PREDAVANJE 8 – Bežične mreže i mobilnost

1. Kakva je veza između brzine prenosa podataka, udaljenosti i brzine kretanja čvorova mobilne mreže?(Kako udaljenost i brzina kretanja utiču na brzinu prenosa podataka?)

- Sa povećavanjem udaljenosti, smanjuje se brzina prenosa podataka. Sa povećavanjem brzine kretanja smanjuje se brzina prenosa podataka.

2. Ako se u bežičnoj IEEE 802.11 mreži koristi protokol za izbjegavanje sudara CSMA/CA, kako stanice za koje nije namijenjen paket za koji se rezerviše medij znaju koliko drugo treba da odgode slanje svojih okvira?

- Kada stanica koja će primiti okvir i koja rezerviše medij, CTS i RTS paket, u CTS paketu se specificira vrijeme koje je rezervisala jedna stanica za slanje paketa te za to vrijeme druge stanice treba da zadrže slanje svog paketa.

*Pošiljatelj šalje mali zahtjev za slanje paketa (Request-for-transmission, RTS) ka baznoj stanici koristeći CSMA. Ovi zahtijevi se mogu sudariti, ali šteta nije velika jer su, kako rekosmo, mali. Ako prođe zahtijev za slanje, bazna stanica broadcastuje slobodno-šalji (Confirm-transmission, CTS) kao odgovor na zahtijev za slanje. Ovaj odgovor čuju svi čvorovi. Pošiljatelj šalje svoj frame a ostale stanice uvide da nisu one dobile dozvolu pa odgađaju slanje. U CTS frameu ima polje "duration" koje govori trajanje rezerviranog vremena slanja pa se ove pasivne stanice po tome ravnaju prije nego probaju svoj vlastiti RTS.

3. Šta može bazna stranica uraditi na sprječavanju povećavanja vjerovatnoće pogrešno primljenih okvira prilikom udaljavanja bežičnog uređaja od bazne stanice?

- Ovo je zapravo pitanje kako se smanjuje BER. BER se smanjuje promjenom načina kodiranja, odnosno modulacije. Izborom modulacije sa manjom brzinom smanjuje se vjerovatnoća pogrešno primljenih bita prilikom udaljavanja bežičnog uređaja. Udaljavanjem bežičnog uređaja smanjuje se odnos signal-šum čime se povećava BER.

Odnosno, prilikom udaljavanja bežičnog uređaja od bazne stanice mijenja se signal-to-noise ration (veći SNR → lakše razlikovanje signala od šuma, tj. veće je bolje. Vrijedi da povećanje snage signala povećava SNR a smanjuje BER tj. bit error rate a posljedično i packet error rate). Kada BER postane previsok, bazne stanice prebacuju se na manju brzinu prijenosa ali sa nižim BER.

4. Da li se kod MobileIP podaci između correspondent-a i mobilnog uređaja(korisnika) razmjenjuju preko home networking mobilnog ili ne? (Obrazložiti odgovor)

- Home network: mobilna mreža čiji smo pretplatnici. Correspodent - ko hoće da razgovara sa nama.

Visited network: mreža u kojoj se mobilni korisnik trenutno nalazi. VLR je visitor location register tj baza podataka sa unosom za svakog korisnika koji je trenutno u mreži.

Kada nas zove, poziv se rutira prvo do home network preko PSTN-a tj. telefonske mreže. Kada dođe do home network, home MSC (mobile services switching center) konsultuje HLR tj. home location register što je u biti baza podataka u home network u kojoj su pohranjeni stalni brojevi mobilnih telefona, korisnički profili i informacije o trenutnoj lokaciji (koja može biti i u drugoj mreži) te dobija roaming broj mobilnog u visited network. Home MSC uspostavlja drugi dio putanje do MSC-a visited networka koji okončava uspostavu poziva preko bazne stanice do mobilnog korisnika.

5. Šta je problem skrivenog terminal?

- Prijemnik prima signale od dva pošiljaoca koji su u koliziji te ne može dobro da ih čuje, a ta dva pošiljaoca nisu u situaciji da detektuju tu koliziju.

6. Zašto se kod mobilnih ad-hoc mreža često koristi reaktivno rutiranje? Koji su nedostaci ovog načina uspostavljanja ruta?

- Reaktivno rutiranje se koristi zato što je efikasnije, odnosno rute se proračunavaju samo po potrebi,. Nedostatak ovog načina uspostavljanja ruta je što se rute uspostavljaju samo po potrebi pa prije nego što se prvi paket pošalje potrebno je vrijeme dok se ne uspostavi ruta.

7. Na koji način kod Mobile IP protokola mobilni uređaji pronalaze agente u mrežama u kojim se trenutno nalaze?

- Agenti objavljuju svoje prisustvo i oni samo osluškuju.

8. Kako udaljavanje bežičnog čvora od pristupne tačke (AP) utiče na brzinu prenosa podataka između njih? Objasniti zašto utiče na taj način.

- Udaljavanjem se smanjuje brzina prenosa podataka. Zašto utiče na taj način? Zato što se udaljavanjem smanjuje odnos signal-šum a povećava BER, a da bi se BER zadržao na prihvatljivom nivou onda se smanjuje brzina slanja.

9. Neka se za uspostavljanje veze sa mobilnim korisnikom koristi direktno rutiranje. Neka je veza uspostavljena dok je korisnik bio u jednoj stranoj mreži, a onda se korisnik tokom kretanja premjesti u drugu (stranu) mrežu. Na koji način se u tom slučaju održava veza (kako se prosljeđuju paketi do korisnika koji je promijenio IP mrežu)?

- Kod direktnog rutiranja kada se upostavi komunikacija sa korisnikom koji se ne nalazi u svojoj mreži home network pozivaocu pošalje njegovu adresu u novoj mreži i kada se ovaj prebaci u drugu mrežu u tom trenutku se nastavlja indirektno rutiranje: foreign agent će prosljeđivati pakete ka novoj mreži korisnika odnosno pokazat će se da se koristi indirektno rutiranje.

Dva pristupa mobilnosti u slučaju kada mobilni korisnik mijenja svoju lokaciju a samim tim i mreže kojima je "pokriven": a) indirektno rutiranje gdje komunikacija od pozivatelja do mobilnog korisnika ide preko home agenta (entitet koji upravlja mobilnosti za mobilnog korisnika dok je mobilni udaljen tj. van svoje stalne "kuće") pa se onda proslеđuje do udaljenog. b) pozivatelj dobija udaljenu adresu mobilnog korisnika i komunicira direktno sa njim.

E sad, kako se održava veza kada dođe do kretanja iz jedne u drugu mrežu a već uspostavljena direktna komunikacija? Mobilni mijenja mrežu a nema indirekcije koja nam nudi transparentnost. Dakle, moramo doći do nove adrese (tzv. care-of-address, nasuprot stalnoj home adresi).

NOTE: foreign agent je entitet u visited network koji će upravljati mobilnosti za mobilnog korisnika.

Imamo foregin agenta kojeg proglašavamo sidrom - to je foreign agent u prvoj od mreža u kojoj je mobilni bio a nije mu domaća. Podaci se uvijek prvo rutiraju do anchor FA. Kada se mobilni korisnik premjesti, novi FA organizuje da mu se prosljeđuju podaci od starog FA (efektivno chaining. Kad se ispregovara zamjena, stari FA se "gasi" za mobilnog a novi se proglašava anchorom).

10. Zašto se kod bežičnih mreža (802.11) ne koristi CSMA/CD za kontrolu pristupa mediju?

- Zato sto nije uvijek moguće otkriti koliziiju(CD- collision detection) jer nema garancije da će svi čvorovi čuti sve pakete koji se šalju unutar jedne mreže.

11. Da li je moguće korištenjem jedne bežične pristupne tačke omogućiti da postoje dvije bežične mreže sa različitim SSID i različitim pravima pristupa žičanoj mreži? Ako nije objasniti zašto, a ako jesto objasniti kako.

Naravno da može biti više bežičnih mreža sa različitim SSID-jevima i različitim pravima pristupa zajedničkoj im žičanoj mreži. Naravno, sve mreže će dijeliti isti kolizijski domen. SSID je u ovom slučaju doslovno način da se čvor koji pristupa mreži identificira kao njen pripadnik, pa na osnovu SSID/key kombinacije AP može odlučiti koji policy primijenjivati.

PREDAVANJE 9 – Mrežna sigurnost

1. Potrebno je napraviti tabelu pravila i tabelu konekcija za filter paketa sa stanjem koja dozvoljava samo slijedeće:

a. Pristup bilo kom vanjskom Web (TCP port 80) serveru korisnicima iz unutrašnje mreže
b. Pristup SMTP (TCP port 25) serveru u unutrašnjoj mreži koji se nalazi na adresi 221.221.1.20 korisnicima iz vanjske mreže.
   Adrese u unutrašnjoj mreži su 221.221.1.0/24. Pretpostaviti da u tabeli konekcija postoje tri konekcije, jedna iz unutrašnje i dvije iz vanjske mreže. Za ove konekcije potrebno je izmisliti adrese i brojeve portova koji nisu zadati.

