UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Přechodové mechanizmy mezi IPv4 a IPv6

Lukáš Uhlíř

Bakalářská práce
2013

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2012/2013**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš Uhlíř**
Osobní číslo:	**I09296**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Přechodové mechanizmy mezi IPv4 a IPv6**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je podrobně popsat a prakticky nakonfigurovat mechanizmy pro komunikaci sítí s adresováním využívající protokol IPv4 a IPv6. Autor práce popíše funkci protokolu IPv6 s důrazem na formát datagramu, adresy IPv6, protokol ICMPv6 a DNS. Dále podrobně představí mechanizmy objevování sousedů, automatické konfigurace a skupinového a multicast vysílání. Autor objasní problematiku směrování s adresami protokolu IPv6. Na závěr teoretické části autor podrobně rozebere přechodové mechanizmy 6to4, 6over4, ISATAP, Teredo, SIIT a NAT-PT. Tyto mechanizmy budou nakonfigurovány v laboratoři počítačových sítí FEI UPCE. Na základě reálné konfigurace a testování provozu budou vytvořeny ukázkové úlohy s kompletním řešením na tyto přechodové mechanismy pro podporu výuky předmětu Počítačové sítě 4.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

***DEERING, S.; HINDEN, R. RFC 2460 - Internet Protocol, Version 6 (IPv6) [1]Specification [online]. December 1998 [cit. 2011-08-02]. Dostupné z WWW: http://tools.ietf.org/html/rfc2460.**
***SATRAPA, Pavel. Internetový protokol IPv6 [online]. Praha : CZ.NIC, 2008 [cit. [2]2011-08-03]. Dostupné z WWW: http://knihy.nic.cz/files/nic/edice/pavel_satrapa_ipv6_2008.pdf. ISBN 978-80-904248-0-7.**
***DUNMORE, Martin (Ed.). An IPv6 Deployment Guide [online]. The 6NET [3]Consorcium, 2005 [cit. 2011-08-04]. Dostupné z WWW: http://www.6net.org/book/deployment-guide.pdf.**

Vedoucí bakalářské práce: **Mgr. Josef Horálek**
Katedra softwarových technologií

Datum zadání bakalářské práce: **21. prosince 2012**
Termín odevzdání bakalářské práce: **10. května 2013**

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 29. března 2013

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 9. 5. 2013 Lukáš Uhlíř

Poděkování

Rád bych tímto způsobem poděkoval svému vedoucímu mé bakalářské práce Mgr. Josefu Janu Horálkovi. Vždy když jsem potřeboval, byl mi ochoten pomoci a poradit s jakýmkoliv problémem. Také bych chtěl poděkovat své rodině, která mi poskytla spoustu užitečných rad a pomáhala mi při psaní a maximálně mě podporovala při mém studiu.

Anotace

Cílem práce je podrobně popsat protokol IPv6 a přechodové mechanizmy mezi protokoly IPv4 a IPv6. Součástí bakalářské práce je popis funkce protokolu, adres protokolu IPv6, objevování sousedů, automatická konfigurace a směrovací protokoly. Na konci teoretické části jsou také ukázky základních příkazů protokolu IPv6. V praktické části bakalářské práce je vložena ukázka automatické konfigurace, konfigurace DHCP a vybrané přechodové mechanizmy.

Klíčová slova

IPv6, Internet Protokol, přechodové mechanizmy, směrovač

Title

Transition mechanisms between IPv4 and IPv6

Annotation

The aim of the thesis is to describe in detail the protocol IPv6 and transition mechanisms between protocols IPv4 and IPv6. In the thesis is functional description of protocol, addresses in protocol IPv6, neighbors discovery, the automatic configuration and the routing protocols. At the end of the theoretical part are also examples for basic commands in protocol IPv6. In practical part in thesis is inserted example of auto-configuration, the DHCP configuration and selected transitions mechanisms.

Keywords

IPv6, Internet Protocol, transition mechanisms, router

Obsah

Seznam zkratek

ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DoS	Denial of Service
DDOS	*Distributed Denial of Service*
DUID	DHCP Unique Identifier
EGP	External Gateway Protocol
EUI	Extended Unique Identifier
IANA	Internet Assigned Numbers Authority
ICMP	*Internet Control Message Protocol*
ICQ	I Seek You
IGP	Internal Gateway Protocol
IP	Internet Protocol
IPSec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISO	*International Organization for Standardization*
LSA	Link State Advertisement
MAC	Media Access Control
MTU	Maximum transmission unit
NAT	Network Address Translation
NAT-PT	Network Address Translation + Protocol Translation
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PC	Personal Computer
RIPng	Routing Information Protocol new generation
RIPv2	Routing Information Protocol version 2
RFC	Request For Comments
TCP	Transmission Control Protocol
TTL	Time to live
UDP	*User Datagram Protocol*

Seznam obrázků

Úvod

V současné době se zvyšuje počet uživatelů a zvyšují se nároky na připojení k celosvětové síti. Technika se neustále zdokonaluje a technologie, které jsou nyní v provozu, začínají být nedostačující. Zvyšují se nároky na bezpečnost a rychlost přenosu, kapacita mechanizmu IPv4 bude brzy nedostačující. Proto je třeba začít postupně nahrazovat IPv4 novým kapacitním prostorem, který bude vyhovovat dnešním požadavkům moderní doby.

V dnešní době začínají velké firmy postupně přecházet na nový protokol IPv6. Protokol IPv6 poskytuje větší adresní prostor než dosavadní protokol IPv4. Protokol IPv6 není zpětně kompatibilní s protokolem IPv4 a tudíž se musí využívat různé přechodové mechanizmy. Mechanizmů zajišťující plynulý přechod a propojení z protokolu IPv4 na protokol IPv6 je více. Některé jsou méně výhodné, jiné více.

Bakalářská práce je členěna do dvou odlišných částí. První část je část teoretická. Druhá část se zabývá ukázkou praktických příkladů konfigurace IPv6 a některých přechodových mechanizmů.

První část bakalářské práce se zabývá popisem protokolu IPv6. Začíná popisem historie a vývojem nového protokolu IPv6. Jsou zde popsány hlavní rozdíly mezi protokoly IPv4 a IPv6. Součástí teoretické části jsou také popsány výhody a nevýhody protokolu IPv6. V dalších kapitolách je popsána funkce nového protokolu, popis adres vyskytujících se v protokolu IPv6 a konfigurace. Neméně důležitou součástí práce jsou směrovací protokoly. Dále jsou v mé práci popsány základní a nejdůležitější přechodové mechanizmy umožňující přechod novějšího a modernějšího protokolu IPv6. V poslední, desáté kapitole jsou uvedeny základní konfigurace na Cisco směrovači.

Druhá část bakalářské práce je praktická. Tato část je zaměřena na testování přechodových mechanizmů mezi protokoly IPv4 a IPv6. Testování přechodových mechanizmů probíhalo v laboratoři Pardubické univerzity. V praktické části je dále ukázána automatická konfigurace protokolu IPv6. V této konfiguraci také ukazuji konfiguraci RIPng. Další konfigurací v mé práci je konfigurace DHCP. Na konci bakalářské práce jsou přiloženy v přílohách A – D náhledy vytvořených konfigurací a jejich popis.

1 Internet protokol verze 6

Protokol IPv6 je v informačních technologiích označení nového a lepšího protokolu, který slouží pro komunikaci v počítačových sítích. Používá se na třetí (síťové) vrstvě ISO/OSI modelu a je nástupcem staršího IPv4 protokolu. Dle ustanovení RFC 6540 je jeho podpora povinná, a to ve všech implementacích IP. Dle ustanovení musí být kvalita minimálně stejná jako u protokolu IPv4. [15] [29]

Tento protokol slouží ke směrování a adresování v počítačové síti. Také ho můžeme využít při oznamování chyb vyskytujících se v síti. Na této vrstvě pracují veškeré směrovače (routery) vyskytující se v síti. [27]

Aplikační	**Poskytuje uživatelské rozhraní**
Prezenční	**Prezentuje data** **Zpracovává další funkce jako je šifrování**
Relační	**Zajišťuje oddělení dat různých aplikací**
Transportní	**Zajišťuje spolehlivé nebo nespolehlivé doručení** **Provádí opravu chyb, případně opakované vysílání**
Síťová	**Zajišťuje logické adresování, podle něhož směrovače určují cestu v síti**
Linková	**Rozděluje pakety do rámců a rámce do bajtů** **Zajišťuje přístup k médiu pomocí MAC adresy** **Provádí detekci chyb, nikoliv však jejich opravy**
Fyzická	**Dopravuje datové bity mezi jednotlivými zařízeními** **Specifikuje úrovně napětí, přenosovou rychlost a rozložení pinu na fyzickém kabelu**

Obrázek 1 - Vrstvy ISO/OSI modelu

Základní požadavky na Internet Protokol verze 6: [27]

- Vytvoření rozsáhlého adresního prostoru, který by vystačil napořád
- Tři typy adres: Unicast (individuální), Multicast (skupinové), Anycast (výběrové)
- Jednotné adresní schéma, které je pro Internet a také vnitřní sítě
- Hierarchické směrování, které je v souladu s hierarchickou adresací
- Zvýšení bezpečnosti - tzn. šifrování, autentizaci a sledování cesty k odesílateli

- Podpora pro služby se zajištěnou kvalitou
- Optimalizace pro vysokorychlostní směrování
- Automatická konfigurace - plug and play
- Podpora mobility
- Hladký a bezproblémový přechod z protokolu IPv4 na protokol IPv6

1.1 Historie IPv6

V devadesátých letech 20. století začalo být jasné, že kapacita adresního prostoru protokolu IPv4 bude v následujících letech nedostačující. Všem tehdy už začalo docházet, že během deseti let dojde k vyčerpání adresního prostoru protokolu IPv4. Dostatek času umožňoval řešit tento problém. Požadavky na nový protokol IPv6 byly celkem dosti vysoké. [15]

Steven Deering a Robert Hinden se dají považovat za zakladatele nového protokolu IPv6. Roku 1995 vydali sadu RFC, která definovala protokol IPv6. Když byla na světě specifikace, nebylo překážek pro uvedení protokolu IPv6 do provozu. Avšak určité překážky se našly, jelikož protokol IPv4 měl zisky okamžité a proto spousta firem raději investovala do protokolu IPv4 něž do protokolu IPv6. Velké riziko pro protokol IPv6 nastal, když se podařilo vyřešit nedostatek adres v protokolu IPv4. Byla zavedena technologie CIDR. [27]

Technologie CIDR upravila výběr pro přidělení síťových adres pomocí mechanizmů pro překlad adres. Jelikož toto obralo protokol IPv6 o hlavní výhody, žádné firmy nechtěly do výzkumu investovat. Musely se nalézt jiné výhody. Myšlenky o tom, že adresní prostor je dostačující, byly špatné. Aplikace CIDR pouze zpomalila tento problém. [16] [27]

Koncem roku 1996 byla vydána revidovaná sada RFC dokumentů, která definovala základní protokoly a služby, jelikož výzkum pro protokol IPv6 nebyl zastaven. I když nedostatek adresního prostoru zatím nehrozil, objevila se nová velká výhoda protokolu IPv6, podpora mobility. S novou dobou přišel nový trend, jako jsou přenosná zařízení. Firmy chtěly tato přenosná zařízení zapojit do Internetu. Právě protokol IPv6 je v podpoře mobility mnohem lepší než protokol IPv4. [26]

Velké oblibě se těšily nástroje pro překlad adres (Network Address Translation, NAT). Jejich funkce tkví v tom, že přístupový směrovač sítě promění IP adresy jednotlivých paketů. Tyto pakety proudí z Internetu do sítě a zpět. Celá síť proto může mít jen jednu veřejnou IP adresu. Avšak počítačům uvnitř sítě nemůžeme přiřazovat IP adresu z vnějšku Internetu. Komunikovat můžeme zevnitř sítě ven, a ne naopak. To představuje velký problém, jelikož poptávka nejen firem, ale i fyzických osob roste pro přímou komunikaci (ICQ, Skype, videokonference). Pokud je tedy uživatel v jiné NATované síti, není možné mezi s sebou komunikovat. Na řadu tudíž přichází protokol IPv6, který slibuje komunikaci bez NAT a neomezený adresní prostor. [10] [19] [27]

V roce 2000 nastala tzv. implementační vlna. V současné době mnozí říkají, že protokol IPv6 je naším jediným řešením pro budoucnost Internetu. Rok 2007 se vyznačuje výrazných růstem protokolu IPv6, až na dvojnásobek. V této době se již pomalu přechází na nový protokol IPv6. [27]

1.2 Využití IPv6

Protokol IPv6 slouží ke komunikaci mezi počítači v síti. V této nové verzi nemáme aplikaci NAT, tudíž komunikace mezi přenosnými zařízeními není problémem.

1.3 Výhody IPv6

Mnoho lidí si pokládá otázku, zdali přechod z protokolu IPv4 na protokol IPv6 bude mít takové výhody, jak vývojáři slibují. Další otázkou je, zdali jednou nebudeme muset řešit ten samý problém, jako řešíme nyní s protokolem IPv4. Ať už si tyto otázky pokládáme nebo ne, je jisté, že přechod na protokol IPv6 je nutný a jednoznačně výhodný. Přechod na protokol IPv6 není přes všechny výhody jednoduchý. Změnit se musí technika jak na straně poskytovatelů internetu, tak na stranách provozovatelů serverů a koncových uživatelů. Protokoly IPv4 a IPv6 přitom spolu nejsou přímo kompatibilní. Nastalo proto období, kdy budou oba protokoly fungovat v síti zároveň do doby, než se IPv6 stane majoritním. [23]

Největší výhodou, která je nanejvýš nutná, je dostatečný adresní prostor. Tento prostor má $3{,}4 * 10^{38}$ adres. Počet adres by měl být rozhodně dostačující. Počet adres se zvýšil díky prodloužení délky adresy. Délka adresy v protokolu IPv6 je čtyřikrát větší než v IPv4. To znamená, že délka adresy v IPv6 je 128 bitů. Má také více skupin číslic, místo čtyř skupin číslic má osm skupin číslic. Skupiny oddělujeme oproti protokolu IPv4 dvojtečkami a jsou v nich obsažena i písmena. Pokud to tedy shrneme, adresa nacházející se v protokolu IPv6 je tvořena z osmi 16- ti bitových hexadecimálních bloků, které musí být odděleny dvojtečkami. [18]

Další výhodou jsou funkce chybějící v protokolu IPv4. Tyto funkce jsou v IPv4 kompenzovány různými doplňky. Tím byla práce obtížnější. V protokolu IPV6 se tyto funkce staly povinnými a zařadily se mezi povinné funkce. [18]

Výhodná je také mobilita protokolu IPv6. To znamená, že přechod jednotlivých zařízení z jedné sítě do druhé je kontinuální, aniž by docházelo k výpadkům při spojení. [18]

Velkou výhodou je zvýšení efektivity v protokolu IPv6. To je dáno mnoha aspekty. Hlavička nacházející se v IPv6 má oproti protokolu půlku polí. Tato polovina polí u hlavičky datagramu v protokolu IPv6 má velikost 64 bitů. Efektivita je umocněna odejmutím velkého množství informací z hlavičky paketu. Informace, které jsou potřebné do hlavičky v protokolu IPv6 zapsat, můžeme vložit pomocí rozšiřujících hlaviček. Rozšiřující pole hlavičky jsou zapsány za základními poli hlavičky. [18]

Další v pořadí je výhoda hlavně pro podniky. Protokol IPv6 umožňuje mít více než jednu adresu. Je tím zajištěna mnohem lepší dostupnost. [18]

Vícesměrová komunikace se samozřejmě musí také zařadit mezi výhody zlepšující dostupnost a efektivitu. To znamená, že jedno zařízení může vysílat více než jednomu hostiteli a atd. Vícesměrová komunikace je náhradou za všesměrové vysílání v protokolu IPv4. Dalším podstatným vylepšením je jednosměrové vysílání (unicast) a výběrové adresy (anycast). [18]

1.4 Nevýhody IPv6

Samozřejmě jako u všeho, tak i u protokolu IPv6 můžeme najít nevýhody. Některé nevýhody jsou pouze dočasného rázu, jiné jsou více zatěžující než ty další.

