Slovenská technická univerzita v Bratislave

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

# Bezpečnosť v IPv6

Roman Panenka

Študijný program: Počítačové komunikačné systémy a siete

Ročník: Ing. 1

Predmet: Bezpečnosť v Internete

Ak. rok: 2010/11

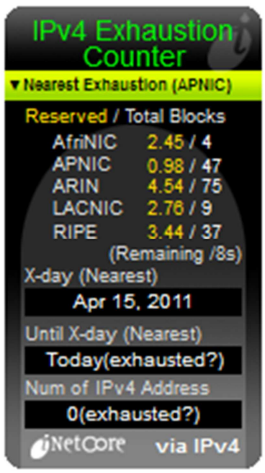
# OBSAH


1. Úvod do problematiky ... 1
2. Vlastnosti a prínos sieťového protokolu IPv6 ... 3
   2.1. Základný opis IPv6 ... 3
   2.2. Datagram v IPv6 ... 4
   2.3. Adresy v IPv6 ... 5
3. Bezpečnostné prvky IPsec ... 7
   3.1. Autentizačné a šifrovacie protokoly ... 7
4. Bezpečnostné problémy pretrvávajúce z IPv4 ... 8
   4.1. Autokonfigurácia ... 8
   4.2. Hľadanie susedov ... 9
   4.3. Detekcia duplikátnych adries ... 9
   4.4. Presmerovanie komunikácie ... 9
   4.5. Ochrana ICMPv6 ... 10
5. Rozširujúce hlavičky ... 11
   5.1. Rozširujúca smerovacia hlavička ... 12
   5.2. Fragmentačná hlavička ... 12
   5.3. Filtrovanie rozširujúcich hlavičiek ... 14
6. Otázky bezpečnosti pri mobilite IP ... 15
   6.1. Formát správ ... 17
   6.2. Bezpečnosť MIPv6 ... 17
   - Podvrhnutý domáci agent ... 17
   - Prelomenie prístupovej vrstvy ... 17
   - Útoky typu man-in-the-middle ... 17
   - Odchytenie komunikácie ... 18
   - Podvrhnutie aktualizácie väzby ... 18
7. Bezpečnosť koncových používateľov ... 19
   7.1. Pripojenie domácich sietí ... 19
   7.2. Nové otázky bezpečnosti ... 19
8. Zhodnotenie problematiky ... 21
9. Zoznam použitej literatúry ... 22

# 1. ÚVOD DO PROBLEMATIKY

Sieťový protokol Internet Protocol verzie 6 (IPv6) sa má stať nasledovníkom súčasného nosného protokolu celého internetu, ktorým je Internet Protocol verzie 4 (IPv4). V niektorých starších literatúrach býva tiež nazývaný ako IP Next Generation (IPng) [1].

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. Na začiatku februára 2011 vyhlásila organizácia IANA[1] vyhlásila minutie všetkých nealokovaných adresných priestorov. Ku dňu 9.5.2011 vo svojej správe [2] predpovedá minutie adresného priestoru IPv4 na úrovni regionálnych poskytovateľov (RIRs) na august roku 2011. Najbližšie minutie adresného priestoru sa predpovedá pre región Asia Pacific(APNIC), ako zobrazuje Obrázok 1 .




**Obrázok 1 - minutie adresného priestoru IPv4 u regionálnych poskytovateľov**

Nakoľko na riešenie tohto problému bolo k dispozícií pomerne veľa času, rozhodlo sa IETF[2] navrhnúť zásadnejšiu zmenu na poly Internetu. Táto navrhovaná zmena v podobe verzie 6 protokolu IP okrem rozšíreného adresného protokolu prináša mnoho ďalších výhod (výhody sú opísané v kapitole *2.1 Základný opis IPv6*)

Samotný vývoj a implementácia nového protokolu verzie 6 do reálneho sveta boli však sprevádzané mnohými prekážkami a verejnými diskusiami pri vydaní každej novej RFC správy, čo spôsobovalo pomalý vývoj niektorých špecifikácii. Pribrzdenie praktického nasadenia protokolu bolo spôsobené hlavne prechodom k smerovaniu na základe sieťovej masky (classless routing) a vznikom mechanizmu prekladu adries a portov (NAT, network address translation).

---

[1] IANA (Internet Assigned Numbers Authority - www.iana.org) – organizácia zodpovedná za globálnu koordináciu adresovania IP, správu koreňových DNS a ďalších internetových protokolov

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

IPv6 je stále do veľkej miery neistou pôdou pre mnohé spoločnosti a okrem mnohých výhod nesie zo sebou aj niekoľko nevýhod, preto sa mnohé organizácie snažili radšej pokračovať vo vývoji IPv4. Medzi tieto nevýhody bezpochyby patrí spätná nekompatibilita so staršími protokolmi, stav v akom sa mnohé protokoly a implementácie nachádzajú a takisto oblasť bezpečnosti, ktorá sa príliš často odvoláva na bezpečnostné mechanizmy IPsec.

IPv6 sa teda ocitá v blúdnom kruhu, kde používatelia oň nemajú záujem, 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 [1]. V poslednej dobe je snaha prispieť k tejto problematike aj politicky, o čom svedčia smelé plány mnohých krajín ako napr. USA, EÚ, Čína, Kórea, Austrália. Vláda Slovenskej Republiky sa tejto problematike venuje vo svojom operačnom programe Informatizácia spoločnosti[3]. O nasadenie IPv6 sa snažia aj rôzne verejné iniciatívy, ako napr. *IPv6 day* – 8 jún 2011. Každopádne, IPv6 je zaujímavý a nádejný protokol, mnohými považovaný za jedinú možnosť budúcnosti internetu.

