kapitola

29

Zavádění protokolu IP verze 6

Obsah kapitoly:

Systém Windows Vista má architekturu TCP/IP nové generace s vylepšenou podporou protokolu IP verze 6 (Internet Protocol version 6, zkráceně IPv6). V této kapitole se dozvíte, proč je protokol IPv6 nezbytný a jak funguje. Tato kapitola popisuje nové funkce protokolu IPv6 v systémech Windows Vista a Windows Server 2008 a radí, jak plánovat migrace síťové infrastruktury vaší firmy na protokol IPv6 pomocí technologií přechodu k protokolu IPv6, jako je například protokol ISATAP (Intra-Site Automatic Tunel Addressing Protocol). Tato kapitola rovněž popisuje, jak konfigurovat a řídit protokol IPv6 v systému Windows Vista a jak řešit problémy sítí s protokolem IPv6.

Protokol IPv6

Potřeba migrace firemních sítí z protokolu IPv4 na IPv6 je daná několika technologickými, obchodními a sociálními faktory. Nejdůležitějšími jsou:

- Exponenciální růst Internetu a existující prostor veřejných adres IPv4. Dočasným řešením tohoto problému se stala technologie překladu adres NAT (Network Address Translation), která mapuje několik privátních (intranetových) adres na jednu veřejnou adresu (Internet). Bohužel použití směrovačů s technologií NAT může přinést další problémy, jako je například rozbíjení připojení mezi koncovými body a zabezpečení pro některé síťové aplikace. Navíc mohutný nárůst počtu mobilních zařízení s přidělenou adresou IP způsobil zmenšování prostoru volných adres IPv4.
- Vzrůstající oblíbenost komunikace se síťovým provozem v reálném čase (RTC) na Internetu, jako je technologie telefonování přes Internet (VoIP), okamžité zprávy (IM) a audio/video konference, ukázala limity podpory kvality služeb (QoS) poskytované protokolem IPv4. Tyto nové technologie RTC potřebují vylepšenou QoS na sítích IP, aby byla zajištěna spolehlivá komunikace mezi koncovými body. Návrh protokolu IPv4 znemožňuje možná vylepšení.
- Vzrůstající počet hrozeb, kterým čelí počítače připojené k sítím IPv4, může být snížen zavedením protokolu IPsec, a to jak na vnitřních sítích, tak na tunelových připojeních přes veřejný Internet. Avšak protokol IPsec byl navržen jako dodatek k protokolu IPv4 a je ve spoustě případů příliš složitý na implementaci. Protokol IPsec nemůže také obejít překlad adres NAT, pokud je část paketu šifrována.

Protokol IPv6, vyvinutý sdružením IETF (Internet Engineering Task Force) pro řešení těchto problémů, obsahuje následující vylepšení:

- Protokol IPv6 rozšiřuje teoretický prostor adres na Internet z $4{,}3 * 10^9$ (podle 32-bitových adres IPv4) na $3.4 * 10^{38}$ možných adres (podle 128bitových adres IPv6), což by mělo být dost pro dohlednou budoucnost, jak se shoduje řada expertů.
- Prostor adres IPv6 byl navržen hierarchicky, což znamená, že směrovací tabulky pro směrovače IPv6 jsou menší a efektivnější než u směrovačů IPv4.
- Protokol IPv6 vylepšil podporu QoS. Hlavičky paketů nyní obsahují pole Traffic Class (třída síťového provozu), které určuje, jak by mělo být se síťovým provozem naloženo, a nové pole Flow Label (označení proudu), které umožňuje směrovačům identifikovat pakety příslušející proudu dat a odpovídajícím způsobem je zpracovat.
- Protokol IPv6 nyní vyžaduje podporu protokolu IPsec pro zabezpečení standardizovaných připojení mezi koncovými body přes Internet. Nová vylepšení QoS fungují, dokonce i když jsou data přenášená protokolem IPv6 šifrována pomocí protokolu IPsec.

Porozumět tomu, jak funguje protokol IPv6, je důležité, pokud chcete mít prospěch ze zavedení protokolu IPv6 ve vaší firmě. Následující části kapitoly obsahují přehled klíčových návrhů, funkcí a termínů pro protokol IPv6.

Poznámka: Více podrobností o návrzích, funkcích a termínech protokolu IPv6 najdete v článku *Introduction to IPv6* na adrese `www.microsoft.com/technet/itsolutions/network/ipv6/introipv6.mspx`. Dalším dobrým zdrojem informací o protokolu IPv6 je kniha *Understanding IPv6* od Josepha Daviese (Microsoft Press, 2002). Aktualizace k této knize můžete stáhnout z `http://www.microsoft.com/downloads/details.aspx?FamilyID=42bf4711-27af-4c4c-8300-7bcf900de5c3`.

Terminologie protokolu IPv6

Následující termíny slouží k definování návrhů protokolu IPv6 a popisují funkce protokolu IPv6:

- **Uzel:** Síťové zařízení s podporou protokolu IPv6, kterým může být hostitel i směrovač.
- **Hostitel:** Síťové zařízení s podporou protokolu IPv6, například počítač s jednou adresou, který nemůže předávat pakety IPv6, které nejsou explicitně adresovány jemu. Hostitel je koncovým bodem komunikace (buď zdroj, nebo cíl) protokolu IPv6 a zahazuje všechny pakety, které mu nejsou explicitně adresovány.
- **Směrovač:** Síťové zařízení s podporou protokolu IPv6, které může předávat pakety IPv6, které mu nejsou explicitně adresovány. Směrovače IPv6 většinou oznamují svou přítomnost hostitelům IPv6 na připojených spojeních.
- **Spojení:** Jedna a více částí sítě LAN (například protokol Ethernet) nebo WAN (například protokol PPP) spojené směrovači.
- **Sousedé:** Uzly připojené ke stejnému fyzickému nebo logickému spojení.
- **Podsíť:** Jedno nebo více spojení se stejným 64bitovým prefixem adresy IPv6. Pokud na podsíti nejsou žádné směrovače, podsíť je rovnocenná se spojením.
- **Rozhraní:** Reprezentace uzlu připojeného ke spojení. Může jím být fyzické rozhraní (například síťový adapter) nebo logické rozhraní (například rozhraní tunelu).

Poznámka: Adresa IPv6 identifikuje rozhraní, a ne uzel. Uzel je identifikován unicast adresou IPv6 přiřazenou jednomu z jeho rozhraní.

Adresování protokolu IPv6

Protokol IPv6 používá 128bitové (16bajtové) adresy, které se zapisují ve formě šestnáctkových čísel oddělených dvojtečkami. Například v adrese `2001:DB8:3FA9:00-00:0000:0000:00D3:9C5A` představuje každý blok 4 šestnáctkových čísel 16bitové binární číslo. Osm takových bloků nám tedy celkově dává 8 * 16 = 128 bitů.

Můžete použít zkrácený zápis adres vynecháním nul v každém bloku. Za použití této techniky se z předchozí reprezentace adresy stane `2001:DB8:3FA9:0:0:0:D3:9C5A`.

Adresu lze dále zkrátit kompresí přilehlých nulových bloků dvojicí dvojteček („::“). Naše ukázková adresa se tedy zkrátí na `2001:DB8:3FA9::D3:9C5A`. Zapamatujte si, že v adrese IPv6 lze použít jen jednu dvojici dvojteček, aby se zachovala její jedinečná reprezentace.

Prefixy IPv6

Prefix IPv6 ukazuje, jaká část adresy je použita pro směrování (podsíť nebo skupina podsítí spojených směrovačem) nebo identifikaci rozsahu adres. Prefixy IPv6 mají podobný tvar jako zápisy CIDR (Classless Inter-Domain Routing) používané protokolem IPv4. Například `2001:DB8:3FA9::/48` může představovat prefix směrovače ve směrovací tabulce IPv6.

U protokolu IPv4 se mohou zápisy CIDR používat pro reprezentaci jednotlivých adres unicast mimo směrovačů a podsítí. Prefixy IPv6 jsou však používány pro reprezentaci směrovačů a rozsahů adres, a ne adres unicast. Je tomu tak proto, že na rozdíl od protokolu IPv4 protokol IPv6 nepodporuje proměnnou délku identifikátorů podsítě – pro identifikaci podsítě v protokolu IPv6 se vždy použije horních 64 bitů. Je tedy zbytečné reprezentovat naši ukázkovou adresu jako `2001:DB8:3FA9::D3:9C5A/64` pro adresu podsítě, protože část `/64` je zřejmá.

Typy adres IPv6

Protokol IPv6 podporuje tři různé typy adres:

- **Unicast:** Identifikuje jediné rozhraní v rozsahu adres. (Rozsah adres IPv6 je ta část vaší sítě, ve které je tato adresa jedinečná.) Pakety IPv6 s cílovými adresami unicast jsou doručeny jednomu rozhraní.
- **Multicast:** Identifikuje žádné nebo více rozhraní. Pakety IPv6 s cílovou adresou multicast jsou doručeny všem rozhraním naslouchajícím na dané adrese. (Všeobecně vzato cílové adresy multicast fungují stejně v protokolu IPv6 jako v protokolu IPv4.)
- **Anycast:** Identifikuje několik rozhraní. Pakety IPv6 s cílovými adresami multicast jsou doručeny nejbližšímu rozhraní (měřené vzdáleností směrování) určenému danou adresou. Adresy anycast jsou momentálně přiřazeny jen směrovačům a mohou reprezentovat jen cílové adresy.

Poznámka: Mezi typy adres IPv6 nepatří adresy broadcast používané protokolem IPv4. U protokolu IPv6 se pro všechna všesměrová vysílání používají adresy multicast. Více informací o adresách multicast najdete v tabulce 29.2.

Adresy unicast

Adresy unicast jsou adresy, které identifikují jediné rozhraní. Protokol IPv6 má několik typů adres unicast:

- **Globální adresa unicast:** Adresa, kterou lze použít pro směrování v té části Internetu, která používá protokol IPv6. Oblastí globálních adres je tedy celý Internet a globální adresy protokolu IPv6 odpovídají veřejným adresám (ne podle standardu RFC 1918) protokolu IPv4. Prefixem adresy, který se aktuálně používá pro globální adresy, je `2000::/3` a struktura globální adresy je následující:
  - Prvních 48 bitů adresy je globální směrovací prefix vaší firemní sítě. (První tři bity tohoto prefixu musí být 001 v binárním zápisu.) Těchto 48 bitů reprezentuje část veřejné topologie adres, která představuje skupinu velkých a malých poskytovatelů internetových služeb na části Internetu s protokolem IPv6 a která je

kontrolována těmito poskytovateli pomocí autority IANA (Internet Assigned Numbers Authority).

- Dalších 16 bitů je identifikátor podsítě. Vaše organizace může díky této části adresy specifikovat až 65 536 jedinečných podsítí pro směrovací účely uvnitř firemní sítě. Těchto 16 bitů reprezentuje část topologie adres, nad kterými má kontrolu vaše firma.
- Posledních 64 bitů je identifikátor rozhraní a určuje jedinečné rozhraní uvnitř každé podsítě.

- **Adresa unicast link-local:** Adresa používaná uzlem pro komunikaci se sousedními uzly na stejném spojení. Tudíž oblast adres link-local tvoří lokální spojení na dané síti, adresy link-local nejsou předávány za hranice lokálního spojení směrovači IPv6. Jelikož adresy link-local jsou přiřazovány rozhraním automatickou konfigurací adres protokolu IPv6, adresy link-local protokolu IPv6 odpovídají adresám APIPA (Automatic Private IP Addressing) používaným v protokolu IPv4 (které jsou přiřazovány z rozsahu adres `169.254.0.0/16`). Prefix adres adresy pro link-local je `FE80::/64` a struktura adres link-local je taková:
  - Prvních 64 bitů adresy je vždy `FE80:0:0:0` (které se zobrazí jako `FE80::`).
  - Posledních 64 bitů tvoří identifikátor rozhraní a specifikuje jedinečné rozhraní na lokálním spojení.