Tabela pravila za filter paketa **sa stanjem** je formata (action = [allow, disallow], src IP, dst IP, protocol, src port, dst port, flag bit, check conn = [NULL, X]).
Tabela konekcija za filter paketa **sa stanjem** je formata (src IP, dst IP, src port, dst port, timeout (sec)).

action	src ip	dst ip	protocol	src port	dst port	flag bit	check con
allow	221.221.1/24	sve	TCP	> 1023	80	sve	
allow	sve	221.221.1/24	TCP	80	>1023	ACK	X
allow	sve	221.221.1.20	TCP	>1023	25	sve	
allow	221.221.1.20	sve	TCP	25	>1023	ACK	X
reject	sve	sve	sve	sve	sve	sve	

src IP	dst IP	src port	dst port	timeout (sec)
221.221.1.2	8.8.8.8	1024	80	60
8.8.8.9	221.221.1.20	1024	25	60
8.8.8.10	221.221.1.20	1025	25	61

2. Koja je namjena digitalnih certifikata? Odakle proističe povjerenje u digitalne certifikate?

Namjena digitalnih certifikata je da poveže javni ključ sa subjekto. Taj subjekt može biti čovjek, uređaj i slično.

Povjerenje u digitalne certifikate proističe iz povjerenja u onoga ko je potpisao taj digitalni certifikat, zato što onaj koji provjerava certifikat je u posjedu javnog ključa potpisnika certifikata. Digitalni potpis garantuje integritet certifikata, a onaj koji provjerava certifikat je u posjedu javnog ključa potpisnika certifikata.

3. Šta je *nonce* (kod različitih protokola za potvrđivanje identiteta, npr SSL)? Koji problem i na koji način rješava?

- Nonce je slučajno generisani broj koji se ne ponavlja tokom konekcije, Rješava problem naknadne reprodukcije snimljenih poruka na način što su poruke vezane za ovaj nonce broj. Poruka koja je kasnije reprodukovana je prepoznata je se neće odnositi na isti nonce broj.

4. Objasniti na koji način se upotrebom kodova za potvrđivanje autentičnosti poruka (MAC) osigurava autentičnost pošiljaoca?

- Prilikom pravljenja hasha se koristi sadržaj poruke kao i tajna informacija koju imaju samo pošiljalac i primalac. Kako samo primalac i pošiljalac imaju samo tu tajnu poruku, odnosno tajnu informaciju, samo je onaj koji ima tu tajnu informaciju mogao napraviti taj MAC. Prilikom hashirana se dodaje tajna informacija koju ima samo pošiljalac. Na taj način primalac zna da je taj MAC mogao napraviti samo taj pošiljalac, odnosno vjeruje u autentičnost poruke.

5. Koje kriptografske funkcije se koriste za zaštitu poruka od (neovlaštenih) izmjena? Na koji način se korištenjem ovih funkcija otkriva da su poruke koje se razmjenjuju izmjenjene?

- Hash funkcije se koriste za zaštitu poruka od neovlaštenih izmjena. Poruka se prije slanja hashira i pošalju se i poruka i hash, na prijemnoj strani se primljena poruka hashira i uporedi se sa hashem koji je stigao i ako se oni razlikuju znači da se poruka izmijenila.

6. Navesti dvije vrste listi za kontrolu pristupa (ACL) koje koristi CISCO i razlike između njih. Napisati ACL koja dozvoljava IP adresu 192.168.0.7/16 a zabranjuje sve ostale IP adrese u tom subnetu (treba napisati samo pravilo/a u sklopu ACL, ne pisati komande).

To su prosirene i obicne- **obicne provjeravaju samo izvorisnu adresu**, a prosirene i ostalo npr. Portove...

akcija	**Izvorišna adresa**	**Odredišna adresa**	**Protokol**	**Izvorišni port**	**Odredišni port**	**Flag bit**
dozvoli	192.168.0.7/16	Različita od 192.168.0.7/16	sve	sve	sve	sve
dozvoli	Različita od 192.168.0.7/16	192.168.0.7/16	sve	sve	sve	sve
zabrani	sve	sve	sve	sve	sve	Sve

7. Šta su liste za kontrolu pristupa(ACL)? Napisati ACL koja zabranjuje IP adresu 192.168.0.2/24 a dozvoljava sve ostale IP adrese u tom subnetu (treba napisati samo pravilo/a u sklopu ACL, ne pisati komande)

ACL - lista za kontrolu pristupa pomoću kojih je moguće ograničiti ili potpuno onemogućiti pristup pojedinim uslugama te otežati izvođenje određenih vrsta mrežnih napada.

akcija	Izvorišna adresa	Odredišna adresa	Protokol	Izvorišni port	Odredišni port	Flag bit
dozvoli	Različita od 192.168.0.2/24	Različita od 192.168.0.2/24	sve	sve	sve	sve
zabrani	Sve	sve	sve	sve	sve	Sve

PREDAVANJE 10 – Prenos multimedijalnih sadržaja preko IP adresa

1. Na predajnoj strani 6 paketa se generiše u trenucima: 1,2,3,4,5 i 6. Paketi na prijemnu stranu dolaze, po redu slanja, u trenucima 10, 12, 12, 14, 16 i 16.

a. **Koje je minimalno kašnjenje reprodukcije koje će omogućiti da su svi od pristiglih paketa stigli na vrijeme za svoju reprodukciju?**
b. **Napraviti dinamičku procjenu prosječnog kašnjenja nakon što četvrti paket po redu stigne na prijemnu stranu, ako je dato u=0,1.**

1	10	9
2	12	10
3	12	9
4	14	10
5	16	11
6	16	10

A) Kako se paketi generišu svakih δ = 1 trenutaka to znači da u svakom trenutku od početka reprodukcije paketi moraju već stići. Npr. ako bi se počelo u trenutku 10, u trenutku 11 nema paketa 2 i sl. Ako se reprodukcija odloži za δ = 3, tada imamo reprodukcije paketa u sljedećim trenucima: 13,14,15,16,17,18. (podrazumijevano je da se paket ne može reproducirati u istom trenutku u kojem je došao jer postoji neko procesiranje, ako to nije slučaj onda je δ = 2).

Minimalno kašnjenje reprodukcije je 11.

B) Dinamička procjena prosječnog kašnjenja na prijemniku se računa po formuli
gdje je **u** konstanta, **t_i** vremenska oznaka i. paketa, **r_i** vrijeme kada je i. paket stigao do prijemnika.
d_i=(1-u)*di-1 + u(ri-ti)
Očito sada ovo moramo računati od prvog do četvrtog tj. traži se **d_4**.
Uzmimo da je d0=0 i u=0.1.

d_1 = 0,1*(10-1)=9*0,1 = 0,9
d_2 = 0,9*0,9 + 0,1*(12-2) = 0,81 + 1 = 1,81
d_3 = 0,9*1,81 + 0,1 (12 - 3) = 2,529
d_4 = 0,9*2,529 + 0,1 (14 - 4) = 3,276

2. Na koji način SIP protokol omogućava da VoIP pozivalac uspostavi komunikaciju sa onim koga poziva? (Uzeti u obzir da se pozvani može nalaziti bilo gdje.)

-SIP pozivalac svom proxy-u prosljeđuje INVITE zahtjev koji proxy dalje prosljeđuje do proxy-a pozvanog. Proxy server pozvanog kontaktirajući lokacijski servis utvrđuje IP lokaciju pozvanog i prosljeđuje mu poziv. Naravno, pošiljalac i prijemnik dogovaraju se i oko portova, preferiranih kodiranja, TCP / UDP izbora itd.

(SIP pozivalac svom proxyu uputi INVITE zahtjev. Proxy proslijedi do Proxy-a pozvanog taj zahtjev. Onda Proxy pozvanog pita Location Service za IP adresu pozvanog. I Onda se ta IP adresa vraca samom pozivaocu i to je to. Pozivalac kontaktira svoj proxy server koji preko svog DNS servera dobiva indirektni odgovor da kontaktira proxy server onoga kojeg poziva. Proxy onoga koji se poziva dalje kontaktira lokacijski server (prosljeđuje INVITE), te se SIP odgovor šalje nazad. Podaci se razmjenjuju među klijentima direktno.)

3. Objasniti koja RTP zaglavlja i kako pomažu u rješavanju poteškoća prilikom prenosa razgovora u realnom vremenu preko IP (VoIP). (koje su smetnje i šta se dodaje na pakete da bi se otklonili).

- To su redni broj paketa i vrijeme nastanka paketa. Numeracija paketa po rednim brojevima omogućava otkrivanje da je neki paket izgubljen, a vremenska oznaka trenutka nastanka paketa omogućava reprodukciju paketa po vremenskim razmacima koji su jednaki vremenskim razmacima nastanka paketa.

*OPĆENITO:

RTP stoji za Realtime Transport Protocol i određuje strukturu paketa koji prenose zvučne i video zapise tj. multimediju. RTP paketi omogućavaju identifikaciju tipa sadržaja i kodiranje, numeriranje sekvence paketa i odgovarajuće vremenske oznake potrebne za ispravnu reprodukciju sadržaja. Izvršava se kod učesnika u komunikaciji tj. end-to-end. RTP paketi pakiraju se u UDP segemente. RTP se smatra transportnim protokolom na aplikativnom nivou. Ide aplikacija → RTP → Socket → UDP → IP. Jasno, RTP ne nudi nikakve mehanizme za QoS jer je transparentan na cijelom putu osim na pošiljatelju i primatelju → zato i nema nikakvog posebnog tretmana RTP paketa.
RTP zaglavlje dodaje se svakom komadu/chunku i pakira se u UDP. RTP zaglavlje daje informacije o kodiraju zvuka u svakom paketu što omogućava da pošiljatelj može promijeniti kodiranje tokom razgovora zavisno o uvjetima na mreži. Također RTP zaglavlje sadrži brojeve tj. sekvencu paketa i odgovarajuće vremenske oznake čime omogućava jednoznačnu reprodukciju (ali i detekciju grešaka).

6. Na koji način SIP lokacijski servis saznaje (trenutno) važeću IP adresu koja odgovara SIP adresi nekog korisnika?

- Prilikom pokretanja SIP klijenata, korisničkih agenata šalje se registar zahtjev preko proxy-a ka lokacijskom servisu. Na taj način lokacijski servis saznaje važeću IP adresu tog korisnika.