[3] OPIS (Operačný program Informatizácia spoločnosti) je referenčný dokument, na základe ktorého bude poskytovaná podpora na všetky projekty informatizácie spoločnosti, podporované zo štrukturálnych fondov. Viac informácií http://www.informatizacia.sk/prechod-z-ipv4-na-ipv6

# 2. VLASTNOSTI A PRÍNOS SIEŤOVÉHO PROTOKOLU IPV6

## 2.1. Základný opis IPv6

Ako už bolo spomenuté vyššie, 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 $3.4\times10^{38}$ (340 sextiliónov) adries. To je približne $4.3\times10^{20}$ (430 triliónov) adries na štvorcový palec zemského povrchu [3].

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

- ✓ Jednotná adresná schéma pre Internet aj vnútorné siete
- ✓ tri druhy adries – unicast, multicast, anycast
- ✓ zavedenie rozširujúcich hlavičiek
- ✓ zvýšenie bezpečnosti komunikácie zahrnutím mechanizmov IPsec
- ✓ podpora pre jumbogramy – pakety prevyšujúce štandardnú veľkosť MTU
- ✓ fragmentovanie iba na koncových uzloch komunikácie
- ✓ automatická konfigurácia siete
- ✓ podpora pre služby zo zaistenou kvalitou
- ✓ podpora mobility (pre prenosné počítače a mobilné zariadenia )
- ✓ hladký a plynulý prechod z IPv4

Z nesporných výhod IPv6 oproti IPv4 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
- ✓ optimalizácia pre vysokorýchlostné smerovanie

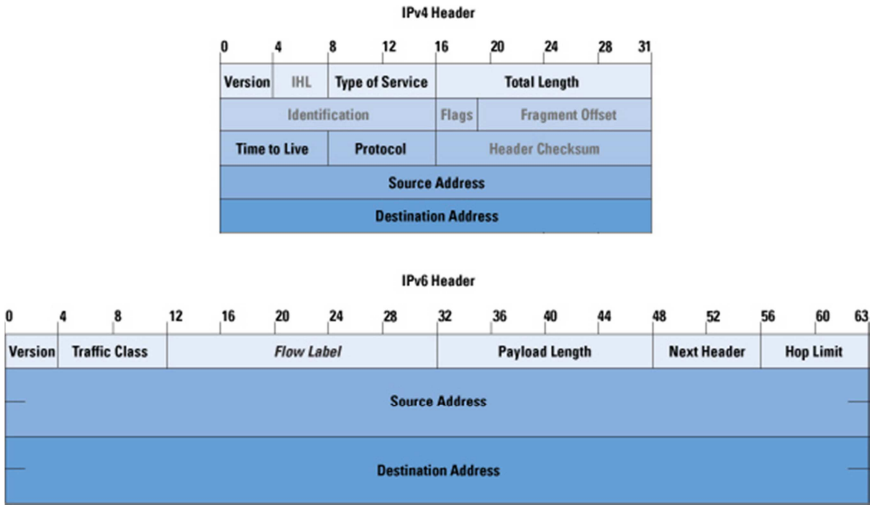
Súčasné nevýhody IPv6 oproti IPv4:

- × Nekompatibilita so starou verziou protokolu, ktorá sa dá ale úspešne riešiť protokolmi na koexistenciu oboch protokolov v sieti
- × Súčasný stav špecifikácií a jednotlivých implementácií
- × Prehnané odkazovanie bezpečnosti IPv6 na mechanizmy IPsec
- × Časté využívanie IPv6 na hľadanie zadných vrátok do infraštruktúry nových sietí

## 2.2. 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 IPv4 pola životnosť datagramu (TTL). Určuje koľko skokov môže datagram po sieti 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 2.3 *Adresy v IPv6.*
-

## 2.3. 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 (anycast):

- 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 [4]:

| | |
|---|---|
| ::1/128 | lokálna adresa – loopback adresa |
| fc00::/7 | unikátne individuálne lokálne – platnosť iba v lokálnej sieti, vytvorené na základe MAC adresy – zaistenie takmer svetovej unikátnosti |
| fe80::/10 | linkové individuálne lokálne - platnosť iba v sieťovom segmente |
| ff00::/8 | skupinové adresy – adresy multicastu |
| *2000::/3* | ostatné, individuálne globálne |

# 3. BEZPEČNOSTNÉ PRVKY IPSEC

Paradoxne sa dostávame do stavu, kedy sa nový IP protokol verzie 6 nepoužíva k tomu, k čomu bol primárne určený (teda ku komunikácií sieťových uzlov). Na mnohých miestach a sieťach vytvára akési zadné dvierka umožňujúce ľahký vstup do sieťovej infraštruktúry. Takisto treba myslieť na skutočnosť, že IPv6 neohrozuje iba samotnú IPv6 infraštruktúru, ale taktiež môže výrazným spôsobom ovplyvniť chod už existujúcich IPv4 zariadení a služieb. Existenciu a implementáciu IPv6 netreba teda brať na ľahkú váhu. Jednoduchá ignorácia bezpečnostných aspektov môže pomerne zásadným spôsobom ohroziť ako samotný chod siete, tak aj chod prevádzkovaných služieb.

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 v sieťach vznikať rôzne softvérové a hardvérové bezpečnostné mechanizmy. 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

## 3.1. Autentizačné a šifrovacie protokoly

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**

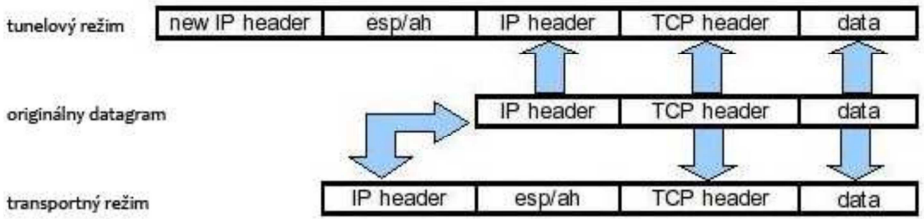
Autentifikačná hlavička (Authentication Header, AH) má na starosti autentifikáciu datagramu, čiže ako som už vyššie písal, overenie pravosti adries a obsahu.

