Internet protokol verzija 6

Ostović, Robert

Sveučilište Jurja Dobrile u Puli
Fakultet informatike Pula

ROBERT OSTOVIĆ

INTERNET PROTOKOL IPv6

Završni rad

Pula, 2020.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike Pula

ROBERT OSTOVIČ

INTERNET PROTOKOL Ipv6

Završni rad

JMBAG: 0303068667, redoviti student

Studijski smjer: Informatika

Predmet: Računalne mreže

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor / Mentorica: prof. dr. sc. Mario Radovan

Pula, rujan 2020.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Robert Ostović, kandidat za prvostupnika ekonomije/poslovne ekonomije, smjera poslovne informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, 2020 godine

Sadržaj

1. UVOD

Internet protokol je protokol koji se nalazi u mrežnom sloju TCP/IP i njegova je uloga adresiranje i usmjeravanje te prijenos datagrama kroz mrežu. Trenutno postoje dvije verzije a to su Internet Protokol verzija 4 i verzija 6. Trenutna verzija Internet Protokola verzije 4 nije izmijenjena od 1981. Razvojem tehnologije i informatike se sve više koriste računala u poslu, svakodnevnome životu i slično. Povećanje korisnika zahtjeva sve više i više broj IP adresa. Trenutna verzija Internet Protokola (IPv4) sadrži više od 4 miljarde adresa, ali zbog brzog trošenja tih adresa dolazi do problema manjka adresa. Međutim, problem nedostatka adresa možemo povezati i sa novim tehnologijama, koje u većini slučaja podatke dobivaju sa interneta. Tom tvrdnjom možemo reći da jedan čovjek treba nekoliko IP adresa jer se spaja na Internet preko više uređaja, npr. računalo, mobilni uređaj i slično. Zbog tog razloga se postepeno uvodi IPv6. Tema ovog završnog rada je Internet Protokol verzija 6 (IPv6). U radu ćemo pojasniti Internet Protokol verziju 4 i verziju 6 te objasniti njihove komponente i značajke te nakraju ih usporediti i donijeti zaključak.

Rad se sastoji od šest međusobno povezanih dijelova a to su:

1. Uvod
2. Internet Protokol
3. Internet Protokol verzija 4
4. Internet Protokol verzija 6
5. Elementi sigurnosti IPv6
6. Zaključak

2. Internet protokol

2.1. Što je internet protokol?

Internet Protokol (IP) je protokol ili skup pravila za usmjeravanje i adresiranje paketa podataka kako bi mogli putovati preko mreža i stići na točno odredište. Podaci koji prolaze Internetom podijeljeni su u manje dijelove, koji se nazivaju paketi. IP podaci su priloženi za svaki paket, a te informacije pomažu usmjerivačima da pošalju pakete na pravo mjesto. Svakom uređaju ili domeni koja se povezuje na Internet dodijeljena je IP adresa, a kako su paketi usmjereni na priložene IP adrese, podaci stižu ondje gdje je potrebno. Jednom kada paketi stignu na svoje odredište, njima se postupa različito, ovisno o tome koji se protokol prijevoza koristi u kombinaciji s IP-om. Najčešći protokoli za transport su TCP i UDP.

2.2. Što je mrežni protokol?

U umrežavanju, protokol je standardiziran način vršenja određenih radnji i oblikovanja podataka tako da dva ili više uređaja mogu međusobno komunicirati i razumjeti se. Da biste razumjeli zašto su protokoli potrebni, potrebno je razmotri postupak slanja pisma. Na kuverti su adrese napisane sljedećim redoslijedom: ime, adresa ulice, grad, država i poštanski broj. Ako se kuverta spusti u poštanski sandučić, prvo će se prikazati napisani poštanski broj, zatim adresa ulice, država, i tako dalje, ako navedeni parametri nisu navedeni na kuverti pošta ga neće dostaviti. Za poštivanje poštanskog sustava postoji dogovoren protokol za pisanje adresa. Na isti način svi IP paketi podataka moraju prezentirati određene podatke određenim redoslijedom, a sve IP adrese slijede standardizirani format.

2.3. Što je IP adresa i kako funkcionira IP adresiranje?

IP adresa je jedinstveni identifikator koji je dodijeljen uređaju ili domeni koja se povezuje na Internet. Svaka IP adresa sadrži niz znakova poput "192.168.1.1". Pomoću Domenskog sustava imena (eng. Domain Name System - DNS) korisnici mogu pristupiti web stranicama bez pamćenja ove složene serije znakova. Svaki IP paket sadrži i IP adresu uređaja ili domene koja šalje paket i IP adresu predviđenog primatelja, slično kao što su odredišna adresa i povratna adresa uključene u komad pošte.

2.4. Što je IP paket?

IP paketi se stvaraju dodavanjem IP zaglavlja svakom paketu podataka prije nego što ga se pošalje na putu. IP zaglavlje je niz bitova (jedinica i nula) i bilježi nekoliko informacija o paketu, uključujući IP adresu za slanje i primanje.

IP zaglavlja također sadrže:

- Duljina zaglavlja,
- Dužina paketa,
- Ograničenje vremena za život (eng. Time to Live – TTL) ili broj mrežnih skokova koje paket može napraviti prije nego što se odbaci,
- Koji se protokol koristi (TCP, UDP itd.).

2.5. Kako radi IP usmjeravanje?

Internet se sastoji od međusobno povezanih velikih mreža koje su odgovorne za određene blokove IP adresa; ove velike mreže poznate su kao autonomni sustavi (AS). Različiti protokoli usmjeravanja, uključujući Protokol graničnog prolaza (eng. Border Gateway Protocol - BGP), pomažu u prijelaznim paketima kroz autonomne sustave na temelju njihove odredišne IP adrese. Usmjerivači imaju tablice usmjeravanja koje upućuju kroz koje bi pakete trebao proći da bi što brže stigli do željenog odredišta. Paketi putuju od AS-a do AS-a dok ne dosegnu onoga koji snosi odgovornost za ciljanu IP adresu. Taj dostignuti AS zatim interno usmjerava pakete do odredišta. Paketi mogu odvesti različite rute do istog mjesta ako je potrebno, baš kao što grupa ljudi koja vozi do dogovorenog odredišta može krenuti različitim cestama da bi tamo stigla.

2.6. TCP/IP i UDP/IP

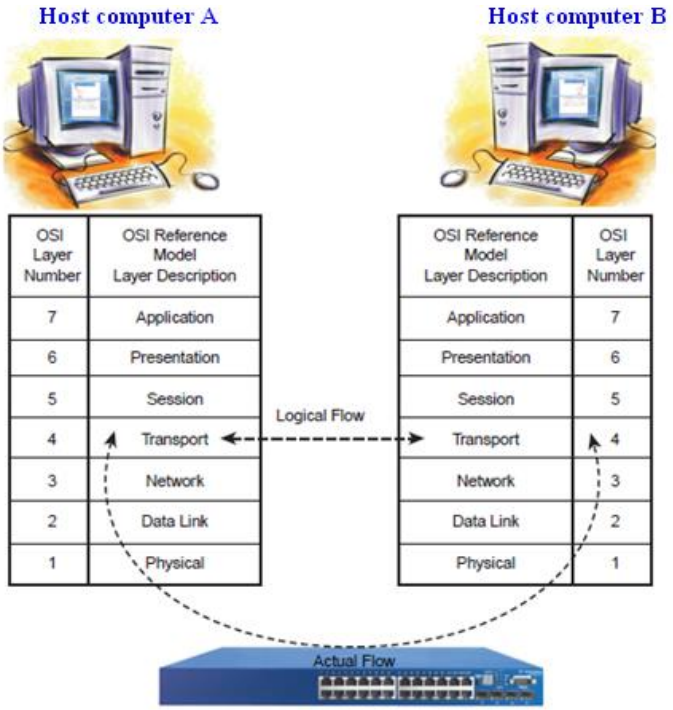
Protokol kontrole prijenosa (eng. Transmission Control Protocol - TCP) protokol je transporta, što znači da diktira način slanja i primanja podataka. TCP zaglavlje je uključeno u podatkovni dio svakog paketa koji koristi TCP / IP. Prije prijenosa podataka, TCP otvara vezu s primateljem. TCP osigurava da svi paketi stignu u red nakon što započne prijenos. Putem TCP-a primatelj će potvrditi primanje svakog paketa koji stigne. Ako nedostaju paketi, ponovno će biti poslani ako potvrda nije potvrđena. TCP dizajniran je za pouzdanost, a ne za brzinu. Budući da TCP mora

osigurati da svi paketi dođu u redu, učitavanje podataka putem TCP / IP može trajati duže ako neki paketi nedostaju.

User Datagram Protocol (UDP) je još jedan od široko korištenih transportnih protokola. Brži je od TCP-a, ali je i manje pouzdan. UDP ne jamči isporuku i narudžbu svih paketa i ne uspostavlja vezu prije pokretanja ili primanja prijenosa. UDP / IP obično se koristi za prijenosa zvuka ili video zapisa u stvarnome vremenu, jer su to slučajevi uporabe u kojima rizik od odbačenih paketa (što znači da nedostaju podaci) nadmašuje potrebu za održavanjem prijenosa u stvarnom vremenu.

2.7. OSI model

Model otvorenog međusobnog povezivanja (OSI) definira mrežni okvir za implementaciju protokola u sedam slojeva. U OSI modelu, kontrola se prenosi s jednog sloja na drugi, počevši od aplikacijskog sloja na jednoj stanici i nastavljajući se do donjeg sloja, preko kanala do sljedeće stanice i sigurnosno kopiranje hijerarhije. OSI model preuzima zadatak međusobnog umrežavanja i dijeli ga na ono što se naziva vertikalnim snopom koji se sastoji od sljedećih 7 slojeva. Slika 1 prikazuje 7 slojeva OSI modela.



