

Komunikacijski protokoli

6. Mrežni protokol IPv6

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 licencom 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.

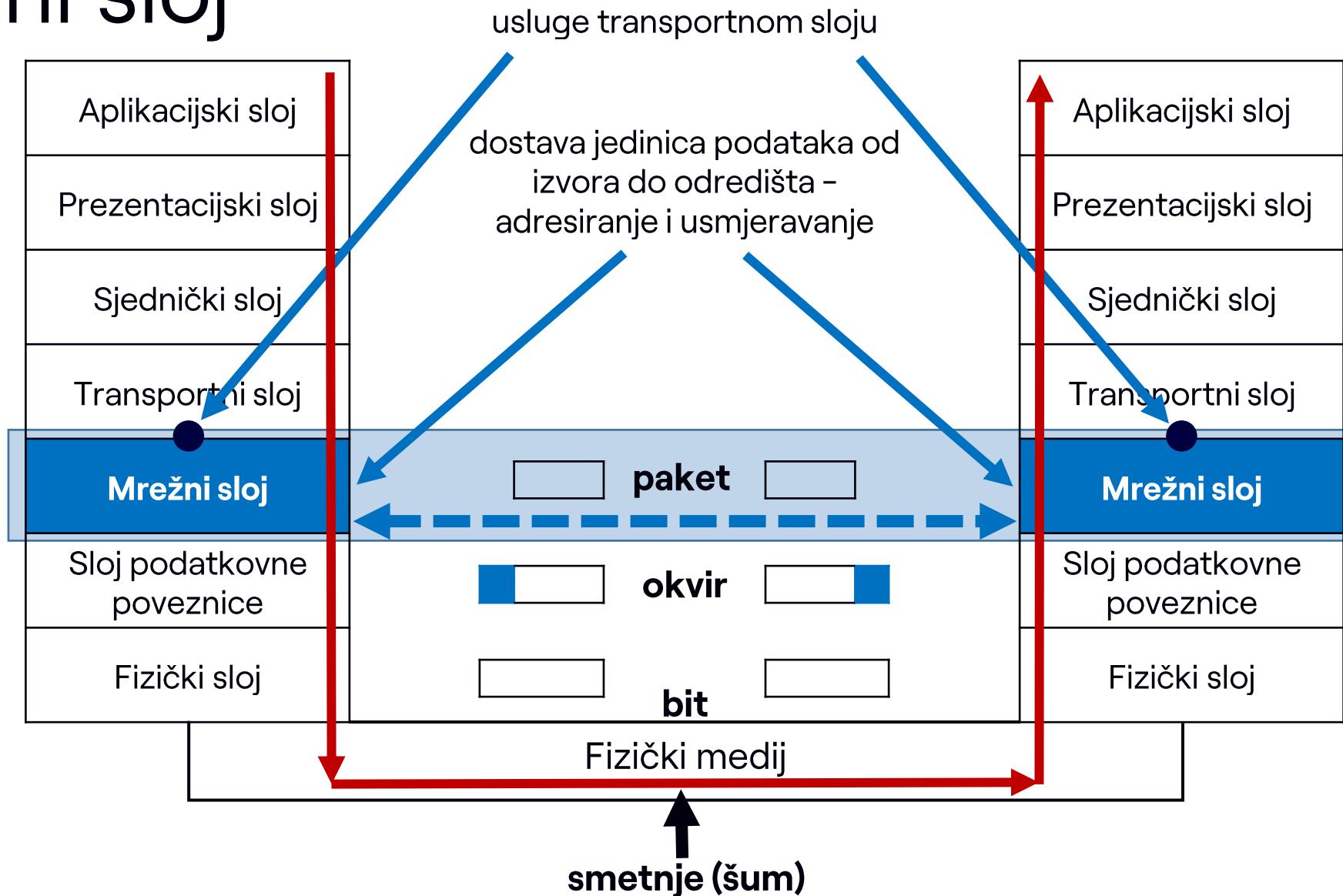
Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

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

Sadržaj predavanja

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

Mrežni sloj



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**

Mrežni sloj u Internetu i IP-mrežama

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

Odlike protokola IPv4 (1)

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
 - 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)
- 
- usluga IP-a
transportnom sloju:
nepouzdana dostava
datagrama**

Odlike protokola IPv4 (2)

- **Nespojna usluga izvedena datagramski:** 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 **retransmisijske** s kraja na kraj mreže
 - pošiljatelj nema povratnu informaciju o ishodu
- Rješavanje ovih problema prepušta se transportnom sloju!

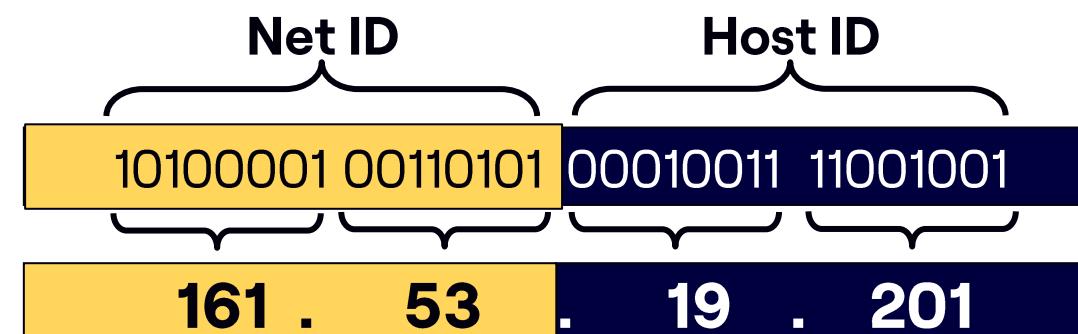
Funkcionalnost protokola IPv4

- Definira **shemu adresiranja** u Internetu
 - jedinstveni **adresni prostor**
 - svako **sustav** (krajnje računalo, mrežni čvor) ima po jednu **IP-adresu** za svako **mrežno sučelje**
 - 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 (**MTU**)
 - **datagram** veći od podatkovnog polja okvira **fragmentirati** se kod **pošiljatelja**, a fragmenti se **sastavljaju** kod **primatelja**

Adresiranje

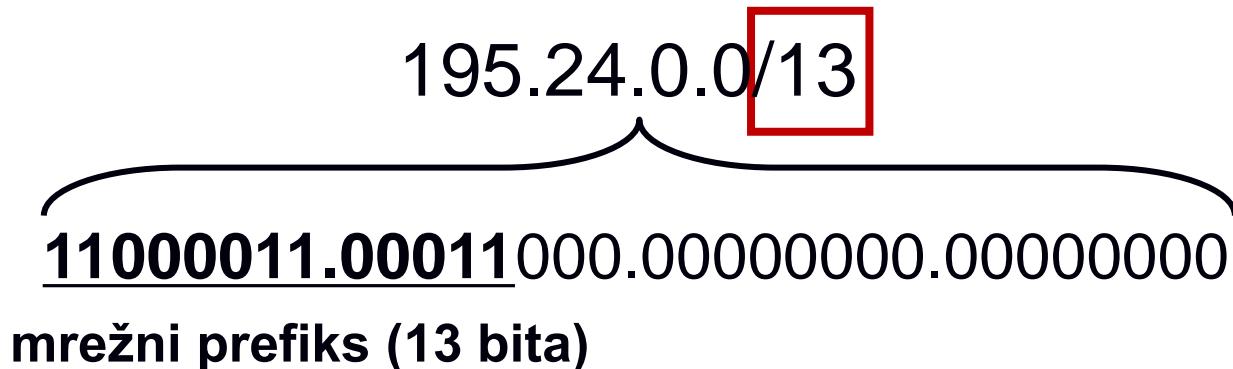
IP-adresa **32 bita** (IPv4): identifikator koji globalno i jednoznačno određuje mrežno sučelje

- 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)



Prefiksni prikaz adrese i besklasno usmjeravanje

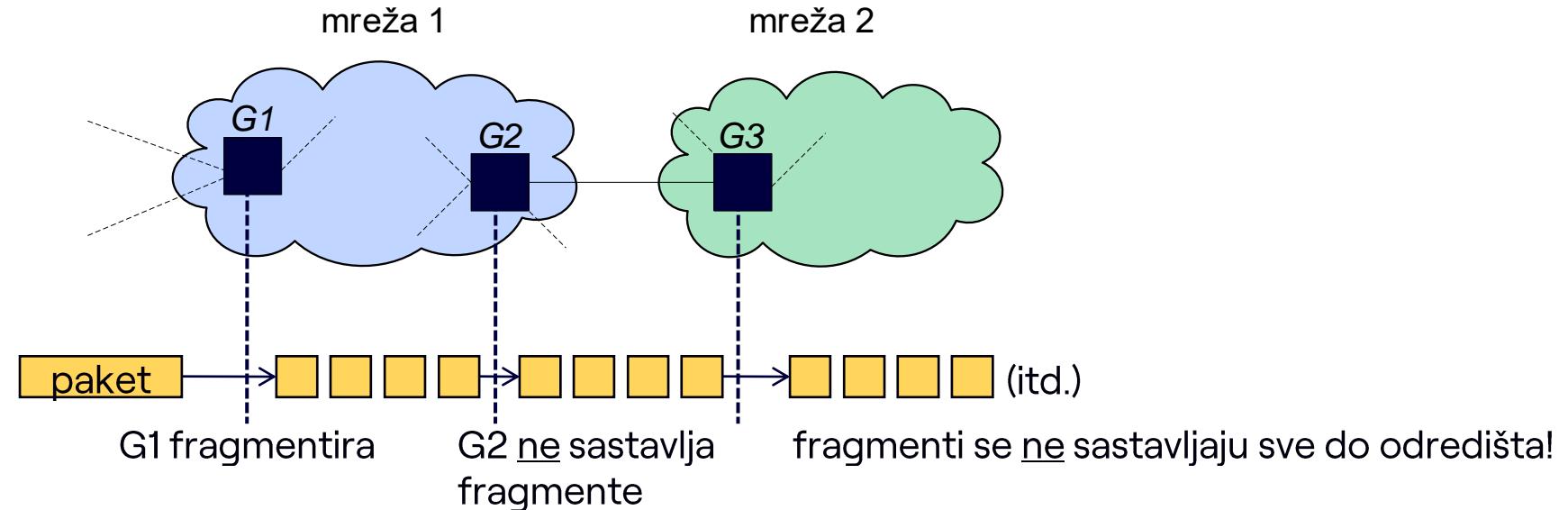
- **prefiksni prikaz** IP-adrese ne uzima u obzir izvorne klase A, B i C
- dioba između mrežnog i računalnog dijela adrese može biti na bilo kojem mjestu unutar adrese (ne samo na granici okteta kao kod klase!)
- duljina mrežnog dijela se označava **mrežnim prefiksom** iza adrese



