Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava 4

Protokol IPv6 a koexistencia s IPv4

Roman Panenka

Študijný program: Počítačové a komunikačné systémy a siete

Predmet: Komunikačné služby a siete

Ročník: Ing. 1.

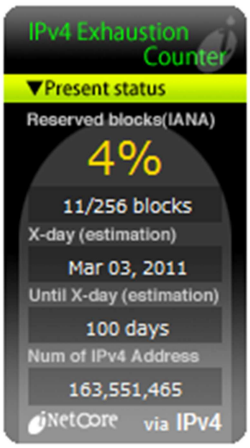
Akademický rok: 2010/2011

Obsah

1. Úvod do problematiky

Internet je verejne dostupný celosvetový systém vzájomne prepojených počítačových sietí. Pozostáva z tisícok menších komerčných, akademických, vládnych a vojenských sietí. Slúži ako prenosové médium pre rôzne informácie a služby ako napr. elektronická pošta, chat, WWW (World Wide Web). Dáta a komunikácia v Internete prebieha pomocou prepínania datagramov, a to hlavne za použitia štandardizovaného sieťového protokolu IP(Internet Protocol) vo verzii 4 a mnohých ďalších protokolov. V tomto protokole je každý uzol identifikovaný 32 bitovým číslom, tzv. IP adresou.

Prvé uzly tvoriace internet vznikli už v roku 1964 ako ARPANET, sieť vytvorená skupinou ARPA (Advanced Research Projects Agency) ministerstva obrany Spojených štátov Amerických. Pri vtedajšom návrhu sieťového protokolu IP sa nepočítalo s takým obrovským rozmachom tejto technológie, čo v súčasnosti spôsobuje míňanie rozsahu voľných verejných IP adries. Organizácia IANA1 vo svojej správe [1] predpovedá minutie adresného priestoru IPv4 na druhý kvartál roku 2011. Toto tvrdenie predstihuje vyobrazenie aktuálnej situácie adresného priestoru(pozri Obrázok 1), ktoré sa generuje na základe informácii IANA.



Obrázok 1 - odpočítavanie voľných IPv4 adries ku dňu 23.11.2010 [2]

Sieťový protokol verzie 6 (Internet Protocol version 6, IPv6) sa má stať nasledovníkom súčasného nosného protokolu celého internetu a má vyriešiť mnohé nedostatky protokolu verzie 4, a to hlavne výrazné rozšírenie adresného rozsahu na 128 bitov. V niektorých starších literatúrach býva tiež nazývaný ako *IP Next Generation* (IPng) [3] a postupne (no veľmi pomaly) sa začína vo svete nasadzovať.

[1] IANA (Internet Assigned Numbers Authority) je zodpovedná za globálnu koordináciu adresovania IP, správy koreňových DNS a ďalších internetových protokolov

2. Vlastnosti a prínos sieťového protokolu IPv6

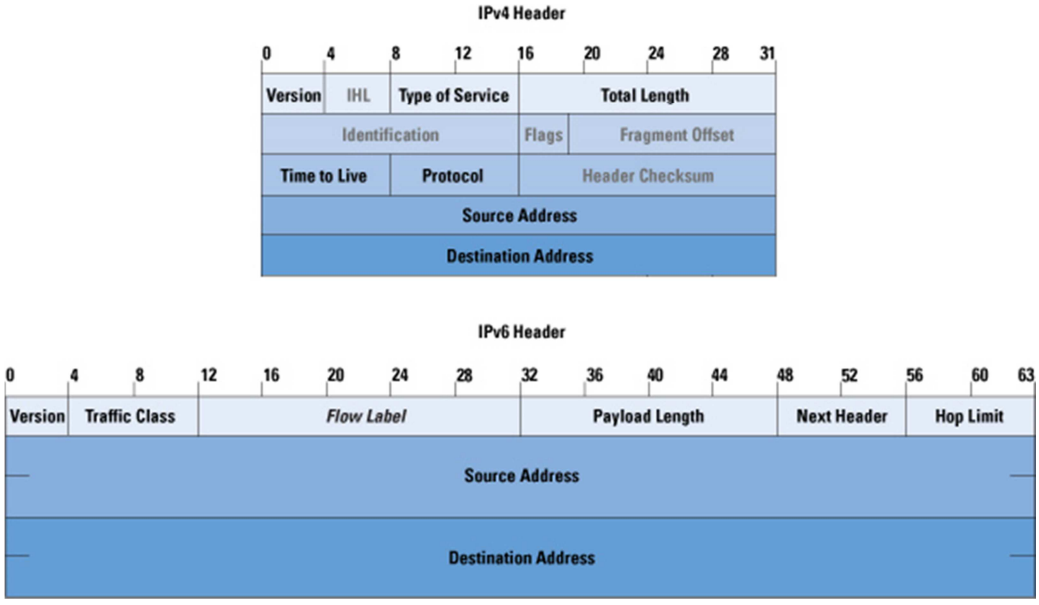
Ako už bolo spomenuté v úvode, sieťový protokol verzie 6 (IPv6) je nasledovník súčasného kmeňového protokolu celého internetu – IPv4. V priebehu 90 rokov dramaticky narástol počet používateľov internetu, ľudia a podniky začali používať nespočetné aplikácie založené na internete (video telefonovanie, hlasový prenos cez internet, kolaboračné nástroje, sociálne siete). To všetko spôsobuje rýchly úbytok IPv4 adries a otvára dvere tomuto novému internetovému protokolu

S novým obrovským (priam až nekonečným) rozsahom IPv6 adries sa predpokladá, že budú mať IP adresu všetky elektrické zariadenia. Nie len mobilné telefóny a autá, no vedci si predstavujú aj výrobu IP chladničiek, IP televízorov a pod. Veď nie je sa čo čudovať, keď v novom protokole IPv6 je rozsah pre 3.4×10^{38} (340 sextiliónov) adries. To je približne 4.3×10^{20} (430 triliónov) adries na štvorcový palec zemského povrchu [4].

