2. MODELIRANJE KOMUNIKACIJE KONAČNIM AUTOMATOM

KONAČNI AUTOMAT = osnovni model koji se primjenjuje u analizi i sintezi telekomunikacijskih procesa za opis I istraživanje komunikacije i koordinacije procesa

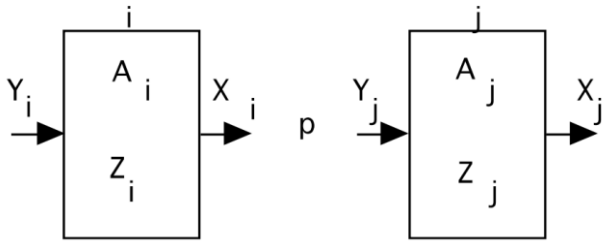
Pi = proces
Ai = automat
Si = skup stanja
Ci = skup uvjeta
Ti = skup prijelaza
Ei = skup događaja
xji = predaja
yki = prijam
zli = unutarnji prijelazi

Dva načina uvođenja kanala u model:

1) kanal se uključi posredno, preko prijelaza vezanih uz prijam i predaju informacijskih jedinica

→ ne dopušta nikakvu obradu informacijske jedinice između predaje i prijama ni djelovanje smetnji.

→ kanalu K(i, j) prodružena su stanja Ks(i, j), a komunikaciji odgovara uređeni slijed događaja: **xpi, Ks (i, j) = p, ypj**

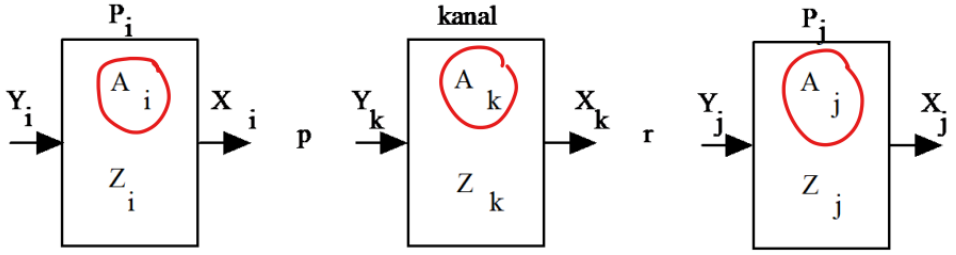


Slika 2.1. Komunikacija između dva automata

2) kanal se modelira automatom Ak kao i sami procesi

→ komunikacija između Pi i Pj opisuje automatima Ai, Ak i Aj preko kanala K (i, k) i K (k, j) uz slijed događaja:

→ xpi, Ks (i, k) = p, ypk, xrk, Ks (k, j) = r, yrj → p = r opisuje komunikaciju bez pogreške, a p ≠ r s pogreškom



Slika 2.2. Komunikacijski kanal modeliran automatom

$$\begin{vmatrix} s_1 & K_S(1,2) & \dots & K_S(1,N) \\ \dots & \dots & \dots & \dots \\ K_S(i,1) & K_S(i,2) & \dots & s_i \\ \dots & \dots & \dots & \dots \\ K_S(N,1) & K_S(N,2) & \dots & s_N \end{vmatrix}$$

→ **MATRICA PRIJELAZA!!!**

Određivanje sljedova prijelaza

M = matrica prijelaza za graf G

mij = element matrice prijelaza M koji sadrži skup svih prijelaza između stanja si i sj

Mi = i-ti redak matrice prijelaza

$Pij^{(k)}$ = skup svih putova između stanja si i sj dužine k

∏ij = $Pij^{(1)}$ skup svih putova između stanja si i sj dužine 1

$P11^{(k)}$ = slijed događaja dužine k

POSTUPAK ODREĐIVANJA SLJEDOVA PRIJELAZA ZA AUTOMAT S n STANJA:

1. odredite M,
2. odredite M' zamjenom elemenata na glavnoj dijagonali od M nulama,
3. k = 1,
4. $M'1^{(k)}$ * M',
5. zamijenite sve neprave cikluse nulom → rezultat je M'1(k+1),
6. k = k+1,
7. za k < n vratite se na 4 , za k = n postupak je završen,
8. P11(k) = m'11(k), k = 1,2,. . , n su sljedovi događaja

Metoda duologa

Zajednički slijed prijelaza za dva komunicirajuća automata.

UNILOG = slijed prijelaza u metodi duologa

Globalno stanje

ALGORITAM:

1. početno stanje sustava je S0.
2. odredite skup svih stanja R(S) za koja prijelazi nisu analizirani. Ako je R(S) prazan skup → postupak je završen.
3. za svako stanje St ∈ R(S) odredite skup sljedećih stanja R'(S).
4. svako stanje za koje je R'(S) prazan skup označuje stanje blokiranja sustava.
   Funkcija δi(Si(t), Ti(t)) nije definirana ni za jedan i.
   Ne postoji unutrašnji prijelaz ili prijelaz uz predaju informacijske jedinice koji se može izvesti.
   Skupovi stanja svih kanala Ks (i, j) su prazni skupovi.
5. svako stanje St u kojemu se ne može izvesti prijelaz uz prijam poruke izaziva pogrešku prijama i valja ga izbaciti iz R'(S)
6. svako stanje St u kojem prijelaz izaziva predaju poruke uz prekoračenje kapaciteta kanala valja izbaciti iz R'(S) ako se kontrola komunikacije provodi potvrdom jer znači pogrešku. Prijelaz izvedite ako se provodi vremenska kontrola komunikacije.
7. dodajte preostale članove skupa R'(S) skupu R(S) ako već nisu uključeni u R(S).
8. ponovite 2.

Pridružena stanja

Stanja iz različitih procesa za koja vrijedi sljedeće:

• svakom stanju ai iz procesa PA pridruženo je stanje bj iz procesa PB ako su ai i bj sadržani u istom zajedničkom stanju sustava komunicirajućih procesa

• sva stanja procesa PB koja su pridružena stanju ai iz procesa PA tvore skup stanja pridruženih stanju ai

---

3. PETRIJEVA MREŽA

- PETRIJEVA MREŽA = mreža mjesta i prijelaza u kojoj mjesta imaju značenje uvjeta, a prijelazi događaja u smislu definicije sustava uvjeta i događaja

- Pravilo izvedbe prijelaza:
Neka je t e T prijelaz s m ulaznih mjesta (a1,…,am) i n izlaznih mjesta (b1,…,bn). Izvedba prijelaza t smanjuje broj oznaka svakog ulaznog mjesta ai za W(ai, t) i povećava broj oznaka svakog izlaznog mjesta bj za W(t, bj).
Prijelaz se može izvesti uz označavanje M ako i samo ako sva ulazna mjesta sadrže dovoljno oznaka: **M(ai) ≥ W(ai, t)** , a sva izlazna mjesta imaju dovoljan kapacitet: **M(bj) ≥ K(bj) - W(t, bj)**.

- KONCESIJA = uvjeti koji moraju biti ostvareni za izvedbu prijelaza

- Ulazna mjesta opisuju preduvjete, a izlazna mjesta postuvjete

Struktura Petrijeve mreže
C = (P, T, I, O)
P = {p1, p2, . . , pn} konačni skup mjesta, n > 0, pi Є P
T = {t1, t2, . . , tm} konačni skup prijelaza, m > 0, tj Є T
P n T = 0
P U T ≠ 0
I : T → P funkcija ulaza → I : P → T
O : T → P funkcija izlaza → O : P → T

DUALNA MREŽA = mreža C' = (T, P, I, O), a izvodi se zamjenom mjesta i prijelaza

INVERZNA PETRIJEVA MREŽA = mreža -C = (P, T, O, I), a izvodi se zamjenom ulaza i izlaza

OZNAČENA PETRIJEVA MREŽA = mreža M = (P, T, I, O, μ), a čini ju Petrijeva mreža C s vektorom oznaka μ

μ = (μ1, μ2, ... , μi, … , μn) → μi = broj oznaka u mjestu pi, odnosno μ(pi) = μi

Prijelaz tj Є T u mreži M = (P, T, I, O, μ) može se izvesti ako je za svaki **pi Є P: μ(pi) ≥ #(pi, I(tj))**, tj. ako svako ulazno mjesto ima najmanje toliko oznaka s koliko je grana povezano s prijelazom.

Provedba prijelaza generira novo stanje μ' tako da za svaki pi Є P vrijedi:
μ'(pi) = μ(pi) - #(pi, I(tj)) + #(pi, O(tj))

Odnos mjesta i prijelaza u procesu izvedbe:
μ'(pi) = μ(pi) → mjesto pi i prijelaz tj nisu povezani,
μ'(pi) = μ(pi) - #(pi, I(tj)) → mjesto pije ulazno mjesto za prijelaz tj ,
μ'(pi) = μ(pi) + #(pi, O(tj)) → mjesto pi je izlazno mjesto za prijelaz tj ,
μ'(pi) = μ(pi) - #(pi, I(tj)) + #(pi, O(tj)) → mjesto pije ulazno i izlazno za prijelaz tj

GRAF STANJA = dobiva se izvedbom Petrijeve mreže uz zadano početno stanje. Mreža može prijeći u sljedeće stanje koje već postoji

Obilježja Petrijeve mreže

DOSTUPNOST

Ako je μ' stanje neposredno dostupno iz μ, a μ'' iz μ', tada je μ'' dostupno iz μ.
Dostupnost se može definirati i za podskup mjesta, i za odabrani skup stanja.

