



Diplomski studij
Informacijska i
komunikacijska tehnologija:
Telekomunikacije i informatika
Obradba informacija

Komunikacijski protokoli

5.
Mrežni protokol IPv6

Ak.g. 2012./2013.

8.11.2012.

Creative Commons



■ slobodno smijete:

- **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
- **remiksirati** — prerađivati djelo

■ pod sljedećim uvjetima:

- **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
- **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
- **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencem koja je ista ili slična ovoj.

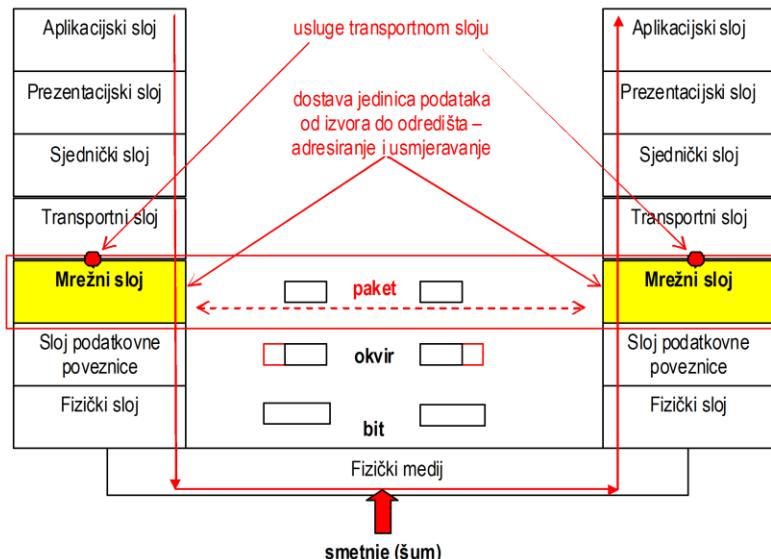
U slučaju daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu.

Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s <http://creativecommons.org/>.

- ◆ Mrežni protokol IPv4 ukratko
- ◆ Glavne značajke protokola IPv6
- ◆ Format datagrama, osnovno i dodatna zaglavlja
- ◆ Adresiranje
- ◆ Upravljački protokoli ICMPv6, NDP, DHCPv6

Mrežni sloj



Podsjetnik:

Smještaj mrežnog sloja u slojevitoj arhitekturi.

Usluge mrežnog sloja



- ◆ osnovna zadaća mrežnog sloja: dostaviti jedinice podataka - pakete od izvorišnog krajnjeg čvora do odredišnog krajnjeg čvora, izravno ili preko niza međučvorova
- ◆ dvije vrste usluge:
 - spojna usluga
 - nespojna usluga ← mrežni sloj u Internetu i IP-mrežama
- ◆ dvije izvedbe usmjeravanja u mrežama s komutacijom paketa:
 - virtualni kanal
 - datagramske ← mrežni sloj u Internetu i IP-mrežama

Podsjetnik:

Definirane su dvije vrste usluga koje mrežni sloj može pružiti sloju transportnom sloju: spojna i nespojna.

Ovisno o vrsti mreže, usluga mrežnog sloja može biti izvedena komutacijom kanala ili komutacijom paketa. Za uslugu izvedenu komutacijom paketa, dva su načina usmjeravanja: virtualnim kanalom i datagramske.

U nastavku naglasak je na nespojnoj usluzi koja je izvedena datagramske, budući da upravo takvu uslugu pruža mrežni sloj u Internetu.

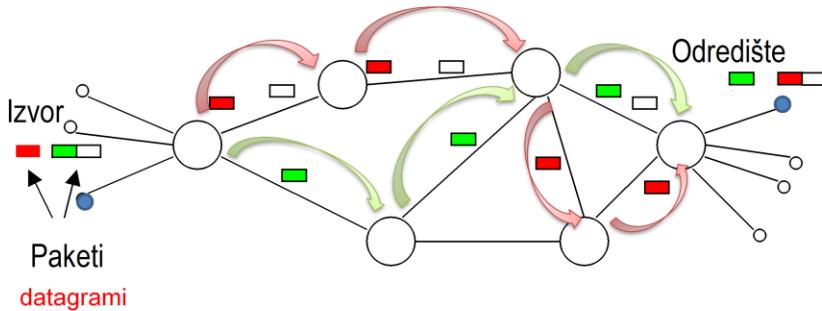
Nespojna usluga izvedena datagramski (1)



Svaki datagram **usmjerava se zasebno** kroz mrežu

Svaki usmjeritelj odluku o usmjeravanju datograma donosi neovisno.

Može se dogoditi da uzastopni datagrami prolaze različitim putovima



Potrebni algoritmi usmjeravanja!

Slika ilustrira nespojnu uslugu izvedenu komutacijom paketa uz datagramskim načinom usmjeravanja.

Internet je mreža koja radi na načelu komutacije paketa u datagramskom načinu rada i u kojoj mrežni sloj transportnom sloju pruža nespojnu uslugu.

Budući da se svaki datagram usmjerava neovisno o ostalima, očito je da mora sadržavati potpunu adresnu informaciju, tj. adrese izvora i odredišta.

Nespojna usluga izvedena datagramske (2)



- ◆ minimalni skup funkcija za dostavu datagrama s kraja na kraj mreže
- ◆ mogući problemi:
 - povremeni gubitak paketa zbog pogreške, smetnji ili kvarova na nekoj od poveznica na putu
 - povremeni gubitak paketa zbog zagušenja u nekom od mrežnih čvorova na putu
 - povremena dostava paketa s narušenim redoslijedom u slučaju kad se izbor puta kroz mrežu promijeni tijekom komunikacije
 - veće kašnjenje u slučaju retransmisije s kraja na kraj mreže
 - pošiljatelj nema povratnu informaciju o ishodu
- ◆ rješavanje ovih problema prepušta se transportnom sloju!

Nespojni način rada relativno brzo rješava osnovni zadatak dostave datagrama s kraja na kraj mreže, ali ništa više od toga. Stoga su navedeni mogući problemi.

Pojašnjenja:

- povremeni gubitak paketa na nekoj od poveznica na putu može se dogoditi zbog neotkrivene pogreške na sloju podatkovne poveznice, smetnji ili kvarova na poveznici.
- povremeni gubitak paketa zbog zagušenja u nekom od mrežnih čvorova na putu može se dogoditi zbog povećanog prometa na tom čvoru. Ako nema kontrole pristupa i kontrole toka, jedini način rukovanja sa "suvišnim" paketima je odbacivanje.
- posljedica promjene puta može izazvati narušen redoslijed paketa na odredištu.
- kašnjenje u slučaju retransmisije s kraja na kraj je bitno veće od onog na sloju poveznice, gdje je retransmisija samo od točke do točke na izravnoj vezi.

4 Aplikacijski sloj (*Application Layer*)

3 Transportni sloj (*Transport Layer*)

2 Mrežni sloj, internetski sloj (*Network Layer, Internet Layer*)

1 nije definiran → sloj podatkovne poveznice i fizički sloj
upotrijebljene mreže (pristup mreži)

IP

Podsjetnik:

Osnovni mrežni protokol u Internetu je *Internet Protocol (IP)*.

Odlike protokola IP

Internet Protocol (IP) verzija IPv4 (RFC 791, STD-5)

◆ Glavne odlike:

- neovisan o nižim protokolima (Ethernet, IEEE 802.3, PPP, ...)
- datagramski način rada
- nespojna usluga bez potvrde
- nema mehanizama kontrole toka
- nema jamstva očuvanja redoslijeda datagrama

usluga IP-a
transportnom sloju:
nepouzdana dostava
datagrama

◆ Uloga u protokolnom složaju TCP/IP:

- ◆ **omatanje** (engl. *encapsulation*): IP prihvata podatke od višeg sloja (npr. transportnog protokola TCP, UDP), smješta ih u podatkovno polje IP datagrama te predaje datagram protokolu sloja podatkovne poveznice (npr. Ethernet)

Protokol IP pruža *datagramsку*, odnosno nespojnu (*connectionless*) mrežnu uslugu. Mrežna povezanost temelji se na načelu komutacije paketa, pri čemu se paketski čvorovi u Internetu nazivaju *usmjeriteljima (router)*. Glavni zadatak usmjeritelja je "prebacivanje" IP datagrama sljedećem usmjeritelju na putu prema odredištu, što uključuje odabir sljedećeg usmjeritelja i odlaznog sučelja po kojem će se datagram prosljediti.