2.1. Datagram v IPv6

Datagram v IPv6 má stále základný tvar, čiže začína hlavičkami, za ktorými nasledujú prenášané dáta. V porovnaní zo staršou verziou protokolu však došlo k výraznej zmene, keďže hlavička má konštantnú veľkosť. Hlavička IPv4 mala premenlivú dĺžku a jednotliví účastníci komunikácie mohli pripájať nepovinné voľby podľa potreby. IPv6 naproti tomu hlavičku minimalizovalo a obmedzilo len na najzákladnejšie polia. Všetky nepovinné, doplňujúce a rozširujúce údaje boli presunuté do rozširujúcich nepovinných hlavičiek.

Tvar základnej hlavičky a IPv4 a IPv6 vidieť na obrázku Obrázok 2. Napriek tomu, že sa zdrojové a cieľové adresy zväčšili štvornásobne, veľkosť celého datagramu vzrástla vďaka zjednodušeniu iba dvojnásobne.



Obrázok 2 - porovnanie datagramov protokolov IPv4 a IPv6 [zdroj: cisco.com]

Opis jednotlivých polí datagramu IPv6:

- *Verzia* (version, 4b) – zahájenie IP datagramu, identifikuje verziu protokolu
- *Trieda prenosu* (traffic class, 8b) – vyjadruje prioritu datagramu alebo jeho zaradenie do určitej prepravnej triedy. Umožňuje poskytovať služby zo zaručenou kvalitou.
- Značka toku (flow label, 20b) – umožňuje označovať prúd datagramov s rovnakými vlastnosťami, a tak uľahčuje smerovačom smerovanie týchto datagramov.
- Dĺžka dát (payload length, 16b) – nesie údaj o dĺžke dát datagramu, resp. počet bajtov nasledujúcich za štandardnou hlavičkou
- Ďalšia hlavička (next header, 8b) – nesie identifikáciu ďalších dát alebo rozširujúcej hlavičky za štandardnou hlavičkou
- Dosah (hop limit, 8b) – náhradník staršieho pola životnosť datagramu (TTL). Určuje koľko skokov môže datagram maximálne spraviť. Každý smerovač po ceste znižuje hodnotu o jedna.
- Zdrojová a cieľová adresa (Source address, destination address, 128b, 128b) – IP adresy komunikácie. Zaberajú najväčšiu časť celej hlavičky. Viac sa hlavičkám venujem v ďalšej kapitole 2.2 *Adresy v IPv6.*

2.2.Adresy v IPv6

Medzi hlavné prínosy IPv6 patria väčšie adresy. V porovnaní s IPv4 sa ich veľkosť zväčšila štvornásobne na 128 bitov a zmizli taktiež oznamovacie (broadcast) adresy. Vznikol ale nový typ správ – výberové, čiže stále existujú tri druhy adries:

- Individuálne (unicast) adresy – klasické adresy identifikujúce jedno sieťové rozhranie
- Skupinové (multicast) adresy – slúžia na adresovanie skupín zariadení, pričom musia byť dáta dopravené všetkým členom skupiny
- Výberové (anycast) adresy - slúžia tiež na adresovanie skupín zariadení, no dáta sú doručované iba jednému najbližšiemu členovi skupiny

IPv6 adresa sa zvyčajne zapisuje ako osem skupín po štyroch hexadecimálnych číslach:

0123:0000:0000:0000:fedc:ba98:4567:89ab

Keďže sú nové adresy o moc dlhšie, boli prijatých niekoľko pravidiel pre zjednodušenie zápisu adries. Ak skupina číslic obsahuje 0000, je možné túto skupinu vynechať. Ak sú výsledkom takéhoto zjednodušenia viac ako dve po sebe nasledujúce dvojbodky, je možné ich zredukovať na dve dvojbodky. Jedinou podmienkou je existencia len jednej skupiny takýchto dvojbodiek. Adresu vyššie môžeme teda skrátiť na niektoré z nasledujúcich adries:

0123:0:0:0:fedc:ba98:4567:89ab
0123:0:0::fedc:ba98:4567:89ab
0123::fedc:ba98:4567:89ab

Rozdelenie IP adries a vymedzenie špeciálnych adries je komplikovanejšie ako pri staršej verzií. Ako základné rozdelenie rozsahu adries sa dá považovať nasledujúce:

::/128	nedefinovaná adresa
::1/128	lokálna adresa (loopback)
fc00::/7	unikátne individuálne lokálne
fe80::/10	linkové individuálne lokálne
ff00::/8	skupinové adresy
ostatní	individuálne globálne

2.3.Prínosy IPv6 a opis vybraných technológií

Nový protokol IPv6 ponúka okrem väčšieho počtu IP adries aj mnoho ďalších zaujímavých výhod, ako napr.:

- jednotné adresné schéma pre Internet aj vnútorné siete
- tri druhy adries – unicast, multicast, anycast
- zvýšenie bezpečnosti komunikácie zahrnutím mechanizmov IPsec
- optimalizácia pre vysokorýchlostné smerovanie
- automatická konfigurácia siete
- podpora pre služby zo zaistenou kvalitou
- podpora mobility (pre prenosné počítače a mobilné zariadenia)
- hladký a plynulý prechod z IPv4

2.3.1. Objavovanie susedov (Neighbor discovery)

Jedným z dobre známych problémov počítačových sietí je zistenie linkovej adresy suseda aby s ním mohol na lokálnej sieti komunikovať. Protokol na objavovanie susedov (Neighbor Discovery Protocol, NDP) je balík nástrojov používaný IPv6 uzlami a koncovými stanicami práve na tento účel a na rôzne iné linkové operácie v počítačovej sieti. Najčastejšie sa používa pre vyhľadanie linkovej adresy k známej IPv6 adrese cieľového uzla.

Mnoho schopností objavovania susedov je podobných k mechanizmom v IPv4, kde sa za týmto účelom používali protokoly ARP a ICMPv4. Objavovanie susedov v IPv6 zo sebou prináša viacero nových funkcionalít, ako napr.:

- Vyhľadanie smerovačov v sieti (Router Discovery)
- Vyhľadanie prefixov a parametrov siete a ďalších údajov pre automatické overovanie dostupnosti susedov(Prefix Discovery and Parameter Discovery)
- Overenie dostupnosti suseda (Neighbor Unreachability Detection)
- Automatické nastavenie linkovej adresy(Address Autoconfiguration)

- Vyhľadanie linkovej adresy uzla v rovnakej sieti (Address Resolution)
- Určenie ďalšieho uzla v komunikácií (Next-Hop Determination)
- Detekcia duplicitných adries (Duplicate Address Detection)
- Presmerovanie komunikácie cez iný smerovač (Redirection)

Inverzné objavovanie susedov má presne opačný cieľ – rieši situáciu, keď počítač pozná linkovú adresu cieľového uzla, no nepozná jeho IPv6 adresu. V prostredí IPv4 sa na tento účel používa reverzný ARP protokol (RARP). Využitie má predovšetkým v sieťach typu frame-relay.