Jednou z největších nevýhod protokolu IPv6 je nekompatibilita s protokolem IPv4. Tento problém se nám však daří celkem úspěšně řešit. Největším problémem jsou koncoví uživatelé, kteří přechod na IPv6 protokol brzdí. [14]

Jako další nevýhodu, můžeme brát pomalý vývoj některých specifikací. Požadavky dnešní doby jsou vysoké a proto je zapotřebí zvýšit efektivitu vývoje a odstraňovat nedostatky objevující se v průběhu provozu protokolu.

Nevýhodou je také nejistý výnos protokolu IPv6. Mnoho firem raději zainvestuje do protokolu IPv4, který je již zaběhnutý v provozu a využívá ho mnoho uživatelů. Stále je mezi uživateli spousta lidí, kteří nedůvěřují přechodu na novější verzi protokolu IPv6.

U aplikací fungujících v protokolu IPv4 dochází k nekompatibilitě. Všechny aplikace musí být přeprogramovány a je nutné upravit jejich konfigurace. Aby mohlo docházet k užívání aplikací na protokolu IPv6, je nezbytné využívat překlady mezi těmito dvěma protokoly

1.5 Rozdíl mezi IPv4 a IPv6

Existují značné rozdíly, které protokol IPv6 značně zvýhodňují oproti protokolu IPv4. Autoři tohoto protokolu se velmi snažili, aby odpovídal a vyhovoval všemu, co je v dnešní době zapotřebí. [6] [22]

IPv4	IPv6
Délka adresy 32 bitů (4 bajty) na délku	Délka adresy 128 bitů (16 bajtů) na délku
IPSec je volitelný a měl by být podporován externě	IPSec podpora není volitelná, tzn je integrována
Záhlaví hlavičky obsahuje kontrolní součet	Záhlaví hlavičky neobsahuje kontrolní součet
Záhlaví hlavičky obsahuje volby	Nepovinné údaje jsou obsaženy v rozšiřující hlavičce
BROATcastová adresa používaná pro každý subnet	Používá se multicast v rámci jednoho subnetu
DNS host má záznam A	DNS host má záznam AAAA

Obrázek 2 - Porovnání mezi IPv4 a IPv6

2 Funkce protokolu IPv6 s důrazem na formát datagramu

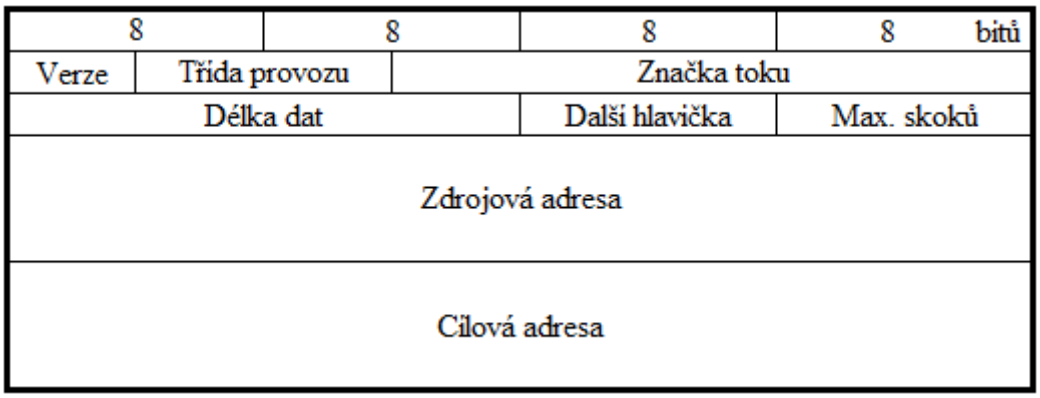
Nejdůležitější dokument specifikující IPv6 je RFC 2460: Internet Protocol Version 6 Specification (IPv6). Tento protokol obsahuje hlavně formát datagramu protokolu IPv6. [7]

Každý datagram v protokolu IPv6 začíná hlavičkami, za kterými následují přenášená data. Hlavička se v protokolu IPv6 oproti protokolu IPv4 změnila. V protokolu IPv4 byla délka hlavičky proměnlivá. Také bylo možné k hlavičce připojovat další nepovinné volby. Hlavička obsahovala kontrolní součet, který byl zapotřebí na každém směrovači, kterým datagram prošel, znovu vypočítat. Důvodem pro přepočet hlavičky byla položka TTL (Time to live). [27]

2.1 Základní hlavička

Základní hlavička v protokolu IPv6 má konstantní velikost. Základní hlavička může obsahovat další rozšiřující údaje. [15]

Adresy odesílatele a příjemce se v protokolu IPv6 prodloužily čtyřikrát. Ale celková délka základní hlavičky vzrostla pouze dvojnásobně oproti IPv4. Velikost hlavičky v protokolu IPv6 je 40 B (v IPv4 byla velikost 20 B), ale 32 B zabírají adresy. [15] [31]



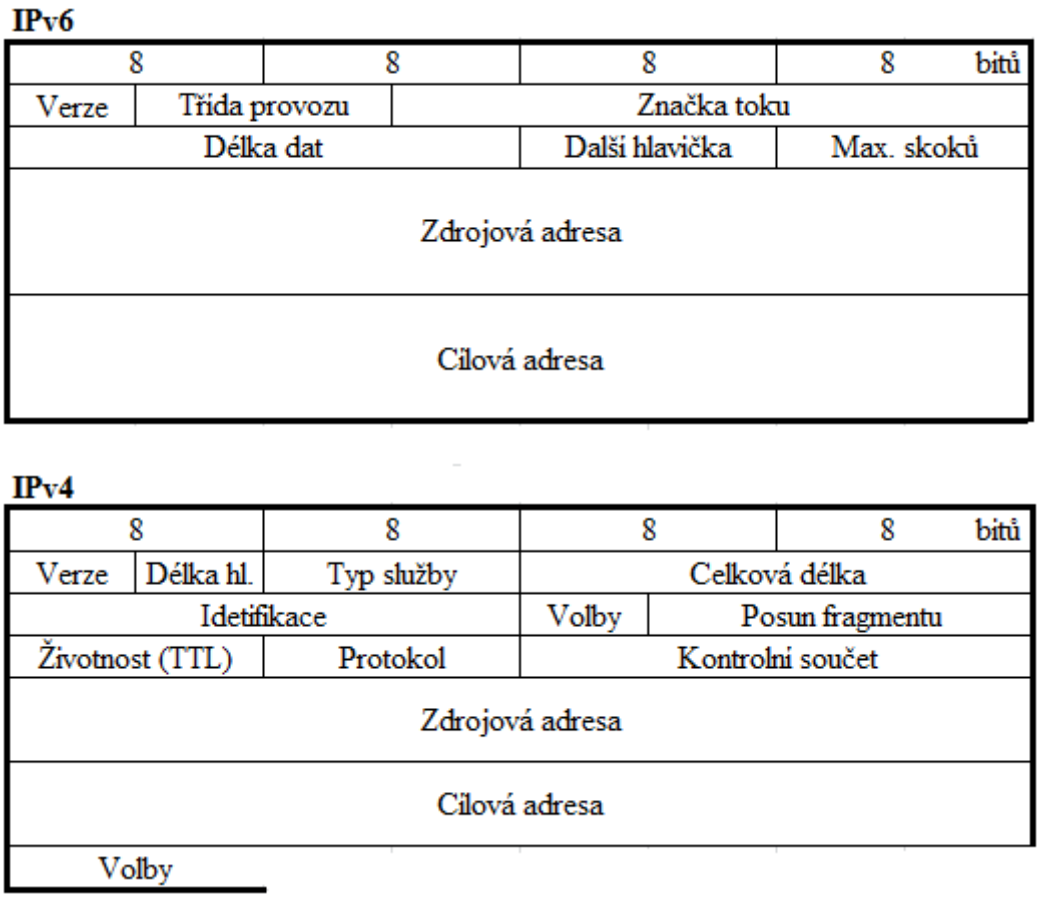
Obrázek 3 - Základní hlavička datagramu

Popis obrázku č. 3 [6] [27]

- Verze IP (Version) - položka identifikuje verzi protokolu, v případě protokolu IPv6 je to hodnota 6, v případě protokolu IPv4 je to hodnota 4
- Třída provozu (Traffic Class) - položka vyjadřuje prioritu datagramu nebo zařazení datagramu do přepravní třídy, cílem této položky je umožnit IP poskytovat služby se zaručenou kvalitou, v této položce existují tzv. diferencované služby (differenciated services) - pomocí této služby mohou mít datagramy různé priority

a odlišné způsoby zacházení (přednostní zpracování nebo odkládání až po ostatních), právě tyto diferencované služby využívají položku Třída provozu

- Značka toku (Flow Label) - tato položka identifikuje jeden dílčí tok dat v síti a to spolu s adresou odesílatele, délka Značky toku je 20 bitů
- Délka dat (Payload Length) - položka zaznamenává délku datagramu (počet bajtů za standartní hlavičkou), nepočítá se základní hlavička do zaznamenané Délky dat, pokud se jedná o rozšiřující hlavičku, poté se Délka dat zaznamenává, maximální délka této položky je 64 KB (jelikož je položka dvoubajtová), v případě vytvoření delšího datagramu můžeme použít rozšiřující hlavičku (Jumbo obsah)
- Další hlavička (Next Header) - položka nese identifikaci o druhu dat za standartní hlavičkou
- Maximální počet skoků (Hop Limit) - používá se místo životnosti datagramu (TTL), který se používal v protokolu IPv4, datagram, který projde jedním směrovačem, se považuje za jeden skok, maximální počet skoků je uveden v této položce Maximální počet skoků, každý směrovač, kterým datagram projde, sníží maximální počet skoků o jedna, v případě vybulování položky dojde k zahození datagramu a odesílateli bude poslána ICMP zpráva, že došlo k vypršení maximálního počtu skoků, pomocí tohoto omezení se předchází cyklům vznikajících při směrování
- Adresy (Source Address, Destination Address) - obě tyto adresy mají 128 bitů a zabírají 80% obsahu základní hlavičky datagramu



Obrázek 4 - Porovnání hlaviček IPv6 a IPv4

2.2 Rozšiřující hlavičky datagramů (Next Header)

Za základní hlavičkou v protokolu IPv6 může stát tzv. rozšiřující, neboli další hlavička. Tato rozšiřující hlavička identifikuje informace následující za hlavičkou základní, jelikož hlavní hlavička byla zjednodušena na maximum a tudíž obsahuje jen ty nejdůležitější a nejnutnější informace. Rozšiřující hlavička obsahuje svojí položku *další hlavička*. Z takto zapsaných hodnot poté vznikne řetězec, sdělující že za základní hlavičkou stojí rozšiřující hlavička a za ní další a další a atd. A za těmito informacemi následují data pro TCP. [11] [27]

Rozšiřující hlavičky mají svoje pořadí, které musí být dodržováno a mohou se objevovat maximálně jednou avšak s výjimkou volby pro cíl. Tato rozšiřující hlavička se může objevit dvakrát, před směrováním a před mobilitou. Na prvním místě musí být takové hlavičky zajímající směrovače, kterými prochází daný datagram. Díky tomuto procesu mají směrovače, kterým datagram prochází svoji práci ulehčenou. Proces probíhá tímto způsobem: nejprve dojde k prozkoumání základní hlavičky a ihned za ní se prozkoumá první položka další hlavičky, je-li tato položka rozpoznána pro ně, je zařazena do

zpracování a dochází k prozkoumání položky další a to do té doby, dokud není rozbalena položka, která je určena jinému cíli. Tím se průzkum paketu ukončí. [11] [27]

Poslední hlavička 59 nese informace o tom, že nic dalšího nenásleduje. Pokud se za touto hlavičkou vyskytují další datagramy, musí být ignorovány.

Průběžného adresáta zajímá jen určitý počet hlaviček, a to první tři (volby pro všechny, volby pro cíl a směrování). Koncového adresáta zajímají všechny rozšiřující hlavičky. [27]

2.3 Pořadí rozšiřujících hlaviček

Jak již bylo řečeno, i rozšiřující hlavičky mají své pořadí, které zjednodušuje průchod jednotlivými cíli. [26]

1. Základní hlavička protokolu IPv6
2. Volby pro všechny (Hop by hop options)
3. Volby pro cíl (Destination options) – první příjemce datagramu
4. Směrování (Routing)
5. Fragmentace (Fragment)
6. Autentizace (Authentication)
7. Šifrování obsahu (Incapsulating security payload)
8. Volby pro cíl (Destination options) – konečný příjemce datagramu
9. Mobilita (Mobility)

Rozšiřující hlavičky	
0	volby pro všechny (hop-by-hop options)
43	směrování (routing)
44	fragmentace (fragment)
50	šifrování obsahu (ESP)
51	autentizace (AH)
59	poslední hlavička (no next header)
60	volby pro cíl (destination options)
135	mobilita (mobility)
Typ nesených dat	
6	TCP
8	EGP
9	IGP
17	UDP
46	RSVP
47	GRE
58	ICMP

Obrázek 5 - Hodnoty položky další hlavička

2.3.1 Volby

Ve tvaru se tyto hlavičky neliší. Tato položka má ve svém obsahu vlastní volby. V konkrétních mechanizmech jsou vedeny jako jejich součást (mobilní počítače mají volbu Domácí adresa). Protokol IPv6 má dvě - Pad1 a PadN. O druhé volby nás informuje první bajt. Jsou součástí skupiny dalších hlaviček a celkem tyto volby mají délku 6 bajtů (48 bitů). [7] [27]

Máme dva typy voleb:

- volby pro všechny

Typ	Význam
0	Pad1
1	PadN
5	Upozornění směrovače
6	Rychlý start
194	Jumbo obsah

Obrázek 6 - Volby pro všechny

- volby pro cíl

Typ	Význam
0	Pad1
1	PadN
201	Domácí adresa

Obrázek 7 - Volby pro příjemce

Pad1 vynechává jeden bajt. Bajt má hodnotu nula a identifikuje typ volby [6]

PadN umožňuje vynechat dva a více bajtů. První bajt má hodnotu jedna a identifikuje typ volby [6]

2.3.2 Směrování

Datagram je posílán do svého cíle podle cílové adresy. Jsou zde využívány dvě položky typu 0 a 2.