Specifikacije:

IP Internet Protocol (RFC [791](#))

ICMP Internet Control Message Protocol (RFC [792](#))

Broadcasting Internet Datagrams (RFC [919](#))

Broadcasting Internet datagrams in the presence of subnets (RFC [922](#))

Internet Standard Subnetting Procedure (RFC [950](#))

IGMP Host extensions for IP multicasting (RFC [1112](#))

Funkcionalnost protokola IP



◆ definira **shemu adresiranja** u Internetu

- jedinstveni adresni prostor
- svako krajnje računalo ima po jednu IP-adresu za svako mrežno sučelje
- svako krajnje računalo može koristiti i više posebnih adresa (npr., adrese *localhost*, *multicast*, *broadcast*, ...)
- ako su izvorišna i odredišna adresa u različitim mrežama, datagrami se usmjeravaju preko jednog ili više IP-usmjeritelja

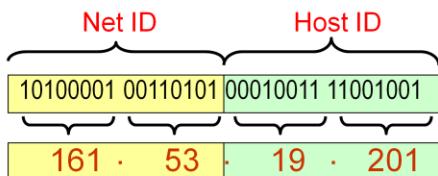
◆ definira provedbu **fragmentacije**

- datagram mora "stati" u podatkovno polje okvira sloja podatkovne poveznice
- datagram veći od podatkovnog polja okvira mora se fragmentirati
- na strani primatelja fragmenti se sastavljuju

IP-adresiranje



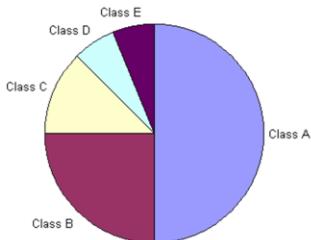
- IP-adresa **32 bita** (IPv4): identifikator koji globalno i jednoznačno određuje mrežno sučelje
- krajnji sustav (npr. računalo priključeno na mrežu) obično ima jedno sučelje i jednu IP-adresu
 - mrežni čvor (npr. usmjeritelj) priključen na više (pod)mreža ima više sučelja i isto toliko IP-adresa
 - IP-adresa ima dva dijela:
 - identifikator mreže (engl. *Network Identifier*, Net ID)
 - identifikator krajnjeg računala (engl. *Host Identifier*, Host ID)



Klase i rasponi IP-adresa



Klasa:	01	7 8	16	31	
A	0	NetID	HostID		0.0.0.0 – 127.255.255.255
B	10	NetID	HostID		128.0.0.0 – 191.255.255.255
C	110	NetID	HostID		192.0.0.0 – 223.255.255.255
D	1110	višeodredišna adresa			224.0.0.0 – 239.255.255.255
E	1111	rezervirano			240.0.0.0 – 247.255.255.255



Odabrane IP-adrese i blokovi IP-adresa rezervirani i zauzeti za posebne namjene!

Dodjela adresa na razini globalnog Interneta: ICANN (*Internet Corporation for Assigned Names and Numbers*)

- upravljanje dodjelom blokova adresa i DNS sustavom
- dodjela adresa se delegira RIR-ovima (*Regional Internet Registry*): APNIC, ARIN, LACNIC, RIPE NCC (za Europu), AFRINIC
- RIR-ovi delegiraju odgovornost nacionalnim (NIR) i lokalnim (LIR) registrima, u Hrvatskoj – CARNet
- u konačnici se blokovi adresa daju ISP-ovima, koji ih dodjeljuju korisnicima ili nižim ISP-ovima

Primjeri rezerviranih i zauzetih adresa

◆ Povratna adresa (engl. *loopback*)

- virtualno mrežno sučelje, adresa "ovo računalo"
- IP datagrami poslani na povratnu adresu se ne predaju na daljnji prijenos sloju podatkovne poveznice, već se "vraćaju natrag" unutar mrežnog sloja
- adrese 127.0.0.0 - 127.255.255.255 (127.0.0.0/8), najčešće 127.0.0.1
- koristi se za testiranje izvedbe TCP/IP-a na računalu

◆ Razašiljanje svima (engl. *broadcast*)

- adresa "svima" 255.255.255.255
- sva sučelja prihvataju takve datagrame (samo u lokalnoj mreži!)

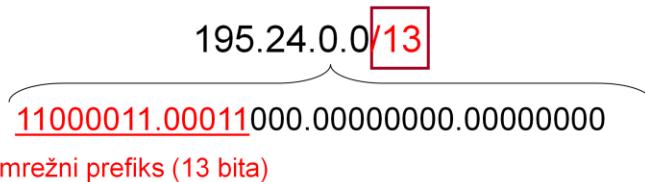
◆ Identifikacija vlastite mreže

- adresa "ova mreža", raspon 0.0.0.0/8.

Prefiksni prikaz adrese i besklasno adresiranje



- ◆ prefiksni prikaz IP-adrese ne uzima u obzir izvorne klase A, B i C
- ◆ dioba između mrežnog i računalnog dijela adrese može biti na bilo kojem mjestu unutar adrese (ne samo na granici okteta kao kod klasa!)
- ◆ duljina mrežnog dijela se označava mrežnim prefiksom iza adrese



- ◆ besklasno usmjeravanje – *Classless Inter-Domain Routing (CIDR)*
 - ◆ putevi usmjeravanja više se ne agregiraju prema klasama adresa, već prema mrežnom prefiksu

Važna napomena:

- danas se koristi načelo usmjeravanja CIDR (*Classless Inter-Domain Routing*)

RFC 4632

Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan

Aug 2006

Format IP-zaglavlja



Komunikacijski protokoli

8.11.2012.

15 od 66

Polja u zaglavju IP datagrama:

verzija: inačica IP-a (IPv4),

IHL, duljina zaglavlja: broj 32-bitnih riječi (od 5 do 15),

TOS, vrsta usluge: oznaka kvalitete usluge tražene za datagram,

duljina: broj okteta u datagramu, uključujući zaglavlje (najviše 65535),

identifikacija: jedinstveni broj datagrama, isti za sve fragmente,

zastavice: 3 bita rezervirana za oznake vezane uz fragmentiranje,

mjesto fragmenta: ako se radi o fragmentu, oznaka za izračunavanje njegovog smještaja u fragmentiranom datagramu,

TTL: najveći dopušteni broj usmjeritelja kroz koje datagram može proći prije nego što bude odbačen (na svakom usmjeritelju TTL se umanjuje za jedan),

protokol: oznaka protokola višeg sloja čije podatke IP nosi (npr. TCP, UDP),

zaštitna suma zaglavlja: zaštitni kôd za otkrivanje pogrešaka u zaglavlju,

izvorišna IP adresa: IP adresa sučelja s koje se odašilje datagram,

odredišna adresa: IP adresa sučelja na koju se šalje datagram,

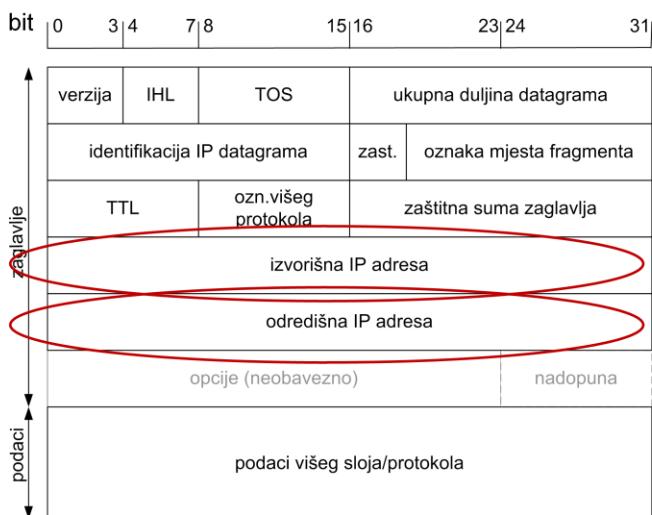
opcije: posebne izborne mogućnosti, npr. za izvorno određivanje puta i sigurnost,

punjjenje: popunjavanje zaglavlja nulama do višekratnika od 32 bita.

IP-zaglavljje: polja vezana uz omatanje



IP-zaglavljje: polja vezana uz adresiranje



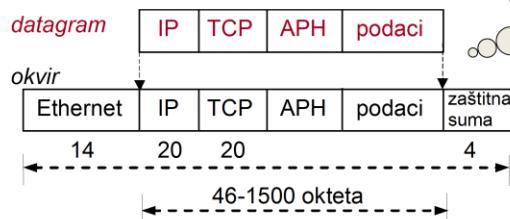
Fragmentacija



- ◆ datagram mora stati u podatkovno polje okvira sloja podatkovne poveznice

■ **MTU (Maximum Transmission Unit)**

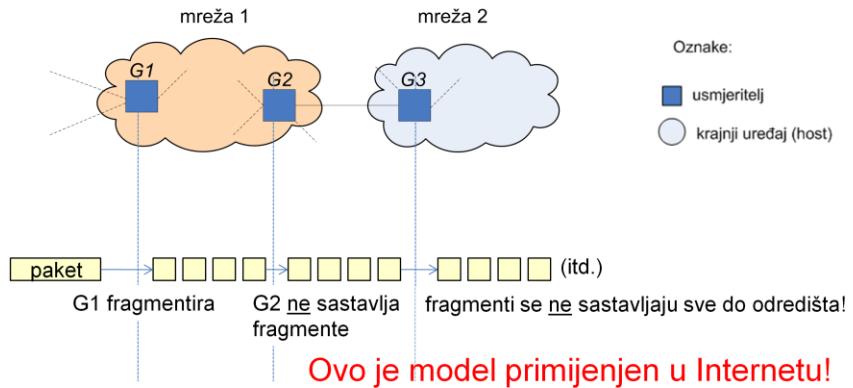
primjer: Ethernet/IEEE 802.3: MTU=1500 okteta



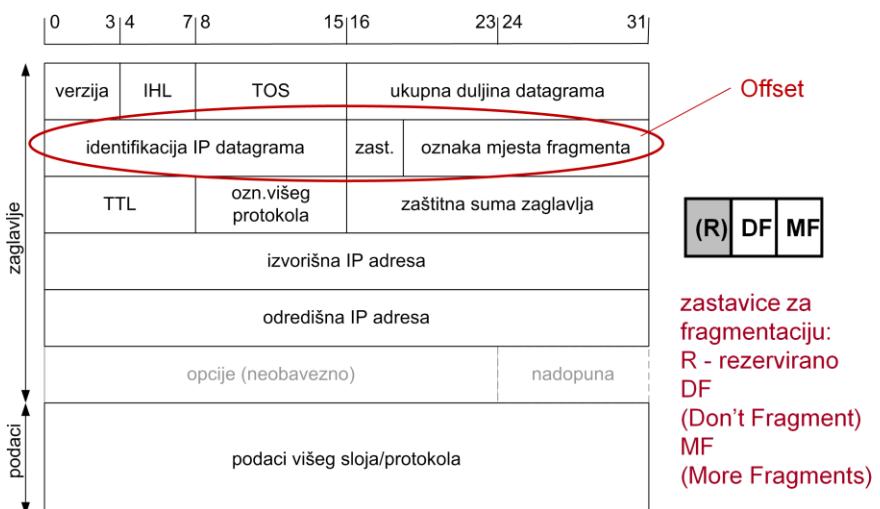
- ◆ datagram veći od MTU, mora se podijeliti na dijelove odgovarajuće veličine – **fragmente** (tko i gdje?)