OGRANIČENOST

Maksimalni broj oznaka u mjestu mreže.
Petrijeva mreža je k-ograničena ako su sva mjesta u mreži najmanje k-ograničena.

SIGURNOST

Broj oznaka u svakome mjestu ne smije biti veći od 1, tj. svaki uvjet može biti samo ispunjen ili neispunjen.
Petrijeva mreža je sigurna ako su sva mjesta u njoj sigurna (znači **ako je mreža 1-ograničena**).

AKTIVNOST

Mogućnost izvedbe prijelaza; **Aktivna mreža isključuje mogućnost postojanja prijelaza koji se nikad ne izvodi ili stanja u kojemu se ne može izvesti nijedan prijelaz.**
- Aktivnost ima više interpretacija:
• prijelaz tj Petrijeve mreže C je potencijalno aktivan u stanju μ ako postoji stanje μ' Є R(C, μ) i ako se tj može izvesti u μ'
• prijelaz tjje aktivan u stanju μ ako je potencijalno aktivan u svim stanjima iz R(C, μ)
• prijelaz tj je aktivan ako se iz jednog stanja, izvedbom drugih prijelaza, može prijeći u stanje u kojemu se izvodi tj

Pet razina aktivnosti prijelaza:

- 0 - tj neaktivan (ne može se izvesti ni u jednom slijedu prijelaza)
- 1 - tj potencijalno aktivan (može se izvesti barem u jednom stanju)
- 2 – tj se u slijedu prijelaza izvodi najmanje n puta
- 3 – tj se u beskonačnom slijedu prijelaza izvodi bezbroj puta
- 4 - tj aktivan (za svako stanje postoji slijed prijelaza u kojem će se prijelaz izvesti → sva stanja dostupna!!)

Petrijeva je mreža i-aktivna ako su svi prijelazi aktivni na razini i. Mreža (prijelaz) je neaktivna ako je razine 0, a aktivna ako je razine 4!

REVERZIBILNOST

Mreža je reverzibilna ako se iz svakog stanja μ' Є R(M) može vratiti u početno stanje μ, odnosno ako je **početno stanje dostupno iz svakog stanja**.

PREKRIVANJE

Stanja za koja vrijedi μ'' ≥ μ' → da li za mrežu C s početnim stanjem μ i stanje μ' postoji stanje μ'' Є R(C, μ) t.d. μ'' ≥ μ'?
Prekrivanje zahtijeva najmanje 1-aktivnu mrežu (potencijalno izvedive prijelaze).

KONVERZACIJA TOKA

Zadržavanje jednakoga, početnog, broja oznaka u svim stanjima mreže → **broj ulaza i izlaza za svaki prijelaz mora biti jednak!**
Petrijeva mreža s početnim stanjem μ je strogo konzervacijska ako za svaki μ' Є R(M) vrijedi: Σ μ'(pi) = Σ μ(pi)
Mreža koja nije strogo konzervacijska može se pretvoriti u takvu mrežu izjednačavanjem broja ulaznih i izlaznih grana za svaki prijelaz (dodavanje paralelnih grana).

KONFLIKTNOST PRIJELAZA

Prijelazi ti i tj su konfliktni ako i samo ako postoji stanje μ u kojemu se oba prijelaza mogu izvesti:
μ(pk) ≥ #(pk, I(ti)), za svaki pk Є P
μ(pk) ≥ #(pk, I(tj)), za svaki pk Є P,
ali **izvedba jednoga isključuje izvedbu drugoga**: μ(pk) < #(pk, I(ti)) + #(pk, I(tj)), za neki pk Є P.

SIMULTANOST PRIJELAZA

Prijelazi ti i tj su simultani ako postoji stanje μ u kojemu se oni mogu izvesti, a **izvedba jednoga ne utječe na izvedbu drugoga**: μ(pk) ≥ #(pk, I(ti)) + #(pk, I(tj)), za svaki pk Є P.

PERZISTENTNOST

Petrijeva mreža je perzistentna ako prijelaz koji se može izvesti gubi uvjete samo vlastitom izvedbom.
Ima značenje odsutnosti konflikta u procesu izvedbe mreže → **AKO MREŽA IMA KONFLIKTE, ONDA NIJE PERZISTENTNA MREŽA!**

SINKRONIČNA DISTANCA

Stupanj usklađenosti dvaju prijelaza ti i tj u M → odgovara razlici broja izvedbi prijelaza u slijedu σ:
dij = max σ (#σ(ti) - #σ(tj))

Izvedeni modeli

- Modeli s mogućnošću ispitivanja neispunjenog uvjeta
- Modeli s klasificiranim mjestima
- Petrijeva mreža s inhibicijskom granom
- Petrijeva mreža s isključivim ILI prijelazom
- Petrijeva mreža s usmjeravajućim prijelazom
- Petrijeva mreža s prioritetima
- Vremenska Petrijeva mreža
- Petrijeva mreža miješanog tipa
- Obojena Petrijeva mreža
- Stohastička Petrijeva mreža
- Neizrazita Petrijeva mreža

Strukturna ograničenja

- Ordinarna Petrijeva mreža

- ako vrijedi **#(pi, I(tj)) ≤ 1** i **#(pi, O(tj)) ≤ 1** → **isključeno višestruko povezivanje mjesta i prijelaza**

- Petrijeva mreža bez vlastitih petlji

- ako vrijedi I(tj) n O(tj) = 0 → **ne može biti i ulazno i izlazno za isti prijelaz**

- Automat stanja

- mreža za koju **svaki prijelaz ima samo jedno ulazno i izlazno mjesto**: |I(tj)| = 1 i |O(tj)| = 1

- Označeni graf

- mreža za koju **svako mjesto ima samo jedan ulazni i izlazni prijelaz:** |I(pi)| = 1 i |O(pi)| = 1

- Mreža slobodnog izbora

- ako je svako mjesto pi za svaki prijelaz tj ili jedino ulazno mjesto ili je prijelaz tj jedini izlazni prijelaz za to mjesto: I(tj) = pi ili O(pi) = tj

- Jednostavna mreža

- ako je **svakom prijelazu najviše jedno ulazno mjesto zajedničko s nekim drugim prijelazom**

4. ANALIZA I SINTEZA KOMUNIKACIJSKIH PROTOKOLA

Sedam slojeva:

1. fizikalni sloj (najniži sloj)
2. sloj podatkovne veze,
3. mrežni sloj,
4. transportni sloj,
5. sloj sesije,
6. sloj prikaza,
7. sloj primjene (najviši sloj)

Dvije ravnine:
• upravljačka ili C-ravnina (control) → upravljanje vezom, upravljanje uporabom veze i pridjeljivanje dodatnih usluga
• korisnička ili U-ravnina (user) → prijenos informacija između korisnika

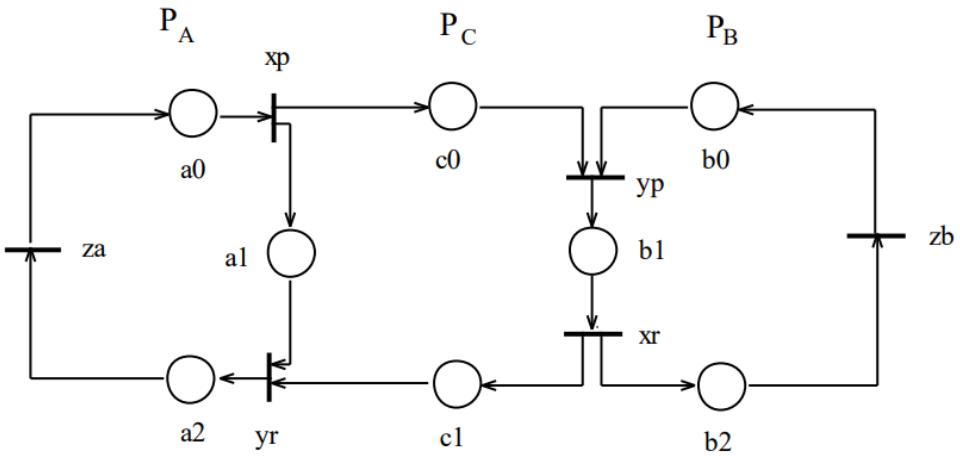
Generički protokolni blok sadrži:
• lokalnu upravljačku ravninu LC
• globalnu upravljačku ravninu GC
• korisničku ravninu U

Pri razvoju protokola provodi se:
• specifikacija (definiranje i formalizacija opisa protokola)
• verifikacija (provjera specificiranog protokola)
• implementacija (izvedba protokola na temelju provjerene specifikacije), te
• ispitivanje podudarnosti (provjera izvedenog u odnosu prema specificiranom protokolu)