Slika 1. Komponente OSI modela.

- *Prvi sloj* olakšava kretanje serijskih binarnih podataka pomoću fizičke veze koja spaja dva ili više mrežnih čvorova. Fizička veza može biti primjer električnih signala na bakrenom kabelu.
- *Drugi sloj* opisuje kako mrežni čvorovi trebaju oblikovati svoje podatke u okvire za prijenos i prijem. Sloj podatkovne veze na čvoru za prijenos podataka gradi okvire i šalje ih u čvor na drugom kraju Ethernet medija preko fizičkog sloja. Sloj veze podataka na čvoru za prijem prima okvire, provjerava jesu li ti okviri bez grešaka, a zatim isporučuje mrežni sloj bez grešaka. Sloj podatkovne veze na prijemniku može poslati čvor okvira bez grešaka u čvor za prijenos. Odašiljač može ponovno poslati okvir ako u određenom vremenu ne primi potvrdu. Ovaj postupak se događa između svakog para čvorova u mreži.
- *Treći sloj* je mrežni sloj te on je odgovoran za formatiranje, adresiranje i fragmentaciju IP paketa. Pri povezivanju na Ethernet prvi put će čvor poslati zahtjev za IPv4 adresu na posebnu IPv4 emitirajuću adresu koja zahtijeva Ethernet adresu ciljnog čvora. To će biti predviđeni čvor koji je jedini odgovorio na zahtjev tražene IPv4 adresa i Ethernet adrese poslane natrag u čvor koji se traži. Ovim načinom se uspostavlja IPv4 povezanost.
- *Četvrti sloj* je transportni sloj koji ugrađuje pouzdanost u OSI sustava pružajući sljedeće usluge gornjim slojevima OSI modela: orijentacija konekcije, komunikacija od točke do točke, potpuna pouzdanost, pokretanje pouzdane veze. Primjer protokola u ovom sloju uključuje protokol za kontrolu prijenosa (TCP).
- *Peti sloj* je sesijski sloj koji služi za omogućavanje komunikacije računalnih aplikacija međusobno preko mreže. Možemo definirati OSI peti sloj kao sloj koji je dizajniran tako da uređajima omogućuju uspostavljanje i upravljanje sesijama. Općenito govoreći, sesija je trajno logično povezivanje dva procesa softverske aplikacije kako bi se omogućila razmjena podataka tijekom dužeg vremenskog razdoblja.
- *Šesti sloj* je prezentacijski sloj OSI modela te je on potreban kako bi softverske aplikacije koje se nalaze na različitim računalima koji su spojeni na mreži mogli komunicirati međusobno i transparentno, čak i ako su njihove informacije u različitim formatima kao što su ASCII ili EBCDIC i slično. Funkcije prezentacijskog sloja se provode na zahtjev aplikacijskog sloja u OSI modelu.

- *Sedmi sloj* je aplikacijski sloj koji pruža korisnicima da koriste softverske programe pomoću grafičkog sučelja (eng. Graphical User Interface - GUI). Kad pregledavamo web stranice potrebno je koristiti web preglednike poput Internet Explorera, Google Chromea i slično, te web preglednik koristi HTTP (*eng. Hyper Text Transfer Protocol*) uslugu koju pruža aplikacijski sloj. Ostali primjeri aplikacijskog sloja su: Domenski sustav imena (DNS), protokol za prijenos podataka (FTP) i slično.

3. Internet protokol verzija 4 (IPv4)

Ubaiti nešto o čemu će se pisati u ovom poglavlju.

3.1. Pojam IPv4

Internetski protokol verzija 4 (IPv4) je četvrta verzija internetskog protokola i protokol se koristi u komunikaciji podataka preko različitih vrsta mreža. IPv4 je protokol koji se koristi u paketno prekrivenim slojevima mreža, kao što je Ethernet. Omogućuje logičnu vezu između mrežnih uređaja pružajući identifikaciju za svaki uređaj. Postoji mnogo načina konfiguriranja IPv4 sa svim vrstama uređaja, uključujući ručnu i automatsku konfiguraciju ovisno o vrsti mreže.

3.2. Adresiranje IPv4

IPv4 adresa označava gdje je određeni mrežni čvor. Svaki IPv4 čvor ima 32 bitnu binarnu adresu, primjer je 01011001.11001100.11110010.11011111. Da bi napravili čitljiviju adresu, binarni brojevi pretvaraju se u bazu deset te se potom odvajaju u oktete točkicama, primjer 89.204.242.223. Sa IPv4 omogućilo se postojanje 4.2×10^8 jedinstvenih IPv4 adresa na Internetu.

3.3. Klasifikacija adresa IPv4

IPv4 adresa spaja adresu mreže i adresu hosta kodirane u jednu adresu. Ovom tehnikom dijelimo 32-bitnu adresu na tri određene granice; te se podjele događaju na 24-bitnom, 16-bitnom i 8-bitnom odjeljku IPv4 adresa. Na slici 2 prikazana je klasifikacija IPv4 adrese.

Class	Leading bits	Network number bit size	Networks produced	Address range
A	0	8	27	1.0.0.1 – 127.255.255.254
B	10	16	214	128.0.0.1 – 191.255.255.254
C	110	24	221	192.0.0.1 – 223.255.255.254
D	1110	-	-	224.0.0.0 – 239.255.255.254
E	1111	-	-	240.0.0.0 – 255.255.255.255

Slika 2. Klasifikacija adresa IPv4.

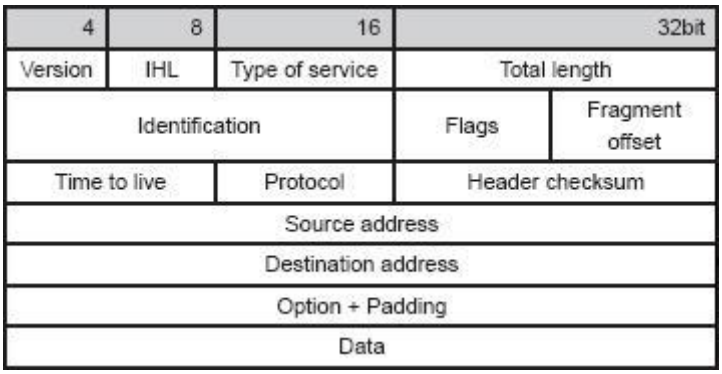
3.4. Enkapsulacija i formatiranje

Drugi sloj OSI modela fokusira se na ethernet sustav, slika 3 prikazuje kako ethernet-okvir obuhvaća cijeli IP paket dok taj paket obuhvaća TCP segment dok TCP segment enkapsulira podatke iz sloja 5,6,7.

Slika 3. Ethernet okvir obuhvaćajući sloj 3 i iznad sloja 3.

Citirajući (Spurgeon, 2000) pojam enkapsulacije: „je mehanizam koji omogućava neovisnim sustavima koji rade zajedno, poput mrežnih protokola i Ethernet LAN-ova, … "(str.36).

Na slici 4 prikazani su svi elementi IP paketa koji su dio ethernet-okvira. Prema izvoru portala *mreze.layer* navedene stavke slike IP paketa obijašnjene su na slijedeći način



Slika 4. Format IP Paketa.

- *Version* - verzija IP protokola,
- *Internet Header Length* (IHL) - duljina IP zaglavlja u 32-bitnim riječima, minimalna duljina ispravnog zaglavlja je 5,
- *Type of Service* - zahtijeva pouzdanost, omogućava usmjernicima različit tretman pojedinih paketa,
- *Total Length* - ukupna duljina IP paketa u oktetima,
- *Identification* - identifikator paketa, važan je pri povezivanju svih fragmenata u paket,

- *Fragment Offset* - definira mjesto fragmenta u originalnom paketu, mjereno u jedinicama od 8 okteta (64 bita); odstupanje prvog fragmenta je nula,
- *Time to Live (TTL)* - Ograničenje vremena za život, nakon čega se neisporučeni paketi odbacuju,
- *Protocol* - označava protokol više razine kojem se podaci prosljeđuju.
- *Header Checksum* - kontrolni zbroj zaglavlja; ponovno se obračunava i provjerava pri svakoj promjeni podataka u zaglavlju.
- *Source Address* - IP adresa predajnika paketa.
- *Destination Address* - IP adresa primatelja paketa.
- *Options* - varijabilne duljine, opcionalno; sadrži kontrolne informacije o usmjeravanju, sigurnosne parametre itd.
- *Padding* - varijabilne duljine, dopuna polja opcija do 32 bita; popunjava se nulama.

3.5. Veličina *datagrama* IPv4 i jedinica za maksimalni prijenos (MTU)

Najmanja veličina *datagrama* je 576 bajta. Broj 576 dopušta prijenos bloka podataka razumne veličine uz tražene podatke zaglavlja. Najveća veličina *datagrama* koja može biti popunjena je 65.535 bajtova. Maksimalna veličina zaglavlja na Internetu je 60 bajtova i prosječno zaglavlje na internetu dugo je 20 bajta.

S obzirom na to da se *datagram* IPv4 može implementirati u veliki broj slojeva podataka tehnologije kao što su Ethernet, FDDI (Fibre Distributed Data Interface) i Token Ring jedinica za maksimalan prijenos ili maksimalnu veličinu *datagrama* varirat će ovisno o tehnologiji prijenosa OSI-a. Na slici 5 prikazana je usporedba MTU-a sa OSI slojevima druge razine.

