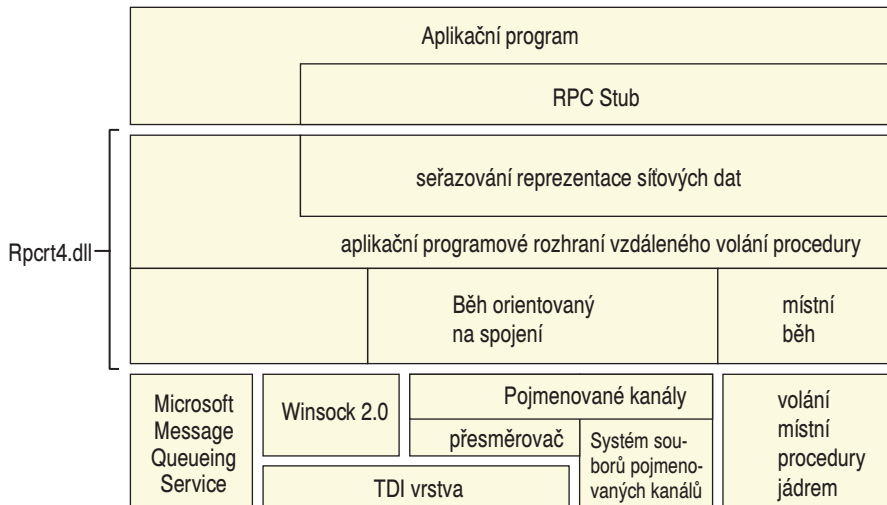


Obrázek B.15 Vzdálená volání procedur

Funkce interpretuje volání jako přicházející od aplikace klienta. Server může hrát roli klienta. Z důvodů zabezpečení může volání RPC používat ověřovací protokoly NTLM, Kerberos nebo Secure Sockets Layer (SSL). Když je funkce dokončena, jsou sebrány všechny vrácené hodnoty a po formátování jsou odeslány zpět klientovi prostřednictvím modulu při výpočtu volání RPC. Když se funkce vrací aplikaci klienta, má příslušná vrácená data nebo indikaci, že funkce selhala. Obrázek B.15 ilustruje vzdálená volání procedur.

Pokud je klientská i serverová část aplikace na stejném počítači, mohou být použita místní volání procedur (LPC) pro efektivní přenos informací mezi procesy. To dělá z volání RPC pružnou a přenosnou volbu komunikace mezi procesy.

Obrázek B.16 ilustruje softwarové součásti volání RPC.



Obrázek B.16 Architektura volání vzdáleného volání klienta a pracovní stanice v systému Windows 2000

Součásti vzdáleného volání procedury jsou:

Stub knihovna (RPC Stub) Část spustitelného souboru aplikace nebo knihovny DLL, která je generována překladačem Microsoft Interface Description Language (MIDL) specificky pro každé rozhraní.

Seřazování reprezentace síťových dat Seřazování je proces balíčkování a vybalování parametrů ve formátu Network Data Representation (NDR) pro komunikaci po síti.

Aplikační programová rozhraní vzdáleného volání procedury Řada aplikačních programových rozhraní, závislých na protokolech, zodpovědných za navázání spojení a zabezpečení jakož i registrování serverů, překlad názvů a koncových bodů.

Modul Datagram Runtime Nástroj protokolu bez spojení pro volání RPC, který přenáší a přijímá požadavky užitím protokolů bez spojení, jako je protokol UDP.

Modul Connection-Oriented Runtime Nástroj protokolu orientovaného na spojení pro volání RPC, který přenáší a přijímá požadavky užitím protokolů orientovaných na spojení, jako je protokol TCP.

Modul Local Runtime Nástroj místního protokolu pro volání RPC, který přenáší a přijímá požadavky mezi procesy na místním počítači.

Překlad názvů RPC

Funkce překladu názvů RPC umožňuje klientům nacházet servery RPC. Servery v síti Windows 2000 posílají zprávy službě Active Directory prostřednictvím lokátoru, což je softwarová služba, spuštěná na serverech RPC. Lokátor exportuje vazby, rozhraní, protokoly a koncové body pro servery, spuštěné na místním počítači. Tyto informace serveru jsou uloženy ve službě Active Directory ve složce System\RPCServices. Když chce klient najít server, položí dotaz službě Active Directory. Klient dostane informace včetně názvů serverů, protokolů a koncových bodů, které byly vloženy do služby Active Directory serverem. S těmito informacemi se může klient přímo spojit se serverem. systém Windows 2000 dále podporuje pojmenované kanály, poštovní přihrádky a všesměrové vysílání zpráv pro překlad názvů rozhraním NetBIOS.

Více informací o překladu názvů RPC najdete v části „Zveřejňování služeb v Active Directory“ v knize *Microsoft® Windows® 2000 Server Distribuované systémy*.

Pojmenované kanály a poštovní přihrádky

Pojmenované kanály a poštovní přihrádky jsou mechanismy komunikace mezi procesy vysoké úrovně, používané síťovými počítači. Pojmenované kanály a poštovní přihrádky jsou napsány jako ovladače systému souborů, takže implementace pojmenovaných kanálů a poštovních přihrádek se liší od implementace jiných mechanismů komunikace mezi procesy. Místní procesy mohou také používat pojmenované kanály a poštovní přihrádky. Jako u všech jiných systémů souborů se uskutečňuje vzdálený přístup k pojmenovaným kanálům a poštovním přihrádkám prostřednictvím přesměrovače Common Internet File System (CIFS). Přesměrovač zachycuje vstupně-výstupní požadavky a směřuje je na jednotku nebo prostředek na jiném počítači v síti. Přesměrovač umožňuje klientovi CIFS vyhledávat, otevírat, číst, zapisovat a odstraňovat soubory na jiném síťovém počítači se spuštěným přesměrovačem CIFS.

Pojmenované kanály

Pojmenované kanály zajišťují zpracování zpráv orientované na spojení použitím kanálů. Na spojení orientované zpracování zpráv požaduje, aby komunikace probíhala po virtuálním okruhu a udržovala spolehlivý a sekvenční přenos dat. Kanál je část paměti, která může být využita jedním procesem k předání informací jinému procesu. Kanál spojuje dva procesy tak, že výstup jednoho z nich je použit jako vstup druhého procesu. Tato technika se používá pro předávání dat mezi klientem a serverem. Pojmenované kanály jsou založeny na voláních rozhraní OS/2 API, které bylo vloženo do aplikačních programových rozhraní WNet. K pojmenovaným kanálům byla přidána další asynchronní podpora pro přenos dat mezi aplikacemi typu klient-server. Pojmenované kanály jsou podporovány z důvodu zpětné kompatibility se správcem sítě Microsoft® LAN Manager a příbuznými aplikacemi.

Operační systém Windows 2000 poskytuje speciální aplikační programová rozhraní pro zvýšení bezpečnosti pojmenovaných kanálů. Použitím vlastnosti nazvané zosobnění (impersonation) může server změnit svou zabezpečovací totožnost na totožnost klienta na druhé straně zprávy. Server má obvykle více oprávnění pro přístup k databázím na serveru než klient vyžadující služby. Když je serveru doručen požadavek pojmenovaným kanálem, server změní svou zabezpečovací totožnost na zabezpečovací totož-

nost klienta. To omezuje server pouze na oprávnění udělená klientovi, namísto jeho vlastních oprávnění, což vede ke zvýšení bezpečnosti pojmenovaných kanálů.

Poštovní přihrádky

Poštovní přihrádky jsou mechanismy komunikace mezi procesy vysoké úrovně bez spojení, často používané k nalezení a ohlašování služeb a počítačů. To znamená, že poštovní přihrádky jsou vysílací službou, používanou pro doručování zpráv. Doručení zprávy není zaručeno, ačkoliv míra doručení ve většině sítí je vysoká.

Operační systém Windows 2000 podporuje pouze poštovní přihrádky druhé třídy, nikoliv přihrádky první třídy. Poštovní přihrádky první třídy jsou orientované na spojení. Poštovní přihrádky druhé třídy zajišťují zpracování zpráv bez spojení pro všesměrově vysílané zprávy.

Poštovní přihrádka může být vytvořena na každém počítači v síti. Když je do přihrádky vyslána zpráva, odesílající aplikace specifikuje ve struktuře zprávy, zda jde o zprávu první nebo druhé třídy doručení. Zpracování zpráv bez spojení je nejužitečnější pro identifikaci jiných počítačů nebo služeb v síti, jako je například služba prohledávání, nabízená v operačním systému Windows 2000. Poštovní přihrádky jsou zahrnuty v systému pro zachování zpětné kompatibility s aplikacemi LAN Manager.

Systém Common Internet File System

Systém *Common Internet File System* (CIFS) je standardní způsob, kterým uživatelé sdílejí soubory v podnikových intranetech a v síti Internet. Protokol CIFS, vylepšená verze otevřeného víceplatformového protokolu Server Message Block (SMB), je přirozeným protokolem sdílení souborů v systému Windows 2000.

Protokol CIFS definuje řadu příkazů, používaných pro předávání informací mezi síťovými počítači. Přesměrovač balíčkuje požadavky, určené pro vzdálené počítače ve struktuře CIFS. Zprávy CIFS mohou být odeslány po síti vzdáleným zařízením. Přesměrovač rovněž používá protokol CIFS pro vytváření požadavků na zásobník protokolů místního počítače. Zprávy CIFS mohou být všeobecně klasifikovány následovně:

- Zprávy o navázání spojení se skládají z příkazů, které zahajují a ukončují spojení přesměrovače se sdíleným prostředkem na serveru.
- Zprávy oboru názvů a manipulace se soubory jsou používány přesměrovačem k získání přístupu k souborům na serveru a k jejich čtení a zapisování.
- Zprávy tiskáren jsou používány přesměrovačem k zasílání dat do tiskové fronty na serveru a k zjištění stavové informace o tiskové frontě.
- Různé zprávy jsou používány přesměrovačem pro zápis do poštovních přihrádek a pojmenovaných kanálů.

Některé z platforem, které protokol CIFS podporuje:

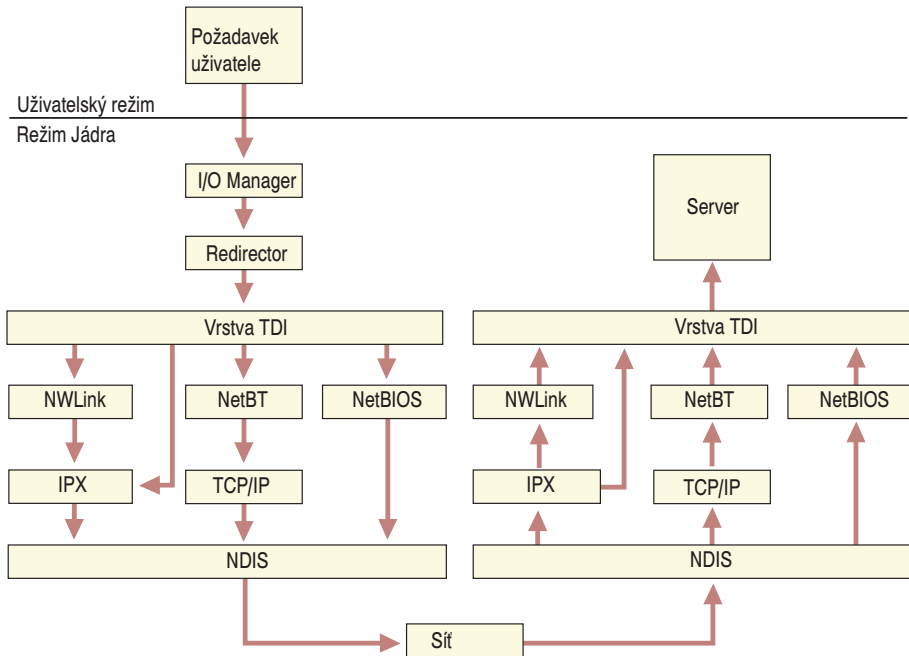
- Microsoft Windows 2000, Microsoft® Windows NT®, Microsoft® Windows® 98, Microsoft® Windows® 95
- Microsoft® OS/2 LAN Manager
- Microsoft® Windows® for Workgroups
- UNIX
- VMS
- Macintosh
- IBM LAN Server
- DEC PATHWORKS
- Microsoft® LAN Manager for UNIX
- 3Com 3+Open
- MS-Net

Protokol CIFS doplňuje protokol Hypertext Transfer Protocol (HTTP), protože poskytuje sofistikovanější sdílení a přenosy souborů než starší protokoly, jako FTP. Obsluha uživatelských požadavků na data ze síťového serveru protokolem CIFS je znázorněna na obrázku B.17.

Pokud se vyskytne požadavek na otevření sdíleného souboru, správce vstupů a výstupů (I/O Manager) volá přesměrovač a žádá jej o zvolení odpovídajícího transportního protokolu. Pro požadavky protokolu NetBIOS jsou zprávy protokolu NetBIOS zapouzdřeny do protokolu IP a transportovány sítí k příslušnému serveru. Požadavek je předán nahoru serveru, který pošle zpět data, aby vyhověl požadavku.

Součástí v přesměrovači, které poskytují podporu pro systém CIFS:

- Rdbss.sys
Všechny interakce na úrovni jádra jsou zahrnuty v tomto ovladači. Zahrnují všechny správce mezipaměti, správce paměti a požadavky na vzdálený systém souborů, takže určený protokol může použít požadovaný server.
- Mrxsmbs.sys
Minipřesměrovač pro systém CIFS má příkazy specifické pro CIFS.
- Mrxnfs.sys
Minipřesměrovač pro systém Network File System (NFS) zajišťuje podporu pro NFS. Mrxnfs.sys je obsažen ve službách pro Unix (Services for Unix).



Obrázek B.17 Architektura protokolu CIFS

V systému Windows NT 4.0 byly služby překladačů názvů Windows Internet Name Service (WINS) a Domain Name System (DNS) vykonávány použitím portu 134 protokolu TCP. Rozšíření protokolů CIFS a NetBT nyní umožňují přímá spojení přes protokol TCP/IP použitím portu 445 protokolu TCP. Oba způsoby překladačů jsou stále dostupné v systému Windows 2000. Jednu nebo obě z těchto služeb lze vypnout v registru.

Vlastnosti, které nabízí systém CIFS:

Integrita a souběžnost Protokol CIFS umožňuje více klientům zpřístupňovat a měnit stejný soubor a brání přitom konfliktům zajišťováním sdílení a zamykání souborů. Sdílení a zamykání souborů je proces, umožňující jednomu uživateli najednou přístup k souboru a blokování přístupu ostatních uživatelů. Tyto mechanismy sdílení a zamykání mohou být použity v síti Internet a v intranetech. Dovolují rovněž agresivní využití mezipaměti a čtení napřed a zapisování později bez ztráty integrity. Mezipaměti vyrovnávacích pamětí souboru musí být vyprázdněny předtím, než je soubor použitelný pro jiné klienty. Tyto schopnosti zaručují, že pouze jedna kopie souboru může být najednou aktivní, čímž zabráňují poškození dat.

Optimalizace pomalých spojů Protokol CIFS byl vyladěn tak, aby dobře fungoval na pomalých linkách s vytáčeným spojením. Výsledkem je zlepšený výkon pro uživatele, kteří používají pro přístup k síti Internet modem.

Zabezpečení Server CIFS podporuje anonymní přenosy i zabezpečený, ověřený přístup k k pojmenovaným souborům. Zásady zabezpečení souborů a adresářů se snadno spravují.

Výkon a škálovatelnost Servery CIFS jsou vysoce integrované v operačním systému a vyladěné na maximální výkon systému.

Názvy souborů Unicode Názvy souborů mohou být v libovolné znakové sadě, nejen ve znakových sadách vytvořených pro angličtinu nebo západoevropské jazyky.

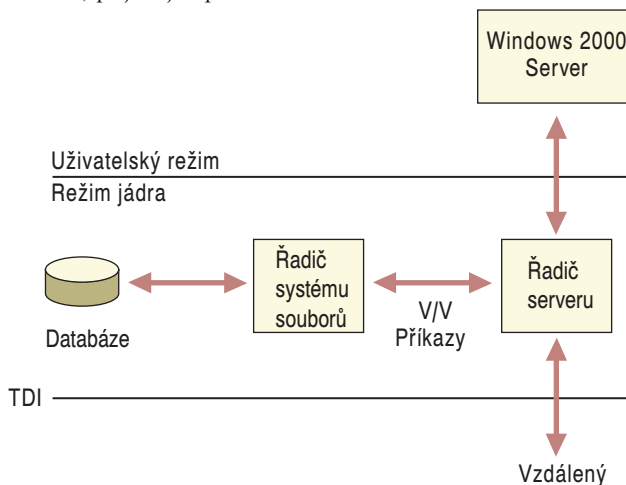
Globální názvy souborů Uživatelé nemusí připojovat vzdálené systémy souborů, ale mohou na ně odkazovat přímo použitím globálně významných názvů (názvů, které mohou být umístěny kdekoliv v síti Internet), místo názvů, které mají pouze místní význam (na místním počítači nebo v místní síti LAN). Distribuované systémy souborů umožňují uživatelům vytvářet obor názvů pro celý podnik. Podporovány jsou názvy souborů v konvenci Uniform Naming Convention (UNC), takže nemusí být vytvořeno písmeno označení jednotky před přístupem ke vzdálenému souboru.

Základní síťové služby

Síťové služby podporují aplikační programy a poskytují součásti a aplikační programová rozhraní nezbytné pro přístup k souborům na síťových počítačích. Služba serveru i služba pracovní stanice může rovněž podporovat přístup ke vstupně-výstupním požadavkům.

Služba serveru

Služba serveru se nachází nad rozhraním TDI a je implementována jako ovladač systému souborů. Služba serveru CIFS spolupracuje přímo s jinými ovladači systému souborů při uspokojování vstupně-výstupních požadavků, jako například čtení nebo zápis souboru. Služba serveru dodává spojení, požadovaná přesměrovači na straně klienta a poskytuje jim přístup k prostředkům, které vyžadují. Obrázek B.18 ukazuje službu serveru, přijímající požadavek na data.



Obrázek B.18 Služba serveru

Když služba serveru přijme požadavek od vzdáleného počítače, žádajícího o čtení souboru, který je umístěn na místním disku, dojde k následujícím krokům:

1. Síťové ovladače nižší úrovně přijmou požadavek a předají jej ovladači serveru.
2. Služba serveru předá požadavek příslušnému ovladači místního systému souborů.
3. Ovladač místního systému souborů volá ovladače disku nižší úrovně pro přístup k souboru.
4. Data jsou předána zpět ovladači místního systému souborů.
5. Ovladač místního systému souborů předá data zpět službě serveru.
6. Služba serveru předá data síťovým ovladačům nižší úrovně pro přenos zpět vzdálenému počítači.

Služba serveru se skládá ze dvou částí:

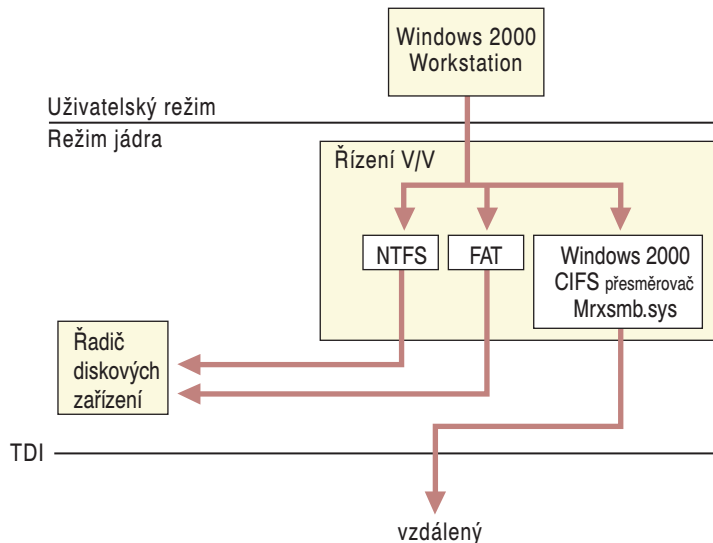
- Služba serveru je součástí modulu Services.exe. Modul Services.exe je správce řízení služeb, ve kterém začínají všechny služby. Narozdíl od služby pracovní stanice není služba serveru závislá na hromadném zprostředkovateli univerzální konvence pro názvy (MUP). Služba MUP vybírá odpovídajícího zprostředkovatele konvence UNC k obsluze požadavků.
- Modul Srv.sys je ovladač systému souborů, který obsluhuje interakce s nižšími úrovněmi zásobníku protokolů a přímo spolupracuje s různými zařízeními systému souborů, aby vyhověl požadavkům příkazů, jako jsou čtení a zápis souborů.

Služba pracovní stanice

Všechny požadavky uživatelského režimu ze služby MUP procházejí službou pracovní stanice. Tato služba se skládá ze dvou součástí:

- Rozhraní uživatelského režimu, které sídlí v modulu Services.exe v systému Windows 2000.
- Přesměrovač (Mrxsm.sys), ovladač systému souborů, který spolupracuje se síťovými ovladači nižší úrovně pomocí prostředků rozhraní TDI.

Služba pracovní stanice přijímá požadavek uživatele a předává jej přesměrovači režimu jádra. Služba pracovní stanice je zobrazena na obrázku B.19.



Obrázek B.19 Služba pracovní stanice

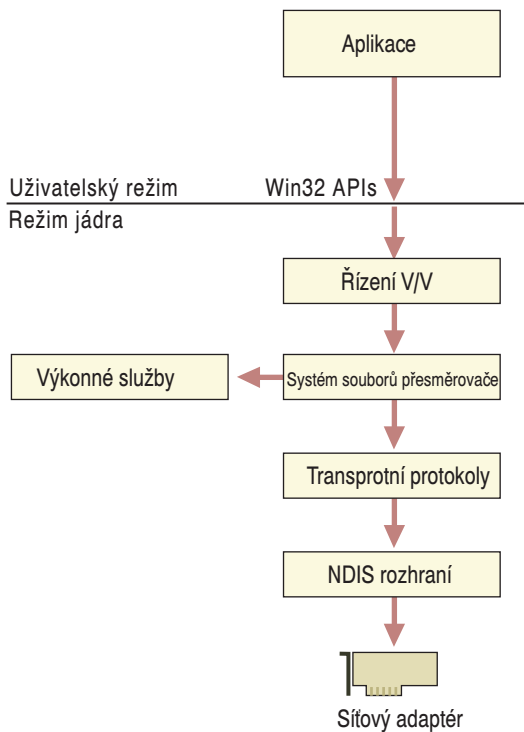
Přesměrovač Windows 2000 Redirector

Přesměrovač je součást, která sídlí nad rozhraním TDI a přes kterou jeden počítač získává přístup k jinému počítači. Přesměrovač operačního systému Windows 2000 umožňuje spojení se servery Windows 98, Windows 95, Windows for Workgroups, LAN Manager, LAN Server, a s dalšími servery protokolu CIFS. Přesměrovač komunikuje s protokoly pomocí prostředků rozhraní TDI.

Přesměrovač je implementován jako ovladač systému souborů Windows 2000. Implementace přesměrovače jako systému souborů má mnoho výhod:

- Umožňuje aplikacím volat jedno aplikační programové rozhraní (Windows 2000 I/O API) pro přístup k souborům na místním i na vzdálených počítačích. Z pohledu správce vstupně-výstupních operací není rozdíl mezi přístupem k souborům, uloženým na vzdáleném počítači v síti a přístupem k souborům uloženým místně na pevném disku.
- Je spuštěn v režimu jádra a může přímo volat jiné ovladače a jiné součásti režimu jádra, jako je správce mezí paměti. To zlepšuje výkon přesměrovače.
- Může být dynamicky zaváděn a uvolňován, jako každý jiný ovladač systému souborů.
- Může existovat společně s jinými přesměrovači.

Obrázek B.20 ukazuje síťovou architekturu přesměrovače Windows 2000 Redirector.



Obrázek B.20 Přesměrovač Windows 2000 Redirector

Spolupráce s jinými sítěmi

Kromě spojení s Windows 98, Windows 95, sítěmi sobě rovných (peer-to-peer), sítěmi LAN Manager, LAN Server, servery MS-Net, může přesměrovač systému Windows 2000 existovat společně s přesměrovači pro jiné sítě, jako jsou síť Novell NetWare a síť UNIX.

Zprostředkovatelé a vrstva rozhraní zprostředkovatelů

Pro každý další typ sítě, jako jsou síť NetWare nebo síť UNIX, musíte instalovat součást, zvanou poskytovatel (provider). Poskytovatel je součást, která umožňuje počítači se spuštěným systémem Windows 2000 Server nebo Windows 2000 Professional komunikovat se sítí. Operační systém Windows 2000 obsahuje několik poskytovatelů: služba Client Services for NetWare a Gateway Services for NetWare.

Služba Client Services for NetWare je obsažena v systému Windows 2000 Professional a umožňuje počítači se spuštěným systémem Windows 2000 Professional, aby se připojil jako klient do sítě NetWare. Služba Gateway Services, obsažená v systému Windows 2000 Server, umožňuje počítači se spuštěným systémem Windows 2000, aby se připojoval jako klient k síti NetWare a poskytoval služby brány mezi klienty sítí Microsoft a servery sítě Novell NetWare. Další zprostředkovatelské knihovny DLL jsou dodávány příslušnými dodavateli sítí.

Přístup ke vzdálenému souboru

Když proces na počítači se systémem Windows 2000 zkouší otevřít soubor, který sídlí na vzdáleném počítači, dojde k následujícím krokům:

1. Proces volá správce vstupně-výstupních operací s požadavkem na otevření souboru.
2. Správce vstupně-výstupních operací rozpozná, že požadavek je na soubor na vzdáleném počítači a předá požadavek ovladači-přesměrovači systému souborů.
3. Přesměrovač předá požadavek síťovým ovladačům nižší úrovně, které ho přenesou vzdálenému serveru ke zpracování.

Přístup k síťovým prostředkům

Aplikace sídlí nad přesměrovačem a službami serveru v uživatelském režimu. Jako u všech ostatních vrstev v síťové architektuře systému Windows 2000 existuje jednotné rozhraní pro přístup k síťovým prostředkům, které je nezávislé na všech přesměrovačích, instalovaných v systému. Přístup k prostředkům je poskytován hromadným zprostředkovatelem univerzální konvence pro názvy (MUP) a směrovačem hromadného zprostředkovatele (MPR).

Hromadný zprostředkovatel univerzální konvence pro názvy

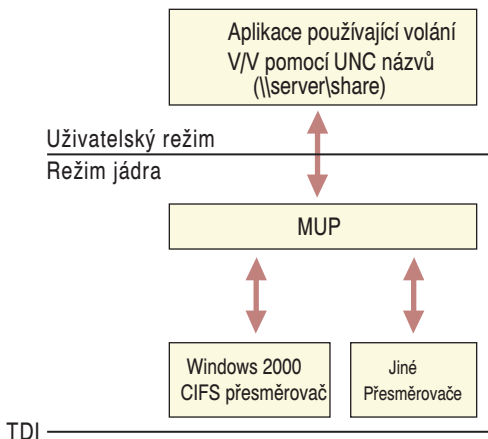
Když aplikace provádí vstupně-výstupní volání, obsahující názvy univerzální konvence pro názvy (UNC), jsou tyto požadavky předány hromadnému zprostředkovateli UNC (MUP). Služba MUP vybírá příslušného zprostředkovatele UNC (přesměrovač) pro obsluhu tohoto vstupně-výstupního požadavku.

Názvy univerzální konvence pro názvy

UNC je názvová konvence pro popis síťových serverů a sdílených bodů těchto serverů. Názvy UNC začínají dvěma obrácenými lomítky, následovanými názvem serveru.

Všechna další pole v názvu jsou oddělena jedním obráceným lomítkem. Typický název UNC vypadá jako: `\\server\share\subdirectory\filename`.

Ne všechny součásti názvu UNC musí být přítomny v každém příkazu; vyžadována je pouze součást s názvem sdílení. Například příkaz `dir \\servername\sharename` může být použit pro výpis adresáře kořenu specifikovaného sdílení. Jedním z cílů návrhu síťového prostředí Windows 2000 je poskytnutí platformy, na které mohou stavět ostatní. Služba MUP je vitální součástí pro umožnění současné existence více přesměrovačů v jednom počítači. Služba MUP zbavuje aplikace nutnosti udržovat své vlastní seznamy poskytovatelů UNC. Pokud je přítomno více přesměrovačů, musí existovat prostředek pro rozhodování, který z nich se použije. Funkcí služby MUP je vystupovat jako arbitr pro rozhodnutí, který přesměrovač je nejvhodnější pro použití. Obrázek B.21 zobrazuje architekturu služby MUP systému Windows 2000.



Obrázek B.21 Architektura služby MUP

Služba MUP je ovladač, narozdíl od rozhraní TDI, který pouze definuje způsob, jak součást v jedné vrstvě komunikuje se součástí v jiné vrstvě. Služba MUP také definovala cesty ke zprostředkovatelům UNC (přesměrovačům).

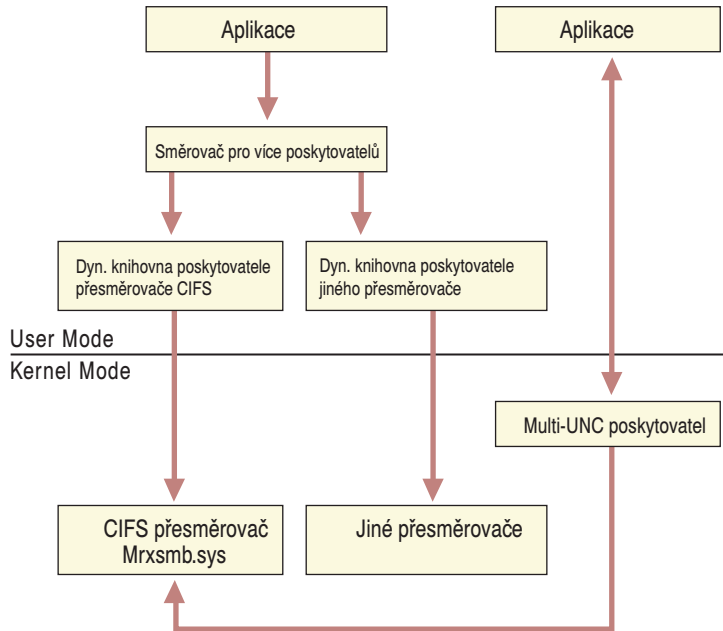
Požadavky vstupů a výstupů od aplikací, které obsahují názvy UNC jsou přijímány správcem vstupů a výstupů, který předává požadavky službě MUP. Pokud služba MUP neviděla název UNC během předchozích 15 minut (toto je pouze přibližné určení času a může se změnit), zašle služba MUP název každému ze zprostředkovatelů UNC, které registruje. Služba MUP je nezbytnou podmínkou pro službu pracovní stanice.

Když je službou MUP přijat požadavek, obsahující název UNC, zkontroluje služba MUP všechny přesměrovače, aby zjistila, který z nich může zpracovat požadavek. Služba MUP hledá přesměrovač s nejvyšší registrovanou prioritou odezvy, který prohlašuje, že dokáže navázat spojení k názvu UNC. Toto spojení zůstává po celou dobu aktivity. Pokud se za dobu 15 minut neobjeví požadavek (to je pouze přibližný čas a podléhá změně) na název UNC, dohodne služba MUP nalezení jiného vhodného přesměrovače.

Směrovač hromadného zprostředkovatele

Ne všechny programy používají názvy UNC ve svých vstupně-výstupních operacích. Některé aplikace používají aplikační programová rozhraní WNet, což jsou síťová aplikační programová rozhraní Win32. Směrovač hromadného zprostředkovatele (MPR) byl vytvořen pro podporu těchto aplikací.

Služba MPR je podobná službě MUP. Služba MPR přijímá příkaz rozhraní WNet, určuje příslušný přesměrovač a předává příkaz tomuto přesměrovači. Protože různí dodavatelé sítí používají různá rozhraní pro komunikaci se svými přesměrovači, existuje řada zprostředkovatelských knihoven DLLs mezi službou MPR a přesměrovači. Zprostředkovatelské knihovny DLL poskytují standardní rozhraní, takže služba MPR s nimi může komunikovat. Příslušné knihovny DLL berou požadavek ze služby MPR a předají jej svému odpovídajícímu přesměrovači. Obrázek B.22 ilustruje architekturu směrovače hromadného zprostředkovatele.



Obrázek B.22 Směrovač hromadného zprostředkovatele

Zprostředkovatelské knihovny DLL jsou dodávány dodavatelem síťového přesměrovače a instalovány automaticky při instalaci přesměrovače.

Poznámka: Akronym MPR je rovněž používán pro službu Multi-Protocol Routing, řadu směrovacích součástí, dodávaných se systémem Windows NT 4. V systému Windows 2000 se ze služby Multi-Protocol Routing stala služba Routing and Remote Access Service.

Další zdroje

- Více informací o síťovém programování v systému Windows 2000 najdete v odkazu Microsoft Platform Software Development Kit (SDK) na webové stránce <http://windows.microsoft.com/windows2000/reskit/webresources>.

- Více informací o vývoji ovladačů pro rozhraní NDIS najdete v odkazu Microsoft Platform Software Development Kit (SDK) na webové stránce <http://windows.microsoft.com/windows2000/reskit/webresources>.

PŘÍLOHA C

Přiřazení portů TCP a UDP



Porty protokolu Transport Control Protocol (TCP) a User Datagram Protocol (UDP) a čísla protokolů jsou důležité pro vytváření sítí TCP/IP, intranetů a sítě Internet. Porty a čísla protokolů zajišťují přístup k hostitelskému počítači. Tvoří však také bezpečnostní riziko, protože povolují nežádoucí přístupy. Proto bezpečnost sítě zvyšuje znalost toho, který port povolit a který zakázat. Pokud jsou z důvodů zabezpečení zakázány nesprávné porty nebo čísla protokolů v zabezpečení systému proti průniku zvenčí (firewall), ve směrovači nebo v serveru proxy, může se stát, že se znepřístupní nezbytné služby.

V této příloze

Úlohy portů a čísel protokolů 662

Čísla protokolů 669

Příbuzné informace v Resource Kitu

- Úplný seznam dobře známých portů, registrovaných portů a čísel protokolů najdete v odkazu Port Assignments na webové stránce <http://windows.microsoft.com/windows2000/reskit/webresources>.

Úlohy portů a čísel protokolů

V sítích TCP/IP je port mechanismem, který umožňuje počítači současně podporovat více komunikačních relací s počítači a programy v síti. Port směřuje požadavek ke konkrétní službě, která se nachází na této adrese IP. Cíl paketu může být dále zadán použitím jedinečného čísla portu. Číslo portu je určeno při navázání spojení.

Organizace Internet Assigned Numbers Authority (IANA) definuje jedinečné parametry a hodnoty protokolů, nezbytné pro fungování sítě Internet a její budoucí rozvoj. V minulosti byla tato čísla dokumentována řadou dokumentů RFC. Od té doby jsou úlohy portů uvedeny na webových stránkách organizace IANA a tyto údaje jsou stále aktualizovány a opravovány, když jsou dostupné nové informace nebo jsou provedena nová přiřazení. Popis portů a protokolů v této kapitole pochází od organizace IANA. Společenství Internet Engineering Task Force (IETF) je řídicí a vývojová sekce protokolů pro Internet. Rovněž společnost Internet Society (ISOC), profesionální organizace internetových expertů, komentuje zásady a postupy a dohlíží na řadu dalších komisí a organizací, které se zabývají tématy zásad sítě. Více informací o úlohách portů najdete v odkazu Port Assignments na webových stránkách <http://windows.microsoft.com/windows2000/reskit/webresources>.

Tato příloha popisuje výchozí přiřazení portů v systémech Microsoft® Windows® 2000 Server a Microsoft® Windows® 2000 Professional a čísla protokolů IP. Čísla protokolů směřují paket příslušnému protokolu, jako je protokol UDP nebo TCP, který je o jednu úroveň výše v zásobníku protokolů. Tato příloha obsahuje tři tabulky:

- Tabulka C.1 uvádí dobře známé porty (Well-Known Ports).
- Tabulka C.2 uvádí registrované porty.
- Tabulka C.3 uvádí porty protokolů TCP a UDP, které podporují běžně používané služby systému Windows 2000.
- Tabulka C.4 uvádí čísla protokolů IP a funkce, které podporují.

Dynamické porty jsou podle své definice náhodně přiřazovány a proto nejsou známy, dokud není provedeno přiřazení. Soukromé porty nejsou registrovány u organizace IANA, ale jsou používány softwarovými aplikacemi.

Přiřazení portů pro dobře známé porty

Dobře známé porty jsou přiřazovány organizací IANA.

Porty se používají v komunikacích TCP nebo UDP k pojmenování konců logických spojení, která přenášejí data. Porty byly vytvořeny pro poskytování služeb neznámým klientům. Tabulka C.1 udává porty používané procesem serveru jako jeho styčné porty. Styčnému portu se také někdy říká dobře známý port.

Přiřazené porty používají malou část možných čísel portů. Po mnoho let měly přiřazené porty čísla v rozsahu od 0 do 255. Rozsah přiřazených portů spravovaných organizací IANA byl rozšířen na rozmezí od 0 do 1023. Seznam v tabulce C.1 obsahuje větší počet přiřazení portů, které mají význam pro operační systém Windows 2000.

Tabulka C.1 Dobře známé porty

Číslo portu	Protokol	Název služby	Alias	Komentář
7	TCP	echo		Služba Echo
7	UDP	echo		Služba Echo

Číslo portu	Protokol	Název služby	Alias	Komentář
9	TCP	discard	sink null	Služba Discard
9	UDP	discard	sink null	Služba Discard
13	TCP	daytime		Služba Daytime
13	UDP	daytime		Služba Daytime
17	TCP	qotd	quote	Služba Quote of the day
17	UDP	qotd	quote	Služba Quote of the day
19	TCP	chargen	ttytst source	Služba Character generator
19	UDP	chargen	ttytst source	Služba Character generator
20	TCP	ftp-data		Přenos souborů
21	TCP	ftp		Řízení FTP
23	TCP	telnet		Protokol Telnet
25	TCP	smtp	mail	Protokol Simple Mail Transfer Protocol
37	TCP	time		Služba Time
37	UDP	time		Služba Time
39	UDP	rlp	resource	Protokol Resource Location Protocol
42	TCP	nameserver	name	Hostitelský názvový server
42	UDP	nameserver	name	Hostitelský názvový server
43	TCP	nicname	whois	Služba Who Is
53	TCP	domain		Název domény
53	UDP	domain		Názvový server domény
67	UDP	bootps	dhcps	Server spouštěcího protokolu
68	UDP	bootpc	dhcpc	Klient spouštěcího protokolu
69	UDP	tftp		Protokol Trivial File Transfer
70	TCP	gopher		Služba Gopher
79	TCP	finger		Služba Finger
80	TCP	http	www, http	Služba World Wide Web
88	TCP	kerberos	krb5	Ověřovací protokol Kerberos
88	UDP	kerberos	krb5	Ověřovací protokol Kerberos
101	TCP	hostname	hostnames	Hostitelský názvový server NIC
102	TCP	iso-tsap		ISO-TSAP Class 0
107	TCP	rtelnet		Vzdálená služba Telnet
109	TCP	pop2	postoffice	Protokol Post Office Protocol – Version 2
110	TCP	pop3	postoffice	Protokol Post Office Protocol – Version 3
111	TCP	sunrpc	rpcbind portmap	Vzdálené volání procedury SUN
111	UDP	sunrpc	rpcbind portmap	Vzdálené volání procedury SUN
113	TCP	auth	ident tap	Ověřovací služba

Číslo portu	Protokol	Název služby	Aliasy	Komentář
117	TCP	uucp-path		Služba UUCP Path Service
119	TCP	nntp	usenet	Protokol Network News Transfer Protocol
123	UDP	ntp		Protokol Network Time Protocol
135	TCP	epmap	loc-srv	Překlad koncových bodů DCE
135	UDP	epmap	loc-srv	Překlad koncových bodů DCE
137	TCP	netbios-ns	nbname	Názvová služba NETBIOS
137	UDP	netbios-ns	nbname	Názvová služba NETBIOS
138	UDP	netbios-dgm	nbdatagram	Datagramová služba NETBIOS
139	TCP	netbios-ssn	nbssession	Relační služba NETBIOS
143	TCP	imap	imap4	Protokol Internet Message Access Protocol
158	TCP	pcmail-srv	repository	Server PC Mail Server
161	UDP	snmp	snmp	Protokol SNMP
162	UDP	snmptrap	snmp-trap	Služba SNMP TRAP
170	TCP	print-srv		Síťový PostScript
179	TCP	bgp		Protokol Border Gateway Protocol
194	TCP	irc		Protokol Internet Relay Chat Protocol
213	UDP	ipx		Protokol IPX přes IP
389	TCP	ldap		Protokol Lightweight Directory Access Protocol
443	TCP	https	MCom	
443	UDP	https	MCom	
445	TCP			Microsoft CIFS
445	UDP			Microsoft CIFS
464	TCP	kpasswd		Ověřovací protokol Kerberos (v5)
464	UDP	kpasswd		Ověřovací protokol Kerberos (v5)
500	UDP	isakmp	ike	Protokol Internet Key Exchange (IPSec)
512	TCP	exec		Vzdálené provádění procesů
512	UDP	biff	comsat	Upozorňuje uživatele na novou poštu
513	TCP	login		Vzdálené přihlášení
513	UDP	who	whod	Databáze přihlášených, průměrné zatížení
514	TCP	cmd	shell	Automatické ověřování
514	UDP	syslog		
515	TCP	printer	spooler	Naslouchá příchozím spojením
517	UDP	talk		Navazuje spojení TCP
518	UDP	ntalk		
520	TCP	efs		Rozšířený server názvů souborů

Číslo portu	Protokol	Název služby	Alias	Komentář
520	UDP	router	router routed	Protokol RIPv.1, RIPv.2
525	UDP	timed	timeserver	Timeserver
526	TCP	tempo	newdate	Služba Newdate
530	TCP,UDP	courier	rpc	Vzdálené volání procedury (RPC)
531	TCP	conference	chat	Služba IRC Chat
532	TCP	netnews	readnews	Služba Readnews
533	UDP	netwall		Pro nouzová vysílání
540	TCP	uucp	uucpd	Uucpd
543	TCP	klogin		Přihlášení protokolu Kerberos
544	TCP	kshell	krcmd	Vzdálené prostředí Kerberos
550	UDP	new-rwho	new-who	Služba New-who
556	TCP	remotefs	rfs rfs_server	Server Rfs
560	UDP	rmonitor	rmonitord	Služba Rmonitor
561	UDP	monitor		
636	TCP	ldaps	sldap	Protokol LDAP přes TLS/SSL
749	TCP	kerberos-adm		Správa protokolu Kerberos
749	UDP	kerberos-adm		Správa protokolu Kerberos

Přiřazení portů pro registrované porty

Registrované porty, porty mezi 1024 a 49151 jsou uvedeny organizací IANA a na většině systémů mohou být používány aplikacemi nebo programy, prováděnými uživateli. Tabulka C.2 specifikuje port, používaný procesem serveru jako jeho styčný port. Organizace IANA registruje použití těchto portů pro pohodlí internetové veřejnosti. V možné míře jsou stejná přiřazení portů použita v protokolu UDP. Registrované porty jsou v číselném rozsahu od 1024 do 49151. Registrovaným portům mezi 1024 a 5000 se také říká pomíjivé porty. Seznam uvedený níže obsahuje většinu úloh portů, které jsou významné pro systém Windows 2000.

Tabulka C.2 Registrované porty

Číslo portu	Protokol	Název služby	Alias	Komentář
1109	TCP	kpop		Služba Kerberos POP
1167	UDP	phone		Konferenční volání
1433	TCP	ms-sql-s		Microsoft-SQL-Server
1433	UDP	ms-sql-s		Microsoft-SQL-Server
1434	TCP	ms-sql-m		Microsoft-SQL-Monitor
1434	UDP	ms-sql-m		Microsoft-SQL-Monitor
1512	TCP	wins		Služba Microsoft Windows Internet Name Service

Číslo portu	Protokol	Název služby	Aliasy	Komentář
1512	UDP	wins		Služba Microsoft Windows Internet Name Service
1524	TCP	ingreslock	ingres	Služba Ingres
1701	UDP	l2tp		Protokol Layer Two Tunneling Protocol
1723	TCP	pptp		Protokol Point-to-point tunneling protocol
1812	UDP	radiusauth		Protokol RRAS (RADIUS authentication protocol)
1813	UDP	radacct		Protokol RRAS (RADIUS accounting protocol)
2049	UDP	nfsd	nfs	Server Sun NFS
2053	TCP	knetd		Služba Kerberos de-multiplexer
2504	UDP	nlbs		Vyrovňávání zatížení sítě
9535	TCP	man		Server Remote Man

Přirazení portů obecně používaným službám

V operačním systému Windows 2000 je mnoho přidružených služeb. Tyto služby mohou pro svou funkci vyžadovat více než jeden port protokolu TCP nebo UDP. Tabulka C.3 udává výchozí porty, používané zmíněnými službami.

Tabulka C.3 Výchozí přiřazení portů pro obecné služby

Název služby	UDP	TCP
Datagramy odezvy Vyhledávání rozhraní NetBIOS přes TCP/IP	138	
Žádosti Vyhledávání rozhraní NetBIOS přes TCP/IP	137	
Komunikace klient-server		135
Common Internet File System (CIFS)	445	139, 445
Content Replication Service		560
Cybercash Administration		8001
Cybercash Coin Gateway		8002
Cybercash Credit Gateway		8000
DCOM (Správce řízení služeb používá udp/tcp k dynamickému přiřazení portů pro model DCOM)	135	135
Klient DHCP		67
Server DHCP		68
Správce DHCP		135
Správa DNS		139
vyhledávání serveru DNS klientem (mění se)	53	53
Exchange Server 5.0		
Client Server Communication		135
Exchange Administrator		135

Název služby	UDP	TCP
IMAP		143
IMAP (SSL)		993
LDAP		389
LDAP (SSL)		636
MTA – X.400 over TCP/IP		102
POP3		110
POP3 (SSL)		995
RPC		135
SMTP		25
NNTP		119
NNTP (SSL)		563
Hledání názvů sdílených položek	137	
Relace sdílení souborů		139
FTP		21
FTP-data		20
HTTP		80
HTTP-Secure Sockets Layer (SSL)		443
Internet Information Services (IIS)		80
IMAP		143
IMAP (SSL)		993
IKE (Více informací najdete v tabulce C.4)	500	
IPSec Authentication Header (AH) (Více informací najdete v tabulce C.4)		
IPSec Encapsulation Security Payload (ESP) (Více informací najdete v tabulce C.4)		
IRC		531
ISPMOD (SBS 2. pořadí průvodce registrací DNS)		1234
Kerberos de-multiplexer		2053
Kerberos klogin		543
Kerberos kpasswd (v5)	464	464
Kerberos krb5	88	88
Kerberos kshell		544
L2TP	1701	
LDAP		389
LDAP (SSL)		636
Přihlašovací posloupnost	137, 138	139
Macintosh, souborové služby (AFP/IP)		548
Členství DPA		568
Členství MSN		569
Microsoft Chat klient-server		6667
Microsoft Chat server-server		6665
Microsoft Message Queue Server	1801	1801
Microsoft Message Queue Server	3527	135, 2101

Název služby	UDP	TCP
Microsoft Message Queue Server		2103,2105
MTA – X.400 přes TCP/IP		102
Datagramy NetBT	138	
Hledání názvů NetBT	137	
relace služeb NetBT		139
NetLogon	138	
NetMeeting Audio Call Control		1731
Nastavení volání programu NetMeeting H.323		1720
proud RTP přes UDP programu NetMeeting H.323	Dynamic	
NetMeeting Internet Locator Server ILS		389
Proud zvukových dat programu NetMeeting RTP	Dynamic	
NetMeeting T.120		1503
Služba umístění uživatelů programu NetMeeting		522
Vyrovňování zatížení sítě	2504	
NNTP		119
NNTP (SSL)		563
Outlook (porty viz „Exchange“)		
Průchozí Ověřování	137, 138	139
POP3		110
POP3 (SSL)		995
Řízení PPTP		1723
Data PPTP (viz Tabulka C.4)		
Hledání názvů sdílení tiskáren	137	
Relace sdílení tiskáren		139
Účtování Radius (Routing and Remote Access)	1646 or 1813	
Ověřování Radius (Routing and Remote Access)	1645 or 1812	
Vzdálená instalace TFTP		69
Požadavky relace RPC klienta s použitím pevného portu		1500
Replikace relace RPC klienta s použitím pevného portu		2500
porty relací RPC		Dyna- mické
správce uživatelů RPC, správce služeb RPC, mapovač portů RPC		135
Správce řízení služeb (SCM) používaný modulem DCOM	135	135
SMTP		25
SNMP	161	
Depeše SNMP	162	
Hledání názvů pro šifrování pojmenovaných kanálů SQL nad jinými protokoly	137	
Hledání názvů pro šifrování vzdáleného volání procedury SQLnad jinými protokoly	137	
Relace SQL		139
Relace SQL		1433

Název služby	UDP	TCP
Relace SQL		1024 – 5000
Mapovač relace SQL		135
Hledání názvu pro SQL klienta TCP	53	53
Telnet		23
Terminal Server		3389
Tisk UNIX		515
Správce rozhraní WINS		135
Názvová služba NetBios přes TCP/IP WINS	137	
WINS Proxy	137	
Registrace WINS		137
Replikace WINS		42
X400		102

Čísla protokolů

V hlavičce IP identifikuje pole Protocol službu v nejbližší vyšší úrovni v zásobníku protokolů, které se předávají data. Tabulka C.4 uvádí tato obecně používaná čísla protokolů IP. Čísla protokolů se používají při nastavování zabezpečení systému proti průniku zvenčí (firewall), směrovačů a serverů proxy.

Tabulka C.4 Obecná čísla protokolů

Služba	Číslo protokolu
Internet Control Message Protocol (ICMP)	1
Transmission Control Protocol (TCP)	6
User Datagram Protocol (UDP)	17
General Routing Encapsulation (Data PPTP přes GRE)	47
Authentication Header (AH) IPsec	51
Encapsulation Security Payload (ESP) IPsec	50
Exterior Gateway Protocol (EGP)	8
Gateway-Gateway Protocol (GGP)	3
Host Monitoring Protocol (HMP)	20
Internet Group Management Protocol (IGMP)	88
MIT Remote Virtual Disk (RVD)	66
OSPF Open Shortest Path First	89
PARC Universal Packet Protocol (PUP)	12
Reliable Datagram Protocol (RDP)	27
Reservation Protocol (RSVP) QoS	46

Další zdroje

- Aktuální seznam čísel protokolů a portů protokolů TCP a UDP naleznete v odkazech Internet Assigned Numbers Authority (IANA) na webové stránce <http://windows.microsoft.com/windows2000/reskit/webresources>.

PŘÍLOHA D

Vzdálené nástroje TCP/IP



Nástroje popsané v této příloze umožňují správci sítě spravovat síťové počítače na dálku. Mnoho z nich je podobných nástrojům systému UNIX.

V této příloze

Finger 672

Ftp 672

Rcp 674

Rexec 677

Rsh 678

Telnet 679

Tftp 680

Poznámka: Všechna hesla používaná síťovými službami systému Windows jsou šifrována. Připojovací nástroje Ftp a Rexec však spoléhají na ověřování hesla v jasném textu vzdáleným počítačem. Hesla v jasném textu nejsou šifrována před odesláním do sítě. To umožňuje jinému uživateli ve stejné síti, vybavenému síťovým analyzátořem, ukrást heslo vzdáleného účtu. Při připojování pomocí prostředků Ftp, Rexec nebo Telnet ke vzdáleným počítačům, které nepoužívají systém Microsoft, volte proto hesla, která se liší od hesel, používaných v počítačích nebo doménách, založených na systému Windows 2000. Pověšměte si, že protokoly samy o sobě zabráňují šifrování; hesla v jasném textu nejsou standardem, který je doporučován společností Microsoft.

Finger

Tento přípojovací příkaz zobrazuje informace o uživateli na určeném hostitelském počítači se spuštěnou službou Finger. Výstup je různý v závislosti na nastavení vzdáleného hostitelského počítače.

Syntaxe **finger [-l]** [uživatel]@název_hostitelského_počítače

Přepínače **-l**

Zobrazuje informace ve formátu dlouhého seznamu, není podporován na všech vzdálených počítačích.

Proměnné *uživatel*

Určuje uživatele, o němž požadujete informace. Vynecháním tohoto parametru zobrazíte informace o všech uživateli určeného hostitelského počítače.

@název_hostitelského_počítače

Specifikuje název nebo adresu IP vzdáleného hostitelského počítače, o jehož informacích chcete získat informace.

Ftp

Tento nástroj připojení přenáší soubory oběma směry s hostitelským počítačem se spuštěnou službou serveru FTP (jako je služba Microsoft® Internet Information Services). V systému Unix se takové službě říká démon – daemon. Nástroj Ftp používá na relaci orientovaný protokol File Transfer Protocol. Nástroj Ftp může být použit interaktivně nebo v režimu zpracování textových souborů ASCII.

Syntaxe **ftp [-v] [-n] [-i] [-d] [-g] [-s: soubor] [-a] [-A] [-w:velikost_okna] [hostitel]**

Přepínače **-v**

Potlačuje zobrazení odpovědí vzdáleného serveru.

-n

Potlačuje automatické přihlášení při počátečním spojení.

-i

Vypíná interaktivní pobídky během hromadného přenosu souborů.

-d

Umožňuje ladění zobrazením všech příkazů FTP, předávaných mezi klientem a serverem.

-g

Zabraňuje globbingu názvů, které povoluje použití zástupných znaků v názvech místních souborů a cest. (Viz též příkaz glob v tabulce D.1.)

-s: [soubor]

Udává název textového souboru, který obsahuje příkazy FTP; tyto příkazy jsou automaticky spuštěny po spuštění nástroje Ftp. Používejte tento přepínač místo přesměrování (<).

-a

Určuje, že smí být použito libovolné místní rozhraní pro vazbu na datové spojení FTP.

-A

Přihlašuje se k serveru FTP jako anonymní.

-w:velikost_okna

Specifikuje velikost přenosové vyrovnávací paměti. Výchozí velikost tohoto okna je 4096 bajtů.

Proměnné *Hostitel*

Udává název hostitelského počítače nebo adresu IP vzdáleného hostitelského počítače, ke kterému se má připojit. Název hostitelského počítače, pokud je uveden, musí být posledním parametrem řádku.

Tabulka D.1 uvádí seznam příkazů FTP. Podrobnosti o syntaxi jednotlivých příkazů naleznete v Nápovědě systému Windows 2000.

Tabulka D.1 Příkazy Ftp v systému Windows 2000

Příkaz	Funkce
!	Spustí určený příkaz na místním počítači.
?	Zobrazí popis příkazů Ftp. Příkaz ? je identický jako příkaz help.
Append	Připojí místní soubor k souboru na vzdáleném počítači s použitím aktuálního nastavení typu souboru.
Ascii	Nastaví typ přenosu souboru na ASCII, což je výchozí nastavení.
Bell	Zapíná zvukovou signalizaci po dokončení každého příkazu přenosu souboru. Ve výchozím nastavení je zvuková signalizace vypnuta.
Binary	Nastavuje typ přenosu souboru na binary.
Bye	Ukončí relaci FTP se vzdáleným hostitelským počítačem a opustí Ftp.
Cd	Změní pracovní adresář na vzdáleném hostitelském počítači.
Close	Ukončí relaci FTP se vzdáleným hostitelským počítačem a vrátí se do interpretu příkazů.
Debug	Přepíná režim ladění. V režimu ladění je každý příkaz, odeslaný vzdálenému hostitelskému počítači, zobrazen za uvádějícím řetězcem -- >. Ve výchozím nastavení je režim ladění vypnut.
Delete	Odstraňuje soubory ze vzdáleného hostitelského počítače.
Dir	Zobrazí seznam souborů a podadresářů vzdáleného adresáře.
Disconnect	Odpojuje se od vzdáleného hostitelského počítače, přičemž zůstává v příkazovém režimu.
Get	Kopíruje vzdálený soubor do místního počítače použitím aktuálního typu přenosu souborů.
Glob	Přepíná globbing názvů souborů. globbing povoluje použití zástupných znaků v názvech místních souborů nebo cest. Ve výchozím nastavení je globbing povolen.
Hash	Přepíná zobrazování znaku čísla (#) pro každý přenesený blok dat. Velikost bloku dat je 2048 bajtů. Ve výchozím nastavení je zobrazování znaku # vypnuto.
Lcd	Mění pracovní adresář místního hostitelského počítače. Ve výchozím nastavení je použit aktuální adresář v místním hostitelském počítači.
Literal	Posílá argumenty, slovo za slovem, vzdálenému serveru FTP. Jako odpověď je očekáván jeden kód odezvy FTP.
Ls	Zobrazí zkrácený seznam souborů a podadresářů vzdáleného adresáře.

Příkaz	Funkce
Mdelete	Odstraní více souborů ze vzdáleného hostitelského počítače.
Mdir	Zobrazí seznam souborů a podadresářů vzdáleného adresáře.
Mget	Kopíruje více vzdálených souborů do místního počítače použitím aktuálního typu přenosu souborů.
Mkdir	Vytvoří vzdálený adresář.
Mls	Zobrazí zkrácený seznam souborů a podadresářů vzdáleného adresáře.
Mput	Kopíruje více místních souborů na vzdálený hostitelský počítač s použitím aktuálních souborů a podadresářů.
Open	Připojuje se k uvedenému serveru FTP.
Prompt	Přepíná výzvy. Nástroj Ftp zobrazuje výzvy při přenosu více souborů, aby vám umožnil selektivně vyhledávat nebo ukládat soubory; příkazy mget a mput přenášejí všechny soubory, když je zobrazování výzev vypnuto. Ve výchozím nastavení se výzvy zobrazují.
Put	Kopíruje místní soubor na vzdálený hostitelský počítač s použitím aktuálního typu přenosu souborů.
Pwd	Zobrazuje aktuální adresář ve vzdáleném hostitelském počítači.
Quit	Ukončí relaci FTP se vzdáleným hostitelským počítačem a opustí nástroj Ftp.
Quote	Stejně jako příkaz Literal.
Recv	Kopíruje vzdálený soubor do místního počítače použitím aktuálního typu přenosu souborů. Příkaz recv je identický s příkazem get.
Remotehelp	Zobrazuje nápovědu pro vzdálené příkazy.
Rename	Přejmenovává vzdálené soubory.
Rmdir	Odstraňuje vzdálený adresář.
Send	Kopíruje místní soubor do hostitelského počítače s použitím aktuálního typu přenosu souborů. Příkaz send je identický s příkazem put.
Status	Zobrazuje aktuální stav spojení FTP a nastavení.
Trace	Přepíná sledování paketů; sledování zobrazuje trasu každého paketu, když je spuštěn příkaz Ftp.
Type	Nastavuje nebo zobrazuje typ přenosu souborů.
User	Udává uživatele vzdálenému hostitelskému počítači.
Verbose	Přepíná režim s podrobnými zprávami. Pokud je zapnut, zobrazují se všechny odpovědi FTP; po skončení přenosu souborů jsou také zobrazeny statistiky o efektivitě přenosu. Ve výchozím nastavení je tento režim zapnut.

Rcp

Tento připojovací příkaz kopíruje soubory mezi počítačem se spuštěným systémem Microsoft® Windows® 2000 a počítačem se spuštěnou službou nebo démonem Rshd – Remote Shell Server. Příkaz rcp může být také použit pro přenosy třetí strany ke kopírování souborů mezi dvěma počítači se spuštěným démonem Rshd, když je příkaz vydán z počítače se systémem Windows 2000. Služba Rshd je dostupná na počítačích se systémem Unix, ale nikoliv na počítači se systémem Windows 2000. Počítač se spuště-

ným systémem Windows 2000 se může účastnit pouze jako počítač, ze kterého jsou vydávány příkazy. Vzdálené počítače musí kromě spuštěné služby Rshd navíc rovněž podporovat nástroj Rcp.

Syntaxe **rcp** [-a] [-b] [-h] [-r] [zdroj zdroj2 zdrojN] [cíl]

Přepínače -a

Specifikuje přenosový režim ASCII. Tento režim převádí znaky konce řádku s posuvem řádku na znaky konce řádku u odcházejících souborů a znaky posuvu řádku na znaky konce řádku s posuvem řádku u přicházejících souborů. Tento režim je výchozím režimem přenosu.

-b

Udává binární režim přenosu. Žádné převody znaků konce a posuvu řádku se neprovádějí.

-h

Přenáší zdrojové soubory, označené atributem Skrytý na počítači se systémem Windows 2000. Bez této volby má uvedení skrytého souboru v přířádku příkazu rcp stejná výsledek, jako kdyby soubor neexistoval.