Netransparentna fragmentacija

- ◆ tko: **usmjeritelj**
- ◆ gdje: fragmenti se šalju u novim, međusobno neovisnim datagramima s usmjeritelja **na izvorštu** i sastavljaju u originalni datagram **na odredištu**



IP-zaglavljje: polja vezana uz fragmentaciju



Primjer fragmentacije



IP datagram zaglavlje 20 okteta	<table border="1"><tr><td>MF</td><td>Offset</td></tr><tr><td>0</td><td>0</td></tr></table>	MF	Offset	0	0	PODACI = 1480 okteta (1460 + TCP-zaglavlje)		
MF	Offset							
0	0							
IP datagram fragment 1	<table border="1"><tr><td>MF</td><td>Offset</td></tr><tr><td>1</td><td>0</td></tr></table>	MF	Offset	1	0	PODACI okteti 1-552		
MF	Offset							
1	0							
IP datagram fragment 2	<table border="1"><tr><td>MF</td><td>Offset</td></tr><tr><td>1</td><td>552</td></tr></table>	MF	Offset	1	552	PODACI okteti 553-1104		
MF	Offset							
1	552							
MTU=572	IP datagram fragment 3	<table border="1"><tr><td>MF</td><td>Offset</td></tr><tr><td>0</td><td>1104</td></tr></table> <table border="1"><tr><td>PODACI</td></tr><tr><td>1105-1480</td></tr></table>	MF	Offset	0	1104	PODACI	1105-1480
MF	Offset							
0	1104							
PODACI								
1105-1480								

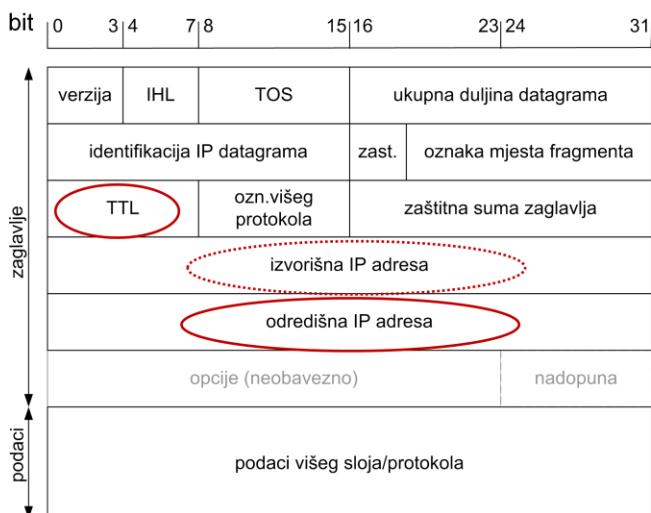
Zašto je fragmentacija nepoželjna:

- ◆ u slučaju gubitka fragmenta, cijeli datagram je uništen
- ◆ prenosi se više kontrolnih podataka, a za istu korisnu informaciju

Postupak pronalaženja puta i proslijedivanja paketa od izvorišnog do odredišnog čvora, izravno ili preko niza usmjeritelja i podmreža, na temelju odredišne IP-adrese:

- ◆ slučaj 1: ako su izvorišni i odredišni čvor u istoj podmreži s dijeljenim medijem, tada komuniciraju izravno,
ili
- ◆ slučaj 2: ako su izvorišni i odredišni čvor u različitim (pod)mrežama, tada komuniciraju preko jednog ili više usmjeritelja.

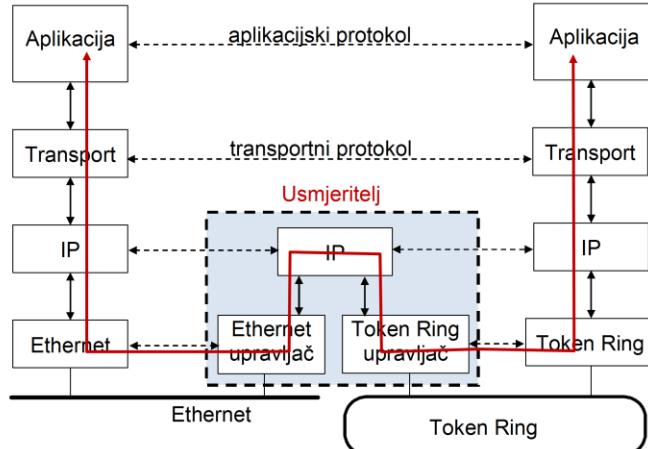
IP zaglavljje: polja vezana uz usmjeravanje



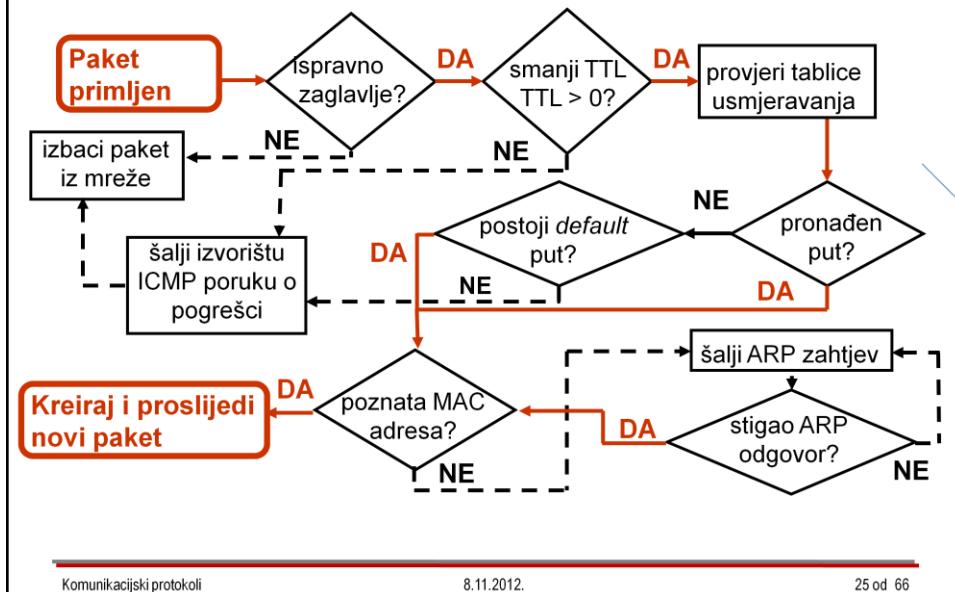
Usmjeravanje paketa preko usmjeritelja



Primjer: Izvorišni i odredišni čvor u lokalnim mrežama različite izvedbe (Ethernet, Token Ring)



Proces usmjeravanja paketa



Slika prikazuje **proces usmjeravanja paketa**, odnosno što se događa s paketom kada ga primi usmjeritelj.

Dakle, kada usmjeritelj primi paket, proces usmjeravanja paketa prvo ispituje je li zaglavje ispravno, provjeravajući zaštitnu sumu zaglavja. U slučaju da je zaglavje neispravno, paket se briše i time "izbacuje iz mreže".

U protivnom smanjuje TTL polje za jedan i provjerava je li TTL = 0. Ako jest, izbacuje paket iz mreže i šalje ICMP poruku izvorištu kojom ga obavještava da je došlo do greške. Inače provjerava tablicu usmjeravanja da vidi kojim putem treba usmjeriti paket.

Ako je u tablici pronađen odgovarajući put, datagram se usmjerava po njemu. Ako u tablici nema odgovarajućeg unosa za zadani adresu, datagram se usmjerava na unaprijed određeni (*default*) put. Unos u tablici usmjeravanja sadrži adresu sljedećeg skoka (IP adresu sučelja prema kojem treba usmjeriti paket) i odlazno sučelje prema toj adresi.

Proces prosljeđivanja datagrama na odlazno sučelje zapravo je priprema za "spuštanje" datagrama u okvir protokola sloja podatkovne poveznice.

Da bi se formirao okvir, tj. odredišna adresa okvira, potrebno je, na temelju IP adrese saznati MAC adresu sučelja koja odgovara IP adresi odredišta. Ako ta MAC adresa nije poznata, računalo šalje ARP zahtjev za MAC adresom tako dugo dok ne dobije odgovor.

Kada dobije odgovarajuću MAC adresu, računalo prosljeđuje paket i u tom trenutku je proces usmjeravanja paketa završio.

