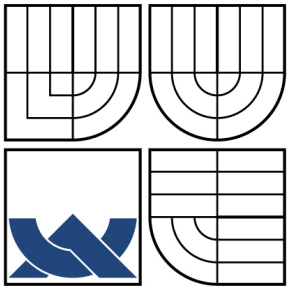
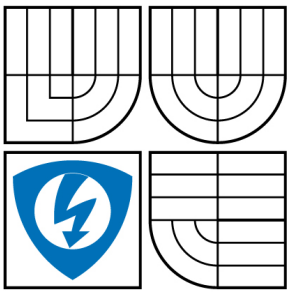


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

VLASTNOSTI A POUŽITÍ PROTOKOLŮ IPV6 A MIPV6

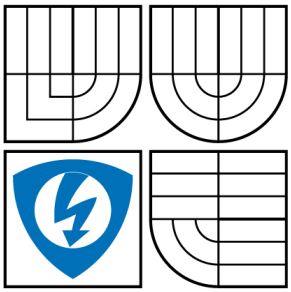
FEATURES AND USE OF IPV6 AND MIPV6 PROTOCOLS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — PETER SULÍK
AUTHOR

VEDOUCÍ PRÁCE — Ing. MICHAL SKOŘEPA
SUPERVISOR

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Sulík Peter	***ID:***	78325
Ročník:	3	***Akademický rok:***	2007/2008

NÁZEV TÉMATU:

Vlastnosti a použití protokolů IPv6 a MIPv6

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou Internet Protokolu verze 6. Podrobně porovnejte tento protokol s Internet Protokolem verze 4. Popište, jak probíhá implementace protokolu IPv6 a jaké jsou jeho výhody či nevýhody při praktickém využití. Prostudujte problematiku mobility v sítích s IPv6 (protokole MIPv6). V simulačním prostředí OPNET Modeler vytvořte model síťové infrastruktury, která demonstruje funkce protokolu MIPv6. Na výsledcích simulací ukažte, jakou výhodu přináší protokol MIPv6 s funkcí optimalizace cesty oproti protokolu MIPv6 bez této funkce. V případě dostupnosti vhodného zařízení proveďte implementaci protokolu IPv6, resp. MIPv6 v laboratorní síti.

DOPORUČENÁ LITERATURA:

[1] SATRAPA, Pavel. IPv6 - Internet Protokol verze 6, Praha : Neocortex, 2002 -- 238 s. : ISBN: 80-86330-10-9

[2] RAAB, Stefan. Cisco: Mobilní IP technologie a aplikace, Grada, 2007, 299 s., ISBN: 978-80-247-1611-4

[3] OPNET Technologies, Inc OPNET Modeler Release 12 Product documentation, 2006

Termín zadání:	11.2.2008	***Termín odevzdání:***	4.6.2008

Vedoucí práce: Ing. Michal Skořepa

prof. Ing. Kamil Vrba, CSc.
předseda oborové rady

UPOZORNĚNÍ:

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Peter Sulík

Bytem: Javornícka 9, 97411, Banská Bystrica

Narozen/a (datum a místo): 23.12.1985, Banská Bystrica

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

se sídlem Údolní 244/53, 602 00, Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

prof. Ing. Kamil Vrba, CSc

(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - □ disertační práce
   - □ diplomová práce
   - □ bakalářská práce
   - □ jiná práce, jejíž druh je specifikován jako .....

   (dále jen VŠKP nebo dílo)

Název VŠKP: Vlastnosti a použití protokolů IPv6 a MIPv6

Vedoucí/ školitel VŠKP: Ing. Michal Skořepa

Ústav: Ústav Telekomunikací

Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v*:

- □ tištěné formě – počet exemplářů ……..
- □ elektronické formě – počet exemplářů ……..

* hodící se zaškrtněte

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - □ ihned po uzavření této smlouvy
   - □ 1 rok po uzavření této smlouvy
   - □ 3 roky po uzavření této smlouvy
   - □ 5 let po uzavření této smlouvy
   - □ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: …….

…….. ……
Nabyvatel Autor

ABSTRAKT

Práca pojednáva o problematike protokolu IPv6 a o podpore mobility v tomto protokole. V prvej časti sú popísané vlastnosti protokolu IPv6 a rozdiely oproti protokolu IPv4. V druhej časti je podrobne popísaný protokol MIPv6 a hlavne jeho výhody u použitia v bezdrôtových sieťach. Väčšina priestoru je pritom venovaná problematike smerovacích mechanizmov Obojsmerné tunelovanie a Optimalizácia cesty. Následne sú v programe OPNET Modeler nasimulované siete demonštrujúce vlastnosti MIPv6 protokolu. Na záver sú zhodnotené výsledky simulácií a výhody aké prináša smerovanie v sieťach s parametrom Optimalizácia cesty.

Kľúčové slová: IPv6, MIPv6, Obojsmerné tunelovanie, Optimalizácia cesty, OPNET Modeler

ABSTRACT

The thesis deals with IPv6 protocol problematic and with mobility support in this protocol. In the first part are described basic IPv6 attributes and differences compared to IPv4 protocol. In the second part, the MIPv6 protocol is described in detail and mainly the advantages in wireless networks usage. Most of the part is dedicated to routing mechanism problematic of Bidirectional tunneling and Route Optimisation. Thereafter, networks are simulated in OPNET Modeler software to demonstrate the attributes of MIPv6 protocol. In conclusion, the simulations results are evaluated and also advantages of Route Optimization routing in networks.

Key words: IPv6, MIPv6, Bidirectional Tunneling, Route Optimization, OPNET Modeler

Prehlásenie

Prehlasujem, že svoju bakalársku prácu na tému *Vlastnosti a použitie protokolov IPv6 a MIPv6* som vypracoval samostatne pod vedením vedúceho bakalárskej práce a s použitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej prehlasujem, že v súvislosti s vytvorením tohto projektu som neporušil autorské práva tretích osôb, najmä som však nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a som si plne vedomý následkov porušenia ustanovení §11 a nasledujúcich autorského zákona č.121/200Sb., vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovení § 152 trestného zákona č 140/1961 Sb.

V Brne dňa 3.6.2008. .....

Poďakovanie

Ďakujem vedúcemu bakalárskej práce Ing. Michalovi Skořepovi za veľmi užitočnú metodickú pomoc a cenné rady pri spracovaní bakalárskej práce.

V Brne dňa ....
(podpis autora)

Zoznam skratiek

AC	Access Category
AP	Acces point – Prístupový bod
AR	Access Routek – Prístupový smerovač
ARP	Address Resolution Protocol
BT	Bidirectional Tunneling – Obojsmerné tunelovanie
CN	Correspondent Node – Korešpondujúci uzol
CoA	Care-of-Address
CoT	Care of Test
CoTI	Care of Test Init
ESP	Encrypted Security Payload
EUI	Extended Unique Identifier
FTP	File Transfer Protokol
HA	Home Agent – Domáci Agent
HoT	Home Test
HoTI	Home Test Init
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IGMP	Internet Group Managment Protocol
IP	Internet Protokol – Internetový protokol
IPsec	Internet Protocol Security
IPv4	Internet Protokol version 4 – Internetový protokol verzia 4
IPv6	Internet Protokol version 6 – Internetový protokol verzia 6
LAN	Lokal Area Network
LSB	Least Significiant Bit
MIPv6	Mobile IPv6
MLD	Multicast Listener Discovery
MN	Mobile Node – Mobilný uzol
MTU	Maximum Transmission Unit

MSB	Most Significiant Bit
ND	Neighbour Discovery
OM	OPNET Modeler
PPP	Point-to-Point
RO	Route Optimization – Optimalizácia cesty
RR	Return Routability
TCP	Transmision Control Protokol - Kontrolný prenosový protokol
TTL	Time-to-Live
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WLAN	Wireless Lan

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

1. ÚVOD

Ľudia v dnešnom svete žijú v informačnej dobe. Realita je taká, že na výmenu informácií medzi sebou nepotrebujú viac ako koncové zariadenie s pripojením na Internet. Celú komunikáciu riadi súbor pravidiel (protokolov), o ktorých bežný človek väčšinou nemá hlbšie znalosti.

Cieľom mojej bakalárskej práce „Vlastnosti a použitie protokolov IPv6 a MIPv6“ je oboznámiť sa s vlastnosťami IPv6 protokolu a porovnať ich so súčasným protokolom IPv4. V kapitole 2 hovorím o zmenách v hlavičke IPv6 paketov ako aj o systéme rozširujúcich hlavičiek, ako novej vlastnosti protokolu IPv6. V časti 3. hovorím o novom type internetových adries a o ich formáte zápisu. V tabuľkách a na niekoľkých obrázkoch som snažil poukázať na vlastnosti protokolu IPv6 resp. rozdiely voči IPv4. V ďalších kapitolách stručne popisujem nové vlastnosti IP protokolu a to spôsob riadenia prenosu, ako aj bezpečnosť IPv6 protokolu a jeho mobilitu. Tieto vlastnosti som popísal z dôvodu ich prínosov pre implementáciu IPv6. V predposlednej kapitole popisujem podporu mobility v protokole IPv6, konkrétne protokol MIPv6. Zameral som sa hlavne na mechanizmy smerovania v mobilných MIPv6 sieťach a na mechanizmy zabezpečenia komunikácie.

V rámci bakalárskej práce som navrhol v programe OPNET Modeler topológiu siete, ktorá podporuje protokol MIPv6 za účelom demonštrácie výhod smerovacieho mechanizmu Optimalizácia cesty.

1.1 Protokol IP next generation – IPv6.

Začiatkom 90-tych rokov sa začalo uvažovať o problémoch protokolu IPv4 súvisiacich s obmedzenosťou a vyčerpaním adresného priestoru, jeho technickými nedostatkami z pohľadu celkového vývoja IT. Úsilie smerovalo do vzniku nového protokolu - protokolu novej generácie (IPng - IP next generation) s predpokladom odstránenia problémov IPv4. Výsledkom je protokol IPv6 z konca 90-tych rokov.

Medzi hlavné rozdiely protokolu IPv6 oproti protokolu IPv4 patria:

- Zväčšený rozsah IP adresného priestoru. IPv4 používa pre adresný priestor 32 bitov (4 miliardy adries), zatiaľ čo IPv6 128 bitov (~ 3,4 * 10^38 adries).
- Lepšia autokonfigurácia. V IPv6 je vyžadovaná bezstavová autokonfigurácia.
- Bezpečnosť. Špecifikácia protokolu IPv6 vyžaduje podporu IPSec.
- Lepšia mobilita. IPv6 má lepšiu podporu pre ad-hoc networking.

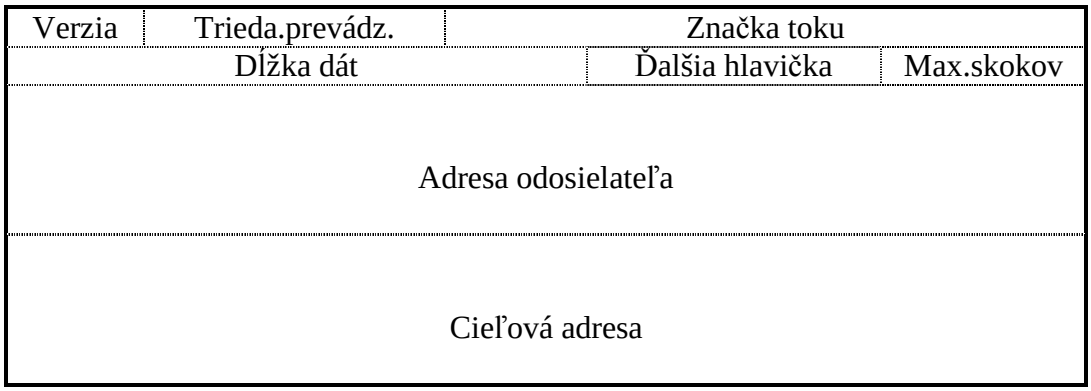
IPv4	**IPv6**
Zdrojová a cieľová adresa má dĺžku 32 bitov (4 byty).	Zdrojová a cieľová adresa má dĺžku 128 bitov (16 bytov).
Podpora IPsec je voliteľná.	Podpora IPsec je vyžadovaná.
Smerovač aj odosielateľ vykonávajú fragmentáciu.	Fragmentáciu vykonáva len odosielateľ.
Hlavička obsahuje kontrolný súčet.	Hlavička neobsahuje kontrolný súčet.
Hlavička obsahuje voľby.	Všetky rozširujúce dáta sú prenesené do rozširujúcich hlavičiek.
Address Resolution Protocol (ARP) používa všesmserové rámce ARP Request na priradenie IPv4 adresy ku MAC adrese.	Rámce ARP Request sú nahradené skupinovými správami Výzva susedovi.

Internet Group Management Protocol (IGMP) je používaný na riadenie skupinového členstva v lokálnych podsietiach.	IGMP je nahradený Multicast Listener Discovery (MLD) správami.
ICMP Objavovanie Smerovača (Router Discovery) je používaný na zistenie IPv4 adresy najvhodnejšej predvolenej brány. Je voliteľný.	ICMP Objavovanie Smerovača (Router Discovery) je nahradený ICMPv6 správami Výzva smerovaču a Ohlásenie smerovača. Je vyžadovaný.
Všesmerové adresy sú používané a na rozposielanie paketov všetkým uzlom v sieti.	V IPv6 neexistujú žiadne všesmerové adresy. Namiesto nich sú používane lokálne linkové skupinové adresy s dosahom na všetky uzly..
IPv4 musí byť nakonfigurované buď manuálne alebo pomocou DHCP.	Nevyžaduje DHCP ani manuálnu konfiguráciu.
Musí podporovať veľkosť paketu 576 bytov (s možnou fragmentáciou).	Musí podporvať veľkosť paketu 1280 bytov (bez fragmentácie).

Tab. 1.1: Základné porovnanie IPv4 a IPv6

2. Hlavička datagramu

Formát paketu IPv6 protokolu oproti IPv4 nedosiahol žiadne zmeny, ma klasický tvar. Skladá sa z hlavičky za ktorou nasledujú nesené dáta. Zmenená však bol samostatný prístup k tvoreniu hlavičky. V minulosti bola dĺžka hlavičky premenlivá a každý účastník komunikácie mohol pripájať ďalšie nepovinné časti. V každej takejto hlavičke bol kontrolný súčet , ktorý bolo treba vždy prepočítať na každom smerovači. Hlavička IPv6 má naproti tomu konštantnú dĺžku. Väčšina prvkov bola odstránená ostali len tie najnutnejšie. Ostatné prvky ktoré boli nepovinné či doplňujúce boli presunuté do systému nadväzujúcich hlavičiek, ktoré sa do paketu pridávajú len podľa potreby. Aj keď sa dĺžka adries zväčšila celkovo až štvornásobne, hlavička sa zväčšila len dvojnásobne. Z pôvodných 20 bajtov na 40 bajtov z toho 32 bajtov tvorí adresa cieľová a zdrojová.



Obr.2.1: IPv6 hlavička

Verzia - Časť verzia je začiatkom datagramu a obsahuje číslo verzie protokolu. U nás bude niesť hodnotu 6.

Trieda prevádzky - Má podobný význam ako položka Type of Service v datagrame IPv4. Pomocou tejto položky môže kedykoľvek na ceste ku adresátovi smerovač označiť a špeciálne spracovať datagram. Praktické využitie Type of Service je napríklad u hlasovej či obrazovej služby. Datagramy hlasu či obrazu sú citlivé na oneskorenie a využitím tohto poľa im užívateľ môže priradiť vyššiu prioritu nad ostatnými paketmi a na ceste sú takéto pakety pri zpracovaní uprednostované.

Značka toku **-** je novinkou, v IPv4 nemá svoj ekvivalent. Umožňuje označiť dátový tok zdrojovou stanicou pre rýchlejšie spracovanie smerovačom. Ak napríklad klient nadviaže FTP spojenie so servrom, všetky pakety z patriace do tohto toku budu označene spoločným číslom flow label. Prvý paket bude smerovaný smerovacou tabuľkou smerovača podľa svojej cieľovej adresy a u nasledujúce datagramy už budú môcť odchádzať rovnakým rozhraním bez nutnosti znovu prechádzať smerovaciu tabuľku.

Dlžka dát - Označuje veľkosť datagramu bez základnej hlavičky. Presne počet bajtov nasledujúcich za základnou hlavičkou, doplnujúce hlavičky sa do dlžky počítajú.

Rozširujúca hlavička - obdobou políčka Protokol u IPv4 a nesie identifikáciu o type nasledujúcej rozširujúcej hlavičky, prípadne o protokole vyššej vrstvy.

Maximálny počet skokov (Hop Limit) - je obdobou Time-to-Live u IPv4 protokolu. Určuje koľko skokov môže datagram absolvovať, než bude zlikvidovaný. Pri prechode smerovačom sa zníži počet skokov o jeden. Pri vypršaní počtu skokov bude datagram zlikvidovaný a odosielateľovi sa pošle ICMP správa o vypršaní maximálneho počtu skokov. Účelom je zabrániť zahlteniu siete „blúdiacimi“ datagramami.

Source Address a Destination Address - hlavnou hnacou silou IPv6 je práve obrovský adresný priestor. Na rozdiel od 32-bitovej IPv4 adresy, je pre adresáciu vyhradených až 128 bitov. Z celkovéj veľkosti datagramu, tvoria adresy až 80%, preto sa im budeme venovať v dalšej kapitole. V celej hlavičke nie je miesto pre kontrolný súčet – to z dôvodu, lebo je už nadbytočný a o kontrolu sa budú starať nižšie vrstvy.

Informácia o rozšírenej hlavičke - je nositeľom informácie príslušnej časti rozšírenej hlavičky. Obvykle pozostáva zo záhlavia a dátovej časti. Rozšírené hlavičky obsahujú voliteľné doplňujúce informácie.

IPv4 Pole hlavičky	**IPv6 Pole hlavičky**
Verzia	Rovnaké pole s odlišným číslom verzie.
Dĺžka Internetovej Hlavičky	Odstránená. IPv6 neobsahuje pole Dĺžka hlavičky, lebo hlavička má vždy fixnú hodnotu 40 bytov. Každá rozširujúca hlavička má fixnú veľkosť alebo indikuje vlastnú.
Typ Služby (Type of Service)	Nahradený poľom Trieda premávky (Traffic Class).
Celková dĺžka	Nahradená poľom Dĺžka dát (Payload length), ktoré indikuje len vekosť prenášaných dát.
Identifikácia Príznaky fragmentácie Odstup fragmentácie	Odstránené. Informácie o fragmentácii nie sú zahrnuté v hlavičke. Sú obsiahnuté v rozširujúcej hlavičke Fragmentácia.
Time to Live	Nahradený poľom Maximálny počet skokov (Hop limit).
Protokol	Nahradený poľom Rozširujúca hlavička (Next Header).
Kontrolný súčet	Odstránený. Kontrolný súčet je vykonávaný na úrovni bitov v linkovej vrstve.
Zdrojová adresa	Pole ostalo nezmenené, len zmenila veľkosť adresy na 128 bitov.
Cieľová adresa	Pole ostalo nezmenené, len zmenila veľkosť adresy na 128 bitov.

Voľby	Odstránené. Pole Volieb bolo nahradené poľom Rozširujúca hlavička (Next Header).