**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 [1]. Pre IPsec existujú dva režimy ochrany (znázornené tiež na obrázku Obrázok 3):

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 3 - režimy ochrany v IPsec**

# 4. BEZPEČNOSTNÉ PROBLÉMY PRETRVÁVAJÚCE Z IPV4

## 4.1. Autokonfigurácia

Bezstavová konfigurácia klientov (SLAAC, Stateless Address Autoconfiguration, RFC 2462) je zmenou oproti prideľovaniu IP adries klientom vo svete IPv4, kde boli adresy priraďované manuálne alebo centrálnou autoritou (napr. DHCP server). Je súčasťou špecifikácie vyhľadávania susedov (Neighbor Discovery for IP Version 6, RFC 2461) V IPv6 smerovač informuje v pravidelných intervaloch všetky pripojené uzly v sieťovom segmente, v akej sieti sa nachádzajú a ktorý smerovač majú použiť, pre pakety smerované mimo siete. Oznamovanie sa vykonáva RA (Router advertisement) oznamovacími správami. Aby bola konfigurácia pružnejšia, klienti si môžu túto konfiguráciu vyžiadať cez RS (Router solicitation) požiadavky. Všetka komunikácia prebieha s využitím protokolu ICMPv6. Odpadá nám teda nutnosť konfigurovania DHCP servera, definovania DHCP pool-ov a DHCP relay.

Keďže v SLAAC nie je zabudovaný žiadny mechanizmus autentifikácie správ, potenciálny útočník môže rozposielať podvrhnuté oznamovacie správy RA a tak sa tváriť ako východzia brána (default gateway) siete. To spôsobí, že všetka komunikácia koncových uzlov smerovaná von zo siete bude smerovaná cez útočníkov počítač. IPv6 konfigurácia je infikovaná hneď po prijatí RA aktualizácie. Útočník môže túto komunikáciu ďalej analyzovať a transparentne preposielať na skutočná bránu (man-in-the-middle útok) alebo pakety zahadzovať (denial-of-service útok).

Tento typ útoku (ako aj ďalšie v tejto kapitole) sa zakladá na podobných princípoch ako ARP spoofing v IPv4.

## 4.2. Hľadanie susedov

IPv6 už pri hľadaní adries susedov nepoužíva protokol ARP (ako to bolo pri IPv4), no používa protokol hľadania susedov (NDP, Neigbor discovery protocol). NDP protokol komunikuje nad ICMPv6 protokolom a v podstate zachováva pôvodný mechanizmus ARP [5]:

1. Zariadenie pošle Neighbor Solicitation (NS) správu ako multicast smerovanú na všetky dostupné uzly na druhej vrstve. NS používa ICMPv6 správu typu 135 a jej obsah tvorí cieľovú / hľadanú adresu.

2. Koncové zariadenie odpovie správou Neighbor Advertisement (NA) používajúc ICMPv6 správu typu 136. Obsahom správy je jeho MAC adresa.

Správy NS a NA žiadnym spôsobom neautentifikujú zdrojový a cieľový uzol. Pre útočníkova sa teda znova otvára možnosť ARP Spoofing útoku, kedy zdroju odpovedá podvrhnutými NA správami a tak je chybne identifikovaný ako hľadaný uzol.

## 4.3. Detekcia duplikátnych adries

Aby sa predchádzalo duplikátnym IP adresám na jednej sieti, IPv6 zavádza mechanizmus, ktorým uzol kontroluje existenciu jeho novej IP adresy v sieti. Detekcia duplikátnych adries (DAD, Duplicate address detection) funguje na princípe rozposielania Neighbor Solicitation (NS) správ, ktoré som opisoval v predchádzajúcej podkapitole. Ak uzol dostane NA odpoveď, znamená to, že v sieti už existuje uzol s takou IP adresou.

Keďže sa DAD spolieha na mechanizmy NDP neobsahujúce žiadnu autentifikáciu, je jednoduché pre útočníka vykonať denial-of-service útok maskovaním sa za všetky IP adresy na sieti.

## 4.4. Presmerovanie komunikácie

Presmerovanie komunikácie je vďačný mechanizmus využívajúci ICMPv6, ktorý umožňuje smerovačom signalizovať zdrojovým uzlom kratšiu cestu do cieľovej siete. Ak chce napríklad uzol A kontaktovať sieť netB, odošle paket na svoju východziu bránu - smerovač R1. Tá podľa svojej smerovacej tabuľky zistí, že sieť netB je lepšie dosiahnuteľná cez smerovač R2. Okamžite toto zistenie ohlási zdrojovému uzlu prostredníctvom ICMPv6 redirect správy. Uzol si zmení svoju internú smerovaciu tabuľku a ďalšiu komunikáciu do siete netB posiela priamo bližšiemu smerovaču R2.

Znova, ani tu neexistuje žiadny autentifikačný mechanizmus, a preto môžu byť správy presmerovania podvrhnuté. ICMPv6 redirect správy majú aspoň jednoduchý ochranný mechanizmus – kópia paketu spôsobujúceho presmerovanie musí byť vložená do ICMPv6 redirect správy. Útočník teda nemôže priamo posielať správy presmerovania.

Spomenutý mechanizmus sa dá ale obísť nasledovným spôsobom [5]:

1. Útočník pošle obeti ICMPv6 echo požiadavku zo zmenenou zdrojovou MAC adresou, povedzme 2001:6666:2::1 .

2. Obeť pošle ako odpoveď ICMPv6 reply správu na podvrhnutú adresu 2001:6666:2::1. Útočník tiež vie (vie si domyslieť) ako bude táto správa vyzerať.

3. Útočník pošle obeti ICMPv6 redirect správu zo znova podvrhnutou zdrojovou adresou s priloženou kópiou domyslenej ICMPv6 reply správy z kroku 2. Táto správa obsahuje tiež adresu nového cieľového smerovača.

