UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Matjaž Drča

VARNOST V OMREŽJIH S PROTOKOLOM IPV6

DIPLOMSKO DELO NA UNIVERZITETNEM ŠTUDIJU

Mentor: doc. dr. Mojca Ciglarič

Ljubljana, 2010

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 01663/2010
Datum: 05.04.2010

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MATJAŽ DRČA**

Naslov: **VARNOST V OMREŽJIH S PROTOKOLOM IPV6**
SECURITY IN IPV6 NETWORKS

Vrsta naloge: Diplomsko delo univerzitetnega študija

Tematika naloge:

Opišite funkcionalnost protokola IPv6 in primerjajte vgrajene varnostne mehanizme s tistimi v IPv4. Preučite relevantne IETF specifikacije in osnutke. Opišite mehanizem napadov, ki jih v podobni obliki poznamo že iz omrežij z IPv4, predvsem pa se posvetite novim napadom, ki so možni le v IPv6, zlasti je ranljiv protokol NDP. Izbrani napad tudi preizkusite v nadzorovanem okolju in komentirajte možne načine obrambe. V zaključku podajte svojo oceno in ugotovitve glede celostne varnosti IPv6 omrežij.

Mentor:
M. Ciglarič
doc. dr. Mojca Ciglarič

Fakulteta za računalništvo in informatiko
2
UNIVERZA V LJUBLJANI

Dekan:
prof. dr. Franc Solina

Original izdane teme

I Z J A V A O A V T O R S T V U

diplomskega dela

Spodaj podpisani/-a **Matjaž DRČA**,

z vpisno številko **63020031**,

sem avtor/-ica diplomskega dela z naslovom:

Varnost v omrežjih s protokolom IPv6

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom (naziv, ime in priimek)

  doc. dr. Mojce CIGLARIČ

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela

- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne 06. 07. 2010 Podpis avtorja/-ice:

”

Zahvala mentorici doc. dr. Mojci Ciglarič in asis. Andreju Krevlu za strokovno pomoč in nasvete pri izvedbi.

Posebna zahvala gre moji družini za vzpodbude in finančno podporo tekom študija ter pisanja diplomskega dela.

“

KAZALO VSEBINE

SEZNAM UPORABLJENIH KRATIC

TCP/IP Transmission Control Protocol / Internet Protocol	Protokol za nadzor prenosa
IP Internet protocol	Internetni protokol
4G	4. generacija mobilne telefonije
DSL Digital Subscriber Line	Digitalna naročniška linija
NAT Network Address Translation	Omrežni translacijski mehanizem namenjen prevajanju omrežnih naslovov. Omogoča, da lahko več naprav ali računalnikov v zasebnem omrežju uporablja enega ali več javnih IPv4 naslovov, ki jih lahko globalno usmerjamo
DHCP Dynamic Host Configuration Protocol	Protokol za dinamično nastavitev gostitelja
PPP Point to Point Protocol	Protokol za vzpostavljanje direktne povezave med mrežnima točkama
SLAAC StateLess Address Auto Configuration	
MAC address Media Access Control address	Fizični naslov naprave na ravni strojne opreme.
DNS Domain Name System	Sistem domenskih imen
VPN Virtual Private Network	Navidezno zasebno omrežje
HTTP HyperText Transfer Protocol	
INTRANET	Spletne strani dostopne samo ljudem znotraj podjetja ali organizacije
EXTRANET	Podobno kot intranet s tem, da je namenjen zunanjim strankam
SSH Secure shell	Orodje za varen dostop do oddaljenih računalnikov
DDos Distributed Denial Of Service	Porazdeljeni napadi zavrnitve storitve
SIP Session Initiation Protocol	Protokol za kontrolo sej multimedijskih komunikacij preko IP protokola
IPsec Internet Protocol security	Varen internetni protokol

Povzetek in ključne besede

Piše se leto 2010. Moderne oblike komunikacij v vedno večji meri uporabljajo infrastrukturo omrežij IP. Pojavljajo se zahteve po hitrejšem usmerjanju omrežnega prometa, globalni dosegljivosti naprav, možnostih za določanje in nadzor kakovosti storitev, predvsem pa po povečanju naslovnega prostora za omrežne naprave. Hkrati se s povečevanjem IP-paketnega prometa odpirajo tudi vprašanja glede varnosti prenosa informacij. Nekatere odgovore na te izzive predstavlja novodobni protokol IPv6.

V diplomskem delu sem uvodoma predstavil temeljne značilnosti tega protokola. Pojasnil sem glavne cilje in namere snovalcev IP protokola prihodnosti, ki so posledica pomanjkljivosti njegovega predhodnika IPv4. Za razumevanje kasnejših navedb in opisov napadov sem v tem delu opisal varnostni protokol IPsec, ki predstavlja temeljni mehanizem za zaščito IP komunikacij.

V osrednjem delu predstavitve sem se osredotočil na izvajanje napadov na IP protokol verzije 6. Ker ta glede na sodobne potrebe na področju komuniciranja predstavlja logično nadgradnjo IPv4, so nekatere nevarnosti ostale identične oziroma zelo podobne IPv4. V tem poglavju sem za vsak tip napada navedel opis izvedbe ter morebitne razlike v pristopu.

V naslednjem poglavju sem skušal zaokrožiti napade, ki se v novi obliki pojavljajo samo pri IP, verzija 6. Ti so vezani predvsem na manipulacijo s sporočili, s katerimi gostitelji omrežja bodisi oglašujejo nastavitvene parametre bodisi izražajo zahteve po njih. Eden izmed napadov temelji na ponarejanju sporočil ob postopku preverjanja zasedenosti IP naslova. Teoretični opis ranljivosti pri postopku preverjanja podvojenih IPv6 naslovov mi je služil kot podlaga pri izvedbi praktičnega poizkusa izvedbe napada v izoliranem in nadzorovanem okolju.

V zadnjem delu sem praktično prikazal možnost izvedbe napada, ki žrtvi onemogoča pridobitev veljavnega naslova. Napad sem realiziral na štirih virtualnih računalnikih z omrežnimi vmesniki. Vsak izmed njih je imel tekom napada točno določeno vlogo. Cilj napada je prikazati zmožnost infiltriranja neavtoriziranih sporočil v omrežje za izvedbo zlonamernih aktivnosti.

IPv6 je od svojega predhodnika nekatere ranljivosti podedoval, spet druge so posledica novih pristopov v zasnovi protokola. Znanje, ki smo si ga pridobili pri analizi IPv4 protokolnih nevarnosti, lahko s pridom izkoristimo. Nenazadnje bo prehodno obdobje na čisto IPv6 omrežje trajalo še kar nekaj časa. Glavni tranzicijski mehanizem naj bi po napovedih strokovnjakov predstavljala uporaba arhitekture dvojnega sklada, ki bo omogočala hkratno delovanje obeh verzij protokolov. Tako bo potrebno biti pri uporabi varnostnih mehanizmov pozoren tako na skupne ranljivosti ter nove možnosti v IPv6 protokolu kot na varnostne luknje v implementacijah mehanizmov tranzicijskega obdobja.

Ključne besede: IPv6, IPsec, NDP, napadi na protokol IPv6

Abstract

It is the year 2010. Modern forms of communication are increasingly using IP networks infrastructure. There are requirements to accelerate network traffic direction, global availability, opportunities for identification and quality control services and, in particular, to increase the address space for network devices. At the same time enhancing the IP packet traffic raise questions about the security of information transfer. Some answers to these challenges introduce a new age protocol IPv6.

Initially the thesis presents the basic characteristics of this protocol. I explained the main planners objectives and goals of future IP protocol which are the result of the imperfection of its predecessor, IPv4. In order to understand the subsequent quotes and attack descriptions I have described also the IPsec security protocol, which represents a fundamental mechanism for the protection of IP communications.

In the central part I focused on the execution of attacks to the IP version 6 protocol. Since IPv6 according to contemporary needs in the field of communication represents a logical upgrade of IPv4, some risks remain identical or very similar to IPv4. In this chapter I listed a description of execution for each type of attack and any differences in approach.

In the next chapter, I tried to sum up the attacks, which appear in a new form only in IP version 6. These are primarily related to messages manipulation with which network hosts advertise configuration parameters or express request for it. One of the attacks is based on message spoofing at the process of verification of IP address availability. The theoretical description of the vulnerability in duplicate address detection procedure served as a basis for the implementation of practical implementation of an attack.

In the last part I have practically demonstrated the possibility of an attack, which prevents the victim to obtain a valid address. I realized the attack on four virtual PCs with network interfaces. Each of them had a defined role during the attack. The aim of the attack is to show the ability of infiltration of unauthorized messages into the network in order to execute malicious activity.

IPv6 inherited certain vulnerability from its predecessor while others are the result of new approaches in the design of the protocol. We can exploit the knowledge we have gained with IPv4 protocol threats analysis since the transitional period to native IPv6 network will take quite some time. The main transition mechanism towards the experts forecast is the usage of dual stack architecture which will allow simultaneous processing of both versions of the protocols. Therefore it will be necessary in the use of security mechanisms to be attentive to the common vulnerabilities and new opportunities in the IPv6 protocol as to the security holes in implementations of the mechanisms of the transition period.

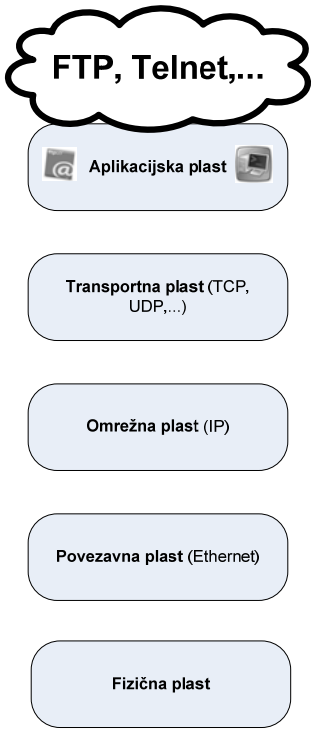
Key words: IPv6, IPsec, NDP, attacks based on IPv6 protocol

1. Protokol IPv6

1.1. Splošno o protokolu IP

Protokol je zbirka pravil. IP protokol je množica pravil za komuniciranje in je definiran v sklopu modela TCP/IP. TCP/IP je de facto standard, model svetovnega omrežja (t.i. interneta). Poleg njega poznamo tudi model OSI, ki je model nacionalnih operaterjev telekomunikacijskih storitev [17] .

TCP/IP model je sestavljen iz plasti, ki definirajo arhitekturo omrežja:



Slika 1: TCP/IP model

Plast IP je ekvivalentna mrežni plasti modela OSI. Slednja je odgovorna za zagotavljanje povezave ter usmerjanje skozi omrežje. Podatkovna protokolarna enota te plasti se imenuje datagram. Ta potuje skozi topologijo omrežja odvisno od usmerjevalnih algoritmov.

1.2. Razlogi za uvedbo IPv6

IPv6 je naslednik protokola IPv4, ki se uporablja že več kot 25 let. Standardiziran je bil že konec leta 1998, a se njegova implementacija ni širila tako hitro, kot je bilo pričakovati. Razloga sta gotovo vsaj dva.
Prvi je nekompatibilnost z IPv4, drugi pa pomanjkanje storitev začetkom novega tisočletja, ki bi temeljile na tem protokolu in s tem pospešile njegovo širjenje. Stanje se zadnjih nekaj let spreminja. Razlogi tičijo poleg hitrega razvoja širokopasovnih omrežij predvsem v hitrem razvoju storitev mobilne telefonije. Naslednja generacija omrežij 4G naj bi temeljila predvsem na hitrem prenosu podatkov in s tem podatkovnih storitvah vse do zmožnosti doseganja pasovnih širin, ki jih trenutno ponujajo ponudniki storitev DSL.

1.2.1. Pomanjkanje naslovnega prostora

Kot je že bilo omenjeno, je hiter razvoj komunikacij v zadnjih letih povzročil paniko zaradi predvidenega pomanjkanja IPv4 naslovov. Naslov je namreč v IP verziji 4 dolg 32 bitov (4 okteti). To teoretično pomeni, da je na razpolago 2^{32} unikatnih naslovov, kar znese dobre 4 milijarde (4,294,967,296) naslovov. Ta številka se je zdela v času uvajanja standarda IPv4 v 80. letih prejšnjega stoletja težko dosegljiva. Internetni naslovni prostor je bil bolj kot za komercialno rabo namreč namenjen in predviden za akademsko in raziskovalno sfero. A kot že rečeno, je hiter razmah širokopasovnih ter mobilnih storitev z možnostjo izbire statičnega naslova povzročil hitro zasedanje razpoložljivih naslovov.

Tako organizacija IANA, ki je odgovorna za globalno koordinacijo DNS, IP naslavljanja in z IP protokoli povezanih storitev, predvideva porabo naslovov razpoložljivega naslovnega prostora oktobra, leta 2011.

Datum	Prosti naslovi v milijonih	Zasedeni naslovi v milijonih
01. 01. 2006	1468.61	
01. 01. 2007	1300.65	167.96
01. 01. 2008	1122.85	177.80
01. 01. 2009	925.58	197.27
01. 01. 2010	**722.18**	**203.40**

Tabela 1: Tabela uporabljenih in še razpoložljivih IP naslovov po analizah spletne strani bgpexpert.com. V letu 2009 je bilo porabljenega cca. 80% razpoložljivega IP naslovnega prostora (3706.65 milijonov naslovov) [3]

To je prisililo veliko uporabnikov in organizacij k uporabi mehanizma NAT, ki lahko na javni IP naslov veže več zasebnih naslovov (t.i. private address space), ki se lahko podvajajo tudi v drugih zasebnih omrežjih.

Kot nadgradnja mehanizma NAT se je uveljavil tudi PAT. Ta na meji med zasebnim in javnim omrežjem omogoča preslikovanje para zasebni IP naslov / številka vrat v javni IP naslov / številka vrat. Paketi iz javnega omrežja so tako usmerjeni v zasebno preko tabel, ki jih mehanizem PAT vzdržuje tekom komunikacije. Primer uporabe predstavlja programska izvedba požarnega zidu.

NAT je tako zmanjšal porabo javnih naslovov in povečal fleksibilnost pri povezovanju v svetovni splet. Po drugi strani pa smo z njim uničili neposredno IP povezljivost, vrste točka v točko (end-to-end), vnesli zakasnitve v preslikave naslovov ter dosegli, da nekatere aplikacije sploh ne bodo delovale z vključenim NAT-om. Težave se pojavijo pri aplikacijah, ki naslove (izvorne, ponorne) prenašajo v podatkovnem delu aplikacijskega sporočila – primer uporabe protokola SIP (angl. Session Initiation Protocol).

Koncept končne globalne povezljivosti in dosegljivosti pa je glede na hiter razvoj tehnologije nujen. V prihodnosti bomo z uporabo IPv6 gradili omrežja senzorjev, razvijali tehnologije RFID (angl. Radio Frequency Indentifiers), na daljavo dostopali do naprav v domačem okolju (TV, osebni pripomočki) itd.

Naslov v glavi IPv6 je dolg 128 bitov. To prinaša približno $3{,}4 \times 10^{38}$ naslovov. Če upoštevamo, da nas na Zemlji trenutno živi približno 6,5 milijarde, bi si vsak Zemljan lahko prilastil približno 5×10^{28} naslovov.

Podatki, ki se nanašajo na naslovni prostor so sicer slišati astronomskih dimenzij, vendar je potrebno vedeti, da bo v prehodnem obdobju za normalno komuniciranje potrebno še vedno imeti dodeljen tudi IPv4 naslov (za dostop do vsebin na IPv4 strežnikih).

1.2.2. Razvoj storitev

Razvoj storitev je tesno povezan z nekaterimi lastnostmi IPv6 protokola: neposredna povezljivost točka v točko, velik naslovni prostor, poenostavljena IPv6 glava …

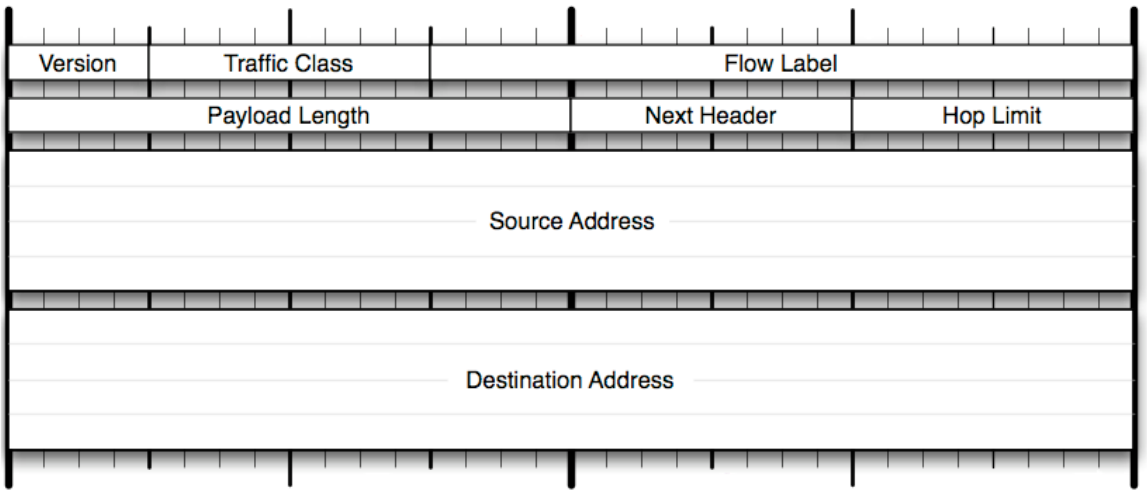
Pomembne prednosti se bodo v veliki meri odražale na področju hitro rastočega trga mobilnih komunikacij. IPv6 vpeljuje novost, ki odpravlja potrebo po oddaljenem agentu v gostujočem omrežju, kar pomeni neodvisnost uporabe storitve od podpore v omrežju, kjer gostuje.
4. generacija mobilnih omrežij (4G) temelji na ponudbi storitev na IP platformi: IP telefonija, ultra-broadband internetni dostop in storitve za zanesenjake računalniških iger so samo nekatere izmed možnosti, ki jih bo tehnologija ponujala. Ko bo operater preko protokola IPv6 zmožen vsaki napravi dodeliti lasten IP naslov, bo to pomenilo visok nivo kontrole nad kvaliteto in varnostjo servisa. To pa je nenazadnje dobra podlaga za razvoj novih inovativnih storitev.

Velik naslovni prostor odpira možnosti za omrežno priključevanje nekaterih naprav, ki niso bile značilne za IPv4 omrežje. Primer predstavlja možnost implementacij omrežij senzorjev in kamer za nadzor. V času, ko so v skrbi za varstvo okolja na pohodu gradnje pametnih, varčnih hiš, nam povezljivost njihovih regulacijskih in nadzornih elementov lahko prinese možnost oddaljenega nadzora delovanja sistema, oddaljeno nastavljanje optimalnih parametrov, nadzor posameznih območij preko video kamer in še kup drugih možnosti.

Ker bo lahko IPv6 komunikacija temeljila na neposrednih komunikacijah med gostitelji omrežja, se odpirajo številne nove možnosti deljenja informacij z ostalimi uporabniki medmrežja. Zakaj bi ob vse zmogljivejših mobilnih aparatih v smislu pomnilniških kapacitet in procesorskih zmogljivosti še bili strežniki nujni za objavo in dostop do osebnih vsebin, ko pa lahko informacije ponujamo preko mobilnih aparatov ali osebnih računalnikov in glede na našo politiko varovanja podatkov vzdržujemo kontrolo nad dostopom in manipulacijo informacij. Končno je tudi zasnova interneta temeljila na principu »fast switching core with smart edge«.

1.2.3. Višja učinkovitost in izkoriščenost omrežja

IPv6 glava ima poenostavljeno strukturo. Za nadaljevanje, ko bodo podane nevarnosti, ki prežijo na protokol IPv6, je nujno razložiti glavo protokola. Velika je 40 oktetov (v IPv4 20 oktetov). Polja, ki jo sestavljajo, so fiksna in so prikazana na sliki 2.



Slika 2: Glava IPv6

- **Verzija** (angl. - version – 4b): izbira različice protokola
- **Razred prometa** (angl. traffic class – 8b): Uporabljamo ga za označevanje podatkov, ki se prenašajo v realnem času ter za določevanje prioritet posameznih razredov prometa.
- **Oznaka podatkovnega toka** (angl. flow label - 20b): To možnost uporabimo, da označimo pakete, ki pripadajo istemu toku podatkov. Kot skupen tok podatkov so mišljeni zaporedni paketi, ki so med sabo v korelaciji. Izvorno vozlišče v primeru toka podatkov izbere vrednost med 1 in FFFFF. Vsi paketi, ki pripadajo istemu toku, morajo imeti isti izvorni in ponorni naslov, enako prioriteto ter oznako podatkovnega toka.

  Polje odpira tudi možnosti identifikacije prometnih značilnosti (angl. Deep Packet Inspection). DPI se nanaša tako na pregledovanje glave paketa kot vsebovanega podatkovnega dela za primerjanje s predefiniranimi vzorci. Ta prinaša možnost identifikacije protokolov in aplikacij, omejevanje prometa, statistike,....

- **Dolžina tovora** (angl. payload length – 16b): V polju je podana velikost podatkovnega dela paketa. Velikost 16 bitov določa največjo velikost, omejeno na 64KB. Če v polju uporabimo vrednost 0, lahko velikost tudi presežemo. Takrat uporabimo možnost »Jumbo Payload«.
- **Naslednja glava** (angl. next header – 8b): To polje določa tip glave, ki sledi glavi IPv6 in je v paketu pred dejanskimi podatki. Najpogosteje se tu pojavljata TCP (povezovalni protokol), UDP (nepovezavni protokol), GGP, RH, ICMP. Hkrati lahko določa tudi **razširitvene glave** IPv6 protokola:

  - Hop-by-Hop options (Next Header Value = 0)
    Uporablja se za prenos neobveznih informacij, ki jih pregleda vsako vozlišče na poti paketa do ponora.
  - Fragment (Next Header Value = 44)
    Z njim lahko izvorno IPv6 vozlišče pošlje paket, ki je večji kot ga določa MTU (Maximum Transfer Unit) na poti. MTU predstavlja največjo velikost okvirja, ki se še lahko prenese na poti do ponora.
  - Routing (Next Header Value = 43)
    Izvorno IPv6 vozlišče uporabi razširitveno glavo za navajanje vmesnih vozlišč na poti paketa do ponora.
  - Destination options (Next Header Value = 60)

Uporablja se za prenos neobveznih informacij, ki so namenjene ponoru določenega paketa. Primer uporabe razširitvenih glav »Routing« in »Destination options« je pri protokolu mobile IPv6. Gre za standard, ki poenostavlja komunikacijo med mobilnimi napravami na način, da se ohrani povezljivost tudi s prehajanjem med gostujočimi omrežji. Tam imata razširitveni glavi funkcijo zagotavljanja trdne TCP povezave aplikacijam med prehodom IPv6 mobilne naprave med posameznimi omrežji.

