

Petrijeve mreže

- **Konačni automat** je osnovni model koji se primjenjuje u analizi i sintezi telekomunikacijskih procesa, i to za opis i istraživanje komunikacije i koordinacije procesa.
- Pojam **Petrijeve mreže** odnosi se na mrežu mjesta i prijelaza u kojoj mjesta imaju značenje uvjeta, a prijelazi događaja u smislu definicije sustava uvjeta i događaja. Za razliku od modela automata izravno se upotrebljava pojam uvjeta, a pojam stanja definira se kao skup istodobno ispunjenih uvjeta što omogućuje detaljniji opis pojedinog procesa i dopušta njihovo međusobno povezivanje.
- **Ograničenost** - Odnosi se na pojam maksimalnog broja oznaka u mjestu mreže.
- **Sigurnost** - Određuje da broj oznaka u svakome mjestu ne smije biti veći od jedan, odnosno da svaki uvjet može biti samo ispunjen ili neispunjen.
- **Aktivnost** - Odnosi se na mogućnost izvedbe prijelaza. Aktivna mreža isključuje mogućnost blokiranja ili potpunog zastoja u modeliranom sustavu koji se manifestira postojanjem prijelaza koji se nikad ne izvodi ili stanja u kojemu se ne može izvesti nijedan prijelaz.
- **Reverzibilnost** - Petrijeva mreža je reverzibilna ako se iz svakog stanja može vratiti u početno stanje μ , odnosno ako je početno stanje dostupno iz svakog stanja.
- **Konzervacija** oznaka - Odnosi se na zadržavanje jednakoga, početnog, broja oznaka u svim stanjima mreže.
- **Konfliktnost i simultanost** prijelaza - Dva osnovna odnosa prijelaza u nekom stanju mreže opisana su konfliktnom i simultanom izvedbom. Prijelazi ti i tj su konfliktni ako i samo ako postoji stanje μ u kojemu se oba prijelaza mogu izvesti. Prijelazi ti i tj su simultani ako postoji stanje μ u kojemu se oni mogu izvesti, a izvedba jednoga ne utječe na izvedbu drugoga.
- **Perzistentnost** - Petrijeva mreža se naziva perzistentnom ako prijelaz koji se može izvesti gubi uvjete samo vlastitom izvedbom. Perzistentnost ima značenje odsutnosti konflikta u procesu izvedbe mreže.