  Adresy link-local mohou být znovu použity, jinými slovy dvě rozhraní na různých spojeních mohou mít stejnou adresu. To umožňuje mít adresy link-local, které jsou nejednoznačné. Dodatečný identifikátor, nazvaný identifikátor oblasti, označuje, kterému spojení je adresa přiřazena nebo nasměrována. V systému Windows Vista odpovídá identifikátor oblasti pro adresu link-local indexu rozhraní pro dané rozhraní. Můžete prohlížet seznam indexů rozhraní na počítači zadáním příkazu `netsh interface ipv6 show interface`. Více informací o identifikátorech oblasti najdete později v této kapitole, v části *Zobrazení nastavení adres IPv6*.
- **Adresa unicast site-local:** Adresa, kterou používá uzel pro komunikaci s dalšími uzly na privátní síti s několika podsítěmi nebo spojeními. Oblastí adres site-local je celá síť na určitém místě, kterým je většinou nějaká budova. Protože adresy site-local nejsou dosažitelné, s výjimkou firemního intranetu, adresy site-local protokolu IPv6 odpovídají privátním adresám (standard RFC 1918) použitým v protokolu IPv4. Struktura adres site-local je následující:
  - Prvních 10 bitů adresy je vždy `FEC0::/10` nebo `1111 1110 11` (binárně).
  - Dalších 54 bitů tvoří identifikátor podsítě. Vaše firma může použít tuto část adresy, aby specifikovala další podsítě pro účely směrování.
  - Na posledních 64 bitech je identifikátor rozhraní, který jednoznačně určuje rozhraní uvnitř každé podsítě.

  Standard RFC 3879 neschvaluje používání adres site-local. Náhradou za adresy site-local jsou jedinečné lokální adresy. Již zavedené protokoly IPv6 mohou v používání adres site-local pokračovat.
- **Jedinečná lokální adresa unicast:** Protože prefix adresy site-local může reprezentovat několik sítí uvnitř firmy, je nejednoznačný a není příliš vhodný pro účely směrování ve firemním prostředí. Proto standard RFC 4193 momentálně navrhuje

nový typ adres: jedinečnou lokální adresu unicast (nebo jen lokální adresu). Oblast této adresy je globální pro všechny sítě ve firmě a použití tohoto typu adresy usnadňuje konfiguraci interní firemní infrastruktury směrování protokolu IPv6. Struktura lokálních adres je následující:

- Prvních 7 bitů adresy je vždy `1111 110` (binárně) a osmý bit jen nastaven na `1`, což označuje lokální adresu. To znamená, že prefix adresy je vždy `FD00::/8` pro tento typ adresy.
- Následujících 40 bitů reprezentuje globální identifikátor – je to náhodně generovaná hodnota, která jednoznačně identifikuje určité místo ve vaší firmě.
- Následujících 16 bitů představuje identifikátor podsítě a lze jej použít pro další rozdělení interní sítě pro účely směrování.
- Na posledních 64 bitech je identifikátor rozhraní, který jednoznačně určuje rozhraní uvnitř každé podsítě.

Identifikace typů adres IPv6

Jak ukazuje tabulka 29.1, můžete rychle určit, s jakým typem adresy IPv6 pracujete, pohledem na úvodní část adresy – bity vyššího řádu dané adresy. Tabulky 29.2 a 29.3 také ukazují příklady běžných adres IPv6, které můžete rozpoznat přímo z jejich reprezentace v šestnáctkových číslech oddělených dvojtečkami.

Tabulka 29.1: Identifikace typů adres IPv6 pomocí bitů vyššího řádu a prefixu adresy

Typ adresy	Bity vyššího řádu	Prefix adresy
Globální unicast	001	2000::/3
Link-local unicast	1111 1110 10	FE80::/64
Site-local unicast	1111 1110 11	FEC0::/10
Multicast	1111 1111	FF00::/8

Tabulka 29.2: Identifikace běžných adres multicast IPv6.

Funkce	Oblast	Reprezentace
Multicast pro všechny uzly	Lokální rozhraní	FF01::1
Multicast pro všechny uzly	Lokální spojení	FF02::1
Multicast pro všechny směrovače	Lokální rozhraní	FF01::2
Multicast pro všechny směrovače	Lokální spojení	FF02::2
Multicast pro všechny směrovače	Lokální místo	FF05::2

Tabulka 29.3: Identifikace speciálních adres IPv6

Funkce	Reprezentace
Nespecifikovaná adresa (bez adresy)	::
Adresa zpětné smyčky	::1

Poznámka: Více informací o typech adres používaných různými technologiemi přechodu na protokol IPv6 najdete v později v této kapitole, v části *Plán migrace k protokolu IPv6*.

Identifikátory rozhraní

U všech typů adres unicast IPv6 popsaných v předchozích částech posledních 64 bitů adresy reprezentuje identifikátor rozhraní, který jednoznačně určuje rozhraní na lokálním spojení nebo podsíti. Ve starších verzích systému Windows je identifikátor rozhraní jednoznačně určen takto:

- U adres link-local, jako je například síťový adaptér na úseku sítě Ethernet, je identifikátor rozhraní odvozen buď z jedinečné 48bitové adresy MAC (Media Access Control), nebo odpovídá jedinečné adrese EUI-64 (Extended Unique Identifier) daného rozhraní, jak definuje institut IEEE (Institute of Electrical and Electronic Engineers).
- U prefixů globálních adres identifikátor rozhraní, založený na EUI-64, vytváří veřejnou adresu IPv6.
- U prefixů globálních adres dočasný náhodný identifikátor rozhraní vytváří dočasnou adresu. Tento přístup popisuje standard RFC 3041 a můžete jím poskytnout anonymitu klientům na Internetu s protokolem IPv6.

V systému Windows Vista je však identifikátor rozhraní generován náhodně pro všechny typy adres unicast IPv6 přiřazených libovolnému typu rozhraní.

Srovnání protokolů IPv6 a IPv4

Tabulka 29.4 porovnává schémata adresování protokolů IPv4 a IPv6.

Tabulka 29.4: Srovnání adresování v protokolu IPv4 versus IPv6

Funkce	IPv4	IPv6
Počet bitů (bajtů)	32 (4)	128 (16)
Forma zápisu	Desítková čísla oddělená tečkami	Šestnáctková čísla oddělená dvojtečkami
Podsítě proměnné délky	Ano	Ne
Veřejné adresy	Ano	Ano (globální adresy)
Privátní adresy	Ano (adresy standardu 1918)	Ano (adresy site-local a lokální adresy)
Automatická konfigurace adres pro lokální spojení	Ano (APIPA)	Ano (adresy link-local)
Podpora pro třídy adres	Ano, ale neschválena směrováním CIDR	Ne
Broadcast adresy	Ano	Místo nich adresy multicast
Maska podsítě	Nutná	Implicitní prefix adresy `/64` pro adresy přiřazené rozhraní

Poznámka: Podrobnější specifikaci adresování protokolu IPv6 najdete v dokumentu RFC 4291 na adrese `http://www.ietf.org/rfc/rfc4291.txt`. Existují také další rozdíly, například ve struktuře hlaviček paketů protokolu IPv4 versus IPv6. Více informací najdete v článku *Introduction to IP Version 6* na adrese `http://www.microsoft.com/technet/itsolutions/network/ipv6/introipv6.mspx`.

Zprávy protokolu ICMP verze 6

S protokolem ICMP (Internet Control Message Protocol) pro protokol IPv4 (ICMPv4) se setkáte v sítích IPv4, kde uzlům sítě umožňuje odesílat a reagovat na chybové nebo informační zprávy. Pokud třeba zdrojový uzel používá nástroj Ping, aby odesílal zprávy ICMP Echo Request (zprávy ICMP typ 8) cílovému uzlu, cílový uzel může reagovat zprávami ICMP Echo (zprávami ICMP typ 0) oznamujícími jeho přítomnost na síti.

U sítí IPv6 plní protokol ICMP pro protokol IPv6 (ICMPv6) tytéž funkce jako protokol ICMPv4 pro sítě IPv4 – zejména poskytuje metodu pro výměnu chybových a informačních zpráv. Protokol ICMPv6 také nabízí informační zprávy pro následující protokoly:

- **Protokol ND (Neighbor Discovery):** Proces, jakým se vzájemně hledají hostitelské počítače a směrovače na síti, aby spolu mohly komunikovat na vrstvě datových spojů.
- **Protokol MLD (Multicast Listener Discovery):** Proces zjištění a udržení členství ve skupinách multicast.

Poznámka: Více informací o protokolu ND najdete později v této kapitole, v části *Protokol ND*. Více informací o typech zpráv a formátech hlaviček protokolu ICMPv6 najdete v článku *Introduction to IP Version 6* na adrese `http://www.microsoft.com/technet/itsolutions/network/ipv6/introipv6.mspx`.

Protokol ND

Protokol ND (Neighbor Discovery) představuje proces, díky kterému spolu mohou vzájemně komunikovat uzly na síti IPv6 výměnou rámců na vrstvě datových spojů. Protokol ND v sítích IPv6 provádí následující:

- Umožňuje uzlům IPv6 (hostitelské počítače IPv6 nebo směrovače IPv6) rozpoznat adresu spojové vrstvy sousedního uzlu (uzlu na stejném fyzickém nebo logickém spojení).
- Umožňuje uzlům IPv6 určit, zda adresa spojové vrstvy sousedního uzlu byla změněna.
- Umožňuje uzlům IPv6 určit, jestli jsou sousední uzly stále dosažitelné.
- Umožňuje směrovačům IPv6 oznamovat svou přítomnost, prefixy spojení a konfiguraci hostitelských počítačů.
- Umožňuje směrovačům IPv6 přesměrovat hostitelské počítače ke směrovačům, které lépe vyhovují určitému cíli.
- Umožňuje hostitelským počítačům zjišťovat adresy, prefixy adres a další nastavení.
- Umožňuje hostitelským počítačům objevovat směrovače připojené k lokálnímu spojení.

Abyste pochopili, jak funguje protokol ND, zkuste jej nejprve srovnat s podobnými procesy používanými u protokolu IPv4. U protokolu IPv4 můžete použít tři různé mechanismy pro správu komunikace mezi uzly:

- **Protokol ARP (Address Resolution Protocol):** Protokol vrstvy datových spojů, který rozpoznává adresy IPv4 přiřazené rozhraním podle jejich adres MAC (adres spojové vrstvy). To umožňuje síťovým adaptérům přijímat jim adresované rámce a odesílat odpovědi zpět ke zdroji rámce. Například předtím než počítač bude moct odeslat data cílovému počítači, jehož adresa IPv4 je `172.16.25.3`, odesílající počítač nejprve použije protokol ARP, aby určil cílovou adresu (pokud je cílový počítač na stejní místní síti) nebo adresu IP lokální brány (jestliže je cílový počítač na jiné síti) k odpovídající 48bitové adrese MAC (ku příkladu `00-13-20-08-A0-D1`).

- **Služba ICMPv4 Router Discovery (služba pro zjišťování směrovačů):** Zprávy této služby protokolu ICMPv4 umožňují směrovačům oznamovat svou přítomnost na sítích IPv4 a dovolují hostitelským počítačům zjišťovat přítomnost těchto směrovačů. Pokud je služba Router Discovery povolena na směrovači, směrovač periodicky odesílá zprávy inzerování směrovače všem počítačům pomocí adresy multicast (`224.0.0.1`), aby oznámil počítačům na síti, že je tento směrovač dostupný. Když je služba Router Discovery povolena na hostitelských počítačích, hostitelské počítače mohou posílat zprávy oslovení směrovačů všem směrovačům pomocí adresy multicast (`224.0.0.2`), aby získaly adresu směrovače přiřazenou k této adrese jako výchozí brána hostitelského počítače.
- **Služba ICMPv4 Redirect (služba pro přesměrování):** Směrovače používají zprávy této služby, aby informovaly hostitelské počítače o jiných směrovačích, které lépe vyhovují určitým cílům. Zprávy služby ICMPv4 Redirect jsou nezbytné, protože hostitelské počítače většinou nepoznají, který směrovač na jejich podsíti nejlépe vyhovuje pro přenos dat k určitému vzdálenému cíli.

U sítí IPv4 tyto tři techniky umožňují uzlům spolu vzájemně komunikovat. U sítí IPv6 byly tyto techniky nahrazeny pěti typy zpráv IMCPv6, které ukazuje tabulka 29.5.

Tabulka 29.5: Typy zpráv ICMPv6 používané pro protokol ND

Typ zprávy	Typ ICMPv6	Popis
Oslovení směrovačů	133	Odesílají všechny hostitelské počítače IPv6 všem směrovačům na lokálním spojení pomocí adresy multicast (`FF02::2`), aby objevily směrovače IPv6 přítomné na tomto lokálním spojení.
Inzerování směrovače	134	Odesílané periodicky směrovači IPv6 všem uzlům na lokálním spojení pomocí adresy multicast (`FF02::1`) nebo odesílané na adresu unicast hostitelského počítače jako odpověď na přijatou zprávu oslovení směrovačů z tohoto počítače. Zprávy inzerování směrovače poskytují hostitelským počítačů informace potřebné pro rozpoznání prefixů spojení, jednotky MTU spojení, zda použít protokol DHCPv6 pro automaticky konfiguraci adresy a životnost automaticky konfigurovaných adres.
Oslovení sousedů	135	Odesílané hostitelskými počítači IPv6 oslovovaným uzlům pomocí adresy multicast hostitelského počítače pro zjištění adresy spojové vrstvy uzlu IPv6 nebo odesílané na adresu unicast hostitelského počítače pro ověření dostupnosti daného hostitelského počítače.
Inzerování sousedů	136	Odesílané uzly IPv6 na adresu unicast hostitelského počítače jako odpověď na přijatou zprávu oslovení sousedů z tohoto hostitelského počítače nebo odesílány všem uzlům na lokálním spojení pomocí adresy multicast pro informování sousedních uzlů o změnách adres spojové vrstvy hostitelského počítače.
Přesměrování	137	Odesílané směrovačem IPv6 na adresu unicast hostitelského počítače kvůli informování hostitelského počítače o lepší cestě pro danou adresu cíle.