- Encapsulating Security Payload (Next Header Value = 60)
  Protokol za šifriranje koristne vsebine.
- Authentication (Next Header Value = 51)
  Protokol avtentikacijskega čela.

- **Omejitev skokov** (angl. hop limit – 8b): Nadomešča polje TTL pri IPv4. Polje je namenjeno zmanjševanju 8-bitne vrednosti z vsakim prehodom skozi vozlišče (usmerjevalnik). Začetno vrednost nastavi gostitelj, ki pošilja paket v omrežje. Z velikostjo polja je določeno največje število usmerjevalnikov na poti med dvema točkama: $2^n - 2 = 254$. Glavni namen tega polja je identificiranje in izločanje paketov, ki krožijo v omrežju – izločijo jih usmerjevalniki, ko doseže polje »hop limit« vrednost 0.
- **Izvorni naslov** (angl. source address – 128 b)
- **Ponorni naslov** (angl. destination address – 128 b)

Glava je v primerjavi s predhodno verzijo poenostavljena, kar omogoča hitrejše procesiranje paketov v vozliščih.

Predvsem pa je iz opisa polj »razred prometa« in »oznaka podatkovnega toka« razvidna pozornost, ki so jo snovalci protokola polagali na zagotavljanje t.i. kakovosti storitev (QoS). Pri IPv4 je princip temeljil na posredovanju na najboljši možen način (angl. best effort). Pri IPv6 pa lahko s pomočjo omenjenih polj točno določamo obravnavo paketov na poti po omrežju in jih prilagajamo prioriteti storitve.

1.2.4. Želja po lažji konfiguraciji

Način pridobivanja omrežnega naslova je pri IPv4 vezan na ročen vnos parametrov ali pa se pri tem uporabljajo uveljavljeni avtomatizirani protokoli: DHCP, PPP ...
Pri ponudnikih internetnih storitev, ki svojim uporabnikom dodeljujejo IPv4 naslove za povezljivost v splet, postopek temelji na dodelitvi enega javnega naslova, uporabnik pa dalje sam preko mehanizma NAT poskrbi za dodeljevanje zasebnih naslovov.

Ponudniki dostopa do IPv6 omrežja lahko svojim odjemalcem dodelijo predpone /48, /56 ali /64, za kontrolo dodeljevanja pa uporabljajo posebne nadzorne mehanizme.

Zaradi porasta naprav, priključenih v globalno omrežje, je nujno zagotoviti mehanizme, ki skrbijo za avtomatizacijo procesa dodeljevanja naslovov in nemoteno zagotavljanje skalabilnosti.

Temeljna mehanizma za dodeljevanje naslova napravi v omrežju IPv6 sta **SLAAC** (angl. StateLess Address Auto Configuration) in **DHCPv6** (angl. Dynamic Host Configuration Protocol v6).

SLAAC se uporablja za dodelitev osnovnih parametrov za priključitev gostitelja v omrežje. Z njegovo pomočjo si lahko gostitelj pridobi svoj omrežni naslov, ki je kombinacija lokalno dosegljivih informacij (identifikacija vmesnika) ter vrednosti oglaševanih s strani usmerjevalnikov

(predpona, ki identificira omrežje). Na tak način si gostitelji pridobijo veljaven, edinstven IPv6 naslov. Hkrati nam protokol za raziskovanje soseščine (angl. NDP) omogoča preverjanje podvojenih IPv6 naslovov.

SLAAC je sicer dober avtomatiziran mehanizem za pridobivanje IP naslovov ter ugotavljanje podvojenosti, je pa kritičen z vidika varnosti in omejitev pri pridobivanju nekaterih ključnih informacij.
Prva kritika sloni na dejstvu, da SLAAC nima vgrajenega nobenega avtentikacijskega mehanizma. To z drugimi besedami pomeni, da lahko napadalec ponareja sporočila, s katerimi oglašuje napačno predpono omrežja.

Omejitve glede pridobivanja nekaterih parametrov komunikacij predstavlja pomanjkljivo oglaševanje nekaterih ključnih podatkov kot na primer naslov domenskega strežnika.

DHCPv6 je protokol, ki gostiteljem omogoča avtomatsko pridobivanje podatkov omrežja. Sporočila, ki si jih obe strani medsebojno izmenjujeta, sta tipov solicit in advertise (prošnja za informacijo in oglaševanje informacije), katerih pomen razkriva poglavje 1.4. Postopek komunikacije med DHCPv6 strežnikom in odjemalcem, ko sta ta na isti povezavi, je naslednji:

- Odjemalec pošlje DHCP SOLICIT sporočilo na naslov FF02::1:2 (vsem DHCP agentom)
- Strežnik(i) se odzovejo s pošiljanjem DHCP ADVERTISE sporočila.
- Odjemalec pošlje DHCP REQUEST sporočilo strežniku (če se odzove več strežnikov, se sporočilo pošlje tistemu, ki ima najvišjo prioriteto).
- Strežnik odgovori z DHCP REPLY sporočilom, ki vsebuje IPv6 naslov in ostale konfiguracijske parametre.
- Odjemalec sedaj poseduje relavantne informacije za obstoj in delovanje v omrežju (glede na način nastavitve DHCPv6 strežnika): IPv6 naslov, IPv6 predpono, podatke o DNS, SIP, SNTP strežnikih,…
- V primeru, da odjemalec naslova(ov) ne potrebuje več, pošlje strežniku sporočilo DHCP RELASE. Strežnik naslov sprosti.

1.2.5. Boljša podpora za določanje prioritete in dostave podatkov v realnem času

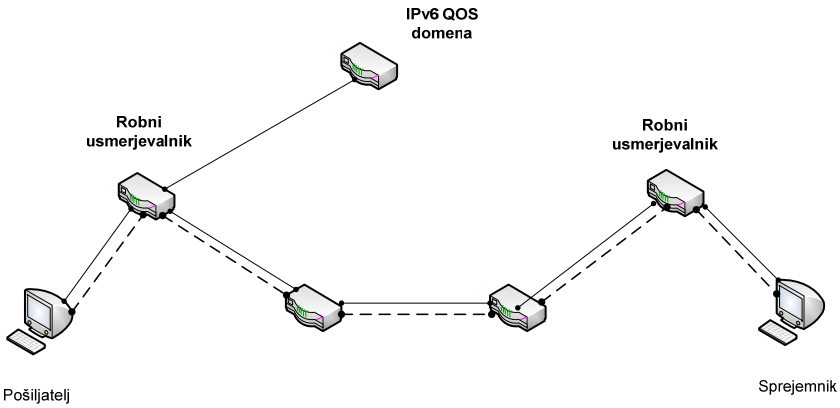
Do uvedbe protokola IPv6 se je omrežni promet stekal v skladu z načelom »po najboljših močeh« (angl. best efford). Načelo temelji na ideji, da je naloga omrežja storiti vse, da se zagotovi dostava vsakega posameznega IP paketa. Po drugi strani pa omrežje ne zagotavlja niti časa za dostavo paketa niti zagotovila, da bo paket tudi dostavljen.
To lahko aplikacijam, ki se izvajajo v realnem času (npr. videokonferenca) in ki so občutljive na zakasnitve ter izgubo paketov, povzroči težave.

Atributi, povezani z zagotavljanjem kakovosti storitev, so:

- **Zakasnitev** (angl. delay) – pretečeni čas od odpošiljanja paketa do prihoda na ciljni sistem.
- **Nivo izgube paketov** – je definiran kot razmerje med zavrženimi paketi in celotnim številom paketov.
- **Pasovna širina** – največja zmogljivost prenosa podatkov med končnima točkama.
- **Variacije zakasnitve** – jitter.

IPv6, kot že rečeno, upravlja z zahtevami QoS s procesiranjem ter nadzorom toka podatkov.

V primeru, da želi gostitelj podatke pošiljati v realnem času, se s svojimi zahtevami obrne na robni usmerjevalnik (angl. Edge router). Ta se o zahtevah pogaja z domenskim upraviteljem, ki glede na okoliščine vrne odgovor. V primeru, da je zahtevi ugodeno, začne pošiljatelj preko robnega usmerjevalnika v omrežje pošiljati svoj tok podatkov. V nadaljevanju ta usmerjevalnik opravlja funkcijo klasifikacije prometa, določanja urnika in nadzora.



Slika 3: Prikaz funkcionalnosti robnega usmerjevalnika pri pošiljanju podatkov v realnem času

1.2.6. Mobilnost

Glavni cilj, ki so si ga inženirji zadali pri načrtovanju mobilnosti v protokolu IPv6, je zagotoviti dostop naprave v poljubnem omrežju na način, da naprava vedno pridobi enak javno dosegljiv naslov.

IPv6 vpeljuje novosti, ki odpravljajo potrebe po oddaljenem agentu v gostujočem omrežju.
V primeru, da se mobilno vozlišče poveže v tuje omrežje, si tam pridobi začasen IP naslov ter o tem obvesti svojega domačega agenta (angl. Home Agent). Slednji preko vzpostavljenega tunela do svojega mobilnega vozlišča preusmeri vse pakete, sicer naslovljene na domači naslov te naprave.

Vsekakor je zelo hitro rastoči trg mobilne telefonije dober pospeševalec vlaganja v IPv6 implementacije. Do konca leta 2010 naj bi po podatkih mednarodne zveze za telekomunikacije ITU z dostopom do hitrega mobilnega omrežja razpolagala ena milijarda ljudi. Ocenjujejo, da bi lahko v obdobju 2010 – 2015 beležili več dostopov do svetovnega spleta preko mobilnih naprav kot pa preko osebnih računalnikov.

1.2.7. Varnost

Kot temeljni prednosti IPv6 protokola prihodnosti se navajata večji naslovni prostor in uporaba varnostnega protokola IPsec (angl. Internet Protocol Security).

V osnovi prvo prednost prinaša ogromen naslovni prostor. Ta za zlonamerne napadalce pri preverjanju naslovnega prostora za namene iskanja potencialne žrtve predstavlja visoko časovno kompleksnost. Primer odkrivanja ranljivih gostiteljev pri širjenju omrežnega črva in demonstracijo porabe časa sem opisal v delu 2.9.3.

IPsec je varnostno ogrodje za zaščito komunikacij preko protokola IPv6.
To ogrodje je bilo že del IP, verzije 4. Tam je bila uporaba opcijska. Resnici na ljubo tudi pri protokolu IPv6 ni veliko drugače. Implementacija tega varnostnega mehanizma je obvezna, ne pa tudi sama uporaba.

Pogosto se v sklopu debat o protokolu IPsec omenja pojem navideznega zasebnega omrežja (VPN). Pri tej vrsti omrežja gre za povezavo med dvema točkama, med katerima je vzpostavljen tunel skozi javno omrežje, v katerem se zagotovi varen in zanesljiv tok podatkov.

Alternativo uporabi protokola IPsec v kontekstu vzpostavljanja navideznega zasebnega omrežja predstavlja protokol **SSL** (angl. Secure Sockets Layer). Čeprav je oba med sabo neposredno težko primerjati, ker delujeta na različnih plasteh modela TCP/IP, (IPsec – omrežna plast; SSL – med omrežno in aplikacijsko plastjo) se je vredno ozreti za razlogi, zakaj je njegova uporaba priljubljena ne glede na to, da je IPsec tako tesno povezan z IP protokolom, preko katerega se v višjih plasteh pretakajo tudi podatki, varovani z SSL.

SSL je varnostni protokol za prenos podatkov, največkrat za zaščito HTTP, IMAP in POP3 transakcij. Kompatibilen je z aplikacijami, ki tečejo preko protokola TCP.

Sestavljajo ga naslednji štirje protokoli:

1.) Handshake protocol – protokol za rokovanje, ki nam omogoča izvedbo avtentikacije in izmenjave ključev.
2.) Change Cipher Spec Protocol – protokol se uporablja za nakazovanje uporabe izbranih ključev.
3.) Alert protocol – protokol se uporablja za signalizacijo napak ter zapiranje seje.
4.) Application data protocol – protokol dejansko prenaša in sprejema kriptirane podatke.

Glede na IPsec je njegova prednost ta, da ne potrebuje posebnih odjemalcev, ker je praktično vgrajen v vsak spletni brskalnik. Vzpostavljanje nastavitev je enostavno, težav z mehanizmom NAT ni. Zagotavlja visoko preciznost nadzora dostopa. Vzpostavljajo se lahko tuneli do določenih aplikacij in ne samo do prostranih LAN omrežij. Omejen je v glavnem s prometom, ki temelji na spletnih aplikacijah.

Na drugi strani je IPsec kompatibilen z vsemi aplikacijami. Z razvojem IPv6 je implementacija IPsec za vsako vozlišče obvezna. Glede na SSL je IPsec bolj kompleksen, nabor parametrov za nastavitev delovanja je širok. Pomanjkljivosti se nanašajo na kompleksnost protokola IKE (za avtomatiziranje vzpostavljanja varnostne zveze ter avtentikacijo končnih točk) ter netransparentnost za naprave, ki se skrivajo za mehanizmom NAT (pri verziji IPv4) oz. NAPT. Težave nastanejo pri prečkanju paketa skozi napravo NAT, kjer se spremenita izvorni naslov in paket. Paket se razveljavi, pogajanja za povezavo VPN ne uspejo. Rešitev predstavlja ovijanje tovrstnega paketa z glavo UDP, ki ji pri prehodu skozi NAT spremenimo naslov. Ko takšen paket doseže sprejemni konec se nova glava odstrani, tako da ostane samo izvirni paket IPsec.

Glavne značilnosti in delovanje IPsec so opisane v podpoglavju 1.5.

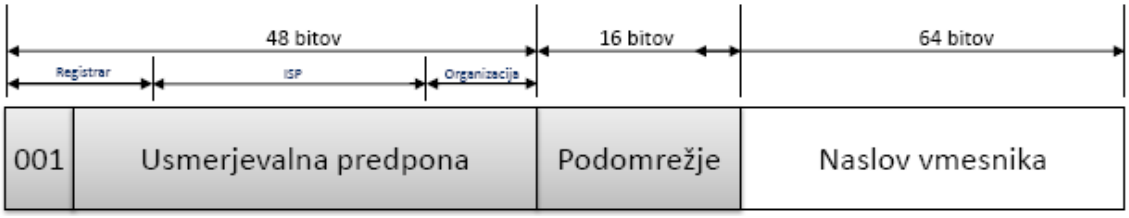
1.3. Tipi naslovov pri IPv6

1.3.1. Unicast

Z unicast naslovi naslovimo določen vmesnik v omrežju.

- Globalni unicast naslovi

  Omogočajo možnost naslavljanja celotnega globalnega IPv6 omrežja.

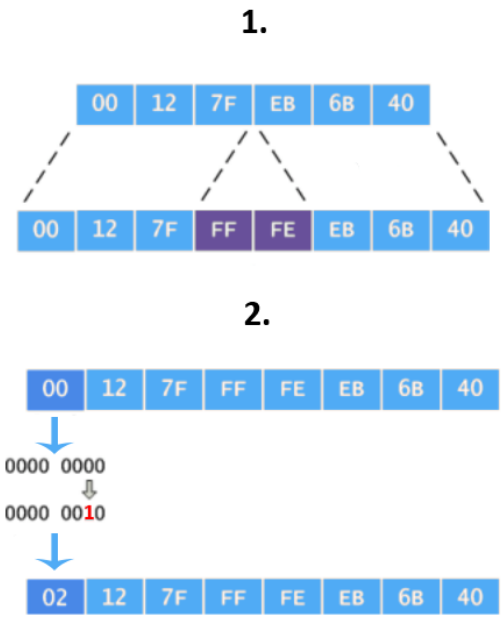


Slika 4: Format "global unicast" naslova

Naslov omrežja (globalne usmerjevalne predpone) je velikosti 48 b. Predstavlja posamezno organizacijo. Sledi 16 bitov namenjenih za usmerjanje in identifikacijo znotraj posamezne organizacije. Zadnjih 64 b identificira končno napravo v IPv6 omrežju. Celoten IPv6 naslov tako hierarhično umesti nek IP naslov preko registrarja, ponudnika internetnih storitev ter organizacije. Hierarhija naslovov je pomembna tudi za boljše zmogljivosti usmerjevalnikov, saj ti ne bodo potrebovali tako obsežnih usmerjevalnih tabel kot do sedaj.

Spodnjih 64 b predstavlja naslov vmesnika. Ta se pridobi na 4 različne načine:

- **Preko vrednosti EUI-64**
  Temelj za izračun predstavlja edinstveni 48 b fizični naslov vmesnika. 48 b razdelimo na 2 dela (2×24 b) ter vmes dodamo 16 b vrednost 0×FFFE. V drugem koraku negiramo 7. bit, kot je prikazano na sliki 5. Rezultat predstavlja spodnjih 64 b edinstvenega IPv6 naslova naprave.



Slika 5: Izračun vrednosti EUI-64

- **Naključno dodeljen naslov**, ki se sčasoma spreminja.
- **Naslov, pridobljen preko t.i. statefull address autoconfiguration** – DHCPv6.
- **Ročna nastavitev vrednosti**

- Link-local unicast naslovi

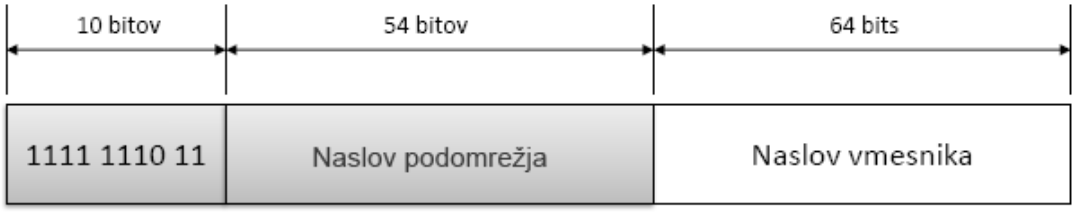
  Ti naslovi se uporabljajo za naslavljanje vmesnika znotraj določenega omrežnega segmenta - povezave. Primer je množica računalnikov, ki med sabo komunicirajo na lokalni ravni. IP naslov lahko dodeli usmerjevalnik, ali pa se ob njegovi odsotnosti naprave same med sabo uskladijo.

Slika 6: Format "link-local unicast" naslova

  Notacija link-local naslovov je oblike FE80::/64.

- Site-local naslovi

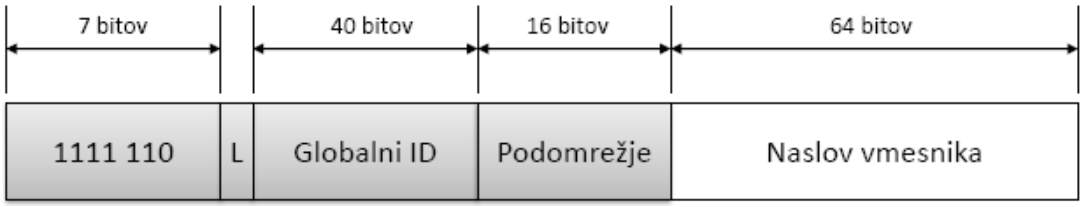
  Omenjeni naslovi imajo podoben namen kot zasebni naslovi v IPv4. Tukaj lahko naslavljamo vmesnike znotraj omrežij, ki niso povezana v internet (npr. intranet okolje)



Slika 7: Format "site-local unicast" naslova

- Unique-local naslovi

  Naslovi unique-local so podobni site-local naslovom - namenjeni so usmerjanju znotraj organizacije, s tem da so glede na druge organizacije enolično določeni. V internetnem omrežju se ne usmerjajo. Vrednost L v formatu je nastavljena na 1, če je predpona dodeljena lokalno.



Slika 8: Format "unique-local unicast" naslova

1.3.2. Multicast

S to vrsto naslovov usmerjevalniki razpošiljajo sporočila množici vmesnikov. Z njim naslavljamo vse vmesnike ali pa vse usmerjevalnike, katerih obseg je določen z dosegom in oznako skupine.

1.3.3. Anycast

Z anycast naslavljamo množico vmesnikov, naslavljamo pa ponavadi najbližjega. Primer je množica DNS strežnikov, ki so dostopni na istem IP naslovu, glede na lokacijo, iz katere naslavljamo, pa se nam odzove tisti, ki nam je najbližje.

Broadcast naslovov pri IPv6 zaradi možnosti napadov z onemogočanjem izvajanja storitve (DoS) ni več.

1.4. ICMPv6

ICMPv6 (angl. Internet Control Message Protocol v4) je internetni protokol, namenjen za tvorjenje kontrolnih sporočil, izvajanje diagnostičnih funkcij (npr. ping6, traceroute6) ter raziskovanje omrežne soseščine (NDP).

Predstavlja naslednika ICMP, ki je bil del internetnega protokola verzije 4. Pomembna razlika med njima je v nujnosti uporabe protokola, saj ICMP kot tak pri IPv4 ni bil zahtevan za nemoten potek komunikacij na omrežni plasti. Pogosto je veljalo, da so administratorji preventivno filtrirali nekatera nevarna ICMP sporočila, ki bi sicer lahko služila napadalcu kot orodje za izvedbo napada.

Eden izmed tovrstnih napadov, ki se je v preteklosti pogosto dogajal, se imenuje PING smrti. Napadalec v tem primeru pošlje paket ICMP ECHO zahteva, ki presega največjo velikost IP paketa (65,535 B). Posledica tega je razbijanje paketa na več delov (fragmentacija). Ker tarča paketa ne more rekonstruirati, lahko to privede do zrušenja operacijskega sistema. Napad se je skušal preprečevati s filtriranjem zunanjih ICMP paketov (ping prometa).

Pri filtriranju ICMPv6 prometa je potrebno biti bolj pozoren, saj je ta protokol bistven za pomembne operacije na omrežni plasti, kot so avtomatska konfiguracija gostiteljev ter determiniranje MTU. Z MTU na povezavah z različnimi vrednostmi tega atributa zagotovimo, da se pri prenosu paketov uporabi ista vrednost za vse gostitelje.

Sporočila, ki jih ta protokol tvori, so dveh tipov: sporočila napak in informacijska sporočila.

Tipi sporočil o napakah so naslednji:

- Nedosegljiv ponor – generira usmerjevalnik ali IPv6 plast kot odziv na paket, ki ga ni moč dostaviti.
- Prevelik paket – sporočilo se generira kot odziv na paket, ki je prevelik (velikost MTU), da bi lahko bil dostavljen ponoru.
- Pretekel čas – tip sporočila se generira, če usmerjevalnik prejme paket z vrednostjo omejitve skokov 0. Do tega pride zaradi kroženja paketa po omrežju ali predhodno prenizko nastavljene vrednosti tega parametra.
- Težava s parametri – služi za pošiljanje obvestila izvoru v primeru, da pride do težave v katerem izmed polj glave IPv6.
- Osebni preizkusi
- Rezervirano za razširitev

Vsako vozlišče mora imeti implementirano tudi funkcionalnost, da se odzove na sporočila tipa ECHO zahteva in ustvari ustrezno sporočilo, ki služi kot odgovor na prejeto zahtevo.