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

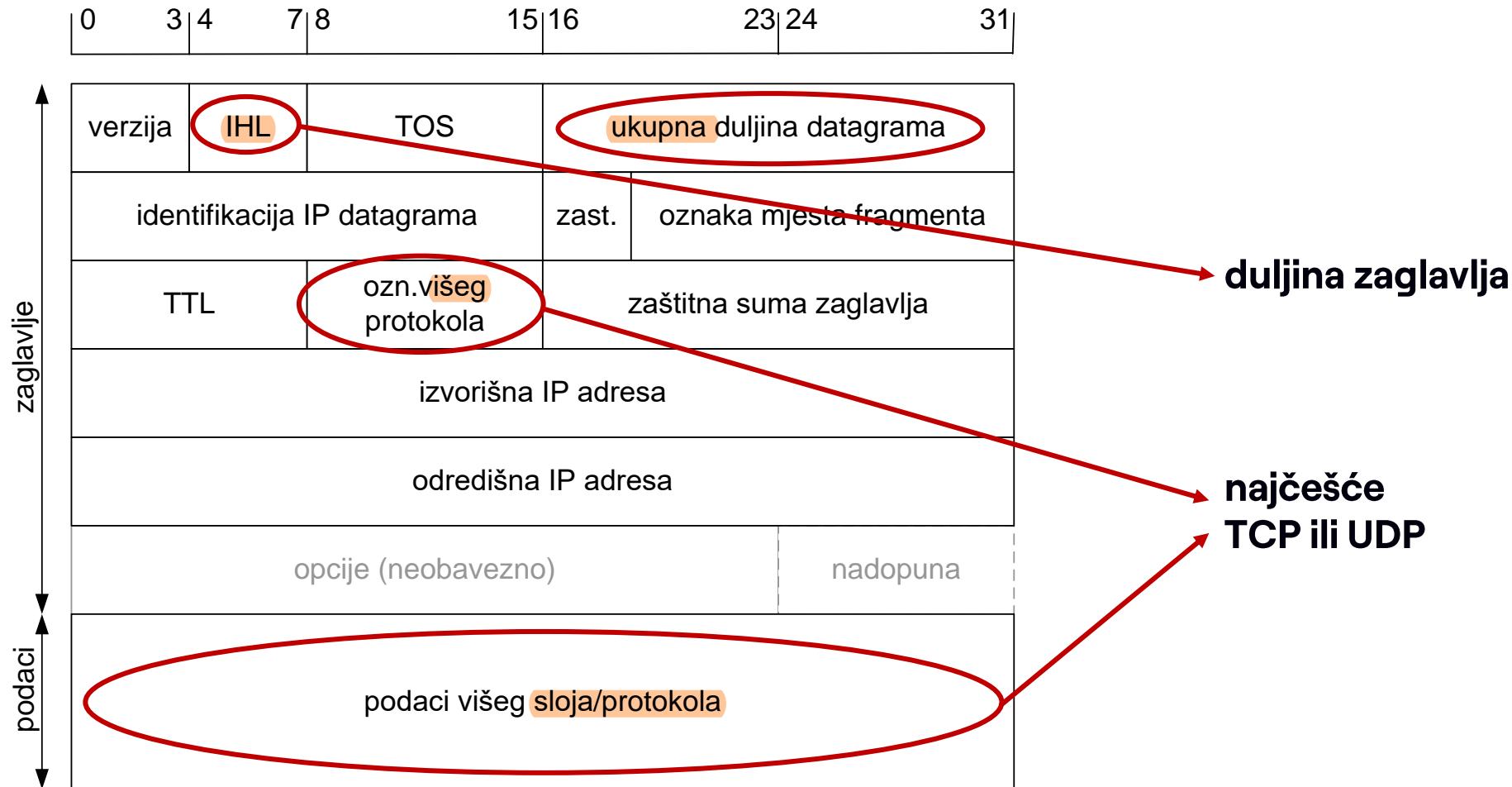
Fragmentacija

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

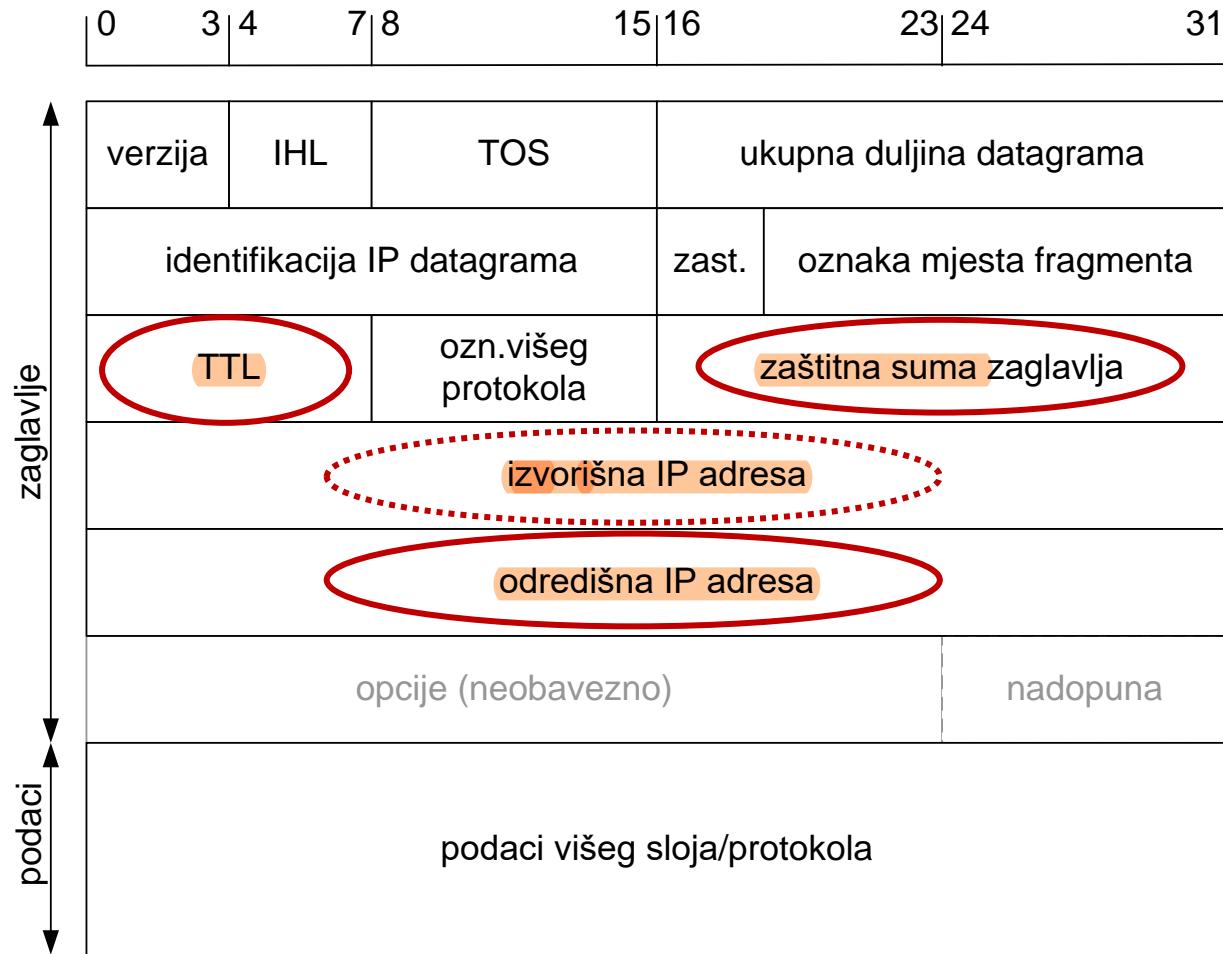


Netransparentna fragmentacija: model primjenjen u Internetu!