Model osnovnog komunikacijskog protokola

U modelu osnovnoga komunikacijskog protokola dva procesa izmjenjuju poruke i potvrde. Svakom se procesu PA, PB, kao i kanalu C pridjeljuje odgovarajuća Petrijeva mreža PA, PB i PC s mjestima koja opisuju uvjete:
a0 - pripravnost za predaju poruke
a1 - čekanje potvrde
a2 - primljena potvrda
b0 - pripravnost za prijam poruke
b1 - primljena poruka
b2 - predana potvrda
c0 - poruka na kanalu
c1 - potvrda na kanalu

i prijelazima koji opisuju događaje:
xp - predaja poruke
yr - prijam potvrde
za - unutrašnji prijelaz
yp - prijam poruke
xr - predaja potvrde
zb - unutrašnji prijelaz

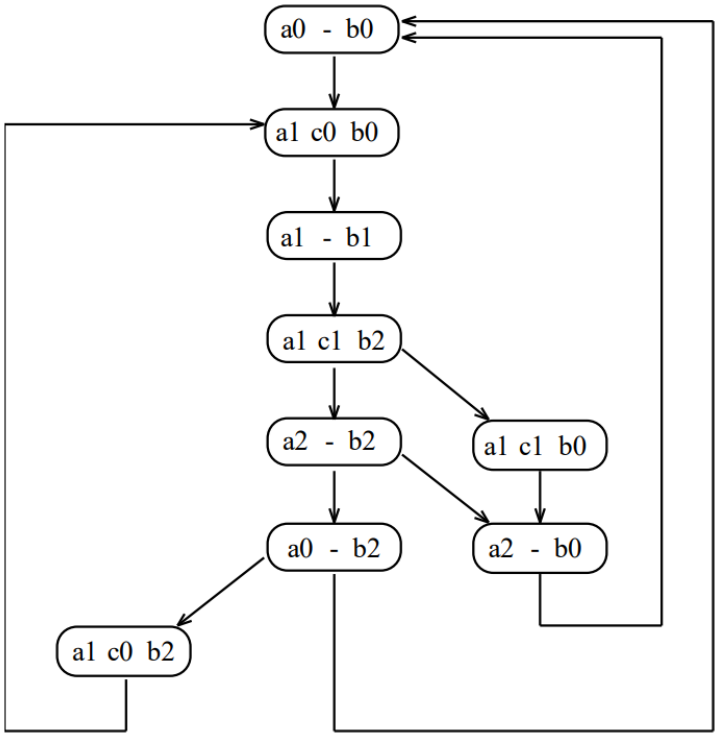


Slika 4.6. Izvorna Petrijeva mreža za model protokola

→ Ova je mreža sigurna, aktivna i perzistentna, a nije konzervacijska!

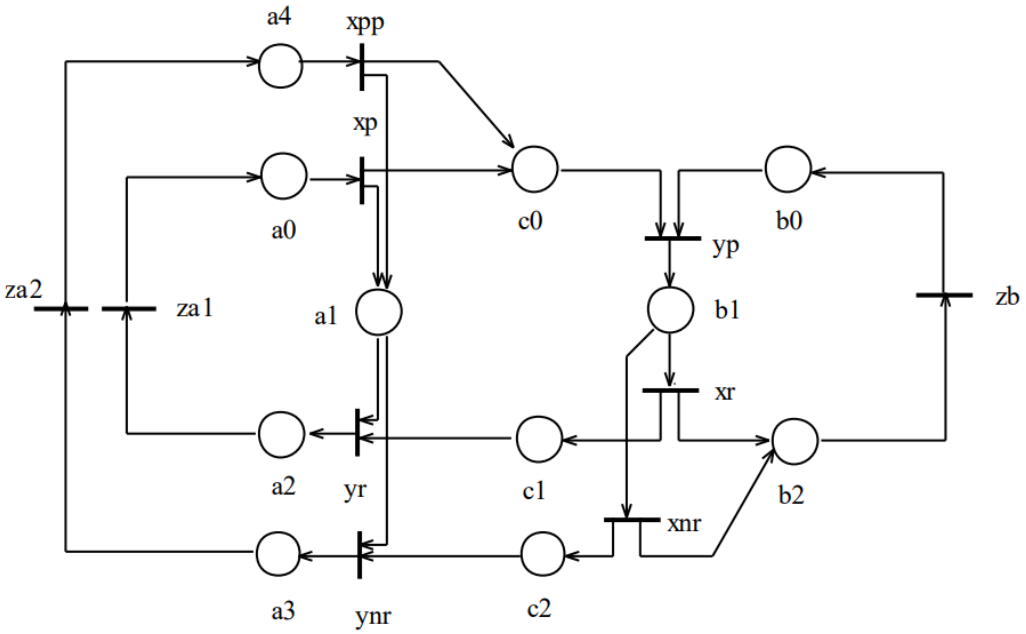
→ Prijelazi yr i zb, xp i zb, za i zb su paralelni, a konfliktnih prijelaza nema!

μ0 = (μa0, μa1, μa2, μb0, μb1, μb2, μc0, μc1) = (1, 0, 0, 1, 0, 0, 0, 0)
μ1 = (0, 1, 0, 1, 0, 0, 1, 0)



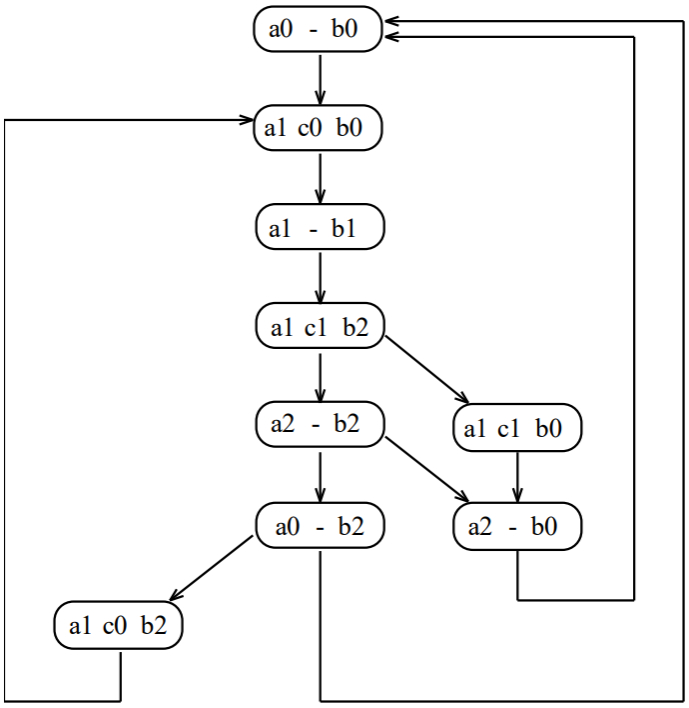
→ Graf stanja izvorne Petrijeve mreže za model protokola

Uvode se pozitivne potvrde (r) i negativne potvrde (nr) → uvode se nova mjesta i prijelazi:
a3 - negativna potvrda prijama
a4 - poruka pripravna za ponovni prijenos (retransmisiju)
c2 - negativna potvrda na kanalu
xnr - predaja negativne potvrde
ynr - prijam negativne potvrde
xpp - retransmisija poruke



→ **Model protokola s pozitivnom i negativnom potvrdom**

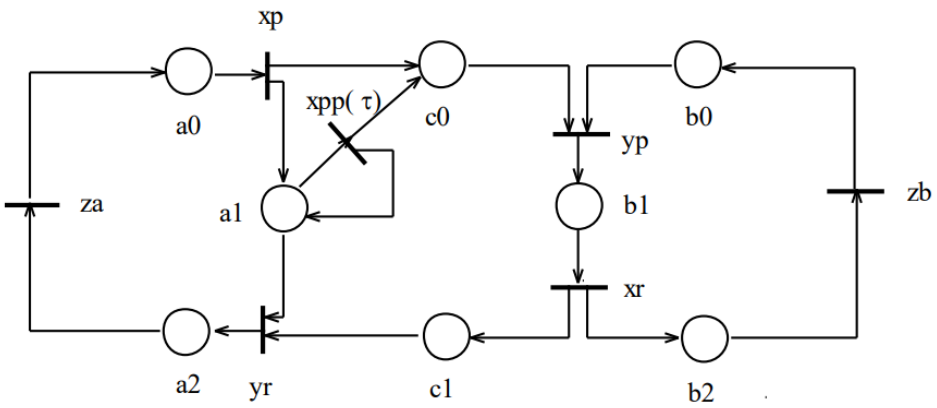
→ **Prijelazi xr i xnr, te yr i ynr su konfliktni!**