Poznámka: Adresa multicast oslovovaných uzlů, která se používá jako cílová adresa zpráv oslovení sousedů protokolu ICMPv6 (zprávy typu 135 protokolu ICMPv6) při procesu rozlišování adres, je zvláštním typem adresy multicast složené z prefixu `FF02::1:FF00:0/104`, za kterým následuje 24 bitů rozlišované adresy IPv6. Výhodou použití adresy multicast pro rozlišování adres v protokolu IPv6 je, že jen cílový hostitelský počítač bývá rušen na lokálním spojení. Oproti tomu zprávy protokolu ARP používané protokolem IPv4 pro dotazy procesu rozlišování adres jsou zasílány na adresu broadcast spojové vrstvy, což ruší všechny hostitelské počítače na lokálním úseku. Uzly IPv6 naslouchají na všech jim přiřazeným adresám IPv6, včetně jejich adres multicast oslovovaných uzlů.

Automatická konfigurace adres

U sítí IPv4 mohou být adresy přiřazeny hostitelským počítačům třemi způsoby:

- Ručně – přiřazením statických adres.
- Automaticky pomocí protokolu DHCP, jestliže je na dané podsíti přítomen server DHCP (nebo konfigurován agent přenosu DHCP).
- Automaticky pomocí adresování APIPA (Automatic Private IP Addressing), které automaticky přiřazuje hostitelskému počítači adresu z rozsahu `169.254.0.0` až `169.254.255.255` s maskou podsítě `255.255.0.0`.

U sítí IPv6 jsou statické adresy většinou přiřazovány jen směrovačům, někdy také serverům, ale jen výjimečně klientským počítačům. Místo toho jsou adresy IPv6 téměř vždy přiřazovány automaticky procesem nazvaným automatická konfigurace adres. Automatická konfigurace adres funguje třemi způsoby: bezstavově, stavově nebo obojí dohromady. Bezstavová automatická konfigurace adres je založena na principu přijímání zpráv inzerování směrovače protokolu ICMPv6. Stavová automatická konfigurace adres naproti tomu používá protokol DHCPc6, aby získala informace o adrese a dalších nastaveních ze serveru DHCPv6.

Poznámka: Služba Server DHCP systému Windows Server 2003 nepodporuje protokol DHCPv6. Systém Windows Server 2008 bude podporovat roli Server DHCPv6.

Všechny uzly IPv6 (hostitelské počítače i směrovače) si automaticky přiřazují adresy link-local (adresy s prefixem adresy `FE80::/64`); děje se tak pro každé rozhraní (fyzické i logické) daného uzlu. Tyto automaticky konfigurované adresy link-local lze použít jen pro přístup k sousedním uzlům (uzlům na stejném spojení). Když specifikujete nějakou takovou adresu jako cílovou adresu, pravděpodobně budete muset zadat identifikátor oblasti pro daný cíl. Navíc adresy link-local nejsou nikdy registrovány na serverech DNS.

Poznámka: Ručně přiřazovat adresy IPv6 je většinou nutné jen směrovačům IPv6 a některým serverům. Počítač se systémem Windows Vista a několika rozhraními můžete nakonfigurovat jako směrovač. Více informací o konfiguraci směrovačů IPv6 najdete v článku *Manual Configuration for IPv6* na adrese `http://www.microsoft.com/technet/community/columns/ cableguy/cg0902.mspx`. Popis směrovací tabulky protokolu IPv6 najdete v článku *Understanding the IPv6 Routing Table* na adrese `http://www.microsoft.com/technet/ community/columnd/cableguy/cg1002.mspx`.

Automaticky konfigurované adresy IPv6 mohou mít několik stavů, jak ukazuje tabulka 29.6.

Tabulka 29.6: Možné stavy automaticky konfigurované adresy IPv6

Stav	Popis
Prozatímní	Jedinečnost adresy se stále testuje pomocí detekce duplicitních adres.
Platná	Adresa je jedinečná a může přijímat a odesílat data protokolem IPv6, dokud nevyprší časový limit pro platnou adresu.
Preferovaná	Adresa může být použita pro přenos dat, dokud nevyprší časový limit pro preferovanou adresu.
Neschválená	Adresu lze stále použít pro přenos dat v existujících komunikačních relacích, ale je zamítnuta pro nové komunikační relace.
Neplatná	Časový limit pro platnou adresu vypršel a tuto adresu nelze dále používat pro přenos dat.

Poznámka: Časové limity pro platnou a preferovanou adresu u bezstavové automatické konfigurace adres IPv6 v systému Windows Vista jsou součástí zpráv oslovení směrovačů.

Podrobný popis toho, jak fungují procesy automatické konfigurace adres, rozlišování adres, zjišťování směrovačů (služba Router Discovery) a detekce nedosažitelnosti sousedů najdete v článku *Introduction to IP Version 6* na adrese `http://www.microsoft.com/technet/itsolutions/network/ipv6/introipv6.mspx`.

Poznámka: Abyste zobrazili stav všech automaticky konfigurovaných adres IPv6 na počítači se systémem Windows Vista, spusťte příkazový řádek a zadejte do něj příkaz `netsh interface ipv6 show addresses`.

Rozlišování názvů

Protokol DNS (Domain Name System) tvoří základ pro rozlišování názvů v sítích IPv4 i IPv6. Na sítích IPv4 jsou záznamy (A) hostitelského počítače použity jmennými servery (servery DNS) pro rozlišení adres IP z plně kvalifikovaných doménových názvů, například server1.contoso.cz, jako odpověď na vyhledávání názvů (dotazy na názvy) z klientů DNS. Kromě toho obrácené vyhledávání, kdy jsou plně kvalifikované doménové názvy rozlišovány z adres IP, podporují záznamy PTR v doméně in-addr.arpa.

Rozlišování názvů funguje na stejném principu u protokolu IPv6 s následujícími rozdíly:

- Záznamy u hostitelských počítačů IPv6 jsou záznamy AAAA, nikoliv záznamy A.
- Doménou pro obrácené vyhledávání adres IPv6 je ip6.arpa, a ne in-addr-arpa.

Poznámka: Vylepšení protokolu DNS, která umožňují použít protokol IPv6, jsou popsána v návrhu standardu RFC 3596 na adrese `http://www.fags.org/rfcs/rfc3596.html`.

Dotazy na názvy

Protože architektura TCP/IP nové generace v systému Windows Vista povoluje ve výchozím nastavení protokol IPv4 i IPv6, vyhledávání názvů protokolu DNS klientskými počítači se systémem Windows Vista může zahrnovat jak záznamy A, tak záznamy AAAA. (To je pravda, jen pokud vaše jmenné servery podporují protokol IPv6, což je

případ role Server DNS v systému Windows Server 2003.) Ve výchozím nastavení systému Windows Vista vykonává služba Klient DNS následují proceduru, když vyhledává názvy pomocí zvláštního rozhraní:

1. Klientský počítač zkusí, zda má dané rozhraní přiřazenou adresu IPv6, různou od adresy link-local. Pokud má takovou adresu přiřazenou, klientský počítač odešle jeden požadavek na vyhledání názvu jmennému serveru, aby se dotázal na záznamy A, ale ne na záznamy AAAA. V případě, že touto přiřazenou adresou je adresa služby Teredo, klientský počítač se opět nedotazuje na záznamy AAAA. (Klient služby Teredo byl v systému Windows Vista navržen tak, aby automaticky neprováděl vyhledávání záznamů AAAA nebo registraci se serverem DNS, aby se zabránilo přetížení serverů DNS.)
2. Jestliže dané rozhraní klientského počítače má přiřazenou adresu různou od adresy link-local, klientský počítač odešle požadavek na vyhledání názvu, aby se dotázal na záznamy A.
   - Pokud klient obdrží odpověď na svůj dotaz (a ne chybovou zprávu), následuje další požadavek na vyhledání, aby se dotázal na záznamy AAAA.
   - Jestliže klient neobdrží žádnou odpověď nebo obdrží chybovou zprávu (s výjimkou chybové zprávy oznamující nenalezení názvu), neodesílá už další požadavek na vyhledání, aby se dotázal na záznamy AAAA.

Poznámka: Protože rozhraní hostitelského počítače IPv6 má typicky několik adres IPv6, proces, kterým probíhá výběr zdrojové a cílové adresy během dotazování na název, je složitější než u rozlišování názvů DNS hostitelskými počítači IPv4. Více o informací o tom, jak funguje výběr zdroje a dresy pro hostitelské počítače IPv6, najdete v článku *Source and Destination Address Selection for IPv6* na adrese `http://www.microsoft.com/technet/community/columns/cableguy/cg0206.mspx`. Více informací o DNS v systému Windows Vista najdete v článku *Domain Name System Klient Behavior in Windows Vista* na adrese `http://www.microsoft.com/technet/itsolutions/network/ipv6/vista_dns.mspx`. Nakonec, více informací o různých typech adres IPv6 obvykle přiřazovaných rozhraním najdete později v této kapitole, v části *Konfigurace a řešení problémů s protokolem IPv6 v systému Windows Vista*.

Poznámka: Problémy nastaly se špatně konfigurovanými jmennými servery DNS na Internetu. Tyto problémy, které popisuje standard RFC 4074 (`http://www.ietf.org/rfc/rfc4074.txt`), se netýkají systému Windows Vista, protože společnost Microsoft upravila chování klientů DNS. Správci serverů DNS by se však měli ujistit, že jsou tyto problémy opraveny, protože mohou ovlivnit rozlišování názvů DNS pro velkou část architektur TCP/IPv6, včetně architektur ve starších verzích systému Windows, třeba v systému Windows XP.

Registrace názvů

Servery DNS v systému Windows Server 2003 mohou dynamicky registrovat záznamy A i AAAA pro klientské počítače se systémem Windows Vista. Dynamická registrace záznamů DNS zjednodušuje údržbu rozlišování názvů na sítích s adresářovou službou Active Directory. Když se spouští klientský počítač se systémem Windows Vista na síti, služba Klient DNS zkouší registrovat následující záznamy pro daný klientský počítač:

- Záznamy pro všechny adresy IPv4 přiřazené všem rozhraním s nastavenou adresou serveru DNS.

- Záznamy AAAA pro adresy IPv6 přiřazené všem rozhraním s nastavenou adresou serveru DNS.
- Záznamy PTR pro všechny adresy IPv4 přiřazené všem rozhraním s nastavenou adresou serveru DNS.

Poznámka: Záznamy AAAA jsou registrovány pro adresy link-local IPv6, které byly přiřazeny rozhraním pomocí automatické konfigurace adres.

Záznamy PTR a protokol IPv6

Klientské počítače se systémem Windows Vista nezkouší registrovat záznamy PTR pro všechny adresy IPv6 přiřazené rozhraním na počítači. Pokud chcete povolit klientským počítačům vykonávat obrácené vyhledávání pro počítače se systémem Windows Vista pomocí protokolu IPv6, musíte ručně vytvořit oblast pro obrácené vyhledávání pro doménu ip6.arpa na vašich serverech DNS a potom ručně přidat záznamy PTR k této oblasti. Podrobnější návod, jak to provést, najdete v článku IPv6 for Microsoft Windows: Frequently Aked Questions na adrese `http://www.microsoft.com/technet/itsolutions/network/ipv6/ipv6faq.mspx`.

Záznamy PTR se obvykle nepoužívají pro obrácené vyhledávání pomocí protokolu IPv6, protože prostor názvů pro dotazy obráceného vyhledávání je složen z jednotlivých šestnáctkových číslic v hexadecimální podobě adresy IPv6, vyjadřujících úrovně v obrácené hierarchii domén. Například záznam PTR přiřazený k adrese IPv6 `2001:0DB8::D3:00FF:FE28:9C5A`, jejíž úplná reprezentace je `2001:0DB8:0000:0000:00D3:00FF:FE28:9C5A`, by se dal vyjádřit jako `A.5.C.9.8.2.E.F.F.F.0.0.3.D.0.0.0.0.0.0.0.0.0.0.8.B.D.0.1.0.0.2.IP6.ARPA`. Rozpoznávání takové reprezentace by bylo většinou příliš náročné na výkon pro většinu implementací serverů DNS.