7. Zašto *interleaving* ima veće kašnjenje nego FEC metoda borbe protiv gubitka paketa? Zašto FEC ima, a *interleaving* nema redundantnosti?

-Interleaving za reprodukciju mora sačekati dok pristignu svi izmiješani interlaved paketi, dok
FEC 2 čeka se samo nakon izgubljenog sljedeći paket koji ima lošiju kopiju prethodno izgubljenog paketa. FEC ima redundantnost jer šalje dodatne informacije, dok interleaving ne šalje nikakve dodatne informacije, šalje istu količinu podatkovnih bita samo drugačije raspoređene. Nema nikakve redundantnosti kao kod FEC-a (jer šaljemo samo podatke koji su korisni), ali je zato i veće kašnjenje reprodukcije (jer valja rekonstruirati originalni tok iz isprepletenog).

8. Na koja od kašnjenja u prenosu paketa je moguće uticati, kako i sa kojim posljedicama?

- **Kašnjene kodiranja, kašnjenje dekodiranja**- može se uticati smanjivanjem vremena kodiranjn.a- rezultat toga je da je zahtjevani propusni opseg veći (slično i dekodiranje)
- **Kašnjenje postavljanja na link**- teoretski se može uticati povećavanjem propusnosti linka (ali ne možemo uticati na sve linkove od pošiljaoca do primaoca)
- **Kašnjenje zbog čekanja na routerima**- ne može se uticati
- **Fizičko kašnjenje- transmisiono** (koliko je potrebno da biti prođu od jedne do druge strane)- ne može se uticati
- **Na prijemniku kašnjenje odužene reprodukcije** radi otklananja varijabilnog kašnjenja- može se uticati (što je kašnjenje manje veća je interaktivnost odnosno veće su šanse da se izgube neki paketi; što je dejitter kašnjenje veće, veće su šanse da imamo kontinualnu reprodukciju, ali imamo i veće kašnjenje koje smanjuje interaktivnost)

9. Na koji način se kod SIP protokola može omogućiti da korisnik koji pokušava stupiti u kontakt sa drugim korisnikom, koji trenutno nije dostupan, bude obaviješten kad traženi korisnik postane dostupan.

-Da korisnik želi biti obaviješten kada nedostupni korisnik postane dostupan šalje putem svog proxy-a do lokacijskog registra poruku SUBSRCIBE i lokacijski servis kada traženi korisnik postane dostupan on tom korisniku šalje poruku preko proxy-a.

* Preko SIP PRESENCE opcije. Neka ovaj što hoće stupiti u kontakt bude A a drugi korisnik B. A šalje SUBSCRIBE TO B na svoj SIP server, koji će preko proxya pronaći lokacijski servis koji vidi B i njemu proslijediti SUBSCRIBE TO. On će javiti "Not signed in" jer B nije uradio sign-in, pa će se vratiti NOTIFY nazad do A koja će reći da korisnik nije prijavljen na sistem pa će se čekati da on dođe.
Kad B pokrene svojg SIP klijenta on šalje SIP REGISTER svom registrar serveru koji će uraditi UPDATE na location service. Pošto ima subscribeovanog korisnika A već, update će triggerovati NOTIFY "signed-in" ka A i tako će A dobiti informaciju da je B došao online i da ga sad može nazvati.

10. Kako odlaganje reprodukcije rješava problem varijabilnog kašnjenja mrežnih paketa kod prenosa multimedijalnih tokova koji se moraju kontinulano reprodukovati?

- Odlaganjem reprodukcije omogućava se privremeno pohranjivanje paketa čime se omogućava da paketi možda dolaze brzinom različitom od one kojom ih treba reprodukovati. Odlaganje reprodukcijom omogućava da ih možemo reprodukovati u vremenskim intervalima kako su i nastali čime se osigurava otklanjanje varijabilnog kašnjenjenja i kontinualna reprodukcija.

Osnovna ideja: Paketi dolaze brzinama koje zavise od mrežnog kašnjenja. Te brzine, odnosno vremena pristizanja, mogu biti različita od onih za reprodukciju (ako ih reprodukujemo onako kako dolaze) i u tom slučaju imamo varijabilno kašnjenje, odnosno nemamo glatku kontinualnu reprodukciju nego ih zapravo pohranjujemo tako da ih kasnije reprodukujemo ali da omogućimo tu kontinualnost.

*Odlaganjem reprodukcije za odgovarajući vremenski raspon daje se dovoljno prostora paketima da ne moraju svi doći tačno na vrijeme tj. radi se kompenzacija unaprijed.

11. Na koji način VoIP pozivalac putem SIP protokola dolazi do IP adrese pozivanog?

- Preko svog proxy-a kontaktira se proxy pozvanog koji u lokacijskom servisu pronalazi IP adresu pozvanog.

Sa svoje SIP-enabled naprave šalje INVITE za identifikator pozivane osobe na svoj proxy server. Proxy server proslijeđuje invite do proxy servera na kojeg je zakačen lokacijski servis i sama pozivana osoba. Lokacijski servis pronalazi korisničkog agenta pozivane osobe sa uređajem kojeg trenutno koristi tj. daje njegovu IP adresu i proxy ga proziva tj proslijeđuje mu invite. Korisnički agent notificira osobu o pozivu (npr. zvoni mobitel) i informacija o uspješnom dosezanju pozivane osobe se šalje preko proxya nazad do korisničkog agenta pozivatelja. Kada je invite prihvaćen, moguće je uspostaviti direktnu komunikaciju između pozivatelja i pozivanog jer su u ovom procesu razmijenjene njihove IP adrese i dogovoreno je kako će se razmjenjivati informacije.

12. Ako su trenuci slanja multimedijalnih paketa: 10, 20, 40, 55 i 60, a trenuci njihovog prijema: 110. 115, 145, 150 i 160, odrediti kada bi trebalo reprodukovati ove pakete da bi se otklonile varijacije u kašnjenju. Objasniti odgovor.

Ovo je interesantno jer su trenuci slanja različito udaljeni jedni od drugih, δ = 10, 20, 15, 5. Očito ako krenemo odmah od 110, u 120 se očekuje sljedeći i ima ga (došao u 115). U 140 se očekuje treći, ali ga nema jer dolazi tek u 145. Dodamo deltu od 5 na sve pa gledamo može li po novom. 115 prvi, OK. 125 drugi, OK. 145 treći, OK. 160 četvrti, OK. 165 peti, OK. Znači krećemo od 115 i onda radimo diffove.

13. Koji dio VoIP (SIP+RTP) sistema je klijent server, a koji P2P? Objasniti odgovor.

SIP je zasnovan na klijent-server principu (klijenti su UA's, serveri služe za lookup klijentskih UA sa trenutnim IPA), a sama razmjena podataka je P2P tj. RTP se odvija samo između pozivatelja i pozivanog (u suprotnom bi serverski kapaciteti takvog jednog sistema morali biti enormni, ovako se load distribuira po klijentima što je daleko efikasnije i brže).

14. Šta se kod VoIP komunikacije prenosi preko SIP, šta preko RTP, a šta preko RTCP protokola?

Preko SIP se prenose podaci vezani uz mehanizme za uspostavljanje i upravljanje pozivom. Preko RTP se prenose konkretni zvučni i video zapisi a kako RTP ne nudi nikakve mehanizme za osiguravanje pravovremene isporuke podataka ili druge QoS garancije (RTP enkapsulaciju vide samo krajnje tačke komunikacije ali ne i ruteri na putu) koristi se RTCP u kombinaciji sa RTP: svaki RTCP paket sadrži izvještaj pošiljatelja ili primatelja u vidu statistike korisne za aplikaciju (broj poslanih, izgubljenih paketa, razlike u kašnjenjima tj. jitter). RTCP ne definiše kako je audio/video spakovan za streaming, ne ograničava kako se stream medij transportuje (UDP vs TCP) i ne određuje kako media player koristi buffer za audio/video. Praktično, SIP je uspostava i kontrola poziva, RTP su raw podaci a RTCP nosi feedback o QoS RTP-a.

15. Šta je *jitter* i zašto predstavlja smetnju?

Jitter predstavlja varijaciju u kašnjenju paketa koji pripadaju istom medijskom toku (tzv. promjenjivo mrežno kašnjenje). Ako ne bi bilo jittera to bi značilo da svi paketi isto kasne pa bi samo na osnovu delaya prvog paketa mogli odrediti kašnjenje reprodukcije koje bi bilo fiksno i reprodukcija na klijentu bi išla konstantnom brzinom. Pošto ima jittera, nemoguće je tako nešto uraditi

16. Na predajnoj strani 6 paketa se generiše u trenucima: 1,2,3,4,5 i 6. Paketi na prijemnu stranu dolaze, po redu slanja, u trenucima 10, 12, 12, 14, 16 i 16.

a. Koje je minimalno kašnjenje reprodukcije koje će omogućiti da su svi od pristiglih paketa stigli na vrijeme za svoju reprodukciju?

b. Napraviti dinamičku procjenu prosječnog kašnjenja nakon što četvrti paket po redu stigne na prijemnu stranu, ako je dato u=0,1.

a) ti- vrijeme nastajanja

ri- stigao paket

Ti	ri	ri-ti (kašnjenje)	Reprodukcija
1	10	9	12
2	12	10	13
3	12	9	14
4	14	10	15
5	16	**11**	16
6	16	10	17

Prvi paket putuje 10-1=9
Drugi paket putuje 12-2=10
III = 12-3=9
IV = 14-4=10
V = 16-5=11
VI = 16-6=10

a) Minimalno kasnjenje reprodukcije je 11 vremenskih jedinica odgoditi reporodukciju svih paketa.

b) ovdje ima formula...