2.3.2. Mobilita

Podpora mobility sa opiera o základnú myšlienku, že aj pohyblivé - mobilné zariadenie je niekde doma. Existuje pre nich tzv. domáca sieť a v nej má zaregistrovanú svoju domácu adresu(home address).

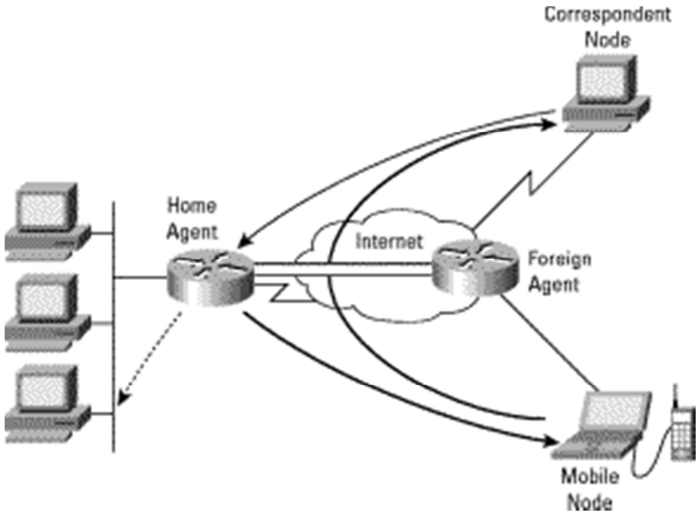
Domáca adresa zariadenia je nemenná a pod touto adresou je zariadenie uvedené aj v systéme DNS. Vďaka systému mobility je zariadenia dosiahnuteľné na tejto adrese aj keď sa nachádza mimo svojej domácej siete. Keď zariadenie vyrazí na cesty mimo domu, bude dostávať ďalšie tzv. dočasné adresy (care-of address, CoA), no pre ostatných bude stále zastihnuteľné aj na svojej domácej adrese.

Aby bol mobilný uzol (mobile node) zastihnuteľný všade pod svojou domácou adresou, musí mať vo svojej domácej sieti tzv. domáceho agenta (home agent). Domáci agent je väčšinou iba klasický smerovač v domácej sieti, ktorý spracováva všetky datagramy smerujúce k mobilnému uzlu a predáva mu ich vytvoreným tunelom. Keď mobilný uzol príjme tunelom datagram od domáceho agenta, dozvie sa z neho, že sa ho niekto pokúša zastihnúť na domácej adrese.

Mobilné IPv6 pripúšťa dva režimy, ktorými bude ďalej prebiehať komunikácia medzi mobilným uzlom a korešpondentom (correspondent node):

1. Celá komunikácia prebieha pomocou tunelov cez domáceho agenta. Korešpondent posiela dáta na domácu adresu, kde ich zbiera domáci agent a preposiela tunelom mobilnému uzlu. Ten vo svojich odpovediach používa ako odosielateľa svoju domácu adresu, predáva ich tunelom späť domácemu agentovi a ten ich preposiela korešpondentovi.
   Komunikácia je v tomto prípade veľmi neefektívna a navyše hrozí preťaženie domácej siete a domáceho agenta. Preto sa tento režim používa iba v prípade, kedy korešpondent nemá podporu pre mobilitu. Znázornenie takejto komunikácie možno pozorovať na obrázku Obrázok 3.

2. Celá komunikácia prebieha pomocou optimalizovanej cesty (mimo domáceho agenta). Ak má korešpondent podporu pre mobilitu v IPv6, prichádza k slovu optimalizácia cesty. Mobilný uzol zaháji optimalizáciu hneď po príchode prvého datagramu komunikácie. Cieľom optimalizácie je oboznámiť korešpondenta s aktuálnou dočasnou adresou mobilného uzla, aby bolo možné ďalšie dáta posielať priamo. K ohláseniu dočasnej adresy slúži voľba Aktualizácia väzby. Predtým ako ju odošle sa musí uzol najskôr kvôli bezpečnosti dokázať, že je ten, za ktorého sa vydáva.



Obrázok 3 - komunikácia uzlov v mobilite cez domáceho agenta

3. Porovnanie protokolov IPv6 a IPv4

3.1.História a vývoj IPv6

Hoci sa zdá, že IPv6 je záležitosťou posledných rokov, jeho korene siahajú až do začiatku deväťdesiatych rokov, kedy začalo byť zrejmé, že adresný priestor IPv4 sa rýchlo míňa.

Nakoľko na riešenie tohto problému bolo k dispozícií pomerne veľa času, rozhodlo sa IETF[2] navrhnúť zásadnejšiu zmenu na poly Internetu. Táto navrhovaná zmena okrem rozšíreného adresného priestoru prináša aj ďalšie nové vlastnosti, ktoré sme si rozobrali v kapitole 2 *Vlastnosti a prínos sieťového protokolu IPv6.*

Okrem iných problémov vyvíjaného IPv6 sa navyše protokolu IPv4 podarilo posilniť svoju pozíciu a obmedziť svoj hlavný nedostatok – nedostatok adries. Začali sa používať technológie ako beztriedne adresovanie (CIDR), sprísnili sa kritéria prideľovania sieťových adries a taktiež boli zavedené mechanizmy pre preklad adries (NAT).

Samotný vývoj a implementácia protokolu do reálneho sveta boli sprevádzané mnohými prekážkami a verejnými diskusiami pri vydaní každej novej RFC správy, čo spôsobovalo pomalý vývoj niektorých špecifikácii za jedinú možnosť budúcnosti internetu.