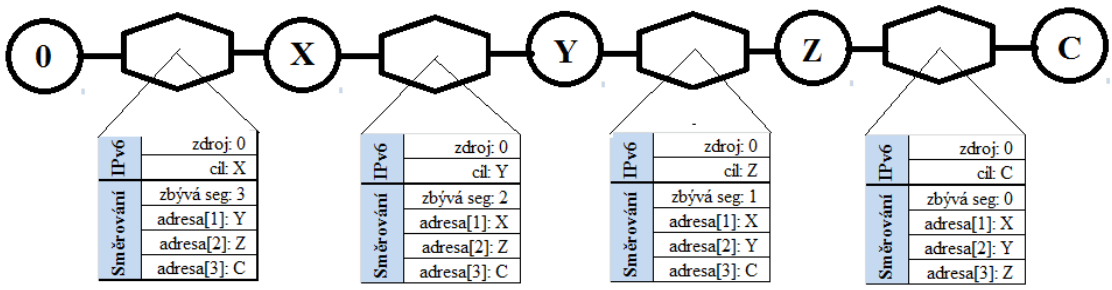
Směrování typu 0 má několik úkolů. Nechává datagram předepsat takové body, kterými má projít v předepsaném pořadí. Také má funkci záznamu a zaznamenává, kudy již prošel. Průchozí body nemusí být řazeny za sebou. Pokud je odesílatelem požadováno, aby datagram prošel těmi uzly, kterými on chce, musí napsat jako cílovou adresu IP adresu prvního průchozího uzlu. Hlavička Směrování sama zapíše adresy, které zbývají. Na závěr je uveden konečný cíl, kam má datagram dojít. Ještě se musí, do položky „Zbývá segmentů“ zapsat jejich počet. [11]

Hlavička typu 0 byla zavedena z jednoho hlavního důvodu - pro testování dosažitelnosti mezi libovolnými adresami. Zapíše se do ní, odkud do jakého cíle mají být dopraveny datagramy. Tím se ověří, jakou funkčnost má dané spojení. [27]

8	8	8	8 bitů
Další hlavička	Délka dat	Typ směrování = 0	Zbývá segmentů
rezerva = 0			
Adresa [1]			
⋮			
Adresa [2]			

Obrázek 8 - Rozšiřující hlavička Směrování typu 0

Směrování typu 2 má speciální definici pro mobilitu. Je to silně zjednodušený typ 0. Umožňuje uložení jen jediné adresy. Její zneužitelnost je tím skoro nulová. [27]



Obrázek 9 - Změny v hlavičkách datagramu

2.3.3 Fragmentace

Jestliže maximální možná velikost paketu má menší velikost než je datagram, musí dojít k fragmentaci. Pokud je tedy velikost větší, datagram nemá šanci se vejít do linky, kterou má projít. Proto musí dojít k rozdělení na menší datagramy.

Pravidla, které fragmentace má jsou v protokolu IPv6 zpřísněna oproti protokolu IPv4. V protokolu IPv4 mohl být datagram fragmentován kdekoliv, jakýmkoliv zařízením. Ovšem v protokolu IPv6 tuto fragmentaci může provádět jen odesílatel. Je-li po cestě k cíli v některém zařízení vyhodnoceno, že datagram díky své velikosti nemůže projít linkou, je zahozen. Odesílateli je odeslána díky ICMPv6 chybová zpráva. Odesílatel musí tedy buď přistoupit k fragmentaci, nebo zmenšit velikost tak, aby linkou datagram prošel. [27]

Fragmentace má vlastní postup, který musí být dodržen. Část, jež má být fragmentována, je rozdělena na úseky s velikostí násobku osmi bajtů. Celková velikost, jak již bylo řečeno, nesmí být větší, než je velikost požadována MTU. Z jednoho datagramu tedy máme fragmenty. [27]

Jejich hlavičky mají tuto sestavu:

- Použije se ta část z původního datagramu, která je nefragmentovatelná. Provedou se jen dvě změny - upraví se velikost v základní hlavičce, upraví se hodnota Další hlavičky na 44. Velikost musí odpovídat skutečné velikosti v hlavičce základní.
- Pak se za ni přidá hlavička Fragmentace. Vytvoří se Identifikátor paketu. Hodnota je dána poté všem fragmentům. Hodnota Další hlavičky je zkopírována z poslední Další hlavičky z původního, nefragmentovatelného datagramu. Dále je tu ještě Posun. Ten je určen jako počet osmi bajtů. Poslední fragment má příznak M nastavený na nulu, ostatní ho mají nastaven na číslo jedna.

- Na konec je připojen dotyčný fragment.

8	8	13	bitů	
Další hlavička	rezerva = 0	Posun fragmentu	rez.	M
Identifikace				

Obrázek 10 - Rozšiřující hlavička Fragmentace

Fragmenty jsou po fragmentaci jako datagramy odeslány adresátovi. Adresát z informací z fragmentace dokáže poskládat původní datagram. Identifikátor řekne adresátovi, jaké fragmenty k sobě patří, Posunutí řekne pořadí a příznak M vypovídá, zdali dorazily všechny části. [27]

Volby pro všechny	0	informace zajímavé pro každého po cestě (př.: upozornění směrovače, že paket nese data, která by ho mohla zajímat)
Směrování	43	datagram musí projít předepsanou cestou
Fragmentace	44	při fragmentaci paketu nese informace nutné pro jeho složení do původní polohy
Šifrování obsahu (ESP)	50	obsah datagramu je zašifrován, ESP hlavička nese odkaz na parametry pro dešifrování
Autentizace (AH)	51	data pro ověření totožnosti odesílatele a původnosti obsahu
Poslední hlavička	59	nic dalšího nenásleduje
Volba pro cíl	60	informace určené příjemci datagramu (př.: domácí adresa mobilního uzlu)
Mobilita	135	pro potřeby komunikace s mobilními zařízeními

Obrázek 11 - Přehled rozšiřujících hlaviček

2.3.4 Velikost datagramů

Velikost datagramů je závislá na fragmentaci. Při zasílání datagramu se musí najít maximální velikost, kterou lze zaslat. K tomu se používá algoritmus MTU cesty. Tento algoritmus hledá maximální velikost paketu, který můžeme poslat danému adresátovi.

Poprvé zašle adresátovi datagram s velikostí MTU dané linky odesílateli. Jestliže příjemce zašle zprávu ICMP (příliš velký paket), tak se velikost datagramu přizpůsobí takové velikosti, kterou má ICMP zprávy. Postup se opakuje do té doby, než je celý datagram doručen adresátovi. Algoritmus se spouští v pětiminutových intervalech, aby se zajistila aktuálnost dat. Minimální velikost MTU v IPv6 je 1280 bajtů (doporučeno 1500 bajtů). [27] [31]

2.3.5 Toky

Toky usnadní a zrychlí zpracování datagramů při průchodu směrovači a dalšími uzly. Zjednodušeně můžeme říci, že toky jsou proudy datagramů. Přiřazují se k příslušnému toku dle adres, které patří odesílateli nebo příjemci. Dále jsou přiřazeny podle značky toku. Tok značky se nesmí během cesty změnit. Odesílatel si zaznamenává záznamy o použitých značkách. Značky po zaznamenání nesou stejné označení. Nastane-li případ, kdy je značka nulová, tak daný datagram nepatří k žádnému toku. [27]

3 Adresy IPv6

Adresy se v protokolu IPv6 nepřiřazují počítačům, ale síťovým rozhraním. Jako příklad můžeme uvést domácnost, ve které máte počítač obsahující dvě síťové karty. Jelikož adresa se nepřiřazuje počítači, ale síťovým rozhraním, tak každá z těchto dvou karet dostane svou adresu.

Máme tři druhy adres v IPv6. Každá tato adresa má své chování, kterým se odlišuje od ostatních: [18] [31]

- Individuální (unicast) - tento typ adresy slouží k identifikaci jednoho síťového rozhraní a jen tomuto rozhraní jsou data přenášena
- Skupinové (multicast) - tento typ adresy slouží pro adresaci celých skupin počítačů či jiných zařízení v síti a data odeslaná z této adresy musí být doručena všem členům skupiny v síti
- Výběrové (anycast) - tento typ adresy označuje celou skupinu, ale tato data se doručí pouze jedinému členovi z této skupiny a to tomu, který je nejblíže

3.1 Typy adres verze IPv6

V protokolu IPv6 existuje několik typu adres. Tyto adresy slouží k různým aplikacím v IPv6 protokolu vrstvy 3. V protokolu IPv6 se nepoužívají všesměrové adresy. Všesměrové adresy jsou nahrazeny speciálními vícesměrovými adresami. [27]

Protokol IPv6 obsahuje tři druhy adres: [1]

- Jednosměrové adresy
- Vícesměrové adresy
- Výběrové anycast adresy

Prefix	Význam
::/128	nedefinovaná adresa
::1/128	smyčka (loopback)
fc00::/7	unikátní individuální lokální
fe80::/10	individuální lokální linkové
ff00::/8	skupinové adresy
ostatní	individuální globální

Obrázek 12 - Základní rozvržení adres

3.1.1 Globální individuální adresy

Globální individuální adresy identifikují svého nositele v rámci celého internetu a musí tudíž být celosvětově jednoznačné. V protokolu IPv6 jsou úplně odstraněny privátní adresy. Privátní adresy se využívají v protokolu IPv4 v jejich sítích z důvodu překladu adres za pomoci NAT. Díky tomu jsou tedy globální adresy přímo adresovatelné odkudkoliv. [1]

V dnešní době se nepoužívá celý platný rozsah adres, používají se adresy, které mají prefix 2000::/3 (binárně 001). [27]

Místní registr LIR dostane přidělené globální adresy od IANA nebo od RIR (Regional Internet Registry, pro Evropu a Blízký východ RIPE NCC). Tento registr dostane rozsah adres, který poté rozděluje zákazníkům. [11] [27]

- Agregace - cílem agregace je popsat jediným záznamem ve směrovací tabulce poskytovatelovu síť se všemi zákazníky
- Globální směrovací prefix - identifikuje koncovou síť, přiděluje se zvenčí pomocí lokálního internetového registru, tím je většinou poskytovatel Internetu, tuto část adresy můžeme označovat jako veřejná topologie
- Identifikátor podsítě - rozlišuje jednotlivé podsítě v dané síti, tuto část můžeme označovat jako místní topologie, 2 bajty nám umožňují adresovat 65 536 podsítí, adresy můžeme buď číslovat postupně od jedničky (tzn. tak jak se objevují v nové podsíti), nebo si vytvoříme vlastní hierarchii, pokud zvolíme postupné číslování, tak se zvětšují směrovací tabulky v koncové síti (každá podsíť musí mít vlastní záznam v tabulce)
- Identifikátor rozhraní - zaujímá celou polovinu adresy, to nám umožňuje v jedné podsíti rozlišovat přes $18*10^{18}$ různých rozhraní

3.1.2 Lokální adresy

Lokální adresy platí pouze v podsíti. Považují se za neveřejné adresy. Můžeme je používat jen v koncových sítích. Lokálním adresám chybí celosvětová jednoznačnost, jednotlivé koncové sítě s nimi mohou pracovat, jak potřebují. [27]

V protokolu IPv6 se nachází tři typy lokální adres. Lokální adresy se od sebe liší prefixem.

- Lokální linkové adresy - označují se prefixem fe80::/10, dalších 54 bitů je nulových, za kterými se nachází 64 bitový identifikátor, oficiálně je interpretováno prvních 64 bitů jako adresa sítě a podsítě, ale neslouží ke směrování, hodnota bitů je neměnná a u nikoho se neliší, lokální linkové adresy jsou omezeny na jednu jedinou linku, cílový datagram, který obsahuje lokální linkovou adresu, neprojde žádným směrovačem (za směrovačem leží jiné linky) [6]
- Lokální místní adresy - označují se prefixem fec0::/10, jejich místem je koncová síť, u těchto adres byl problém při připojení jedné organizace v různých lokalitách a tudíž došlo k nahrazení Lokální místní adresy adresami Unikátními lokálními [6]

- Unikátní lokální adresy - jsou nástupcem Lokální místní adresy, označují se prefixem fc::/7, za prefixem se nachází jednobitový příznak L, který označuje, zdali byla adresa přiřazena lokálně (L=1), nebo jinak, v současnosti jsou tyto adresy generovány lokálně, jejich příznak L je nastaven na jedničku a začínají prefixem fd::/8, následujících 40 bitů obsahuje globální identifikátor nesoucí náhodně vygenerované číslo, tato položka může nabývat více než bilionu různých hodnot. [27]

3.1.3 Skupinové adresy

Skupinové adresy se používají především k přenosu zvukového a obrazového signálu v reálném čase (např. videokonference, rozhlasové a televizní vysílání). Největší část adresy slouží k identifikaci skupiny, pomocí níž se dopravují data. Slouží k tomu dvě krátké podpůrné položky - příznaky a dosah skupiny. [27]

Příznaky jsou celkem čtyři: [27]

- První příznak - má vždy hodnotu nula, bude využíván v budoucnosti, tudíž v dnešní době je bezvýznamný
- Příznak R - dle příznaku R poznáme, jestli obsahuje nebo neobsahuje adresu shromaždiště, pokud obsahuje, nabývá bit hodnoty jedna, jestliže neobsahuje, bit nabývá hodnoty nula, příznak R nabývá hodnoty jedna jen za toho předpokladu, že příznak P bude mít také hodnotu jedna
- Příznak P - má hodnotu jedna nebo nula, hodnotu jedna bude mít, jestliže skupinová adresa vychází z individuální anebo z adresy rozhraní
- Příznak T - určuje, zdali je adresa trvalá, nebo dočasná, pokud je adresa trvalá nabývá hodnoty nula, ale pokud je adresa dočasná, nabývá hodnoty jedna

Dosah skupiny nám určuje, jakou vzdálenost mají jednotliví členové. Velikost položky dosahuje hodnoty 4 bitů. Jednotlivé adresy se od sebe mohou lišit. Pro skupinové adresy je v současnosti definováno šest stupňů lokality.

Dosah		Význam
1	rozhraní	nepřekročí jediné rozhraní, vysílání pro lokální smyčku
2	linka	jedna fyzická síť
4	správa	podsíť - nejmenší dosah konfigurovaný správcem
5	místo	část topologie patřící jedné organizaci
8	organizace	několik míst náležících jedné organizaci
E	globální	celosvětový dosah

Obrázek 13 - Dosah skupinových adres

3.1.4 Výběrové adresy

Nejčastěji se používají výběrové adresy pro přibližné rozkládání zátěže, zrychlení doby odezvy, lepší odolnosti proti útokům typů DoS a DDoS a zmenšení počtu adres. [27]

Výběrové adresy nemají svou část adresního prostoru. Výběrové adresy je možné libovolně míchat s adresami individuálními. Pomocí syntaxe nerozdělíme adresy výběrové od adres individuálních. [22] [27]

Síť či skupina sítí je charakterizována prefixem P. Výběrová adresa uvnitř dané sítě, která je charakterizovaná prefixem P, musí mít vlastní směrovací záznam. Tento směrovací záznam vždy ukazuje na nejbližšího člena skupiny v jednotlivých směrovačích. Směrovací záznamy odesílají pakety do jednotlivých výběrových skupin. [27]

3.2 Rozsahy adres verze IPv6

Délka adres protokolu IPv6 je 128 bitů. To je čtyřikrát více než u adres IPv4. Adresy IPv6 se rozdělují do osmi skupin. Každá skupina obsahuje 16 bitů. Adresa se zapisuje hexadecimálním číslem a jednotlivé skupiny adresy se oddělují dvojtečkami. [27]

1234:5678:9ACB:DEF0:1234:5678:9ABC:DEF0

Jednosměrové adresy v IPv6 se skládají z prefixu a ID rozhraní (síť: rozhraní). Maska podsítě se v adresách IPv6 označuje lomítkem. [27]

1234:5678:9ACB:DEF0:1234:5678:9ABC:DEF0/64

V příkladu máme znázorněnou adresu IPv6 s prefixem o délce 64 bitů. Prefix vyjadřuje určitou síť nebo podsíť. Všechna rozhraní, která jsou obsažena v jedné síti, mají stejný prefix (začátek adresy). [27]

3.2.1 Pravidla pro zkracování adres

Pro adresy IPv6 bylo zavedeno několik zkracovacích metod, pomocí nichž můžeme s adresami lépe pracovat. [27]

Pokud je adresa v protokolu IPv6 v jedné či více po sobě jdoucích 16 bitových skupinách tvořena samými nulami, nuly můžeme vynechat a zapsat místo nich dvě dvojtečky (::). Avšak tuto zkratku můžeme použít v adrese jen jednou. [18] [27]

Například adresu:

0123:0000:0000:0000:fedc:ba98:7654:3210

můžeme zkrátit na:

123:0:0:0:fedc:ba98:7654:3210

nebo dokonce jen na:

1234::fedc:ba98:7654:3210

Pokud je adresa v protokolu IPv6 tvořena jednou nebo více nulami, můžeme nuly vynechat. Oproti předchozímu zkrácení můžeme takto zkrátit vícekrát dle potřeby, i když jsme již použili zkratku se dvěma dvojtečkami. [27]

4 Objevování sousedů

Objevování sousedů užíváme k tomu, abychom zjistili linkovou adresu počítače (MAC). V tom se liší protokol IPv6 od protokolu IPv4, kde nám k tomu sloužil samostatný protokol ARP. [27]

Další funkce objevování sousedů v protokolu IPv6: [27]

- Zjišťování linkových adres sousedních uzlů ve stejné lokální síti, dále jejich aktualizace
- Rychlé aktualizace neplatných položek
- Detekování změn v linkových adresách
- Vyhledávání směrovačů
- Přesměrovávání
- Zjišťování prefixů, parametrů sítě a ostatních údajů sloužících pro automatickou konfiguraci adresy
- Ověřování dosažitelnosti sousedů
- Zjištění duplicitních adres

Protokol pro objevování sousedů používá pět typů ICMP zpráv. ICMP zprávy spolu s SEND zprávami zasílají dále.