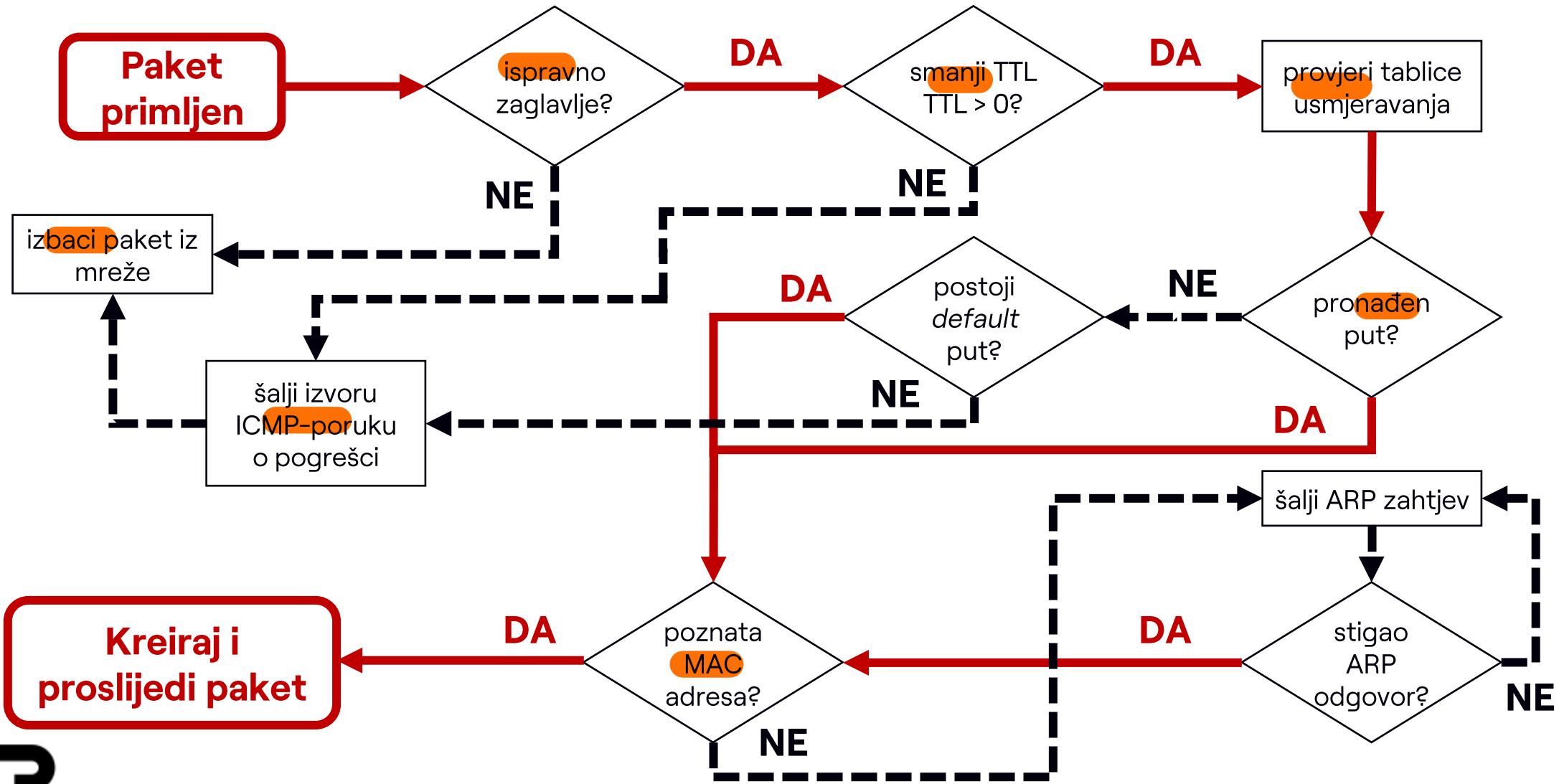
IPv4-zaglavje: polja vezana uz omatanje



IPv4-zaglavje: polja vezana uz usmjeravanje



Proces usmjeravanja IPv4-paketa u usmjeritelju (1)



Proces usmjeravanja IPv4-paketa u usmjeritelju (2)

1. U kojim se poljima razlikuju zaglavlje IPv4-paketa kojeg je primio usmjeritelj i zaglavlje paketa kojega je usmjerio prema odredištu i proslijedio sljedećem čvoru?
2. U kakvim okolnostima IPv4-usmjeritelj izaziva gubitak paketa (izbacuje ga) i zašto?

Sadržaj predavanja

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

Internet Protocol v6

Internet Protocol Version 6, IPv6 (RFC 2460 → RFC 8200)

- 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

IPv4 – IPv6: ograničenja IPv4

- ograničenja IPv4:
 - broj raspoloživih adresa postao premalen (**32 bitne adrese**)
 - prevelike tablice **usmjeravanja** ← **ZAŠTO?**
 - 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 - Quality of Service)**

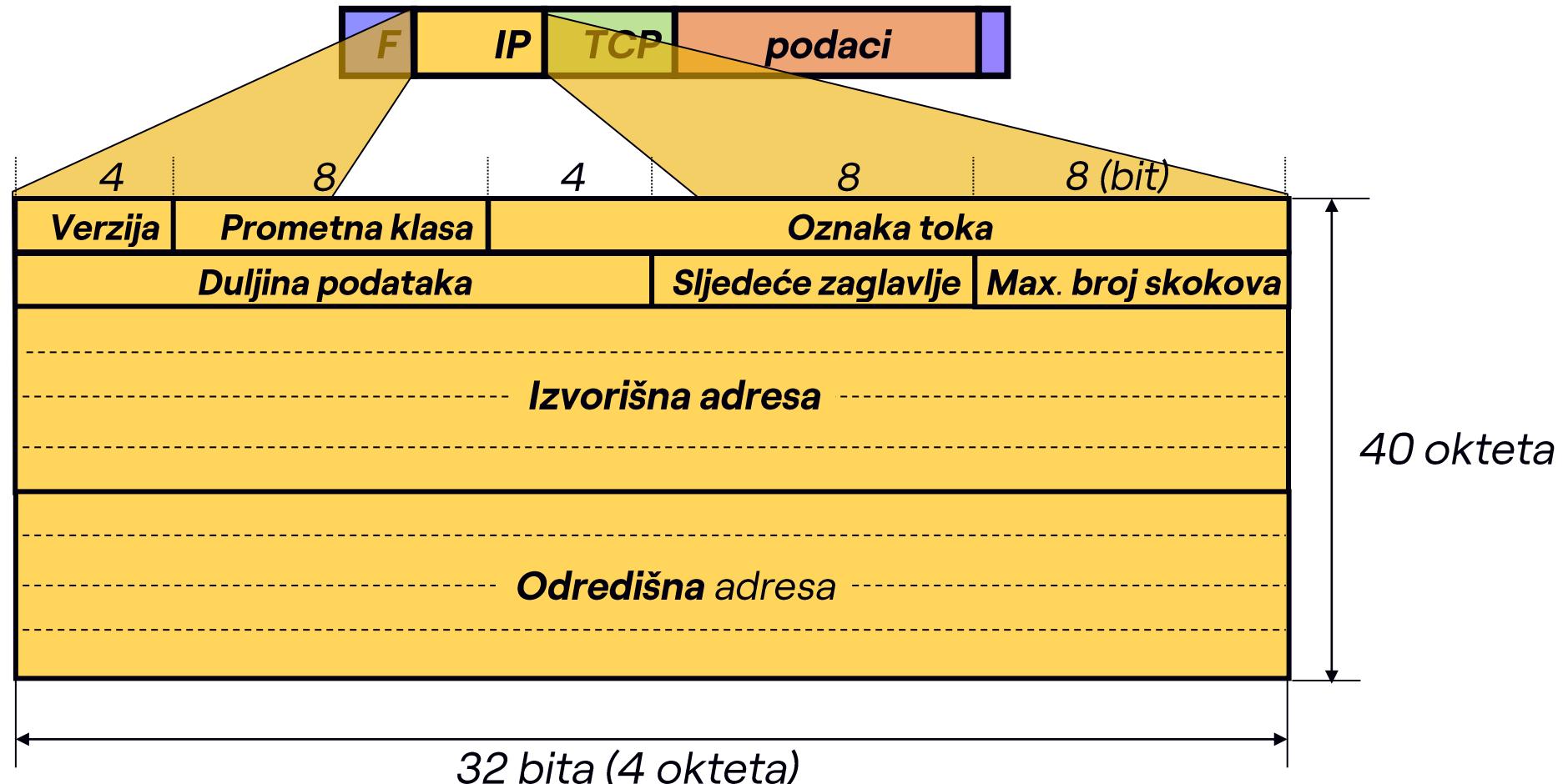
IPv4 – IPv6: nova rješenja u IPv6

- novosti u IPv6:
 - veći adresni prostor (**128 bitne adrese**)
 - pojednostavljenje formata zaglavlja
(fiksna duljina, manje polja) ← **ZAŠTO?**
 - dodatna zaglavljia za posebne mogućnosti
 - unaprijeđeno usmjeravanje
 - mogućnost označavanja tokova (tj. paketa koji pripadaju istom toku)
 - bolja potpora za sigurnost: provjera autentičnosti i zaštita privatnosti, integritet podataka, povjerljivost
 - bolja potpora za pokretljivost (*Mobile IPv6*)
 - potpora za kvalitetu usluge