Tipa informacijskih sporočil sta tako naslednja :

- Sporočilo za ECHO zahtevo
- Sporočilo ECHO povratni odgovor

Preostali protokoli/mehanizmi, ki so del funkcionalnosti ICMPv6, so naslednji:

- PMTUD
  Služi za določanje ustrezne velikosti MTU.

- MLD
  Usmerjevalniku služi kot orodje za odkrivanje gostiteljev, ki želijo prejemati pakete tipa multicast.

- MRD
  Služi za odkrivanje multicast usmerjevalnikov.

- NIQ
  Mehanizem uporabljamo za deljenje informacij o gostiteljih v omrežjih med njimi samimi.

- Mobile IPv6
  Uporaba za mobilne komunikacije.

- Protokol za raziskovanje omrežne soseščine – NDP (angl. Neighbor discovery protocol)
  Ta protokol je dejansko nadomestilo za protokole ARP, ICMP router discovery in ICMP preusmeritvena sporočila iz IPv4.

  Ponuja naslednje možnosti:

  - iskanje parametrov,
  - iskanje usmerjevalnikov,
  - iskanje predpon
  - samodejno nastavljanje naslovov,
  - resolucija naslovov,
  - zaznavanje,
  - ugotavljanje nedosegljivosti sosedov,
  - ugotavljanje podvojenih naslovov,
  - določanje naslednjega HOP-a,
  - preusmeritve.

  Ker NDP kot tak ne vsebuje nikakršne zaščite pred morebitnimi zlorabami, je bil v letu 2005 po RFC3971 standardu uveden varni NDP - **SEND** (angl. Secure Neighbor Discovery). Ta vzpostavlja zaupanja vreden model gostiteljev na področju LAN. NDP razširja s tremi dodatnimi zmožnostmi:

  - zaščitna IP naslovov (par ključev – zasebni : javni),
  - zaščita sporočil (RSA podpis, zaščita integritete),
  - avtorizacija usmerjevalnika,

  Glavne značilnosti te tehnologije so:

  - Možnost uporabe mehanizma se nanaša na vsa NDP sporočila.
  - Z uporabo SEND je kraja IPv6 naslova praktično »nemogoča«.
  - Lahko se uporabi pri postopkih odkrivanja usmerjevalnikov, razreševanja naslovov in odkrivanju podvojenih naslovov.
  - Zahteva in posledični odziv sta vedno v korelaciji.

  Vsako vozlišče si pred začetkom komunikacije vzpostavi svoj par ključev (javni : zasebni). Preko naključnega števila, javnega ključa in predpone podomrežja se preko SHA-1 algoritma izračuna povzetek, ki določa identifikator vmesnika. Skupaj z omrežno predpono tvorita **kriptografsko določen naslov naprave** (angl. Cryptographically Generated Address - CGA). S takšnim naslovom dosežemo zagotovilo, da je pošiljatelj sporočil ND protokola dejansko lastnik naslova s katerim se legitimira.

  V primeru, da želi gostitelj X raziskati MAC naslov gostitelja Y, mu pošlje NS zahtevo za kriptografsko določen naslov (CGA) naprave Y. Ta odgovori z digitalno podpisanim NA-sporočilom, ki poleg IPv6 naslova vsebuje tudi CGA parametre, s katerimi je Y izračunal svoj kriptirani naslov.

Gostitelj X tako na drugi strani preko javnega ključa CGA parametrov preveri podpis. S tem se potrdi pristnost CGA parametrov z gostiteljem Y.

V protokolu NDP imajo pomembno mesto tudi RA oglaševalska sporočila usmerjevalnika. Pomembno bi bilo zagotoviti, da je vsako RA sporočilo podpisano s strani usmerjevalnika, ki ga razpošilja. Ta varnostna zaščita terja vpeljavo X.509 certifikatov, ki predstavljajo standard javne infrastrukture ključev. Certifikat ter podpis se skupaj preneseta preko RA sporočil k naslovniku. Ker je certifikat izdan s strani pooblaščene ustanove za izdajanje in upravljanje z digitalnimi certifikati, lahko naslovniki usmerjevalniku zaupajo v poslane informacije.

Protokol SEND vpeljuje v omrežje dodatno kompleksnost. Uporaba certifikatov in kriptografskih postopkov pomeni zamike pri pošiljanju sporočil ter obremenjevanje virov (angl. resource) enot, ki procesirajo informacije. Operacije nad javnimi ključi so namreč lahko precej kompleksne. Problem je tudi v majhnem številu implementacij, ki bi potrdile/ovrgle prednosti tega protokola.

NDP nam torej omogoča razreševanje medsosedskih odnosov naprav (vmesnikov ali usmerjevalnikov) v omrežju. Naprave se na ta način lahko samodejno konfigurirajo, razrešujejo naslove ali iščejo usmerjevalnike. Usmerjevalniki na drugi strani vmesnikom oglašujejo svojo prisotnost in nastavitvene parametre na določeni povezavi.

Protokol NDP definira 5 tipov sporočil, ki temeljijo na ICMPv6 sporočilih ter rešujejo medsebojne relacije med vozlišči na isti povezavi (link):

a) **NS – Neighbor Solicitation**
   Pošljemo vozlišču v omrežju za ugotavljanje naslovov sosedov in ugotavljanje dosegljivosti IP naslova. Uporablja se tudi za ugotavljanje podvojenih IP naslovov.

b) **NA - Neighbor Advertisement**
   Sporočilo je poslano kot odgovor na NS. Uporablja se tudi za oznanjevanje spremenjenih naslovov. NS in NA sporočila se izmenjujejo s ciljem tvorjenja parov IP naslov – fizični naslov vmesnika.

c) **RS – Router Solicitation**
   Sporočilo se uporabi kot zahteva, da usmerjevalnik / pošlje sporočilo tipa RA.

d) **RA – Router Advertisement**
   S sporočilom usmerjevalniki naznanijo svojo prisotnost in sporočijo parametre kot so nastavitev omrežne predpone, omejitve skokov…

e) **Redirect**
   Uporabljajo usmerjevalniki za obveščanje gostitelja, da obstaja boljši izbor poti za doseganje ciljnega naslova.

1.5. IPsec

Glavni namen IPsec je zagotavljanje varnostnih mehanizmov na omrežni plasti oziroma IP plasti modela TCP/IP:

- **ZAUPNOST**
  Z njo zagotavljamo, da podatki niso dosegljivi nepooblaščeni osebi. Zagotavljamo jo z uporabo šifriranja. Tvorimo skrivni ključ s pomočjo katerega lahko podatke šifrirata in dešifrirata samo izvor in ponor.

- **INTEGRITETA PODATKOV**
  S to lastnostjo ima prejemnik možnost, da ugotovi, ali je dejansko prejel podatke takšne, kot jih je poslal pošiljatelj. Tako lahko imamo nadzor nad spreminjanjem podatkov na transportni poti.

- **AVTENTIKACIJA**
  Potrebna je, da se točki, ki se med sabo povezujeta in želita komunicirati, medsebojno identificirata. S tem imamo možnost ugotoviti, če so podatki res poslani iz pristnih virov.

- **ZAŠČITA PRED ODGOVORI**
  Isti podatki niso poslani večkrat in dostava je več ali manj v skladu z redom, kakršen je določen pri odpošiljanju. Vsekakor pa IPsec ne zagotavlja, da bo vrstni red identičen, kot je pri odposlanem toku podatkov.

- **ZAŠČITA PRED ANALIZO PROMETA**
  Z njo želimo preprečiti, da bi si vohljač s pomočjo opazovanja prometa ustvaril pravo sliko in pridobil koristne informacije.

- **NADZOR DOSTOPA**
  Omogoča filtriranje dostopa v posamezna območja. Tako lahko preprečujemo neavtorizirane dostope kot tudi blokiramo določen tip omrežnega prometa.

Glavni **gradniki IPsec-a** so:

1. Dogovor o načinu šifriranja in izmenjava ključev

   Strani se morata dogovoriti o:

   - algoritmu in ključu za overjanje (AH) in za šifriranje podatkov (ESP),
   - IP naslovih,
   - časovni veljavnosti ključev,
   - ostalih neobveznih parametrih.

   IPsec arhitektura, ki definira mehanizme za izmenjavo ključev, se imenuje **IKE** (angl. Internet Key Exchange).

2. Preverjanje nespremenjenosti podatkov in overjanje brez šifriranja (AH)

Paketu dodamo glavo AH, ki vsebuje povzetek vsebine paketa – podatki se na tem mestu ne šifrirajo.

3. Šifriranje podatkov

   Za protokol ESP.

V okviru **varnostne zveze** (angl. security associations - SA) se vzpostavi enosmerna povezava za varovani tok podatkov (dvosmerni promet zahteva dve zvezi).

V povezavi z vzpostavljanjem varnostne zveze se določijo 3 parametri:

- SPI – kazalec varnostnih parametrov,
- ciljni IP naslov,
- identifikacija varnostnega protokola (AH ali ESP).

Poznamo dva načina varnostne zveze:

- varnostna zveza v **transportnem načinu** (za povezovanje dveh končnih računalniških sistemov; s tem načinom ne moremo med sabo povezovati omrežij);
- varnostna zveza v **tunelskem načinu** (za povezovanje dveh vmesnih sistemov – varnostnih prehodov na poti med dvema končnima točkama).

Glavna razlika med načini je v obsegu varovanja paketa.
Tunelski način za razliko od transportnega varuje celoten paket vključno z IP glavo. Pri njemu je tako moč pri dobrem šifriranju sklepati le o točkah, med katerima poteka povezava, vse ostalo ostane skrivnost.

1.5.1. Protokol AH

Za postopek avtentikacije pri vzpostavitvi varnostne zveze se uporablja protokol **AH** (angl. Authentication Header), ki skrbi za zagotavljanje integritete koristnih podatkov (brez glave IP) in avtentičnost pošiljatelja, nima pa zmožnosti kriptiranja informacij. V primerjavi z ESP se izkaže za bolj racionalnega v primerih, ko potrebujemo samo overjanje.

Ključne značilnosti AH so:

- Omogoča nepovezavno celovitost (zagotovilo, da prejeti podatki med potjo niso bili spremenjeni)
- Omogoča avtentikacijo izvora podatkov
- Zagotavljanje zaščite proti IP-spoofing in Reply napadom

Preden si dve IPv6 končni točki začneta preko IPsec protokola izmenjevati pakete, se morata pogoditi glede avtentikacijskega algoritma in ključa, kriptirnega algoritma in ključa ter metod izmenjave ključev, ki se bodo posodabljali in izmenjevali tekom komunikacije. Kot že omenjeno, je za to zadolžen **IKE**, ki se izvaja v dveh fazah:

I. FAZA

V prvem koraku se strani dogovorita o uporabi varnostnih protokolov, ki jih uporabita tekom te faze.
V drugem koraku preko protokola Diffie-Hellman tvorita skrivni ključ. Ta je osnova za tvorjenje še treh ključev, ki se dalje uporabljajo za avtentikacijo in šifriranje podatkov.
V tretjem koraku se sistema medsebojno avtenticirata. Za te namene se lahko poslužimo digitalnih certifikatov (pridobljenih s strani priznanega cirtifikatnega urada) ali pa uporabimo predhodno določen skupni ključ (angl. Pre-shared key).

II. FAZA

Strani vzpostavita varnostno zvezo.

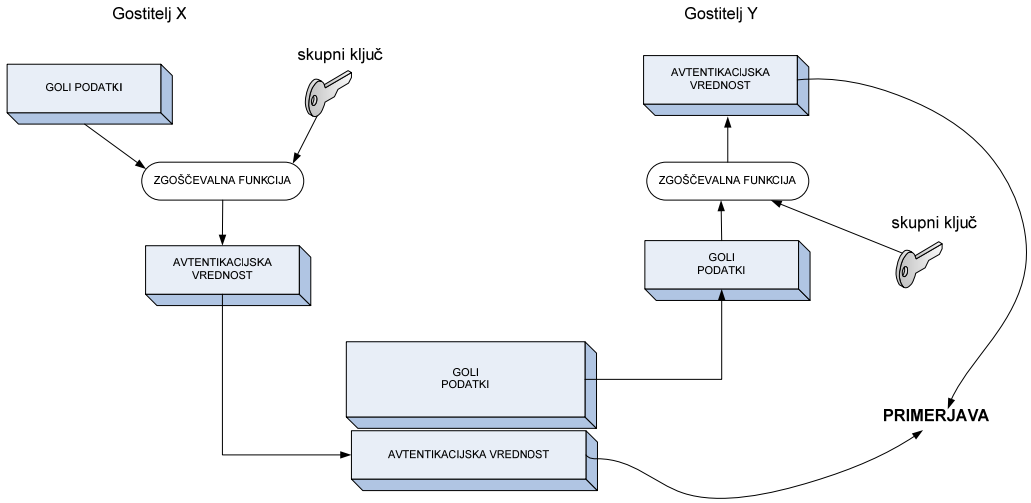
Pri avtentikaciji se uporablja **zgoščevalna funkcija** simetričnega ključa. To pomeni, da tako pošiljatelj kot naslovnik za zagotavljanje avtentikacijske vrednosti uporabljata enak ključ.

Zgoščevalna funkcija dejansko preslika nek niz znakov v blok konstantne dolžine, ki predstavlja prstni odtis vhodne sekvence znakov. Funkcija z varnostnega vidika predstavlja naslednje koristi:

- praktično nemogoče je najti dve različni sporočili, ki bi se s pomočjo zgoščevalne funkcije preslikali v isti blok;
- iz zgoščevalnega bloka je nemogoče restavrirati izvorna sporočila;
- isto sporočilo se vedno preslika v enak blok;
- tudi najmanjša sprememba v izvornem sporočilu spremeni vsebino zgoščevalnega bloka.

Vse to predstavlja nepooblaščeni osebi visoko prepreko pri poizkušanju manipulacije sporočil med pristnim izvorom in ponorom.

Postopek avtentikacije se prične z izračunom povzetka s pomočjo HMAC-SHA1 (128b ključ) ali HMAC-MD5 (160b ključ) algoritmov. Ta se vzporedno s pošiljanjem golega besedila pošlje k naslovniku, ki kot že rečeno, uporabi za izračun isti ključ, kot pošiljatelj (angl. shared key). Ko naslovnik iz prejetega sporočila izračuna povzetek na svoji strani, se sproži primerjava.

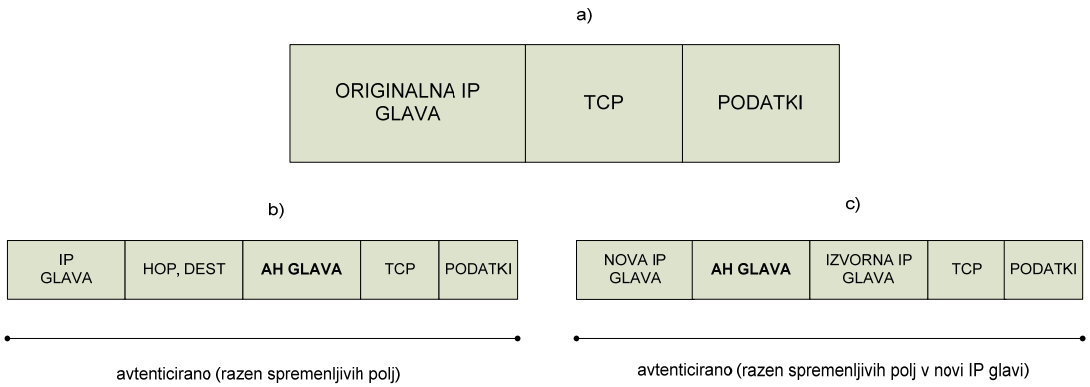


Slika 9: avtentikacijski postopek IPsec: za izračun primerjalne vrednosti je potrebno poznati zgoščevalno funkcijo in ključ

V uvodu tega podpoglavja sem omenil, da je lahko varnostna zveza vzpostavljena v transportnem ali tunelskem načinu. Razlike med obema načinoma se pri uporabi v protokolu IPv6 izražata na naslednji način.

Pri prvem je glava AH postavljena za IP glavo. Za avtentikacijo se uporablja celoten paket. Spremenljivim in nepredvidljivim poljem (npr. časovni žig) se dodeli vrednost 0 pred izračunom. AH glava je postavljena za osnovno IP glavo in za polji možnosti ter razširitev, kot so: hop-by-hop možnosti, ponorne možnosti in razširitve za fragmentiranje ter usmerjanje.

Pri tunelskem načinu IPv6 glava in podatki postanejo tovor (angl. payload) za nov paket. Avtentikacija zajema vsa polja paketa razen spremenljivih polj nove IP glave.



Slika 10: Originalna struktura paketa brez AH (a) in struktura z AH v transportnem (b) in tunelskem (c) načinu

1.5.2. Protokol ESP

ESP (Encapsulating Security Payload) ponuja možnost kriptiranja omrežnega prometa. S tem zagotovimo zaščito paketov za varen pretok podatkov po omrežju.

Ključne značilnosti ESP so:

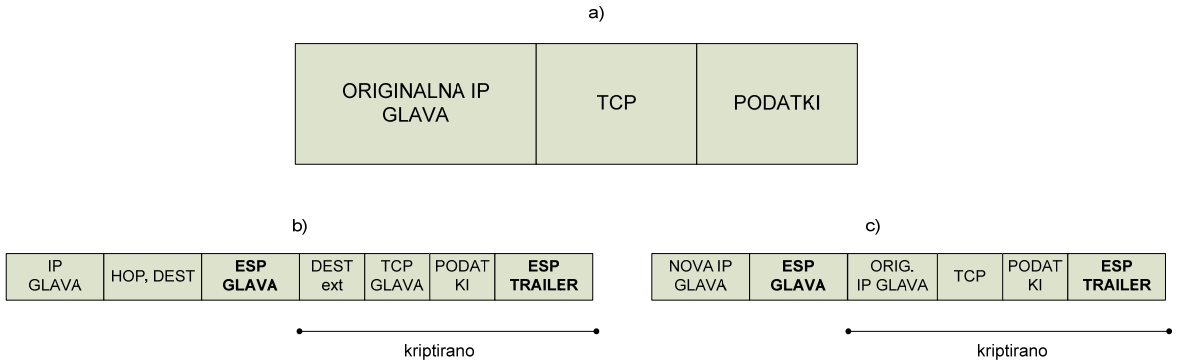
- Omogoča kriptiranje podatkov
- Zagotavlja zaupnost
- Omogoča nepovezavno celovitost
- Omogoča avtentikacijo izvora podatkov

Kriptiranje poteka preko skupnega ključa in naslednjih kriptirnih algoritmov:

- DES-CBC (56b dolžina ključa),
- 3DES-CBC (56b dolžina ključa za vsako iteracijo),
- AES128-CBC (128b dolžina ključa)

CBC (angl. Cipher Block Chaining) predstavlja način uporabe DES algoritma in je podrobno opisan z dokumentom RFC (angl. Request For Comments) 1829.

Tudi tu se način kriptiranja in avtentikacije razlikuje glede, na to v kakšnem načinu izvajamo varnostno zvezo.



Slika 11: Originalna struktura paketa brez ESP (a) in struktura z ESP v transportnem (b) in tunelskem (c) načinu

ESP kriptirni mehanizem kot sam nam ne nudi nobene zaščite glede avtentikacije in integritete podatkov. Dodatno varnost lahko zagotovimo z:

- **Uporabo avtentikacijskega ESP formata**
  Za kriptiranje uporabnih podatkov se uporabi simetrični ključ, za izračun avtentikacijske vrednosti kriptiranih podatkov pa uporabimo drugi simetrični ključ ter HMAC-SHA1 ali HMAC-MD5 algoritem. Avtentikacijska vrednost se pripne na konec paketa. Prejemnik na drugi strani sprva preveri avtentičnost podatkov, nato pa jih še dekodira.

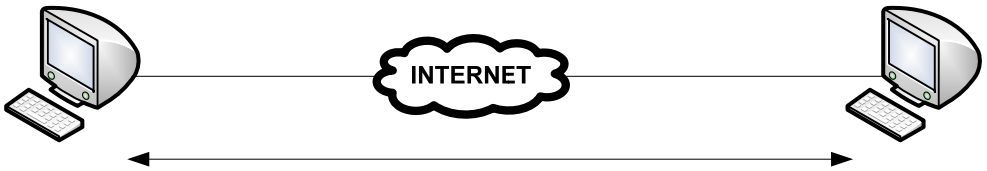
- **Gnezdenje ESP v AH mehanizem**
  Primer: 3DES-CBC ESP paket lahko vgnezdimo v HMAC-MD5 paket.

1.5.3. Področja uporabe

Glavno področje zaščite je v preteklosti temeljilo na komunikacijah preko navideznih zasebnih omrežij (VPN). Pri tej vrsti omrežja gre za povezavo med dvema točkama, med katerima je postavljen tunel skozi javno omrežje, v katerem je potrebno zagotoviti varen in zanesljiv tok podatkov.

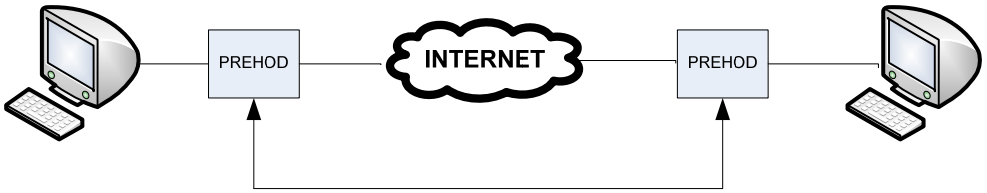
Dve strani lahko pri uporabi IPsec protokola komunicirata na 4 različne načine [10]:

- **Dva sistema preko internetnega omrežja vzpostavita varno IPsec povezavo.** Takšen model je ponavadi uporabljen v primerih, ko preko zaupanja vredne skupine uporabnikov administriramo ali vršimo samo dostop do oddaljenih sistemov. Za uporabnika ni transparenten, saj se mora pred začetkom uporabe avtenticirati.