Protokolu IPv4 podarilo doimplementovať mnohé lákavé vlastnosti, s ktorými prišla predtým IPv6. Samozrejme nie tak isto elegantne a efektívne ale principiálne boli k dispozícií. IPv6 tým stratila svoju hlavnú „hnaciu silu", vývoj a nasadzovanie sa aj tak nezastavili, no spomalili.

Neznamenalo to však, že by sa mal vývoj zastaviť. Na vývoji IPv6 a jeho komponent sa začalo podieľať a stále podieľa celá rada pracovných skupín IETF. Protokol IPv6 si získal taktiež silnú politickú podporu. Veľmi aktívna je Ázia, ktorá ale do kolotoča IPv6 vstúpila neskoro. Dôsledkom toho začali mnohé krajiny (a hlavne Čína) pociťovať akútny nedostatok IPv4 adries. Priam ukážkové (ako obvykle na poly informačných technológií) je Japonsko. Vláda prišla s plnou podporou už v roku 2000 a následne ju uplatňovala v množstve projektoch alebo formou daňových úľav. V roku 2002 nasledovala Európska komisia a v roku 2005 Spojené štáty americké [3]. Mnohé štáty sa teda snažia posúvať rôznymi metódami rozvoj IPv6 dopredu, pretože vnímajú vyčerpanie IPv4 adries a jeho ďalšie nedostatky ako ohrozenie vlastného vývoja.

[2] IETF (Internet Engineering Task Force) - organizácia zodpovedná za vývoj a podporu väčšiny internetových protokolov a hlavne protokolov balíka TCP/IP

3.2.Výhody a nevýhody IPv6 oproti IPv4

IPv6 je stále neistou pôdou pre mnohé spoločnosti a okrem mnohých výhod nesie zo sebou aj viacero nevýhod, a preto sa mnohé organizácie snažili radšej pokračovať vo vývoji IPv4. Medzi tieto nevýhody bezpochyby patrí spätná nekompatibilita so staršími protokolmi. Z toho dôvodu bolo vymyslených mnoho protokolov a mechanizmov na prechod od starého protokolu na nový, ktorým sa budem v práci venovať v sekcií 4 Koexistencia s protokolom IPv4.

IPv6 sa potáca v bludnom kruhu, keďže používatelia nemajú oň záujem a pretože nie sú dostupné služby. A kto by prevádzkoval služby pod IPv6, keď tam nie sú používatelia? Štatistiky stále ukazujú objem IPv6 komunikácie v desatinách percenta [5]. V poslednej dobe je snaha prispieť k tejto problematike aj politicky. Každopádne, IPv6 je zaujímavý a nádejný protokol, mnohými považovaný

Z nesporných výhod IPv6 treba ale spomenúť nasledovné:

- ✓ Väčší adresný priestor (128 bitové adresy namiesto 32 bitových)
- ✓ Lepší formát hlavičky, pre efektívnejšie smerovanie
- ✓ Podpora rozširovanie protokolu
- ✓ Podpora pre označovanie komunikácie, ktorá má byť vybavovaná prednostne
- ✓ Bezpečnostné mechanizmy IPsec pre dosiahnutie integrity a hodnovernosti

4. Koexistencia s protokolom IPv4

Nasadenie novej verzie každého protokolu zo sebou prináša aj problém koexistencie zo staršou verziou. Niekoľko násobne viac to platí pri protokole IP, ktorý je hnacím motorom dnešného Internetu a lokálnych sietí. Navyše nie je nová, šiesta, verzia protokolu plne kompatibilná zo staršou verziou.

Pri súčasnej veľkosti Internetu sa teda nedá jednoducho vyhlásiť presný termín prechodu na nový protokol. Je potrebný dlhší časový úsek, v ktorom budú v súčasných sieťach koexistovať oba protokoly. Zo začiatku bude dominovať starší protokol, no postupne by malo dominanciu preberať novšia verzia protokolu. K úplnému prechodu ale pravdepodobne vôbec nedôjde. Vždy zostane totiž niekoľko sieťových ostrovčekov, ktoré budú fungovať aj na staršej verzií. S tým prichádza aj potreba nástrojov, ktoré túto medziprotokolovú komunikáciu umožňujú.

V súčasnosti existujú desiatky návrhov, ktoré sa snažia tento problém riešiť. Všeobecne ich môžeme rozdeliť do troch skupín:

- Mechanizmy s dvojitým zásobníkom
- Tunelovacie mechanizmy
- Prekladové mechanizmy

4.1.Dvojitý zásobník

Dvojitý zásobník, ako základný prekladový mechanizmus, je implementovaný priamo v operačnom systéme. V systéme sú implementované oboje verzie IPv4 a IPv6, pričom je umožnený prenos IPv6 datagramov cez nezmenenú IPv4 infraštruktúru [6].

Zásobníky pre adresy sú v systéme implementované buď oddelene alebo v tzv. hybridnej forme. To umožňuje vývojárom sieťových aplikácií písať kód transparentne pre oba protokoly. Ak majú oba uzly pridelenú IPv6 adresu tak komunikujú novým protokol, ak jeden z uzlov alebo obaja nedisponujú podporou pre IPv6, komunikácia prebieha po IPv4. Hybridné zásobníky reprezentujú IPv4 adresy v špeciálnom adresnom formáte IPv6 adresy (napr. ::ffff:192.168.1.2 reprezentuje IPv4 adresu 192.168.1.2).