Usmjeritelj je sada spremjan prihvati novi paket iz ulaznog spremnika i ponoviti proces usmjeravanja.

ICMP služi za "dijagnostiku"

- ◆ podsjetimo: IP je jednostavan protokol koji nema mogućnost dojave pogreške – to za njega radi ICMP
- ◆ ICMP definira mehanizam kojim se prenose dvije vrste kontrolnih poruka
 1. dojave o pogrešci – povratna informacija pošiljatelju o nekom problemu u mreži
 2. zahtjevi za informacijom – traži se informacija vezana za stanje u mreži
- ◆ ICMP ne otklanja problem niti djeluje na temelju tih poruka, samo javlja stanje
- ◆ ICMP je proširiv - i drugi internetski protokoli osim IP-a mogu definirati svoje kontrolne poruke

0792 Internet Control Message Protocol. J. Postel. September 1981. (Format: TXT=30404 bytes) (Obsoletes RFC0777) (Updated by RFC0950) (Also STD0005) (Status: STANDARD)

Internet Protocol Version 6, IPv6 (RFC 2460)

- ◆ naziva se i IPng (*next generation*)
- ◆ zadržava dobra svojstva prethodne verzije IP-a (IPv4), a ispravlja nedostatke i unosi poboljšanja:
 - veći adresni prostor omogućuje globalnu umreženost i dostupnost svih čvorova, bez "skrivenih" mreža i računala
 - učinkovitije usmjeravanje
 - nove mogućnosti

◆ ograničenja IPv4:

- broj raspoloživih adresa postao premalen (**32 bitne adrese**)
- prevelike tablice usmjeravanja
- problemi upravljanja mrežom
- nedovoljni **sigurnosni mehanizmi** na mrežnom sloju
- nedovoljni **mehanizmi pokretljivosti** na mrežnom sloju
- slaba potpora za prijenos podataka u stvarnom vremenu – **kvaliteta usluge (QoS)**

Sadašnja verzija Internet protokola (IPv4) postaje ograničavajuća, s obzirom da su se pojavili novi zahtjevi, nove aplikacije i usluge veće složenosti. Osim toga, svakim danom pojavljuju se novi korisnici koji žele pristup Internetu, tako da adresni prostor postaje premalen. Uz to, protokolu IPv4 nedostaju određene funkcije i nema dovoljno sigurnosnih mjera i zaštite podataka.

S promjenom prirode mreže Internet, koja postaje sve više poslovna mreža, IPv4 neće zadovoljavati nove zahtjeve. U početku se TCP/IP brinuo za jednostavnu distribuciju aplikacija poput prijenosa datoteka, elektroničke pošte i rada na udaljenom računalu. Međutim Internet je postao i više od toga, multimedija i hipermedija, okolina bogata aplikacijama i uslugama. Uz to veća je potreba za **komunikaciju s više krajnjih točaka** (IP multicast, Mbone) i zahtjevne **višekorisničke i višemedijske aplikacije** (višemedijska konferencija interaktivne višemedijske aplikacije, WWW, strujanje višemedijskih podataka, IP telefonija).

◆ novosti u IPv6:

- veći adresni prostor (**128 bitne adrese**)
- pojednostavljenje formata zaglavlja (**manje polja, fiksna duljina**)
- unaprjeđeno usmjeravanje
- mogućnost označavanja tokova (označavanje paketa koji pripadaju istom toku)
- podrška za kvalitetu usluge, QoS (prijenos u stvarnom vremenu)
- provjera autentičnosti i zaštita privatnosti, integritet podataka, povjerljivost
- bolja potpora za pokretljivost

Tijekom uporabe IPv4 protokola ustanovljena je potreba za boljim rješenjima, tako da nova inačica IPv6 unosi neke novosti.

Kako bi se mogao adresirati veći broj računala, IPv6 koristi **128-bitno** adresiranje umjesto 32-bitnog. Zatim, osnovno zaglavje paketa novog protokola je smanjeno po broju polja i sad ima **fiksnu duljinu od 40 okteta**. Time je omogućena brža obrada paketa u usmjeriteljima, a dodana su posebna proširena zaglavla kako bi se unaprijedilo usmjeravanje.

Uvedeni su zahtjevi na kvalitetu usluge (*Quality of Service*) koji posebno dolaze do izražaja kod prijenosa podataka u stvarnom vremenu. Fragmentacija se može vršiti **isključivo** na izvorišnom čvoru. Zatim, postoji mogućnost **označavanja tokova** paketa. Što se tiče sigurnosti, razvijena su dva mehanizma zaštite: **mehanizam provjere autentičnosti (authentication)** i **mehanizam zaštite privatnosti (privacy)**. Izbačeno je izračunavanje zaštitne sume zaglavlja.

Usporedba zaglavja IPv4 i IPv6

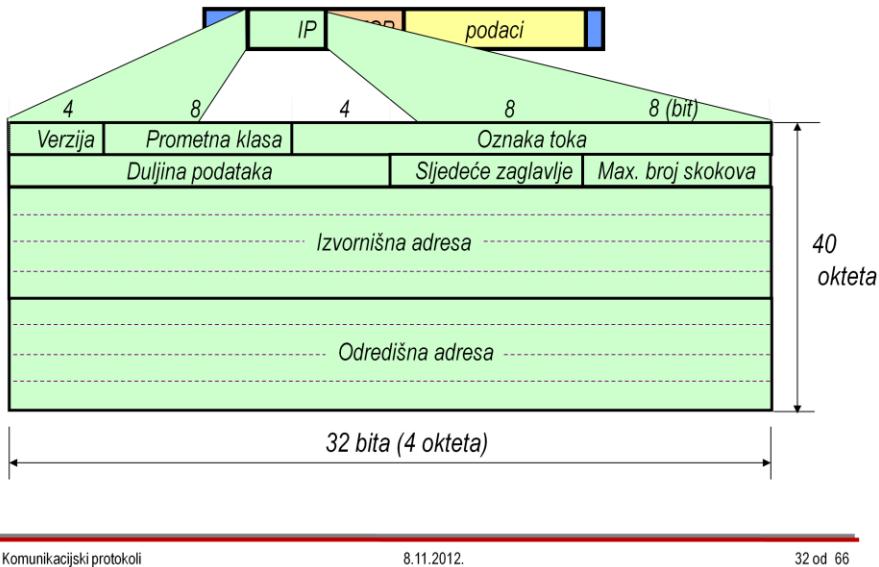


0	8	16	24	31
version	IHL	TOS	total length	
	identification		flags	fragment offset
	TTL	protocol		header checksum
			source IP address	
			destination IP address	
		options		padding

Izbačeno!

0	5	8	12	16	24	31
version		class		flow label		
			payload length		next header	hop limit
IP source address (128 bits)						
IP destination address (128 bits)						

Zaglavje IPv6



Verzija (*version*) označava protokol, tj. IPv6.

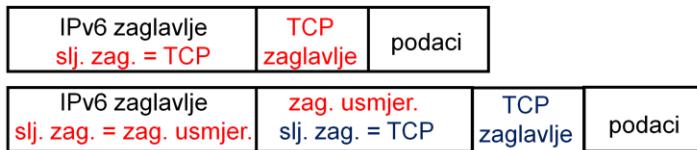
Prometna klasa (*class*) određuju rukovanje paketima ovisno o stanju mreže, tj. zagušenju. Razlikuju se dvije prometne klase: promet upravljan zagušenjem (*congestion controlled traffic*) i promet neupravljan zagušenjem (*non-congestion controlled traffic*), unutar kojih su definirani prioriteti za pojedine vrste informacijskog prometa. Promet upravljan zagušenjem je onaj za koji izvorište provodi kontrolu zagušenja. U toj klasi najviši prioritet ima upravljački promet (npr. protokoli usmjeravanja), zatim interaktivni promet (npr. korisnički upit – odgovor), pa prijenos velike količine podataka (npr. FTP, HTTP) itd. Promet neupravljan zagušenjem je onaj kod kojeg su poželjni stalna ili približno ista brzina prijenosa i kašnjenje (npr. video, audio).

Oznaka toka (*flow label*) određuje niz paketa iz nekog izvorišta namijenjenih nekom odredištu koji pripadaju istoj usluzi ili aplikaciji, a za koji se zahtijeva posebno rukovanje u usmjeriteljima (npr. rezervacija resursa).

Dodatna zaglavlj



- ◆ korištenje posebnih opcija u IPv4 usporava proslijđivanje paketa u usmjeriteljima
- ◆ u IPv6 dodaju se iza osnovnog zaglavlja dodatna zaglavlj po potrebi



Nakon osnovnog zaglavlja koje je fiksne duljine od 40 okteta, u IPv6 je moguće nizati proizvoljan broj dodatnih zaglavlj, koja nisu obvezna, a to su:

- zaglavlje skok po skok (*hop-by-hop header*),
- zaglavlje usmjeravanja (*routing header*),
- zaglavlje fragmenta (*fragment header*),
- zaglavlje za provjeru autentičnosti (*authentication header*),
- zaglavlje za sigurnosno ovijanje podataka(*encapsulating security payload*).
- zaglavlje namijenjeno odredištu (*destination header*),

Nakon dodatnih zaglavlj (svih ili nekih) dolazi zaglavlje transportnog sloja (TCP ili UDP) i zatim podaci.