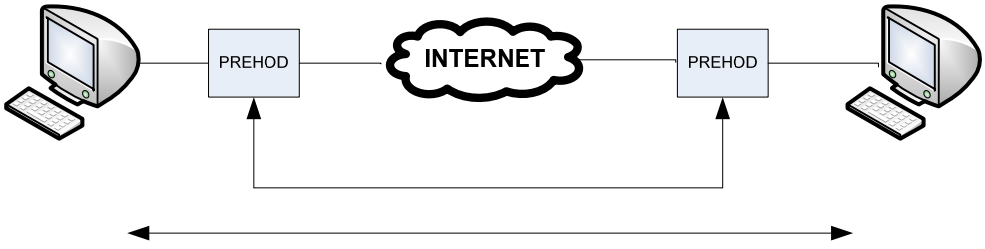


Slika 12: Primeri uporabe IPsec zaščite

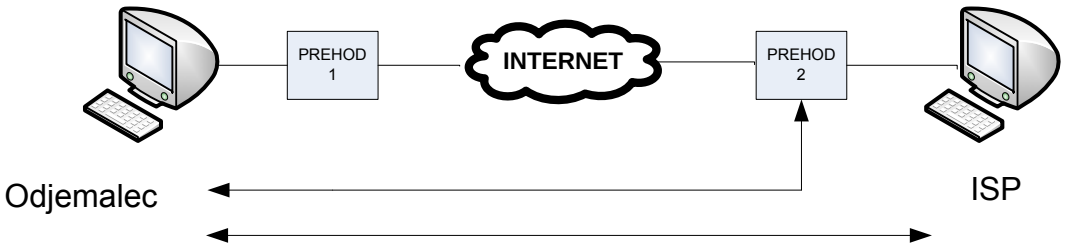
- **Komunikacija med dvema prehodoma (angl. gateway),** na katera sta priključeni lokalni omrežji. Povezava med varnostnima prehodoma je za razliko od povezave med prehodom in končnim vozliščem zaščitena. IPsec, ki vzpostavi tunel med prehodoma, lahko zaščiti promet med dvema omrežjema. Za zaščito večjega števila razredov prometa je potrebno vzpostaviti več IPsec povezav, vsako za svojega.
  Nezaščitena pa ostaja povezava med prehodom in ciljnim sistemom. Promet, ki poteka med njima, lahko brez težav zajemamo z ustreznim programskim orodjem.



- Tretji primer odpravlja varnostno tveganje nezaščitene povezave med varnostnim prehodom in odjemalci v njegovem omrežju. **Tu je zaščitena tudi zveza med končnima računalniškima sistemoma.**



- **Primer povezovanja s ponudnikom internetnih storitev (angl. internet service provider).** Odjemalec od njega dobi IP naslov in vzpostavi tunel s prehodom 2. Zatem vzpostavi še tunel v transportnem načinu s končnim sistemom (ISP). Varnostni prehod 2 mora biti sposoben prepuščati promet IPsec in upravljanja z izmenjanimi ključi.



Poleg gradnje navideznih zasebnih omrežij se protokol IPsec uporablja še v naslednjih primerih:

- varna povezava IPsec naprav ali lokalnih omrežij,
- varen dostop do oddaljenih računalnikov,
- varen dostop mobilnih uporabnikov.

1.6. Kompatibilnost IPv4 in IPv6

Protokola med sabo nista kompatibilna oz. sta kompatibilna na nivoju žice. To pomeni, da si lahko delita isto fizično infrastrukturo in bivata sočasno.

Obdobje prehoda do čiste IPv6 infrastrukture bo trajalo precej časa. Vsekakor pa je v tem prehodnem obdobju pomembno, ne glede na izbrano infrastrukturo, zagotoviti povezljivost omrežnih naprav in zagotoviti dostop do vsebin in storitev.

Tako so se sčasoma razvile tehnike za soobstoj obeh protokolov, t.i. **tranzicijski mehanizmi** (angl. transition mechanisms):[5]

- Uporaba obeh protokolov
  - arhitektura dvojne IP plasti (Double IP layer)
  - arhitektura dvojnega sklada (Dual stack)
- Tunelski mehanizem IPv6 skozi IPv4
- Translacija protokola

1.6.1. Uporaba obeh protokolov

Slika 13: Uporaba dvojnega sklada : razvoj IPv4 in IPv6 na isti infrastrukturi

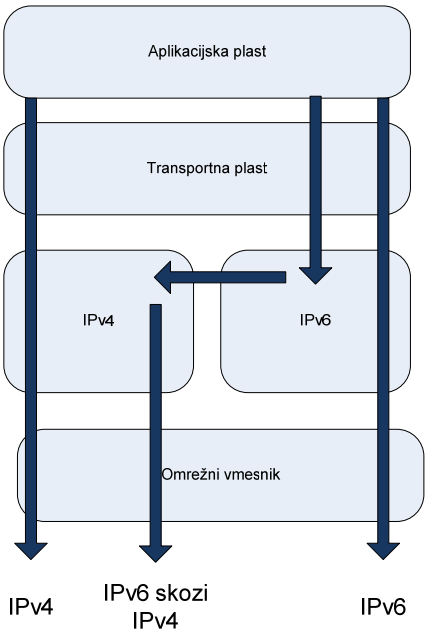
Dvojni sklad nam zagotavlja, da se ne glede na vrsto prometa vsak paket obdeluje v svojem protokolnem skladu. Implementiran je lahko kot del operacijskega sistema končnega uporabnika ali pa v omrežnem usmerjevalniku.

Usmerjevalnik z dvojnim skladom lahko posreduje IPv4 in IPv6 promet. Nadgradnja za takšen način delovanja je lahko programska, čeprav se bodo z rastjo količine prometa začele porajati potrebe po strojni izvedbi. V primeru souporabe protokolov IPv4 in IPv6 je potrebno vzdrževati usmerjevalni tabeli za oba protokola.

Na nivoju implementacije dvojnega sklada kot del operacijskega sistema aplikacije same izbirajo protokolni sklad. Razlika med obema arhitekturama je v implementaciji protokolov na transportni plasti. Za razliko od arhitekture dvojne plasti, kjer so protokoli transportne plasti enkratno implementirani za obe verziji (IPv4 in IPv6), je pri arhitekturi dvojnega sklada implementacija takšna, da paketa obeh verzij IP protokolov preko transportne plasti potujeta neodvisno drug od drugega.

- **Arhitektura dvojne IP plasti**

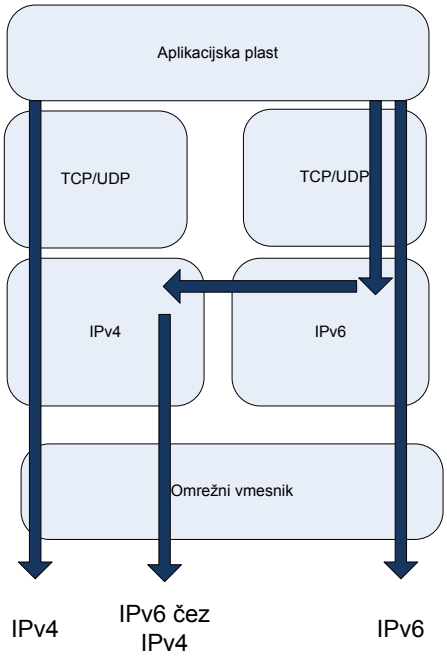
  Ta arhitektura vsebuje oba protokola z enkratno implementacijo protokolov na transportni plasti. Vrste paketov, ki se pojavljajo, so tipa IPv4, IPv6 ali IPv6 skozi IPv4.



Slika 14: Tipi paketov pri arhitekturi dvojne IP plasti

- **Arhitektura dvojnega sklada**

Podobna je arhitektura dvojnega sklada, pri čemer sta tu implementaciji transportne plasti ločeni. Ta arhitektura predstavlja dominantno tranzicijsko strategijo.



Slika 15: Tipi paketov pri arhitekturi dvojnega sklada

IPv6 čez IPv4 predstavlja ovijanje IPv6 paketa z glavo IPv4 z namenom, da so lahko IPv6 paketi poslani preko IPv4 omrežne infrastukture.

Mehanizem dvojnega sklada si deli vse ranljivosti, ki lahko prizadenejo izvirni IPv4 in IPv6 omrežji.

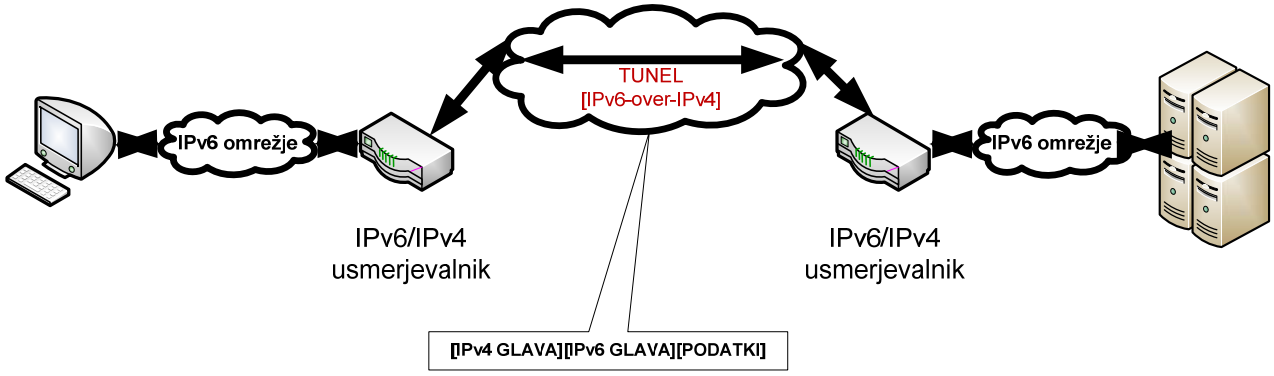
1.6.2. Tunelski mehanizem IPv6 skozi IPv4

Tunel je povezana pot med dvema vozliščema in predstavlja rešitev za prenos IPv6 prometa čez obstoječo IPv4 infrastrukturo. S tem izkoristimo obstoječo IPv4 usmerjevalno topologijo in zmogljivost infrastrukture.

Tuneli se lahko vzpostavijo na 4 različnih relacijah:

- usmerjevalnik – usmerjevalnik (slika 16),
- gostitelj – usmerjevalnik,
- gostitelj – gostitelj,
- usmerjevalnik – gostitelj.

Bistvo ideje tuneliranja je v ovijanju (angl. encapsulation). IPv4/IPv6 gostitelji ter usmerjevalniki lahko tunelirajo IPv6 datagrame skozi IPv4 usmerjevalno topologijo z ovijanjem v IPv4 pakete. Z drugimi besedami povedano: uporabimo IPv4 pakete kot transportni medij, v katerega vložimo IPv6 pakete.



Slika 16: Princip tuneliranja in zgradba paketa: tunel povezuje usmerjevalnika, ki ponavadi vsebujeta dvojni sklad.

Tipi tunelov:

- **ISATAP** (angl. Intra-Site Automatic Tunnel Addressing protocol)
  Protokol ISATAP povezuje gostitelje, ki uporabljajo arhitekturo dvojnega sklada in so izolirani s čistim (angl. native) IPv4 omrežjem. Uporablja se za medsebojno izmenjavo IPv6 prometa in izmenjavo prometa z globalnim IPv6 internetom.
  Ta protokol omogoča avtomatsko tuneliranje ne glede na to, ali gostitelj uporablja javni ali zasebni IPv4 naslov. ISATAP naslov formira z uporabo avtomatskih mehanizmov za pridobivanje IPv6 naslova.

  Format ISATAP naslova:

  Unicast predpona (64 b) : 0 : 5EFE : a.b.c.d, kjer je a.b.c.d zasebni IPv4 unicast naslov.

ali

Unicast predpona (64 b) : 200: 5EFE : a.b.c.d, kjer je a.b.c.d javni IPv4 unicast naslov

Naslov formiran preko ISATAP, je lahko klasični IPv4 naslov (IPv4 medgostiteljsko povezovanje), IPv6 povezavno-lokalni (izmenjava prometa med direktno povezanimi gostitelji ali usmerjevalniki) ali pa IPv6 globalni unicast.

- **6to4**
  Je tehnologija za določanje naslovov ter avtomatsko vzpostavitev tunelov na relacijah usmerjevalnik – usmerjevalnik, gostitelj – usmerjevalnik ali usmerjevalnik – gostitelj. 6to4 je bil zasnovan za komunikacijo posameznih IPv6 paketov skozi IPv4 omrežja brez potrebe po eksplicitnem vzpostavljanju tunela.

  Format 6to4 naslova:

  2002_{Hex} | javni IPv4 naslov (32 b) | ID podomrežja (16 b) | ID vmesnika (64 b)

  Funkcije, ki jih izvaja tehnologija 6to4, so naslednje:
  - dodelitev IPv6 naslova gostitelju, ki ima globalno dosegljiv IPv4 naslov;
  - ovijanje IPv6 paketa v IPv4 paket (IPv4 glava z vrednostjo »protocol type« 41);
  - usmerjanje prometa med 6to4 in čistimi IPv6 omrežji.

  6to4 pristop je bil zasnovan za enostavno povezovanje izoliranih IPv6 strani, ki tako niso odvisne od svojih IPv4 ponudnikov spletnih storitev (ISP) in njihovih implementacij IPv6 protokola.

- **Teredo**
  Teredo mehanizem omogoča tuneliranje unicast prometa (IPv6/IPv4) gostiteljem, ki se nahajajo za enem ali več IPv4 NAT mehanizmov. Teredo gostitelji tunelirajo IPv6 promet v IPv4 UDP paketih, katerih koristna vsebina sta glava in vsebina IPv6 paketa.

  Format Teredo IPv6 naslova:

  Teredo predpona (32 b) | IPv4 naslov Teredo strežnika (32 b) | Zastavice (16 b) | Preslikana odjemalčeva UDP vrata (16 b) | Preslikan odjemalčev IPv4 naslov (32 b)

- **Posredniški tuneli** (angl. Tunnel Broker)
  Posrednike tunelov predstavljajo organizacije, ki omrežnim gostiteljem ali usmerjevalnikom z dvojnim skladom omogočajo vzpostavljanje tunela za njihovo povezljivost v IPv6 omrežje. Tunel povezuje končni računalniški sistem (ali usmerjevalnik) z robno točko ponudnika za posredovanje tunelov.

Tuneli se lahko nastavljajo avtomatsko (6to4, ISATAP, posredniški) ali pa je za delovanje parametre potrebno vnesti ročno. Pri prvem načinu se tunel vzpostavi samodejno med robnima omrežjema. Naslov, ki predstavlja ponor na robni točki, je vsebovan v ponornem naslovu IPv6 paketa. Drugi tip tunelov zahteva ročno vzpostavitev parametrov. Uporabljajo se, kadar uporabljamo IPv6 naslove, ki ne vsebujejo ciljnih IPv4 naslovov gostiteljev.

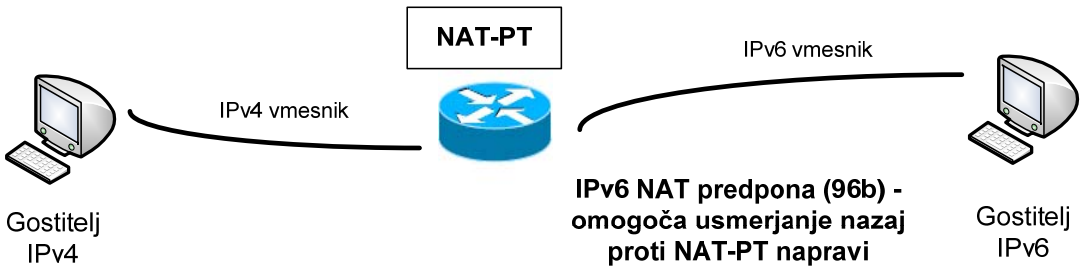
1.6.3. Translacija protokola

Tolmač protokola deluje kot vmesni člen med IPv4 in IPv6 svetovoma. Ta rešitev je kompleksna, poleg tega pa ni moč zagotoviti, da se tekom translacije popolnoma vse informacije ohranijo.

Slika 17: Uporaba translacijskega mehanizma

Pregled translacijskih mehanizmov

- **NAT-PT (angl. Network Address Translation-Port Translation)**
  Mehanizem omogoča IPv6 gostiteljem in njihovim aplikacijam komunikacijo z IPv4 gostitelji in njihovimi aplikacijami ter komunikacijo v nasprotni smeri (naslove torej prevaja v obeh smereh). Za svojo uporabo zahteva tako IP kot IPv6 tabele.



Slika 18: Koncept delovanja NAT-PT

Primer uporabe IPv6 gostitelja PC X, ki želi komunicirati s spletno stranjo www.yyy.com (IPv4):

  - Ob vpisu url naslova v spletni brskalnik njegov računalnik pošlje na DNS strežnik poizvedbo tipa AAAA (IPv6 naslovni zapis).
  - NAT-PT paket prestreže ter naredi vez med PC X ter IPv4 naslovom iz svojega bazena naslovov.
  - Za novo ustvarjeni paket IPv4 NAPT poišče ustrezno pot ter paket pošlje na DNS strežnik IPv4 omrežja.
  - DNS pošlje odgovor (A zapis) in NAT-PT ga ponovno prestreže. Nato poišče ustrezen IPv6 naslov za preslikavo ter z dodajanjem NAT-PT predpone iz zapisa A tvori zapis AAAA.
  - Pošiljanje DNS zapisa gostitelju PC X.

Za nemoteno komunikacijo mora mehanizem NAT-PT vzdrževati tri različne bazene naslovov – vsakega za svoj protokol: TCP, UDP, ICMP.

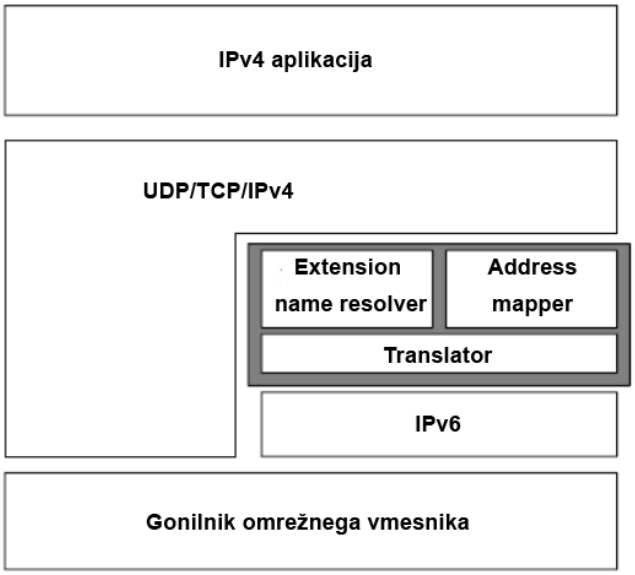
- **BIS (angl. Bump-In-the-Stack Mechanism)**
  BIS je translacijski mehanizem med IPv4 aplikacijo ter IPv6 omrežjem. IPv4 promet je preveden v IPv6 in obratno. Omogoča komunikacijo aplikacije na strani gostitelja z bodisi IPv4 ali IPv6 gostiteljem na drugi strani.

Sestavljen je iz 3 komponent:

- Translator
  Njegova naloga je spreminjanje IPv4 glave v glavo IPv6, fragmentacija paketa in razpošiljanje paketov, ki jih tvorijo IPv4 aplikacije, v IPv6 omrežje.

- Extension name resolver
  Namenjen tvorjenju odzivov IPv4 aplikacijam, ki tipično dajejo zahteve po razreševanju IP naslovov tipa A.

- Address mapper
  Zadolžen je za vzdrževanje bazena IPv4 naslovov ter vzdrževanje relacij med pari naslovov IPv4 – IPv6.



Slika 19: BIS- protokolni sklad

Mehanizem je uporaben v prehodnem obdobju uvajanja čistega IPv6 protokola. Večno pa bo služil za programsko opremo (aplikacije), ki nikoli ne bodo nadgrajene za uporabo z IPv6 protokolom.

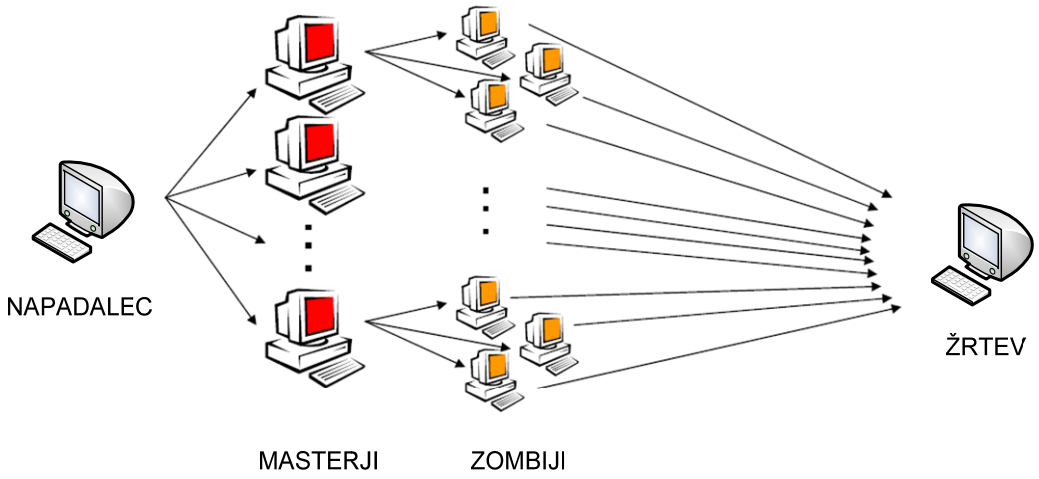
Poleg opisanih translacijskih mehanizmov obstajajo še TCP-UDP relay, BIA (angl. Bump-in-the-api), SOCKS-based gateway.

2. Pregled napadov skupnih v omrežjih IPv4 in IPv6

2.1. DoS/DDoS

Kratici **DoS** (angl. Denial-of-Service-attack) in **DDoS** (angl. Distributed Denial-of-Service-attack) označujeta napad z namenom onemogočanja (zavrnitve) izvajanja storitve, ki temelji na IP protokolu. V svetu interneta predstavljata s stališča varnosti in nemotenega delovanja omrežja vodilno grožnjo.

DDoS ima za razliko od DoS še karakteristiko distribucije. V tem primeru napadalca predstavlja množica povezanih gostiteljev iz različnih lokacij, ki imajo en sam cilj – simultan napad in onemogočanje izvajanja storitve – ponavadi takšne, ki je namenjena širšim krogom uporabnikov (bančne storitve, napad na domenske strežnike).



Slika 20: Grafični prikaz direktnega DDoS napada. Ponavadi obstaja vsaj en napadalec, žrtev ter razširjeno omrežje gostiteljev (zombiji)

Najpogostejši načini izvedbe tega napada so: [18]

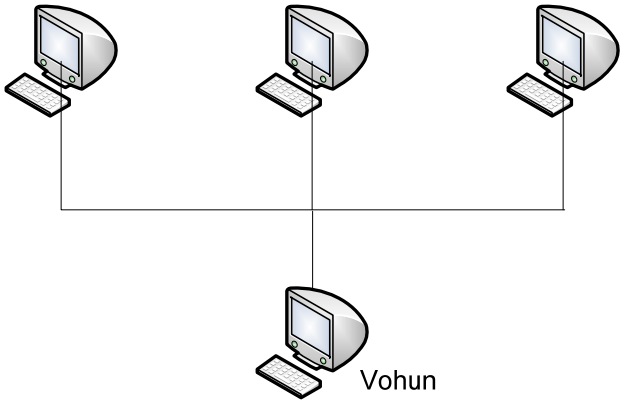
- poraba sistemskih virov (pasovna širina, procesorska zmogljivost),
- zastrupljanje konfiguracijskih nastavitev usmerjanja,
- prekinjanje medija za pretok podatkov med ponudnikom storitev in uporabniki,
- razdor povezav med fizičnimi komponentami v omrežju.