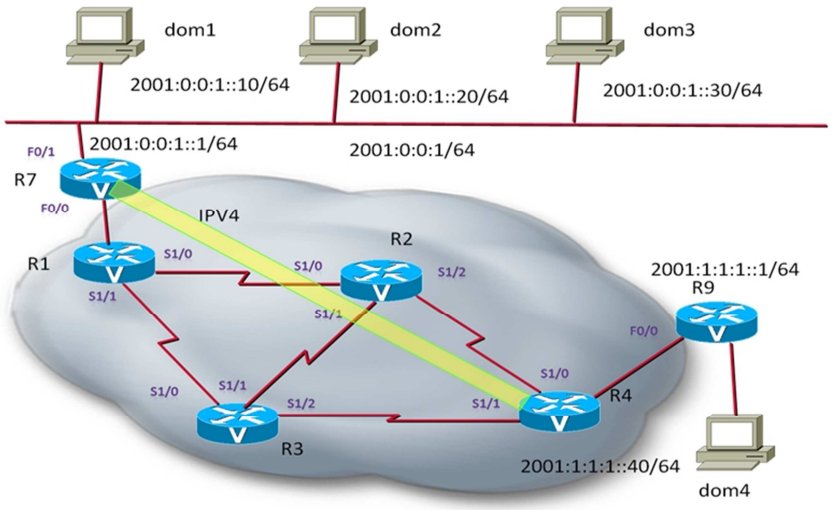
Kooperácia medzi oboma protokolmi sa teda odohráva až na aplikačnej vrstve. Daná aplikácia príjme dáta z jedného protokolu, upraví ich na základe vlastnej konfigurácie a svojich vlastností a odošle ich druhým protokolom von.

Dvojitý zásobník nepatrí práve k najlepším riešeniam kooperácie oboch protokolov, no, keďže k svojmu fungovaniu vyžaduje zachovanie IPv4, no na druhej strane slúži ako východisko pre ďalšie dva mechanizmy.

4.2.Tunelovacie mechanizmy

Tunelovanie je všeobecne známy spôsob ako prejsť nepriechodným terénom efektívne a rýchlo. Takisto to je v informačných technológiách a koexistencii dvoch rôznych protokolov. Pri IPv4 vs. 6 sa datagramy zabalia do datagramu druhého protokolu, ktorý je v sietí podporovaný, a to nám zabezpečí úspešný prenos viacprotokolovou infraštruktúrou.

Fungovanie IPv4 tunelu v IPv6 sieti znázorňuje obrázok Obrázok 4. Tunel má dva konce, pričom každý má svoju IPv6 adresu. Keď na základe smerovacej tabuľky a cieľovej adresy smerovač R4 zistí, že prijatý IPv4 datagram nemôže poslať priamo do IPv6 siete, ale do tunelu, zoberie ho a celý zabalí do novovytvoreného IPv6 datagramu. Cieľová adresa novovytvoreného datagramu je IPv6 adresa smerovača na druhej strane. Vnorený datagram je identifikovaný polom „Protokol obaľujúci IP diagram“ v hlavičke IPv6 datagramu.



Obrázok 4 - IPv4 tunel v IPv6 sieti

Datagram je ďalej normálne poslaný do IPv6 siete a prijatý na druhej strane tunela. Druhý smerovač zistí, že prijal tunelovaný datagram, rozbalí ho a ďalej spracováva podľa jeho smerovacích politík.

4.2.1. Konfigurovaný režim tunelovania

Prvý a základný režim tunelovania. Pri tomto spôsobe sú na daných zariadeniach predkonfigurované príkazy, ktoré funkcionalitu tunelovania vytvárajú. Na smerovači vznikne nové sieťové virtuálne rozhranie a v smerovacej tabuľke vznikne záznam pre smerovanie určených rámcov na toto rozhranie.

Konfigurované tunely sa najčastejšie používajú pri trvalých spojeniach sietí alebo IPv4 počítačov. Výborne poslúži pri experimentovaní s IPv6, no treba myslieť aj na to, že niektoré cesty v sieti nemusia byť optimálne a správa siete bude náročnejšia.

Pre zjednodušenie konfigurovania boli vytvorené tzv. tunel servery. Na tomto servery sa používateľ musí najskôr zaregistrovať prostredníctvom web stránky, robot následne vytvorí druhú stranu tunela a používateľovi pošle konfiguračný skript na jeho stanu tunela. Komunikáciu medzi používateľom a tunel serverom sprostredováva tzv. tunel broker, ktorý vyberá používateľovi najvhodnejší server. Komunikácia prebieha protokolom TSP (Tunnel Setup Protocol)

4.2.2. Automatický režim tunelovania

Automatické tunelovanie poskytuje kompromis medzi jednoduchým používaním automatizovaného tunelovania a determinizmom konfigurovaného režimu. Pre automatické nastavenie tunelovania vzniklo viacero známych mechanizmov:

6to4

Najrozšírenejší návrh automatického tunelovania definovaný v RFC 3056: *Connection of IPv6 Domains via IPv4 Clouds*. 6to4 tunely umožňujú komunikáciu izolovaných IPv6 sietí prostredníctvom automatických tunelov cez IPv4 sieť. V každej sieti, kde treba podporu 6to4, treba vymedziť jeden hraničný smerovač s IPv4 adresou, ktorý sa bude zúčastňovať na vytváraní tunelov do iných 6to4 sietí alebo natívnych IPv6 sietí [7].

6to4 poskytuje tieto tri funkcie:

- ✓ Priradenie IPv6 bloku adries počítačom alebo sieťam, ktoré majú globálnu IPv4 adresu
- ✓ Obaľovanie IPv6 datagramov do IPv4 pre prenos po IPv4 sieti použitím 6in4 (funkcionalita bola opísaná v sekcií 4.2)
- ✓ Smerovanie komunikácie medzi 6to4 a natívnymi IPv6 sieťami

Keď má 6to4 sieť fixnú globálnu IPv4 adresu, tak jej IPv6 prefix je taktiež fixný a nemenný. Takisto to nespôsobuje žiadne problémy pri zaraďovaní týchto adries do DNS. Jediný problém je iba s reverzným DNS a s delegáciou zodpovednosti za príslušnú časť doménového priestoru na prevádzkovateľa koncovej siete. Preto si musí vlastník IPv4 adresy delegovať doménu odpovedajúcu jeho 48 bitovému prefixu na https://6to4.nro.net [3].

ISATAP

Cieľom ISATAP protokolu je umožniť komunikáciu viacerých IPv6 uzlov, no na rozdiel od 6to4 v rámci jednej IPv4 siete. Práve preto je ideálnym doplnkom k 6to4 a spolu vytvárajú mocný mechanizmus na koexistenciu oboch protokolov. ISATAP protokol je definovaný v RFC 5214*: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*.