Tab. 2.2: Význam polí v hlavičke IPv4 a ich ekvivalent u IPv6

2.1 Rozširujúce hlavičky

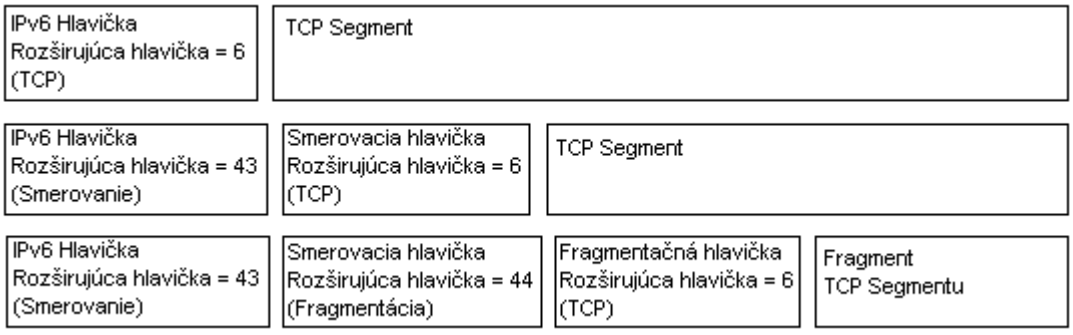
Hlavička IPv4 obsahuje všetky voľby. Z tohto dôvodu každý smerovač musí skontrolovať ich prítomnosť a narábať s nimi podľa potrieb. Negatívnym efektom je spomalenie výkonu v spracovaní a doprave paketov ďalej. V protokole IPv6, voľby doručenia a dopravy sú presunuté do rozširujúcich hlavičiek. Jediná rozširujúca hlavička, ktorá musí byť spracovaná na každom smerovači, je hlavička *Voľby pre všetkých (Hop-by-hop options).* Tento systém urýchľuje spracovanie hlavičiek a dopravu paketov po sieti. Nasledujúce hlavičky musia byť podporované všetkými IPv6 uzlami:

- *Voľby pre všetkých*
- *Voľby pre cieľ*
- *Smerovanie*
- *Fragmentácia*
- *Autentifikačná hlavička*
- *Hlavička šifrovania (Encapsulating Security Payload)*

Hodnota (decimálna)	Hlavička
0	Voľba pre všetkých (Hop-by-Hop Options)
6	TCP
17	UDP
43	Smerovanie
44	Fragmentácia
50	Šifrovanie obsahu (Encapsulating Security Payload - ESP)
51	Autentifikácia
58	ICMPv6
59	Posledná hlavička (No next header)
60	Voľba pre cieľ (Destination Options)

Tab. 2.3: Vybrané hodnoty rozširujúcich hlavičiek

Základný IPv6 paket neobsahuje rozširujúce hlavičky. Ak je vyžadované, aby sa s paketom špeciálne zaobchádzalo, je pridaná jedna alebo viac rozširujúcich hlavičiek. Podmienkou je aby veľkosť rozširujúcich hlavičiek bola násobkom 8 bytov.



Obr.2.2: Príklad zreťazenia rozširujúcich hlavičiek

3. Adresovanie

Najdôležitejším rozdielom oproti IPv4 je rozsah adresného priestoru. Veľkosť jednej adresy je 128 bitov, to je štyrikrát viac ako u adresy IPv4 protokolu. 32 bitová adresa povoľuje celkom 2^{32} alebo 4,294,967,296 možných adries, zatiaľ čo 128 bitová adresa povoľuje celkom 2^{128} alebo 340,282,366,920,938,463,463,374,607,431,768,211,456 ($3{,}4.10^{38}$) možných adries. Laické je to možné prirovnať k uloženiu 10 adries na jeden centimeter štvorcový z celého zemského povrchu

Je dôležité si uvedomiť, že 128 bitový adresný priestor nebol navrhnutý za účelom „nikdy sa neminúť“. Tento veľký priestor adresy IPv6 protokolu bol navrhnutý pre delenie na hierarchické routovacie domény, ktoré odzrkadľujú súčasný moderný Internet. 128 bitová adresa dovoľuje navrhnúť mnoho úrovní v hierarchii a flexibilite pri tvorení topológie siete, čiže to čo v dnešnom Internete fungujúcom na protokole IPv4 chýba.

3.1 Syntax adries

Adresa u protokolu IPv4 bola reprezentovaná štyrmi osem bitovými číslami prevedenými do desiatkovej sústavy a oddelenými bodkami. Dokopy 32 bitov. Adresa u IPv6 protokolu na prvý pohľad vyzerá úplne odlišne ale je tvorená na podobnom princípe. Celých 128 bitov je rozdelených na menšie časti o dĺžke 16 bitov. Tieto bloky 16 bitov sú prevedené na štvorciferné čísla v hexadecimálnom tvare a jednotlivé bloky sú oddelené dvojbodkami. Nižšie je uvedená IPv6 adresa v binárnom tvare:

0010000000000001000011011011100000000000000000000010111100111011
0000001010101010000000001111111111111111000101000100111000101101O

Celá adresa je rozdelená na 16 bitové bloky:

0010000000000001 0000110110111000 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

A nakoniec prevedená do hexadecimálneho tvaru:

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

IPv6 reprezentácia adresy môže byť ďalej zmenšená a to o nuly v každom bloku. Avšak, v každom bloku musí ostať aspoň jedna cifra. Vyššie uvedená adresa má potom tvar 2001:DB8:0:2F3B:2AA:FF:FE28:9C5A.

3.2 Kompresia núl

Niektoré adresy môžu obsahovať dlhé sekvencie núl nasledujúce za sebou. Zapisovanie takýchto adries bolo nutné nejakým spôsobom skrátiť. Adresu v tvare

FA98:0:0:0:0:0:0:FF02

môžeme pomocou kompresie zapísať v tvare FA98::FF02. Podmienkou však je, že takáto kompresia núl sa môže vyskytnúť v adrese iba jediný krát, teda ak existujú ďalšie 16bitové bloky núl nasledujúce za sebou, musia byť zapísané formou poslednej nuly v bloku. Napríklad adresu FA98:0000:0000:12BB:0000:0000:0000:FF02 zapíšeme v tvare

FA98:0:0:12BB::FF02

Taktiež je dovolené komprimovať len bloky 16 bitov, nemôžeme do komprimácie zahrnúť nuly z nenulových blokov.

3.3 Prefixy

Prefix je časť adresy označujúca bity, ktoré majú nemennú hodnotu alebo sú súčasťou určitej podsiete. Prefixy pre IPv6 podsiete, cesty a rozsahy adries sú definované rovnakým spôsobom ako Classless Inter-Domain Routing (CIDR) v protokole IPv4. IPv6 prefix je písaný v tvare *adresa/prefix.* Ako príklad poslúži

FA98::FF02/64

Je dôležité uvedomiť si, že IPv4 používal 32 bitovú adresu v decimálnom tvare ako reprezentáciu prefixu. V IPv6 nič ako maska podsiete neexistuje. Existuje len dĺžka prefixu.

3.4 Typy adries

Existujú tri typy IPv6 adries:

- *Individálna (unicast) adresa* – identifikuje jedno rozhranie v rozsahu typu individuálnej adresy. Pakety adresované indviduálnej adrese sú doručené jedinému rozhraniu.
- *Skupinová (multicast) adresa* – identifikuje viac rozhraní. Pakety adresované skupinovej adrese sú doručené všetkým rozhraniam identifikovaným skupinovou adresou. Používa one-to-many typ komunikácie s doručovaním viacerým rozhraniam.
- *Výberová (anycast) adresa* – identifikuje viac rozhraní. Pakety adresované výberovej adrese sú doručené jedinému rozhraniu, najbližšiemu definovanému výberovou adresou. Pod „najbližším“ rozumieme rozhranie definované v pojmoch smerovania, ktoré budú vysvetlené v neskoršej kapitole.

V IPv6 protokole neexistujú *všesmerové (broadcast) adresy.* Tie sú nahradené skupinovými adresami.

IPv4 Adresa	IPv6 Adresa
Triedy Internetových adries	V IPv6 sa nedajú aplikovať
Skupinové adresy (224.0.0.0/4)	IPv6 skupinové adresy (FF00::/8)
Všesmerové adresy	V IPv6 sa nedajú aplikovať
Nešpecifikovaná adresa má tvar 0.0.0.0	Nešpecifikovaná adresa má tvar ::
Loopback adresa má tvar 127.0.0.1	Loopback adresa má tvar ::1
Verejné IP adresy	Globálne individuálne adresy
Súkromné IP adresy (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Lokálne miestne adresy (FEC0::/10)
Autokonfigurované adresy (169.254.0.0/16)	Lokálne linkové adresy (FE80::/64)

Formát zápisu: Decimálny, čísla oddelené bodkami	Formát zápisu: Hexadecimálny, čísla oddelené dvojbodkami s potlačením vedúcich núl a kompresiou núl. IPv4 kompatibilné adresy sú v desiatkovej sústave oddelné bodkami.
Formát zápisu sieťových bitov: Maska podsiete v desiatkovej sústave, čísla oddelené bodkami alebo dĺžka prefixu.	Formát zápisu : Len dĺžka prefixu

Tab. 3.4: Význam IPv4 adries a ich ekvivalent u IPv6

3.5 Typy individuálnych IPv6 adries

Členenie adries v IPv6 je rozdelené podľa ich využitia:

- Globálne individuálne
- Lokálne linkové
- Lokálne miestne
- Unikátne lokálne IPv6 individuálne adresy
- Špeciálne adresy

3.5.1 Globálne individuálne adresy

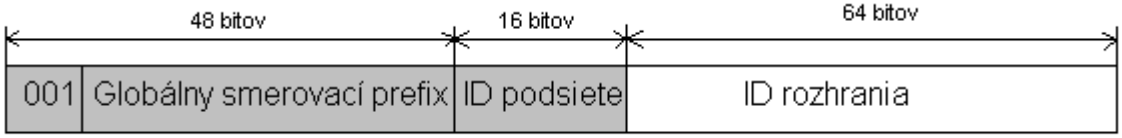
Globálne individuálne adresy sú ekvivalentné ku IPv4 verejným adresám. Rozsah siete, na ktorom sú tieto adresy unikátne, je samotný Internet. Ak by celý svet fungoval na IPv6 protokole, znamenalo by to, že žiadny dvaja účastníci pripojení do Internetu by nemali rovnakú adresu. Na obrázku nižšie je zobrazená štruktúra adresy:

Nemenná časť 001 – tri bity MSB (Most Significiant Bits) majú hodnotu 001. To znamená, že prefix pre globálne adresy má hodnotu 2000::/3.

Globálny smerovací prefix – Má dĺžku 45 bitov a vyznačuje určité miesto organizácie. Globálny smerovací prefix spolu s prvými troma bitmi tvoria 48 bitový smerovací prefix pre dané miesto organizácie. Smerovače potom smerujú pakety so zhodným 48 bitovým prefixom na smerovače patriace danému miestu organizácie.

ID posdiete – Organizácia ďalej používa ID na identifikovanie podsiete. ID ma dĺžku 16 bitov, teda môže byť vytvorených až 65536 podsietí.

Identifikátor rozhrania – identifikuje rozhranie na špecifickej podsieti.

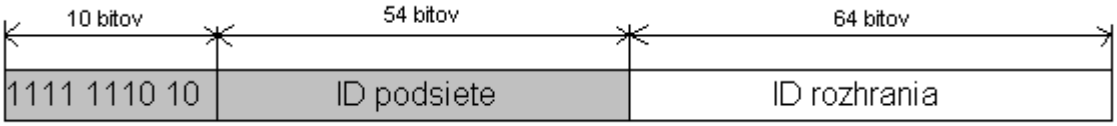


Obr. 3.3: Štruktúra globálnej individuálnej adresy

3.5.2 Lokálne linkové adresy

Linkové lokálne adresy sú používané pri komunikácii na rovnakej linke. Napríklad dva počítače spojene spoločnou linkou bez prítomnosti smerovača použijú lokálnu linkovú adresu. Sú ekvivalentné ku IPv4 linkovým adresám ktoré používajú prefix 169.254.0.0/16. U IPv6 protokolu vždy začínajú bitmi FE80 a s 64 bitovým identifikátorom rozhrania tvoria adresu FE80::/64. Lokálna linková adresa je potrebná

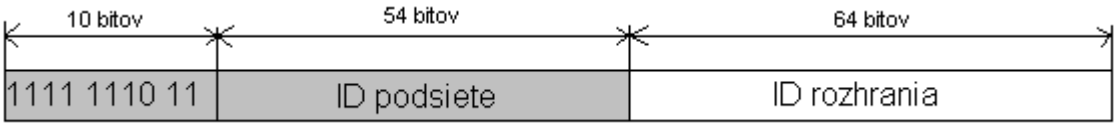
pre objavovanie susedov (Neighbour Discovery) a je vždy automaticky nakonfigurovaná aj bez prítomnosti všetkých zvyšných typov unicast adries.



Obr. 3.4: Štruktúra lokálnej linkovej adresy.

3.5.3 Lokálne mieste adresy

Lokálne mieste adresy sú ekvivaletné IPv4 adresám z privátneho rozsahu, tzn. 10.0.0.0/8, 172.16.0.0/12 a192.168.0.0/16. Napríklad siete, ktoré nemajú pripojenie na internet môžu použiť lokálne mieste adresy spolu s globálnymi individuálnymi adresami bez obavy akýchkoľvek konfliktov. Tak ako privátne adresy, tak aj lokálne mieste adresy nie sú dosažiteľné zvonku a smerovače nesmú smerovať pakety miestnych adries von zo siete. Lokálne mieste adresy sú zamerané na použitie napríklad v organizáciách, internátoch či dokonca v kanceláriách. Naproti lokálnym linkovým adresám sa musia konfigurovať manuálne. Prvých 10 bitov je nemenných a majú hodnotu (FEC0::/10). Za nimi nasleduje 54 bitov určujúcich adresu podsiete a na záver 64 bitov identifikujúcich špecifické rozhranie v podsieti.



Obr.3.5: Štruktúra lokálnej miestnej adresy.

3.5.4 Špeciálne IP adresy

- *Nešpecifikované adresy* – majú tvar 0:0:0:0:0:0:0:0 alebo :: . Používajú sa na indikáciu absencie adresy. To znamená, že ekvivalentom u IPv4 protokolu je adresa 0.0.0.0.
- *Loopback adresy* – majú tvar 0:0:0:0:0:0:0:1 alebo ::1. Používajú sa na identifikáciu loopback rozhrania, dovoľujúc hostovi posielať pakety sebe samému. Ekvivalentom u protokolu IPv4 je adresa 127.0.0.1. Pakety adresované na loopback adresu sa nikdy nesmú dostať na linkové spojenie alebo byť poslané ďalej smerovačom.

3.5.5 Kompatibilné adresy

Aby bol prechod z IPv4 na protokol IPv6 čo najľahší, boli definované nasledujúce typy adries:

- *Adresy kompatibilné s IPv4* – majú tvar 0:0:0:0:0:0:a.b.c.d alebo ::a.b.c.d, kde a.b.c.d je adresa typu IPv4. Sú používané účastníkmi zvládajúcimi obidva protokoly ale komunikujúcimi len pomocou IPv6. Keď je IPv4-kompatibilná adresa použitá ako cieľová IPv6 adresa, IPv6 datagram je automaticky zabalený použitím IPv4 hlavičky a poslaný IPv4 infraštruktúrou.
- *IPv4-namapované adresy* – má tvar 0:0:0:0:FFFF:a.b.c.d alebo ::FFFF:a.b.c.d. Je používaná len za účelom identifikovať sa ako účastník komunikujúci len

pomocou IPv4 pred IPv6 účastníkom. Nikdy sa nepoužíva ako cieľová či zdrojová adresa IPv6 paketu.

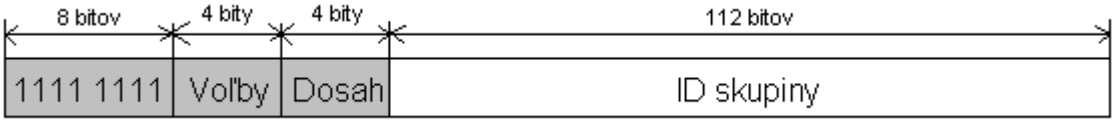
- *6to4* – je adresa používaná na komunikáciu medzi účastníkmi zvládajúcimi obidva protokoly cez IPv4 infraštruktúru. Je tvorená kombináciou prefixu 2002::/16 a 32 bitovou IPv4 verejnou adresou tak, že vznikne prefix o dĺžke 48 bitov. Adresa 6to4 je používaná technikou zvanou tunelovanie, ktorú vysvetlím v neskoršej kapitole.

3.6 Skupinové adresy

V IPv6, skupinový prenos pracuje na rovnakom princípe ako skupinový prenos u IPv4. To znamená, že účastník siete počúva a hľadá prenos na skupinovej adrese. Účastník môže počúvať na viacerých skupinových adresách naraz a môže sa pripojiť či opustiť skupinu hocikedy. Tvar skupinovej adresy je uvedený nižšie:

Adresa začína 8 bitmi 11111111. Tým pádom je ľahké klasifikovať IPv6 adresu ako skupinovú, lebo vždy začína hexadecimálnou hodnotou „FF“. Ďalej nasledujú informácie

- *Voľby* – veľkosť tohto poľa sú 4 bity. Bit s najmenšou hodnotu (LSB) sa vola príznak T (Transient). Keď má hodnotu 0, skupinová adresa je permanentne priradená, dobre známa, organizáciou IANA. Adresa, ktorá nie je permanentne priradená má hodnotu bitu 1. Bit s druhou najmenšou hodnotu sa volá príznak P (Prefixu) a označuje či adresa je postavená na prefixe individuálnej adresy.
- *Dosah* – Indikuje dosah siete, pre ktorý je skupinový prenos určený. Popri skupinovom smerovaní používajú smerovače dosah na rozhodovanie, či skupinový prenos posielať ďalej.
- *ID skupiny* – identifikuje skupinu a je unikátne v celom dosahu skupinového prenosu. Má dĺžku 112 bitov. Permanentne pridelené identifikátory skupiny sú nezávislé na dosahu. Dočasné identifikátory skupiny sú platne len v dosahu skupinovej adresy. Skupinové adresy v rozsahu FF01:: až FF0F:: sú rezervované, známe adresy.



Obr.3.6: Štruktúra skupinových adries.

4. IPv6 Identifikátory rozhrania

Posledných 64 bitov IPv6 adresy určuje identifikátor rozhrania, ktorý je unikátny k 64 bitovému prefixu. Nižšie sú uvedené spôsoby pridelovania identifikátorov rozhrania. Podrobne popíšem však len prvý spôsob.

- 64 bitový identifikátor rozhrania, ktorý je odvodený z EUI-64 adresy (Extended Unique Identifier) a definovaný inštitútom IEEE. EUI-64 sú buď pridelené sieťovým kartám alebo odvodené od IEEE 802 (MAC) adries.