5. predavanje - mrežni protokol IPv6

IPv4

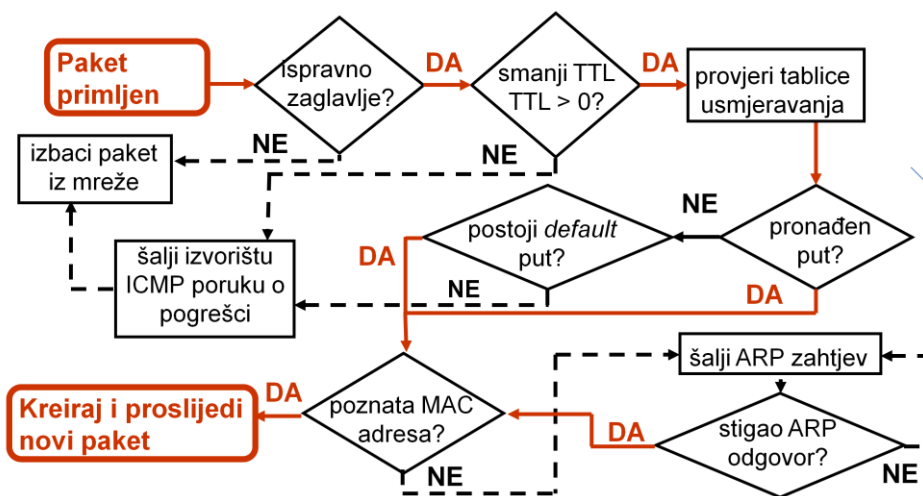
- Glavne odlike:
 - neovisan o nižim protokolima
- Mogući problemi:
 - datagramski način rada
 - nespojna usluga bez potvrde
 - nema mehanizama kontrole toka
 - nema jamstva za očuvanje
 - gubitak paketa zbog greške na poveznici ili zagušenja u čvoru
 - poremećen redoslijed paketa
 - veće kašnjenje u slučaju retransmisije s kraja na kraj
 - pošiljatelj nema povratnu informaciju
- Uloge u protokolnom složaju TCP/IP:
 - Omatanje - IP prihvaća podatke od višeg sloja (transportni sloj), stavlja ih u podatkovno polje IP datagrama, te ih isporučuje protokolu nižeg sloja (sloj podatkovne poveznice).
- Funkcionalnost:
 - 1) definira shemu adresiranja u internetu
 - 2) definira provedbu fragmentacije
- IP-adresiranje:
 - **IP adresa 32 bita (IPv4)** - identifikator koji globalno i jednoznačno određuje mrežno sučelje
 - dva dijela:
 - 1) identifikator mreže - NetID
 - 2) identifikator krajnjeg računala - HostID
- Rezervirane i zauzete adrese:
 - a) Povratna adresa (loopback)
 - koristi se za testiranje izvedbe TCP/IP
 - 127.0.0.0 do 127.255.255.255 (127.0.0.0/8), najčešće 127.0.0.1
 - datagram se ne predaje dalje, sloju podatkovne poveznice, već se vraća unatrag u mrežnom sloju.
 - b) Razašiljanje svima (broadcast)
 - 255.255.255.255
 - sva računala u lokalnoj mreži primaju
 - c) Identifikacija vlastite mreže
 - 0.0.0.0/8
- Prefiksni prikaz - besklasno adresiranje:
 - ne uzima u obzir klase adresa, već putevi usmjeravanja idu prema mrežnom prefiksu iza adrese (označava koliko bitova zauzima mrežni dio adrese)
 - granica mrežnog i računalnog dijela može biti na bilo kojem dijelu adrese (ne samo na granici okteta kao kod klasa)

- Fragmentacija:

- datagram mora stati u podatkovno polje okvira sloja podatkovne poveznice (MTU)
- ako ne stane, fragmentira se
- fragmentaciju provodi usmjeritelj na izvoru, a datagram se sastavlja tek na odredištu
- mane fragmentacije:
 - ako se izgubi jedan fragment, propada cijeli datagram
 - više kontrolnih podataka za istu korisnu informaciju
- zastavice:
 - R - rezervirano
 - DF - don't fragment
 - MF - more fragments

- Usmjeravanje:

- ako su čvorovi u istoj (pod)mreži, onda komuniciraju direktno, a u suprotnom preko usmjeritelja



- ICMP protokol:

- služi za dijagnostiku za IP protokol
- definira mehanizam kojim se prenose dvije vrste kontrolnih poruka:
 - 1) dojave o grešci
 - 2) zahtjevi za informacijom

- Ograničenja IPv4:

- broj raspoloživih adresa je 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.

IPv6

- Novosti i poboljšanja:

- veći adresni prostor (128-bitne adrese)
- jednostavnije zaglavlje
- unaprijeđeno usmjeravanje
- označavanje tokova
- bolja podrška za prijenos podataka u stvarnom vremenu
- provjera autentičnosti, zaštita privatnosti, integritet podataka, povjerljivost
- bolja potpora za pokretljivost

- **Zaglavlja u IPv6:**

1. zaglavlje IPv6 → obvezno!!!
 2. zaglavlje skok po skok
 3. zaglavlje namijenjeno odredištu (1)
 4. zaglavlje usmjeravanja
 5. zaglavlje fragmenta
 6. zaglavlje za provjeru autentičnosti
 7. zaglavlje za sigurnosno ovijanje podataka
 8. zaglavlje namijenjeno odredištu (2)
- zaglavlje transportnog sloja