Di=(1-u)*di-1 + u*(ri-ti)

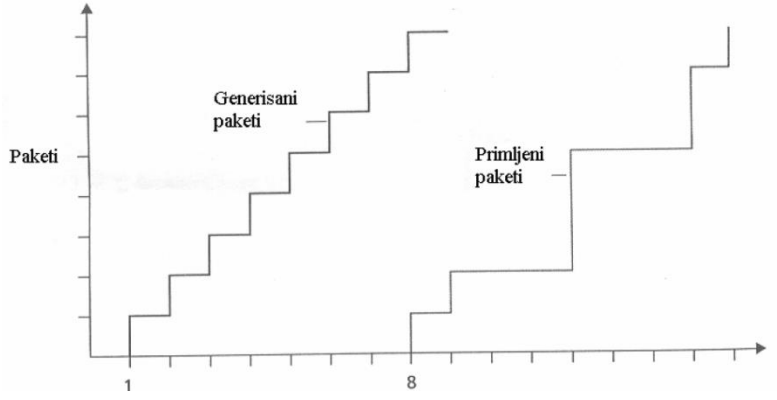
Di-> to dinamicko kasnjenje.
u - konstanta
ri - kada je dosao I-ti paket
ti - kada je poslan iti paket

b)
di=(1-u) * d i-1 + u(ri - ti)
d0=0
d1=0,9*0 + 0,1 *9 =0,9
d2=0,9*0,9 + 0,1*10=1,81
d3= 0,9*1,8 + 0,1*9= 2,2529
d4= 0,9 * 2,2529 + 0,1*9= 2,927

17. Prilikom ostvarivanja VoIP komunikacije između dva klijenta potrebno je odraditi niz koraka. Navesti po redu sve potrebne korake za uspostavljanje ove komunikacije u odgovarajućem redoslijedu:

a) Registracija klijenta na centrali
b) Instalacija RTP servera
c) Uspostavljanje veze između klijenata
d) Instalacija VoIP klijenta
e) Instalacija i podešavanje VoIP centrale
f) Dodavanje klijenta na centralu
g) Podešavanje parametara klijenta (upisivanje IP adrese centrale)
e->d->g->f->a->c

18. Prema dijagramu sa slike, pošiljalac periodično počinje da šalje pakete audio saobraćaja, počevši u trenutku t=1. Prvi paket dolazi na prijemnik u trenutku t=8.



a) Ako reprodukcija prvog paketa počinje u trenutku t=9, koji paketi neće stići na vrijeme za 'svoju' reprodukciju?
b) Koje je minimalno kašnjenje reprodukcije koje će omogućiti da su svi od pristiglih paketa stigli na vrijeme za vlastitu reprodukciju?
c) Izračunati procjenu kašnjenje za pakete od 2 do 5. Uzimati vrijednost u=0,1 (i d_0=7).

Ti	ri	ri-ti (kašnjenje)	Reprodukcija
1	8	7	9
2	9	7	10
3	12	9	11
4	12	8	12
5	12	7	13
6	15	9	14
7	15	8	15
8	16	8	16

a) Paketi 3 i 6
b) Minimalno kašnjenje = 9
c)di=(1-u) * di-1 + u(ri - ti)

19.Na predajnoj strani 6 paketa se generiše u trenucima: 1, 2, 3, 4, 5 i 6. Paketi na prijemnu stranu dolaze po redu slanja u trenucima 10, 12, 12, 14, 16 i 16.

a) **Koje je minimalno kašnjenje reprodukcije koje će omogućiti da su svi od pristiglih paketa stigli na vrijeme za svoju reprodukciju?**
b) **Napraviti dinamičku procjenu prosječnog kašnjenja nakon što četvrti paket po redu stigne na prijemnu stranu ako je dato u=0,1.**

1	2	3	4	5	6
10	12	12	14	16	16

Paket	1	-	2	3	4	-	5	6
T	10	11	12	13	14	15	16	17

Dolasci	1	-	2,3		4	-	5,6			
Paketi u usluzi		1		2	3	4		5	6	
Odlasci			1		2	3	4		5	6
T	10	11	12	13	14	15	16	17	18	19

a) Treba napraviti da nemamo slucajeva za neko t da nemamo dolazaka, npr u T=11, t=13 i t=15 nemamo dolazaka...

Pokusamo prvo tako sto cemo odgoditi reprodukciju za t=1, tj da prvi paket umjesto da dođe u 10 dolazi u t=11.

Dolasci	1	2	3	4	-	5	6	
Paketi u usluzi		1	2	3	4	5	6	
Odlasci			1	2	3	4	5	6
T	11	12	13	14	15	16	17	18

Opet moramo pomjeriti reprodukciju za t=1 jer u t=15 nema dolazaka.

Dolasci	1	2	3	4	5	6		
Paketi u usluzi		1	2	3	4	5	6	
Odlasci			1	2	3	4	5	6
T	12	13	14	15	16	17	18	19

Na osnovu ovoga vidimo da je minimalno kasnjenje reprodukcije 2 jer smo pomjerili za dvije vremenske jedinice.

b)

ti–vremenskaoznaka i-tog paketa
ri–vrijemekad je i-tipaketstigao do prijemnika
pi–vrijemekad je i-tipaketreprodukovannaprijemniku
ri–ti–mrežnokašnjenje i-tog paketa
di–procjenaprosječnogmrežnogkašnjenjapoprijemu i-tog paketa

dinamičkaprocjenaprosječnogkašnjenjanaprijemniku:

di= (1 –u)di-1+ u(ri–ti)

gdje je u izabranakonstanta (npr. u = 0,01)

traži se d4=?

d0=0
d1=(1-0,1)*d_0 + 0,1*(10-1) =0,9
d2=(1-0,1)*d_1 + 0,1*(12-2)=0,9*0,9 + 0,1*10 = 0,81 + 1 = 1,81
d3=(1-0,1)*d_2 + 0,1*(12-3)=0,9*1,81 + 0,1*9=1,629 + 0,9=2,529
d4=(1-0,1)*d_3 + 0,1*(14-4)=0,9*2,529 + 1 =2,2761 + 1=3,2761

PREDAVANJE 11 – Kontrola zagušenja i MPLS

1. Na koji način RED protokol izbjegavanja zagušenja spriječava globalnu sinhronizaciju(zajedničko ubrzavanje i usporavanje slanja velikog broja TCP konekcija)?

- Ruter koji podržava RED protokol će preventivno odbacivati pojedine pakete (prije nego što se buffer napuni) slučajnim izborom. Konekcije čiji je paket odbačen će to shvatiti kao zagušenje i smanjit će svoje brzine, ali samo te neke konekcije usporavaju tako da će ruter držati buffer na nivou da uvijek može propustiti pakete- ne dolazi do globalnog usporavanja.

Odbacivanje paketa signalizira zagušenje konekciji, s tim da je to kod RED-a "buduće" zagušenje jer RED buffer ima tri dijela - donji dio buffera je sigurna zona gdje se nijedan paket neće odbaciti. Ako je malo paketa, svi su u sigurnoj zoni i sve je OK. Onda ide zona od donjeg do gornjeg dijela u kojoj vrijedi da se paketi koji tu zaglave (jer je donja zona puna) odbacuju sa sve rastućom vjerovatnoćom, a gornji dio buffera tehnički i nije buffer jer se svi ti paketi iznad odbacuju.

2. Kakva je razlika između kontrole toka i kontrole zagušenja?

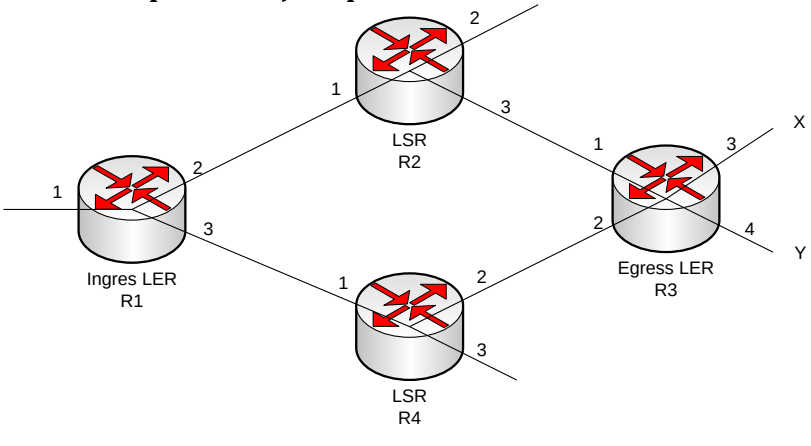
- **Kontrola toka** osigurava da pošiljalac neće slati podatke brže nego što prijemnik može da primi. Kontrola zagušenja pokušava ostvariti da pošiljalac ne šalje pakete većom brzinom nego što ih mreža može posluživati.

- Kontrola zagušenja je metod kojim se osigurava da svi čvorovi u mreži imaju "fer" pristup mrežnim resursima u svakom trenutku.

3. Na slici je prikazan dio MPLS domena. Potrebno je napraviti tabele prosljeđivanja na svim ruterima koje će omogućiti:

a. **da se paketi koji uđu u domen putem rutera R1, a odredište im je X, svrstaju u klasu proslijeđivanja x i šalju putem preko rutera R4**
b. **da se paketi koji uđu u domen putem rutera R1, a odredište im je Y, svrstaju u klasu proslijeđivanja y i šalju putem preko rutera R2**

U tabelama proslijeđivanja potrebno je navesti neophodne elemente (u zavisnosti od uloge rutera i njegovih interfejsa) kao što su odredište, ulazni i izlazni interfejs, te ulazne i izlazne naljepnice.
Ove tabele potrebno je napisati u zadaćnice sa imenom rutera.