-r

Rekurzivně kopíruje obsah všech podadresářů zdroje do cíle. Přitom zdroj i cíl musí být adresáře.

Proměnné zdroj a cíl

Musí být ve tvaru [hostitel[.uživatel]:]soubor. Pokud je vynechána část [hostitel[.uživatel]:], předpokládá se, že hostitelským počítačem je místní počítač. Pokud je vynechána část uživatel, je použito uživatelské jméno aktuálně přihlášeného uživatele systému Windows 2000. Pokud je uveden úplný název hostitelského počítače, který obsahuje tečkové (.) oddělovače, pak musí být část [.uživatel] uvedena. V opačném případě je poslední část názvu hostitelského počítače interpretována jako uživatelské jméno. Pokud je uvedeno více zdrojových souborů, musí být cíl adresář..

Pokud název souboru nezačíná lomítkem (/) u počítačů se systémem Unix nebo zpětným lomítkem (\) u počítačů se systémy Windows, předpokládá se, že jde o relativní název vzhledem k aktuálnímu pracovnímu adresáři. V systému Windows 2000 je to adresář, ze kterého je příkaz vydán. Na vzdáleném počítači je to přihlašovací adresář vzdáleného uživatele. Tečka (.) označuje aktuální adresář. Použijte únikové znaky (\, „, nebo ') ve vzdálených cestách, pokud chcete použít zástupné znaky na vzdáleném hostitelském počítači.

Vzdálená oprávnění

Příkaz rcp se neptá na hesla; aktuální nebo uvedené uživatelské jméno musí existovat na vzdáleném hostitelském počítači a umožňovat vzdálené provádění příkazů nástrojem Rcp.

Soubor Rhosts

Soubor Rhosts udává, který vzdálený počítač nebo uživatel mají přístup k místnímu účtu použitím příkazů **rsh** nebo **rcp**. Tento soubor (nebo soubor s názvem hosts.equiv) je vyžadován na vzdáleném počítači pro přístup ke vzdálenému počítači použitím těchto příkazů. Příkazy **rsh** i **rcp** přenášejí místní uživatelské jméno vzdálenému počítači. Vzdálený počítač používá toto jméno plus adresu IP (obvykle přeloženou jako ná-

zev hostitelského počítače) nebo požadující počítač k určení, zda poskytne přístup. Neexistuje žádné opatření pro udávání hesla k přístupu k účtům pomocí těchto příkazů.

Když je uživatel přihlášen k doméně serveru Windows 2000 Server, musí být dostupný řadič domény pro překlad aktuálně přihlášeného uživatelského jména, protože uživatelské jméno přihlášeného uživatele se neukládá v místním počítači. Protože uživatelské jméno je vyžadováno jako část protokolu RSH, příkaz selže, pokud není možné uživatelské jméno získat.

Soubor Rhhosts je textový soubor, kde každý řádek je záznamem. Ten se skládá z názvu místního hostitelského počítače, místního uživatelského jména a libovolného komentáře k záznamu nebo k názvu místního hostitelského počítače a libovolného komentáře k záznamu. Položky jsou odděleny tabelátorem nebo mezerou a komentáře začínají dvojitým křížkem (#), například:

```
Computer5   marie   #Toto je počítač v místnosti 41A.
Computer7   #Toto je počítač v místnosti 42.
```

Soubor Rhhosts musí být v domovském adresáři uživatele na vzdáleném počítači.

Navíc musí být vaše název hostitelského počítače přidáno do souboru /Etc/Hosts na vzdáleném počítači. (Normálně se místo souboru Hosts používá názvový server DNS).

Více informací o implementaci souboru Rhhosts specifické pro vzdálený počítač naleznete v dokumentaci vzdáleného počítače.

Specifikování hostitelských počítačů

Pro použití jiného než aktuálního uživatelského jména použijte proměnné *hostitel.uživatel*. Pokud je *hostitel.uživatel* specifikováno se zdrojem, musí soubor Rhhosts na vzdáleném hostitelském počítači obsahovat položku pro tohoto uživatele.

Pokud je uveden název hostitelského počítače jako úplný doménový název obsahující tečku, musí být uživatelské jméno připojeno za názvem hostitelského počítače. To zabraňuje v interpretaci posledního prvku doménového názvu jako uživatelského jména. Například:

```
Rcp domain-name1.user:johns domain-name2.user:buddyg
```

Vzdálené zpracování

Vzdálené zpracování se na většině počítačů se systémem Unix provádí příkazem, spuštěným z přihlašovacího prostředí uživatele. Před rozбором názvů souborů se provede uživatelský profil neboli Cshrc a exportované proměnné prostředí (s použitím únikových znaků nebo uvozovek) mohou být použity v názvech vzdálených souborů.

Kopírování souborů

Pokud se pokusíte kopírovat několik souborů do souboru místo do adresáře, je zkopírován pouze poslední soubor. Příkaz rcp také nemůže kopírovat soubor na sebe sama.

Syntaxe příkazu rcp

Následující příklady demonstrují syntaxi nejobvyklejších použití příkazu rcp.

Kopírování místního souboru do přihlašovacího adresáře vzdáleného počítače:

```
rcp <název souboru vzdálený počítač >
```

Kopírování lokálního souboru do existujícího adresáře vzdáleného počítače pod novým názvem:

```
rcp <název souboru vzdálený počítač:/adresář/nový název souboru>
```

Kopírování více místních souborů do podadresáře vzdáleného přihlašovacího adresáře:

```
rcp <soubor1 soubor2 soubor3 vzdálený počítač:podadresář/adresář souborů>
```

Kopírování ze vzdáleného zdroje do aktuálního adresáře místního počítače:

```
rcp <Vzdálený počítač:název souboru>
```

Kopírování více souborů z více vzdálených zdrojů do vzdáleného cíle s různými uživatelskými jmény:

```
rcp <vzdálený1.uživatel1:soubor1 vzdálený2.uživatel2:soubor2 vzdálenýcíl.cílový-uživatel:adresář>
```

Kopírování ze vzdáleného počítače s použitím adresy IP do lokálního počítače (zde je uživatelské jméno povinné, protože tečka je použita v názvu vzdáleného hostitelského počítače):

```
rcp <adresa IP.uživatel:název souboru název souboru>
```

Rexec

Tento připojovací nástroj spouští příkazy na vzdálených hostitelských počítačích se spuštěnou službou Rexecd. Nástroj Rexec ověřuje uživatelské jméno na vzdáleném hostitelském počítači užitím hesla předtím, než provede zadaný příkaz.

Syntaxe **rexec** *hostitel* [-**I** *uživatelské jméno*] [-**n**] *příkaz*

Přepínače -**I** [*uživatelské jméno*]

Specifikuje uživatelské jméno na vzdáleném hostitelském počítači.

-**n**

Přesměruje vstup příkazu Rexec na NUL.

Proměnné *hostitel*

Udává vzdálený hostitelský počítač, na kterém se spustí příkaz.

příkaz

Udává příkaz, který se spustí.

Použití příkazu Rexec

Příkaz Rexec vyzve uživatele k zadání hesla a ověří heslo na vzdáleném hostitelském počítači. Pokud se ověření podaří, je příkaz proveden.

Příkaz Rexec kopíruje standardní vstup vzdálenému *příkazu*, standardní výstup vzdáleného *příkazu* na svůj standardní výstup a standardní chyby vzdáleného příkazu na své standardní chyby. Signály přerušení a ukončení jsou šířeny vzdálenému příkazu. Příkaz Rexec skončí normálně, když normálně skončí vzdálený příkaz.

Použití přesměrovacích symbolů

Symbole pro přesměrování uzavírejte do uvozovek, pokud chcete dosáhnout přesměrování na vzdáleném hostitelském počítači. Pokud nejsou použity uvozovky, dojde

k přesměrování na místním počítači. Například následující příkaz připojí vzdálený soubor *remotefile* k místnímu souboru *localfile*:

```
Rexec otherhost cat remotefile >> localfile
```

Následující příkaz připojí vzdálený soubor *remotefile* k jinému vzdálenému souboru *otherremotefile*:

```
Rexec otherhost cat remotefile">>" otherremotefile
```

Použití interaktivních příkazů

Většinu interaktivních příkazů není možné spustit pomocí příkazu *Rexec*. Například příkazy **vi** a **emacs** nemohou být spuštěny použitím příkazu *Rexec*. Ke spuštění interaktivních příkazů použijte nástroj *telnet*.

Rsh

Tento připojovací nástroj spouští příkazy na vzdálených hostitelských počítačích použitím služby *Rsh*. Informace o souboru *Rhosts*, který se používá pro podporu tohoto prostředku, najdete v popisu nástroje *Rcp*.

Syntaxe **rsh** *hostitel* [**-l** *uživatelské jméno*] [**-n**] *příkaz*

Přepínače **-l** [*uživatelské jméno*]

Udává uživatelské jméno, které má být použito u vzdáleného hostitelského počítače. Pokud je tento parametr vynechán, je použito uživatelské jméno přihlášeného uživatele.

-n

Přesměruje vstup příkazu *Rsh* na *NUL*.

Proměnné *hostitel*

Udává vzdálený hostitelský počítač.

příkaz

Specifikuje příkaz, který má být spuštěn.

Použití nástroje Rsh

Nástroj *Rsh* kopíruje standardní vstup vzdálenému příkazu, standardní výstup vzdáleného příkazu na svůj standardní výstup a standardní chyby – *stderr* vzdáleného příkazu na své standardní chyby. Příkaz *Rexec* skončí, když skončí vzdálený příkaz.

Použití přesměrovacích symbolů

Symbole pro přesměrování uzavírejte do uvozovek, pokud chcete dosáhnout přesměrování na vzdáleném hostitelském počítači. Pokud nejsou použity uvozovky, dojde k přesměrování na místním počítači. Například následující příkaz připojí vzdálený soubor *remotefile* k místnímu souboru *localfile*:

```
Rsh otherhost cat remotefile >> localfile
```

Následující příkaz připojí vzdálený soubor *remotefile* k jinému vzdálenému souboru *otherremotefile*:

```
Rsh otherhost cat remotefile ">>" otherremotefile
```

Použití nástroje Rsh v doméně Windows 2000 Server

Je-li uživatel přihlášen k doméně Microsoft® Windows® 2000 Server, musí být k dispozici řadič domény k překladu aktuálně přihlášeného uživatelského jména, protože přihlášené uživatelské jméno se neukládá v místním počítači. Protože uživatelské jméno je vyžadováno jako část protokolu RSH, příkaz selže, pokud není možné uživatelské jméno získat.

Soubor Rhosts

Soubor Rhosts obecně povoluje síťová přístupová práva v počítačích se systémem Unix. Soubor Rhosts uvádí seznam názvů počítačů a přidružená uživatelská jména, která mají přístup ke vzdáleným počítačům. Když je vydán některý z příkazů **rcp**, **rexec**, nebo **rsh** vzdálenému počítači se správně nastaveným souborem Rhosts, nemusíte vzdálenému počítači poskytovat přihlašovací informace a heslo.

Soubor Rhosts je textový soubor, ve kterém každý řádek představuje záznam. Záznam se skládá z názvu místního počítače, místního uživatelského jména a libovolného komentáře k záznamu. Položky jsou odděleny tabelátorem nebo mezerou a komentáře začínají dvojítm křížkem (#), například:

```
Computer5      marie    #Tento počítač je v místnosti 41A
```

Soubor Rhosts musí být v domovském adresáři uživatele na vzdáleném počítači. Více informací o implementaci souboru Rhosts specifické pro vzdálený počítač naleznete v dokumentaci vzdáleného počítače.

Telnet

Tento přípojovací prostředek spouští emulaci terminálu se vzdáleným hostitelským počítačem se spuštěnou službou serveru telnet. Prostředek Telnet poskytuje emulaci terminálu DEC VT 100, DEC VT 52 nebo ANSI použitím služeb protokolu TCP založených na spojení.

K zajištění emulace terminálu z počítače se systémem Windows musí být na vzdáleném hostitelském počítači spuštěn protokol a služba serveru telnet. Uživatel služby telnet v systému Windows musí také mít uživatelský účet na vzdáleném serveru se službou telnet.

Pro spuštění služby klienta **telnet** zadejte telnet v příkazovém řádku. V této části jsou popsány syntaxe a použití pro spuštění služby klienta telnet z příkazového řádku.

Poznámka: Systémy Windows 2000 Server a Microsoft® Windows® 2000 Professional poskytují nástroj klienta telnet a také službu serveru telnet. Tato služba je zabudována, ale musí být spuštěna předtím, než může obsluhovat klienty telnet.

Syntaxe **telnet** [*hostitel* [*port*]]

Proměnné *hostitel*

Udává název hostitelského počítače nebo adresu IP vzdáleného počítače, ke kterému se chcete připojit.

port

Udává vzdálený port, ke kterému se chcete připojit. Pokud není uveden, je pro připojení TCP výchozí hodnota portu 23.

Tftp

Tento připojovací prostředek přenáší soubory na vzdálený počítač a ze vzdáleného počítače se spuštěnou službou Trivial File Transfer Protocol (TFTP). Je to podobný nástroj jako Ftp, ale neposkytuje ověření uživatele, ačkoliv soubory vyžadují oprávnění pro čtení a zápis systému Unix. Nástroj Tftp lze použít pouze pro jednosměrný přenos souborů.

Syntaxe **tftp** [-i] *hostitel* [**get** | **put**] *zdroj* [*cíl*]

Přepínače -i

Udává binární přenosový režim obrazu (také nazývaný oktet). V režimu binárního obrazu je soubor přesouván doslova bajt po bajtu. Tento režim používejte pro přenos binárních souborů.

Pokud je přepínač -i vynechán, je soubor přenesen v režimu ASCII. Ten je výchozím režimem přenosu. Tento režim převádí znaky konce řádku (EOL) na odpovídající formát daného systému. Použijte tento režim, když přenášíte textové soubory. Pokud je přenos úspěšný, je zobrazena rychlost přenosu dat.

get

Přenáší *cíl* ze vzdáleného počítače do *zdroje* na místní počítač.

Protože protokol TFTP nepodporuje ověřování uživatele, musí být uživatel přihlášen a soubor musí být na vzdáleném počítači zapsatelný.

put

Přenáší *zdroj* z místního počítače do *cíle* na vzdáleném počítači.

Proměnné *hostitel*

Specifikuje vzdálený nebo místní hostitelský počítač.

zdroj

Udává soubor, který má být přenesen.

cíl

Udává kam má být soubor přenesen.

PŘÍLOHA E

Možnosti služby DHCP

Následující témata podávají popis všech předdefinovaných možností dostupných při používání služby DHCP systému Microsoft® Windows® 2000. Tyto možnosti jsou definovány podle aktualizované příručky standardů pro možnosti DHCP (RFC 2132, DHCP Options and BOOTP Vendor Extensions).

Můžete používat dialogová okna Vlastnosti ve Správci služby DHCP pro nastavení každé možnosti služby DHCP na určité hodnoty a pak je zpřístupnit pro přidělování a distribuci klientům služby DHCP podle serveru, rozsahu, třídy nebo úrovní preferencí specifických pro klienta.

V této příloze

Základní možnosti (RFC 1497)	682
Možnosti hostitelského počítače IP	688
Možnosti rozhraní IP	690
Možnosti linkové vrstvy	692
Možnosti protokolu TCP	693
Možnosti aplikační vrstvy	693
Možnosti rozhraní NetBIOS pro TCP/IP	696
Možnosti specifické pro dodavatele	697
Možnosti třídy uživatele	698
Rozšíření služby DHCP	699
Nedefinované možnosti	704
Možnosti Microsoft	706

Příbuzné informace v Resource Kitu

- Více informací o službě DHCP najdete v části „Protokol DHCP“ v této knize.
- Více informací o zprávách služby DHCP najdete v části „Zprávy DHCP“ v této knize.

Základní možnosti (RFC 1497)

Následující tabulka udává seznam základních typů možností služby DHCP, původně definovaných ve specifikaci RFC 1497, „BOOTP Vendor Information Extensions“ pro použití služeb DHCP a BOOTP. Ve službě BOOTP jsou tyto typy možností označovány jako *rozšíření dodavatele*.

Služba DHCP podporuje nastavování a distribuci každé z těchto možností, které jsou nastaveny Správcem služby DHCP. Ve výchozím nastavení vyžadují, podporují a interpretují klienti služby Microsoft DHCP pro výchozí nastavení klienta pouze možnosti 1, 3, 6 a 15 z typů možností, uvedených v tomto odstavci. Další možnosti jsou předdefinovány pro přidělování a distribuci službou DHCP, ale jsou rozpoznávány pouze když klienti používají software DHCP dodaný třetí stranou, jenž podporuje tyto další typy možností.

Výplň (Pad Option)

Kód	0
Délka	Nepoužito.
Hodnota	Nepoužito.
Popis	Tento typ možnosti je nulový oktet („00“), používaný jako výplň. Tato možnost se liší od většiny typů možností služby DHCP v tom, že nepoužívá pole délky a hodnoty. Když je použita, způsobí, že následující typy možností služby DHCP, které se objeví v paketu DHCP, jsou zarovnávány na hranici slova. Tato možnost nevyžaduje nastavení.

Struktura Kód

0

Konec (End Option)

Kód	255
Délka	Nepoužito.
Hodnota	Nepoužito.
Popis	Tato možnost je oktet s desítkovou hodnotou 255 („FF“), používaný pro označení konce oblasti možností služby DHCP v paketech zpráv DHCP. Tato možnost se liší od většiny typů možností služby DHCP, protože nepoužívá pole pro délku a hodnotu. Typicky se používá na konci pole možností k označení toho, že se v paketu zprávy DHCP nevyskytují již žádná další data možností. Může být rovněž použita uvnitř zprávy ve spojení s informacemi specifickými pro dodavatele (možnost 43) pro označení konce zapouzdřeného pole s možnostmi specifickými pro dodavatele. Tato možnost nevyžaduje nastavení.

Struktura Kód

255

Maska podsítě (Subnet Mask)

Kód	1
Délka	Pevná, 4 oktety.

- Hodnota** 32bitové celé číslo se znaménkem, reprezentující masku podsítě adresy IP, dodané ve zprávě DHCP.
- Popis** Specifikuje masku podsítě klienta, jak je popsáno ve specifikaci RFC 950 „Internet Standard Subnetting Procedure“. Hodnota pro tuto možnost se přebírá z pole Maska podsítě, jak je definováno v dialogovém okně Vlastnosti oboru DHCP ve Správci služeb DHCP.

Struktura	Kód	Délka	Maska podsítě
	1	4	m1, m2, m3, m4

Posunutí času (Time Offset)

- Kód** 2
- Délka** Pevná, 4 oktety
- Hodnota** 32bitová se znaménkem, používaná pro posunutí vzhledem ke střednímu času (Universal Coordinated Time – UCT).
- Popis** Udává hodnotu posunutí (v sekundách) od středního času UCT, která se používá v podsíti klienta. Tuto hodnotu je možno nastavovat jako 32bitové celé číslo se znaménkem. Kladné hodnoty posunutí udávají umístění podsítě na východ od nulového poledníku. Negativní hodnoty posunutí udávají umístění podsítě na západ od nulového poledníku.

Struktura	Kód	Délka	Posunutí času
	2	4	čas

Směrovač

- Kód** 3
- Délka** Proměnlivá; minimální délka 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu směrovače.
- Hodnota** 32bitové celé číslo se znaménkem, reprezentující adresu IP každého přiřazeného směrovače
- Popis** Udává seznam adres IP pro směrovače podsítě klienta. Pokud je přiřazen více než jeden směrovač, klient vyhodnocuje a používá adresy v uvedeném pořadí.

Struktura	Kód	Délka	Adresa 1	Adresa 2
	3	n	a1, a2, a3, a4	a1, a2, ...

Časový server (Time Server)

- Kód** 4
- Délka** Proměnlivá; minimální délka 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro adresu každého časového serveru podle specifikace RFC 868, která je uvedena.
- Hodnota** 32bitové celé číslo se znaménkem, reprezentující adresu IP pro každý přiřazený časový server podle specifikace RFC 868.
- Popis** Udává seznam adres IP časových serverů podle specifikace RFC 868, které jsou dostupné pro klienta. Pokud je přiřazen více než jeden časový server, klient vyhodnocuje a používá adresy v uvedeném pořadí.

Struktura	Kód	Délka	Adresa 1	Adresa 2
	4	n	a1, a2, a3, a4	a1, a2, ...

Názvový server IEN (IEN Name Server)

Kód	5								
Délka	Proměnlivá; minimální délka 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou adresu názvového serveru IEN, která je uvedena.								
Hodnota	32bitové celé číslo se znaménkem, reprezentující adresu IP každého přiřazeného názvového serveru IEN.								
Popis	Udává seznam adres IP pro názvové servery Internet Engineering Note (IEN), dostupné pro klienta. Pokud je přiřazen více než jeden server, klient vyhodnocuje a používá adresy v uvedeném pořadí.								
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>Adresa 1</th><th>Adresa 2</th></tr><tr><td>5</td><td>n</td><td>a1, a2, a3, a4</td><td>a1, a2, ...</td></tr></table>	Kód	Délka	Adresa 1	Adresa 2	5	n	a1, a2, a3, a4	a1, a2, ...
Kód	Délka	Adresa 1	Adresa 2						
5	n	a1, a2, a3, a4	a1, a2, ...						

Server DNS (DNS Server)

Kód	6								
Délka	Proměnlivá; minimální délka 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru DNS.								
Hodnota	32bitové celé číslo se znaménkem, reprezentující adresu IP pro každý přiřazený server DNS.								
Popis	Udává seznam adres IP pro názvové servery Domain Name System (DNS), dostupné klientovi. Pokud je přiřazen více než jeden server, klient vyhodnocuje a používá adresy v uvedeném pořadí. Klientské počítače služby DHCP, které jsou vícedomé a mohou dostat více zapůjčení DHCP, mohou mít pouze jeden seznam serverů DNS na počítač, nikoliv na rozhraní adaptéru, kromě klientů systému Windows 2000.								
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>Adresa 1</th><th>Adresa 2</th></tr><tr><td>6</td><td>n</td><td>a1, a2, a3, a4</td><td>a1, a2, ...</td></tr></table>	Kód	Délka	Adresa 1	Adresa 2	6	n	a1, a2, a3, a4	a1, a2, ...
Kód	Délka	Adresa 1	Adresa 2						
6	n	a1, a2, a3, a4	a1, a2, ...						

Protokolovací server (Log Server)

Kód	7								
Délka	Proměnlivá; minimální délka 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu protokolovacího serveru.								
Hodnota	32bitové celé číslo se znaménkem, reprezentující adresu IP každého přiřazeného protokolovacího serveru.								
Popis	Udává seznam adres IP pro protokolovací servery MIT-LCS UDP, dostupné klientovi. Pokud je přiřazen více než jeden server, klient vyhodnocuje a používá adresy v uvedeném pořadí.								
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>Adresa 1</th><th>Adresa 2</th></tr><tr><td>7</td><td>n</td><td>a1, a2, a3, a4</td><td>a1, a2, ...</td></tr></table>	Kód	Délka	Adresa 1	Adresa 2	7	n	a1, a2, a3, a4	a1, a2, ...
Kód	Délka	Adresa 1	Adresa 2						
7	n	a1, a2, a3, a4	a1, a2, ...						

Server Cookie (Cookie Server)

Kód	8
------------	---

Délka	Proměnlivá; minimální délka 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru cookie.			
Hodnota	32bitové celé číslo se znaménkem, reprezentující adresu IP cookie.			
Popis	Udává seznam adres IP pro servery cookie podle specifikace RFC 865. Pokud je přiřazen více než jeden server, klient vyhodnocuje a používá adresy v uvedeném pořadí.			
Struktura	Kód	Délka	Adresa 1	Adresa 2
	8	n	a1, a2, a3, a4	a1, a2, ...

Server LPR (LPR Server)

Kód	9			
Délka	Proměnlivá; minimální délka 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru LPR.			
Hodnota	32bitové celé číslo se znaménkem, reprezentující adresu IP LPR.			
Popis	Udává seznam adres IP pro tiskové servery podle specifikace RFC 1179, dostupné klientovi. Pokud je přiřazen více než jeden server, klient vyhodnocuje a používá adresy v uvedeném pořadí.			
Struktura	Kód	Délka	Adresa 1	Adresa 2
	9	n	a1, a2, a3, a4	a1, a2, ...

Server Impress (Impress Server)

Kód	10			
Délka	Proměnlivá; minimální délka 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru Impress.			
Hodnota	32bitové celé číslo se znaménkem, reprezentující adresu IP každého přiřazeného serveru Impress.			
Popis	Udává seznam adres IP pro servery Imagen Impress, dostupné klientovi. Pokud je přiřazen více než jeden server, klient vyhodnocuje a používá adresy v uvedeném pořadí.			
Struktura	Kód	Délka	Adresa 1	Adresa 2
	10	n	a1, a2, a3, a4	a1, a2, ...

Server vyhledávání zdrojů (Resource Location Server)

Kód	11			
Délka	Proměnlivá; minimální délka 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru vyhledávání zdrojů.			
Hodnota	32bitové celé číslo se znaménkem, reprezentující adresu IP každého přiřazeného serveru vyhledávání zdrojů.			
Popis	Udává seznam adres IP pro servery vyhledávání zdrojů podle specifikace RFC 887, dostupné klientovi. Pokud je přiřazen více než jeden server, klient vyhodnocuje a používá adresy v uvedeném pořadí.			
Struktura	Kód	Délka	Adresa 1	Adresa 2
	11	n	a1, a2, a3, a4	a1, a2, ...

Název hostitelského počítače (Host Name)

Kód 12

Délka Délka se mění v závislosti na datech. Minimální délka je 1 oktet. Maximální délka je omezena na 63 znaků, nebo jeden oktet na každý znak, použitý v názvu hostitelského počítače, nastaveném pro použití touto možností.

Hodnota Text ze znaků ASCII.

Popis Udává název hostitelského počítače klienta s délkou do 63 znaků. (Viz specifikace RFC 1035, Domain Names – Implementation and Specification, pro možná omezení sady znaků). V některých případech může být tento název doplněn připojením hodnoty, poskytnuté zde názvem domény DNS, jak je uvedeno u možnosti 15. Pro klienty systému Windows není tato možnost podporována pro použití při nastavení názvu hostitelského počítače klienta, který se nastavuje v klientském počítači v dialogovém okně Vlastnosti identifikace v síti jako Název počítače.

Struktura

Kód	Délka	Název hostitelského počítače
12	n	název

Velikost spouštěcího souboru (Boot File Size)

Kód 13

Délka Pevná, 2 oktety.

Hodnota 16bitové celé číslo bez znaménka, udávající počet bloků o velikosti 512 oktetů, které jsou zapotřebí pro sestavení spouštěcího souboru.

Popis Udává velikost výchozího obrazu spouštěcího souboru pro klienta.

Struktura

Kód	Délka	Velikost souboru
13	02	16bitové celé číslo

Soubor se stavem systému (Merit Dump File)

Kód 14

Délka Délka se mění v závislosti na hodnotě dat. Minimální délka je 1 oktet.

Hodnota Text ze znaků ASCII

Popis Udává a cestu k souboru, do kterého má být vypisován obraz jádra paměti klienta v případě havárie klienta. Pro tento typ možnosti je hodnota dat ve tvaru textu ze znaků ASCII. Délka pole dat závisí na počtu znaků použitých ve specifikaci cesty. Pokud má například zadaná cesta délku 20 znaků, bude pole s hodnotou pro tuto možnost mít také délku 20 oktetů.

Struktura

Kód	Délka	Cesta k souboru
14	n	cesta

Název domény DNS

Kód 15

Délka Délka se mění v závislosti na hodnotě dat. Minimální délka je 1 oktet.

Hodnota Text ze znaků ASCII

Popis Udává název domény, kterou by měl klient služby DHCP používat při překladu názvů hostitelských počítačů službou DNS. Pro tento typ možnosti se jako datová hodnota

používá text ze znaků ASCII. Délka pole dat závisí na počtu znaků, použitým v zadaném názvu domény DNS. Pokud má například název domény 20 znaků, měla by být délka pole s hodnotou pro tuto možnost rovněž 20 oktetů.

Struktura	Kód	Délka	Název domény
	15	n	název domény

Odkládací server (Swap Server)

Kód 16

Délka Délka je pevná, 4 oktety.

Hodnota Jednoduchá adresa IP pro odkládací server klienta (32bitové celé číslo bez znaménka).

Popis Udává adresu IP odkládacího serveru klienta.

Struktura	Kód	Délka	Adresa odkládacího serveru
	16	n	a1, a2, a3, a4

Kořenová cesta (Root Path)

Kód 17

Délka Délka je proměnlivá v závislosti na hodnotě dat. Minimální délka je 1 oktet.

Hodnota Text ze znaků ASCII.

Popis Udává cestu, která obsahuje kořenový disk klienta. Cesta je formátována jako text ze znaků ASCII. Pro tento typ možnosti jsou data použita jako hodnota textem ze znaků ASCII. Délka pole s hodnotou závisí na počtu znaků, použitých v zadané kořenové cestě. Pokud má například zadaná kořenová cesta 20 znaků, měla by být délka pole s hodnotou pro tuto možnost rovněž 20 oktetů.

Struktura	Kód	Délka	Cesta ke kořenovému disku
	17	n	název cesty

Cesta rozšíření (Extensions Path)

Kód 18

Délka Délka je proměnlivá v závislosti na hodnotě dat. Minimální délka je 1 oktet.

Hodnota Text ze znaků ASCII.

Popis Udává soubor, který je možno vyhledat použitím protokolu Trivial File Transfer Protocol (TFTP), obsahující informace, které se interpretují stejným způsobem jako 64oktetové pole rozšíření dodavatele v odpovědi BOOTP. K umožnění více než 64 oktetů v rozšiřujících informacích dodavatele v protokolu BOOTP lze použít tuto možnost. Při použití této možnosti není délka specifikované cesty rozšíření omezena velikostí a všechny odkazy v souboru rozšíření na značku 18 (jako jsou výskyty pole cesty rozšíření protokolu BOOTP) jsou ignorovány.

Struktura	Kód	Délka	Cesta rozšíření
	18	n	název souboru

Poznámka: Pro všechny typy možností poskytnuté v „cestě rozšíření“, které používají seznam adres IP jako hodnoty dat možnosti, se vždy používají adresy IP z důvodu upřednostňování klientem DHCP tak, aby první adresa v seznamu byla použita jako první.

Možnosti hostitelského počítače IP

Následující tabulky popisují možnosti DHCP, které ovlivňují činnost vrstvy IP v závislosti na hostitelském počítači.

Povolení a zákaz předávání protokolu IP (IP Forwarding Enable/Disable)

Kód	19						
Délka	Délka je pevná, 1 oktet.						
Hodnota	1 = Povolit předávání protokolu IP. 0 = zakázat předávání protokolu IP.						
Popis	Používá se pro určení, zda klient služby DHCP povoluje nebo zakazuje předávání datagramů ve vrstvě IP.						
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>Hodnota</th></tr><tr><td>19</td><td>1</td><td>0 1</td></tr></table>	Kód	Délka	Hodnota	19	1	0 1
Kód	Délka	Hodnota					
19	1	0 1					

Povolení a zákaz směrování nemístních zdrojů (Nonlocal Source Routing Enable/Disable)

Kód	20						
Délka	Délka je pevná, 1 oktet.						
Hodnota	1 = Povolit předávání datagramů z nemístních zdrojů. 0 = Zakázat předávání datagramů z nemístních zdrojů.						
Popis	Používá se pro určení, zda klient služby DHCP povoluje nebo zakazuje předávání datagramů ve vrstvě IP v závislosti na tom, zda přijatý datagram pochází z místního nebo nemístního zdroje.						
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>Hodnota</th></tr><tr><td>20</td><td>1</td><td>0 1</td></tr></table>	Kód	Délka	Hodnota	20	1	0 1
Kód	Délka	Hodnota					
20	1	0 1					

Filtr zásad (Policy Filter)

Kód	21																
Délka	Proměnlivá. Minimální délka je 8 oktetů pro jednoduché párování cíle a masky. Délka roste v násobcích 8 oktetů pro každé další použité párování.																
Hodnota	Dvě po sobě jdoucí 32bitová celá čísla bez znaménka, udávající párovou hodnotu, sestávající z adresy IP, následované maskou podsítě.																
Popis	Udává filtry zásad pro směrování nemístních zdrojů u klienta. Filtry se skládají ze seznamu párů adres IP a masek, udávajících páry cíl a maska, pro které se mají filtrovat trasy zdrojů všech příchozích datagramů. Klient zahazuje všechny datagramy zdrojově směrované s adresou dalšího směrování, která se neshoduje s některým z filtrů. Další informace o zásadách filtrování, jak se uplatňují u tohoto typu možnosti najdete ve specifikaci RFC 1122 „Requirements for Internet Hosts – Communication Layers“.																
Struktura	<table><tr><td>Kód</td><td>Délka</td><td>Adresa 1</td><td>Maska 1</td></tr><tr><td>21</td><td>n</td><td>a1, a2, a3, a4</td><td>m1, m2, m3, m4</td></tr><tr><td></td><td></td><td>Adresa 2</td><td>Maska 2</td></tr><tr><td></td><td></td><td>a1, a2, a3, a4</td><td>m1, m2, m3, m4, ...</td></tr></table>	Kód	Délka	Adresa 1	Maska 1	21	n	a1, a2, a3, a4	m1, m2, m3, m4			Adresa 2	Maska 2			a1, a2, a3, a4	m1, m2, m3, m4, ...
Kód	Délka	Adresa 1	Maska 1														
21	n	a1, a2, a3, a4	m1, m2, m3, m4														
		Adresa 2	Maska 2														
		a1, a2, a3, a4	m1, m2, m3, m4, ...														

Maximální velikost znovu sestaveného datagramu (Maximum Datagram Reassembly Size)

Kód 22

Délka Pevná, 2 oktety.

Hodnota 16bitové celé číslo, udávající maximální velikost datagramu pro nové sestavení. Minimální velikost pro datagram je 576.

Popis Udává maximální velikost datagramu, který může klient znovu sestavit.

Struktura	Kód	Délka	Velikost
	22	2	16bitové celé číslo

Výchozí hodnota Time-To-Live protokolu IP (Default IP Time-To-Live)

Kód 23

Délka Pevná, 1 oktet.

Hodnota Číslo (v sekundách) mezi 1 a 255.

Popis Udává výchozí hodnotu Time-To-Live (TTL), kterou klient používá u odcházejících datagramů.

Struktura	Kód	Délka	TTL
	23	1	hodnota TTL v sekundách

Časový limit stárnutí jednotky MTU cesty (Path MTU Aging Time-out)

Kód 24

Délka Pevná, 4 oktety.

Hodnota 32bitové celé číslo bez znaménka, které udává hodnotu časového limitu (v sekundách).

Popis Udává časový limit pro hodnoty stárnutí největší přenosové jednotky (MTU) cesty. (Hodnoty jsou zjišťovány mechanismem definovaným ve specifikaci RFC 1191 „Path MTU Discovery“).

Struktura	Kód	Délka	Časový limit
	24	4	hodnota časového limitu v sekundách

Cesta k tabulce MTU Plateau Table (Path MTU Plateau Table)

Kód 25

Délka Proměnlivá; minimální délka je 2 oktety. Když je délka větší než 2, zvětšuje se v násobcích 2.

Hodnota Tabulka formátovaná jako seznam 16bitových celých čísel bez znaménka, seřazených od nejmenšího po největší. Nejmenší hodnota MTU v tabulce nemůže být menší než 68.

Popis Udává tabulku velikostí MTU k použití pro zjištění MTU cesty, jak je definováno ve specifikaci RFC 1191, „Path MTU Discovery“.

Struktura	Kód	Délka	Velikost	Velikost 2
	25	n	s1, s2	tabulka velikostí MTU

Možnosti rozhraní IP

Následující tabulka popisuje možnosti DHCP, které ovlivňují činnost vrstvy IP v závislosti na rozhraní.

Jednotka MTU rozhraní (Interface MTU)

Kód	26						
Délka	Pevná, 2 oktety.						
Hodnota	16 bitové celé číslo bez znaménka, udávající hodnotu MTU rozhraní. Minimální platná hodnota pro jednotku MTU je 68.						
Popis	Udává hodnotu velikosti jednotky MTU, která může být použita na určeném rozhraní adaptéru hostitelského počítače.						
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>MTU</th></tr><tr><td>26</td><td>2</td><td>jednotka MTU rozhraní</td></tr></table>	Kód	Délka	MTU	26	2	jednotka MTU rozhraní
Kód	Délka	MTU					
26	2	jednotka MTU rozhraní					

Všechny podsítě jsou místní (All Subnets Are Local)

Kód	27						
Délka	Pevná, 1 oktet.						
Hodnota	1 = Klienti předpokládají, že všechny podsítě jsou místní a sdílejí stejnou hodnotu velikosti jednotky MTU. 0 = Klienti předpokládají, že některé podsítě nejsou místní že u vzdálených podsítí se mohou používat menší hodnoty velikosti jednotky MTU.						
Popis	Udává, zda klienti předpokládají, že všechny podsítě uvnitř propojených sítí klienta používají stejnou hodnotu velikosti jednotky MTU jako místní podsít, ke které je klient připojen.						
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>Hodnota</th></tr><tr><td>27</td><td>1</td><td>0 1</td></tr></table>	Kód	Délka	Hodnota	27	1	0 1
Kód	Délka	Hodnota					
27	1	0 1					

Adresa všesměrového vysílání (Broadcast Address)

Kód	28						
Délka	Pevná, 4 oktety.						
Hodnota	Obvykle omezená adresa IP pro všesměrové vysílání (255.255.255.255), ale může být změněna použitím platných hodnot pro adresy všesměrového vysílání, jak je určeno v odstavci 3.2.1.3 specifikace RFC 1122 Requirements for Internet Hosts – Communication Layers.						
Popis	Udává adresu všesměrového vysílání, používanou v podsíti klienta.						
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>Adresa všesměrového vysílání</th></tr><tr><td>28</td><td>4</td><td>b1, b2, b3, b4</td></tr></table>	Kód	Délka	Adresa všesměrového vysílání	28	4	b1, b2, b3, b4
Kód	Délka	Adresa všesměrového vysílání					
28	4	b1, b2, b3, b4					

Provést zjištění masky (Perform Mask Discovery)

Kód	29
Délka	Pevná, 1 oktet.

Hodnota 1 = Klient provede zjištění masky podsítě.
0 = Klient neprovádí zjištění masky podsítě.

Popis Udává zda klient používá protokol Internet Control Message Protocol (ICMP) pro zjišťování masky podsítě.

Struktura	Kód	Délka	Hodnota
	29	1	0 1

Poskytovatel masky (Mask Supplier)

Kód 30

Délka Pevná, 1 oktet.

Hodnota 1 = Klient odpovídá na požadavky na masky podsítě.
0 = Klient neodpovídá na požadavky na masky podsítě.

Popis Udává zda klient odpovídá na požadavky na masky podsítě použitím protokolu ICMP.

Struktura	Kód	Délka	Hodnota
	30	1	0 1

Provést zjištění směrovače (Perform Router Discovery)

Kód 31

Délka Pevná, 1 oktet.

Hodnota 1 = Klient provádí zjištění směrovače.
0 = Klient neprovádí zjištění směrovače.

Popis Udává, zda klient oslovuje směrovače použitím metody zjištění směrovače podle specifikace RFC 1256, ICMP Router Discovery Messages.

Struktura	Kód	Délka	Hodnota
	31	1	0 1

Adresa oslovování směrovače (Router Solicitation Address)

Kód 32

Délka Pevná, 4 oktety.

Hodnota Adresa IP (32bitové celé číslo bez znaménka).

Popis Udává adresu IP, které klient posílá požadavky na oslovování směrovačů.

Struktura	Kód	Délka	Adresa
	32	4	a1, a2, a3, a4

Statická trasa (Static Route)

Kód 33

Délka Proměnlivá; minimální délka 8 oktetů; délka roste v násobcích 8 oktetů pro každou další statickou trasu, dodávanou touto možností.

Hodnota Seznam párů adres IP. Každých 8 oktetů poskytuje dvě po sobě jdoucí adresy IP, párující adresu cíle a směrovače, používané pro každou trasu. První 4 oktety udávají adresu cíle, druhé 4 oktety udávají směrovač pro adresu cíle.

Popis Udává seznam statických tras, které klient instaluje ve své směrovací mezipaměti. Všechny vícenásobné trasy do stejného cíle jsou uvedeny v klesajícím pořadí priorit. Výchozí trasa s hodnotou 0.0.0.0 je neplatným cílem pro statickou trasu.

Struktura	Kód	Délka	Cíl 1	Směrovač 1
	33	n	d1, d2, d3, d4	r1, r2, r3, r4
			Cíl 2	Směrovač 2
			d1, d2, d3, d4	r1, r2, r3, r4, ...

Možnosti linkové vrstvy

Následující tabulky popisují možnosti služby DHCP, které mají vliv na činnost linkové vrstvy v závislosti na rozhraní.

Zapouzdření koncové části (Trailer Encapsulation)

Kód 34

Délka Pevná, 1 oktet.

Hodnota 1 = Klient se pokouší použít koncovou část.
0 = Klient se nepokouší použít koncovou část.

Popis Udává zda klient sjednává použití koncových částí, jak je popsáno ve specifikaci RFC 893 ISO Transport Services on Top of the TCP, když používá protokol překládání adres (ARP).

Struktura	Kód	Délka	Hodnota
	34	1	0 1

Časový limit mezipaměti ARP (ARP Cache Time-Out)

Kód 35

Délka Pevná, 4 oktety.

Hodnota 32bitové celé číslo bez znaménka, udávající hodnotu časového limitu v sekundách.

Popis Udává časový limit pro položky mezipaměti ARP.

Struktura	Kód	Délka	Čas
	35	4	hodnota časového limitu v sekundách

Zapouzdření sítě Ethernet (Ethernet Encapsulation)

Kód 36

Délka Pevná, 1 oktet.

Hodnota 1 = Klient používá zapouzdření podle specifikace RFC 1042.
0 = Klient používá zapouzdření podle specifikace RFC 894.

Popis Udává, zda klient používá zapouzdření sítě Ethernet v.2 (RFC 894) nebo zapouzdření IEEE 802.3 (RFC 1042), pokud je rozhraním síť Ethernet.

Struktura	Kód	Délka	Hodnota
	36	1	0 1

Možnosti protokolu TCP

Následující tabulky popisují možnosti služby DHCP, které ovlivňují činnost relační vrstvy TCP v závislosti na rozhraní.

Výchozí hodnota TTL protokolu TCP (TCP Default TTL)

Kód	37		
Délka	Pevná, 1 oktet.		
Hodnota	8bitové celé číslo bez znaménka, udávající hodnotu Time-To-Live (TTL) v sekundách. Minimální hodnota TTL je 1.		
Popis	Udává výchozí hodnotu TTL, kterou klient používá při posílání segmentů TCP.		
Struktura	Kód	Délka	TTL
	37	1	hodnota TTL v sekundách

Interval udržení naživu protokolu TCP (TCP Keep-Alive Interval)

Kód	38		
Délka	Pevná, 4 oktety.		
Hodnota	32bitové celé číslo bez znaménka, které udává interval udržení naživu v sekundách.		
Popis	Udává interval, po který klient čeká, než odešle zprávu keep-alive po spojení TCP. Hodnota 0 oznamuje, že klient neposílá po spojení zprávy keep-alive, pokud o to není výslovně požádán aplikací.		
Struktura	Kód	Délka	Čas
	38	4	interval udržení naživu v sekundách

Posílání nepotřebných informací při udržení naživu protokolu TCP (TCP Keep-Alive Garbage)

Kód	39		
Délka	Pevná, 1 oktet.		
Hodnota	1 = Klient posílá oktet nepotřebných informací udržení naživu. 0 = Klient neposílá oktet nepotřebných informací udržení naživu.		
Popis	Udává zda klient posílá nebo neposílá zprávy keep-alive protokolu TCP s oktetem nepotřebných informací pro kompatibilitu se staršími implementacemi.		
Struktura	Kód	Délka	Hodnota
	39	1	0 1

Možnosti aplikační vrstvy

Následující tabulky popisují možnosti služby DHCP, které ovlivňují činnost aplikační vrstvy v závislosti na rozhraní. Jsou to různé možnosti, které můžete využít pro nastavení programů a služeb.

Pro tyto možnosti můžete dynamicky nastavovat klienty služby DHCP, kteří mají více než jedno rozhraní na základě vlastností rozhraní použitím dodatečných zapůjčení služby DHCP (jedno na rozhraní) pro každý z těchto typů možností.

Název domény NIS (NIS Domain Name)

Kód	40		
Délka	Délka je proměnlivá v závislosti na hodnotě dat. Minimální délka je 1 oktet.		
Hodnota	Text ze znaků ASCII.		
Popis	Udává název domény Network Information Service (NIS) jako řetězec znaků ASCII.		
Struktura	Kód	Délka	Název domény NIS
	40	n	název domény NIS

Servery NIS (NIS Servers)

Kód	41		
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru.		
Hodnota	32bitové celé číslo se znaménkem, reprezentující adresu IP serveru NIS.		
Popis	Udává seznam adres IP v pořadí podle preference pro servery Network Information Service (NIS), dostupné klientovi.		
Struktura	Kód	Délka	Adresa 1 Adresa 2
	41	n	a1, a2, a3, a4 a1, a2, ...

Servery NTP (NTP Servers)

Kód	42		
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru.		
Hodnota	32bitové celé číslo se znaménkem, reprezentující adresu IP serveru NTP.		
Popis	Udává seznam adres IP v pořadí podle preference pro servery Network Time Protocol (NTP), dostupné klientovi.		
Struktura	Kód	Délka	Adresa 1 Adresa 2
	42	n	a1, a2, a3, a4 a1, a2, ...

Servery písem systému X Window (X Window System Font Servers)

Kód	48		
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru.		
Hodnota	32bitové celé číslo se znaménkem reprezentující adresu IP serveru.		
Popis	Udává seznam adres IP v pořadí podle preference pro servery písem systému X Window, dostupné klientovi.		
Struktura	Kód	Délka	Adresa 1 Adresa 2
	48	n	a1, a2, a3, a4 a1, a2, ...

Servery správy zobrazení systému X Window (X Window System Display Manager Servers)

Kód	49
------------	----

Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru.		
Hodnota	32bitové celé číslo se znaménkem reprezentující adresu IP serveru.		
Popis	Udává seznam adres IP v pořadí podle preference pro servery správy zobrazení systému X Window, dostupné klientovi.		
Struktura	Kód	Délka	Adresa 1 Adresa 2
	49	n	a1, a2, a3, a4 a1, a2, ...

Název domény NIS+ (NIS+ Domain Name)

Kód	64		
Délka	Délka je proměnlivá podle hodnoty dat. Minimální délka je 1 oktet.		
Hodnota	Text ze znaků ASCII.		
Popis	Udává název domény Network Information Service Plus (NIS+) klienta jako řetězec ze znaků ASCII.		
Struktura	Kód	Délka	Název domény NIS+
	64	n	název domény NIS

Servery NIS+ (NIS+ Servers)

Kód	65		
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu serveru.		
Hodnota	32bitové celé číslo se znaménkem reprezentující adresu IP serveru.		
Popis	Udává seznam adres IP v pořadí podle preference pro servery Network Information Service Plus (NIS+), dostupné klientovi.		
Struktura	Kód	Délka	Adresa 1 Adresa 2
	65	n	a1, a2, a3, a4 a1, a2, ...

Mobilní domácí agenti IP (Mobile IP Home Agents)

Kód	68		
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu mobilního domácího agenta IP.		
Hodnota	32bitové celé číslo se znaménkem reprezentující adresu IP mobilního domácího agenta IP.		
Popis	Udává seznam adres IP v pořadí podle preference pro mobilní domácí agenty IP, dostupné klientovi.		
Struktura	Kód	Délka	Adresa 1 Adresa 2
	68	n	a1, a2, a3, a4 a1, a2, ...

Možnosti rozhraní NetBIOS pro TCP/IP

Následující typy možností se používají pro podporu rozhraní NetBIOS pro protokol TCP/IP. Všichni klienti služby DHCP a servery DHCP v prostředí Microsoft dovedou rozpoznat a podporovat použití těchto typů možností.

Názvový server NetBIOS (NetBIOS Name Server)

Kód	44		
Délka	Proměnlivá; minimální délka je 4 oktety; délka může být zvětšována v násobcích 4 pro každou uvedenou adresu.		
Hodnota	Každé 4 oktety v tomto poli obsahují adresu IP uvedeného serveru WINS, zadanou jako 32bitové celé číslo bez znaménka.		
Popis	Udává adresy IP pro názvové servery Windows Internet Name Service (WINS) nebo pro názvové servery rozhraní NetBIOS (NBNS).		
Struktura	Kód	Délka	Adresa 1 Adresa 2
	44	n	a1, a2, a3, a4 b1, b2, b3, ,, ...

Server distribuce datagramů rozhraní NetBIOS (NetBIOS Datagram Distribution (NBDD) Server)

Kód	45		
Délka	Proměnlivá; minimální délka je 4 oktety; délka může být zvyšována pouze v násobcích 4.		
Hodnota	Každé 4 oktety v tomto poli obsahují adresu IP uvedeného serveru NBDD, zadanou jako 32bitové celé číslo bez znaménka.		
Popis	Udává adresy IP pro servery distribuce datagramů rozhraní NetBIOS (NBDD).		
Struktura	Kód	Délka	Adresa 1 Adresa 2
	45	n	a1, a2, a3, a4 b1, b2, b3, b4, ...

Typ uzlu rozhraní NetBIOS (NetBIOS Node Type)

Kód	46		
Délka	Pevná, 1 oktet.		
Hodnota	1 = uzel b, 2 = uzel p, 4 = uzel m a 8 = uzel h.		
Popis	Nastavuje typ uzlu klienta pro klienty rozhraní NetBIOS pro TCP/IP (NetBT), podle popisu ve specifikacích RFC 1001 a 1002 (Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods a Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications). U vícedomých počítačů s více adresami je typ uzlu přiřazen počítači, nikoliv jednotlivým síťovým adaptéřům.		
Struktura	Kód	Délka	Typ uzlu
	46	1	Viz výše.

ID oboru rozhraní NetBIOS (NetBIOS Scope ID)

Kód	47		
Délka	Proměnlivá; délka v oktetech se rovná počtu znaků, použitých v ID oboru rozhraní NetBIOS.		
Hodnota	Udává identifikátor oboru rozhraní NetBIOS pomocí TCP/IP, používaný klientem. Používaný formát pro tyto identifikátory rozhraní je dále popsán ve specifikacích RFC 1001 a 1002, „Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods“ a „... Detailed Specifications“. Informace o omezeních znakové sady naleznete ve specifikacích RFC.		

Popis	Udává řetězec, který je identifikátorem oboru rozhraní NetBIOS pomocí TCP/IP pro klienta, jak je uvedeno ve specifikacích RFC 1001 a 1002. Na počítačích s více adresami je typ uzlu přiřazen počítači, nikoliv jednotlivým síťovým adaptérům.		
Struktura	Kód	Délka	Obor rozhraní NetBIOS
	47	n	řetězec identifikátoru oboru

Možnosti specifické pro dodavatele

Tato část popisuje vyhrazené typy možností služby DHCP, určené pro použití třídy dodavatele. Typy možností specifické pro dodavatele jsou popsány ve specifikaci RFC 2132. Třídy dodavatele mohou být použity službou DHCP a na počítači klienta služby DHCP se spuštěným systémem Windows 2000. Pro jiné klienty služby DHCP mohou být použity výchozí třídy, poskytované službou DHCP k seskupování a zatřídění neidentifikujících klientů na serveru DHCP.

Navíc Správce služby DHCP poskytuje jednu výchozí třídu dodavatele, třídu standardních možností služby DHCP, která může být použita pro seskupování a zatřídění klientů, kteří službě DHCP neurčují třídu dodavatele.

Informace specifické pro dodavatele (Vendor-Specific Information)

Kód	43
Délka	Proměnlivá; Minimální délka je 1 oktet.
Hodnota	Objekt o délce n oktetů (kde n je rovno délce specifikované v této možnosti). Definice hodnot, ukládaných pro tento typ možnosti je závislá na dodavateli a o dodaných hodnotách se předpokládá, že budou interpretovány dodavatelským kódem na klientech služby DHCP a na serveru DHCP.
Popis	<p>Tato možnost je používána klienty a servery pro výměnu informací, specifických pro dodavatele. Servery, které nejsou vybaveny pro interpretování těchto informací, je ignorují. Klienti, kteří očekávají, ale nedostávají tyto informace, se pokusí pracovat bez nich.</p> <p>V některých případech používá dodavatel tento typ možnosti pro odeslání více než jedné informační položky; proto může tato možnost sloužit jako zapouzdřené pole možností pro zapouzdřování možností specifických pro dodavatele. Při zapouzdřování možností dodržují servery DHCP stejnou syntaxi (to znamená stejnou posloupnost kód-délka-pole hodnot) pro každý zapouzdřený typ možnosti, jaká by se normálně objevila v plně standardním poli možnosti s následujícími výjimkami pro zapouzdřená pole specifická pro uživatele:</p> <p>Nemohou být použity „magic cookie“.</p> <p>Všechny kódy standardních možností – jiné než výplň (0) nebo konec (255) – mohou být předefinovány.</p> <p>Možnost konec (255) označuje, pokud je přítomna, konec zapouzdřených dodavatelských možností, ale nikoliv konec zapouzdřeného pole specifického pro dodavatele. Pokud není přítomna možnost konec, konec zapouzdřeného pole specifického pro dodavatele je určen z jeho ohlášené délky.</p>
Struktura	Kód Délka Informace specifické pro dodavatele
	43 ... n i1, i2, ...

Pokud tento typ možnosti používá zapouzdřené pole specifické pro dodavatele, informační bajty 1–n mají následující formát:

Kód	Délka	Datová položka	Kód	Délka	Datová položka	Kód
T1	n	d1, d2, ...	T2	n	D1, D2,

Identifikátor třídy dodavatele (Vendor Class Identifier)

- Kód** 60
- Délka** Minimum je 1 oktet. Délka se mění v závislosti na n (počet oktetů, použitých jako identifikátor).
- Hodnota** Hodnota n oktetů interpretovaná serverem DHCP, který podporuje dodavatelské zařizování klientů.
- Popis** Může být použito klienty služby DHCP k rozpoznání jejich dodavatelského typu a nastavení. Při použití této možnosti mohou dodavatelé definovat své vlastní hodnoty identifikátorů, jako je poskytování informací o systémovém nastavení hardware nebo operačního systému nebo jiné identifikační informace.
- Všechny počítače v systému Windows 2000, které fungují buď jako servery DHCP nebo jako klienti služby DHCP, mohou používat a podporovat tento typ možnosti. Když jsou použity třídy dodavatele, odpovídá server DHCP identifikujícím klientům použitím možnosti s kódem 43 (popsané výše), vyhrazeného typu možnosti pro vrácení informací specifických pro dodavatele klientovi.
- U serverů DHCP, které automaticky neinterpretují tuto možnost, se očekává, že ji budou ignorovat, když je specifikována klienty. Pro klienty starších verzí Windows a jiné klienty, kteří nepodporují tento typ možnosti, zařazuje služba DHCP tyto klienty jako část výchozí třídy dodavatele, třídy standardních možností služby DHCP, která je předdefinována pro servery DHCP v systémech Microsoft.

Struktura

Kód	Délka	Identifikátor třídy dodavatele
60	n	i1, i2, ...

Možnosti třídy uživatele

Tato část popisuje vyhrazené typy možností služby DHCP, vymezené pro použití tříd uživatele. Typ možnosti třídy uživatele je dodatečnou specifikací návrhu DHCP, která je v současnosti navrhována jako standard pro síť Internet. Třídy uživatelů mohou být použity službou DHCP a počítači klientů služby DHCP se spuštěným systémem Windows 2000. Pro jiné klienty služby DHCP mohou být použity výchozí třídy, poskytované službou DHCP k seskupování a zařizování neidentifikujících klientů na serveru DHCP.

Informace o třídě uživatele (User Class Information)

- Kód** 77
- Délka** Proměnlivá; minimum je 2 oktety.
- Hodnota** Text ze znaků ASCII.
- Popis** Klient služby DHCP může používat tuto možnost pro identifikaci typu nebo kategorie uživatele nebo aplikací, které zastupuje. Informace, obsažené v této možnosti tvoří

textový objekt ve znakové sadě NVT ASCII, který představuje třídu uživatele, jejímž členem je klient.

Pro definování určených tříd uživatelů můžete použít Správce služby DHCP. Když jsou vytvořeny třídy uživatelů, každá třída nastavuje identifikační řetězec, používaný službou DHCP pro zatřídování identifikujících klientů. Může být také vytvořena výchozí třída uživatelů pro zatřídování klientů, kteří nejsou schopni podporovat identifikátory třídy uživatelů.

Třídy uživatelů mohou být užitečné pro oddělování klientských počítačů, které mají sdílenou nebo společnou potřebu podobných softwarových nastavení nebo uživatelských předvoleb. Identifikátor může například udávat, že určitý klient služby DHCP bude členem třídy „účetních auditorů“, kteří mají zvláštní požadavky na služby, jako například určitý databázový server.

Pro klienty služby DHCP v systémech Microsoft podporují pouze počítače se systémem Windows 2000 posílání nebo používání tohoto typu možnosti. Jiní klienti služby DHCP starších verzí neposílají identifikátor třídy ani nemají schopnost rozeznat pojem uživatelské třídy. Tito klienti jsou proto zařazeni jako členové výchozí třídy uživatelů, což je třída uživatelů, předdefinovaná pro okamžité použití ve Správci služby DHCP. Jiné třídy uživatelů musí být vytvořeny manuálně.

Struktura

Kód	Délka	Informace o třídě uživatele
77	n	c1, c2, c3, c4, ...

Rozšíření služby DHCP

Následující typy možností jsou specifické pro službu DHCP a používají se pro implementaci výchozí interakce protokolu a chování systému mezi servery a klienty. Některé z těchto možností jsou implicitně nastaveny při konfiguraci serveru a vlastností oboru užitím Správce služby DHCP.

Vyžadovaná adresa IP (Requested IP Address)

Kód 50

Délka Pevná, 4 oktety.

Hodnota Jednoduché 32bitové celé číslo se znaménkem, udávající vyžadovanou adresu IP.

Popis Může být použita klienty při odesílání zprávy DHCPDiscover pro vyžádání, aby byla serverem přiřazena určitá adresa IP.

Struktura

Kód	Délka	Vyžadovaná adresa IP
50	n	a1, a2, a3, a4

Doba zapůjčení adresy IP (IP Address Lease Time)

Kód 51

Délka Pevná, 4 oktety.

Hodnota Jednoduché 32bitové celé číslo se znaménkem, představující dobu zapůjčení klientovi v sekundách.

Popis Tento typ možnosti se používá dvěma možnými způsoby pro dohodnutí a výměnu informací o době zapůjčení mezi klienty služby DHCP a servery. V prvním způsobu může být tato možnost použita ve zprávách DHCPDiscover nebo DHCPRequest odes-

laných klientem pro vyžádání doby zapůjčení pro svou adresu IP. Ve druhém způsobu může být tato možnost použita ve zprávě DHCP Offer vyslané serverem pro určení doby zapůjčení, kterou server může nabídnout klientovi.

Struktura	Kód	Délka	Doba zapůjčení
	51	4	doba zapůjčení v sekundách

Přeplnění možnosti (Option Overload)

Kód	52
Délka	Pevná, 1 oktet.
Hodnota	Předdefinovaná, mezi hodnoty, akceptované touto možností patří: 1 = Pole File je přepsané. 2 = Pole Sname je přepsané. 3 = Obě pole file a sname jsou přepsaná.
Popis	Používá se ve zprávách, odesílaných serverem DHCP, které udávají, že některé ze standardních polí zprávy v paketu DHCP pro název_ hostitelského_serveru (sname) a název_spouštěcího_souboru (file) je přepsané (použito k předání možností). Tato možnost, pokud je použita, rozšíří oblast možností v každém paketu označením, že nepoužitý prostor pro jedno nebo obě z těchto polí má být přidělen oblasti, používané pro přenos možností služby DHCP.

Struktura	Kód	Délka	Hodnota
	52	1	1 2 3

Název serveru TFTP (TFTP Server Name)

Kód	66
Délka	Délka je proměnlivá v závislosti na hodnotě dat. Minimální délka je 1 oktet.
Hodnota	Text ze znaků ASCII.
Popis	Udává název hostitelského počítače serveru pro Trivial File Transfer Protocol (TFTP), když pole název_ hostitelského_serveru (sname) v paketu zprávy DHCP je přepsaná je použito pro přenos dodatečných možností služby DHCP.