- *2. zaglavlje skok po skok:*

- zaglavlje varijabilne duljine, koje sadrži informaciju namijenjenu svakom čvoru na putu dostave datagrama
- sadrži informacije o duljini zaglavlja, koje je sljedeće zaglavlje, te akciju koju treba poduzeti čvor

- *3. i 8. zaglavlje namijenjeno odredištu:*

- (1) → za prvi sljedeći čvor i za sve ostale čvorove koje sadrži zaglavlje usmjeravanja, a koji se smatraju odredištima
- (2) → samo za krajnje odredište
- definicija ista kao i za skok po skok

- *4. zaglavlje usmjeravanja:*

- sadrži podatke o veličini zaglavlja, sljedećem zaglavlju, vrsti usmjeravanja, te popis čvorova koje datagram treba proći na putu do odredišta

- *5. zaglavlje fragmenta:*

- fiksna duljina
- sadrži:
 - podatke o sljedećem zaglavlju
 - polje koje pokazuje kojem dijelu originalnog paketa pripada taj fragment
 - bit MF koji prikazuje da li ima još fragmenata ili je to zadnji (0 - zadnji, 1 - ima ih još)
 - identifikacijski dio koji sadrži adrese izvorišta i odredišta

- *6. zaglavlje za provjeru autentičnosti (AH):*

- jamči identitet pošiljatelja, te da poruka nije mijenjana u prijenosu

- *7. zaglavlje za sigurnosno ovijanje podataka (ESP):*

- osigurava privatnost podataka i integritet datagrama

- mehanizmi zaštite (šifriranje i dešifriranje):
 - a) transport-mode - nad podacima transportnog sloja
 - b) tunel-mode - nad cijelim paketom
- privatnost osigurava: na odredištu se provodi dešifriranje na temelju ESP zaglavlja, pa samo legitimni pošiljalac može pročitati
- ako se radi tunel-mode, mora se dodati dodatno IP zaglavlje, kako bi usmjerenik mogao procesirati paket

- Zapis adresa IPv4 - IPv6

- IPv4 - 4 grupe po 8 binarnih znamenaka zapisanih dekadski (161.53.19.201)
- IPv6 - 8 grupa po 4 hex znamenke, odvojeno dvotočkama
- IPv4 → IPv6 - **samo 1 niz nula** zamijenimo s dvije dvotočke (::), eventualno dekadski promijenimo u hex.
(::A135:13C9 ili ::161.53.19.201)

- Vrste adresa - IPv6:

- 1) Unicast - jednodređena
 - adresira jedno sučelje računala / čvora
 - a) globalne → u javnom internetu
 - b) lokalne → na razini organizacije → za organizacije koje nisu fizički spojene na internet, a koriste TCP/IP
 - c) lokalne na razini podatkovne poveznice → izvode se iz MAC adrese, dodavanjem prefiksa FE80::
 - d) posebne (nespecificirane, loopback, kompatibilne)
- 2) Multicast - višedređena adresa (slanje na više odredišta, ne na sva)
- 3) Anycast - adresa više sučelja, dostava jednom sučelju

- Dodjela IPv6 adrese:

- autokonfiguracija - stvaranje lokalne adrese na razini poveznice i provjera njene jedinstvenosti
- utvrđivanje informacija treba samostalno konfigurirati
- ako se konfiguriraju adrese:
 - a) autokonfiguracija bez poslužitelja:
 - na temelju MAC adrese
 - b) autokonfiguracija sa poslužiteljem:
 - DHCPv6 poslužitelj

- Kontrolni protokoli za IPv6:

- ICMPv6 (NDP, MLD), DHCPv6

- ICMPv6:

- proširuje funkcionalnost ICMPv4 (pogreške i dijagnostika), sa kontrolnim funkcijama za višedređeno slanje (sad su u MLD)
- vrste poruka:
 - o pogrešci
 - IPv6 ping
 - pripadnost grupi
 - za samokonfiguraciju i otkrivanje susjeda (NDP)