Ruter 1

Ulazni interfejs	Izl. interfejs	Izl. naljepnica	FEC (Klasa)
1	3	50	X
1	2	20	Y

Ruter 2

Ul. interfejs	Ul. Naljepnica	Izl. interfejs	Izl. naljepnica	FEC
1	20	3	30	Y

Ruter 4

Ul. interfejs	Ul. Naljepnica	Izl. interfejs	Izl. naljepnica	FEC
1	50	2	20	X

Ruter 3

Ulazni interfejs	Ul. naljepnica	Izl. interfejs	FEC (Klasa)
2	20	3	X
1	30	4	Y

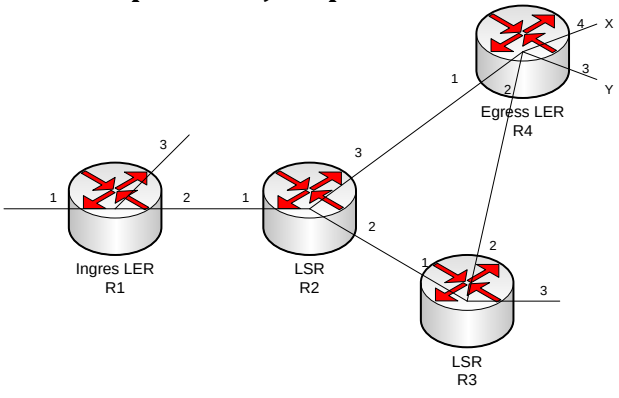
(Krenuti od posljednjeg rutera (dodjela ulaznih naljepnica).

Multiprocol Label Switching je mehanizam u telekomunikacijskim mrežama visokih performansi koji usmjerava podatke između mrežnih čvorova i njegovih susjeda na osnovu kratkih labela, a ne mrežnih adresa čime se eliminiraju složena pretraživanja tabele rutiranja. Labele određuju virtuelne linkove između udaljenih čvorova umjesto krajnjih tačaka. MPLS enkapsulira pakete različitih mrežnih protokola (djeluje između nivoa veze podataka i mrežnog nivoa). Pored toga MPLS pruža podršku za QoS, oblikovanje saobraćaja i virtuelne privatne mreže. Za labele se još koristi i naziv "naljepnice".
Naljepnice su nizovi bita stalne iste dužine koji označava tok paketa između dvije krajnje tačke ili multicast odredišta.
LER - Label Edge Router, MPLS čvor koji povezuje MPLS domen sa čvorom koji je van domena (jer ili nije MPLS ili pripada drugom MPLS domenu).
Ingress LER - MPLS čvor koji obrađuje saobraćaj koji ulazi u MPLS domen.
Egress LER - MPLS čvor koji obrađuje saobraćaj koji izlazi iz MPLS domena.
LSR - Label Switched Router. MPLS čvor koji prosljeđuje pakete sa nekog od svojih ulaza na neki od svojih izlaza na osnovu labele na paketu.
MPLS grupiše pakete u Forwarding Equivalence Class (FEC) tj. grupu paketa koji se prosljeđuju na isti način, po istoj putanji sa istim tretmanom. FEC se utvrđuje na osnovu parametara paketa, npr. IP adresa, brojevi portova, identifikatora protokola u IP zaglavlju, IPv6 flow labela i sl. Svaki FEC ima definiran traženi QoS i definisanu putanju tj. tzv. Label Switch Path kroz LSR-ove. MPLS je konekciono orijentiran. IP zaglavlje se uopće ne obrađuje, što je mnogo brže jer se radi switching umjesto routinga.
LSP je nužno uspostaviti prije početka rada sa paketima. QoS parametri definiraju se duž putanje (resursi koje se odvaja za putanju, politika čekanja i odbacivanja na LSR).
Da bi sve ovo radilo nužni su protokoli za unutrašnje rutiranje i dodjelu naljepnica. Npr. OSPF može se koristiti za unutrašnje rutiranje tj. za razmjenu informacija o vezama i putanjama. Naljepnice se može ručno dodijeliti, a postoje i protokoli LDP, nekakva proširena varijanta RSVP-a. Važno! Naljepnice imaju samo lokalno značenje tj. između susjednih MPLS rutera.
Kako se bira ruta tj. LabelSwitchPath za određenu ForwardingEquivalenceClass? Hop-by-hop ili eksplicitno. Hop-by-hop: LabelSwitchedRouter nezavisno svaki za sebe bira sljedeći hop i nije podržano oblikovanje saobraćaja ili politika rutiranja. S druge strane imamo eksplicitno biranje rute: LabelSwitchedRouter navodi neke ili sve LSR-ove u LSP za dati FEC.
Naljepnice se onda distribuira za uspostavljeni LSP: informira se sve potencijalne "uzvodne" čvorove o naljepnici koju je LSR dodijelio FEC-u.
Šaltaju se dolazne i odlazne naljepnice jer svaki ima svoj neki lokalni policy i onda se šalje sljedećem LSR duž LSP.
MPLS tabela prosljeđivanja je drugačija od IP tabele prosljeđivanja. Mapira naljepnicu sa sljedećim odredištem. Paketi između dvije iste krajnje tačke mogu pripadati različitim FEC. Pakete se prosljeđuje na izlazne interfejse samo na osnovu vrijednosti na naljepnici.

3'. Na slici je prikazan dio MPLS domena. Potrebno je napraviti tabele prosljeđivanja na svim ruterima koje će omogućiti:

a. **da se paketi koji uđu u domen putem rutera R1, a odredište im je X, svrstaju u klasu proslijeđivanja x i šalju putem preko rutera R3**
b. **da se paketi koji uđu u domen putem rutera R1, a odredište im je Y, svrstaju u klasu proslijeđivanja y i šalju putem koji ne uključuje ruter R3 (od R2 direktno ka R4)**

U tabelama proslijeđivanja potrebno je navesti neophodne elemente (u zavisnosti od uloge rutera i njegovih interfejsa) kao što su ulazni i izlazni interfejs, te ulazne i izlazne naljepnice.
Ove tabele potrebno je napisati u zadaćnice sa imenom rutera.



R1	Ulazni Interfejs	Ulazna Naljepnica	Izlazni Interfejs	Iz. Naljepnica
x	1	-	2	1
y	1	-	2	2
R2				
x	1	1	2	1
y	1	2	3	2
R3				
x	1	1	2	1
R4				
x	2	1	4	-
y	1	2	3	-

4. Neka je TCP konkecija tek uspostavljena i neka je MSS od klijenta do servera 1500 bajta. Neka klijent pošalje sedam paketa za koje dobije potvrdu, a za osmi potvrda ne stigne do isticanja vremena čekanja na potvrdu (timeout). Kolika će biti veličina prozora zagušenja nakon itseka vremena čekanja? Kolika bile veličina prozora da su prije isticanja vremena čekanja stigle tri duple potvrde za sedmi poslani paket?

Na početku konekcije veličina prozora zagušenja (CongWin) = 1MSS. Za svaku potvrdu povećaj CongWin za 1MSS → za potvrdu prvog paketa imamo CongWin = 2MSS, za potvrdu drugog imamo CongWin= 3MSS, … za potvrdu sedmog paketa imamo CongWin = 8MSS.
Onda se osmi paket izgubi tj. potvrda ne dođe u vremenu određenom timeoutom. CongWin se postavlja na 1MSS i onda bi za sljedeće pakete prozor rastao eksponencijalno do praga nakon čega bi rastao linearno.

Ako bi stigle tri duple potvrde da sedmi poslani paket, CongWin bi se prepolovio i bio bi CongWin = 4MSS nakon čega bi prozor rastao linearno sa svakim uspješno isporučenim paketom. 3 duple potvrduje ukazuju na to da mreža može isporučiti makar neke segmente tj. nije toliko zeznut scenarij kao kad dođe do timeouta.

4'. **Neka je TCP konkecija tek uspostavljena i neka je MSS od klijenta do servera 1000 bajta. Ako je klijent poslao 11 paketa, a dobio uredne potvrde za prvih osam, te dvije ponovne za osmi paket, šta se dogodilo? Kolika je veličina prozora zagušenja klijenta bila kad je poslao 11 paket? Kolika će biti veličina prozora zagušenja nakon pristizanja tri duple potvrde za osmi poslani paket?**

Inicijalno CongWin = 1MSS. Nakon prve potvrde = 2MSS, … nakon osme potvrde 9MSS. Deveta ne dolazi već se ponavljaju potvrde za osmi paket => ali dvije duple potvrde što je nedovoljno da se prepolovi CongWin (nije rečeno je li timeoutalo, u tom slučaju CongWin = 1). Dakle kad šalje 11. paket CongWin = 12 MSS. Da su došle tri duple potvrde, prepolovi se CongWin na 4.5MSS. Došlo je do značajnog zagušenja na mreži. Prelazi se u fast recovery mod, za deveti paket kad dođe potvrda biće 5.5MSS, u trenutku slanja 11 paketa CongWin = 6.5 MSS. Duple potvrde su indikator da paketi prolaze ali je prisutno zagušenje u mreži.

5. U koju fazu ulazi TCP kontrola zagušenja nakon što pošiljalac dobije tri duple potvrde za isti paket?

- Faza linearnog rasta. (Ulazi u fazu congestion-avoidance ,gdje je rast brzine linearan)

6. Šta znači „aditivno povećanje, multiplikativno smanjivanje“ kod TCP kontrole zagušenja i koja je logika ovog pristupa?