Komunikujúce počítače musia podporovať oba protokoly. Princíp je jednoduchý a podobný k mechanizmu 6over4. Podľa štandardnej tunelovacej procedúry je zabalený IPv6 datagram do IPv4, pričom IPv6 adresa v sebe obsahuje IPv4 adresu. Ďalej sa odošle na adresu získanú z cieľovej ISATAP adresy.

Keď teda chce poslať počítač datagram na adresu s ISATAP prefixom v rovnakej sieti, tuneluje ho priamo adresátovi. Pre ostatné datagramy použije pri rozhodovaní svoju smerovaciu tabuľky, čoho výsledkom je väčšinou poslanie datagramu (opäť tunelom) niektorému zo smerovačov.

ISATAP zavádza teda špeciálny formát lokálnej adresy, ktorá je vytvorená z 64 bitov prefixu siete, z 32 bitovej konštanty 0000:5efe a z IPv4 adresy sieťového rozhrania. Ak je IPv4 adresa 192.0.2.143 (c000028f v šestnástkovej sústave), tak potom bude IPv6 adresa rozhrania fe80::5efe:c000:28f.

Medzi nevýhody ISATAP patrí neschopnosť prenášania skupinových datagramov a jeho závislosť na protokole vyššej vrstvy - DNS, čo je proti zásadám návrhu sietí.

TEREDO

Veľmi nepríjemnou prekážkou okrem DNS je pre kopu tunelovacích protokolov aj NAT. NAT skrýva počítače vnútornej siete, skrýva ich IP adresu, poprípade port a navyše je často nastavený tak aby komunikácia mohla začať iba z vnútornej siete. S týmito problémami sa snaží vysporiadať mechanizmus TEREDO definovaný v RFC 4380: *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*.

Rovnako ako ISATAP je vhodný na sprostredkovanie IPv6 komunikácie uzlov v IPv4 sieti, no navyše dokáže do značnej miery prechádzať aj cez NAT, a preto je vhodný pre domáce siete zvyčajné skryte za NAT-om. Tato výhoda však spôsobuje nízku efektivitu protokolu.

Teredo používa komplikovaný formát adries. Prvá polovica adresy je určená TEREDO serverom a skladá sa z konštantného prefixu 2001::/32 a IPv4 adresou servera. Druha polovica je identifikátor rozhrania, začínajúci príznakmi U,G a C. Príznak C (Cone) sa nastavuje ak toto rozhranie za tzv. kornútovým NAT-om (cone NAT). Nasleduje číslo portu a IPv4 adresa rozhrania.

Aby mohol počítať v IPv4 sieti získať IPv6 adresu, musí prejsť nasledujúcou procedúrou:

1. Počítač pošle výzvu na adresu Teredo serveru, ktorú má buď predkonfigurovanú alebo si ju používateľ nastavil sám (v MS Windows je teredo.ipv6.microsoft.com). Vo svojom identifikátore rozhrania si nastaví príznak C.
2. Výzva prejde NAT-om z klientskej siete, pričom sa zmení zdrojová adresa a port

3. Server odpovie ohlásením smerovača, ku ktorému pripojí aj IPv4 adresu a port z výzvy, no toto ohlásenie pošle z inej IPv4 adresy.
4. Ak klientovi toto ohlásenie príde, znamená to, že je ho NAT je kornútový (Cone NAT), nastaví si identifikátor rozhrania a môže začať pracovať.
5. Pokiaľ mu ohlásenie ani po viacerých pokusoch nepríde, znamená to, že je ho NAT nie je kornútový (Cone NAT). Preto si vytvorí identifikátor rozhrania bez príznaku C a znova odošle výzvu na inú adresu TEREDO servera. Ak sa vráti ohlásenie z inou adresou, znamená to, že NAT je symetrický a Teredo sa nedá použiť. Ak dostane rovnaké údaje, NAT je obmedzený, no Teredo sa s ním dokáže vyrovnať.
6. Klient získal v posledných dvoch bodoch adresu, čím sa procedúra končí

4.3.Prekladové mechanizmy

Prekladové mechanizmy sa snažia sprostredkovať komunikáciu medzi IPv4 a IPv6 uzlami prekladaním datagramov z jedného typu na druhý (na rozdiel od tunelovacích mechanizmov).

SIIT

Stateless IP/ICMP Translation (SIIT) používa pri prekladaní datagramov tzv. bestavový prístup, čiže si neuchováva informácie o prechádzajúcich spojeniach a každý datagram prekladá úplne samostatne, bez akýchkoľvek návezností na predošlé datagramy. Je definovaný v RFC 2765: *Stateless IP/ICMP Translation Algorithm (SIIT).*

Tento prekladací uzol je zvyčajne smerovač a stojí na rozhraní medzi IPv4 a IPv6 sieťou. Problém vzájomnej identifikácie zdrojov rieši prideľovaním dočasných IPv4 adries. SIIT používa pre preklad jednotlivých hlavičiek medzi oboma protokolmi presné pravidlá. Tieto pravidlá sú bohužiaľ značne obmedzené, a preto musíme zabudnúť na rozširujúce hlavičky ako IPsec alebo mobilita. SIIT taktiež nerieši dôležitý problém, akým je väzba IPv6 a IPv4 adresami a odraz v DNS systéme.

NAT-PT

Network Address Translation – Protocol Translation (NAT-PT) je práve jedným z prístupov, ktorý využíva základné konvencie SIIT a doplňuje k ním chýbajúcu podporu pre rozširujúce hlavičky. Jeho hlavným cieľom je poskytnúť kompletnú podporu pre koexistenciu oboch protokolov a využiť pri tom skúsenosti s prekladačmi adries. Všetka komunikácia musí prechádzať smerovačom s podporou NAT-PT, ktorý býva spravidla prístupový smerovač pre danú IPv6 sieť.

NAT-PT používa pri prekladaní švindľovanie s DNS, ktoré je nutné pre nadviazanie spojenia dovnútra prekladanej IPv6 siete. Odpovede prichádzajúce z IPv4 siete sa menia na IPv6 a adresy v nich sa mapujú pomocou vyčleneného prefixu.

Hoci bol dlho považovaný za jeden z kľúčových prekladových algoritmov, no kvôli viacerým nedostatkom bol označený ako zastaraný mechanizmus v RFC 4966: *Reasons toMove the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status.* Toto rozhodnutie sa stretlo s vlnou odporu a podľa viacerých hovoril skôr o kvalite IETF ako o kvalitách NAT-PT. Navyše treba povedať, že za neho neexistuje rovnocenná náhrada [3].