- Ďalším spôsobom je mať pridelený náhodný identifikátor rozhrania, ktorý bude ponúkať určitý stupeň anonymity.
- Identifikátor rozhrania môže byť definovaný z adresy na spojovej vrstve, alebo môže byť náhodne vygenerovaný pri nastavovaní Point-to-Point (PPP) protokolu keď EUI-64 adresa nie je dostupná.
- Je priradený počas manuálnej konfigurácie

4.1 Identifikátory rozhrania postavené na EUI-64 adresách

Adresy IEEE EUI-64 predstavujú nový štandard v adresovaní sieťových rozhraní. Majú dĺžku 64 bitov, pričom ID výrobcu ma stále 24 bitov ako u MAC adresy, tzn. na určenie adresy výrobcom ostáva až 40 bitov, teda omnoho väčší adresný priestor. EUI-64 adresa používa príznak globality, je to druhý najmenej významný bit v prvom bajte. Ak má hodnotu 0, označuje celosvetovo jednoznačnú adresu (globálnu) a hodnota 1 udáva adresu lokálnu.

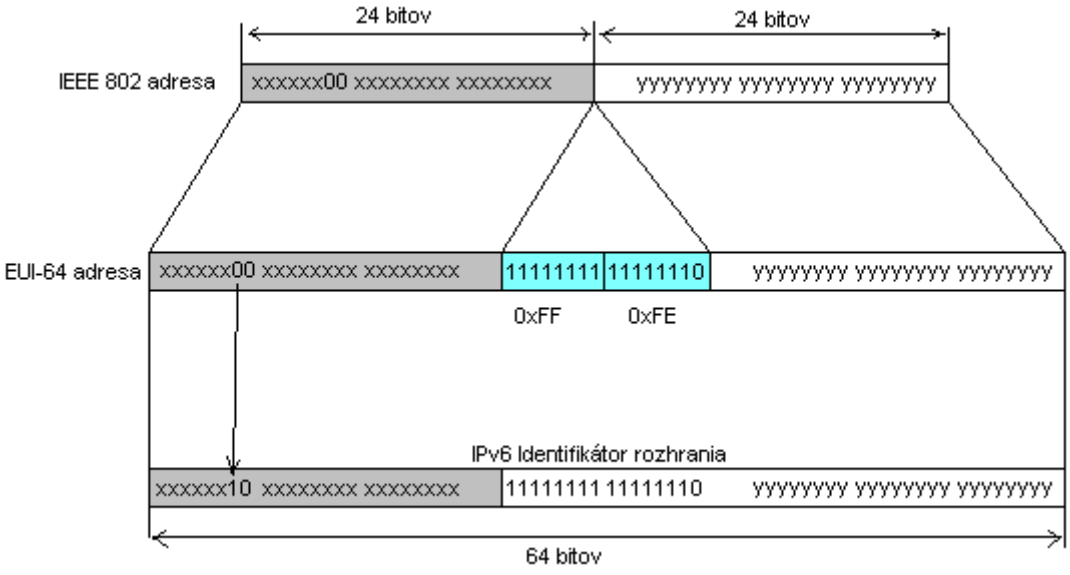
4.2 Mapovanie MAC adresy na EUI-64 adresu

Na vytvorenie EUI-64 adresy z IEEE802 adresy treba vložiť 16 bitov do MAC adresy o hodnote 11111111 11111110 (0xFFFE) medzi ID výrobcu a ID prípony. Názorný príklad je uvedený nižšie.

4.3 Mapovanie EU-64 adries do identifikátorov rozhrania

Získať 64-bitový identifikátor rozhrania je veľmi jednoduché. K druhému najmenej významnému bitu spravíme komplement (ak má hodnotu 1 je nastavený na 0, ak hodnotu 0 je nastavený na 1).

Aby sme získali identifikátor rozhrania z MAC adresy, musíme najprv namapovať IEEE 802 adresu na EUI-64 adresu a potom spraviť komplement k siedmemu bitu v prvom bajte adresy. Proces bude vyobrazený na obrázku nižšie.



Obr. 3.7: Identifikátor rozhrania vytvorený z linkovej adresy

5. Servisný protokol ICMPv6

Tak ako u protokolu IPv4, ani IPv6 protokol nepodporuje mechanizmy pre ohlasovanie chýb. Namiesto toho, IPv6 používa updatovanú verziu protokolu ICMP (Internet Control Message Protocol) pomenovaný ICMPv6. Má tie isté bežné funkcie ako jeho predchodca ICMP u protokolu IPv4, teda oznamovanie doručenia, oznamovanie chýb.

Takisto séria niekoľkých paketov ICMPv6 tvorí nasledujúce služby:

- Multicast Listener Discovery (MLD)

  MLD tvorí séria troch za sebou nasledujúcich ICMPv6 paketov. Jeho funckiou je riadiť členstvo v skupinových adresách podsietí. Tým pádom je náhradou protokolu IGMP verzie 2 pre IPv4.

- Neighbour Discovery (ND)

  ND tvorí séria piatich ICMPv6 správ, ktoré riadia komunikáciu na úrovni dvoch uzlov na jednej linke. ND má nahradiť protokol ARP, ICMPv4 Routing Discovery (Objavovanie smerovačov), ICMPv4 Redirect Message (Premserovanie správ).

Protokol ICMPv6 je potrebný pre implementáciu protokolu IPv6.

5.1 Hlavička ICMPv6 protokolu

Hlavička ICMPv6 protokolu je indikovaná hodnotou rozširujúcej hlavičky 58.

Jednotlivé polia v hlavičke sú:

- *Typ* – indikuje typ ICMPv6 správy. Veľkosť poľa má hodnotu 8 bitov a pri chybových správach má najvýznamnejší bit hodnotu 0 (tzn. že môže nadobudnúť hodnotu 0 až 127). Pri správach informačných má najvýznamnejší bit hodnotu 1 (tzn. že môže nadobudnúť hodnotu 128 až 255).
- *Kód* – Mení sa s počtom správ jedného typu. Ak máme len jednu správu pre daný typ, jeho hodnota je nastavená na nulu. Veľkosť poľa je 8 bitov.
- *Kontrolný súčet* – Ukladá kontrolný súčet pre ICMPv6 paket. Veľkosť poľa je 16 bitov. Pri výpočte kontrolného súčtu musí IPv6 pridať takzvanú pseudo-hlavičku na začiatok ICMPv6 paketu.
- *Telo správy* – Obsahuje samotné dáta nesené ICMPv6 správou.

5.2 Typy ICMPv6 správ

Existuje viac typov ICMPv6 správ. Pre rozsah práce popisujem vybrané správy.

- Chybové správy - Chybové správy sa používané na ohlasovanie chýb pri prenose IPv6 paketov cez sieť alebo pri ich nesprávnom doručení cieľovému hostovi buď cieľovým uzlom alebo medziľahlým smerovačom. Chybové správy zahŕňajú typy Cieľ nedosiahnuteľný, Čas vypršal, Paket príliš veľký a problém s parametrom.
- Informačné správy - Informačné správy slúžia na diagnostické účely a na nadstavbové funkcie ako napríklad MLD a ND. Zahŕňajú typy správ Echo request a Echo reply.
- Objavovanie susedov – séria piatich ICMPv6 správ, ktorá určuje vzťah medzi susediacimi uzlami.

5.2.1 Chybové správy

Chybové správy sú používane cieľovým hostom a medziľahlými smerovačmi na oznamovanie chýb pri prenose alebo doručení. Aby chybové správy nezaberali veľkú časť z šírky pásma bol ich počet zredukovaný. Tým pádom sa chybové správy nepoužijú na každú chybu čo nastane.

Cieľ nedostupný - ICMPv6 správa typu cieľ nedostupný je poslaná v prípade keď paket z nejakého dôvodu nemohol doraziť k cieľu. V tomto type správy má položka Typ hodnotu 1 a položka Kód nadobúda hodnôt od 0 po 4. Po položke kontrolný súčet nasleduje 32 bitová položka Nevyužité pole a za ním zvyšok veľkosti paketu, ktorý doplní ICMPv6 správu na IPv6 paket maximálnej veľkosti 1280 bytov. Ak je ICMPv6 správa poslaná bez rozširujúcej hlavičky, 1232 bytov zaberá časť zahodeného paketu, 40 bytov IPv6 hlavička a 8 bytov hlavička ICMPv6).

Paket príliš veľký - ICMPv6 správa Paket príliš veľký je poslaná vtedy, keď MTU na linke je menšie ako veľkosť posielaného paketu IPv6. V tomto type správy má položka Typ hodnotu 2 a pole Kód má hodnotu 0. Po poli Kontrolného súčtu nasleduje 32 bitové MTU pole, ktoré ukladá hodnotu MTU prenosovej linky po ktorej paket cestuje. Správa Paket príliš veľký je používaný v procese objavovania MTU cesty.

Čas vypršal - Správa Čas vypršal je obyčajne posielaná smerovačom v prípade, keď pole Limit skokov v IPv6 hlavičke dosiahne nulu. V správe čas vypršal, pole Typ má hodnotu 3 a pole Kód má hodnotu 0 (keď počet skokov dosiahne nulový počet) alebo 1 (keď čas na fragmentáciu vypršal). Po poli kontrolý súčet nasleduje 32 bitové nevyužité pole. Príjem správ Čas vypršal s kódom 0 indikuje buď, že počet skokov na dosiahnutie adresáta je nedostatočný alebo existuje smerovacia „skratka“.

Problém s parametrami - ICMPv6 správu problém s parametrami môže poslať smerovač alebo adresát danej správy. Tento typ správy je poslaný v prípade výskytu chyby v hlavičke IPv6 protokolu alebo v jednej z rozširujúcich hlavičiek. Jej úlohou je zabrániť v ďalšom prenose takto chybného paketu počítačovou sieťou. Pole Typ má hodnotu 4 a pole Kód môže nadobúdať hodnoty v rozsahu 0 – 2. Po poli kontrolný súčet nasleduje 32 bitové pole Ukazovateľa (Pointer field). Hodnota Ukazovateľa je nastavená na korektnú hodnotu aj keď pozícia chyby nie je zahrnutá v pakete IPv6.

ICMPv4 Správa	ICMPv6 Ekvivalent
Cieľ Nedosiahnuteľný - Sieť nedosiahnuteľná (Typ 3, Kód 1)	Cieľ Nedosiahnuteľný – Neexistuje cesta k cieľu (Typ 1, Kód 0)
Cieľ Nedosiahnuteľný - Hostiteľ nedosiahnuteľný (Typ 3, Kód 1)	Cieľ Nedosiahnuteľný – Adresa nedosiahnuteľná (Typ 1, Kód 3)
Cieľ Nedosiahnuteľný - Protokol nedosiahnuteľný (Typ 3, Kód 2)	Problém s parametrami – Rozširujúca hlavička nerozpoznateľná (Typ 4, Kód 1)
Cieľ Nedosiahnuteľný - Port nedosiahnuteľný (Typ 3, Kód 3)	Cieľ Nedosiahnuteľný - Port nedosiahnuteľný (Typ 1, Kód 4)
Cieľ Nedosiahnuteľný – Potrebná fragmentácia (Typ 3, Kód 4)	Paket príliš veľký (Typ 2, Kód 0)
Cieľ Nedosiahnuteľný – Komunikácia s cieľovým hostiteľom administratívne zakázaná (Typ 3, Kód 10)	Cieľ Nedosiahnuteľný - Komunikácia s cieľovým hostiteľom administratívne zakázaná (Typ 1, Kód 1)
Čas Vypršal - TTL na trase vypršal (Typ 11, Kód 0)	Čas Vypršal – Vyčerpaný limit skokov (Typ 3, Kód 0)
Čas Vypršal – Časovač fragmentácie vypršal (Typ 11, Kód 1)	Čas Vypršal - Časovač fragmentácie vypršal (Typ 3, Kód 1)
Problém s parametrami (Typ 12, Kód 0)	Problém s parametrami (Typ 4, Kód 0 alebo Kód 2)
Stlmenie zdroja (Typ 4, Kód 0)	V IPv6 neexistuje.
Presmerovanie (Typ 5, Kód 0)	Objavovanie susedov (Neighbour discovery) - Správa presmerovanie (Typ 137, Kód 0).

Tab. 5.5: Chybové správy ICMPv4 a ich ekvivalent v ICMPv6

5.2.2 Informačné správy

Informačné správy sú správy určené na diagnostické účely, zistenie dostupnosti hostiteľa.

***Požiadavka na echo (Echo request*) -** Správa ICMPv6 echo request je posielaná cieľovému adresátovi s požiadavkou na okamžitú odpoveď (Echo reply). Systém správ Echo request/Echo reply ponúka jednoduché diagnostické funkcie na pomoc pri zisťovaní problémov dostupnosti sieťového uzla a smerovacích problémov. V správe Echo request má pole Typ hodnotu 128 a pole kód hodnotu 0. Po poli kontrolný súčet nasledujú 16-bitové polia Identifikátor a Číslo sekvencie. Hodnoty týchto dvoch polí nastavuje Odosielateľ a zhodujú sa s hodnotami v korešpondujúcom pakete Echo reply.

***Odpoveď na echo (Echo reply*) -** Ako je uvedené vyššie, ICMPv6 správa Echo reply je odpoveďou ku správe Echo request. Pole Typ má hodnotu 129 a pole Kód hodnotu 0. Po poli kontrolného súčtu nasledujú 16 – bitové polia Identifikátor a Číslo sekvencie. Identifikátor, číslo sekvencie a dátove polia majú rovnaké hodnoty ako polia v korešpondujúcej správe Echo request.

5.2.3 Neighbour Discovery (Objavovanie susedov)

IPv6 Neighbour Discovery (Objavovanie Susedov) je séria piatich ICMPv6 správ, ktorá určuje vzťah medzi susediacimi uzlami. ND nahradzuje ARP, ICMP Router discovery a ICMP Redirect používané v IPv4 a dodáva ďalšie funkcie.

Hostitelia používajú ND na nasledujúce účely:

- Objavovanie susedných smerovačov
- Objavovanie adries, adresných prefixov a ďalších konfiguračných parametrov

Smerovače používajú ND na:

- Oznamovanie svojej prítomnosti, parametre konfigurácie a na linkových prefixov
- Informovanie hostov o lepšej next-hop adrese na doručovanie paketov adresátovi

Uzly používajú ND na:

- Zistenie linkovej adresy susedného uzlu na ktorý je IPv6 paket posielaný a na zistenie, kedy a či sa linková adresa susedného uzlu zmenila.
- Zistenie, či je susedný uzol stále dostupný.

Nasledujúcich 5 správ vykonáva všetky funkcie Objavovania susedov:

- Výzva susedovi (Neighbour Solicitation)
- Ohlásenie suseda (Neighbour Advertisement)
- Výzva smerovaču (Router Solicitation)
- Ohlásenie smerovača (Router Advertisement)
- Presmerovanie (Redirect)

Prvé dve správy nahradzujú protokol ARP (Address Resolution Protocol) v IPv4. Keď odosielateľ potrebuje poslať dáta na známu IPv4 adresu adresáta sídliaceho v rovnakej lokálnej sieti, musí zistiť jeho linkovú adresu. K tomu slúži protokol ARP, ktorý na všesmerovú adresu 255.255.255.255 (všetky uzly v lokálnej sieti) rozošle výzvu „Kto má IP adresu a.b.c.d ?“. Majiteľ a zároveň adresát tejto adresy mu odpovie a do odpovede pridá svoju linkovú adresu.
Podobný mechanizmus sa u IPv6 vykonáva pomocou správ Výzva susedovi a Ohlásenie suseda. Odosielateľ pošle skupinovú správu Výzva susedovi, ktorá je poslaná na skupinovú adresu pre výzývaný uzol odvodenú z IP adresy adresáta. Na tieto účely boli definované skupinové adresy so spoločným prefixom

FF02:0:0:0:0:1:FF00::/104

Ak teda hostiteľ A chce poslať správu hostiteľovi B na adresu

FE80::2AA:FF:FE22:2222

a hľadá k nej korešpondujúcu linkovú adresu, zoberie posledných 24 bitov z cieľovej adresy (22:2222) a pripojí ich za prefix uvedený vyššie. Dostane skupinovú adresu pre vyzývaný uzol

FF02::1:FF22:2222

Hneď ako hostiteľ B dostane správu Výzva susedovi, pridá do svojej tabuľky susedov zdrojovú adresu a zdrojovú lokálnu linkovú adresu hostiteľa A. Potom odošle správu Ohlásenie suseda na adresu Hostiteľa A kde uvedie vlastnú a lokálnu linkovú adresu. Hostiteľ A potom pridá do vlastnej tabuľky susedov záznam o lokálnej linkovej adrese hostiteľa B. Existuje prípad, keď hostiteľ posiela správu Ohlásenie suseda bez vyžiadania iným hostiteľom. Je to vtedy, keď sa zmení lokálna linková adresa rozhrania. V tom prípade, je cieľová adresa tejto správy skupinová adresa všetkých hostiteľov na sieti.

5.2.4 Router Discovery (Objavovanie smerovača)

Objavovanie routerov prebieha veľmi podobne. Ak router príjme správu Výzva susedovi alebo Výzva smerovača, odpovie správou Ohlásenie smerovača. Táto správa sa používa na autokonfiguráciu a na rozdiel od Neighbour Discovery, cieľová adresa je vždy FF02::2 (lokálna linková skupinová adresa z dosahom na všetky routere v sieti). Obyčajne je smerovač vysiela hneď po nabootovaní a tým pádom nemusí čakat až ostatné routere v sieti sa ozvú sami správou Výzva smerovača. Správne nakonfigurovaný smerovač posiela Ohlasovacie správy periodicky do siete.

5.3 Objavovanie MTU cesty

MTU cesta je linka spomedzi všetkých liniek na ceste medzi odosielateľom a adresátom s najmenšou hodnotou MTU. IPv6 pakety s maximálnou veľkosťou MTU cesty nevyžadujú od odosielateľa žiadnu fragmentáciu a sú úspešne doručené až k adresátovi. Aby sme zistili MTU cesty, odosielajúci uzol použije informáciu z prijatej ICMPv6 správy „Paket príliš veľký“. MTU cesty sa zisťuje nasledujúcim procesom:

1. Odosielajúci uzol predpokladá, že MTU cesty je MTU linky pripojenej na rozhranie, z ktorého je dátový prenos vysielaný.
2. Odosielateľ vyšle IPv6 pakety o veľkosti MTU.
3. Ak nejaký smerovač nemôže ďalej poslať paket cez linku, ktorej MTU je menšie ako MTU paketu, zahodí IPv6 paket a pošle ICMPv6 správu „Paket príliš veľký“ späť odosielateľovi. ICMPv6 „Paket príliš veľký“ správa obsahuje MTU linky na ktorej prenos paketu zlyhal.
4. Odosielateľ nastaví MTU odosielaných paketov na hodnotu MTU poľa v ICMPv6 „Paket príliš veľký“ správe.

Odosielateľ opakuje proces od bodu 2 až po bod 4 toľkokrát, kým neobjaví MTU cesty. MTU cesty je zistené v tom momente, keď odosielateľ neprijíma už žiadne ICMPv6 „Paket príliš veľký“ správy alebo keď dostane potvrdenie od adresáta.

6. Automatická konfigurácia

Asi najsilnejším aspektom IPv6 je jeho schopnosť autokonfigurácie dokonca aj bez použitia protokolu stavovej konfigurácie ako Dynamic Host Configuration Protocol pre IPv6 (DHCPv6). Podľa základných nastavení dokáže IPv6 užívateľ nakonfigurovať lokálnu linkovú adresu pre každé rozhranie. Použitím objavovania smerovačov môže hostiteľ odvodiť adresu smerovačov, iné konfiguračné parametre, ďalšie prídavné adresy a linkové prefixy.