Struktura	Kód	Délka	Server TFTP
	66	n	název hostitelského počítače TFTP

Název spouštěcího souboru (Boot File Name)

Kód	67
Délka	Délka je proměnlivá v závislosti na hodnotě dat. Minimální délka je 1 oktet.
Hodnota	Text ze znaků ASCII.
Popis	Udává název spouštěcího souboru na serveru TFTP, když je pole název_spouštěcího_souboru (file) v paketu zprávy DHCP přepsaná je použito pro přenos dodatečných možností služby DHCP.

Struktura	Kód	Délka	Název spouštěcího souboru
	67	n	c1, c2, c3, ...

Typ zprávy DHCP (DHCP Message Type)

Kód	53						
Délka	Pevná, 1 oktet.						
Hodnota	Předdefinovaná, přijímanými hodnotami pro tento typ možnosti jsou: 1 = Zjišťovací zpráva DHCP (DHCPDiscover). 2 = Nabízející zpráva DHCP (DHCPOffer). 3 = Zpráva s požadavkem DHCP (DHCPRequest). 4 = Odmítací zpráva DHCP (DHCPDecline). 5 = Potvrzovací zpráva DHCP (DHCPAck). 6 = Negativní potvrzovací zpráva DHCP (DHCPNak). 7 = Uvolňovací zpráva DHCP (DHCPRelease). 8 = Informační zpráva DHCP (DHCPInform).						
Popis	Tato možnost je vyžadována ve všech zprávách DHCP pro poskytnutí informací o typu zasílané zprávy.						
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>Typ</th></tr><tr><td>53</td><td>1</td><td>1–8</td></tr></table>	Kód	Délka	Typ	53	1	1–8
Kód	Délka	Typ					
53	1	1–8					

Identifikátor serveru (Server Identifier)

Kód	54						
Délka	Pevná, 4 oktety.						
Hodnota	Jednoduchá 32bitová adresa IP, která označuje server DHCP.						
Popis	<p>Tato možnost se používá ve zprávách DHCPOffer a DHCPRequest a někdy se objevuje v potvrzovacích zprávách DHCP (DHCPAck, DHCPNak). Identifikátorem serveru je adresa IP vybraného serveru DHCP. Tento typ možnosti se používá dvěma možnými způsoby. V prvním způsobu použití zahrnuje server tuto možnost do zpráv DHCPOffer, takže klienti mohou rozlišovat mezi více nabídkami zapůjčení.</p> <p>Ve druhém způsobu zahrnují klienti tento typ možnosti do zpráv DHCPRequest pro výběr zapůjčení a oznámení, která z více nabídek zapůjčení je přijata. Klienti mohou také použít obsah tohoto pole pro jednosměrné vysílání zpráv s požadavkem určitým serverům DHCP pro obnovení aktuálního zapůjčení.</p>						
Struktura	<table><tr><th>Kód</th><th>Délka</th><th>Adresa</th></tr><tr><td>54</td><td>4</td><td>a1, a2, a3, a4</td></tr></table>	Kód	Délka	Adresa	54	4	a1, a2, a3, a4
Kód	Délka	Adresa					
54	4	a1, a2, a3, a4					

Seznam požadavků parametrů (Parameter Request List)

Kód	55
Délka	Minimálně 1 oktet. Délka narůstá po 1 oktetu pro každý další kód možnosti, uvedený v seznamu požadavků.
Hodnota	Seznam 8bitových hodnot, z nichž každá představuje kód typu možnosti mezi 0 a 255.
Popis	Používán klientem DHCP k vyžádání hodnot určitého typu možností od serveru DHCP. Každý typ možnosti je vyžadován a uveden jednou oktetovou hodnotou, obsahující platný nebo rozpoznávaný kód možnosti DHCP pro daný server.

Pro klienty, kteří používají tento typ možnosti, může být seznam seřazen podle preference, přestože od serveru DHCP se nevyžaduje, aby vracel možnosti v pořadí, ve kterém jsou požadovány. Server DHCP se však pokouší vkládat požadované možnosti v pořadí vyžadovaném klientem.

Struktura	Kód	Délka	Kódy možností
	55	n	c1, c2, ...

Nepovinná zpráva (Optional Message)

Kód 56

Délka Minimálně 1 oktet. Délka závisí na délce posílané zprávy.

Hodnota Text ze znaků ASCII.

Popis Může být použita servery i klienty DHCP následujícími způsoby:

Server může použít tento typ možnosti k poskytnutí a začlenění chybové zprávy do negativní potvrzovací zprávy DHCP (DHCPNak) v případě chyby.

Klient může použít tento typ možnosti v odmítací zprávě DHCP (DHCPDecline) k udání důvodu, proč odmítl nabízené parametry.

Zpráva sestává z textového řetězce znaků ASCII proměnlivé délky, který může přijímající počítač zaznamenat nebo zobrazit.

Struktura	Kód	Délka	Text
	56	n	c1, c2, ...

Maximální velikost zprávy (Maximum Message Size)

Kód 57

Délka Pevná, 2 oktety.

Hodnota 16bitové celé číslo udávající maximální velikost v bajtech-oktetech pro paket se zprávou DHCP. Maximální platná hodnota pro tuto možnost je 576.

Popis Používána klientem pro udání maximální délky paketu se zprávou DHCP, který dokáže přijmout. Klient může zahrnout tento typ možnosti do zprávy DHCPDiscover nebo do zprávy DHCPRequest; tento typ možnosti však nezahrnuje do zpráv DHCPDecline.

Struktura	Kód	Délka	Délka
	57	2	maximální velikost

Časová hodnota obnovení (T1) (Renewal Time Value (T1))

Kód 58

Délka Pevná, 4 oktety.

Hodnota 32bitové celé číslo bez znaménka, udávající počet sekund do doby, kdy klient začne obnovovat své zapůjčení adresy u serveru DHCP.

Popis Tento čas je funkcí, která je obvykle 50 procent celého nastaveného trvání (nebo doby zapůjčení) pro klientovo zapůjčení. K přizpůsobení této časové hodnoty změňte délku zapůjčení klienta ve vlastnostech oboru klienta nebo prostřednictvím třídy uživatele na serveru DHCP. Můžete také změnit hodnotu v prostředí NetShell (více informací najdete v nápovědě online).

Struktura	Kód	Délka	Interval T1
	58	4	začátek obnovovacího intervalu

Hodnota doby obnovení vazeb (T2) (Rebinding Time Value (T2))

Kód	59
Délka	Pevná, 4 oktety.
Hodnota	32bitové celé číslo bez znaménka udávající počet sekund předtím, než klient vstoupí do stavu obnovení vazeb pokud neobnovil své aktuální zapůjčení adresy se serverem DHCP.
Popis	Tento čas je funkcí (typicky 87,5 procenta) celého nastaveného trvání (nebo doby zapůjčení) pro klientovo zapůjčení. K přizpůsobení této časové hodnoty změňte délku zapůjčení klienta ve vlastnostech oboru klienta nebo prostřednictvím třídy uživatele na serveru DHCP. Můžete také změnit hodnotu v prostředí NetShell (více informací najdete v nápovědě online).

Struktura	Kód	Délka	Interval T2
	59	4	začátek intervalu obnovení vazeb

Jedinečný identifikátor klienta (Client Unique Identifier)

Kód	61
Délka	Proměnlivá; minimální délka je 2 oktety.
Hodnota	Řada 2 nebo více oktetů, která je považována serverem DHCP za proměnlivý objekt. Server může tuto hodnotu interpretovat a používat k jedinečné identifikaci klientů.
Popis	Používáno klienty k udání jejich jedinečného identifikátoru serveru. Tento typ možnosti je nejužitečnější pro vyhrazené klienty. Když vyhrazený klient kontaktuje server, služba DHCP může kontrolovat a porovnávat hodnotu identifikátoru klienta s odpovídajícím identifikátorem, použitým k nastavení vyhrazení adresy v databázi serveru. Když je nalezeno shodné vyhrazení, vrátí server DHCP vyhrazenou adresu a její příbuzné parametry správnému klientovi. Z tohoto důvodu musí být každý identifikátor klienta jedinečný mezi všemi ostatními identifikátory klientů, použitými v platné síti DHCP, ke které je klient připojen (to je místní podsít klienta a všechny vzdálené podsítě, dosažitelné použitím přenosu DHCP). Dodavatelé a správci systému odpovídají za výběr identifikátorů klientů, které vyhovují tomuto požadavku na jedinečnost. Jeden obvyklý přístup k zajištění jedinečnosti je nastavit vyhrazení klienta na serveru DHCP podle adresy řízení přístupu k médiu klienta jako hodnotu identifikátoru klienta. Adresa řízení přístupu k médiu je zakódovaná v hardwaru klienta síťového adaptéru a je přiřazena výrobcům hardwaru takovým způsobem, že zaručují, že jsou jedinečné pro každé zařízení.

Struktura	Kód	Délka	Typ	Identifikátor klienta
	61	n	t1	i1, i2, ...

Nedefinované možnosti

Tato část popisuje typy možností, které jsou vyhrazeny a určeny pro použití ve specifikaci RFC 2132 DHCP Options and BOOTP Vendor Extensions, ale nejsou předdefinované.

vány pro použití ve Správci služby DHCP. Tyto typy možností mohou být přidány pro podporu klientů služby DHCP, dodaných třetí stranou, kteří používají tyto možnosti.

Server SMTP (Simple Mail Transport Protocol (SMTP) Server)

Kód	69			
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu IP serveru.			
Hodnota	32bitová celá čísla se znaménky udávající adresy IP serverů.			
Popis	Udává seznam adres IP v pořadí podle preference pro servery SMTP, dostupné klientovi.			
Struktura	Kód	Délka	Adresa 1	Adresa 2
	69	n	a1, a2, a3, a4	a1, a2, ...

Server POP3 (Post Office Protocol (POP3) Server)

Kód	70			
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu IP serveru.			
Hodnota	32bitová celá čísla se znaménky, udávající adresy IP serverů.			
Popis	Udává seznam adres IP v pořadí podle preference pro servery POP3, dostupné klientovi.			
Struktura	Kód	Délka	Adresa 1	Adresa 2
	70	n	a1, a2, a3, a4	a1, a2, ...

Server NNTP (Network News Transport Protocol (NNTP) Server)

Kód	71			
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu IP serveru.			
Hodnota	32bitová celá čísla se znaménky, udávající adresy IP serverů.			
Popis	Udává seznam adres IP v pořadí podle preference pro servery NNTP, dostupné klientovi.			
Struktura	Kód	Délka	Adresa 1	Adresa 2
	71	n	a1, a2, a3, a4	a1, a2, ...

Výchozí server služby World Wide Web (Default World Wide Web Server)

Kód	72			
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu IP serveru.			
Hodnota	32bitová celá čísla se znaménky, udávající adresy IP serverů.			
Popis	Udává seznam adres IP v pořadí podle preference pro výchozí webové servery, dostupné klientovi.			

Struktura	Kód	Délka	Adresa 1	Adresa 2
	72	n	a1, a2, a3, a4	a1, a2, ...

Výchozí server služby Finger (Default Finger Server)

Kód	73
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu IP serveru.
Hodnota	32 bitová celá čísla se znaménky, udávající adresy IP serverů.
Popis	Udává seznam adres IP v pořadí podle preference pro výchozí servery služby Finger, dostupné klientovi.

Struktura	Kód	Délka	Adresa 1	Adresa 2
	73	n	a1, a2, a3, a4	a1, a2, ...

Výchozí server protokolu IRC (Default Internet Relay Chat Server)

Kód	74
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu IP serveru.
Hodnota	32bitová celá čísla se znaménky, udávající adresy IP serverů.
Popis	Udává seznam adres IP v pořadí podle preference pro servery protokolu IRC, dostupné klientovi.

Struktura	Kód	Délka	Adresa 1	Adresa 2
	74	n	a1, a2, a3, a4	a1, a2, ...

Server protokolu StreetTalk (StreetTalk Server)

Kód	75
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu IP serveru.
Hodnota	32bitová celá čísla se znaménky, udávající adresy IP serverů.
Popis	Udává seznam adres IP v pořadí podle preference pro servery protokolu StreetTalk, dostupné klientovi.

Struktura	Kód	Délka	Adresa 1	Adresa 2
	75	n	a1, a2, a3, a4	a1, a2, ...

Server protokolu STDA (StreetTalk Directory Assistance Server)

Kód	76
Délka	Proměnlivá; minimální délka je 4 oktety; délka v oktetech se zvyšuje v násobcích 4 pro každou uvedenou adresu IP serveru.
Hodnota	32bitová celá čísla se znaménky, udávající adresy IP serverů.
Popis	Udává seznam adres IP v pořadí podle preference pro servery protokolu STDA, dostupné klientovi.

Struktura	Kód	Délka	Adresa 1	Adresa 2
	76	n	a1, a2, a3, a4	a1, a2, ...

Možnosti Microsoft

Tato část popisuje vyhrazené typy možností služby DHCP, definované společností Microsoft. Tyto možnosti jsou dostupné pouze pro použití s podporujícími klienty DHCP v systémech Microsoft, jako jsou počítače se systémem Windows 2000.

Tyto možnosti jsou poskytovány jako zapouzdřená dodavatelská datová pole uvnitř možnosti informací specifických pro dodavatele.

V současnosti lze tyto možnosti přiřazovat pouze v konzole DHCP prostřednictvím následujících tříd dodavatele: možnosti Microsoft a možnosti systému Microsoft Windows 2000.

Zakázat rozhraní NetBIOS pro TCP/IP (Disable NetBIOS over TCP/IP (NetBT))

Kód 1

Délka 4

Hodnota 1= Rozhraní NetBT zůstává povoleno.

2= Zakáže rozhraní NetBIOS pro TCP/IP (NetBT) pro klienty služby DHCP v systému Windows 2000.

Popis Tato možnost může být použita pro výběrové povolování nebo zakazování rozhraní NetBT na počítačích podporujících službu DHCP pouze se spuštěným systémem Windows 2000. Ve výchozím nastavení instalace, pokud není tato možnost přítomna, systém Windows 2000 umožňuje použití rozhraní NetBT pro síťová připojení, která jsou nastavena pro použití protokolu TCP/IP. Klienti starších verzí Windows požadují rozhraní NetBT a nepodporují tuto možnost.

Struktura	Kód	Délka	NetBT
	001	4	zapnuto-vypnuto

Uvolnit zapůjčení DHCP při vypnutí (Release DHCP Lease on Shutdown)

Kód 2

Délka 4B

Hodnota 0=Klienti služby DHCP v systému Windows 2000 nepošílají zprávu DHCPRelease při řádném vypnutí.

1= Klienti služby DHCP v systému Windows 2000 posílají zprávu DHCPRelease při řádném vypnutí.

Popis Tato možnost může být použita pro určení, zda počítače se systémem Windows 2000, podporující službu DHCP posílají uvolnění pro svá zapůjčení DHCP serveru DHCP, když dojde k jejich vypnutí. Ve skutečnosti je implementována a interpretována službou klienta DHCP jako hodnota bitově maskovaná. Ve většině případů ve výchozím nastavení (tedy funkčně ekvivalentní nepřítomnosti hodnoty této možnosti ve zprávách DHCP) klienti se systémem Windows 2000 nepošílají zprávy DHCPRelease při řádném vypnutí.

Struktura	Kód	Délka	Uvolnění
	002	4	zapnuto-vypnuto

Výchozí základ metriky směrovače (Default Router Metric Base)

Kód 3

Délka 4B

Hodnota Tato hodnota je udaným základem metriky směrovače pro použití pro všechny trasy výchozích bran, používaných u klientských počítačů se systémem Windows 2000 a podporou služby DHCP.

Tato hodnota může být přiřazena jako celočíselná matrice nákladů v rozsahu od 1 do 9999. Používá se při výpočtech nejrychlejších, nejspolehlivějších a nejméně nákladných tras. Pokud není hodnota uvedena, je jako výchozí hodnota použita jednička (1) nebo aktuálně nastavená hodnota metriky pro rozhraní.

Popis Tato možnost může být použita pro nastavení výchozího základu metriky pro klienty služby DHCP v systému Windows 2000. Když je tato možnost nastavena, služba klienta DHCP používá zde nastavenou hodnotu jako základ metriky pro své výchozí brány.

Struktura	Kód	Délka	Metrika trasy
	003	4	základ metriky směrovače

Automatické zjišťování proxy pro Internet Explorer 5 (Proxy Autodiscovery for Internet Explorer 5 Only)

Kód 252

Délka Proměnlivá

Hodnota Adresa URL, která odkazuje ke konfiguračnímu souboru, který by měl klient používat pro automatické nastavení programu Internet Explorer 5. Soubor, na který tato adresa URL odkazuje, může být soubor s příponou .pac, .jvs, .js, nebo .ins, vytvořený správcem systému nebo správcem sítě při rozmísťování prohlížeče Internet Explorer 5 na intranetu. Může obsahovat nastavení pro další konfigurovatelné možnosti programu Internet Explorer 5, jako například kterou domovskou stránku má používat nebo nastavení pro hledání a používání serveru proxy.

Popis Tato možnost je přenášena mezi klientskými počítači s programem Internet Explorer 5 a serverem DHCP použitím zprávy DHCPInform, která je momentálně podporována pouze pro servery a klienty služby DHCP v systému Windows 2000.

Použití dodatečných nastavení služby DHCP je podporováno pouze programem Internet Explorer 5, nikoliv staršími verzemi, které používají jiné metody pro automatické zjišťování a nastavování serverů proxy.

Můžete rovněž přidat a nastavit záznam o aliasu (CNAME) v serveru DNS pro podporu vlastností automatického rozpoznávání a nastavování serverů proxy v programu Internet Explorer 5.

Více podrobností naleznete v příručce Microsoft® Internet Explorer 5 Resource Kit.

Struktura	Kód	Délka	URL
	252	n	název url

PŘÍLOHA F

Formát zpráv služby DHCP



Následující tabulky poskytují podrobné informace a popisy všech zpráv služby DHCP, používaných službou DHCP v systému Microsoft® Windows® 2000. Formát těchto zpráv je definován podle aktualizovaných referenčních standardů pro službu DHCP ve specifikaci RFC 2131 Dynamic Host Configuration Protocol. Tyto informace jsou podány především pro správce sítí pro odstraňování potíží nebo sledování komunikace DHCP.

V této příloze

Zprávy služby DHCP 710

Příbuzné informace v Resource Kitu

- Více informací o službě DHCP najdete v části „Protokol DHCP“ v této knize.
- Více informací o možnostech služby DHCP najdete v části „Správa možností DHCP“ v této knize.

Zprávy služby DHCP

Tabulka F.1 zobrazuje pole ve zprávě služby DHCP.

Tabulka F.1 Pole zprávy služby DHCP

Název pole	Oktety	Popis
op	1	Kód option zprávy/typ zprávy. 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Typ adresy hardwaru.
hlen	1	Délka adresy hardwaru.
hops	1	Klient nastavuje na nulu; volitelně používáno přenosovými agenty při spouštění cestou přenosového agenta.
xid	4	Číslo ID transakce, náhodné číslo vybrané klientem a používané klientem a serverem k spojování zpráv a odpovědí mezi klientem a serverem.
secs	2	Vyplňováno klientem; v sekundách uplynulých od doby, kdy klient zahájil proces získání nebo obnovení adresy.
flags	2	Příznaky. Pro práci s některými klienty, kteří nemohou přijímat datagramy IP typu unicast před nastavením softwaru TCP/IP, používá služba DHCP pole příznaků flags. Bit nejvíce vlevo je definován jako příznak BROADCAST (B). Zbývající bity pole flags jsou vyhrazeny pro budoucí použití. Musí být klienty nastaveny na nulu a jsou ignorovány servery a přenosovými agenty.
ciaddr	4	Adresa IP klienta; je vyplňována pouze když je klient ve stavu BOUND, RENEW nebo REBINDING a může odpovídat na požadavky ARP.
yiaddr	4	Adresa IP klienta.
siaddr	4	Adresa IP dalšího serveru, používaného při spouštění; vráceno ve zprávách DHCP Offer, DHCP Ack serverem.
giaddr	4	Adresa IP přenosového agenta; používáno při spouštění cestou přenosového agenta.
chaddr	16	Adresa hardwaru klienta.
sname	64	Volitelný název hostitelského serveru, řetězec zakončený nulovým znakem.
file	128	Název souboru, řetězec zakončený nulovým znakem; „generic“ název nebo prázdný ve zprávě DHCP Discover, úplný název cesty ve zprávě DHCP Offer.
options	proměnlivé	Pole volitelných parametrů. Více informací o možnostech služby DHCP najdete v části „Správa možností DHCP“ v této knize.

Tabulka F.2 ukazuje pole a možnosti používané servery DHCP.

Poznámka: V tabulkách F.2 a F.3 „MUSÍ“, „NESMÍ“, „MĚLA BY“ a „MŮŽE“ udává, zda určitá informace musí, nesmí měla by nebo může být zahrnuta ve zprávě.

Tabulka F.2 Pole a možnosti zpráv

Pole	DHCPOffer	DHCPAck	DHCPCnak
op	BOOTREPLY	BOOTREPLY	BOOTREPLY
htype	Závisí na typu hardwaru; pro více informací viz specifikace RFC 1700 Assigned Numbers.		
hlen	Délka dresy hardwaru v oktetech		
hops	0	0	0
xid	xid ze zprávy DHCPDiscover klienta	xid ze zprávy DHCPRequest klienta	xid ze zprávy DHCPRequest klienta
secs	0	0	0
ciaddr	0	ciaddr ze zprávy DHCPRequest nebo 0	0
yiaddr	Adresa IP nabízená klientovi	Adresa IP přiřazená klientovi	0
siaddr	Adresa IP dalšího serveru, používaného při spouštění	Adresa IP dalšího serveru, používaného při spouštění	0
flags	flags ze zprávy DHCPDiscover klienta	flags ze zprávy DHCPRequest klienta	flags ze zprávy DHCPRequest klienta
giaddr	giaddr ze zprávy DHCPDiscover klienta	giaddr ze zprávy DHCPRequest klienta	giaddr ze zprávy DHCPRequest klienta
chaddr	chaddr ze zprávy DHCPDiscover klienta	chaddr ze zprávy DHCPRequest klienta	chaddr ze zprávy DHCPRequest klienta
sname	Název nebo možnosti hostitelského počítače serveru	Název nebo možnosti hostitelského počítače serveru	(Nepoužito)
file	Soubor nebo možnosti klienta	Soubor nebo možnosti klienta	(Nepoužito)
options	Možnosti	Možnosti	
Možnost	DHCPOffer	DHCPAck	DHCPCnak
Vyžadovaná adresa IP	NESMÍ	NESMÍ	NESMÍ
Doba zapůjčení adresy IP	MUSÍ	MUSÍ (DHCPRequest) NESMÍ (DHCPInform)	NESMÍ
Použití pole file nebo sname	MŮŽE	MŮŽE	NESMÍ
Typ zprávy DHCP	DHCPOffer	DHCPAck	DHCPCnak
Seznam požadavků parametrů	NESMÍ	NESMÍ	NESMÍ
Zpráva	MĚLA BY	MĚLA BY	MĚLA BY
Identifikátor klienta	NESMÍ	NESMÍ	MŮŽE
Identifikátor třídy dodavatele	MŮŽE	MŮŽE	MŮŽE
Identifikátor serveru	MUSÍ	MUSÍ	MUSÍ

Pole	DHCPOffer	DHCPAck	DHCPNak	
Maximální velikost zprávy dodavatele		NESMÍ	NESMÍ	NESMÍ
Všechno ostatní	MŮŽE	MŮŽE	NESMÍ	

Tabulka F.3 zobrazuje pole a možnosti používané klienty DHCP.

Tabulka F.3 Pole a možnosti zprávy klienta DHCP

Pole	DHCPDiscover DHCPInform	DHCPRequest	DHCPDecline DHCPRelease
op	BOOTREQUEST	BOOTREQUEST	BOOTREQUEST
htype	Závisí na typu hardwaru; pro více informací viz Assigned Numbers.	Závisí na typu hardwaru; pro více informací viz Assigned Numbers.	Závisí na typu hardwaru; pro více informací viz Assigned Numbers.
hlen	Délka dresy hardwaru v oktetech	Délka dresy hardwaru v oktetech	Délka dresy hardwaru v oktetech
hops	0	0	0
xid	Vybráno klientem	xid ze zprávy DHCPOffer serveru	Vybráno klientem
secs	0 nebo počet sekund od spuštění procesu DHCP	0 nebo počet sekund od spuštění procesu DHCP	0
flags	Nastavuje příznak BROADCAST pokud klient vyžaduje odpověď všesměrového vysílání	Nastavuje příznak BROADCAST pokud klient vyžaduje odpověď všesměrového vysílání	0
ciaddr	0 (DHCPDiscover) nebo adresa sítě (DHCPInform)	0 nebo adresa sítě (BOUND/RENEW/REBIND)	0 (DHCPDecline) nebo adresa sítě (DHCPRelease)
yiaddr	0	0	0
siaddr	0	0	0
giaddr	0	0	0
chaddr	adresa hardwaru	adresa hardwaru	adresa hardwaru
sname	Možnosti, pokud je uvedeno v možnosti sname nebo file; jinak nepoužito	Možnosti, pokud je uvedeno v možnosti sname nebo file; jinak nepoužito	(Nepoužito)
file	Možnosti, pokud je uvedeno v možnosti sname nebo file; jinak nepoužito	Možnosti, pokud je uvedeno v možnosti sname nebo file; jinak nepoužito	(Nepoužito)
options	Možnosti	Možnosti	(Nepoužito)
Vyžadovaná adresa IP	MŮŽE (DISCOVER) NESMÍ (INFORM)	MUSÍ (v SELECTING nebo INIT-REBOOT) NESMÍ (v BOUND nebo RENEWING)	MUSÍ (DHCPDecline) NESMÍ (DHCPRelease)

Pole	DHCPDiscover DHCPInform	DHCPRequest	DHCPDecline DHCPRelease
Doba zapůjčení adresy IP	MŮŽE (DISCOVER) NESMÍ (INFORM)	MŮŽE	NESMÍ
Použití polí file nebo sname	MŮŽE	MŮŽE	MŮŽE
Typ zprávy DHCP	DHCPDiscover/ DHCPInform	DHCPRequest	DHCPDecline/ DHCPRelease
Identifikátor klienta	MŮŽE	MŮŽE	MŮŽE
Identifikátor třídy dodavatele	MŮŽE	MŮŽE	NESMÍ
Identifikátor serveru	NESMÍ	MUSÍ (po SELECTING), NESMÍ (po INIT-REBOOT, BOUND, RENEWING nebo REBINDING)	MUSÍ
Seznam požadavků parametrů	MŮŽE	MŮŽE	NESMÍ
Maximální velikost zprávy	MŮŽE	MŮŽE	NESMÍ
Zpráva	NEMĚLA BY	NEMĚLA BY	MĚLA BY
Specifické pro sídlo (Site-specific)	MŮŽE	MŮŽE	NESMÍ
Všechno ostatní	MŮŽE	MŮŽE	NESMÍ

PŘÍLOHA G

Typy objektů databáze MIB



Služba SNMP v systému Microsoft® Windows® 2000 podporuje úplnou řadu objektů databáze informací o správě (Management Information Base – MIB) dodaných třetí stranou nebo společností Microsoft. Následující informace poskytují stručný přehled o databázi MIB a obsahují informace o jejím schvalovacím orgánu – společenství IETF, o organizaci objektů databáze MIB a tabulku se seznamem objektů databáze MIB, které se dopravují službou SNMP systému Windows 2000.

V této příloze

Databáze informací o správě 716

Příbuzné informace v Resource Kitu

- Více informací o službě SNMP najdete v části „Simple Network Management Protocol“ v této knize.
- Informace o zabezpečování zpráv SNMP najdete v části „Zabezpečení protokolu IP“ v této knize.

Databáze informací o správě

Databáze informací o správě (Management Information Base – MIB) je kolekce formálně popsaných objektů, z nichž každý představuje určitý typ informace. K objektům databáze MIB lze přistupovat a spravovat je službou Simple Network Management Protocol (SNMP) přes systém správy sítě. Tato kolekce objektů obsahuje informace, požadované systémem správy a tyto informace jsou uloženy jako sada proměnných databáze MIB.

Pro každou příbuznou sadu entit, které mohou být spravovány, jsou definována rozšíření objektů databáze. Definují záznamy o stavu pro informace, jakými jsou statistiky provozu sítě, počet chyb a aktuální obsah vnitřních datových struktur, jako je směrovací tabulka IP počítače.

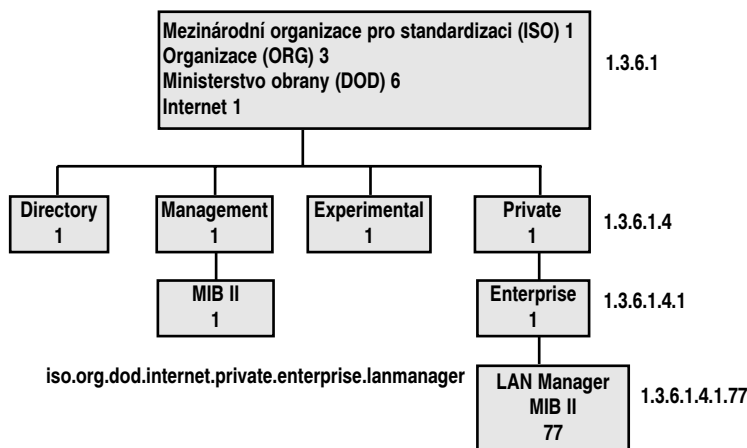
Všechny objekty databáze MIB jsou založeny na společné definici informací o správě. Té se říká struktura informací o správě (Structure of Management Information – SMI) a zahrnuje model informací o správě, povolené datové typy a pravidla pro specifikaci tříd informací o správě.

Identifikátory objektů

Pro sledování všech informací, uložených v databázi MIB je každý objekt označen jedinečnou značkou, zvanou identifikátor objektu. Identifikátor objektu je implementován jako mezinárodně přijaté hierarchické schéma složených názvů, které je řízeno společenstvím Internet Engineering Task Force (IETF). Toto schéma názvů umožňuje vývojářům a dodavatelům vytvářet nové součásti a prostředky a přiřazovat globálně jedinečný identifikátor objektu pro každou novou součást nebo prostředek bez duplikování jakéhokoliv existujícího oboru názvů.

Softwarové aplikace správy SNMP používají identifikátor objektu k rozpoznání spravovaných objektů u každého agenta. Systém správy posílá zprávu, která vyžaduje informace o objektu a určuje objekt identifikátorem objektu. Agent používá identifikátor objektu k vyhledání příslušných informací a posílá odpověď zpět systému správy.

Samotný identifikátor objektu je ve skutečnosti řadou označení, která začíná na vrcholu hierarchie a končí u objektu, jemuž je identifikátor objektu přiřazován. Jako příklad ilustruje obrázek G.1 název objektu `iso.org.dod.internet.private.enterprise.lanmanager` pro správce sítě a číslo tohoto objektu je 1.3.6.1.4.1.77.



Obrázek G.1 Hierarchie oboru názvů databáze MIB

Na určité úrovni v hierarchii oboru názvů uděluje společenství IETF jednotlivým organizacím oprávnění vytvářet nové databáze MIB pod těmito organizacemi. Soukromý obor názvů, přiřazený společnosti Microsoft, je 1.3.6.1.4.1.311. Společnost Microsoft má oprávnění vytvářet nové objekty databází MIB pod tímto oborem názvů a přiřazovat jim názvy, jako je objekt databáze MIB Microsoft IIS Service.

Agent protokolu SNMP v systému Windows 2000

Agent protokolu SNMP v systému Windows 2000 má modulární rozšiřitelný návrh, který podporuje více databází MIB prostřednictvím aplikačního programového rozhraní (API) agenta. Agent protokolu SNMP v systému Windows 2000 je rovněž znám jako rozšiřitelný agent, zatímco podporované objekty databáze MIB jsou také známy jako podagenti nebo agenti rozšíření. Když je spuštěna služba SNMP, zavede agent SNMP všechny dynamicky připojované knihovny (DLL) agentů rozšíření SNMP, které jsou nastaveny v registru. Tento návrh umožňuje snadno přidávat nové databáze MIB. Společnost Microsoft a vývojáři z třetích stran mohou vyvíjet databáze MIB pro nové hardwarové a softwarové součásti a integrovat je snadno do existující služby SNMP.

Když je služba SNMP spuštěna, posílá každý agent systému správy identifikátor objektu pro základní objekt ve své databázi MIB. To umožňuje systému správy u každého agenta určovat, které spravované objekty jsou skutečně instalovány v době, kdy správce zasílá požadavky na informace.

Tabulka G.1 udává databáze MIB v systému Windows 2000 a základní objekty, ze kterých jsou odvozeny všechny další objekty v databázi MIB. Knihovny DLL pro databáze MIB-II, LAN Manager MIB-II a databáze MIB prostředků hostitelského počítače jsou instalovány se službou SNMP. Další databáze MIB, uvedené v této tabulce, jsou instalovány, když jsou instalovány jim odpovídající služby.

Tabulka G.1 Databáze MIB dodávané se službou SNMP systému Windows 2000

Název databáze MIB a název souboru	Popis	Identifikátor objektu	RFC	Závislost
ACS.MIB acsmib.dll	Databáze MIB definovaná společností Microsoft pro službu Quality of Service Admission Control Service (QoS ACS)	1.3.6.1.4.1.311.1.15	(žádná)	(žádná)
ACCSERV.MIB iasperf.dll	Databáze RADIUS-ACC-Server-MIB obsahuje typy objektů pro sledování účtovacích informací mezi serverem přístupu k síti a sdíleným serverem účtování.	1.3.6.1.3.79	2139	Služba Internet Authentication Service
AUTHSERV.MIB iasperf.dll	Databáze RADIUS-AUTH-Server-MIB obsahuje typy objektů pro sledování informací o ověřování, opravňování a nastavení u serveru přístupu k síti.	1.3.6.1.3.79	2138	Služba Internet Authentication Service

Název databáze MIB a název souboru	Popis	Identifikátor objektu	RFC	Závislost
DHCP.MIB dhcplib.dll	Databáze MIB definovaná společností Microsoft obsahuje typy objektů pro sledování síťového provozu mezi vzdálenými hostitelskými počítači a serverem DHCP.	1.3.6.1.4.1.311.1.3	(žádná)	Služba DHCP
FTP.MIB ftplib.dll	Databáze MIB definovaná společností Microsoft obsahuje typy objektů pro sledování služby File Transfer Protocol (FTP).	1.3.6.1.4.1.311.1.7.2	(žádná)	Server IIS
HOSTMIB.MIB hostmib.dll	Obsahuje typy objektů pro sledování a správu prostředků hostitelského počítače.	1.3.6.1.2.1.25	1514	(žádná)
HTTP.MIB httpmib.dll	Databáze MIB definovaná společností Microsoft pro službu Hypertext Transfer Protocol (HTTP).	1.3.6.1.4.1.311.1.7.3	(žádná)	Server IIS
IGMPV2.MIB igmpagnt.dll	Sbírá informace o skupinách připojených k podsíti.	1.3.6.1.359	(žádná)	Služba Routing and Remote Access
IPFORWD.MIB inetmib1.dll	Definuje objekty pro správu tras v síti Internet IP.	1.3.6.1.2.1.2	1354 2096	(žádná)
LMMIB2.MIB lmmib2.dll	Databáze LAN Manager MIB-II pokrývá služby pracovních stanic a serverů.	1.3.6.1.4.1.77.1	(žádná)	(žádná)
MCASTMIB.MIB mcastmib.dll	Modul MIB pro správu vícesměrového směrování IP	1.3.6.1.3.60.1.1	(Nevyřízená)	Služba Routing and Remote Access
MIB-II.MIB intermib1.dll	Databáze Management Information Base (MIB-II) poskytuje jednoduchou, přizpůsobivou architekturu a systém pro správu propojených sítí s protokolem TCP/IP.	1.3.6.1.2.1.1 1.3.6.1.2.1.2 1.3.6.1.2.1.4 1.3.6.1.2.1.5 1.3.6.1.2.1.6 1.3.6.1.2.1.7	1213	(žádná)
MIB-II.MIB snmpmib.dll	Databáze Management Information Base (MIB-II) poskytuje jednoduchou, přizpůsobivou architekturu a systém pro správu propojených sítí s protokolem TCP/IP.	1.3.6.1.2.1.11	1213	(žádná)

Název databáze MIB a název souboru	Popis	Identifikátor objektu	RFC	Závislost
MIPX.MIB rtipxmib.dll	Databáze MIB definovaná společností Microsoft pro protokol Internetwork Packet Exchange (IPX)	1.3.6.1.4.1.311.1.8	(žádná)	Služba Routing and Remote Access
MRIPSAP.MIB rtipxmib.dll	Databáze MIB definovaná společností Microsoft pro protokol Routing Information Protocol (RIP)	1.3.6.1.4.1.311.1.9	(žádná)	Služba Routing and Remote Access
MSIPBTP.MIB btpagnt.dll	Databáze MIB definovaná společností Microsoft pro službu Boot Protocol (BOOTP)	1.3.6.1.4.1.311.1.12	(žádná)	Služba Routing and Remote Access
MSIPRIP2.MIB ripagnt.dll	Databáze MIB definovaná společností Microsoft pro protokol Routing Information Protocol version 2 (RIP2)	1.3.6.1.4.1.311.1.11	(žádná)	Služba Routing and Remote Access
NIPX.MIB rtipxmib.dll	Databáze MIB definovaná společností Novell pro protokol IPX	1.3.6.1.4.1.23.2.5	(žádná)	Služba Routing and Remote Access
SMI.MIB (žádné .dll)	Poskytuje obecné definice pro strukturu a identifikaci informací o správě propojených sítí s protokolem TCP/IP.	(Identifikátor objektu není k dispozici)	1155 1215 1902 1903 1904	(žádná)
WFOSPF.MIB ospfagnt.dll	Databáze MIB definovaná společností Nortel Networks pro směrování Open Shortest Path First (OSPF)	1.3.6.1.4.1.18	(žádná)	Služba Routing and Remote Access
WINS.MIB winsmib.dll	Databáze MIB definovaná společností Microsoft pro službu Windows Internet Name Service (WINS)	1.3.6.1.4.1.311.1.2	(žádná)	Rozhraní WINS

Kromě toho, že jsou konfigurovány v registru agenta služby SNMP, musí být nové objekty databáze MIB také registrovány v softwarové aplikaci správy SNMP v systému správy. Více informací o registrování nových objektů databází MIB ve správci najdete v dokumentaci ke své softwarové aplikaci správy.

Další zdroje

Více informací o databázi MIB a službě SNMP najdete v následujících knihách:

- Douglas E. Comer: *Internetworking with TCP/IP*, 1995, Upper Saddle River: Prentice Hall, Inc.
- D. Perkins, E. McGinnis: *Understanding SNMP MIBs*, 1997, Upper Saddle River: Prentice Hall PTR.

- M. T. Rose: *The Simple Book: An Introduction to Internet Management*, Revised Second Edition, 1996, Upper Saddle River: Prentice-Hall PTR.
- W. Stallings: *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, třetí vydání*, 1999, Reading: Addison-Wesley Publishing Company.

PŘÍLOHA H

Soubor LMHOSTS

Systém Microsoft® Windows® 2000 podporuje několik různých služeb překladu názvů pro vyhledávání, komunikaci a připojování prostředků v síti. Například příkaz pro připojení k aplikačnímu serveru použitím názvu serveru musí být v sítích TCP/IP přeložen na adresu IP dříve, než může být příkaz úspěšně dokončen. Toto bývá označováno jako překlad názvu.

Pokud je v síti dostupná služba Windows Internet Name Service (WINS), může být pro podporu podsítí, které nemají server WINS, použit soubor LMHOSTS, a poskytovat záložní službu překladu názvů, pokud není server WINS k dispozici. Soubor LMHOSTS poskytuje metodu překladu názvů pro NetBIOS, která může být použita pro malé sítě, které nepoužívají server WINS.

V této příloze

Použití souboru LMHOSTS k nalezení počítačů a služeb 722

Vytváření souboru LMHOSTS 724

Nastavení TCP/IP pro použití překladu názvů souborem LMHOSTS 731

Použití souboru LMHOSTS k nalezení počítačů a služeb

Systémy Windows 2000 a Microsoft® Windows NT® verze 4.0 a 3.5x poskytují služby překladu názvů pro názvy počítačů pro NetBIOS i pro názvy hostitelských počítačů ve službě Domain Name System (DNS) v sítích TCP/IP. Informace o překladu názvů pomocí služby WINS a souborů LMHOSTS najdete v části „Služba Windows Internet Name Service“ v této knize. Informace o překladu názvů pomocí služby DNS najdete v části „Služba Windows 2000 DNS“ v této knize.

Použití souboru LMHOSTS je jedna z metod překladu názvů pro názvy pro NetBIOS v sítích TCP/IP. V závislosti na konfiguraci počítače mohou být použity také následující metody pro překlad názvů pro NetBIOS v sítích TCP/IP:

- Mezipaměť pro názvy pro NetBIOS
- Všesměrová vysílání podsítím IP
- Názvový server WINS pro NetBIOS
- Překlad názvů DNS

Poznámka: Služba NetBIOS prostřednictvím TCP/IP (NetBT) je definována společenstvím Internet Engineering Task Force ve specifikacích RFC 1001 a 1002. Tyto specifikace definují různé režimy překladu názvů – všesměrové vysílání, point-to-point, smíšené a hybridní – které používá počítač pro překlad adres IP z názvů pro NetBIOS.

Ve výchozím nastavení po instalaci používá počítač se systémem Windows 2000, který není nastaven jako klient WINS nebo server WINS, režim všesměrového vysílání pro překlad názvů a je nazýván uzle B. Uzel B je počítač, který používá všesměrové vysílání IP pro překlad názvů pro NetBIOS.

Překlad názvů všesměrovým vysíláním IP může poskytovat dynamický překlad názvů. K nevýhodám všesměrového vysílání dotazů na názvy však patří zvýšený provoz v síti a neefektivita ve směrovaných sítích. Prostředky, nacházející se mimo místní podsítě nepřijímají dotaz na název všesměrovým vysíláním IP, protože podle definice všesměrová vysílání úrovně IP nejsou předávána vzdáleným podsítím směrovačem (výchozí bránou) v místní podsíti.

Jako alternativní metodu k všesměrovému vysílání IP vám systém Windows 2000 umožňuje manuálně mapovat názvy pro NetBIOS na adresy IP pro vzdálené počítače použitím souboru LMHOSTS. Zvolená mapování ze souboru LMHOSTS jsou udržována v omezené mezipaměti pro mapování. Tato mezipaměť je inicializována při spuštění počítače. Když počítač potřebuje přeložit název, je nejdříve prozkoumána mezipaměť a teprve když zde není dosaženo shody, použije systém Windows 2000 režim všesměrového vysílání IP, aby se pokusil nalézt počítač s daným názvem pro NetBIOS. Když dotaz všesměrovým vysíláním IP selže, počítač analyzuje celý soubor LMHOSTS (nikoliv jen mezipaměť), aby našel název pro NetBIOS a odpovídající adresu IP. Tato strategie umožňuje, aby soubor LMHOSTS obsahoval velké množství mapování bez vyžadování velkého kusu statické paměti pro udržování málo používané mezipaměti. V případě, že počítač nedokáže přeložit název použitím souboru LMHOSTS, použije pro překlad názvu službu DNS.

Soubor LMHOSTS může být použit pro mapování názvů počítačů a adres IP pro počítače mimo místní podsítě (výhoda proti metodě všesměrového vysílání). Soubor

LMHOSTS můžete použít pro nalezení vzdálených počítačů pro souborové a tiskové služby, pro služby procedur a domén jako jsou přihlašování, prohledávání a replikace. Metoda překladu názvů souborem LMHOSTS v systému Windows 2000 je kompatibilní se soubory LMHOSTS v sítích TCP/IP pro Microsoft® LAN Manager 2.x.

Vyhledávání vzdálených počítačů

Názvy počítačů mimo místní podsítí všesměrového vysílání mohou být přeloženy, pokud názvy vzdálených počítačů a jejich odpovídající adresy IP jsou uvedeny v souboru LMHOSTS. Předpokládejme například, že váš počítač s názvem KlientA je konfigurován bez služby klienta WINS, ale vy chcete použít síť TCP/IP pro připojení k počítači s názvem ServerB, který se nachází v jiné podsíti sítě TCP/IP. Ve výchozím nastavení je váš počítač uzlem B, který používá mezipaměť NetBIOS a všesměrová vysílání IP a je mu umožněno prohledávání souboru LMHOSTS, přičemž obsah souboru LMHOSTS vám poskytly správce sítě.

Při spuštění systému je mezipaměť pro názvy v počítači KlientA „předem naplněna“ pouze těmi položkami ze souboru LMHOSTS, které jsou určeny pro naplňování předem označením klíčovým slovem #PRE. (Více informací o klíčových slovech v souboru LMHOSTS najdete v části „Vytváření položek v souboru LMHOSTS“ dále v této příloze). V tomto příkladu se ServerB nachází ve vzdálené podsíti mimo oblast všesměrového vysílání vaší místní podsítě a není jednou z položek mezipaměti. Všesměrové vysílání přesně podle pravidel pro uzel B (jak je definováno ve specifikacích RFC 1001 a 1002) selže na nedodržení časového limitu, kdy odpověď není přijata, protože ServerB se nachází ve vzdálené podsíti a nemůže přijmout požadavky všesměrového vysílání od počítače KlientA.

V případě popsaného příkladu by mohla činnost, týkající se překladu názvu, proběhnout v následujících krocích:

1. Uživatel na počítači KlientA spustí příkaz systému Windows 2000, například příkaz pro tisk souboru, který použije název pro NetBIOS počítače ServerB.
2. V mezipaměti názvů pro NetBIOS v počítači KlientA proběhne hledání adresy IP, která odpovídá názvu pro NetBIOS počítače ServerA.
3. Protože název pro NetBIOS počítače ServerA a jeho adresa IP nebyly předem zavedeny do mezipaměti, jeho název pro NetBIOS není nalezen v mezipaměti pro názvy a KlientA vyšle všesměrově dotaz na název s názvem pro NetBIOS počítače ServerB.
4. Protože počítač ServerB se nachází ve vzdálené podsíti a všesměrová vysílání IP nejsou směrována do vzdálených podsítí, nedostane KlientA odpověď na svůj dotaz na název. (Pokud by ServerB byl v místní síti, dostal by KlientA odpověď na své všesměrové vysílání a tato odpověď by obsahovala adresu IP počítače ServerB.)
5. Protože na počítači KlientA je umožněna metoda překladu názvů souborem LMHOSTS, pokračuje systém Windows 2000 v pokusech o překlad adresy IP z názvu pro NetBIOS. Je prozkoumán soubor LMHOSTS v adresáři %systemroot%\System32\Drivers\Etc, aby byl nalezen název pro NetBIOS počítače ServerB a jemu odpovídající adresa IP. Pokud název pro NetBIOS není nalezen v souboru LMHOSTS a není nastavena žádná další metoda překladu názvů pro počítač KlientA, obdrží uživatel zprávu o chybě.

Určování řadičů domén

Nejběžnější použití souboru LMHOSTS je vyhledávání vzdálených serverů pro souborové a tiskové služby. Soubor LMHOSTS však může být také použit pro nalezení řadičů domén, poskytujících doménové služby ve směrovaných sítích TCP/IP. Mezi příklady takových aktivit řadičů domén patří pulsy řadiče domény (používané pro synchronizaci databáze účtů), ověřování přihlášení, změny hesel, synchronizace seznamu hlavního prohlédáváče a další aktivity správy domény.

Primární řadiče domény (PDC) a záložní řadiče domény (BDC) v systému Windows 2000 udržují zabezpečovací databázi účtů uživatelů a spravují další služby, vztahující se k síti. Protože velké domény v systému Microsoft® Windows NT® mohou obsahovat více podsítí IP, je možné, že jednotlivé řadiče domén jsou odděleny směrovači nebo že směrovače oddělují počítače v doméně od řadičů domény. V sítích, které nepoužívají servery WINS, může být použit překlad názvů pomocí souboru LMHOSTS pro umožnění spojení počítačů klientů s řadiči domény, umístěnými za směrovači v různých podsítích.

Použití centralizovaných souborů LMHOSTS

Primární soubor LMHOSTS je v každém počítači vždy umístěn v adresáři %systemroot%\System32\Drivers\Etc. V systému Microsoft TCP/IP můžete zahrnout jiné soubory LMHOSTS z místních nebo vzdálených počítačů.

Správci sítě mohou spravovat soubory LMHOSTS používané počítači v síti poskytnutím jednoho nebo více globálních souborů LMHOSTS na centrálním serveru. Počítače se systémem Windows 2000 mohou být v síti nastaveny tak, že importují správná a aktuální mapování názvů počítačů na adresy IP.

Uživatelé mohou importovat soubor LMHOSTS ze vzdálených počítačů v síti použitím příkazů #INCLUDE v souboru LMHOSTS nebo kliknutím na **Importovat soubor LMHOSTS** v dialogovém okně **Upřesňující nastavení TCP/IP**.

Správce může alternativně použít službu Replicator pro distribuci více kopií globálního souboru LMHOSTS více serverům.

Poznámka: Pokud klient sítě přistupuje k centrálnímu souboru LMHOSTS, musí být v počítači, na kterém je soubor umístěn, položka registru NullSessionShares pro umístění souboru LMHOSTS. Položka NullSessionShares je v následujícím podklíči registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
  \lanmanserver\parameters
```

Podrobné informace o registru najdete v nápovědě systému Windows 2000 Server. Informace o obsahu registru najdete na doprovodném CD v souboru Technical Reference to the Windows 2000 Registry (Regentry.chm).

Vytváření souboru LMHOSTS

Před nastavením počítače pro používání souboru LMHOSTS musíte vytvořit primární soubor LMHOSTS na každém počítači, nazvat tento soubor LMHOSTS a uložit ho v adresáři %systemroot%\System32\Drivers\Etc.

Soubor LMHOSTS můžete vytvořit a měnit pomocí textového editoru – například Poznámkového bloku – protože se jedná o jednoduchý textový soubor. (Příklad souboru

LMHOSTS nazvaný LMHOSTS.sam je dodáván se systémem Windows 2000 v adresáři %systemroot%\System32\Drivers\Etc. Tento soubor je pouze příkladem; nepoužívejte tento soubor jako primární soubor LMHOSTS.)

Následující odstavce popisují různé typy položek, které můžete vytvořit a upravovat v souboru LMHOSTS.

Vytváření položek v souboru LMHOSTS

Při vytváření a úpravě položek v souboru LMHOSTS se řiďte následujícími pravidly:

- Položka se skládá z adresy IP počítače, následované alespoň jednou mezerou nebo tabelátorem a názvem počítače pro NetBIOS.

Upozornění Nemůžete přidávat položku souboru LMHOSTS pro počítač, který je klientem služby DHCP, protože adresy IP klientů služby DHCP se mění dynamicky. Abyste předešli problémům, ujistěte se, že počítače, jejichž názvy jsou uvedeny v souborech LMHOSTS jsou nastaveny se statickými adresami IP.

- Každá položka musí být na zvláštním řádku. Poslední položka v souboru musí být ukončena znakem konce řádku.
- Názvy pro NetBIOS smějí obsahovat pouze velká a malá písmena abecedy a zvláštní znaky. Pokud je název uveden v uvozovkách, je použit přesně tak, jak je napsán.. Například název „AccountingPDC“ je názvem se střídáním malých a velkých písmen a název „HumanRscSr \0x03“ je názvem se zvláštním znakem.
- Každý název pro NetBIOS je dlouhý 16 bajtů. Uživatel může definovat prvních 15 znaků názvu pro NetBIOS. 16. znak je nastaven automaticky, aby identifikoval síťovou službu klienta, která název registrovala. Nejznámějším příkladem názvu pro NetBIOS je název libovolného počítače se systémem Windows. Když je počítač spuštěn, spustí se služby klienta sítě Microsoft a registrují své názvy, které se skládají z názvu počítače a jedinečného 16. znaku. Například název <název_počítače{0x00}> je služba pracovní stanice Microsoft Workstation; název < název_počítače{0x20}> je služba serveru Microsoft Server. Jak vidíte, jediný rozdíl mezi těmito dvěma názvy je 16. znak. Tento 16. znak umožňuje jednoznačně identifikovat každou ze síťových služeb klienta, která je spuštěna na počítači.
- Položky v souboru LMHOSTS mohou představovat počítače se spuštěným systémem Microsoft® Windows® 2000 Server, Microsoft® Windows® 2000 Professional, Microsoft® Windows NT® Server, Microsoft® Windows NT® Workstation, Microsoft® Windows® 95, Microsoft® LAN Manager a Microsoft® Windows® for Workgroups 3.11 se sítí Microsoft TCP/IP. V souboru LMHOSTS není potřeba rozlišovat mezi různými platformami.
- Znak dvojitého křížku (#) se obvykle používá jako začátek poznámky. Označuje však také zvláštní klíčová slova, jak jsou popsána v tabulce H.1.

Klíčová slova, uvedená v následující tabulce mohou být použita v souboru LMHOSTS pro počítače se systémem Windows 2000. (Systém LAN Manager 2.x, který také používá soubor LMHOSTS pro překlad názvů NetBT, považuje tato klíčová slova za poznámky).

Tabulka H.1 Klíčová slova souboru LMHOSTS

Klíčové slovo	Popis
\0xnn	Podpora netisknutelných znaků v názvech pro NetBIOS. Název pro NetBIOS uzavřete do uvozovek a použijte notaci \0xnn pro zadání hexadecimální hodnoty znaku. Toto umožňuje ve směrovaných topologiích správné fungování zákaznických aplikací, které používají zvláštní názvy. Protokol TCP/IP v systému LAN Manager však nerozpoznává hexadecimální formát a nemůžete tedy použít zpětnou kompatibilitu, pokud tuto možnost využíváte. Všimněte si, že hexadecimální notace platí pouze pro jeden znak v názvu. Název by měl být vyplněn mezerami tak, aby zvláštní znak (16.znak) byl posledním znakem v řetězci.
#BEGIN_ALTERNATE	Používá se pro seskupování více příkazů #INCLUDE. Každý jednotlivý úspěšný příkaz #INCLUDE ve skupině způsobuje, že je úspěšná skupina.
#END_ALTERNATE	Používá se pro označení konce skupiny příkazů #INCLUDE.
#DOM:<doména>	Část položky, mapující název pro NetBIOS na adresu IP, která udává, že adresa IP je řadičem domény v doméně, uvedeně jako doména. Toto klíčové slovo ovlivňuje způsob chování služeb prohledávače a přihlášení ve směrovaných prostředích TCP/IP. Pro zavedení položky #DOM předem se v položce musí nejdříve vyskytovat klíčové slovo #PRE. Skupiny #DOM jsou omezeny do 25 členů.
#INCLUDE <název_souboru>	Přiměje systém, aby vyhledal soubor, uvedený svým názvem název_souboru a prozkoumal ho, jako kdyby byl částí souboru LMHOSTS. Uvedení názvu souboru ve tvaru univerzální konvence pro názvy (UNC) vám umožňuje použít centrální soubor LMHOSTS na serveru. Pokud server s tímto souborem je umístěn mimo místní podsít všesměrového vysílání, musíte přidat předem zaváděnou položku pro tento server, která bude před položkou v sekci #INCLUDE.
#MH	Část položky, mapující název pro NetBIOS na adresu IP, která označuje vstup jako jedinečný název, který může mít více než jednu adresu. Maximální počet adres, které mohou být přiřazeny jednomu názvu, je 25. Počet položek se rovná počtu síťových adaptérů v počítači.
#PRE	Část položky, mapující název pro NetBIOS na adresu IP, která způsobí, že položka je předem zavedena do mezipaměti pro názvy. Položky nejsou do mezipaměti pro názvy zaváděny automaticky, ale jsou analyzovány teprve když název nelze přeložit službou WINS a všesměrovým vysíláním dotazů na názvy. Klíčové slovo #PRE musí být připojeno k položkám, které se také vyskytují v příkazech #INCLUDE; v opačném případě je položka v příkazu #INCLUDE ignorována.
#SG <název>	Část položky, mapující název pro NetBIOS na adresu IP, která spojuje tuto položku se speciální skupinou, definovanou uživatelem (Internet), uvedenou jako název. Klíčové slovo #SG definuje skupiny v síti Internet použitím názvu pro NetBIOS, který má v 16. bajtu znak 0x20. Speciální skupina je omezena do 25 členů.

Následující příklad ukazuje, jak se používají všechny tato klíčová slova:

```
102.54.94.102 "appname          \0x14"          #zvláštní aplikační server
102.54.94.123 printsrv          #PRE              #zdrojový server
102.54.94.98  localsrv          #PRE
102.54.94.97  primary           #PRE #DOM:mydomain      #PDC pro mydomain
102.54.94.112 machinename       #SG:sg26members
102.54.94.167 multihome26        #MH
102.54.94.168 multihome26        #MH
#BEGIN_ALTERNATE
#INCLUDE \\localsrv\public\lmhosts      #přidává soubor LMHOSTS ze serveru
#INCLUDE \\primary\public\lmhosts      #přidává soubor LMHOSTS ze serveru
#END_ALTERNATE
```

Všimněte si následujících vlastností předchozího příkladu:

- Servery s názvy `printsrv`, `localsrv` a `primary` jsou označeny klíčovým slovem `#PRE` jako položky, které mají být předem zavedeny do mezipaměti názvů pro NetBIOS při spuštění systému.
- Servery s názvy `localsrv` a `primary` jsou také uvedeny v příkazech `#INCLUDE` jako místa s centrálně udržovanými soubory LMHOSTS.
- Server s názvem „appname \0x14“ má v názvu mezery a obsahuje zvláštní znak za prvními 15 znaky. Protože název obsahuje mezery, je spolu se zvláštním znakem uzavřen do uvozovek.

Následující odstavce dále vysvětlují použití klíčových slov `#PRE`, `#DOM`, `#INCLUDE` a `#SG`.

Přidávání názvů vzdálených systémů použitím klíčového slova **#PRE**

Použití položek s klíčovým slovem `#PRE` zlepšuje přístup k označeným počítačům, protože jejich názvy a adresy IP jsou obsaženy v mezipaměti počítače. Ve výchozím nastavení však systém Windows 2000 omezuje velikost mezipaměti na 100 položek. (Tento limit se týká pouze položek, označených klíčovým slovem `#PRE`).

Pokud uvedete více než 100 položek s klíčovým slovem `#PRE`, bude předem do mezipaměti počítače zavedeno pouze prvních 100 položek s klíčovým slovem `#PRE`. Všechny další položky s klíčovým slovem `#PRE` jsou při spuštění počítače ignorovány a použijí se pro překlad názvů pouze tehdy, když selže překlad pomocí mezipaměti a překlad všesměrovým vysíláním IP. Pokud překlad pomocí mezipaměti ani všesměrové vysílání nevedou k překladu názvu, analyzuje systém Windows 2000 celý soubor LMHOSTS, včetně položek s klíčovým slovem `#PRE`, které překročily limit 100 položek mezipaměti.

Výchozí maximální počet položek s klíčovým slovem `#PRE` můžete změnit přidáním položky **MaxPreloadEntries** do registru. Tato položka musí být přidána do následujícího podklíče registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Netbt\Parameters
```

Položka **MaxPreloadEntries** má výchozí a minimální hodnotu 1000 položek pro systémy Windows 2000 a Windows NT verze 3.x a 4.0; maximální hodnota je 2000 položek. Pro systémy Windows 9x je výchozí minimální hodnota 100 položek a maximální hodnota je 500 položek.

Upozornění Nepoužívejte editor registru pro přímou úpravu registru, pokud máte jinou možnost. Editory registru obcházejí standardní zabezpečovací opatření, poskytovaná prostředky pro správu. Tato zabezpečovací opatření vám brání v zadání konfliktních nastavení nebo nastavení, která pravděpodobně sníží výkon nebo poškodí váš systém. Přímá úprava registru může mít závažné neočekávané následky, které mohou zabránit spuštění systému a mohou vyžadovat opětovnou instalaci systému Windows 2000. Pro nastavení nebo přizpůsobení systému Windows 2000 použijte programy v Ovládacích panelech nebo konzolu Microsoft Management Console (MMC) kdykoli je to možné.