IP adresu zjistíme tak, že na adresu s prefixem ff02:0:0:0:0:1:ff00::/104 a se zbytkem tvořících posledních 24 bitů adresy počítače, které chceme zjistit, je odeslána výzva sousedovi. Pokud tuto zprávu obdrží počítač, který chceme zjistit, dostaneme odpověď ohlášením souseda s obsahem zjišťované MAC adresy (linkové adresy). Dojde-li ke zjištění změny této MAC adresy, může, ale nemusí, změnu ohlásit nevyžádaným ohlášením souseda. Toto hlášení odešle na adresu ff02::1. [27]

4.1 Detekce dosažitelnosti souseda

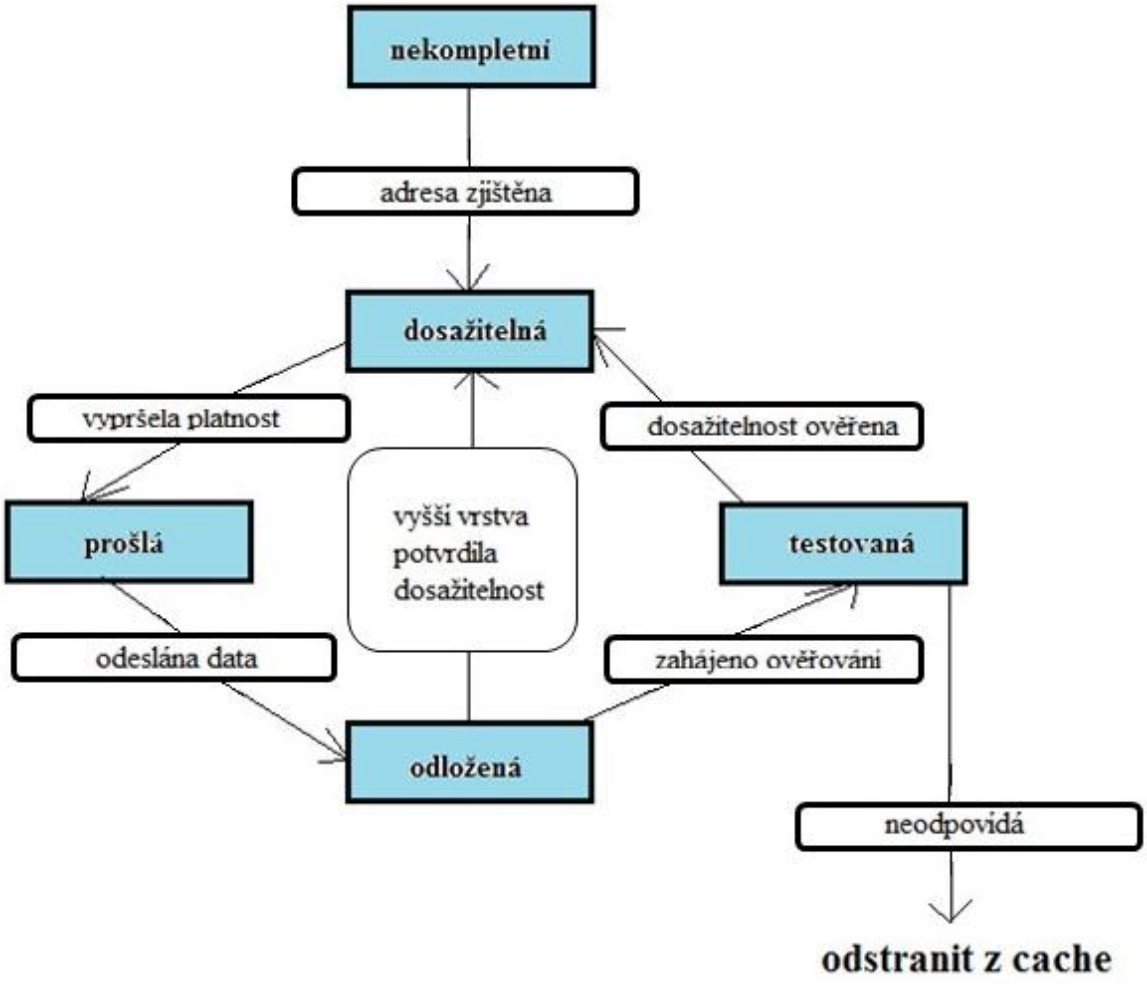
K tomu, že je soused dosažitelný, nám slouží dva možné způsoby. [27]

- Prvním způsobem je získávání zprávy od vyšší vrstvy (TSP).
- Druhým způsobem je to, že zašleme výzvu sousedovi. Jestliže soused odpoví, máme jistotu, že je spojení v pořádku.

Existuje tzv. cache sousedů, ve které jsou uchovány informace o stavu sousedů. Máme několik druhů stavů adres: [15]

- Nekompletní (Incomplete) - zatím neznáme linkovou adresu a její zjištění právě probíhá
- Dosažitelná (Reachable) - cíl bereme za dosažitelný
- Prošlá (Stále) - dané položce prošla platnost, její obnova je možná pouze tehdy, budou-li pro cíl zjištěna data

- Odložená (Delay) - dané položce prošla platnost, avšak data byla k cíli odeslána, musíme čekat, až vše potvrdí vyšší vrstva
- Testovaná (Probe) - dané položce prošla platnost, výzvy jsou ale odeslány sousedovi



Obrázek 14 - Změny stavu adresy v cache sousedů

5 Funkce protokolů

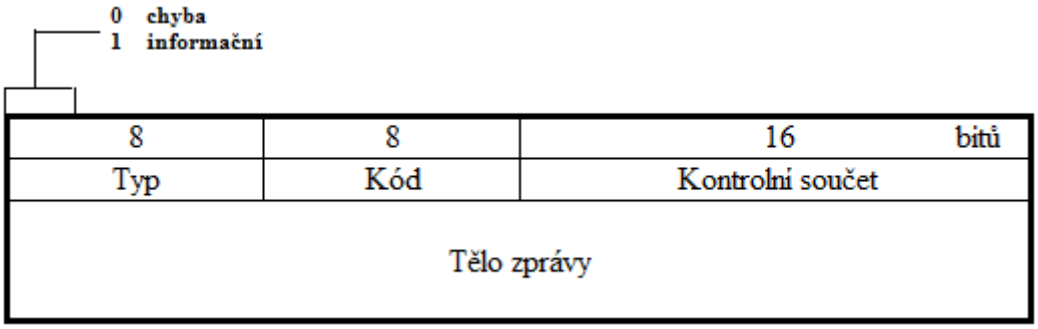
5.1 ICMPv6

ICMPv6 je nová verze protokolu ICM. Protokol ICM je nedílnou součástí tohoto novějšího protokolu. ICMP zprávy jsou předávány uvnitř IPv6 paketu, který můžeme zahrnout jako rozšiřující hlavičky IPv6. ICMPv6 nabízí komplexní řešení a různé funkce. Zjednodušuje proces komunikace odstraněním zastaralých zpráv. [30]

Protokol ICMPv6 můžeme využít k: [30]

- Ohlašování chybových stavů
- Testování dosažitelnosti
- Výměně některých provozních informací

Všechny zařízení mající protokol IP, musí užívat i protokol ICMPv6. Je obsažen za základní hlavičkou protokolu IPv6. Pomocí protokolu ICMPv6 nedochází k fragmentaci protokolu IPv6. Hodnota 58 v položce další hlavička nám říká, že IP datagram obsahuje ICMP zprávu. [18] [27]



Obrázek 15 - Formát ICMP zprávy

Všechny ICMP zprávy tvoří stejný základ, jak je možné vidět na obrázku č. 15 výše. [6] [27]

- Typ (Type) - první bit nám říká, o jaký druh zprávy se jedná - jedná-li se o chybovou nebo informační zprávu, pokud je to zpráva chybová, hodnota je nula, ale pokud se jedná o zprávu informační, bude hodnota jedna.
- Kód (Code) - pomocí kódů rozpoznáváme několik podtypů
- Kontrolní součet (XXX) - pokud by došlo k nějakému poškození datagramu, tato položka obsahuje celkovou velikost dat
- Tělo zprávy (Message body) - je závislé na typu zprávy, většinou je hodnota 4 bajty, tato položka může obsahovat užitečnou informaci nebo nemusí obsahovat nic

Chyby	
1	cíl je nedosažitelný
2	příliš velký paket
3	vypršela životnost paketu
Echo	
128	požadavek na echo
129	odpověď na echo
Objevování sousedů	
133	výzva směrovači
134	ohlášení směrovače
135	výzva sousedovi
136	ohlášení souseda
137	přesměrování
Informace o uzlu	
139	dotaz na informace
140	odpověď s informacemi

Obrázek 16 - Typy ICMP zpráv

V rozmezí 0-127 máme zprávy chybové a v rozmezí hodnot 128- 255 se nachází zprávy informační. Pokud máme hodnotu 100, 101, 200 a 201, jedná se o zprávy pro soukromé experimenty. Hodnoty 127 a 225 jsou rezervovány pro další rozšiřování ICMP zpráv do budoucna. [13]

5.1.1 Chybové zprávy

Jsou zatím definovány prozatím jen čtyři: [13] [27]

1) Nedosažitelnost cíle - zpráva je odeslána směrovačem, pokud obdrží datagram určený pro adresu, kam ho není možné dopravit z důvodu chybějící adresy, nastavení firewallu atd., nedosažitelnost cíle má hodnotu jedna, podrobnosti nalezneme v kódu k ICMP zprávě

0	neznám žádnou cestu k cíli
1	správce zakázal komunikaci
2	mimo dosah zdrojové adresy
3	nedosažitelná adresa (cíl neodpovídá)
4	nedosažitelný port (cíl neodpovídá)
5	zdrojová adresa odporuje vstupně/výstupní politice
6	cesta k cíli je zakázána

Obrázek 17 - Kódy pro Nedosažitelnost cíle

2) Příliš velký paket - jestliže MTU linka je menší než je datagram, odešle směrovač zprávu příliš velký paket
3) Vypršela životnost paketu - jestliže je vyčerpán maximální počet skoků (hop limit) v hlavičce, odešle směrovač zprávu „Vypršela životnost paketu“
4) Problém s parametry - zpráva je odeslána po obdržení datagramu adresátem a ten není poté schopen se vyrovnat s parametry dané informace

5.1.2 Informační zprávy

Informačních zpráv existuje více, než zpráv chybových. Nejdůležitější informační zprávy jsou dvě, další zprávy referují hlavně o objevování sousedů a dalších více komplexních služeb. [13] [27]

- Echo - používáme příkaz ping, po užití tohoto příkazu zjistíme, jaká je dostupnost uzlu a jakou odezvu uzel má
- Informace o uzlu - tímto příkazem zjistíme jméno uzlu a jeho IP adresy, tato zpráva nám velmi dobře poslouží ve chvíli, kdy dojde k výpadku DNS

5.1.3 Bezpečnostní opatření

Typy tohoto zabezpečení mají minimalizovat útoky na ICMP, a to hlavně DoS. Jedním z řešení bylo omezení počtu ICMP datagramů za časovou jednotku. Dalším řešením je to, že ICMP datagramům přidáme autentizační či šifrovací hlavičku. Jestliže hlavička neodpovídá u datagramu, bude datagram zahozen. [27]

6 Automatické přidělování adres

Automatická konfigurace slouží k přidělování IP adres hostitelům bez příslušnosti jakéhokoliv serveru. To nám ulehčuje konfiguraci jednotlivých počítačů, které se nacházejí v síti. V protokolu IPv6 se užívají dva způsoby automatického přidělování adres: [22]

- Stavová konfigurace
- Bezstavová konfigurace

6.1 Stavová konfigurace

Funkce stavové konfigurace se velmi podobá principu funkce DHCP v protokolu IPv4. Rozdílem je identifikace. Původně se využívala s pomocí MAC adresy. Nyní nám k identifikaci slouží DHCP Unique Identifier (DUID). [27]

Každému uzlu musí být připojeny tři DUID:

- Sériové číslo (číslo je dáno výrobcem) – je neměnné po celou dobu existence
- Kombinace linkové adresy, čas vytvoření
- Linková adresa

DUID má každý klient a server. Měl by být pokud možno stálý a neměnit se ani při výměně síťové karty počítače. [27]

DHCPv6 je síťový protokol, který se používá pro konfiguraci IPv6 hostitele s adresami IP, které jsou potřebné k provozu v síti IPv6. [8]

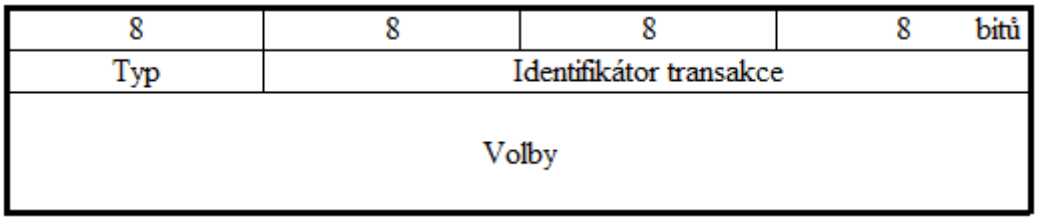
Získat síťové parametry můžeme pomocí protokolu DHCP ve čtyřech fázích: [27]

- Objevování (Discover) - Klient zašle všesměrový dotaz (na IP adresu 255.255.255.255), který obsahuje jeho ethernetovou adresu.
- Nabídka (Offer) - Servery, ke kterým se dotaz dostane (často bývá jeden, ale může jich být také volitelné množství), prohledají své tabulky, a pokud mají pro klienta použitelné parametry, zašlou mu nabídku.
- Požadavek (Request) - Klient přijme veškeré nabídky, které mu byly zaslány, a poté vybere takovou nabídku, která je pro něj nejlepší. V dalším kroku příslušnému serveru zašle požadavek, ve kterém požádá o přidělení parametrů.
- Potvrzení (Acknowledge) - Server zašle potvrzení, že žádost byla kladně vyřízena. Tímto okamžikem jsou příslušné parametry připraveny k využívání klientem. Přidělení parametrů má omezenou platnost, po vypršení platnosti je nutné žádat o prodloužení nebo získat zcela nové parametry.