6.1 Stavy autokonfigurovaných adries

Automaticky nakonfigurované adresy môžu mať nasledovné stavy:

- Pokusné (Tentative) - Adresa je v procese verifikovania unikátnosti. Verifikácia sa robí pomocou dvojitej detekcie adresy. Uzol nemôže prijímať individuálny prenos na pokusnú adresu.
- Platné (Valid) – Adresa ktorej unikátnosť bola overená a z ktorej môže byť individuálny (unicast) prenos odosielaný a zároveň prijímaný. Platný stav pokrýva adresy v stave preferované a zároveň odmietané.
- Preferované (Preferred) – Uzol môže odosielať a prijímať individuálny (unicast) prenos z a na preferovanú adresu.
- Odmietané (Deprecated) – Adresa ktorá je stále platná, ale jej použitie je postupne presmerované na iný typ komunikácie. Uzol môže odosielať a prijímať individuálny (unicast) prenos z a na odmietanú adresu.
- Neplatné (Invalid) – Adresa ktorej uzol už nemôže posielať individuálny (unicast) prenos alebo na ňu prijímať akýkoľvek individuálny prenos. Adresa vstupuje do stave neplatnosti po vypršaní stavu platnosti.

6.2 Typy autokonfigurácií

Existujú trojaký výskyt typov autokonfigurácie:

- Bezstavová
- Stavová
- Obidve súčasne

Bezstavová autokonfigurácia – funguje na princípe rozposielanie informácií o konfigurácii do všetkých sietí, ktorých je daný smerovač členom. Informácie sú rozposielané v náhodných okamžikoch alebo na vyžiadanie a každý uzol v sieti po získaní takejto konfiguračnej informácii zistí, v akej sieti sa nachádza, aký je prednastavený smerovač, ďalšie konfiguračné parametre a pod.
Stavová autokonfigurácia - Stavová konfigurácia je postavená na použití stavových konfiguračných protokolov ako DHCPv6 na získanie IPv6 adresy a iných konfiguračných možností. Stavová konfigurácia je použitá po prijatí správy Ohlásenie smerovača so špecifickými hodnotami niektorých polí hlavičky. Je tiež použitá v prípade, keď na linke nie je zapojený žiadny smerovač. V každom z troch typov autokonfigurácie je lokálna linková adresa vždy nastavená.

7. Bezpečnosť v IPv6 (IPsec)

Bezpečnosť v IPv4 nie je vôbec implementovaná. O bezpečnosť sa starajú mechanizmy vo vyšších vrstvách. V protokole IPv6 autori zahrnuli bezpečnostné mechanizmy do sieťovej vrstvy. Volá sa IPsec. IPsec je v protokole IPv6 povinná no použitie pre každý prenos je otázne. Bezpečnostné mechanizmy so sebou prinášajú značnú réžiu a obmedzenie prenosového pásma. IPv6 k zaisteniu bezpečnosti používa rozširujúce hlavičky. Rozširujúce hlavičky sú dve a ponúkajú dve základné služby: autentifikáciu a šifrovanie. Účelom autentifikácie je zaručiť, že údaje odoslal skutočne ten, kto ich odoslal. Šifrovanie utají údaje aby boli pre potenciálnych útočníkov nečitateľné.

7.1 Autentifikačná hlavička (Autentification Header)

Slúži k overeniu pôvodcu odosielateľa datagramu, k overeniu integrity ako aj k ochrane pred znovu poslaním dát, ktoré sa útočníkovi podarilo zachytiť. Pred odoslaním sa vygeneruje sekvenčné číslo. Vytvorí sa kontrolný súčet integrity pomocou techník ako SHA-1 či MD-5 ktorý je uložený do dátovej časti AH paketu. Ak je to nutné, vykoná sa fragmentácia. Na strane adresáta je kontrolný súčet integrity znovu prepočítaný a porovnaný s hodnotou uvedenou v AH paketu. Ak autentifikácia zlyhá, je paket zahodený. Pakety len s autentifikačnou hlavičkou sú bežne čitateľné treťou stranou.

7.2 ESP (Encrypted Security Payload) hlavička

Slúži na šifrovanie obsahu. Okrem toho poskytuje služby podobné autentifikačnej hlavičke. Nemôže však poskytovať obe služby naraz. Pri šifrovaní je na strane odosielateľa obsah paketu pomocou kryptografických kľúčov zašifrovaný a na strane adresáta pomocou rovnakých kľúčov obsah rozšifrovaný. Môžeme rozhodnúť ktorú časť IPv6 paketu chceme šifrovať. Ak chceme šifrovať len transportnú časť IPv6 paketu, je ESP vložená pred rozširujúce hlavičky TCP. Tým však nie sú šifrované hlavičky nachádzajúce sa pred ESP. Tento spôsob prenosu dát sa nazýva *Transportný mód*. Ak chceme zašifrovať celý IPv6 paket, musíme použiť tzv. *Tunelový mód* prenosu. Týmto spôsobom prenosu sa zašifruje celý IPv6 paket, vloží sa pred neho ESP a hlavička a celé sa to zabalí do ďalšieho IPv6 paketu.

8. Implementácia IPv6

Aj keď je stav implementácie v niektorých operačných systémoch celkom dobrý, prechod celého Internetu na IPv6 sa nemôže odohrať behom jedného dňa. Pre mnoho operačných systémov už existuje podpora IPv6, ale väčšinou nie je kompletná. Funkcie ako mobilita, bezpečnosť ešte nie sú podporované každým výrobcom OS pre osobné počítače či smerovače.

Z teoretického hľadiska je potrebné na úspešnú implementáciu v počítačovej sieti mať nastavený backbone smerovač na podporu IPv6. Tento smerovač potom poskytne adresu jednotlivým hostiteľom ako aj ďalšie konfiguračné parametre. V nasledujúcom kroku si jednotlivý užívatelia musia nainštalovať podporu IPv6 na svoje osobné počítače. Prístup k internetu je potom sprostredkovaný IPv6 proxy serverom. Pakety z klientského HTTP prehliadača komunikujú s proxy serverom na báze IPv6, zatiaľ čo komunikácia medzi proxy serverom a Internetom prebieha na báze IPv4.

Toto je veľmi idealizovaná predstava. V skutočnosti je v dnešnej dobe realizovateľná len koexistencia protokolu IPv4 a IPv6. To je možné dosiahnuť nasledujúcimi spôsobmi:

- dvojitý zásobník
- tunelovanie
- translátor

8.1 Dvojitý zásobník (Dual Stack)

IPv4 a zároveň IPv6 je podporované všetkými uzlami. Vďaka tomu je možná komunikácia s uzlami z obidvoch protokolov. Nevýhodou je, že dvojitý zásobník vyžaduje na svoju funkciu len IPv4 protokol a tým pádom riešenie je len „náhradné“ a nie kompletné.

8.2 Tunelovanie

Technika tunelovania slúži na podporu komunikácie medzi dvoma uzlami pomocou jedného protokolu cez sieť, ktorá tento protokol nepodporuje. To znamená, že potrebujeme prenášať IPv6 pakety cez IPv4 Internet. Sú definované dva typy tunelovania:

Manuálne konfigurované - Manuálne konfigurované tunelovanie nastaví správca zariadenia. Pomáhajú mu vtom tzv. tunelové servre. Tie vytvoria tunel tak, že sa dotyčný záujemca na nich zaregistruje, zadá požadované informácie o pripojení a dostane od servru skript, po ktorého spustení sa vytvorí tunel.

Automaticky konfigurované - Je tunel vytvorený automaticky bez ľudského zásahu. Existuje viac mechanizmov na automatické tunelovanie, napríklad *6to4 , 6over4* alebo *Teredo*. Mechanizmus funguje tak, že z IPv4 adresy prístupového smerovača sa odvodí IPv6 prefix pre celú sieť, ktorá potom komunikuje s podobne vytvorenou IPv6 sieťou.

8.3 Translátor

Ak potrebuje komunikovať zariadenie zvládajúce výlučne IPv4 protokol so zariadením zvládajúcim výlučne IPv6 protokol, je potrebné použiť translátor. Základom je *SIIT (Stateless IP/ICMP Translation),* súbor pravidiel ktorý definuje spôsob prekladu IPv4 paketu na IPv6 a opačne.

8.4 Zhrnutie implementácie

Postup implementácie je rozsiahly cez všetky vrstvy prostriedkov informačných technológií. Tak ako je publikované v odborných materiáloch, jedná sa o časovo dlhé riešenia, ktorým obvykle predchádza starostlivá príprava za použitia programov pre modelovanie a simulovanie navrhovaných riešení. Na základe zvoleného cieľa /rozšírenie možností konektivity na vonkajšie prostredie, rozšírenie sieťových služieb, stav prevádzkovania siete na IPv4 a jej obmedzenia a pod./ sa navrhne optimálny postup. Nevýhodou môže byť, že súčasné používanie IPv4 je veľmi veľké . Implementácia IPv6 však ponúka vhodnú základovú platformu pre aplikáciu služieb na protokole IPv6 a využívanie ich možností.

9. Podpora mobility v IPv6, protokol MIPv6

Ako sa komunikácia v Internete rozvíja z IPv4 na IPv6, podpora mobility v Internete sa rozvíja spolu sním. S postupom času bude mobilita čoraz dôležitejšia pretože mobilný užívatelia budú tvoriť značnú časť populácie Internetu. Hoci vnútorné princípy Internetu ostávajú nemenné, IPv6 prichádza s novými princípmi ktoré by mali

byť zvážené podpornými protokolmi už pri ich návrhu. Hlavným cieľom mobility v IP je zneviditeľniť handovery na úrovni sieťovej vrstvy pre vyššie vrstvy. IP adresa mobilného uzlu musí ostať nezmenená po handovery aby spojenie medzi komunikujúcimi uzlami mohlo pokračovať. V protokole Mobile IPv6 nazývame túto adresu domácou adresou mobilného uzlu, zatiaľčo podsieť do ktorej táto adresa nazývame domácou sieťou. Smerovač v tejto domácej sieti nazývame domácim agentom (HA – Homa Agent).

9.1 Mechanizmus protokolu

Protokol Mobile IPv6 je špecifikovaný v RFC 3775. Pracuje podobne ako protokol Mobile IPv4 s niekoľkými rozdielmi.

Keď vstúpi mobilný uzol (MN – Mobile Node) do novej IPv6 siete, detekuje zmenu topológie siete a signalizuje ju svojmu Domácemu agentovi (HA – Home Agent). HA spravuje väzbu medzi domácou adresou MN a jeho súčasnou CoA adresou. Domáca IP adresa je adresa domácej siete ktorá identifikuje zdroj komunikácie mobilného uzlu. CoA je prístupová IP adresa na cudziu sieť ktorá identifikuje lokáciu mobilného uzlu. Keď domáci agent obdrží signál, je integrita informácie overená a zdroj informácie je autentifikovaný ešte predtým než sa vytvorí záznam o väzbe. Vďaka väzbe sa vytvorí záznam o preposlaní prenosu z domácej adresy MN na jeho CoA. V tomto štádiu spojenia MN komunikuje bezproblémovo aj pri zmene pri prechode sieťami. Z tohto pohľadu to vyzerá ako podpora mobility v protokole IPv4, ale rozdielom je že v MIPv6 nie je miesto pre cudzieho agenta (FA).

V podstate protokol MIPv6 zahŕňa štyri základné funkcie: detekciu pohybu, konfiguráciu CoA, (domácu alebo korešpondujúcu) registráciu a smerovanie paketov. Avšak je vyvíjane len malé úsilie na zlepšenie efektívnosti smerovania paketov pre MN. Myslím, že účinné smerovanie je potrebné na plné si uvedomenie potenciálu mobility v dnešnom Internete. Na úrovni sieťovej vrstvy existuje riešenie, tradičné smerovanie použitím mechanizmu tunelovania ktoré nazývame v MIPv6 Obojsmerné tunelovanie (Bidirectional Tunneling). Avšak, BT smeruje všetky pakety patriace MN cez HA. Tým pádom pakety prenášané na adresu MN sú často smerované cestami, ktoré sú značne dlhšie ako optimálna cesta. Z toho dôvodu bol okrem tradičného tunelovania u MIPv6 vyvinutý mechanizmus smerovania zvaný Route Optimization (RO). RO dovoľuje smerovať pakety priamo na CoA adresu mobilného uzlu z čoho pre pakety vyplýva, že môžu cestovať po najkratšej možnej ceste. Taktiež mechanizmus RO eliminuje preťaženie domácej linky mobilného uzlu a domáceho agenta samotného. Avšak, u RO mechanizmu musí MN registrovať nielen jeho CoA adresu u HA, ale tiež aktualizovať väzbu k CN, z čoho vyplýva väčší kontrolný prenos. Navyše sa spolieha pri smerovaní paketov na rozširujúce hlavičky Routing a Destination Options čo má za následok zväčšenie veľkosti celkovej hlavičky.

9.1.1 Detekcia pohybu

Pohybujúci sa uzol musí detekovať svoju polohu. V MIPv6 mobilný uzol môže zistiť svoju polohu načúvaním správam router advertisement od smerovača a porovnaním prefixu siete zdrojovej adresy v správach router advertisement s prefixom

siete svojej domácej linky. Ak sa prefix siete v správach router advertisement rovná prefixu siete domácej adresy MN, potom MN je na svojej domácej linke. V opačnom prípade sa MN nachádza v cudzej sieti. Ako náhle je v novej sieti, mobilný uzol získa novú IPv6 adresu buď použitím DHCP alebo autokonfigurácie a registruje sa u svojho domáceho agenta a korešpondujúceho uzlu. Tento mechanizmus opisuje dokument The IPv6 Neighbour Discovery (RFC 2461). Avšak tento dokument nebol navrhnutý do mobilného prostredia, pretože minimálny interval medi vyslaním správ Ohlásenie smerovača je 3 sekundy, čo je príliš dlhá doba pre mobilný uzol aby zistil včas či sa zmenila podsieť. V MIPv6 je tento interval zmenený aby podporoval milisekundy.

Mobilný uzol však nemusí len vyčkávať na periodické správy Ohlásenie smerovača. Hneď ako sa uskutoční handover na linkovej vrstve môže vyslať správy Výzva smerovaču. Tento spôsob detekcie pohybu je nadradený výčkávaniu na periodické ohlásenia smerovača a to z dôvodu asynchronnej podstaty, ktorá menej zaťažuje šírku bezdrôtového pásma.

9.1.2 Konfigurácia CoA

Potom ako MN detekuje, že sa premiestnil zo svojej domácej siete do cudzej siete, vytvorí si novú care-of-address. Predtým než novú CoA pridelí WLAN rozhraniu musí mobilný uzol skontrolovať či je adresa unikátna v celej sieti. Tento mechanizmus sa volá detekcia duplikátnej adresy (Duplicate Address Detection). Na skontrolovanie duplicity adresy musí uzol nastaviť kontrolovanú adresu ako cieľovú adresu. Zdrojovú adresu neudá a cieľovú adresu upraví podla skupinovej adresy určenej na kontrolu duplicity adries v sieti (viď 5.2.3). Ak potom cieľový uzol zachytí správu Výzva susedovi ktorej cieľová adresa sa zhoduje s jeho vlastnou adresou a ktorej zdrojová adresa je nastavená na neznámu, odpovie zaslaním správy Ohlásenie suseda. Týmto spôsobom mobilný uzol zistí či je adresa unikátna v sieti. Ak teda neexistuje v sieti duplikát zvolenej adresy, tak MN ktorý vykonýva detekciu duplikátnej adresy neobdrží žiadnu odpoveď vo forme správy Ohlásenie suseda. V súbore správ Neighbour Discovery je odporučené aby uzol vykonávajúci detekciu duplikátnej adresy vyčkal 1000ms predtým, než danú IPv6 adresu uzná za unikátnu v sieti. Teda, celkový handover je oneskorený o jednu sekundu.

9.2 Registračné správy

Podstata mobility je v dvoch nasledujúcich správach, ktorých účelom je signalizovať domácemu agentovi a korešpondujúcemu uzlu prechod mobilného uzlu do novej siete. Sú to správy:

- Aktualizácia väzby (Binding Update)
- Potvrdenie väzby (Binding Acknowledgement)

Mobilnú uzol vyšle správu Aktualizácia väzby aby informoval svojho domáceho agenta alebo CN o jeho momentálnej polohe. Vzťah medzi CoA a domácou adresou je uložený v zozname väzieb (Binding Cache), ktorý v podstate určuje logiku smerovania na HA a CN pri doručovaní paketov mobilnému uzlu na jeho domácu adresu ale smerom k CoA. Tento spôsosb dynamickej zmeny CoA dovoľuje mobilnému uzlu

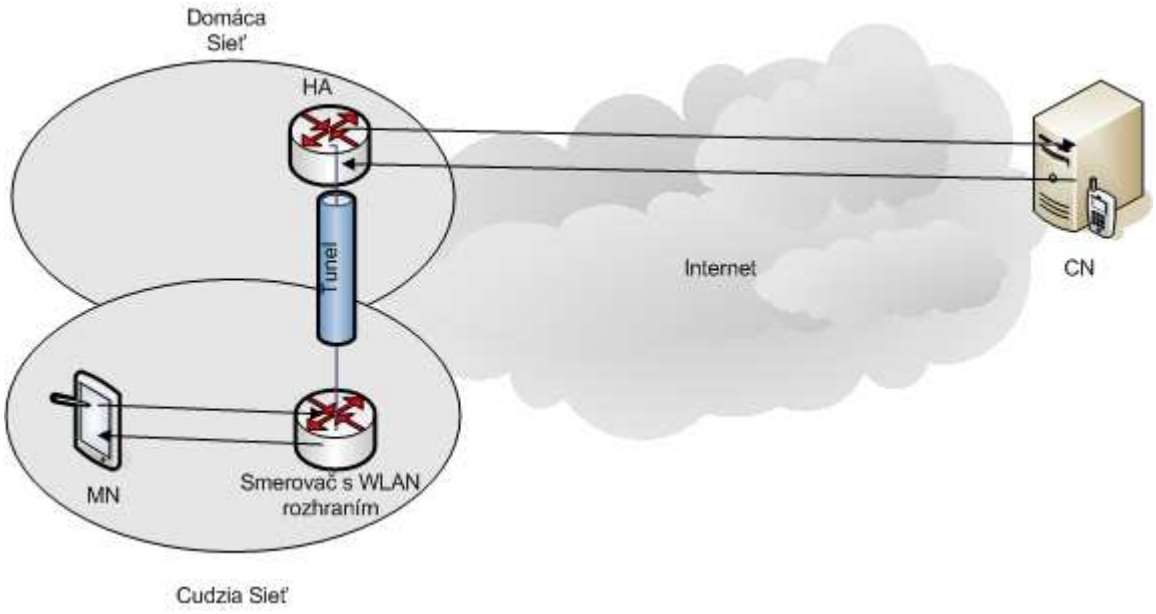
udržiavať spojenie za použitia jeho domácej adresy a zároveň meniť polohu a podsieť indikovanú v CoA. Následne domáci agent alebo CoA vyšle správu Potvrdenie väzby aby oznámil, že prijal Aktualizáciu väzby. Obe správy sú chránené medzi MN a CN protokolom IPsec špecifikovaným v RFC 3776 a to špeciálnym kľúčom, ktorý popíšem nižšie.