Soubor LMHOSTS by mohl například obsahovat následující informace:

```
102.54.94.91      accounting      #server účtárny
102.54.94.94      payroll        #server mezd
102.54.94.97      stockquote     #PRE      #server kurzů akcií
102.54.94.102    printqueue     #tiskový server v budově 7
```

V tomto příkladu je server s názvem stockquote zaveden předem do mezipaměti, protože je označen klíčovým slovem #PRE. Servery s názvy accounting, payroll a printqueue jsou překládány pouze tehdy, když při jejich překladu selže prohledávání mezipaměti a všesměrově vysílání dotazů na názvy. Po přeložení názvů hostitelských počítačů, jejichž položky v souboru LMHOSTS nejsou označeny pro předběžné zavádění, udržuje systém mapování názvu pro NetBIOS na adresu IP po určitou dobu v mezipaměti pro další použití.

Přidávání řadičů domény použitím klíčového slova #DOM

Klíčové slovo #DOM může být použito v souborech LMHOSTS k odlišení řadiče domény systému Windows 2000 od dalších počítačů v síti. Pro použití značky #DOM uveďte za názvem pro NetBIOS a adresou IP řadiče domény v souboru LMHOSTS klíčové slovo #DOM, dvojtečku a doménu, ve které se řadič domény účastní. Například:

```
102.54.94.97      primary #PRE      #DOM:mydomain      #řadič PDC domény mydomain
```

Použití klíčového slova #DOM k označení řadičů domény způsobuje, že počítač přidává položky do mezipaměti názvů domén, kterou používá při navazování kontaktu s dostupnými řadiči při zpracování požadavků na domény. Když dojde k aktivitě řadiče domény, jako je požadavek na přihlášení, posílá počítač požadavky názvu skupiny domény. V místní podsíti počítač všesměrově vysílá požadavek a ten je vyzvednut některým z místních řadičů domény. Řadiče domény ve vzdálených podsítích však také přijímají požadavky, protože síť Microsoft TCP/IP používá datagramy pro předávání požadavků řadičům domény, umístěným ve vzdálených podsítích, když použijete klíčové slovo #DOM k označení řadičů domény v souboru LMHOSTS. Přidání více řadičů domény do souboru LMHOSTS pomůže distribuovat zátěž požadavků domén mezi všemi řadiči domény..

Při mapování důležitých členů domény použitím klíčového slova #DOM se držte následujících vodítek:

- Položky s klíčovým slovem #DOM by měly být předem zavedeny do mezipaměti použitím klíčového slova #PRE. Všimněte si, že klíčové slovo #PRE musí předcházet klíčovému slovu #DOM v souboru LMHOSTS.
- Pro každý místní soubor LMHOSTS v počítači s operačním systémem Windows 2000, který je členem domény, je zapotřebí uvést položky s klíčovým slovem

#DOM pro všechny řadiče domény v doménách, které jsou umístěny ve vzdálených podsítích. To zajišťuje, že ověřování přihlášení, změny hesel, prohledávání atd. funguje správně pro místní doménu.

- Místní soubory LMHOSTS na všech serverech, které mohou být záložními řadiči domény musí obsahovat název a adresu IP primárního řadiče domény a mapování pro všechny další záložní řadiče domény. To zajišťuje, že povýšení záložního řadiče domény na primární řadič domény neovlivní schopnost povýšeného řadiče domény nabízet všechny služby členům domény.
- Pokud mezi dvěma doménami existují vztahy důvěryhodnosti, všechny řadiče domény pro všechny důvěryhodné domény musí být také uvedeny v místním souboru LMHOSTS.
- Pro domény, které chcete prohledávat ze své místní domény, musí místní soubor LMHOSTS obsahovat alespoň název a adresu IP primárního řadiče domény ve vzdálené doméně. Také záložní řadiče domény ve vzdálených doménách musí být opět uvedeny, aby povýšení na primární řadiče domény nenarušilo schopnost prohledávání vzdálených domén.

Názvy, které se vyskytují v položce s klíčovým slovem #DOM v souboru LMHOSTS se ukládají ve zvláštní doménové mezipaměti pro NetBT. Když je rozhraním NetBT odeslán takové doméně datagram, používající název DOMAIN<1C>, je název překládán nejdříve pomocí služby WINS nebo všesměrového vysílání IP. Datagram je pak odeslán na všechny adresy, obsažené v seznamu ze souboru LMHOSTS a rovněž je provedeno všesměrové vysílání v místní podsíti.

Přidávání zvláštních skupin definovaných uživatelem použitím klíčového slova #SG

Můžete seskupovat prostředky, jakými jsou tiskárny nebo počítače, které patří do skupiny v propojených sítích, použitím klíčového slova #SG k definování speciální skupiny v souboru LMHOSTS. Speciální skupiny jsou omezeny do počtu 25 členů.

Můžete uvést název skupiny přesně tak, jak byste uvedli název domény s tím, že v položce použijete klíčové slovo #SG. Následující příklad vytváří speciální skupinu mycompany:

```
102.54.94.99    printsrvsg      #SG:mycompany #Speciální skupina počítačů
```

V některých případech možná budete chtít pouze uvést název speciální skupiny bez udání adresy IP. To lze provést neuvedením adresy IP v jinak úplné položce, jako v následujícím příkladu:

```
printsrvsg      #SG:mycompany      #Speciální skupina počítačů
```

Přidávání zařízení s více adresami použitím klíčového slova #MH

Zařízení s více adresami (někdy také vícedomé zařízení) je počítač s více síťovými adaptéry. Zařízení s více adresami může být definováno jedním jednoznačným názvem, se kterým je spojeno více adres IP.

V soubor LMHOSTS můžete uvést mapování názvů pro NetBIOS s více adresami na adresy IP vytvořením položek, které jsou označeny jako položky s více adresami klíčovým slovem. Položka s klíčovým slovem #MH spojuje jeden jedinečný název počítače pro NetBIOS s adresou IP. Můžete vytvořit více položek pro stejný název počítače pro

NetBIOS pro každý síťový adaptér v zařízení s více adresami až do maximálního počtu 25 různých adres IP pro stejný název.

Formát položky souboru LMHOSTS, který se používá pro specifikaci mapování názvu pro NetBIOS na adresu IP pro zařízení s více adresami je stejný jako u ostatních položek s klíčovými slovy. Následující příklad ukazuje položky, požadované pro mapování názvů na adresy IP pro počítač s více adresami se dvěma síťovými adaptéry:

```
102.54.94.91 accounting      #MH      #adresa NIC 1 serveru accounting
102.54.94.92 accounting      #MH      #adresa NIC 2 serveru accounting
```

Definování centrálního souboru LMHOSTS použitím klíčového slova #INCLUDE

Pro malé až střední síť s méně než 20 doménami obvykle uspokojí požadavky všech pracovních stanic a serverů v síti jeden společný soubor LMHOSTS. Správce sítě může použít službu Replicator systému Windows 2000 k udržování synchronizovaných místních kopií globálního souboru LMHOSTS a používat centralizované soubory LMHOSTS, jak je popsáno v tomto odstavci.

Použitím klíčových slov #BEGIN_ALTERNATE a #END_ALTERNATE poskytnete seznam serverů, které udržují kopie stejného souboru LMHOSTS. Toto je známo jako zahrnutí bloku (block inclusion), které umožňuje vyhledávání platné kopie určitého souboru na více serverech. Následující příklad ukazuje použití klíčového slova #INCLUDE k zahrnutí místního souboru LMHOSTS (umístěného v adresáři C:\Private), a použití klíčového slova #_ALTERNATE k zahrnutí serverů, spravujících kopie stejného souboru LMHOSTS:

```
102.54.94.97    primary      #PRE  #DOM:mydomain    #primární řadič d.
102.54.94.99    backupdc     #PRE  #DOM:mydomain    #záložní řadič d.
102.54.94.98    localsvr     #PRE  #DOM:mydomain
#INCLUDE        c:\private\lmhosts      #zahrne místní lmhosts
#BEGIN_ALTERNATE
#INCLUDE        \\primary\public\lmhosts  #zdroj pro globální s.
#INCLUDE        \\backupdc\public\lmhosts #záložní zdroj
#INCLUDE        \\localsvr\public\lmhosts #záložní zdroj
#END_ALTERNATE
```

Upozornění: Tato možnost by neměla být nikdy používána pro zahrnutí vzdáleného souboru z přesměrované jednotky, protože soubor LMHOSTS je sdílen mezi místními uživateli, kteří mají různé profily a různé přihlašovací skripty. I na systémech s jedním uživatelem se může měnit mapování přesměrovaných jednotek mezi relacemi přihlášení.

V předchozím příkladu se nacházejí servery primary a backupdc na vzdálených podsítích vzhledem k počítači, který vlastní soubor. Místní uživatel se rozhodl zahrnout seznam preferovaných serverů v místním souboru LMHOSTS, umístěném v adresáři C:\Private. Během překladu názvů zahrne systém Windows 2000 nejdříve tento privátní soubor, pak získá globální soubor LMHOSTS z jednoho ze tří umístění: primary, backupdc nebo localsvr. Všechny názvy serverů v příkazech #INCLUDE musí mít adresy zavedené předem do mezipaměti použitím klíčového slova #PRE; v opačném případě jsou příkazy #INCLUDE ignorovány.

Zahrnutí bloku je vyhověno, pokud je dostupný některý ze zdrojů pro globální soubor LMHOSTS a není použit žádný z dalších serverů. Pokud není žádný server k dispozici nebo je cesta k souboru LMHOSTS z nějakého důvodu neplatná, je k protokolu událostí přidána položka, která udává, že zahrnutí bloku se nezdařilo.

Nastavení TCP/IP pro použití překladu názvů souborem LMHOSTS

Ve výchozím nastavení umožňuje systém Windows 2000 použití souboru LMHOSTS pro překlad názvů, když je na počítači instalována síť TCP/IP. Použití souboru LMHOSTS pro překlad názvů můžete zakázat uvolněním zaškrtnutí políčka **Povolit hledání v souboru LMHOSTS** v záložce **WINS** v dialogovém okně **Upřesňující nastavení TCP/IP**. Zákaz používání souboru LMHOSTS pro překlad názvů se však nedoporučuje, protože soubor LMHOSTS poskytuje záložní názvovou službu pro servery WINS, které nejsou připojeny nebo jsou nedostupné.

Pro použití souboru LMHOSTS ze vzdáleného počítače nebo z jiného adresáře místního počítače klepněte na **Importovat soubor LMHOSTS** v záložce **WINS** v dialogovém okně **Upřesňující nastavení TCP/IP**.

Údržba souboru LMHOSTS

Když používáte soubor LMHOSTS, ujistěte se, že ho udržujete aktuální a uspořádaný. používejte následující vodítka:

- Aktualizujte soubor LMHOSTS pokaždé, když u počítače v síti dojde ke změně nebo odstranění názvu pro NetBIOS.
- Protože soubory LMHOSTS jsou prohledávány řádek po řádku, uvádějte vzdálené počítače v pořadí podle priority, s nejpoužívanějšími z nich na začátku souboru, za nimiž následují vzdálené systémy, uvedené v příkazech #INCLUDE.
- Použijte položky s klíčovými slovy #PRE k předběžnému zavedení často používaných pracovních stanic a serverů, uváděných v příkazech #INCLUDE, do místní mezipaměti počítače. Položky s klíčovým slovem #PRE by měly být uváděny na konci souboru, protože jsou předem zavedeny do mezipaměti při spuštění a později se k nim nepřistupuje. To zvyšuje rychlost hledání pro nejčastěji používané položky, protože všechny poznámky, které přidáte, zvyšují čas, potřebný pro analýzu souboru.
- Používejte příkaz **nbtstat** pro odstranění nebo opravu u předběžně zavedených položek, které mohly být zapsány nesprávně, nebo u názvů, uložených do mezipaměti po úspěšném překladu všesměrovým vysíláním. Můžete obnovit původní obsah mezipaměti pro názvy spuštěním příkazu **nbtstat -R**, což vyčistí a znovu zaplní mezipaměť pro názvy, znovu přečte soubor LMHOSTS a poté vloží položky, označené klíčovým slovem #PRE. Více informací o příkazu **nbtstat** najdete v nápovědě systému Windows 2000 Server.

Odstraňování potíží se souborem LMHOSTS

Při používání souboru LMHOSTS se mohou vyskytnout problémy, jako neschopnost nalézt vzdálený počítač, které mohou být způsobeny přítomností jedné nebo více z následujících chyb v souboru LMHOSTS:

- Scházející položka pro vzdálený server.
- Nesprávně napsaný název počítače pro NetBIOS. (Všimněte si, že názvy pro NetBIOS jsou automaticky převáděny na velká písmena).
- Neplatná adresa IP pro název počítače.
- Scházející znak konce řádku na konci poslední položky.

PŘÍLOHA I

Prohledávací služba v systému Windows 2000



Systémy Microsoft® Windows® 2000 Server a Microsoft® Windows® 2000 Professional nadále podporují službu prohledávače, původně zavedenou v systému Microsoft® Windows® for Workgroups verze 3.1, aby zajistily spolupráci s doménami a počítači, které nedokáží používat adresářovou službu Active Directory™. V sítích pouze s počítači se systémem Windows 2000 mohou klienti najít síťové servery a prostředky sdílení souborů prostřednictvím objektu sdílené složky v adresářové službě Active Directory. Z praktických důvodů však bude většina organizací používat v dohledné budoucnosti službu prohledávače pro obsluhu starších počítačů, které nedokáží používat službu Active Directory. Služba prohledávače a rozhraní NetBIOS jsou povoleny ve výchozím nastavení po instalaci Windows 2000.

V této příloze

Úvod do služby Browser	734
Přehled systému prohledávačů v systému Windows 2000	734
Volby prohledávačů	739
Oznámení prohledávačů	741
Požadavky prohledávače	744
Počet prohledávačů v doméně nebo pracovní skupině	745
Vypnutí nebo selhání prohledávače	745
Prohledávací služba přes více pracovních skupin a domén	747
Počítače se systémy Windows for Workgroups, Windows 95 a Windows 98 jako hlavní prohledávače	752
Registrace a šíření	752
Testovací techniky	754

Příbuzné informace v Resource Kitu

- Informace o směrovacích službách IPX systému Windows 2000 IPX najdete v části „Směrování IPX“ v knize *Microsoft® Windows® 2000 Server Internetworking*.
- Informace o přenášení ze systému NetWare do systému Windows 2000 najdete v části „Určování strategií přenosu domén“ v knize *Microsoft® Windows® 2000 Server Plánování a implementace sítě*.

Úvod do služby Browser

Uživatelé často potřebují vědět, které domény a počítače jsou přístupné z jejich místního počítače. Prohlížení všech síťových prostředků dostupných v síti počítačů se systémem Microsoft® Windows® 2000 nebo Microsoft® Windows NT® se říká prohlédávání (browsing). Služba prohlédávace systému Windows udržuje seznam – nazvaný seznam prohlédávání sítě (browse list) – všech dostupných domén a serverů. Seznam prohlédávání sítě může být prohlížen použitím Průzkumníka a je poskytován službou Browser v doméně místního počítače.

Poznámka: Pro účely této diskuse bude termín server odkazovat na každý počítač, který může poskytovat prostředky zbytku sítě. Pokud počítač se spuštěným systémem Microsoft® Windows® 95, Microsoft® Windows® 98, Microsoft® Windows® for Workgroup verze 3.11, Microsoft® Windows NT® Workstation nebo Windows 2000 Professional může sdílet prostředky souborů nebo tisku s jinými počítači v síti, je v kontextu systému prohlédavačů považován za server. Počítač nemusí aktivně sdílet prostředky, aby byl považován za server.

Tato příloha obsahuje popis následujících témat:

- Úloha prohlédavacích počítačů v systému prohlédavačů.
- Koordinace prohlédavacími počítači pro poskytnutí přesného seznamu prohlédávání sítě, i když hlavní prohlédavač selže.
- Volba hlavního prohlédavače.
- Volání aplikačního programového rozhraní (API), používaná pro registraci počítačů pro seznam prohlédávání sítě a pro příjem seznamu od hlavního prohlédavače.
- Prohlédávání přes domény.
- Odstraňování problémů prohlédavačů.

Přehled systému prohlédavačů v systému Windows 2000

Systémy Windows 2000 a Windows NT pro zajištění služeb prohlédavačů přiřazují úkoly určitým počítačům v síti. Počítače spolupracují při poskytování centralizovaného seznamu sdílených prostředků, přičemž odstraňují potřebu udržování vlastních seznamů všemi počítači. Tím se snižuje potřeba času jednotky CPU a síťového provozu pro vytvoření a údržbu seznamu.

Systém prohlédavačů v systému Windows 2000 se skládá z hlavního prohlédavače, záložních prohlédavačů a klientů prohlédavačů. Počítač, který je hlavním prohlédavačem, udržuje seznam prohlédávání sítě a pravidelně posílá jeho kopie záložním prohlédavačům. Když potřebuje klient prohlédavače informace, dostane aktuální seznam prohlédávání sítě vzdáleným zasláním volání aplikačního programového rozhraní **NetServerEnum** buď hlavnímu, nebo záložnímu prohlédavači.

Systém prohlédavačů se skládá ze dvou součástí, služby prohlédavače a příjemce datagramů.

Služba prohledávače je částí systému prohledávače pracující v uživatelském režimu a je zodpovědná za udržování seznamu prohledávání sítě, odesílání požadavků API a správu různých rolí prohledávačů, které počítač může mít. Služba prohledávače ve skutečnosti sídlí uvnitř Správce služeb (program Services.exe který volá knihovnu browser.dll).

Přijímač datagramů je částí systému prohledávačů pracující v režimu jádra a je jednoduše přijímačem datagramů a poštovní přihrádkou. Přijímá směrované a všesměrové datagramy, které jsou předmětem zájmu služeb systémů Windows 2000 Professional a Windows 2000 Server. Přijímač datagramů rovněž poskytuje podporu na úrovni jádra pro aplikační programové rozhraní **NetServerEnum**, podporu pro vzdálený příjem zpráv do poštovní přihrádky (zprávy druhé třídy, založené na datagramech, poštovní zprávy) a služby oznamování požadavků.

V systémech Microsoft® Windows NT® verze 3.5 a pozdějších je přijímač datagramů implementován v přeměrovači systému Windows NT (Rdr.sys). V systému Microsoft® Windows NT® verze 3.1 existuje zvláštní ovladač Browser.sys pro přijímač datagramů.

Centralizovaná architektura prohledávačů rovněž snižuje požadavky na jednotku CPU a paměť počítače klienta.

Určování prohledávacích počítačů

Když spustíte počítač se systémem Windows 2000, hledá prohledávací služba v registru položku **MaintainServerList**, aby určila, zda se počítač stane prohledávačem. Položka **MaintainServerList** se nachází v následujícím podklíči registru:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  \Browser\Parameters
```

Tabulka I.1 ukazuje hodnoty, které mohou být nastaveny pro položku **MaintainServerList** a jejich význam pro účast počítače ve službách prohledávače.

Tabulka I.1 Pripustné hodnoty pro položku registru MaintainServerList Registry

Hodnota	Význam
No	Tato hodnota zabraňuje počítači, aby se účastnil jako prohledávač.
Yes	Tato počítače udělá z počítače prohledávač. Při spuštění se počítač pokouší spojit s hlavním prohledávačem, aby získal aktuální seznam prohledávání sítě. Pokud nelze nalézt hlavní prohledávač, vyvolá počítač volby prohledávačů. Počítač je buď zvolen hlavním prohledávačem nebo se stane záložním prohledávačem. Tato hodnota je výchozí hodnotou pro počítače se systémy Windows 2000 Server a Windows NT Server.
Auto	Tato hodnota udělá z počítače potenciální prohledávač. Může se stát prohledávačem podle počtu aktuálně aktivních prohledávačů. Hlavní prohledávač informuje tento počítač, zda se stane nebo nestane záložním prohledávačem. Tato hodnota je výchozí hodnotou pro počítače se systémy Windows 2000 Professional a Windows NT Workstation.

Na každém počítači s hodnotou položky **MaintainServerList** nastavenou na **Yes** nebo **Auto** je spuštěna služba prohledávače při spuštění systému počítače.

Upozornění: Nepoužívejte editor registru pro přímou úpravu registru, pokud máte jinou možnost. Editory registru obcházejí standardní zabezpečovací opatření, poskytovaná

prostředky pro správu. Tato zabezpečovací opatření vám brání v zadání konfliktních nastavení nebo nastavení, která pravděpodobně sníží výkon nebo poškodí váš systém. Přímá úprava registru může mít závažné neočekávané následky, které mohou zabraňovat spuštění systému a mohou vyžadovat opětovnou instalaci systému Windows 2000. Pro nastavení nebo přizpůsobení systému Windows 2000 použijte programy v Ovládacích panelech nebo konzolu Microsoft Management Console (MMC) kdykoli je to možné.

Jiná položka registru, **IsDomainMaster**, pomáhá určovat, které servery se stanou hlavními prohledávači a záložními prohledávači. Nastavení hodnoty položky **IsDomainMaster** na **True** udělá z počítače *upřednostňovaný hlavní prohledávač*. Každý počítač se spuštěným systémem Windows 2000 nebo Windows NT může být nastaven jako upřednostňovaný hlavní prohledávač.

Když je spuštěna prohledávací služba na upřednostňovaném hlavním prohledávači, vyvolá prohledávací služba volby. Upřednostňované hlavní prohledávače dostanou ve volbách prioritu, což znamená, že upřednostňovaný hlavní prohledávač vždy vyhraje volby, pokud tomu nezabrání jiná podmínka. To dává správci sítě možnost nastavit určitý počítač jako hlavní prohledávač.

Pro stanovení počítače upřednostňovaným hlavním prohledávačem nastavte hodnotu položky **IsDomainMaster** na **True**. Tato položka (typ `dat Reg_SZ`) se objevuje v následujícím podklíči registru:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
\Browser\Parameters
```

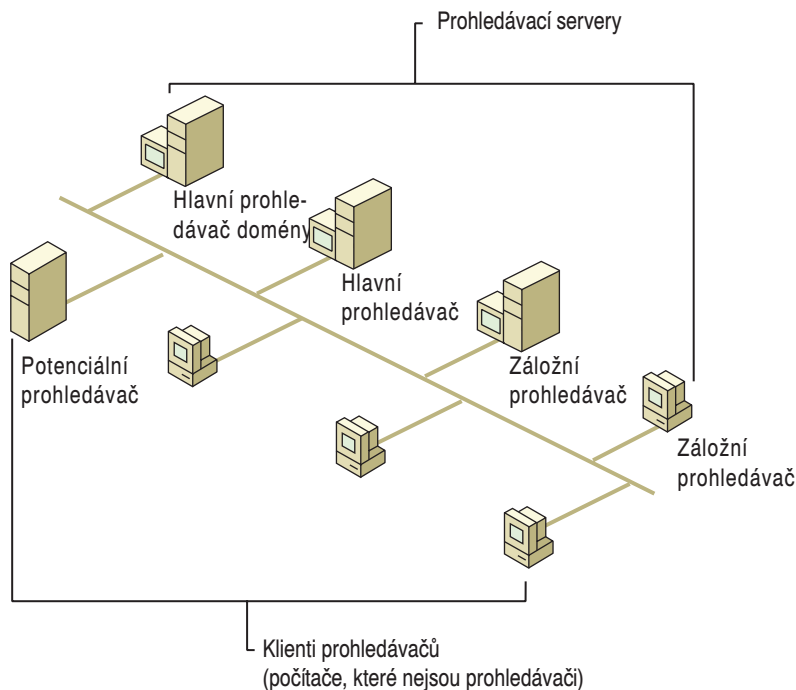
Pokud není počítač nastaven jako upřednostňovaný hlavní prohledávač, je hodnota položky **IsDomainMaster** vždy nastavena na **False** nebo **No**. K provádění těchto změn není k dispozici žádné uživatelské rozhraní; registr musí být změněn použitím editoru registru (`Regedt32.exe` nebo `Regedit.exe`).

Role v systému prohledávačů

Počítače se systémy Windows 2000, Windows NT 3.1, Microsoft® Windows NT® Advanced Server verze 3.1, Microsoft® Windows NT® Workstation verze 3.5 nebo pozdější, Microsoft® Windows NT® Server verze 3.5 nebo pozdější, Windows for Workgroups 3.11, Windows 95 nebo Windows 98 mohou být prohledávači. V systému prohledávačů je pět typů počítačů:

- Počítače, které nejsou prohledávači
- Potenciální prohledávače
- Záložní prohledávače
- Hlavní prohledávače
- Hlavní prohledávače domén

Obrázek I.1 Ukazuje podsít s prohledávači a počítači, které nejsou prohledávači.



Obrázek I.1 Prohledávače a počítače, které nejsou prohledávači

Počítač, který není prohledávačem (Non-Browser)

Počítač, který není prohledávačem je počítač, který byl nastaven tak, že neudrhuje seznam síťových prostředků nebo seznam prohledávání sítě.

Potenciální prohledávač (Potential Browser)

Potenciální prohledávač je počítač, který je schopen udržovat seznam prohledávání síťových prostředků a může být zvolen hlavním prohledávačem. Potenciální prohledávač může jednat jako záložní prohledávač, pokud je mu k tomu dán pokyn hlavním prohledávačem.

Záložní prohledávač (Backup Browser)

Záložní prohledávač dostává kopii seznamu prohledávání síťových prostředků od hlavního prohledávače a rozděljuje tento seznam na vyžádání počítačům v doméně nebo pracovní skupině. Všechny řadiče domén v systému Windows 2000 jsou nastaveny buď jako hlavní, nebo jako záložní prohledávače.

Počítače se spuštěnými systémy Windows 2000 Professional, Windows NT Workstation, Microsoft® Windows® for Workgroups nebo Windows 95 mohou být záložními prohledávači, pokud jsou v síti méně než tři počítače se systémy Windows 2000 nebo Windows NT Server, provádějící funkce záložních prohledávačů pro doménu.

Seznam serverů je omezen velikostí do 64 kilobajtů (KB) na počítačích se systémy Windows NT s verzí starší než 4.0, Windows for Workgroups a Windows 95. To omezuje

počet počítačů v seznamu prohledávání sítě pro jednu pracovní skupinu nebo doménu na počet mezi 2000 a 3000.

Poznámka: Obsáhlé poznámky u serverů mohou významně snižovat počet počítačů, které mohou být uvedeny v seznamu prohledávání sítě, protože seznam je omezen velikostí 64 kilobajtů (KB).

Hlavní prohledávač (Master Browser)

Hlavní prohledávač je odpovědný za sběr informací, nezbytných pro vytvoření a udržování seznamu prohledávání sítě. Seznam prohledávání sítě obsahuje všechny servery v doméně nebo pracovní skupině hlavního prohledávače a seznam všech domén sítě.

Jednotlivé servery oznamují svou přítomnost hlavnímu prohledávači posíláním směrovaných datagramů, nazývaných oznámení o serveru (server announcement), hlavnímu prohledávači domény nebo pracovní skupiny. Počítače se systémy Windows 2000, Windows NT, Windows for Workgroups, Windows 95, Windows 98 nebo Microsoft® LAN Manager posílají oznámení o serveru. Když hlavní prohledávač přijme oznámení o serveru od počítače, přidá tento počítač k seznamu prohledávání sítě.

Pokud doména obsahuje více než jednu podsít, provede hlavní prohledávač následující úkoly:

- Udržuje seznam prohledávání sítě pro část domény ve své podsíti.
- Poskytuje seznam záložních prohledávačů v místní podsíti sítě TCP/IP počítačům se systémy Windows 2000, Windows NT, Windows 95, Windows 98 a Windows for Workgroups.

podsít v síti TCP/IP se skládá z více než jedné domény, každá doména má svůj vlastní hlavní prohledávač a záložní prohledávače. V sítích s protokolem NWLink, který je kompatibilní se síťovým protokolem IPX/SPX, jsou obvykle nastaveny směrovače pro předávání paketů typu 0x14. Protože pakety všesměrového vysílání včetně hlasovacích paketů jsou šířeny tímto způsobem, je tak zaručeno, že vždy existuje pouze jeden hlavní prohledávač. Naproti tomu rámec NetBEUI (NBF), který není vytvořen pro síť se směrováním, vyžaduje oddělený hlavní prohledávač pro podsít.

Když je počítač spuštěn a hodnota položky registru **MaintainServerList** je nastavena na **Auto**, hlavní prohledávač musí počítači sdělit, zda se má nebo nemá stát záložním prohledávačem.

Hlavní prohledávač domény

Hlavní prohledávač domény zodpovídá za sběr oznámení pro celou doménu, seznamů od hlavních prohledávačů v jiných podsítích a za poskytování seznamů prostředků domény hlavním prohledávačům. Hlavní prohledávač domény je vždy primárním řadičem domény (PDC).

Primární řadič domény dostává prioritu ve volbách prohledávačů, která mu zajišťuje, že se stane hlavním prohledávačem. Prohledávací služba systému Windows, spuštěná na primárním řadiči domény má zvláštní dodatečnou úlohu být hlavní prohledávačem domény.

Pro doménu, která používá protokol TCP/IP a zasahuje do více než jedné podsítě funguje každá podsít jako nezávislá prohledávací entita se svým vlastním hlavním prohledávačem a záložními prohledávači. Přenosy pomocí protokolů NWLink a NBF nepo-

užívají úlohu hlavního prohledávače domény, protože tyto přenosy mají pouze jeden hlavní prohledávač pro celou síť. Prohledávání přes směrovač IP do jiných podsítí vyžaduje alespoň jeden prohledávač se spuštěným systémem Windows 2000, Windows NT, nebo Microsoft® Windows® for Workgroups 3.11b v doméně pro každou podsíť. Primární řadič domény obvykle funguje jako hlavní prohledávač domény ve své podsíti.

Když doména zasahuje do více podsítí, hlavní prohledávač v každé podsíti oznamuje sám sebe jako hlavní prohledávač hlavnímu prohledávači domény použitím směrovaného datagramu, nazvaného oznámení hlavního prohledávače (MasterBrowserAnnouncement). Hlavní prohledávač domény pak posílá vzdálené volání aplikačního programového rozhraní **NetServerEnum** každému hlavnímu prohledávači, aby získal seznam serverů v každé podsíti. Hlavní prohledávač domény spojuje seznamy serverů z každé podsítě se svým vlastním seznamem serverů a vytváří seznam prohledávání pro doménu. Tento proces se opakuje každých 12 minut, aby bylo zajištěno, že hlavní prohledávač domény má úplný seznam prohledávání všech serverů v doméně.

Poznámka: Hlavní prohledávač domény musí být schopen překládat název serveru pro každý hlavní prohledávač v síti TCP/IP (například použitím rozhraní WINS). Každý hlavní prohledávač musí být schopen překládat názvy DOMAIN[1B] a rovněž názvy primárních řadičů domén.

Hlavní prohledávač v každé podsíti rovněž posílá vzdálené volání aplikačního programového rozhraní **NetServerEnum** hlavnímu prohledávači domény, aby dostal úplný seznam prohledávání pro doménu. Tento seznam prohledávání je dostupný klientům prohledávače v podsíti.

Jeden počítač může hrát více rolí v systému prohledávačů. Například hlavní prohledávač by mohl být také hlavním prohledávačem domény.

Poznámka: Pracovní skupiny systému Windows nemohou zasahovat do více podsítí. Každá pracovní skupina, která přesahuje podsíť ve skutečnosti funguje jako dvě oddělené pracovní skupiny se stejnými názvy.

Volby prohledávačů

Volby prohledávačů slouží k výběru nového hlavního prohledávače a nastávají za následujících okolností:

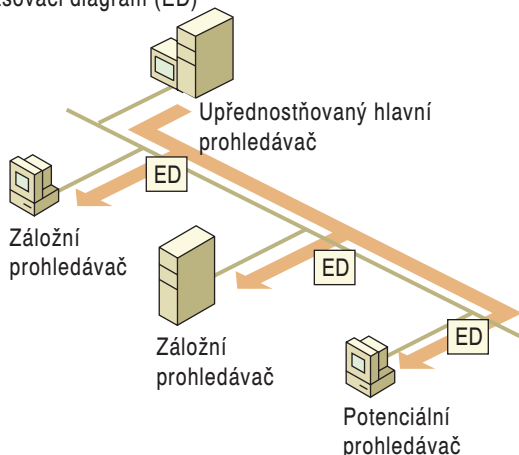
- Když počítač nedokáže nalézt hlavní prohledávač.
- Když se připojí upřednostňovaný hlavní prohledávač.
- Když je spuštěn systém řadiče domény v systému Windows.

Počítač vyvolá volby odesláním zvláštního datagramu, kterému se říká *hlasovací datagram*. Když dojde k volbám, prohledávací služba na počítači, který vyvolal volby, zaznamená událost do systémového protokolu s uvedením, že vyvolal volby. Událost je zapsána pro každý síťový protokol, ve kterém prohledávací služba vyvolá volby.

Všechny prohledávače mohou přijímat hlasovací datagramy. Když prohledávač přijme hlasovací datagram, přezkoumá volební kritéria tohoto datagramu. Pokud má prohledávač lepší volební kritéria než odesílatel hlasovacího datagramu, vydá svůj vlastní hlasovací datagram a vstoupí do stavu probíhajících voleb (election in progress). Pokud

prohledávač nemá lepší volební kritéria než odesílatel hlasovacího datagramu, pokusí se určit, který systém je novým hlavním prohledávačem. Obrázek I.2 ukazuje počítače provádějící volby prohledávače.

Hlasovací diagram (ED)



Obrázek I.2 Volby prohledávače

Volební kritéria pro prohledávač jsou založena na aktuální úloze prohledávače v doméně a jeho aktuálním stavu, přičemž se využívá hierarchie, uvedená v tabulce I.2.

Tabulka I.2 Hierarchie kritérií pro volby prohledávače

Typ operačního systému	Pole voleb Windows
Windows for Workgroups a Windows 95 a Windows 98	0x01000000
Windows 2000 Professional a Windows NT Workstation	0x10000000
Windows 2000 Server a Windows NT Server	0x20000000
Verze voleb	0x00FFFF00
Volební kritéria v rámci verze	0x000000FF
Primární řadič domény (PDC)	0x00000080
Systém WINS	0x00000020
Upřednostňovaný hlavní prohledávač	0x00000008
Spuštěný hlavní prohledávač	0x00000004
Položka registru MaintainServerList = Yes	0x00000002
Spuštěný záložní prohledávač	0x00000001

Prohledávač používá všechna příslušná volební kritéria, aby určil volební kritéria odesílajícího počítače.

Následující kritéria určují, zda prohledávač vyhrál nebo nevyhrál ve volbách:

- Pokud verze voleb prohledávače je vyšší než verze voleb odesílatele, vyhrává prohledávač. Pokud tomu tak není, použije prohledávač další volební kritérium. Verze voleb je konstantní hodnota, která určuje verzi protokolu voleb prohledáva-

če. Verze voleb je číslo revize protokolu prohledávače a nemá vztah k verzi operačního systému.

- Pokud jsou volební kritéria prohledávače větší než volební kritéria odesílatele, vyhraje prohledávač. Pokud tomu tak není, použije prohledávač další volební kritérium.
- Pokud byl prohledávač spuštěn déle než odesílatel, vyhraje prohledávač. Pokud tomu tak není, použije prohledávač další volební kritérium.
- Pokud žádné z výše uvedených kritérií neurčilo vítěze voleb, vyhraje server s prvním názvem v abecedním pořadí (v alfabetském třídění včetně číslic a symbolů). Například server s názvem „A“ se stane hlavním prohledávačem před serverem s názvem „X“.

Když prohledávač přijme hlasovací datagram, udávající, že vyhrává volby, vstoupí do stavu spuštěných voleb (running election). Když je v tomto stavu, vysílá prohledávač po prodlevě volební požadavek. Délka prodlevy závisí na aktuální úloze prohledávače v doméně:

- Hlavní prohledávače a primární řadiče domén čekají 100 mikrosekund (ms).
- Záložní prohledávače a záložní řadiče domén náhodně čekají 200 ms a 600 ms.
- Všechny ostatní prohledávače náhodně čekají mezi 800 ms a 3000 ms.

Tato prodleva je naprogramována, protože prohledávače v systému Windows for Workgroups „ohluchnou“ na několik stovek milisekund po odeslání hlasovacího datagramu. Tato prodleva snižuje počet posílaných hlasovacích datagramů, protože prohledávač, který vyhrává ve volbách by pak mohl přijmout jiný hlasovací datagram, způsobující, že by volby později prohrál. Pokud přimějeme k delší prodlevě počítače, jejichž vítězství ve volbách je méně pravděpodobné, je také méně pravděpodobné, že tyto počítače by posílaly hlasovací datagramy.

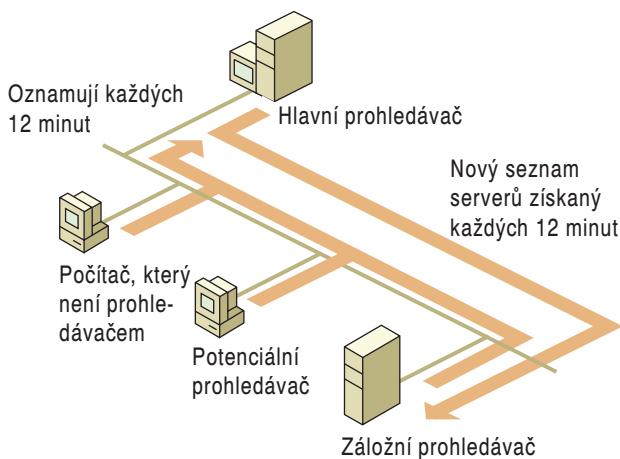
Prohledávač odesílá až čtyři hlasovací datagramy. Pokud žádný jiný prohledávač neodpoví s hlasovacím datagramem, který vyhrává volby, je počítač povýšen na hlavní prohledávač. Pokud prohledávač přijme hlasovací datagram, udávající že ve volbách vyhrál jiný počítač a tento počítač je momentálně hlavním prohledávačem, degraduje se z hlavního prohledávače a stane se záložním prohledávačem.

Oznámení prohledávačů

Prohledávací služba musí být uvědomena prostředkem, když je prostředek k dispozici pro použití v síti. Když je spuštěn počítač se systémy Windows 2000, Windows NT, Windows for Workgroups, Windows 95, nebo Windows 98, posílá oznámení prohledávací službě, aby informoval prohledávač o své dostupnosti. Obrázek I.3 ukazuje přenašení oznámení prohledávačů.

Hlavní prohledávače odpovídají za příjem oznámení a navrácení seznamu záložních prohledávačů počítačům s některým z následujících operačních systémů:

- Windows NT 3.1
- Windows NT Advanced Server 3.1
- Windows for Workgroups
- Windows 95
- Windows 98



Obrázek I.3 Oznámení prohlédávačů

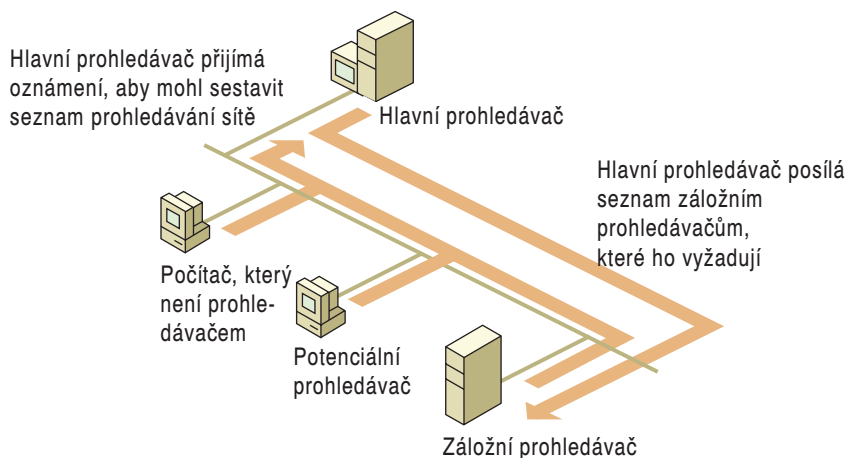
- Windows NT Workstation 3.5 nebo pozdější
- Windows NT Server 3.5 nebo pozdější
- Windows 2000 Professional
- Windows 2000 Server

Když je počítač spuštěn a hodnota položky **MaintainServerList** v jeho registru je nastavena na **Auto**, odpovídá hlavní prohlédávač za sdělení systému, zda se stane nebo nestane záložním prohlédávačem.

Když se počítač stane hlavním prohlédávačem vítězstvím ve volbách a seznam prohlédávání sítě je prázdný, hlavní prohlédávač přinutí všechny systémy, aby odpověděly svým oznámením. Hlavní prohlédávač vyšle všesměrově datagram nazvaný žádost o oznámení (RequestAnnouncement). Všechny počítače, které tento datagram přijmou, musí odpovědět po náhodné prodlevě do 30 sekund. Tento 30sekundový rozsah pro odpověď brání hlavní prohlédávač před zahlcením a ztrátou odpovědí a chrání síť před záplavou odpovědí. Obrázek I.4 ukazuje počítače vyhledávající záložní seznamy.

Hlavní prohlédávač nemůže být přinucen, aby znovu sestavil seznam prohlédávání sítě pro pracovní skupinu nebo doménu. Vypnutí a restartování počítače, který je nastaven jako upřednostňovaný hlavní prohlédávač, nebo zastavení a opětovné spuštění prohlédávací služby však vynutí sestavení nového seznamu prohlédávání sítě. Když je spuštěn upřednostňovaný hlavní prohlédávač, vyvolá volby, které vyhraje. Protože neexistuje seznam prohlédávání sítě, přinutí pak všechny členy domény nebo pracovní skupiny, aby se seznámili.

Pokud hlavní prohlédávač přijme oznámení od jiného počítače, který prohlašuje, že je hlavním prohlédávačem, degraduje hlavní prohlédávač sám sebe z úlohy hlavního prohlédávače a vyvolá volby. Tím je zajištěno, že v každé pracovní skupině nebo doméně je vždy nejvýše jeden hlavní prohlédávač.



Obrázek I.4 Vyhledávání záložních seznamů

Oznámení počítačů, které nejsou prohledávači

Počítač, který není prohledávačem, periodicky oznamuje sám sebe hlavnímu prohledávači odesláním směrovaného datagramu hlavnímu prohledávači v síti. Počítač oznamuje svou dostupnost v intervalech 1 minuty, 2 minut, 4 minut, 8 minut a 12 minut, dále pak oznamuje hlavnímu prohledávači sám sebe každých 12 minut. Pokud hlavní prohledávač nedostane oznámení od počítače ve třech po sobě jdoucích intervalech, vyjme tento počítač ze seznamu prohledávání sítě.

Poznámka: Z tohoto důvodu může trvat až 36 minut než místní hlavní prohledávač vyjme zastaralou položku. Navíc zbytku domény může trvat dalších 12 – 24 minut (dvojnásobek periody hlavního prohledávače), než odhalí odejmutí zastaralé položky.

Oznámení potenciálních prohledávačů

Většina počítačů je potenciálními prohledávači; to znamená, že jsou schopny stát se záložními nebo hlavními prohledávači. Tyto počítače oznamují samy sebe stejným způsobem, jako počítače, které nejsou prohledávači.

Oznámení záložních prohledávačů

Záložní prohledávače oznamují samy sebe stejným způsobem jako počítače, které nejsou prohledávači. Záložní prohledávače se však účastní ve volbách prohledávačů. Záložní prohledávače se připojují k hlavnímu prohledávači každých 12 minut, aby obdržely aktualizovaný seznam prohledávání síťových prostředků a seznamy pracovních skupin a domén. Záložní prohledávač ukládá tyto seznamy do mezipaměti a vrací seznam prohledávání sítě každému klientu, který vyšle prohledávací požadavek na záložní prohledávač voláním aplikačního programového rozhraní NetServerEnum. Pokud záložní prohledávač nedokáže najít hlavní prohledávač, vyvolá volbu.

Nastavení času oznámení prohlédávače

Pro změnu intervalu, ve kterém prohlédávač oznamuje sám sebe přidejte položku registru, nazvanou **Announce** s datovou hodnotou typu REG_DWORD. Nastavte hodnotu položky **Announce** na počet sekund, který má prohlédávač čekat mezi oznámeními. Položku **Announce** přidejte do následujícího podklíče registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
  \lanmanserver\parameters
```

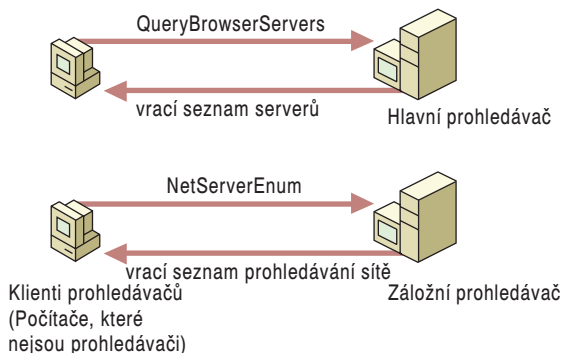
Pokud má například položka **Announce** ve výchozím nastavení hodnotu 720, je interval oznámení 12 minut.

Hodnota položky **Announce** musí být změněna na všech počítačích v pracovní skupině nebo doméně předtím, než může být nová hodnota používána všemi počítači. Když snižujete tuto hodnotu, stoupá oznamovací provoz. Zvýšení hodnoty položky **Announce** snižuje objem oznamovacího provozu, ale prodlužuje dobu, po kterou se nedostupný počítač objevuje na seznamu prohlédávání sítě.

Požadavky prohlédávače

Účelem prohlédávací služby je vytvořit seznam síťových prostředků, dostupných klientovi prohlédávací služby. Aby mohl používat tento seznam, musí klient prohlédávací služby vědět, který počítač má kontaktovat s požadavkem na kopii seznamu.

Obrázek I.5 ukazuje tok požadavků na prohlédávání.



Obrázek I.5 Tok požadavků na prohlédávání

Požadavkem, vydávaným pro získání seznamu dostupných síťových prostředků, je volání aplikačního programového rozhraní **NetServerEnum**. Tento požadavek je odeslán, pokud je v příkazovém řádku spuštěn příkaz **net view** a když je vybráno tlačítko **Procházet** v dialogovém okně **Připojit síťovou jednotku**. Klient posílá volání aplikačního programového rozhraní **NetServerEnum** záložnímu prohlédávači.

Předtím než může klient poprvé poslat volání aplikačního programového rozhraní **NetServerEnum**, musí nejdříve zjistit, které počítače jsou záložními prohlédávači pro jeho pracovní skupinu nebo doménu. Toho klient dosáhne vysláním datagramu s názvem **GetBackupList** hlavnímu prohlédávači.

Hlavní prohlédávač přijme a zpracuje datagram **GetBackupList**. Hlavní prohlédávač vrátí seznam záložních prohlédávačů, aktivních uvnitř dotazované pracovní skupiny nebo domény. Klient vybere názvy tří záložních prohlédávačů ze seznamu a uloží si je pro

budoucí použití. Volání aplikačního programového rozhraní **NetServerEnum** je zasláno náhodně vybranému záložnímu prohledávači z těchto tří uložených názvů.

Pokud není možné nalézt hlavní prohledávač pro pracovní skupinu nebo doménu po třech pokusech, vyvolá klient volbu nového hlavního prohledávače pro doménu. Klient také vrátí zprávu **ERROR_BAD_NETPATH** prohledávající aplikaci, oznamující, že není možné nalézt hlavní prohledávač.

Počet prohledávačů v doméně nebo pracovní skupině

Následující pravidla určují počet prohledávačů v doméně nebo pracovní skupině.

Pokud v doméně aktuálně existuje primární řadič domény (PDC), je hlavním prohledávačem pro tuto doménu.

Každý záložní řadič domény (BDC) v doméně je záložním prohledávačem pro tuto doménu. Jedinou výjimkou je případ, kdy je záložní řadič domény zapotřebí jako hlavní prohledávač, protože primární řadič domény selhal. V takovém případě je záložní řadič domény hlavním prohledávačem pro doménu.

Poznámka: Toto může být problém, protože položka **DOMAIN[1B]**, používaná pro vyhledání hlavního prohledávače domény je aktualizována pouze tehdy, když je povýšen záložní řadič domény.

Pokud je v registru počítače hodnota položky **MaintainServerList** nastavena na **Yes**, je počítač záložním prohledávačem pro doménu nebo podsít TCP/IP.

Pokud nejsou vybrány žádné záložní prohledávače pro doménu na základě předchozích pravidel, určuje hlavní prohledávač počet záložních prohledávačů pro doménu. Hlavní prohledávač vybere některé z počítačů s hodnotou položky registru **MaintainServerList** nastavenou na **Auto**, aby vystupovaly jako záložní prohledávače.

Tabulka I.3 ukazuje počet záložních prohledávačů, které jsou vybrány podle počtu počítačů v doméně.

Tabulka I.3 Počet prohledávačů v doméně nebo pracovní skupině

Počet počítačů	Počet záložních prohledávačů	Počet hlavních prohledávačů
1	0	1
2 až 31	1	1
32 až 63	2	1

Pro každých dalších 32 počítačů, přidaných do domény je pro doménu vybrán další záložní prohledávač.

V síti TCP/IP network, vynucuje každá podsít předchozí pravidla nezávisle.

Vypnutí nebo selhání prohledávače

Pokud je záložní prohledávač řádně vypnut, posílá oznámení hlavnímu prohledávači, že je vypínán. Záložní prohledávač provede odesláním oznámení, které neobsahuje službu prohledávače v seznamu spuštěných služeb.

Pokud je řádně vypnut hlavní prohlédávač, vyšle datagram ForceElection (vyvolání voleb), takže bude zvolen nový hlavní prohlédávač.

Když není počítač správně vypnut nebo když z nějakého důvodu selže, musí být odstraněn ze seznamu prohlédávání sítě. Služba prohlédávače spravuje selhání prohlédávačů.

Selhání počítače, který není prohlédávačem

Když selže počítač, který není prohlédávačem, přestane sám sebe oznamovat. Nastavený interval oznámení je mezi 1 a 12 minutami. Když počítač, který není prohlédávačem, neoznámí sám sebe po třech intervalech oznámení, odstraní hlavní prohlédávač tento počítač ze seznamu prohlédávání sítě. Proto může trvat až 72 minut než se všechny prohlédávače dozvědí o selhání počítače, který není prohlédávačem. Tato potenciální prodleva zahrnuje až 36 minut pro zjištění chyby hlavním prohlédávačem a 12 minut pro všechny záložní servery pro vyhledání aktualizovaného seznamu z hlavního prohlédávače.

Selhání záložního prohlédávače

Jako u selhání počítače, který není prohlédávačem může při selhání záložního prohlédávače tento počítač zůstat v seznamu hlavního prohlédávače dalších až 72 minut. Pokud nemůže být získán seznam prohlédávání sítě ze scházejícího záložního prohlédávače, zvolí klient jiný záložní prohlédávač ze svého seznamu tří záložních prohlédávačů, který udržuje v mezipaměti. Pokud všechny záložní prohlédávače známé klientovi selžou, pokusí se klient získat nový seznam záložních prohlédávačů od hlavního prohlédávače. Pokud klient není schopen kontaktovat hlavní prohlédávač, vyvolá volby.

Selhání hlavního prohlédávače

Když selže hlavní prohlédávač, záložní prohlédávač zjistí selhání do 12 minut a vyvolá volby nového hlavního prohlédávače.

Pokud klient provede svůj požadavek na prohlédávání (voláním aplikačního programového rozhraní NetServerEnum) poté, co selže hlavní prohlédávač a předtím, než záložní prohlédávač zjistí selhání, vyvolá klient volby. Pokud selže hlavní prohlédávač a neexistují záložní prohlédávače, prohlédávání v pracovní skupině nebo doméně nefunguje správně.

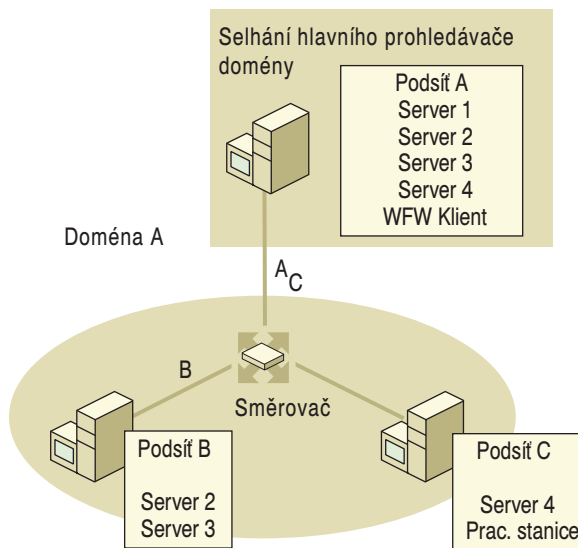
V mezeře mezi selháním hlavního prohlédávače a volbou nového hlavního prohlédávače může pracovní skupina nebo doména zmizet ze seznamů, které jsou viditelné pro počítače v jiných pracovních skupinách nebo doménách.

Selhání hlavního prohlédávače domény

Když selže hlavní prohlédávač domény, hlavní prohlédávač pro každou podsít v síti poskytuje seznam prohlédávání sítě, který obsahuje pouze servery z místní podsítě. Všechny servery, které nejsou v místní podsíti sítě jsou případně odstraněny ze seznamu prohlédávání sítě. I poté, co jsou tyto servery odstraněny, mohou mít stále uživatelskou možnost se připojovat k serverům v jiných podsítích sítě, pokud znají název takového serveru.

Protože hlavní prohlédávač domény je také primárním řadičem domény, může správce opravit toto selhání zvýšením záložního řadiče domény na primární řadič domény;

toto způsobí, že záznam DOMAIN[IB] bude aktualizován ve službě WINS. Záložní řadič domény může provádět většinu úkolů primárního řadiče domény, jako je ověřování požadavků na přihlášení, ale nepovyšuje se sám na primární řadič domény a nestává se hlavním prohledávačem domény v případě selhání primárního řadiče domény. Obrázek I.6 ukazuje události při selhání hlavního prohledávače.



Obrázek I.6 Selhání hlavního prohledávače

Prohledávací služba přes více pracovních skupin a domén

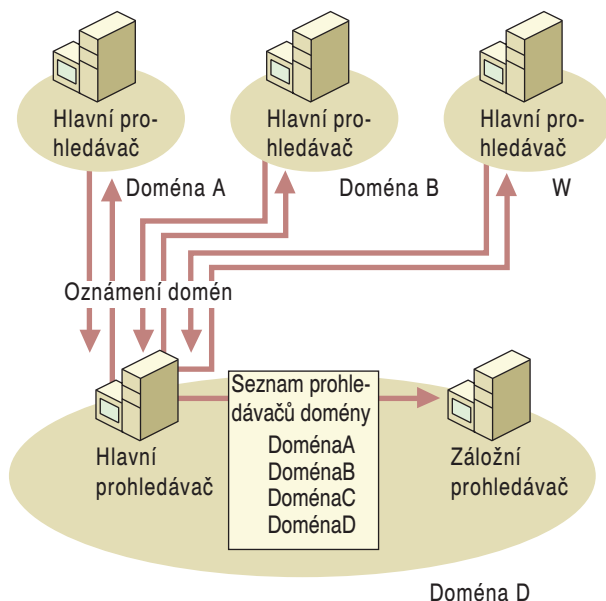
Uživatelé musí prohledávat více pracovních skupin a domén, aby vyhledali seznam serverů uvnitř své skupiny nebo domény a seznam dalších pracovních skupin a domén.

Obrázek I.7 ukazuje prohledávací službu přes více pracovních skupin a domén.

Poté co se stane hlavním prohledávačem, každý hlavní prohledávač v každé pracovní skupině a doméně vysílá datagram oznámení domény (DomainAnnouncement) každou minutu po prvních pět minut. Po prvních pěti minutách posílá hlavní prohledávač datagram DomainAnnouncement jednou za každých 12 minut. Jestliže se pracovní skupina nebo doména neohlásí ve třech oznamovacích intervalech, je taková pracovní skupina nebo doména odstraněna ze seznamu pracovních skupin a domén. Proto je možné, že pracovní skupina nebo doména se objevuje v seznamu prohledávání 45 minut poté, co pracovní skupina nebo doména selhala nebo byla vypnuta.

Datagram DomainAnnouncement obsahuje následující informace.

- Název domény
- Název hlavního prohledávače pro tuto doménu, což může (ale nemusí) být primární řadič domény.
- Verze operačního softwaru



Obrázek I.7 Prohledávací služba přes více pracovních skupin a domén

Pokud je na prohledávacím počítači spuštěn systém Windows 2000 Server nebo Windows NT Server, datagram DomainAnnouncement také udává, zda prohledávací počítač je nebo není primárním řadičem domény.

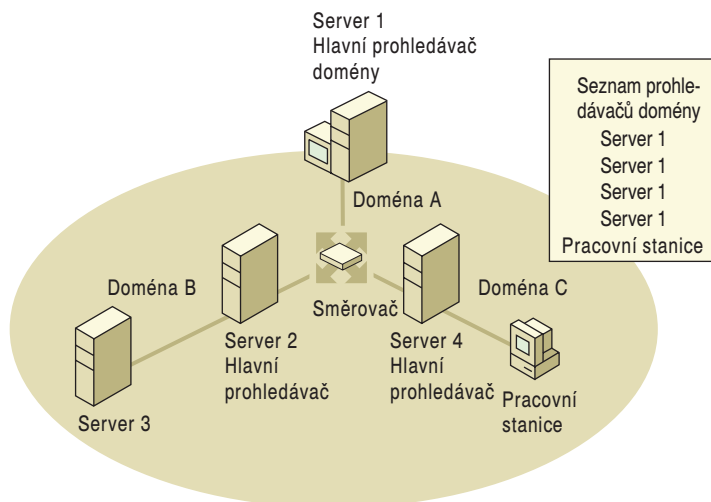
Prohledávací služba přes směrovač IP

Při používání domén, které jsou rozděleny přes směrovače, funguje každá podsíť sítě TCP/IP jako nezávislá prohledávací entita se svým vlastním hlavním prohledávačem a záložními prohledávači. Proto se odehrávají volby prohledávačů v každé podsíti sítě. Hlavní prohledávače domén odpovídají za sdružování podsítí sítě pro sběr informací o názvech počítačů a udržování celodoménového seznamu prohledávání dostupných prostředků sítě. Hlavní prohledávač domény a spolupracující hlavní prohledávače v každé podsíti zajišťují prohledávání domén, které existují napříč více podsítěmi sítě TCP/IP. Hlavní prohledávač domény je primární řadič domény. Počítače, které jsou hlavními prohledávači v podsítích mohou mít spuštěn systém Windows 2000, Windows NT, Windows for Workgroups verze 3.11b, Windows 95 nebo Windows 98.

Obrázek I.8 ukazuje prohledávací službu přes směrovač IP.

Když doména zahrnuje více podsítí sítě, hlavní prohledávač každé podsítě v síti používá směrovaný datagram s názvem MasterBrowserAnnouncement (oznámení hlavního prohledávače), aby oznámil sám sebe hlavnímu prohledávači domény. Datagram MasterBrowserAnnouncement uvědomuje hlavní prohledávač domény, že vysílající počítač je hlavním prohledávačem ve stejné doméně a že hlavní prohledávač domény potřebuje kopii seznamu prohledávání tohoto hlavního prohledávače. Když dostane hlavní prohledávač domény datagram MasterBrowserAnnouncement, vrátí oznamujícímu hlavnímu prohledávači požadavek na seznam serverů v podsíti hlavního prohledávače.

Hlavní prohledávač domény pak spojuje svůj vlastní seznam serverů se seznamem serverů z hlavního prohledávače, který vydal oznámení.



Obrázek I.8 Prohledávací služba přes směrovač IP

Tento proces se opakuje každých 15 minut a zaručuje, že hlavní prohledávač domény má úplný prohledávací seznam všech serverů v doméně. Když vydá klient prohledávací požadavek záložnímu prohledávači, záložní prohledávač vrátí seznam všech serverů v doméně, bez ohledu na podsítě, ve které jsou umístěny.

Překlad názvů

Překlad názvů je u distribuovaného prohledávání rozhodující pro jeho správnou činnost.

Všechny počítače, které mají schopnost stát se hlavními prohledávači v propojených sítích IP musí být schopné přeložit položku `DomainName<1b>` pro hlavní prohledávač domény. Po přijetí pozitivní odpovědi na datagram `Query for Primary DC` (dotaz na primární řadič domény) musí být hlavní prohledávače rovněž schopny překládat název `ComputerName<00>` hlavního prohledávače domény. Aby se hlavní prohledávač domény mohl spojit s každým hlavním prohledávačem, musí být schopen překládat názvy všech serverů, které se mohou potenciálně stát hlavními prohledávači. Hlavní prohledávač domény naslouchá směrovaným datagramům `MasterBrowserAnnouncement`, odeslaným hlavními prohledávači přes port UDP 138. Tato oznámení způsobují, že hlavní prohledávač domény překládá název počítače `ComputerName<00>` hlavního prohledávače a vyžádá od hlavního prohledávače jeho místně shromážděný seznam prohledávání sítě.

Je také důležité pochopit, že když je seznam prohledávání sítě předložen klientovi, klient musí přeložit název `ComputerName<20>` každého serveru v seznamu, aby viděl jeho sdílené prostředky. Proto všichni klienti v doméně musí být schopni překládat adresy IP každého serveru v doméně. Pro většinu sítí to znamená, že musí správně pracovat distribuovaná infrastruktura služby WINS nebo DNS.

Informace o překladu názvů prostřednictvím služeb WINS nebo DNS nebo souboru LMHOSTS najdete v části „Windows Internet Name Service“ v této knize.

Prohledávací služba přes směrovač IP s protokolem TCP/IP

Komunikace prohledávací služby aktuálně spoléhá téměř zcela na všesměrová vysílání. V propojených sítích IP, kde jsou domény odděleny směrovači, mohou nastat různé problémy při všesměrovém vysílání, protože všesměrové vysílání neprochází automaticky přes směrovače. V úvahu je třeba vzít dva problémy:

- Jak mohou provádět prohledávací funkce prohledávače, oddělené směrovačem
- Jak mohou místní klienti prohledávat vzdálené domény, které nejsou v jejich místní podsíti

Následující témata diskutují tři metody, které můžete použít pro nastavení prohledávání v propojených sítích IP s protokolem TCP/IP. Jsou uvedeny v pořadí podle přednosti.

Systém Domain Name System

Systém Windows 2000 používá systém DNS jako svou primární metodu překladu názvů. Každý řadič domény založený na systému Windows 2000 registruje při spuštění dva názvy: doménový název DNS u služby DNS a název pro NetBIOS u služby WINS nebo jiné transportní služby.

Když vytvářející počítač a cílový počítač jsou nastaveny pro používání adres IP a služby DNS, je název přeložen použitím DNS; jinak služba WINS překládá adresy IP z názvů pro NetBIOS, takže mohou být datagramy zasílány cílovému počítači. Překlad názvů nemusí pracovat správně, pokud se používá pouze služba DNS, kvůli omezením překladu názvů pro NetBIOS prostřednictvím DNS. Je doporučeno používat kromě služby DNS i služby WINS.

Více informací o pojetí systému DNS najdete v části „Úvod do systému DNS“ v této knize.

Služba Windows Internet Name Service

Služba Windows Internet Name Service (WINS) překládá adresy IP z názvů pro NetBIOS, takže mohou být datagramy posílány cílovému počítači. Implementace služby WINS odstraňuje potřebu nastavovat soubor LMHOSTS nebo povolovat port UDP 137. Použití služby WINS vyžaduje následující konfiguraci:

- Služba WINS je nastavena na počítači se spuštěným systémem Windows 2000 Server, Windows NT Server 3.5 nebo pozdější.
- Klienti umožňují službu WINS.

Klienty služby WINS mohou být počítače se systémy Windows 2000, Windows NT 3.5 nebo pozdější, Windows 95, Windows 98, Windows for Workgroups 3.11b se spuštěnou službou TCP/IP-32, Microsoft® LAN Manager 2.2c for MS-DOS nebo Microsoft Network Client 3.0 for MS-DOS. Poslední dva systémy jsou poskytnuty na instalačních discích pro Windows NT Server verze 3.5 nebo pozdější.

Doporučuje se implementovat službu WINS pro překlad názvů a podporu prohledávání. Jako alternativa je možné mít úplné prohledávání domény pouze použitím souborů LMHOSTS na všech počítačích, to ale omezuje prohledávání pouze na místní doménu. Klienti, kteří nepoužívají službu WINS přesto potřebují soubor LMHOSTS pro prohledávání propojených sítí IP i když byla v doméně implementována služba WINS.

Poznámka: Klient se bude podílet na prohledávání domény pouze když tento klient používá název pracovní skupiny, který je ekvivalentem názvu domény.

Soubor LMHOSTS

Překlad názvů pro NetBIOS je obvykle proveden všesměrovým vysíláním, které překládá pouze názvy v místní podsíti. Pro překlad názvů počítačů, umístěných v jiné podsíti, musí být nastaven soubor LMHOSTS (uložený v adresáři %Systemroot%\System32\drivers\etc). Soubor LMHOSTS musí obsahovat mapování názvů pro NetBIOS na adresy IP pro všechny počítače, které nejsou v místní podsíti sítě.

Pro implementaci komunikace mezi podsítěmi sítě a hlavním prohledávačem domény musí správce sítě nastavit soubor LMHOSTS s názvy pro NetBIOS a adresami IP pro všechny prohledávače. Pro zajištění toho, že hlavní prohledávač pro každou podsít' bude mít přístup k primárnímu řadiči domény, musí mít primární řadič pro každou doménu položku v souboru LMHOSTS v každém hlavním prohledávači. Každá položka musí rovněž mít značku #DOM, která označuje pojmenovaný počítač jako řadič domény.

Soubor LMHOSTS v hlavním prohledávači každé podsítě musí obsahovat následující informace:

- Adresu IP a název pro NetBIOS každého hlavního prohledávače domény
- Název domény, předcházený značkami #PRE a #DOM jako v následujícím příkladu:

```
130.20.7.80 <název_prohledávače> #PRE #DOM:<název_domény >
```

Aby bylo zaručeno, že primární řadič domény může požadovat místní seznam prohledávání sítě od hlavního prohledávače podsítě, musí protokol TCP/IP ukládat adresu klienta do mezipaměti.

Všesměrová vysílání názvové služby pro NetBIOS

Ne všechny směrovače blokují všechny typy provozu všesměrového vysílání. Některé směrovače mohou být nastaveny, aby předávaly určité typy všesměrového vysílání.

Všechna všesměrová vysílání systému NetBIOS pro TCP/IP (NetBT) jsou odesílána na port UDP číslo 137, který je definován jako port pro názvovou službu NetBT. Směrovače normálně blokují předávání těchto rámců, protože jsou posílány na hardwarovou adresu všesměrového vysílání a adresu všesměrového vysílání podsítě. Některé směrovače však umožňují, aby všechny rámce všesměrového vysílání, odeslané na tento konkrétní port UDP – který je používán pouze rozhraním NetBT – byly předávány. Jako důsledek pro prohledávač to vypadá, jako by byl v jednom velkém segmentu sítě. Všechny domény a pracovní skupiny ve všech segmentech sítě jsou vidět všemi počítači.

Poznámka: Toto může být problematické, protože zpoždění na směrovači nebo další problémy s připojením mohou způsobit, že je zvoleno nesprávné množství prohledávačů (žádný nebo dva nebo více). Podpora společnosti Microsoft doporučuje, aby zákazníci nepovolovali předávání všesměrových paketů pro port UDP číslo 137 a port UDP číslo 138.

Počítače se systémy Windows for Workgroups, Windows 95 a Windows 98 jako hlavní prohlédávače

Soubory Vserver.386 a Vredir.386 na instalačních CD systémů Windows NT Server verze 3.51 a 4.0 se liší od souborů se stejnými názvy na instalačním CD systému Windows NT Server verze 3.5.

V systému Windows 2000 byly tyto dva soubory změněny, takže počítače se systémy Windows for Workgroups 3.11b, Windows 95 nebo Windows 98 mohou být hlavními prohlédávači pro síť. Tato modifikace umožňuje počítači v síti s počítači s jedním z těchto tří operačních systémů prohlédávat domény systémů Windows 2000 a Windows NT v jiných sítích.

Jako hlavní prohlédávač pro síť komunikuje počítač se systémem Windows for Workgroups 3.11b, Windows 95, nebo Windows 98 s primárním řadičem domény, aby dostal seznam prohlédávání sítě pro celou doménu.

Hlavní prohlédávač na počítači se systémem Windows for Workgroups 3.11b, Windows 95, nebo Windows 98 funguje, jako kdyby byl hlavním prohlédávačem se spuštěným systémem Windows 2000. Kontaktuje primární řadič domény každých 15 minut, aby mu předal seznam prohlédávání místní sítě a dostal celodoménový seznam prohlédávání sítě.

Aby počítač se spuštěným systémem Windows for Workgroups 3.11b, Windows 95 nebo Windows 98 mohl být hlavním prohlédávačem, musí být jak tento počítač, tak primární řadič domény klienty služby WINS. Hlavní prohlédávač musí rovněž vyhovovat následujícím podmínkám:

- Používat protokol TCP/IP
- Používat službu WINS pro překlad názvů
- Být v pracovní skupině, která má stejný název jako doména

Registrace a šíření

Prohlédávací služba spoléhá na všesměrová vysílání serverů bez spojení pro oznámení hostitelských počítačů, která jsou již z definice nespolehlivá. Když je server spuštěn, okamžitě odesílá datagram oznámení hostitelského počítače. Datagramy oznámení hostitelských počítačů jsou pak opět přenášeny po čtyřech a po osmi minutách. Oznamovací perioda se pak stabilizuje a datagram je vyslán ve výchozím nastavení každých 12 minut.

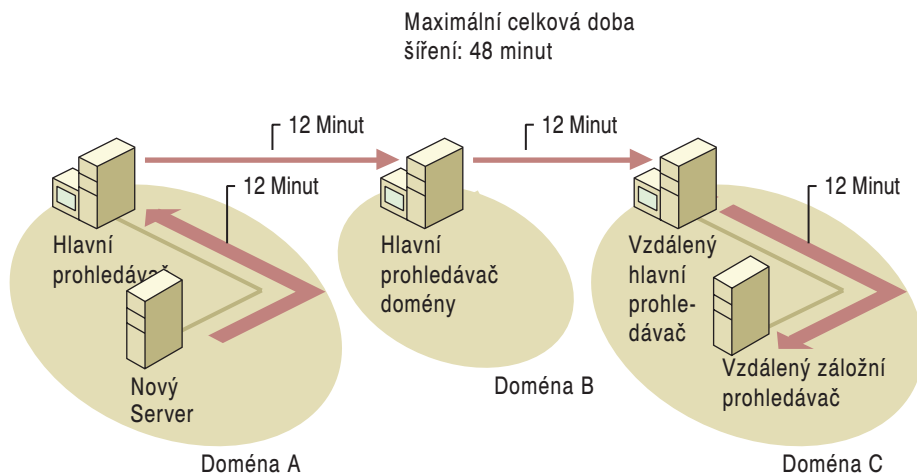
Počítaje se ztrátou několika datagramů je rozumné očekávat, že server vystupující jako hlavní prohlédávač přidá nový server do svého seznamu do 12 minut po spuštění nového serveru.

Poznámka: Po počátečním vysílání oznámení a oznámení hostitelského počítače jsou cestou relací přeneseny nové položky do seznamu prohlédávání hlavního prohlédávače domény a nové položky z hlavního prohlédávače domény do hlavních prohlédávačů. Relace jsou orientované na spojení a jsou tudíž deterministické a spolehlivější.

Do dalších 12 minut se hlavní prohlédávač spojí s hlavním prohlédávačem domény, aby získal celodoménový seznam a zároveň se hlavní prohlédávač domény spojí s hlavním prohlédávačem a zjistí nový server. Hlavní prohlédávače ve vzdálených podsítích

se připojují k hlavnímu prohledávači domény ve 12minutových intervalech a brzy zjistí nový server. Do 12 minut od okamžiku, kdy vzdálený hlavní prohledávač zjistí nový server, se všechny záložní prohledávače připojí ke svému hlavnímu prohledávači a zjistí nový server. V prostředí s více podsítěmi tedy maximální doba, kterou trvá všem klientům v doméně zjištění nového serveru, je 72 minut. V plně funkční síti, kde bezpečně funguje všesměrové vysílání a používání sítě, může být tato doba přibližně poloviční.

Obrázek I.9 ukazuje šíření oznámení hostitelského počítače.



Obrázek I.9 Šíření oznámení hostitelského počítače

Odstraňování počítačů ze seznamů prohledávání může trvat déle. Hlavní prohledávač neodstraní server ze seznamu, dokud neuplynou tři oznamovací periody, aby toleroval ztracené datagramy. Pokud nebyl server řádně vypnut nebo pokud došlo ke ztrátě síťového spojení, zůstává server v seznamu hlavního prohledávače po dobu až 36 minut. Po tomto čase hlavní prohledávač domény je uvědomen, aby odstranil název serveru ze svého seznamu. Během dalších 12 minut obdrží hlavní prohledávač ve vzdálené podsíti celodoménový seznam od hlavního prohledávače domény a během dalších 12 minut je uvědomen každý záložní prohledávač ve vzdálené podsíti, aby odstranil název serveru ze svého seznamu. Odstraňování počítače ze seznamu prohledávání může trvat až 72 minut do doby, než je dokončeno. Pokud je server správně vypnut, výše prohledávač jednu zprávu HostAnnouncement, která udává, že již nadále nevystupuje jako server. Okamžitě po příjmu tohoto datagramu hlavní prohledávač odstraní server ze svého místního seznamu. Ve zdravé síti, kde dobře funguje všesměrové vysílání, může odstranění názvu serveru trvat méně než polovinu výše uvedené doby.

Serverové role prohledávače nejsou definovány staticky, jak je tomu u služeb WINS nebo DNS, ale jsou definovány dynamicky s periodickými volbami. Výsledkem je, že určení komunikačního toku, používaného servery pro poskytnutí seznamu prohledávání určitému klientovi může být značně složité. Distribuovaný návrh prohledávací služby spoleská na servery, které zůstávají v síti aktivní a tudíž udržují své prohledávací role v síti stále.

Pokud je hlavní prohledávač správně vypnut, vyvolá volby nového hlavního prohledávače a ten je stanoven okamžitě. Nejrychlejší změna nastane, když volby vyhraje záložní prohledávač, který již má zcela obydlý seznam prohledávání.

Pokud server, který vystupuje jako hlavní prohledávač v podsíti, nebyl správně vypnut, popřípadě když byl ztracen datagram ForceElection pro vyvolání voleb, může dojít k prodávě několika minut, než je v podsíti opět aktivní služba prohledávání. Pokud klient nedokáže najít hlavní prohledávač vydáním datagramu GetBackupListRequest, vyvolá volby. Pokud žádný klient nepožaduje seznam prohledávání, může trvat až 12 minut, než záložní prohledávač zjistí, že neexistuje hlavní prohledávač. Když k tomu dojde, vyvolá volby a do 12 minut je prohledávání opět umožněno.

Testovací techniky

Zatímco neexistuje centralizovaná metoda pro určení, zda seznamy prohledávání sítě se všemi servery v síti IP jsou úplné, existují testovací techniky pro určení, zda servery v konkrétní podsíti jsou zastoupeny v seznamu prohledávání ve vzdálené podsíti. Tyto testy mohou být použity u všech podsítí v propojené síti. Výsledky těchto testů se mohou měnit kvůli změnám úloh serverů při volbách prohledávačů. Pouze pokud všechny servery v doméně zůstávají zcela statické po dobu testů, mohou si výsledky zachovávat význam.

Upozornění: Testy zde popsané spoléhají na nástroj příkazového řádku Browstat.exe. Více informací o nástroji Browstat.exe najdete v nápovědě k podpůrným nástrojům systému Windows 2000. Více informací o instalaci a používání podpůrných nástrojů systému Windows 2000 a o instalaci nápovědy pro podpůrné nástroje najdete v souboru Sreadme.doc v adresáři \Support\Tools na CD s operačním systémem Windows 2000.

Výstup v následujících příkladech je pouze pro síť TCP/IP. Jako u diagnózy většiny síťových problémů, také při odstraňování potíží ve službě prohledávání musí mít správce úplnou znalost o hranicích podsítí a nastavení směrovačů v síti.

Překlad názvů mezi všemi prohledávači je rozhodující. Překlad názvů (užitím služby WINS, DNS nebo souborů LMHOSTS) musí v síti správně fungovat, aby správně fungovalo prohledávání. Můžete ztratit značné množství času při pokusech vystopovat potíže prohledávačů, které jsou ve skutečnosti způsobeny špatným překladem názvů. Informace o překladu názvů pomocí služby WINS a souborů LMHOSTS najdete v části „Služba Windows Internet Name Service“ v této knize. Informace o překladu názvů pomocí systému DNS najdete v části „Služba Windows 2000 DNS“ v této knize.

Z důvodu časové citlivosti prohledávací služby počkejte 48 minut po spuštění testového serveru před prováděním následujících testů.

Sledování prohledávačů

Hlavní a záložní prohledávače v rámci pracovní skupiny nebo domény můžete sledovat pomocí nástroje Browstat.exe. Kromě sběru informací o fungování prohledávače umožňuje nástroj Browstat.exe vyvolat volby a přinutit hlavní prohledávač k ukončení činnosti, takže nastanou volby. Spuštění programu Browstat.exe z příkazového řádku zobrazí seznam možností.

Obrázek I.10 ukazuje možnosti příkazu Browstat.exe.

```

Příkazový řádek
Microsoft Windows 2000 [Verze 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

E:\>browstat
Usage: BROWSTAT Command [Options ! /HELP]
Where <Command> is one of:

ELECT      < EL> - Force election on remote domain
GETBLIST   < GB> - Get backup list for domain
GETMASTER < GM> - Get remote Master Browser name (using NetBIOS)
GETPDC     < GP> - Get PDC name (using NetBIOS)
LISTWFW    < WF> - List WFW servers that are actually running browser
STATUS     < ST> - Dump browser statistics
TICKLE     < TI> - Display status about a domain
UIEW       < UW> - Remote NetServerEnum to a server or domain on transport
DUMPNET    < DN> - Display the list of transports bound to browser

In server <or domain> list displays, the following flags are used:
W=Workstation, S=Server, SQL=SQLServer, PDC=PrimaryDomainController,
BDC=BackupDomainController, TS=TimeSource, AFP=APPServer, NU=Novell,
MBC=MemberServer, PQ=PrintServer, DL=DialinServer, XN=Xenix,
NT=Windows NT, WFW=WindowsForWorkgroups, MFPM=MS Netware,
SS=StandardServer, PBR=PotentialBrowser, BBR=BackupBrowser,
MBR=MasterBrowser, OSP=OSPServer, UMS=UMSServer, W95=Windows95,
DFS=DistributedFileSystem, CLUS=NTCluster, DCE=IBM DSS

E:\>_

```

Obrázek I.10 seznam možností příkazu Browstat.exe

Vystopování problému

Nejčastějším problémem u prohledávací služby je neprovádění replikace názvů serverů v seznamech prohledávání po síti. Následující příklad předpokládá, že klient v jedné podsíti nevidí server, umístěný v jiné podsíti, ve svém seznamu prohledávání. Provedením posloupnosti příkazů popsané v následujících krocích můžete určit, ve kterém bodu přestal server, scházející v seznamu prohledávání, provádět replikaci názvu. Přitom je důležité, abyste rozuměli architektuře své sítě, abyste mohli provést správnou analýzu.

Pro dosažení nejlepších výsledků spusťte následující testovací procedury ve směru šíření, počínaje podsítí, kde je umístěn pohřešovaný server a pokračujte dále k podsíti, kde se nachází klient, který nemůže pohřešovaný server nalézt.

Poznámka: Pokud vám některý z těchto kroků zabraňuje v pokračování dalším krokem, ověřte, zda žádný z prohledávacích serverů, které jste objevili, nemá chybu konfliktu názvů. Pro určení, zda došlo k chybě konfliktu názvů můžete spustit následující příkaz:

nbtstat -n

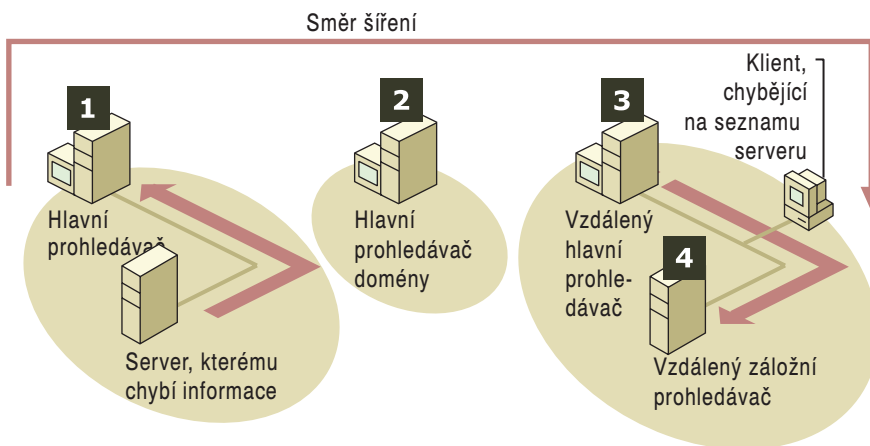
Pokud došlo ke konfliktu názvů, nástroj Nbtstat jej uvede ve sloupci Stav. Pokud název DomainName <ld> nebo <le> způsobuje konflikt, ukončete a znovu spusťte prohledávací službu na příslušném počítači.

Tento příkaz může být spuštěn vzdáleně použitím možnosti -a v příkazovém řádku.

Ilustrační příklady, zahrnuté v následujících procedurách používají zástupné symboly pro různé části příkazů, které musíte použít. Tabulka I.4 popisuje tyto zástupné symboly.

Tabulka I.4 Popis zástupných symbolů v ilustračních příkladech

Zástupné symboly	Popis
<název domény>	Název domény
<protokol>	Identifikuje přenosový protokol. Formát: netbt_tcpip
<ID síťového adaptéru>	Jedinečný identifikátor pro síťový adaptér počítače Formát: nn-nn-nn-nn-nn-nn kde n zastupuje hexadecimální číslo
<hlavní prohlédávač>	Název hlavního prohlédávače
<záložní prohlédávač>	Název záložního prohlédávače
<DMB>	Název hlavního prohlédávače domény. Protože funkčnost hlavního prohlédávače tkví v primárním řadiči domény (PDC), bývá hlavní prohlédávač domény běžně označován jako PDC.
<pohřešovaný server>	Server, který schází v seznamu prohlédávání

**Obrázek I.11 Směr šíření**

Následující příkaz vám umožňuje určit, který server vystupuje jako hlavní prohlédávač v podsíti, kde sídlí pohřešovaný server.

- **Pro nalezení hlavního prohlédávače v podsíti, kde sídlí pohřešovaný server**
 - v příkazovém řádku v podsíti, kde sídlí pohřešovaný server spusťte příkaz **browstat status**

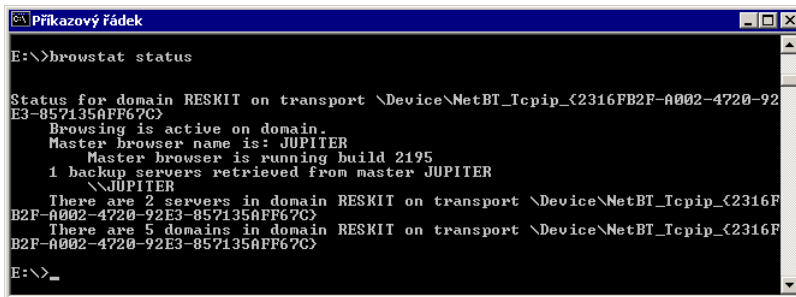
Spuštění tohoto příkazu vám sdělí, který server vystupuje jako hlavní prohlédávač v podsíti, ale pokud místní hlavní prohlédávač reaguje pomalu, můžete tuto informaci dostat od hlavního prohlédávače domény.

Poznámka: Výsledek tohoto příkazu vám udává řetězec s adresou \Device\<Protokol>_<ID síťového adaptéru> rozhraní počítače, kde je příkaz spuštěn. Tento řetězec s adresou pak může být použit u dalších příkazů nástroje Browstat.exe.

- **Pro určení, který server vystupuje jako hlavní prohlédávač v podsíti**

- v příkazovém řádku v podsíti, kde sídlí pohřešovaný server spusťte příkaz **browstat status**.

Nástroj **Browstat.exe** vrací informace, podobné příkladu na obrázku I.12.



```
Příkazový řádek
E:\>browstat status

Status for domain RESKIT on transport \Device\NetBT_Tcpip_{2316FB2F-A002-4720-92E3-857135AFF67C}
  Browsing is active on domain.
  Master browser name is: JUPITER
  Master browser is running build 2195
  1 backup servers retrieved from master JUPITER
  \\JUPITER
  There are 2 servers in domain RESKIT on transport \Device\NetBT_Tcpip_{2316FB2F-A002-4720-92E3-857135AFF67C}
  There are 5 domains in domain RESKIT on transport \Device\NetBT_Tcpip_{2316FB2F-A002-4720-92E3-857135AFF67C}
E:\>_
```

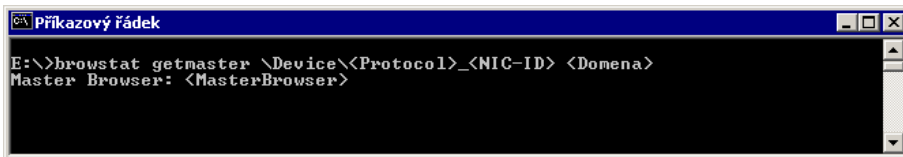
Obrázek I.12 Výsledky spuštění nástroje **Browstat.exe**

Zatímco přepínač příkazového řádku **status** způsobí, že nástroj **Browstat.exe** spustí místní dotaz na název DomainName[1D] i vzdálený dotaz na název DomainName[1B] pro hlavní prohledávač domény, přepínač **getmaster** vydá pouze dotaz na název DomainName[1D] a vrátí aktuální hlavní prohledávač pro tuto podsít.

► **Pro dotaz na hlavní prohledávač pouze v místní podsíti**

- v příkazovém řádku v podsíti, kde sídlí pohřešovaný server spusťte následující příkaz:
browstat getmaster \device\<protokol>_<ID síťového adaptéru> <název domény>

Nástroj **Browstat.exe** vrací informace, podobné příkladu na obrázku I.13.



```
Příkazový řádek
E:\>browstat getmaster \Device\<Protocol>_<NIC-ID> <Domena>
Master Browser: <MasterBrowser>
```

Obrázek I.13 Vyhledání aktuálního hlavního prohledávače

Použití přepínače **getmaster** poskytuje nejpresnější výsledky při určování hlavního prohledávače, protože tato metoda vydává požadavek pouze pro místní podsít.

Tento krok může být proveden také vzdáleně použitím samotné prohledávací služby, aby vám sdělila které počítače vystupují jako hlavní prohledávač v podsíti, ale to vyžaduje, aby správce sítě znal názvy všech serverů v každé podsíti a aby distribuovaná služba prohledávání pracovala správně.

► **Pro vzdálené určení seznamu hlavních prohledávačů v doméně**

- v příkazovém řádku spusťte následující příkaz:
browstat view \device\<protokol>_<ID síťového adaptéru> \\<DMB> | findstr /i mbr

Nástroj Browstat.exe vrací informace, podobné příkladu na obrázku I.14.

```

E:\>browstat view \Device\<Protocol>\_<NIC-ID> \\\DMB\findstr /i mbr

\\<MasterBrowser1> NT 04.00 <W.S.NT.PBR.BBR.MBR>
\\<MasterBrowser2> NT 05.00 <W.S.NT.SS.MBR>
\\<MasterBrowser3> NT 04.00 <W.S.NT.SS.PBR.MBR>
\\<MasterBrowser4> NT 05.00 <W.S.NT.PBR.BBR.MBR>
\\<MasterBrowser5> NT 04.00 <W.S.PQ.NT.PBR.MBR>
  
```

Obrázek I.14 Vyhledání hlavních prohlédávačů v doméně

Výhodou této metody je, že tento příkaz můžete vydat vzdáleně. Výsledky však mohou být rozporuplné, protože tento test používá samotnou prohlédávací službu k řešení problémů s prohlédávačem. Navíc i v případě, že tato část prohlédávací služby nemá potíže, může být vrácený seznam starý až 36 minut.

Protože tato vzdálená metoda poskytuje úplný seznam hlavních prohlédávačů, potřebujete určit, který hlavní prohlédávač je v podsíti, obsahující pohřešovaný název serveru.

Pokud hlavní prohlédávač v podsíti pohřešovaného serveru nemůže být nalezen, můžete vyvolat volby zastavením a spuštěním prohlédávací služby na řadiči domény nebo záložním prohlédávači, který je v podsíti serveru. Po několika minutách spusíte tento test znovu, abyste zjistili, zda se pohřešovaný server opět neobjeví na seznamu. Alternativně můžete vyvolat volby v podsíti serveru z prostředí konzoly serveru.

► Pro vyvolání voleb hlavního prohlédávače z konzoly serveru

- v příkazovém řádku spusíte následující příkaz:

browstat elect \device\<protokol>_<ID síťového adaptéru> <název domény>

Určete, zda má hlavní prohlédávač pohřešovaný název serveru ve svém seznamu

Hlavní prohlédávač v podsíti pohřešovaného serveru je prvním serverem v komunikačním řetězci, který musí obsahovat názvy serverů ve své podsíti. Pokud není název pohřešovaného serveru na jeho seznamu, určili jste místo selhání v posloupnosti šíření.

► Pro určení, zda má hlavní prohlédávač pohřešovaný název serveru ve svém seznamu

- v příkazovém řádku spusíte následující příkaz:

browstat view \device\<protokol>_<ID síťového adaptéru> \\\<hlavní prohlédávač> | findstr /i <pohřešovaný server>

Pokud má hlavní prohlédávač pohřešovaný server ve svém seznamu, vrátí nástroj Browstat.exe informace, podobné příkladu na obrázku I.15.

```

E:\>browstat view \Device\<Protocol>\_<NIC-ID> \\\<MasterBrowser>\findstr /i <ChybejiciServer>
\\<ChybejiciServer> NT 04.00 <W.S.NT>
  
```

Obrázek I.15 Určení, zda má hlavní prohlédávač pohřešovaný server ve svém seznamu

Pokud místní hlavní prohledávač nemá název serveru, nezobrazí nástroj Browstat.exe žádné informace a vrátíte se do režimu příkazové řádky. V takovém případě můžete přinutit všechny hostitelské počítače v podsíti, aby se ohlásily, pohřešovaný server by se pak měl opět objevit na seznamu hlavního prohledávače.

► **Pro vynucení ohlášení všech hostitelských počítačů v podsíti**

- v příkazovém řádku na libovolném počítači v podsíti s pohřešovaným serverem spusťte následující příkaz:

**browstat forceannounce \device\<protokol>_<ID síťového adaptéru>
<název domény>**

Uvědomte si, že oznámení hostitelských počítačů jsou všesměrová vysílání a že se tudíž mohou ztratit. Pohřešovaný server může být také restartován, aby byl donucen vyslat datagram HostAnnouncement.

Rovněž by mohlo být užitečné ověřit, zda pohřešovaný server dokáže mapovat síťovou jednotku hlavnímu prohledávači, aby bylo ověřeno spojení v síti.

Po uplynutí 12 minut, zkontrolujte, zda se pohřešovaný server objevil na seznamu hlavního prohledávače. Pokud ano, měl by se jeho název šířit po zbytku domény a vyřešit problém.

► **Pro určení, zda hlavní prohledávač domény přijal název serveru od hlavního prohledávače.**

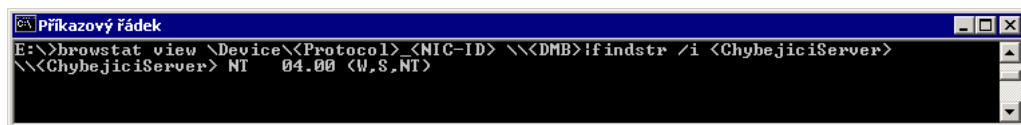
- Sledujte řetěz šíření od hlavního prohledávače v podsíti pohřešovaného serveru k hlavnímu prohledávači domény a určete, zda hlavní prohledávač domény přijal název serveru od hlavního prohledávače.

► **Pro určení, zda hlavní prohledávač domény má pohřešovaný server ve svém seznamu názvů**

- v příkazovém řádku spusťte následující příkaz:

**browstat view \device\<protokol>_<ID síťového adaptéru> \\<DMB> |
findstr /i <pohřešovaný server>**

Pokud má hlavní prohledávač domény server ve svém seznamu, vrátí nástroj Browstat.exe informace, podobné příkladu na obrázku I.16.



Obrázek I.16 Určení, zda hlavní prohledávač domény přijal název serveru od hlavního prohledávače

Pokud hlavní prohledávač domény nemá název serveru, nezobrazí nástroj Browstat.exe žádné informace a vrátíte se do režimu příkazové řádky.

Pokud název serveru chybí na seznamu hlavního prohledávače domény, je jeho absence nejpravděpodobněji způsobena potížemi s překladem názvů. Aby hlavní prohledávač domény dostal seznam serverů od hlavního prohledávače, musí hlavní prohledávač serveru dokázat překládat dotazy na názvy DomainName[1B], aby mohl poslat směrovaný datagram MasterAnnouncement použitím portu UDP číslo 138 hlavního prohledávače domény. Aby mohl hlavní prohledávač domény odpovědět na toto oznámení a dostat seznam serverů, musí také být schopen překládat název počítače hlavní-

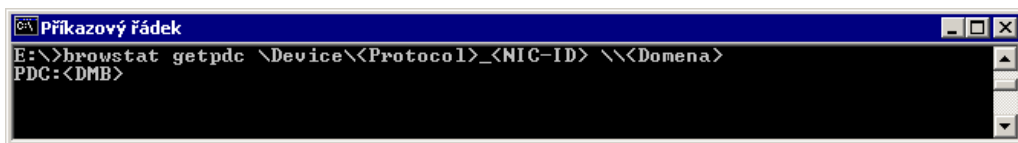
ho prohlédávané z adresy IP hlavního prohlédávané. Schopnost překladu oběma směry z názvu počítače na adresu IP a z adresy IP na název počítače je rozhodující.

► **Pro ověření, zda hlavní prohlédávací server dokáže překládat položku DomainName<1b> v seznamu prohlédávání**

- v příkazovém řádku spusíte následující příkaz:

browstat getpdc \device\<protokol>_<ID síťového adaptéru> <název domény>

Pokud hlavní prohlédávací server dokáže překládat dotaz na název DomainName<1b>, vrátí nástroj Browstat.exe informace, podobné příkladu na obrázku I.17.



Obrázek I.17 Ověření, zda hlavní prohlédávací server dokáže překládat položku DomainName<1b>

Pro ověření, zda hlavní prohlédávací domény i hlavní prohlédávací navzájem dokážou překládat své názvy, vytvořte mapování síťové jednotky z hlavního prohlédávací domény a z hlavního prohlédávací domény na hlavní prohlédávací. Pokud není možné některým směrem jednotky mapovat, mohl by být problém v překladu názvů.

Najděte hlavní prohlédávací v podsíti klienta

Tento krok sleduje řetěz šíření přesunutím testovacího procesu do podsítě klienta. Použijte stejné procedury, jak je uvedeno u kroku číslo 1, ale spusíte je v podsíti klienta.

Určete, zda hlavní prohlédávací v podsíti klienta má název pohřešovaného serveru

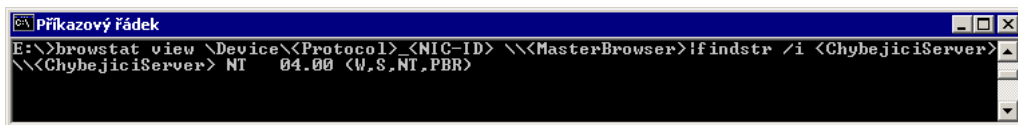
Hlavní prohlédávací v podsíti pohřešujícího klienta dostává svůj seznam od hlavního prohlédávací domény výměnou za svůj vlastní seznam názvů. Určete, zda hlavní prohlédávací klienta má pohřešovaný server ve svém seznamu názvů.

► **Pro určení, zda hlavní prohlédávací v podsíti klienta má název pohřešovaného serveru**

- v příkazovém řádku spusíte následující příkaz:

browstat view \device\<protokol>_<ID síťového adaptéru> \\<hlavní prohlédávací> | findstr /i <pohřešovaný server>

Pokud má hlavní prohlédávací server ve svém seznamu, vrátí nástroj Browstat.exe informace, podobné příkladu na obrázku I.18.



Obrázek I.18 Určení, zda si hlavní prohlédávací klienta vyměnil seznamy s hlavním prohlédávacím domény

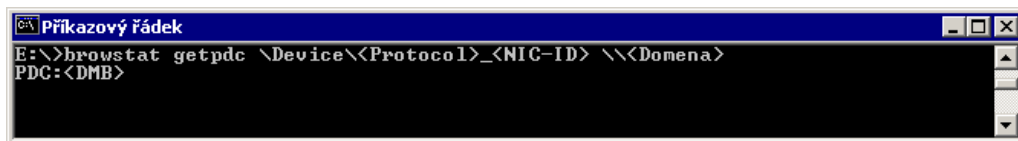
Pokud hlavní prohledávač nemá název pohřešovaného serveru, je to pravděpodobně způsobeno potížemi při překladu názvu. Pak potřebujete ověřit, zda hlavní prohledávač v podsíti klienta dokáže překládat název DomainName<1b>.

► **Pro určení, zda hlavní prohledávač dokáže překládat položku DomainName<1b> v seznamu názvů**

- v příkazovém řádku spusíte následující příkaz:

browstat getpdc \device\<protokol>_<ID síťového adaptéru> <název domény>

Pokud hlavní prohledávač klienta dokáže překládat název DomainName<1b>, vrátí nástroj Browstat.exe informace, podobné příkladu na obrázku I.19.



Obrázek I.19 ověření, zda hlavní prohledávač v podsíti klienta dokáže překládat název DomainName<1b>

Hlavní prohledávač musí také být schopen překládat název počítače hlavního prohledávače domény. Pro ověření vytvořte mapování síťové jednotky z hlavního prohledávače na hlavní prohledávač domény, pak mapujte síťovou jednotku z hlavního prohledávače domény na hlavní prohledávač v podsíti klienta.

Pokud některý z těchto testů selže, musíte napravit potíže s překladem názvů.

Určete záložní prohledávače v podsíti klienta

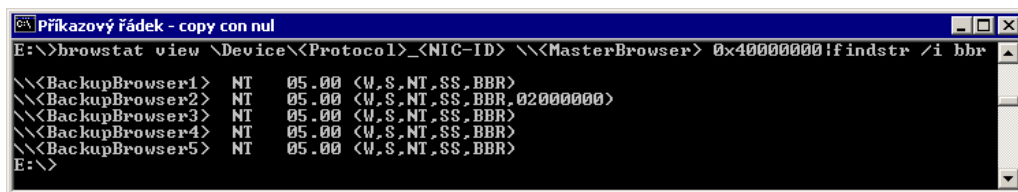
Pro snížení požadavků na zpracování hlavním prohledávačem podsítě jsou požadavky klienta na seznamy prohledávání směrovány především na záložní prohledávač.

► **Pro vyhledání seznamu záložních prohledávačů v podsíti klienta na dálku užítím hlavního prohledávače**

- v příkazovém řádku spusíte následující příkaz:

**browstat view \device\<protokol>_<ID síťového adaptéru>
\\<hlavní prohledávač> 0X40000000 | findstr /i bbr**

Pokud se v podsíti klienta nacházejí záložní prohledávače, vrátí nástroj Browstat.exe informace, podobné příkladu na obrázku I.20.



Obrázek I.20 Vyhledání seznamu záložních prohledávačů

Hexadecimální číslo **0x40000000** je bitová maska, která udává určenému hlavnímu prohlédáči, že seznam má být vytvořen z jeho místní domény. Tyto bitové masky jsou definovány v protokolu Common Internet File System Browsing Protocol.

Určete, zda záložní prohlédáče mají název pohřešovaného serveru

Aby klienti v této podsíti mohli získat spolehlivý seznam prohlédávání, musí být přítomnost názvu pohřešovaného serveru ověřena u všech záložních prohlédáčů.

- ▶ Pro kontrolu přítomnosti názvu pohřešovaného serveru v seznamech názvů záložních prohlédáčů
 - pro každý záložní prohlédáč zadejte v příkazovém řádku následující příkaz:


```
browstat view \device\<protokol>_<ID síťového adaptéru>  
\\<záložní prohlédáče>| findstr /i <pohřešovaný server>
```

Nástroj Browstat.exe vrací informace, podobné příkladu na obrázku I.21.

```
Command Prompt
C:\>browstat view \device\<Protocol>_<NIC-ID> \\<BackupBrowser> |findstr /i <MissingServer>
\\<MissingServer>    NT    05.00 <W.S.NT.SS.BBR>
C:\>
```

Obrázek I.21 Kontrola přítomnosti názvu pohřešovaného serveru u záložních prohlédáčů

Pokud záložní prohlédáč neobsahuje název pohřešovaného serveru, ověřte, zda záložní prohlédáč dokáže mapovat síťovou jednotku na hlavní prohlédáče.

Úloha záložního prohlédáče je nejdynamičtější úlohou prohlédáče. Hlavní prohlédáče dávají pokyn potenciálním prohlédáčům, aby se staly záložními prohlédáči. Počet záložních prohlédáčů, které jsou uvedeny do služby, závisí na počtu spuštěných serverů v podsíti hlavního prohlédáče.

Pokud probíhají volby prohlédáče, počkejte 12 nebo více minut a pak zkuste najít pohřešované servery.

Další úvahy

Pokud dochází k trvalým nebo občasným potížím s funkcí prohlédáče, můžete se rozhodnout vyhradit počítače pro vyhledávací procesy v každé podsíti, aby udržovaly trvalý celodomenový seznam. Pokud jsou servery často vypínány a restartovány, zvažte umístění záložního řadiče domény nebo členského serveru systému Windows NT v každé podsíti s hodnotou položky registru počítače **IsDomainMaster** nastavenou na **True**. Tato položka (datový typ Reg_SZ) se objevuje v následujícím podklíči registru:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser
\Parameters
```

Nastavení hodnoty položky IsDomainMaster na true dává serveru preference během voleb, aby se stal hlavním prohlédáčem pro podsít. Více informací o položce **IsDomainMaster** naleznete v části „Volby prohlédáčů“ dříve v této kapitole.

Upozornění: Nepoužívejte editor registru pro přímou úpravu registru, pokud máte jinou možnost. Editory registru obcházejí standardní zabezpečovací opatření, poskytovaná prostředky pro správu. Tato zabezpečovací opatření vám brání v zadání konfliktních nastavení nebo nastavení, která pravděpodobně sníží výkon nebo poškodí váš systém. Přímá úprava registru může mít závažné neočekávané následky, které mohou zabránit spuštění systému a mohou vyžadovat opětovnou instalaci systému Windows 2000. Pro nastavení nebo přizpůsobení systému Windows 2000 použijte programy v Ovládacích panelech nebo konzolu Microsoft Management Console (MMC) kdykoli je to možné.

Prohledávací služba je velmi citlivá na nastavení směrovačů v propojené síti IP. Protože úlohy prohledávačů jsou určovány všesměrovými volbami, nemohou být předávána všesměrová vysílání protokolu UDP. Předávání všesměrového vysílání protokolu UDP pouze jedním směrem může mít za následek nepředvídatelné chování. Může způsobovat souvislý cyklus voleb.

Další krok, který lze učinit pro vyřešení potíží s prohledávači je zachytávání síťového provozu analyzátozem protokolu, jakým je například Microsoft Network Monitor. Pro přímé sledování komunikace mezi prohledávači může být prohledávací služba zastavena a znovu spuštěna. Bohužel neexistuje záruka, že prohledávač přijme stejnou úlohu, kterou měl před restartováním služby. Tato metoda však může být velmi užitečná pro ověření komunikačního procesu, když hlavní prohledávač vyžaduje celodomenový seznam od hlavního prohledávače domény a bezprostředně nato hlavní prohledávač domény požaduje místní seznam od hlavního prohledávače. Po spuštění prohledávací služby na hlavním prohledávači se během několika minut odehraje úplná výměna. Nastavte velikost sběrné vyrovnávací paměti analyzátoru protokolu a velikost rámce podle této velikosti provozu.

Velikost seznamu serverů, vráceného službou prohledávače do Windows NT 4.0 byla omezena na 64 kilobajtů. Když je tato velikost překročena, vidí uživatel pouze zkrácený abecední seznam serverů. Aby bylo zabráněno tomuto chování, musí být na všech prohledávacích spuštěn systém Windows NT verze 4.0 nebo novější.

Glosář

3DES

Šifrovací algoritmus, který zpracovává každý blok dat třikrát, přičemž pokaždé používá jedinečný klíč. 3DES je mnohem obtížněji rozluštitelný než nekombinovaný DES. Je to nejbezpečnější z kombinací DES, proto je také pomalejší.

802.1p

Protokol, jenž podporuje mapování signálů RSVP na signály vrstvy 2 použitím značení priority 802.1p, aby umožnil stanovení priorit provozu po zařízeních vrstvy 2, jako jsou přepínače, na segmentech sítě. IEEE 802 odkazuje na technologii vrstvy 2 používanou v sítích LAN včetně vrstvy datového spojení a vrstvy řízení přístupu k médiím.

10BaseT

Specifikace 802.3 pro síť Ethernet, která definuje způsob přenosu dat kroucenou dvojlinkou kategorie 3, 4, nebo 5.

A

ACL

Viz seznam řízení přístupu.

ActiveX

Sada technologií, umožňující softwarovým komponentám vzájemnou interakci v síťovém prostředí bez ohledu na jazyk, ve kterém byly tyto komponenty vytvořeny.

adresa IP – IP address

32bitová adresa, používaná pro identifikaci uzlu v síti IP. Každý uzel v síti IP musí mít přiřazenu jednoznačnou adresu IP, která je vytvořena z čísla ID sítě a jednoznačného čísla ID hostitele. Tato adresa se obvykle zapisuje desítkovým zápisem každého oktetu, odděleným tečkami (například 192.168.7.27). V systému Windows 2000 může být adresa IP nastavena ručně nebo dynamicky protokolem DHCP. Viz

též protokol Dynamic Host Configuration Protocol (DHCP); uzel.

adresa IP pro předávání – forwarding IP address

Adresa IP, na kterou je předáván paket podle cílové adresy IP a obsahu směrovací tabulky IP.

adresa IP třídy A – Class A IP address

Adresa IP typu unicast v rozsahu od 1.0.0.1 do 126.255.255.254. První oktet udává síť, poslední tři oktety udávají hostitelský počítač v síti. Viz též adresa IP třídy B; adresa IP třídy C; adresa IP.

adresa IP třídy B – Class B IP address

Adresa IP typu unicast v rozsahu od 128.0.0.1 do 191.255.255.254. První dva oktety udávají síť, poslední dva oktety udávají hostitelský počítač v síti. Viz též adresa IP třídy A; adresa IP třídy C; adresa IP.

adresa IP třídy C – Class C IP address

Adresa IP typu unicast v rozsahu od 192.0.0.1 do 223.255.255.254. První tři oktety udávají síť, poslední oktet udává hostitelský počítač v síti. Vyrovnávání zatížení sítě poskytuje volitelnou podporu relace pro adresy IP třídy C (navíc k podpoře pro jednu adresu IP) pro přizpůsobení klientů, kteří využívají více serverů proxy na straně klienta. Viz též adresa IP třídy A; adresa IP třídy B; adresa IP.

adresa IP třídy D – Class D IP address

Třída adres v síti Internet, navržená pro adresy IP typu multicast. Hodnota prvního oktetu pro adresy IP třídy D a síť je v rozsahu od 224 do 239.

adresa IP třídy E – Class E IP address

Třída adres v síti Internet, určená pouze pro experimentální použití. Hodnota prvního oktetu pro adresy IP třídy E a síť začíná na 240.

adresa paměti – memory address

Část paměti počítače, která může být přidělena zařízení nebo používána programem nebo operačním systémem. Zařízením je obvykle přidělena oblast adres paměti.

adresa řízení přístupu k médiím – media access control address

Adresa, používaná pro komunikaci mezi síťovými adaptéry ve stejné podsíti. Každý síťový adaptér má přiřazenou adresu řízení přístupu k médiu..

adresa všesměrového vysílání všem podsítím – all-subnets directed broadcast address

Adresa všesměrového vysílání konstruovaná tak, aby zasáhla všechny podsítě v rámci ID sítě protokolu IP založeného na třídách.

adresa zpětné smyčky – loopback address

Adresa místního počítače, používaná pro směřování odcházejících paketů zpět ke zdrojovému počítači. Tato adresa se používá převážně pro testování.

adresář – directory

Zdroj informací, který obsahuje údaje o souborech nebo dalších objektech v počítači. V systému souborů ukládá adresář informace o souborech. V rozložených výpočetních prostředích (jako jsou domény systému Windows 2000) ukládá adresář informace o objektech, jakými jsou tiskárny, aplikace, databáze a uživatelé.

adresářová služba – directory service

Zahrnuje zdroj informací o adresářích a službu, která tyto informace zpřístupňuje k použití. Adresářová služba umožňuje uživateli nalézt objekt zadáním jeho atributů. Viz též služba Active Directory; adresář.

adresářový strom – directory tree

Hierarchie objektů a kontejnerů v adresáři, která může být graficky znázorněna jako obrácený strom s kořenovým objektem nahoře. Koncové body stromu jsou obvykle jednotlivé objekty (listy), uzly neboli větve stromu jsou kontejnerové objekty. Strom ukazuje jak jsou objekty spojeny ve smyslu cesty z jednoho objektu k druhému. Jednoduchý strom je jeden kontejner a jeho objekty. Souvislý podstrom je každá

nepřerušená cesta ve stromu se všemi prvky všech kontejnerů, které obsahuje.

agent

Aplikace, která běží na zařízení spravovaném protokolem Simple Network Management Protocol (SNMP). Aplikace agent je objektem aktivít řízení. Rovněž počítač, na kterém běží agent SNMP, je někdy označován jako agent

agent zásad – policy agent

Zabezpečovací mechanismus protokolu Internet Protokol, který vyhledává zásady zabezpečení protokolu IP přiřazené počítači z adresářové služby systému Windows 2000 directory service (nebo z registru, pokud není počítač připojen k doméně) a předává je službě IKE k použití při sestavování zabezpečených spojení. Viz též zásady zabezpečení protokolu IP.

akce filtrů – Filter Actions

Zásady vyjednávání v systému IPSec, které nastavují požadavky na zabezpečení pro mechanismus IPSec SA, nebo pro fázi 2 komunikace. Tyto požadavky jsou uvedeny v seznamu zabezpečovacích metod, obsaženém v akci filtru, včetně toho, jaké algoritmy, zabezpečovací protokoly a vlastnosti klíče mají být použity.

algoritmus

Pravidlo nebo postup pro řešení problému. Zabezpečení internetového protokolu používá šifrovací algoritmy pro zašifrování dat.

algoritmus Diffie-Hellman (DH)

Algoritmus, který předchází šifrování Rivest-Shamir-Adleman (RSA) a nabízí lepší výkon. Je to jeden z nejstarších a nejbezpečnějších algoritmů pro výměnu klíčů. Dvě strany si vyměňují informace o klíčích, které systém Windows 2000 navíc chrání šifrováním funkcí hash. Žádná ze stran si nikdy nevyměňuje skutečný klíč; přesto po výměně klíčových údajů je každá ze stran schopna vytvořit identický sdílený klíč. Skutečný klíč se nevyměňuje nikdy.

algoritmus hash message authentication code (HMAC)

Mechanismus zajišťování integrity dat u komunikace online, který pro zajišťování kontroly integrity online používá u přenášených dat kryptografické funkce výtahu ze zprávy (message

digest). Algoritmus HMAC může být použit u každé iterační kryptografické funkce výtahu ze zprávy, například u funkcí MD5 a SHA-1, v kombinaci s důvěrným sdíleným klíčem. Kryptografická síla algoritmu HMAC závisí na vlastnostech základní funkce výtahu ze zprávy. Algoritmus HMAC se bývá také označován jako algoritmus Hash-based Message Authentication Code. Viz též výtah ze zprávy; funkce výtahu ze zprávy.

algoritmus hash message authentication code-secure hash algorithm (HMAC-SHA)

Algoritmus, vyvinutý institutem National Institute of Standards and Technology a popsaný v e specifikaci FIPS PUB 180-1. Proces SHA je vytvořen podle vzoru MD5. Algoritmus SHA používá 79 32bitových konstant k výpočtu, jehož výsledkem je 160bitový klíč, který se používá ke kontrole integrity.

alias

Další název, který může být použit k přístupu na určitý port.

alokovat – allocate

Označit médium pro použití nějakou aplikací. Dostupná média mohou být alokována.

aplikační programové rozhraní – application programming interface (API)

Sada rutin, které používá aplikace k vyžádání a provedení služeb nižší úrovně, prováděných operačním systémem počítače. Tyto rutiny obvykle provádějí úkoly údržby jako je správa souborů a zobrazování informací.

aplikační vrstva – application layer

Vrstva, ve které aplikace přistupují k síťovým službám. Tato vrstva představuje služby, které přímo podporují aplikace, jako jsou programy pro přenos souborů, přístup k databázím a elektronickou poštu.

AppleTalk

Architektura a protokoly sítě počítačů Apple. Síť s klientskými počítači Macintosh a počítačem, na kterém běží Windows 2000 Server s funkcí Services for Macintosh funguje jako síť AppleTalk.

ARP

Viz protokol překládání adres.

asynchronní režim přenosu – Asynchronous Transfer Mode (ATM)

Vysokorychlostní protokol orientovaný na připojení, používaný pro přenosy mnoha různých typů síťového provozu.

atribut objektu – attribute (object)

Ve službě Active Directory popisuje atribut charakteristiky objektu a typ informace, kterou objekt může obsahovat. Schéma pro každou třídu objektů definuje, jaké atributy instance objektu mít musí a jaké další atributy mít může.

auditování – auditing

Sledování aktivit uživatelů zaznamenáváním vybraných typů událostí v bezpečnostním deníku serveru nebo pracovní stanice.

automatické privátní IP adresování

– Automatic Private IP Addressing (APIPA)

Vlastnost systému Windows 2000 TCP/IP, která automaticky nastavuje jednoznačnou adresu IP v rozsahu od 169.254.0.1 do 169.254.255.254 a masku podsítě 255.255.0.0, pokud je protokol TCP/IP nastaven pro dynamické adresování a není dostupná služba Dynamic Host Configuration Protocol (DHCP).

autonomní systém – autonomous system (AS)

Skupina směrovačů, které si vyměňují informace o směrování užitím běžného protokolu pro směrování.

AXFR

Viz úplný zónový přenos.

B

bez připojení – connectionless

Síťový protokol, ve kterém vysílač vysílá přenos v síti zamýšlenému příjemci bez předchozího vytvoření spojení k příjemci.

bezpečná dynamická aktualizace – secure dynamic update

Proces, kterým klient bezpečné dynamické aktualizace odesílá požadavek dynamické aktualizace serveru DNS a server se pokouší provést aktualizaci pouze pokud klient může prokázat

svou totožnost a má správné pověření k provedení aktualizace. Viz též dynamická aktualizace.

binární – binary

Číselný systém se základem 2, v němž se hodnoty vyjadřují jako kombinace dvou číslic – 0 a 1.

bit

Nejmenší jednotka informace, zpracovávaná počítačem. Jeden bit vyjadřuje binární hodnotu 1 nebo 0, případně logickou hodnotu true (pravda) nebo false (nepravda). Skupina osmi bitů tvoří byte, který může reprezentovat mnoho druhů informace, například číslo abecedy, desítkovou číslici nebo jiný znak. Bitu se někdy také říká binární číslice.

bitové logické a – bit-wise logical AND

Matematická operace, která porovnává stejná množství bitů použitím logického A (AND). Pokud jsou obě porovnávané hodnoty 1, je výsledek také 1. Jinak je výsledek 0.

blok CIDR- CIDR block

Blok adres IP, alokovaný použitím zápisu Classless Interdomain Routing (CIDR).

brána – gateway

Zařízení, připojené k více fyzickým sítím TCP/IP, schopné mezi nimi směrovat nebo doručovat pakety IP. Brána překládá mezi různými transportními protokoly nebo formáty dat (například IPX a IP) a obecně se přidává k sítím především pro své schopnosti překladu. Viz též adresa IP; směrovač IP.

C

cesta – path

Posloupnost názvů adresářů (též složek), která udává umístění adresáře, souboru nebo složky ve stromu adresářů systému Windows. Každý název adresáře a souboru uvnitř cesty musí být zepředu oddělen obráceným lomítkem (\). Například pro specifikaci cesty k souboru s názvem Readme.doc, uloženému v adresáři Windows jednotky C zadejte C:\Windows\Readme.doc.

class-based

Adresování nebo směrování IP, založené na třídách adres sítě internet.

Classless Interdomain Routing (CIDR)

Metoda alokace veřejných adres IP, která není založena na původních internetových třídách. Zápis Classless Interdomain Routing (CIDR) byl vyvinut, aby pomohl zabránit vyčerpání veřejných adres IP a minimalizoval velikost směrovacích tabulek sítě Internet.

CLIP

Viz protokol Classical IP over ATM.

cluster

Skupina nezávislých počítačových systémů, nazývaných též uzly nebo hostitelské počítače, které pracují společně jako jeden systém, aby zajistily, že rozhodující aplikace a prostředky zůstanou dostupné pro klienty. Server cluster je typem clusteru, který implementuje služba Cluster service. Vyrovnávání zatížení sítě poskytuje softwarové řešení pro vytváření clusterů z více počítačů se systémem Windows 2000 Server, které poskytuje síťové služby v síti Internet a v soukromých intranetech.

CNAME

Ve službě Active Directory se jedná o jedinečný název objektu, zapisovaný s kořenem na prvním místě bez značek atributu LDAP (jako jsou CN= nebo DC=). Segmenty názvu jsou odděleny lomítky (/). Například CN=MyDocuments,OU=MyOU,DC=Microsoft,DC=Com je v kanonickém tvaru převeden na microsoft.com/MyOU/MyDocuments. V DNS, jde o typ záznamu prostředku. Viz též jedinečný název; protokol Lightweight Directory Access Protocol (LDAP); záznam objektu kanonického názvu (CNAME).

cyklická obsluha – round robin

Jednoduchý mechanismus používaný servery DNS pro sdílení a rozdělování zátěže síťových prostředků. Cyklická obsluha se používá k rotaci pořadí záznamů prostředků, vrácených jako odpověď na dotaz, pokud existuje více záznamů prostředků stejného typu pro dotazovaný název domény DNS.

Č

čas konvergence – convergence time

Čas, který je potřeba pro dosažení konvergence v síti. Viz konvergence.

čas odezvy – response time

Doba, potřebná pro vykonání činnosti od začátku do konce. V prostředí klient-server se obvykle měří na straně klienta.

časová razítka TCP – TCP timestamps

Možnost protokolu TCP, používaná pro záznam času kdy byl segment TCP odeslán a času, kdy byl potvrzen příjemcem.

čekací doba – latency

Viz čekací doba replikace.

černá díra – black hole

Situace v síťové komunikaci, kdy dojde ke ztrátě paketů bez hlášení chyby.

číslo ID hostitelského počítače – host ID

Číslo, používané k identifikaci rozhraní ve fyzické síti, ohraničené směrovači. Číslo ID hostitelského počítače by mělo být jedinečné v síti.

číslo ID sítě – network ID

Číslo, používané k identifikaci systémů, které jsou umístěny ve stejné fyzické síti, ohraničené směrovači. Číslo ID by mělo být v síti jedinečné.

číslo ID verze – version ID

Počítadlo, používané k určení, které položky databáze WINS musí být aktualizovány během replikace. Viz též replikace.

číslo protokolu – protocol number

Pole v paketu IP, které udává další úroveň výše v zásobníku protokolu.

členský server – member server

Počítač se spuštěným Windows 2000 Server, který však není řadičem domény systému Windows 2000. Členské servery se podílejí na doméně, ale neukládají kopii databáze adresářů.