Poredak dodatnih zaglavlja



IPv6 datagram:

1. Zaglavljje IPv6
2. Zaglavljje skok po skok
3. Zaglavljje namijenjeno odredištu (1)
4. Zaglavljje usmjeravanja
5. Zaglavljje fragmenta
6. Zaglavljje za provjeru autentičnosti
7. Zaglavljje za sigurnostno ovijanje podataka
8. Zaglavljje namijenjeno odredištu (2)
- Zaglavljje transportnog sloja (TCP, UDP)

Samo zaglavljje IPv6 je obvezno!

Zaglavlj skok po skok

Hop-by-Hop Header

- ◆ zaglavlj varijabilne duljine koje sadrži informaciju namijenjenu svakom čvoru na putu dostave datagrama
- ◆ sadrži podatke o sljedećem zaglavlj, veličini samog zaglavlja i polje s jednom ili više definicija akcije koju poduzima čvor
- ◆ primjer primjene:
 - prijenos vrlo velikih paketa $> 2^{16}$ okteta ("jumbo payload") na putu s velikim MTU (npr. video)
 - polje "duljina podataka" u IPv6 zaglavlj = 0
 - ne primjenjuje se fragmentacija

Destination Header (1), (2)

- ◆ zaglavlja varijabilne duljine koje sadrži dodatnu informaciju:
 - (1) za prvi sljedeći čvor i sve čvorove koje sadrži *Routing Header*,
a koji se smatraju odredištim
■ (2) samo za krajnje odredište
- ◆ sadrži podatke o sljedećem zaglavljvu, veličini samog zaglavlja i polje s jednom ili više definicija akcije koju poduzima čvor - odredište
- ◆ primjer primjene:
 - Mobile IPv6

Routing Header

- ◆ zaglavje varijabilne duljine koje sadrži popis usmjeritelja kojima datagram treba proći na putu od izvorišta do odredišta
- ◆ sadrži podatke o sljedećem zaglavljtu, veličini samog zaglavlja, vrsti usmjeravanja i popis čvorova koje paket još treba prijeći prije nego što dođe do odredišta
- ◆ primjer primjene:
 - Mobile IPv6

Fragment Header

- ◆ zaglavje fiksne duljine koje se primjenjuje za slanje datagrama većih od MTU-a puta
 - IPv6 propisuje minimalni MTU od 1280 okteta
- ◆ sadrži podatke o sljedećem zaglavljtu, polja koje pokazuju kojem dijelu originalnog paketa pripada određeni fragment, bita koji označava ima li još segmenata (bit = 1) ili je riječ o zadnjem segmentu (bit = 0) i identifikacijskog polja koje sadrži adrese izvorišta i odredišta
- ◆ **datagrami se mogu fragmentirati samo na izvorištu**, a ukoliko se pojavi potreba za fragmentacijom na nekom usmjeritelju, takav se datagram odbacuje i šalje ICMPv6 poruka izvorištu (datagram prevelik).

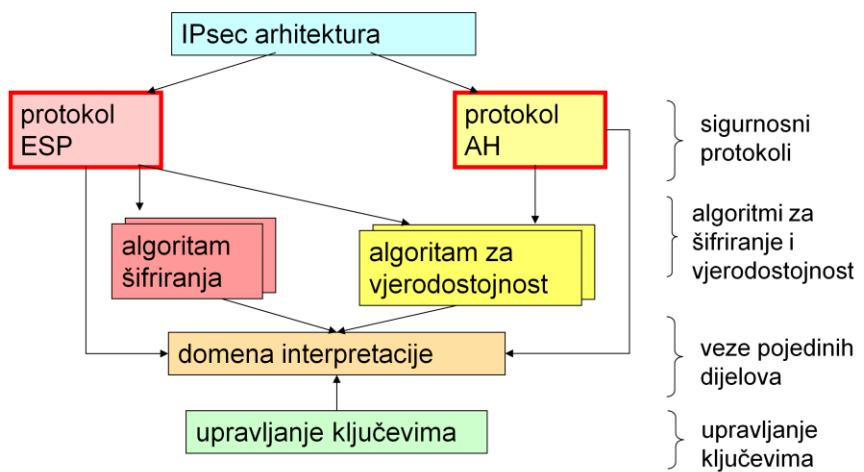
Internet Protocol Security (IPsec)

- ◆ sigurnosna opcija za IPv4
- ◆ sastavni dio IPv6: dodatna zaglavlja AH i ESP
- ◆ sigurnosna arhitektura
 - sigurnosni protokoli
 - kriptografski algoritmi za šifriranje i vjerodostojnost
 - procedure i protokoli za upravljanje kriptografskim ključevima
- ◆ primjena postupaka kojima se postiže:
 - autentičnost pošiljatelja datagrama (izvorišna IP adresa)
 - integritet datagrama (nepromijenjen tijekom prijenosa)
 - povjerljivost/tajnost cijelog datagrama ili samo polja podataka

Specifikacije:

<http://www.ietf.org/html.charters/ipsec-charter.html>

Sigurnosna internetska arhitektura



Izvor: RFC 2411 IP Security Document Roadmap

Authentication Header (AH)

- ◆ specifikacija u RFC 4302
- ◆ jamstvo da je primljeni datagram odaslan s izvorišne IP adrese :
 - autentičnost izvorišta IP datagrama,
 - integritet podataka – datagram nije mijenjan tijekom prijenosa

Primjena AH zaglavlja



- ◆ siguran identitet pošiljatelja
- ◆ sigurno je da podaci nisu mijenjana pri prolasku kroz mrežu
- ◆ može se primijeniti u kombinaciji s ostalim zaglavljima, npr.:



Da li su podaci koji se šalju s izvorišta čitljivi? Da li očuvana privatnost komunikacije?

Zaglavljem za provjeru autentičnosti ovijaju se podaci namijenjeni odredištu.

Treba napomenuti da AH zaglavje ne služi za povjerljivost/tajnost podataka. Ono samo jamči identitet pošiljatelja te da poruka nije mijenjana, međutim, svi su podaci i dalje čitljivi na razini paketa. Da bi se zaštitila tajnost podataka, mora se koristiti ESP zaglavlje.

Encapsulating Security Payload Header (ESP)

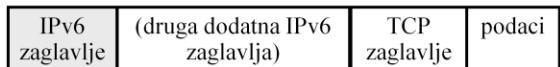
- ◆ specifikacija u RFC 4303
- ◆ šifriranjem osigurava povjerljivost/tajnost i integritet datagrama
 - jamči povjerljivost podataka tj. da podaci nisu bili čitani
 - jamči integritet podataka tj. da podaci nisu bili mijenjani
- ◆ dva načina rada:
 - transportni način ESP (*transport-mode* ESP): zaštita polja podataka u kojem je TCP/UDP paket
 - tunelski način ESP (*tunel-mode* ESP): zaštita cijelog datagrama

Sigurnosno ovijanje podataka ostvaruje se ESP zaglavljem (*Encapsulating Security Payload*) koje osigurava privatnost podataka i integritet datagrama. Ovisno o zahtjevima korisnika, mehanizam zaštite (šifriranje i dešifriranje) se može provesti nad podacima transportnog sloja pod nazivom *transport-mode* ESP ili nad cijelim paketom pod nazivom *tunel-mode* ESP.

Prijenos podataka se vrši na sljedeći način: na izvođačkoj strani formiraju se paketi-datagrami koji se sastoje od šifriranog i nešifriranog dijela. Paketi se usmjeravaju do odredišta i svaki usmjeritelj na putu ispituje osnovno IP zaglavje i dodatna zaglavja koja nisu šifrirana. Na odredišnoj strani provodi se dešifriranje na temelju ESP zaglavja, tako da samo legitimni pošiljatelj može pročitati podatke.

Tunelski način ESP se koristi za šifriranje cijelog datagrama. Ovim načinom ESP zaglavje je dodano na početku paketa i tada se paket šifrira. Budući da su tako šifrirani IP zaglavje i dodatna zaglavja, potrebno je formirati novo IP zaglavje kako bi usmjeritelji mogli procesirati takav datagram.

Primjena ESP zaglavlja – transportni način



posljednje zaglavje koje je čitljivo
usmjeriteljima



↔
šifrirano

Kako bi izgledao datagram pri tunelskom načinu rada ESP?
Kako postići i autentičnost i tajnost podataka?

ESP zaglavlje osigurava tajnost podataka i, ovisno o algoritmu, dodatne razine zaštite. Nakon ESP zaglavlja slijede šifrirani podaci, pri čemu sam format tih podataka ovisi o odabranom algoritmu šifriranja.

ESP i AH zaglavlja se mogu kombinirati .