- NDP:

a) otkrivanje između računala i usmjeritelja:

- otkrivanje usmjeritelja
- otkrivanje prefiksa
- otkrivanje parametara
- autokonfiguracija adrese

b) komunikacija između računala

- razlučivanje adrese (MAC)
- određivanje sljedećeg skoka
- provjera dostupnosti susjednog uređaja
- provjera dvostruke adrese

c) funkcija redirect → usmjeritelj informira računalo o boljem putu do nekog odredišta

- DHCPv6:

- omogućuje klijentu dobivanje parametara od poslužitelja
- transport poruka se vrši preko UDP protokola
- zasniva se na dvije mogućnosti IPV6:
 - lokalna adresa na razini poveznice, koju formira samo računalo
 - višeodredišno adresiranje DHCPv6 poslužitelja i njihovih posrednika

6. predavanje - Pokretljivost u IP mreži, Uvođenje IPv6 u mrežu

Pokretni IPv4 (Mobile IPv4)

- u klasičnom internetu je promjena priključne točke moguća samo ako računalo promijeni i IP adresu.

• Adrese:

a) domaća adresa

- ne mijenja se za čvor, vrijedi i u domaćoj i u posjećenoj točki priključka
- izvorišna adresa datagrama koje šalje pokretni čvor

b) trenutna adresa (care-of)

- ne mijenja se za priključnicu
- odredišna adresa za datagrame koje prima pokretni čvor
- trenutna adresa posredstvom stranog agenta
 - IP adresa stranog agenta
 - njen mrežni prefiks mora odgovarati mrežnom prefiksu stranog linka
 - nju može koristiti više pokretnih čvorova istovremeno
- mjesna trenutna adresa
 - IP adresa privremeno pridružena sučelju pokretnog čvora na stranom linku
 - mrežni prefiks mora odgovarati mrežnom prefiksu stranog linka
 - samo jedan MN istovremeno

• Funkcijski entiteti:

1) MN - pokretni čvor

- čvor koji mijenja točku priključka s jednog linka na drugi i pritom koristi svoju domaću adresu

2) HA - domaći agent

- usmjeritelj sa sučeljem na domaćem linku MN-a
- MN ga obavještava o svojoj trenutnoj točki priključka / IP adresi
- omogućuje usmjeravanje prema domaćoj adresi MN-a
- preusmjerava datagrame poslane na domaću adresu MN-a prema njegovoj trenutnoj adresi

3) FA - strani agent

- usmjeritelj na linku gdje je MN povezan na trenutnu točku priključka
- javlja HA-u trenutnu adresu MN-a
- usmjerava datagrame ka/od MN-a

4) CN - čvor sugovornik (Corresponding Node)

• Procedure MN-a:

1) otkrivanje agenta

- utvrđuje je li spojen na domaći ili strani link
- je li promijenio link
- dobiva trenutnu adresu
- poruke (ICMP):
 - AA (Agent Advertisement) - usmjeritelj redovito šalje na linkove gdje može služiti kao HA ili FA
 - AS (Agent Solicitation) - čvor želi potaknuti usmjeritelja na AA

- Utvrđivanje promjene poveznice:
 - MN može pretpostaviti da je promijenio poveznicu (link) ako:
 - u vremenu određenom lifetime poljem ne dobije AA od agenta koji ga je dotad posluživao
 - usporedbom mrežnog prefiksa (iz Router Address i Prefix) drugog AA sa svojim, shvati da je promijenio link
 - dva slučaja pri promjeni agenta:
 - 1) novi agent ima isti mrežni prefiks / na istom je linku kao i stari → ne treba ponovna registracija
 - 2) novi agent ima drugi mrežni prefiks → drugi link → ponovna registracija
- 2) registracija - UDP**
 - REQ - MN šalje registracijski zahtjev s trenutnom adresom preko FA do HA
 - REP - HA prima/odbija registraciju i šalje registracijski odgovor MN-u preko FA
 - registracija moguća i bez FA, pomoću DHCP-a
 - deregistracija:
 - REQ - MN se prijavljuje HA pri povratku u domaću mrežu i time odregistrira trenutnu adresu
 - REP - HA potvrđuje deregistraciju
 - registracijske poruke se štite sa postupkom mobile-home authentication (jamči se autentičnost i integritet)