Servery DNS běžící pod systémem Windows Server 2003 ve výchozím nastavení nenaslouchají síťovému provozu DNS posílanému protokolem IPv6. Abyste umožnili serverům DNS naslouchat požadavkům na vyhledávání názvů a registraci názvů přes protokol IPv6, musíte nejprve tyto servery konfigurovat příkazem `dnscmd /config /EnableIPv6 1`. Musíte později ručně nastavit všem klientským počítačům se systémem Windows Vista adresu unicast IPv6 vašich serverů DNS pomocí příkazu `netsh interface ipv6 add dns interface=NázevNeboIndex address=AdresaIPv6 index=Úroveňpřiority`. (Servery DHCP běžící pod systémem Windows Server 2003 aktuálně nepodporují stavové přiřazování adres pomocí protokolu DHCPv6.)

Poznámka: Více informací o povolení podpory protokolu IPv6 u serverů DNS v systému Windows Server 2003 najdete v kapitole 9 nebo v knize on-line *TCP/IP Fundamentals for Microsoft Windows*, kterou lze stáhnout z adresy `http://www.microsoft.com/downloads/details.aspx?FamilyID=c76296fd-61c9-4079-a0bb-582bca4a846f`. Více podrobností o chování registrací a dotazů na názvy DNS v systému Windows Vista najdete na adrese `http://www.microsoft.com/technet/itsolutions/network/ipv6/vista_dns.mspx`.

Rozšíření protokolu IPv6 v systému Windows Vista

Architektura TCP/IP v systémech Windows XP a Windows Server 2003 používala dvojitou strukturu, která oddělovala transportní a rámcové vrstvy pro protokoly IPv4 a IPv6 a která byla založená na samostatných ovladačích: `Tcpip.sys` a `Tcpip6.sys`. Jen transportní a rámcové vrstvy pro protokol IPv4 byly instalovány ve výchozím na-

stavení, přidání podpory pro protokol IPv6 vyžadovalo nainstalovat dodatečné součásti protokolu IPv6 přes složku Síťová připojení.

Naproti tomu architektura TCP/IP v systémech Windows Vista a Windows Server 2008 byla navržena kompletně celá znovu a nyní používá dvojitou síťovou vrstvu, kde protokoly IPv4 a IPv6 sdílí stejnou transportní a rámcovou vrstvu. Kromě toho protokol IPv6 je instalován a povolen ve výchozím nastavení v nových verzích systému Windows, aby existovala podpora pro nové funkce, jako je aplikace Centrum spolupráce, které používají jen protokol IPv6. Architektura s dvojitou síťovou vrstvou také znamená, že všechna vylepšení výkonu, která platí pro protokol IPv4, platí také pro protokol IPv6. Mezi tato vylepšení patří algoritmus CTCP (Compound TCP), technologie Receive Windows Auto-Tuning a další funkce, které mohou významně vylepšit výkon v síťových prostředích s velkým zpožděním a velkou ztrátovostí.

Poznámka: Více informacích o vylepšení výkonu architekturou TCP/IP nové generace najdete v kapitole 26, *Nastavení sítě*.

Přehled vylepšení protokolu IPv6 v systému Windows Vista

Následující seznam obsahuje změny v protokolu IPv6 podporované systémem Windows Vista ve srovnání se staršími verzemi systému Windows:

- **Architektura dvojité síťové vrstvy:** Architektura TCP/IP nové generace, která používá stejné transportní a rámcové vrstvy pro protokol IPv4 i IPv6.
- **Povolené ve výchozím nastavení:** Protokoly IPv4 a IPv6 jsou instalovány a povoleny ve výchozím nastavení a architektura upřednostňuje protokol IPv6, když je to vhodné, aniž by negativně ovlivnila komunikaci protokolem IPv4 na dané síti. Pokud třeba dotazy na názvy DNS vrací hostitelskému počítači jak adresy IPv4, tak adresy IPv6, klientský počítač zkusí nejprve použít protokol IPv6 pro komunikaci s hostitelským počítačem. Tato priorita také vylepšuje výkon aplikací používajících protokol IPv6.
- **Podpora konfigurace uživatelským rozhraním:** Kromě konfigurování protokolu IPv6 z příkazového řádku pomocí příkazů v kontextu netsh interface ipv6 jej můžete rovněž konfigurovat pomocí uživatelského rozhraní. Více informací najdete později v této kapitole, v části *Konfigurace protokolu IPv6 v systému Windows Vista pomocí uživatelského rozhraní*.
- **Plná podpora protokolu IPsec:** Podpora protokolu IPv6 ve starších verzích systému Windows nabízela jen omezenou ochranu síťového provozu protokolem IPsec. V systému Windows Vista je však podpora protokolu IPsec pro protokol IPv6 srovnatelná s podporou pro protokol IPv4, můžete konfigurovat pravidla zabezpečení připojení u protokolu IPv6 stejně jako u protokolu IPv4, a to pomocí modulu snap-in Brána firewall systému Windows s vyspělým zabezpečením konzoly MMC.
- **Podpora protokolu LLMNR:** Implementace protokolu IPv6 v systému Windows Vista podporuje protokol LLMNR (Link-Local Multicast Name Resolution), který umožňuje uzlům IPv6 na stejné podsíti rozlišovat názvy ostatních uzlů bez přítomnosti serveru DNS. Protokol LLMNR funguje tak, že nechá uzly odesílat dotazy multicast na názvy DNS místo dotazů unicast. Počítače se systémem Windows Vista naslouchají síťovému provozu multicast protokolu LLMNR ve výchozím nasta-

vení, což eliminuje potřebu provádět rozlišování názvů lokálních podsítí pomocí protokolu NetBIOS nad architekturou TCP/IP, když není dostupný server DNS. Protokol LLMNR je momentálně na cestě k tomu, aby se stal standardem RFC.

- **Podpora protokolu MLD verze 2:** Implementace protokolu IPv6 v systému Windows Vista podporuje protokol MLD verze 2 (Multicast Listener Discovery version 2), popsaný standardem RFC 3810, který umožňuje hostitelským počítačům IPv6 registrovat zájem o přenos dat multicast z určitého zdroje u místních směrovačů multicast specifikováním zahrnujícího (zahrnuje určité zdrojové adresy, o které je zájem) a vyřazujícího (vyřazuje nežádoucí zdrojové adresy) seznamu.
- **Podpora DHCP verze 6:** Služba Klient DHCP systému Windows Vista podporuje protokol DHCP pro protokol IPv6 (protokol DHCPv6), který definují standardy RFC 3736 a 4361. Z toho plyne, že počítače se systémem Windows Vista mohou vykonávat stavovou i bezstavovou konfiguraci protokolem DHCPv6 na sítích s protokolem IPv6.
- **Podpora protokolu IPv6CP:** Vestavěná klientská součást pro vzdálený přístup v systému Windows Vista podporuje protokol IPv6CP (IPv6 Control Protocol) (standard RFC 2472) pro konfiguraci uzlů IPv6 na spojeních protokolu PPP (Point-to-Point Protocol). To znamená, že síťový provoz protokolu IPv6 lze poslat přes síťová připojení založená na protokolu PPP, jako jsou telefonická připojení nebo širokopásmová připojení protokolu PPP nad protokolem Ethernet (PPPoE), k poskytovateli internetových služeb. Protokol IPv6CP také podporuje připojení k virtuálním privátním sítím založená na protokolu L2TP (Layer 2 Tunneling Protocol). Více informací o podpoře protokolu IPv6CP v systému Windows Vista najdete v kapitole 28, *Připojení vzdálených uživatelů a sítí*.
- **Náhodné identifikátory rozhraní:** Systém Windows Vista generuje náhodné identifikátory rozhraní pro automaticky konfigurované adresy IPv6 (ne dočasné), včetně veřejných adres (globálních adres registrovaných v systému DNS) a adres link-local. Více informací najdete později v této kapitole, v části *Zakázání náhodných identifikátorů rozhraní*.
- **Písemné adresy IPv6 v adresách URL:** Systém Windows Vista podporuje písemné adresy IPv6 v adresách URL podle standardu RFC 2732 s použitím nového rozhraní API WinINet podporovaného prohlížečem Microsoft Internet Explorer 7.0. To může být užitečné pro řešení problémů s připojením k Internetu u webových serverů podporujících protokol IPv6.
- **Nové chování služby Teredo:** klient služby Teredo zůstává v systému Windows Vista neaktivní, dokud jej neaktivuje nějaká aplikace s podporou protokolu IPv6, která zkouší použít službu Teredo. V systému Windows Vista mohou spustit službu Teredo tři věci: aplikace zkoušející komunikovat s použitím adresy služby Teredo, naslouchající aplikace, která má povolené pravidlo pro funkci Edge Traversal v bráně Windows Firewall (libovolná aplikace podporující protokol IPv6, která chce použít službu Teredo, to může provést jednoduše nastavením příznaku Edge Traversal pomocí rozhraní API brány Windows Firewall) a pomocné rozhraní API protokolu IP NotifyStableUnicastIpAdressTable. Více informací o pravidlech brány Windows Firewall najdete v kapitole 27, *Konfigurace brány Windows Firewall a protokolu IPsec*.

Jak to funguje: Chování služby Teredo v systému Windows Vista

Služba Teredo je povolena ve výchozím nastavení, ale je neaktivní jak pro skupiny, tak pro domény. Služba Teredo se aktivuje ve dvou hlavních případech:

- Aplikace zkouší komunikovat za použití adresy služby Teredo (například pomocí adresy URL s adresou Teredo ve webovém prohlížeči). Toto je aktivování služby Teredo přenosem odchozích dat a služba Teredo se opět deaktivuje po 60 minutách neaktivity. Brána firewall hostitelského počítače dovolí jen přenos příchozích dat, která odpovídají určitému odchozímu požadavku, zajišťuje tak zachování zabezpečení systému. To se nijak neliší od toho, jak funguje zahajování přenosem odchozích dat u protokolu IPv4. (Jinými slovy – přenos všech odchozích dat je povolen ve výchozím nastavení a stavová tabulka povoluje odpovědi, které korespondují s odchozími požadavky.)
- Aplikace nebo služba má oprávnění používat službu Teredo díky upřesňujícímu příznaku Edge Traversal brány Windows Firewall. Pokud aplikace má příznak Edge Traversal, může přijímat libovolná příchozí data službou Teredo z libovolného zdroje (jako je nevyžádaný přenos dat). Nástroje Centrum spolupráce a Vzdálená pomoc si tento příznak nastavují automaticky, ale uživatelé jej mohou nastavit ostatním službám systému Windows Vista, pokud budou chtít.

Michael Surkan,
programový manažer pro protokoly TCP a IPv6.

Konfigurace a řešení problémů s protokolem IPv6 v systému Windows Vista

Přestože protokol IPv6 byl navržen, aby uzlům s podporou protokolu, jako jsou počítače se systémem Windows Vista, umožnil automaticky nastavovat svým rozhraním adresy link-local, tyto automaticky konfigurované adresy nejsou registrovány na serverech DNS a lze je použít jen pro komunikaci s ostatními uzly na lokálním spojení. Eventuálně můžete pomocí serveru DHCPv6 automaticky přiřadit globální, site-local nebo jedinečnou lokální adresu IPv6 k rozhraním spojení přiřazeného těmto uzlům. Toto je upřednostňovaný způsob připojení mezi koncovými body protokolem IPv6 v prostředích, která mají síťovou infrastrukturu založenou na protokolu IPv6.

Můžete však tyto dvě metody použít také pro ruční konfiguraci protokolu IPv6 na počítačích se systémem Windows Vista:

- Pomocí nového uživatelského rozhraní protokolu IPv6.
- Pomocí příkazů v kontextu `netsh interface ipv6`.

Navíc je důležité rozumět rozdílům mezi různými druhy adres IPv6 přiřazovaných počítačům se systémem Windows Vista, abyste mohli řešit problémy s připojením protokolu IPv6, pokud nastanou.