Sadržaj predavanja

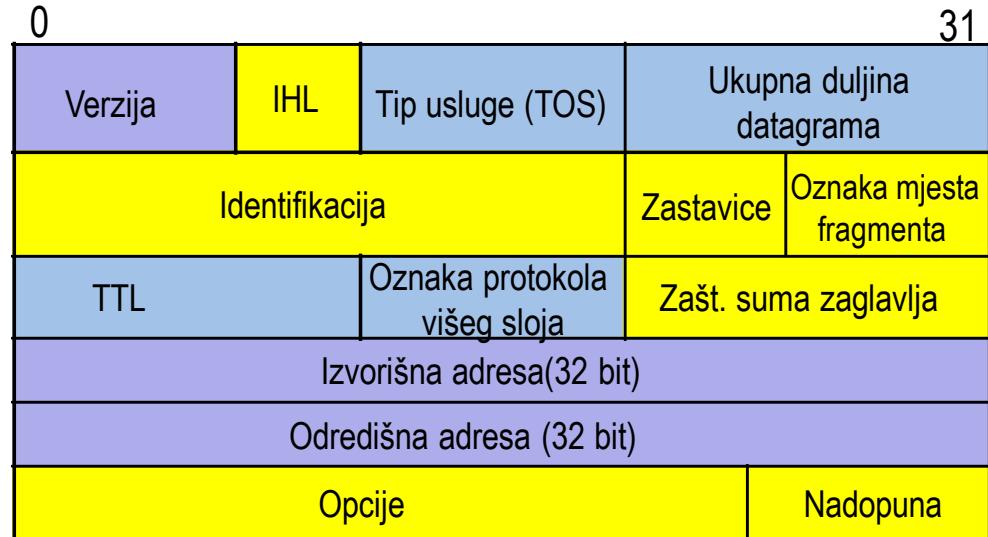
- Mrežni sloj i mrežni protokol IPv4 ukratko
- Glavne značajke protokola IPv6
- **Format datagrama, osnovno i dodatna zaglavla**
- Adresiranje
- Upravljački protokoli
 - ICMPv6
 - NDP
 - DHCPv6

Zaglavje IPv6



Usporedba zaglavlja IPv4 i IPv6

IPv4 -zaglavljje



Duljina zaglavlja: bez opcija 20 okteta; s opcijama max. 60 okteta

Značenje boja na slikama:

- naziv polja isti u IPv4 i IPv6
- polje izbačeno u IPv6
- promjena imena i pozicije polja u IPv6
- novo polje u IPv6

IPv6 -zaglavljje



Fiksno 40 okteta

Izvor:
https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

Proces usmjeravanja IPv6-paketa u usmjeritelju

1. U kojim se poljima razlikuju zaglavlje IPv6-paketa kojeg je primio usmjeritelj i zaglavlje paketa kojega je usmjerio prema odredištu i proslijedio sljedećem čvoru?
2. U kakvim okolnostima IPv6-usmjeritelj izaziva gubitak paketa (izbacuje ga) i zašto?
3. Kakve mogu biti posljedice pogreške u zaglavlju IPv6-paketa?

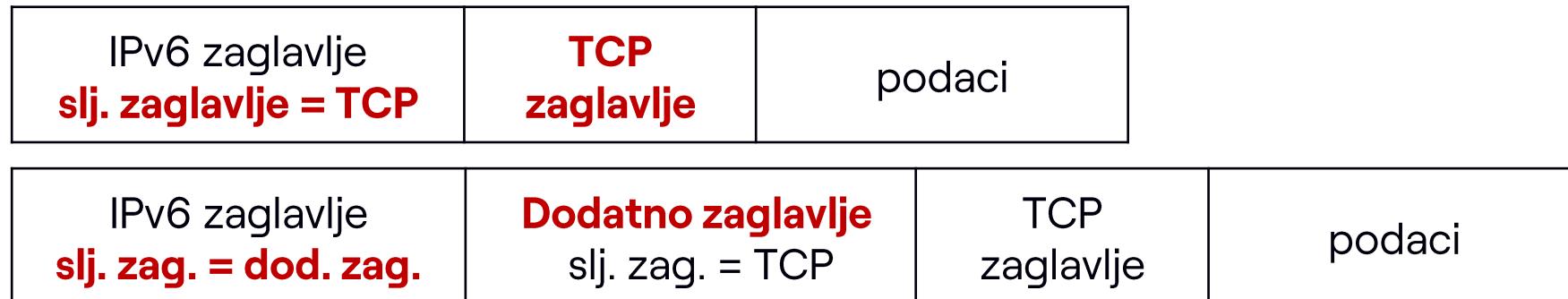
Dodatna zaglavlja IPv6

IPv4:

- korištenje posebnih opcija usporava prosljeđivanje paketa u usmjeriteljima

IPv6:

- umjesto opcija koriste se dodatna zaglavlja za proširenja koja se po potrebi dodaju iza osnovnog zaglavlja, npr.:



- sama specifikacija protokola IPv6 omogućuje uvođenje novih vrsta dodatnih zaglavlja:
<https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml>

Vrste i poredek dodatnih zaglavlja IPv6

IPv6 datagram:

1. Zaglavljje IPv6

2. Zaglavljje skok po skok (engl. *Hop-by-Hop Options header*)
3. Zaglavljje namijenjeno odredištu (1) (engl. *Destination Options header*)
4. Zaglavljje usmjerenja (engl. *Routing header*)
5. Zaglavljje fragmenta (engl. *Fragment header*)
6. Zaglavljje za provjeru autentičnosti (engl. *Authentication header*)
7. Zaglavljje za sigurnosno ovijanje podataka (engl. *Encapsulating Security Payload header*)
8. Zaglavljje namijenjeno odredištu (2)
 - nakon zadnjeg dodatnog IPv6 zaglavljja slijede zaglavljje i podaci protokolne jedinice transportnog sloja (TCP ili UDP) ili zaglavljje i podaci protokolne jedinice ICMPv6

Samo zaglavljje IPv6 je obvezno!

Zaglavljje skok po skok

Hop-by-Hop Options Header

- zaglavljje varijabilne duljine koje sadrži informaciju namijenjenu svakom čvoru na putu dostave datagrama
- sadrži podatke o sljedećem zaglavljju, veličini samog dodatnog zaglavja i opcionsko polje s jednom ili više definicija akcije koju poduzima čvor

Primjer primjene:

- prijenos vrlo velikih paketa $> 2^{16}$ okteta ("jumbo payload"), npr. video sadržaj, na putu s velikim MTU
 - polje "duljina podataka" u IPv6 zaglavljju = 0
 - ne primjenjuje se fragmentacija

Zaglavlje namijenjeno odredištu (1)

Destination Options Header (1)

- zaglavlje varijabilne duljine koje sadrži dodatnu informaciju za **prvo odredište i sva odredišta** koje sadrži **dodatno zaglavlje Routing Header**
- sadrži podatke o sljedećem zaglavlju, veličini samog dodatnog zaglavla i polje s jednom ili više definicija akcije koju poduzima čvor - odredište

Primjer primjene:

- **Mobile IPv6**

Zaglavlje namijenjeno odredištu (2)

Destination Header (2)

- zaglavlje varijabilne duljine koje **sadrži** dodatnu informaciju samo **za krajnje odredište**
- sadrži podatke o sljedećem zaglavljtu, veličini samog dodatnog zaglavlja i polje s jednom ili više definicija akcije koju poduzima čvor - odredište

Primjer primjene:

- *Mobile IPv6*

Zaglavlje usmjeravanja

Routing Header

- zaglavlje varijabilne duljine koje **sadrži popis usmjeritelja** na putu od **izvora** do **odredišta**
- sadrži podatke o sljedećem zaglavlju, veličini samog dodatnog zaglavlja, vrsti usmjeravanja i popis čvorova koje paket još treba prijeći prije nego što dođe do odredišta
- početna specifikacija nesigurna za mrežu:
 - zlonamjerno usmjeravanje datagrama na neki čvor: zagušenje! (**DDoS** napad)

Primjer primjene:

- odabir niza usmjeritelja putem kojih se povezuju izvor i odredište
- *Mobile IPv6*

Zaglavlje fragmenata

Fragment Header

- zaglavje fiksne duljine koje se primjenjuje za slanje datagrama većih od MTU-a puta
 - IPv6 propisuje minimalni MTU od 1280 okteta
- nefragmentirani dio zajednički za sve fragmente:
 - osnovno zaglavje i dodatna zaglavja skok po skok i usmjeravanja
 - sadrži podatke o sljedećem zaglavljtu, polje s mjestom fragmenata, zastavicu koja označava ima li još fragmenata (1) ili je riječ o zadnjem (0) i identifikacijsko polje koje označava fragmentirani paket

Primjena:

- fragmentiranje datagrama – isključivo na izvoru!