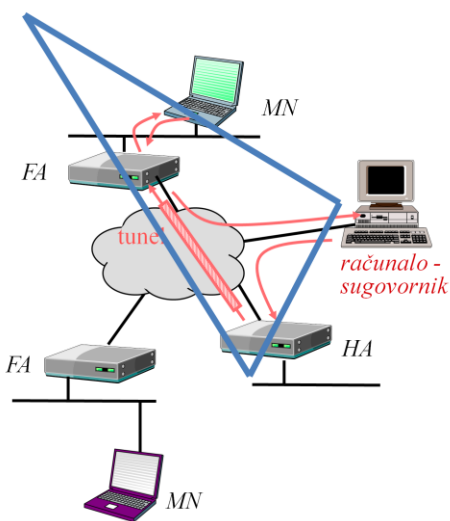
• Slanje datagrama s/na MN

a) slanje na MN:

- HA presreće datagrame upućene na domaću adresu MN-a i tunelira ih do FA
- FA zatim vadi izvorne datagrame iz tuneliranih i daje ih MN-u

b) slanje s MN:

- preko FA direktno na CN
- problem trokutastog usmjeravanja:
- najviše dolazi do izražaja kada su MN i CN blizu, a daleko od HA
 - bolje rješenje bi bilo direktno tuneliranje MN-CN, ali bi to jako povećalo složenost, pa se ne primjenjuje u IPv4
 - u IPv6 je riješeno.



Pokretni IPv6 (Mobile IPv6)

- Razlike u odnosu na Mobile IPv4:

- adresiranje
- nema FA → umjesto njega je IPv6 usmjeritelj
- anycast adresiranje olakšano je komunikacijom s točno jednim HA
- optimizacija puta (rješenje za trokutasto usmjeravanje)
- zaštita podataka u IPv6 (IPsec)

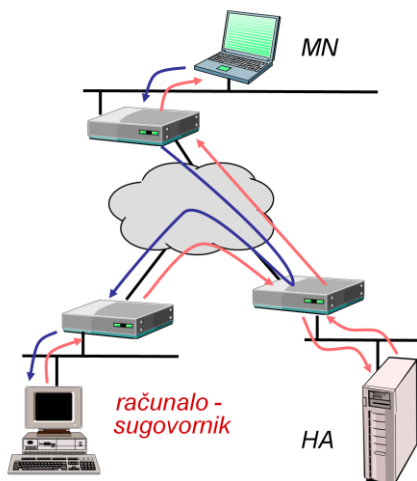
- Način rada:

- 1) MN registrira promjenu priključka
- 2) MN autokonfigurira trenutnu adresu i registrira je kod HA
- 3) HA preusmjerava pakete adresirane na domaću adresu MN-a na njegovu trenutnu adresu (od MN-a)
- 4) ako CN nema podršku za mobilni IPv6, onda se uspostavlja dvosmjerni tunel između MN i CN; u suprotnom se pokreće optimizacija usmjeravanja
- 5) paketi između HA i MN su zaštićeni sa IPsec

→ usmjeritelj se otkriva pomoću NDP

**2) nakon što utvrdi promjenu poveznice, prelazi na autokonfiguraciju i registraciju*

- Autokonfiguracija - rješava se dobivanje trenutne adrese
- Registracija - kao kod MIPv4, samo se preko zaglavlja pokretljivosti prenose Binding poruke (Binding Update, Binding Acknowledgement, Binding Refresh Request - CN zahtijeva Binding Update od MN-a, Home Address - MN šalje poruku o domaćoj adresi)