Pro přidělení adresy se používají tři prvky: [27]

- Klient – získává informace od zařízení
- Server – zařízení poskytující informace

- Zprostředkovatel – zprostředkovává informace mezi klientem a serverem, pokud se nacházejí na různých linkách

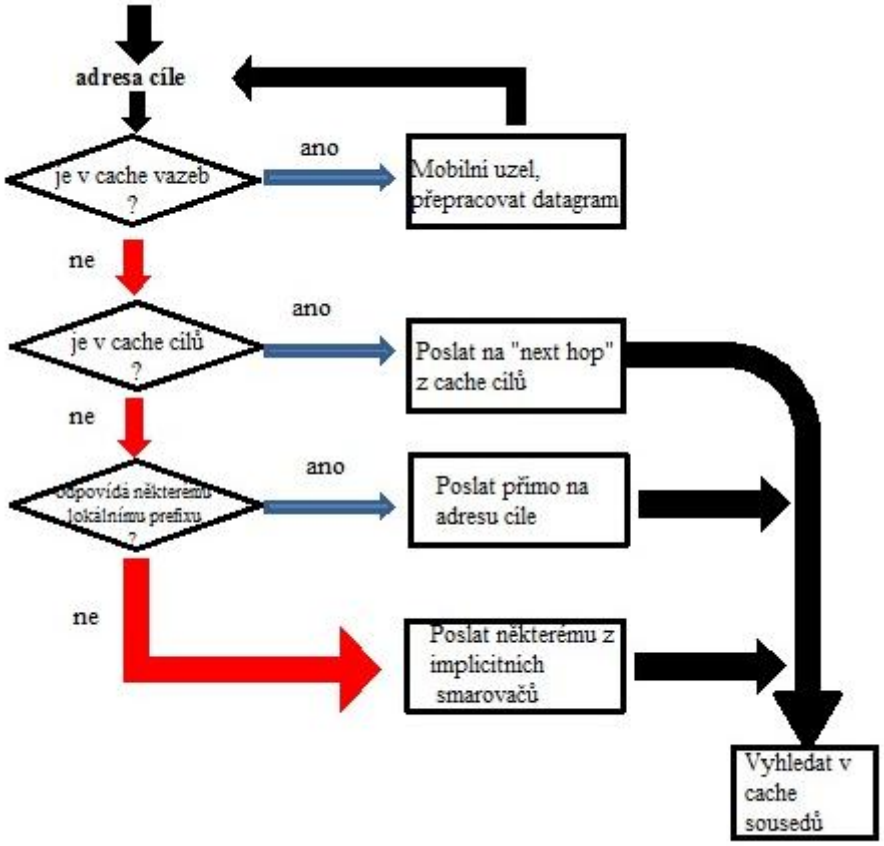


Obrázek 18 - Formát zprávy DHCPv6

6.2 Bezstavová konfigurace

Bezstavová konfigurace nám sdělí jen velmi málo informací. Konfigurace doplňuje další součásti jiným způsobem. Bezstavová konfigurace postrádá adresy místních DNS serverů. Bezstavová konfigurace využívá informace ve zprávách směrovačů. Tyto zprávy jsou zasílány v náhodných časových intervalech. [6] [27]

Při přidělování adresy si uzel vygeneruje lokální linkovou adresu a pomocí mechanizmu objevování sousedů zjistí, jestli je tato adresa unikátní. Po zjištění adresy dostane ohlášení od směrovače, zdali má použít stavovou konfiguraci (DHCP). Získá další informace o lokální síti. V případě, že se nemá použít stavová konfigurace, musí získat z dostupných informací prefix. Prefix se připojí před vygenerovanou část linkové adresy a tím se získá adresa unikátní. [6] [18] [27]



Obrázek 19 - Postup při odesílání datagramu

7 Funkce protokolu DNS

DNS, celým názvem Domain Name System, se používá pro překlad IP adres počítačů na taková jména, která si uživatelé zapamatují snadněji, než složité zápisy IP adres. Příkladem je třeba adresa www.seznam.cz, což je mnohem lépe zapamatovatelné, než IP adresa, která je 77.75.72.3. V protokolu IPv6 je funkce protokolu DNS nepostradatelná a to z toho důvodu, že IP adresy jsou delší a mnohem hůře zapamatovatelné. [9] [27]

DNS obsahuje dva typy dotazů:

1. Dopředné dotazy (AAAA)
2. Zpětné dotazy (PTR)

7.1 Dopředné dotazy

Překládají ze symbolických jmen na IP adresy. V IPv4 se používá zápis typu A, a protože IPv6 adresy jsou čtyřnásobně větší, musíme používat zápis AAAA. Například počítač pc.kdesi.cz má adresu 2001:db8:89ab:1:123:45ff:fe67:, bude pro doménu kdesi.cz obsažen záznam: [5] [22] [27]

pc AAAA 2001:db8:89ab:1:123:45ff:fe67:89ab.

Jestliže počítač pc má více adres v dané síti, všechny záznamy budou uvedené v AAAA. [5] [27] Příkladem je:

pc AAAA 2001:db8:89ab:1:123:45ff:fe67:89ab

AAAA 2002:a00:1:1:123:45ff:fe67:89ab

7.2 Zpětné dotazy

Jsou opakem dopředných dotazů, tudíž se užívají k překladu na symbolická jména z IP adres. K překladu se používají záznamy typu PTR. Prvním krokem je doplnění nul, které se nesmí vynechat. Dalším krokem je otočení pořadí hexadecimálních číslic. Posledním krokem je přidání ip6.arpa nakonec. [5] [27]

Příkladem je:

b.a.9.8.7.6.e.f.f.f.5.4.3.2.1.0.1.0.0.0.b.a.9.8.8.b.d.0.1.0.0.2.ip6.arpa.

7.3 Adresy v DNS

Do DNS můžeme zařadit tyto adresy: [27]

- Globální individuální adresy - mají dlouhodobou platnost
- Dlouhodobě platné adresy přechodových mechanizmů (6 to 4)

Do DNS nepatří tyto adresy: [27]

- Lokální linkové adresy - platnost těchto adres je pouze pro místní linku, DNS klient nemůže zjistit adresu linky
- Náhodně generované krátkodobé adresy

Pokud počítač komunikuje jen přes IPv4 nebo IPv6 adresu, je zařazení DNS jednoznačně dáno. Pokud ale počítač komunikuje oběma protokoly, tak se používají dva základní přístupy - stejné jméno a odlišná jména. [27]

8 Směrovací protokoly IPv6

Pod pojmem směrování si můžeme představit hledání určité cesty. Touto cestou odesíláme datagram s informacemi k potřebnému cíli. Hlavním ukazatelem, který dovede datagram k cíli, je tzv. směrovací tabulka. Ve směrovací tabulce jsou zapsány veškeré informace o tom, kudy musí datagram projít (jakými rozhraními), aby došel ke svému cíli. [27]

Směrovače, routery, vlastní jedny z nejrozsáhlejších směrovacích tabulek. Tyto tabulky mají jak statické, tak dynamické záznamy. Pomocí dynamických záznamů získává směrovač aktuální informace mezi ostatními směrovači. Dynamické záznamy mají na starosti směrovací protokoly. [27]

Směrovací protokoly se dají rozdělit do dvou skupin. První skupinou jsou tzv. Internal Gateway Protocol (IGP). Druhou skupinu tvoří tzv. External Gateway Protocol (EGP). [27]

8.1 Internal Gateway Protocol (IGP)

Protokol IGP jsou využívány k výměně dat o směrování v rámci autonomního systému. Autonomní systémy utváří soubor sítí, které mají společnou administrativní doménu. Tzn, že v praxi všechny směrovače, které jsou součástí autonomního systému, sdílejí stejná data ze směrovacích tabulek. [18]

Protokoly IGP slouží ke správě směrovacích tabulek uvnitř jednoho autonomního systému. Protokoly se snaží hlavně o to, aby reakce v síti byla rychlá. [27]

V současné době můžeme zmínit tři druhy IGP protokolů. Ty můžeme použít pro protokol IPv6. Jmenovitě to jsou protokoly: RIPng, IS-IS, OSPFv3. [27]

8.2 External Gateway Protocol (EGP)

Tyto protokoly slouží k výměně směrovacích informací mezi autonomními systémy. Díky EGP se směrovače (routery) dozvídají, jakou cestou se dostanou do autonomního systému a které prefixy jsou v něm dostupné. Vstupní směrovač autonomního systému uchovává ve svých tabulkách prefixy do celého internetu a musí mít adekvátní kapacitu. [27]

EGP protokoly přenášejí obrovské objemy informací. Díky této skutečnosti ve srovnání s protokoly IGP reagují pomaleji. [27]

V současné době máme jediný protokol, který je upravený pro protokol IPv6. Tímto protokolem je BGP4+. [18]

8.3 Směrovací protokol RIPng

Routing Information Protocol next generation (RIPng) je novější verzí protokolu RIPv2. Jedním z hlavních rozdílů je využívání IPv6 adres. Ve verzi RIPv2 se využívaly adresy IPv4. [27]

Protokol RIPng můžeme hledat hlavně v menších koncových sítích. Jedná se o protokol s vektorem vzdáleností, maximální počet přeskoků je patnáct a používá rozdělení horizontu a další mechanizmy, které předcházejí smyčkám. Standardně je využíván na portu 521 protokolu UDP. [18]

Směrovací tabulka musí pro potřeby RIPng ke každému cíli obsahovat následující údaje: [27]

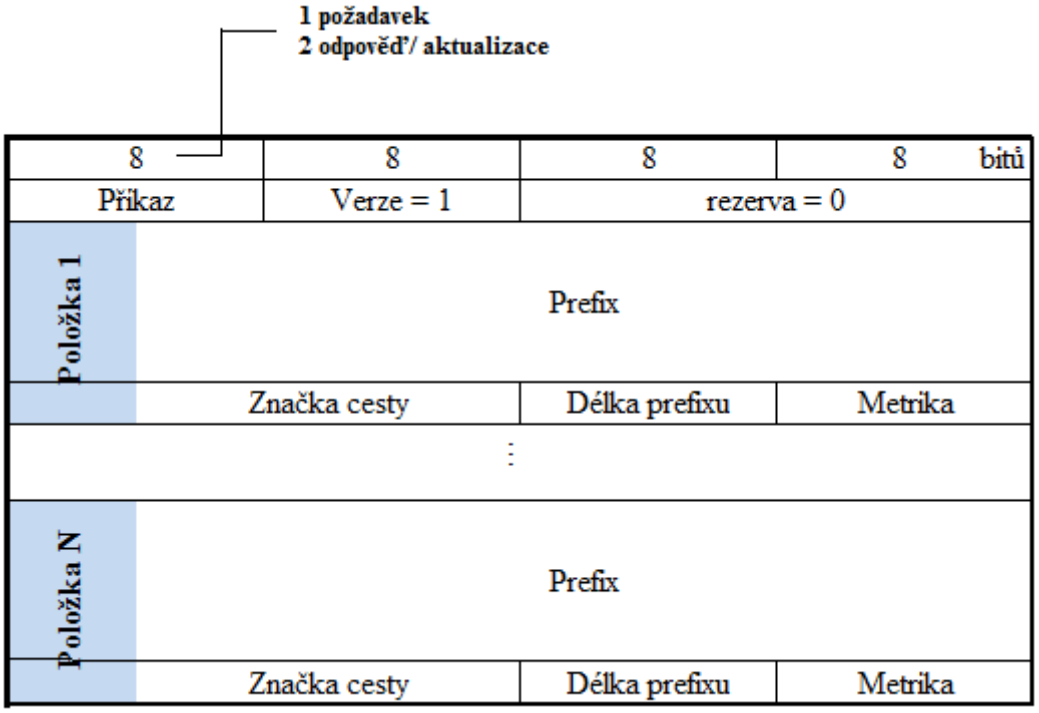
- Prefix cíle (hodnota, délka)
- Metriku odpovídající celkové ceně cesty
- Adresu dalšího směrovače na cestě (komu se mají datagramy předávat, které směřují k cíli)
- Příznak změny
- Časovače (doba platnosti a likvidační interval)

Směrovače zasílají údaje z tabulky svým sousedům každých 30 sekund. Aby se zabránilo synchronizaci, je čas intervalu posunut od -15 s do +15 s. Směrovače si tímto způsobem udržují informace o všech cestách neustále aktualizované. [27]

Jakmile směrovač obdrží aktualizovanou tabulku od souseda, dojde k přičtení hodnoty k cestě ceny linky. Tato cena pochází z té linky, od které přišlo ohlášení. Dojde k porovnání směrovačem všech svých údajů dle své tabulky. Jestliže se některé údaje liší, aktualizuje si stávající směrovací tabulku. [27]

Jak již výše bylo řečeno, cesty nabývají hodnot 1-15. Dojde-li k hodnotě vyšší, např. 16, považuje se cesta za nedosažitelnou, tzn. datagramy budou zahozeny a ztraceny. [18] [27]

Oproti protokolu RIPv2 v protokolu IPv4 je RIPng v protokolu IPv6 vybaven aktualizací, která zabraňuje vznikům smyček, pokud dojde k nedosažitelnosti cíle. Tímto byl vyřešen problém se zacyklením. [27]



Obrázek 20 - Formát zprávy pro RIPng

8.4 Směrovací protokol OSPFv3

Open Shortest Path First (OSPFv3) je směrovacím protokolem, který byl vytvořen k tomu, aby nás informoval o tom, v jakém stavu se linky nachází. [20] [27]

Pro každý směrovač je důležité, aby měl mapu sítě. Tyto mapy si směrovače aktualizují, aby měli přehled o tom, jaké informace mají okolní směrovače, dále jsou zde informace o cenách linek, prefixech sítí aj. [20] [27]

Reakce na přicházející nové aktuální informace je velmi rychlá. Jakmile dojde ke změně tabulky u některého směrovače, dojde k zaslání o této nově vzniklé změně všem ostatním směrovačům. Ostatní směrovače si poté mohou své tabulky aktualizovat dle nově zaslaných informací. [18] [27]

Mapa sítě je vlastně orientovaný graf. Jednotlivými vrcholy jsou směrovače a skupinové sítě. Aby byl příklad zjednodušen, vezmeme v potaz dva druhy linek: dvoubodové a skupinové. Dvoubodovou linkou je např. ADSL. Zde je spojena dvojice směrovačů. Skupinovou linkou je např. Ethernet. V tomto linkovém připojení je připojeno několik směrovačů a je zde podpora skupinového adresování. V grafu se nachází uzly (tvořeny směrovači a koncovými sítěmi) a hrany (ty tvoří jednotlivé linky). Každé hraně je vždy přiřazena jedna hodnota, která se musí pohybovat v rozmezí 0 - 65535. Hodnota, která je přiřazena, vypovídá o ceně cesty. OSPF při hledání optimálních cest sčítá ceny linek a hledá ty, které mají nejnižší součet. [18] [27]

8	8	8	8 bitů
Verze = 3	Typ zprávy	Délka paketu	
Identifikátor směrovače			
Identifikátor oblasti			
Kontrolní součet		Ident. Instalace	0

Obrázek 21 - Hlavička OSPF zprávy

Úkolem jednotlivých směrovačů je rozřazení okolních směrovačů do jedné ze dvou skupin. V OSPF dle Satrapy se tomu říká výměna informací o změnách v topologii.