9.3 Bidirectional Tunneling (Obojsmerné tunelovanie)

Obojsmerné tunelovanie ako tradičný mód je prezentovaný už v IPv4 (MIPv4). Keďže BT nevyžaduje od CN podporu mobility a je dostupné aj keď MN neregistroval u CN väzbu, je jednoduchšie na zavedenie. Z toho dôvodu je jeho špecifikácia zaradená aj v MIPv6. Obrázok 1 ilustruje BT mechanizmy.

Prvý mechanizmus, obojsmerné tunelovanie, od CN nevyžaduje podporu mobility v IPv6 a je dostupný dokonca aj keď si MN nezaregistroval súčasnú väzbu u CN. V obojsmernom tunelovaní pakety prenášané od CN sú smerované domácemu agentovi a potom tunelované mobilnému uzlu. Pakety adresované CN sú tunelované z MN na adresu HA a toto nazývame spätným tunelovaním. Potom sú smerované normálne do domácej siete CN. V tomto móde používa HA proxy Neighbour Discovery na zachytenie IPv6 paketov adresovaných domácej adrese MN v domácej sieti a každý takto zachytený paket je potom tunelovaný na CoA adresu mobilného uzlu. Tento spôsob tunelovania je vykonávaný za použitia IPv6 zapúzdrenia.

Avšak nevýhoda BT tkvie v nadbytočnom oneskorení prenosu. Navyše sa HA môže stať bodom zlyhania prenosu alebo miestom s veľmi zníženým výkonom pri prenose s narastajúcim počtom užívateľov mobilných zariadení v Internete. Tým pádom sa môže presadiť koncept mechanizmu RO.



Obr. 9.8: Princíp obojsmerného tunelovania

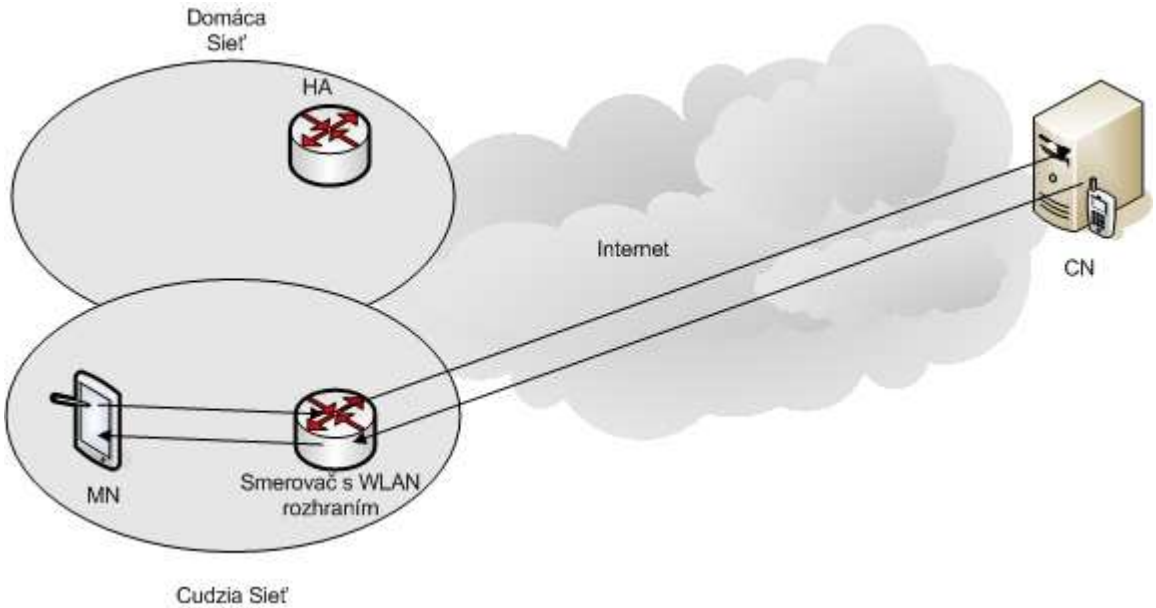
9.4 Route Optimization (Optimalizácia cesty)

V prípade použitia mechanizmu route oprtimization už domáci agent nemapuje adresy ale každý CN má svoju tzv. Binding Cache (tabuľku známych väzieb). Tým

pádom pre komunikáciu sa používa najkratšia možná cesta. Tento spôsob smerovania eliminuje zahltenie domácej siete a domáceho agenta. A navyše je redukovaný dopad na plynulosť komunikácie pri výpadku domáceho agenta alebo siete na ceste. V smere od MN ku CN pakety zaslané mobilným uzlom z inej ako svojej domácej siete sú doručené CN s voľbou Domáca Adresa v hlavičke Destination Option Extention. V tomto prípade nastaví MN v hlavičke IPv6 zdrojovú adresu na svoju CoA a doplní hlavičku voľbou Domáca Adresa kde bude uložená domáca adresa MN. Keď CN zachytí tento paket od MN zamení zdrojovú adresu IPv6 paketu domácou adresou MN ešte predtým než zašle paket vyššej vrstve. Týmto spôsobom nielenže MN udržuje mobilitu transparentnú pre vyššie vrstvy softvéru ale dokáže tiež prepasovať paket cez filtre nastavené v medziľahlých smerovačoch.

V opačnom smere, keď CN posiela pakety na adresu MN, hľadá CN najprv vo svojom zozname väzieb záznam o cieľovej adrese paketu. Ak je taký záznam o väzbe nájdený, CN použije Smerovaciu hlavičku na smerovanie paketov k MN určením CoA ako cieľovej adresy v IPv6 hlavičke a domácu adresu MN ako finálnu adresu v Smerovacej hlavičke. Keď MN zachytí pakety, spracuje Smerovaciu hlavičku a pošle pakety vyššej vrstve s použitím domácej adresy MN ako keby bol mobilný uzol doma. V prípade, že CN nemá záznam o väzbe pre cieľovú adresu, napríklad z dôvodu vypršania životnosti väzby, tak nevie momentálnu polohu mobilného uzlu. Tým pádom vyšle pakety z použitím domácej adresy MN ako cieľovej adresy. Domáci agent MN zachytí pakety a tuneluje ich na momentálnu polohu MN. Keď MN zachytí pakety od jeho HA, zistí že CN nepozná jeho CoA a informuje ho zaslaním správy Binding Update (Aktualizácia väzby) o svojej súčasnej CoA.

Doposiaľ opísaný mechanizmus optimalizácie cesty má však jednu dôležitú slabinu. Každý uzol ktorý pozná domácu adresu MN môže vyslať aktualizáciu väzby smerom k CN mobilného uzlu a požadovať aby sa jeho IP adresa stala novou CoA. Výsledkom je, že CN preruší prenos smerom k MN a začne vysielať pakety na adresu neoprávneného uzlu. Aby bolo zaručené, že len platné MN vysielajú správy Aktualizácia väzby bol do optimalizácie cesty zahrnutý mechanizmus zvaný return routability. Return routability silne obmedzuje počet lokácií z ktorých potenciálny útočník môže vysielať falošné aktualizácie väzby smerom k CN.



Obr. 9.9: Princíp optimalizácie cesty

9.5 Správy optimalizovanej cesty (Return Routability)

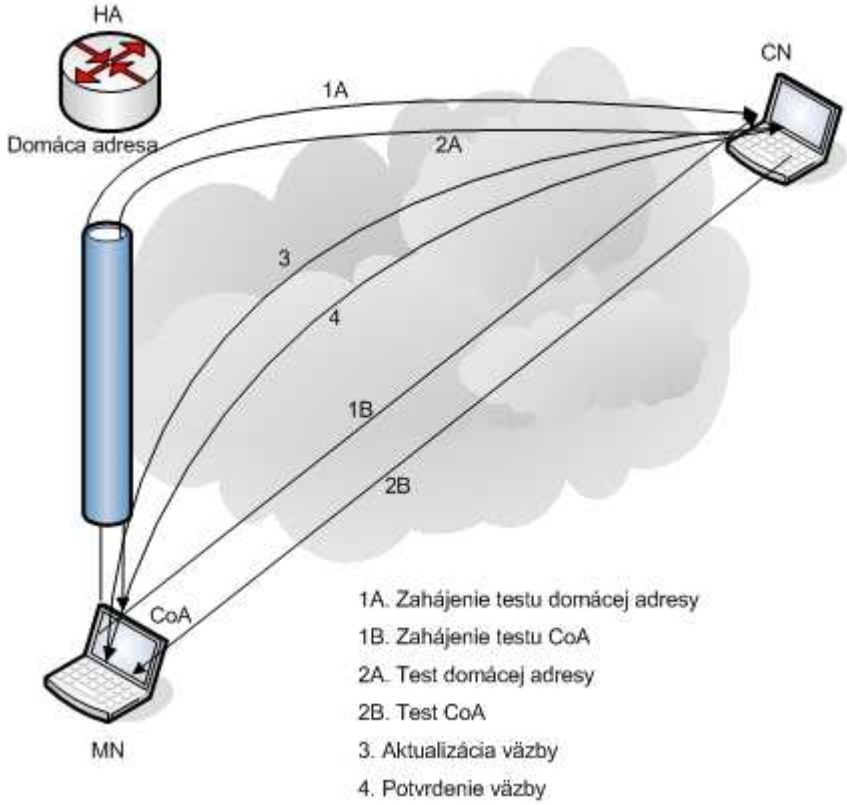
Správy uvedené nižšie dovoľujú aby medzi dvomi IPv6 uzlami bola udržiavaná optimalizovaná cesta:

- Zahájenie testu domácej adresy (Home test init - HoTI)
- Zahájenie testu CoA (Care of test init - CoTI)
- Test domácej adresy (Home test - HoT)
- Test CoA (Care of test - CoT)
- Žiadosť o obnovu väzby
- Chyba väzby
- Voľba pre cieľ
- Smerovacia hlavička Typ 2
- Autorizácia väzby

Aby bola dosiahnutá optimálna cesta, musí si CN vytvoriť záznam o väzbe domácej adresy mobilného uzlu a jeho súčasnej CoA. Aby toho bolo dosiahnuté musí MN vyslať správu o aktualizácii väzby. A toto signalizovanie musí byť autorizované korešpondujúcim uzlom. Z toho dôvodu bol vymyslený autorizačný mechanizmus Return routability a funguje nasledovne. CN vlastní bezpečnostný kľúč pomocou ktorého autentifikuje všetky prichádzajúce správy Aktualizácii Väzby z ktoréhokoľvek mobilného uzlu. Tento bezpečnostný kľúč sa rozdelí na dva žetóny, ktorých znovu zložením vznikne kľúč na strane mobilného uzlu na autentifikáciu správ Aktualizácia väzby. Každý z žetónov je vyslaný na jednu adresu (jeden na domácu, druhý na CoA). Na vytvorenie kľúča schopného autentifikovať väzbové správy je potrebné vlastniť obidva žetóny. Aby adresát získal obidva žetóny, musí byť dostihnuteľný na oboch svojich adresách, Domácej a CoA.

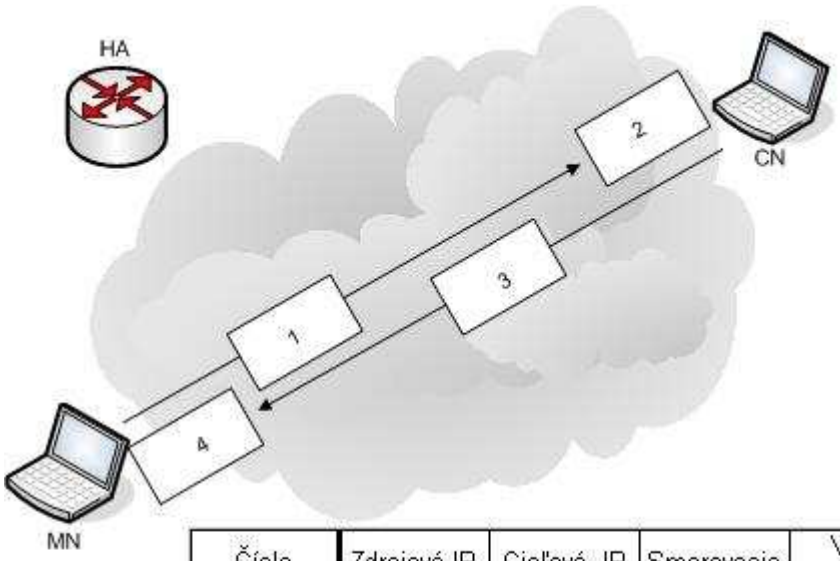
Obrázok ilustruje výmenu správ v procedúre Return Routability. Na začiatku procedúry vyšle mobilný uzol HoTI správu aby si vyžiadal od CN žetón, ktorý mu bude poslaný cez domáceho agenta (1A). Účelom správy HoT je doručiť žetón mobilnému uzlu cestou cez domáceho agenta (2A). Hodnota žetónu je založená na hodnote bezpečnostného kľúča CN, domácej adresy a náhodného čísla. Následne mobilný uzol vyšle CoTI správu priamou cestou s žiadosťou o druhý žetón (1B). Korešpondujúci uzol vyšle CoT správu taktiež priamou cestou (2B). Hodnota druhého žetónu je vypočítaná z bezpečnostného kľúču CN, CoA adresy a náhodného čísla. MN odvodí z domácej adresy a oboch žetónov väzbový kľúč. V tomto bode procedúry už mobilný uzol môže posielať správy Aktualizácia väzby s voľbou Autorizácia väzby obsahujúcou krytpografické hodnoty vypočítané z väzbového kľúču. Následne na strane CN sú opäť vypočítane hodnoty oboch žetónov na základe správy Aktualizácia väzby a potom

zložené do rovnakého väzbového kľúča. Tým pádom môže CN overiť totožnosť Mobilného uzlu. Na záver je mobilnému uzlu vyslaná správa Potvrdenie väzby.



Obr. 9.10: Procedúra Return Routability

Po vytvorení záznamu v zozname väzieb výmenou správ Aktualizácia väzby a Potvrdenie väzby, môže prenos plynúť ďalej. V kroku 1, mobilný uzol vyšle pakety smerom ku CN s použitím domácej adresy vo voľbe pre cieľ čím identifikuje domácu adresu MN v IP hlavičke. Voľba pre cieľ s hodnotou domácej adresy dovoľuje MN komunikovať priamo s CN za použitia CoA ako zdrojovej adresy vyslaných paketov. Teda CN pozná IP adresu MN aj keď nezáleží kde sa nachádza. Domáca adresa je nemenná zatiaľ čo CoA sa mení spolu s polohou MN. V kroku 2, ak CN zachytí data paket s hodnotou domácej adresy vo voľbe pre cieľ od MN ktorý nevykonal procedúru Return Routability tak CN vyšle správu Chyba väzby na zdrojovú adresu prichádzajúceho paketu. Po inej stránke je zdrojová adresa nahradená domácou adresou z poľa Voľba pre cieľ hneď ako dorazí k CN. V kroku 3, CN vysiela pakety na CoA MN za použitia smerovacej hlavičky s hodnotou domácej adresy MN. V kroku 4, MN zachytí paket a zamení CoA (z poľa zdrojová adresa) za domácu adresu (z poľa voľba pre cieľ). Tým pádom aplikácie na MN a CN komunikujú medzi sebou použitím domácej adresy a nie sú oboznámené s CoA ktorá smeruje pakety medzi nimi.



Číslo Paketu	Zdrojová IP Adresa	Cieľová IP Adresa	Smerovacia Hlavička	Voľba Domáca Adresa
1	CoA	CN Adresa	Žiadna	Zahrnutá
2	Domáca Adresa	CN Adresa	Žiadna	Zahrnutá
3	CN Adresa	CoA	Domáca Adresa	Žiadna
4	CN Adresa	Domáca Adresa	Domáca Adresa	Žiadna

Obr. 9.11: Optimalizovaná prenosová cesta

10. Konštrukcia MIPv6 siete v programe OPNET Modeler

Program OPNET Modeler má široké možnosti pre simulovanie v počítačových sieťach. Medzi jeho vlastnosti patrí aj to, že dokáže pracovať s protokolmi IPv4 a IPv6. Z jeho širokých možností som v rámci bakalárskej práce spracoval návrh siete demonštrujúcej vlastnosti MIPv6 protokolu a dopadu parametru Route Optimization na výkonnosť bezdrôtovej siete. V rámci rozsahu práce nepopíšem jednotlivé základné prvky a vlastnosti programu OPNET Modeler ale priamo popisujem návrh MIPv6 sietí.

Aby bolo možne vykonávať operácie spojené s mobilitou, bol MIPv6 model v programe OPNET Modeler navrhnutý a vyvinutý tak aby podporoval mnoho štandardou ako Rozširujúce hlavičky, Neighbour Discovery, Router Advertisements (zahrňujúc detekciu pohybu, stavovú a bezstavovú autokonfiguráciu a detekciu adresy domáceho agenta) či detekciu duplikátnej adresy (DAD – Duplicate Address Detection). Súčasťou sú aj modely mobilného uzlu MN, korešpondujúceho uzlu CN a domáceho agenta HA. MIPv6 model podporuje tiež dva spôsoby smerovania medzi MN a CN: obojsmerné tunelovanie a optimalizáciu cesty. Tým pádom je možné pozorovať

a analyzovať výsledky simulácií demonštrované v MIPv6 modele a porovnať ich s reálnym MIPv6 sieťovým prostredím.

Za účelom simulovania parametru Route Optimization som navrhol dva scenáre:

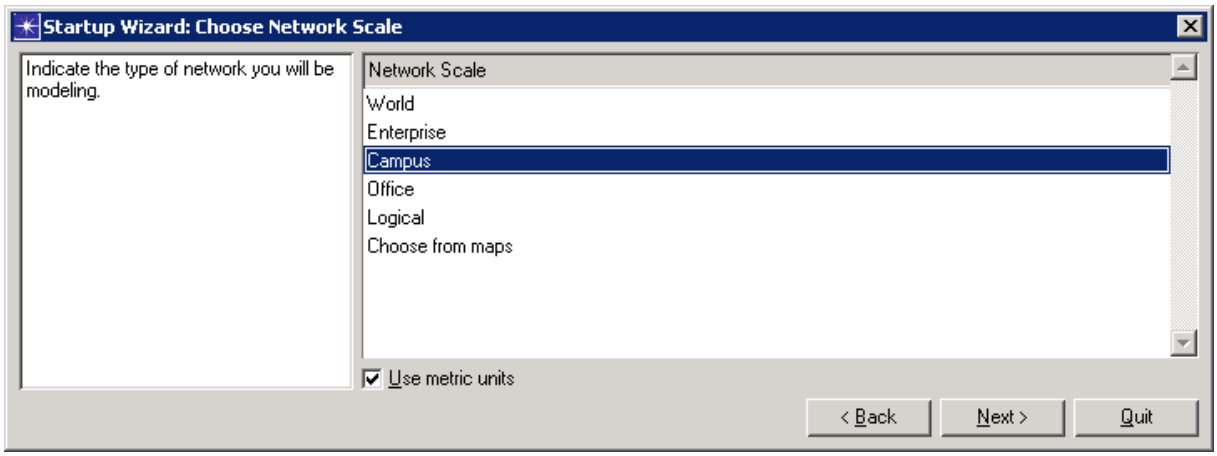
- Bezdrôtovú MIPv6 sieť s použitím smerovania Obojsmerné tunelovanie
- Bezdrôtovú MIPv6 sieť s použitím smerovania Route optimization

Pre určenie v čom spočíva výhoda Route Optimization je potrebné porovnať výsledky z oboch scenárov. Zameriame sa hlavne na koncové oneskorenie paketov pri videokonferencii (end-to-end packet delay) a dĺžku trvania odpovede na žiadosť sťahovania z FTP serveru (Download response).