TRT

Transport Relay Translator (TRT) sa snaží o podobnú vec ako NAT-PT, no tento krát o jednu vrstvu vyššie - na transportnej vrstve. Je definovaný v RFC 3142: *An IPv6-to-IPv4 Transport Relay Translator.*

TRT podobne ako NAT-PT vyžaduje vyčlenenie jedného IPv6 prefixu pre mapovanie IPv4 adries a taktiež dochádza k úpravám DNS. Keď chce počítač X6 v miestnej IPv6 sieti komunikovať zo vzdialeným strojom Y4 v IPv4 sieti, dostal od DNS servera adresu Y4 zmenenú na IPv4 adresu prefix:Y4. Žiadosť o doručenie je preto doručená TRT stroju, ktorý mu odpovie, naviaže s ním spojenie a predstiera, že je Y4.

Zároveň však otvorí cez IPv4 a TCP spojenie zo strojom Y4, pričom predstiera, že je X6. Medzi jedného spojenia teda vzniknú spojenie dve, pričom TRT zariadenie komunikáciu medzi nimi transparentne predáva [8]. Keďže je prenos dát rozpojený, nepoužívajú sa prekladové pravidlá SIIT, no dáta sa iba vybaľujú a preposielajú novým datagramom.

5. Bezpečnostné aspekty IPv6

Hoci bol internetový protokol verzie 4 vyvíjaný pôvodne pre armádu, je prekvapujúce, že neobsahuje žiadne bezpečnostné mechanizmy. Časom sa ukázalo, že tieto funkcionality v IPv4 naozaj chýbajú, a preto začali vznikať rôzne softvérové alebo hardvérové bezpečnostné mechanizmy v sieťach. Pri vývoji novej generácie protokolu sa na túto skutočnosť nezabudlo a preto vzniklo viacero bezpečnostných mechanizmov priamo na úrovni IP. Medzi hlavné novinky v IPv6 v oblasti bezpečnosti patria:

- ✓ Nutnosť implementácie IPsec (ESP + AH)
- ✓ Autentifikácia oddelená od šifrovania pre prípady, kde nie je šifrovanie povolené
- ✓ Protokoly pre výmenu kľúčov nezávislé na IP
- ✓ Automatická bezstavová konfigurácia
- ✓ Podpora pre verejné privátne siete
- ✓ Zabezpečenie smerovacích aktualizácií

5.1. Bezpečnostné prvky IPsec

Bezpečnostné prvky IPsec poskytujú používateľom autentifikáciu a šifrovanie komunikácie. Vďaka autentifikácii dokáže príjemca zistiť, či dáta poslal naozaj ten, kto je spomenutý ako zdroj a či neboli dáta počas prenosu niekým zmenené. Šifrovanie obsahu umožňuje jeho utajenie počas prenosu a ich rozšifrovanie môže spraviť iba príjemca. Na dosiahnutie tejto funkcionality existujú dve rozširujúce hlavičky, AH a ESP.

AH

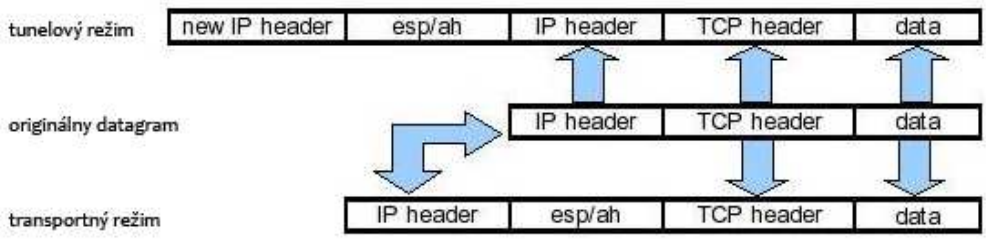
Autentifikačná hlavička (Authentication Header, AH) má na starosti autentifikáciu datagramu, čiže ako som už vyššie písal, overenie pravosti adries a obsahu.

ESP

Bezpečnostná hlavička ESP (Encapsulating Security Payload) zaisťuje podobné autentifikačné služby, no navyše dokáže obsah aj zašifrovať. Keďže dokáže poskytnúť rovnaké služby ako AH, bola podľa RFC 4301 určená povinná implementácia iba pre ESP, zatiaľ čo pre AH iba dobrovoľná [3].

Pre IPsec existujú dva režimy ochrany (znázornené tiež na obrázku Obrázok 5):

- ✓ *Transportný režim* – bezpečnostné hlavičky sa vkladajú priamo ako súčasť datagramu medzi jeho rozširujúce hlavičky
- ✓ *Tunelujúci režim* – pôvodný datagram je obalený do nového datagramu, ktorý obsahuje aj bezpečnostné hlavičky



Obrázok 5 - režimy ochrany v IPsec

5.2.Bezpečnosť koncových používateľov

Síce je v IPv6 na jednej strane zvýšená bezpečnosť siete implementáciou mechanizmov IPsec, no na druhej strane prinášajú ďalšie nové funkcionality IPv6 zo sebou nové bezpečnostné riziká. Často sa tiež stáva, že sa administrátori uspokoja iba zo základnou implementáciou IPv6, sú spokojní, že nový protokol funguje, no neuvedomujú si ďalšie vzniknuté riziká (ako napr. neprispôsobenie pravidiel bezpečnostných brán aj pre nový protokol).

Nové otázky v oblasti bezpečnosti koncových sietí sa vyskytujú pri protokole ICMPv6, ktorý nemôžeme len tak jednoducho celý v sieti zablokovať ako to bolo pri ICMPv4, kedy sa zabezpečilo, že sa ICMP nezneužíva na zahlcovanie siete, falšovanie správ, skenovanie siete alebo pašovanie informácii von zo siete. Verzia 6 totiž k svojej plnej funkcionalite potrebuje viacero nových mechanizmov ako objavovanie susedov, autokonfigurácia, mobilita a pod.