**4) Optimizacija usmjeravanja:*

- MN šalje CN-u Binding Update sa trenutnom adresom
- paketi se prema MN sad mogu usmjeravati izravno, koristeći zaglavlje pokretljivosti (novo u IPv6)

**5) Zaštita*

- IPsec: AH i ESP zaglavlja: autentičnost, integritet i tajnost

Uvođenje IPv6

- Postizanje kompatibilnosti sa IPv4:

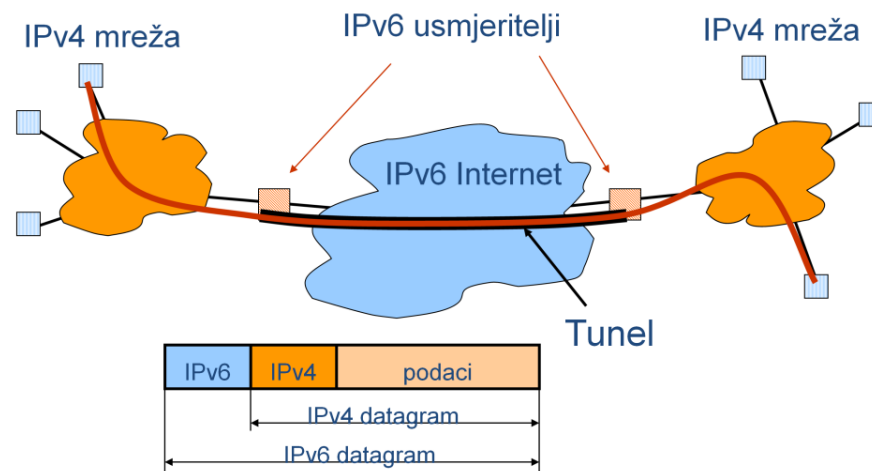
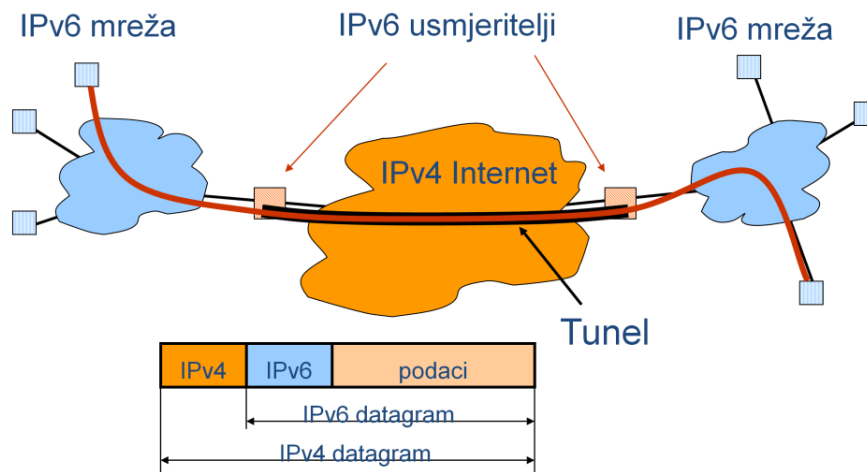
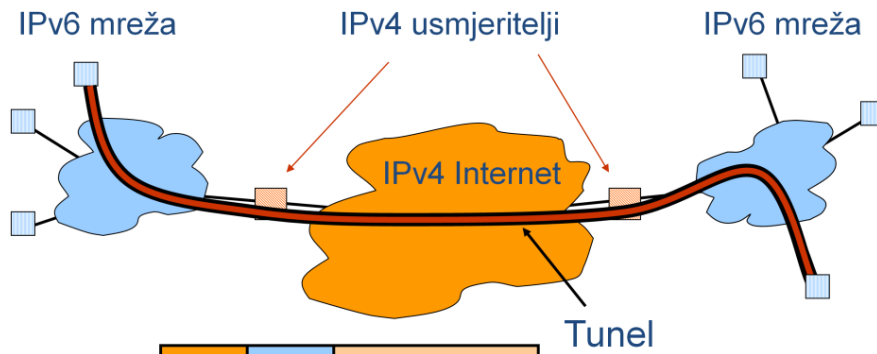
- a) dvostruki IP sloj (IPv6/IPv4 čvor = IPv6 čvor koji sadrži i izvedbu IPv4 protokola za kompatibilnost unatrag)