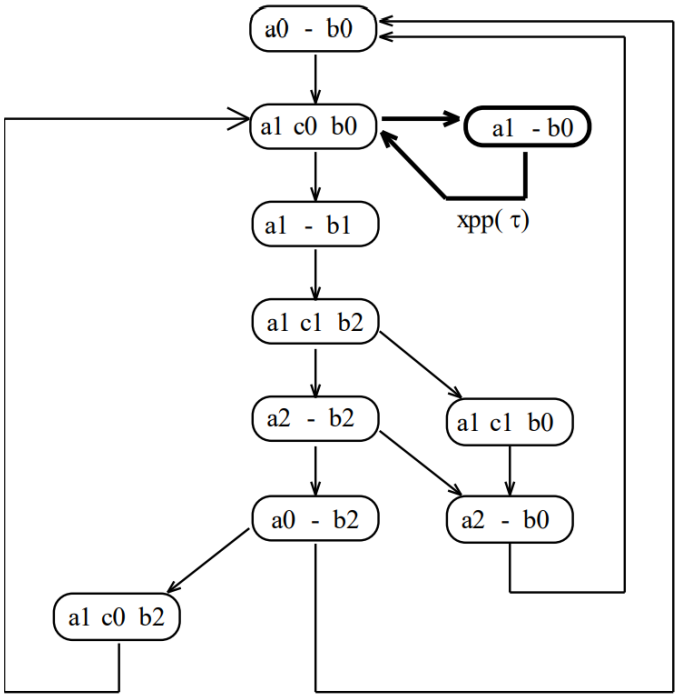


→ **u slučaju gubitka poruke ne može se izvesti nijedan novi prijelaz i riječ je o stanju blokiranja**

Primjena vremenske Petrijeve mreže

Osnovni model treba proširiti vremenskim prijelazom koji će odašiljati poruku nakon isteka vremenske kontrole i vratiti procese u regularno stanje.





---

6. MREŽNI PROTOKOL IPv6

Mrežni sloj

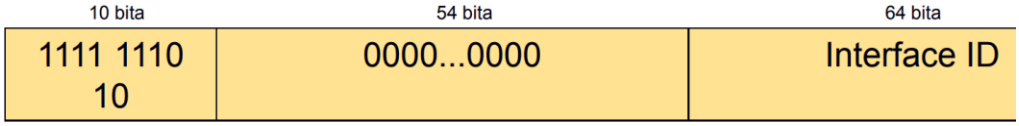
- osnovna zadaća: dostaviti jedinice podataka (pakete) od izvorišnog krajnjeg čvora do odredišnog krajnjeg čvora, izravno ili preko niza međučvorova
- dvije vrste usluge: spojna usluga i nespojna usluga (mrežni sloj u Internetu i IP-mrežama)
- dvije izvedbe usmjeravanja u mrežama s komutacijom paketa: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

IPv4

- Karakteristike:
    - 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: ometanje → IP prihvaća podatke od višeg sloja (npr. transportnog protokola TCP, UDP), smješta ih u podatkovno polje IP datagrama i predaje datagram protokolu sloja podatkovne poveznice
- Nespojna usluga izvedena datagramski → minimalni skup funkcija za dostavu datagrama s kraja na kraj mreže
- Funkcionalnosti:
    → Definira shemu adresiranja u Internetu
        - jedinstveni adresni prostor ; svaki sustav ima po jednu IP-adresu za svako mrežno sučelje ; krajnje računalo može koristiti više posebnih adresa ; 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 sastavljanju kod primatelja
- Adresiranje:
    - IP-adresa 32 (2^5) bita (2^32 mogućih adresa)
    - krajnji sustav 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 2 dijela: mrežni (identifikator mreže) i računalni dio (identifikator krajnjeg računala)
- Prefiksni prikaz adrese:
    - prefiksni prikaz IP-adrese ne uzima u obzir izvorne klase A, B i C
    - duljina mrežnog dijela se označava mrežnim prefiksom iza adrese (195.24.0.0**/13**)
- Besklasno usmjeravanje:
    - putevi usmjeravanja više se ne agregiraju prema klasama adresa, već prema mrežnom prefiksu
- Fragmentacija:
    - provodi ju usmjeritelj
    - fragmenti se šalju u novim, međusobno neovisnim datagramima s usmjeritelja na izvoru i sastavljaju u originalni datagram na odredištu
- IPv4 zaglavlje:
    - polja vezana uz ometanje: IHL, ukupna duljina datagrama, ozn.višeg protokola, podaci višeg sloja/protokola
    - polja vezana uz usmjeravanje: TTL, zaštitna suma zaglavlja, izvorišna IP-adresa, odredišna IP-adresa
- 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

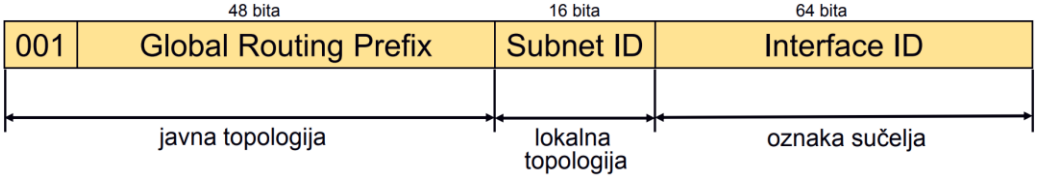
IPv6

- ispravlja nedostatke koje ima IPv4 i unosi poboljšanja:
    - veći adresni prostor → globalna umreženost i dostupnost svih čvorova, bez "skrivenih" mreža i računala
    - učinkovitije usmjeravanje
- Novosti u IPv6:
    - veći adresni prostor (128 bitne adrese)
    - pojednostavljenje formata zaglavlja (fiksna duljina od 40 okteta, mPanje polja)
    - dodatna zaglavlja za posebne mogućnosti
    - unaprjeđeno 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
- Adresiranje:
    - Duljina IPv6-adresa je 128 (2^7) bitova (2^128 mogućih adresa)
    - omogućuje stvaranje domena koje odražavaju današnju topologiju Interneta, jer 128 bita dozvoljava višestruke razine hijerarhije i fleksibilnost
    - Zapis adresa:
        - notacija: 8 grupa po 4 heksadekadske znamenke → npr. EFD1:0989:AB02:7654:C4ED:890B:DE65:1240
        - sažimanje okteta :00: u :: → 1080:0:0:0:0:8:800:200C u 1080::8:800:200C ; 0:0:0:0:0:0:0:1 u ::1
            - dvije dvotočke (::) smiju se upotrijebiti samo jednom u adresi!!!
                → npr. 1080:0:0:8:800:0:0:200C u 1080::8:800::200C nije dozvoljeno!
    - IP-adresa ima 2 dijela: mrežni (identifikator mreže) i računalni dio (identifikator krajnjeg računala)
        - prefiksni zapis: ip-adresa/prefiks → 12AB:0:0:CD30::/60
    - Vrste IPv6 adresa:
        1) **Unicast** – jednoodredišna adresa
            - identificira jedno sučelje računala/čvora
            → Lokalna jednoodredišna adresa:
                - IPv6 prefiksna notacija: **FE80::/10**
                - Potrebne za otkrivanje susjednih čvorova
                - Čvorovi ne komuniciraju putem usmjeritelja



                - IPv6-usmjeritelj ne prosljeđuje pakete s link-local adresom izvan poveznice

            → Globalna jednoodredišna adresa:
                - 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

2) **Multicast** – višeodredišna adresa

- određuje skup sučelja (obično na različitim čvorovima)
- paket se dostavlja svim sučeljima unutar grupe definirane multicast adresom (Group ID)
- IPv6 prefiksna notacija: **FF00::/8**
-

→ F: zastavica (flag), zastavica Transient

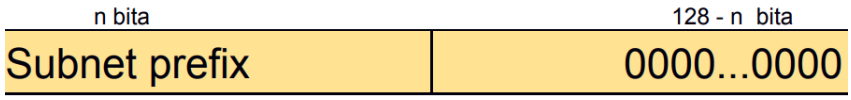
- T = 0 (trajno dodijeljena multicast adresa)
- T = 1 (privremeno dodijeljena multicast adresa)

→ S: doseg (scope), označava doseg adrese

- sučelje (interface-local), poveznica (link-local), globalno (global)

3) **Anycast** – adresa jednog iz skupa sučelja

- dostava jednom iz skupa sučelja
- paket se dostavlja se samo jednom ("najbližem") sučelju od onih s tom anycast adresom
-



- 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

→ Ta adresa omogućuje komunikaciju s jednim od usmjeritelja u podmreži

4) **Unspecified** – nespecificirana adresa

- **0:0:0:0:0:0:0:0 ili ::** (naznačuje da nema adrese) → ekvivalentno adresi 0.0.0.0 u IPv4!
- IPv6 prefiksna notacija: **::/128**
- primjena: autokonfiguracija (izvorišna adresapaketa za provjeravu jednoznačnosti tražene adrese) ; definiranje čvorova i usmjeritelja dosega sučelja i poveznice
- ne smije se dodijeliti mrežnom sučelju niti koristiti kao odredišna adresa