Implementácia IPsec a reťazenie IP hlavičiek značne skomplikovali život bezpečnostným bránam (firewallom). Napr. bezpečnostná hlavička ESP spôsobuje, že bezpečnostná brána nevie o pôvodnom datagrame dôležité informácie ako zdroj a cieľ komunikácie, porty komunikácie a pod, a preto nedokáže komunikáciu dostatočne filtrovať. Taktiež v prípade kedy bezpečnostná brána nájde neznámu rozširujúcu hlavičku, bude ťažké určiť, či komunikáciu filtrovať alebo nie.

Načrtnuté problémy si vynútia posun vo vnímaní bezpečnosti lokálnych sietí. Na upokojenie musím však dodať, že už v súčasnosti sa tejto problematiky venuje viacero mechanizmov, odporúčaní a RFC dokumentov na posilnenie komplexnej bezpečnosti IPv6 sietí.

6. Záver

6.1.Zhodnotenie problematiky

Protokol novej generácie IP – IPv6 je jediným rozumným východiskom súčasných problémov spájajúcich sa s IPv4 (nedostatočný adresný priestor, slabá podpora bezpečnosti a pod.). Okrem 4-násobne väčšieho adresného priestoru prichádza viacerými novinkami, ktoré sa prispôsobili súčasným požiadavkám koncových používateľov a súčasným bezpečnostným potrebám. Výhodám a prínosom protokolu IPv6 sa venujem v kapitole 2- *Vlastnosti a prínos sieťového protokolu IPv6.*

História vývoja IPv6 bola sprevádzaná mnohými komplikáciami a negatívnymi ohlasmi odporcov nového protokolu. Väčšina avizovaných nedostatkov bolo vyriešených radov RFC a niektoré sú stále v stave riešenia. Tejto problematike som venoval kapitolu 3 - Porovnanie protokolov IPv6 a IPv4

Keďže prechod medzi protokolmi takejto veľkosti nemôže byť vykonaný za pár dní, existuje reálna požiadavka na podporné mechanizmy pre koexistenciu a vzájomnú komunikáciu IPv4 a IPv6 sietí. Preto vzniklo množstvo prechodových mechanizmov, ktoré túto funkcionality zabezpečujú. Myslím, že problém koexistencie protokolov je vyriešený a administrátori majú na výber viacero alternatív. Jediné problémy môžu stále vznikať pri používaní špeciálnych rozširujúcich hlavičiek v IPv6. Celkovo sa tejto problematike venujem v kapitole 4 - *Koexistencia s protokolom IPv4*

Bezpečnosť v IPv6 bola umocnené povinnou implementáciou bezpečnostných mechanizmov IPsec. To zaručuje autentifikáciu a šifrovanie komunikácie. Na druhej strane protokol IPv6 zo sebou priniesol mnoho otázok a zmien v súčasnom vnímaní bezpečnosti. Techniky zabezpečenia musia byť pri implementácií nového protokolu prehodnotené, no už v súčasnosti existuje množstvo návrhových vzorov a dokumentov RFC. Bezpečnostným aspektov v novom protokole sa venujem v kapitole 5 - *Bezpečnostné aspekty IPv6.*

IPv6 siete sa začínajú, čím ďalej tým viac nasadzovať do reálnych sieti, dokonca často aj s podporou vlády danej krajiny. IPv6Forum vydalo viacero certifikačných testov, ktoré overujú, či nové siete odpovedajú štandardom protokolu IPv6. Tieto testy sú na rôznych úrovniach náročnosti a komplexnosti a sú znázornené na obrázku Obrázok 6.

Obrázok 6 - IPv6 Ready Logo

6.2.Zhodnotenie časového plánu práce

Pred začatím vypracovávanie práce som zanalyzoval zložitosť jednotlivých častí a prihliadajúc na povinné termíny prezentácií práce som vypracoval nasledovný časový plán:

1. – 3. týždeň:	Analýza a špecifikácia cieľovej témy
4. týždeň:	Prezentácia analýzy a výslednej špecifikácie
5. týždeň:	Opis vlastností IPv6 a porovnanie s IPv4
6. – 7. týždeň:	Rozpracovanie koexistencie s IPv4
8. týždeň:	Rozpracovanie bezpečnostných aspektov IPv6
9. týždeň:	Prezentácia stavu riešenia
10. týždeň:	Dopracovanie pripomienok, finalizácia dokumentu
11. – 12. týždeň:	Odovzdanie výslednej dokumentácie a prezentovanie projektu

Po vypracovaní kompletného dokumentu zhodnocujem plnenie svojho plánu za úspešné. Všetky predpokladané termíny sa mi podarilo splniť, okrem rozpracovania bezpečnostných aspektov IPv6, ktoré som musel presunúť do 10. týždňa.

6.3.Zoznam použitej literatúry

[1]**Vegoda, Leo.** *Why IPv6 Support by Domain Registrars is important.* [Online] [Dátum: 12. 10 2010.] www.iana.org.

[2]**Takashi Arano, Intec NetCore.** IPv4 Address Report. [Online] http://www.potaroo.net/tools/ipv4/index.html.

[3]**Satrapa, Pavel.** *IPv6.* Praha : CZ.NIC, 2008.

[4]**Odom, Wendell.** *CCNP Route 642-902 Official Certification Guide.* Indianapolis : Cisco Press, 2010.

[5]**Huston, Geoff.** Presentations about IPv6 perspective. [Online] 12. 10 2010. http://www.potaroo.net/presentations/.

[6]**RFC:4213.** Basic Transition Mechanisms for IPv6 Hosts and Routers. [Online] http://tools.ietf.org/html/rfc4213.

[7]**Oracle.** *SystemAdministrationGuide: IP Services.* september 2010. 816–4554–21.

[8]I**pv6.cz.** Transport Relay Translator . [Online] https://www.ipv6.cz/TRT.

[9]**Donahue, Gary A.** *Kompletní prúvodce sítového experta.* Brno : Computer Press, a.s., 2009.

[10]**Libor Dostálek, Alena Kabelová.** *Velký průvodce protokoly TCP/IP a systémem DNS.* Praha : Computer Press, 2000.

[11]**Lioy, Antonio.** Security Features of IPv6. [Online] december 2010. www.cu.ipv6tf.org/literatura/chap8.pdf.