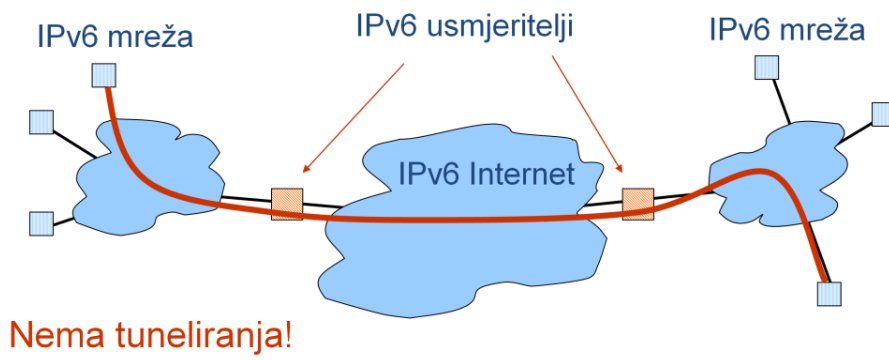
b) tuneliranje

- router to router
- host to router
- router to host
- host to host

c) prevođenje protokola

- pogledati slajdove 49-54

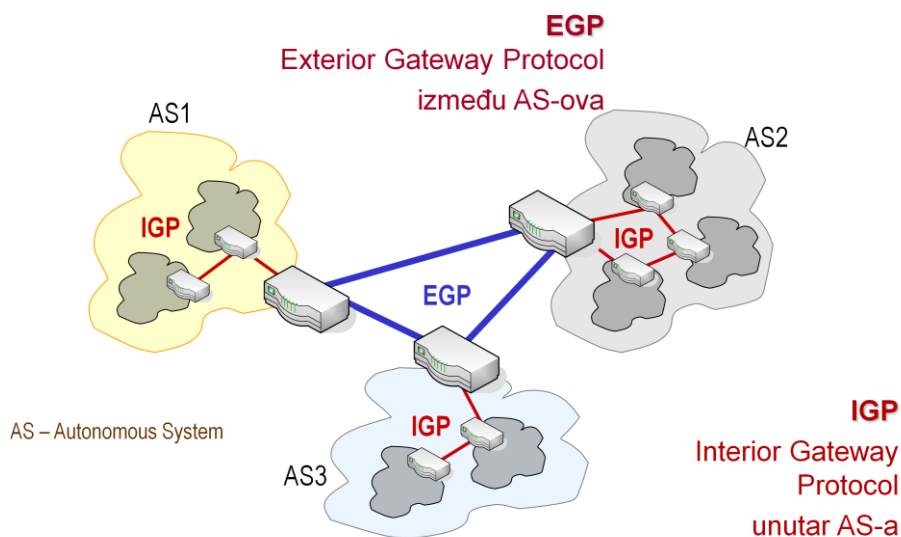




7. predavanje - Protokoli usmjeravanja u Internetu

Protokoli usmjeravanja

- Usmjeravanje:
 - postupak pronalaženja puta i prosljeđivanja paketa od izvorišta do odredišta
 - datagrami mogu putovati različitim putevima
 - usmjeritelj = sustav s minimalno dva različita sučelja u dvije različite mreže, sadrži tablicu usmjeravanja
- Podjela protokola usmjeravanja:
 - s obzirom na područje djelovanja:
 - a) unutar autonomnog sustava - IGP → RIP, OSPF
 - b) između autonomnih sustava - EGP → BGP
 - autonomni sustav - skup usmjeravajućih entiteta koji pripadaju npr. jednom mrežnom operatoru