-“Adaptivno povećanje” kod TCP-a predstavlja proces u kojem TCP pokušava da poveća brzinu slanja (da postigne brzinu slanja) što veću moguće u zavisnosti od trenutnog stanja na mreži. (povećavat će brznu slanaj sve do trenutka dok neki paket ne bude izgubljen.)

Multiplikativno smanjvanje je pojava smanjivanja TCP brzine slanja zbog toga što je došlo do gubitka paketa.
Logika : Sporo se približavaj maximalnoj brzini prenosa, nakon gubitka paketa drastično smanji brzinu.
Prozor se povećava linearno za po 1 MSS, a smanjuje se bar za pola (dijeli se).

7. Kako MPLS ruter zna da li ispod naljepnica koju obrađuje ima još naljepnica?

-Na osnovu stacka, ako je stack 0 onda ima naljepnica, a ako je 1 onda nema. (Stek = S polje u paketu)

8. Mogu li različiti paketi ući u MPLS domen putem istog *ingress* LER i izaći iz MPLS domena putem istog *egress* LER, a da pri tome idu različitim putanjama kroz MPLS domen? Ako mogu objasniti kako se to realizuje i zašto može biti korisno. Ako ne mogu objasniti zašto.

-Mogu, to i jeste svrha MPLS-a. Različiti paketi sa različitim najljepnicama se šalju različitim putanjama. Korisno je što se različitim putanjama mogu slati različite vrste paketa.
A može biti korisno da se na taj način implementira neka politika QoS-a. Npr ukoliko je video stream saobracaj njega jednom putanjom (najboljom) ukoliko je neki standardni download njega drugim itd.

9. Neka se za raspoređivanje paketa na ruteru koristi cikličko raspoređivanje paketa sa težinskim faktorima koje ima četiri reda čekanja. Neka je propusnost izlaznog linka rutera na koji se primjenjuje ovo raspoređivanje 10 Mb/s, a težinski faktori redova čekanja 8,6,4 i 2. Koliku će propusnost dobiti tokovi paketa koji se raspoređuju u treći red čekanja (sa težinskim faktorom 4)?

Imamo redove čekanja Q1 {8}, Q2 {6}, Q3 {4}, Q4 {2}. Propusnost izlaznog linka rutera je 10Mb/s.
Propusnost koji dobijaju tokovi paketa raspoređeni u treći red čekanja dobijaju propusnost datu izrazom:

$$propusnost_i = \frac{w_i}{\sum w_j} * propusnostIzlaznogLinka$$

$$propusnost_3 = \frac{4}{8+6+4+2} * 10 \left[\frac{Mb}{s}\right]$$

$$propusnost_3 = 0.2 * 10 = 2 \left[\frac{Mb}{s}\right]$$

8+6+4+2= 20

4/20=1/5

1/5*10Mb/s= 2Mb/s

10. Razlika između kontrole toka i kontrole zagušenja.

Kontrola zagušenja (mrežni nivo):

- Obezbjeđuje da podmreža podnese saobraćaj
- Globalni zahtjev koji uključuje hostove i rutere

Kontrola toka (data link layer)

- Point-to-point kontrola između izvora i odredišta
- Cilj da brzi izvor ne uguši sporo odredište
- Uključuje direktnu povratnu reakciju od odredišta ka izvoru.

PREDAVANJE 12 – IPv6

1. Koja je namjena i kako se koristi polje "Slijedeće zaglavlje" u IPv6 zaglavlju?

- Namjena je da se prikaže koje je iza tog zaglavlja sljedeće zaglavlje, a sljedeće zaglavlje može biti bilo da je sadržaj paketa, bilo da je TCP/UDP ili neko do dodatnih zaglavlja. U njemu piše vrsta sljedećeg zaglavlja koje se može očekivati i dužina polja tog zaglavlja.

2. Na koji način se kod IPv6 može automatski formirati *host* dio adrese? Navesti jedan način podešavanja mrežnog dijela adrese.

- Adresa se uvijek sastoji od host dijela i dijela za mrežu. Host dio adrese se automatski može formirati na osnovu MAC adrese po EUI-64 formatu. Mrežni dio adrese se može dobiti od routera, DHCP-a, može se i automatski dobiti neka adresa.
* IPv6 nudi interesantnu mogućnost tj. tzv. stateless autoconfiguration. To omogućava mrežnim čvorovima spojenim na IPv6 mrežu da se povežu na internet bez potrebe za postojanjem posredničke podrške poput DHCP servera, ili ručnim unošenjem konfiguracije na svakom od mrežnih čvorova. IPv6 omogućava automatsko kreiranje IP adresa . Stateless se odnosi na to da će IP adresa biti jedinstvena bez obzira na trenutno stanje u mreži tj. nije potreban DHCP koji "pamti" koje je IP adrese leasovao.
SAC procedura ima sljedeće korake:
Prvo se generiše link-local adresa. Mrežnom čvoru se dodjeljuje adresa koja se sastoji od 1111111010 kao prvih 10 bita nakon čega slijede 54 nule i 64 bitni identifikator mrežnog interfejsa. On se formira na osnovu MAC adrese (48bita) koju se proširuje primjenom IEEE EUI-64 algoritma čime se MAC dograđuje do identifikatora mrežnog sučelja na jedinstven način.
Nakon toga se obavlja testiranje jedinstvenosti link-local adrese. Mrežni čvor sada pokušava osigurati da je prethodno generirana adresa jedinstvena u mreži.

Kada prođe validacija jedinstvenosti u lokalnoj mreži, IP interfejsu se dodjeljuje link-local adresa. Ona je upotrebljiva kroz lokalnu mrežu, ali ne i putem interneta (neće biti rutirana).
Potom se mrežni čvor povezuje sa lokalnim ruterom kako bi dogovorio sljedeći korak u auto-konfiguraciji. Ruter će mrežnom čvoru poslati mrežni prefiks koji će biti iskorišten za formiranje globalno jedinstvene IP adrese (uz prethodno generisanu link-local adresu).

3. Koja IPv6 adresa ima istu funkciju kao IPv4 adresa 127.0.0.1?

- Ovo je loopback adresa- adresa kojom računar pokazuje sam na sebe i to je ona sve 0 i zadnja 1. (0:0:0:0:0:0:0:1.)

4.Da li Ipv6 ima broadcast adrese? Da li ima način(adresu) na koji može poslati paket svim uređajima vezanim za neki njegov interfejs? Na koju adresu šalje paket.

- U suštini nema broadcast adresu, ali postoji način na koji može poslati paket svim uređajima vezanim za neki njegov interfejs (broadcast na inrefejsu).

5. Ima li IPv6 broadcast adresu? Na koju adresu šalje paket?

Nema, svim uređajima ili ruterima.

6. Dva osnovna dijela svake mrežne IP adrese? Kako se dođe do ovih dijelova?

- Adresa mreže i čvora u mreži
- Na ruteru preko mrežnog prefiksa, DHCP može dati adrese, mogu se ručno podesiti ili ih računari mogu generisati na osnovu MAC adrese

7. Koja zaglavlja IPv6 pregledaju?

- Hop by hop, zaglavlje rutiranja
- Destination-ne gledaju
- Fragm- ne gledaju
- Sigurnosni samo krajnji čvorovi

8. Brže procesiranje zaglavlja?

IPv6 brže od IPv4- svi paketi imaju ista zaglavlja

9. Fragmentacija kod IPv6.

Nema fragmentacije na ruterima, pošiljalac otkrije koja je najveća veliičina okvira i paket dijeli.

10. Oznaka toka prosljeđivanje->svi paketi sa istom oznakom toka moraju imati istu izvorišnu i odredišnu adresu. **Zašto**? Jer je brže.

11. IPv6 fiksno ili varijabilno zaglavlje?

Osnovno fiksno ali ima proširenja. Osnovno pregledaju svi ruteri.

PREDAVANJE 13 – Broadcast i multicast rutiranje

1. Radi čega se koristi RFP (proslijeđivanje obratnim putem) logika prilikom pravljenja *multicast* stabla?

Specifičnosti: za stablo, da se ne koriste sve putanje između rutera. Za stablo prema izvoru, da postoji različito stablo od svakog pošiljatelja do prijemnika. Za dijeljeno stablo postoji isto stablo koje koriste svi članovi grupe.
E sad, Reverse path forwarding je tehnika koja se koristi u ruterima u svrhe osiguravanja mehanizma proslijeđivanja multicast paketa kod multicast rutiranja koje ne sadrži petlje, a i kako bi se pomoglo spriječiti spoofing IP adresa kod unicast rutiranja. Oslanja se na znanje rutera o najkraćoj unicast putanji od njega do pošiljatelja. Ako je multicast paket došao po linku na najkraćoj putanji do izvorišta, onda pošalji paket na sve izlazne linkove, u suprotnom ga ignoriši i time smo se kutarisali petlji.

2. Koji protokol koriste računari i ruteri da utvrde koji računari žele biti članovi kojih *multicast* grupa, a koje protokole koriste ruteri međusobno da razmjene informacije na osnovu kojih se formiraju *multicast* stabla?

Računar i ruter koriste Internet Group Management Protocol (IGMP) da bi razmjenjivali informacije u multicast grupi. Računari šalju ruterima poruke za prijavljivanje i odjavljivanje u/iz grupe. Grupa je definirana multicast adresom, a na ruterima je da utvrde koje grupe interesiraju koje računare.
Za razmjenu informacija na osnovu kojih se formiraju multicast stabla koriste se Internet Multicasting Routing (Distance Vector Multicast Routing Procol), Multicast Extension to OSPF, te Protocol Independent Multicast.