## 4.5. Ochrana ICMPv6

Slabá ochrana správ ICMPv6 je priam lákadlom pre najrôznejšie typy útokov. Napríklad dobre premyslený zásah do procesu autokonfigurácie môže podvrhnutím odpovede útočníkovi umožniť presmerovať celú cudziu komunikáciu cez svoj počítač alebo mu podvrhnúť adresy rekurzívnych DNS serverov. Viaceré útoky sú známe aj zo sveta IPv4, a preto existovalo niekoľko mechanizmov znemožňujúcich alebo aspoň obmedzujúcich tieto útoky:

- **DHCP Snooping –** na prepínačoch sa definujú dôveryhodné porty, cez ktoré môžu prechádzať DHCP odpovede servera. Prípadný DHCP server na počítači útočníka tak nemôže ohrozovať ostatných klientov podvrhnutými DHCP správami. Na poly IPv6 existuje podobná ochrana pod názvom RA Guard, ktorá kontroluje správy Router Advertisement.

- **Dynamic ARP inspection –** z DHCP komunikácie sa prepínač naučí na dvojicu MAC adresa – IP adresa a tú kontroluje v ARP odpovediach.

- **Dynamic IP Lockdown -** naučená dvojica IP – MAC je kontrolovaná v paketoch na portoch prepínača. Takisto nedovoľuje klientom komunikovať pokiaľ si nevyžiadajú IP adresu z DHCP servera.

Podobné princípy sa dajú presadiť aj na poly IPv6. Nové mechanizmy spomínané v tejto kapitole (SLAAC, NDP, DAD) majú veľmi slabé zabudované ochranné mechanizmy:

- Zdrojové adresy musia byť linkové lokálne alebo nešpecifikované adresy (::/128) pre RA a NS správy

- Skokový limit (hop limit) musí byť 255 – maximálna hodnota

Tieto mechanizmy sú z bezpečnostného hľadiska nedostačujúce a preto organizácia IETF špecifikovala bezpečnostné vylepšenie **SEND** (SEcure Neighbor Discovery, RFC 3971). Vo svojej funkcionalite využíva kryptograficky generované adresy (CGA, Cryptographically Generated Addresses, RFC 3972) .

SEND pre svoju funkčnosť nevyžaduje podporu na úrovni aktívnych prvkov siete. Overenie pravosti sa vykonáva až na koncovom uzle prostredníctvom certifikátu správy. IPv6 adresa uzla je daná výsledkom kryptografickej funkcie (ďalšia autokonfiguračná funkcia). Použitie SENDu teda úplne vylučuje používanie klasických EUI 64 adries. Medzi ďalšie vlastnosti patrí:

- Riešenie bezpečnostnej problematiky autokonfigurácie a ostatných problémov v NDP
- Nezávislosť na sieťovej infraštruktúre
- Vyžaduje podporu infraštruktúry verejného kľúča podľa X 509 a nainštalovaný certifikát autority, ktorá vydáva certifikáty pre smerovače.

# 5. ROZŠIRUJÚCE HLAVIČKY

Jednou z najvýznamnejších zmien nového protokolu sú rozširujúce hlavičky. Rozširujúce hlavičky obohacujú funkcionality IPv6 paketov na sieťovej vrstve. Pridávajú možnosti fragmentácie, mobility, vlastného smerovania, bezpečnosti a pod. Nasledujú hneď za štandardnou IPv6 hlavičkou kde ich môže byť zreťazených aj viac za sebou. Pole nextHeader v IPv6 hlavičke (na rozdiel od IPv4) určuje typ nasledujúcej hlavičky, resp. hlavičku vyššieho transportného protokolu. Ich poradie a pravidlá radenia sú definované v RFC 2460. Je teda dôležité spomenúť, že pri použití viacerých rozširujúcich hlavičiek musí byť dodržané nasledovné poradie:

1. IPv6 hlavička
2. Hlavička Hop-by-hop možností na jednotlivých uzloch
3. Hlavička možností spracovávaná koncovým uzlom
4. Smerovacia hlavička
5. Hlavička fragmentácie
6. Autentifikačná hlavička
7. ESP bezpečnostná hlavička
8. Hlavička ďalších možností spracovávaná koncovým uzlom
9. Hlavička vyššieho transportného protokolu

## 5.1. Rozširujúca smerovacia hlavička

Štandard RFC 2460 hovorí, že každý uzol v sietí musí vedieť prijímať a preposielať pakety s rozširujúcou smerovacou hlavičkou. Momentálne poznáme dva typy smerovacích hlavičiek:

- **RH0** – podobné konceptu zdrojového smerovania z IPv4 (source routing)

- **RH2** – potrebná pre fungovanie IPv6 mobility. Tejto hlavička sa viac venujem v sekcií **XXX**

Pri použití RH0 hlavičky je možné paketu predpísať cestu, po ktorej má sieťou ísť. Na každom definovanom uzle sa cieľová adresa IPv6 hlavičky mení. Preto je filtrovanie takejto komunikácie zložité a filtrovanie podľa cieľovej adresy je nedostatočné.

RH0 hlavička sa dá zneužiť známym útokom už zo sveta IPv4, kde to bol obľúbený tip útokov. Podstata útoku sa opiera o základný mechanizmus smerovacích hlavičiek – hop-by-hop smerovania. Útočník môže teda svoj paket smerovať na niektorý z dôveryhodných uzlov v sieti (napríklad uzol v demilitarizovanej zóne) , kde sa paket bez obmedzenia presmeruje do vnútornej siete k žiadanému cieľu. Ďalšou možnosťou útoku je zahlcovanie dôležitých sieťových liniek. Pri vhodnom predpísaní smerovacích adries v smerovacej hlavičke je možné docieliť cyklické preposielanie paketu medzi dvoma linkami a tak ju postupne zahltiť. Po určitom počte cyklov a správnom načasovaní všetkých paketov môžu byť pakety presmerované k cieľovému uzlu, pričom vzniká distribuovaný DOS útok.