Zobrazení nastavení adres IPv6

Abyste zobrazili konfiguraci adres IPv4 a IPv6 na lokálním počítači, spusťte příkazový řádek a zadejte do něj příkaz `ipconfig /all`. Následující příklad ukazuje informace zobrazené tímto příkazem o počítači se systémem Windows Vista, který je připojen k doméně, má jediný síťový adaptér, nemá žádná další síťová připojení a na připojené podsíti nejsou žádné směrovače IPv6:

```
Konfigurace protokolu IP systému Windows

   Název hostitele . . . . . : KBERG-PC
   Primární přípona DNS. . . . . : contoso.cz
   Typ uzlu. . . . . : hybridní
   Povoleno směrování IP . . . . . : Ne
   WINS Proxy povoleno . . . . . : Ne
   Seznam hledání přípon DNS . . . . : contoso.cz

Adaptér sítě Ethernet Připojení k místní síti:

   Přípona DNS podle připojení . . . :
   Popis . . . . . : Broadcom 440x 10/100 Integrated
                                 Controller
   Fyzická adresa. . . . . : 00-C0-9F-6E-D5-02
   Protokol DHCP povolen . . . . . : Ne
   Automatická konfigurace povolena. : Ano
   Spojení - místní adresa IPv6. . . : fe80::3530:6107:45a2:a92c%8
                                 (Preferované)
   Adresa IPv4 . . . . . : 172.16.11.13(Preferované)
   Maska podsítě . . . . . : 255.255.255.0
   Zapůjčeno . . . . . : 29. října 2007 16:03:56
   Zápůjčka vyprší . . . . . : 28. října 2008 16:03:55
   Výchozí brána . . . . . : 172.16.11.1
   Server DHCP . . . . . : 172.16.11.32
   IAID DHCPv6 . . . . . : 150998581
   Servery DNS . . . . . : 172.168.11.32
   Rozhraní NetBios nad protokolem TCP/IP. . . . . : Povoleno

Adaptér pro tunelové připojení Připojení k místní síti* 6:

   Přípona DNS podle připojení . . . :
   Popis . . . . . : isatap.{1F1E1761-FF83-4866-
                                 AE6C-9FCEE1E49099}
   Fyzická adresa. . . . . : 00-00-00-00-00-00-00-E0
   Protokol DHCP povolen . . . . . : Ne
   Automatická konfigurace povolena  : Ano
   Spojení - místní adresa IPv6. . . : fe80::5efe: 172.16.11.13%9
                                 (Preferované)
   Výchozí brána . . . . . :
   Servery DNS . . . . . : 172.168.11.32
   Rozhraní NetBios nad protokolem TCP/IP . . . . . : Povoleno

Adaptér pro tunelové připojení Připojení k místní síti* 7:
   Přípona DNS podle připojení . . . :
   Popis . . . . . : Teredo Tunneling Pseudo-Interface
   Fyzická adresa. . . . . : 02-00-54-55-4E-01
   Protokol DHCP povolen . . . . . : Ne
   Automatická konfigurace povolena  : Ano
   Adresa IPv6 . . . . . : 2001:0:4136:e38c:3481:2fbb:3f57:fecd
                                 (Preferované)
   Spojení - místní adresa IPv6. . . : fe80::3481:2fbb:3f57:fecd%11
```

```
                                    (Preferované)
   Výchozí brána . . . . . . . . . . . : : :
   NetBIOS nad TCP/IP. . . . . . . . . : zakázáno
```

Předchozí výstup příkazu zobrazuje tři rozhraní počítače:

- Připojení k místní síti (instalovaný síťový adaptér).
- Připojení k místní síti* 6 (rozhraní tunelování pro protokol ISATAP).
- Připojení k místní síti* 7 (rozhraní tunelování pro službu Teredo).

Rozhraní Připojení k místní síti je síťový adaptér protokolu Ethernet a má přiřazenou adresu IPv4 (`172.16.11.13`) od serveru DHCP a adresu link-local IPv6 (`fe80::35-30:6107:45a2:a92c`) automaticky přidělenou pomocí automatické konfigurace adres IPv6. (Adresu link-local můžete poznat podle prexifu adresy `FE80::/64`.)

Přípona `%8` přiřazená této adrese je identifikátor oblasti, která označuje, na jaké části sítě se daný počítač nachází. Identifikátor oblasti odpovídá indexu rozhraní u rozhraní Připojení k místní síti. Abyste zobrazili seznam všech indexů rozhraní na počítači, zadejte příkaz `netsh interface ipv6 show interface` do příkazového řádku. Pro předchozí příklad by výstup vypadal takto:

```
Idx  Met   MTU   Stav         Název
---  ---  -----  -----------  -------------------
  1   50 4294967295  connected    Loopback Pseudo-Interface 1
  9   25   1280  connected    Připojení k místní síti* 6
 10   10   1280  connected    Připojení k místní síti* 7
  8   20   1500  connected    Připojení k místní síti
```

Sloupec Idx obsahuje indexy rozhraní. Identifikátor oblasti může být nezbytný, když testujete síťové připojení s tímto počítačem z jiných počítačů pomocí příkazů `ping` a `tracert`. Více informací najdete později v této kapitole, v části *Řešení problémů s připojením protokolem IPv6*.

Stav adres link-local přiřazených připojení k místní síti je Preferované, což značí platnou adresu IPv6, kterou můžete použít jako adresu unicast pro odesílání a příjem dat protokolem IPv6.

Rozhraní pro tunelování protokolem ISATAP má automaticky konfigurovanou adresu link-local `fe80::5efe:172.16.11.13`. Formát této adresy ISATAP je:

- Na prvních 64 bitech je prefix unicast, který může být link-local, globální, site-local nebo jedinečný lokální prefix adresy IPv6. Tento příklad používá prefix link-local adresy, protože na síti není přítomen žádný směrovač ISATAP. To znamená, že výsledná adresa ISATAP může být použita jen pro komunikaci s dalšími hostitelskými počítači ISATAP na dané síti IPv4, a tato adresa ISATAP není registrována na servery DNS.
- Dalších 32 bitů adresy ISATAP tvoří obvykle `0:5EFE`. (Standard RFC 4214 také povoluje `100:5EFE`, `200:5EFE` a `300:5EFE` v této části adresy ISATAP.)
- Posledních 32 bitů tvoří 32bitová adresa IPv4 hostitelského počítače ve tvaru desítkových čísel s tečkami (172.16.11.13 v tomto příkladu).

Poznámka: Více informací o adresování ISATAP najdete v článku *IPv6 Transition Technologies* na adrese `http://www.microsoft.com/downloads/details.aspx?FamilyID=afe56282-2903-40f3-a5ba-a87bf92c096d` a v článku *Intra-site Automatic Tunel Addressing Protocol Deployment Guide* na adrese `http://www.microsoft.com/downloads/details.aspx?FamilyID=0f3a-8868-e337-43d1-b271-b8c8702344cd`. Více informací najdete později v této kapitole, v části *Protokol ISATAP*.

Pseudorozhraní tunelování služby Teredo zobrazuje adresu IPv6 klienta služby Teredo jako `2001:0:4136:e37c:4e8:3426:53ef:f4f2`. Formát adresy pro klienta služby Teredo je:

- Prvních 32 bitů je vždy prefix služby Teredo, a to `2001::/32`.
- Dalších 32 bitů obsahuje veřejnou adresu IPv4 serveru Teredo, který pomohl nastavit tuto adresu Teredo (u tohoto příkladu `4136:E37C` šestnáctkově se převádí na `65.54.227.124` ve tvaru desítkových čísel s tečkami). Klient Teredo v systému Windows Vista a Windows Server 2008 ve výchozím nastavení zkouší určit adresy IPv4 serverů Teredo rozlišením názvu teredo.ipv6.microsoft.com.
- Následujících 16 bitů je rezervováno pro různé příznaky služby Teredo.
- Následujících 16 bitů obsahuje zatemněnou verzi čísla externího portu UDP, která odpovídá všem přenášeným datům služby Teredo pro daného klienta Teredo. (Číslo externího portu UDP se zatemňuje operací XOR s druhým operátorem `0xFFFF`, v tomto příkladě `0x3426 XOR 0xFFFF = 0xCBD9` nebo desítkově `52185`, což představuje port UDP 52185.)
- Posledních 32 bitů obsahuje zatemněnou verzi externí adresy IPv4, která odpovídá přenosu všech dat služby Teredo pro tohoto klienta Teredo. (Externí adresa IPv4 se zatemňuje operací XOR s druhým operandem `0xFFFF FFFF`, v tomto příkladu tedy `0x53EF F4F2 XOR 0xFFFF FFFF = 0xAC10 0B0D` nebo ve formě desítkových čísel s tečkami `172.16.11.13`.)

Poznámka: Sdružení IANA vyhradilo prefix adresy IPv6 `2001::/32` pro službu Teredo od ledna 2006 (více podrobností najdete ve standardu RFC 4830 na adrese `http://www.rfc-editor.org/rfc/rfc4380.txt`). Klienti služby Teredo v systému Windows XP používali původně prefix `3FFE:831F::/32`. Klienti služby Teredo v systému Windows XP s aktualizací Microsoft Security Bulletin MS06-64, k dispozici na adrese `http://www.microsoft.com/technet/security/Bulletin/ MS06-64.mspx`, nyní používají prefix `2001::/32`.

Dalším způsobem zobrazení nastavení protokolu IPv6 na počítači se systémem Windows Vista je zadat příkaz `netsh interface ipv6 show address` do příkazového řádku. Výsledek pro stejný počítač jako v předchozím příkladě by vypadal takto:

```
Rozhraní 1: Loopback Pseudo-Interface 1

Typ adresy  Stav DAD   Platná doba života Upřed. doba života Adresa
---------  ----------- ---------- ---------- ------------------------
Jiné       Upřednostňovaný   infinite   infinite ::1

Rozhraní 9: Připojení k místní síti* 6

Typ adresy  Stav DAD   Platná doba života Upřed. doba života Adresa
---------  ----------- ---------- ---------- ------------------------
```

```
Jiné       Upřednostňovaný   infinite   infinite fe80::5efe:172.16.11.13%9

Rozhraní 10: Připojení k místní síti* 7

Typ adresy  Stav DAD   Platná doba života Upřed. doba života Adresa
---------  ----------- ---------- ---------- -----------------------
Veřejná    Upřednostňovaný   infinite   infinite 2001:0:4136:e37c:1071:
                                                3426:31d2:bfce
Jiné       Upřednostňovaný   infinite   infinite fe80::1071:3426:31d2:
                                                bfce%10

Rozhraní 8: Připojení k místní síti

Typ adresy  Stav DAD   Platná doba života Upřed. doba života Adresa
---------  ----------- ---------- ---------- -----------------------
Jiné       Upřednostňovaný   infinite   infinite fe80::3530:6107:45a2:
                                                a92c%8
```

Poznámka: Výhodou zobrazení nastavení adres IPv6 pomocí příkazu `netsh interface ipv6 show address` místo příkazu `ipconfig` je, že příkaz `netsh` můžete zadávat vzdáleně díky parametru `-r NázevVzdálenéhoPočítače`.

Více informací o tom, jak používat nástroje Ipconfig, Netsh a jiné nástroje pro zobrazení konfigurace protokolu IPv6, najdete v článku *Using Windows Tools to Obtaion IPv6 Configuration Information* na adrese `http://www.microsoft.com/technet/itsolutions/network/ipv6/ipv6config.mspx`.

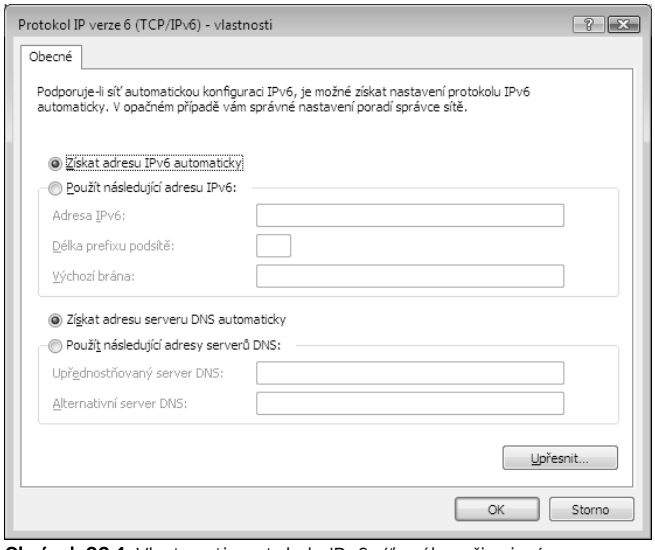
Konfigurace protokolu IPv6 v systému Windows Vista pomocí uživatelského rozhraní

Protokol IPv6 pro síťové připojení v systému Windows Vista můžete konfigurovat pomocí uživatelského rozhraní, stačí se řídit těmito kroky:

1. Klepněte na tlačítko Start, vyberte položku Síť, klepněte na položku Centrum sítí a sdílení.
2. Klepněte na odkaz Spravovat síťová připojení a poklepejte na síťové připojení, které chcete konfigurovat.
3. Klepněte na tlačítko Vlastnosti a reagujte na výzvu Řízení uživatelských účtů.
4. Vyberte položku Protokol IP verze 6 (TCP/IPv6) a klepněte na tlačítko Vlastnosti, abyste otevřeli dialogové okno Protokol IP verze 6 (TCP/IPv6) (viz obrázek 29.1).
5. Konfigurujte protokol IPv6 pro dané síťové připojení dle libosti.