Vrste i poredek dodatnih zaglavlja IPv6

IPv6 datagram:

1. Zaglavljje IPv6

2. Zaglavljje skok po skok (engl. *Hop-by-Hop Options header*)
3. Zaglavljje namijenjeno odredištu (1) (engl. *Destination Options header*)
4. Zaglavljje usmjeravanja (engl. *Routing header*)
5. Zaglavljje fragmenta (engl. *Fragment header*)

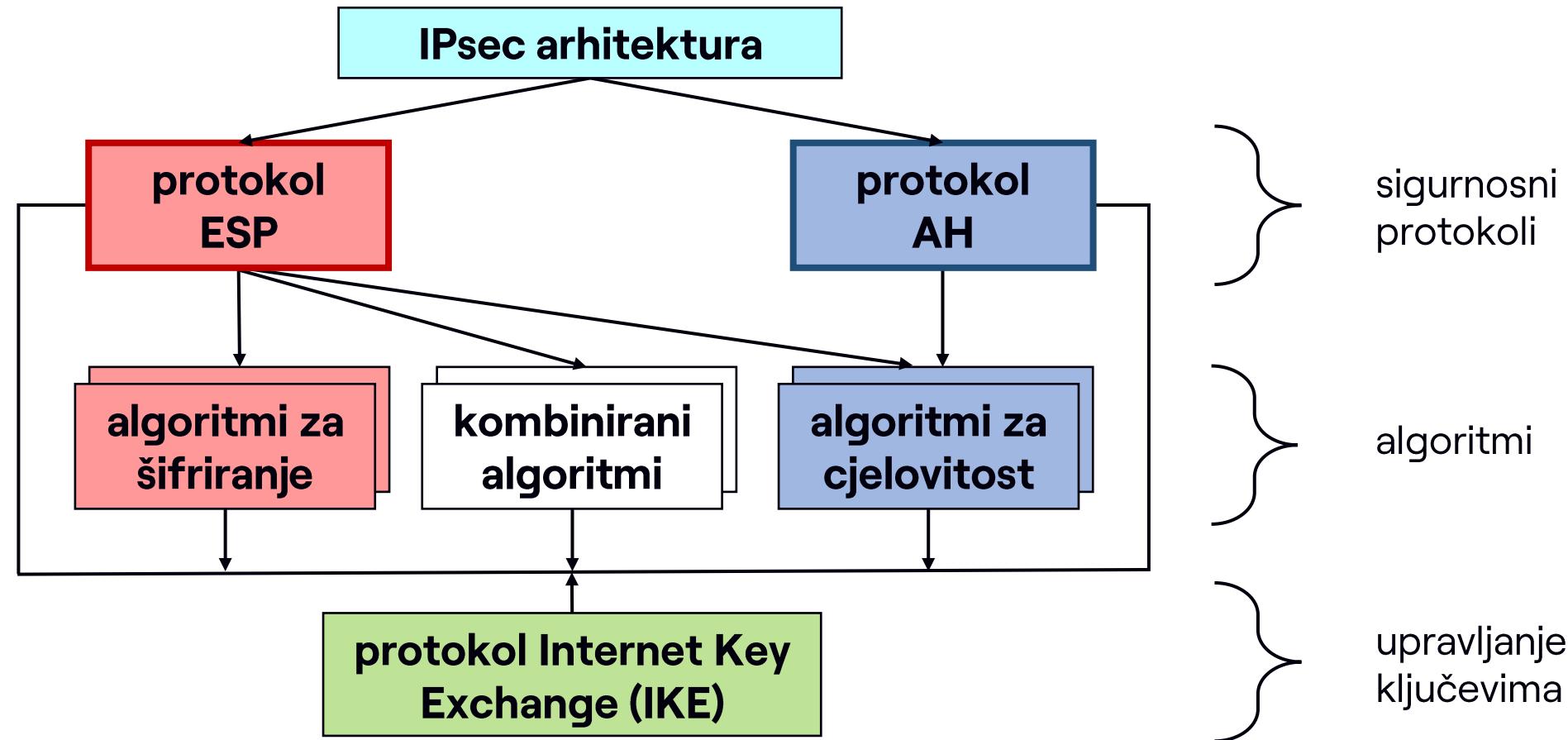
u okviru sigurnosne internetske arhitekture (IPsec)

6. Zaglavljje za provjeru autentičnosti (engl. *Authentication header*)
7. Zaglavljje za sigurnosno ovijanje podataka (engl. *Encapsulating Security Payload header*)
8. Zaglavljje namijenjeno odredištu (2)

- nakon zadnjeg dodatnog IPv6 zaglavljja slijede zaglavljje i podaci protokolne jedinice transportnog sloja (TCP ili UDP) ili zaglavljje i podaci protokolne jedinice ICMPv6

Samo zaglavljje IPv6 je obvezno!

Sigurnosna internetska arhitektura (IPsec)



Ova tema obrađuje se detaljno na kolegiju „Sigurnost u Internetu“.

Izvor: RFC 6071 IP Security (IPsec) and Internet Key Exchange (IKE)
Document Roadmap

Arhitektura IPsec, glavna obilježja

- IPSec definira protokole čija zadaća je prijenos podataka, pri čemu se podaci tijekom prijenosa mogu štititi na dva načina:
 - protokol AH: zaglavlje autentičnosti (engl. *Authentication Header*, AH):
 - štiti integritet datagrama, autentičnost izvora datagrama te štiti od napada ponavljanjem ranije snimljenih datagrama
 - protokol ESP: sigurnosno ovijeni podaci (engl. *Encapsulating Security Payload*, ESP):
 - sve što i AH te, dodatno, povjerljivost podataka
 - oba protokola mogu štiti bilo koji protokol više razine koji se prenosi IP datagramom
 - definirana su dva načina rada: transportni i tunelski način rada
- Dodatno, definira protokol IKE (Internet Key Exchange) koji provodi uzajamnu autentifikaciju dviju strana te između njih uspostavlja sigurnosnu asocijaciju, koja koristi protokole AH ili ESP i skup kriptografskih algoritama za zaštitu prometa koji se prenosi preko sigurnosne asocijacije.
 - protokol IKE omogućuje razmjenu informacija o podržanim algoritma i pregovaranje o onima koji će se primijeniti
 - u primjeni je verzija IKEv2 (RFC 7296)
- u implementaciji IPsec(v3) je protokol ESP definiran kao obavezan, a AH kao opcionalan

Arhitektura IPsec, primjene

- Vrlo široka primjena za ostvarivanje virtualnih privatnih mreža (engl. *Virtual Private Network*, skr. **VPN**)
 - koristi se ESP u tunelskom način rada (*gateway - gateway*)
 - krajne točke komunikacije "ne znaju" za tuneliranje, a kada paket prolazi dionicom kroz javni Internet, potencijalni napadači ne mogu sazнати ništa o unutarnjoj mreži (primjerice, IP adrese krajnjih točaka)
- VPN se može se iskoristiti i za **sigurnu komunikaciju** dvaju krajnjih računala, primjerice **poslužitelja i klijenta**
- Protokol AH se koristi za zaštitu određenih poruka protokola Mobile IPv6 (više na nekom od sljedećih predavanja)

Primjena IPsec-a u IPv4 i IPv6 mreži

Internet Protocol Security (IPsec) u IPv4 i IPv6

- sigurnosna opcija za IPv4
- sastavni dio IPv6: dodatna zaglavla AH i ESP
- sigurnosna arhitektura
 - sigurnosni protokoli
 - kriptografski algoritmi za šifriranje i vjerodostojnost (autentičnost)
 - 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

Zaglavlje za provjera autentičnosti

Authentication Header (AH)

- jamstvo da je primljeni datagram odaslan s izvorišne IP-adrese:
 - autentičnost izvora IP-datagrama,
- jamstvo da podaci nisu mijenjani pri prolasku kroz mrežu:
 - integritet podataka – IP-datagram nije mijenjan tijekom prijenosa

Zaglavlje za sigurnosno ovijanje podataka

Encapsulating Security Payload Header (ESP)

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

IPsec, transportni i tunelski način rada

izvorni IP-datagram

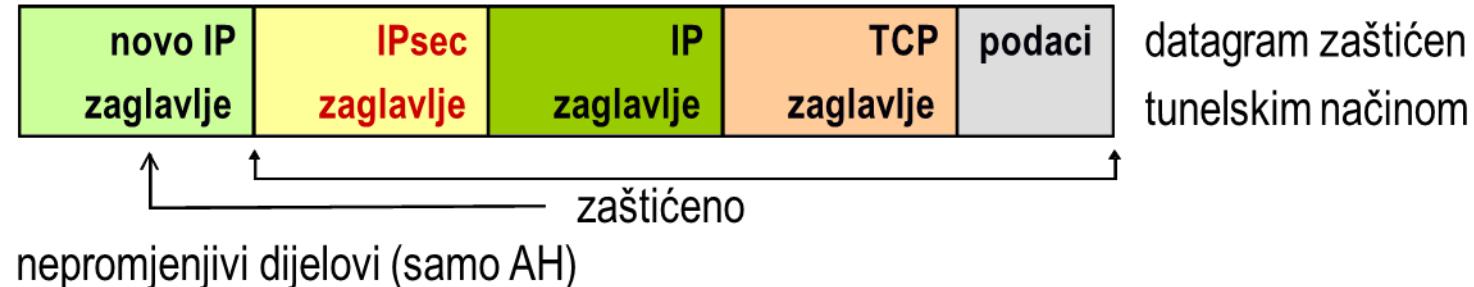


Transportni način: štiti podatke protokola viših slojeva (od transportnog na više)

datagram zaštićen
transportnim načinom



Tunelski način: štiti cijeli izvorni IP-paket



Sadržaj predavanja

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

Adresni prostor

- **Duljina IPv6-adresa je 128 bitova**
 - usporedba broja mogućih adresa:
 - IPv4: 2^{32} , odn. 4 294 967 296
 - IPv6: 2^{128} , odn. 340 282 366 920 938 463 463 374 607 431 768 211 456
- obilježja adresnog prostora IPv6:
 - 655 570 793 348 866 943 898 599 adresa za 1 m² površine Zemlje
 - omogućuje stvaranje domena koje odražavaju današnju topologiju Interneta, jer 128 bita dozvoljava višestruke razine hijerarhije i fleksibilnost
 - učinkovitije usmjeravanje, jer je omogućeno združivanje (agregaciju) adresa u hijerarhije mreža, davatelja usluga, korporacija, zemljopisnih područja i druge