**Protiopatrenia:**

Po dlhých diskusiách sa organizácia IETF v decembri roku 2007 rozhodla zavrhnúť používanie RH0 smerovacích hlavičiek – RFC 5095. Znamená to, že vo všetkých nových implementáciách protokolu by sa táto zraniteľnosť nemala vyskytovať. Hrozba však stále pretrváva pri starších systémoch. Spoločnosť Cisco ponúka na svojich zariadeniach možnosť filtrovania paketov zo smerovacou hlavičkou. Táto možnosť bola výhodná pri IPv4, no pri IPv6 je obmedzujúca, keďže sú blokované aj pakety s RH2 smerovacou hlavičkou pre mobilitu. Preto bola pridaná možnosť filtrovania podľa typu smerovacej hlavičky.

## 5.2. Fragmentačná hlavička

**Fragmentácia** je proces rozdeľovania veľkých IP paketov na menšie, aby bolo možné smerovať veľké pakety aj v sieťach s nízkou hodnotou MTU (Maximum Transmission Unit). Pri IPv4 mohla nastať fragmentácia v ktorejkoľvek časti siete. Ak je teda prijatý veľký paket na rozhraní A smerovača a rozhranie B malo nižšiu hodnotu MTU, musí nastať fragmentácia. Každý fragment má pridelený unikátny identifikátor a ofset (offset), vyjadrujúci vzdialenosť fragmentu od začiatku celého paketu. Koncový uzol po prijatí všetkých fragmentov spojí a vytvorí pôvodný paket.

Pri IPv6 sa fragmentácia nikdy nevykonáva v uzloch po ceste. Podľa RFC 2460 môžu pakety fragmentovať iba koncové uzly. Fragmentácia sa vykonáva na smerovačoch v sieti, jedine v prípade, že sú oni koncový uzol. Pri komunikácií klienstských staníc však smerovače pakety nefragmentujú, no dokážu fragmenty smerovať. Pre korektné fungovanie tohto mechanizmu musia koncové uzly najskôr zistiť najväčšiu možnú MTU po ceste k cieľu a dohodnúť sa na fragmentovaní. Tento proces sa nazýva Path MTU Discovery (**PMTUD**, RFC 1981). Pre zistenie maximálnej MTU sa používajú chybové

ICMPv6 správy typu 2 (Packet Too Big). Správy sú poslané na smerovače z nízkym MTU, ktoré odpovedajú spomínanou chybovou správou spolu s doporučovanou veľkosťou paketu.

IPv6 fragmentácia navyše definuje minimálnu veľkosť každého fragmentu, a to 1280 B. Všetky menšie fragmenty by mali byť automaticky zahadzované. To zabraňuje útokom, pri ktorých útočník rozposiela veľké množstvo malých fragmentov, čím vyčerpáva zdroje koncových uzlov. Pri IPv6 nemá žiadny zmysel povoľovať posielanie menších fragmentov, okrem prípadu, že je daný fragment v sérií posledný (m fragment bit je nastavený na 0 – žiadne ďalšie fragmenty).


**Obrázok 4 - fragmentácia IP paketu**

Jeden z najväčších bezpečnostných problémov pri IPv6 fragmentácií je neurčitá prítomnosť informácií vyššieho protokolu v prvom fragmente. TCP/UDP hlavička môže byť v niektorom z ďalších fragmentov. Tá je potrebná pre celkovú analýzu paketu sieťovým firewallom a pre rozhodnutie či je komunikácia povolená v sieti. Takáto detailná analýza vyžaduje nedeterministickú analýzu viacerých fragmentov, čo má nepriaznivé vplyvy na výpočtové zdroje firewallu.

Fragmenty môžu byť použité na cielené útoky voči systémom zo zlou implementáciou spracovania fragmentov. Typickým útokom je posielanie veľkého množstva fragmentov jednému koncovému uzlu (pričom sa každý fragment tvári ako časť iného paketu), kedy môže dôjsť k naplneniu pamäťového zásobníka koncovej stanice. To spôsobí, že koncová stanica nebude môcť prijímať ďalšie fragmenty regulárnej komunikácie. Podobný účinok sa dá docieliť posielaním množstva fragmentov jednej komunikácie, no bez posledného koncového fragmentu. V takom prípade koncová stanica čaká 60 sekúnd pred zahodením prijatých častí paketu, čo má znova nepriaznivý vplyv na jej hardvérové zdroje.

Obľúbeným útokom sú útoky fragmentami o veľkosti 65536 B, ktorú spôsobujú denial-of-service na staniciach z chybnou implementáciou kontroly fragmentov (ping-of-death). Tento fragment je totiž o 1 Byte väčší ako maximálna dĺžka IP paketu – 65535 bytov. Podobné zlyhanie sa dá docieliť aj posielaním chybných prelínajúcich sa ofsetov fragmentov.

**Protiopatrenia:**

- Filtrovanie fragmentov na smerovačoch, Cisco ACL umožňujú pokročilé filtrovanie
- VFR – Virtual Fragment Reassembly – mechanizmus v Cisco IOS. Keď smerovač vidí v pakete rozširujúcu fragmentačnú hlavičku, začne zberať všetky fragmenty paketu a usporiada ich do originálneho paketu. Následne podrobí paket hĺbkovej analýze a v prípade rozporov z bezpečnostnou politikou je paket zahodený. Takisto obsahuje mechanizmy pre zabránenie útokov načrtnutých v tejto kapitole.