5) **Loopback** - povratna adresa

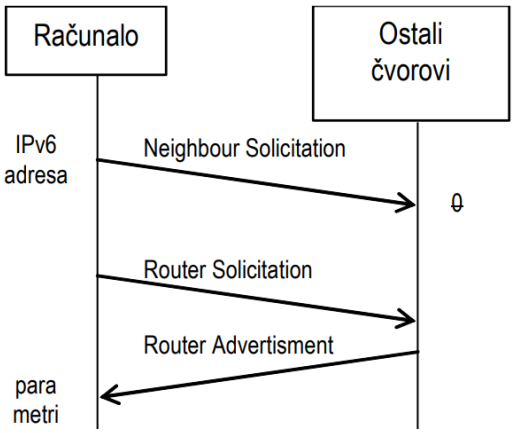
- **::1** → ekvivalent adresi 127.0.0.1 u IPv4
- IPv6 prefiksna notacija: **::1/128**
- primjena: testiranje (omogućuje čvoru da šalje podatke sam sebi) ; definiranje čvorova i usmjeritelja dosega sučelja i poveznice
- paketi adresirani na povratnu adresu ne smiju se poslati na poveznicu

- Dodjela IPv6 adrese:
    - **Dva mehanizma AUTOKONFIGURACIJE:**
        1) samostalna (bez poslužitelja) autokonfiguracija adrese bez poznavanja stanja (stateless)
            - u mrežama bez poslužitelja DHCPv6
            - primjena upravljačkog protokola NDP (Neighbor Discovery Protocol)
            - POSTUPAK:
                1. Jednoznačno adresiranje čvora na lokalnoj poveznici (link-local unicast)
                    - IPv6 adresa izvedena iz MAC-adrese
                2. Provjera jedinstvenosti adrese
                    - računalo šalje višeoodredišnu poruku „**Neighbor Solicitation**“
                    - ako se neki drugi čvor odazove na tu adresu porukom „**Neighbor Advertisment**“ koja označava dupliciranu 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
                3. Određivanje načina autokonfiguracije i parametara za autokonfiguraciju globalne adrese
                    - računalo otkriva poslužitelja koji određuje način autokonfiguracije (autokonfiguracija s poznavanjem stanja s poslužiteljem DHCPv6 – statefull , ili autokonfiguracija bez poznavanja stanja)
                    - za autokonfiguraciju bez poznavanja stanja dostavlja potrebne parametre
                    - ako se usmjeritelj ne oglašava, preostaje autokonfiguracija putem poslužitelja DHCPv6
        2) autokonfiguracija s poslužiteljem uz poznavanje stanja (statefull)
            - **primjena upravljačkog protokola DHCPv6**
            - uz samu IPv6-adresu, omogućena je potpuna konfiguracija za TCP/IP
- Upravljački protokoli za IPv6:
    → 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)
        - služi za dojavu pogrešaka i dijagnostiku (npr. ICMPv6 “ping”)
        - određivanje MTU-puta (Path MTU Discovery):
            - IPv6 propisuje minimalni MTU od 1280 okteta
            - datagrami se mogu fragmentirati samo na izvoru i sastavljati na odredištu
            - POSTUPAK:
                1. izvor šalje datagram veličine MTU vlastite poveznice
                2. usmjeritelj na putu prosljeđuje 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. Koraci 2 i 3 se ponavljaju sve dok paket ne stigne na odredište. Time je određen MTU-puta
        - prenosi poruke za protokole NDP i MLD

- Vrste poruka:
    1) poruke o pogreškama (odredište nedostupno, prevelik paket, istek vremena, problem s parametrima)
    2) informativne poruke (echo request, echo replay) → IPv6 ping
    3) specifične poruke vezane uz druge protokole (npr. NDP, MLD)

→ Neighbor Discovery Protocol (NDP)

- preuzima i proširuje funkcije protokola ICMP i ARP iz IPv4 i definira nove poruke ICMPv6
- čvorovi (računala i usmjeritelji) na istoj poveznici
- poruke i procesi kojima se određuje odnos susjednih čvorova
- osigurava funkcije na lokalnoj poveznici
    - za sve čvorove: razlučivanje adrese (IP-adresa – MAC-adresa, otkrivanje duplicirane adrese, dostupnosti čvora i sljedećeg skoka)
    - za računala: otkrivanje usmjeritelja, mrežnog prefiksa i parametara, autokonfiguracija adrese, preusmjeravanje
    - za usmjeritelje: oglašavanje prisutnosti
- primjenjuje se i za Mobile IPv6
- **FUNKCIJE PROTOKOLA NDP:**
    - Razlučivanje adrese → za otkrivanje MAC-adrese na temelju poznate IP sučelja (odgovora ARP-zahtjevu u IPv4)
    - Otkrivanje duplicirane adrese → provjera koristi li se već IP-adresa u istoj mreži
    - Provjera dostupnosti → određivanje dostupnosti susjednog čvora
    - Određivanje sljedećeg skoka
        → određuje slanje datagrama na temelju odredišne adrese datagrama
    - Preusmjeravanje → usmjeritelj informira računalo o boljem putu do odredišta
    - Autokonfiguracija adrese → automatska konfiguracija adrese računala
    - Otkrivanje usmjeritelja
        → računalo otkriva usmjeritelja na svojoj lokalnoj poveznici
        → 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)
    - Otkrivanje prefiksa → računalo otkriva kojoj mreži pripada
    - Otkrivanje parametara → računalo otkriva parametre lokalne poveznice i/ili usmjeritelja (npr. MTU)
- Poruke protokola NDP:



IPv6 zaglavlje **slj. zag. = 68 (ICMPv6)**	**ND** **zaglavlje poruke**	**ND** **opcije poruke**

→ Vrste poruka ICMPv6:
- **Router Solicitation** → traženje/pobuđivanje usmjeritelja
- **Router Advertisement** → oglašavanje usmjeritelja
- **Neighbor Solicitation** → traženje/pobuđivanje susjeda
- **Neighbor Advertisement** → oglašavanje susjeda
- **Redirect** → preusmjeravanje

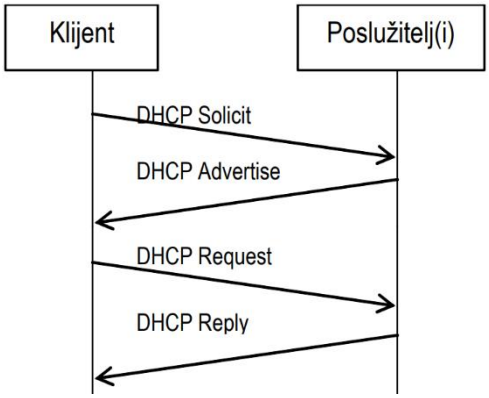
→ Adresiranje poruka ICMPv6:
- zahtjevi za nekom funkcijom → višeoodredišno (multicast)
- odgovori → jednoodredišno (unicast)

→ Multicast Listener Directory (MLD)

- zamjenjuje IGMP za IPv4 i proširuje njegovu funkcionalnost

→ Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

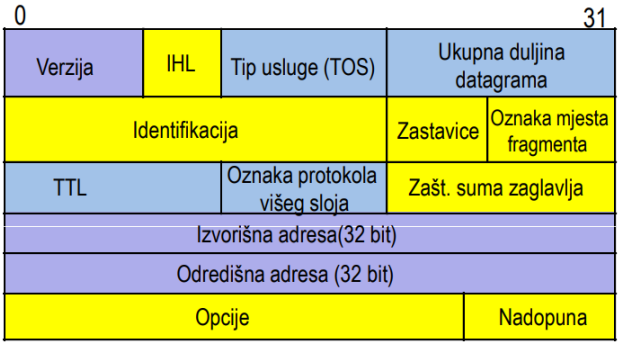
- protokol za autokonfiguraciju adrese s poznavanjem (pomoću poslužitelja)
- omogućuje računalu (DHCPv6-klijent) dobivanje konfiguracijskih parametara od poslužitelja (DHCPv6-poslužitelj) → poslužitelj dinamički dodjeljuje IPv6 adresu i pruža druge konfiguracijske informacije
- transport poruka između klijenta i poslužitelja: UDP
- višeodredišno adresiranje DHCPv6-poslužitelja i njihovih posrednika (relay)
- Vrste poruka DHCPv6:



- **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)
- **DHCP Release** → otpuštanje nekih parametara (npr. adrese koju više neće koristiti)
- **DHCP Reconfigure** → promjena nekih parametara

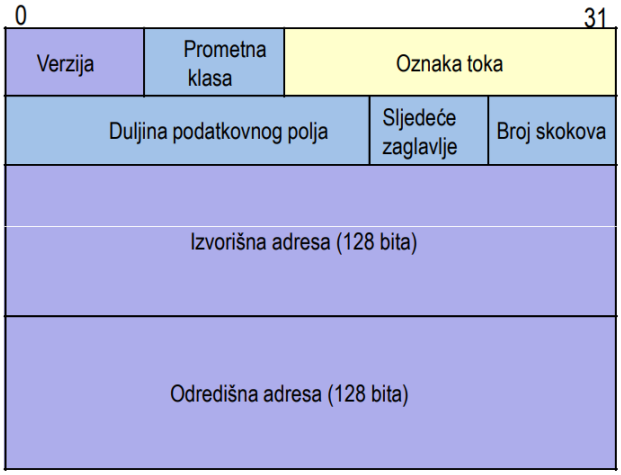
- Format datagrama:

IPv4 -zaglavlje



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

IPv6 -zaglavlje



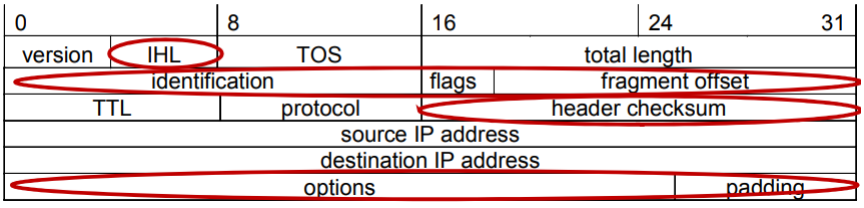
Fiksno 40 okteta

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

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

Uklonjeno:

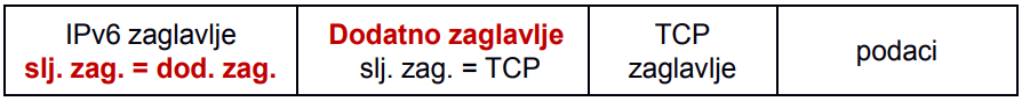


- pojednostavljen format datagrama →
- fragmentiranje samo na izvoru
- preimenovana/redefinirana polja u zaglavlju → duljina polja podataka, ograničenje broja skokova

- nova polja u zaglavlju → prometna klasa (određuje rukovanje paketima ovisno o stanju mreže, tj. zagušenju), oznaka toka (određuje niz paketa koji pripadaju istoj usluzi ili aplikaciji, a za koji se zahtijeva posebno rukovanje u usmjeriteljima, npr. rezervacija resursa)

- Izvorni IP-datagram:

- Dodatna zaglavlja IPv6:
  - IPv4 koristi posebne opcije i tako usporava prosljeđivanje paketa u usmjeriteljima → zato IPv6 umjesto opcija koristi dodatna zaglavlja za proširenja koja se po potrebi dodaju iza osnovnog zaglavlja



- IPv6 datagram dodatna zaglavlja:

→ **Zaglavlje skok po skok (Hop-by-Hop Options Header)**
- zaglavlje varijabilne duljine ; sadrži informaciju namijenjenu svakom čvoru na putu dostave datagrama
- sadrži podatke o sljedećem zaglavlju, veličini samog dodatnog zaglavlja i opcijsko polje s jednom ili više definicija akcije koju poduzima čvor
- Primjer primjene: prijenos vrlo velikih paketa > 2^{16} okteta, npr. video sadržaj, na putu s velikim MTU (polje "duljina podataka" u IPv6 zaglavlju = 0)

→ **Zaglavlje namijenjeno odredištu (Destination Options Header)**
- zaglavlje varijabilne duljine ; sadrži dodatnu informaciju za prvo odredište i sva odredišta koje sadrži dodatno zaglavlje Routing Header
- sadrži podatke o sljedećem zaglavlju, 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
- 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 fragmenta (Fragment Header)**
- zaglavlje fiksne duljine koje se primjenjuje za slanje datagrama većih od MTU-a puta (IPv6 propisuje min MTU od 1280 okteta)
- sadrži podatke o sljedećem zaglavlju, polje s mjestom fragmenta, zastavicu koja označava ima li još fragmenata (1) ili je riječ o zadnjem (0) i identifikacijsko polje koje označava fragmentirani paket
- nefragmentirani dio zajednički za sve fragmente: osnovno zaglavlje i dodatna zaglavlja skok po skok i usmjeravanja
- Primjer primjene: fragmentiranje datagrama – isključivo na izvoru!

Sigurnosna internetska arhitektura (Internet Protocol Security, IPsec)

- Obilježja:
    - IPSec definira protokole čija zadaća je prijenos podataka, pri čemu se podaci tijekom prijenosa mogu štititi na dva načina (oba protokola mogu štiti bilo koji protokol više razine koji se prenosi IP datagramom):
        1) **protokol AH:** zaglavlje za provjeru autentičnosti (Authentication Header)
            - štiti integritet datagrama, autentičnost izvora datagrama i štiti od napada ponavljanjem ranije snimljenih datagrama
            - jamči da je primljeni datagram odaslan s izvorišne IP-adrese → autentičnost izvora IP-datagrama
            - jamči da podaci nisu mijenjani pri prolasku kroz mrežu → integritet IP-datagama
        2) **protokol ESP:** zaglavlje za sigurnosno ovijanje podataka (Encapulating Security Payload Header)
            - sve što i AH + dodatno povjerljivost podataka
            - šifriranjem zaglavlja osigurava se privatnost podataka i integritet datagrama, tj. da podaci nisu bili čitani niti mijenjani
            - dva mehanizma zaštite (šifriranje i dešifriranje):
                1) **transportni način ESP** → zaštita nad podacima transportnog sloja
                    - štiti podatke transportnog sloja
                2) **tunelski način ESP** → šifriranje cijelog datagrama, uključujući zaglavlje
                    - štiti cijeli izvorni IP-paket
                    - ESP zaglavlje je dodano na početku paketa i tada se paket šifrira. Budući da su tako šifrirani IP zaglavlje i dodatna zaglavlja, potrebno je formirati novo IP zaglavlje kako bi usmjeritelji mogli procesirati takav datagram
            - Prijenos podataka: na izvorišnoj strani formiraju se datagrami koji se sastoje od šifriranog i nešifriranog dijela. Paketi se usmjeravaju do odredišta i svaki usmjeritelj na putu ispituje osnovno IP zaglavlje i dodatna zaglavlja koja nisu šifrirana. Na odredišnoj strani provodi se dešifriranje na temelju ESP zaglavlja, tako da samo legitimni pošiljatelj može pročitati podatke zaglavlja
    - Dodatno, IPsec definira protokol IKE 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 info o podržanim algoritmina i pregovaranje o onima koji će se primijeniti
    - u implementaciji IPsec protokol ESP je definiran kao obavezan, a AH kao opcionalan
- Arhitektura, primjene:
    → primjena IPsec:
        - ostvarivanje virtualnih privatnih mreža (Virtual Private Network, **VPN**):
            - koristi se ESP u tunelskom način rada (gateway - gateway)
            - krajnje točke komunikacije "ne znaju" za tuneliranje, a kada paket prolazi dionicom kroz javni Internet, potencijalni napadač ne može saznati ništa o unutarnjoj mreži (npr. IP adrese krajnjih točaka)
        - može se iskoristiti i za sigurnu komunikaciju dvaju krajnjih računala (npr. poslužitelja i klijenta)
- Primjena IPsec-a u IPv4 i IPv6:
    - sigurnosna opcija za IPv4
    - sastavni dio IPv6: dodatna zaglavlja AH i ESP
    - sigurnosna arhitektura (sigurnosni protokoli, kriptografski algoritmi za šifriranje i autentičnost, procedure i protokoli za upravljanje kriptografskim ključevima)
    - primjenon IPsec se postiže: autentičnost pošiljatelja datagrama (izvorišna IP-adresa), integritet datagrama (nepromijenjen tijekom prijenosa), povjerljivost/tajnost cijelog datagrama ili samo polja podataka

Primjer 2.2.

Dva procesa PA i PB opisana automatima A i B komuniciraju tako da PA šalje poruku p prema PB koji je prima i vraća potvrdu r.

Stanja za automat A:
a0 - pripravan za predaju poruke
a1 - čeka potvrdu
a2 - primio potvrdu

Stanja za automat B:
b0 - pripravan za prijam poruke
b1 - primio poruku
b2 - predao potvrdu

Prijelazi za automat A:
xp - predaja poruke
yr - prijam potvrde
za - unutrašnji prijelaz