- Osnovne upravljačke informacije:
 - izvorišna adresa
 - odredišna adresa
 - TTL
- CIDR - routing bez klasa
 - + efikasnije iskorištavanje IP prostora
 - + manje routing tablice
 - veća složenost
- Podjela algoritama usmjeravanja:
 - 1) statički (neadaptivan)
 - 2) dinamički (adaptivan) - RIP, OSPF

RIP

- Glavne odlike:
 - besklasno usmjeravanje
 - ruta sljedećeg skoka
 - autentifikacija
 - multicast usmjeravanje
 - koristi UDP
 - distance-vektor
- Timing:
 - prilikom pokretanja šalje poruku svim susjedima tražeći njihove tablice
 - svoju tablicu šalje svakih 30s
 - svaku promjenu broadcasta
 - ako u 6x30s ne dobije tablicu, postavlja metriku na 16, a nakon još 2x 30s briše rutu
- Ograničenja:
 - ne uzima u obzir stanje linka, samo broj hopova
 - metrika je ograničena na 16 → neprikladno za veće mreže
 - spora konvergencija protokola
 - brojanje u beskonačnost
- Rješenja za brojanje u beskonačnost:
 - split horizon - nikad ne oglašavati rutu na interface s kojeg je dobivena
 - split horizon with poisoned reverse - javiti da je zanemario tu rutu (metrika 16)
 - postaviti hold-down timer 60-12s - u tom vremenu zanemariti bilo kakve nove informacije o ruti
- Rješenje za sporu konvergenciju:
 - triggered update - slati update čim se detektira promjena

OSPF

- Glavne odlike:
 - brza konvergencija
 - CIDR
 - manji promet između routera
 - složeniji od RIPv2
- Osnovne operacije:
 - otkrivanje susjeda
 - izbor nadležnog usmjeritelja (DR) i pomoćnog nadležnog (backup)
 - sinkronizacija tablice usmjeravanja
 - kreiranje/održavanje tablica
 - oglašavanje stanja poveznica (LSA - link state advertisement)
- Hijerarhijsko usmjeravanje - grupiranje u područja (areas), gdje svako područje ima svoj DR i backup DR. Kategorizira se: internal, border, backbone
- Multipath routing - više linkova s istim cost-load balancing
- Identične informacije u svim routerima:

- router posjeduje potpunu sliku mreže - svaki router šalje informacije o stanju poveznica DR-u i backup DR-u
- DR i backup DR primljene informacije šalju svim ostalim routerima s kojima nisu direktno vezani
- Uzima u obzir stanje linka pri računanju costa
- Šalju se samo promjene u tablici, ne cijele tablice
- Podržava autentifikaciju
- Svaki usmjeritelj održava LSDB (link-state database) - informacije o svim routerima s kojima nisu direktno vezani

- Tipovi poruka:
 - Hello - otkrivanje i održavanje susjednih odnosa kod usmjeritelja - šalje se svakih 10s, nakon 40s bez Hello paketa zaključuje prekid veze
 - Database Description - opisuje bazu podataka, poruke se razmjenjuju tijekom inicijalne sinkronizacije
 - Link State Request - poruka kojom se zahtijeva stanje linka
 - Link State Update - poruke kojima se opisuju ili osvježavaju stanja linkova
 - Link State Acknowledgement - poruke kojima se potvrđuje osvježeno stanje linka

- Inicijalna sinkronizacija → razmjena baza podataka:
 - šalju se zaglavlja svih LSA-ova (serijom paketa database description)
 - šalju se zahtjevi svih LSA-ova kojih nema (Link State Request) i odgovori (Link State Update)

- Kontinuirana sinkronizacija:
 - pojavom novih LSA-ova
 - preplavlivanjem
 - počinje kada usmjeritelj želi osvježiti neki od svojih LSA-ova