Pri napadih, v nadaljevanju poglavja katerih cilj je povzročitev DoS, bom v nadaljevanju to eksplicitno poudaril.

2.2. Vohunjenje (angl. sniffing)

Vohunjenje je način sledenja in prestrezanja podatkov, ki se pretakajo po omrežju in jih je praktično moč zajeti.

Vohuni so programske aplikacije, ki so zmožne spremljati pakete na mrežni plasti standarda TCP/IP. Postavljeni so med dvema vozliščema, ki sta lahko bodisi del lokalnega omrežja (angl. LAN) bodisi del prostranega računalniškega omrežja (angl. WAN).



Slika 21: Primer vohunjenja v lokalnem omrežju

Koristi, ki jih lahko ima nepooblaščena oseba pri vohunjenju po omrežju, so vezane predvsem na pridobivanje podatkov pri protokolih na aplikacijskem sloju, ki pri prenosu uporabljajo golo besedilo (podatke, ki niso šifrirani). Primer sta protokola POP3 in SMTP.

Načina prestrezanja omrežnega prometa sta dva. Razlikujeta se glede na to, ali je potrebno za doseganje cilja poseči tudi po suplementarnih tehnikah (npr. zastrupljanje ARP (IPv4) – več o tem v nadaljevanju) ali pa se samo priključimo v omrežje:

- **AKTIVNI** način (deluje v omrežjih z mrežnimi stikali (angl. switch), kjer se promet pošilja skupini odjemalcem, usmerjanje pa poteka na podlagi fizičnih naslovov naprav (angl. MAC)).

- **PASIVNI** način (deluje v omrežjih z razdelilniki (angl. Hub), ki spadajo po standardu OSI v fizično plast in kjer se na podlagi električnih signalov signal širi v vsa vozlišča).

2.2.1. Aktivno vohunjenje

Najbolj znana načina aktivnega vohunjenja sta MAC poplavljanje in zastrupljanje ARPa.

Poplavljanje MAC (angl. MAC flooding) temelji na principu delovanja stikala. Ti imajo v svojem pomnilniku vgrajeno tabelo (CAM), ki povezuje fizične naslove priklopljenih naprav z vrati, skozi katere se vrši pretok podatkov k odjemalcem. Če zagotovimo, da se tabela zapolni do svoje maksimalne kapacitete, je lahko odraz tega pošiljanje paketov skozi vsa vrata stikala (razpršeno oddajanje). To pomeni, da se v omrežju pojavi ogromno podatkov, kar je lahko za napadalca, ki filtrira samo določene, tudi moteče.

Zastrupljanje ARP tabel (angl. ARP cache poisoning) izkorišča možnost prevare tabel, ki so zadolžene za preslikavo naslova internetnega protokola v fizični naslov vmesnika. Preden se dva računalnika sploh povežeta, je potrebno, da se opravi povezovanje IP naslovov s fizičnima enoličnima naslovoma obeh naprav. Če se torej želi računalnik A povezati z B v IPv4 omrežjih,

mora v omrežje na razprševalni naslov poslati zahtevo ARP, ki želi kot povratno informacijo dobiti fizični naslov računalnika B. Ko/če ga prejme, si vrednost shrani v svoj predpomnilnik ARP.

S pomočjo ARP tabel si tako mrežni odjemalci zgradijo dinamične ARP tabele s pari: IP naslov - fizični naslov.

Ranljivost protokola se navezuje na dejstvo, da ta ne preverja pristnosti pošiljatelja oz. zaupa pristnosti povratnega odgovora. ARP ne zagotavlja nobenega preverjanja ali je naprava, ki se je identificirala za sogovornika res tista, s katero želimo komunicirati.

2.2.2. Pasivno vohunjenje

Za izvedbo pasivnega vohunjenja potrebujemo samo primerno programsko orodje (Packet sniffer). Napad je omejen na omrežja brez omrežnih stikal in mostov. Možnost prestrezanja paketov je vezana na način komunikacije med gostitelji (IPv4 omrežje):

- Neko vozlišče pošlje podatke vsem ostalim, v omrežje priključenim gostiteljem. Pri sprejemu podatkov vozlišče preveri ponorni naslov. V primeru, da je ena izmed naslovljenih naprav, paket sprejme, v nasprotnem primeru pa ga zavrže. To funkcijo opravlja filter v kartici omrežnega vmesnika (angl. Network Interface Card). Vozlišče, ki se infiltrira v omrežje postavi svoj omrežni vmesnik v promiskuitetni način (angl. promiscuous mode) delovanja. To lahko storimo npr. z uporabo odprokodne knjižnice Libpcap, ki predstavlja vmesnik za programsko opremo s katero prestrezamo pakete.
  Tako lahko sistem začne sprejemati podatke čeprav nanj morda niso naslovljeni. Podatki so mimo filtra posredovani neposredno v jedro (angl. kernel) sistema.

Obstaja tudi nekaj načinov za prepoznavanje vohljačev v IPv4 omrežju:

- V omrežje pošiljamo pakete, ki vsebujejo neveljavne naslove. Če kateri izmed odjemalcev pakete sprejema, lahko predpostavimo, da igra vlogo vohuna
- Uporabimo upravitelja omrežnih protokolov (angl. Network Management Protocol)
- Uporaba komercialnih programov, ki na podlagi testov ocenijo, ali član omrežja prisluškuje omrežnim komunikacijam.

Poleg tega se lahko vohunjenje uporablja tudi kot dobronamerno administrativno orodje za naslednje primere:

- analiza težav v omrežju (primer: nezmožnost komuniciranja točke A s točko B),
- zaznavanje poskusov vdorov v omrežje,
- razhroščevanje implementacij raznih protokolov,
- nadzor in spremljanje delovanje omrežja,
- zbiranje podatkov za namene statistike.

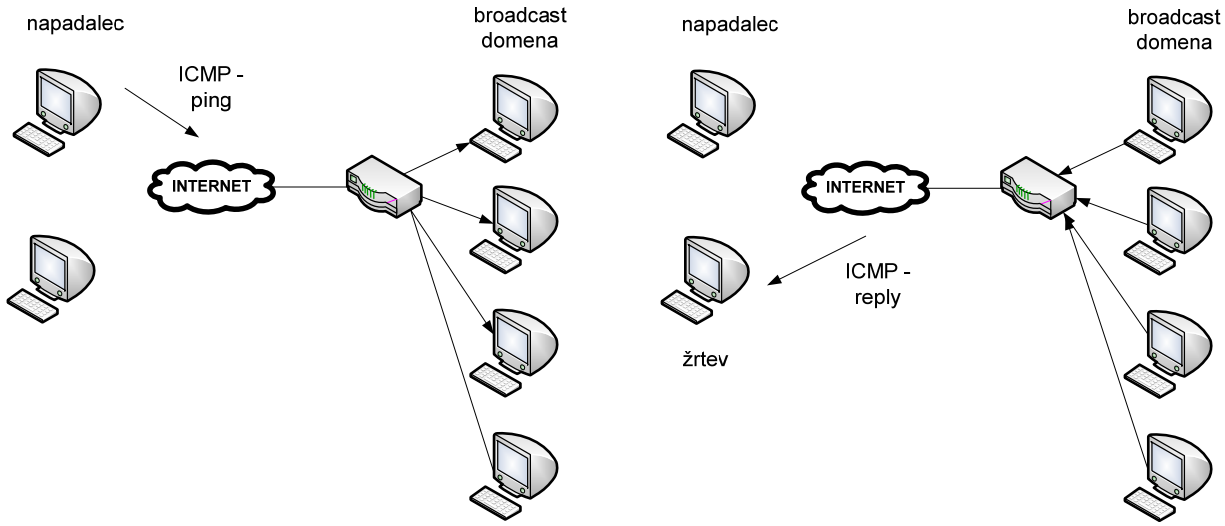
Vohuni dandanes niso več tako nevarni, ker se večina zaupnih podatkov šifrira in je njihov pomen težko razbrati.
Principi vohunjenja v IPv6 se bistveno niso spremenili. Poleg šifriranja podatkov na transportni plasti je za zagotavljanje zaupnosti informacij pomembno tudi to, da je implementacija IPsec za IP protokol verzije 6 obvezna. V kolikor se uporabnik posluži uporabe ESP mehanizma, se nevarnosti povezane z vohunjenjem minimizirajo.

Temeljne koristi, ki jih ima vohun v IPv6 omrežju so vezane na prestrezanje NDP sporočil protokola ICMPv6. Prisluškovanje sporočilom, ki si jih izmenjujejo omrežni gostitelji ima za cilj razkritje vseh gostiteljev in posledično boljše predispozicije za razne napade (npr. črvi).

2.3. Poplavljanje

2.3.1. Smurf napad

Ideja teh napadov je zasičenje in poplavljanje (angl. flooding) žrtev s povratnimi sporočili vozlišč. Napadalec v omrežju IPv4 v tem primeru pošlje ICMP Echo paket z veliko vsebine na broadcast naslov. V paketu je lahko zahteva ping, ki meri čas potovanja paketa do ciljnega sistema. Naslov pošiljatelja v paketu, ki ga razpošlje, ponaredi, tako da ta ustreza žrtvi. Vsi gostitelji v omrežju se na paket odzovejo, kar pomeni, da se v smeri žrtve steče veliko prometa. Zaradi preobremenitve pride do onemogočanja izvajanja storitve (DoS).



Slika 22: Prikaz SMURF napada

Specifikacije protokola ICMPv6 navajajo, da se tvorjenja ICMPv6 paketa, kot odziva na ICMPv6 sporočilo z multicast naslovov ne dopušča. Izjema sta naslednja primera.

- Sporočilo »**prevelik paket**« (angl. The Packet Too Big Message)
  Z njim usmerjevalnik pošlje sporočilo za IP paket, ki je večji, kot pa znaša MTU izhodne povezave.

- Sporočilo »**težava s parametrom**« (angl. The Parameter Problem Message)
  Z njim poročamo o neprepoznavni možnosti IPv6 protokola.

Možnost tega napada v IPv6 omrežjih je torej pogojena z upoštevanjem skladnosti IPv6 gostiteljev Z RFC specifikacijami (RFC2463).

2.3.2. SYN poplavljanje

Ta vrsta poplavljanja je povezana z uporabo trosmernega rokovanja (angl. 3-way handshake), ki ga uporabljamo za vzpostavljanje ter rušenje transportnih povezav (TCP) in lahko povzroči onemogočanje izvajanja storitve (DoS). Z njim se skušamo v izvedbi transportne plasti izogniti globalni časovni sinhronizaciji vozlišč.

Ker je TCP povezavni protokol, poskrbi, da so pred začetkom komunikacije vsi segmenti ustrezno poravnani ter potrjeni in sta oba gostitelja, ki si izmenjujeta podatke, ustrezno sinhronizirana. Trosmerno rokovanje poteka po naslednjem postopku:

1.) Odjemalec pošlje sinhronizacijski paket za začetek vzpostavljanja povezave. Ta paket vsebuje 32-bitno številko sekvence X. S pomočjo njene vrednosti prejemnik pakete ustrezno uredi, jih identificira in ugotovi manjkajoče ali podvojene pakete.

```
SYN = true; SEQ id = x;
```

2.) Prejemnik prejme številko sekvence in odgovori s potrditvijo in sinhronizacijsko vrednostjo Y (SYN vrednost), ki ima isti namen kot pri 1.). Potrditvena informacija (ACK) vsebuje vrednost, ki jo prejemnik pričakuje kot naslednjo (X+1).

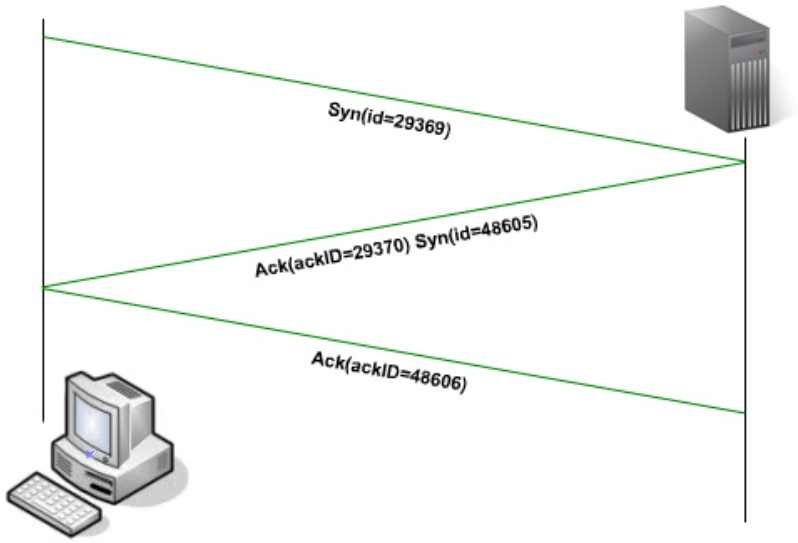
```
ACK = true; ACK id = x+1;
SYN = true; SEQ id = y;
```

3.) Odjemalec se odzove z vrednostjo za potrditev Y+1.

```
ACK = true; ACK id = y+1;
```

4.) Pričetek izmenjave podatkov

Številke sekvenc so zahtevane za zanesljivo povezavo. Obe strani si z njihovo pomočjo urejata tako pravi vrstni red paketov kot identifikacijo pogrešanih in podvojenih paketov.

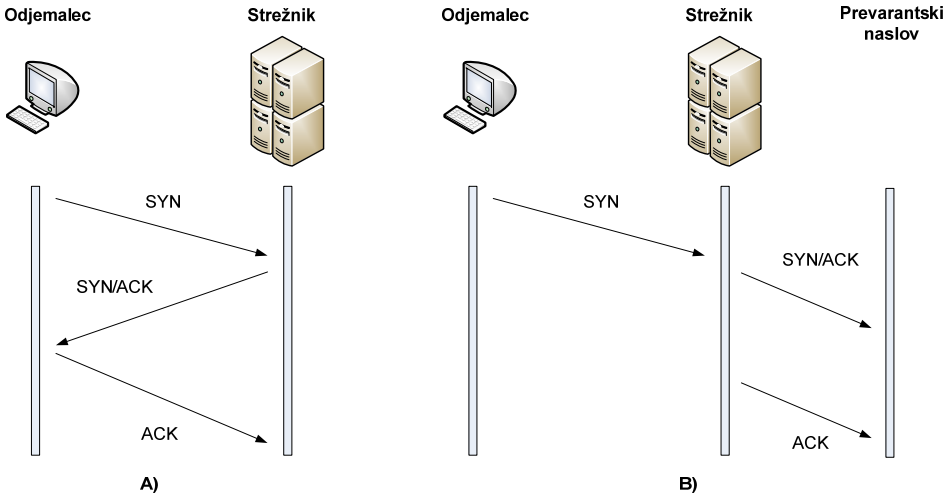


Slika 23: Prikaz izvajanja trosmernega rokovanja

Tekom napada (slika 24, primer b) napadalec pošlje več SYN zahtev z lažnim naslovom (naslov v omrežju ne obstaja) kamor naj mu odgovori. Strežnik kot žrtev tega napada odgovarja s signaloma SYN in ACK na lažen napadalčev naslov, a povratnega odziva s signalom ACK ni.

Ko se tabele zahtev za vzpostavitev povezave zapolnijo, se prične postopno zavračanje zahtev za nove povezave. Tako lahko napad povzroči onemogočanje izvajanja storitve.

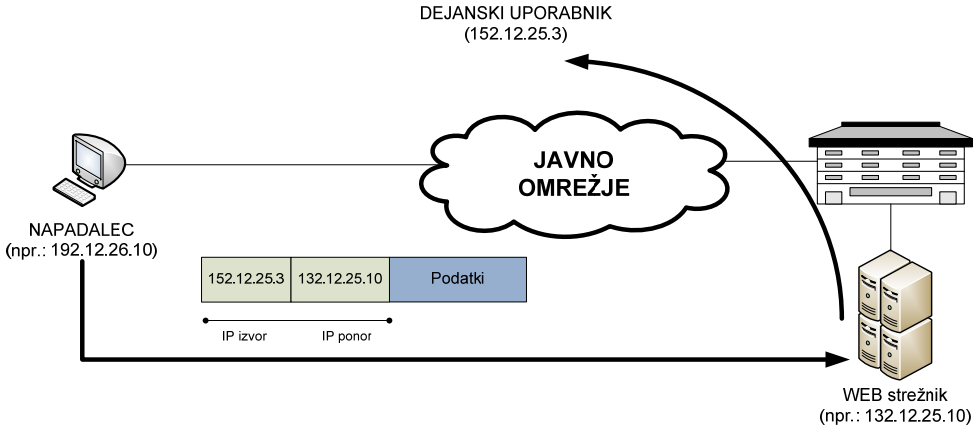
Napad ostaja aktualen v isti obliki tudi pri verziji IPv6.



Slika 24: Princip SYN poplavljanja

2.4. Sleparjenje plast 3 – plast 4

Ti napadi so danes v omrežjih IPv4 pogosti. Bistvo pri sleparjenju je spreminjanje izvornega IP naslova ter številke vrat, kar pripomore k anonimnosti napadalca. Ta želi promet prikazati, kot da prihaja z drugega naslova oz. druge aplikacije.



Slika 25: Primer IPv4 DoS napada s ponarejanjem izvornega naslova

V verziji IPv4 preko napadov dosežemo težjo izsledljivost za napade z onemogočanjem izvajanja storitve (DoS), razne viruse in črve. Plasti (omrežna in transportna plast) sodelujeta pri napadih na naslednji način:

- **Omrežna plast** je deležna manipulacije na način, da si napadalec pridobi zaupanja vreden lažni naslov. Pošiljanje paketa gostitelju temelji na tehnikah pridobivanja kredibilnega naslova in prirejanja glave IP paketa.
- **Transportna plast** se izkorišča tako, da skušamo kot napadalec prikazati, da promet prihaja iz ponarejenega vira. Uporablja se nepovezavni protokol UDP, ki za prenos podatkov ne potrebuje nobene vzpostavitvene procedure. Primer je infiltriranje lažnih SNMP sporočil na transportni plasti.

Cilj prirejanja naslova je skrivanje identitete napadalca, ki bi sicer lahko bila zabeležena v datoteki z dnevnikom (angl. Log File). S tem se izognemo tudi sprejemanju povratnega prometa s strani žrtve.

Primeri uporabe tehnike so del naslednjih napadov:

- napad tipa »mož v sredini« (angl. Man-in-the-middle-attack – MITM),
- poplavljanje (angl. flooding),
- sleparjenje (angl. blind spoofing),
- izvorno usmerjanje (angl. source routing)…

V IP, verzija 6, so naslovni bloki organizacijam dodeljeni s strani ponudnikov internetnih storitev. Zaradi evidentne hierarhije na IPv6 naslovnem področju lahko dosežemo dvoje:

1.) Če je paket poslan iz območja neke organizacije, njegov izvorni naslov pa s tem ni skladen, se naj takšen paket zavrže.

2.) Če ima paket, ki je sprejet v območju organizacije, drugačen naslov, kot pa je njegov naslovni blok, tak paket ni veljaven in se zavrže.

Eden izmed ukrepov preprečevanja je izvajanje varnostne politike s strani ponudnikov dostopa do interneta (ISP). Slednji bi morali poskrbeti, da njihovi uporabniki izven svojega področja ne morejo širiti paketov z lažnim izvornim naslovom.

Naslednji ukrep je vezan na uporabo IPsec. Kriptiranje in uporaba avtentikacijskega mehanizma pripomoreta k eliminaciji tovrstnih napadov.

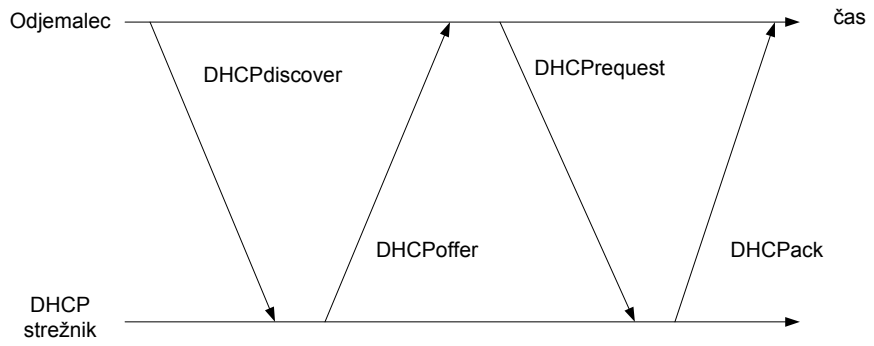
Lahko pa se poslužimo tehnike UNICAST RPF [8]. Na usmerjevalnikih Cisco RPF preverimo Cisco Express Forwarding tabelo na temelju preverjanja prometa oz. smeri, od koder naj bi paketi prihajali. Te informacije so shranjene v FIB (angl. forwarding Information Base). Tako usmerjevalnik primerja izvorni naslov v paketu s podatki v FIB in presodi, kateri vmesnik se uporabi za prepuščanje prometa na določeno podomrežje. Če rezultat primerjave usmerjevalnikov (določenega glede na usmerjevalno tabelo in tistega, ki je sprejel paket) ni logična 1, se paket razveljavi, ker se sklepa, da je naslov prirejen.

2.5. DHCP napadi

DHCP je omrežni protokol za dinamično nastavitev gostitelja.

Protokol služi kot mehanizem za omrežne administratorje, ki tako ohranjajo nadzor nad dodeljevanjem nastavitvenih parametrov odjemalcem, ki so s tem razbremenjeni postopkov pridobivanja omrežnega naslova.

Dodeljevanje naslova preko DHCP v omrežju IPv4 poteka na način, kot je prikazano na sliki 26:



Slika 26: Časovni potek izmenjave sporočil med odjemalcem in DHCP strežnikom

Odjemalec pošlje broadcast sporočilo DHCPdiscover. Strežnik odgovori z DHCPoffer, ki vsebuje prost naslov in konfiguracijske nastavitve. Odjemalec z DHCP request pošlje zahtevo za naslov in v zadnjem koraku strežnik odgovori (glede na razpoložljivost) z DHCPack, DHCPnoack ali DHCPdecline.

Pri DHCPv6 se sporočila tipa »discover« in »offer« nadomestita z DHCP solicit in DHCP advertise.

Glede na implementacijo strežnik DHCP(v4) uporablja 3 načine dodeljevanja IP naslovov:

- DINAMIČNO
  Omrežni skrbnik določi območje naslovnega prostora, ki je namenjen za odjemalce omrežja. Uporablja se način zakupa določenega naslova za neko časovno obdobje. V kolikor odjemalec DHCP naslova ne rabi več, to sporoči DHCP strežniku, ki ga sprosti.