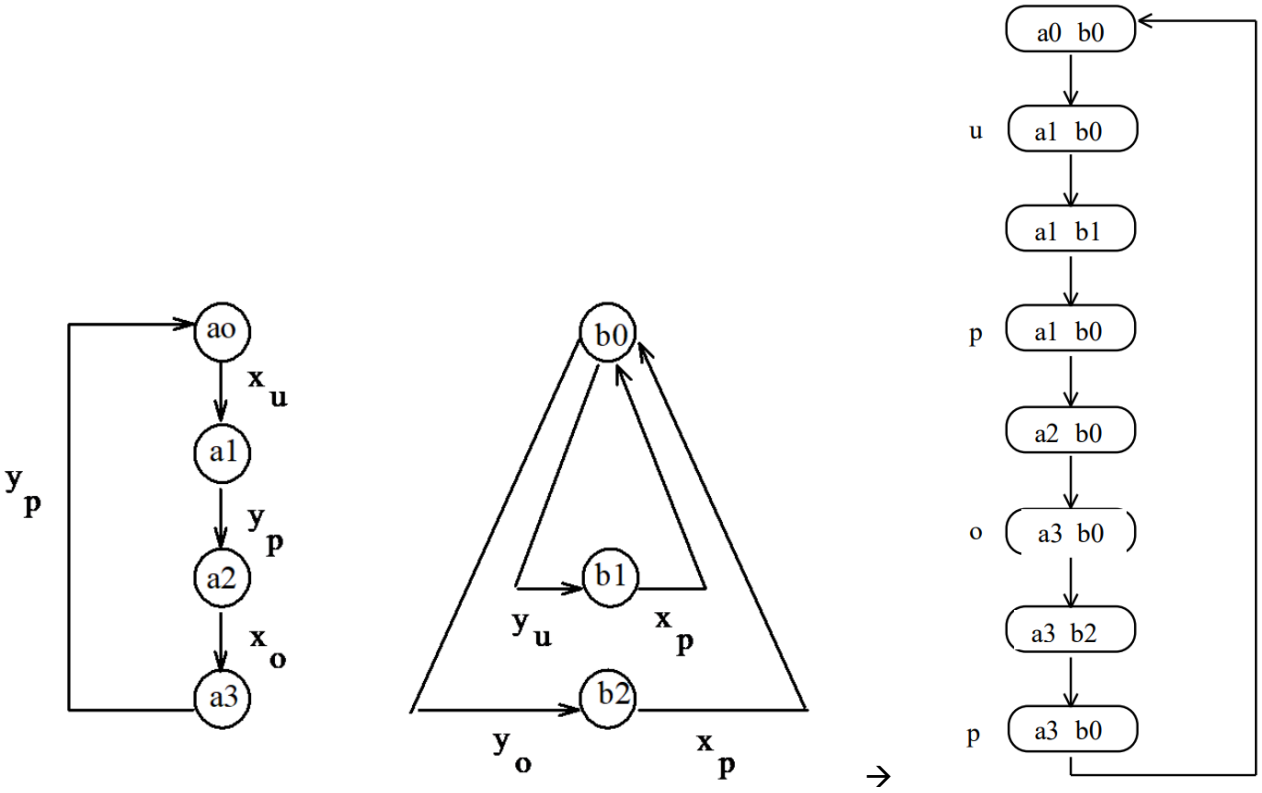
Prijelazi za automat B:
yp - prijam poruke
xr - predaja potvrde
zb - unutrašnji prijelaz

Unilozi:
A: (xp, yr, za)
B: (yp, xr, zb)

Duolozi:
A x B1: (xp, yp, xr, yr, za, zb) → proces PA "brži" od procesa PB
A x B2: (xp, yp, xr, yr, zb, za) → proces PB "brži" od procesa PA
A x B3: (xp, yp, xr, zb, yr, za) → proces PB "brži" od procesa PA

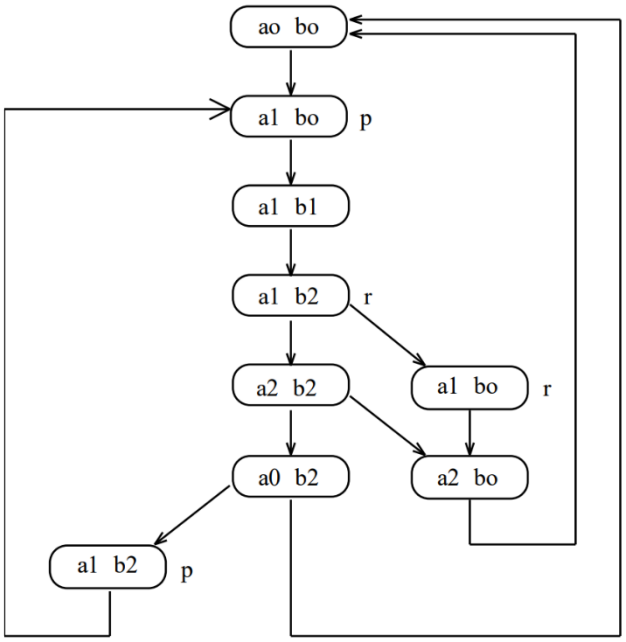
Primjer 2.4.

Automat A odašilje automatu B naloge za upisivanje (u) u memoriju i očitavanje (o), a automat B potvrđuje (p) provedbu svake operacije. Automat A prolazi početnim stanjem samo jednom, a B izvede pritom dva prolaza.



Primjer 2.6.

Iz dijagrama stanja za primjer sa slike izvedite pridružena stanja:



Pridružena stanja:
a0 - (b0, b2)
a1 - (b0, b1, b2)
a2 - (b0, b2)
b0 - (a0, a1, a2)
b1 - (a1)
b2 - (a0, a1, a2)

Primjer 3.1.

Predočite grafički strukturu Petrijeve mreže ako je zadano:

$$P = \{p_1, p_2, p_3, p_4\}$$
$$T = \{t_1, t_2, t_3\}$$

IZLAZI IZ p_m IDU U t_m

BROJ STRELICA KOJE IZLAZE

$$I(t_1) = (p_1) \qquad \#(p_1, I(t_1)) = 2$$
$$I(t_2) = (p_2, p_3) \qquad \#(p_2, I(t_2)) = 1 \qquad \#(p_3, I(t_2)) = 1$$
$$I(t_3) = (p_3) \qquad \#(p_3, I(t_3)) = 1$$

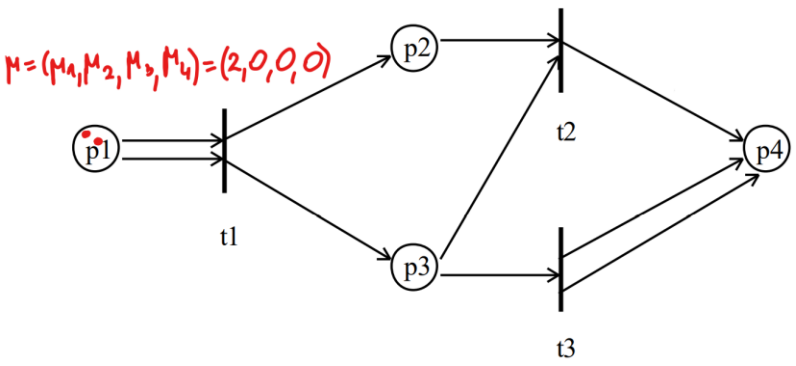
IZLAZI IZ t_m IDU U p_m

$$O(t_1) = (p_2, p_3) \quad \#(p_2, O(t_1)) = 1 \qquad \#(p_3, O(t_1)) = 1$$
$$O(t_2) = (p_4) \qquad \#(p_4, O(t_2)) = 1$$
$$O(t_3) = (p_4) \qquad \#(p_4, O(t_3)) = 2.$$

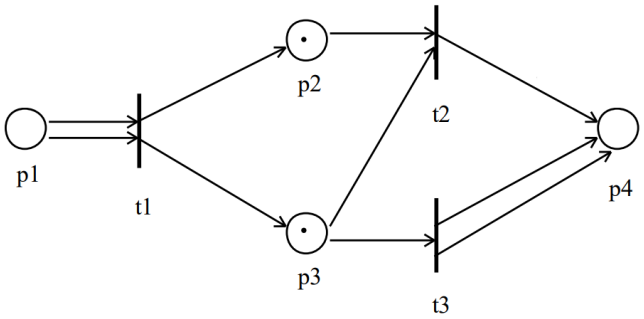
- uz μ kao početno stanje može se izvesti samo prijelaz t1:

μ = (2, 0, 0, 0)

μ(p1) = 2 ≥ #(p1, I(t1)) = **2** ; μ(p2) = 0 ≥ #(p2, I(t1)) = **0** ; μ(p3) = 0 ≥ #(p3, I(t1)) = **0** ; μ(p4) = 0 ≥ #(p4, I(t1)) = **0**



- novo stanje nakon izvedbe prijelaza t1 → sva ulazna mjesta prijelaza gube oznake, a sva izlazna ih dobivaju:
μ' = (0, 1, 1, 0)
μ'(p1) = μ(p1) - #(p1, I(t1)) + #(p1, O(t1)) = 2 - 2 + 0 = **0**
μ'(p2) = μ(p2) - #(p2, I(t1)) + #(p2, O(t1)) = 0 - 0 + 1 = **1**
μ'(p3) = μ(p3) - #(p3, I(t1)) + #(p3, O(t1)) = 0 - 0 + 1 = **1**
μ'(p4) = μ(p4) - #(p4, I(t1)) + #(p4, O(t1)) = 0 - 0 + 0 = **0**



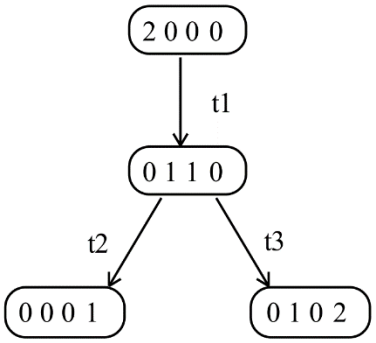
Primjer 3.2.