3. U kom će slučaju ruter poslati poruku orezivanja (*prune*) po multicast stablu? Zašto baš u tom slučaju?

Ako stablo proslijeđivanja sadrži podstabla bez članova multicast grupe, ne postoji potreba da se datagrami proslijeđuju po tim podstablima pa ih je potrebno ukloniti. Radi po principu da se prune poruke šalju "uzvodno" od rutera koji nema članova grupe "nizvodno". Tj. ruteri koji ne žele grupu šalju uzvodno poruke orezivanja. Pri tome se pod "uzvodno" misli obrnutim smjerom po putanji kojom je multicast došao do rutera.

4. Da li je u mreži u kojoj je većina računara član *multicast* grupe bolje koristiti „plavi i orezuj“ (*flood and prune*) pristup ili praviti centrirano stablo, i zašto?

Ako je većina računara član multicast grupe bolje je koristiti plavi i orezuj pristup jer onda će oni koji ne žele biti članovi poslati eksplicitne zahtijeve da ih se ukloni i tih zahtijeva će biti relativno malo.
Nasuprot tome, ako je manjina računara član multicast grupe bolje je praviti centrirano stablo tj. da nema članstva u grupi do eksplicitne prijave.
Poenta je da bude što manje saobraćaja i da se sve obavi što brže. Ako pretpostavljamo većinu članova, onda neka se sami jave oni koji ne žele biti u grupi. Ako pretpostavljamo manjinu, neka se jave oni koji žele biti u grupi.

5. Na koji način se računari kod IGMP protokola prijavljuju da postanu članovi Multicast grupe. (Ko kome šalje koje poruke?)

Računari šalju ruterima poruke za prijavljivanje i odjavljivanje u grupu, a ruteri utvrđuju koje grupe interesiraju koje računare, tj. dozvoljeno je računarima da navedu od kojih računara žele dobijati saobraćaj. Saobraćaj od drugih računara je blokiran na ruterima (da se ne bi desilo da se neko može umiješati u transmisiju). Multicast ruter šalje **membership query** koji pokušava ustanoviti koje grupe imaju članove u mrežama vezanim za ruter, ima li grupa neka članove u mrežama vezanim za ruter, kao i da li uređaji vezani za ruter žele pakete poslane na određenu multicast adresu od pošiljatelja sa određene liste.

7. IGMP- Kako se prijavljuje da se postane član multcast grupe (Ko kome šalje poruke?).

IGMP- protokol gdje računari i ruteri razmjenjuju poruke.
Računari šalju poruke ruterima (žele da budu član) ili ruteri pozivaju računare

PREDAVANJE 14 – Peer to peer mreže

1. Na koji način BitTorrent stimuliše fer ponašanje (da korisnici dobijaju onoliko koliko daju)?

Tako što dozvoljava najbržim peerovima da preuzimaju chunkove torrenta od peera sa kojim su involvirani u razmjenu kroz swarm. Povremeno se tek dopusti hit'n'run. To radi na način da čvor A šalje chunkove određenom broju susjednih čvorova koji čvoru A šalju chunkove najvećom brzinom (npr. prva 4 čvora). Svakih x sekundi (npr. 10), prvih N "najboljih" čvorova se preračunava, a svakih y sekundi (npr. 30) se bira neki random čvor kojem će čvor A početi slati chunkove. Novoizabrani čvor može ući u top N čvorova, tj. radi se tzv. optimistično neograničavanje.
Efekat navedenog je da se sa većom brzinom slanja mogu naći bolji partneri za razmjenu chunkova torrenta što na kraju rezultira bržim downloadom datoteke (: čvor A random bira čvor B sa optimističnim neograničavanjem pa mu šalje chunkove velikom brzinom što uzrokuje da čvor A čvoru B postaje jedan od N prvih, na što B uzvraća održavanjem veze i bržim slanjem pa B postaje jedan od prvih N čvorova kod čvora A).

2. Na koji način se upotrebom DHT (Distribuirane *hash* tabele) pohranjuje i pronalazi neki sadržaj (za razliku od izvedbi koje imaju centralni server sadržaja ili su potpuno decentralizovane)?

DHT je distribuirana peer-to-peer baza podataka koja sadrži parove ključ-vrijednost, gdje je ključ identifikator npr. tipa sadržaja a vrijednost je IP adresa na kojoj se taj sadržaj nalazi. Peerovi rade upite nad DHT-om kako bi za ključ dobili vrijednost (sadržaj→ip adresa), a također mogu i ubacivati vlastite parove. Dodjeljuje se cjelobrojni identifikator svakom peeru koji je u opsegu od 0 do 2^n -1 tj. moguće ga je predstaviti sa n bita. Svaki ključ je cijeli broj u istom opsegu. Da se dobije cjelobrojni ključ, radi se hash originalnog ključa npr. ključ = hash("Star Wars").
Dakle, ako peer ima neki sadržaj potrebno je da mu se dodijeli par (ključ, vrijednost). Pravilo je da se dodjeljuje ključ peeru koji ima najbliži ID, a najbliži je prvi sljedebnik ključa. Npr. ako je broj bita tj. n=4, onda neka imamo peerove 1,3,4,5,8,10,12,14. Za ključ 13slijedi sljedbenik peer=14, za 15 je peer=1 itd. Svaki peer zna samo za neposrednog prethodnika i sljedbenika. Cirkularna DHT sa kraticama omogućava da se u O(log n) poruka u upitu pronađe ko je odgovoran za neki ključ tj. ko ima neku datoteku. Svaki peer pamti IP adrese prethodnika, sljedbenika i kratica.

3. Kako se kod Gnutella P2P protokola pronalazi neki sadržaj? Koje su prednosti, a koji nedostaci ovog pristupa?

Gnutella predstavlja nestruktuirani tip p2p mreže. Zasniva se na tzv. query floodingu tj. prilikom pristupanja mreži kontaktira se nekoliko drugih čvorova po nekom kriteriju kako bi postali tj. identificirali se kao susjedi novom čvoru. Pretraga se potom obavlja na način da novi čvor pita svoje susjede, koji kasnije pitaju svoje susjede. Nema fiksne strukture već se ona dinamički mijenja. Dohvatanje datoteka radi se direktno od drugog čvora na kojem se query floodingom utvrdi da dijeli datoteku.
Dakle, Gnutella je potpuno distribuirana i nema centralnog servera. Troškovi pretrage su distribuirani kroz cijelu mrežu pa je to dobro jer je dozvoljena složena obrada upita na svakom od čvorova (neće se kompleksan upit vrtiti na jednoj mašini). Nedostaci ovog pristupa je da floodanje uzrokuje da je obim pretrage prilično širok, vrijeme pretrage može biti jako dugo posebno ako se uzme u obzir da čvorovi stalno dolaze i odlaze iz mreže.

4. Na koji način CDN sistem omogućava da različiti korisnici dobiju isti objekat (isti URL) sa različitih, njima najbližih, servera?

Content Delivery Network podrazumijeva repolikaciju sadržaja na serverima širom interneta. Stavljanje sadržaja blizu korisnika smanjuje poteškoće prilikom njegovog pristupa sadržaju. CDN server je tipično u rubnoj/pristupnoj mreži. Postoji izvorišni server gdje je npr. film, a onda se on synca preko distribucijskog čvora do lokalnih CDN servera posvuda u svijetu. Stvarčica je haman transparentna za korisnika jer kad hoće sadržaj sa originalnog URL-a, kad uradi DNS upit za IP dobiće CDN-ovu IP adresu za koju se DNS resolver pobrinuo da bude "bliska" korisničkoj IP adresi.

5. Objasniti zašto distribucija datoteke korištenjem BitTorrent protokola bolje skalira od distribucije korištenjem klijent server pristupa.

Datoteka se dijeli u mnogo manjih dijelova koji se repliciraju kako ih peerovi preuzimaju. Jednom kada peer preuzme makar jedan dijelić, on ga može dijeliti sa drugim peerovima. Time je omogućeno istovremeno preuzimanje tj. preuzimanje različitih dijelova datoteke od različitih peerova u isto vrijeme.
Na taj način je opterećenje distribuirano preko peerova a nije lokalizirano na jedan (ili više) servera, a i gubitak u slučaju grešaka u prenosu je manji jer otpadaju tek djelići ukupnog sadržaja. Jedini problem je inicijalna razmjena datoteke između originalnog izvora i prvog skupa leechera.

6. Po čemu su Kazaa mreže slične Gnutella, a po čemu Napster mrežama?

Napster: centralni direktorij sa kojim kontaktiraju klijenti koji u direktorij registruju listu datoteka koje dijele. Klijenti direktorije mogu pretraživati, kada pronađu što žele Napster identificira klijienta koji je online i ima datoteku, šalje njegovu IP adresu i onda dva klijenta (tačnije klijent i ponuđač) dogovaraju razmjenu i prijavljuju status Napsteru. Centralni direktorij je slaba tačka sistema. Ukratko za Napster: prijenos datoteka decentraliziran, ali je lociranje sadržaja isključivo centralizirano.

Gnutella: isključuje publishovanje vlastitog sadržaja na središnji direktorij, pretraga je decentralizovana, sadržaji su poznati samo na peerovima. Centralna tačka služi samo da se susjedi dozovu.

KaZaA: na početku klijent kontaktira super-čvor i šalje mu svoju listu datoteka (Join & Publish). Pretraga (Search) ide preko super-čvora, ako nema u lokalnom, ide do susjednih super-čvorova (flood pretraga). Dohvatanje ide direktno od peerova, može čak i više odjednom (Fetch). Svaki peer je ili vođa grupe ili je dodijeljen vođi grupe koji prati sadržaj kod svoje "djece". Svaki peer je povezan sa vođom grupe, a postoje i veze između nekih parova vođa grupa (TCP veze naravno).
Sada o sličnostima i razlikama: KaZaa i Gnutella: oboje imaju decentraliziranu pretragu mada različito implementiranu (Kazaa ide preko super čvorova koji imaju lokalne spiskove sadržaja svih susjeda, a Gnutella ide floodingom kroz sve čvorove). Kazaa i Napster: sadržaji su samo na peerovima i pretraga nije baš decentralizovana tj. postoje lokalne vođe grupa kojima su poznati spiskovi datoteka u lokalnoj grupi.