Adresni prostor

- ◆ adresnu arhitekturu IPv6 protokola opisuje RFC 4291
- ◆ umjesto 32 bita koristi se **128 bitova**
 - IPv4: 4 294 967 296 računala
 - IPv6: 340 282 366 920 938 463 463 374 607 431 768 211 456 čvorova
- ◆ obilježja adresnog prostora IPv6:
 - 655 570 793 348 866 943 898 599 adresa za 1 m² površine Zemlje
 - omogućuje stvaranje domena koje odražavaju topologiju Interneta danas, jer 128 bita dozvoljava višestruke razine hijerarhije i fleksibilnost
 - učinkovitije usmjeravanje, jer je omogućeno združivanje (agregacija) adresa u hijerarhije mreža, davatelja usluga, korporacija, zemljopisnih područja i druge

Zapis adresa (1)

- ◆ notacija: 8 grupa po 4 heksadekadske znamenke:
npr: EFD1:0989:AB02:7654:C4ED:890B:DE65:1240
- ◆ adrese v4 mogu se pretvarati u v6 umetanjem nula:
npr: 161.53.19.201 (hex: A135:13C9) postaje
0000:0000:0000:0000:0000:A135:13C9
- ◆ mogući načini zapisa: ::161.53.19.201 ili ::A135:13C9
- ◆ IPv6 adrese imaju mrežni i računalni dio

IPv6 adresa sastoji se od 128 bita, koja se zapisuju kao skupina 16-bitnih brojeva odvojenih dvotočkama. Svaki broj pisan je u heksadekadskoj notaciji. Kako bi se olakšalo pisanje takvih adresa, uvodi se mogućnost kraćenja adresa, zamjenom niza "0" znakom :: (dvije dvotočke), što će biti čest slučaj kad će se sadašnje 32-bitne adrese pretvarati u 128-bitne. Pri tome se znakom :: može zamijeniti isključivo jedan niz "0", kako bi se adresa mogla jednoznačno interpretirati.

Stare IP adrese verzije 4 pretvarat će se u IPv6 adresu dodavanjem niza od 96 "0" ispred adrese, dok će zadnja 32 bita moći ostati u dekadskom ili heksadekadskom obliku. Nakon kraćenja niza "0" znakom ::, adrese će ostati u obliku ::161.53.19.201 ili ::A135:13C9.

Kao i kod IPv4 adresa, postoji podjela na mrežni dio adrese i računalni dio adrese, koji se koristi kod usmjeravanja paketa. Primjerice, notacija FEDC:BA98:7600::40 definira adrese gdje je mrežni dio FEDC:BA98:76 (prvih 40 bitova – binarno 1111 1110 1101 1100 1011 1010 1001 1000 0111 0110).

Zapis adresa (2)

◆ sažimanje okteta :00: → ::

- 1080:0:0:0:0:8:800:200C → 1080::8:800:200C
- FF01:0:0:0:0:0:101 → FF01::101
- 0:0:0:0:0:0:1 → ::1
- 0:0:0:0:0:0:0 → ::

■ nije dobro:

- 1080:0:0:8:800:0:0:200C → 1080::8:800::200C

◆ kombinacija heksadekadskog i dekadskog:

- 0:0:0:0:0:161.53.19.201 → ::161.53.19.201

◆ prefiks: ip-adresa/prefix

- npr: 12AB:0:0:CD30::/60

Znak :: zamjenjuje niz bitova vrijednosti "0".

Važno je primijetiti da se znakom :: ne može zamijeniti dio adrese :0:0 u adresi u kojoj se već upotrijebilo znak ::.

Primjer:

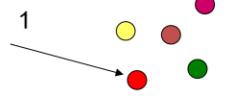
Kad bi se u adresi 12AB:0:0:CD30::/60 zamijenilo ":0:0" s "::", adresa bi se zapisala u obliku 12AB::CD30::/60. Vraćanjem niza "0" dobila bi se adresa 12AB:0:0:0:0:0:CD30/60, u kojoj je prvih 64 bita 12AB:0:0:0, a ne 12AB:0:0:CD30, kao u početno zapisanoj adresi.

Vrste IPv6 adresa (1)



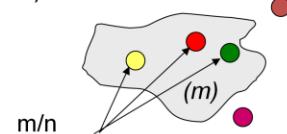
◆ *Unicast* – jednoodredišna adresa

- identificira jedno sučelje računala/čvora
- globalne i lokalne adrese
- posebne adrese (*loopback*, nespecificirane, ...)



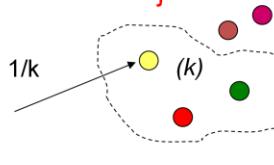
◆ *Multicast* – višeodredišna adresa

- određuje skup sučelja
(obično na različitim čvorovima)
- paket se dostavlja svima sučeljima određenim tom adresom



◆ *Anycast* – adresa više sučelja, dostava jednom sučelju

- paket se dostavlja se samo jednom
(najbližem) sučelju s definiranom adresom



Kao i kod IPv4, IP adrese identificiraju sučelje čvora prema mreži. IPv6 adrese dijele se u tri skupine:

- **Unicast** adrese definiraju jedno sučelje. Paket poslan na *unicast* adresu, bit će dostavljen samo sučelju kojem je dodijeljena ta IP adresa
- **Multicast** adrese identificiraju skupinu sučelja (čvorova). Paket poslan na *multicast* adresu bit će dostavljen na sva sučelja u skupini.
- **Anycast** adrese također definiraju skupinu sučelja, no, paket poslan na *anycast* adresu bit će dostavljen samo jednom, najčešće najbližem članu grupe. Ta mogućnost ne postoji u IPv4

Postoji više vrsta unicast adresa:

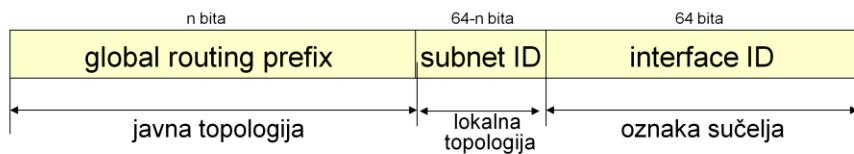
- **globalne adrese** koje se koriste za adresiranje u javnom Internetu
- **lokalne adrese na razini organizacije** koriste se kod organizacija koje nisu fizički spojene na Internet, a koriste TCP/IP skup protokola
- **lokalne adrese na razini podatkovne poveznice** se izvode iz MAC adrese, dodavanjem prefiksa FE80::
- **posebne adrese** koje se mogu koristiti za različite namjene

Vrste IPv6 adresa (2)

Vrsta adrese	Binarni prefiks	IPv6 prefiksna notacija
Nespecificirana (<i>unspecified</i>)*	00...0 (128 bita)	::/128
Povratna (<i>loopback</i>)*	00...1 (128 bita)	::1/128
Višeodredišna (<i>multicast</i>)	11111111	FF00::/8
Lokalna jednoodredišna na poveznici (<i>Link-Local Unicast</i>)	1111111010	FE80::/10
Globalna jednoodredišna (<i>Global Unicast</i>)	(sve ostalo)	
Anycast	iz jednoodredišnog raspona	

*posebne (rezervirane) adrese

Globalne unicast adrese



001 - FP (*Format prefix*)

globalni prefiks usmjeravanja (*global routing prefix*) – identifikator organizacije

identifikator podmreže (*subnet ID*) – identifikator podmreže u okviru organizacije

identifikator sučelja (*interface ID*) – u IEEE EUI-64 formatu

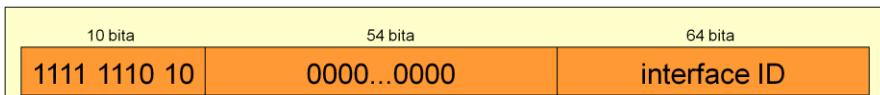
Globalna jednoodredišna adresa je globalbno dostupna. Organizirana je u tri dijela:

1. *Javna topologija* – davatelji internetske usluge (ISP) koji pružaju javne usluge Interneta
2. *Lokalna topologija* – topologija na razini određenog mjesta ili organizacije koja nepruža javne usluge čvorovima van nje
3. *Oznaka sučelja* – identificira pojedino sučelje

Značenja oznaka su:

- FP – Format prefiks (001)
- TLA ID (*Top-Level Aggregation Identifier*) – sam vrh hijerarhije združenih adresa
- RES – Rezervirano za eventualna proširenja polja *TLA ID* i/ili *NLA ID*
- NLA ID (*Next-Level Aggregation Identifier*) – organizacije kojima je dodijeljen pojedini *TLA ID* mogu raspodijeliti ovaj adresni prostor po želji, ili pružajući uslugu drugim organizacijama, ili za svoje potrebe
- SLA ID (*Site-Level Aggregation Identifier*) – pojedine organizacije ovdje mogu, ukoliko to žele, raspodijeliti svoj adresni prostor u najviše $2^{16}-1$ podmreža (što je više podmreža, tablice usmjeravanja su sve manje)
- Interface ID – Identifikator sučelja, mora biti jedinstven na poveznici kojoj pripada, no može i šire. Identifikator mora biti konstruiran u IEEE EUI-64 formatu.

Lokalne *unicast* adrese (1)



Lokalne adrese na razini poveznice (*link local*) - FE80::/64

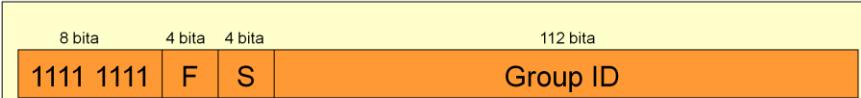
- ◆ konfiguiraju se automatski i koriste se za komunikaciju čvorova na lokalnoj poveznici (lokalna mreža, podmreža, mrežni segment)
- ◆ potrebne su za samokonfiguraciju adresa i postupak otkrivanja susjednih čvorova (*Neighbor Discovery*)
- ◆ usmjeritelj s potporom za IPv6 ne smije prosljeđivati pakete adresirane na *link-local* adrese

Lokalne *unicast* adrese (2)



- ◆ specifikacija: analogue IPv4 privatnim adresama iz adresnog prostora 10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16
- ◆ primjena: ne koristi se!