Výchozí nastavení protokolu IPv6 pro síťové připojení jsou následující:

- **Získat adresu IPv6 automaticky:** Toto určuje, že fyzické nebo logické rozhraní přiřazené tomuto připojení používá stavovou nebo bezstavovou automatickou konfiguraci, aby získalo svou adresu IPv6.
- **Získat adresu serveru DNS automaticky:** Toto určuje, že fyzické nebo logické rozhraní přiřazené tomuto připojení používá stavovou automatickou konfiguraci (DHCPv6), aby získalo adresy IPv6 preferovaných a alternativních serverů DNS.



Obrázek 29.1: Vlastnosti protokolu IPv6 síťového připojení

Volbou možnosti Použít následující adresu IPv6 můžete ručně konfigurovat adresu IPv6 pro síťové připojení tak, že zadáte údaje do následujících polí:

- **Adresa IPv6:** Zadejte adresu unicast IPv6, kterou chcete přiřadit fyzickému nebo logickému rozhraní přiřazenému tomuto připojení, a to ve tvaru šestnáctkových čísel s dvojtečkami. Pokud potřebujete tomuto rozhraní přiřadit další adresy unicast IPv6, klepněte na tlačítko Upřesnit a vyberte záložku Nastavení protokolu IP.
- **Délka prefixu podsítě:** Zadejte délku prefixu podsítě pro adresu IPv6, kterou jste přiřadili fyzickému nebo logickému rozhraní přiřazenému tomuto připojení. U adres unicast IPv6 by měla být délka prefixu podsítě vždy 64.
- **Výchozí brána:** Zadejte adresu unicast IPv6 výchozí brány pro lokální podsíť IPv6 ve tvaru šestnáctkových čísel s dvojtečkami. Jestliže potřebujete specifikovat dodatečné výchozí brány, klepněte na tlačítko Upřesnit a potom vyberte záložku Nastavení protokolu IP.

Volbou možnosti Použít následující adresy serverů DNS můžete ručně nastavit adresy IPv6 pro preferovaný a alternativní server DNS vašeho síťového připojení. Pokud potřebujete zadat dodatečné alternativní servery DNS, klepněte na tlačítko Upřesnit a potom vyberte záložku DNS. Zbývající nastavení pod záložkou DNS fungují stejně jako ta, kterými konfigurujete adresu IPv4.

Poznámka: Dialogové okno Upřesnit nastavení TCP/IP neobsahuje záložku WINS, protože protokol IPv6 nepoužívá protokol NetBIOS pro rozlišování názvů.

Konfigurace protokolu IPv6 v systému Windows Vista pomocí nástroje Netsh

Abyste konfigurovali protokol IPv6 pro síťové připojení v systému Windows Vista nástrojem Netsh, spusťte příkazový řádek jako správce systému a zadejte příslušný příkaz

nástroje Netsh v kontextu `netsh interface ipv6 context`. Několik příkladů konfigurace protokolu IPv6 z tohoto kontextu:

- Pro přidání adresy unicast IPv6 `2001:DB8::8:800:20C4:0` k rozhraní s názvem Připojení k místní síti jako trvalé adresy IPv6 s nekonečnou platností a časovými limity preferování zadejte následující příkaz:

```
netsh interface ipv6 add address "Připojení k místní síti"
      2001:DB8::8:800:20C4:0
```

- Abyste nastavili výchozí bráně adresu unicast IPv6 `2001:DB8:0:2F3B:2AA:FF:FE28: 9C5A` pro rozhraní s názvem Připojení k místní síti, přidejte výchozí cestu s touto adresou specifikovanou jako adresa příštího skoku (adresa next-hop) zadáním následujícího příkazu:

```
netsh interface ipv6 add route ::/0 "Připojení k místní síti"
      2001:DB8:0:2F3B:2AAA:FF:FE28:9C5A
```

- Abyste nastavili adresu unicast IPv6 2001:DB8:0:1::1 jako druhý (alternativní) server DNS v seznamu serverů DNS pro rozhraní s názvem Připojení k místní síti, zadejte následující příkaz:

```
netsh interface ipv6 add dnsserver "Připojení k místní síti"
      2001:DB8:0:1::1 index=2
```

Nápovědu kontextu `netsh interface ipv6` získáte zadáním příkazu `netsh interface ipv6 /?` do příkazového řádku.

Další úlohy konfigurace protokolu IPv6

Následující části popisují některé dodatečné úlohy konfigurace protokolu IPv6, u kterých by měli správci sítě vědět, jak je provést na počítačích se systémem Windows Vista.

Povolení nebo zakázání protokolu IPv6

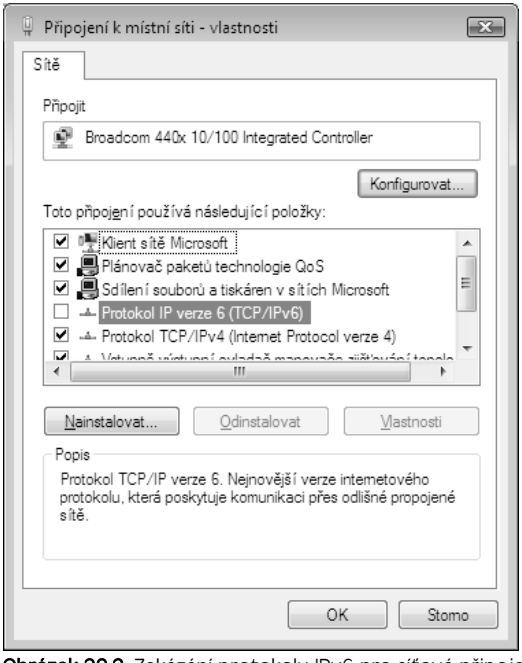
Protokol IPv6 nemůžete odinstalovat ze systému Windows Vista, ale můžete protokol IPv6 zakázat pro jednotlivá síťová připojení. Postupujte následovně:

1. Klepněte na tlačítko Start, vyberte položku Síť, klepněte na položku Centrum sítí a sdílení.
2. Klepněte na odkaz Spravovat síťová připojení a poklepejte na síťové připojení, které chcete konfigurovat.
3. Klepněte na tlačítko Vlastnosti a reagujte na výzvu Řízení uživatelských účtů.
4. Zrušte zaškrtnutí pole Protokol IP verze 6 (TCP/IPv6) a klepněte na tlačítko OK (viz obrázek 29.2).

Pokud zakážete protokol IPv6 pro všechna síťová připojení za použití metody konfigurace uživatelským rozhraním, popsané v předchozím postupu, protokol IPv6 stále zůstane povolen na rozhraních tunelování a na rozhraní zpětné smyčky.

Alternativou k zakázání protokolu IPv6 pro jednotlivá připojení pomocí uživatelského rozhraní je výběrově zakázat určité funkce protokolu IPv6 vytvořením a konfigurací následující hodnoty typu DWORD v registru systému:

HKLM\SYSTEM\CurrentControlSet\Services\tcpip6\Parametres\DisabledComponents



Obrázek 29.2: Zakázání protokolu IPv6 pro síťové připojení

Tabulka 29.7 popisuje hodnoty příznaku, který kontroluje jednotlivé funkce protokolu IPv6. Kombinací těchto hodnot příznaku do bitové masky můžete zakázat několik funkcí současně (ve výchozím nastavení má příznak `DisabledComponents` hodnotu `0`).

Tabulka 29.7: Hodnoty bitové masky pro zakázání funkcí protokolu IPv6 v systému Windows Vista

Pořadové číslo bitu v příznaku	Výsledek nastavení hodnoty tohoto bitu na 1
0	Zakáže všechna rozhraní tunelování protokolu IPv6, včetně tunelů ISATAP, 6to4 a Teredo.
1	Zakáže všechna rozhraní založená na protokolu 6to4.
2	Zakáže všechna rozhraní založená na protokolu ISATAP.
3	Zakáže všechna rozhraní založená na službě Teredo.
4	Zakáže protokol IPv6 nad všemi rozhraními, která neslouží tunelování, včetně rozhraní místní sítě a protokolu PPP (Point-to-Point).
5	*Upraví tabulku zásad výchozích prefixů, aby upřednostnila protokol IPv4 před protokolem IPv6 při pokusech o připojení.

* Více informací týkajících se tabulky zásad prefixů protokolu IPv6 najdete v článku *Source and Destination Address Selection for IPv6* na adrese `http://www.microsoft.com/ technet/community/columns/cableguy/cg0206.mspx`.

Například nastavením hodnoty `DisabledComponents` na `0xFF` můžete současně zakázat protokol IPv6 na všech vašich síťových připojeních a rozhraních tunelování. Pokud to provedete, protokol IPv6 bude však stále povolen na rozhraní zpětné smyčky.

Poznámka: Další příklady běžných kombinací příznaku, kterými lze povolit nebo zakázat různé funkce protokolu IPv6 v systému Windows Vista, najdete v článku *Changes to IPv6 in Windows Vista and Windows Server 2008* na adrese `http://www.microsoft.com/technet/community/columns/cableguy/cg1005.mspx`.

Zakázání náhodných identifikátorů rozhraní

Můžete zakázat generování náhodných identifikátorů rozhraní ve výchozím nastavení pro automaticky konfigurované veřejné adresy (které nejsou dočasné, tedy globální adresy registrované na serveru DNS) a adresy link-local pomocí následujícího příkazu:

```
netsh interface ipv6 set global randomizeidentifiers=disabled
```

Abyste znovu povolili generování náhodných identifikátorů rozhraní, zadejte následující příkaz:

```
netsh interface ipv6 set global randomizeidentifiers=enabled
```

Poznámka: Zakázání náhodných identifikátorů rozhraní způsobuje, že se adresy link-local vrátí zpět k 48bitovým adresám MAC (nebo 64bitovým EUI) pro generování části adresy s identifikátorem rozhraní. V systému Windows Vista se tak stane okamžitě, nemusíte tedy počítač restartovat.

Resetování konfigurace protokolu IPv6

Odstranit všechna uživatelská nastavení protokolu IPv6 a obnovit konfiguraci protokolu IPv6 do výchozího stavu můžete zadáním následujícího příkazu:

```
netsh interface ipv6 reset
```

Aby se změny způsobené tímto příkazem projevily, musíte restartovat počítač.

Zobrazení stavu klienta služby Teredo

Aktuální stav klienta služby Teredo na vašem počítači ověříte tak, že spustíte příkazový řádek jako správce systému a zadáte následující příkaz:

```
netsh interface teredo show state
```

U počítače se systémem Windows Vista, na kterém není služba Teredo právě aktivní, by výstup tohoto příkazu vypadal nějak takto:

```
Parametry služby Teredo
---------------------------------------------
Typ: default
Název serveru: teredo.ipv6.microsoft.com.
Interval aktualizace klienta: 30 s
Port klienta: unspecified
Stav: dormant
Typ klienta: Teredo klient
Síť: managed
NAT: none (global connectivity)
```

Poznámka: Pokud váš výstup příkazu neobsahuje všechny předchozí informace, pravděpodobně jste spustili příkazový řádek běžným způsobem, a ne jako správce systému.

Když nyní spustíte aplikaci s podporou protokolu IPv6, která používá službu Teredo, například nástroj Centrum spolupráce nebo Vzdálená pomoc, a zadáte stejný příkaz nástroje Netsh, výstup příkazu bude zřejmě teď vypadat takto:

```
Parametry služby Teredo
------------------------------------------------
Typ: default
Název serveru: teredo.ipv6.microsoft.com.
Interval aktualizace klienta: 30 s
Port klienta: unspecified
Stav: qualified
Typ klienta: Teredo klient
Síť: managed
NAT: restricted
```

Po srovnání těchto dvou výstupů příkazu zjistíte, že spuštění aplikace používající službu Teredo změnilo stav klienta služby Teredo z `dormant` (neaktivní) na `qualified` (aktivní).

Poznámka: Výstup příkazu `netsh interface teredo show state` také říká, jaký je typ služby NAT (pokud vůbec nějaký). V předchozím příkladě byl počítač schován za službou NAT typu `restricted`. Služba Teredo funguje správně, když je schovaná za službou NAT typu `restricted` nebo `cone`, ale ne za službou NAT typu `symmetric`. Pokud plánujete koupit směrovač SOHO pro širokopásmové připojení k Internetu, nejlepší volbou je směrovač s podporou protokolu 6to4. Více informací o různých typech služby NAT a o tom, jak funguje služba Teredo, najdete v článku *Teredo Overview* na adrese `http://www.microsoft.com/technet/prodtechnol/ winxppro/maintain/teredo.mspx`.