Network Type	MTU size in Bytes
Ethernet	1500
IEEE 802.3	1492
Token Ring	4440 to 17940
FDDI	4352
IEEE 802.	4 8166
SMDS	9180
X.25	1007

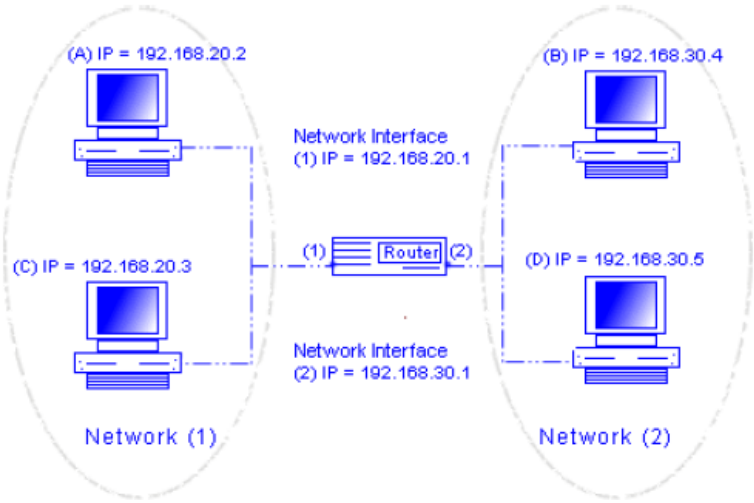
Slika 5. Usporedba MTU sa OSI slojevima 2 razine.

3.6. Fragmentacija IPv4

Tijekom slanja IP paketa preko interneta, paketi prolaze kroz mnoštvo različitih mreža koji su izgrađene na različitim OSI slojevima i tehnologijama, pa zato IP paket mora biti razlomljen na manje dijelove kako bi prošao kroz različite MTU tehnologije s kojima se susreće u svakoj mreži. Ti razlomljeni dijelovi moraju biti sastavljani u sekvenci pri završetku prolaska kroz navedene tehnologije. Ovaj proces je odrađuje mehanizma fragmentiranja u IPv4. Prilikom fragmentacija neke opcije biti će kopirane, dok druge opcije ostaju sa prvim fragmentom. Polja koja mogi biti pogođena fragmentacijom su: Polje opcija (Options field), Više zastavica fragmenata (More fragments flag), Fragment odstupanje (Fragment offset), Polje dužine internetskog zaglavlja (Internet Header Length Field), Polje ukupne dužina (Total Length Field) i Suma zaglavlja (Header Checksum). Polje fragment odstupanja (Fragment offset) se odnosi na lokaciju fragmenta, od početka do kraja fragmentiranja.

3.7. Dostava i usmjeravanje IPv4

Svrha IPv4 je primanje *datagrama* od jednog domaćina (hosta) te slanje ka drugom domaćinu (hosta). Svaka mreža ima dva domaćina s omogućenim IPv4. Slika 6 prikazuje dostavu i usmjerenje paketa uz IPv4. Računala A i C su izravno međusobno povezana, eliminirajući potrebu za usmjeravanjem podataka putem usmjerivača, isto vrijedi za računala B i D. Ako je potrebna komunikacija između mreže 1 i mreže 2, tada usmjerivač djeluje kao posrednik između strana koje komuniciraju.



Slika 6. Dostava i usmjeravanje IPv4.

3.8. Višesmjerni IPv4

Višesmjerni IP (*IP multicasting*) je specijalizirani oblik emitiranja u kojem se IP paketi šalju većem broju domaćina koji su naveli da žele primiti višesmjerne prijenose. IP *multicasting* je izgrađen na posebnom rasponu IP adresa; prema Internet Assigned Numbers Authority (IANA), adresni prostor za višestruko slanje zauzima raspon od 224.0.0.0 do 239.255.255.255. artikuliraju sljedeće točke *multicasting* IP-a:

U jedinstvenom okruženju čvor ima mogućnost slanja samo jednom drugom čvoru. U okruženju s višestrukim prijelazom, jedan čvor može učinkovito poslati jedan paket informacija većem broju odredišnih čvorova u jednoj operaciji. Operativni sustav čvora i TCP / IP složenica mora podržavati IP *multicasting* za čvor sudjelovanja u *multicastingu*. IP *multicasting* stvara jedinstveni tok podataka na koji se korisnici pretplaćuju. IP *multicasting* smanjuje zahtjeve za širinom pojasa prijenosa samo jedne instance podataka na više odredišta. Da bi IP *multicasting* mogao raditi, usmjerivači, sklopke i domaćini moraju imati Internet Protokol za upravljanje grupama (IGMP).

4. Internet protokol verzija 6 (IPv6)

Napisati nešto o ovoj cijelini.

4.1. Pojam IPv6

IPv6 je razvijen na temelju bogatog iskustva koje imamo iz razvoja i korištenja IPv4. U IPv6 su zadržani dokazani i uspostavljeni mehanizmi, poznata ograničenja su odbačena, a skalabilnost i fleksibilnost su prošireni. IPv6 protokol je dizajniran za obradu podataka na Interneta i za udovoljavanje zahtjevnim uslugama, mobilnost i krajnju sigurnost.

4.2. Zašto trebamo IPv6?

Iz povijesnih razloga, organizacije i vladine agencije Sjedinjenih Američkih Država, koristile su se najveći dio dodijeljenog IPv4 adresnog prostora. Ostatak svijeta morao je koristiti preostali dio IPv4 adresnog prostora. Određene organizacije su imale više IPv4 adresnog prostora od čitave Azije (gdje živi više od 50% svjetske populacije). Ovo je jedan od razloga zašto je implementacija IPv6 u Aziji mnogo češća nego u Europi i SAD-u. IPv4 ima teoretsku granicu od 4,3 milijarde adresa. Međutim, ranije metode distribucije adresa dodjeljivale su se neučinkovito. Slijedom toga, neke su organizacije dobile adresne blokove mnogo veće nego što su trebali. Moramo uzeti u obzir da će nam u budućnosti trebati IP adrese za milijarde uređaja. Dobavljači u svim industrijama razvijaju nadzor, kontrolu i sustave upravljanja temeljenima na IP-u.

4.3. Adresiranje IPv6

IPv4 adresni prostor pruža teorijski maksimum od 2^{32} adrese, što iznosi otprilike 4,29 milijardi adresa. Trenutno svjetska populacija prelazi otprilike 7 milijardi ljudi. Pa čak i ako je moguće koristiti 100 posto IPv4 adresnog prostora, ne bismo mogli pružiti IP adresu svima. Međutim, samo mali dio ovog adresnog prostora može se koristiti. U prvim danima IP-a, nitko nije predvidio postojanje interneta kakav danas poznajemo. Stoga veliki adresni blokovi su dodijeljeni bez razmatranja za globalno usmjeravanje i očuvanje adresna pitanja. Ovi se rasponi adresa ne mogu lako povratiti, pa stoga su mnoge neiskorištene adrese koje nisu dostupne za dodjelu. Evolucija Interneta i naših usluga pokazuje da ćemo u budućnosti, trebati imati adrese za korisnike i računala, ali trebat će nam i sve više adresa za sve vrste uređaja koji trebaju stalne internetske veze, poput pametnih telefona, tableta, web kamera, automobila i električnih brojila te

ostalih predmeta i stvari koje će koristiti Internet. Proizvođači automobila kao primjer, koji dizajniraju umreženi automobil budućnosti, trebat će puno IP adresa.

IPv6 adresni prostor koristi 128-bitnu adresu, što znači da ima maksimalno dostupno 2^{128} adresa. To je jednako 340.282.366.920.938.463.463.374.607.431.768.211.456, ili drugim riječima 6.65×10^{23} adrese po kvadratnom metru na zemlji. IPv6 adresa može se razvrstati u jednu od tri kategorije: Unicast, Multicast i Anycast adrese. *Unicast* - jedinstvena adresa koja jedinstveno identificira sučelje IPv6 čvora. Paket poslan na jednostranoj adresi se isporučuje na sučelju koje je identificirano tom adresom. *Multicast* - Adresa za višestruko slanje, identificira skupinu IPv6 sučelja. Paket poslan u multicast adresu obrađuju svi članovi grupe za višestruko slanje. *Anycast* adresa - adresa koja se dodjeljuje na više sučelja (obično na više čvorova). Paket poslan na anycast adresu isporučuje se samo jednom od tih sučelja, obično najbližem. IPv6 adrese dodjeljuju se sučeljima kao i u IPv4, a ne u čvorovima kao u OSI, tako da svako sučelje čvora mora imati jednu jednostranu (unicast) adresu. Može i jedno sučelje biti dodijeljeno više IPv6 adresa bilo koje vrste (unicast, multicast i anycast). Čvor može prepoznati adresu bilo kojeg od njegovih sučelja. Također je moguće dodjeljivanje jednu jednostranu (unicast) adresu većem broju sučelja zbog opterećenja dijeljenja, ali ako se to učini tada se mora osigurati hardver i upravljački program koji to podržava.

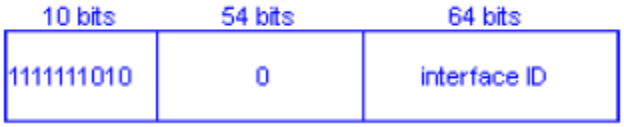
Svaka IPv6 adresa ima 128-bitnu binarnu datotečnu adresu, primjer je 10000000000001111011100001100010000000000000000000000000000000000110 00001000000011101101100111001. Ove adrese se mogu pretvoriti u heksadecimalni oblik, tako da su razdvojeni u osam 16 bitnih blokova razdvojeni kolonama; pretvaranjem gornje binarne adrese stvara se sljedeći IPv6 adresa 2001:770:18:2::c101:db39. IPv6 protokol je zbog svoje 128-bitne adrese u mogućnosti pružiti jedinstvene adrese.