Multicast adrese



F – zastavice

S - doseg adrese

- ◆ F - zastavica (*flag*), definirana je zastavica *Transient*:
 - T = 0, trajno dodijeljena *multicast* adresa
 - T = 1, privremeno dodijeljena *multicast* adresa
- ◆ S – doseg (*scope*), označava doseg adrese, npr.:
 - čvor (*node-local*), poveznica (*link-local*), organizacija (*site-local*)
 - globalna

Multicast kod IPv6 mreža radi kao i kod IPv4 mreža. Paketi upućeni na *multicast* adresu dostavljaju se svim sučeljima unutar grupe definirane tom adresom. Sve IPv6 *multicast* adrese imaju prefiks FF, tj. 8 bitova 1 u prvom oktetu adrese. *Multicast* adresa ne može se koristiti kao izvorišna adresa paketa. Osim prefiksa, svaka *multicast* adresa ima još polja:

- F - zastavica (*flag*). Prema RFC 2373, definirana je jedino zastavica Transient, T, koja koristi krajnji desni bit od 4 bita predviđena za to polje. Ukoliko je T postavljen na 0, *multicast* adresa je trajno dodijeljena adresa koju dodjeljuje IANA. Ukoliko je T jednak 1, radi se o privremeno dodijeljenoj *multicast* adresi.
- S - doseg adrese (*scope*). Naznačuje doseg adrese i duljine je 4 bita. Vrijednost 1 naznačuje da je doseg adrese čvor (*node-local*), 2 znači da je doseg link (*link-local*), 5 je za site (*site-local*), 8 za organizaciju, E je globalno.
- Group ID - oznaka grupe, koja je jednoznačna za definirani doseg. Veličina polja je 112 bitova. Zbog načina na koji se IPv6 preslikavaju u Ethernet adrese, RFC 2373 preporuča da se Group ID kreira od donja 32 bita, a da se prvi 80 bitova popuni nulama.

Za definiranje svih čvorova i usmjeritelja na *node-local* i *link-local* dosezima, koriste se posebne adrese:

- FF01::1 - node-local scope all-nodes multicast
- FF02::2 - link-local scope all-nodes multicast
- FF01::1 - node-local scope all-routers multicast
- FF02::2 - link-local scope all-routers multicast
- FF05::2 - site-local scope all-routers multicast

Anycast adrese



- ◆ paketi usmjereni na *anycast* adresu prosljeđuju se najbližem sučelju iz adresirane grupe sučelja
 - mjera bliskosti je broj skokova
- ◆ za sad se dodjeljuju isključivo usmjeriteljima
 - svim sučeljima usmjeritelja dodijeljena je *Subnet-Router anycast* adresa za odgovarajuću podmrežu. Ta je adresa jednaka *unicast* adresi sučelja u toj podmreži s Interface ID dijelom postavljenim u 0.

Anycast adresa dodjeljuje se većem broju sučelja. Paketi adresirani na *anycast* adresu prosljeđuju se do najbližeg sučelju kojem je ta adresa dodijeljena. Blizina sučelja određuje se u smislu metrike usmjeritelja (broj skokova).

Trenutno se *anycast* adrese koriste kao odredišne adrese i dodjeljuju se usmjeriteljima. Nema pouzdanog načina da se odredi je li adresa *anycast* ili ne, budući da se adrese dodjeljuju iz adresnog prostora namijenjenog *unicast* adresama i njihov je doseg ekvivalentan dosegu *unicast* adresa na osnovu koje su dodijeljene.

Jedina predefinirana *anycast* adresa je tzv. *Subnet-Router* adresa koja se uvijek dodjeljuje usmjeriteljima, a stvara se od prefiksa podmreže za pojedino sučelje. Za konstruiranje *Subnet-Router* adrese, prepisuj se bitovi koji označavaju podmrežu dok se svi ostali bitovi popune nulama.

Svim sučeljima usmjeritelja dodijeljena je *Subnet-Router* anycast adresa koja odgovara podmreži na kojoj se nalazi sučelje. *Subnet-Router* adresa se koristi za komunikaciju s jednim od više usmjeritelja na udaljenoj podmreži.

◆ nespecificirane adrese

- 0:0:0:0:0:0 ili :: naznačuju da nema adresu
- ekvivalentno adresi 0.0.0.0 u IPv4

◆ loopback adrese

- ::1 ekvivalent 127.0.0.1

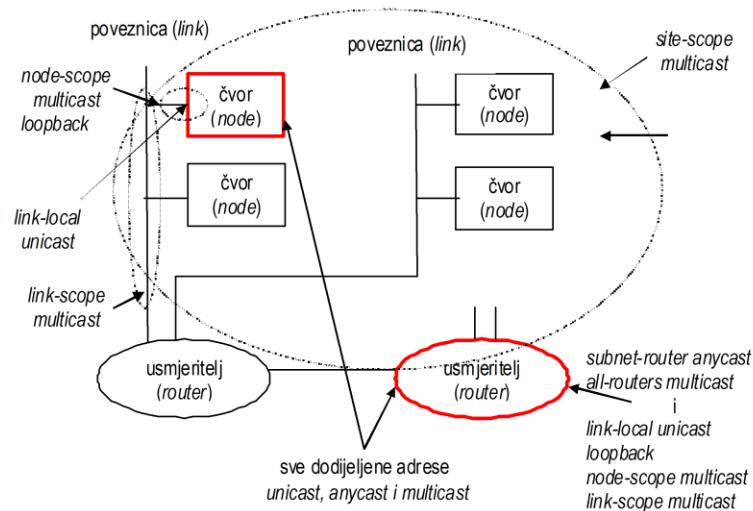
◆ kompatibilne adrese

- IPv4 kompatibilne adrese
 - 0:0:0:0:a.b.c.d ili ::a.b.c.d (npr: ::161.53.19.201)
- IPv4 preslikane adrese
 - 0:0:0:FFFF:a.b.c.d ili ::FFFF:a.b.c.d (interno)
- 6to4 adrese - 2002::/16 – za tuneliranje preko IPv4

Sljedeće adrese spadaju u posebne IPv6 adrese:

- nespecificirane adrese (*unspecified addresses*) - sastoje se od niza 0 bitova i kraće se zapisuju kao ::, a koriste se kao i adresa 0.0.0.0 kod IPv4, najčešće kao izvođena adresa paketa u kojima stanice pokušavaju provjeriti jednoznačnost traženih adresi (npr. kod autokonfiguracije). Ta se adresa nikad ne smije dodijeliti mrežnom sučelju ili se koristiti kao odredišna adresa.
- *loopback* adresa, ::1, koristi se za označavanje loopback sučelja, omogućujući da čvor šalje podatke sam sebi kroz svoj protolni složaj. Ekvivalentna je IPv4 adresi 127.0.0.1. Paketi poslani na tu adresu nikad se ne smiju naći na linku.
- kompatibilne adrese pomažu kod prelaska s IPv4 na IPv6 i paralelnom korištenju obje vrste adresa:
 - IPv4 kompatibilne adrese sastoje se od niza 0 bitova iza kojih slijedi IPv4 adresa, a koriste ih računala koja imaju podršku za oba protokola a komuniciraju putem IPv6
 - IPv4 preslikane adrese koriste se kako bi se čvor koji podržava samo IPv4 prikazao čvoru koji podržava samo IPv6. Koristi se isključivo za interno prikazivanje i nikad se ne koristi kao izvođena ili odredišna adresa IPv6 paketa.
 - 6to4 adrese se koriste za komunikaciju između 2 čvora koji podržavaju i IPv4 i IPv6 preko IPv4 računalne infrastrukture. To je tehnika tuneliranja, opisana u RFC 3056.

Adrese čvora (računala) i usmjeritelja



Svaki čvor (računalo) treba prepoznati sljedeće adrese:

- lokalna adresa na razini poveznice za svako sučelje (*link-local unicast address*)
- *loopback* adresa
- *multicast* adrese dosega čvora i poveznice
- sve druge *unicast* i *anycast* adrese dodijeljene ručno ili automatski
- *multicast* adrese svih grupa kojima je čvor pridružen
- *solicited-node multicast* adrese za svaku *unicast* i *anycast* adresu

Svaki usmjeritelj treba, uz sve adrese dodijeljene čvoru, prepoznati još sljedeće adrese:

- *Subnet-Router anycast* i druge *anycast* adrese za sučelja za koja je konfiguriran kao usmjeritelj
- *all routers multicast* adrese namijenjene svim usmjeriteljima u dosegu
- *solicited node multicast* adrese za svaku *unicast* i *anycast* adresu

Dodjela IPv6 adrese

◆ postupak autokonfiguracije

- stvaranje lokalne adrese na razini poveznice (*link-local*) i provjera njene jedinstvenosti (primjena protokola *Neighbour Discovery Protocol*, RFC 2461)
- utvrđivanje informacija treba samostalno konfigurirati (adrese, druge informacije)
 - ako se konfiguriraju adrese, koristiti mehanizam:
 - autokonfiguracija bez poslužitelja (*stateless*) – zasnovano na MAC adresi (RFC 2462); EUI-64 bitni broj izведен iz Ethernet 48 bitne adrese
 - autokonfiguracija s poslužiteljem (*statefull*) – koristi DHCPv6 poslužitelj (RFC 3315); potpuna konfiguracija TCP/IP (uz IPv6 adresu)

◆ autoregistracija u DNS-u

- DHCPv6 može koristiti dinamičko osvježavanje informacije u DNS-u za registraciju IPv6 adrese i imena (RFC 2136)