- AVTOMATIČNO
  Uporablja se v primerih, ko je na voljo dovolj naslovnega prostora za vse naprave, ki se želijo priključiti v omrežje. Slednje tudi niso občutljive na to, kakšen naslov se jim dodeli. Je torej način dinamičnega dodeljevanja, kjer zakup naslova ni omejen.

- STATIČNO
  Je najenostavnejši način, saj administrator napravi naslov dodeli ročno. Primeren je za konfiguracijo strežnikov, usmerjevalnikov in naprav, ki v omrežju zahtevajo stabilen in stalen naslov.

Napadi povezani z DHCP(v4) so:

- **Stradanje DHCP (angl. Starvation attack)**
  Ta napad se doseže z naslavljanjem DHCP zahtev iz naslovov vmesnikov, ki so izmišljeni. To se lahko doseže na primer s programskim orodjem Goobler.

S pošiljanjem velike količine zahtev dosežemo izčrpanje bazena prostih naslovov DHCP(v4) strežnika za določeno časovno obdobje. S tem je praktični uporabnik zaradi zasedenosti naslovov prikrajšan za priključitev v omrežje. To je torej vrsta napada z onemogočanjem izvajanja storitve (DoS).

Za preprečevanje tovrstnih napadov se lahko v omrežjih IPv4 uporabi tehnika, imenovana DHCP vohljanje. Mehanizem je lahko implementiran na LAN stikalih, ki nadzorujejo DHCP transakcije. Z njim filtriramo nezaupljiva DHCP sporočila ter iz njih sestavimo tabele podatkov vmesnikov, ki so sumljivi. Hranijo se fizični naslov vmesnika, IP naslov, ID VLAN-a, trajanje zakupa in vrsta vezi.

Naloge, ki jih opravlja mehanizem, so naslednje:

- dovoljevanje DHCP sporočil iz vrat, ki so vredna zaupanja,
- sledenje fizičnim lokacijam odjemalcev,
- zagotavljanje, da odjemalci uporabljajo samo IP naslove dodeljene njim samim,
- zagotavljanje, da so dosegljivi samo avtorizirani DHCP strežniki.

Stradanje DHCP je tudi v verziji IPv6 ostalo tveganje, četudi je to presenetljivo glede na veliko količino naslovnega prostora. Težava je v tem, da je potrebno za vsak zaseden naslov voditi evidenco. Tako kot vsak strežnik je tudi DHCPv6 omejen s pomnilniškimi kapacitetami, kar lahko ob prekoračitvi privede do neprijetnih posledic.

Ena izmed možnosti preprečevanja DoS na strežnikih DHCPv6 je omejitev števila sporočil z zahtevo po dodelitvi IP naslova, poslanih s strani odjemalca.
Zaenkrat je ena redkih možnosti uvajanje pravil politike kakovosti storitve z omejitvijo pasovne širine za DHCPv6 promet (npr. na 8 kb/s [8]). To mora biti implementirano na vseh točkah, ki so namenjene prenašanju DHCPv6 sporočil (angl. relay agent). Te točke prenašajo DHCPv6 sporočila med odjemalci in strežniki v različnih podomrežjih.

- **Lažni DHCP**

Če dosežemo, da se strežnik zaradi nezmožnosti dodeljevanja novih naslovov sesuje, lahko v omrežje infiltriramo nov DHCP strežnik z nastavitvami, prikrojenimi po napadalčevih željah. To pomeni, da s pomočjo novih podatkov o domenskih strežnikih ali privzetih prehodih dosežemo, da ves promet speljemo na strežnik, ki je pod napadalčevo kontrolo.

Za odkrivanje lažnih DHCP strežnikov lahko uporabimo 2 načina:

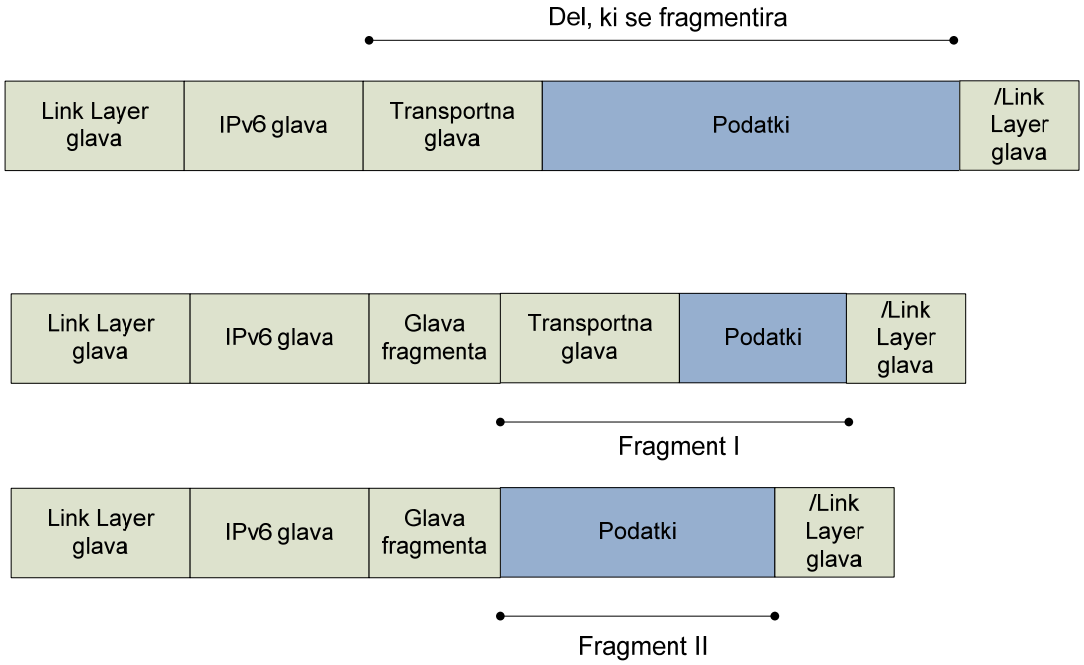
- Ročno odkrivanje
  Je zamudno in najtežje. Nanaša se na preverjanje strežnikov z ukazi – npr. dhcping. Uporabniki sistemov na Unix platformi se lahko poslužijo orodja dhcp_probe. Vse, kar se prikaže v rezultatih preverjanja, ni pa formalno del omrežne infrastrukture, je vzrok za sum.
- Preverjanje s pomočjo avtomatiziranih programskih orodij oz. skriptov.

Tudi nevarnostim z lažnimi DHCP strežniki v IPv6 se ni moč izogniti. Možen je napad moža v sredini (MITM). Poanta tega napada je v preusmerjanju prometa med dvema gostiteljema proti tretjemu (napadalec), ki se predstavlja kot legitimna komunikacijska točka. Ta nevarnost je zelo izrazita. V IPv4 omrežjih se je bilo potrebno najprej vključiti v

LAN omrežje, pri IPv6 pa se lahko napadalec v primeru nezaščitene multicast skupine področja »site-local« priključi tej skupini in prestreza vsa sporočila tipa solicitation. Najboljši način za preprečevanje napada je uporaba možnosti avtentikacije DHCPv6 strežnika.

2.6. Napadi, povezani s fragmentacijo

Fragmentacija je postopek razbijanja IP paketov v pakete manjšega velikostnega ranga. Postopek se izvaja zaradi omejitve MTU, ki določa največjo velikost paketa, ki ga prepuščajo usmerjevalniki na poti do ponora. Tam se fragmenti ponovno združijo.



Slika 27: Fragmentacija IPv6 paketa

S to metodo smo pri verziji IPv4 lahko določali oz. prilagajali velikost paketa MTU vsakega vozlišča.

Višja vrednost MTU po eni strani pomeni višjo efektivnost (vsak paket prenaša več podatkov, glave so fiksne), po drugi strani pa prinaša višje zakasnitve pri prenosu sledečih si podatkov. Maksimalna vrednost MTU je pri IPv4 znašala 1500 bajtov.

Potrebe po fragmentiranju paketa na poti po IPv4 omrežjih so prizadele predvsem hrbtenične usmerjevalnike. Od njih se zahteva zagotavljanje čim višje propustnosti, ki pa jo delno omejuje tudi proces fragmentiranja s porabo sistemskih sredstev.
Pri IPv6 so z eliminacijo postopka fragmentacije in ponovnega sestavljanja (razen pri izvornem gostitelju) povečane zmogljivostim omrežnih usmerjevalnikov.

V okolju IPv6 je fragmentacija na izvoru prilagojena zmogljivosti prenosne poti, po kateri se prenašajo paketi.

2.6.1. Tipičen napad pri fragmentiranju IPv4 paketa

Napad se izvaja z namenom, da se zaobide varnostno politiko požarnih zidov. Podatke se dostavi na vrata (angl. port), ki jih sicer požarni zid blokira.

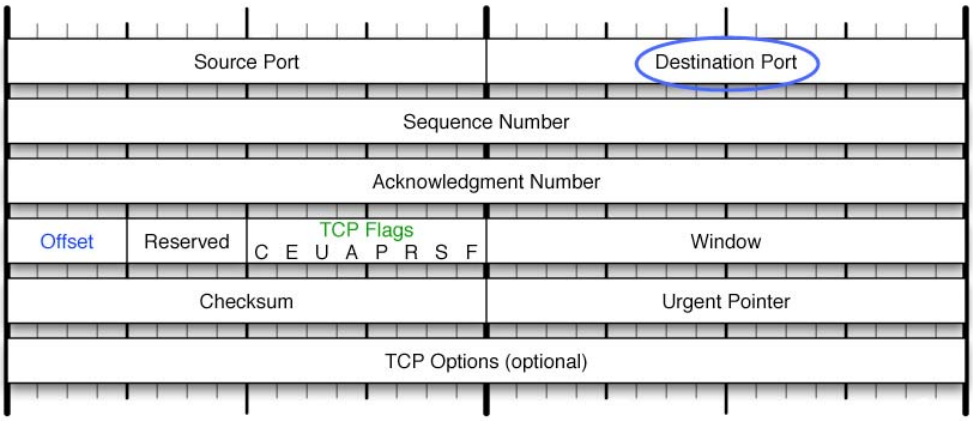
Bistvo je v manipulaciji vrednosti polja »fragment offset« (odmik), ki je del glave fragmenta in določa položaj fragmenta glede na originalni IP paket. V primeru razbitja paketa na dva dela lahko drugemu vrednost dodelimo tako nizko, da namesto združevanja na ciljni strani povozi podatke in del TCP glave predhodnega fragmenta.

V našem primeru bomo IPv4 paket razstavili na dva dela:

1.) »offset« nastavimo na **0** | DF = 0 | MF = 1 | DESTINATION PORT = 25 (požarni zid ga prepušča).

2.) »offset« nastavimo na **25** | DF = 0 | MF = 0 | DESTINATION PORT = 118 (požarni zid takšne pakete v našem primeru zavrača).

   Za primer napada bi lahko vrednost »offset« polja nastavili na 1, s čimer bi prepisali tudi nekaj podatkov glave TCP (od 8 bajta dalje).



Slika 28: Glava TCP paketa

Ko požarni zid filtrira sekvenco zgornjih paketov pri drugem fragmentu, opazi, da je nastavitev odmika enaka 1, iz česar sklepa, da gre za del neke celote in ga spusti skozi svoje varnostno sito. Ko se na ciljni strani paketa združujeta, prirejeni podatki drugega fragmenta prepišejo del vsebine prvega. Posledica tega je možnost, da se paket preusmeri na sicer zastražena vrata 118.

IPv6 fragmentacije na poti ne dovoljuje – ta je možna samo pri izvoru podatkov. MTU možnost v ICMPv6 omogoča določanje priporočljive velikosti MTU preko sporočil Router Advertisement. Minimalna priporočena velikost znaša 1280 oktetov. Vse, kar je manj, se zavrže razen v primeru, da je paket zadnji v toku podatkov.

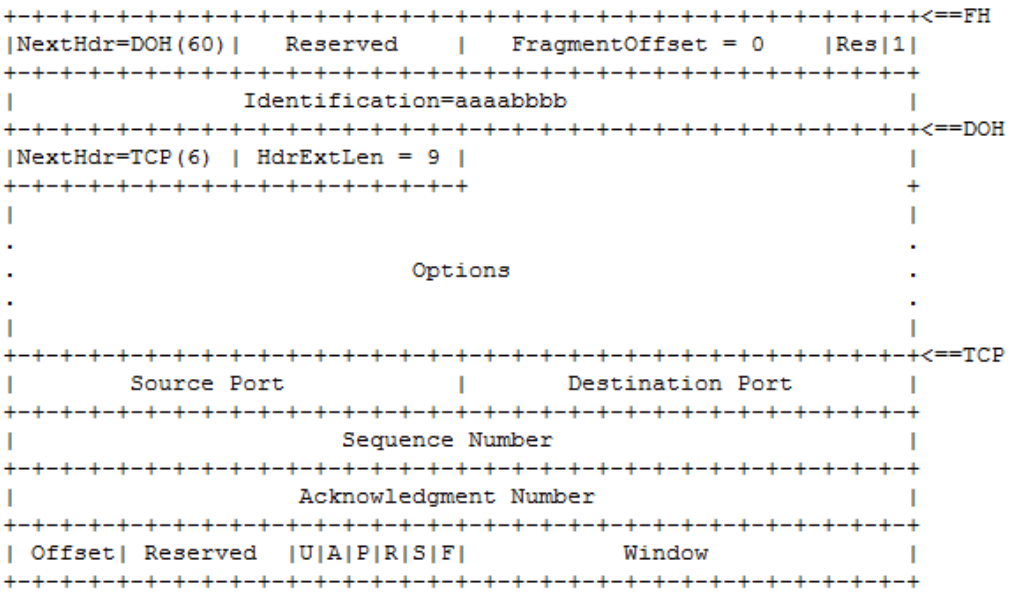
2.6.2. Nevarnost prekrivajočih fragmentov pri IPv6

Do prekrivanja fragmentov pride, če imata dva fragmenta v istem IP paketu masko nastavljeno tako, da se prekrivata. To lahko bodisi pomeni, da je fragment A popolnoma prekrit (prepisan) s fragmentom B bodisi, da je fragment A delno prepisan s strani fragmenta B. Poleg vseh ostalih

žrtev so ogroženi tudi operacijski sistemi, ki so lahko po prejemu takšnih paketov obsojeni na napake v delovanju.

Zgoraj opisani napad s prekrivanjem fragmentov v IPv6 ni možen, saj direktiva določa, da se paketi, katerih vrednost »offset« fragmenta je 1, zavržejo. Pač pa je bolj kritičen naslednji scenarij:

- Recimo, da je v prvem fragmentu nekega paketa glava »možnosti ponora« dolga 80 bajtov in ji sledi TCP glava:



Slika 29: I. fragment paketa

Predpostavimo, da imamo primer vzpostavljanja povezave preko trosmernega rokovanja. Predpostavimo še, da imamo v našem primeru v glavi TCP prvega fragmenta vrednost SYN = 1 in ACK = 1. Tak paket si požarni zid lahko interpretira kot odziv na paket, ki je prišel iz varovanega dela omrežja (tj. za požarnim zidom) in je imel namen vzpostaviti TCP povezavo. Tako bo fragmentu dovolil prehod. To pa bo dovolil tudi vsem ostalim sledečim fragmentom z enako identifikacijsko oznako v glavi fragmenta.

Priporočila za preprečevanje tovrstnih napadov s prekrivanjem določajo, da naj se v primeru odkritja takšnih fragmentov paketi enostavno zavržejo.

2.7. Lažne naprave (rogue devices)

Gre za naprave, ki so neavtorizirano pripojene v omrežje. Pristopi in posledice so podobni kot pri IP, verzija 4.

Pri obravnavi teh napadov bolj kot o posameznih računalnikih govorimo gostiteljih, kot so domenski strežnik, usmerjevalnik, brezžična dostopna točka, itd. Cilj vključevanja zlonamernega usmerjevalnika v omrežje predstavlja oglaševanje ponarejenih RA sporočil. Če napadalcu uspe preusmeritev prometa na drugi prehod, lahko prestreza in analizira omrežni promet.
Razloge za tovrstne napade gre iskati predvsem v neuporabi IPsec (avtentikacijskega postopka).

2.8. Napadi na aplikacijski plasti

2.8.1. Buffer overflow napad

Tarče tega napada so lahko usmerjevalniki, na katere skuša napadalec vplivati s prekomernim pošiljanjem informacij. S tem lahko potencialno doseže prekoračitev pomnilnika. Odziv usmerjevalnika na napad je sesutje programske opreme, nerazumljivo delovanje ali celo pridobitev oddaljenega dostopa, ki omogoči ponastavljanje parametrov. Tudi pri protokolu IPv6 ostaja ta možnost napada še vedno aktualna.

2.8.2. Napadi na aplikacijski plasti

Ti napadi predstavljajo visok delež zlonamernih poizkusov vsiljivcev. Ker niso povezani z delovanjem nižje ležečih plasti, z uvedbo IPv6 niti ne moremo pričakovati višje zaščite.

V glavnem se napadi zanašajo na prekoračitev medpomnilnika, napade na spletne aplikacije ter črve in viruse.

ČRVI so zlonamerni programi, ki se hitro širijo po omrežju s ciljem, da prizadenejo čim več uporabnikov neke storitve. Za svoje širjenje ne potrebujejo interakcije s človekom.

Njihov princip je odkrivanje ranljivih računalnikov v omrežju, ki jih iščejo preko imenika, imenovanega IP naslovni prostor. Ko najdejo tarčo(e), začnejo z obremenjevanjem gostitelja, prav tako pa tudi omrežja zaradi velikega pretoka podatkov. Cilji napadov so lahko tudi porazdeljeni napadi onemogočanja izvajanja storitve (DDoS), ki povzročijo preplavljanje tarč z enormnim omrežnim prometom.

Najbolj znani črvi, ki so uporabnikom v preteklosti povzročili veliko sivih las, so bili Blaster, Slammer, Code red in Sasser.

Pri verziji IPv4 je najpogosteje uporabljan način iskanja žrtev pregledovanje IPv4 naslovnega prostora. Ker je IPv6 naslov 96 bitov daljši, je verjetnost, da med vsemi naslovi z naključnim izbiranjem najdemo veljavnega, majhna.

V omrežjih IPv4 so naslovi predvsem razreda C (192.0.0.0. – 223.255.255.255), kar pomeni manipulacijo z 8-biti za naslavljanje gostitelja znotraj podomrežja.
Tako lahko za tipično IPv4 omrežje izračunamo čas poizvedovanja pri normi 1 gostitelj na sekundo preko formule:

$$2^8 \times \frac{1 sekunda}{1 gostitelj} \times \frac{1 \min uta}{60 sekund} = 4.2 \min \qquad (1)$$

V omrežju IPv6 za iskanje gostitelja v nekem podomrežju (najmanjše lokalno omrežje ima 2^{64} možnih naslovov (/64)) porabimo:

$$2^{64} \times \frac{1 sekunda}{1 gostitelj} \times \frac{1 leto}{31{,}536{,}000 sekund} = 584{,}942{,}417{,}355 let \qquad (2)$$

Vrednost izračuna po formuli (2) je skorajda nepredstavljiva in predstavlja velik izziv za akterje zlonamernega delovanja v omrežjih.

Zato so se začele pojavljati nove, bolj inteligentne strategije, ki iščejo žrtve na bolj sofisticiran način. Voda na mlin črvom je množična uporaba DNS imen omrežnih gostiteljev. Preko napada na domenski strežnik lahko pridobimo veliko informacij glede zasedenih naslovov.

Internetne črve delimo v naslednje skupine:

E-mail črvi

Propagirajo se skozi priponke, ki jih uporabniki odpirajo tekom pregledovanja spletne pošte. Za širjenje tipično uporabljajo baze, v katerih se nahajajo imeniki (npr. MS Outlook address book).

Črvi, ki temeljijo na spletnih iskalnikih

Ti za svoje delovanje izkoriščajo priljubljene spletne iskalnike (Google, Yahoo). Izrabljajo jih na način, da si širijo bazo podatkov strani, katerih informacije pridobijo preko poizvedb na iskalnih portalih.

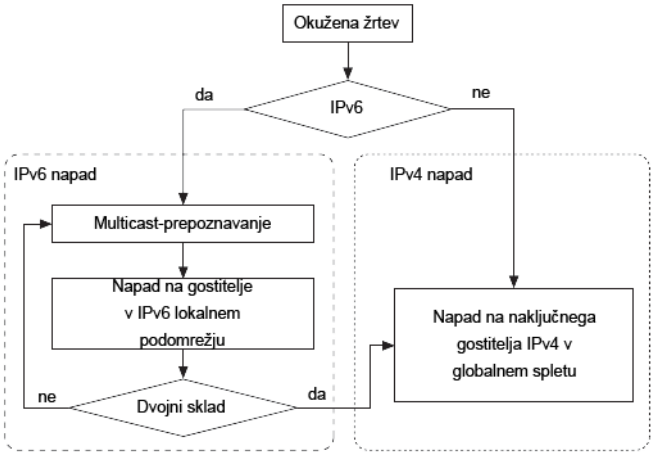
Črvi, ki temeljijo na DNS

Ti črvi namesto iskanja IP naslovov ugibajo preko imen domen, za pretvorbo pa uporabljajo sisteme domenskih strežnikov.

Črvi dvojnega sklada [12]

Za uspešen prehod na IPv6 je v tranzicijskem obdobju zelo pomembna arhitektura dvojnega sklada, ki omogoča kompatibilnost pri komunikaciji gostiteljev obeh protokolov. Tako lahko zaradi dosedanjega polžjega prehajanja na čiste IPv6 implementacije pričakujemo, da bo omenjeni prehodni mehanizem ostal v uporabi še lep čas. Vse to je voda na mlin razvijalcem črvov, ki že skrbijo, da tudi arhitektura dvojnega sklada ne bo imuna na napade.

Črv dvojnega sklada zazna žrtve v skupnem IPv6 podomrežju preko prepoznavanja z multicast načinom ali pa napade odjemalce v IPv4 omrežju s pomočjo naključnega prepoznavanja.



Slika 30: Strategija napada črva dvojnega sklada

Prepoznavanje se vrši preko naslova FF02::1 (FF – oznaka za multicast način, 02 – link-local scope, vsi gostitelji). V primeru, da usmerjevalnik pošlje na ta naslov RA (angl. router advertisement) sporočilo, ki vsebuje informacije za nastavitev gostitelja, se bodo slednji odzvali s povratnim NS sporočilom. To bo v polju »target« vsebovalo tudi veljavni IPv6 naslov – bistveno informacijo, ki jo črv potrebuje pri opravljanju svojega poslanstva.