D

databáze informací o správě – Management Information Base (MIB)

Kolekce formálně popsaných objektů, z nichž každý představuje určitý typ informace, kterou lze spravovat a využívat v protokolu Simple Network Management Protocol (SNMP) systémem správy sítě.

databáze WINS – WINS database

Databáze, používaná pro zaznamenávání a překlad názvů počítačů na adresy IP v sítích se systémem Windows. Obsah této databáze je v pravidelných intervalech replikován po síti. Viz též partnerský server pro vyžádanou replikaci; partnerský server pro nabízenou replikaci; replikace.

datagram

Nepotvrzený datový paket, odeslaný na jiné místo sítě. Cílem může být jiné zařízení, přímo dosažitelné v lokální síti (LAN) nebo vzdálený cíl, dosažitelný pomocí směrovaného doručení přes síť s přepínáním paketů.

datagram hlasování – election datagram

Zvláštní datagram, vytvářený počítači v sítích Microsoft k vyvolání voleb v systému prohledávačů.

datagram všesměrového vysílání – broadcast datagram

Datagram IP, odeslaný všem hostitelským počítačům v podsíti. Viz též datagram.

datagramový soket – datagram socket

Soket, používající rozhraní Windows Sockets API, který poskytuje nespolehlivý tok dat bez připojení.

datový model služby Active Directory – Active Directory data model

Model odvozený z datového modelu LDAP. Adresář udržuje objekty, které reprezentují entity různých druhů, popsané atributy. Objekty a třídy objektů, které mohou být uloženy v adresáři, jsou definovány ve schématu. Pro každou třídu objektů schéma definuje, jaké atributy musí mít instance této třídy, jaké další atributy může mít a která třída může být jejím rodičem. Viz též atribut; LDAP; schéma.

datový proud – data stream

Všechny informace, přenášené v daném čase po síti.

dávaný ARP – gratuitous ARP

Rámec požadavku ARP, odeslaný hostitelským počítačem pro jeho vlastní adresu IP, když protokol TCP/IP obdrží adresovací informace. Dávané ARP se používají ke kontrole duplicitních adres IP v podsíti.

delegování – delegation

Schopnost přiřadit odpovědnost za správu části oboru názvů jinému uživateli, skupině nebo organizaci. U DNS jde o záznam názvové služby v nadřazené zóně, který udává název serveru ověřeného pro delegovanou zónu. Viz též dědičnost; nadřazenost.

depeše – trap

Zpráva v protokolu Simple Network Management Protocol (SNMP), odeslaná agentem správním systému, udávající, že došlo k události na hostitelském počítači, kde je agent spuštěn. Viz též agent; ověřování; protokol Internet Protocol; protokol Simple Network Management Protocol (SNMP).

desítkový tvar s tečkami**– dotted decimal notation**

Formát adresy IP, podle kterého je adresa rozdělena po bajtech, převedených do desítkové soustavy a oddělených tečkami. (Příklad: 192.168.3.24)

dešifrování – decryption

Proces, který učiní šifrovaná data čitelnými převedením šifrovaného textu na prostý text. Viz též šifrovaný text; šifrování; prostý text.

Dfs

Viz distribuovaný systém souborů.

DHCP

Viz protokol Dynamic Host Configuration Protocol.

disk

Fyzické zařízení pro ukládání dat, připojené k počítači. Viz též základní disk; dynamický disk.

distribuované zpracování – distributed processing

Počítačové prostředí, které obsahuje klienta a server. Tato struktura umožňuje rozdělit na části pracovní zatížení, které dosud bylo jedním procesem.

distribuovaný systém souborů**– Distributed file system (Dfs)**

Služba systému Windows 2000 sestávající ze software, umístěného na síťových serverech a klientech, která transparentně spojuje sdílené adresáře, umístěné na různých souborových serverech v jednom oboru názvů pro zlepšené sdílení zátěže a dostupnost dat.

doména – domain

V systémech Windows NT a Windows 2000 jde o propojenou sadu počítačů se spuštěnými systémy Windows NT nebo Windows 2000, která sdílí databázi Security Accounts Manager (SAM) a která může být spravována jako skupina. Uživatel s účtem v určité doméně se může přihlásit nebo přistupovat na svůj účet z libovolného počítače v této doméně. Doména je jedním bezpečnostním oborem v počítačové síti Windows NT. V systému DNS jde o větev pod uzlem ve stromu DNS.

doména druhé úrovně – second-level domain

Doména v systému Domain Name System (DNS), která leží bezprostředně pod doménou nejvyšší úrovně.

doména in-addr.arpa – in-addr.arpa domain

Zvláštní doména DNS nejvyšší úrovně, vyhrazená pro zpětné mapování adresy na názvy hostitele DNS. Viz též zpětné vyhledávání; domény nejvyšší úrovně.

doménová struktura – forest

Kolekce jednoho nebo více stromů služby Active Directory systému Windows 2000, rovnocenně organizovaných a propojených dvousměrnými vztahy důvěryhodnosti mezi kořenovými doménami každého stromu. Všechny stromy v doménové struktuře sdílejí společné schéma, nastavení konfigurace a globální katalog. Pokud doménová struktura obsahuje více stromů, tvoří tyto stromy souvislý obor názvů.

doménový strom – domain tree

V systému DNS jde o převrácenou hierarchickou stromovou strukturu, která se používá pro indexování názvů domén. Doménové stromy mají podobný účel a koncepci jako adresářové stromy, užívané systémem souborů počítače k ukládání na disk. Viz též doménový název; obor názvů.

domény nejvyšší úrovně – top-level domains

Názvy domén, které jsou hierarchicky zakořeněné v první vrstvě oboru názvů domény přímo pod kořenem (.) oboru názvů DNS. V síti Internet se používají názvy domén nejvyšší úrovně, jakými jsou „.com“ a „.org“ ke klasifikaci a přiřazování názvů domén druhé úrovně (jakou je například „microsoft.com“) jednotlivým organizacím a podnikům podle jejich organizačního účelu. Viz též domény druhé úrovně.

dopředné vyhledávání – forward lookup

V systému DNS, jde o zpracování dotazů, ve kterém se vyhledává popisný název DNS hostitelského počítače pro nalezení adresy IP. Ve správci DNS jsou založeny zóny dopředného vyhledávání na názvech domén DNS a obvykle udržují záznamy prostředků adres hostitelského počítače.

dostupná přenosová rychlost – available bit rate (ABR)

Služba typu ATM, která podporuje provoz dostupnou přenosovou rychlostí, minimální zaručenou přenosovou rychlost a vrcholy přenosové rychlosti. Služba ABR rovněž umožňuje alokaci šířky pásma v závislosti na dostupnosti a používá řízení toku pro komunikaci o šířce pásma s koncovým uzlem.

dostupnost – availability

Míra odolnosti proti chybám počítače a jeho programů. Vysoce dostupný počítač běží 24 hodin denně, 7 dní v týdnu. Viz též odolnost proti chybám.

dostupný stav – available state

Stav, ve kterém může být médium alokováno pro použití aplikacemi.

dotaz na název – name query

dotaz, vyslaný do místní sítě nebo názvovému serveru systému NetBIOS pro přeložení adresy

IP, když jedna aplikace systému NetBIOS chce komunikovat s jinou aplikací systému NetBIOS.

dotaz na název v rozhraní NetBIOS – NetBIOS name query

Paket odeslaný buď názvovému serveru rozhraní NetBIOS, jakým je třeba server WINS, nebo vyslaný všemi směry k překladu adresy IP názvu v rozhraní NetBIOS.

duplex

Systém, schopný přenosu informací po komunikačním kanálu oběma směry. Viz též plný duplex; poloduplex.

důvěrnost – confidentiality

Základní bezpečnostní funkce kryptografie. Důvěrnost poskytuje záruku, že pouze oprávnění uživatelé mohou číst nebo používat důvěrné nebo tajné informace. Bez důvěrnosti může kdokoliv s přístupem k síti používat snadno dostupné nástroje k tajnému naslouchání síťovému provozu a odposlouchávat cenné informace pro vnitřní potřebu. Například služba zabezpečení v protokolu Internet Protocol zajišťuje šifrováním dat, že zpráva je odhalena pouze zamýšleným příjemcům. Viz též kryptografie; ověřování; integrita; neodvolatelnost.

dvousměrný vztah důvěryhodnosti – two-way trust relationship

Spojení mezi doménami, ve kterém každá doména důvěřuje uživatelským účtům jiné domény pro použití svých prostředků. Uživatelé se mohou přihlásit z počítačů každé takové domény k doméně, která obsahuje jejich účet. Viz též vztah důvěryhodnosti.

dynamická aktualizace – dynamic update

Aktualizovaná specifikace standardu Domain Name System (DNS), která povoluje hostitelským počítačům, které ukládají informace o názvech v systému DNS, dynamicky zaznamenávat a aktualizovat jejich záznamy v zónách, udržovaných servery DNS, které mohou přijímat a zpracovávat dynamické zprávy o aktualizacích.

dynamická obnova klíčů – dynamic re-keying

Metoda, používaná protokolem IPsec k určování, jak často se během komunikace vytváří nový klíč. Komunikace probíhá po blocích a kaž-

dý blok dat je zabezpečen jiným klíčem. To zabráňuje narušiteli, který získal část komunikace a odpovídající klíče relace, aby získal zbytek zprávy.

dynamické porty – dynamic ports

Porty v rozsahu od 49151 do 65535, které jsou vydávány na základě náhodných čísel.

dynamické směrování – dynamic routing

Použití směrovacích protokolů k aktualizaci směrovacích tabulek. Dynamické směrování reaguje na změny v topologii sítě.

dynamicky připojované knihovny – dynamic-link library (DLL)

Význačný rys operačních systémů rodiny Microsoft Windows a operačního systému OS/2. Knihovny DLL umožňují, aby spustitelné rutiny, obecně sloužící určité funkci nebo sadě funkcí, aby byly uloženy v oddělených souborech s příponou .dll a byly zaváděny do paměti pouze tehdy, když to vyžádá program, který je potřebuje.

dynamický směrovač – dynamic router

Směrovač s dynamicky nastavovanými směrovacími tabulkami. Dynamické směrování se skládá ze směrovacích tabulek, které jsou vytvářeny a udržovány automaticky pokračující komunikací mezi směrovači. Tato komunikace je usnadněna směrovacím protokolem. Kromě svého výchozího nastavení vyžadují dynamické směrovače málo běžné údržby a proto se hodí pro větší sítě.

E

emulace sítě LAN – LAN emulation (LANE)

Sada protokolů, které umožňují existujícím službám sítě Ethernet a Token Ring překrývat síť ATM. Emulace ANE umožňuje konektivitu mezi stanicemi, připojenými k sítím LAN a ATM. Viz též asynchronní režim přenosu.

export

V systému NFS jde o zpřístupnění souboru serverem klientovi pro připojování.

externí obor názvů – external namespace

Veřejný obor názvů, který je dostupný každému v síti Internet.

F

filtr – filter

V systému IPsec jde o pravidlo, které poskytuje schopnost aktivovat vyjednávání zabezpečení pro komunikaci podle zdroje, cíle a typu přenosu IP.

filtrování paketů – packet filtering

Zabráňuje určitým typům síťových paketů v odeslání nebo příjmu. To může být použito z bezpečnostních důvodů (k zabránění přístupu neoprávněným uživatelům) nebo pro zlepšení výkonu nepovolením zbytečných paketů v průchodu pomalým spojením. Viz též paket.

filtry – filters

V přenosech IP a IPX jde o filtrování paketů, řady definic, které udávají směrovači typ přenosů, povolených nebo nepovolených na každém rozhraní.

firewall

Kombinace hardware a software, která poskytuje zabezpečovací systém, obvykle pro zabránění neoprávněných přístupů zvnějšku do vnitřní sítě nebo intranetu. Firewall brání v přímé komunikaci mezi sítí a externími počítači směrováním provozu přes server proxy mimo síť. Server proxy určuje, zda je bezpečné nechat soubor proniknout do sítě. Firewall je někdy označován jako bezpečnostní brána.

fond adres – address pool

Skupina adres IP v rozsahu. Adresy z fondu jsou pak dostupné pro dynamické přiřazení serverem DHCP klientům DHCP.

fragmentace a opětovné sestavení – fragmentation and reassembly

Proces, používaný protokolem Internet Protocol (IP) pro fragmentaci datagramu IP do menších paketů, které jsou opět sestaveny cílovým hostitelským počítačem.

fronta – queue

Seznam programů nebo úkolů, čekajících na provedení. V terminologii tisku v systému Windows 2000 označuje fronta skupinu dokumentů, čekajících na tisk. V prostředích NetWare a OS/2 jsou fronty primárním softwarovým rozhraním mezi aplikací a zařízením

pro tisk; uživatelé posílají dokumenty do fronty. V systému Windows 2000 je však tímto rozhraním tiskárna; dokument je odeslán tiskárně a ne do fronty.

funkce hash – hash function

Viz výtah ze zprávy; funkce výtahu ze zprávy.

funkce výtahu ze zprávy – message digest function

Jednosměrný matematický algoritmus, používaný pro vytvoření výtahu ze zprávy. Viz též výtah ze zprávy.

fyzická vrstva – physical layer

Softwarová vrstva, která přenáší bity z jednoho počítače na druhý a řídí přenos proudu bitů fyzickým médiem. Tato vrstva definuje způsob připojení kabelů k síťovému adaptéru a výběr použité techniky přenosu k odeslání dat kabelem..

fyzické médium – physical media

Objekt uložení dat, na který je možno zapisovat, například disk nebo magnetická páska. Na fyzické médium se odkazuje jeho číslem ID fyzického média (PMID).

G

geografická doména – geographical domain

Typ domény s názvem, užívajícím dvouznakový kód regionu nebo země, stanovený v souladu s normou 3166 organizace International Organization of Standardization (ISO).

globálně jedinečný identifikátor – globally unique identifier (GUID)

16bajtová hodnota, vytvořená z jedinečného identifikátoru zařízení, aktuálního data a času a pořadového čísla. Identifikátor GUID se používá k určení konkrétního zařízení nebo součásti.

H

hash

Viz výtah ze zprávy; funkce výtahu ze zprávy.

hexadecimální – hexadecimal

Číselná soustava se základem 16, jehož čísla jsou zapisována číslicemi od 0 do 9 a písmeny

od A (ekvivalent desítkového čísla 10) do F (ekvivalent desítkového čísla 15).

hierarchický obor názvů

– hierarchical namespace

Obor názvů jako je obor názvů DNS nebo obor názvů Active Directory, který je hierarchicky strukturovaný a poskytuje pravidla, jež umožňují rozdělit obor názvů do oddílů. Viz též obor názvů; plochý obor názvů; nesouvislý obor názvů.

hlášení serveru – Server Announcement

Zvláštní datagram, vytvářený počítači v sítích Microsoft, který slouží k ohlášení jejich přítomnosti hlavním prohledávacím.

hlavní server – master server

Při zónovém přenosu DNS jde o počítač, který je zdrojem zóny. Hlavní servery se mohou lišit a jsou jedním ze dvou typů (buď primární nebo sekundární), v závislosti na tom, jak server získává údaje o zóně. Viz též primární server; sekundární server; zóna; zónový přenos.

hodnota DWORD

Datový typ, složený z hexadecimálních údajů s maximálním přiděleným prostorem 4 bajtů.

hodnota Time To Live (TTL)

Hodnota časovače, uváděná v paketech posílaných v sítích TCP/IP, která sděluje příjemcům, jak dlouho mají udržovat nebo používat paket nebo jakákoliv data v něm obsažená do vypršení platnosti a zahození paketu nebo dat. V systému DNS se používají hodnoty TTL v záznamech prostředků v zóně k určení, jak dlouho mají klienti tyto údaje udržovat v mezipaměti a používat je, pokud se objeví v odpovědi na dotaz serveru DNS pro zónu.

hostitelská adresa – host address

Číslo ID hostitelského počítače.

hostitelská skupina – host group

Sada hostitelských počítačů přijímající vícesměrové vysílání IP, odeslané na určitou adresu skupiny vícesměrového vysílání.

hostitelská trasa – host route

Trasa k určité síťové adrese (číslo ID sítě a číslo ID hostitelského počítače). Místo rozhodování o trase, založeného pouze na čísle ID sítě je roz-

hodnutí o trase založeno na kombinaci čísla ID sítě a čísla ID hostitelského počítače. Hostitelské trasy umožňují inteligentní rozhodování o trasách pro každou adresu v síti. Hostitelské trasy se obvykle používají pro vytváření vlastních tras pro řízení a optimalizaci určitého typu síťového provozu. Pro směrovací tabulky IP má hostitelská trasa síťovou masku 255.255.255.255.

hostitelský počítač, hostitel – host

Počítač se systémem Windows 2000 se spouští ným serverovým programem nebo službou, používanou sítí nebo vzdálenými klienty. U vyrovnávání zatížení sítě se jedná o cluster, obsahující více hostitelských počítačů, propojených v lokální síti.

Hosts

Viz soubor Hosts.

hraniční vrstva – boundary layer

Obecné rozhraní mezi dvěma softwarovými součástmi, jež je standardizováno, aby jiným součástem umožnilo připojení k tomuto rozhraní.

hromadný zprostředkovatel univerzální konvence pro názvy – multiple universal naming convention provider (MUP)

Mechanismus, který vybírá vhodný přesměrovač, když se aplikace pokouší překládat název UNC (univerzální konvence pro názvy – universal naming convention).

hvězdička – wildcard

Znak v systému DNS, který může být při dotazu nahrazen jiným znakem.

I

index parametrů zabezpečení – Security Parameters Index (SPI)

Jedinečná rozlišující hodnota v přidružení zabezpečení, používaná k rozlišení mezi několika přidruženími zabezpečení, existujícími v přijímajícím počítači.

infračervené zařízení – infrared device

Počítač nebo počítačové periferní zařízení, jako například tiskárna, které je schopno komunikovat použitím infračerveného světla. Viz též infračervený.

infračervený – infrared (IR)

Světlo, které se ve spektru nachází za červenou. Toto světlo není viditelné pro lidské oko, infračervené vysílače a přijímače však mohou vysílat a přijímat infračervené signály. Viz též protokol Infrared Data Association; infračervené zařízení; infračervený port.

infračervený port – infrared port

Optický port počítače, který umožňuje bezdrátovou komunikaci s jinými počítači nebo zařízeními použitím infračerveného světla. Infračervené porty se nacházejí na některých počítačích, tiskárnách a kamerách. Viz též infračervené zařízení.

integrita – integrity

Základní zabezpečovací funkce kryptografie. Integrita poskytuje ověření, že původní obsah informace nebyl změněn nebo porušen. Bez funkce integrity by někdo mohl informaci změnit nebo by mohlo dojít k jejímu porušení, ale tyto změny by mohly zůstat neodhaleny. Například vlastnost zabezpečení protokolu Internet Protocol, která chrání data před neoprávněnými modifikacemi při přenosu, zajišťuje, že přijímaná data jsou přesně stejná jako data odeslaná. Funkce hash podepisuje každý paket kryptografickým kontrolním součtem, který přijímající počítač ověřuje před otevřením paketu. Pokud se změnil paket a tedy i kontrolní součet, je paket odmítnut. Viz též kryptografie; ověřování; důvěrnost; neodvolatelnost.

Integrovaná zóna služby Active Directory – Active Directory-integrated zone

Primární zóna, uložená ve službě Active Directory. Viz též zóna.

integrované služby při pomalém spojení – Integrated Services over slow links (ISSLOW)

Mechanismus front používaný pro optimalizaci pomalých (nízkokapacitních) síťových rozhraní snižováním čekací doby. Je navržen především pro rozhraní, která posílají přenosy po modemových spojích, kanálech ISDN-B a spojení s nižší rychlostí než T1.

internet

Dva nebo více segmentů sítě, propojených směrovači. Jiný termín pro internetwork. Pomo-

cí protokolu TCP/IP, může být internet vytvořen spojením dvou nebo více sítí IP počítačem s více adresami se spuštěným systémem Windows 2000 Server nebo Windows 2000 Professional. Na trase mezi připojenými segmenty sítě IP musí být umožněno předávání.

Internet

Celosvětová veřejná síť typu internetwork TCP/IP, skládající se z tisíců sítí, propojující výzkumné ústavy, univerzity, knihovny a soukromé společnosti.

internetwork

Alespoň dva síťové segmenty, spojené použitím směrovačů.

interval obnovení – renewal interval

Doba, daná klientovi pro obnovení jeho názvu v serveru WINS. Pokud není název do konce této periody obnoven, bude uvolněn. Interval obnovení je rovněž znám jako prodleva obnovení názvu (name refresh timeout), nebo hodnota Time To Live (TTL).

interval platnosti – expire interval

V systému DNS jde dobu v sekundách, kterou mají servery DNS, pracující jako sekundární hlavní servery zóny, používat pro určení, zda vypršela platnost údajů zóny, pokud není zóna obnovena.

interval zániku – extinction interval

Hodnota databáze WINS, která stanovuje, jak dlouho setrvávají položky v uvolněném a neplatném stavu.

intranet

Síť uvnitř organizace, která používá technologie a protokoly sítě Internet, ale je dostupná pouze některým lidem, jako například zaměstnancům společnosti. Síť intranet se také někdy říká soukromá (privátní) síť.

IP

Viz protokol Internet Protocol.

iterace – iteration

Metoda překladu dotazu na název od klienta. Server DNS nemusí poskytovat požadovaný název, pokud používá iteraci. Pokud server DNS je oprávněný pro požadovaný název, vrátí tento název. Pokud ne, vrátí seznam záznamů

prostředků A a NS o serverech s názvy, které se podobají dotazovanému názvu, ale nepokouší se tyto servery kontaktovat. Klient může pokračovat v hledání názvu kontaktováním těchto doporučených serverů. Alternativní metodou je rekurzivní překlad.

iterační dotaz – iterative query

Dotaz na server DNS, ve kterém tázající dává serveru pokyn, že očekává nejlepší odpověď, kterou dokáže server poskytnout bez vyhledávání další pomoci jiných serverů DNS. Iteračním dotazům se také říká nerekurzivní dotazy. Viz též iterace; rekurze; odkaz.

iterační dotaz na název – iterative name query

Viz iterační dotaz.

IXFR

Viz přírůstkový zónový přenos.

J

jádro – kernel

Jádro architektury vrstev, které spravuje nejzákladnější operace operačního systému a procesoru počítače v systémech Windows NT a Windows 2000. Jádro plánuje pro procesor různé bloky provedení kódu, zvané podprocesy, aby je co nejvíce vytížilo, a koordinuje více procesorů pro optimalizaci výkonu. Jádro rovněž synchronizuje aktivity součástí výkonné úrovně, jako je správce vstupů a výstupů a správce procesů a řídí hardwarové výjimky a další funkce, závislé na hardware. Jádro úzce spolupracuje s vrstvou HAL (hardware abstraction layer).

jasný text – cleartext

Viz prostý text.

jazyk structured query language (SQL)

Široce akceptovaný standardní databázový podjazyk, používaný pro dotazy, aktualizace a správu relačních databází.

jednoznačný název – distinguished name (DN)

Název, který jednoznačně identifikuje objekt užitím relativního jednoznačného názvu objektu plus názvu kontejneru objektu a názvu domény, která obsahuje objekt. Jednoznačný název identifikuje objekt a rovněž jeho umístění ve stromu.

Každý objekt ve službě Active Directory má jednoznačný název. Příkladem jednoznačného názvu je CN=MyName,CN=Users,DC=Reskit,DC=Com.

Tento jednoznačný název identifikuje uživatelský objekt „MyName“ v doméně reskit.com.

jmenovka – label

Viz jmenovka názvu domény.

jmenovka názvu domény – domain name label

Každá část úplného názvu domény v systému DNS, které představuje uzel ve stromu oboru názvů domény. Názvy domén se sestavují z posloupností jmenovek, jako například tři jmenovky „noam“, „reskit“, a „com“ tvoří název domény DNS „noam.reskit.com“. Každá jmenovka, použitá v systému DNS musí mít 63 nebo méně znaků.

k okamžitému použití – Plug and Play

Sada specifikací, vyvinutá firmou Intel, která umožňuje počítači automaticky zjišťovat a nastavit zařízení a instalovat příslušné ovladače.

karta smart card

Zařízení velikosti kreditní karty, které se používá s kódem PIN pro ověření, založené na certifikátech a jednoduché přihlášení k podniku. Karty smart card bezpečně ukládají certifikáty, veřejné a privátní klíče, hesla a další druhy osobních informací. Čtecí zařízení pro karty smart card, připojené k počítači, čte kartu smart card. Viz též ověřování; certifikát; neodvolatelnost.

kategorie everyone – everyone category

V prostředí Macintosh jde o jednu z uživatelských kategorií, které jsou přiřazena povolení pro složku. Povolení, udělená kategorii everyone platí pro všechny uživatele včetně hostů, kteří používají server.

kilobit

Jednotka dat rovná 1000 bitům.

kilobity za sekundu – kilobits per second (Kbps)

Rychlost přenosu dat v síti, měřená v násobcích 1000 bitů za sekundu.

klíč – key

Tajný kód nebo číslo, požadované pro čtení, změny nebo ověřování zabezpečených dat. Klí-

če se používají ve spojení s algoritmy k zabezpečení dat. Systém Windows 2000 zpracovává vytváření klíče automaticky. V registru je klíč položkou, která může obsahovat podklíče a položky. Ve struktuře registru jsou klíče obdobou složek a položky obdobou souborů. V okně Editoru registrů se klíč objevuje jako složka souborů v levé části okna. V souboru odpovědí jsou klíče řetězce znaků, které určují parametry, ze kterých se získávají data pro bezobslužnou instalaci operačního systému.

klíč registru – registry key

Identifikátor pro záznam nebo skupinu záznamů v registru.

klíč relace – session key

Klíč, používaný především pro šifrování a dešifrování. Klíče relací se obvykle používají pro symetrické šifrovací algoritmy, kde se stejný klíč používá pro šifrování i dešifrování. Z tohoto důvodu obvykle označují pojmy symetrický klíč a klíč relace stejný typ klíče. Viz též šifrování symetrickým klíčem.

klient – client

Jakýkoli počítač nebo program, připojený k jinému počítači nebo programu nebo vyžadující služby jiného počítače či programu. Viz též server.

kombinovaný režim – mixed mode

Výchozí nastavení režimu pro domény v řadících domén systému Windows 2000. Kombinovaný režim umožňuje řadičům domén systému Windows 2000 a záložním řadičům domén systému Windows NT společně existovat v doméně. Kombinovaný režim nepodporuje univerzální skupiny a vnošené skupiny systému Windows 2000. Nastavení režimu domény můžete změnit na nativní režim Windows 2000 tehdy, když jsou všechny řadiče domén systému Windows NT buď odstraněny z domény nebo aktualizovány na Windows 2000. Viz též nativní režim.

komprimace – compaction

Proces, který uvolňuje prostor a defragmentuje disky, aby zvýšil výkon serveru WINS.

**komunikace orientovaná na spojení
– connection-oriented communication**

Síťová přenosová služba, kde je vyjednáno a vytvořeno fyzické nebo logické spojení před přenosem paketu.

koncový systém – end system

Síťové zařízení bez schopnosti předávat pakety mezi částmi sítě. Viz též hostitelský počítač.

**konstantní přenosová rychlost
– constant bit rate (CBR)**

Služba typu ATM, která podporuje přidělení konstantní šířky pásma. Tento typ služby se používá pro přenosy hlasu a pohyblivého obrazu, které vyžadují malé nebo žádné ztráty buněk a přesné řízení časování během přenosu.

konvence Universal Naming Convention (UNC)

Konvence vytváření názvů souborů a dalších prostředků, začínající dvěma obrácenými lomítky (\), která označují, že prostředek se nachází na síťovém počítači. Názvy UNC odpovídají syntaxi \\SERVERNAME\SHARENAME, kde SERVERNAME je název serveru a SHARENAME je název sdíleného prostředku. Název UNC pro adresář nebo soubor může rovněž obsahovat cestu k adresáři za názvem sdíleného prostředku: \\SERVERNAME\SHARENAME\DIRECTORY\FILENAME.

konvergence – convergence

Proces stabilizace systému poté, co dojde ke změně v síti. Pro směrování, pokud se trasa stane nedostupnou, směrovače vysílají zprávy o aktualizaci po síti a znovu vytvářejí informace o preferovaných trasách. Pro vyvažování zatížení sítě jde o proces, kterým si hostitelské počítače vyměňují zprávy, aby určily nový, konzistentní stav clusteru a zvolily hostitelský počítač s nejvyšší prioritou hostitele, který je také znám jako výchozí hostitel. Během konvergence je určeno nové rozdělení zátěže pro hostitelské počítače, které sdílejí zpracování síťového provozu pro specifické porty TCP nebo UDP. Viz též cluster; výchozí hostitel; hostitelský počítač; protokol User Datagram Protocol (UDP).

konzola Microsoft Management Console (MMC)

Struktura hostitelských správních konzol. Konzola je definována položkami ve svém stromu, což mohou být složky nebo jiné kontejnery, stránky WWW a jiné správní položky. Konzola má jedno nebo více oken, která poskytují pohled na strom konzoly a správní vlastnosti, služby a události, které vystupují jako položky stromu konzoly. Hlavní okno konzoly MMC poskytuje příkazy a nástroje pro vytváření obsahu konzol. Prostředky pro vytváření obsahu a strom konzoly MMC mohou být skryté, pokud je konzola spuštěna v uživatelském režimu. Viz též strom konzoly.

kořen – root

Nejvyšší úroveň v hierarchicky organizované množině informací. Kořen je bodem, ze kterého se větví další podmnožiny v logické posloupnosti, která se pohybuje od širších nebo obecnějších ohnisek k užším perspektivám.

kořenová doména – root domain

Počátek oboru názvů systému Domain Name System (DNS). Ve službě Active Directory počáteční doména ve stromu Active Directory. Také počáteční doména doménové struktury.

kořenové servery – root servers

Servery DNS, které jsou oprávněné pro kořen oboru názvů. Viz též oprávněný; obor názvů; kořen; soubor odkazů na kořeny.

kořenový adresář systému – systemroot

Název cesty a složky, kde jsou umístěny systémové soubory Windows 2000. Obvykle je to C:\Winnt, ale při instalaci systému Windows 2000 může být určena jiná jednotka nebo složka. Hodnota %systemroot% může být použita pro nahrazení skutečného umístění složky, která obsahuje systémové soubory Windows 2000. Pro určení kořenového adresáře systému klikněte na Start, klikněte na Spustit a zadejte %systemroot%.

kořenový server DNS – root DNS server

Server DNS, oprávněný pro kořen Internetu. Viz též server DNS.

kryptografický klíč – cryptographic key

Viz šifrovací klíč.

kryptografie – cryptography

Umění a věda informační bezpečnosti. Poskytuje čtyři základní funkce informační bezpečnosti: důvěrnost, integritu, ověření a neodvolatelnost. Viz též důvěrnost; integrita; ověřování; neodvolatelnost.

kryptografie veřejným klíčem – public key cryptography

Kryptografická metoda, ve které se pro poskytnutí zabezpečovacích funkcí používají dva různé klíče, které se vzájemně doplňují: veřejný klíč a privátní klíč. Kryptografie veřejným klíčem je někdy označována jako kryptografie s asymetrickým klíčem. Viz též kryptografie; veřejný klíč; privátní klíč.

kvalita služby – Quality of Service (QoS)

Sada standardů a mechanismů zajištění kvality přenosu dat, implementovaná v systému Windows 2000.

L**LocalTalk**

Síťový hardware firmy Apple, zabudovaný v každém počítači Macintosh. LocalTalk zahrnuje kabely a propojovací schránky pro spojení počítačů a síťových zařízení, které jsou součástí síťového systému AppleTalk. LocalTalk byl dříve znám jako AppleTalk Personal Network.

lokátor řadiče domény – domain controller locator (Locator)

Algoritmus, který je spuštěn v kontextu služby Netlogon a který nalézá řadiče domén v síti Windows 2000. Lokátor může nalézt řadiče domén použitím názvů DNS (pro počítače kompatibilní s IP/DNS) nebo použitím názvů NetBIOS (pro počítače se systémy Windows 3.x, Windows for Workgroups, Windows NT 3.5 nebo pozdější, Windows 95 nebo Windows 98, případně v sítích, kde není k dispozici přenos IP).

logická podsít' IP – logical IP subnet (LIS)

Skupina hostitelů a členů IP, patřící do stejné podsítě IP a u nichž je stejná adresa ATM jejich hostitelského serveru ATMARP.

LPM

Viz modul místních zásad.

M**malá kancelář/domácí kancelář – Small Office/Home Office (SOHO)**

Kancelář s několika počítači, která může být malým podnikem nebo částí větší sítě.

mapování názvů – name mapping

Vlastnost systému Windows 2000, která umožňuje přístup k systému souborů pro uživatele systémů MS-DOS a Windows 3.x na svazky NTFS a FAT a umožňuje přiřazování uživatelských účtů pro uživatele systému Kerberos ze sfér jiných než Windows 2000 nebo externím uživatelům (mimo rozlehlou síť) s certifikáty X.509. Pro přístup do systému souborů povoluje systém Windows 2000 sdílet názvy o délce až 255 znaků, na rozdíl od systémů MS-DOS a Windows 3.x, které jsou omezeny na osm znaků, následovaných tečkou a příponou z maximálně tří znaků. Každý soubor nebo složka s názvem, který nevyhovuje standardu MS-DOS 8.3, dostane automaticky přiřazený druhý název, který vyhovuje. Uživatelé systémů MS-DOS a Windows 3.x, kteří se připojují k souboru nebo adresáři po síti, vidí název ve formátu 8.3; uživatelé systému Windows 2000 vidí dlouhý název.

maska podsítě – subnet mask

32bitová hodnota, vyjádřená jako čtyři desítková čísla od 0 do 255, oddělená tečkami (například 255.255.0.0). Toto číslo umožňuje protokolu TCP/IP určovat část čísla ID sítě pro adresu IP.

maska podsítě proměnlivé délky – variable length subnet masks (VLSM)

Masky podsítí, používané k vytváření podsítí čísla ID sítě IP různých velikostí.

metrika – metric

Číslo, používané k vyjádření nákladů na směrování ve směrovací tabulce IP, umožňující výběr nejlepší trasy mezi více trasami do stejného cíle.

mezipaměť – cache

Pro systémy DNS a WINS jde o lokální místo uložení informací pro záznamy prostředků pro naposledy překládané názvy vzdálených hostitelských počítačů. Typicky je mezipaměť vytvá-

řena dynamicky tak, jak počítač zjišťuje a překládá názvy; mezipaměť pomáhá optimalizovat čas, potřebný pro překlad zjišťovaných názvů. Viz též vyrovnávací soubor; služba vytváření názvů; záznam prostředku.

mezipaměť ARP – ARP cache

Tabulka adres IP a jim odpovídajících adres řízení médií. Pro každé rozhraní existuje oddělená mezipaměť ARP.

meziprocesová komunikace – interprocess communication (IPC)

Řada součástí, požívaných programy i procesy v počítačích v síti. Meziprocesová komunikace umožňuje klientskému počítači a počítači se službou server komunikovat s dalšími počítači.

minimální TTL – minimum TTL

Výchozí hodnota Time To Live (TTL), nastavená v sekundách pro použití u všech záznamů prostředků v zóně. Tato hodnota je pro každou zónu nastavena v záznamu prostředku Start of Authority (SOA). Ve výchozím nastavení server DNS zahrnuje tuto hodnotu do odpovědi na dotazy, aby informoval příjemce, jak dlouho mohou ukládat a používat záznam prostředku, poskytnutý odpovědí na dotaz, než vyprší platnost údajů, uložených v záznamech. Pokud jsou hodnoty TTL nastaveny pro jednotlivé záznamy prostředků, přepíší tyto hodnoty minimální hodnotu TTL. Viz též hodnota Time To Live (TTL).

místní počítač – local computer

Počítač, ke kterému lze přistupovat přímo, bez použití komunikační linky nebo komunikačního zařízení, jako jsou síťový adaptér nebo modem. Podobně znamená spuštění lokálního programu spuštění programu na vašem počítači narozdíl od spuštění programu na serveru.

místní síť – local area network (LAN)

Komunikační síť, propojující skupinu počítačů, tiskáren a dalších zařízení, umístěných v relativně omezené oblasti (například v budově). Místní síť umožňuje každému připojenému zařízení spolupracovat s každým jiným zařízením v síti. Viz též rozlehlá síť.

místní skupina domény – domain local group

Skupina systému Windows 2000, dostupná pouze pro domény v nativním režimu, která může obsahovat členy z každého místa v doménové struktuře, v důvěryhodné doménové struktuře nebo v důvěryhodné doméně se systémem starším než Windows 2000. Místní skupiny domény mohou udělovat oprávnění pouze k prostředkům uvnitř domény, ve které se nacházejí. Místní skupiny domény se obvykle používají ke sběru zaregistrovaných objektů zabezpečení z doménové struktuře k řízení přístupu k prostředkům uvnitř domény.

místní úřad zabezpečení – local security authority (LSA)

Chráněný podsystém, který ověřuje a přihlašuje uživatele k místnímu systému. Navíc udržuje systém LSA informace o všech aspektech lokálního zabezpečení v systému (společně nazývaných místní zásady zabezpečení) a poskytuje různé služby pro překlad mezi názvy a identifikátory.

množina oborů – superscope

Správní seskupování oborů, které může být použito pro podporu více logických podsítí IP ve stejné fyzické podsíti. Množiny oborů obsahují seznam oborů, které jsou jejich členy neboli podřízenými obory, které lze aktivovat jako kolekci.

model Component Object Model (COM)

Objektově založený programovací model, vytvořený pro podporu softwarové spolupráce; umožňuje dvěma nebo více aplikacím nebo součástí snadno spolupracovat i tehdy, když jsou vytvořeny různými dodavateli, v různé době, různých programovacích jazycích nebo když běží na různých počítačích pod různými operačními systémy. COM je základní technologií, na které mohou být vybudovány nadřazené technologie. Na technologii COM jsou vybudovány technologie Object linking and embedding (OLE) a ActiveX.

model DARPA

Čtyřvrstvý model, který se používá k popisu sady protokolů TCP/IP. Čtyři vrstvy modelu Department of Defense Advanced Research Pro-

jects Agency (DARPA) jsou: aplikační, transportní, internetová a síťového rozhraní.

model DCOM

Viz model Distributed Component Object Model.

model Distributed Component Object Model (DCOM)

Specifikace modelu Component Object Model (COM) firmy Microsoft, která definuje způsob komunikace součástí v sítích založených na systému Windows. Použijte konfigurační nástroj DCOM pro integraci aplikací klient-server na více počítačích. Model DCOM lze rovněž použít pro integraci robustních aplikací pro prohlížení webu. Viz též konfigurační nástroj DCOM.

modul místních zásad – local policy module

Mechanismus systému Windows 2000, který poskytuje službě QoS Admission Control vyhledávání informací o zásadách služby Active Directory. Služba QoS Admission Control vyvolává modul LPM, když je nalezen objekt zásad s tiketem Kerberos v systému Windows 2000. Modul LPM vybere název uživatele z objektu zásad a zprávy protokolu RSVP a vyhledá zásady řízení přístupu uživatele ve službě Active Directory.

moduly emulátorů – emulator modules

Softwarové součásti, které umožňují aplikacím, vytvořeným pro systém NetBIOS a rozhraní Windows Sockets, připojení k rozhraní ovladačů přenosové vrstvy.

multinetting

Praxe používání více logických podsítí v jedné fyzické síti.

N

na spojení orientované NDIS – Connection-Oriented NDIS (Co-NDIS)

Specifikace rozhraní síťového ovladače (Network Driver Interface Specification), která podporuje přenos dat orientovaný na spojení.

nadřazená doména – parent domain

Domény v doménách DNS a doménách služby Active Directory, které jsou umístěny v oboru názvů přímo nad jinými odvozenými názvy do-

mén (podřízené domény). Například „reskit.com“ by byla nadřazenou doménou pro doménu „eu.reskit.com“, která je podřízenou doménou. Viz též podřízená doména; oddíl adresáře; doména.

nadřazený objekt

Objekt, který je bezprostředně nadřazen jinému objektu v hierarchii. Nadřazený objekt může mít více podřízených objektů. Ve službě Active Directory určuje schéma, které objekty mohou být nadřazené kterým jiným objektům. V závislosti na své třídě může být nadřazený objekt podřízeným objektem jiného objektu. Viz též podřízený objekt; objekt.

nadřazování – parenting

Koncepce správy růstu a delegování nadřazených domén do dalších podřízených domén, které jsou odvozeny a delegovány z nadřazeného názvu. Viz též podřízená doména; nadřazená doména.

nastavení hub-and-spoke

Nastavení serveru WINS, které používá centrální rozbočovač (hub) jako místo kontaktu pro mnoho vzdálených serverů WINS – paprsků (spoke), čímž zlepšuje čas konvergence.

nástroj Line Printer Remote (LPR)

Nástroj pro připojování, který je spuštěn na klientských systémech a používá se k tisku souborů na počítačích se spuštěnou službou LPD. Viz též služba Line Printer Daemon (LPD).

nástroj Nslookup

Nástroj, spuštěný z příkazového řádku, který umožňuje uživatelům klást dotazy DNS pro testování a odstraňování chyb instalací DNS.

nativní režim – native mode

Podmínky, za kterých všechny řadiče domén v doméně jsou řadiče domén systému Windows 2000 a správce sítě umožnil činnost nativního režimu (nastavením Uživatelé a Počítače ve službě Active Directory). Viz též kombinovaný režim.

název domény – domain name

V systému Windows 2000 a ve službě Active Directory jde o jméno, zadané správcem skupině počítačů, které sdílejí společný adresář. V systému DNS jsou názvy domén specifickými

názvy uzlů ve stromu oboru názvů DNS. Názvy domén v DNS používají jednoduché názvy uzlů, označované též „jmenovky“, spojené tečkami (.), které určují každou úroveň uzlu v oboru názvů. Viz též Domain Name System (DNS); obor názvů.

název domény podle připojení – connection-specific domain name

Název domény specifický pro adaptér na rozdíl od globálního názvu specifického pro počítač. Viz též název domény.

název hostitele – host name

Název počítače v síti. V Resource Kitu systému Windows 2000 Server, je název hostitele používán k označení prvního pojmenování v úplném názvu domény. Viz též soubor hostitelů.

název počítače – computer name

Jedinečný název složený z nejvýše 15 velkých písmen, který identifikuje počítač v síti. Tento název nesmí být shodný s názvem jiného počítače nebo domény v síti.

název sítě – network name

V serverových clusterech jde o název, pomocí něhož přistupují uživatelé k prostředkům serverového clusteru. Název sítě se podobá názvu počítače, pokud je kombinován ve skupině prostředků s adresou IP a přístupem klientů aplikací, představuje pro klienty virtuální server.

název skupiny – group name

Jedinečný název, identifikující místní nebo globální skupinu v systému Windows 2000. Název skupiny nesmí být stejný se názvem žádné další skupiny nebo uživatelským jménem ve vlastní doméně nebo počítači. Viz též globální skupina; lokální skupina.

název služby – service name

Název, pod kterým je znám port.

název UNC – UNC name

Úplný název systému Windows 2000 pro síťový prostředek. Vyhovuje syntaxi \\servername\sharename, kde servername je název serveru a sharename je název sdíleného prostředku. Názvy UNC pro adresáře a soubory mohou rovněž obsahovat cestu k adresáři za názvem sdí-

leného prostředku s následující syntaxí: \\servername\sharename\directory\filename. Konvence UNC bývá také označována jako Universal Naming Convention.

název v rozhraní NetBIOS – NetBIOS name

16bajtový název procesu, používajícího rozhraní NetBIOS. Název je rozpoznáván službou WINS, která tento název mapuje na adresu IP.

názvová služba – naming service

Služba, poskytovaná například službami WINS nebo DNS, která umožňuje překládat popisné názvy na adresy nebo jiné speciálně definované údaje o prostředcích, které se využívají při vyhledávání síťových prostředků k různým účelům.

názvový server – name server

V modelu klient-server systému DNS jde o server, oprávněný pro část databáze DNS. Server zpřístupňuje názvy a další informace klientským resolverům – překladačům, které kladou dotazy na překlad názvů v Internetu nebo intranetu. Viz též systém názvů domén (DNS).

názvový server rozhraní NetBIOS – NetBIOS name server

Počítač, který překládá názvy v rozhraní NetBIOS na adresy IP. Server WINS je názvovým serverem rozhraní NetBIOS.

negativní odezva na registraci názvu – negative name registration response

Odezva na požadavek registrace názvu od hostitelského počítače nebo serveru NetBIOS, udávající, že jiný hostitelský počítač nebo server NetBIOS již registroval požadovaný název.

negativní ukládání do mezipaměti – negative caching

Situace, ve které počítače, používající dotazy DNS, ukládají na omezenou dobu negativní odpovědi do mezipaměti. Negativní odpověď dostanou tehdy, když server DNS přímo odpoví na dotaz na název sdílením, že nebyly nalezeny žádné existující záznamy o požadovaném názvu domény DNS. Využití tohoto způsobu ukládání do mezipaměti může pomoci zrychlit reakci na další dotazy z jiných počítačů na stejný název.

největší přenosová jednotka
– maximum transmission unit (MTU)

Maximální velikost rámce, podporovaná technologií sítě jako jsou Ethernet nebo Token Ring.

největší přenosová jednotka cesty
– path maximum transmission unit (PMTU)

Maximální velikost paketu, která je podporována všemi síťovými technologiemi na cestě mezi zdrojovým a cílovým hostitelským počítačem.

největší velikost segmentu
– maximum segment size

Maximální velikost segmentu TCP, který může být vyslán ve spojení TCP.

nekontejnerový objekt

Objekt, který nemůže logicky obsahovat jiné objekty. Soubor je nekontejnerovým objektem. Viz též kontejner; objekt kontejneru.

neodvolatelnost, nepopíratelnost
– nonrepudiation

Základní zabezpečovací funkce kryptografie. Neodvolatelnost poskytuje záruku, že účastník komunikace nemůže nepravdivě popřít, že část komunikace proběhla. Bez neodvolatelnosti by někdo mohl komunikovat a později komunikaci popřít nebo tvrdit, že ke komunikaci došlo jindy. Viz též kryptografie; ověřování; důvěrnost; integrita.

neplatná adresa – illegal address

Duplicitní adresa, která způsobuje konflikt s veřejnou adresou IP, která již byla přiřazena sdružením InterNIC jiným organizacím.

nepřátelský server DHCP – rogue DHCP server

Neoprávněný server DHCP server.

nepřímé doručení – indirect delivery

Doručení paketu IP uzlem IP zprostředkujícím směrovači.

nesouvislý obor názvů – noncontiguous namespace

Obor názvů, vycházející z různých názvů kořenových domén DNS, jakým je například několik stromů v jedné doménové struktuře. Viz též obor názvů; hierarchický obor názvů; plochý obor názvů.

NetBEUI

Viz protokol NetBIOS Extended User Interface.

NetBT

Viz rozhraní NetBIOS nad protokolem TCP/IP.

NetWare

Síťový operační systém firmy Novell.

nezávislí dodavatelé software – independent software vendors (ISVs)

Třetí strana, vyvíjející software; jednotlivec nebo organizace, který nezávisle vytváří počítačový software.

NNTP

Viz protokol Network News Transfer Protocol.

O**obecná kvalita služby**
– generic Quality of Service

Metoda, kterou síť TCP/IP nabízí záruky kvality služby pro multimediální aplikace. Obecná kvalita služby přiděluje různé šířky pásma pro každé spojení podle potřeby.

objekt – object

Entita, kterou může být soubor, složka, sdílená složka, tiskárna nebo objekt služby Active Directory, popsaná jednoznačnou pojmenovanou sadou atributů. Například mezi atributy objektu soubor patří jeho název, umístění a velikost; mezi atributy objektu Uživatel služby Active Directory mohou patřit jméno, příjmení a adresa elektronické pošty. U objektů OLE a ActiveX může být objekt také libovolnou dávkou informací, kterou lze připojit nebo zahrnout do jiného objektu. Viz též atribut; objekt kontejneru; nekontejnerový objekt; nadřazený objekt; podřízený objekt.

objekt kontejneru – container object

Objekt, který může logicky obsahovat další objekty. Například složka je objekt kontejneru. Viz též nekontejnerový objekt; objekt.

objekt zásad skupiny – Group Policy object

Kolekce nastavení zásad skupiny. Objekty zásad skupiny jsou dokumenty, vytvořené modulem snap-in zásad skupiny. Objekty zásad skupiny se ukládají na úrovni domény a týkají se

uživatelů a počítačů v sídlech (sites), doménách a organizačních jednotkách. Každý počítač se systémem Windows 2000 má právě jednu skupinu nastavení uloženou lokálně, říká se jí lokální objekt zásad skupiny (local Group Policy object).

obnovení – refresh

Aktualizace zobrazených informací aktuálními daty.

obnovovací interval – refresh interval

V systému DNS jde o 32bitový časový interval, který musí uplynout dříve, než jsou obnoveny údaje zóny. Když obnovovací interval projde, sekundární server ověří u hlavního serveru zóny, zda jsou údaje o zóně stále aktuální nebo zda je nutné je obnovit zónovým přenosem. Tento interval se nastavuje v záznamu prostředku Start of Authority (SOA) pro každou zónu. Viz též záznam prostředku; sekundární server; záznam prostředku Start of Authority (SOA); zóna; přenos zóny.

obor názvů – namespace

Sada jedinečných názvů zdrojů nebo položek, používaná ve sdíleném počítačovém prostředí. Názvy v oboru názvů mohou být překládány na objekty, které zastupují. Pro konzolu Microsoft Management Console (MMC) představuje obor názvů strom konzoly, který zobrazuje všechny moduly snap-in a prostředky, které jsou pro konzolu přístupné. V systému názvů domén (Domain Name System – DNS) je obor názvů vertikální nebo hierarchickou strukturou stromu doménových názvů. Například každé pojmenování domény jako „host1“ nebo „example“, použité v úplném názvu domény jakým je „host1.example.microsoft.com“, udává větev ve stromu doménových názvů. Ve službě Active Directory odpovídá obor názvů svou strukturou oboru názvů DNS, ale překládá se na názvy objektů služby Active Directory.

obor názvů domény – domain namespace

Databázová struktura, používaná systémem Domain Name System (DNS). Viz též systém Domain Name System (DNS).

obor vícesměrového vysílání – multicast scope

Oblast vícesměrových adres IP v rozsahu od 239.0.0.0 do 239.254.255.255. Adresám víces-

měrového vysílání v tomto rozsahu může být zabráněno v šíření oběma směry (vysílání i příjem) užitím oborového ohraničení vícesměrového vysílání.

oddělené sítě – disjoint networks

Separátní sítě, které o sobě navzájem nevědí.

oddíl – partition

Logické členění pevného disku. Oddíly usnadňují uspořádání informací. Každý oddíl může být formátován pro jiný systém souborů. Oddíl musí být celý uložen na jednom fyzickém disku a tabulka oddílů v hlavním spouštěcím záznamu může obsahovat až čtyři položky pro oddíly.

odhad času okružní cesty

– round trip time estimation (RTTE)

Doba potřebná k dokončení okružní cesty od vysílače k přijímači a zpět.

odolnost proti chybám – fault tolerance

Zajištění integrity dat, když nastanou hardwarové chyby. V platformách Windows NT a Windows 2000 poskytuje ochranu proti chybám ovladač Ftdisk.sys.

ochrana proti obaleným pořadovým číslům

– protection against wrapped sequence numbers (PAWS)

Použití časových razítek TCP k tomu, aby bylo příjemci TCP zabráněno v záměně nového pořadového čísla se starým pořadovým číslem, ježhož příjem očekává.

oktet – octet

V programování označuje oktet osm bitů nebo jeden bajt. Například adresy IP jsou obvykle zapisovány v desítkovém zápisu s tečkami; to znamená s desítkovou hodnotou každého oktetu adresy, oddělenou tečkou. Viz též adresa IP.

omezená adresa všesměrového vysílání

– limited broadcast address

Adresa všesměrového vysílání 255.255.255.255.

operační systém Unix

Výkonný víceuživatelský víceúlohový operační systém, původně vyvinutý v AT&T Bell Laboratories v roce 1969 pro použití na minipočítačích. Operační systém Unix je považován za více přenosný – to jest méně závislý na počítači

— než ostatní operační systémy, protože je napsán v jazyce C. Novější verze operačního systému Unix byly vyvinuty na University of California v Berkeley a ve společnosti AT&T.

oprávnění – permission

Pravidlo, spojené s objektem, určující, kteří uživatelé mohou získat přístup k objektu a jakým způsobem. Oprávnění jsou udělena nebo odeprána vlastníkem objektu. Viz též objekt; oprávnění; uživatelská práva.

oprávněný, nadřazený – authoritative

V systému názvů domén Domain Name System (DNS) jde o použití zón serverem DNS k registraci a překladu názvu domény. Pokud je server DNS konfigurován jako hostitelský server pro zónu, je oprávněný pro názvy uvnitř této zóny. Servery DNS získávají oprávnění na základě informací, uložených v zóně. Viz též zóna.

organizace Internet Assigned Numbers Authority (IANA)

Organizace, která přiděluje adresy IP a jejich rozvržení organizacím, jako je InterNIC.

organizační doména – organizational domain

Typ domény, označený tříznakovým kódem, který udává primární funkce nebo činnosti organizací, obsažených v doméně, jako například .org, .edu, nebo .gov.

organizační jednotka – organizational unit (OU)

Kontejnerový objekt služby Active Directory, používaný uvnitř domén. Organizační jednotka je logický kontejner, ve kterém jsou umístěni uživatelé, skupiny, počítače a další organizační jednotky. Může obsahovat objekty pouze ze své nadřazené domény. Organizační jednotka je nejmenším oborem, ke kterému lze připojit objekt zásady skupiny a ke které lze delegovat správní úřad.

orientovaný na spojení, se spojením – connection-oriented

Typ síťového protokolu, který vyžaduje virtuální koncové spojení mezi vysílačem a příjemcem před zahájením síťové komunikace.

OSI

Viz referenční model propojování otevřených systémů.

OSPF

Viz protokol Open Shortest Path First.

ověřovací hlavička

– Authentication Header (AH)

Hlavička, zajišťující ověření, integritu a ochranu proti znovupřehraní pro celý paket (jak hlavičku IP, tak přenášená data v paketu).

ověřovací protokol Kerberos – Kerberos authentication protocol

Ověřovací mechanismus pro ověřování identity uživatele nebo hostitelského počítače. Ověřovací protokol Kerberos v5 je výchozí ověřovací službou v systému Windows 2000. Zabezpečení protokolu IP a služba QoS Admission Control používají pro ověřování protokol Kerberos. Viz též služby Internet Protocol security (IPSec); ověřovací protokol NTLM; služba QoS Admission Control.

ověřování – authentication

Proces protokolu IPSec, který ověřuje původ a integritu zprávy zjišťováním pravé identity každého počítače. Bez silného ověřování je podezřelý každý neznámý počítač a veškerá z něj odeslaná data. Protokol IPSec poskytuje více metod ověřování pro zajištění kompatibility se staršími systémy, používajícími předchozí verze systému Windows, se systémy, které nepoužívají Windows a se sdílenými počítači.

Proces v síťovém přístupu, kterým systém ověřuje uživatelské přihlašovací informace. Jméno uživatele a heslo je porovnáváno s autorizovaným seznamem. Pokud systém zjistí shodu, je povolen přístup v rozsahu specifikovaném seznamem povolení pro daného uživatele. Pokud se uživatel přihlásí k účtu na počítači se systémem Windows 2000 Professional, je ověření provedeno klientem. Pokud se uživatel přihlásí k účtu v doméně systému Windows 2000 Server, může být ověření provedeno libovolným serverem této domény. Viz též server; vztah důvěryhodnosti.

ovladač IPSec – IPSec driver

Ovladač, který používá seznam filtrů IP z aktivních zásad zabezpečení IPSec ke sledování odchozích paketů IP, které musí být zabezpečeny, a příchozích paketů IP, které musí být ověřeny a dešifrovány.

ovladače miniportu – miniport drivers

Ovladač, který je připojen ke zprostředkujícímu ovladači a hardwarovému zařízení.

P**paket – packet**

Přenosová jednotka pevné maximální délky, která obsahuje binární informace. Tyto informace reprezentují data i hlavičku, obsahující číslo ID, adresu zdroje a cíle a data pro řízení chyb.

paket Magic – Magic Packet

Paket, který obsahuje 16 souvislých kopií adresy přijímajícího adaptéru Ethernet. Paket Magic se používá k probuzení počítače z úsporného režimu.

partnerský server pro nabízenou replikaci – push partner

Vlastnost služby Windows Internet Name Service (WINS), která posílá repliky partnerským serverům pro vyžádanou replikaci po přijetí jejich požadavku. Viz též partnerský server pro vyžádanou replikaci.

partnerský server pro vyžádanou replikaci – pull partner

Vlastnost služby Windows Internet Name Service (WINS), která čte repliky z partnerských serverů pro nabízenou replikaci vyžádáním a přijetím nabízených replik. Viz též partnerský server pro nabízenou replikaci.

Ping

Nástroj, který ověřuje připojení k jednomu nebo více vzdáleným hostitelským počítačům. Příkaz ping používá vysílá pakety požadavku na ozvěnu a odpovědi na ozvěnu protokolu ICMP, ke zjištění, zda je určitý systém IP v síti funkční. Nástroj Ping je užitečný pro diagnostiku sítí IP nebo chyb směrovačů. Viz též protokol Internet Control Message Protocol (ICMP).

plochy obor názvů – flat namespace

Obor názvů, který není strukturovaný a nemožnou v něm být vytvořeny oddíly, jakým je například obor názvů základního systému vstupu a výstupu sítě (NetBIOS). V plochem oboru názvů musí mít každý objekt jednoznačné jméno. Viz též obor názvů; hierarchický obor názvů; nesouvislý obor názvů.

PMTU

Viz největší přenosová jednotka cesty.

počet směrování – hop count

Hodnota v poli řízení přenosu Transport Control, která udává počet směrovačů IPX, které zpracovávají paket IPX.

počítač s více adresami, vícedomý počítač – multihomed computer

Počítač, který má více síťových adaptérů nebo kterému bylo nastaveno více adres IP pro jeden síťový adaptér.

počítače a uživatelé služby Active Directory – Active Directory Users and Computers

Prostředek, vytvořený pro provádění denních úkolů správy služby Active Directory. Tyto úkoly zahrnují vytváření, odstraňování, změny, přesouvání a nastavování povolení pro objekty uložené v adresáři. Těmito objekty jsou organizační jednotky, uživatelé, kontakty, skupiny, počítače, tiskárny a sdílené souborové objekty. Viz též objekt; povolení.

poddoména – subdomain

Doména DNS, umístěná přímo pod jinou doménou (nadřazenou doménou) ve stromu oboru názvů. Například „eu.reskit.com“ je poddoménou domény „reskit.com.“

podpora velkých oken – large window support

V komunikacích protokolu TCP jde o největší množství dat, které může být přeneseno bez potvrzení. Okno má pevnou velikost. Podpora velkých oken dynamicky přepočítává velikost okna a umožňuje přenášení větších objemů dat najednou, čímž zlepšuje průchodnost.

podproces – thread

Typ objektu uvnitř procesu, který spouští programové instrukce. Použití více podprocesů umožňuje současné operace uvnitř procesu a umožňuje jednomu procesu spouštět různé části svého programu současně na různých procesorech. Podproces má svou vlastní sadu registrů, vlastní zásobník jádra, blok prostředí podprocesu a uživatelský zásobník v adresovém prostoru svého procesu.

podřízená doména – child domain

Pro DNS a službu Active Directory jde o doménu, umístěnou ve stromové struktuře oboru názvů přímo pod názvem jiné domény (tzv. nadřazené domény). Například doména „example.reskit.com“ je podřízenou doménou nadřazené domény „reskit.com“. Pro podřízenou doménu se také používá označení poddoména. Viz též oddíl adresáře; doména; nadřazená doména.

podřízený – slave

Server, který se nepokouší sám překládat dotazy. Místo toho posílá všechny dotazy serverům pro předávání. Viz též server pro předávání.

podsíť – subnet

Pododdíl sítě IP. Každá podsíť má své jedinečné podsíťové číslo ID sítě.

podsíť se samými jedničkami – all-ones subnet

Podsíť, pro kterou jsou všechny bity v podsíťové části ID sítě nastaveny na 1.

podsíť se samými nulami – all-zeros subnet

Podsíť, pro kterou jsou všechny bity v podsíťové části ID sítě nastaveny na 0.

podsíťové číslo ID sítě – subnetted network ID

Číslo ID sítě pro segment sítě, který tvoří podsíť jako výsledek rozdělení čísla ID sítě TCP/IP.

pojmenovaný kanál – Named Pipe

Část paměti, která může být použita jedním procesem pro předání informací jinému procesu, takže výstup jednoho procesu je vstupem druhého procesu. Druhý proces může být místní (na stejném počítači) nebo vzdálený (na počítači v síti).

poloduplex – half-duplex

Systém, schopný přenášet informace komunikačním kanálem v daný okamžik pouze jedním směrem. Viz též duplex; plný duplex.

položka – entry

Prvek nejnižší úrovně v registru. položky se objevují v pravé části okna editoru registru. Každá položka se skládá z názvu položky, jejího datového typu a její hodnoty.

Položky ukládají skutečné údaje o nastavení, která ovlivňují operační systém a programy, spuštěné v tomto systému. Liší se od klíčů a podklíčů registru, což jsou kontejnery.

pomíjivé porty – ephemeral ports

Porty v rozsahu od 1024 do 5000.

port

Mechanismus, umožňující více relací. Zpřesnění adresy IP. Ve Správci zařízení jde o místo připojení počítače, ke kterému lze připojit zařízení, předávající a získávající data. Například tiskárna je obvykle připojena k paralelnímu portu (rovněž označovanému jako port LPT), modem bývá obvykle připojen k sériovému portu (rovněž označovanému jako port COM).

porty Well-Known Ports

Porty v rozsahu od 0 do 1023.

posunutí – offset

Počet bajtů od začátku rámce, kde se vyskytuje hledaný vzor definovaný ve filtru při sledování sítě.

posunutí fragmentu – fragment offset

Pole v hlavičce protokolu Internet Protocol (IP), které se používá k obnovení fragmentované datové části IP. Posunutí fragmentu určuje pozici fragmentu relativně k původní datové části IP.

požadavek registrace názvu – name registration request

Zpráva, odeslaná názvovému serveru systému NetBIOS, když hostitelský počítač TCP/IP zahajuje pokus registrace názvu domény.

požadavky přerušení – interrupt request (IRQ) lines

Hardwarové linky, po kterých mohou zařízení posílat signály, aby získaly pozornost procesoru, když je zařízení připraveno přijímat nebo vysílat informace. Požadavky přerušení (IRQ) jsou číslovány od 0 do 15. Každé zařízení musí mít jedinečný požadavek přerušení.