Global unicast	(everything else)	
Link-Local unicast	1111111010	FE80::/10
Multicast	11111111	FF00::/8
Address type	**Binary prefix**	**IPv6 notation**

Slika 7. Dodjela IPv6 unicast adrese.

Prva vrsta unicast adresiranja IPv6 naziva se Link-Local unicast adresiranje; ova vrsta IPv6 adrese dodijeljena je fizičkom sučelju na 3. stupnju. Link-Local unicast adresa je

identifikator za jedno sučelje. Sva sučelja moraju imati najmanje jednu Local-Link unicast adresu. Jedno sučelje može imati više IPv6 adresa bilo koje vrste (unicast, anycast i multicast). Link-Local adrese su dizajnirane za adresiranje na jednom linku zbog svrha poput automatske konfiguracije adresa, otkrivanje susjeda ili kada nema usmjerivača u blizini. Link-Local adrese imaju sljedeći format:

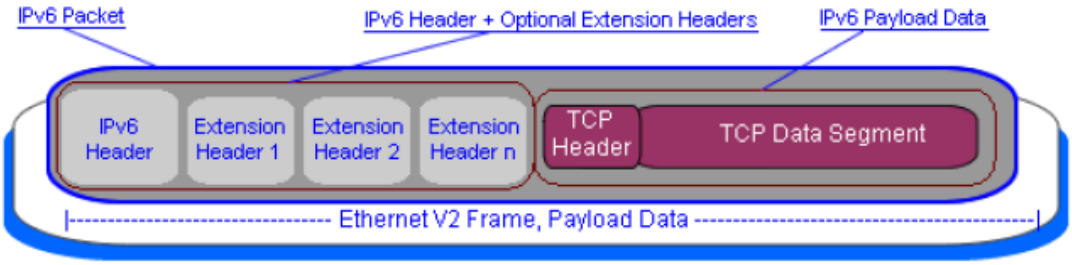


Slika 8. Link-Local unicast adresa.

Slika 9. Global unicast adresa.

Globalni prefiks usmjeravanja je vrijednost dodijeljena web mjestu, ID podmreže je identifikator veze unutar web lokacije, a ID sučelja obično se izrađuje s MAC adrese sučelja.

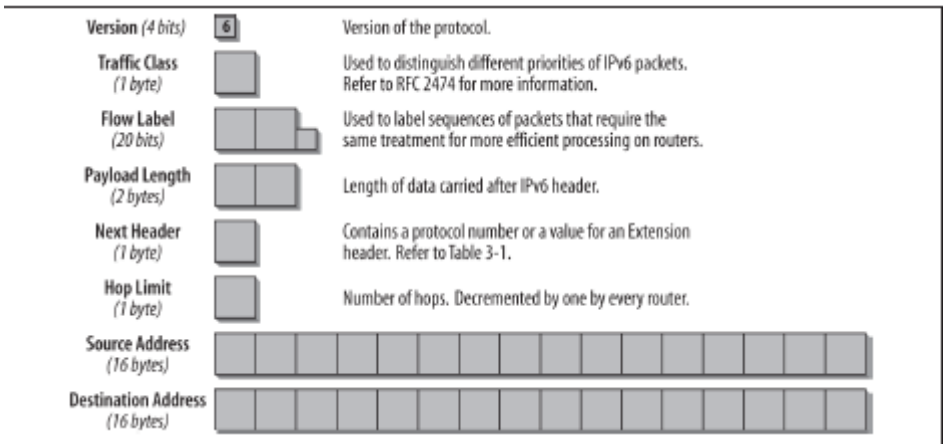
4.4 Enkapsulacija i formatiranje IPv6



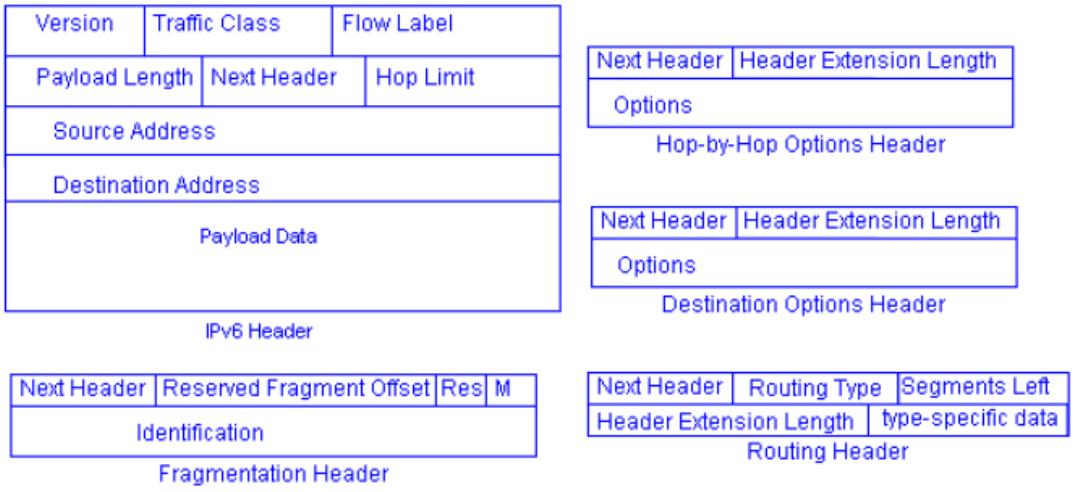
Slika 10. IPv6 enkapsulacija.

IPv6 je enkapsuliran u sloju 2 na gotovo isti način kao i IPv4, ali zaglavlje i opcijska proširenja zaglavlja zauzimaju više prostora u IPv6, 20 bajtova za IPv4 u odnosu na 40 bajtova za IPv6. Glavna razlika između IPv4 i IPv6 je struktura i format zaglavlja paketa. Specifikacija za IPv6 zaglavlje je sljedeća: 4 bitno polje Verzija (Version field) sadrži broj verzije internetskog protokola 4 ili 6. 8-bitni Polje Klasa prometa (Traffic Class) omogućuje izvoru da identificira željeni prioritet isporuke paketa, u odnosu na

ostale pakete iz istog izvora. 20-bitno polje Tok (Flow Label Field) se koristi se za označavanje slijeda paketa koji bi trebali dobiti poseban tretman od usmjerivača. 16-bitno polje dužina korisnog opterećenja (Payload Length field) označava duljinu podataka o korisnom opterećenju uključujući i proširenja zaglavlja. 8-bitno polje Sljedeće zaglavlje (Next Header Field) identificira vrstu zaglavlja odmah nakon IPv6 zaglavlja. 8-bitno Preskok limit (Hop Limit field) polje koristi se za kontrolu kako kroz koje čvorove paket može proći. 128-bitno polje izvora adrese sadrži adresu inicijatora paketa i 128-bitna odredišna adresa sadrži adresu predviđenog primatelja paketa.



Slika 11. Polja u IPv6 zaglavlju.



Slika 12. Proširenja zaglavlja IPv6.

Zaglavlje Skok-po-Skok (*Hop-by-Hop Options*) koriste se za prenašanje neobaveznih informacija koje pregledava svaki čvor duž putovanja paketa. Opcija Skok-po-Skok se

u IPv6 zaglavlju identificira s vrijednošću zaglavlja (vrijednost 0). Odredište zaglavlja opcija (*Destination Options header*) koristi se za prenošenje neobaveznih podataka koji moraju ispitati samo odredišni čvor/ove paketa. Odredište zaglavlja opcija identificirano je vrijednošću zaglavlja (vrijednost 60) u prethodnom zaglavlju. Zaglavlje usmjeravanja (*Routing header*) koristi IPv6 izvor za popis jednog ili više srednjih čvorova koji će biti "posjećeni" na putu do odredišta paketa. Zaglavlje usmjeravanja identificira se s vrijednošću zaglavlja od 43. Zaglavlje fragmenta (*Fragment Header*) koristi IPv6 izvor za slanje većih paketa. Za razliku od IPv4, fragmentaciju u IPv6 izvode samo izvorni čvorovi, a ne usmjerivači duž puta isporuke paketa. Zaglavlje fragmenta identificirano je s vrijednošću 44 sljedećeg zaglavlja u prethodnom zaglavlju.

4.5. Veličina IPv6 Datagrama

IPv6 ima minimalnu veličinu datagrama od 1280 bajtova. U Ethernet sustavima preporučuje se najmanja datagram IPv6 veličina od 1500 bajtova. Ako je IPv6 podvrgnut prijevodu na IPv4, gdje je najmanja zakonska veličina datagrama 576 bajtova, IPv6 sustavima dopušteno je smanjiti svoju nosivost na 1232 bajta što omogućava prostor za 40-bajtno zaglavlje IPv6 i 8-bajtno zaglavlje fragmentacije. S obzirom na to korisni teret polja duljine u zaglavlju IPv6 iznosi 16 bita i može prenositi do 65.535 bajtova podataka. Postoji dodatak IPv6 koji se zove Jumbo-gram, to su paketi s korisnim opterećenjem većim od 65.535 bajtova. Jumbo grami se postižu upotrebom produžetka zaglavlja koji koristi 32-bitno polje duljine korisnog opterećenja koje dopušta polju da popuni do 4.294.967.295 bajta podataka. Drugačija mrežna oprema podržava različite datagram veličine, tako da podaci prelaze preko linkova različitog kapaciteta. Maksimalna propusnost određena je jedinicom za maksimalni prijenos (MTU) cijele veze.