RFC koji se odnose na konfiguraciju adrese:

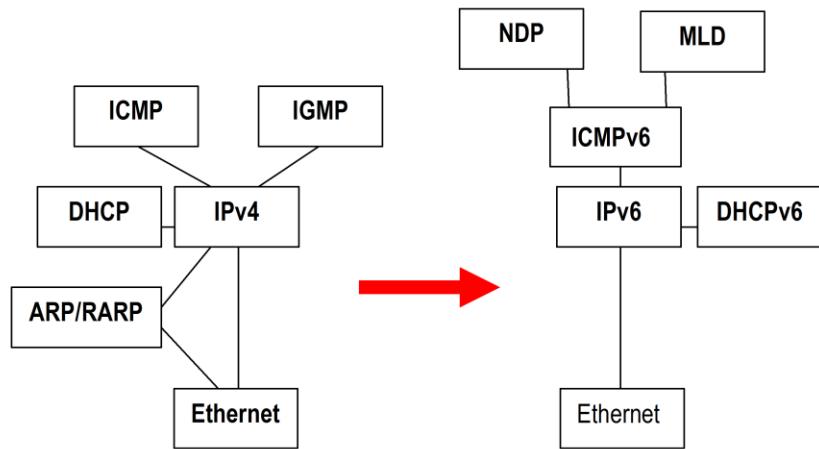
- [1] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.
- [2] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.
- [3] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
- [4] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.
- [5] Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

***** AUTOREGISTRATION – for both IPv4 and IPv6 *****

2136 Dynamic Updates in the Domain Name System (DNS UPDATE). P. Vixie, Ed., S. Thomson, Y. Rekhter, J. Bound. April 1997. (Format: TXT=56354 bytes) (Updates RFC1035) (Updated by RFC3007, RFC4035, RFC4033, RFC4034) (Status: PROPOSED STANDARD)

MM Note: RFC 3007, 4033-4035: Updates are related to security extensions for DNS!

Kontrolni protokoli za IPv6 (1)



Kontrolni protokoli za IPv6 (2)

- ◆ *Internet Control Message Protocol for IPv6 (ICMPv6)*
 - specifikacija u RFC 4433
 - služi za dojavu pogrešaka i dijagnostiku (npr. ICMPv6 "ping")
- ◆ *Neighbor Discovery Protocol (NDP)*
 - specifikacija u RFC 2461
 - zamjenjuje ARP i proširuje njegovu funkcionalnost, sastavni dio ICMPv6
- ◆ *Multicast Listener Directory (MLD)*
 - specifikacija u RFC 3810
 - zamjenjuje IGMP i proširuje njegovu funkcionalnost, sastavni dio ICMPv6
- ◆ *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
 - specifikacija u RFC 3315
 - protokol za autokonfiguraciju adrese pomoću poslužitelja – DHCP poslužitelj dinamički dodjeljuje IPv6 adresu
 - pruža druge konfiguracijske informacije

3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6). R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney. July 2003.
(Format: TXT=231402 bytes) (Updated by RFC4361) (Status: PROPOSED STANDARD)

4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. A. Conta, S. Deering, M. Gupta, Ed.. March 2006. (Format: TXT=48969 bytes) (Obsoletes RFC2463) (Updates RFC2780) (Updated by RFC4884) (Status: DRAFT STANDARD)

Internet Control Message Protocol for IPv6 (ICMPv6)

- ◆ ICMPv6 - proširuje funkcionalnost ICMPv4 (STD-5), RFC 4433
- ◆ ICMPv6 sadrži kontrolne funkcije za višeodredišnu komunikaciju (*multicasting*) koje su bile dio IGMP u IPv4
- ◆ ICMP v4 i v6 nisu kompatibilni
- ◆ Vrste poruka:
 - Poruke o pogreškama (nema puta, nedostupno odredište, ...)
 - IPv6 ping (npr: *echo request, echo reply*)
 - Pripadnost grupi (npr: *query, report*)
 - Poruke koje se koriste kod otkrivanja susjeda i samokonfiguriranja (NDP)

Prigodom definiranja IPv6, definiran je i Internet Control Message Protocol verzije 6. Funkcije koje se nisu koristile u ICMPv4 su izbačene, a dodane su kontrolne funkcije vezane uz *multicast* koje su bile sadržane u Internet Group Membership Protocolu v4 (IGMP). Zbog promjene formata zaglavlja, verzije 4 i 6 nisu kompatibilne. Sve ICMPv6 poruke imaju isti općeniti format, a specifikacija definira različite tipove poruka, od kojih navodimo neke:

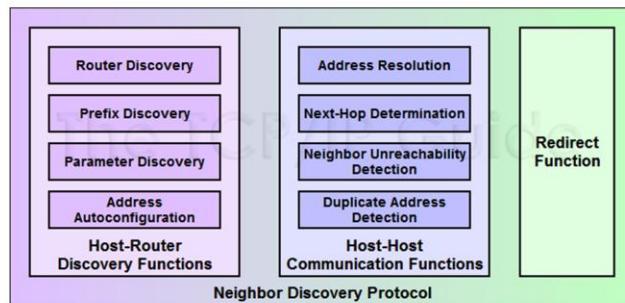
- **poruke o pogreškama** (*error messages*), koje šalje IPv6 čvor prema izvođištu paketa, kad izbaci paket iz mreže. Četiri su vrste takvih poruka: paket može biti odbačen, jer je odredište nedostupno (nema puta do odredišta, zabranjena je komunikacija, nedostupna adresa ili port), paket je previelik, paket predugo putuje po mreži ili je došlo do problema s parametrima (pogreška u polju zaglavlja, nepoznat tip zaglavlja ili nepoznata opcija u IPv6)
- **IPv6 Ping**, s *Echo Reply* i *Echo Request* porukama
- **poruke o pripadnosti multicast grupi** (*Group Membership Query, Group Membership Report* i *Group Membership Reduction*)
- **poruke kod otkrivanja susjeda i postupka autokonfiguriranja** (*Router Solicitation, Router Advertisment, Neighbor Solicitation, Neighbor Advertisement, Redirect*)

Protokol NDP



NDP (*Neighbor Discovery Protocol*)

- ◆ kontrolni protokol - preuzima funkcije ICMP i ARP protokola iz IPv4, definira nove ICMP poruke



Funkcije protokola NDP (1)



◆ Otkrivanje između računala i usmjeritelja (*host-router*):

- Otkrivanje usmjeritelja (*router discovery*) – računalo otkriva usmjeritelja u svojoj lokalnoj mreži
- Otkrivanje pefiksa (*prefix discovery*) – računalo otkriva kojoj mreži pripada
- Otkrivanje parametara (*parameter discovery*) – računalo otkriva parametre lokalne mreže i/ili usmjeritelja (npr. MTU)
- Autokonfiguracija adrese (*address autoconfiguration*) – automatska konfiguracija adrese računala

Funkcije protokola NDP (2)

◆ Komunikacija između računala (host-host):

- Razlučivanje adrese (*address resolution*) – računalo otkriva MAC adresu računala (odgovora ARP zahtjevu u IPv4)
- Određivanje sljedećeg skoka (*next-hop determination*) – određuje slanje datagrama na temelju odredišne adrese datagrama
- Provjera dostupnosti (*neighbor unreachability detection*) – određivanje dostupnosti susjednog uređaja
- Provjera dvostrukе adrese (*duplicate address detection*) – provjerava da li adresa uređaja koju želi koristiti već postoji

◆ Funkcija *redirect*

- Usmjeritelj informira računalo o boljem putu do određenog odredišta

Dynamic Host Configuration Protocol v6 (DHCPv6)

- ◆ protokol klijent – poslužitelj koji omogućuje klijentu (računalo) dobivanje konfiguracijskih parametara od poslužitelja (poslužitelj DHCPv6)
- ◆ transport poruka između klijenta i poslužitelja: UDP
- ◆ zasniva se na dvije mogućnosti IPv6:
 - lokalna adresa na razini poveznice koju formira samo računalo (*client link-local address*)
 - višeodredišno adresiranje poslužitelja DHCPv6-a i njihovih posrednika (*relay*)

Protokol DHCPv6 (2)



DHCP Solicit

- traži se poslužitelj DHCP-a ili posrednik (*relay*) - *multicast*

DHCP Advertise

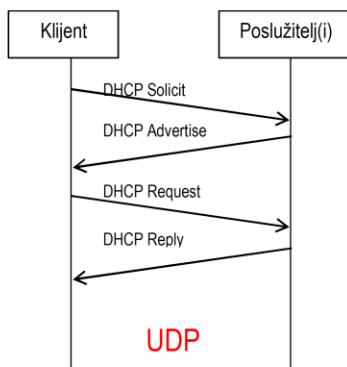
- oglašava se poslužitelj DHCP-a

DHCP Request

- klijent odabire jednog od poslužitelja koji su se oglasili i zahtijeva konfiguracijske parametre

DHCP Reply

- poslužitelj dostavlja klijentu IPv6 adresu i druge zahtijevane parametre (npr. vrijeme valjanosti, poslužitelj DNS-a)



Uz navedene poruke, upotrebljavaju se još dvije:

DHCP Release: otpuštanje nekih dobivenih parametara, npr. adresu koju više neće koristiti

DHCP Reconfigure: promjena nekih parametara

Zadatak

- ◆ Usporediti IPv4 i IPv6 s obzirom na funkcionalnost i performanse.