Rešitev predvideva blokiranje vseh multicast paketov globalnih in site-local področij v omrežnem dosegu. Link-local multicast komunikacije, ki so zahtevane za raziskovanje omrežja in usmerjevalne protokole, dovolimo. To dosežemo z uvedbo IPv6 dostopne liste (ACL). Ta mehanizem se nastavi na meji nekega omrežja in klasificira promet v 2 skupini: tak, ki se prepušča in tak, ki se zavrača.

Primer konfiguracije usmerjevalnika Cisco:

```
Ipv6 access-list BLOCKMCAST
remark Allow Link-Local Scope
permit any ff02::/16
permit ff02::/16 any
remark Block other multicasts
deny ipv6 any ff00::/16
deny ipv6 ff00::/16 any
remark Allow all other ipv6 packets
permit ipv6 any any
interface FastEthernet 0/0
ipv6 traffic-filter BLOCKMCAST in
```

Ko/če se v podomrežju črv učinkovito naseli h gostiteljem, lahko učinkovito migrira v druga IPv6 ali IPv4 omrežja preko domenskega strežnika, IPv6/IPv4 naslovov, e-mail storitev, ipd.

S prehodom na IPv6 še ne bomo dobili nobenega zagotovila, da se bo uporaba črvov v zle namene zmanjšala. Najboljšo obrambo pred njimi še vedno predstavljajo sprotno nameščanje posodobitev operacijskih sistemov, ažurni protivirusni programi in požarni zidovi.

VIRUSI za svojo replikacijo potrebujejo okuženo gostiteljsko datoteko. Najbolj razširjen primer so tovrstni virusi, ki se širijo preko elektronske pošte. Pri tem je za širjenje potreben uporabnik, ki z odpiranjem priponke sproži širjenje zlonamernih aktivnosti tudi k drugim uporabnikom.

Omrežni virusi delujejo v treh fazah: nalaganje, širjenje, okužba sistema.

Delimo jih lahko na viruse visoko in nizko inteligentnega značaja. Značilnost prvih je, da so implementirani na kompleksen način z namenom, da prikrojijo delovanje na transportni, omrežni ali celo povezavni plasti modela OSI. Njihova inteligenca jim torej omogoča izgradnjo poti širjenja na nižje ležečih protokolih (TCP, UDP, IP).

Nizko inteligentni virusi so tisti, ki pri svojem delovanju uporabljajo vgrajene omrežne aplikacije (končnice spletnih strani, že omenjene aplikacije elektronske pošte) ali pa protokole aplikacijske plasti (npr. FTP).

Generični cikel širjenja virusa je naslednji:

- **Lociranje žrtev**

  V lokalnih sistemih iščejo potencialne šibkosti v omrežnih aplikacijah oz. protokolih aplikacijske plasti.

- **Ocenjevanje**

  Odločevanje med ustvarjanjem/iskanjem obstoječih povezav ali iskanjem novih poti/žrtev.

- **Okužba sistema**

  Ob okužbi sistema se prevzame nadzor in naloži modul za širjenje virusa.

- **Odločitev: iskanje novih žrtev (prvi korak) ali zadušitev delovanja (glede na zasnovo virusa)**

Tipični znaki, preko katerih uporabnik lahko zazna, da je njegov računalnik okužen z virusom, so naslednji:

- rušenje programov, ki so sicer delovali brezhibno,
- izginjanje datotek s trdega diska,
- naključni ponovni zagoni računalnika oz. nenadna zaustavitev delovanja sistema,
- Močno upočasnjeno delovanje …

Tekme med uporabniki računalnikov (protivirusnih programov) ter izdajatelji virusov so večne. Največ, kar lahko naredi uporabnik je pazljivost in vestna uporaba protivirusnih programov (z ažurnimi definicijami za zaznavanje) ter uporaba ščitov za sprotno pregledovanje datotek.

S prehodom na IPv6 se tehnike ne bodo veliko spremenile. Oteženo bo le iskanje žrtev v podomrežjih zaradi izredno velikega naslovnega prostora, ki ga nudi ta verzija protokola.

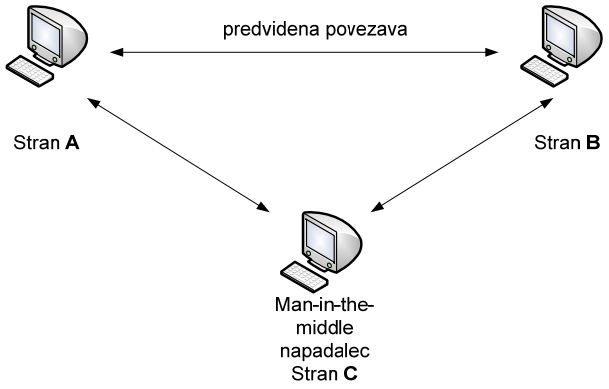
2.9. Napad moža v sredini (MITM)

S tem pojmom označujemo vsiljivca, ki prestreza sporočila, poslana med stranema A in B. Pogoj za uspešno izvedbo napada je zmožnost prestrezanja in infiltriranja lastnih sporočil v vzpostavljeno povezavo med dvema vozliščema.

MITM napad je zanimiv predvsem iz naslednjih razlogov:

- Med napadom žrtvi še vedno normalno komunicirata in se ponavadi sploh ne zavedata, da se v ozadju odvija napad.
- Posledice napada so lahko katastrofalne, saj je moč pakete zajeti, spremeniti in posredovati naprej v obliki, prikrojeni napadalčevim nameram.
- Ta vrsta napadov preži tudi v IPv6.

V primeru MITM si napadalec zavzame mesto med dvema končnima točkama v omrežju, ki medsebojno komunicirata. Sprva komunikacijam prisluškuje, nato pa glede na cilj napada izvaja prestrezanje in zajem paketov, ugrabljanje seje, vbrizgavanje omrežnega prometa ali ukazov v smeri proti žrtvi ali pa pošiljanje zapoznelih odzivov.



Slika 31: Princip MITM napada

Ker glave IPv6 protokola same po sebi ne nudijo nobenih varnostnih mehanizmov, so tudi napadi tega tipa v IPv6 omrežju odvisni predvsem od uporabe IPsec. Nezaščitena IPv6 omrežja so potencialne tarče teh napadov. IPsec z možnostjo kriptiranja in avtenticiranja gostitelja tvori dobro zaščito za preprečevanje spreminjanja vsebine podatkov s strani tretje osebe.

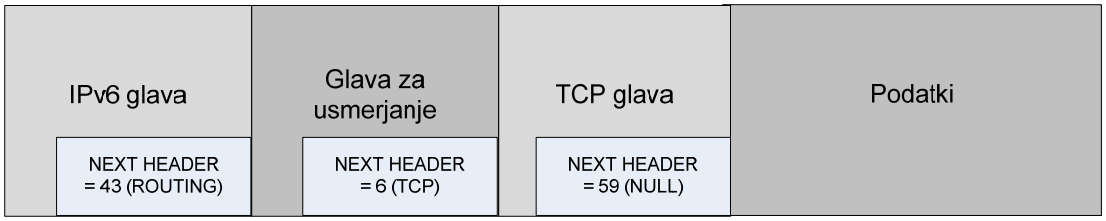
3. Edinstveni napadi v IPv6

Napade, ki so vezani na IPv6, lahko razvrstimo v tiste, ki se nanašajo na sam protokol, takšne, ki so (bodo) značilni za tranzicijsko obdobje do uveljavitve t.i. »native« IPv6, ter napade, ki so povezani z ranljivostmi operacij, ki uporabljajo IPv6 protokol. V nadaljevanju so opisane tiste, ki prežijo na protokol kot tak.

3.1. Ranljivost razširitvenih glav

Protokol IPv6 uporablja dva tipa zaglavij: izvirna IPv6 glava ter različne razširitvene glave. Te uporablja za razširjanje funkcionalnosti protokola ali pa za izkazovanje prisotnosti vsebin transportne plasti.

Dodatne glave so identificirane s poljem Next header v glavi IPv6. Tipični format razširitvene glave je naslednji: 8b za identifikacijsko številko naslednje glave v strukturi, 8b vrednost dolžine glave in spremenljiva velikost polja možnosti parametrov podatkov.



Slika 32 : Primer paketa z razširitvenimi glavami

3.1.1. Napad z dolgo verigo razširitvenih glav

Napad izkorišča možnost dodajanja poljubnega števila razširitvenih glav k izvirni IPv6 glavi. Razlika med specifikacijo protokola ter možnostmi manipuliranja je velika. Prva priporoča, da se lahko vsaka razširitvena glava pojavi enkrat z izjemo glave »možnosti ponora«.
Po drugi strani pa se od usmerjevalnikov zahteva, da procesirajo razširitvene glave v poljubnem vrstnem redu in ne glede na število pojavitev vsake izmed možnosti (razen glave hop-by-hop, ki se lahko pojavi samo neposredno za izvirno IPv6 glavo). Nevarna je tudi možnost IPv6, da lahko ovijemo en paket v drugega, ki lahko ima prav tako dolgo sekvenco razširitvenih glav.

V kolikor napadalec ustvari paket, v katerem se pojavi sosledje večjega števila razširitvenih glav, lahko to privede do napada onemogočanja izvajanja storitve (DoS) na ciljnem računalniku. V takih primerih količina glav potisne podatkovno vsebino v drugi fragment, ki pa se v primeru prečkanja požarnega zidu ne preverja (preveri se samo prvi fragment). To gotovo predstavlja varnostno tveganje.

Vrstni red	Tip glave (angl. izvirno ime)	Koda (next header)
1	**Basic IPv6 header**	-
2	**Hop-by-hop options**	0
3	**Destination options**	60
4	**Routing header**	43

5	**Fragment header**	44
6	**Authentication header**	51
7	**Encapsulation security payload header**	50
8	**Destination options**	60
9	**Mobility header**	135
	No next header	59
višja plast	**TCP**	6
višja plast	**UDP**	17
višja plast	**ICMPv6**	58

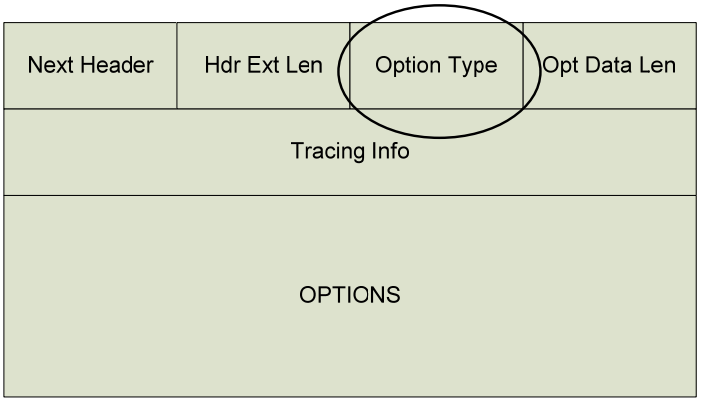
Tabela 2: IPv6 razširitvene glave in njihov vrstni red

Pri tovrstnih napadih mora varnostna politika vključevati filtriranje seznama razširitvenih glav ali pa uvesti mehanizme za posebno obravnavo samo tistih glav, ki jim dovolimo prehod in obravnavo.

3.1.2. DoS napad s pomočjo manipulacije nastavitev hop-by-hop

Polje »hop-by-hop« mora biti prvo razširitveno polje v paketu. Preko polja »option« (možnosti) tvori posebne karakteristike za dostavljanje paketa do ponora. Vsaka možnost je zapisana v formatu TLV (angl. Type Length Values), ki je pogosto uporabljen v zvezi s TCP/IP protokoli.

Na poti paketa po omrežju je polje pregledano s strani vsakega vozlišča. Po tej plati je podobno IPv4 polju možnosti (angl. Options).



Slika 33: Hop-by-Hop glava

Prva dva bita v polju nastavitvenih možnosti (option type) določata način obravnave paketa s strani usmerjevalnika:

Koda	Funkcija
00	Preskoči operacijo
01	Zavrzi paket
10	Zavrzi paket in pošlji ICMPv6 sporočilo izvoru
11	Zavrzi paket in pošlji ICMPv6 sporočilo izvoru (samo, če ponorni naslov ni tipa multicast)

Tabela 3: Možnosti hop-by-hop polja

Bistvena je manipulacija z vrednostmi TLV. Protokolu IPv6 sta k usmerjevalnemu protokolu IS-IS (del protokola IGP) dodani dve možnosti TLV:

- **IPv6 reachability TLV** (koda EC_{hex})
  Opisuje dosegljivost omrežja: IPv6 usmerjevalno predpono, metrične informacije, bite, ki povedo, ali je bila predpona oglaševana s strani višjega nivoja,…

- **IPv6 naslov vmesnika TLV** (koda $E8_{hex}$)
  Vsebuje 128-bitni naslov.

Napad temelji na formiranju paketa z velikim številom TLV možnosti, ki služijo za prenos informacij, zahtevanih za izvedbo IPv6 usmerjanja.
S stališča napadalca je bistvenega pomena zagotoviti, da vplivamo na vse usmerjevalnike na poti – preprečiti želimo, da se paket zavrže in pošlje obvestilo ICMPv6.

Potek napada: [7]

- Kreiramo paket z veliko količino podatkov možnosti TLV.

- Vrednost polja »option type« nastavimo v obsegu 0×02 do 0×63 (s tem preprečimo pošiljanje ICMPv6 sporočil napak).

- Vozlišče paket sprejme in ga procesira (s tem v pravilnem vrstnem redu tudi vse možnosti TLV).

- Zaradi velike količine informacij, ki se procesirajo pride do ohromitve usmerjevalnikov. Najbolj so izpostavljeni tisti, ki imajo elemente nadzora in usmerjanja v skupnem delu. Hitrost procesiranja informacij se lahko zmanjša tudi do 4× [6].

Za preprečevanje težav so razviti 3 načini:

1. **Odvračanje**
   Skušamo odvračati »hop-by-hop« možnosti iz specifikacij IPv6 omrežja.

2. **Preziranje**

Ta možnost omogoča vozliščem preziranje polja možnosti glave »hop-by-hop«. Najvarnejša vozlišča so tista, ki procesiranja teh možnosti sploh ne podpirajo.

3. **Omejevanje**
   Vzpostavimo limitno vrednost paketov z možnostmi »hop-by-hop«. Vse, kar to mejo prekorači, se zavrže. To prepreči, da bi postala CPE prekomerno obremenjena s procesiranjem teh možnosti. Rešitev je enostavna in hkrati neoptimalna, saj ima pristen paket verjetnost, da je zavržen enako kot tisti, ki je napadalno usmerjen.

3.2. NDP napadi

ICMPv6 in napadi s pripadajočimi »solicitation« in »advertisement« sporočili so vezani na določeno LAN področje. To pomeni, da mehanizmi za zaznavanje napadov ne morejo biti centralizirani, ampak so vezani na povezanost v LAN omrežja.

Napadi, vezani na to področje, se nanašajo predvsem na manipulacijo sporočil, s katerimi razpolaga protokol NDP.

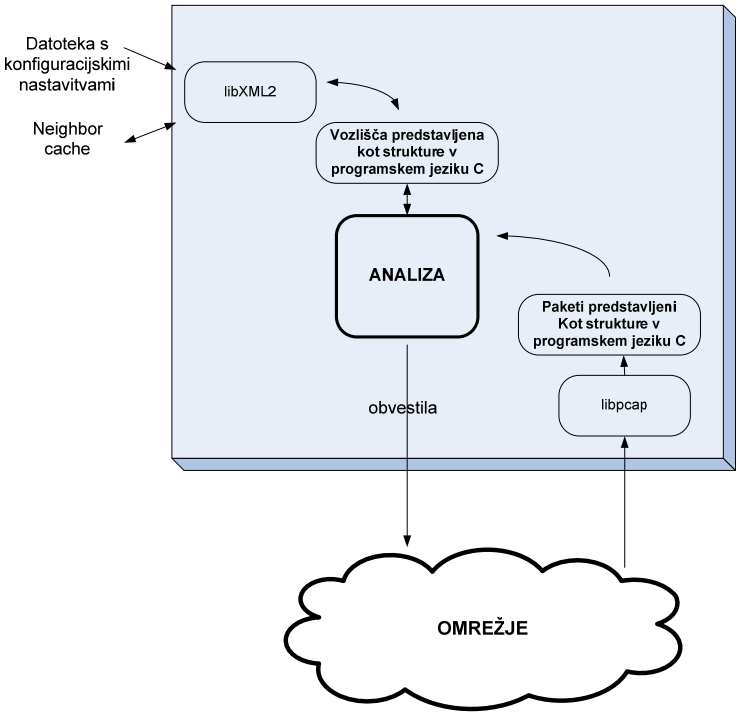
Eden izmed načinov omilitve števila tovrstnih napadov je mikrosegmentacija. Bistvo ideje je v tem, da se veliko omrežje razdeli na več manjših (VLANi), pri čemer se vsakemu dodeli ustrezna IPv6 predpona. S tem zmanjšamo število gostiteljev, vezanih na določen usmerjevalnik v primeru izvedbe napada.

3.2.1. Neighbor solicitation / advertisement prevare

Težava se lahko pojavi, v kolikor se v omrežje infiltrira neavtoriziran gostitelj, ki pošilja zlonamerna in odvečna sporočila. Nekateri od možnih scenarijev:

- Vozlišča ga privzamejo kot privzeti usmerjevalnik.
- Z oglaševanjem namišljene predpone omrežja lahko pride to tega, da paketi nikoli ne dosežejo ponora.
- Zlonamerni vsiljivec onemogoči možnost avtomatskega pridobivanja parametrov omrežja.
- Z dovolj nizko vrednostjo parametra HOP povzročijo, da se usmerjanje paketa predčasno konča.

Najenostavnejša rešitev je uporaba orodja NDPMon, ki je nastal kot odziv na široko uporabno orodje ArpWatch iz verzije IPv4. NDPMon analizira vsa RA sporočila in njihovo avtentičnost preverja v skladu s predhodno pripravljeno konfiguracijsko datoteko v XML formatu. V kolikor zazna sumljiva sporočila, o tem obvesti administratorja preko obveščanja po elektronski pošti ali zapisa v dnevnik dogodkov (angl. log file).



Slika 34: Delovanje NDPmon

3.2.2. Izdajanje lažnih parametrov

Sporočila tipa RA vsebujejo nekatere parametre, ki jih gostitelji uporabijo pri vključevanju v omrežje.
Napadalec lahko v omrežje pošlje RA paket s pristnim izgledom ki gostiteljem narekuje, da morajo za pridobitev omrežnega naslova kontaktirati DHCPv6 strežnik. Ker ta ni del omrežja, gostitelji pa vseeno skušajo z njim vzpostaviti povezavo, je rezultat napada neuspešen poskus pridobitve javnega IPv6 naslova.

Ena izmed možnosti ponarejanja informacij, je tudi posredovanje napačnih predpon podomrežja – na primer takšnih, ki niso v skladu s pravili o dodeljevanju predpon. Žrtev tako ne dobi veljavnega naslova in s strani drugih ni naslovljiva.

3.2.3. Napad pri ugotavljanju nedosegljivosti vozlišča

Sosed v omrežju je zaznamovan kot dosegljiv, če prejmemo potrditev, da je bil nedavno poslani paket sprejet s strani tega naslovljenega vozlišča.
Omrežno vozlišče pa lahko zaradi razlogov, kot so težave v omrežju, strojna napaka, tudi izpade. V tem primeru se informacija pridobi iz višje ležečega sloja.

Pri povezavno orientiranem TCP protokolu je stvar zaradi postopka trosmernega rokovanja trivialna. Pri protokolu UDP, ki je nepovezavni (princip »pošlji in upaj na najboljše«), pa vozlišče pošlje v unicast načinu sporočilo (angl. neighbor solicitation) in čaka na odziv. S tem dejanjem od gostitelja zahteva, da izvede povratni odziv in posreduje informacijo o svoji dosegljivosti. Če tega ni, se vozlišče obravnava kot nedosegljivo.

Efektiven napad temelji na gostitelju, ki si v omrežju priredi veljaven naslov, nato pa s ponarejenimi NA sporočili, ki so odziv na sporočila NS povzroči, da je gostitelj zaznamovan kot nedosegljiv.

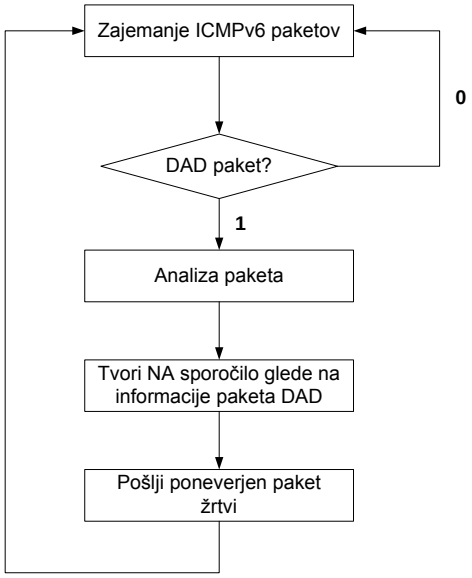
3.2.4. Ugotavljanje podvojenih naslovov

Ugotavljanje podvojenih naslovov (angl. duplicate address detection) je preko NS sporočil izveden proces preverjanja podvojenosti IPv6 naslova v omrežju.

Pri načinu pridobivanja naslova preko »stateless« mehanizma (SLAAC) je postopek naslednji:

- Pošiljatelj paketa (ki želi pridobiti določen omrežni naslov) sprva preveri, ali je v omrežju naslov še razpoložljiv. Če je naslov že zaseden dobi od vozlišča, ki uporablja ta naslov, NA sporočilo.

Tekom preverjanja se lahko odvija napad, ki povzroči onemogočanje izvajanja storitve - DoS. To se zgodi, kadar se napadalec odzove na vsako preverjanje zasedenosti naslova. Če ta v vseh primerih trdi, da je IP naslov že zaseden si ga gostitelj nikoli ne bo uspel pridobiti in bo tako ostal zunaj želenega podomrežja.



Slika 35: Napad v sklopu postopka preverjanja podvojenih naslovov

3.2.5. Zlonamerni »last hop« usmerjevalnik

Polje »HOP limit« glave IPv6 je nadomestilo TTL polju verzije IPv4, ki je določalo, kako dolgo lahko paket ostane v omrežju preden se uniči. Pri IPv6 pa imamo namesto časovne, vrednostno komponento. Vrednost HOP zmanjša vsak usmerjevalnik, ki ga paket prečka.

V primeru, da se usmerjevalnik v omrežju (s pomočjo periodičnih RA sporočil) oglašuje kot zadnji usmerjevalnik pred ponorom, kamor je namenjen paket ga lahko žrtev izbere za privzet usmerjevalnik. Ta lahko ponujeno priložnost izkoristi za črpanje gostiteljevega prometa. Zatem začne dotični usmerjevalnik napadenemu gostitelju razglašati sporočila o boljšem »first-hop«

naslovu ponora za njegove pakete. S tem zakrije sledi svojega delovanja in se čez čas popolnoma umakne.