4.6. IPv6 fragmentacija, dostava i usmjeravanje

U slučajevima kada je fragmentacija potrebna, tada se koristi zaglavlje ekstenzije u fragmentaciji od izvora IPv6, međutim za razliku od IPv4, fragmentaciju u IPv6 izvode samo izvorni čvorovi, ne usmjerivači na putu isporuke paketa.

Metodologija isporuke i usmjeravanja u IPv6 prilično se razlikuje od svoje prethodnice IPv4. Kad se IPv6 čvorovi povežu s mrežom, prvi se put konfiguriraju s lokalnom vezom za unicast (*Link-Local unicast address*), oni tada pokreću protokol otkrivanja susjeda

(*Neighbour Discovery Protocol*). Čvorovi (domaćini i usmjerivači) koriste otkrivanje susjeda kako bi odredili adrese sloja veze (Sloj 2) za susjede za koje se zna da borave na priloženim vezama. Domaćini također koriste otkrivanje susjeda kako bi pronašli susjedne usmjerivače koji su voljni proslijediti pakete u njihovo ime. IPv6 također koristi zaglavlje proširenja za usmjeravanje koje izvor IPv6 može upotrijebiti za popis jednog ili više srednjih čvorova koji će biti "posjećeni" na putu do odredišta paketa.

4.7. IPv6 Multicast

Razlikujemo tri vrste adresiranja u IPv6: unicast, anycast i multicast.

Jedinstvena adresa (unicast address) jedinstveno identificira sučelje IPv6 čvora. Paket poslan na tu adresu se isporučuje na sučelju koje je identificirano tom adresom.

Anycast je identifikator za skup sučelja, koji uobičajeno pripadaju različitim čvorovima. Paket poslan na anycast adresu isporučuje se na jedno od sučelja koje identificira tu adresu ("najbližu", u skladu s mjerom udaljenosti protokola usmjeravanja).

Multicast je identifikator za skup sučelja, koji uobičajeno pripadaju različitim čvorovi. Paket poslan na adresu za višestruko slanje isporučuje se svim sučeljima koje identificira ta adresa. IPv6 adrese za višestruko slanje nalaze se u sljedećem rasponu FF00 :: / 8, bilo koje adrese koje su preuzete iz baze podataka unicast adresa, one uključuje sve druge adrese osim :: / 128, :: 1/128, FF00 :: / 8 i FE80 :: / 10. Na slici 13 prikazan je oblik adrese IPv6 za višestruke adrese.

Slika 13. Format adrese IPv6 Multicast.

Prikazuje grupu internetskih poslužitelja multicasta kojima je dodijeljen ID grupe od 101Hex, što rezultira adresu sljedećeg formata, FF0E: 0: 0: 0: 0: 0: 0: 101. Finalno IPv6 multicast koristi *Multicast Listener Discovery* (MLD) protokol koji ga razlikuje od IPv4 koji koristi IGMP. Tijekom prelaskom na IPv6 inženjeri su razvili dva kratkoročna rješenja za pitanje iscrpljivanja IPv4 adrese, besklasno usmjeravanje inter domena (CIDR) i prevođenje mrežnih adresa (NAT). Ove dvije tehnologije su dizajnirane kako bi produžile životni vijek IPv4 adresnog prostora, te su tehnologije stekle prednost

prvog pokretača u odnosu na IPv6. Te tehnologije trenutno ometaju implementaciju IPv6.

4.8. Sigurnost IPv6

Da bi zaštitili podatke korisnika, korisnici moraju biti svjesni mogućih prijetnji. Korisnici se često usredotočuju isključivo na zlonamjerne napade stranih mreža. Sveobuhvatni sigurnosni koncept treba razmotriti mnoge druge aspekte. Neke od mogućih točka slabosti su: nedovoljni ili nepostojeći koncepti informatičke sigurnosti i odgovarajuće odredbe, nepridržavanje ili nedovoljna kontrola IT sigurnosnih odredaba, ometanje prava (krađa lozinke), nepravilna upotreba ili neispravna administracija IT sustava, zloupotreba prava, slabosti u softveru (npr. međuspremnik), manipulacije, krađe ili uništavanja IT uređaja, softvera ili podataka, prisluškivanje mreže (njuškanje ožičenih ili bežičnih mreža) ili ponovno reproduciranje poruke, trojanski konji, virusi i crvi, sigurnosni napadi poput maskiranja, prevara IP-a, napada uskraćivanja usluge (DoS), napadi čovjeka u sredini, zlouporaba usmjeravanja. Postoje mnoge statistike koje pokazuju da su napadi izvana samo manji dio svih mogućih rizika. Mnoge prijetnje dolaze iz unutarnje mreže te se u mnogim slučajevima mogu povezati s korisnikovim nedoličnim ponašanjem ili neispravnim upravljanjem. Većinu tih rizika ne možemo kontrolirati tehničkim mehanizmima. Standardne sigurnosne prakse uključuju dva pravca razmišljanja: CIA i AAA.

CIA pravac uključuje: povjerljivost integritet dostupnost (*Confidentiality Integrity Availability*): *Povjerljivost* označuje da pohranjene ili prenesene informacije neovlašteno se ne mogu pročitati ili biti promijenjen od treće strane. *Integritet* označuje da se mogu otkriti bilo kakve promjene prenesenih ili pohranjenih podataka. *Dostupnost* označuje da dotične informacije u svakom trenutku su lako dostupne ovlaštenim korisnicima.

AAA pravac uključuje: ovjeru autorizaciju izvještavanje (*Authentication Authorization Accounting*): *Ovjera* osigurava pojedince ili grupe korisnika koji potvrđuju svoj identitet uz pomoć: korisničkog imena, e-mail adrese, lozinke, PIN ili TAN kodom.

Autorizacija osigurava ovjerenom korisniku ili grupi korisnika da imaju odgovarajuća prava pristupa informacija kojima pokušavaju pristupiti. Uobičajene implementacije uključuju popis za kontrolu pristupa (*Access Control List*). *Izvještavanje* služi za

prikupljanja podataka o korištenju resursa. Dnevnik HTTP poslužitelja bio bi uobičajeni oblik izvještavanja.

Neopovrgavanje (*nonrepudiation*) nije uključeno u pravce CIA i AAA. Neopovrgavanje predstavlja određenu radnju, poput slanja, primanja ili brisanja podataka, nju ne može odbiti bilo koja od uključenih strana. Ovi sigurnosni zahtjevi trebaju osigurati dva osnovna sigurnosna elementa: šifriranje (za pružanje povjerljivosti) i sigurne kontrolne sume (radi osiguranja integriteta). Kombinacijom ova dva elementa mogu se koristiti za pružanje više složene usluge, kao npr. autentičnost.

Postoje dva oblika šifriranja koji se obično koriste za šifriranje. *Prvi oblik šifriranja* zove se tajna kriptografija ključeva, koja se također nazvana i simetrično šifriranje ključa. Ona zahtijeva od pošiljatelja i primatelja da odgovore na zajedničku tajnu (tj. ključ ili lozinku) koja se zatim koristi za šifriranje i dešifriraju razmijenjene podatke. Uobičajeni algoritmi simetričnih ključeva su AES, DES, 3DES, IDEA i RC-4. *Drugi oblik šifriranja* zove se kriptografija javnog ključa, koja se također naziva asimetrična enkripcija. Algoritam za asimetrično šifriranje koristi ključni par koji se sastoji od poznatog i distribuiranog javnog ključa i pojedinačni privatni ključeva. Kad se poruka šifrira pomoću javnog ključa i dešifrira ih primatelj odgovarajućim privatnim ključem, samo predviđeni primatelj moći će vidjeti šifriranu poruku. Ovaj oblik šifriranja može biti koristan za uspostavljanje povjerljive razmjene podataka. Uobičajeni algoritmi asimetričnih ključeva su RSA, ElGamal i kriptografija eliptičnih krivulja (ECC). Sigurne kontrolne sume ili *hash* funkcije često pružaju integritet podataka. *Hash* funkcija uzima unos proizvoljne duljine i izlazne fiksne duljine. Izlazne fiksne duljine se nazivaju *message digest* ili *hash-om* originalne ulazne poruke. Ovi *hashei* su jedinstveni i tako pružaju cjelovitost poruke. Uobičajene jednosmjerne *hash* funkcije su SHA-1 i MD-5. IPsec standard koristi kombinaciju algoritamskih izbora na temelju simetrične i asimetrične kriptografije, kao i jednosmjerne hash funkcije.

IPsec, opisan je u RFC 4301, i on definira sigurnosnu arhitekturu za obje verzije IP-a i za IPv4 i za IPv6. Elementi IPsec okvira su: opći opis sigurnosnih zahtjeva i mehanizama na mrežnom sloju, protokol za šifriranje (ESP), protokol za provjeru autentičnosti (AH), definicija za uporabu kriptografskih algoritama za šifriranje i ovjera, definicija sigurnosnih politika i sigurnosnih udruga između komunikacije kolega i

upravljanje ključevima. Konfiguracija IPsec stvara granicu između zaštićenog i nezaštićenog područja. Granica može biti oko jednog domaćina ili mreže. Pravila kontrole pristupa određuje administrator te utvrđuje što se događa s paketima koji prelaze granicu. Sigurnosni zahtjevi definirani su bazom podataka sigurnosnih politika (SPD), općenito svaki je paket zaštićen pomoću IPsec sigurnosnih usluga, odbačen je ili dopušten zaobići IPsec zaštitu na temelju primjenjivih SPD pravila koje su prepoznali selektori. Selektori su specifični kriteriji podudaranja prometa koje je definirao administrator npr., određena aplikacija koja se prenosi s podmreže na određenog domaćina.