Zapis adresa

- notacija: 8 grupa po 4 heksadekadske znamenke:
 - npr: EFD1:0989:AB02:7654:C4ED:890B:DE65:1240
- sažimanje okteta :00: → ::
 - npr. 1080:0:0:0:0:8:800:200C → 1080::8:800:200C
 - 0:0:0:0:0:0:1 → ::1
 - 0:0:0:0:0:0:0 → ::

dvije dvotočke (::) smiju se upotrijebiti **samo jednom** u adresi

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

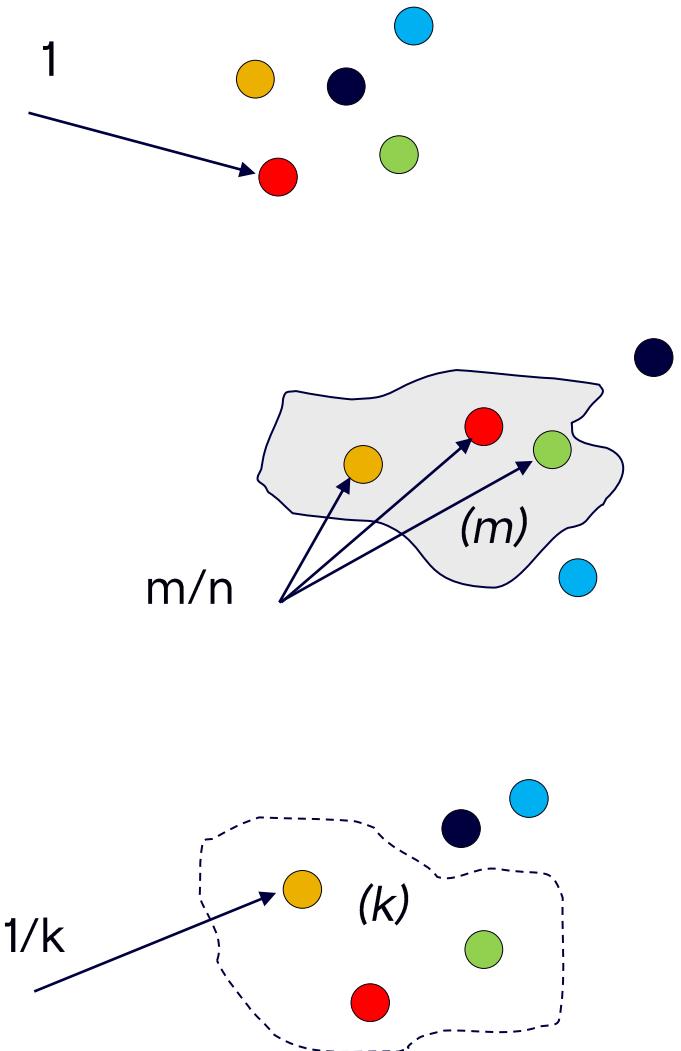


ZAŠTO?

- kao i kod IPv4, i IPv6-adrese imaju mrežni i računalni dio
prefiksni zapis: ip-adresa/prefiks
12AB:0:0:CD30::/60

Vrste IPv6 adresa (1)

- **Unicast – jednoodredišna adresa**
 - identificira jedno sučelje računala/čvora
 - globalna i lokalna adresa
- **Multicast – višeodredišna adresa**
 - određuje skup sučelja (obično na različitim čvorovima)
 - paket se dostavlja svim sučeljima određenima tom *multicast* adresom
- **Anycast – adresa više sučelja, dostava jednom iz skupa sučelja**
 - paket se dostavlja se samo jednom ("*najbližem*") sučelju od onih s tom *anycast* adresom



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 jednoodredišnjog raspona | |

Posebne IPv6-adrese

- **nespecificirana (*unspecified*) adresa**
 - 0:0:0:0:0:0 ili :: (naznačuje da nema adresu)
 - ekvivalentno adresi 0.0.0.0 u IPv4
 - primjena: izvorišna adresa paketa kojima se provjerava jednoznačnost tražene adrese (npr. kod autokonfiguracije).
 - ne smije se dodijeliti mrežnom sučelju niti koristiti kao odredišna adresa.
- **povratna (*loopback*) adresa**
 - ::1
 - ekvivalent adresi 127.0.0.1 u IPv4
 - omogućuje čvoru da šalje podatke sam sebi (npr. testiranje)
 - paketi adresirani na povratnu adresu ne smiju se poslati na poveznicu

Višeodredišna adresa (*multicast*)



Paketi se dostavljaju **svim sučeljima** unutar grupe definirane adresom (*Group ID*)

- F - zastavica (*flag*), zastavica *Transient*:
 - T = 0, trajno dodijeljena *multicast* adresa
 - T = 1, privremeno dodijeljena *multicast* adresa
- S – doseg (*scope*), označava doseg adrese:
 - sučelje (*interface-local*), poveznica (*link-local*), globalno (*global*)
- posebne adrese koriste se za definiranje čvorova i usmjeritelja dosega sučelja i poveznice te druge primjene

Lokalna jednoodredišna adresa (*link-local unicast*)



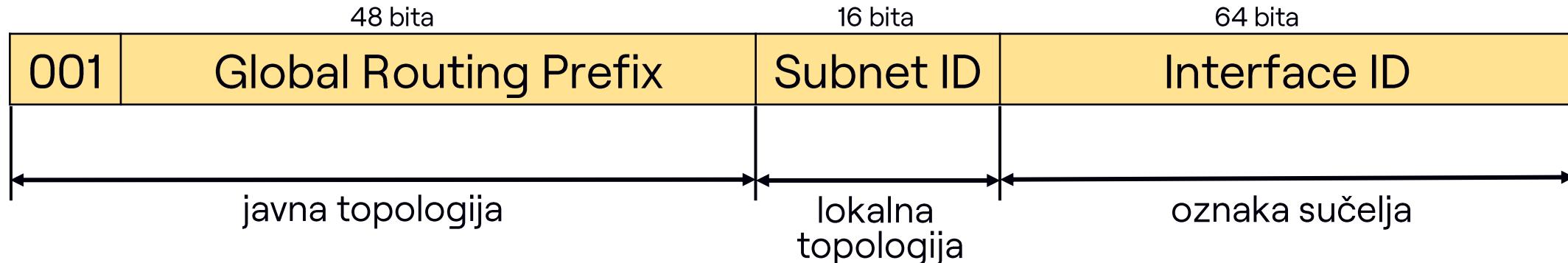
Za komunikaciju čvorova na istoj poveznici*:

- konfiguiraju se automatski
- IPv6-usmjeritelj ne prosljeđuje pakete s *link-local* adresom izvan poveznice
- potrebne za otkrivanje susjednih čvorova (Neighbor Discovery)

Prefiksni zapis = ?

*čvorovi ne komuniciraju putem usmjeritelja

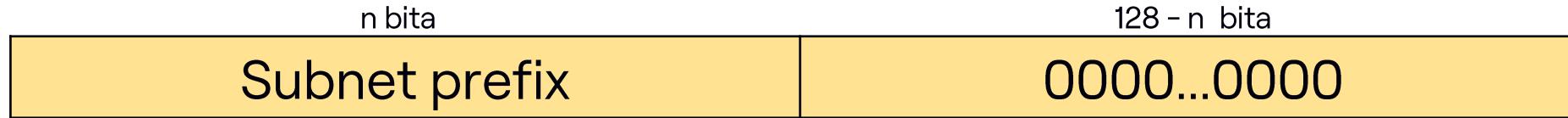
Globalna jednoodredišna adresa (*global unicast*)



Javna globalno dostupna jedinstvena adresa:

- **001** – format prefiksa (*format prefix*)
- **globalni prefiks usmjeravanja** (*Global Routing Prefix*) – identifikator organizacije – davatelja internetske usluge
- **identifikator podmreže** (*Subnet ID*) – identifikator podmreže u okviru organizacije
- **identifikator sučelja** (*Interface ID*) – u IEEE EUI-64 formatu

Adresa jednog iz skupa sučelja (anycast)



Paketi se dostavljaju „najbližem“ iz adresirane grupe sučelja

- mjera „bliskosti“ je broj skokova
- adresa *Subnet-Router anycast* dodjeljuje se usmjeriteljima (svakom sučelju za podmrežu u kojoj se nalazi. Ta je adresa jednaka prefiksu podmreže (*Subnet prefix*) u *unicast* adresi, sa svim ostalim bitovima postavljenima u 0.
- adresa *Subnet-Router anycast* omogućuje komunikaciju s jednim od usmjeritelja u podmreži.