PPP

Viz protokol point-to-point.

pravidla – rules

Mechanismus zásad IPSec, který řídí jak a kdy zásady IPSec zabezpečují komunikaci. Pravidlo poskytuje schopnost spouštět a řídit zabezpečenou komunikaci podle zdroje, cíle a typu provozu IP. Každé pravidlo obsahuje seznam filtrů IP a kolekci zabezpečovacích akcí, které se vykonají v případě shody se seznamem filtrů

prezenční signál – heartbeat

V clusteru serveru nebo clusteru vyvažování síťového zatížení jde o signál, periodicky vysílaný mezi uzly, který umožňuje rozpoznávat systémové chyby na každém uzlu.

prezentační vrstva – presentation layer

Vrstva sítě, která překládá data z aplikační vrstvy do meziformátu. Tato vrstva rovněž spravuje otázky zabezpečení poskytovaním takových služeb, jako je šifrování dat, a komprimuje data tak, že po síti je přenášeno menší množství bitů.

**primární název domény
– primary domain name**

Název, používaný k určení domény, ve které se počítač nachází. Viz též název domény podle připojení.

primární server – primary server

Oprávněný (autoritativní) server DNS pro zónu, který může být použit jako místo aktualizace pro zónu. Pouze hlavní primární servery mají schopnost být přímo aktualizovány a zpracovat aktualizace zóny, jimiž jsou přidávání, odstraňování a změny záznamů prostředků, které jsou uložena jako údaje o zóně. Hlavní primární servery se také používají jako první zdroje replikace zóny jiným serverům DNS.

primární zóna – primary zone

Kopie zóna, která je spravována místně. Viz též zóna; sekundární zóna.

**privátní adresní prostor
– private address space**

Sada privátních adres. Prostor privátních adres se skládá z následujících tří bloků adres: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

privátní adresy – private addresses

Adresy IP, navržené pro použití v organizacích k privátnímu adresování intranetu v jednom z následujících bloků adres: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

privátní klíč – private key

Tajná polovina páru kryptografických klíčů, která se používá s algoritmem veřejného klíče. Privátní klíče se obvykle používají k digitálním podpisům dat a k dešifrování dat, která byla zašifrována odpovídajícím veřejným klíčem. Viz též veřejný klíč.

**proces určení trasy
– route determination process**

Proces výběru rozhraní a přenosu adres IP, vycházející z cílové adresy IP datagramu IP a obsahu směrovací tabulky IP.

program Systems Management Server

Část sady produktů Windows BackOffice. Program Systems Management Server (SMS) obsahuje nástroje pro inventarizaci, rozmístění a diagnostiku. Program SMS může významně automatizovat úkoly aktualizace softwaru, umožnit vzdálené řešení problémů, poskytovat cenné informace pro správu, spravovat softwarové licence a sledovat počítače a síť.

program Windows 2000 Redirector

Softwarová součást, která přijímá síťové požadavky a přesměrovává je na síťové servery, pracovní stanice a sdílené adresáře.

prohledávací seznam – browse list

Jakýkoliv seznam položek, který je možné prohlížet, jako seznam serverů v síti nebo seznam tiskáren v průvodci pro přidání tiskárny.

prohledávání WINS – WINS lookup

Proces, kterým žádá server DNS službu WINS o překlad názvů, které nenajde ve svých oprávněných zónách.

prohlížeč, prohlídač – browser

Klientský prostředek pro navigaci a přístup k informacím v síti Internet nebo intranet. V kontextu sítí se systémem Windows, může „browser“ rovněž znamenat službu Computer Browser, která udržuje aktualizovaný seznam počítačů v síti nebo v části sítě a poskytuje ten-

to seznam aplikací, pokud je to vyžádáno. Když se uživatel pokusí připojit k prostředku v doméně, je zavolán prohlížeč domény, aby poskytl seznam dostupných prostředků.

proměnlivá rychlost přenosu – variable bit rate (VBR)

Služba typu ATM, která zaručuje službu, založenou na průměrné a špičkové rychlosti přenosu. VBR se používá pro provoz, který vyžaduje malé nebo žádné ztráty buněk. Přenáší data ve shlucích, nikoliv souvislým proudem

propustnost – throughput

Přenosová kapacita systému disků.

prostředí – shell

Interpret příkazů, který se používá pro předávání příkazů operačnímu systému.

prostý text – plaintext

Data, která nejsou zašifrovaná. Někdy bývá označován názvem jasný text. Viz též šifrovaný text; šifrování; dešifrování.

protokol – protocol

Sada pravidel a konvencí, podle kterých si dva počítače předávají po síti informace. Síťový software obvykle implementuje více úrovní protokolů, které se vrství jedna na druhou. Systémy Windows NT a Windows 2000 obsahují protokoly, kompatibilní s protokoly NetBEUI, TCP/IP, a IPX/SPX.

protokol – Server Message Block (SMB)

Protokol sdílení souborů síťovými počítači, vytvořený pro transparentní přístup k souborům na vzdálených systémech v různých sítích. Protokol SMB definuje sérii příkazů, které předávají informace mezi počítači. Protokol SMB používá zprávy čtyř typů: řízení relace, soubor, tiskárna a zpráva.

protokol Classical IP over ATM (CLIP)

Navrhovaný standard sítě Internet, popsáný ve specifikaci RFC 2225 a dalších specifikacích RFC, který umožňuje komunikaci protokolu IP přímo ve vrstvě protokolu ATM. Viz též asynchronní režim přenosu; Internet Protocol.

protokol Common Internet File System (CIFS)

Protokol a odpovídající rozhraní API, používané aplikačními programy k vyžádání aplikač-

ních služeb vyšší úrovně. Protokol CIFS byl dříve znám jako SMB (Server Message Block).

protokol Data Link Control (DLC)

Protokol používaný hlavně u centrálních počítačů IBM a pro připojení tiskáren.

protokol Dynamic Host Configuration Protocol (DHCP)

Síťový protokol, který poskytuje bezpečné, spolehlivé a jednoduché nastavení sítě TCP/IP a nabízí dynamické nastavování adres Internet Protocol (IP) pro počítače. Protokol DHCP zajišťuje, že nenastávají konflikty adres a pomáhá šetřit použití adres IP centralizovanou správou přidělování adres.

protokol encapsulating security payload (ESP)

Protokol zabezpečení IPsec, který poskytuje důvěrnost navíc k ověřování, integritě a ochraně proti přehrání. Protokol ESP může být použit samostatně, v kombinaci s ověřovací hlavičkou (AH) nebo vnořeně v protokolu Layer Two Tunneling Protocol (L2TP). Protokol ESP obvykle nepodepisuje celý paket, pokud není tunelován – běžně jsou chráněna pouze přenášená data a nikoliv hlavička IP.

protokol File Transfer Protocol (FTP)

Protokol, který definuje, jak jsou přenášeny soubory po síti Internet z jednoho počítače na druhý. FTP je rovněž aplikace typu klient-server, která přenáší soubory s použitím tohoto protokolu.

protokol HTTP

Viz protokol Hypertext Transfer Protocol.

protokol Hypertext Transfer Protocol (HTTP)

Protokol, používaný pro přenos informací v síti World Wide Web. Adresa HTTP (jeden typ adresy Uniform Resource Locator [URL]) má tvar: <http://www.microsoft.com>.

protokol Challenge Handshake Authentication Protocol (CHAP)

Ověřovací protokol typu challenge-response pro připojení PPP, dokumentovaný ve specifikaci RFC 1994, který používá standardní jednosměrné šifrovací schéma Message Digest 5 (MD5) k hashování odpovědi na výzvu vydanou serverem pro vzdálený přístup.

protokol Infrared Data Association (IrDA)

Síťový protokol, používaný k přenosu dat, vytvořených infračervenými zařízeními. Infrared Data Association je rovněž název průmyslové organizace dodavatelů počítačů, součástí a telekomunikací, které stanovuje standardy pro infračervenou komunikaci mezi počítači a periferními zařízeními, jako jsou tiskárny. Viz též infračervený; infračervené zařízení; infračervený port.

protokol Internet Control Message Protocol (ICMP)

Vyžadovaný protokol údržby v sadě TCP/IP, který podává zprávy o chybách a umožňuje jednoduché připojování. Protokol ICMP je používán nástrojem Ping k odstraňování potíží v síti TCP/IP.

protokol Internet Group Management Protocol (IGMP)

Protokol v sadě protokolů TCP/IP, který zodpovídá za správu členství ve skupinách protokolu IP pro vícesměrový přenos.

protokol Internet Protocol (IP)

Protokol ze sady protokolů TCP/IP, používající směrování. Zodpovídá za adresování IP, směrování a fragmentaci a opětovné sestavení paketů IP.

protokol Internet Protocol Control Protocol (IPCP)

Síťový řídicí protokol pro spojení PPP založená na IP. IPCP vyjednává parametry IP pro dynamické nastavení stran PPP, založených na TCP/IP ve spojení point-to-point. IPCP je dokumentováno ve specifikacích RFC 1332 a RFC 1877.

protokol Internetwork Packet Exchange (IPX)

Síťový protokol ze sítě NetWare, řídící adresování a směrování paketů uvnitř a mezi lokálními sítěmi. Protokol IPX nezaručuje, že zpráva bude úplná (bez ztracených paketů). Viz též protokol Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

protokol Internetwork Packet Exchange Control Protocol (IPXCP)

Síťový řídicí protokol pro spojení PPP založená na protokolu IPX. IPXCP vyjednává parametry

IPX pro dynamické nastavení stran PPP, založených na protokolu IPX ve spojení typu point-to-point. Protokol IPXCP je dokumentován ve specifikaci RFC 1552.

protokol Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

Přenosový protokol, používaných v sítích Novell NetWare a v dalších sítích.

protokol LDAP

Viz protokol Lightweight Directory Access Protocol.

protokol Lightweight Directory Access Protocol (LDAP)

Protokol adresářové služby, který je spuštěn přímo nad protokolem TCP/IP a primárním přístupovým protokolem pro službu Active Directory. Protokol LDAP verze 3 je definován v dokumentu Proposed Standard ve specifikaci Internet Engineering Task Force (IETF) RFC 2251. Viz též aplikační programové rozhraní protokolu Lightweight Directory Access Protocol (LDAP API).

protokol NetBIOS Extended User Interface (NetBEUI)

Síťový protokol, součást sítě Microsoft, který je obvykle používán v místních sítích s jedním až 200 klienty. Protokol NetBEUI používá zdrojové směrování Token Ring jako svou jedinou metodu směrování. Jde o implementaci standardu NetBIOS společností Microsoft.

protokol NWLink

Implementace protokolů Internetwork Packet Exchange (IPX), Sequenced Packet Exchange (SPX), a NetBIOS, používaná v sítích Novell. Protokol NWLink je standardním síťovým protokolem, který podporuje směrování a může podporovat aplikace typu klient-server v systému NetWare, kde aplikace založené na soketech systému Netware komunikují s aplikacemi, založenými na soketech IPX/SPX. Viz též protokol Internetwork Packet Exchange (IPX); základní vstupně-výstupní systém sítě (NetBIOS).

protokol Open Shortest Path First (OSPF)

Směrovací protokol, používaný u středních a velkých sítí. Tento protokol je složitější než

protokol RIP, ale umožňuje lepší řízení a je efektivnější při šíření směrovacích informací.

protokol point-to-point

– Point-to-Point Protocol (PPP)

Standardní sada protokolů pro použití ve spojeních typu point-to-point k přenosu víceprotokolových datagramů. Protokol PPP je dokumentován ve specifikaci RFC 1661.

protokol Post Office Protocol

Služba poštovní schránky, která umožňuje klientu přijímat poštu, kterou pro něj má server. Poslední implementací je verze 3, známá jako POP3.

protokol překládání adres – Address Resolution Protocol (ARP)

V protokolu TCP/IP používá všesměrový provoz na lokální síti k překládání logicky přiřazených adres IP na adresy fyzického zařízení nebo adresy vrstvy řízení přístupu k médiím. V protokolu ATM se používá protokol ARP dvěma různými způsoby. Pro protokol Classical IP over ATM se používá protokol ARP k překládání adres na adresy hardware v protokolu ATM. Pro emulaci sítě LAN v protokolu ATM se používá protokol ARP k překládání adres protokolů Ethernet/802.3 nebo Token Ring na adresy hardware protokolu ATM. Viz též řízení přístupu k médiím; Transmission Control Protocol/Internet Protocol.

protokol Resource Reservation Protocol (RSVP)

Signalizační protokol, který umožňuje odesílateli a příjemci v komunikaci nastavit vyhrazenou sběrnici pro přenos dat určenou kvalitou služby.

protokol Routing Information Protocol (RIP)

Sada síťových protokolů, která zabezpečuje komunikaci v propojených sítích, vytvořených z počítačů s různou architekturou hardware a s různými operačními systémy. Protokol TCP/IP zahrnuje standardy pro to, jak počítače komunikují a konvence pro propojování sítí a směrovací provoz. Viz též protokol; protokol Transmission Control Protocol/Internet Protocol (TCP/IP).

protokol Simple Mail Transfer Protocol (SMTP)

Protokol používaný v síti Internet k přenosu pošty. Protokol SMTP je nezávislý na konkrétním přenosovém subsystému a vyžaduje pouze spolehlivý a řazení dodržující kanál proudu dat.

protokol Simple Network Management Protocol (SNMP)

Protokol pro správu sítí, instalovaný v protokolu TCP/IP a široce používaný v sítích TCP/IP a IPX. Protokol SNMP přenáší řídicí informace a příkazy mezi programem pro správu, spuštěným správcem, a agentem správy sítě, spuštěným na hostitelském počítači. Agent protokolu SNMP posílá informace o stavu jednomu nebo více hostitelským počítačům na vyžádání hostitelských počítačů nebo pokud nastane významná událost.

protokol Telnet

Protokol emulace terminálu, který je v síti Internet široce využíván pro přihlašování k síťovým počítačům. Pojem Telnet také označuje aplikaci, která používá protokol Telnet pro uživatele, kteří se připojují ze vzdálených umístění.

protokol Transmission Control Protocol/Internet Protocol (TCP/IP)

Sada softwarových síťových protokolů, široce používaná v síti Internet, která poskytuje komunikaci po propojených sítích počítačů s různou hardwarovou architekturou a s různými operačními systémy. Protokol TCP/IP zahrnuje standardy komunikace počítačů a konvence pro připojování sítí a síťový provoz.

protokol Trivial File Transfer Protocol (TFTP)

Protokol, používaný serverem IntelliMirror ke stahování inicializačních souborů, potřebných pro zahájení spouštění nebo instalace.

protokol tunelového spojení point-to-point – Point-to-Point Tunneling Protocol (PPTP)

Protokol tunelového spojení, který obaluje rámce protokolu point-to-point (PPP) do datagramů IP pro přenos v síti IP (Internet nebo soukromý intranet).

protokol tunelového spojení vrstvy 2 – Layer two Tunneling Protocol (L2TP)

Protokol tunelového spojení, který obaluje rámce PPP, které mají být odeslány pomocí sítí IP,

X.25, Frame Relay nebo ATM. protokol L2TP je kombinací protokolu Point-to-Point Tunneling Protocol (PPTP) a protokolu Layer 2 Forwarding (L2F), jde o technologii navrženou společností Cisco Systems, Inc.

protokol událostí – Event Log

Soubor, ve kterém jsou zaznamenávány položky, protokolující události.

protokol User Datagram Protocol (UDP)

Součást protokolu TCP/IP, která poskytuje službu datagramů bez připojení, která nezaručuje ani doručení ani správné řazení doručovaných paketů.

protokolování událostí – event logging

Proces v systému Windows 2000, kterým se zaznamenávají položky auditu v auditovacím sledu vždy, když se vyskytnou určité události, jako jsou spouštění a ukončování služeb nebo přihlašování a odhlašování uživatelů a přístupy k prostředkům. Prohlížeč událostí můžete použít k získání přehledu o událostech systému Macintosh i událostí systému Windows 2000.

proudový soket – stream socket

Soket, používající rozhraní Windows Sockets API, který poskytuje dvousměrný, spolehlivý, sekvenční a neduplicitní tok dat.

průvodce instalací služby Active Directory – Active Directory Installation wizard

Nástroj systému Windows 2000 Server, který během instalace umožňuje následující činnosti: instalaci Active Directory, vytváření stromů v doménové struktuře, replikaci existujících domén, instalaci ověřovacího modulu Kerberos, povýšení serverů na řadiče domény.

předpona sítě – network prefix

Počet bitů v čísle ID sítě IP, začínající významově nejvyšším bitem. Předpona sítě je jiným způsobem vyjádření masky podsítě.

předsdílený klíč – pre-shared key

Ověřovací technologie, užívaná službou IPSec. Předsdílený znamená, že se strany musí shodnout na síleném tajném klíči, který se stane součástí zásad zabezpečení IPSec. Informace jsou zašifrovány před přenosem použitím sdíleného klíče a dešifrovány na přijímacím konci

použitím téhož klíče. Pokud přijímač dokáže dešifrovat informace, jsou totožnosti považovány za ověřené.

překlad názvu – name resolution

Proces softwarového překladu mezi názvy, které jsou snadno použitelné pro uživatele, a numerickými adresami IP, které jsou pro uživatele obtížné, ale nezbytné pro komunikaci v protokolu TCP/IP. Překlad názvů může být poskytován softwarovými součástmi, jako je systém názvů domén (Domain Name System – DNS) nebo Windows Internet Name Service (WINS). V adresářové službě jde o fázi zpracování adresářové operace LDAP, která vyvolává nalezení řadiče domény, který uchovává cílový záznam pro operaci. Viz též systém Domain Name System (DNS); protokol Transmission Control Protocol/Internet Protocol (TCP/IP); systém Windows Internet Name Service (WINS).

překlad názvů v rozhraní NetBIOS – NetBIOS name resolution

Proces překladu názvu v rozhraní NetBIOS na jeho adresu IP.

překlad názvu všesměrového vysílání – broadcast name resolution

Mechanismus, definovaný ve specifikaci RFC 1001/1002, který používá všesměrového vysílání k překladu názvů na adresy IP procesem registrace, překladu a uvolnění názvu. Viz též datagram všesměrového vysílání; specifikace Request for Comments (RFC).

překladač – resolver

Programy klienta DNS, používané k vyhledávání informací o názvech DNS. Překladače mohou být buď malé („stub“ – omezená sada programových rutin, poskytující základní funkce dotazů) nebo větší programy, které poskytují další vyhledávací funkce klienta DNS, jakou je ukládání do mezipaměti. Viz též ukládání do mezipaměti; překladač s mezipamětí.

překladač s mezipamětí – caching resolver

V systému Windows 2000 jde o klientskou službu překladu názvů Domain Name System (DNS), která ukládá do mezipaměti naposledy zjištěné informace o názvech domén DNS. překladač s mezipamětí poskytuje v celém systému přístup k programům, používajícím službu DNS

pro záznamy prostředků, získané ze serveru DNS během zpracování dotazů na názvy. Data, umístěná v mezipaměti, se používají po omezenou dobu a zastarávají podle aktivní hodnoty Time To Live (TTL). Hodnotu TTL můžete nastavit individuálně pro každý záznam prostředku (RR) nebo použít výchozí nastavení minimální hodnoty TTL, nastavené při spuštění úřadu RR pro zónu. Viz též mezipaměť; ukládání do mezipaměti; interval platnosti; minimální TTL; překladač; záznam prostředku; hodnota Time To Live (TTL).

překladač síťové adresy – network address translator

Směrovač IP, definovaný ve specifikaci RFC 1631, který u přenášených paketů dokáže překládat adresy IP a čísla portů TCP/UDP.

přenášení názvů – name devolution

Proces, kterým služba DNS resolver připojuje jeden nebo více názvů k neúplnému názvu domény, čímž vytváří úplný název domény, a předává úplný název domény serveru DNS.

přenesení – migrate

Proces převodu souborů nebo programů ze staršího formátu nebo protokolu do aktuálnějšího formátu nebo protokolu. Například položky databáze WINS mohou být přeneseny ze statických položek databáze WINS do dynamicky znamenovaných položek protokolu DHCP.

přenosový agent – relay agent

Malý program, který přenáší určitý typ zprávy ostatním v síti. V sítích TCP/IP, se pro přenos paketů IP a propojení hardwaru a softwaru v různých podsítích používají směrovače.

přenosový agent DHCP – DHCP relay agent

Směrovací součást, která přenáší zprávy mezi klienty DHCP a službou DHCP, umístěnými na oddělených sítích.

přepínač – switch

Počítač nebo jiné síťové zařízení, které ovládá směrování a provoz jedné cesty. V clusterech se používá přepínač k připojení hostitelů clusteru ke směrovači nebo jinému zdroji příchozích síťových spojení. Viz též směrování.

přepínač vrstvy 2 – layer 2 switch

Přepínač, který funguje jako vrstva datového spojení v referenčním modelu OSI.

přepínač vrstvy 3 – layer 3 switch

Přepínač, který pracuje na síťové vrstvě referenčního modelu OSI.

přesměrovač – redirector

Viz Přesměrovač systému Windows 2000.

přidružení zabezpečení – security association (SA)

Sada parametrů, která definuje služby a mechanismy potřebné k ochraně zabezpečené komunikace protokolu IP. Viz služba Internet Protocol security (IPSec).

přihlášení – log on

Zahájení používání sítě zadáním uživatelského jména a hesla, jež identifikují uživatele v síti.

přímé doručení – direct delivery

Doručení paketu IP uzlem IP do konečného cíle na přímo připojené síti.

přímé hostování – direct hosting

Vlastnost, která umožňuje počítačům v systému Windows 2000 používat sdílení souborů a tiskáren Microsoft pro komunikaci přes IPX s vynecháním vrstvy NetBIOS.

přímý přístup do paměti – direct memory access (DMA)

Přístup do paměti, který nevyžaduje mikroprocesor. DMA se často využívá pro přímý přenos dat mezi pamětí a periferním zařízením, jakým je například disková jednotka.

připojení TCP – TCP connection

Logické spojení mezi dvěma procesy, používajícími protokol TCP pro výměnu dat.

připojení VPN – VPN connection

Část připojení, ve které jsou zašifrována vaše data.

připojení vyžádaného volání – demand-dial connection

Připojení, které typicky využívá spojení na rozlehlost síť obvodově přepínanou. Spojení je zahájeno, když je vyžadován přenos dat. Připoje-

ní vyžádaného volání bývá typicky ukončováno, pokud nedochází k přenosu dat.

přípona DNS – DNS suffix

Volitelný název nadřazené domény, který může být přidán na konec názvu relativní domény, jenž se používá v dotazech na název nebo při vyhledávání hostitelského počítače. Přípona DNS může být použita pro doplnění jinak úplného názvu v doméně DNS, když selže první pokus dotazu na název.

přípona DNS podle připojení – connection-specific DNS suffix

Přípona DNS specifická pro adaptér na rozdíl od globální přípony specifické pro počítač. Při překládání názvů je připojena k neúplnému názvu. Neúplný název může být jednoduchý název nebo složený název který není zakončen tečkou a nemůže být přeložen jako úplný název domény. Přípony DNS podle připojení mohou být rovněž použity pro registraci názvu počítače.

přirůstkový zónový přenos – incremental zone transfer (IXFR)

Alternativní typ dotazu, který lze použít u některých serverů DNS k aktualizaci a synchronizaci údajů zóny když dojde ke změně zóny. Když je podporován přirůstkový zónový přenos mezi servery DNS, mohou si servery pamatovat a přenášet pouze tyto přirůstkové změny záznamů prostředků mezi každou verzí zóny. Viz též úplný zónový přenos; zóna; zónový přenos.

příznak více fragmentů – more fragments flag

Pole v hlavičce protokolu IP, které udává že za tímto fragmentem následuje více fragmentů.

R

rámec – frame

V synchronní komunikaci jde o balíček informací, přenesený jako jedna jednotka z jednoho zařízení na jiné. Pojem rámec se nejčastěji používá u sítí Ethernet. Rámec je podobný paketu u jiných sítí. Viz též paket.

referenční model propojování otevřených systémů – open systems interconnection reference model

Síťový model, zavedený organizací International Organization for Standardization (ISO) pro podporu vícedodavatelské univerzálnosti. Model Open Systems Interconnection (OSI) je sedmivrstvý konceptuální model, skládající se z aplikační, prezentační, relační, transportní, síťové, linkové a fyzické vrstvy.

registr – registry

V systémech Windows 2000, Windows NT, Windows 98, a Windows 95 je takto nazvána databáze informací o nastavení počítače. Registr je organizován jako hierarchická struktura a skládá se z podstromů a jejich klíčů, podregistrů a položek.

registrace názvů – name registration

Proces registrování názvu počítače názvovým serverem, jako jsou servery DHCP nebo WINS, když se klientský počítač připojuje k síti. Tento proces registrování názvu vytváří položku v databázi, kterou mohou využívat další síťové služby pro nalezení tohoto počítače.

registrované porty – registered ports

Porty v rozsahu od 1024 do 49151.

rekurze – recursion

Jeden ze tří typů postupů pro překlad názvů DNS. V tomto procesu požádá překladač (klient DNS) server DNS o poskytnutí úplné odpovědi na dotaz, která neobsahuje odkazy na další servery DNS. Když klient položí dotaz a požádá server o použití rekurze u odpovědi, účinně přesune pracovní zátěž spojenou s překladem dotazu z klienta na server DNS. Pokud server DNS podporuje a používá rekurzi, kontaktuje další servery DNS podle potřeby (použitím iterčních dotazů ve prospěch klienta), dokud neobdrží konečnou odpověď na dotaz. Tento typ překladu umožňuje, aby klientský překladač byl malý a jednoduchý. Viz též iterace; iteráční dotaz; rekurzivní dotaz.

rekurzivní dotaz – recursive query

Dotaz položený serveru DNS, ve kterém dotazovatel vyžaduje od serveru plné pracovní zatížení a odpovědnost za poskytnutí úplné odpo-

vědi na dotaz. Server DNS pak kladě oddělené iterační dotazy jiným serverům DNS v zájmu dotazovatele pro pomoc s vyplněním rekurzivního dotazu. Viz též iterace; iterační dotaz; rekurze.

rekurzivní dotaz na název – recursive name query

Viz rekurzivní dotaz.

relace – sessions

Logické spojení, vytvořené mezi dvěma hostitelskými počítači pro výměnu dat. Relace obvykle používají sekvenční zpracování a potvrzování, aby data byla posílána spolehlivě.

relační vrstva – session layer

Síťová vrstva, která umožňuje dvěma aplikacím na různých počítačích navázat, používat a ukončit relaci. Tato vrstva stanovuje řízení dialogu mezi dvěma počítači v relaci, určuje, která strana přenáší a také jak dlouho přenáší.

replika – replica

V replikaci služby Active Directory jde o kopii oddílu Active Directory, která je synchronizována replikacemi mezi řadiči domén, které udržují kopie stejného oddílu adresáře. „Replica“ může rovněž označovat složenou sadu oddílů adresářů, udržovanou jedním řadičem domény. Těm se pak specificky říká replika oddílů adresáře respektive replika serveru. Viz též úplná replika; částečná replika.

replikace – replication

Proces kopírování dat z úložiště dat nebo systému souborů na více počítačů, které ukládají stejná data z důvodu synchronizace dat. V systému Windows 2000 dochází k replikaci adresářové služby prostřednictvím replikace služby Active Directory a replikace systému souborů nastává prostřednictvím služby replikace souborů. Viz též replikace služby Active Directory replication; služba replikace souborů; distribuovaný systém souborů.

replikace služby Active Directory – Active Directory replication

Synchronizace replik oddílů adresářů mezi řadiči domén systému Windows 2000. Repliky oddílů adresářů mohou být zapsány na každém řadiči domény kromě replik globálního katalo-

gu. Replikace automaticky kopíruje změny z dané repliky oddílu adresáře na všechny ostatní řadiče domény, které udržují repliku stejného oddílu adresáře. Přesněji řečeno, server nazývaný „cíl“ stahuje změny z jiného serveru, nazývaného „zdroj“. Viz též oddíl adresáře; služba replikace souborů; replikace multimas-ter; replikace.

replikační zpoždění – replication latency

Ve službě Active Directory jde o prodlevu mezi dobou, kdy je provedena aktualizace dané repliky oddílu adresáře s dobou, kdy je provedena u jiné repliky stejného oddílu adresáře. Server nepřijme změny, dokud buď není upozorněn o změně svými sousedy ve stejném sídle nebo vyprší doba pro jeho periodickou replikaci.

režim jádra – kernel mode

Vysoce privilegovaný pracovní režim, v němž má programový kód přístup k hardwaru a do celé paměti včetně paměťového prostoru všech uživatelských procesů a aplikací. Režimu jádra se také říká režim supervizora, chráněný režim nebo Ring 0.

režim Wake-On-LAN

Schopnost ovládat vypínání a zapínání podle událostí v síti, jakými jsou nepřítomnost aktivity sítě nebo odpojení.

RFC

Viz žádost o komentář.

RIP

Viz protokol routing information protocol.

root hints file

Viz soubor odkazů na kořeny.

rozbočovač – hub

Síťové zařízení, spojující komunikační linky do centrálního umístění, poskytujícího společné místo pro připojení všech zařízení v síti.

rozhraní CryptoAPI (CAPI)

Aplikační programové rozhraní (API), které je dodáváno jako součást systému Windows 2000. CryptoAPI poskytuje sadu funkcí, které aplikacím umožňují šifrovat nebo digitálně podepisovat data flexibilním způsobem, přičemž poskytuje ochranu pro soukromé klíče. Skutečně

kryptografické operace jsou vykonávány nezávislými moduly, kterým se říká zprostředkovatelé kryptografických služeb – cryptographic service providers (CSP). Viz též zprostředkovatel kryptografických služeb; soukromý klíč.

rozhraní Fiber Distributed Data Interface (FDDI)

Typ síťového média, navrženého pro použití s optickými vlákny. Viz též LocalTalk; Token Ring.

rozhraní Messaging API (MAPI)

Viz rozhraní Messaging Application Programming Interface.

rozhraní NetBIOS

Viz základní vstupně-výstupní systém sítě.

rozhraní NetBIOS nad protokolem TCP/IP

– NetBIOS over TCP/IP (NetBT)

Vlastnost, která poskytuje programové rozhraní NetBIOS nad protokolem TCP/IP. Používá se pro sledování směrovaných serverů, které používají překlad názvů v rozhraní NetBIOS.

rozhraní Network Driver Interface Specification (NDIS)

Softwarová součást, která poskytuje síťovým protokolům systému Windows 2000 společné rozhraní pro komunikaci se síťovými adaptéry. Rozhraní NDIS umožňuje, aby na jednom síťovém adaptéru pracoval současně více než jeden přenosový protokol.

rozhraní open database connectivity (ODBC)

Aplikační programové rozhraní, které umožňuje databázovým aplikacím přístup k datům z různých existujících zdrojů.

rozhraní služby Active Directory

– Active Directory Service Interfaces (ADSI)

Sada vysokoúrovňových programových rozhraní, která poskytuje jednotnou, konzistentní a otevřenou sadu rozhraní, jež umožňuje klientským uživatelským aplikacím systémů Windows 2000, Windows NT, a Windows 9x přístup k několika síťovým adresářovým službám včetně Active Directory. Rozhraní ADSI poskytuje klientským aplikacím adresářových služeb prostředky pro využití jedné sady rozhraní pro komunikaci s libovolným oborem názvů, který

poskytuje implementaci rozhraní ADSI (poskytovatel).

rozhraní telefonního subsystému

– Telephony API (TAPI)

Aplikační programové rozhraní (API), používané komunikačními programy pro komunikaci s telefonními a síťovými službami. Viz též protokol Internet Protocol.

rozhraní Transport Driver Interface (TDI)

Síťový model v systémech Windows NT a Windows 2000, poskytující obecné rozhraní pro součásti vrstev sítě. Rozhraní TDI netvoří jeden program, ale specifikace protokolu, podle které jsou napsány horní hranice ovladačů zařízení transportního protokolu. Umožňuje softwarovým součástem nad a pod transportní vrstvou smíšený provoz bez přeprogramování.

rozhraní Windows Sockets (Winsock)

Standardní aplikační programové rozhraní používané operačním systémem Microsoft Windows, které poskytuje dvousměrný, spolehlivý, uspořádaný a neduplicitní tok dat.

rozlehlá síť (WAN) – wide area network (WAN)

Komunikační síť, propojující geograficky vzdálené počítače, tiskárny a další zařízení. Síť WAN umožňuje každému připojenému zařízení spolupracovat s jiným zařízením v síti. Viz též místní síť (LAN).

rozpoznávání chyb – error detection

Technika pro rozpoznávání ztráty dat v průběhu přenosu. Umožňuje softwaru obnovit ztracená data žádostí, aby přenášející počítač opakoval přenos.

rychlý přenos zóny – fast zone transfer

Druh přenosu zóny, ve kterém může být v jedné zprávě odeslán více než jeden záznam prostředku.

Ř

řadič domény – domain controller

V doménách systémů Windows NT Server nebo Windows 2000 Server se jedná o server, který ověřuje přihlášení k doméně, zajišťuje zásady zabezpečení a udržuje hlavní databázi účtů zabezpečení domény. v doméně systému Win-

dows 2000 jde o počítač se spuštěným systémem Windows 2000 Server, který spravuje přístup uživatele k síti, což zahrnuje přihlašování, ověřování a přístup k adresáři a sdíleným prostředkům.

řetězení šifrovaných bloků – cipher block chaining (CBC)

Proces, používaný k ukrytí vzorů identických bloků dat uvnitř paketu. Používá se inicializační vektor (náhodné počáteční číslo) jako první náhodný blok k šifrování a dešifrování bloku dat. Pro zašifrování každého bloku se používají různé náhodné bloky ve spojení s tajným klíčem.

řízení provozu – Traffic Control

Mechanismus systému Windows 2000, který vytváří a řídí toky dat s definovanými parametry QoS. Programové rozhraní Traffic Control (TC API) vytváří filtry pro směrování vybraných paketů. Rozhraní Traffic control je vyvoláváno rozhraním QoS a obsluhováno protokolem RSVP SP.

řízení přístupu – admission control

Služba užívaná k řízení správy síťových prostředků ve sdílených segmentech sítě.

řízení přístupu – access control

Bezpečnostní mechanismus v systémech Windows NT a Windows 2000, jenž určuje, které objekty mohou zaregistrované objekty zabezpečení používat a jak je mohou používat. Viz též autorizace; zaregistrovaný objekt zabezpečení.

řízení přístupu k médiím

– media access control

Podvrstva ve specifikaci IEEE 802, která definuje metody přístupu k síti a rámce.

S

SA

Viz přidružení zabezpečení.

sada záznamů prostředků

– resource record set (RRset)

Kolekce více než jednoho záznamu prostředku, vrácená jako odpověď na dotaz serverem DNS. Sady záznamů prostředků (resource record sets

– RRsets) se používají v odpovědích, u kterých je součástí odpovědi více než jeden záznam. Viz též záznam prostředku.

sběrnice Universal Serial Bus (USB)

Sériová sběrnice s šířkou pásma 1,5 megabitů za sekundu (Mbps) pro připojování periferních zařízení k počítači. Sběrnice USB může propojovat až 127 periferních zařízení (například externí jednotky CD-ROM, tiskárny, modemy, myši, klávesnice) se systémem prostřednictvím jednoho víceúčelového portu. Toho se dosahuje řetězovým propojením periferních zařízení mezi sebou. sběrnice USB podporuje připojení za běhu a vícenásobné proudy dat.

sdílení tisku – print sharing

Schopnost počítačů se spuštěným systémem Windows 2000 Professional nebo Windows 2000 Server sdílet tiskárnu v síti.

sdílení zátěže – load sharing

Viz cyklická obsluha.

segment TCP – TCP segment

Veličina, skládající se z hlavičky TCP a k ní přiřazených dat. Segmenty TCP se vyměňují použitím připojení TCP.

sekundární server – secondary server

Oprávněný server DNS pro zónu, který se používá jako zdroj pro replikace zóny dalším serverům. Hlavní sekundární servery obnovují data své zóny přenosem dat zóny z jiných serverů DNS a nejsou schopny provádět aktualizace zóny. Viz též hlavní server; přenos zóny.

sekundární zóna – secondary zone

Kopie zóny, která musí být replikována ze serveru, obsahujícího primární zónu.

selektivní potvrzování

– selective acknowledgement (SACK)

Možnost protokolu Transmission Control Protocol (TCP), která povoluje přijímači znovu vyžádat od vysílače pouze scházející data.

server

Počítač, který poskytuje síťovým uživatelům sdílené zdroje.

server DNS – DNS server

Počítač, na kterém jsou spuštěny serverové programy DNS, obsahující mapování názvů na adresy IP, mapování adres IP na názvy, informace o stromové struktuře domény a další informace. Servery DNS se také pokoušejí překládat dotazy klientů.

server mezipaměti – caching-only server

Názvový server DNS, který pouze provádí dotazy, ukládá odpovědi do mezipaměti a vrací výsledky. Není autoritativní pro žádné názvy a neobsahuje žádné zóny. Ukládá pouze data, která vložil do mezipaměti při překladu dotazů. Viz též ukládání do mezipaměti; názvový server; zóna.

server pro předávání – forwarder

Server DNS, určený dalšími interními servery DNS k předávání dotazů na překládání externích nebo vnějších názvů domén DNS.

server pro síťový přístup – network access server (NAS)

Zařízení, které přijímá spojení PPP a umísťuje klienty v síti, kterou obsluhuje. Server NAS bývá také nazýván terminálovým serverem.

server sítě – site server

Počítač se systémem Windows NT Server, na kterém byl spuštěn program Systems Management Server (SMS). Pokud je na počítači instalován program SMS, je tomuto počítači přiřazena role serveru sítě. Server sítě, který hostí součásti programu SMS, potřebné pro dohled a správu sítě SMS, obvykle provádí další role SMS, včetně serveru součástí, přístupového místa klientů a distribučního místa.

server vzdáleného přístupu – remote access server

Počítač se systémem Windows 2000 Server se spuštěnou službou Routing and Remote Access, nastavený pro poskytování vzdáleného přístupu.

seznam filtrů IP – IP Filter List

Seznam filtrů, kde každý popisuje určitou podmnožinu sítě, která má být zabezpečena jak pro příchodí, tak pro odchodí provoz.

seznam kompatibilního hardwaru – Hardware Compatibility List (HCL)

Seznam zařízení, podporovaných systémem Windows 2000, dostupný na serveru WWW společnosti Microsoft.

seznam pro upozornění – notify list

Seznam, udržovaný primárním serverem pro zónu, jiných serverů DNS, které mají být upozorněny, když dojde ke změnám zóny. Seznam pro upozornění je tvořen adresami IP serverů DNS, nastavených jako sekundární servery pro zónu. Sekundární servery pak mohou zkontrolovat, zda je zapotřebí zahájit přenos zóny. Viz též upozornění DNS.

seznam řízení přístupu – access control list (ACL)

Seznam bezpečnostních ochran, jež se týkají celého objektu, sady vlastností objektu nebo jednotlivé vlastnosti objektu. Existují dva typy seznamů řízení přístupu: volitelný a systémový. Viz též položka řízení přístupu; volitelný seznam řízení přístupu; popisovač zabezpečení; systémový seznam řízení přístupu.

síť Integrated Services Digital Network (ISDN)

Typ telefonní linky, používaný pro zrychlení sítě WAN. Linky ISDN umožňují přenos dat rychlostmi 64 nebo 128 kilobitů za sekundu, zatímco standardní telefonní linky typicky přenášejí rychlostí 28,8 kilobitů za sekundu. Linka ISDN musí být zavedena telefonní společností na straně serveru i na straně vzdáleného klienta. Viz též rozlehlá síť.

síť k okamžitému použití – Network Plug and Play

Kombinace hardwarové a softwarové podpory, která umožňuje počítačovému systému rozpoznat a přizpůsobit se změnám konfigurace hardwaru s malými nebo žádnými zásahy uživatele.

síť LAN

Viz lokální síť.

síť Token Ring

Typ síťového média, které spojuje uživatele v uzavřeném kruhu a používá předávání tokenů pro zpřístupnění sítě uživatelům. Viz též

rozhraní Fiber Distributed Data Interface (FDDI).

síť všesměrového vysílání

Síť, jež podporuje více než dva připojené uzly a má schopnost adresovat jednu fyzickou zprávu všem připojeným uzlům (všesměrové vysílání – broadcast). Příkladem sítě všesměrového vysílání je síť Ethernet.

síťová adresa – network address

Viz číslo ID sítě.

síťová architektura systému

– Systems Network Architecture (SNA)

Komunikační struktura, vyvinutá firmou IBM pro definování síťových funkcí a stanovení standardů, umožňujících počítačům sdílet a zpracovávat data.

síťová trasa – network route

Trasa k určitému číslu ID sítě v síti typu inter-network.

síťová vrstva – network layer

Vrstva, která adresuje zprávy a překládá logické adresy a názvy na fyzické adresy. Určuje rovněž trasu ze zdrojového k cílovému počítači a řídí problémy provozu, jako jsou přepínání, směrování a kontrola a řízení zahlcení paketů.

síťové médium – network media

Typ fyzického zapojení a protokolů nižších vrstev, používaných pro přenos a příjem rámců. Příklady: Ethernet, FDDI, Token Ring.

síťový adaptér – network adapter

Software nebo hardwarová připojovací karta, která spojuje uzel nebo hostitelský počítač k místní síti.

skript – script

Typ programu, složeného ze sady instrukcí pro aplikaci nebo nástroj. Skript obvykle vyjadřuje instrukce užitím syntaxe aplikace nebo nástroje v kombinaci s jednoduchými řídicími strukturami, jako jsou smyčky a výrazy typu if/then. V prostředí Windows se často místo pojmu skript používá pojem dávkový program (batch program).

skupina – group

Kolekce uživatelů, počítačů, kontaktů a dalších skupin. Skupiny lze používat jako kolekce pro zabezpečení nebo rozesílání elektronické pošty. Distribuční skupiny se používají pouze pro elektronickou poštu. Skupiny se zabezpečením lze používat jak pro povolování přístupu k prostředkům, tak jako seznamy pro rozesílání elektronické pošty. V clusteru serverů je skupina kolekcí zdrojů a základní jednotkou překlopení. Viz též místní skupina domény; globální skupina; nativní režim; univerzální skupina.

skupina protokolu IP pro vícesměrový přenos – IP multicast group

Viz hostitelská skupina.

skupina vícesměrového vysílání – multicast group

Skupina hostitelských počítačů v síti TCP/IP, nastavená pro příjem datagramů, zaslaných na určitou cílovou adresu IP. Cílová adresa pro skupinu je sdílená adresa IP třídy D (v rozsahu od 224.0.0.0 do 239.255.255.255). Viz též datagram.

skupinová adresa – group address

Adresa IP typu multicast v rozsahu třídy D od 224.0.0.0 do 239.255.255.255, definovaná nastavením prvních čtyř nejvýznamnějších bitů adresy IP na 1110.

skupiny Diffie-Hellman – Diffie-Hellman Groups

Skupiny, používané pro určení délky základu primárních čísel (klíčové údaje) pro výměnu DH. Síla každého klíče, odvozeného z výměny DH závisí částečně na síle skupiny DH, ze které vycházejí primární čísla.

sledování – tracing

Schopnost součástí služby Routing and Remote Access systému Windows 2000 zaznamenávat vnitřní proměnné součástí, volání funkcí a interakce. Sledování můžete použít při řešení složitých síťových problémů.

sledování sítě – Network Monitor

Nástroj pro zachycování a analýzu paketů, používaný pro sledování síťového provozu. Je obsažen v systému Windows 2000 Server; úplnější verze je však v serveru Systems Management Server.

služba Active Directory

Adresářová služba, která je součástí Windows 2000 Server. Ukládá informace o objektech v síti a zpřístupňuje tyto informace uživatelům a správcům sítě. Active Directory poskytuje uživatelům sítě přístup k povoleným prostředkům v libovolném místě sítě použitím jednoho přihlašovacího procesu. Poskytuje správcům sítě intuitivní hierarchický pohled na síť a jediné místo pro správu všech síťových objektů. Viz rovněž adresář; adresářová služba.

služba agenta zásad protokolu IPSec**– IPSec Policy Agent Service**

Mechanismus systému Windows 2000, který vyhledává informace o zásadách protokolu IPSec a předává je dalším mechanismům protokolu IPSec, které tyto informace vyžadují, aby mohly provádět služby zabezpečení.

služba Berkeley Internet Name Domain (BIND)

Implementace služby Domain Name System (DNS) napsaná pro nejběžnější verze operačního systému UNIX. Software BIND udržuje Internet Software Consortium. Viz též spouštěcí soubor BIND.

služba BIND

Viz služba Berkeley Internet Name Domain.

služba Client Service for NetWare

Služba obsažená v systému Windows 2000 Professional, která umožňuje klientům vytvářet přímá spojení s prostředky na počítačích, provozujících serverový software NetWare 2.x, 3.x, 4.x, nebo 5.x.

služba Cluster service

Clusssvc.exe, primární spustitelný soubor komponenty Windows Clustering, který vytváří server cluster, řídí všechny aspekty jeho činnosti a spravuje databázi clusterů. Na každém uzlu v server clusteru běží jedna instance služby Cluster service.

služba DHCP – DHCP service

Služba, která umožňuje počítači fungovat jako server DHCP a konfigurovat klienty, pracující s protokolem DHCP v síti. Služba DHCP běží na serveru a umožňuje tak automatickou centralizovanou správu adres IP a dalších nastavení konfigurace TCP/IP pro síťové klienty.

služba DNS resolver

Součást protokolu TCP/IP, která zasílá dotazy na systém doménových názvů (Domain Name System – DNS) serveru DNS.

služba Gateway Service for NetWare

Služba, vytvářející bránu, ze které mohou klienti sítě Microsoft prostřednictvím systému Windows 2000 server přistupovat k sítím s jádrem založeným na protokolu NetWare, jako jsou souborové a tiskové služby NetWare.

služba Key Distribution Center (KDC)

Síťová služba, která poskytuje tikety pro relace a dočasné klíče pro relace, používané v ověřovacím protokolu Kerberos. V systému Windows 2000, se spouští služba KDC jako privilegovaný proces na všech řadičích domén. Služba KDC používá službu Active Directory pro správu citlivých informací o účtech, jakými jsou hesla pro uživatelské účty. Viz též ověřovací protokol Kerberos; tiket relace.

služba Line Printer Daemon (LPD)

Služba tiskového serveru, která přijímá dokumenty (tiskové úlohy) z nástrojů line printer remote (LPR), spuštěných na klientských systémech. Viz též nástroj Line Printer Remote (LPR).

služba Novell Directory Services (NDS)

Distribuovaná databáze, udržující informace o všech prostředcích a poskytující přístup k těmto prostředkům v sítích se spuštěným systémem Novell NetWare 4.x a NetWare 5.x.

služba překládání adres víceměrového vysílání – multicast address resolution service (MARS)

Služba pro překládání víceměrových adres IP na adresy ATM klientů, kteří se připojili ke skupině víceměrového vysílání. Služba MARS může pracovat ve spojení se serverem víceměrového vysílání MCS a klienty při šíření víceměrových dat přes spojení typu point-to-multipoint.

služba překladu názvů**– name resolution service**

Služba, vyžadovaná sítěmi TCP/IP k převodu názvu počítače na adresu IP a adresy IP na název počítače. (Lidé používají „popisné“ názvy pro připojení k počítačům; programy používají adresy IP). Viz též internetwork; adresa IP; pro-

tokol Transmission Control Protocol/Internet Protocol (TCP/IP).

služba QoS Admission Control Service

Softwarová služba, která ovládá šířku pásma a síťové prostředky v podsíti, které je přiřazena. Důležitým aplikacím může být přidělena větší šířka pásma, méně důležitým aplikacím menší šířka pásma. Služba QoS Admission Control Service může být instalována na každém síťovém počítači se systémem Windows 2000.

služba Server – Server service

Softwarová součást, která poskytuje podporu vzdáleného volání procedury (RPC) a sdílení souborů, tiskáren a pojmenovaných kanálů. Viz též pojmenovaný kanál; vzdálené volání procedury.

služba vzdáleného přístupu – Remote Access Service (RAS)

Služba systému Windows NT 4.0, která poskytuje vzdálené síťové služby pro vzdálené pracovníky, mobilní pracovníky a správce systému, kteří sledují a spravují servery ve více kancelářích.

služba Windows Internet Name Service (WINS)

Softwarová služba, která dynamicky mapuje adresy IP na názvy počítačů (názvy systému NetBIOS). To umožňuje uživatelům přistupovat k prostředkům podle jejich názvů místo vyžadování adres IP, které jsou obtížně zapamatovatelné. Servery WINS podporují klienty se systémem Windows NT 4.0 a staršími verzemi operačního systému Windows. Viz též služba Domain Name System (DNS).

služba Workstation service

Systémová služba, která poskytuje síťové připojení a komunikaci.

služby Internet Information Services (IIS)

Softwarové služby, které podporují vytváření, nastavování a správu webových serverů, spolu s dalšími funkcemi sítě Internet. Služby Internet Information Services zahrnují protokol Network News Transfer Protocol (NNTP), protokol File Transfer Protocol (FTP) a protokol Simple Mail Transfer Protocol (SMTP). Viz též protokol File Transfer Protocol (FTP); protokol Network

News Transfer Protocol (NNTP); protokol Simple Mail Transfer Protocol (SMTP).

služby Internet Protocol security (IPSec)

Sada standardních kryptografických ochranných služeb a protokolů. IPSec chrání všechny protokoly v sadě TCP/IP a komunikaci v síti Internet použitím protokolu L2TP. Viz též protokol Layer Two Tunneling Protocol (L2TP).

směrovací protokol – routing protocol

Série periodických zpráv nebo zpráv na vyžádání, obsahujících směrovací informace, které jsou vyměňovány mezi směrovači, aby si vyměnily směrovací informace a poskytly odolnost proti chybám. Kromě počátečního nastavení vyžadují dynamické směrovače málo průběžné údržby a proto se hodí pro větší sítě.

směrovací protokol vícesměrového vysílání – multicast routing protocol

Protokoly jako Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF) nebo Protocol Independent Multicast (PIM), používané pro výměnu informací o členství hostitelských počítačů ve vícesměrovém vysílání. Údaje o skupinovém členství se předávají buď explicitně zasláním informace tvaru [adresa skupiny, podsítě] nebo implicitně informováním směrovačů v opačném směru, že ve směru vícesměrového vysílání jsou nebo nejsou členové skupiny.

směrovací smyčka – routing loop

Cesta v propojených sítích pro číslo ID sítě, která se vrací zpět na sebe.

směrovací tabulka – routing table

Databáze tras, obsahující informace o číslech ID sítě, předávající adresy a metriky pro dosažitelné segmenty v propojených sítích.

směrovač – černá díra PMTU – PMTU black hole router

Směrovač, který tiše ztrácí datagramy IP, které vyžadují fragmentaci, když je nastaven příznak nefragmentovat (Don't Fragment – DF) v hlavičce IP na hodnotu 1.

směrovač – router

Síťové zařízení, které pomáhá místním sítím LAN a rozlehlým sítím WAN dosáhnout univer-

zálnosti a propojitelnosti a které dokáže spojit místní síť LAN s různými topologiemi (například Ethernet a Token Ring)

směrovač hromadného prostředkovatele – multiple provider router (MPR)

Softwarová součást, která podporuje požadavky na přesměrování síťového rozhraní Win32 network API a předává je odpovídajícímu přesměrovači.

směrovač internetu – internet router

Zařízení, které spojuje dvě sítě a směruje síťové informace do jiných sítí, obvykle výběrem nejefektivnější trasy přes další směrovače. Viz též směrovač.

směrovač protokolu IP – IP router

Systém, připojený k více fyzickým sítím TCP/IP, který může směrovat nebo doručovat pakety IP mezi sítěmi. Viz též paket; směrovač; směrování; protokol Transmission Control Protocol/Internet Protocol.

směrování – routing

Proces předávání paketů v propojených sítích od zdrojového hostitelského počítače k cílovému hostitelskému počítači.

směrování zdrojů – source routing

Sestavování seznamů sítí nebo směrovačů v hlavičce síťové vrstvy k posílání paketů po konkrétní cestě v propojených sítích.

sniffer

Aplikace nebo zařízení, které dokáže číst, sledovat a zachytávat výměny dat v síti a číst síťové pakety. Pokud nejsou pakety šifrované, poskytuje sniffer úplný pohled na data v paketu.

snížování zátěže – Task Offload

Proces, umožňující síťovým adaptérem zpracovávat úkoly, normálně vykonávané vrstvou přenosu. Tím se u těchto úkolů snižuje zatížení procesoru a zvyšuje průchodnost.

SNMP

Viz protokol Simple Network Management Protocol.

softwarový směrovač – software router

Směrovač, který není vyhrazený pro směrování, ale provádí směrování jako jeden z několika procesů, spuštěných na směrovacím počítači.

soket – socket

Dvousměrný kanál pro přicházející a odcházející data mezi síťovými počítači. Rozhraní Windows Sockets API je síťové programové rozhraní, používané programátory při vytváření programů pro sokety TCP/IP.

soubor Hosts – Hosts file

Lokální textový soubor ve stejném formátu jako soubor 4.3 Berkeley Software Distribution (BSD) UNIX/etc/hosts. Tento soubor mapuje názvy hostitelů na adresy IP. V systému Windows 2000, je tento soubor uložen ve složce %SystemRoot%\System32\Drivers\Etc. Viz též kořenový adresář systému.

soubor Lmhosts – Lmhosts file

Lokální textový soubor, který mapuje názvy systému NetBIOS (běžně používané jako názvy počítačů) na adresy IP pro hostitelské počítače, které nejsou umístěny v místní podsíti. V systému Windows 2000, je tento soubor uložen ve složce SystemRoot\System32\Drivers\Etc.

soubor mezipaměti – cache file

Soubor, používaný serverem Domain Name System (DNS) k předběžnému zaplnění mezipaměti jmen při spuštění služby. Rovněž bývá nazýván souborem odkazů na kořenové servery, protože záznamy prostředků, uložené v tomto souboru, jsou používány službou DNS k pomoci při vyhledávání kořenových serverů, které poskytují odkaz na oprávněné servery pro vzdálené názvy. Pro servery Windows DNS se nazývá soubor mezipaměti Cache.dns a nachází se ve složce %SystemRoot%\System32\Dns. Viz též oprávněný; mezipaměť; kořenový adresář systému.

soubor odkazů na kořenové servery – cache hints file

Viz soubor mezipaměti.

soubor odkazů na kořeny – root hints

Místní informace, uložené na serveru DNS, která poskytuje pomocné záznamy prostředků pro směrování serveru k jeho kořenovým serverům.

Ve službě DNS společnosti Microsoft je soubor odkazů na kořeny uložen pod názvem `Cache.dns`, umístěn je ve složce `\\%SystemRoot%\System32\Dns`. Soubor odkazů na kořeny bývá také označován jako soubor mezipaměti. Viz též oprávněný; obor názvů; kořen; kořenový server; kořenový adresář systému.

soubor protokolu – log file

Soubor, který ukládá zprávy, vydávané aplikací, službou nebo operačním systémem. Tyto zprávy se používají ke sledování provedených operací. Například webové servery udržují soubory protokolu se seznamem všech požadavků, učiněných na server. Soubory protokolu jsou obvykle soubory ASCII a často mají příponu `.log`. V zálohování jde o soubor, který obsahuje záznam o datu, kdy byly vytvořeny pásky a názvy souborů a adresářů, které byly úspěšně zálohovány a obnoveny. Služba Výstrahy a protokolování výkonu rovněž vytváří soubory protokolu.

soubor zóny – zone file

Textový soubor na názvovém serveru DNS, obsahující záznamy prostředků zóny. Viz též zóna.

souborový server – file server

Server, poskytující pro celou organizaci přístup k souborům, programům a aplikacím.

soukromé porty – private ports

Viz dynamické porty.

specifikace toku dat – Flowspec

Parametr provozu, který udává typ požadované kvality služby. Specifikace Flowspec se používá pro nastavení parametrů plánovače paketů.

specifikace Windows Driver Model (WDM)

Specifikace ovladačů vstupně-výstupních zařízení, která podporuje systémy Windows 2000 a Windows 98. Specifikace WDM je založena na architektuře ovladačů `class/miniport`, která je modulární a rozšiřitelná. Specifikace WDM usnadňuje dodavatelům hardwaru podporu zařízení.

spojovací záznam – glue record

Záznam, udávající adresu IP serveru při delegování úřadu pro zónu z jednoho názvového serveru na jiný.

společenství Internet Engineering Task Force (IETF)

Otevřené společenství síťových návrhářů, operátorů, dodavatelů a výzkumníků, zabývající se vývojem architektury Internetu a jeho hladkým provozem. Technickou práci provádějí pracovní skupiny, organizované podle témat (jako například směrování, přenos, zabezpečení) a prostřednictvím seznamů adresátů. Standardy sítě Internet jsou vyvíjeny v žádostech o komentář (Requests for Comments – RFC) společenství IETF, což jsou série poznámek, které rozebírají mnoho aspektů souvisejících s počítači a počítačovou komunikací, s důrazem na síťové protokoly, programy a koncepce.

spoušť – trigger

Sada podmínek, definovaných uživatelem, při jejichž splnění zahájí systém zachycování dat akci jakou může být ukončení zachycování dat, nebo provedení programu nebo příkazového souboru.

spouštěcí protokol – bootstrap protocol (BOOTP)

Sada pravidel nebo standardů, umožňující počítačům vzájemné propojení, užívaná především v sítích TCP/IP pro konfiguraci pracovních stanic bez použití diskových médií. Specifikace RFC 951 a 1542 definují tento protokol. Protokol DHCP je protokol konfigurace spuštění, který používá tento protokol.

spouštěcí soubor BIND – BIND boot file

Konfigurační soubor, používaný servery DNS (Domain Name System), které používají implementace softwarové služby Berkeley Internet Name Domain (BIND). Spouštěcí soubor BIND je textový soubor `Named.boot`, kde jednotlivé řádky v souboru tvoří seznam spouštěcích direktiv, používaných pro spuštění služby, když je spuštěn server DNS. Microsoft DNS server používá ve výchozím nastavení parametry služby DNS, uložené v registru systému Windows 2000, ale umožňuje použití spouštěcího souboru BIND jako alternativu pro čtení nastavení parametrů při spuštění. Viz též služba BIND; spuštění z registru.

spouštění z registru – registry boot

Výchozí možnost spouštění, používaná většinou serverů DNS v systémech Microsoft. Při spouštění z registru je zahájena služba DNS s parametry a jejich hodnotami, které jsou uloženy v registru systému Windows 2000. Jako alternativa nastavení služby DNS po spuštění může být použit spouštěcí soubor Berkeley Internet Name Domain (BIND). Viz též spouštěcí soubor BIND.

správa klíčů – key management

Zabezpečená správa soukromých klíčů pro šifrování veřejným klíčem. Systém Windows 2000 spravuje soukromé klíče a uchovává jejich důvěrnost pomocí rozhraní a zprostředkovatelů kryptografických služeb (CSP). Viz též soukromý klíč; rozhraní; zprostředkovatel kryptografických služeb.

správa názvů – name management

Registrace, dotazování a uvolňování názvů v systému NetBIOS.

správce sítě – network administrator

Osoba, zodpovědná za nastavení a správu radičů domén nebo místních počítačů a účtů jejich uživatelů a skupin, přiřazující hesla a oprávnění a pomáhající uživatelům s problémy se sítí. Administrátoři jsou členy skupiny a mají úplnou kontrolu nad doménou nebo počítačem.

správce služby DHCP – DHCP Manager

Základní nástroj, používaný pro správu serverů DHCP. Správce služby DHCP je nástroj konzoly Microsoft Management Console (MMC), který je přidán k nástrojům pro správu při instalaci služby DHCP.

správce volání – Call Manager

Softwarová součást, která vytváří, udržuje a ukončuje spojení mezi dvěma počítači.

správní konzola SNMP – SNMP Management Console

Rozhraní, kterým správce (uživatel nebo program) provádí správní činnosti.

spuštění – boot

Start nebo restart počítače. Počítač při prvním zapnutí nebo restartu spustí software, který za-

vede a spustí operační systém počítače, jenž připraví počítač k použití.

standard DNS Notify

Revize standardu DNS (RFC 1996), která navrhuje, aby hlavní server zóny oznamoval určitým sekundárním serverům této zóny změny a sekundární servery mohou pak ověřovat, zda potřebují zahájit přenos zóny. Viz též hlavní server; sekundární server.

standard šifrování dat**– Data Encryption Standard (DES)**

Šifrovací algoritmus, který používá 56bitový klíč a mapuje 64bitový vstupní blok na 64bitový výstupní blok. Klíč je zdánlivě 64bitový, ale vždy jeden bit v každém z osmi bajtů je použit jako paritní, z čehož vychází 56 bitů použitelných pro klíč.

stanice připojení – link station

Hardwarové a softwarové součásti uvnitř uzlu, které představují spojení se sousedním uzlem konkrétním připojením.

statické směrování – static routing

Směrování omezené pevnými směrovacími tabulkami, na rozdíl od dynamicky aktualizovaných směrovacích tabulek. Viz též dynamické směrování; směrování; směrovací tabulka.

statický směrovač – static router

Směrovač s ručně nastavenými směrovacími tabulkami. Správce sítě se znalostí topologie propojených sítí manuálně vytváří a aktualizuje směrovací tabulku a programuje všechny trasy ve směrovací tabulce. Statické směrovače mohou dobře fungovat v malých sítích, ale nepřípůsobují se dobře velkým nebo dynamicky proměnlivým sítím z důvodu své manuální správy.

supernetting

Vytváření oboru ID čísel sítě IP použitím jednoho ID čísla sítě IP a masky podsítě. Supernetting je technika sdružování a sumarizace tras.

svazek – volume

Část fyzického disku, která funguje jako by byla fyzicky odděleným samostatným diskem. V Průzkumníku systému Windows se v části

Tento počítač objevují svazky jako lokální disky, jako jsou jednotka C nebo jednotka D.

synchronizační agent Active Directory Connector (ADC)

Synchronizační agent ve Windows 2000 Server, Windows 2000 Advanced Server a Windows 2000 Enterprise Server, který poskytuje automatizovaný způsob udržování konzistentních informací o adresářích mezi adresáři. Bez ADC byste museli manuálně vkládat nová data a změny v obou adresářových službách.

systém Domain Name System (DNS)

Hierarchický systém názvů, používaný pro vyhledávání názvů domén v síti Internet a v soukromých sítích TCP/IP. Systém DNS poskytuje službu pro mapování doménových názvů DNS na adresy IP a naopak. To umožňuje uživatelům, počítačům a aplikacím klást systému DNS dotazy na určení vzdálených systémů úplnými doménovými názvy místo adres IP. Viz též doména; příkaz ping.

systém Security Accounts Manager (SAM)

Chráněný podsystém, který spravuje informace o účtech uživatelů a skupin. V systému Windows NT 4.0 ukládá systém SAM objekty lokálního i doménového zabezpečení do registru. V systému Windows 2000 ukládá systém SAM účty pracovních stanic do registru místního počítače, zabezpečené účty řadiče domény ukládá služba Active Directory.