Za Petrijevu mrežu zadanu u primjeru 3.1. i početno stanje μ0 = (2, 0, 0, 0) odredite skup dostupnih stanja, generirane sljedove stanja i prijelaza, te dostupna stanja i odredite ograničenost.

μ0 = (2, 0, 0, 0) → početno stanje
μ1 = (0, 1, 1, 0) → nakon izvedbe t1
μ2 = (0, 0, 0, 1) → nakon izvedbe t2
μ3 = (0, 1, 0, 2) → nakon izvedbe t3

Generirani sljedovi stanja i prijelaza: (μ0, μ1, μ2) (t1, t2) , (μ0, μ1, μ3) (t1, t3)
Neposredno dostupna stanja: μ0 i μ1 , μ1 i μ2 , μ1 i μ3
Dostupnja stanja: μ0 i μ2 , μ0 i μ3

Provedbom prijelaza generira se skup stanja:



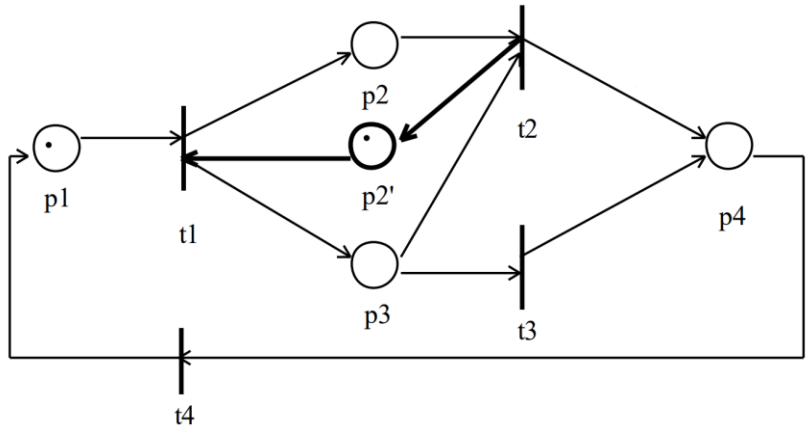
→ **OVA MREŽA JE 2-OGRANIČENA I NIJE REVERZIBILNA!**
→ **PRIJELAZI t2 I t3 SU KONFLIKTNI!**

Primjer 3.3.

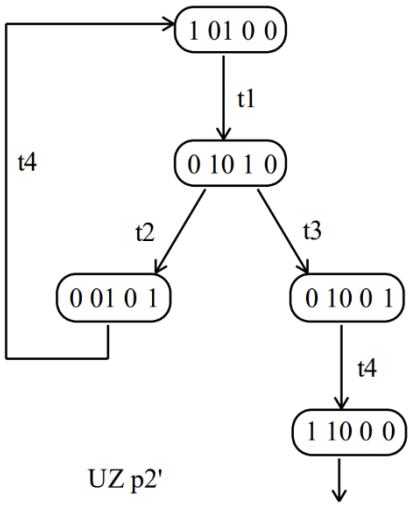
Modificirajte mrežu iz primjera 3.1. tako da postane sigurna i odredite sigurnost mreže.

Uvodi se novi prijelaz t4 između mjesta p4 i p1 → ukida se višestruka povezanost mjesta i prijelaza

Nadalje, početno stanje mora biti sigurno: μ0 = (1, 0, 0, 0) → to nije dovoljno za postizanje sigurnosti mreže jer se gomilaju oznake u p2. Mjesto p2 nije sigurno pa se sigurnost mreže ostvaruje uvođenjem komplementarnog mjesta p2'.



Prijelazi su aktivni na razini:
1 → t3 (postoji stanje u kojem se prijelaz može izvesti)
3 → t1, t2, t4 (postoji slijed prijelaza u kojem se prijelaz može izvesti bezbroj puta)



→ **Ova mreža je 1- aktivna i sigurna, pri čemu se u stanju (1, 1, 0, 0, 0) ne može izvesti nijedan prijelaz (stanje blokiranja - zastoja)!!**

→ **OVA MREŽA NIJE REVERZIBILNA!**

→ **PRIJELAZI t2 I t3 SU KONFLIKTNI!**

Zadaci 6. cjelina (IPv6):

Kakve su vrste adresa podržane protokolom IPv6?
Unicast (jednoodredišna), Multicast (višeodredišna), Anycast (adresa jednog iz skupa sučelja), Unspecified (nespecificirana adresa), Loopback (povratna adresa).

Koje su zadaće protokola NDP?
Razlučivanje adrese, otkrivanje duplicirane adrese, provjera dostupnosti, određivanje sljedećeg skoka, preusmjeravanje, autokonfiguracija adrese, otkrivanje usmjeritelja, otkrivanje prefiksa, otkrivanje parametara.

Petrijeva mreža je reverzibilna ako se iz barem jednog stanja može vratiti u početno stanje. → **NETOČNO**

U protokolu IPv6 datagrami se mogu fragmentirati samo na izvorištu. → **TOČNO**

Objasnite načelo zaštite privatnosti u protokolu IPv6 korištenjem zaglavlja ESP.
Šifriranjem zaglavlja osigurava privatnost podataka i integritet datagrama, tj. da podaci nisu bili čitani niti mijenjani.
Dva mehanizma zaštite: transportni način ESP (zaštita nad podacima transportnog sloja) i tunelski način ESP (zaštita čitavog datagrama, uključujući zaglavlje).
Prijenos podataka: na izvorišnoj strani se formiraju datagrami koji se sastoje od šifriranog i nešifriranog dijela. Paketi se usmjeravaju do odredišta i svaki usmjeritelj na putu ispituje osnovno IP zaglavlje i dodatna zaglavlja koja nisu šifrirana. Na odredišnoj sztrani se provodi dešifriranje na temelju ESP zaglavlja.

Navedite koja su ograničenja iz IPv4 protokola riješena u IPv6 protokolu.
Veći adresni prostor, učinkovitije usmjeravanje, dodatna zaglavlja za posebne mogućnosti, jednostavniji format zaglavlja, mogućnost označavanja paketa koji pripadaju istom toku.

Navedite dva mehanizma autokonfiguracije pri dodjeli IPv6 adrese. Koji se protokoli pritom koriste?
Stateless: Samostalna autokonfiguracija adrese (bez poslužitelja) bez poznavanja stanja uz primjenu protokola NDP (Neighbour Discovery Protocol).
Statefull: Autokonfiguracija s poslužiteljem uz poznavanje stanja uz primjenu protokola DHCPv6.

U kojim se poljima razlikuju zaglavlje IPv4-paketa kojeg je primio usmjeritelj i zaglavlje paketa kojega je usmjerio prema odredištu i proslijedio sljedećem čvoru?
TTL i zaštitna suma

U kojim se poljima razlikuju zaglavlje IPv6-paketa kojeg je primio usmjeritelj i zaglavlje paketa kojega je usmjerio prema odredištu i proslijedio sljedećem čvoru?
Samo TTL

U kakvim okolnostima IPv6-usmjeritelj izaziva gubitak paketa (izbacuje ga) i zašto?
Situacije u kojima se paket izbacuje: TTL=0, zaglavlje nije ispravno, ne može se razriješiti MAC adresa

Objasnite dodatno zaglavlje usmjeravanja koje definira protokol IPv6 i primjer njegove primjene.
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.
Primjer primjene: odabir niza usmjeritelja putem kojih se povezuju izvor i odredište, Mobile IPv6

Usporedite protokole IPv4 i IPv6 s obzirom na funkcionalnost i performanse.
IPv4 funkcionalnosti: Definira shemu adresiranja u Internetu i provedbu fragmentacije
IPv4 performanse: 32-bitne adrese, datagramski način rada, nema mehanizam kontrole toka, nema jamstva očuvanja redoslijeda datagrama
IPv6 funkcionalnosti:
IPv6 performanse: 128-bitne adrese, pojednostavljenje formata zaglavlja, potpora za kvalitetu usluge

U kakvim okolnostima IPv4-usmjeritelj izaziva gubitak paketa (izbacuje ga) i zašto?

Autokonfiguracija kod IPv6 sa poznavanjem stanja protokola DHCPv6, skicirati razmjenu.

Što će se dogoditi IPv6-datagramu ako tijekom prijenosa smetnje izazovu pogrešku jednog bita u odredišnoj adresi?

Tijekom prijenosa IPv6 datagrama došlo je do izmjene polja koje sadrži podatke o izvorišnoj IP adresi. Kako će postupati usmjeritelj s takvim datagramom?

Kako se provodi fragmentacija za protokol IPv6 i kako se ustanovljava 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.

Navedite primjer autokonfiguracije IPv6 bez poznavanja stanja (stateless) i objasnite kako se provodi.

Navedite primjer autokonfiguracije IPv6 s poznavanjem stanja (stateful) i objasnite kako se provodi.

Zašto se u protokolu DHCPv6 primjenjuje višeodredišno adresiranje?

Kakve mogu biti posljedice pogreške u zaglavlju IPv6-paketa?