Sigurnosna udruženja (SA) su sporazumi između komunikacijskih vršnjaka (*communication peers*). Taj ugovor sastoji se od tri elementa: ključ, mehanizam za enkripciju ili provjeru autentičnosti, i dodatne parametre za algoritam. SA-ovi su jednosmjerni i svaka zasebna sigurnosna služba zahtijeva SA. To znači da dvoje komunikacijskih vršnjaka koji žele za šifriranje i provjeru autentičnosti dvosmjerne komunikacije, potrebni su im četiri SA-i (jedan par za enkripcija i jedan par za provjeru autentičnosti). Dvosmjerni promet aplikacija npr, dvosmjerna Telnet veza također zahtijeva četiri SA-a pri svakoj komunikaciji. Vršnjak A mora zaštititi promet koji pokreće i koji povraća promet od Vršnjak B. Također zahtijeva dva dodatna SA kako bi se osiguralo da ako *Peer B* pokrene *Telnet* sesiju da su i jedno i drugo zaštićeni i povratni promet za ovaj scenarij.

IPsec razlikuje dva načina transporta: transkort mode i tunnel mode.

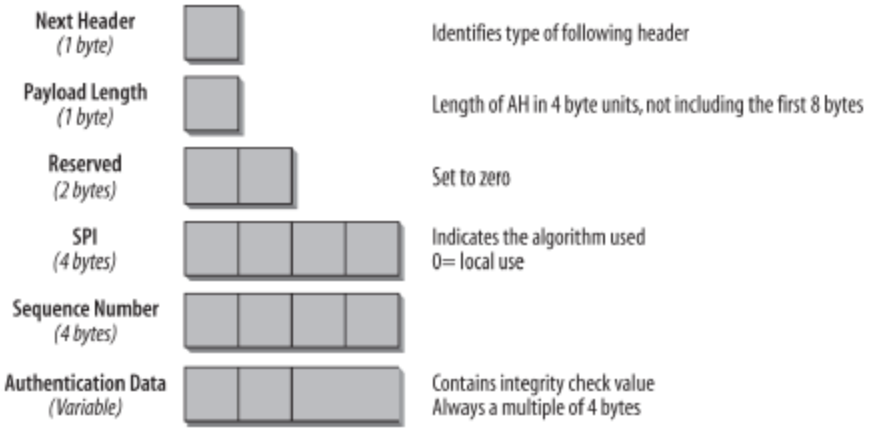
1. *Transport mode*: SA je napravljen između dva krajnja čvora i definira šifriranje ili provjeru autentičnosti za korisni teret svih IP paketa za tu vezu. IP zaglavlje nije šifrirano.
2. *Tunnel mode*: SA se obično izvodi između dva sigurnosna prolaza (obično vatrozida). cijeli paket, uključujući izvorno IP zaglavlje, šifrira ili ovjerava enkapsulirajući ga u novo zaglavlje. Ovo je temelj virtualne privatne mreže (VPN).

Većina sigurnosnih mehanizama koje pruža IPsec zahtijevaju uporabu kriptografskih ključeva. Određen skup mehanizama definiran je za postavljanje ključeva. Potrebna je podrška za ručnu i automatiziranu distribuciju ključeva. RFC 4301 specificira IKEv2 kao mehanizam automatizirane raspodjele ključeva. Mogu se koristiti i drugi

mehanizmi. Da bi se osnovalo sigurnosno udruženje (SA), vršnjaci u komunikaciji moraju se složiti na kriptografskom algoritmu i ključevima za pregovaranje. Pregovaranje o ugovoru o stabilizaciji i pridruživanju često se događa preko nesigurnih staza. Internet razmjena ključeva (IKE) određuje protokol koji dopušta razmjenu i pregovaranje parametara za SA.

5. Elementi sigurnosti IPv6

IPsec opisuje opće sigurnosne mehanizme koji se mogu koristiti i s protokolom IPv6 i protokolom IPv4. To znači da IPv6 nije sigurniji od IPv4. U početku se IPv6, primjenjivao u svakom IPsec-u IPv6 skupu koji je bio obvezna te se preporučila uporaba IKE-a za upravljanje ključevima. S RFC 6434, „IPv6 zahtjevi čvorova", koji imaju strogo pravilo, ono se moralo ublažiti tako da bi IPv6 skup trebao koristiti IKE-u. S time prepušta se dobavljačima da odluče trebaju li njihovi IPv6 proizvodi IPsec ili ne. Glavni razlozi za nepraktičnost primijene je taj što se tražiti implementacija IPsec na svim vrstama posebnih vrsta uređaja, npr. senzorima na kojima su resursi vrlo ograničeni ili vrste uređaja s vrlo posebnim aplikacijama koje mogu imati sigurnosni pristup. S druge strane, isti RFC navodi da su čvorovi koji implementiraju IPsec jače zahtjeve nego prije. Podrška za RFC 4301, „Sigurnosna arhitektura za Internet Protokol ", trenutno je obvezna, što uključuje upotrebu IKEv2 za automatsko upravljanje ključevima i zahtjevima za podršku za minimalni skup kriptografskih algoritama. Izrada IPsec je interoperabilniji u svim implementacijama dobavljača. Specifikacija IPsec definira protokole za zaglavlje autentifikacije (AH) i inkapsuliranje sigurnosnog zaglavlja opterećenja (ESP). Uz IPv6, ta su zaglavlja uključena kao zaglavlja za produženje. Implementacija IPsec-a mora podržavati ESP i AH. Starija specifikacija je zahtijevala potrebnu podršku za oba protokola. Zahtjev za AH podršku uklonjen je zbog toga što se ESP može koristiti za pružanje integriteta, koji se u većini slučajeva pokazalo dovoljnim. Zaglavlje identiteta (AH) pruža integritet i autentifikaciju (bez povjerljivosti) za sve krajnje podatke koji se prenose u IP paketu. Podržava različite provjere autentičnosti. AH se nalazi između zaglavlja IPv6 i zaglavlja gornjeg sloja (npr. TCP, UDP, ICMP). Ako postoje zaglavlja nastavka, tada se oni moraju smjestiti nakon sljedećih elemenata: Skok-po-Skok (Hop-by-Hop), zaglavlja za usmjeravanje i proširenje fragmenata. Slika 14 opisuje zaglavlje identiteta.zaglavlja za usmjeravanje i proširenje fragmenata. Slika 14 opisuje zaglavlje identiteta.

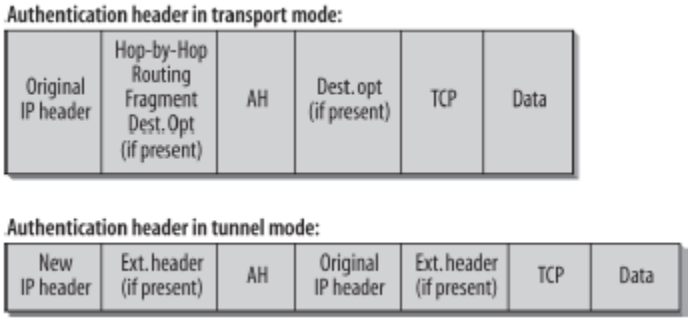


Slika 14. Zaglavlje identiteta.

- Zaglavlje 1 bajt predstavlja polje sljedećeg zaglavlja te identificira vrstu zaglavlja koje slijedi provjeru autentičnosti zaglavlja.
- Dužina korisnog opterećenja 1 bajt, opisuje duljinu zaglavlja u četverobajterskim jedinicama, ne uključujući prvih osam bajtova u proračunu. Ta duljina je potrebna zbog toga što ona provjera autentičnosti podataka u AH, te se mogu razlikovati po duljini,a ovisne su o algoritmu koji se koristi.
- Rezerva 2 bajta, ne koristi se zbog toga što je postavljena na nulu.
- Indeks sigurnosnih parametara (SPI) 4 bajta predstavlja proizvoljnu 32-bitnu vrijednost. Prijemnik se koristi za identificiranje SA do kojega dolazni pripadni paket. Polje SPI mehanizam obvezno je za mapiranje ulaznih prometa do jednokratnih (unicast) SA koji moraju podržavati sve AH implementacije. Ako IPsec implementacija podržava multicast, tada mora podržati i multicast SA-i koriste algoritam de-multipleksa u svrhu mapiranja ulaznih podataka IPsec datagrama na SA. SPI vrijednosti u rasponu od 1 do 255 predstavljaju rezerve od strane IANA (*Internet Assigned Numbers Authority*) za buduću upotrebu. SPI vrijednost od 0 rezervirano je za lokalnu upotrebu koje je specifičnu za implementaciju.
- Redni broj 4 bajta, ovaj 32-bitni redoslijedni broj predstavlja porast brojača. To mora postaviti pošiljatelj, ali na primatelju je odluka hoće li djelovati na njega. To osigurava da se paketi s identičnim podacima ne ponavljaju više puta. Također se sprječavaju napadi ponovnog ponavljanja u SA s jednokatnim ili s jednim pošiljateljem. Za više pošiljateljski SA, značajke protiv ponovnog ponavljanja AH nisu dostupne, jer AH nema sredstva za sinkronizaciju brojila

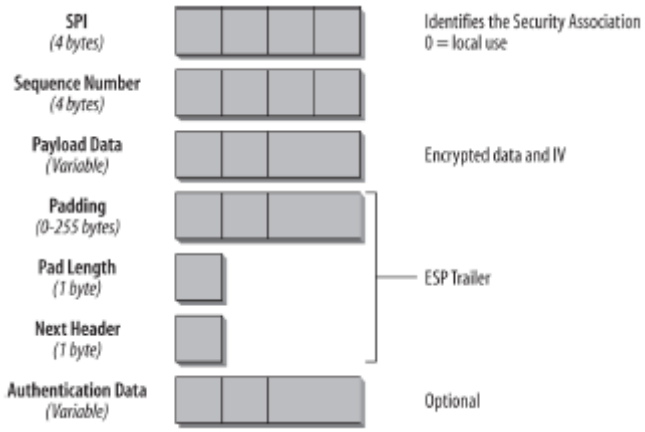
paketa među više pošiljatelja. Pri uspostavljanju SA-a vrijednost je postavljena na 0 kod pošiljatelja i kod primatelja. Prvi paket uvijek ima vrijednost 1, te se povećava za jedan za svaki uzastopni paket. Kad je dosegnuta vrijednost 232, brojač se ponovo vraća na nulu.