Š

šifra – cipher

Metoda vytváření skryté zprávy. Šifra se používá k převodu čitelné zprávy, zvané prostý text (někdy též zvané jasný text) do nečitelné, zakódované nebo skryté zprávy, zvané šifrovaný text. Pouze někdo s tajným dekodovacím klíčem může převést šifrovaný text zpět na původní prostý text. Viz též šifrovaný text; prostý text; kryptografie.

šifrovací klíč – encryption key

Bitový řetězec, který je použit ve spojení s šifrovacím algoritmem k šifrování a dešifrování dat. Viz též veřejný klíč; soukromý klíč; symetrický klíč.

šifrování – encryption

Proces utajování zprávy nebo dat způsobem, který ukrývá její obsah.

šifrování symetrickým klíčem – symmetric key encryption

Šifrovací algoritmus, který vyžaduje stejný tajný klíč pro šifrování i dešifrování. Často se mu říká šifrování tajným klíčem. Pro svou rychlost je symetrické šifrování používáno častěji než šifrování veřejným klíčem, pokud odesílatel zprávy potřebuje šifrovat velký objem dat.

šifrovaný text – ciphertext

Text, který byl zašifrován použitím šifrovacího klíče. Šifrovaný text nedává smysl pro nikoho, kdo nemá šifrovací klíč. Viz též dešifrování; šifrování; šifrovací klíč; prostý text.

šířka pásma – bandwidth

Rozdíl mezi nejvyšší a nejnižší frekvencí daného rozsahu v analogových komunikacích. Například telefonní linka poskytuje šířku pásma 3,000 Hz, rozdíl mezi nejnižší (300 Hz) a nejvyšší (3,300 Hz) frekvencí, kterou je schopna přenášet. V digitálních komunikacích jde o rychlost přenosu informací, vyjádřenou v bitech za sekundu (bps).

škálovatelnost – scalability

Měřítko schopnosti rozšíření počítače, služby nebo aplikace v závislosti na rostoucích požadavcích na výkon. Pro cluster serverů schopnost přidat jeden nebo více systémů do existujícího clusteru, pokud celkové zatížení clusteru přesahuje jeho možnosti.

T

T1

Přenos dat rychlostí 1.544 Mbps. Linka T1 bývá také označována jako linka DS-1.

T3

Přenos dat rychlostí 44.736 Mbps. Linka T3 bývá také označována jako linka DS-3.

tajný klíč, důvěrný klíč – secret key

Šifrovací klíč, který společně používají dvě strany a nikdo další. Viz též šifrování symetrickým klíčem.

TCP

Viz protokol Transmission Control Protocol.

TCP/IP

Viz protokol Transmission Control Protocol/Internet Protocol.

terminál – terminal

Zařízení složené z obrazovky monitoru a klávesnice, které slouží ke komunikaci s počítačem.

three-way handshake

Série tří segmentů TCP, které se vyměňují při navázání spojení TCP.

tiché zahazování – silent discard

Situace, kdy je paket zahozen a vysílající hostitelský počítač není informován proč byl zahozen.

tichý RIP – silent RIP

Schopnost počítače poslouchat a zpracovávat hlášení protokolu Routing Information Protocol (RIP) bez ohlašování své vlastní trasy.

tiskový server – print server

Počítač, který je vyhrazen pro správu tiskáren v síti. Tiskovým serverem může být každý počítač v síti.

tok – flow

Proud dat, odesílaný nebo přijímaný hostitelským počítačem. Rovněž bývá označován jako síťový provoz.

topologie – topology

Vztahy mezi sadou síťových součástí v operačních systémech Windows. V kontextu replikace služby Active Directory označuje topologie sadu spojení, kterou používají řadiče domén k replikaci informací mezi sebou. Viz též řadič domény; replikace.

transportní protokol – transport protocol

Protokol, který definuje jak mají být data prezentována další přijímající vrstvě v modelu sítí se systémy Windows NT a Windows 2000 a balíčkuje data tomu odpovídajícím způsobem. Transportní protokol předává data ovladači síťového adaptéru prostřednictvím specifikace rozhraní síťového adaptéru (NDIS) a redirekto-

ru prostřednictvím rozhraní Transport Driver Interface (TDI).

transportní vrstva – transport layer

Vrstva sítě, která obsluhuje rozpoznávání chyb a zotavení z chyb. Když je to nezbytné, mění strukturu dlouhých zpráv zmenšením velikosti paketů pro přenos a jejich zpětným převodem na původní velikost na přijímacím konci. Přijímací transportní vrstva také odesílá potvrzení příjmu.

trvalá trasa – persistent route

Trasy, které nejsou založeny na nastavení TCP/IP a jsou automaticky přidány do směrovací tabulky IP při spuštění protokolu TCP/IP. Znamenány jsou trasy, přidané do směrovací tabulky IP použitím směrovacího nástroje s parametrem příkazového řádku „-p“.

trvalé připojení – persistent connection

Připojení, které je vždy aktivní. Například servery WINS v systému Windows 2000 používají trvalého připojení pro stálé aktualizace svých databází WINS.

třída adresy – address class

Viz třída internetové adresy.

třída adresy sítě Internet – Internet address class

Původní návrh sítě Internet na rozdělení oboru adres IP do definovaných tříd, přizpůsobených sítím různé velikosti. V moderní síti Internet se již třídy adres nepoužívají. Viz adresa IP třídy A; adresa IP třídy B; adresa IP třídy C.

tunel – tunnel

Logická cesta, kterou cestují zapouzdřené pakety tranzitním síťovým propojením.

tunelování – tunneling

Metoda využití infrastruktury propojených sítí jednoho protokolu k přenosu objemu dat (rámců nebo paketů) jiného protokolu.

typ uzlu systému NetBIOS – NetBIOS Node Type

Popis přesného mechanismu, kterým se názvy v rozhraní NetBIOS překládají na adresy IP.

typy možností – option types

Konfigurační parametry klienta, které může přiřadit server DHCP, když nabízí pronájem adre-

sy IP klientovi. Obvykle jsou typy možností umožňovány a nastavovány pro každý obor. Většina možností je předdefinována specifikací RFC 2132, ale je možné použít správce DHCP k definování vlastních možností, pokud je to zapotřebí.

U

událost – event

Každý výskyt význačné události v systému nebo v aplikaci, který vyžaduje, aby byli upozorněni uživatelé nebo aby do byla přidána položka do protokolu.

UDP

Viz protokol User Datagram Protocol.

ukládání do mezipaměti – caching

Ve službě DNS jde o schopnost serverů DNS ukládat informace o oboru názvů domény, zjištěné během zpracování a překladu dotazů na názvy. V systému Windows 2000 je ukládání do mezipaměti dostupné rovněž prostřednictvím služby klienta DNS (resolver) jako způsob, kterým udržují klienti DNS informace o názvech, zjištěných během posledních dotazů. Viz též služba caching resolver.

úklid – scavenging

Proces čištění a odstraňování neplatných nebo zastaralých dat z databáze WINS.

UNC

Viz konvence Universal Naming Convention.

Unicast – jednosměrové vysílání

Adresa, která identifikuje specifický, globálně jedinečný hostitelský počítač.

univerzální skupina – universal group

Skupina v systému Windows 2000, dostupná pouze v nativním režimu, která je platná kdekoliv v doménové struktuře. Univerzální skupina se vyskytuje v globálním katalogu, ale obsahuje především globální skupiny z domén v doménové struktuře. Je to nejjednodušší forma skupiny a může obsahovat další univerzální skupiny, globální skupiny a uživatele odkudkoliv z doménové struktury. Viz též lokální skupina domény; doménová struktura; globální katalog.

úplný duplex – full-duplex

Systém schopný simultánního přenosu informací komunikačním kanálem oběma směry. Viz též duplex; poloduplex.

úplný název domény, úplný doménový název – fully qualified domain name (FQDN)

DNS doménový název, který je stanoven nedvojsmyslně tak, že označuje s absolutní jistotou své umístění ve stromu oboru názvů. Například client1.reskit.com. Úplný doménový název bývá také označován jako úplný název počítače..

úplný název počítače – full computer name

Typ úplného názvu domény (FQDN). Úplný název domény bývá také nazýván úplným názvem počítače. Jeden počítač může být označován více než jedním FQDN. Přesto ale pouze takový úplný název domény, který je zřetězením názvu hostitele a primární přípony DNS je úplným názvem počítače.

úplný zónový přenos – full zone transfer (AXFR)

Standardní dotaz, podporovaný všemi servery DNS k aktualizaci a synchronizaci údajů o zóně, když je zóna změněna. Pokud je vytvořen dotaz DNS jako zvláštní typ dotazu, používající AXFR, jako odpověď dojde k přenosu celé zóny. Viz též přírůstkový zónový přenos (IXFR); zóna; zónový přenos.

úprava velikosti okna TCP – TCP Window Scaling

Použití možnosti protokolu TCP pro vytvoření přijímacího okna TCP o velikosti větší než 65,535 bajtů. Použití úpravy velikosti okna TCP může zlepšit průchodnost protokolu TCP v prostředích s velkou šířkou pásma a dlouhou prodlevou.

určení depeše – trap destination

Správný systém, který přijímá zprávu depeše protokolu SNMP.

uvolnění názvu – name release

Zpráva, odeslaná serveru systému NetBIOS, oznamující, že název domény byl uvolněn a je k dispozici pro použití jiným serverem.

uzel – node

Ve stromových strukturách jde o místo ve stromu, které může mít spoje k jedné nebo více položkám pod sebou. V místních sítích (LAN) jde o zařízení, které je připojeno k síti a je schopno komunikovat s ostatními zařízeními v síti. v clusteru serverů jde o server, který je členem clusteru a má nainstalován software Cluster service. Viz též místní síť.

uzel h – h-node

Typ uzlu systému NetBIOS, který používá hybridu uzlu b a uzlu p k registraci a překladu názvů systému NetBIOS na adresy IP. Počítač s typem uzlu h pokládá dotazy serveru a přechází na všesměrové vysílání pouze tehdy, když přírný dotaz selže. Počítače se systémem Windows 2000 jsou ve výchozím nastavení uzly h.

uzel m – m-node

Typ uzlu v systému NetBIOS, který používá kombinaci komunikací uzlů b a uzlů p pro registraci a překlad názvů systému NetBIOS. Uzel M nejdříve používá všesměrové vysílání pro překlad; pak, pokud je to nezbytné, použije dotaz na server.

uzel p – p-node

Uzel v rozhraní NetBIOS, který pro překlad názvů a adres IP používá komunikaci typu point-to-point názvovým serverem.

uživatelské jméno – user name

Jedinečné jméno, identifikující uživatelský účet ve Windows 2000. Uživatelské jméno účtu musí být jedinečné mezi ostatními názvy skupiny a uživatelskými jmény ve své vlastní doméně nebo pracovní skupině.

uživatelský účet – user account

Záznam, který obsahuje všechny informace, definující uživatele v systému Windows 2000. K nim patří uživatelské jméno a heslo, požadované při přihlášení uživatele, skupiny, ve kterých má uživatelský účet členství a práva a oprávnění, která má uživatel pro použití počítače a sítě a pro přístup k jejich prostředkům. V systému Windows 2000 Professional a členských serverech jsou uživatelské účty spravovány použitím služby Local Users and Groups. V řadičích domén systému Windows 2000 Server jsou uživatelské účty spravovány službou

Microsoft Active Directory Users and Computers. Viz též řadič domény; skupina; uživatelské jméno.

V**vazba – binding**

Proces, kterým jsou spojeny softwarové komponenty a vrstvy. Při instalaci síťové součásti jsou pro tuto součást stanoveny vazební vztahy a závislosti. Vazba umožňuje součastem vzájemnou komunikaci.

vazební databáze – bindery

Databáze v systémech Novell NetWare 2.x a 3.x, která obsahuje organizační a bezpečnostní informace o uživateli a skupinách.

veřejné adresy – public addresses

Adresy IP, přiřazené organizací Internet Network Information Center (InterNIC), které jsou zaručeně globálně jedinečné a dosažitelné v síti Internet.

veřejný klíč – public key

Neutajovaná polovina kryptografického klíče, která se používá s algoritmem veřejného klíče. Veřejné klíče se obvykle používají k ověřování digitálních podpisů nebo k dešifrování dat, zašifrovaných odpovídajícím privátním klíčem. Viz též privátní klíč.

větev – branch

Segment logické stromové struktury, reprezentující složku a všechny další složky v ní obsažené.

vícesměrové vysílání – multicast

Síťový provoz, určený pro sadu hostitelských počítačů, které patří do skupiny vícesměrového vysílání. Viz též skupina vícesměrového vysílání.

vícesměrový protokol DHCP – multicast DHCP (MDHCP)

Rozšíření standardu protokolu DHCP, které podporuje dynamické přiřazování a nastavování adres IP pro vícesměrové vysílání v sítích s protokolem TCP/IP.

virtuální okruh – Virtual Circuit (VC)

Spojení typu point-to-point pro přenos dat. Umožňuje rozsáhlejší ovládání atributů volání,

jako jsou šířka pásma, zpoždění, variace prodlevy a řazení.

virtuální soukromá síť – virtual private network (VPN)

Rozšíření soukromé sítě, které zahrnuje spoje po sdílených a veřejných sítích, například po síti Internet.

vlastní maska podsítě – custom subnet mask

Maska podsítě, která není založena na třídách adres sítě internet. Vlastní masky podsítě se obecně používají při vytváření podsítí.

vlastník – owner

V systému Windows 2000 jde o osobu, která určuje, jak jsou nastavována oprávnění u objektů a může udělovat oprávnění ostatním. V prostředí Macintosh jde o uživatele, zodpovídajícího za nastavení oprávnění pro složku na serveru. Uživatel systému Macintosh, který vytvoří složku na serveru, se automaticky stává jejím vlastníkem. Vlastník může přenést vlastnictví na někoho jiného. Každý svazek na serveru, který je přístupný ze systému Macintosh, má rovněž svého vlastníka.

volitelný seznam řízení přístupu

– discretionary access control list (DACL)

Část popisovače zabezpečení objektu, která uděluje nebo zamítá povolení přístupu k tomuto objektu pro určité uživatele a skupiny. Pouze vlastník objektu může měnit povolení udělovaná nebo zamítaná v DACL; přístup k objektu tedy závisí na vlastnickově uvážení. Viz též řízení přístupu; objekt; seznam řízení auditovaného přístupu; popisovač zabezpečení.

VPN

Viz virtuální soukromá síť

vrstva datového spojení – data-link layer

Vrstva, která balíčkuje čisté bity z fyzické vrstvy do rámců (logicky strukturovaných paketů dat). Tato vrstva zodpovídá za bezchybný přenos rámců z jednoho počítače na druhý. Po odeslání rámce čeká vrstva datového spojení na potvrzení přijímajícího počítače.

vrstva internet – internet layer

Vrstva v modelu TCP/IP DARPA, která zodpovídá za funkce adresování, balíčkování a směrování.

vrstva Secure Sockets Layer (SSL)

Navrhovaný otevřený standard, vyvinutý společností Netscape Communications, pro vytvoření zabezpečeného komunikačního kanálu, bránícího odposlechu kritických informací, jakými jsou například čísla kreditních karet. Umožňuje především bezpečné elektronické finanční transakce v síti WWW, i když je navržen pro práci i v jiných službách sítě Internet.

vrstva síťového rozhraní – network interface layer

Vrstva datového modelu TCP/IP DARPA, která zodpovídá za umísťování paketů TCP/IP v síťovém médiu a příjem paketů TCP/IP ze síťového média. Vrstvě síťového rozhraní se také říká vrstva přístupu k síti.

vstupně-výstupní port – input/output (I/O) port

Kanál, kterým jsou přenášena data mezi zařízením a mikroprocesorem. Port se jeví mikroprocesoru jako jedna nebo více paměťových adres, které může využívat k vysílání a příjmu dat.

všesměrové vysílání – broadcast

Adresa, která je určena pro všechny hostitelské počítače v konkrétním segmentu sítě. Viz též síť všesměrového vysílání.

vyhledávací seznam přípon DNS – DNS suffix search list

Seznam názvů domén, specifikovaný v záložce DNS na stránce Upřesnit nastavení TCP/IP. Během překladu názvů přidává resolver tyto názvy domén jeden po druhém, aby vytvořil úplný název domény.

vyhrazení – reservation

Zvláštní adresy IP uvnitř oboru trvale vyhrazené pro určitého klienta DHCP. Vyhrazení klientů se provádí v databázi DHCP použitím správce DHCP na základě jedinečného identifikátoru zařízení klienta pro každý vyhrazený záznam. Ve službě QoS ACS jde o přidělení síťových prostředků obsažených v rezervačním požadavku protokolu Resource Reservation Protocol (RSVP), spravované službou QoS Admission

Control Service. viz též protokol Dynamic Host Configuration Protocol (DHCP).

výchozí brána

Položka konfigurace protokolu TCP/IP, která je adresou IP přímo dosažitelného směrovače IP. Nastavení výchozí brány vytváří výchozí trasu v tabulce směrování IP.

výchozí maska podsítě – default subnet mask

Maska podsítě, používaná v síti založené na třídách Internet Address Class. Maska podsítě pro třídu A je 255.0.0.0. Maska podsítě pro třídu B je 255.255.0.0. Maska podsítě pro třídu C je 255.255.255.0.

výchozí trasa – default route

Trasa, která se používá, pokud v tabulce směrování nejsou nalezeny žádné jiné trasy pro cíl. Například pokud směrovač nebo koncový systém nemůže najít síťovou trasu nebo hostitelskou trasu pro cíl, použije se výchozí trasa. Výchozí trasa se používá pro zjednodušení nastavení koncových systémů nebo směrovačů. Pro tabulky směrování IP je výchozí trasou trasa v síti s cílem 0.0.0.0 a síťovou maskou 0.0.0.0.

výchozí zóna – default zone

Zóna, ke které jsou ve výchozím nastavení přiřazeni všichni klienti Macintosh v síti.

výměna klíčů – key exchange

Důvěrná výměna tajných klíčů v režimu online, která se běžně provádí u šifrování veřejným klíčem. Viz též šifrování veřejným klíčem.

vynucené obnovení – authoritative restore

Jde o typ operace obnovení v zálohování řadiče domén systému Windows 2000, v němž objekty v obnoveném adresáři jsou považovány za oprávněné a nahrazují (prostřednictvím replikace) všechny existující kopie těchto objektů. Vynucené obnovení lze použít pouze pro replikovaná data stavu systému jako jsou data služby Active Directory a data služby File Replication service. K provedení vynuceného obnovení se používá nástroj Ntdsutl.exe. Viz též nevynucené obnovení; stav systému.

vyrovnávací paměť – buffer

Oblast paměti, používaná pro dočasné ukládání dat, dokud nemohou být použita.

vyrovnávací paměť pro sběr – capture buffer

Maximální velikost zachytávacího souboru. Pokud zachytávací soubor dosáhne maximální velikosti, jsou odstraněny nejstarší rámce, aby vzniklo místo pro novější (fronta FIFO).

vysoká dostupnost – high availability

Schopnost udržet aplikaci nebo službu provozuschopnou a použitelnou pro klienty většinu času.

výstupní filtry – output filters

Filtrování, definující provoz, který smí být odeslán z daného rozhraní.

výtah ze zprávy – message digest

Výsledek o pevné délce, získaný aplikováním jednosměrné matematické funkce, zvané funkce výtahu ze zprávy (message digest function, někdy též hash function nebo hash algorithm) na libovolný objem dat. Pokud dojde ke změně vstupních dat, výsledná hodnota výtahu ze zprávy se rovněž změní. Výtahu ze zprávy se také říká hash. Viz funkce výtahu ze zprávy.

vytváření podsítí – subnetting

Rozdělování adresního prostoru sítě čísla ID sítě TCP/IP do menších síťových segmentů, z nichž každý má své vlastní ID čísla sítě.

vytváření podsítí proměnlivé délky – variable length subnetting

Rozdělování adresního prostoru čísla ID sítě IP do podsítí různých velikostí.

vzájemné ověřování – mutual authentication

Proces, při kterém se volající směrovač sám ověřuje odpovídajícímu směrovači a odpovídající směrovač se ověřuje volajícímu směrovači. Oba konce spojení ověřují totožnost opačného konce spojení. Vzájemné ověřování provádějí ověřovací metody MS-CHAP v2 a EAP-TLS.

vzdálené volání procedury

– remote procedure call (RPC)

Vybavení k předávání zpráv, které umožňuje distribuované aplikaci volat služby, které jsou dostupné na různých počítačích v síti. Používá se při vzdálené správě počítačů.

Zpoždění se někdy označuje jako zpoždění šíření (propagation delay). Viz též replikace multimaster.

vzdálený počítač – remote computer

Počítač, který je přístupný pouze použitím komunikačních linek nebo komunikačního zařízení (síťového adaptéru nebo modemu).

vztah důvěryhodnosti – trust relationship

Logický vztah, stanovený mezi doménami, který umožňuje postupování ověřování, ve kterém důvěřující doména uznává ověření přihlášení k důvěryhodné doméně. Uživatelské účty a globální skupiny, definované v důvěryhodné doméně mohou dostat práva a oprávnění v důvěřující doméně i tehdy, pokud uživatelské účty a skupiny neexistují v adresáři důvěřující domény. Viz též ověřování; doména; dvousměrný vztah důvěryhodnosti.

W

webový server – Web server

Server, který poskytuje možnost vyvíjet aplikace modelu COM a vytvářet rozsáhlá sídla pro Internet a firemní intranety.

WINS

Viz služba Windows Internet Name Service.

WINS proxy

Počítač, který naslouchá vysílaným dotazům na názvy a odpovídá pro názvy, které nejsou v místní podsíti. Server proxy komunikuje se serverem WINS při překladu názvů pak je na určenou dobu ukládá do mezipaměti. Viz též služba Windows Internet Name Service (WINS).

Z

zabezpečovací metoda – security method

Proces, který určuje zabezpečovací služby, nastavení klíčů a algoritmy, které se použijí k ochraně dat během komunikace IP.

základní disk – basic disk

Fyzický disk, který obsahuje primární oddíly nebo rozšířené oddíly s logickými jednotkami, používanými systémem Windows 2000 a všemi verzemi systému Windows NT. Základní disky mohou rovněž obsahovat sady svazků, zrcadle-

né a prokládané sady nebo svazky typu RAID-5, které byly vytvořeny systémem Windows NT 4.0 nebo starším. Na základní disky lze přistupovat ze systémů MS-DOS, Windows 95, Windows 98, a všech verzí systému Windows NT, pokud je použit kompatibilní formát souborů.

základní vstupně-výstupní systém sítě – network basic input/output system (NetBIOS)

Aplikační programové rozhraní, které může být použito aplikacemi v místní síti nebo počítačích se spuštěným systémem MS-DOS, OS/2, nebo s některými verzemi systému UNIX. Rozhraní NetBIOS poskytuje jednotnou sadu příkazů pro vyžadování síťových služeb nižší úrovně.

záložní řadič domény – backup domain controller

V systému Windows NT Server 4.0 a dřívějších jde o počítač se systémem Windows NT Server, který přijímá kopii databáze adresářů domény (která obsahuje všechny informace o účtech a zásadách zabezpečení domény). Kopie se periodicky synchronizuje s hlavní databází na primárním řadiči domény. záložní řadič domény rovněž ověřuje uživatelské přihlašovací informace a může být povýšen do funkce primárního řadiče domény, pokud je to zapotřebí. V doméně systémů Windows NT 3.51 a 4.0 může existovat více záložních řadičů domény. záložní řadiče domény se mohou podílet na doméně systému Windows 2000, pokud je tato doména konfigurována ve smíšeném režimu. Viz též smíšený režim; primární řadič domény.

zapínání OnNow Power Initiative

Systémový přístup k řízení spotřeby. Všechny součásti mohou být okamžitě zapnuty nebo vypnuty a spolupracovat s hardwarovými a softwarovými součástmi při změně jejich stavu zapnutí jak vyžaduje využití systému.

zápis předpony sítě – network prefix notation

Praxe vyjadřování masky podsítě jako síťové předpony místo desítkového zápisu s tečkami.

zapouzdření – encapsulation

Viz tunelové propojení.

**zaregistrovaný objekt zabezpečení
– security pal**

Držitel účtu, jaký je například uživatel, počítač nebo služba. Každý zaregistrovaný objekt zabezpečení v doméně systému Windows 2000 je označen jedinečným číslem ID zabezpečení (security ID – SID). Když se zaregistrovaný objekt zabezpečení přihlásí k počítači se spuštěným systémem Windows 2000, místní úřad zabezpečení (LSA) ověřuje uživatelské jméno a heslo zaregistrovaného objektu zabezpečení. Pokud je přihlášení úspěšné, vytvoří systém přístupový token. Každý proces, prováděný pro tento zaregistrovaný objekt zabezpečení bude mít kopii jeho přístupového tokenu. Viz též přístupový token; číslo ID zabezpečení; název zaregistrovaného objektu zabezpečení.

zásady skupiny – Group Policy

Nástroj správce pro definování a ovládání toho, jak programy, síťové prostředky a operační systém pracují pro uživatele a počítače v organizaci. V prostředí služby Active Directory se zásady skupiny používají u uživatelů nebo počítačů na základě jejich členství v sídle (site), doménách nebo organizačních jednotkách.

zásady vyjednávání – negotiation policy

Pojmenovaná kolekce zabezpečovacích metod v pravidle, obsaženém v zásadách zabezpečení protokolu Internet Protocol, používaná ke stanovení přidružení zabezpečení mezi dvěma komunikujícími stranami. Viz též zásady zabezpečení protokolu Internet Protocol.

zásady zabezpečení IP**– Internet Protocol security policy**

Vynucuje zabezpečení protokolu Internet Protocol určením, které zabezpečovací služby se použijí k ochraně dat pro koho je určena správa zabezpečení IP k spravování zásad zabezpečení IP. Viz též zabezpečení IP.

záznam prostředku – resource record (RR)

Informace v databázi DNS, kterou lze využít při zpracování dotazů klientů. Každý server DNS obsahuje záznamy prostředků, které potřebuje k zodpovídání dotazů na část oboru názvů DNS, pro kterou je oprávněn.

záznam prostředku A – A resource record

Viz záznam prostředku adresy.

záznam prostředku adresy**– address (A) resource record**

Záznam prostředku, používaný k mapování názvu domény systému DNS na hostitelskou adresu IP v síti. Viz též záznam prostředku.

záznam prostředku názvového serveru (NS)**– name server (NS) resource record**

Záznam prostředku, používaný v zóně k určení doménových názvů DNS pro oprávněné servery DNS pro zónu. Viz též záznam prostředku.

záznam prostředku NS (název serveru)**– NS (name server) resource record**

Viz záznam prostředku název serveru (NS).

záznam prostředku PTR**– PTR (pointer) resource record**

Viz záznam prostředku ukazatele (PTR).

záznam prostředku služby (SRV)**– service (SRV) resource record**

Záznam prostředku, používaný v zóně k registraci a nalezení dobře známých služeb TCP/IP. Záznam prostředku SRV je popsán ve specifikaci RFC 2052 a používán systémem Windows 2000 k nalezení řadičů domény pro službu Active Directory. Viz též záznam prostředku.

záznam prostředku SOA**– SOA (start of authority) resource record**

Viz záznam prostředku start of authority (SOA).

**záznam prostředku SRV – SRV (service)
resource record**

Viz záznam prostředku služby (SRV).

záznam prostředku start of authority (SOA)**– start of authority (SOA) resource record**

Záznam, udávající výchozí bod autority pro informace, uložené v zóně. Záznam prostředku SOA je první záznam prostředku, který se vytváří při přidávání nové zóny. Obsahuje rovněž několik parametrů, používaných ostatními k určení, jak dlouho budou jiné servery DNS používat informace o zóně a jak často jsou vyžadovány aktualizace. Viz též oprávněný; zóna.

záznam prostředku ukazatele (PTR)**– pointer (PTR) resource record**

Záznam prostředku, používaný v zóně zpětného vyhledávání, vytvořený uvnitř domény in-addr.arpa. ke stanovení zpětného mapování adresy IP hostitelského počítače na název domény DNS hostitelského počítače. Viz též záznam prostředku.

zjištění největší přenosové jednotky cesty**– path maximum transmission unit discovery**

Proces zjišťování největšího datagramu IP, který může být poslán po cestě bez fragmentace.

zjištění PMTU – PMTU Discovery

Viz zjištění největší přenosové jednotky cesty.

zjišťování – discovery

Proces, kterým se služba přihlášení k síti systému Windows 2000 pokouší najít řadič domény se systémem Windows 2000 Server v důvěryhodné doméně. Řadič domény je , poté co byl zjištěn, použit pro další ověřování uživatelského účtu. Ve službě SNMP představuje dynamické zjišťování identifikaci zařízení, připojených k síti SNMP.

zjišťování mrtvých bran – dead gateway detection

Postup protokolu TCP/IP ve Windows 2000, který slouží ke změně výchozí brány na další výchozí bránu v seznamu nastavených výchozích bran, když určitý počet spojení opakovaně odesílá segmenty.

zjišťování směrovačů – router discovery

Použití zpráv protokolu Internet Control Message Protocol (ICMP) k zajištění odolnosti proti chybám pro nastavení výchozí brány hostitelského počítače.

zjišťování směrovačů ICMP**– ICMP router discovery**

Viz zjišťování směrovačů.

zóna – zone

V databázi DNS, je zóna souvislou oblastí stromu DNS, která je spravována jako jedna oddělená entita serverem DNS. Zóna obsahuje záznamy prostředků pro všechny názvy uvnitř zóny. V prostředí Macintosh je zóna logickým seskupením, které zjednodušuje procházení sí-

ťových prostředků, jakými jsou servery a tiskárny. To se podobá doméně v sítích se systémem Windows 2000 Server. Viz též doména; služba Domain Name System (DNS); server DNS.

zóna odkazů WINS – WINS referral zone

Zóna, která odkazuje dotazy DNS na službu WINS.

zóna zpětného vyhledávání**– reverse lookup zone**

Zóna, obsahující informace potřebné pro provádění zpětného vyhledávání. Viz též zpětné vyhledávání.

zóna zpětného vyhledávání v podsíti**– subnetted reverse lookup zone**

Zóna zpětného vyhledávání, oprávněná pouze pro část síťových adres třídy C. Zóny zpětného vyhledávání v podsíti nejsou požadovány ani u sítí s podsítěmi; jsou pouze správním volbou. Viz též zóna zpětného vyhledávání.

zónový přenos – zone transfer

Proces, kterým servery DNS spolupracují při údržbě a synchronizaci autoritativních údajů o názvech. Pokud je server DNS nastaven jako sekundární server zóny, posílá periodicky dotazy na hlavní server DNS, nastavený jako jeho zdroj pro zónu. Pokud se verze zóny, uložené na hlavním serveru, liší od verze, uložené na sekundárním serveru, stáhne sekundární server údaje o zóně z hlavního serveru DNS a aktualizuje údaje o zóně. Viz též úplný zónový přenos (AXFR); přírůstkový zónový přenos; sekundární server; zóna.

zosobnění – impersonation

Okolnost, která nastává, když systém Windows NT nebo Windows 2000 umožní jednomu procesu převzít atributy zabezpečení jiného procesu.

zpětná doména – reverse domain

Zvláštní doména, nazvaná in-addr.arpa, která se používá pro mapování adres IP na názvy (označováno jako zpětné vyhledávání).

zpětné vyhledávání – reverse lookup

Dotaz, ve kterém je zadána adresa IP k určení názvu DNS pro počítač.

zpráva depeše – Trap message

Výstražná zpráva protokolu SNMP.

zpráva všesměrového vysílání**– broadcast message**

Síťová zpráva, odeslaná z jednoho počítače, která je distribuována všem dalším zařízením ve stejném segmentu sítě, ve kterém se nachází odesílající počítač.

zprostředkovatel kryptografických služeb**– cryptographic service provider (CSP)**

Nezávislý softwarový modul, který provádí kryptografické operace jako jsou výměna tajného klíče, digitální podepisování dat a ověřování veřejného klíče. Každá služba nebo aplikace systému Windows 2000 může vyžádat kryptografické operace od CSP. Viz též rozhraní CryptoAPI.

zprostředkující systém – intermediate system

Síťové zařízení se schopností předávat pakety mezi částmi sítě. Mosty, přepínače a směrovače jsou příklady zprostředkujících systémů.

Ž**žádost o komentář****– Request for Comments (RFC)**

Dokument, definující standard. Dokumenty RFC jsou publikovány sdružením Internet Engineering Task Force (IETF) a dalšími pracovními skupinami.

Rejstřík

A

Active Directory, 290, 299, 341
 adresa IP, 137
 – je lokální, 128
 – je vzdálená, 128
 – oslovování směrovače (Router Solicitation Address), 691
 – všesměrového vysílání (Broadcast Address), 690
 adresový obor, 36
 adresy IPX, 602
 agent protokolu SNMP, 717
 – zásad, 525
 – zásad IPSec, 500
 agenti, 590
 akce filtrů, 512
 aktualizace databáze DHCP, 201
 – starších klientů, 470
 – záznamů v mezipaměti ARP, 62
 algoritmus Nagle, 85
 – pomalého spuštění, 84
 APIPA, 217
 aplikace, 89
 aplikační vrstva, 488, 611, 693
 architektura Microsoft TCP/IP, 57
 – protokolu SNMP, 597
 – rozhraní Winsock, 635
 – TCP/IP, 9
 Arp, 105
 ATM, 556
 automatická konfigurace klienta, 99
 – partnerských serverů, 459
 autorizace serverů DHCP, 204

B

bezpečnost klíče, 487
 BOOTP, 193
 brána, 128

C

centralizované soubory LMHOSTS, 724
 certifikát veřejného klíče, 493
 cesta k tabulce MTU Plateau Table, 689
 – rozšíření (Extensions Path), 687
 CIDR (Beztrídové mezidoménové směrování), 69
 CIDR (Classless Interdomain Routing), 35
 clustering – seskupování, 413
 – serverů DHCP, 205
 Common Internet File System, 651
 Component Object Model, 647

Č

časová hodnota obnovení (T1) (Renewal Time Value (T1)), 703
 – razítka protokolu TCP, 80
 časovače, 423
 časový limit mezipaměti ARP (ARP Cache Time-Out), 692
 – server (Time Server), 683
 černé díry, 149
 činitelé propustnosti, 88
 čísla protokolů, 662, 669
 číslo verze, 438
 čištění databáze, 420

D

databáze DHCP, 189
 – WINS, 417
 datagramové služby rozhraní NetBIOS, 98
 datagramy, 19
 dědictví rozhraní NetBIOS, 392
 dědičnost zásad, 510
 delegace beztrídové zóny, 296
 delegovaná zóna, 342
 délka života záznamu, 330
 délky klíčů, 497
 denní audit, 230

- spouštění, 403
- depeše, 594
- desítkový zápis, 24
- detekce duplikovaných adres IP, 67
- média, 620
- diagnostika problémů, 72
- diskový hardware, 415
- DNS Resolver Cache Service, 101
- server, 41
- doba zapůjčení adresy IP (IP Address Lease Time), 700
- dodavatelé, 697
- Domain Name System, 750
- doména, 272
- služby Active Directory, 343
- doménové názvy, 39, 241
- dotaz na název, 349
- dotazy, 348
- DNS, 277
- duplicitní replikace, 463
- duplikované adresy IP, 142
- dynamická aktualizace, 216, 263, 311
- aktualizace klienta DNS, 100
- dynamické členství, 188
- překlíčování, 496
- směrovače IP, 49

E

Error 53 (Chyba 53), 132

F

filtr zásad (Policy Filter), 688

filtrování paketů, 144

- paketů IP, 511
- protokolu TCP/IP, 101

filtry, 511

Finger, 672

firewall, 444

Ftp, 672

fyzická adresa, 50

- vrstva, 608

H

hardware pro síťové rozhraní, 415

hierarchie zásady, 564

hlavní prohlížeč (Master Browser), 738

- prohlížeč domény, 738

hodiny serveru, 425

hodnota doby obnovení vazeb (T2) (Rebinding Time Value (T2)), 703

- TTL, 320

hostitel, 270

hostitelský počítač IP, 688

Hostname, 106

CH

chování serveru, 331

chybné pakety SPI, 522

chybové kódy RSVP, 573

I

ID hostitele, 22

- oboru rozhraní NetBIOS (NetBIOS Scope ID), 696
- síť, 22

identifikátor serveru (Server Identifier), 701

identifikátory objektů, 716

informace o třídě uživatele (User Class Information), 699

inicializace, 167

instalace služby DHCP, 199

- součástí IPSec, 526

integrované ukládání, 300

interaktivní příkazy, 678

Internet Authentication Service, 600

interoperabilita, 468

intranet, 521

IP adresování, 19

- Forwarding Enable/Disable, 688
- na odesílajícím hostiteli, 48
- na směrovači, 48

Ippconfig, 106, 222

iterativní dotazy, 248

J

jakostní aplikace, 552

jedinečný identifikátor klienta (Client Unique Identifier), 703

jednotka MTU rozhraní (Interface MTU), 690

- PMTU, 70, 149

jednotky MTU, 149

K

klasifikátor paketů (Msgpc.sys), 536
klíče registru služby DHCP, 152
– DNS, 153
– Simple TCP/IP Services, 152
– SNMP, 152
– TCP/IP Printing, 152
– WINS, 152
klíčové slovo #DOM, 728
– #INCLUDE, 730
– #MH, 729
– #PRE, 727
– #SG, 729
klient služby DHCP, 161
klienti BOOTP, 193
– WINS své názvy, 397
klientské přenosy, 457
– služby, 99
knihovna Windows Sockets, 76
knihovny pomocných modulů, 637
kódování, 500
kolize názvů, 308
komprimace databáze serveru DHCP, 234
komprimování databáze WINS, 420
komunikace mezi procesy, 646
– protokolu TCP/IP, 127
komunity, 594
konec (End Option), 682
konfigurace DNS, 134
– klienta, 405
– protokolu TCP/IP, 137
– sítě, 464
– tabulky BOOTP, 195
– WINS, 136
konfigurační nastavení replikace, 458
konflikt názvů, 321
konflikty adres, 178
– klientů, 401
– ze strany klienta, 179
– ze strany serveru, 178
kontrola konzistence, 422
kontroly disku, 230
konvergence replikace, 461
konzola DNS, 363

kopírování souborů, 676
kořenová cesta (Root Path), 687
kořenové servery, 259
kvalita služby, 628

L

linková vrstva, 609
lokální databáze, 42

M

MAC adresa, 128
malé sítě, 207
Management Information Base, 591
mapování statických adres, 450
maska podsítě (Subnet Mask), 682
masky podsítí, 23
maximální velikost znovu sestaveného datagramu, 689
– velikost zprávy (Maximum Message Size), 702
Maximum Datagram Reassembly Size, 689
mezipaměť, 249
– ARP, 62, 140
Microsoft, 706
minimalizace počtu serverů WINS, 414
mobilní domácí agenti IP (Mobile IP Home Agents), 695
model DCOM, 647
– IPsec, 507
– OSI, 608
modul místních zásad, 562
modulu NetShell, 478
moduly emulátorů, 634
možnost FQDN, 326
možnosti informace, 182
– konfigurace, 187
– linkové vrstvy, 692
– protokolu, 182
– rozhraní NetBIOS pro TCP/IP, 696
mrtvá brána, 82
Multimaster, 299

N

nadsítě, 35
nalezení počítačů a služeb, 722

- nastavení dotazů, 283
 - portů SNMP, 599
 - služby DNS, 367
 - nástroj ARP, 61
 - IPConfig, 137, 361
 - Nslookup, 358
 - Route, 65, 123
 - Rsh, 678
 - nástroje, 576
 - služby SNMP, 601
 - název domény DNS, 686
 - NIS (NIS Domain Name), 694
 - NIS+ (NIS+ Domain Name), 695
 - název hostitelského počítače (Host Name), 686
 - serveru TFTP (TFTP Server Name), 700
 - spouštěcího souboru (Boot File Name), 700
 - názvový server IEN (IEN Name Server), 684
 - server NetBIOS (NetBIOS Name Server), 696
 - názvy systému NetBIOS, 476
 - typu NetBIOS, 92
 - Nbtstat, 108
 - NDIS a TCP/IP, 58
 - neautorizované servery, 204
 - nedefinované možnosti, 704
 - nedůvěryhodné domény, 459
 - největší přenosová jednotka (MTU), 60
 - nelze se připojit k serveru, 145
 - nepovinná zpráva (Optional Message), 702
 - nepřátelské servery DHCP, 203
 - nepřímé doručení, 45
 - nesprávná odpověď, 375
 - nesprávné přiřazení zásady IPsec, 522
 - NetBIOS pro TCP/IP, 91
 - Netdiag, 109
 - NetMon, 578
 - Netstat, 113
 - Nonlocal Source Routing Enable/Disable, 688
 - Nslookup, 116
- O**
- obecná konfigurace, 210
 - obecně používané služby, 666
 - objekty podsítě v konzole QoS ACS, 565
 - obnova dat serveru, 231
 - obnovení, 169
 - dat pomocí replikace, 419
 - klíče relace, 505
 - vazeb, 170
 - obnovování zápůjčky, 171
 - obor doménových názvů, 240
 - názvů, 344
 - odebírání oborů, 178
 - odkládací server (Swap Server), 687
 - odmítnutí služby, 487
 - odolnost proti chybám, 213
 - serveru WINS proti chybám, 415, 462
 - odstraňování problémů, 521
 - zón, 305
 - ochrana, 489
 - klíče, 504
 - zpráv SNMP, 599
 - okamžitá replikace, 309
 - okna protokolu TCP, 77
 - okružní cesta, 628
 - opakovaný přenos, 83
 - operační stav serveru WINS, 446
 - systém, 341
 - opětná instalace protokolu TCP/IP, 151
 - opožděná potvrzení, 79
 - oprava databáze WINS, 418
 - ověřovací záhlaví, 497
 - ověřování, 513
 - ovladače miniportů, 623
 - rozhraní NDIS, 622
 - označování paketů, 537
 - oznámení prohledávačů, 741
- P**
- parametr rezerva, 90
 - parametry stárnutí, 328
 - úklidu, 332
 - vyhledávání WINS, 336
 - PathPing, 119, 138, 143, 576
 - Perfect Forward Secrecy, 506
 - Ping, 121, 138
 - plánovač paketů QoS (Psched.sys), 537
 - plánování oboru názvů, 346
 - pro protokol DHCP, 195
 - zón, 295
 - počet bitů hostitele, 26

- počítač, který není prohlížečem (Non-Browser), 737
- podpis paketu, 498
- podpora klientů BOOTP, 192
 - režimu shlukového zpracování, 413
 - služby MADCAP, 188
 - velkých oken, 627
- pod síť, 23, 470, 690
 - s různou délkou, 33
- pojmenované kanály, 651
- porty, 662
- poskytovatel masky (Mask Supplier), 691
- poskytovatelé překladů názvů rozhraní, 638
- posunutí času (Time Offset), 683
- poškození údajů, 232
- poštovní přihrádka, 650, 651
- potenciální prohlížeč (Potential Browser), 737
- požadavek, 167
- požadavky prohlížeče, 744
- pravidla, 510
- pravidlo 80/20, 173
- prezentační vrstva, 611
- priorita možností, 187
- priority podsítě, 287
- problémy databázových souborů protokolu TCP/IP, 151
 - klientů DHCP, 222
 - protokolu ARP, 147
 - překladového přemostění, 148
 - s bránami, 147
 - s dynamickou aktualizací, 385
 - s nesprávnými určujícími daty, 377
 - s rekurzí, 378
 - se serverem DNS, 376
 - se zabezpečenou dynamickou aktualizací, 386
 - se zónovým přenosem, 380
 - serverů DHCP, 223
 - směrování IP, 145
- proces ARP, 51
 - zápůjčky, 164
- prodloužená vypnutí, 404
- prohlídací počítače, 735
- prohlížeč událostí, 362, 602
- prostředník, 487
- protokol AppleTalk, 631
 - ARP (Address Resolution Protocol), 13, 61
 - ARP pro adresu brány, 132
 - ATM, 628
 - DHCP, 157
 - DLC, 632
 - DNS, 362
 - ICMP (Internet Control Message Protocol), 13, 69
 - IGMP (Internet Group Management Protocol), 14, 75
 - IP, 12
 - IP nad sítí ATM, 69
 - IPSec, 522
 - NetBEUI, 631
 - NWLink, 631
 - rezervace prostředků, 638
 - RSVP (Resource reservation Protocol), 73, 544
 - síť Internet (Protokol IP), 63
 - TCP (Transmission Control Protocol), 15, 77, 693
 - UDP (User Datagram Protocol), 16, 88
- protokolovací server (Log Server), 684
- protokolování auditu DHCP, 229
- protokoly IrDA, 632
 - RSVP, 572
 - TCP/IP, 11
- prověření cest, 147
- průvodce instalací služby Active Directory, 291
 - nastavením serveru DNS, 292
- předběžné sdílení klíče, 494
- předdefinovaná pravidla, 518
- předdefinované akce filtru, 519
- překlad adres, 39
 - adresy IP na adresu MAC, 141
 - názvu, 89, 247, 275, 368, 749
- překlad názvů a adres, 89
 - DNS, 276
 - hostitele, 39
 - hostitele na adresu IP, 128
 - na adresu IP, 127
 - NetBIOS, 393
 - RPC, 650
- překladač pro Windows 2000, 275
 - událostí SNMP, 597
- přenos, 537
- přenosový agent, 209, 221

přeplnění možnosti (Option Overload), 700
přesměrovací symboly, 677
přesměrovač Windows 2000 Redirector, 656
přesun databáze serveru DHCP, 234
přijímání odpovědí od nedotázaných serverů, 289
příkaz Nbtstat -RR, 405
– Ping, 140, 151
– Rexec, 677
přímé doručení, 45
připojení k síti, 138
přírůstkový zónový přenos, 262
přirazování názvu NetBIOSu, 43
přístup ke vzdálenému souboru, 657
– na síť internet, 344
push bit, 90

Q

QoS v systému Windows 2000, 552
Qossp.aid, 583
Qtcp, 581
Quality of Service, 530

R

Rapilib.aid, 583
Rcp, 674
Readpol, 582
registr, 601
registrace a šíření, 752
– názvů skupin, 407
registrované porty, 665
rekurzivní dotazy, 248
relace, 19
– rozhraní NetBIOS, 98
relační vrstva, 611
replikace, 419
– multimaster, 308
– WINS, 430
Resource Reservation Protocol, 539
restartování klienta DHCP, 171
Rexec, 677
rezervace názvů, 323
režim Wake-On-LAN, 620
RFC, 55
role v systému prohlížečů, 736

Routing and Remote Access, 210
rozdělování sítě, 26
rozhraní aplikací TCP/IP, 17
– IP, 690
– NDIS a další, 58
– NetBIOS, 18, 96
– NetBIOS API, 644
– QoS API, 534
– síťového ovladače, 618
– síťových aplikací, 89
– telefonního subsystému, 641
– Windows Sockets, 18
– Winsock API, 634
– WNet API, 645
– zpracování zpráv, 645
rozpoznání média (Media Sense), 100
rozsahy adres víceměrového vysílání, 188
rozšíření služby DHCP, 699
Rsh, 678
Rsping, 579
Rsvpsm, 583
Rsvptrace, 577

Ř

řadič IPsec, 506
řadiče domén, 724
řešení problémů, 126
řízení proudu, 73
– přenosů, 535
– přístupu aktualizace k zónám, 322

S

SA typu Phase I, 502
– Phase II, 503
sada protokolů TCP/IP, 8
scénáře služby DHCP, 207
sdílení zatížení, 247
sekundární servery WINS, 409
selektivní potvrzení protokolu TCP, 79
– potvrzování, 627
selhání komunikace uvnitř sítě intranet, 521
– prohlížeče, 745
server Cookie (Cookie Server), 684
– DNS (DNS Server), 684
– Impress (Impress Server), 685

- LPR (LPR Server), 685
- NNTP (Network News Transport Protocol (NNTP) Server), 704
- POP3 (Post Office Protocol (POP3) Server), 704
- protokolu STDA (StreetTalk Directory Assistance Server), 706
- protokolu StreetTalk (StreetTalk Server), 705
- proxy, 409
- služby World Wide Web, 704
- SMTP (Simple Mail Transport Protocol (SMTP) Server), 704
- vyhledávání zdrojů (Resource Location Server), 685
- servery DNS, 245
 - NIS (NIS Servers), 694
 - NIS+ (NIS+ Servers), 695
 - NTP (NTP Servers), 694
 - písem systému X Window (X Window System Font Servers), 694
 - služby Microsoft WINS, 405
 - vyrovnávací paměti, 246
- seskupené servery DHCP, 206
- seznam požadavků parametrů (Parameter Request List), 702
- shlukové zpracování, 412
- shlukový přenos, 412
- Simple Network Management Protocol, 587
- sít k okamžitému použití, 621
- sítě WAN, 459
- síťová aplikační programová rozhraní, 634, 645
 - architektura, 616
 - vrstva, 609
- síťové prostředky, 657
 - protokoly, 626
 - přenosy, 455
 - služby, 654
 - útoky, 486
- skupiny typu Diffie-Hellman, 505
- sledování prohlédávačů, 755
- sledování systému, 581, 600
- služba Browser, 734
 - pracovní stanice, 655
 - QoS (Quality of Service), 73
 - Routing and Remote Access, 211
 - řízení podsítě QoS, 558
 - serveru, 654
 - Windows Internet Name Service, 750
 - WINS, 332, 602
- služby serveru na vzdáleném počítači, 143
- směrovací proces, 48
- směrovací tabulka, 70, 146
 - IP, 46
 - ve Windows 2000, 47
- směrovač, 151, 683
- hromadného zprostředkovatele, 658
- směrované sítě, 208
- směrování, 63
 - IP, 44, 146
- snižování zátěže sítě TCP/IP, 621
- SNMP, 517, 588
- soubor Hosts, 41, 133
- LMHOSTS, 136, 721, 751
- Rhosts, 675, 679
- se stavem systému (Merit Dump File), 686
- soubory databáze služby DHCP, 190
- LMHOSTS, 395
- protokolu auditu, 230
- rozhraní Winsock, 635
- soukromé adresy, 37
- speciální názvy skupin, 408
- specifikace filtru, 542
- služby WINS (RFC), 480
- specifikování hostitelských počítačů, 676
- spojení dvou systémů WINS, 404
- spouštěcí soubor, 194
 - (soubor Boot), 260
- správa, 590
 - databáze, 189
 - názvů NetBIOS, 18
 - oborů, 172
 - přenosových agentů, 219
 - rezervací, 174
 - serverů WINS, 445
- správa služby DHCP, 600
 - IAS, 601
 - WINS, 600
- správa úložného prostoru, 190
- vícedomých serverů, 450
- záznamů, 189
- standardní zóna zpětného vyhledávání, 296

standardy TCP/IP, 8
stárnutí jednotky MTU, 689
– mezipaměti ARP, 62
statická trasa (Static Route), 691
statické směrovače IP, 49
stavy klienta DHCP, 166
styly filtru, 542
superobory, 175
syndrom SWS (Silly Window Syndrome), 85
syntaxe nástroje Netdiag, 112
– příkazu rcp, 676
systém prohlédávačů v systému
Windows 2000, 734

Š

šifrování veřejných klíčů, 494
štěnice, 488

T

tajné sledování, 486
Tcmon, 580
TCP porty, 15
– třicetné vyjednávání, 16
TCP/IP, 8, 627
Telnet, 679
testovací techniky, 754
testování zón zpětného vyhledávání, 366
Tftp, 680
tok dat, 542
– v modelu OSI, 612
topologie, 457
Tracert, 124, 143, 584
transportní vrstva, 610
trvalá připojení, 443
trvalé záznamy směrovací tabulky, 143
třída služby, 554
– uživatele, 185, 698
třídy adres, 20
– dodavatele, 184
– možností, 184
Ttcp, 583
tunelová propojení, 508
typ uzlu rozhraní NetBIOS (NetBIOS
Node Type), 696
– zprávy DHCP (DHCP Message Type), 701

U

účtovací protokoly, 571
účtování, 572
UDP porty, 16
ukládání do mezipaměti, 285
– negativních odpovědí, 285
úklid paměti záznamů zastaralých názvů, 327
úložiště, 303
– zásad, 563
úplný zónový přenos, 261
upozornění DNS (DNS Notify), 263
určení cesty, 46
uzly NetBIOSu, 44

V

vadné záznamy v mezipaměti ARP, 142
vazba, 169
velikost spouštěcího souboru
(Boot File Size), 686
velké sítě, 208
vertikální rozhraní v modelu OSI, 613
veřejné adresy, 37
vícedomé počítače, 87, 95
– servery DHCP, 217
vícedomí klienti, 319
vícedomost (Multihoming), 68
vícesměrové vysílání, 187
– vysílání IP, 77
– vysílání protokolu IP, 69, 90
vnější obor názvů, 346
vnitřní obor názvů, 346
volby prohlédávačů, 739
vrstva poskytovatelů služeb vrstev, 637
– rozhraní transportního ovladače, 634
vrstvy připojení, 60
výběr, 167
vyhledávání vzdálených počítačů, 723
– WINS, 334
vyhnutí se zahlcení, 84
výchozí brána, 140
– hodnota Time-To-Live, 689
– hodnota TTL protokolu TCP (TCP Default
TTL), 693
– server protokolu IRC (Default Internet Relay
Chat Server), 705

- server služby Finger (Default Finger Server), 705
- výkon serveru, 227
- WINS, 458
- výměna klíčů, 501
- výplň (Pad Option), 682
- výpočet adres IP, 31
- ID podsítí, 29
- ztrát, 121
- vyprázdnění mezipaměti, 363
- vyrovnávací paměť ARP, 50
- vysílání v překladu názvů NetBIOS, 394
- vytváření souboru LMHOSTS, 724
- vyžadovaná adresa IP (Requested IP Address), 699
- zabezpečení, 520
- vzdálená oprávnění, 675
- vzdálené systémy používající název hostitele, 133
- volání procedury, 648
- zpracování, 676
- vzdálený hostitel, 145

W

Wdsbm, 576

Windows 2000, 77

- 2000 Server, 210
- Internet Name Service, 389, 600
- NT Server 4.0, 211
- Sockets, 89

Winipcfg, 222

Z

zabezpečená dynamická aktualizace, 309

zabezpečení, 515, 563, 594

- heslem, 486
- metodou zásad, 491
- proti útokům, 489
- protokolem IPSec, 514
- protokolu IP, 74, 144, 486, 628

zabezpečovací brány, 517

- protokol IPSec, 488

zákaz předávání protokolu IP, 688

- směrování nemístních zdrojů, 688

základní možnosti (RFC 1497), 682

- protokoly, 61

zálohování databáze serveru WINS, 418

zálohy databáze, 190

záložní prohlížeč (Backup Browser), 737

záměna identity (Padělení adresy IP), 486

- informací, 486

zapojování klienta do jiné podsítě, 403

zapouzdření koncové části (Trailer Encapsulation), 692

- síť Ethernet (Ethernet Encapsulation), 692

zápůjčka DHCP, 163

zásady skupiny, 274

zásuvka pošty, 89

záznamy prostředků, 250

- A, 252
- CNAME, 252
- MX, 253
- NS, 252
- SOA, 251

záznamy PTR, 252

- SRV, 254

- ve směrovací tabulce IP, 46

zbezpečená dynamická aktualizace, 322

zjištění masky, 691

- názvu typu NetBIOS, 93

zjišťování směrovače, 73, 691

změna velikosti okna, 77

znaková sada Unicode, 341

zóna dopředného vyhledávání, 258

- zpětného vyhledávání, 258, 294

zónový přenos, 261, 340

zóny, 243, 257

zotavení, 232

zpoždění TIME-WAIT protokolu TCP, 86

zprávy ARP a UDP, 63

- DHCP, 163
- Keep-Alive protokolu TCP, 84
- RSVP, 547
- služby DHCP, 710
- SNMP, 592

zprostředkující ovladače, 622

Ž

životnost klíče, 504



Microsoft® Windows Server 2000

Sítě TCP/IP

Kniha *Sítě TCP/IP* vám vysvětlí problematiku sítí založených na protokolech TCP/IP a ukáže možnosti jejich konfigurace a správy.

Z obsahu:

- Úvod do problematiky TCP/IP, pochopení svazku protokolů Windows TCP/IP a NETBIOSu.
- Implementace a podpora sítí založených na protokolech TCP/IP pod Microsoft Windows 2000.
- Konfigurace sítí TCP/IP a rozlišování jmen pomocí protokolu DHCP, systému DNS a služby WINS.
- Rozdělování priorit v síťovém provozu a maximalizace propustnosti sítě pomocí služby QoS (Quality of Service).
- Zajišťování privátní a zabezpečené síťové komunikace protokolem IPSec (Internet Protocol Security).
- Správa síťových zdrojů prostřednictvím protokolu SNMP.
- Řešení nejčastějších potíží v sítích TCP/IP.



**Vydalo vydavatelství
a nakladatelství
Computer Press®**
Hornocholupická 22,
143 00 Praha 4,
<http://www.cpress.cz>

Distribuce:

Computer Press Brno,
náměstí 28. dubna 48,
635 00 Brno-Bystrc,
tel. (05) 46 12 21 11,
fax: (05) 46 12 21 12,
e-mail: distribuce@cpress.cz

Computer Press Bratislava,
Hattalova 12
831 03 Bratislava, SR,
tel.: +421 (7) 44 45 20 48,
44 25 17 20,
fax: +421 (7) 44 45 20 46,
e-mail: distribucia@cpress.sk
Publikaci lze objednat
také na adrese
<http://www.vltava.cz>



VŠECHNY CESTY
K INFORMACI

Microsoft®