Dodjela IPv6 adrese

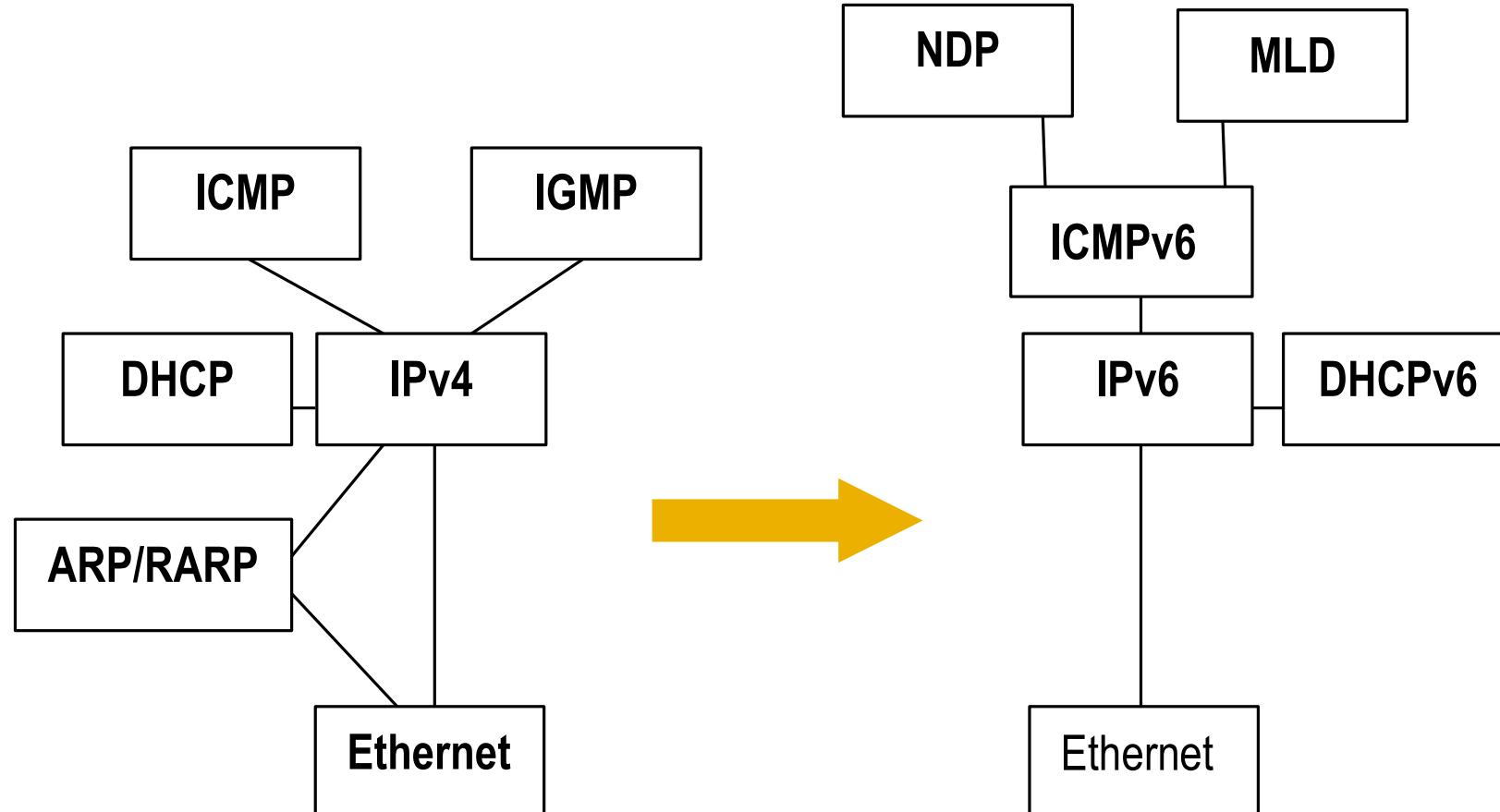
- **Dva mehanizma autokonfiguracije:**
- samostalna (bez poslužitelja) autokonfiguracija adrese (stateless)
 - zasnovana na MAC adresi predočenoj EUI-64-bitnim brojem (izведен iz eternetske 48 bitne adrese); primjena protokola **Neighbor Discovery Protocol (NDP)**
- autokonfiguracija s poslužiteljem (statefull)
 - koristi se poslužitelj **Dynamic Host Configuration Protocol for IPv6 (DHCPv6)**
 - uz samu IPv6-adresu, omogućena je potpuna i konfiguracija za TCP/IP

Upravljački protokoli!

Sadržaj predavanja

- Mrežni sloj i mrežni protokol IPv4 ukratko
- Glavne značajke protokola IPv6
- Format datagrama, osnovno i dodatna zaglavlja
- Adresiranje
- **Upravljački protokoli**
 - ICMPv6 (Internet Control Message Protocol for IPv6)
 - NDP (Neighbor Discovery Protocol)
 - DHCPv6 (Dynamic Host Configuration Protocol for IPv6)

Upravljački protokoli za IPv6 (1)



Podsjetimo se



pa uočimo razliku!

Upravljački protokoli za IPv6 (2)

- ***Internet Control Message Protocol for IPv6 (ICMPv6)***
 - slično kao kod IPv4; služi za dojavu pogrešaka i dijagnostiku (npr. ICMPv6 "ping")
 - prenosi poruke za protokole NDP i MLD
- ***Neighbour Discovery Protocol (NDP)***
 - zamjenjuje protokol Address Resolution Protocol (ARP) iza IPv4 i proširuje njegovu funkcionalnost
- ***Multicast Listener Directory (MLD)***
 - zamjenjuje Internet Group Management Protocol (IGMP) za IPv4 i proširuje njegovu funkcionalnost
 - višeodredišno usmjeravanje i komunikacija obrađuju se u predmetu „Višemedijske komunikacije“
- ***Dynamic Host Configuration Protocol for IPv6 (DHCPv6)***
 - protokol za autokonfiguraciju adrese pomoću poslužitelja – slično kao kod IPv4, DHCPv6 poslužitelj dinamički dodjeljuje IPv6 adresu i pruža druge konfiguracijske informacije

Protokol ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6)

- IP je jednostavan protokol koji nema mogućnost dojave pogreške – to za njega radi ICMP (“dijagnostika” u IP-mreži)
- ICMPv6 proširuje funkcionalnost ICMPv4
- ICMPv4 i ICMPv6 nisu međusobno kompatibilni
- Vrste poruka:
 - poruke o pogreškama (odredište nedostupno, prevelik paket, istek vremena, problem s parametrima)
 - informativne poruke (echo request, echo replay) – IPv6 ping
 - specifične poruke vezane uz druge protokole (npr. NDP, MLD)
- Primjena vezana uz fragmentiranje:
 - Određivanje MTU-puta (Path MTU Discovery)

Protokol ICMPv6: određivanje MTU-puta

- IPv6 propisuje minimalni MTU od 1280 okteta
- datagrami se mogu fragmentirati samo na izvoru i sastavljati na odredištu: **MTU-puta = MTU-poveznice_{min}**
- Postupak:
 1. izvor šalje datagram veličine MTU vlastite poveznice
 2. usmjeritelj na putu proslijedi datagram ako nije veći od MTU-poveznice po kojoj ga šalje, inače ga **odbacuje** i izvoru vraća **ICMPv6** poruku „prevelik paket“ s informacijom o njegovom MTU-poveznice (prihvatljiva veličina paketa)
 3. izvor po primitku poruke „prevelik paket“ smanjuje veličinu paketa na novu vrijednost MTU i šalje paket takve veličine. Postupak 2 - 3 se ponavlja sve dok paket ne stigne na odredište. Time je određen **MTU-puta**.

Protokol NDP

NDP (*Neighbour Discovery Protocol*)

- upravljački protokol – preuzima i proširuje funkcije protokola ICMP i ARP iz IPv4 i definira nove poruke ICMPv6
- „susjedi” – čvorovi (računala i usmjeritelji) na istoj poveznici
- „otkrivanje susjeda” – poruke i procesi kojima se određuje odnos susjednih čvorova
- osigurava funkcije na lokalnoj poveznici
 - za sve čvorove: razlučivanje adrese (IP-adresa – MAC-adresa, otkrivanje duplicitne adrese, dostupnosti čvora i sljedećeg skoka)
 - za računala: otkrivanje usmjeritelja, mrežnog prefiksa i parametara, autokonfiguracija adrese, preusmjeravanje
 - za usmjeritelje: oglašavanje prisutnosti

Funkcije protokola NDP (1)

- **Razlučivanje adrese** (*address resolution*) – za otkrivanje MAC-adrese na temelju poznate IP sučelja (odgovora ARP-zahtjevu u IPv4)
- **Otkrivanje duplicitne adrese** (*duplicate address detection*) – provjera koristi li se već IP-adresa u istoj mreži
- **Provjera dostupnosti** (*neighbor unreachability detection*) – određivanje dostupnosti susjednog čvora
- **Određivanje sljedećeg skoka** (*next-hop determination*) – određuje slanje datagrama na temelju odredišne adrese datagrama
- **Preusmjeravanje** (*redirect*) – usmjeritelj informira računalo o boljem putu do određenog odredišta

Funkcije protokola NDP (2)

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

Napomena: Protokol NDP primjenjuje se i za pokretni IPv6 (*Mobile IPv6*).