Skupiny, do kterých se okolních směrovače řadí, jsou: [27]

- Okolní směrovače (Neighbors) - s těmito směrovači je navázané spojení přímé (buď je spojení dvoulinkové, či jsou připojení ke stejné lince)
- Sousedé (Adjacent routers) - selekce z okolních směrovačů, dochází k výměně informací o mapě sítě

Sousedem se nestane každý okolní směrovač. U dvoubodových spojů je vytvoření sousedství stoprocentní. U skupinových linek dochází dle Satrapy ke zvolení v rámci jedné skupinové linky tzv. pověřeného směrovače (designated router). Všichni sousedé pověřeného směrovače se stanou sousedy. Tuto skutečnost se dozví tak, že všichni sousedé obdrží, tzv. Hello paket. V tomto paketu jsou ukryty informace (identifikace pověřeného směrovače pro danou síť, identifikátory všech směrovačů, o nichž ví). [27]

Mapa sítě je databáze linek, která slouží k oznamování stavu v určitém místě. Toto oznámení se v OSPF jmenuje, Link State Advertisament (LSA) a posílá je ten směrovač, u něhož informace vzniká. Existuje několik typů LSA. [18] [27]

Jestliže chtějí dva sousední směrovače mezi sebou komunikovat, naváží mezi sebou sousedský stav. Po navázání tohoto stavu dojde následně k aktualizaci mapy sítě. Aktualizace mapy sítě probíhá tak, že protokol OSPF zašle svému protějšku sadu zpráv (popis databáze). Popis databáze obsahuje identifikátory a verze LSA. Protější směrovač zkontroluje verzi LSA, a pokud ji nezná a nebo má starší verzi než přijal, tak dojde k aktualizaci této verze. Následně o ně požádá pomocí Žádostí o stav linky (Link state request) a očekává, že mu soused pošle „Aktualizaci stavu linky“ (Link state update) pro všechny požadované. Po obdržení všech aktualizací o stavu linky, jsou databáze synchronní a informace, které vlastní oba sousedé, jsou stejné. [18] [22] [27]

Aktualizace stavu linky slouží jako hlášení pro sousedy o tom, že v síti došlo ke změně. Synchronizace map je velice rychlá. V protokolu OSPF se posílají pouze aktuální změny, proto má protokol velmi malou režii. [18] [27]

Typ	Název	Význam
1	Hello	zjištění okolních směrovačů
2	Popis databáze	shrnuje obsah databáze
3	Žádost o stav linky	požaduje LSA
4	Aktualizace stavu linky	aktualizuje databáze (posílá LSA)
5	Potvrzení stavu linky	potvrzuje aktualizaci

Obrázek 22 - Typy OSPF zpráv

V OSPF mluvíme o tzv. oblastech sloužících k rozdělení autonomního systému na části omezující objem přenášených informací. [27]

Za oblast (area) je v OSPF označována skupina souvislých sítí a strojů v nich a také všechny směrovače, které mají rozhraní do některé z těchto sítí. [27] Každá oblast má v sobě ukryté mapy. Tyto mapy reprezentují vlastní síti v oblasti. [20]

Hraničním směrovačem nazýváme takový směrovač, jenž vlastní rozhraní do více než jedné oblasti. Hraniční směrovač musí obsahovat samostatnou mapu sítě pro každou oblast, ve které je zapojený. [27]

8.5 Směrovací protokol IS- IS

Intermediate system to Intermediate system (IS- IS) byl základem při tvorbě směrovacího protokolu OSPF. Základ je tedy v podstatě stejný jako u protokolu OSPF, ale určitými detaily se liší, jako např.: [20] [27]

- Terminologií
- Formáty zpráv
- Postupy pro zpracování zpráv
- Hierarchické směrování v IS- IS - kompletní mapa topologie je udržována jen v rámci jedné oblasti, celý směrovač je jen v jedné oblasti, hranice jsou mezi oblastmi, které procházejí linkami
- Při vzniku oblasti musí být v IS- IS obsažen nejméně jeden směrovač
- Směrovače v protokolu IS-IS mají dvě úrovně
  - podle Satrapy úroveň 1 patří takovým směrovačům, které patří dovnitř oblasti, na starost mají topologii vnitřní
  - směrovače úrovně 2 zajišťují komunikaci a výměnu informací mezi oblastmi
  - komunikace je možná vždy jen mezi směrovači nacházejícími se ve stejné úrovni

- tzv. L1/L2 směrovač má úrovně obě, tudíž jemu je umožněna komunikace vnitřní oblasti s vnějším okolím

- Absence páteřní oblasti oproti OSPF - IS-IS má libovolné kompozice
  - zde je páteř tvořena souvislou typologií L2 směrovačů, jež může procházet libovolně
  - po odeslání je datagram doručen L1 směrovači odesilatelovi oblasti do vhodného L2 směrovače, dále putuje L2 infrastrukturou do cílové oblasti, kde je místními L1 směrovači doručen adresátovi

8.6 Směrovací protokol BGP4+

Border Gateway Protocol (BGP4+) patří do kategorie EGP. Pomocí BGP4+ dochází k výměně směrovacích informací, které jsou mezi autonomními systémy. [3]

Proces v protokolu BGP4+ je celkem jednoduchý. Dojde ke shrnutí prefixů z vlastní sítě. Ty potom uloží jako jednu cestu. Tuto nově vzniklou cestu rozešle svým sousedům, kteří se nachází v jiných autonomních systémech. Informace se šíří stále dál tím, jak si ji jednotlivé systémy předávají a vědí, kudy je síť dále dostupná. [27]

Správce systému nastaví staticky všechny sousedy. Spojení mezi sousedy je udržováno pomocí TCP. Na počátku tohoto spojení dojde k výměně směrovací informace. Jestliže je spojení přerušeno, směrovač vyhodnotí, že je soused nedosažitelný. Směrovač si ze svých směrovacích tabulek vymaže všechny cesty, které pocházely od nedosažitelného souseda. [27]

9 Přechodové mechanizmy

Jelikož nemůžeme přejít z protokolu IPv4 na protokol IPv6 ze dne na den, musíme využívat tzv. přechodové mechanizmy. Přechodové mechanizmy nám umožňují, aby byl přechod plynulý a bez větších obtíží. [27]

Je několik různých mechanizmů, které nám tento přechod umožní: [27]

- Dvojí zásobník – zařízení funguje jak s protokolem IPv4, tak i s protokolem IPv6
- Tunelování – zařízení zabalí datagram pocházející z protokolu IPv6 jako data a pošle je přes síť IPv4 [20]
- Translátory (Překladače) – zařízení, které umožňuje překládat pakety z protokolu IPv4 do protokolu IPv6 a obráceně

Tunelování	
6to4	RFC 3056
6over4	RFC 2529
ISATAP	RFC 5214
Teredo	RFC 4380
Translátory	
SIIT	RFC 2765
NAT-PT	RFC 2766
NAT64	draft - bagnulo - behave - nat64

Obrázek 23 - Metody pro přechod k IPv6

9.1 Dvojí zásobník

Toto zařízení používá jeden zásobník, ve kterém jsou uchovány oba dva typy IPv4 a IPv6 adres. Abychom obdrželi adresy, musíme použít jednu ze standardních metod – manuální konfiguraci nebo DHCP. Pro získání IPv6 se kromě manuální konfigurace používá některá z forem automatických – bezstavová a nebo DHCPv6. Komunikace mezi protokoly probíhá na vyšší vrstvě TCP/ IP modelu (zpravidla na aplikační vrstvě). Nevýhodou dvojího zásobníku je nutnost mít i IPv4 adresu, což není vzhledem k přechodu na protokol IPv6 optimální. Zařízení podporující oba protokoly jsou označovány jako IPv4/ IPv6 uzly. [18] [20] [27]

9.2 Tunelování

Mezi IPv4 a IPv6 nemůžeme provádět přímé spojení, jelikož oba protokoly mají rozdílnou adresaci. To znamená, že protokol IPv4 nerozumí adresám odeslaných z IPv6. Musíme tedy vytvořit tzv. překrytou síť. Koncová síť IPv4 musí získat IPv6 adresu. Následně po získání této adresy je umožněna komunikace mezi oběma protokoly a je zpřístupněna cesta k odesílání datagramů. [21] [24] [27]

Pomocí tunelování dochází k balení jednoho protokolu do protokolu druhého. Tunel obsahuje dva konce. Každý konec nese svou IPv4 adresu. Když dojde na jednom konci ke komunikaci, vezme se IPv6 datagram a ten se vloží do nově vytvořeného IPv4 datagramu. Cílovou adresou je adresa IPv4 druhého konce tunelu. Odesílatelem je IPv4 adresa, kde se zahájil přenos. Při tunelování IPv6 datagram vyznačí hodnotu 41 v položce protokolu obalujícího IPv4 datagramu. [22] [27]

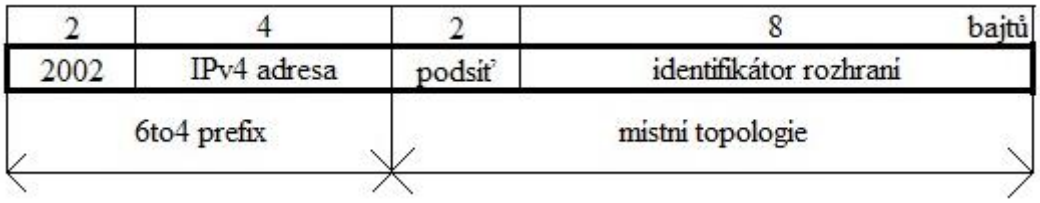
Datagram je odeslán přes IPv4 síť. Jakmile datagram dorazí do cíle (na konec tunelu), příjemce pozná dle protokolu 41, že se jedná o tunelovaný paket. Z tohoto paketu rozbalí IPv6 datagram a ten poté zpracuje podle jeho cílové adresy a směrovacích tabulek pro IPv6. [20] [27]

Během průchodu tunelem se IPv6 datagram neprojde žádnou změnou. Průchod tunelem se považuje za jeden skok a vybalující směrovač zmenší položku Max. skoků v IPv6 hlavičce o jedničku. [27]

9.2.1 6to4

Tunelovací mechanismus 6to4 je definován v RFC 3056 jako jeden z automatických mechanizmů. Tyto mechanizmy mají za úkol spojovat IPv6 ostrůvky přes IPv4 síť. 6to4 je využíván celým internetem jako jedna síť, která vše spojuje. [2] [6] [25]

Hlavní výhodou je nezávislost 6to4. Nemusí mít podporu od poskytovatele Internetu, jelikož při používání 6to4 musíme mít alespoň jednu veřejnou IPv4 adresu. Tuto adresu má přiřazen směrovač, který je připojen jak k IPv4 internetu, tak ke koncové IPv6 síti. Tímto směrovačem prochází všechna data, která jsou přepravována pomocí 6to4. Díky této výhodě je 6to4 velmi oblíbený mezi těmito uživateli. [18] [28]



Obrázek 24 - Struktura 6to4 adresy

Při používání 6to4 se vytvoří z IPv4 adresy IPv6 prefix mající délku 48 bitů. Prefix má hodnotu 2002::/16 a podle prefixu se pozná, že jde o prefix 6to4. Ostatních 32 bitů tvoří IPv4 adresa přístupového směrovače. Vzniká prefix standartní délky, který umožňuje adresovat počítače v síti obvyklým způsobem. [22] [27]

9.2.2 6over4

Počítače nacházející se v síti musí pracovat jak s protokolem IPv4, tak s protokolem IPv6, jelikož dochází k tunelování Pv6 datagramů do IPv4. Datagramy se posílají tunelem směrovači, který podporuje 6over4. Směrovač podporující 6over 4 posílá dále datagram do IPv6 sítě. Jakýkoliv počítač podporující 6over4 musí mít svou IPv4 adresu. [2] [27]

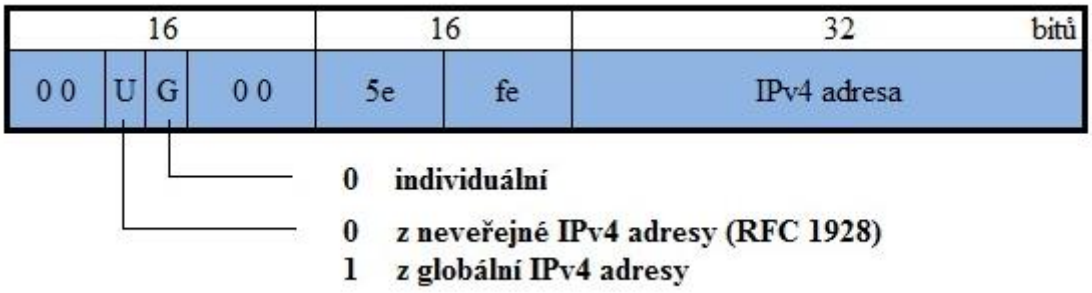
Aby došlo ke vzniku IPv6 adresy, musíme k prefixu podsítě připojit identifikátor rozhraní. První čtyři bajty mají hodnotu nula. Další bajty mají IPv4 adresu příslušného rozhraní. Počítače, které využívají 6over4, používají běžné mechanizmy protokolu IPv6, jako např. objevování sousedů, anebo automatická konfigurace. [2] [27]

9.2.3 ISATAP

Přechodový mechanizmus ISATAP je složen ze tří částí. První část tvoří počítač zapojený jenom do sítě IPv4, druhou část tvoří zapojený počítač do sítě IPv6. Třetí částí je server ISATAP zapojený jak do sítě IPv4, tak do sítě IPv6. Hlavním úkolem ISATAP serveru je přidělování globální IPv6 adresy do IPv4 uzlu. Dále komunikuje mezi oběma sítěmi. [24] [26]

Principem se nijak výrazně neliší od předchozího 6over4. Cíl je také stejný, ale výhodou je, že nevyžaduje žádné nadstandardní služby od protokolu IPv4. Adresa se skládá z prefixu, jehož velikost je 64 bitů. Potom je 32 bitů, které jsou tvořené identifikátorem ISATAP a posledních 32 bitů tvoří IPv4 adresa. V IPv6 adrese je zabalená adresa IPv4. Zabalení datagramu probíhá dle standardní tunelovací procedury. Aby mohlo dojít k zabalení, je podmínkou mít zařízení podporující ISATAP. [22] [27]

ISATAP zavedl speciální formát pro adresu rozhraní, která je tvořena na základě IPv4 adresy dotyčného stroje. Prvních 32 bitů obsahuje konstantu 0000:5efe, za níž následuje 32 bitů s IPv4 adresou. [27]