## 5.3. Filtrovanie rozširujúcich hlavičiek

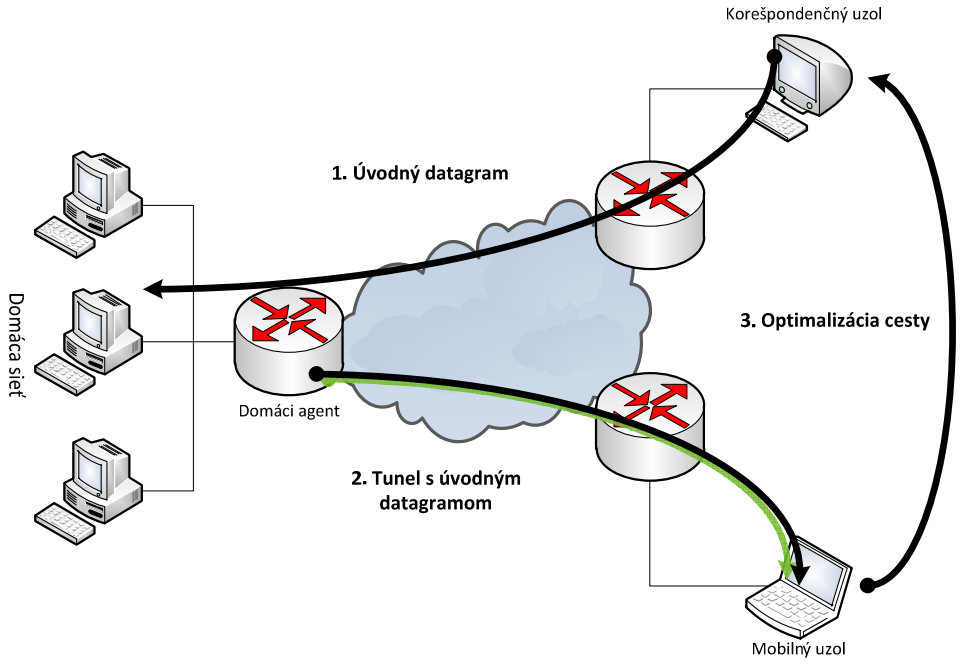
Keďže špecifikácia protokolu neobmedzuje použitie rozširujúcich hlavičiek, otvára bránu pre útoky zamerané na cielene preusporiadanie hlavičiek a úmyselné predlžovanie zoznamu hlavičiek. Útočník môže napríklad vytvoriť paket, ktorý odpovedá špecifikácii, no taktiež má za sebou nalinkované početné množstvo rozširujúcich hlavičiek. Takýto záškodnícky paket môže vytvoriť útok typu DOS alebo výrazne ovplyvniť výkonnosť zariadení po ceste k cieľu, vrátane samotného cieľa. Množstvo hlavičiek v jednom pakete môže byť rozdelené do ďalšieho fragmentu. Ten môže pôsobiť záškodnícky, keďže niektoré firewally kontrolujú iba začiatočný fragment.

Riešením predchádzania útokom tohto typu je aplikácia jednoduchého filtrovania rozširujúcich hlavičiek na sieťových uzloch. Definovaním pravidiel prístupu môžeme kontrolovať aké typy hlavičiek sú pre komunikáciu povolené. Počet zreťazených hlavičiek je nedeterministický, čo môže nepriaznivo ovplyvniť výkonnosť uzla pri filtrovaní a kontrolovaní všetkých hlavičiek. Problém sa neobjavuje ani tak pri softvérovom spracovaní ako pri hardvérovom. Pri IPv4 sme dokázali spracovať paket v jednom až dvoch taktoch. V IPv6 je nutné prechádzať celý zoznam s neznámym počtom hlavičiek. Tento prístup sa dostáva taktiež do konfliktu zo špecifikáciou RFC 2460, ktorá povoľuje uzlom po ceste kontrolovať iba hlavičky typu hop-by-hop. Zahadzovanie neznámych hlavičiek môže tiež spôsobiť problémy pri nasadzovaní a vyvíjaní nových aplikácií.

# 6. OTÁZKY BEZPEČNOSTI PRI MOBILITE IP

Podpora mobility sa opiera o základnú myšlienku, že aj pohyblivé - mobilné zariadenie je niekde doma. V klasickom prostredí mobilných zariadení sa IP adresa zariadenia mení pri každom pohybe medzi podsieťami, či už v rámci jednej firemnej siete alebo medzi WiFi prístupovými bodmi v uliciach. Výsledkom je zrušenie všetkých otvorených používateľských relácií (session) založených na zdrojovej a koncovej IP adrese. Keďže tradičné transportné protokoly (UDP, TCP) používajú IP adresu ako statický identifikátor uzla, nové relácie sa inicializujú až keď korešpondent pozná novú IP adresu.

Pri využití mechanizmov IP mobility (Mobile IP, MIPv6), existuje pre mobilné uzly tzv. domáca sieť v ktorej majú zaregistrovanú svoju domácu adresu (Home Address). Domáca adresa zariadenia je nemenná a pod domácou adresou je zariadenie zaznamenané aj v systéme DNS. Vďaka IP mobilite je zariadenia dosiahnuteľné na tejto adrese aj keď sa nachádza mimo svojej domácej siete. Keď sa zariadenie presunie mimo svoju domácu sieť, bude dostávať nové tzv. dočasné adresy novej podsiete (Care-of Address, CoA), no pre ostatných bude stále zastihnuteľná aj na svojej domácej adrese. Teda napr. keď bude používateľ cestovať vo vlaku, jeho mobilný telefón bude dostávať adresy v rámci siete daného mobilného operátora. Tá sa bude stále meniť pri prechádzaní cez jednotlivé podsiete operátora(medzi rôznymi BTS), no vďaka mobilite bude stále zastihnuteľný aj na rovnakej domácej adrese.




**Obrázok 5 - Komunikácia uzlov cez domáceho agenta**

### Domáci agent

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, ktorý spracováva všetky datagramy smerujúce k mobilnému uzlu a predáva ich