7. Koje elemente Gnutella i Napster pristupa objavljivanju i pretrazi sadržaja koristi Kazaa i na koji način?

Kazaa koristi Napsterov pristup da postoji neka centralna tačka u kojoj se bilježe sadržaji peerova, ali je Gnutellin "dodatak" na to u tome da centralna tačka nije globalni direktorij već samo lokalna grupa, pa se onda niz centralnih tačaka vezuje kako bi se uspostavila globalna mreža. Isto tako centralne tačke su opet sami peerovi samo koji su često online i imaju dobre linkove, tako da su zakonski pokriveniji u odnosu na Napsterov centralni firmin direktorij. Pretraga ide floodingom preko peerova, kod Gnutelle preko svih a kod Kazaae preko superčvorova.

8. Koji problem rješavaju Distribuirane *hash* tabele?

Problem skaliranja do ogromnog broja čvorova u mreži i problem opsluživanja cijele mreže u situaciji kada čvorovi stalno dolaze, odlaze ili postaju nedostupni uslijed grešaka. DHT je distribuirana baza podataka pa je odgovornost na održavanje i mapiranje između ključeva i vrijednosti distribuirano između čvorova na takav način da promjena u skupu članova mreže uzrokuje minimalne poremećaje. Nema nikakve centralne koordinacije.

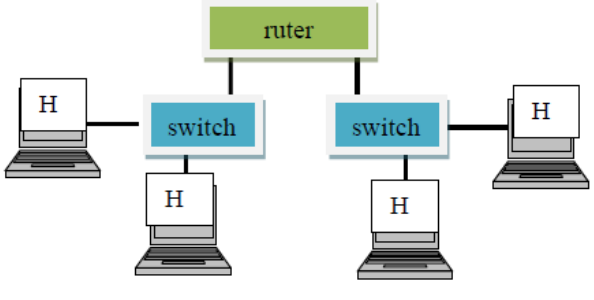
PITANJA SA VJEŽBI

1. Prilikom ostvarivanja VoIP komunikacije između dva klijenta potrebno je odraditi niz koraka. Navesti po redu sve potrebne korake za uspostavljanje ove komunikacije u odgovarajućem redoslijedu:

a. Registracija klijenta na centrali
b. Instalacija RTP servera
c. Uspostavljanje veze između klijenata
d. Instalacija VoIP klijenta
e. Instalacija i podešavanja VoIP centrale
f. Dodavanje klijenata na centralu
g. **Podešavanje parametara klijenta (upisivanje IP adrese centrale)**

e. f. d. g. a. c.
Instalacija i podešavanje VoIP centrale, dodavanje klijenata na centralu, instalacija VoIP klijenta, podešavanje parametara klijenta, registracija klijenta na centrali i uspostavljanje veze između klijenata.

2. Potrebno je ostvariti komunikaciju između svih računara u predstavljenoj mreži. Napisati sve potrebne postavke za pojedine uređaje u mreži kako bi ova komunikacija bila moguća. Mreža nije povezana na Internet. Nije potrebno pisati komande za pojedine uređaje već završne postavke – IP adrese za sve interfejse, subnet maske, gateway, ... Kratko objasniti sve navedene parametre i njihovu ulogu (na po jednom računaru iz svake mreže i na ruteru)



Konfiguracija hosta = (IP adresa, subnet maska, default gateway) - dns izostavljam.

H1 (192.168.1.2, 255.255.255.0, 192.168.1.1)
H2 (192.168.1.3, 255.255.255.0, 192.168.1.1)
H3 (192.168.2.2, 255.255.255.0, 192.168.2.1)
H4 (192.168.2.3, 255.255.255.0, 192.168.2.1)
Switch plug 'n play.
Router:
iface 1 ip=192.168.1.1 sm=255.255.255.0 iface 2 ip=192.168.2.1 sm=255.255.255.0
tablica rutiranja: 192.168.1.0/24 na iface 1, 192.168.2.0 na iface 2.

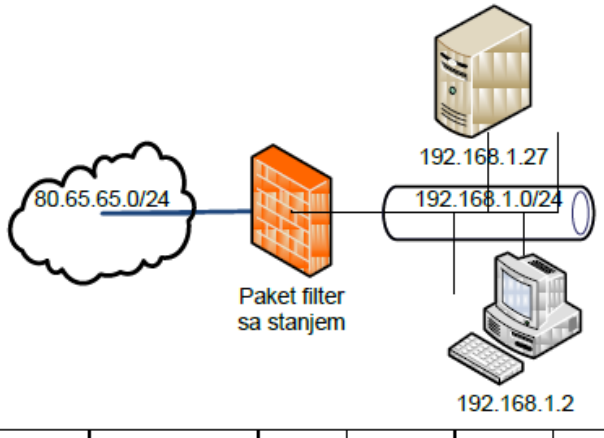
3. Navesti dvije vrste listi za kontrolu pristupa (ACL) koje koristi CISCO i razlike između njih. Napisati ACL koja dozvoljava IP adresu 192.168.0.7/16 a zabranjuje sve ostale IP adrese u tom subnetu (treba napisati samo pravilo/a u sklopu ACL, ne pisati komande).

Standardne i proširene (standard and extended ACL). Standardne ACL mogu blokirati saobraćaj samo na osnovu IP adrese hosta ili cijelog subneta, tj. nije moguće filtrirati pakete na osnovu odredišta za paket. Proširene ACL su fleksibilnije i omogućavaju filtriranje paketa na osnovu i IP adresa, i subneta, i protokola i portova.
Standardna:
access-list *access-list-number* **{permit|deny}**
{*host*|*source source-wildcard***|any}**

4. Šta su liste za kontrolu pristupa (ACL)? Napisati ACL koja zabranjuje IP adresu 192.168.0.2/24 a dozvoljava sve ostale IP adrese u tom subnetu (treba napisati samo pravilo/a u sklopu ACL, ne pisati komande).

ACL je tabela pravila primjenjivih po redoslijedu kojim su zapisana odozgo nadole na sve pakete na koje se filtriranje primjenjuje. Sastoji se od parova oblika (akcija, uslovi).
{akcija, src ip, dst ip, protokol, src port, dst port, flag bit} = [(deny. 192.168.0.2, any, any, any, any, any), (allow, any not 192.168.0.2, any, any, any, any any)];

5. Dvije mreže na slici povezane su sa paket filter *firewall*-om sa stanjem i sa tabelom stanja datom u tabeli



Izvorišna adresa	Odredišna adresa	Protokol	Izvor. port	Odr. Port	Timeout
192.168.1.2	80.65.65.66	TCP	2853	80	60
192.168.1.27	80.65.65.70	TCP	3241	53	50

Odrediti da li će slijedećim paketima biti dozvoljen ili zabranjen prolaz (na osnovu tabele stanja) i objasniti zašto:

a. **80.65.65.70:80 -> 192.168.1.27:3241 (TCP)**
b. **80.65.65.66:80 -> 192.168.1.2:2853 (TCP)**
c. **80.65.65.70:53 -> 192.168.1.2:2853 (TCP)**

Pretpostavimo da tabela stanja označava Dozvoli a ne Zabrani.

Podrazumijevam da se pravila primjenjuju sekvencijalno odozgo prema dole te da prioritet imaju specifičnija/konkretnija pravila
Paket a) će biti odbijen jer iako postoji konekcija na relaciji 80.65.65.70 < = > 192.168.1.27, odredišni port se ne poklapa (80 vs 53) .
Paket b) će biti prihvaćen.
Paket c) će biti odbijen jer ne postoji konekcija na relaciji 80.65.65.70 < = > 192.168.1.2.

6. Koje parametre treba podesiti na Juniper SSG5 ruteru da bi se omogućilo IPv6 adresiranje u mreži?

Telnet na ruter → set envar IPV6=yes → save → reset. Pronaći bgroup0 interfejse i izmijeniti postavke za IPv6, dodijeliti unicast address prefix /64, npr. fe80::/64. Dozvoliti RA. (lulz).

7. Na koji način je na laboratorijskoj vježbi u sklopu koje je obrađo IPv6 adresiranje provjerena konektivnost između dva računara sa IPv6 adresama (koja je razlika između ove provjere kod IPv4 i IPv6)?

Mora se koristiti ping -6 komanda kao u sljedećim primjerima:
ping -6 www.cyberciti.biz
ping -6 2607:f0d0:1002:51::4

8. Na koji način je na Netgear-u na laboratorijskim vježbama omogućen pristup iz vanjske mreže aplikaciji koja se izvršava u unutrašnjoj mreži na računaru sa IP adresom A i osluškuje na portu B?

Aplikacija mora biti na računaru koji ima statičku IP adresu A, a onda se uključi port forwarding po portu B kad dođe paket na IP adresu Netgeara:B, da se usmjeri saobraćaj na A:B (ako hoćemo da budu isti portovi, a i ne moraju). Odabere se i jel' TCP ili UDP.

9. Šta je potrebno uraditi da bi se zabranio ftp pristup prema vani iz lokalne mreže na Netgear FR328S uređaju korištenom na laboratorijskim vježbama.

Dodati unos u ACL koji će blokirati sav odlazni saobraćaj po portovima 20 i 21 bez obzira na odredišnu IP adresu. Ako već ima odgovarajući unos koji to dozvoljava, obrisati ga.