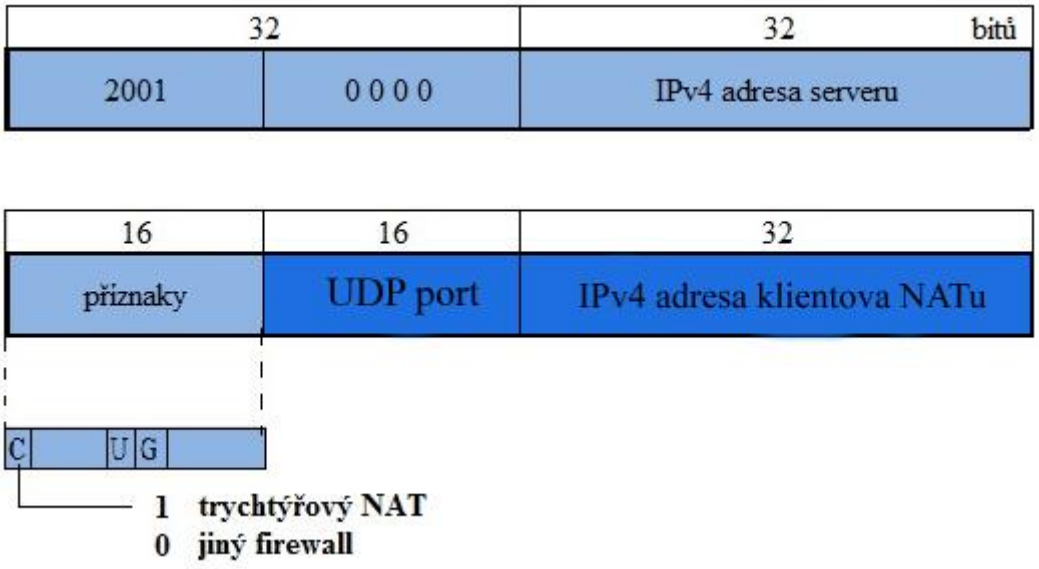


Obrázek 25 - Identifikátor rozhraní ISATAP

9.2.4 Teredo

Mechanizmus Teredo byl vytvořen vývojáři z Microsoftu. Využití Teredo mechanizmu by mělo být zúženo jen na nejnutnější případy, kdy nemůžeme využít jiných přechodových mechanizmů. Nicméně v operačním systému Windows Vista je tento tunelovací mechanizmus pro IPv6 nastaven jako výchozí. [1] [27]

Teredo je jeden z dalších mechanizmů tunelování. Vzhledem ke komplikacím, které přináší NAT (změny portu a adres), umožňuje Teredo provádět tunelování uvnitř Natované sítě. Tunelovací mechanizmus Teredo je vhodný díky již zmíněnému tunelování uvnitř NATů pro domácí sítě. Nevýhodou je ale velmi nízká efektivita. [6] [11]



Obrázek 26 - Struktura adresy pro Teredo

Teredo využívá dosti složitý formát IPv6 adres. Adresy začínají konstantním prefixem 2001::/32. Za prefixem je zapsána IPv4 adresa Teredo serveru. Adresa má délku 64 bitů a tvoří první polovinu, která je součástí serveru. [27]

Druhá polovina je složená z identifikátoru rozhraní, který určuje klient sám. Délka identifikátoru rozhraní je 16 bitů. Posledních 48 bitů, které definují konec NATu, se skládají z 16b čísla UDP portu a 32b IPv4 adresy klientova NATu. [27]

Jako Teredo klient je označován ten počítač, který je v lokální síti IPv4 za NATem a chtěl by přistupovat k IPv6 internetu. Jakmile zahájí komunikaci, musí si nejdříve obstarat adresu. Adresu získá odesláním výzvy směrovači, kterou zabalí do UDP paketu. Zašle ji prostřednictvím serveru na IPv4 adresu. Server obsahuje IPv4 a IPv6 adresu. Server odešle klientovi odpověď ve formátu ohlášení směrovače. Klient si z odpovědi sestaví IPv6 adresu. [11] [27]

Z důvodu nízké režie, je vhodné Teredo používat v takových případech, ve kterých nemáme jinou možnost se připojit do sítě IPv6. Hlavním problémem Tereda je velmi špatný výkon v porovnání s ostatními přechodovými mechanizmy. Pokud vezmeme v potaz rozdíl mezi IPv4 a IPv6 na totožné síti, je hodnota klasického ping 6 ms, ale v IPv6 je to už 220 ms. [17] [27]

9.3 Translátory

Pokud máme zařízení podporující jen IPv4 a zařízení podporující jen IPv6, a chtěli bychom je zapojit do IPv6 sítě, musíme využít tzv. Translátory (Překladače). Translátory umožňují komunikovat mezi oběma sítěmi. [21] [27]

9.3.1 Stateless IP/ ICMP Translation (SIIT)

SIIT funguje pomocí bezstavového přístupu. U SIIT nedochází k uchovávání informací o datagramech. Ke každému datagramu přistupuje zcela individuálně, bez předchozí návaznosti o předešlém datagramu. V IPv6 síti se používají dva formáty adres mající IPv4 adresu: [26]

- IPv4 mapované adresy (IPv4 mapped address) – jsou využívány uzly, které podporují jen IPv4 protokol, formát adresy je: ffff:a.b.c.d, a.b.c.d tvoří adresu IPv4
- IPv4 překládané adresy (IPv4 translated address) – využívají je uzly pro IPv6 mající dočasnou a.b.c.d IPv4 adresu

Jestliže chceme překládat v opačném směru, musí si nejprve cílová zařízení v protokolu IPv6 zmapovat IPv4 adresu. SIIT jsou používány jen při překladu adres v podporovaném formátu. Rozšiřující možnosti (např.: další hlavičky, mobilita a atd.) jsou SIIT zahozeny. Využití v praxi je téměř nulové, avšak SIIT je základním kamenem pro další přechodové mechanizmy. [27]

9.3.2 Network Address Translation - Protocol Translation (NAT- PT)

Základ je tvořen SIIT. Díky jeho vylepšením je možná spolupráce mezi IPv4 a IPv6. Základ tvoří tedy pravidla SIIT, ale jako doplněk obsahuje mechanizmy poskytující mapování a překlady adres. Při používání NAT-PT musíme mít směrovač (překladač), který podporuje NAT-PT. Souvislé datagramy musí procházet stejným NAT-PT překladačem. [22] [27]

NAT-PT překladač pracuje tehdy, má-li prostor IPv4 adres. IPv4 adresy poté rozděluje jednotlivým IPv6 počítačům v dané síti. Přiděluje je buď staticky, nebo dynamicky. Pokud se jedná o statické přidělování, počítači je přidělena jedna a ta samá adresa. Jestliže jsou adresy přiděleny dynamicky, jsou přidělovány zcela náhodně podle dané situace. NAT-PT si zapisuje tzv. stavovou informaci. Stavová informace vypovídá o všech přidělených adresách. Je důležitá pro korektní zachovávání NAT-PT, protože musí po celou dobu dojít k zachování stejné mapové adresy. [11] [18] [27]

Pro správný chod NAT-PT překladače je ještě důležitý prefix. Prefix bude NAT-PT překladač přidělovat IPv4 adresám, které budou přicházet z vnějšího světa, při překládání

do IPv6. Prefix musí splňovat jednu podmínku - vyhrazení jen pro NAT-PT překladač. [27]

Máme dva kroky, které provádí NAT-PT při překládání. Jakmile dorazí IPv6 datagram, kdy cílová adresa má v počátku PrefiX, provede NAT-PT dva kroky: [27]

1. Při navázání spojení datagramu je přidělena odesílateli IPv4 adresy ze sady, kterou má k dispozici. Jakmile dojde k přidělení adresy, je informace o přidělení uložena. Pokud nastane situace, že datagram není první v pořadí v daném spojení, má uložené údaje o mapování jeho adres a jen je použije.
2. Dojde k převedení IPv6 datagramu na IPv4. Cílová adresa je získána z posledních 4 bajtů cíle původního datagramu. Odesílatel je dosazen IPv4 adresou, která se získá v předchozím kroku. Aby mohlo dojít k převodu, jsou využívány pravidla SIIT.

Při opačném převádění z IPv4 sítě je postup analogický. Dojde k převedení na IPv6 datagram. V tomto případě je cíl stanoven podle uložených údajů o mapování. Odesílatel je ve tvaru PrefiX::odesilatel_IPv4, a předá do IPv6 sítě. [27]

Aby mohlo dojít ke spojení v obou směrech, musí být povolen a zajištěn zásah do DNS. Podmínkou je umístění DNS serverů pro NATovanou síť v síti, kde informace procházejí skrz NAT-PT překladačem. [27]

9.3.3 NAT64

NAT64 je vylepšeným nástupcem NAT-PT. V NAT64 jsou vynechány operace s DNS, které byly velmi problematické. Aby se vyřešily tyto problémy, tak využívá dvou řešení - došlo k omezení služeb (spojení probíhá jen z IPv6 do IPv4) a označuje upravené DNS odpovědi (klienti potom se rozhodnou, jak s nimi naloží dále). [26]

Základ NAT64 je téměř totožné s NAT-TP (překladač s minimálně jedním rozhraním do IPv6 a IPv4 sítě). Překlad datagramů probíhá podle pravidel SIIT. Mapování adres je mezi oběma světy. Translátor je předurčen hlavně k tomu, aby koncové IPv6 síti zprostředkoval přístup k IPv4 službám nacházejících se v Internetu. [20] [27]

Prefix má délku 96 bitů. Tato hodnota je částí adresního prostoru, který byl určen správcem. Využívá se pro potřeby NAT64. Jako označení nese Prefix64::/96. Pokud se v síti vyskytuje více než jeden NAT64 překladač, ponese každý překladač svůj vlastní prefix. Za prefix se připíše adresa IPv4. [20] [27]

Směrovací tabulka odesílá datagramy do IPv4. Prefix64 je doručen až k překladači. Překladač přeloží datagram a pošle ho dále ven. Jestliže nastane situace, kdy přijde od odesílatele první datagram, zároveň překladač udělá mapování na IPv4 adresu. V tomto případě se uchovávají záznamy do té doby, dokud jsou potřebné. Počet IPv4 adres není neomezený, musí s nimi hodně šetřit. Ve většině případů může disponovat jen s jednou IPv4 adresou. [27]

9.3.4 DNS64

DNS64 je používán pro komunikaci počítačů v IPv4 Internetu.

Na začátku je AAAA dotaz, který pochází od stroje, zaslaného DNS serverem. Poté jsou dvě možnosti - buď dojde k předání v podobě původní anebo musí dojít k upravení. Při upravování DNS server zašle dotaz na záznam typu A. Tento A záznam je poté upraven na AAAA záznam. Adresu poté připojí a Prefix64::/96. Takto je provedena odpověď na DNS dotaz. Vše je doručeno NAT64 překladači, jehož práce je mapování klientovi adresy na IPv4. NAT64 provede překlad daného datagramu a postará se zároveň o jeho odeslání dále. [27]

Tzv. SAS (Status of Answer Section) slouží k označování odpovědí, které provádí DNS64. Výhodou je využití bezpečnostních prvků pro DNS i IP. [27]

Stane-li se, že máme kombinaci NAT64 a DNS64, nemůže dojít k připojení počítače z IPv4 sítě do IPv6. V tomto případě je nám povoleno jen mapování, které bylo vytvořeno ve směru opačném. Klienti využívající IPv4 tudíž nemohou využívat protokol IPv6. [26]

10 Konfigurace IPv6 na Cisco směrovači

V této kapitole se budu věnovat základním příkazům pro konfiguraci protokolu IPv6 na Cisco směrovačích. [4] [12]

Povolení protokolu IPv6 pro globální konfiguraci:

ipv6 unicast-routing

Pro konfiguraci linkové lokální adresy použijeme příkaz:

ipv6 enable

Přidání IPv6 adresy provedeme příkazem:

ipv6 address adresa/délka_prefixu
ipv6 address prefix/délka_prefixu eui-64

Druhým příkazem říkáme zařízení, aby použilo svoji vlastní MAC adresu a jejím doplněním získá identifikátor rozhraní. **(Todd Lamme- opraveno)**

Příkazy pro nakonfigurování tunelu u přechodového mechanizmu 6to4:

interface tunnel0 [1]
ipv6 address adresa/prefix [2]
tunnel source FastEthernet 0/0 [3]
tunnel mode ipv6ip 6to4 [4]

Příkazy pro nakonfigurování přechodového mechanizmu NAT-PT:

ipv6 nat [5]
ipv6 nat prefix prefix/délka [6]
ipv6 access-list natptACL [7]
permit ipv6 prefix/délka_prefixu any
ipv6 nat v6v4 pool název_poolu první_IPv4 poslední_IPv4 prefix-length délka_prefixu
ipv6 nat v6v4 source list natptACL pool název_poolu
ipv6 nat v6v4 source list natptACL interface rozhraní overload

[1] konfigurace tunelového rozhraní
[2] přiřazení IPv6 adresy na rozhraní
[3] zvolíme mód tunelu na 6to4
[4] udává typ rozhraní a číslo rozhraní tunelu
[5] zapnutí přechodového mechanizmu NAT
[6] nastavení prefixu u IPv4 rozhraní
[7] nastavení ACL

show ipv6 nat translations [8]
show ipv6 nat statistics [9]

Kontrola konfigurace IPv6:

show ipv6 interface [10]
show ipv6 interface brief [11]
show ipv6 route [12]
show ipv6 traffic [13]
show ipv6 tunnel [14]

[8] mapování NAT
[9] statistiky NAT
[10] zobrazení stavu rozhraní
[11] zobrazení souhrnného stavu rozhraní
[12] zobrazení směrovací tabulky IPv6
[13] zobrazení statistiky provozu IPv6
[14] zobrazení informací tunelu IPv6

Závěr

V mé bakalářské práci jsem uvedl celkový pohled na nový nastupující protokol IPv6. Tento protokol byl zaveden hlavně z důvodu nedostačující kapacity nynějšího protokolu IPv4. V praktické části ihned v počátečních kapitolách byly zmíněny výhody a nevýhody nového protokolu IPv6. Je patrné, že výhody jsou veliké a značně převyšují nevýhody, které jsou tedy zanedbatelné oproti problému, kterému nyní čelíme. Neustálý vývoj kupředu zlepšuje přechod na protokol IPv6 z IPv4 protokolu, který není zcela bezproblémový. Právě problémy s přechodem na nový protokol nejvíce zpomalují plné využívání IPv6. Proto v současné době využívají protokol IPv6 spíše klienti tam, kde je nativní podpora od poskytovatele. Běžní uživatelé stále fungují v IPv4 síti. Součástí bakalářské práce je tedy i popis přechodových mechanizmů, které umožňují komunikaci mezi protokoly IPv4 a IPv6. V práci jsou popsány jejich výhody, nevýhody a využití.

Návrhy konfigurací protokolu IPv6 byly vytvořeny v programu Cisco Packet Tracer za účelem podpoření výuky v Počítačových sítích a v kurzech Cisco Networking Academy. Náhled na vytvořené konfigurace je možné nalézt v přílohách A – D. Součástí výzkumné práce bylo testování přechodových mechanizmů. Byly vybrány dva přechodové mechanizmy – NAT-PT a Dual Stack (Dvojí zásobník). Volba těchto dvou přechodových mechanizmů byla z důvodu omezených možností programu Cisco Packet Tracer. Ostatní přechodové mechanizmy byly testovány v síťové laboratoři.

V příloze A je provedena automatická konfigurace protokolu IPv6. Příloha obsahuje náhled na vytvořenou síť pro tuto bakalářskou práci. Dále je v příloze popsána automatická konfigurace na jednotlivých směrovačích. V příloze B je ukázka DHCP konfigurace protokolu IPv6. Příloha opět obsahuje náhled na vytvořenou síť a ukázku konfigurace. V příloze C – D jsou testovány vybrané přechodové mechanizmy, které se využívají ke komunikaci mezi protokoly IPv4 a IPv6.

Dle mého názoru protokol IPv6 je nezbytný pro blízkou budoucnost. Jeho výhody jsou oproti protokolu IPv4 značné, především dostačující adresní prostor. Myslím si, že výhody, které tento protokol přináší, převažují nad nevýhodami. Mým názorem je, že by mělo dojít k rychlejší expanzi mezi běžnými uživateli a protokol by měl být postupně nahrazován. Největším problémem je v současné době nekompatibilita s jednotlivými zařízeními. Krokem vpřed by byla lepší propagace tohoto protokolu.