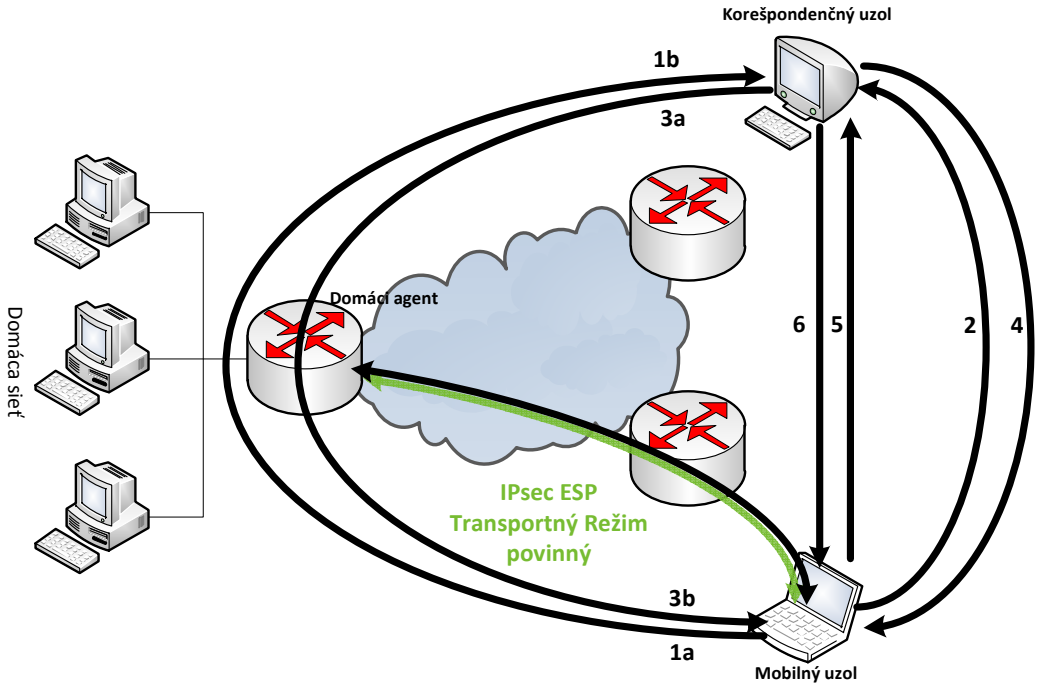
mobilnému uzlu vytvoreným tunelom. Keď mobilný uzol príjme datagram týmto tunelom, zistí, že sa ho niekto pokúša kontaktovať na domácej adrese.

**Komunikácia uzlov**

Mobilné IPv6 teraz pripúšťa dva režimy, ktorými bude ďalej prebiehať komunikácia medzi mobilným uzlom a korešpondentom (Correspondent Node):

- Celá komunikácia prebieha pomocou IPsec 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 svoju domácu adresu ako odosielateľa, predáva ich tunelom späť domácemu agentovi a ten ich preposiela korešpondentovi. Komunikácia je v tomto prípade veľmi neefektívna a navyše hrozí preťaženie domácej siete alebo domáceho agenta. Preto sa tento režim používa iba v prípade, kedy korešpondent nemá podporu pre mobilitu. Znázornenie takejto komunikácie možno pozorovať na obrázku č. 5.

- Celá komunikácia prebieha pomocou optimalizovanej cesty (mimo domáceho agenta). Ak má korešpondent podporu pre IPv6 mobilitu, prichádza k slovu optimalizácia cesty. Mobilný uzol zahájí optimalizáciu hneď po príchode prvého datagramu komunikácie. Cieľom optimalizácie je oboznámiť korešpondenta s aktuálnou dočasnou adresou mobilného uzla, aby bolo možné posielať ďalšie dáta priamo. Vďaka optimalizácií prechádza komunikácia medzi uzlami priamo, bez použitia a zaťažovania domáceho agenta. Model optimalizovanej komunikácie je zobrazený na obrázku Obrázok 6.




**Obrázok 6 - model priamej optimalizovanej MIPv6 komunikácie**

## 6.1. Formát správ

Napriek jednoduchosti mechanizmu mobility zasahuje mobilita do viacerých častí IPv6:

- Rozširujúca hlavička mobilita (test domácej a dočasnej adresy – overovanie dôveryhodnosti uzla pri optimalizácií cesty, správa väzieb)
- Rozširujúca hlavička Voľby pre príjemcu (domáca adresa)
- Rozširujúca smerovacia hlavička typu 2 (doručovanie dát mobilnému uzlu)
- 4 nové typy správ v ICMPv6
- Rozšírenie ohlasovanie smerovača

## 6.2. Bezpečnosť MIPv6

Mobilita IP umožňuje použitie zariadení z vnútra firemnej siete aj mimo chránenej zóny. To samozrejme zo sebou prináša aj mnoho bezpečnostných rizík. Zneužitie týchto rizík môže spôsobiť nepríjemné následky, a to nie len pre firemný sektor. Preto bola tejto problematike venovaná veľká pozornosť už od začiatku vývoja IP mobility. Medzi najznámejšie riziká MIPv6 patria:

### ➢ Podvrhnutý domáci agent

Ak je smerovač na sieti korektne nakonfigurovaný pre podporu MIPv6, tak je mechanizmus mobility automaticky prístupný aj pre ďalšie zariadenia v link-local segmente. Útočník si v takejto sieti môže vytvoriť vlastného záškodníckeho domáceho agenta a vytvárať prostredníctvom neho ďalšie útoky. Takisto môže najskôr naviazať väzbu z domácim agentom a tieto útoky vykonávať z iného miesta. Jedná sa hlavne o útok typu man-in-the-middle, kedy útočník odpočúva komunikáciu smerovanú k mobilnému uzlu cez domáceho agenta. Útočník navyše zahadzuje všetky správy HoTI, čím zamedzí vytvoreniu priamej optimalizovanej komunikácie mobilného uzla a korešpondenta.

### ➢ Prelomenie prístupovej vrstvy

Uzly využívajúce IP mobilitu často komunikujú cez rôzne druhy bezdrôtových sietí. Bezdrôtové siete v mnohých prípadoch neposkytujú takú úroveň zabezpečenia proti odpočúvaniu ako pri pevných sieťach. A preto môže byť IP mobilita zraniteľná pri odchytení signálu. Inak povedané, ak je zabezpečenie na prvej a druhej sieťovej vrstve slabé, tretia vrstva je zraniteľná tiež.

### ➢ Útoky typu man-in-the-middle

Procedúra spätného smerovania je vďaka dvojitému poslaniu náhodných čísel dvoma rôznymi trasami ťažko prelomiteľná. V prípade, že útočník odchytí iba jednu zo správ HoTI alebo CoTI, nepodarí sa mu podvrhnúť korektné CoT a HoT odpovede. Podarí sa mu to jedine, keď je veľmi blízko mobilného alebo korešpondenčného uzla, čiže v časti siete, kde je priama a nepriama cesta rovnaká.