10.1 Vytvorenie projektu a topológie siete

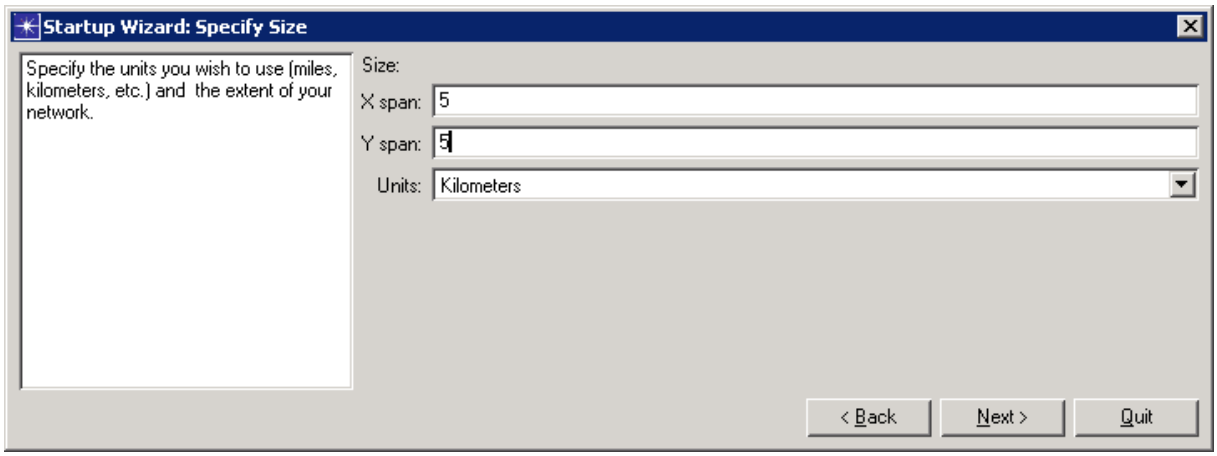
Vytvoril som v programe OPNET Modeler projekt s názvom MIPv6. Tento projekt bude slúžiť na vytvorenie simulácie oboch scenárov. Preto prvému scenáru dáme meno MIPv6_RouteOptimization.

V ďalšom kroku určíme prostredie v ktorom bude prebiehať simulácia. V našom prípade to bude prostredie Campus (Obr. 10.12).



Obr. 10.12: Výber prostredia simulácie

V nasledujúcom kroku zvolíme dosah simulovaného prostredia. V našom prípade je to rozsah 5x5 kilometrov (Obr. 10.13).



Obr. 10.13: Dosah prostredia simulácie

10.1.1 Modely sieťových prvkov použitých v simulácii

Na simuláciu vlastností protokolu MIPv6 sme použili modely sieťových prvkov z palety MIPv6_adv. Sú to nasledovné zariadenia:

- Wlan_ethernet_slip4_adv – Toto je model bezdrôtového smerovača s jedným ethernet rozhraním a štyrmi sériovými rozhraniami. V simulácii sme použili tento model sedem-krát s označením AR_1_HA až AR_7.

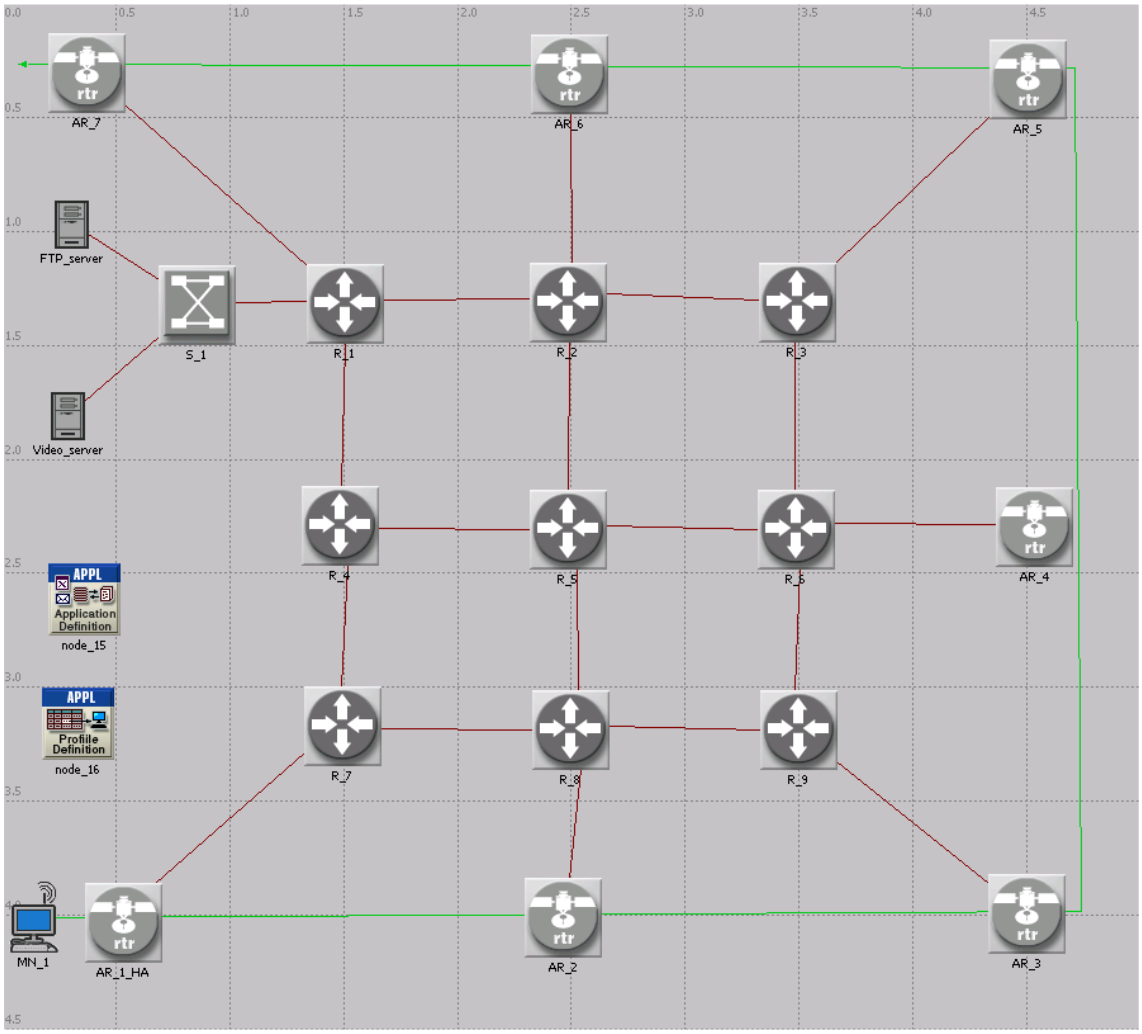
- Ethernet4_slip_gtwy_adv – tento model smerovača podporuje štyri Ethernetové rozhrania, osem sériových rozhraní. Môže mať funkciu brány, čo sme v našej simulácii nevyužili. V našej topológii je použitý 9krát s označením R_1 až R_9.

- Mipv6_ethernet_server_adv – Tento model reprezentuje nepohyblivý server s podporou protokolu MIPv6. Môže byť nakonfigurovaný ako korešpondujúci uzol komunikujúci s mobilnými uzlami za použitia optimalizácie cesty. Podporuje serverové aplikácie typu TCP/IP a UDP/IP. Má jedno ethernetové rozhranie podporujúce rýchlosťi 10Mbps, 100Mbps a 1Gbps. V našej simulácii sme použili dva kusy označené Video_server a FTP_server.

- Wlan_wkstn_adv – tento model mobilnej stanice podporuje aplikácie typu klient-server na báze TCP/IP a UDP/IP. Stanica má jedno wlan rozhranie podporujúce rýchlosti prenosu 1Mbps, 2Mbps, 5,5 Mbps a 11Mbps. V simulácii je použitý jeden model s označením MN_1 pohybujúci sa po trajektórii.

- Ethernet16_switch – tento model reprezentuje prepínač so šestnástimi ethernetovými rozhraniami. Prepínač má implementovaný Spanning Tree algoritmus. Do simulácie je zaradený jeden prepínač s označením S_1.

Jednotlivé modely prvkov sme zoskupili do topológie siete zobrazenej nižšie.



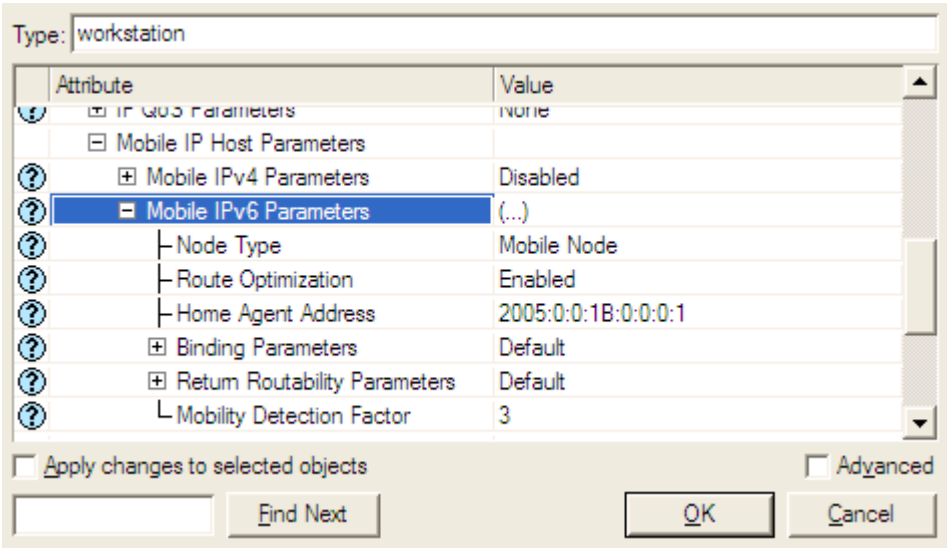
Obr. 10.14: Sieťové prvky zostavené do siete

10.1.2 Konfigurácia sieťových prvkov na podporu MIPv6

- *Konfigurácia mobilného uzlu*

V OPNET MIPv6 modele môžu byť modely staníc konfigurované ako MN nastavením parametru Node Type na: IP->Mobile IP Host Node Parameters->Mobile IPv6 Parameters. Ak chceme zapnúť alebo vypnúť optimalizáciu cesty, nastavíme parameter Route Optimization na Enabled alebo Disabled. IP adresu HA môže MN získať pomocou router advertisements keď je v domácej sieti. Avšak keď je MN mimo svojej domácej siete a exsitujú viaceré AP, musíme špecifikovať IP adresu domáceho agenta v poli Home Agent Address. Môžeme taktiež nastaviť počet stratených správ Router Advertisement za účelom simulovania handoveru v sieťovej vrstve a to parametrom Detection Attribute. Je možné nastaviť parametre Väzby a Return Routability v položke Binding Parameters a Return Routability Parameters. Globálna adresa u mobilného uzlu by mala používať rovnaký prefix ako adresa domáceho agenta. Dôležitou súčasťou konfigurácie MN v našej simulácii je priradenie trajektórie po ktorej sa mobilný uzol bude pohybovať. Trajektória je zobrazená zelenou šípkou a je rozdelená na tri segmenty. Prvý segment a posledný segment majú dĺžku 4,5 km a stredný segment má dĺžku 3,75km. Každý segment prejde stanica za 3 minúty, teda

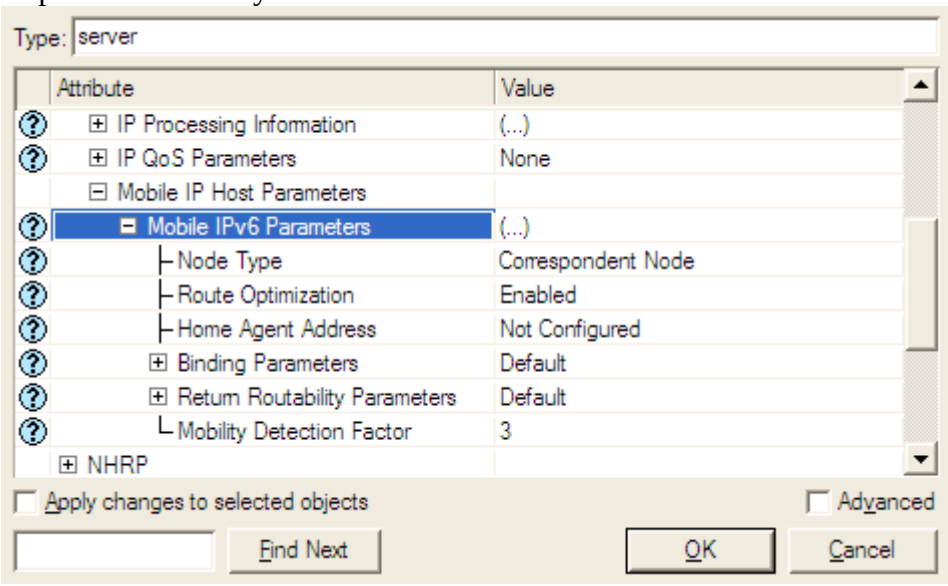
celkový čas pohybu po trajektórii je 9 minút, čo je zároveň aj dĺžka celej simulácie. Na obrázku je zobrazená konfigurácia MN s použitím modelu wlan_wkst_model.



Obr. 10.15: Konfigurácia mobilného uzlu

- *Konfigurácia korešpondujúceho uzlu*

V MIPv6 modele OPNETu je funkcia korešpondujúceho uzlu zahrnutá v funkcii mobilného uzlu. Nakonfigurovať uzol ako korešpondujúci je možné v nastaveniach parametrov a to nastavením položky Node Type na Correspondent Node. Nápodobne je možné zapnúť alebo vypnúť optimalizáciu cesty v modeloch mipv6_ppp_wkstn_adv, mipv6_ppp_server_adv, mipv6_ethernet_wkstn_adv, mipv6_ethernt_server_adv. Navyše, všetky obyčajné modely pracovných staníc sa chovajú ako korešpondujúce uzly bez optimalizácie cesty.

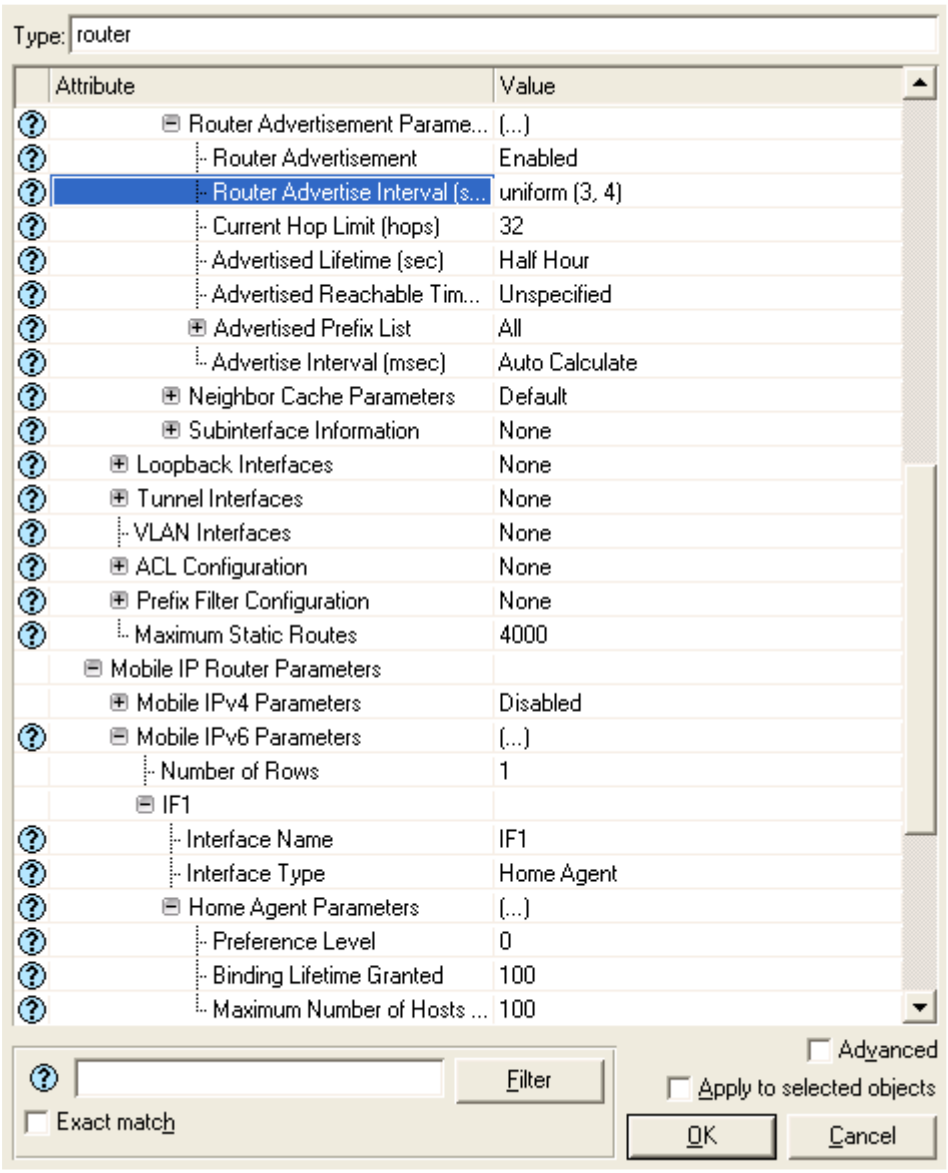


Obr. 10.16: Konfigurácia korešpondujúceho uzlu

- *Konfigurácia domáceho agenta*

Konfigurácia domáceho agenta je možná na každom rozhraní smerovača zvlášť. Smerovač môže mať viac rozhraní ktoré sa budú chovať ako domáci agent a každé

rozhranie musí byť nakonfigurované individuálne. Rozhraním domáceho agenta môže byť bezdrôtové alebo klasické rozhranie. Na obrázku nižšie je špecifikácia rozhrania IF1 ako domáceho agenta. Aby sa mobilný uzol mohol dozvedieť o prítomnosti domáceho agenta vo svojom dosahu, je potrebné aby mal domáci agent povolenú funkciu Router Advertisement. Hodnota intervalu Router Advertisement by mala byť dostatočne krátka aby boli smerovacie tabuľky čo najpresnejšie. Ak je interval príliš dlhý, môže sa zmeniť poloha mobilného uzlu až príliš často pred vyslaním aktualizácie. V moje simulácii som nastavil položku router advertisements na hodnotu uniform (3, 4) v sekundách.



Obr. 10.17: Konfigurácia domáceho agenta

10.1.3 Nastavenie sieťovej prevádzky

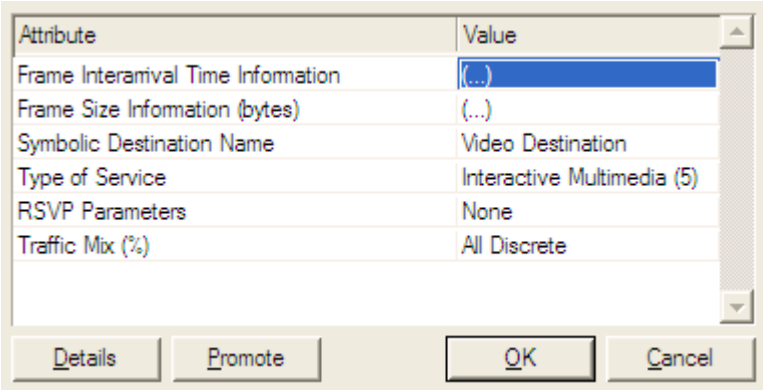
V programe OM sa celkový prenos v sieti definuje dvoma modelmi:

- Application Definition – v našej topológii siete ma označenie node_15. Slúži na definovanie aplikácií generujúcich prenos.