Literatura

[1] **ANTOŠ, David. 2008.** *Úvod do IPv6.* [online] 3. únor 2008. [cit. 2013-04-27]. Dostupné z www: <http://www.ics.muni.cz/bulletin/articles/572.html>.

[2] **BEIJNUM, Iljitsch. 2006.** *Running IPv6.* New York : Apress, 2006. ISBN 1-59059-527-0.

[3] **Border Gateway Protocol. 2013.** *Border Gateway Protocol.* [online] 23. Duben 2013. [cit. 2013-04-30].
Dostupné z www: <http://en.wikipedia.org/wiki/Border_Gateway_Protocol>.

[4] **BROWN, Sam et al. 2002.** *Configuring IPv6 for Cisco IOS.* USA : Syngress Publishing, 2002. ISBN 1-928994-84-9.

[5] **CRICKET, Liu. 2011.** *DNS and BIND on IPv6.* USA : O´Reilly, 2011. ISBN 978-1-449-30519-2.

[6] **DAVIES, Joseph. 2012.** *Understanding IPv6. USA :* Microsoft Press, 2012. ISBN 978-0-7356-5914-8.

[7] **DEERING, S.; HINDEN, R. 1998.** *RFC 2460 - Internet Protocol Version 6 (IPv6) Specification.* [online] December 1998. [cit. 2013-04-26]. Dostupné z WWW: <http://tools.ietf.org/html/rfc2460>.

[8] **DHCPv6. 2013.** *DHCPv6.* [online] 27. duben 2013. [cit. 2013-04-30]. Dostupné z www: <http://en.wikipedia.org/wiki/DHCPv6>.

[9] **Domain Name System. 2013.** *Domain Name System.* [online] 30. duben 2013. [cit. 2013-04-30]. Dostupné z www: < http://en.wikipedia.org/wiki/Domain_Name_System>.

[10] **DOSTÁLEK, Libor**, **KABELOVÁ, Alena. 2008.** *Velký průvodce protokoly TCP/IP a systémem DNS.* 5. vyd. Praha : Computer Press,a.s., 2008. ISBN 978-80-251-2236-5.

[11] **DUNMORE, Martin (Ed.). 2005.** *An IPv6 Deployment Guide.* [online] 2005. [cit. 2013-05-02]. Dostupné z WWW: <http://www.6net.org/book/deployment-guide.pdf>.

[12] **EMPSON, Scott. 2009.** *CCNA Kompletní přehled příkazů.* Brno : Computer Press, a.s., 2009. ISBN 978-80-251-2286-0.

[13] **HAGEN, Silvia. 2006.** *IPv6 Essentials.* USA : O´Reilly, 2006. ISBN 0-596-10058-2.

[14] **Interoperability between IPv6 and IPv4.** *Interoperability between IPv6 and IPv4.* [online]. [cit. 2013-04-30].
Dostupné z www: <http://ntrg.cs.tcd.ie/undergrad/4ba2.02/ipv6/interop.html>.

[15] **IPv6. 2012.** *IPv6.* [online] 14. září 2012. [cit. 2013-04-28]. Dostupné z www: <https://www.ipv6.cz/Hlavn%C3%AD_strana>.

[16] **IPv6. 2013.** *IPv6.* [online] 27. duben 2013. [cit. 2013-04-28]. Dostupné z www: <http://cs.wikipedia.org/wiki/IPv6#Vznik_IPv6>.

[17] **KRČMÁŘ, Petr. 2008.** *IPv6 přes NAT jedním příkazem: Technologie Teredo.* [online] 18. prosinec 2008. [cit. 2013-04-28]. Dostupné z www: <http://www.root.cz/clanky/ipv6-pres-nat-jednim-prikazem-technologie-teredo/>.

[18] **LAMMLE, Todd. 2010.** *CCNA Výukový průvodce přípravou na zkoušku 640-802.* Brno : Computer Press, a.s., 2010. ISBN 978-80-251-2359-1.

[19] **LOSHIN, Pete. 2004.** *IPv6 - theory, protocol and practice.* San Francisco : Elsevier, 2004. ISBN 1-55860-810-9.

[20] **McFARLAND, Shannon a kol. 2011.** *IPv6 Kompletní průvodce nasazením v podnikových sítích.* Brno : Computer Press, a.s., 2011. ISBN 978-80-251-3684-3.

[21] **NAT64 Technology: Connecting IPv6 and IPv4 Networks. 2012.** *NAT64 Technology: Connecting IPv6 and IPv4 Networks.* [online] duben 2012. [cit. 2013-04-30]. Dostupné z www: <http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-676278.html>.

[22] **ODOM, Wendell, HEALY, Rus, MEHTA, Naren. 2009.** *Směrování a přepínání sítí.* Brno : Computer Press, a.s., 2009. ISBN 978-80-251-2520-5.

[23] **POLESNÝ, David, ČERNOHOUZ, Petr. 2013.** *Běžte naproti IPv6, cest je hned několik.* [online] 29. březen 2013. [cit. 2013-04-28]. Dostupné z www: <http://www.zive.cz/clanky/bezte-naproti-ipv6-cest-je-hned-nekolik/sc-3-a-167763/default.aspx>.

[24] **ROHLEDER, David. 2011.** *Přechodové mechanismy k IPv6 (1).* [online] 3. únor 2011. [cit. 2013-04-27].
Dostupné z www: <http://www.ics.muni.cz/bulletin/articles/667.html>.

[25] **ROHLEDER, David. 2011.** *Přechodové mechanismy k IPv6 (2).* [online] 4. duben 2011. [cit. 2013-04-27].
Dostupné z www: <http://www.ics.muni.cz/bulletin/articles/671.html>.

[26] **SATRAPA, Pavel. 2008.** *Internetový protokol IPv6.* [online] 2008. [cit. 2013-04-26]. Dostupné z WWW: <http://knihy.nic.cz/files/nic/edice/pavel_satrapa_ipv6_2008.pdf>.

[27] **SATRAPA, Pavel. 2008.** *Internetový protokol IPv6.* Praha : CZ.NIC, z. s. p. o., 2008. ISBN 978-80-904248-0-7.

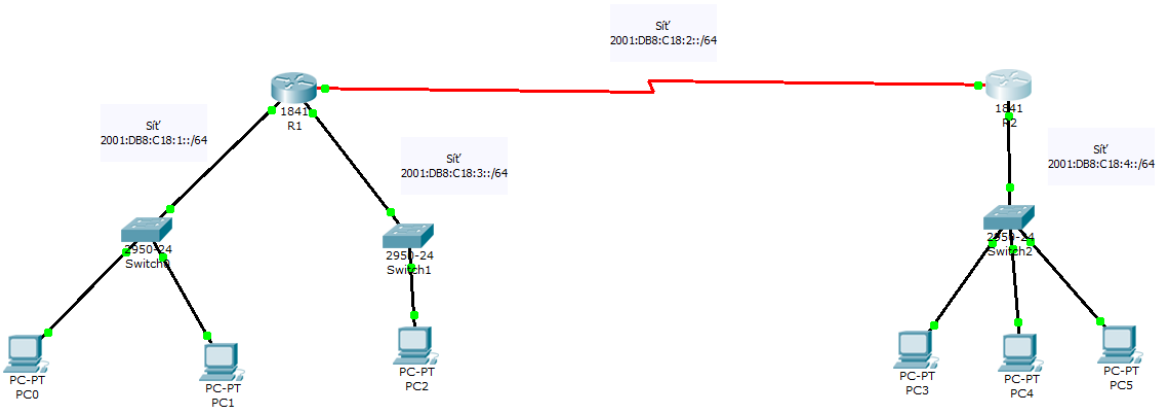
[28] **SATRAPA, Pavel. 2011.** *6to4 na šikmé ploše.* [online] 30. červen 2011. [cit. 2013-04-28]. Dostupné z www: <http://www.lupa.cz/clanky/6to4-na-sikme-plose/>.

[29] **VANGIE, Beal. 2011.** *What is The Difference Between IPv6 and IPv4?.* [online] 27. leden 2011. [cit. 2013-04-30]. Dostupné z www: <http://www.webopedia.com/DidYouKnow/Internet/ipv6_ipv4_difference.html>.

[30] **What is ICMPv6. 2008.** *What is ICMPv6?.* [online] 2008. [cit. 2013-04-28]. Dostupné z www: <http://www.ipv6.com/articles/general/ICMPv6.htm>.

[31] **YOUNGSONG, Mun, HYEWON, K. Lee. 2005.** *Understanding IPv6.* USA : Springer, 2005. ISBN 0-378-25429-3.

Příloha A – Automatická konfigurace



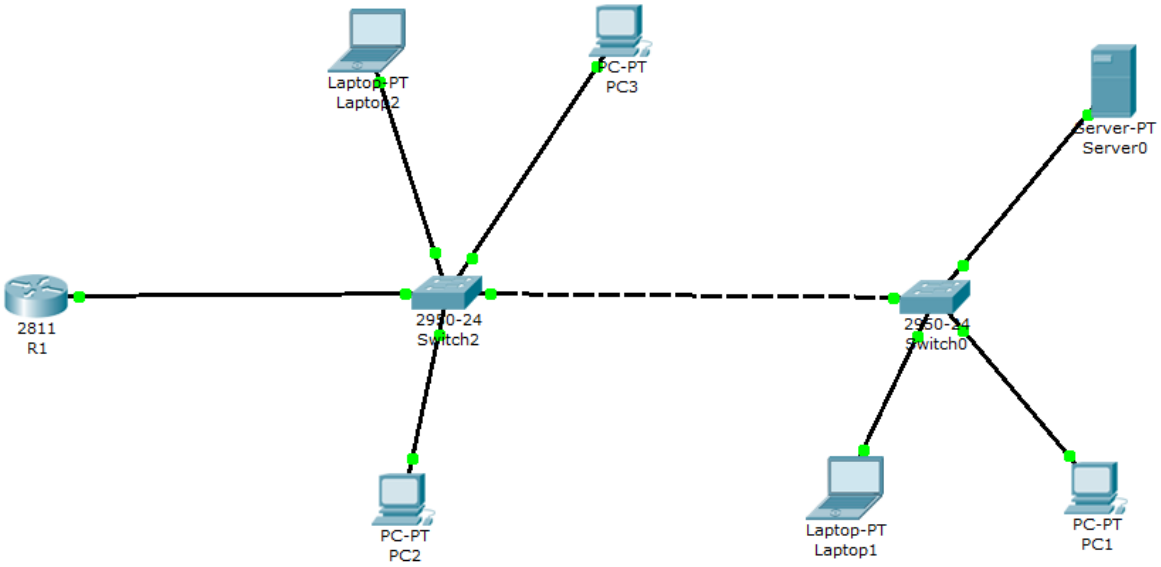
Router R1

```
!
hostname R1
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:C18:1::/64 eui-64
 ipv6 rip cisco enable
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:C18:3::/64 eui-64
 ipv6 rip cisco enable
 ipv6 enable
!
interface Serial0/0/0
 no ip address
 ipv6 address 2001:DB8:C18:2::/64 eui-64
 ipv6 rip cisco enable
 ipv6 enable
 clock rate 64000
!
ipv6 router rip cisco
!
```

Router R2

```
!
hostname R2
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:C18:4::/64 eui-64
 ipv6 rip cisco enable
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 ipv6 address 2001:DB8:C18:2::/64 eui-64
 ipv6 rip cisco enable
 ipv6 enable
!
ipv6 router rip cisco
!
```

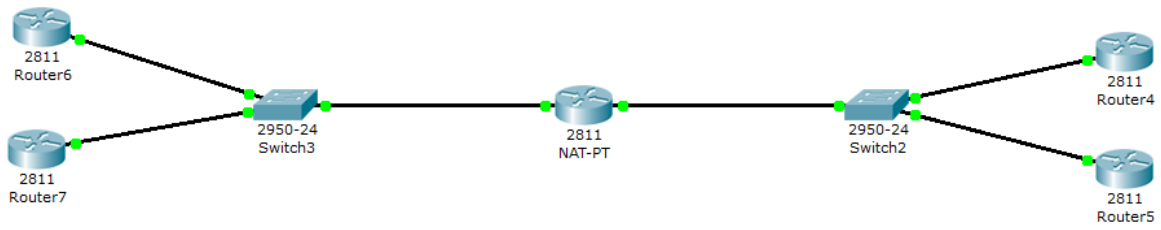
Příloha B – Konfigurace DHCPv6



Router R1

```
!
hostname R1
!
ipv6 unicast-routing
!
ipv6 dhcp pool cisco
 prefix-delegation pool cisco-prefix-new
 dns-server FE80::202:4AFF:FE1E:A045
 domain-name cisco.com
!
ipv6 local pool client-prefix-pool 2001:DB8:C18:1::/40 64
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:C18:1::/64 eui-64
 ipv6 dhcp server cisco
!
```

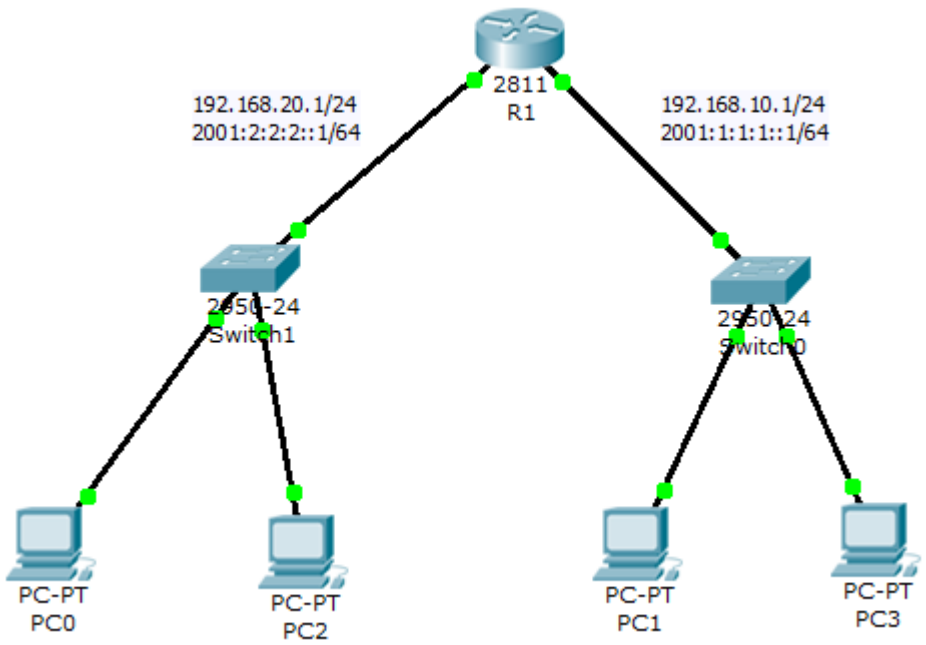
Příloha C – Přechodový mechanizmus NAT-PT



Router NAT – PT

```
!
hostname R1
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:ABCD::1/64
 ipv6 enable
 ipv6 nat
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 nat
!
interface Vlan1
 no ip address
 shutdown
!
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 redistribute static
!
ip classless
ip route 172.168.0.0 255.255.255.0 172.168.0.1
!
ipv6 nat v4v6 source 192.168.0.2 2001:12::2
ipv6 nat v4v6 source 192.168.0.3 2001:12::3
ipv6 nat v6v4 source 2001:ABCD::2 172.168.0.2
ipv6 nat v6v4 source 2001:ABCD::3 172.168.0.3
ipv6 nat prefix 2001:12::/96
!
```

Příloha D – Přechodový mechanizmus Dual Stack



Router R1

```
!
hostname R1
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:1:1:1::1/64
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:2:2:2::1/64
!
```