Ďalšími prekážkami k vykonaniu útoku man-in-the-middle je nutnosť znalosti IPv6 adries HA, MN, CN a pohybovanie sa s mobilným uzlom medzi rôznymi sieťami.

- **Odchytenie komunikácie**

Signalizácia a MIPv6 komunikácia je posielaná v nešifrovanej forme. To sa dá zneužiť aj podvrhnutím útočníkových aktualizácií väzieb. Po poslaní aktualizácie väzby (BU) domácemu uzlu, domáci uzol odpovie potvrdením väzby (BA). Odteraz bude domáci agent posielať všetku komunikáciu smerovanú na mobilného agenta k útočníkovi. Útočník potrebuje poznať IPv6 adresu domáceho uzla a domácu adresu mobilného uzla.

- **Podvrhnutie aktualizácie väzby**

Okrem zneužitia aktualizácie väzby medzi MN a HA sa dá zneužiť aj medzi MN a CN. V prípade, že sa aktualizácie väzby neautentifikujú a útočník je na rovnakej sieti ako mobilný uzol, tak môže útočník poslať podvrhnuté aktualizácie väzby k CN (v čase keď sa mobilný uzol vypne alebo mu vyprší časovač väzby). Útočníkovi sa tak môže podariť ukradnúť reláciu komunikácie (session hijacking).

# 7. BEZPEČNOSŤ KONCOVÝCH POUŽÍVATEĽOV

## 7.1. Pripojenie domácich sietí

Vyriešenie problému pripojenia domácich sietí je stále otvorenou záležitosťou pri prechode na IPv6. Pri IPv4 sa domácim sieťam z pravidla prideľuje jedna IPv4 adresa, pričom je na túto adresu pripojené priamo koncové zariadenie, alebo je možno prostredníctvom technológie NAT/PAT pripojiť ďalšie zariadenia. Využitie tejto technológie je pri IPv6 neprijateľné, a preto vzniklo niekoľko smerov, ktorými sa môžu poskytovatelia pri pripájaní domácich sietí uberať.

**IPv6-NAT**

Existujú snahy vytvorenia NAT aj pre IPv6, no fungujúca a v praxi využiteľná implementácia ešte neexistuje. Kompromisným riešením by mohlo napríklad byť mapovanie ULA adries (unikátne lokálne adresy) na verejné adresy.

**L2 zariadenie**

Domáca lokálna sieť sa pripája k poskytovateľovi na linkovej úrovni, teda s použitím prepínača. Napriek to mu, že sa riešenie zdá ako veľmi jednoduché, vzniká problém pri koexistencií protokolov IPv4 a IPv6. Uvažovať by sa teda dalo iba nad variantov, kedy by boli na vrstve L2 prepínané iba IPv6 pakety. Avšak na trhu potrebné jednoduché zariadenie neexistuje.

**L3 zariadenie**

Domáci smerovač bude naďalej plniť funkciu NATu pre IPv4, zatiaľ čo pre IPv6 bude plnohodnotným L3 smerovačom. Vzniká tu ale problém, ako informovať domáci smerovač o prefixe vnútornej siete a ako vytvoriť smerovací záznam na strane poskytovateľa. K tomuto účelu sa používa špeciálna voľba DHCPv6 s názvom prefix delegation (RDC 3633), ktorá informuje domáce zariadenia o sieťach, ktoré má použiť pre vnútorné adresovanie.

## 7.2. Nové otázky bezpečnosti

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.

# 8. 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. 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.

Bezpečnosť v IPv6 bola umocnená 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. Netreba ale podľahnúť chybnej mienke, že IPsec je dostačujúca podmienka na zachovanie bezpečnosti siete. Siete môžu byť stále náchylné aj na zraniteľnosti z čias IPv4 a na mnohé iné nové zraniteľnosti.

IPv6 siete sa začínajú, čím ďalej tým viac nasadzovať do reálnych sieti, dokonca často aj s podporou vlády danej krajiny. To značí o tom, že IPv6 sa dostáva na dobrú cestu a že otázka bezpečnosti sa aktívne rieši. 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 7.


**Obrázok 7 - logo IPv6 ready**

# 9. ZOZNAM POUŽITEJ LITERATÚRY


1.**Satrapa, Pavel.** *IPv6.* Praha : CZ.NIC, 2008.

2.**Takashi Arano, Intec NetCore.** IPv4 Address Report. [Online] http://inetcore.com/project/ipv4ec/index_en.html.

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

4.**Carter, Earl.** *IPv6 Addressing.* [Online] Marec 2011. http://blogs.cisco.com/security/ipv6-addressing/.

5.**Hogg, Scott.** *IPv6 security.* s.l. : Cisco press, 2009.

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

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

8.**Marin, Eric.** 6net. *IPv6 Security.* [Online] February 2011. http://www.6net.org/events/workshop-2003/marin.pdf.

9.**Soliman, Hesham.** *Mobile IPv6: Mobility in a Wireless Internet.* s.l. : Addison-Wesley Professional , 2004.

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

11.**Donahue, Gary A.** *Kompletní průvodce sítového experta.* Brno : Computer Press, a.s., 2009.

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

13. **Oracle.** *SystemAdministrationGuide: IP Services.* september 2010. 816–4554–21.

14. **Tomáš Podermański, Matěj Grégr.** Pohněme s IPv6. *IPv6 Mýty a skutečnost.* [Online] Marec 2011. http://www.lupa.cz/serialy/pohneme-s-ipv6/.

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

16. **Hagen, Silvia.** *IPv6 Essentials.* s.l. : O'Reilly Media, 2006. ISBN-13: 9780596100582 .

17. **Wolfgang Fritshe, Florian Heissenhuber.** Mobility support for Next Generation Internet . [Online] IABG, 2008. http://www.ipv6forum.com/navbar/papers/MobileIPv6_Whitepaper.pdf.