4. Napad na protokol IPv6

V tem poglavju bom demonstriral napad na ICMPv6 protokol s ciljem onemogočanja izvajanja storitve (pridobivanja IPv6 naslova) za omrežnega gostitelja, ki želi v podomrežju pridobiti veljaven IPv6 globalni naslov.

4.1. Teoretična podlaga za izvedbo napada

Primer postopka pridobivanja omrežnega naslova preko mehanizma SLAAC za vmesnik, ki že ima IPv6 naslov tipa link-local, se izvaja na naslednji način:

- Usmerjevalnik periodično oglašuje nastavitvene parametre (RA sporočila) vsem gostiteljem preko multicast naslova.
- Za hitro pridobivanje usmerjevalnikovih parametrov gostitelj pošlje sporočilo tipa RS.
- Gostitelj izvede preverjanje podvojenosti naslovov (DAD).
- V primeru, da pri preverjanju ne pride do kolizije (detekcije podvojenega naslova), gostitelj pridobi IPv6 globalni naslov.
- Gostitelj si glede na razpoložljivost in potrebe nastavi še dodatne parametre:
  - MTU,
  - prioriteto usmerjevalnika,
  - dodatne zastavice,
  - naslov usmerjevalnika.

Naslov tipa »link-local« omrežni vmesnik pridobi s pripenjanjem predpone FE80::0 k identifikatorju vmesnika. Pridobivanje tovrstnega naslova se vrši ob naslednjih dogodkih:

- prva priključitev vmesnika na povezavo,
- inicializacija vmesnika ob zagonu sistema,
- omogočanje vmesnika s strani administratorja po tem, ko je bil predhodno onemogočen ali strani sistema, če je medtem prišlo do napake.

Postopek **DAD** (angl. duplicate address detection) je način za zaznavanje podvojenih IP naslovov znotraj omrežja. Preverjanje je potrebno izvesti na vseh IPv6 naslovih tipa »unicast«. Uporabljen mora biti pred kakršnokoli dodelitvijo naslova vmesniku. V nasprotnem primeru bi lahko dotični vmesnik začel sprejemati promet, ki bi bil naslovljen na gostitelja z enakim, predhodno dodeljenim, IPv6 naslovom.

Zagotavljanje edinstvenosti naslovov je tesno povezano z NS in NA ICMPv6 sporočili. Ker je slednji moč poneveriti opisani postopek ni primer zanesljivega mehanizma.

Postopek se odvija na naslednji način:

1.) Gostitelj X z naslovom A želi pridobiti IPv6 naslov na vmesniku I.
2.) X pošlje NS sporočilo (**SRC** = ::, **DST** = ciljni naslov, ki si ga želi vmesnik dodeliti).
3.) Ali obstaja NA sporočilo, poslano na naslov FF02::1 (vsem gostiteljem)?

Preden je torej vmesniku dodeljen naslov, je potrebno preveriti, ali ni v omrežju že kakšen drug gostitelj zasedel enak IPv6 naslov. Zato gostitelj pošlje NS sporočilo in kot ponorni naslov določi tistega, ki ga želi sam zasesti. V primeru, da je naslov zaseden, dotični gostitelj z NA sporočilom pošlje obvestilo, da takšna dodelitev ni mogoča. V primeru, da si edinstvenega naslova ne moremo pridobiti, se postopek nastavljanja parametrov iz avtomatskega preklopi na ročno.

Z vidika varnosti je kritična možnost, da lahko na postopek preverjanja podvojenosti naslovov odgovori vsak gostitelj in tako prepreči, da bi se žrtev preko opisanega postopka legitimno vključila v omrežje.

4.2. Infrastruktura in orodje za napad

4.2.1. Infrastruktura

Infrastruktura je bila vzpostavljena v Laboratoriju za računalniške komunikacije in omrežja (LRK) na Fakulteti za računalništvo in informatiko v Ljubljani. Sam napad je bil izveden v izoliranem ter nadzorovanem okolju.
Simulacija napada je potekala na 4 virtualnih računalnikih. Virtualizacija nam omogoča kreiranje navideznih sistemov, ki tečejo znotraj operacijskega sistema. Strojni ukazi, ki se izvajajo, se prenašajo na strojno opremo fizičnega računalnika.

Operacijski sistem je predstavljala distribucija DEBIAN 5 z Linux jedrom 2.6.26-2-686. Do konzole posameznega sistema sem dostopal preko odjemalca vSphere Client v4.0.0.

Vsak izmed virtualnih gostiteljev je imel po dva omrežna vmesnika: eth1 in eth0. Prvi je bil namenjen za povezavo v javno IPv4 omrežje, eth0 pa je služil za vzpostavljanje internega omrežja definiranih omrežnih gostiteljev:

- **Strežnik IPv6** – *IPv6 »link-local« naslov – fe80 :: 20c : 29ff : fe22 : d658 / 64*
  Nanj je bil nameščen IPv6 RA deamon, ki je zmožen predstavljati IPv6 usmerjevalnik in pošiljati RA sporočila, ki so potrebna za IPv6 StateLess konfiguracijo (SLAAC).

  Konfiguracijska datoteka je vsebovala naslednje nastavitve:

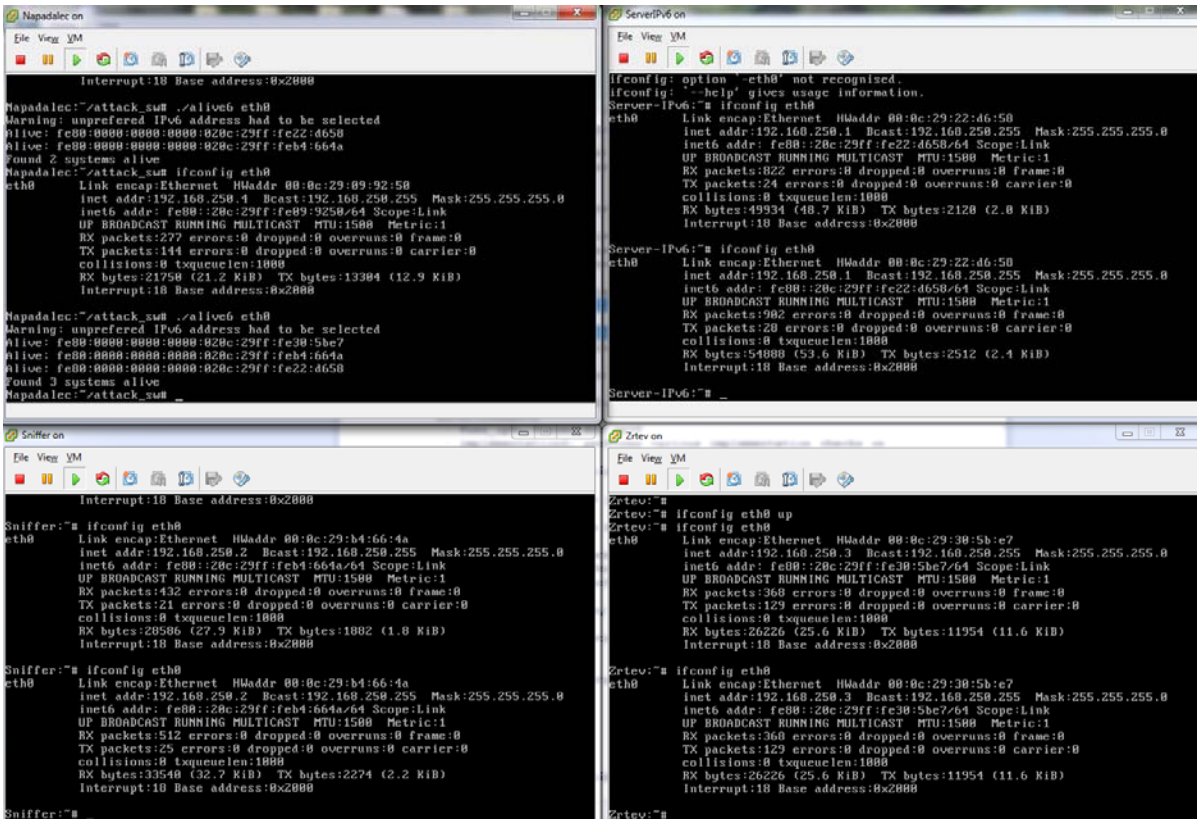
```
interface eth0{

AdvSendAdvert on;
MinRtrAdvInterval 3;
MaxRtrAdvInterval 8;

Prefix 2001:1470:fffd:aaaa::/64{

AdvOnLink on;
AdvRouterAddr on;
AdvAutonomous on;

}

}
```

Bistveni del predstavlja predpona omrežja, ki jo virtualni IPv6 strežnik oglašuje. S parametroma Min(Max)RtrAdvInterval je določen minimalni in maksimalni čas v sekundah, ki lahko preteče med pošiljanjem RA sporočil.

- **Napadalec** – *IPv6 »link-local« naslov: fe80 :: 20c : 29ff : fe09 : 9250 / 64*
  Napadalec je izvajal program iz paketa THC-IPv6 in prisluškoval NS sporočilom na povezavi. Zmožen je izvajanja DoS napada z vrivanjem pri ugotavljanju podvojenih naslovov za vsakega novega gostitelja.

- **Žrtev napada** - *IPv6 »link-local« naslov: fe80 :: 20c : 29ff : fe30 : 5be7 / 64*
  Ta gostitelj je igral vlogo nedolžne žrtve, ki ji zaradi napada ni uspelo pridobiti IPv6 naslova, tipa »global scope«.

- **Prestreznik prometa** (angl. sniffer) - *IPv6 »link local« naslov: fe80 :: 20c : 29ff : feb4 : 664a / 64*
  Vmesnik prestreznika je deloval v promiskulitetnem načinu in je preko vmesnika TCPdump zajemal ICMPv6 promet, ki je služil za končno analizo napada.



Slika 36: Dostop do konzol akterjev pri izvedbi napada

4.2.2. Programski paket THC-IPv6

THC je set orodij za izkoriščanje ranljivosti protokola IPv6.

Orodja, ki so vključena v paket, so naslednja:

- Alive6 – odkrivanje IPv6 lokalnih sistemov,

- Parasite6 – ICMPv6 sleparjenje,
- Redir6 – preusmerjanje omrežnega prometa,
- Fake_Router6 – ustvarjanje lažnega usmerjevalnika v omrežju,
- Detect-New-IPv6 – odkrivanje novih sistemov v LAN omrežjih + samodejno zaganjanje skripta,
- **DOS-New-IPv6 – DoS napad za preprečitev vključevanja v omrežje novim gostiteljem,**
- Smurf6 – orodje za smurf napad,
- RSmurf6 – orodje za oddaljeni smurf napad,
- TooBig6 – Zmanjševanje MTU vrednosti gostitelja,
- Fake_MIPv6 – preumerjanje prometa od mobilne naprave k željenemu gostitelju,
- Sendpees6 – NS sporočila,
- PIT – protocol implementation tester.

4.3. Izvedba napada

Za kasnejšo analizo paketov na strani prestreznika v ukazni vrstici poženemo TCPdump z ukazom:

```
Tcpdump ip6 –i eth0 –w Capture.log
```

V ukazni vrstici napadalca poženemo program DOS-New-IPv6:

```
./dos-new-ip6 eth0
```

Ukaz sprejme v ukazni vrstici samo en argument – vmesnik, na katerem prisluškuje NS sporočilom in kamor potem pošlje NA sporočilo, s katerim trdi, da naslov ni več na razpolago.

Pri žrtvi tega je potrebno predhodno preveriti, ali je možnost preverjanja podvojenih naslovov omogočena.

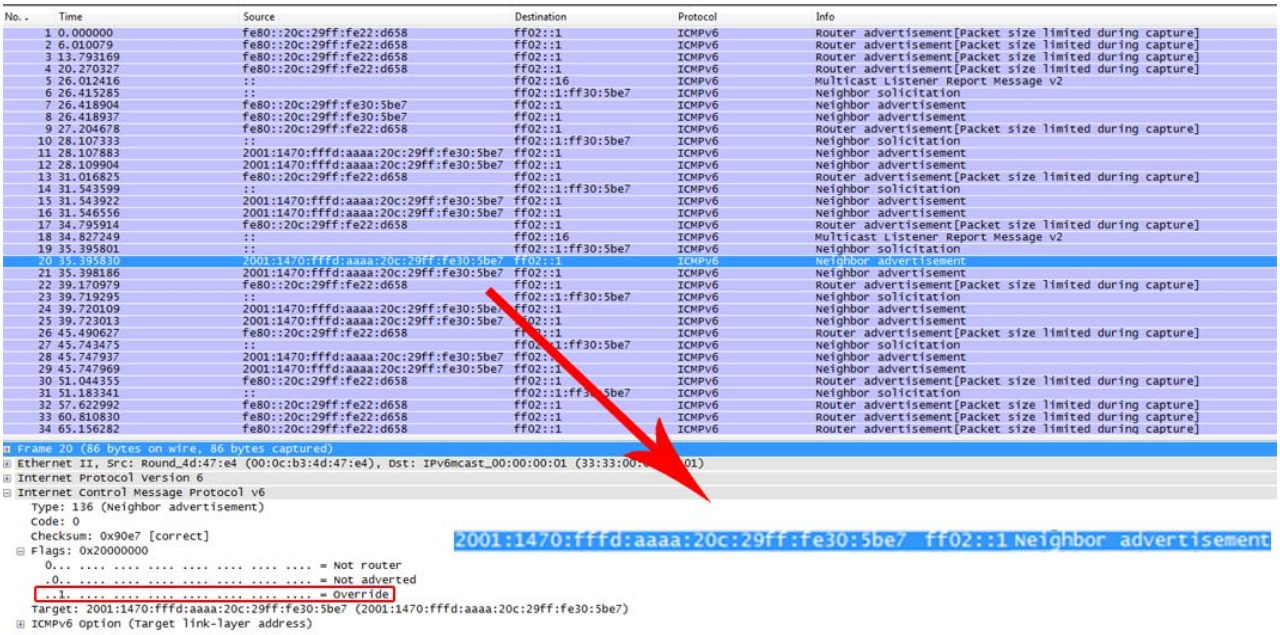
Omrežni vmesnik, ki je tarča napadalca, onemogočimo in ga v naslednjem koraku spet omogočimo:

```
1.)  ifconfig eth0 down
2.)  ifconfig eth0 up
```

Prične se postopek pridobivanja IPv6 naslova preko oglaševane predpone podomrežja. Napadalec ob vsakem poskusu preverjanja podvojenosti naslovov pošlje ponarejeno sporočilo na naslov ff02::1 (vsem gostiteljem na povezavi tipa link-local).

4.4. Ugotovitve

Analiza paketov razkriva dogajanje v omrežju tekom izvedbe napada.



Slika 37: Analiza paketov z orodjem Wireshark

Virtualni IPv6 strežnik periodično pošilja sporočila tipa RA in gostiteljem oglašuje ključne informacije. Žrtev pošlje v omrežje RS sporočilo z nedefiniranim izvornim naslovom.
V tistem trenutku začne napadalec ustvarjati lažna ICMPv6 NA sporočila, katerih izvorni naslov predstavlja IPv6 naslov, ki ga žrtev želi pridobiti.
Kot ponor definira naslov ff02::1. Z njim zagotovimo, da je paket poslan vsem gostiteljem v omrežju, med drugim tudi žrtvi. Z vsebino sporočila ji lažno sporočimo, da je naslov že zaseden.

Vrednost zastavice »override« protokola ICMPv6 je v NA sporočilu nastavljena na 1. To pomeni, da se s tem v predpomnilnikih omrežnih sosedov prepišejo vsi zapisi (sklic drugega fizičnega naslova vmesnika na IP naslov) dotičnega gostitelja z informacijami v NA sporočilu.

Predstavljen napad je realen primer nevarnosti, ki preži na gostitelje, ko je v njihovi okolici nekdo, ki želi ovirati komunikacije v omrežju.

Varnostna ukrepa za preprečevanje tovrstnih scenarijev sta dva:

- Vrednost možnosti »hop limit« glave paketa IPv6 mora biti 255 (najvišja vrednost) – s tem ukrepom preprečimo pošiljanje RA in NS sporočil preko vmesnega usmerjevalnika. To pomeni, da je napad omejen na napadalca v lokalnem omrežju.
- Uporaba protokola SEND

5. Zaključek

V diplomski nalogi sem preučil temeljne nevarnosti, ki ogrožajo varno omrežno komunikacijo preko protokola IPv6. Ker ta predstavlja naslednika IPv4, je bilo smotrno skupne vrste ranljivosti predstaviti na protokolu verzije 4 in pojasniti posledice ter morebitna odstopanja pri napadanju na novodobnem IPv6.

Največje število varnostnih lukenj IPv6 je osredotočenih na protokol za raziskovanje omrežne soseščine (NDP). Ta ureja medsebojna gostiteljska razmerja in nadomešča ARP, ICMP odkrivanje usmerjevalnikov in ICMP preusmeritvena sporočila v IPv4. Glavni vrsti napadov v tem kontekstu sta napad z onemogočanjem izvajanja storitve ter napad moža v sredini.
Rešitev, ki so jo inženirji predstavili s protokolom SEND, se zdi na prvi pogled privlačna. Vse dokler se ne analizira porabe sistemskih sredstev. Obremenitev predstavljajo predvsem izračuni med pari javnega in zasebnega ključa, ki so obvezni za vse gostitelje. Širok nabor orodij za napadanje protokola ICMPv6 v paketu THC-IPv6 nakazuje širok spekter možnosti manipuliranja s sporočili in s tem posredno z gostitelji v omrežju. Verjetno bo intenzivnejše vlaganje v implementacije IPv6 protokola spodbudilo razvojne strokovnjake k pospešenem iskanju novih rešitev.

Neposredna primerjava protokolov IPv4 in IPv6 v smislu varnosti je kočljiva. Sama po sebi ne vsebujeta nobenih varnostnih mehanizmov, ampak se v glavnem zanašata na varnostni protokol IPsec. IPv6 je s specifikacijami po varnostni plati predhodni protokol nadgradil samo z zahtevo po obvezni implementaciji IPsec mehanizma v področje delovanja gostitelja. Kaj naj to pomaga napravi, ki je združljiva z IPv6, nima pa vgrajene možnosti uporabe IPsec-a?

Med pisanjem diplomske naloge sem spoznal tudi nevarnosti, ki pretijo v prehodnem obdobju. Predvsem bo potrebno paziti na vedno aktualne črve, ki bodo zaradi velikega območja naslovnega prostora postali bolj sofisticirani in se njihova strategija ne bo več zanašala na naključno raziskovanje naslovnega prostora. Ko bodo našli prvo žrtev, bo tudi iskanje ostalih na nivoju iste povezave preko multicast odkrivanja lažje. Zraven pa bo v arhitekturi dvojnega sklada odprta še »druga fronta«, ki jo predstavlja manjše in bolj ranljivo IPv4 omrežje.
Pozornost bo potrebno posvetiti tudi gostiteljskim kontrolnim mehanizmom: požarnim zidovom, odjemalcem VPN, sistemom IDS (angl. Intrusion Detection System). Potrebno bo uvesti varnostno politiko, ki bo znala analizirati promet obeh verzij in ga po potrebi tudi omejevati.

Kazalo slik

Kazalo tabel

Seznam virov literature

[1] [2002] Ansari, S.; Rajeev, S.G.; Chandrashekar, H.S.: Packet sniffing: a brief introduction. Dostopno na: http://ieeexplore.ieee.org.nukweb.nuk.uni-lj.si/search/srchabstract.jsp?tp=&arnumber=1166620&queryText%3Dpacket+sniffing%26openedRefinements%3D*%26searchField%3DSearch+All

[2] Paul Asadoorian, Protecting your Network from Internal Attacks. Dostopno na: http://pauldotcom.com/Defense%20in%20Depth%20Protecting%20your%20Netowrk%20for%20Internal%20Attacks.pdf

[3] 2009 IPv4 Address use report. Dostopno na: http://www.bgpexpert.com/addrspace2009.php

[4] IPv6 security – Information assurance for the next-generation internet protocol, CISCO, 2009.

[5] Joseph Davies, Understanding IPv6, second edition, Microsoft 2008, str. 262-270.

[6] Suresh Krishnan Ericsson, Arrangement of IPv6 Hop-by-hop options. Dostopno na: www.ietf.org/proceedings/60/slides/ipv6-8.pdf

[7] Suresh Krishnan Ericsson, The case against Hop-by-Hop options. Dostopno na: http://tools.ietf.org/html/draft-krishnan-ipv6-hopbyhop-04

[8] Scott Hogg, Eric Vyncke, IPv6 security, Cisco press, 2008.

[9] HP IPsec Overview, Dostopno na: http://docs.hp.com/en/J4256-90005/ch01s02.html?btnNext=next%A0%BB

[10] Robert Kolar: Varnost v IP VPN omrežjih z uporabo tehnologije IPsec. Dostopno na: http://www.ltfe.org/wp-content/pdf/Varnost_IPsec.pdf

[11] Urban Kunc (Apek), Prehod na IPv6. Dostopno na: http://www.apek.si/datoteke/File/2010/Prehod%20na%20IPv6_2.pdf

[12] Ting Liu, Xiaohong Guan, Qinghua Zheng, Yu Qu, MOE KLINN Lab., Xi'an Jiaotong Univ., Xi'an: A new worm exploiting IPv6 and IPv4-IPv6 dual-stack networks: experiment, modeling, simulation, and defense, 2009.

[13] 2010, Pet milijard mobilnih telefonov za slabih sedem milijard ljudi. Dostopno na: http://www.racunalniske-novice.com/novice/mobilna-telefonija/dogodki-in-obvestila/pet-milijard-mobilnih-telefonov-za-slabih-sedem-milijard-ljudi.html

[14] Allan Riordan, Rogue DHCP detector in Nagios, 2010. Dostopno na: http://allanrbo.blogspot.com/2010/01/rouge-dhcp-detector-in-nagios.html

[15] 2010, Slovenija vodilna pri uvajanju internetnega protokola IPv6. Dostopno na: http://www.siol.net/tehnologija/racunalnistvo/2010/05/slovenija_vodilna_pri_uvajanju_internetnega_protokola_ipv6.aspx

[16] Samuel Sotillo, Ipv6 security issues, East Caroilna University.

[17] Tone Vidmar, Informacijsko-komunikacijski sistem, Ljubljana 2002, str. 148-149.

[18] Wikipedia: Denial-of-service-attack. Dostopno na: http://en.wikipedia.org/wiki/Denial-of-service_attack

[19] (2010) Wikipedia: IPv6. Dostopno na: http://en.wikipedia.org/wiki/IPv6

[20] Jing Yang, Fast Worm Propagation In IPv6 Networks. Dostopno na: www.cs.virginia.edu/~evans/malware/yang.ppt

[21] Xinyu Yang, Ting Ma, Yi Shi: Typical DoS/DDoS threats under IPv6, 2007.