- Vrijednost provjere integriteta, sadrži kontrolni zbroj (Vrijednost provjere integriteta ili ICV) paket. Duljina ovisi o algoritmu odabranom za uspostavljanje SA. Uvijek je a više od četiri bajta.



Slika 15. Zaglavlje autentifikacije.

Inkapsuliranje zaglavlja sigurnosnog opterećenja (eng. *The Encapsulating Security Payload header*) je također jedan od elemenata sigurnosti. Pruža integritet, povjerljivost, provjeru izvornosti podataka, uslugu protiv ponovnog ponavljanja i ograničenu povjerljivost protoka prometa za sve krajnje podatke koji se prenose u IP paketu. ESP je definiran u RFC 4303. ESP zaglavlje nalazi se u transportu (npr., UDP ili TCP), mrežnoj kontroli (npr. ICMP) ili u zaglavlju protokola usmjeravanja (npr. OSPF).

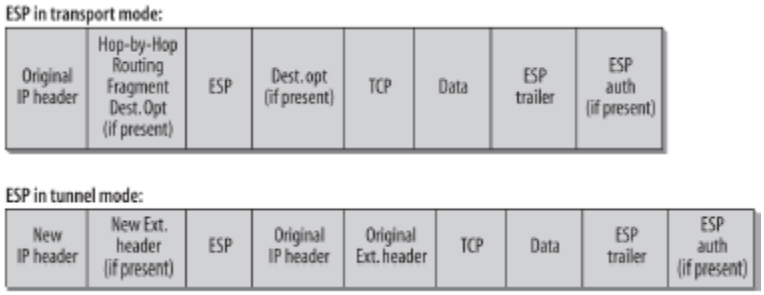


Slika 16. Format ESP-a.

- Indeks sigurnosnih parametara (SPI) 4 bajta predstavlja 32-bitnu vrijednost. Prijemnik se koristi za identificiranje SA do kojeg dolazni pripadajući paket. Za polje SPI obvezan je i mehanizam koji se koristi za mapiranje ulaznog prometa do jednokratnih SA te mora podržavati sve implementacije ESP-a. Ako IPsec implementacija podržava multicast, a mora ju podržati, SA-i koriste algoritme de-multipleksa koji su navedeni u tu svrhu za mapiranje ulaznih podataka IPsec datagrama na SA. SPI vrijednosti su u rasponu od 1 do 255 koji su rezervirani od strane IANA (Internet Assigned Numbers Authority) a služe za buduću upotrebu. SPI vrijednost 0 rezervirana je za lokalnu upotrebu, koja je specifična za implementaciju te se ne smije slati.
- Redni broj (*Sequence number*) 4 bajta – ovaj 32-bitni broj predstavlja porast brojača. Njega postavlja pošiljatelj, ali primatelj je taj koji odlučuje hoće li to djelovati na njega. S time se osigurava da se paketi s identičnim podatcima ne ponavljaju više puta. Također sprječava napade ponovnog ponavljanja u SA. U slučaju više pošiljatelja, značajke protiv ponovnog ponavljanja ESP-a nisu dostupne jer ESP nema način za sinkronizaciju brojila paketa među više pošiljatelja. Prilikom uspostavljanju SA-a vrijednost je postavljena na nulu i kod pošiljatelja i kod prijemnika. Prvi paket uvijek ima vrijednost 1, time se povećava za jedan za svaki uzastopni paket. Kad je vrijednost 232 dostignut, brojač se ponovo vraća na 0.
- Podaci o korisnom opterećenju (promjenjiva vrijednost) sadrže šifrirane podatke, kao i vektor inicijalizacije enkripcije.
- Poravnanje (0 do 255 bajtova): koristi se za poravnanje paketa u više od 4 bajta i za postizanje minimalnog paketa veličina ako mehanizam za šifriranje zahtijeva jedan.
- Dužina poravnanja (1 bajt) označava broj prethodnih bajtova.
- Sljedeće zaglavlje (*Next header*) (1 bajt) služi za identifikaciju vrste zaglavlja koje slijedi zaglavlje ESP-a. Kako bi se olakšalo brzo stvaranje i odbacivanje prometa u podršci povjerljivosti protoka prometa, vrijednost protokola 59 (nema sljedećeg zaglavlja) označava pivotni (eng. *dummy*) paket. Prijemnik lažnog paketa mora ga odbaciti bez kreiranje poruke o pogrešci
- Vrijednost provjere integriteta (*Authentication data*) predstavlja vrijednost provjere integriteta (ICV) a to je polje promjenjive duljine koja sadrži kontrolni

zbroj. Izračunava se preko polja ESP zaglavlja, korisnog opterećenja i ESP-a. Prisutan je samo ako je odabrana usluga integriteta, a pruža bilo odvojeni algoritam integriteta ili algoritam kombiniranog načina koji koristi ICV. Duljina polja određena je odabranim algoritmom integriteta i povezan je sa SA.

Polja poravnanja, dužina poravnanja i sljedeće zaglavlje su dio ESP-a. Šifriranje algoritam je ili određen ručno i uključeno u SA za paket protoka ili se dinamički dogovara protokolom razmjene ključeva. ESP se može koristiti i u načinu prijevoza (*transport mode*) i u tunelima (*tunnel mode*). Na slici 17 prikazan je izgled prijevoznog i tunelnog načina ESP-a.



Slika 17. Prikaz ESP-a u načinu prijevoza i u tunelima.

U načinu prijevoza, zaglavlje IP-a i produžeci zaglavlja koja slijede nisu šifrirani, inače se paket ne može proslijediti. Ako kompletni paket mora biti šifriran, treba koristiti način tunela. Isto kao kod AH u načinu tunelu, unutarnji paket sadrži IP adresu pošiljatelja i primatelja, dok vanjsko IP zaglavlje sadrži IP adresu krajnjih točaka tunela. ESP zaglavlje se može koristiti s NULL opcijom šifriranja, koja je definirana u RFC 2410. S NULL enkripcijom upotrebljava se samo opcija provjere autentičnosti ESP-a i paket nije šifriran.

Kombinacija zaglavlja identiteta (AH) i inkapsuliranje zaglavlja sigurnosnog opterećenja (ESP) moguća je. Dva zaglavlja mogu se koristiti i u kombinaciji. U tom slučaju AH mora prethoditi zaglavlju ESP-a za provjeru autentičnosti i integriteta prije nego što se paket dešifrira. Opcija autentifikacije uključena je u zaglavlje ESP-a kako bi se omogućila autentifikacija šifriranih paketa sa samo jednim zaglavljem.

Ako se AH zaglavlje koristi u načinu tunela, prvo IP zaglavlje uključeno je u autentifikaciju. Ako se koristi zaglavlje ESP, tada je samo dio paketa koji slijedi zaglavlje ESP-a ovjereno. Ako je potrebno šifriranje i integritet IP adresa, oba zaglavlja

moraju se kombinirati. Ako se koriste oba zaglavlja, nije potrebno koristiti provjeru autentičnosti u zaglavlju ESP-a. S druge strane, ESP zaglavlje s NULL enkripcijom može se koristiti ako je dana autentifikacija dovoljna. Interakcija IPsec s elementima IPv6 odvija se uz korištenje IPsec za IPv6 koji pruža istu sigurnost kao i IPsec za IPv4. Međutim postoje područja na kojima se IPsec ne može lako kombinirati s drugim uslugama, kao što su: način tunela, temeljni elementi i IPsec-a i višestrukih tranzicijskih mehanizama. U tom slučaju se mogu stvarati poteškoće za postojeće vatrozidove i sigurnosne prolaze na rubu interne mreže. Šifrirani IPsec tunel izgrađen kroz vatrozid koji pruža potpunu sigurnost za domaćine s obje strane ali, onemogućuje vatrozidu da otkrije opasan ili neovlašten sadržaj. Jedan od načina da se to pitanje riješi je definiranje SA-ova između sigurnosnih prolaza, a ne između krajnjih čvorova. Još jedno pitanje da li unutarnji paket može sadržavati informacije koje predstavljaju prijetnju za unutarnje mreže. Te prijetnje mogle bi biti informacije o usmjeravanju ili upravljačke poruke mreže (npr. ICMP preusmjeravanje). Proširene mogućnosti mobilnosti s neprekidnim mijenjanjem IP adresa mogu dovesti do situacije s kojom se teško upravlja i kontrolira u IPsec okruženjima. Dinamične adrese poput adrese privatnosti (RFC 4941) stvaraju poteškoće ako se koriste za IKE provjere identiteta.