Řešení problémů s připojením protokolem IPv6

Standardní přístup k řešení problémů se síťovými připojeními architektury TCP/IP na sítích IPv4 představuje následující postup:

- Zadejte příkaz `ipconfig /all` do příkazového řádku, abyste ověřili konfiguraci protokolu IPv4 na počítači, na kterém nastaly problémy.
- Jestliže ověřujte konfiguraci protokolu IPv4 na počítači, na kterém nenastaly problémy, zkuste použít příkaz `ping`, abyste otestovali síťové připojení, začněte u lokálního počítače a postupuje vně, dokud nerozpoznáte příčinu problému. Postupujte následovně:
  - Zašlete požadavek na odezvu na adresu zpětné smyčky `127.0.0.1`, abyste ověřili, že architektura TCP/IP je na počítači nainstalována a nakonfigurována správně.
  - Potom zašlete požadavek na odezvu na adresu IPv4 lokálního počítače.
  - Potom zašlete požadavek na odezvu na adresu IPv4 výchozí brány.
  - Potom zašlete požadavek na odezvu na adresu IPv4 hostitelského počítače IPv4 na vzdálené podsíti.

Mezi další způsoby řešení problémů s architekturou TCP/IP na sítích IPv4 patří:

- Použijte příkaz `route print` k ověření konfigurace směrovací tabulky lokálního počítače.

- Použijte příkaz `tracert` k ověření toho, že mezilehlé směrovače jsou konfigurovány správně.
- Použijte příkaz `pathping` ke zjištění ztrátovosti paketu na cestách s více uzly.
- Vyprázdněte vyrovnávací paměť protokolu ARP zadáním příkazu `netsh interface ip delete arpcache` do příkazového řádku.
- Ověřte konfiguraci protokolu DNS, vyprázdněte vyrovnávací paměť pro synchronní přenosy klienta DNS a ověřte funkci rozlišování názvů DNS.

Poznámka: Více informací o tom, jak systematicky řešit problémy s připojeními protokolem IPv4, najdete v kapitole 32.

K řešení problémů s připojeními k síti protokolem IPv6 použijete řadu stejných nástrojů jako u řešením problému s protokolem IPv4. Avšak některé z těchto nástrojů použijete jiným způsobem, což vyplývá z povahy adresování IPv6 a způsobu implementace protokolu IPv6 v systému Windows Vista. Mezi tyto rozdíly patří:

- Pravděpodobně budete muset specifikovat identifikátor oblasti, když zkusíte ověřit síťové připojení protokolem IPv6 s cílovým hostitelským počítačem pomocí příkazu `ping`. Zápis toho příkazu pro protokol IPv6 bude vypadat takto: `ping adresaIPv6%IdentifikátorOblasti`, kde `IdentifikátorOblasti` je identifikátorem oblasti cílového hostitelského počítače. Kdyby třeba cílový hostitelský počítač měl adresu link-local unicast `IPv6 FE80::D3:00FF:FE28:9C5A` přiřazenou rozhraní s identifikátorem oblasti 12, zadali byste do příkazového řádku příkaz `ping FE80::D3:00FF:FE28:9C5A%12`. Identifikátor oblasti příslušeného rozhraní zjistíte buď zadáním příkazu `ipconfig /all`, nebo příkazu `netsh interface ipv6 show interface` do příkazového řádku. Zapamatujte si, že ačkoliv identifikátor oblasti je definován lokálně, odesílající a přijímající počítač na stejném spojení mohou mít jiné identifikátory oblasti. (Globální adresy unicast IPv6 nepotřebují identifikátory oblasti.)
- Měli byste prohlédnout a vyprázdnit vyrovnávací paměť sousedních uzlů na vašem počítači, než zkusíte příkazem `ping` ověřovat síťové připojení protokolem IPv6. Vyrovnávací paměť sousedních uzlů obsahuje nedávno rozpoznané adresy link-local IPv6, můžete ji prohlédnout příkazem `netsh interface ipv6 show neighbors` a vyprázdnit příkazem `netsh interface ipv6 delete neighbors` v příkazovém řádku spuštěném s právy správce systému.
- Měli byste také prohlédnout a vyprázdnit vyrovnávací paměť cílů na vašem počítači, než zkusíte ověřit síťové připojení protokolem IPv6 pomocí příkazu `ping`. Vyrovnávací paměť cílů obsahuje adresy příštího skoku IPv6 pro cíle. Tuto vyrovnávací paměť můžete prohlédnout příkazem `netsh interface ipv6 show destinationcache` a vyprázdnit příkazem `netsh interface ipv6 delete destinationcache` v příkazovém řádku spuštěném s právy správce systému.
- Měli byste použít parametr `-d`, pokud zkoušíte najít cestu ke vzdálenému hostitelskému počítači IPv6 příkazem `tracert`, nebo parametr `-n`, když používáte příkaz `pathping`. Tyto parametry brání daným příkazům ve vykonávání dotazů zpětného vyhledávání názvů DNS na všech rozhraních směrovačů podél směrovací cesty. Tyto parametry mohou pomoct zrychlit zobrazení směrovací cesty.

Poznámka: Více informací o řešení problémů se síťovými připojeními protokolem IPv6 najdete v článku *Troubleshooting IPv6* na adrese `http://www.microsoft.com/technet/community/columns/cableguy/cg0305.mspx`. Prohlédněte také kapitolu 12, *Troubleshooting TCP/IP*, v knize online *TCP/IP Fundamentals for Microsoft Windows*, kterou můžete stáhnout na adrese `http://www.microsoft.com/downloads/details.aspx?FamilyID=c76296fd-61c9-4079-a0bb-582bca4a846f`.

Poznámka: Zakázání protokolu IPv4 může také být užitečnou technikou pro řešení problémů, když chtějí programátoři ověřit, že jejich aplikace jsou kompatibilní s protokolem IPv6.

Plán migrace k protokolu IPv6

Migrace vaší existující síťové infrastruktury založené na protokolu IPv4 k protokolu IPv6 vyžaduje, abyste porozuměli různým technikám přechodu k protokolu IPv6, které vám mohou pomoci. Systémy Windows Vista a Windows Server 2008 podporují tři takové technologie:

- **Protokol ISATAP:** ISATAP je zkratka pro Intra-site Automatic Tunnel Adressing Protocol, technologii přiřazování adres a automatického tunelování, definovanou standardem RFC 4214, která může poskytnout připojení unicast protokolem IPv6 mezi hostitelskými počítači IPv6/IPv4 (hostitelské počítače, které podporují protokol IPv6 i IPv4) přes intranet založený na protokolu IPv4 (privátní síť, jejíž hardwarová infrastruktura, jako jsou směrovače, podporuje pouze protokol IPv4, ale ne protokol IPv6).
- **Protokol 6to4:** Technologie přiřazování adres a automatického tunelování, definovaná standardem RFC 3056, která může poskytnout připojení unicast protokolem IPv6 mezi hostitelskými počítači IPv4/IPv6 a místy přes veřejný Internet založený na protokolu IPv4. Protokol 6to4 umožňuje přiřazovat globální adresy IPv6 uvnitř privátní sítě, aby vaše počítače mohly přistupovat k různým místům na Internetu založeném na protokolu IPv6, aniž by musely být k Internetu připojeny přímo, nebo přes prefix globální adresy IPv6 přidělený poskytovatelem internetových služeb. (Komunikace mezi uzly s podporou protokolu 6to4 a uzly s podporou protokolu IPv6 vyžaduje však přenos protokolem 6to4.)
- **Služba Teredo:** Technologie přiřazování adres a automatického tunelování, definovaná standardem RFC 4380, která může poskytnout připojení unicast protokolem IPv6 mezi hostitelskými počítači IPv6/IPv4 přes veřejný Internet založený na protokolu IPv4, když jsou tyto hostitelské počítače schovány za jednou nebo více službami NAT. Služba Teredo nabízí obdobnou funkcionalitu jako protokol 6to4, ale nevyžaduje, aby koncová zařízení podporovala tunelování 6to4.

Poznámka: Více informací o technologiích přechodu mezi protokoly IPv4 a IPv6 najdete v článku *IPv6 Transition Technologies* na adrese `http://www.microsoft.com/downloads/ details.aspx?FamilyID=afe56282-2903-40f3-a5ba-A87bf92c096d&DisplayLang=en`.

Tyto tři technologie přechodu k protokolu IPv6 jsou dostupné v operačních systémech Windows Vista, Windows Server 2008, Windows XP Service Pack 2 a Windows Server

2003 Service Pack 1. Z těchto tří je protokol ISATAP hlavní technologií přechodu, kterou byste měli používat pro migraci existujícího intranetu založeného na protokolu IPv6 – je popsán podrobněji v následujících částech. Služba Teredo je především užitečná pro prostředí domácí kanceláře nebo malé firmy (prostředí SOHO), kde širokopásmové směrovače s podporou služby NAT poskytují uživatelům přístup k Internetu. (O službě Teredo jako technologii přechodu přemýšlejte až v posledním případě, protože jak vzrůstá počet připojení protokolem IPv6, zájem o službu NAT bude upadat, dokud nebude zbytečná i služba Teredo.)

Jak to funguje: Blokování služby Teredo

Služba Teredo je spotřebitelskou technologií a není příliš doporučována pro firmy. Je tomu tak proto, že služba Teredo požaduje, aby koncová zařízení umožňovala přenos odchozích dat protokolem UDP. Například řada správců systému nechce z bezpečnostních důvodů umožnit klientským počítačů připojeným k firemní síti přístup k Internetu; v takovém případě je vypnutí služby Teredo dobrý nápad.

Jestliže správci systému chtějí zakázat službu Teredo na klientských počítačích nebo jednoduše blokovat její funkce, mohou to udělat třemi způsoby:

- Blokovat přenos všech odchozích dat protokolem UDP ve výchozím nastavení.
- Blokovat rozlišování názvů u názvů hostitele služby Teredo, což je ve výchozím nastavení počítačů se systémem Windows Vista teredo.ipv6.microsoft.com.
- Pomocí zásad skupiny nebo skriptu vytvořit následující hodnotu typu DWORD v registru systému, která vypne službu Teredo na cílových počítačích se systémem Windows Vista (toto nastavení registru systému není dostupné v zásadách skupiny ve výchozím nastavení, ale lze jej povolit souborem ADMX):