- Profile Definition – v našej topológii má označenie node_16. Slúži na definovanie profilov požadujúcich prenos od aplikácií definovaných v Application Definiton.

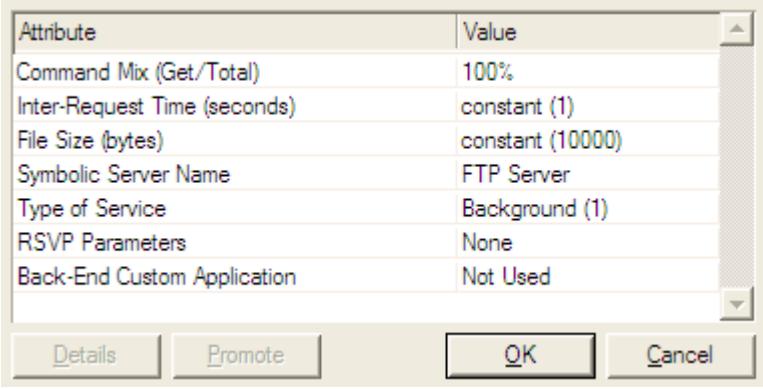
Pomocou týchto prvkov sme nastavili špecifický prenos v našej sieti. Pomocou prvku Application Definition sme nastavili dve aplikácie – Video konferenciu a FTP prenos:

- Video konferencia – Tento typ aplikácie poskytuje reálny prenos cez protokol UDP s konštantnou prenosovou rýchlosťou. V našej simulácii sme nastavili veľkosť prijímaného a odosielaného snímku kódovaného videa na konštantnú veľkosť 1024 bytov. Počet prijímaných a odosielaných obrázkov sme nastavili na 100 snímkov za sekundu. Konfigurácia je zobrazená nižšie.



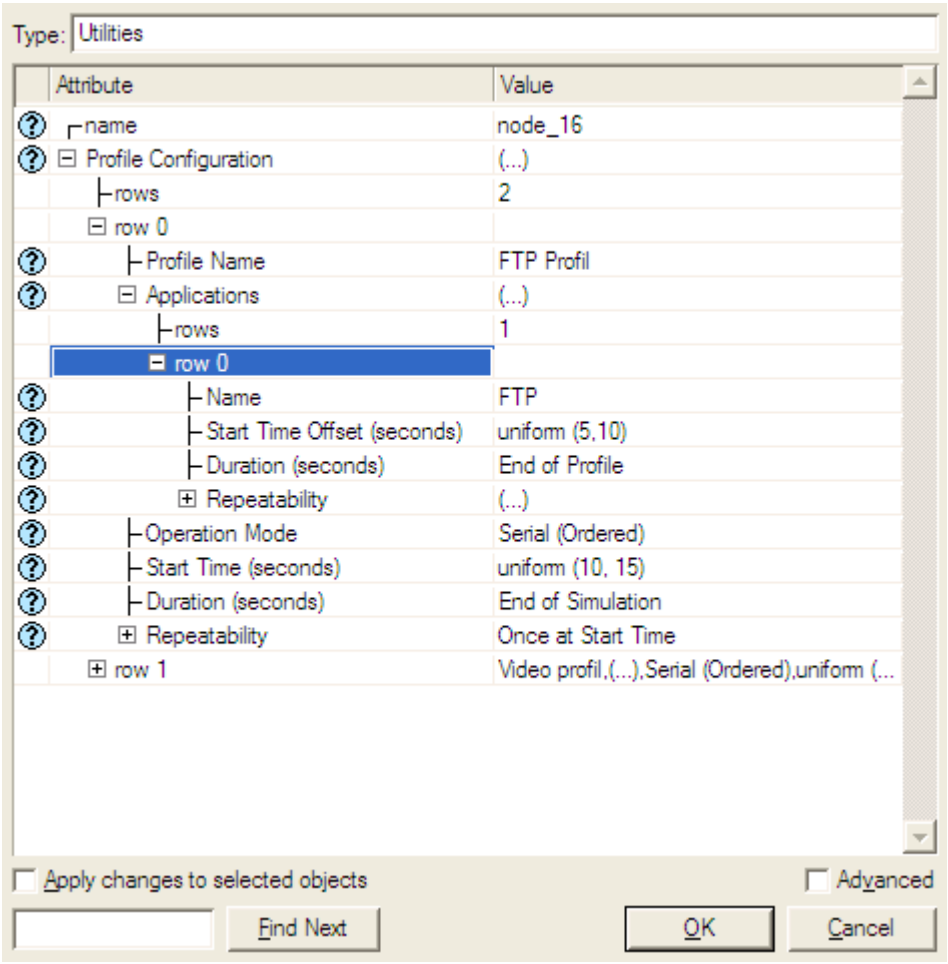
Obr. 10.18: Nastavenie aplikácie pre Video konferenciu

- FTP prenos – Tento typ aplikácie je nastavený aby odosielal každú sekundu FTP dáta. Veľkosť sťahovaného súboru je nastavená na konštantnú 10kBytov. Pomer medzi žiadosťami na stiahnutie súboru a celkovým počtom žiadostí je 100%, teda žiadosti na stiahnutie súboru tvoria celkové množstvo žiadostí.



Obr. 10.19: Nastavenie aplikácie pre FTP prenos

Obe aplikácie majú zhodný profil, teda u oboch aplikácií sa mobilný uzol začína dožadovať prenosu v rovnakú dobu medzi 10 až 15 sekundou od začiatku simulácie a požadovanie o dáta trvá až do konca simulácie. Konfiguráciu profilu je zobrazená nižšie.



Obr. 10.20: Nastavenie profilu

10.1.4 Sledovanie charakteristík

Pred spustením samotnej simulácie musíme nastaviť na žiadaných modeloch sieťových prvkov aké charakteristiky má OM sledovať. V našom prípade to budú:

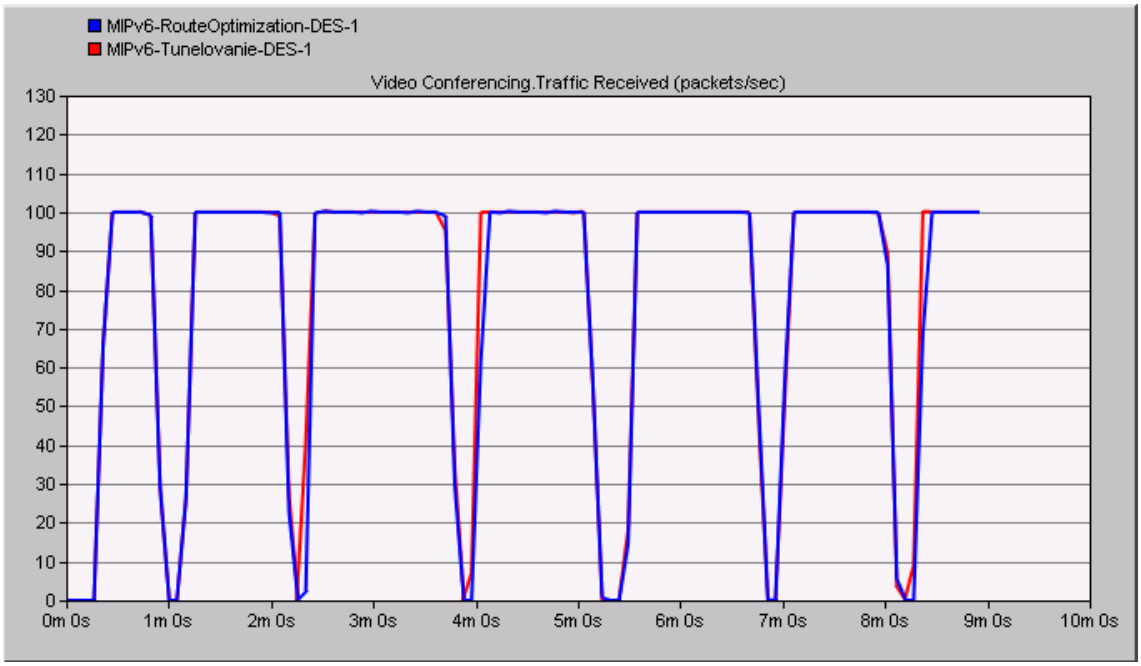
- Wireless Lan
- Mobile IPv6
- Video Conferencing
- Server FTP
- Client FTP

10.1.5 Konfigurácia scenára s použitím Obojsmerného tunelovania

Aby sme mohli porovnať a analyzovať výhody a nevýhody optimalizácie cesty v bezdrôtovej sieti, musíme vytvoriť druhý scenár so zhodnou topológiou siete, zhodnými sieťovými prvkami a taktiež zhodnými definíciami profilov a podporovaných aplikácií v nich použitých. V programe OPNET Modeler toho docielime funkciou duplikovanie scenáru. Vznikne nám druhý scenár totožný s prvým MIPv6_RouteOptimization. Pomenujeme ho MIPv6_Tunelovanie a jedinú zmenu ktorú vykonáme, bude deaktivácia parametru Route Optimization v modele mobilného uzlu MN_1 a v uzloch MIPv6 serverov označených Video_server a FTP_server.

10.2 Všeobecné pozorovania

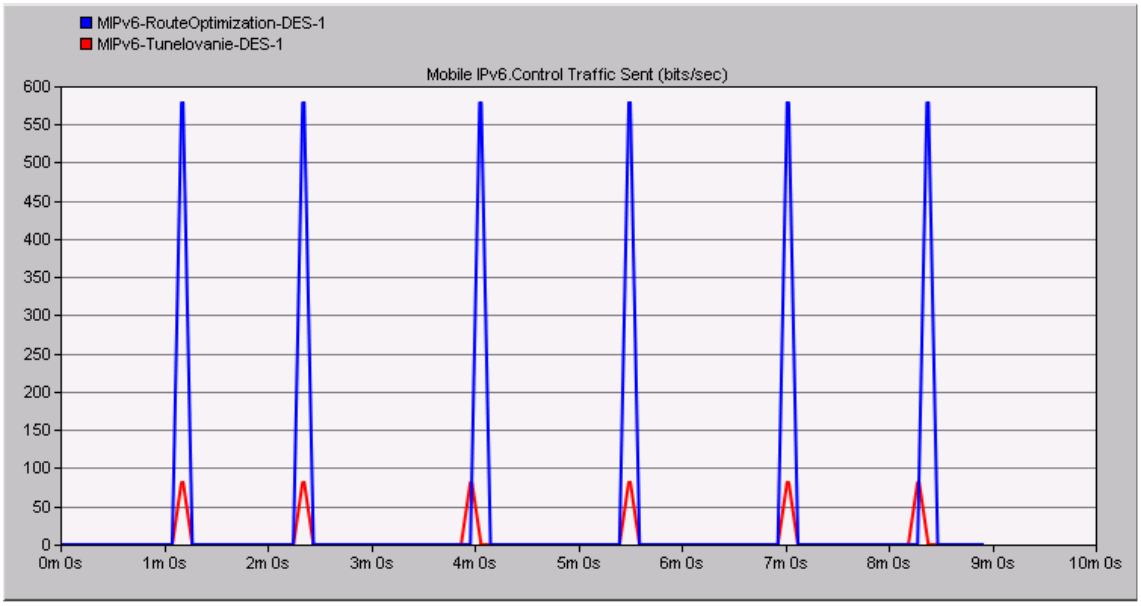
Na grafe zobrazenom nižšie je možné pozorovať prenos dát pri videokonferencii. V grafe sú patrné hlboké priehlbiny. Každá z týchto prihlbín je vytvorená v momente keď MN mení svoju súčasnú podsieť a spustí pritom procedúry registrácie a tvorby väzieb aby informoval svojho HA a CN o novej CoA. Zatiaľčo registračné a väzbové procedúry aktualizujú záznamy u domáceho agenta a korešpondujúceho uzlu celý prenos generovaný aplikáciami a smerovaný ku mobilnému uzlu je prerušený.



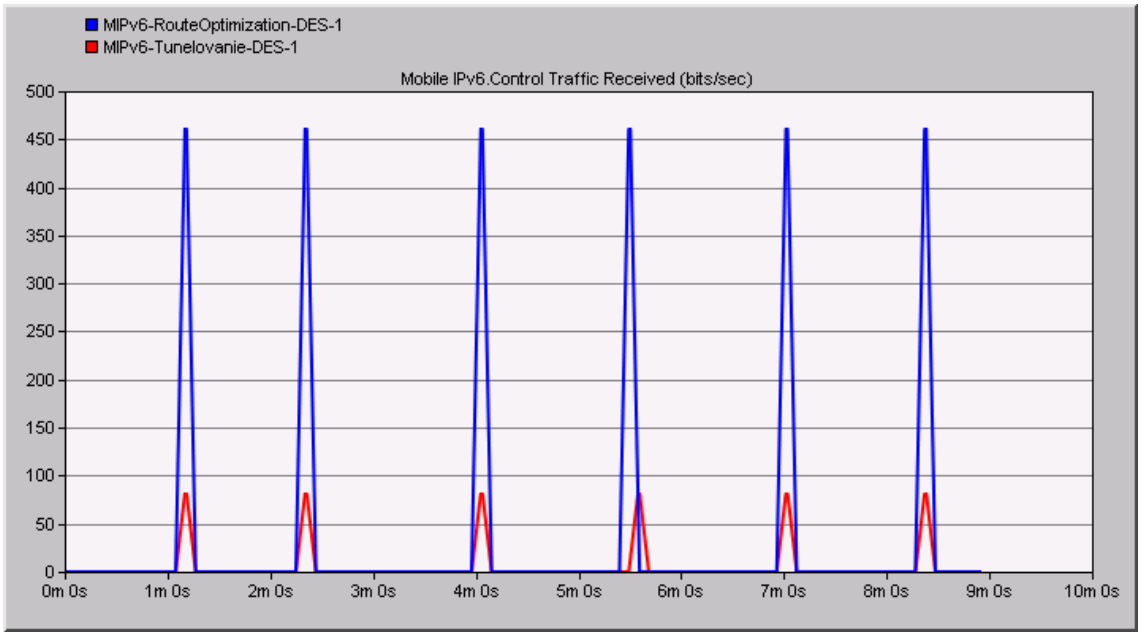
Obr. 10.21: Videokonferenčný prenos prijatý mobilným uzlom MN_1

Kontrolný prenos reprezentuje MIPv6 signalizovanie na mobilnom uzle MN_1. Signalizovanie zahŕňa registračné správy, väzbové správy a iné. V grafe zobrazenom nižšie je kontrolný prenos generovaný MIPv6 správami meraný v bitoch za sekundu. Môžeme vidieť, že kontrolný prenos generovaný optimalizáciou cesty je značne väčší než kontrolný prenos generovaný obojsmerným tunelovaním. Je to tým, že u mechanizmu optimalizácia cesty musí mobilný uzol registrovať nielen CoA

u AR_1_HA ale taktiež aktualizovať väzbu u korešpondujúcich uzlov Video_server a FTP_server. U obojsmerného tunelovania musí mobilný uzol registrovať len CoA u domáceho agenta.

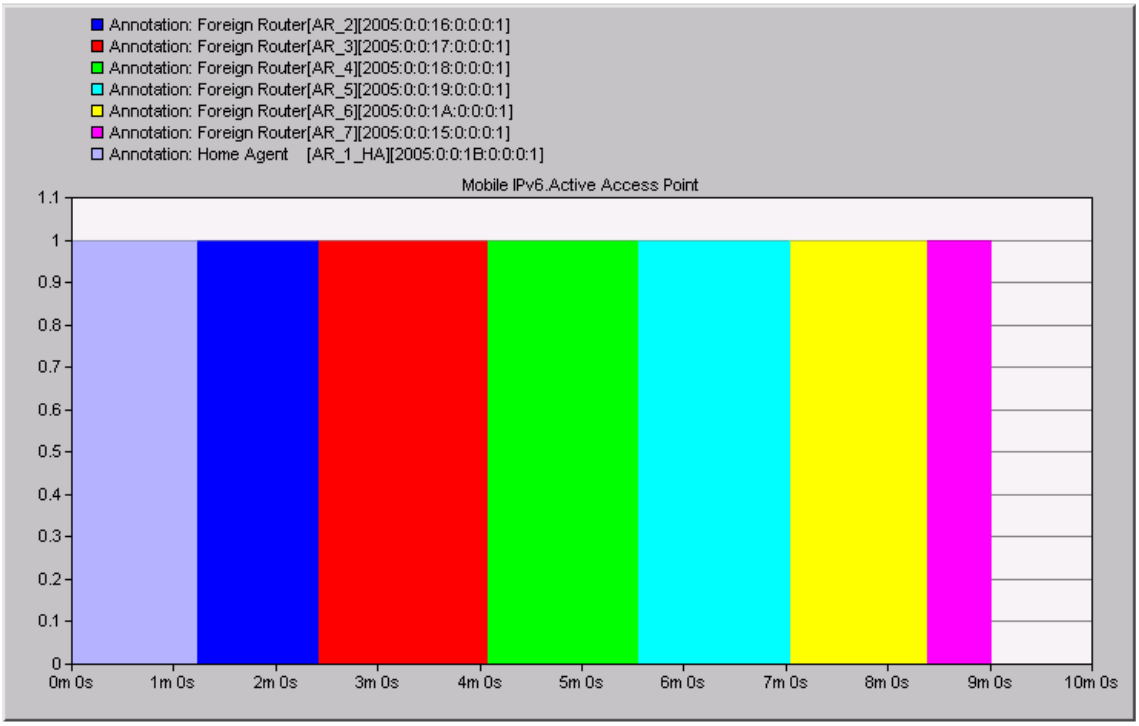


Obr. 10.22: Odoslaný kontrolný prenos z mobilného uzlu



Obr. 10.23: Kontrolný prenos prijatý mobilným uzlom

V nasledujúcom grafe môžeme pozorovať ako pri svojom pohybe MN_1 navštívil rôzne podsiete patriace WLAN smerovačom. Rôzna farba stĺpca identifikuje rôzny bezdrôtový smerovač a šírka stĺpca reprezentuje dobu za ktorú mobilný uzol tento smerovač využíval predtým než nadviazal spojenie z nasledujúcim smerovačom.