5.1. IPv6 sigurnosne zamke (*eng. Gotchas*)

Sigurnost u IPv6 mreži bitno se ne razlikuje od sigurnosti u IPv4 mreži. Mnogi postojeći dobro poznati IPv4 napadi mogu se izvoditi s IPv6, pa su tako sredstva za osiguravanje podataka slična. Dizajneri sigurnosnih koncepata i računalne sigurnosne zajednice morat će pronaći načine kojima će zaštititi njihove mreže od novih napada. Uz primjenu snažnih i dobro osmišljen sigurnosnih dizajna u dvosmjernoj mreži. Prije implementacije IPv6 potrebno je napraviti prvi korak zaštite. IPv6 je uključen u većinu operativnih sustava, obično ga je jednostavno konfigurirati i često je postavljen prema zadanim postavkama, čak i mehanizmi tunela postavljeni su prema zadanim postavkama. IPv4 mrežni administratori vjeruju da se ne trebaju brinuti zbog IPv6, ali oni ne shvaćaju da možda već postoji promet IPv6 u njihovoj mreži. Tu činjenicu koriste IPv6 hakeri koji upadaju u IPv4 mreže. Kao prvi korak zaštite, poželjno je filtrirati sav promet IPv6 koji ulazi i izlazi iz vaše mreže. Uz to bi moglo biti pametno nadzirati i revidirati IPv6 promet, posebno poruke poput rutera ili oglasa susjeda koji se može koristiti za pogrešno konfiguriranje klijenata. Većina sigurnosnih stručnjaka slaže se da ne postoji najbolji mehanizam u osiguravanju mreže za unutarnji ili vanjski napad.

Primjerima najboljih praksi i obukama korisnika može se svesti na najmanju moguću mjeru rizika.

5.2. Infrastruktura javnog ključa (PKI)

Iako RFC 4301 specificira zahtjev za IPSec u IPv6 protokolu, to ne obuhvaća način na koji će se ključevi razmjenjivati. Moguće je ručno postaviti unaprijed podešene ključeve, ali u velikim poduzećima ovaj zadatak postaje naporan i dugotrajan. U takvim sredinama korištenje centralnog poslužitelja je idealno. Donedavno uz IPv6 nije bilo centraliziranih poslužitelja. To se promijenilo s poslužiteljima koji se temelje na IKEv2 protokolu koji je naveden u RFC 5996. Prednosti IKEv2 su njegova upotrebljivost i na IPv4 i na IPv6 te na njegovu jednostavniju implementaciju. Nije kompatibilan s uređajem prva verzija IKE, ali obrasci zaglavlja obje verzije dovoljno su slični da ih pokreću obje preko istog UDP ulaza.

5.3. Vatrozidovi i sustavi za otkrivanje/sprečavanje provale

Iako se IPsec smatra jednom od glavnih prednosti IPv6, on uvodi i nove probleme. Ako su paketi šifrirani od kraja do kraja, kako središnji uređaj pregledava pakete bez dešifriranja? Pohranjivanje svih ključeva za šifriranje u središnjoj lokaciji ostavlja „točku otkaza“ za hakere pomoću koje mogu provaliti i ukrasti sve ključeve šifriranje mreže. Tunelska izdanja IPv4 IDS / IPS sustav, uključuju nedostatak detekcije IPv6 protokola i opće nedostatke potpisa za napad na IPv6. Vatrozidi koji podržavaju IPv6 uključeni su u većini operativnih sustava, ali vatrozidi koji drže stanje veza nisu implementirani. Cisco, Checkpoint i NetScreen (Juniper), imaju državni pregled IPv6 paketa. Proizvodi vatrozida moraju se pažljivo ocijeniti i testirati na posebnom popisu RFC zahtjeva. Mnoge implementacije IPv6 poprilično su nove, te dovode do dva moguća sigurnosna pitanja. Prvo pitanje je nedostatak alata za procjenu IPv6. Uobičajena praksa u svijetu informacijske sigurnosti je provođenje revizije vlastite mreže s dobro poznatim sigurnosnim alata. Mnogi od popularnih alata su u procesu prijenosa na reviziji IPv6 mreža, tako da je potrebno provjeriti razinu zrelosti alata. Drugi problem je neprovjereni kod u IPv6 implementacijama (za kojega nema alata za testiranje implementacije). Kod koji nije "probijen provalnikom", vjerojatno će imati više sigurnosnih propusta od koda koji se već dugo koristi u proizvodnim okruženjima. Dobavljači moraju paziti na reakcije korisnika i izvještaje o incidentima, kojima se ispravljaju postojeći propusti u implementaciji.

5.4. Problemi s otkrivanjem susjeda

Citirajući citat iz literature RFC 4862 govori: „Ako čvor utvrdi da njegova probna lokalna adresa veze nije jedinstvena, automatski se konfigurira zaustavljanje te je potrebna ručna konfiguracija sučelja.“ To predstavlja mogući napad uskraćivanja usluge jer se može dodijeliti više IPv6 adresa na jedno sučelje. Radnoj stanici moglo bi biti dodijeljeno nekoliko tisuća adresa a drugih radnih stanica te uskratiti mogućnost stjecanja lokalne veze. Ili čak puno jednostavnije, može se izraditi softverski odazivač koji uvijek reagira s "adresom u uporabi".

5.5. Fragmentacija

RFC određuje da čvorovi ne smiju koristiti IPv6 fragmentaciju za slanje bilo kojih od sljedećih poruka u otkrivanju susjeda i sigurnosti susjeda: susjedno traženje, reklamiranje susjeda, traženje usmjerivača, oglašavanje usmjerivača, preusmjeravanje i traženje certifikacije.

5.6. Skeniranje adresa i priključaka

Danas je skeniranje adresa postalo mnogo složenije, nego li je to bilo prije nekoliko godina. Identifikator sučelja u IPv6 ima 64 bita. U RFC 4846, "Zaštita lokalne mreže za IPv6", kaže da „Napadač mora poslati nerealan broj pingova kako bi preslikao mrežu i širenje virusa / crva bit će onemogućeno u tom procesu. S punom brzinom 40 Gbps (400) 100 Mbps LAN-ova, i 13.000 puta više od uobičajene pristupne veze DSL / Cable, potrebno je više od 5000 godina za skeniranje jednog 64-bitnog prostora.“

5.7. Problemi višestrukih (multicast) adresa

IPv6 podržava višestruke adrese, što potencijalno može omogućiti napadaču da prepozna određene važne resurse na web mjestu ako se ono zloporabi. Konkretni primjeri su adrese svih usmjerivača (ff05 :: 2) i sve DHCP-poslužitelje (ff05 :: 1: 3). Napadač može upasti u potencijalnu poruku namijenjenu tim adresama na web mjestu te za uzvrat dobiti informacije o prepoznavanju ključnih resursa na web mjestu. Rizik se može umanjiti osiguravanjem toga da svi vatrozidi i usmjerivači graničnih mjesta su konfigurirani za takvu situaciju.

5.8. Mehanizmi tunela i tranzicije

Ne očekuje se da će IPv4 uskoro izaći iz upotrebe. Vrlo je vjerojatno da će postojati IPv4 čvorovi na mrežama u budućnosti. IPv4 domaćini ne mogu komunicirati s IPv6 domaćinima bez nekakvog mehanizma prijelaza ili tunela, što može dodati složenost na postojeću topologiju mreže i temeljni kod mrežnog skupa. Mehanizmi tunela i tranzicije također se mogu koristiti kao drugačiji način da se pristupi IPv4 mrežama. Općenito, korištenjem tunela mora se osigurati da paketi koji uđu u mrežu kroz tunel ne mogu zaobići dolazne filtre paketa. Napadač s Interneta bi mogao, npr., poslati IPv4 paket do krajnje točke tunela, koji sadrži paket IPv6 s IPv6 izvorom adrese iz vaše interne mreže. Krajnja točka tunela dekapsulira paket i prosljeđuje IPv6 paket u internu mrežu. Prijemnik vjeruje da je ovaj paket potječe od domaćina iz interne mreže.

6. Zaključak

Temeljem iznesenih opisa i pojašnjenja Internet Protokola verzije 4 i Internet Protokola verzije 6 možemo zaključiti završni rad. Internet Protokol verzija 4 jest napravljen 1981. godine, ali se od tada nije promjenio te rast Interneta i potreba za većim brojem IP adresa predstavlja najveći problem tog protokola.

Stvaranje Internet Protokola verzije 6 jest napravljeno u skladu riješavanja nedostataka koje ima Internet Protokol verzija 4, a to su npr. broj raspoloživih adresa, dodjela adresa, životni vijek adresa opseg i tip adresa te još mnogo važnih čimbenika. Osim toga, Internet Protokol verzija 6 ima poboljšane elemente sigurnosti i zaštite.

U budućnosti kad se bude napravio prijelaz, tj. sa Internet Protokola verzije 4 na Internet Protokol verziju 6 svi nedostatci poput pitanja sigurnosti, bolje pohrane podataka i njhove brzine procesiranja će biti uklonjeni.

Zbog navedenih razloga i zaključaka možemo predvidjeti prijelaz u bliskoj budućnosti.

7. Popis literature

7.1. Knjige i radovi:

1. Charles E. Spurgeon, 2000, *Ethernet: The Definitive Guide*, O'Reilly Media
2. Kevin F. Doyle, 2012, *Into the future with IPv4 or IPv6?*
3. Silvia Hagen, 2006, *IPv6 Essentials*, O'Reilly Media

7.2. Internet izvori:

1. http://mreze.layer-x.com/s030100-0.html
2. https://www.internetsociety.org/deploy360/ipv6/security/
3. https://www.ipv6.com/general/ipv6-the-future-of-the-internet/

8. Popis slika

Slika 17. ESP u načinu prijevoza i u tunelima (IPv6 Essentials: Silvia Hagen, (2006.))