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisabledComponents
```

Tomuto klíči můžete zadat hodnoty:

- **0x10:** nastavením této hodnoty vypnete službu Teredo jen na daném počítači.
- **0x01:** nastavením této hodnoty zakážete všechna rozhraní tunelování na daném počítači.

Pokud správci systému chtějí na svých sítích podporovat jen protokol IPv6 nebo nechtějí povolit žádný přenos dat protokolem IPv6, dokud zcela nezavedou protokol IPv6, mohou vypnout technologie tunelování volbou druhé hodnoty z předchozího seznamu.

Protokol ISATAP

Ve výchozím nastavení systému Windows Vista protokol IPv6 automaticky konfiguruje adresu link-local unicast IPv6 tvaru `FE80::5EFE:w.x.y.z`. Tato adresa se nazývá adresa ISATAP a je přiřazena rozhraní tunelování ISATAP. Pomocí svých adres ISATAP spolu mohou dva hostitelé (například počítače se systémem Windows Vista) komunikovat protokolem IPv6 tunelováním přes síťovou infrastrukturu založenou na protokolu IPv4 (jako je síť se směrovači předávajíícmi jen pakety IPv4, ale ne pakety IPv6).

Přidáním dalšího nebo více směrovačů ISATAP (směrovače s podporou protokolu IPv6, které inzerují prefixy adres, předávají pakety mezi hostitelskými počítači ISATAP a dalšími směrovači ISATAP a vystupují jako výchozí směrovače pro hostitelské počítače ISATAP) lze vytvořit různé topologie přechodů, včetně:

- připojení hostitelských počítačů ISATAP na intranetu jen s podporou protokolu IPv4 k sítím s podporou protokolu IPv6
- připojení několika hostitelských počítačům ISATAP prostřednictvím páteřní sítě s podporou protokolu IPv6

Tato nastavení jsou možná, protože směrovače ISATAP oznamují prefixy adres, které umožňují hostitelům ISATAP (jako jsou počítače se systémem Windows Vista) automaticky konfigurovat globální, site-local nebo jedinečné lokální adresy unicast IPv6. Bez přítomnosti směrovače ISATAP mohou hostitelské počítače ISATAP automaticky konfigurovat jen adresy link-local unicast IPv6, které omezují komunikaci protokolem IPv6 mezi dvěma počítači jen na intranet založený na protokolu IPv4.

Poznámka: Více informací o tom, jak funguje protokol ISATAP, najdete v článku IPv6 Transition Technologies na adrese `http://www.microsoft.com/downloads/details.aspx?FamilyID=afe-56282-2903-40f3-a5ba-a87bf92c096d`.

Migrace intranetu k protokolu IPv6

Nejlepší způsoby migrace existujících síťových infrastruktur založených na protokolu IPv4 k protokolu IPv6 se stále vyvíjí. Tato část kapitoly tedy popisuje jen běžné způsoby migrace intranetu k protokolu IPv6 a odkazuje na další podrobnější informace, které by vás mohly zajímat.

Hlavním cílem migrace od protokolu IPv4 k protokolu IPv6 je dosáhnout toho, abyste měli síťovou infrastrukturu založenou čistě na protokolu IPv6, na které jsou jen počítače podporující protokol IPv6. Z praktických důvodů je však zatím lepší se zaměřit na to, abyste měli síťovou infrastrukturu s podporou protokolu IPv6 i IPv4, na které počítače podporují oba tyto protokoly, ale převážně používají protokol IPv6. Dosáhnout tohoto cíle je velmi dlouhý proces zahrnující sedm hlavních kroků:

1. Aktualizace vašich aplikací a služeb.
2. Příprava vaší infrastruktury DNS.
3. Příprava vaší infrastruktury DHCP.
4. Aktualizace vašich počítačů.
5. Migrace od protokolu IPv4 k protokolu ISATAP.
6. Aktualizace vaší infrastruktury směrovačů.
7. Migrace od protokolu ISATAP k protokolu IPv6.

Aktualizace vašich aplikací a služeb

Abyste připravili své aplikace a služby na migraci, budete muset aktualizovat existující aplikace a služby, aby kromě protokolu IPv4 podporovaly také protokol IPv6. To bude pravděpodobně vyžadovat aktualizace od nezávislých výrobců softwaru nebo vlastní zásah do kódu. Přestože konečným cílem je, aby vaše aplikace a služby podporovaly jen protokol IPv6, mnohem vhodnějším cílem by mělo být, aby podporovaly jak protokol IPv6, tak protokol IPv4.

Návod na to, jak to provést, najdete v článku *IPv6 Guide for Windows Sockets Applications* na adrese `http://msdn2.microsoft.com/en-us/library/ms738649.aspx`.

Příprava vaší infrastruktury DNS

Musíte připravit svoji infrastrukturu DNS, aby podporovala záznamy AAAA pro rozlišování názvů DNS na adresy IPv6. To může vyžadovat aktualizaci stávajících serverů DNS. Služba Server DNS v systému Windows Server 2003 nabízí dynamickou registraci záznamů AAAA pro adresy unicast IPv6 (kromě adres link-local).

Více informací o konfiguraci serverů DNS v systému Windows Server 2003 pro podporu hostitelských počítačů IPv6 najdete v kapitole 9, *Windows Support for DNS*, v knize online TCP/IP Fundamentals for Microsoft Windows, kterou lze najít na adrese `http://www.microsoft.com/technet/network/evaluate/technol/tcpipfund_ch09.mspx`.

Příprava vaší infrastruktury DHCP

Měli byste připravit svoji infrastrukturu DHCP, aby podporovala protokol DHCPv6 pro automatické přiřazování globálních, site-local a jedinečných lokálních adres unicast IPv6 nebo konfiguraci uzlů IPv4/IPv6 na vaší síti. Díky protokolu DHCPv6 mohou hostitelské počítače IPv6 získávat prefixy podsítí a další nastavení protokolu IPv6. Běžně se protokol DHCPv6 používá pro konfiguraci klientských počítačů se systémem Windows Vista s adresami serverů DNS na síti (servery DNS nejsou konfigurovány prostřednictvím služby pro zjišťování směrovačů na sítích IPv6).

Služba Server DHCP v systému Windows Server 2003 nepodporuje stavovou automatickou konfiguraci protokolu DHCPv6. Role Server DHCP v systému Windows Server 2008 však bude podporovat stavovou i bezstavovou automatickou konfiguraci adres pomocí protokolu DHCPv6. Služba Klient DHCP v systémech Windows Vista a Windows Server 2008 nepodporuje automatickou konfiguraci adres pomocí protokolu DHCPv6.

Stejně jako u protokolu DHCP v kombinaci s protokolem IPv4, také zde musíte zavést a konfigurovat agenty přenosu protokolu DHCPv6 pro každou podsíť obsahující klientské počítače se systémem Windows Vista. Spousta směrovačů již nabízí agenty přenosu DHCPv6. Agentům přenosu musíte nastavit adresu IPv6 serverů DHCPv6 na vaší síti. Agenty přenosu lze konfigurovat, ale neměli byste je zapínat, dokud nezavedete směrování protokolu IPv6 na vašich podsítích.

Aktualizace vašich počítačů

Měli byste aktualizovat některé vaše počítače, dokud nebudou všechny počítače podporovat protokol IPv6 i IPv4. Operační systémy Windows již od verze Windows XP Service Pack 2 podporují protokoly IPv4 i IPv6, plná podpora protokolu IPv6 u vestavěných programů a služeb je však dostupná až v systému Windows Vista a novějším.

Migrace od protokolu IPv4 k protokolu ISATAP

Jakmile připravíte vaše aplikace, služby, hostitelské počítače a infrastrukturu DNS/DHCP, můžete začít zavádět směrovače ISATAP, abyste vytvořili ostrůvky založené na protokolu IPv6 uvnitř vašeho intranetu založeného na protokolu IPv4. Musíte přidat záznamy A k příslušným oblastem DNS, aby hostitelské počítače ISATAP mohly určit adresy IPv4 vašich směrovačů ISATAP.

Pravděpodobně se rozhodnete zavést jeden nebo více směrovačů ISATAP pro směrovaní ve vaší podsíti ISATAP uvnitř vašeho intranetu, podle velikosti vašeho intranetu a geografického rozmístění vašich sídel. Možná se rozhodnete zavést dodatečné smě-

rovače ISATAP, aby poskytovaly trvalou dostupnost prefixů adres IPv6 a dalších nastavení pro vaše hostitelské počítače ISATAP. Asi zavedete také jeden nebo více směrovačů, které budou poskytovat připojení protokolem IPv6 mezi síťovou infrastrukturou založenou na protokolu IPv4 a veřejným Internetem založeným na IPv6 během migrace.

Více informací o zavádění směrovačů ISATAP pro různé případy migrace najdete v článku Intra-site Automatic Tunnel Addressing Protocol Deployment Guide na adrese `http://www.microsoft.com/downloads/details.aspx?FamilyID=0f3a8868-e337-43d1-b271-b8c8702344cd`.

Aktualizace vaší infrastruktury směrovačů

Jakmile zavedete protokol ISATAP, který umožní hostitelským počítačům IPv6 komunikovat přes síťovou infrastrukturu založenou na protokolu IPv4, měli byste začít aktualizovat vaši síťovou infrastrukturu (včetně směrovačů, výchozích bran a dalších zařízení pro přístup k síti), aby podporovala protokol IPv6. Raději než aktualizovat vaši infrastrukturu, aby podporovala jen protokol IPv6, je daleko rozumnější aktualizovat na podporu obou protokolů: IPv4 i IPv6. V mnoha případech náhrada hardwaru pro směrování není nutná. Protože spousta moderních hardwarových směrovačů podporuje směrování protokolem IPv4 i IPv6, aktualizace směrovací infrastruktury na podporu protokolu IPv6 se mění na konfiguraci, ne na náhradu. Když povolíte podporu směrování protokolem IPv6, povolte také agenta přenosu protokolem DHCPv6 pro danou podsíť.

Většinou začnete aktualizovat infrastrukturu směrovačů brzo při zavádění protokolu ISATAP aktualizací hlavních směrovačů na páteřní síti pro podporu IPv6. Budete tedy mít části sítě s hostitelskými počítači ISATAP, které se připojují k páteřní síti, aby komunikovaly s dalšími hostitelskými počítači kdekoliv na vašem intranetu.

Migrace od protokolu ISATAP k protokolu IPv6

Když konečně všechna zařízení vaší síťové infrastruktury podporují protokol IPv6, můžete začít vyřazovat z provozu vaše směrovače ISATAP, protože už je nebudete potřebovat. Zda také převedete vaši infrastrukturu a počítače, aby podporovaly jen protokol IPv6, je rozhodnutí, které je lepší nechat na vzdálenou budoucnost.

Shrnutí

Tato kapitola popisovala funkce protokolu IPv6 v systému Windows Vista, obsahovala krátký přehled toho, jak funguje protokol IPv6, a nejlepší techniky migrace existující sítě založené na protokolu IPv4 k protokolu IPv6. Migrace k protokolu IPv6 požaduje opatrné plánování a důkladné porozumění funkcím protokolu IPv6. Systémy Windows Vista a Windows Server 2008 nabízí nástroje, které potřebujete k úspěšné migraci vaší sítě.

Další zdroje

Následující zdroje obsahují dodatečné informace a nástroje týkající se této kapitoly.

Související informace

- Článek *Introduction to IP Version 6* najdete na internetové adrese `http://www.microsoft.com/downloads/details.aspx?FamilyID=CBC0B8A3-B6A4-4952-BBE6-D976624C257C&displaylang=en`.
- Často kladené otázky k protokolu IPv6, *IPv6 for Microsoft Windows: Frequently Asked Questions*, najdete na internetové adese `http://www.microsoft.com/technet/network/ipv6/ipv6faq.mspx`.
- Článek *Changes to IPv6 in Windows Vista and Windows Server „Longhorn“*, který je součástí série článků The Cable Guy od Josepha Daviese, najdete na internetové adrese `http://www.microsoft.com/technet/community/columns/cableguy/ cg1005.mspx`.
- Článek *Performance Enhancements in the Next Generation TCP/IP Stack*, který je součástí série článků The Cable Guy od Josepha Daviese, najdete na internetové adrese `http://www.microsoft.com/technet/community/columns/cableguy/cg1105.mspx`.
- Článek *Understanding the IPv6 Routing Table*, který je součástí série článků The Cable Guy od Josepha Daviese, najdete na internetové adrese `http://www.microsoft.com/technet/community/columns/cableguy/cg1002.mspx`.
- Článek *Manual Configuration for IPv6*, který je součástí série článků The Cable Guy od Josepha Daviese, najdete na internetové adrese `http://www.microsoft.com/technet/community/columns/cableguy/cg0902.mspx`.
- Článek *Using Windows Tools to Obtain IPv6 Configuration Information* najdete na stránkách Microsoft TechNet na internetové adrese `http://technet.microsoft.com/cs-cz/library/bb726952(en-us).aspx`.
- Článek *Troubleshooting IPv6*, který je součástí série článků The Cable Guy od Josepha Daviese, najdete na internetové adrese `http://www.microsoft.com/technet/community/columns/cableguy/cg0305.mspx`.
- Článek *Domain Name System Client Behavior in Windows Vista* najdete na internetové adrese `http://technet.microsoft.com/cs-cz/library/bb727035(en-us).aspx`.
- Článek *Source and Destination Address Selection for IPv6*, který je součástí série článků The Cable Guy od Josepha Daviese, najdete na internetové adrese `http://www.microsoft.com/technet/community/columns/cableguy/cg0206.mspx`.
- Článek *IPv6 Transition Technologies* najdete na internetové adrese `http://www.microsoft.com/downloads/details.aspx?familyID=afe56282-2903-40f3-a5ba-a87bf92c096d`.
- Článek *Intra-site Automatic Tunnel Addressing Protocol Deployment Guide* najdete na internetové adrese `http://www.microsoft.com/downloads/details.aspx?FamilyID=0f3a8868-e337-43d1-b271-b8c8702344cd&displaylang=en`.
- Kniha *Understanding IPv6* od Josepha Daviese (Microsoft Press, 2002). Aktualizace pro tuto knihu můžete stáhnout v centru pro stahování Microsoft Download Center na internetové adrese `http://www.microsoft.com/downloads/details.aspx?familyID=42bf4711-27af-4c4c-8300-7bcf900de5c3&displaylang=en`.

- Kapitola 9, *Windows Support for DNS*, z elektronické knihy *TCP/IP Fundamentals for Microsoft Windows*, kterou můžete stáhnout v centru pro stahování Microsoft Download Center na internetové adrese `http://www.microsoft.com/downloads/details.aspx?FamilyID=c76296fd-61c9-4079-a0bb-582bca4a846f`.
- Kapitola 12, *Troubleshooting TCP/IP*, z elektronické knihy *TCP/IP Fundamentals for Microsoft Windows*, kterou můžete stáhnout v centru pro stahování Microsoft Download Center na internetové adrese `http://www.microsoft.com/downloads/details.aspx?FamilyID=c76296fd-61c9-4079-a0bb-582bca4a846f`.

Na doprovodném DVD

- `DisableIPv6.vbs`
- `EnableIPv6.vbs`
- `viewIPv6Config.vbs`
- `viewIPv6Settings.vbs`
- `viewIPv6Stats.vbs`