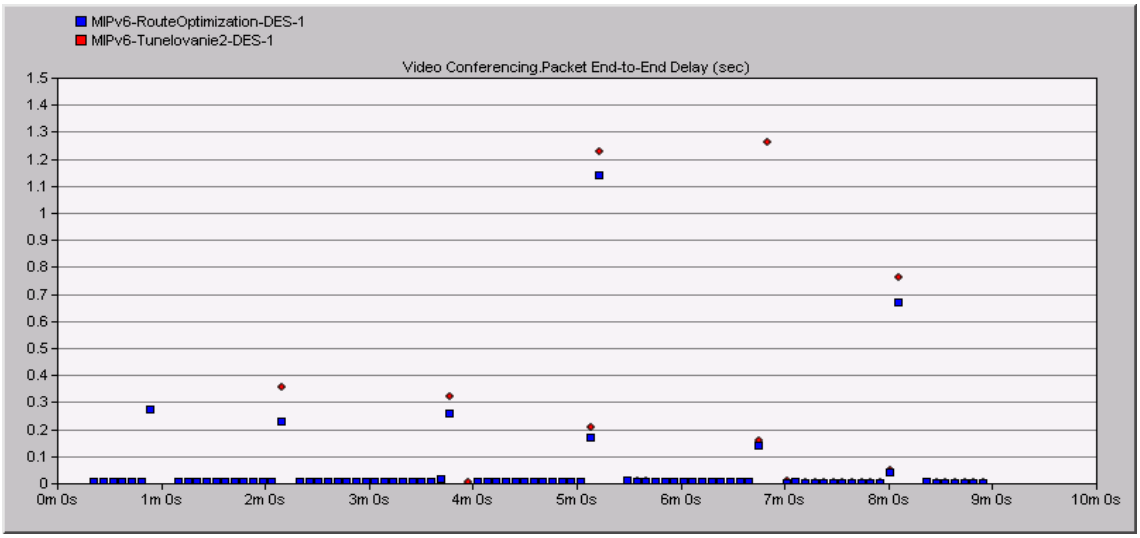


Obr. 10.24: Navštívené AP počas simulácie

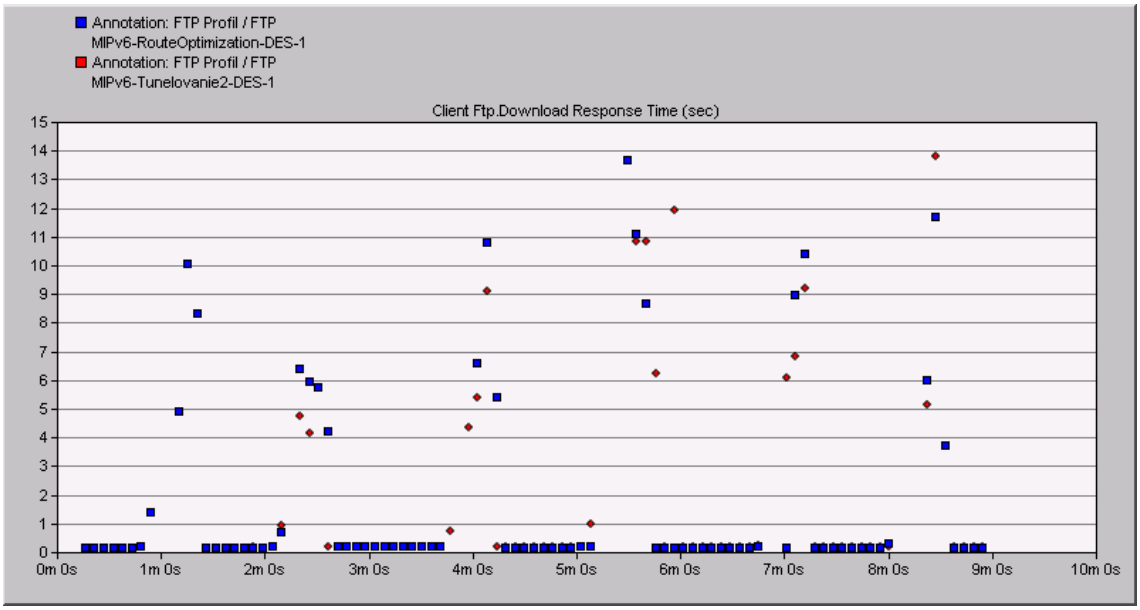
10.3 End-to-end packet delay (doba odozvy) a FTP prenos

- *Doba odozvy pri nulovej záťaži*

Doba, ktorú aplikácia potrebuje na odpoveď požiadavky prenosu je priamo ovplyvnená smerovacími mechanizmami, teda obojsmerným tunelovaním a optimalizáciou cesty. Grafy ukazujú dobu potrebnú na odpoveď pri obojsmernom tunelovaní a pri optimalizácii cesty. Z grafov vidíme, že oneskorenie paketov je pre oba mechanizmy smerovania skoro nulové okrem prípadu keď MN_1 prechádza z jednej podsiete do druhej. Je to dané tým, že v našej sieti sme definovali aplikácie tak, aby vytvorili maximálny prenos v priemere 1,2Mbit za sekundu a smerovače sú prepojené ethernetovým štandardom 100BaseT podporujúcim prenosové rýchlosti až do 100Mbit za sekundu.



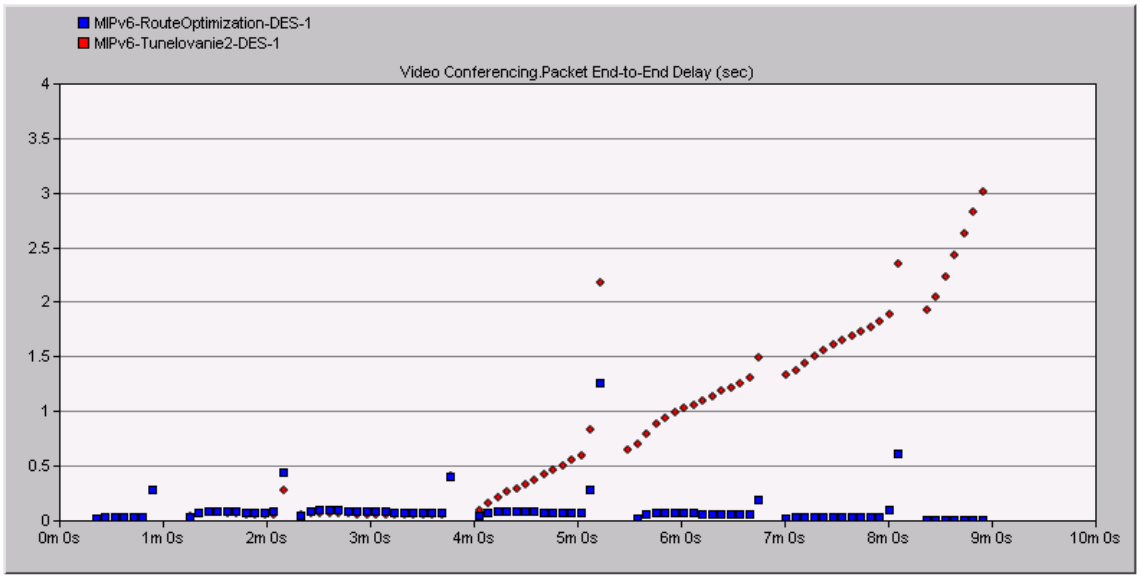
Obr. 10.25: Doba odozvy Video konferenčnej prevádzky s nulovou záťažou



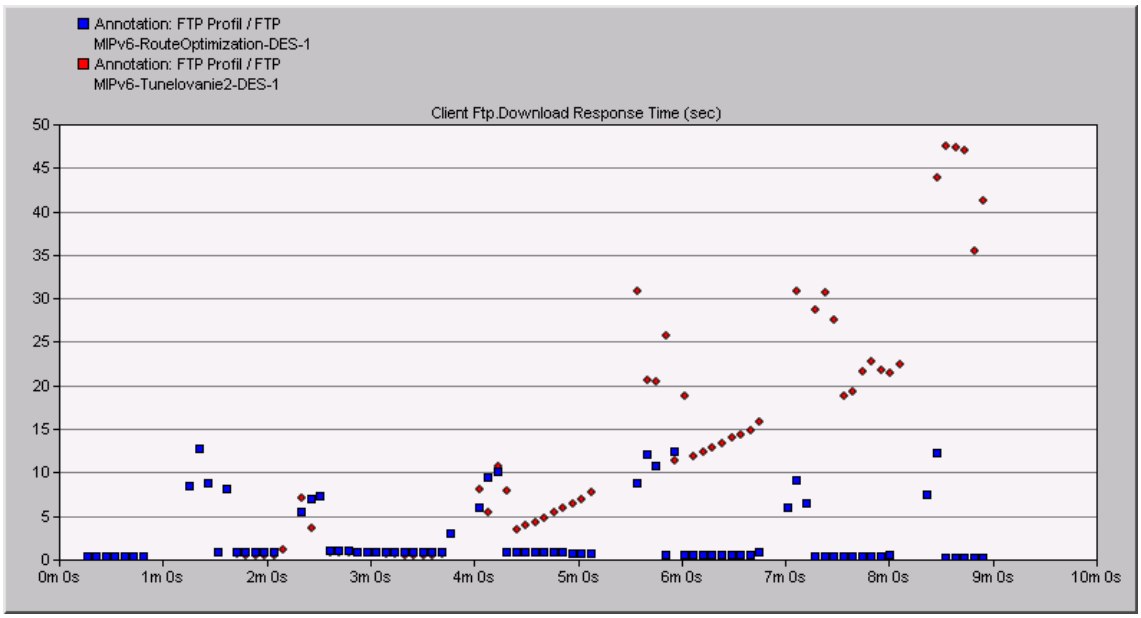
Obr. 10.26: Doba odozvy FTP prevádzky s nulovou záťažou

- *Doba odozvy pri záťažení siete prenosom 99Mbit/s*

Ak chceme analyzovať dopad smerovacieho mechanizmu na oneskorenie paketov medzi komunikujúcimi uzlami v MIPv6 sieti, je potrebné sieť zaťažiť. Pri generovanej prevádzke 1,2Mbit za sekundu zaťažíme sieť prevádzkou 99Mbit za sekundu. Ako je patrné z grafov, oneskorenie paketov už nemá charakteristiku ako v prípade bez záťaže. Pri obojsmernom tunelovaní dochádza k viditeľnému oneskoreniu paketov zatiaľ čo pri mechanizme optimalizácia cesty je oneskorenie skoro v každom bode merania nulové. Je to dané tým, že pri použití optimalizácie cesty komunikujú mobilný uzol MN_1 a korešpondujúce uzly Video_server a FTP_server použitím najkratšej komunikačnej cesty zatiaľ čo pri obojsmernom tunelovaní je každý paket tunelovaný domácemu agentovi a z domácej siete korešpondujúcim uzlom. To vytvára oneskorenie.



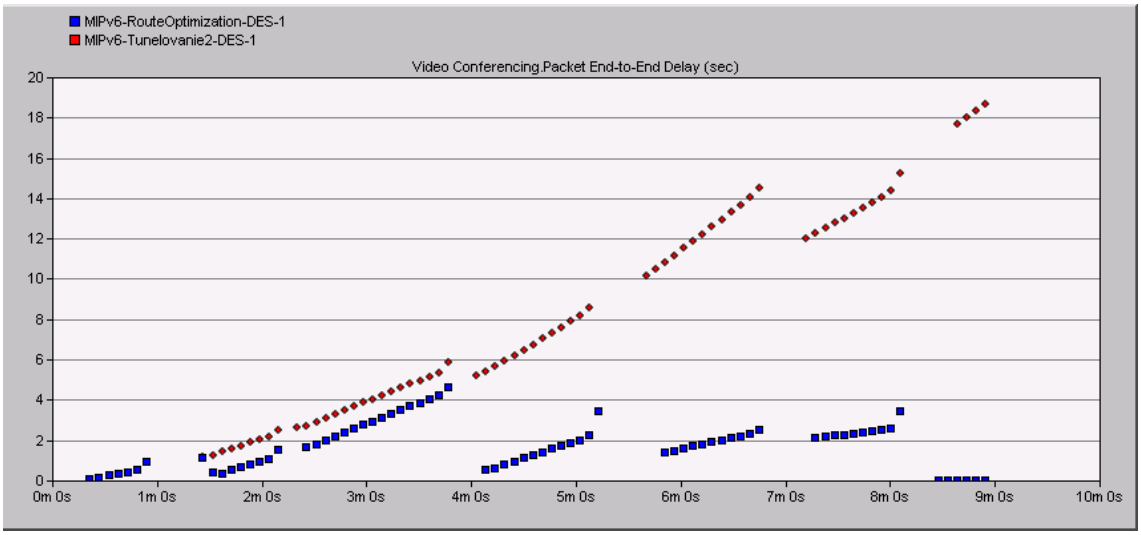
Obr. 10.27: Doba odozvy Video konferenčnej prevádzky pri zaťažení siete prenosom 99Mbit/s



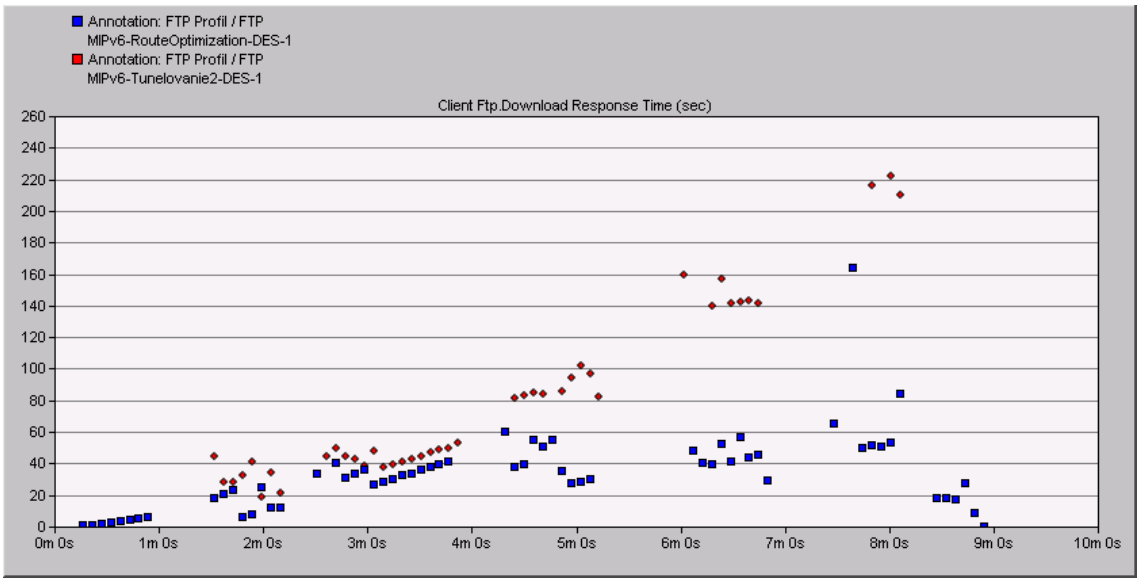
Obr. 10.28: Doba odozvy FTP prevádzky pri zaťažení siete prenosom 99Mbit/s

- *Doba odozvy pri zaťažení siete prenosom 99,9Mbit/s*

Aby sme zistili aký dopad ma veľkosť zaťaženia siete na efektivitu smerovania pri optimalizácii cesty, zaťažíme sieť prevádzkou 99,9Mbit za sekundu. Pri takomto veľkom zaťažení je na našu komunikáciu (Video konferencia, FTP prenos) vyhradená teoretická šírka pásma len 0,1Mbit. Aj pri takto veľmi vyťaženej sieti si komunikujúce uzly používajúce optimalizáciu cesty zachovávajú prijateľnú hodnotu oneskorenia. To sa však nedá povedať o tunelovaných paketoch, kde oneskorenie dosahuje až 18 a viac sekúnd pri video konferencii a dvesto sekúnd pri FTP prenose.



Obr. 10.29: Doba odozvy Video konferenčnej prevádzky pri zaťažení siete prenosom 99,9Mbit/s



Obr. 10.30: Doba odozvy FTP prevádzky pri zaťažení siete prenosom 99,9Mbit/s

Z uvedených nameraných charakteristík oneskorenia paketov pri video konferencii a doby odozvy pri FTP prenose je jasné, aký významný dopad má optimalizácia cesty na efektívne smerovanie vo vyťažených Mobilných IPv6 sieťach s veľkým počtom sieťových prvkov medzi komunikujúcim mobilným uzlom a korešpondujúcim uzlom. Mnou navrhnutá simulácia a dosiahnuté výsledky demonštrujú modelovanie reálnych IPv6 sietí a taktiež ponúkajú prehľad o vplyve MIPv6 protokolov na prenos generovaný aplikáciami.

11. Záver

Cieľom tejto bakalárskej práce „Vlastnosti a použitie protokolov IPv6 a MIPv6“ bolo získať potrebné vedomosti z problematiky vlastností protokolov IPv6 a MIPv6.

Je zjavné, že protokol IPv6 prináša plno pozitívnych zmien oproti stávajúcim mechanizmom v adresovaní v Internete. Funkcie ako Neighbour Discovery a Automatická konfigurácia sa nesú v duchu *Plug and Play*, čo pridáva plno výhod pri interakcii s koncovým zákazníkom. Ďalšou výhodou je obrovský adresný priestor a systém IPv6 hlavičiek. Čo sa týka bezpečnosti a podpory mobility, prináša IPv6 množstvo prevratných zmien. Hlavne kapitola o podpore mobility a protokole MIPv6 je veľmi obsiahla. Hlavne zo súčasným rozmachom mobilných zariadení čoraz viac využívajúcich pripojenie na Internet je mobilita horúcou témou. V mojej práci som sa oboznámil hlavne so spôsobom smerovania paketov koncovým uzlom ako aj s autentifikáciou a zabezpečením dát.

V programe OM som simuloval dve siete podporujúce protokol MIPv6 a porovnával efektivitu smerovania za použitia mechanizmu Obojsmerného tunelovania a Optimalizácie cesty. Z dosiahnutých výsledkov je zrejmé, že smerovanie s použitím Optimalizácie cesty je efektívnejšie ako smerovanie s Obojsmerným tunelovaním.

Protokol IPv6 je v skutku Internetovým protokolom nadchádzajúcej generácie a súčasný stav jeho vývoja a implementácie do svetových sietí môže znamenať, že o pár rokov bude celý Internet ako ho poznáme komunikovať vďaka tomuto protokolu.

Zoznam použitej literatúry.

[1] SATRAPA, Pavel. IPv6 - Internet Protokol verze 6, Praha : Neocortex, 2002 -- 238 s. : ISBN: 80-86330-10-9

[2] OPNET Technologies, Inc OPNET Modeler Release 12 Produst documentation, 2006

[3] Ing.MOLNÁR, Karol, Ph.D., Bc.ZEMAN, Otto, Moderní síťové technologie – laboratorní cvičení, VUT v Brně, FET, Ústav TLKM, 2006.

[4] PETRENEC, Stanislav – Internetový protokol verzia 6,: vzdelávací modul http://fubu.yweb.sk/ipv6/format_dat.htm

[5] 2003 OPNET Technologies, IPv6 Modeling in OPNET

[6] Johnson, D., Perkins, C.E., Arkko, J.: Mobility Support in IPv6. RFC 3775, http://www.ietf.org/rfc/rfc3775.txt (2004)

[7]Conta, A., Deering, S.: Generic Packet Tunneling in IPv6 Specification. RFC 2473, http://www.ietf.org/rfc/rfc2473.txt (1998)

[8] Deering, S., Hinden, R.: Internet Protocol Version 6 (IPv6) Specification. RFC 2460, http://www.ietf.org/rfc/rfc2460.txt (1998)

[9]RAAB, Stefan. Cisco: Mobilní IP technologie a aplikace, Grada, 2007, 299 s., ISBN: 978-80-247-1611-4

[10]Deering, S., Hinden, R.: Internet Protocol Version 6 Addressing Architecture. RFC 3513, http://www.ietf.org/rfc/rfc3513.txt (2003)