Poruke protokola NDP

| | | |
|---|-------------------------------|----------------------------|
| IPv6 zaglavje slj. zag. = 68 (ICMPv6) | ND zaglavlje poruke | ND opcije poruke |
|---|-------------------------------|----------------------------|

Vrste poruka ICMPv6:

- traženje/pobudživanje usmjeritelja (*Router Solicitation*)
- oglašavanje usmjeritelja (*Router Advertisement*)
- traženje/pobudživanje susjeda (*Neighbour Solicitation*)
- oglašavanje susjeda (*Neighbour Advertisement*)
- preusmjeravanje (*Redirect*)

Adresiranje poruka ICMPv6:

- zahtjevi za nekom funkcijom - višeoodredišno (*multicast*)
- odgovori - jednoodredišno (*unicast*)

NDP: otkrivanje usmjeritelja

- računalo, nakon spajanja na mrežu, treba otkriti adresu najbližeg usmjeritelja
- usmjeritelj se periodički oglašava porukom *Router Advertisement* kojom dojavljuje svoju IP-adresu i druge parametre adresirajući sve čvorove u dosegu (*multicast*)
- računalo, da ne bi čekalo oglašavanje, može adresirati sve usmjeritelje u dosegu (*multicast*) porukom *Router Solicitation* koji će se odazvati s *Router Advertisement* samo tom računalu (*unicast*)

NDP: samostalna autokonfiguracija IP-adrese (1)

Autokonfiguracija bez poznavanja stanja (*stateless*):

- u mrežama bez poslužitelja DHCPv6

Postupak:

1. Jednoznačno adresiranje čvora na lokalnoj poveznici (*link-local unicast*): IPv6 adresa izvedena iz EUI-64 fizičke adrese (MAC-adrese)
2. Provjera jedinstvenosti adrese
3. Određivanje načina autokonfiguracije i parametara za autokonfiguraciju globalne adrese



NDP: samostalna autokonfiguracija IP-adrese (2)

Provjera jedinstvenosti adrese:

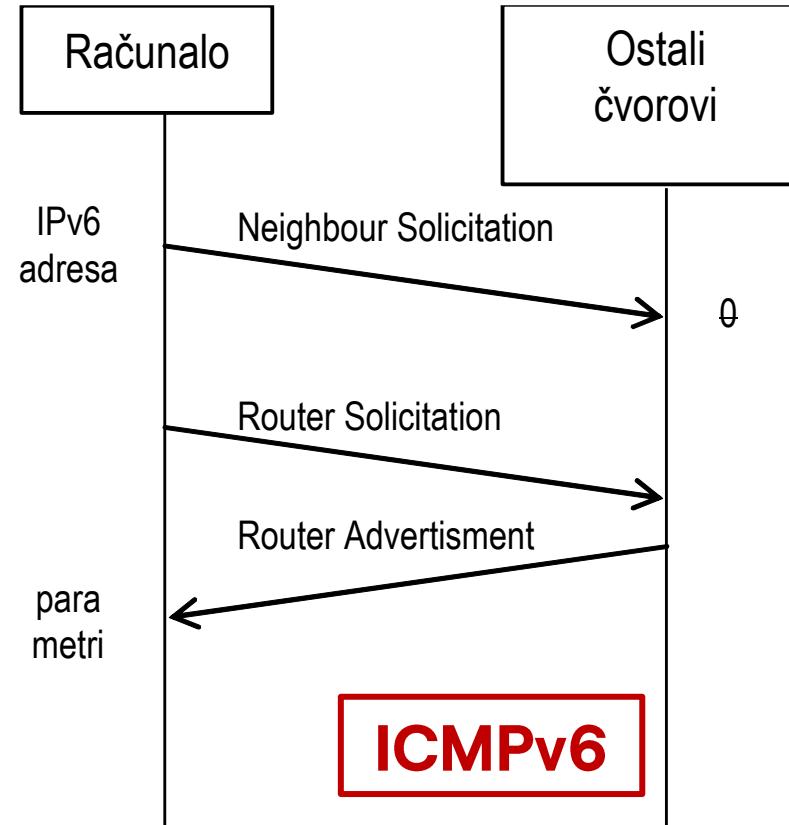
- računalo šalje višeoodredišnu poruku *Neighbour Solicitation*
- ako se neki drugi čvor odazove na tu adresu porukom *Neighbour Advertisement* koja označava duplicitanu adresu, autokonfiguracija nije moguća i prekida se – prelazi se na ručnu konfiguraciju (mrežni administrator)
- ako je adresa jedinstvena, računalo je spojeno na mrežu i omogućeni su prijam/predaja paketa na lokalnoj poveznici

NDP: samostalna autokonfiguracija IP-adrese (3)

Određivanje načina autokonfiguracije i informacije za autokonfiguraciju:

- računalo otkriva poslužitelja koji određuje način autokonfiguracije
 - autokonfiguracija s poznavanjem stanja s poslužiteljem DHCPv6 (*stateful*)
 - autokonfiguracija bez poznavanja stanja
- za autokonfiguraciju bez poznavanja stanja dostavlja potrebne parametre
- ako se usmjeritelj ne oglašava, preostaje autokonfiguracija putem poslužitelja DHCPv6

NDP: samostalna autokonfiguracija IP-adrese (3)



Uspješna samostalna autokonfiguracija adrese:

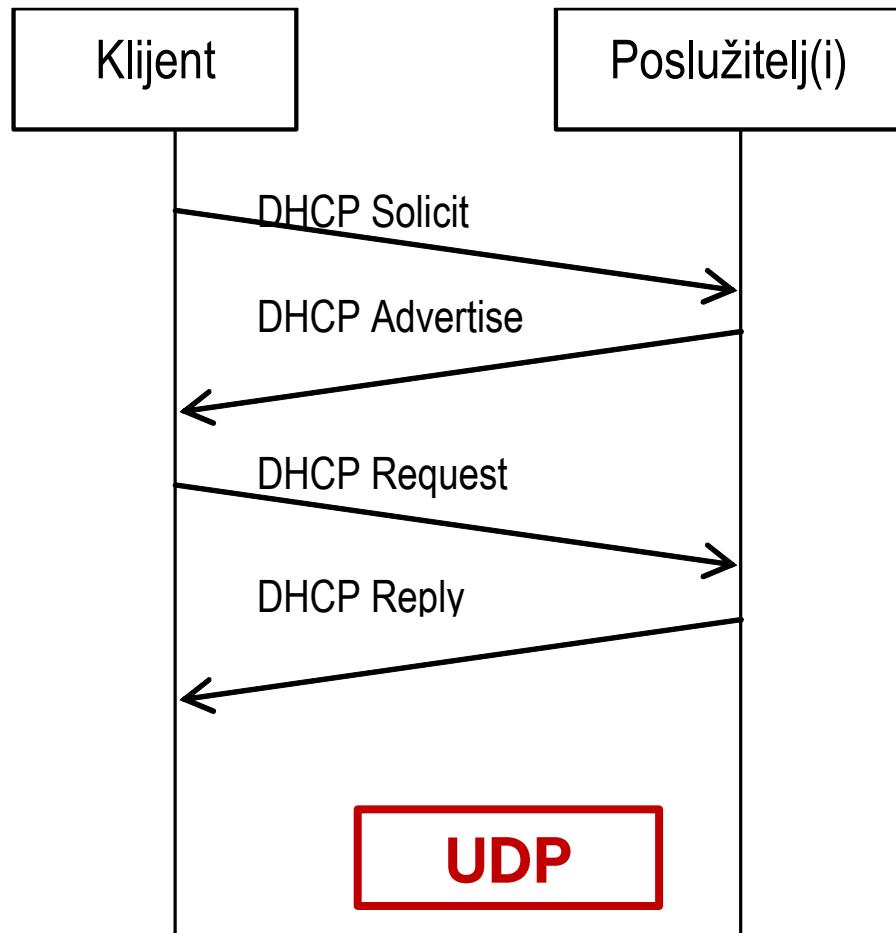
- Jedinstvena lokalna adresa na poveznici
- Usmjeritelj određuje način autokonfiguracije bez poznavanja stanja i dostavlja potrebne parametre

Protokol DHCPv6

Dynamic Host Configuration Protocol v6 (DHCPv6)

- autokonfiguracija adrese s poznavanjem stanja
- protokol klijent–poslužitelj koji omogućuje računalu (DHCPv6-klijent) dobivanje konfiguracijskih parametara od poslužitelja (DHCPv6-poslužitelj)
- transport poruka između klijenta i poslužitelja: UDP
- zasniva se na mogućnostima IPv6:
- višeodredišno adresiranje DHCPv6-poslužitelja 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)

Protokol DHCPv6 (3)

Uz navedene poruke, primjenjuju se još dvije:

- **DHCP Release**: otpuštanje nekih dobivenih parametara, npr. adresu koju više neće koristiti
- **DHCP Reconfigure**: promjena nekih parametara

Zadaci (1)

- Istražite stanje primjene protokola IPv6 u svijetu i Hrvatskoj te pripremljenost web-sjedišta za rad s IPv6.
- Istražite internetski promet, podatke o broju korisnika i korištenju karakterističnih vrsta usluga (pretraživanje, trgovanje, društveno umrežavanje, ...)
- Izmjerite brzinu fiksnog pristupa Internetu u svojem stanu/studentskom domu u karakterističnim dijelovima dana u kojima se može očekivati/prepostaviti različit intenzitet internetskog prometa.
- Istražite napade na internetski promet i usluge.

Zadaci (2)

- Usporedite protokole IPv4 i IPv6 s obzirom na funkcionalnost i performanse.
- Što će se dogoditi IPv6-datagramu ako tijekom prijenosa smetnje izazovu pogrešku jednog bita u odredišnoj adresi?
- Kako se provodi fragmentacija za protokol IPv6 i kako se ustanavlja najveća dopuštena duljina fragmenta?
- Navedite i objasnite razloge zbog kojih protokol IPv6 omogućuje učinkovitije usmjeravanje u mreži u odnosu na sadašnje stanje koje je proizašlo iz načina adresiranja i usmjeravanja te dodjele IPv4–adresa.
- Kakve su vrste adresa podržane protokolom IPv6?

Zadaci (3)

- Koje su zadaće protokola NDP?
- Navedite primjer autokonfiguracije IPv6 bez poznavanja stanja (*stateless*) i objasnите kako se provodi.
- Navedite primjer autokonfiguracije IPv6 s poznavanjem stanja (*stateful*) i objasnите kako se provodi.
- Zašto se u protokolu DHCPv6 primjenjuje višeodredišno adresiranje?