Projektovanje računarskih mreža

Ispitna pitanja (2020/21.)

**+1. Pravilo 5-4-3-2-1 i određivanje minimalne dužine Ethernet frejma za 100BaseT standard.**

Naziv 5-4-3-2-1 (često i samo 5-4-3) je posledica činjenice da je na jednom kolizionom domenu moguće imati pet mreža povezanih pomoću četiri veze, od kojih su tri mreže sa računarima, preostale dve mreže bez računara.

Nije moguće detektovati koliziju ako je rastojanje između računara veće od “dužine” minimalnog frejma. Naime, paket ima svoju “dužinu” u bitovima (oko 64 bajta). Moguće je jednostavno izračunati “trajanje” jednog bita ako se uzme u obzir brzina mreže. Na primer, ako je mreža gigabitna, radi se o 109 bitova usekundi, pa je trajenje jednog bita 10−9 s = 1 ns.

Kada se 64 bajta pretvori u bitove i ta vrednost pomnoži jednom nanosekundom, dobija se vreme koje je neophodno da se pošalje jedan frejm (vremenski interval između trenutka kada prvi i poslednji bit napuste mrežnu karticu). To vreme mora biti dovoljno da vrh frejma pređe put do odredišnog računara kako ne bi došlo do kolizije. Zbog ovoga je dužina kabla ograničena Eternet standardom u zavisnosti od brzine protoka podataka kroz kabl.

Konkretno, ako se radi o mreži sa najviše pet segmenata po 100 metara povezanih ripiterima, i ako se uzme da je brzina prostiranja talasa kroz vodove 3 × 10^8 m/s, dobija se da je ukupna dužina segmenta L = 2 × 500 m = 1000 m. Pošto znamo vreme trajnja jednog bita, možemo da odredimo dužinu jednog bita.

B = 100 · 10^6 b/s

Tb = 1/B = 10^−8

Sb = V · Tb = 3 · 10^8 · 10^−8 m = 3 m

F = L/Sb = 334 b = 42 B

(uzeli su malo iznad toga)

B je brzina mreže, Tb je trajanje jednog bita, i F je ukupan broj bitova. Zato je Ethernet između 46 i 1500 bajtova.

**+2. Na primeru 1Gbps mreže objasniti kontrolu toka zadavanjem veličine prozora kod TCP protokola, ako je potrebno vreme za put paketa od izvora do odredišta i nazad 1ms.**

Kritično vreme je vreme za propagaciju nazad i vreme dok se računar B “smisli” da treba da primi odgovor. Oznake su sledeće:

• tp – vreme potrebno za slanje paketa od računara A do računara B,

• to – vreme obrade,

• tf – vreme za slanje jednog frejma,

• tw – vreme potrebno za slanje celog prozora

U jednom frejmu postoji F = 1500 B = 12 · 10^3 b podataka.

**trtt (round trip time)** uključuje: vreme potrebno da frejm stigne, da se obradi i da se vrati. trtt = 1ms

Iz tw = tp + w · tf + to + tp sledi da je:

tw = trtt + w · tf .

Realna brzina je količina informacija koja je provedena kroz mrežu za određeno vreme. Dakle, realni throughput je H = I/tw, pri čemu je I količina informacija koja je preneta.

Dakle, vreme trajanja jednog frejma iznosi

tf = 12 · 10^3/10^9 = 12 · 10−6 s.

Prenos celog paketa informacija se može izračunati po formuli

tw = trtt + w · tf

Za različite vrednosti w jer su svi podaci sa desne strane jednakosti poznate.

Na primer, za w = 1 dobija se tw = 10^−3 s + 12 · 10^−6 s ≈ 1 ms.

Odavde je I = 1 · 12 · 10^3 b i H = 12 · 10^6 b/s = 12 Mb/s. Slično, za w = 65535, dobija se tw = 0.788 s, kao i I ≈ 787 · 106 b i H = 0.998 Gb/s

**+3. Hierarhijski model i enterprise arhitektura: logička i fizička struktura, nivoi, karakteristike, dostupnost.**

Prednosi hijerarhijskog modela su:

• **skalabilnost,**

**• redundansa,**

**• performanse,**

**• bezbednost,**

**• upravljivost i**

**• održavanje.**

**Logički** je mreža podeljena na tri sloja: *pristupni (access), distribucioni (distribution) i središnji (core)*. *Pristupni* sloj omogućuje povezivanje kranjih korisnika. *Distribucioni* sloj se koristi za prosleđivanje sa jedne lokalne mreže na drugu. Središnji nivo je brza okosnica između rasutih mreža. Saobraćaj inicira korisnik na prisutpnom sloju i on prolazi kroz druge slojeve ako je funkcionalnost tih slojeva potrebna. Za potrebe manjih mreža, središnji i distribucioni sloj se stapaju u jedan, što smanjuje cenu i kompleksnost.

**Enterprajz arhitektura** deli mrežu na funkcionalne komponente, ali i dalje zadržava tri gore pomenuta sloja.

Primarni moduli su:

* **Enterprajz kampus** – Sastoji se od cele infrastrukture kampusa, i uključuje sva tri sloja iz hijerarhijske strukture. Modul pristupnog nivoa sadrži svičeve drugog ili terćeg sloja odgovarajuće gustine portova.Ovde se implementiraju VLAN-ovi i trunkovi. Redundansa igra veliku ulogu. Rutiranje, kontrola pristupa, kvalitet servisa, itd. se takođe podešavaju ovde. Pored ovih modula, enterprajz kampus može sadržati i neke podmodule:
  + **Farma servera i datacentar modul** – Pružaju brzu vezu i zaštitu usluga. Kritično je obezbediti bezbednost, redundansu i toleranciju na greške.
  + **Moduli za servise** – Ova oblast pruža pristup svim servisima, kao što su IP telefonija, bežični servisi, itd.
* **Enterprajz ivica** – Ivica se sastoji od interneta, VPN-a, i WAN modula koji povezuju enterprajz servise sa udaljenim sajtovima i omogućavaju enterprajzu korišćenje interneta i partnerskih resursa.
* **Ivica provajdera** – Pruža internet, PSTN i WAN servise. Svi podaci koji ulaze u ili izlaze iz ECNM-a (Enterprise Composite Network Model ) prolaze kroz ivični uređaj. Ovo je tačka gde svi paketi mogu da se ispitaju i da se napravi odluka o tome da li paketu treba dozvoliti ulaz u i izlaz iz interprajz mreže.

**Dijametar mreže** je parametar u projektovanju mreže i predstavlja maksimalan broj uređaja kroz koje podaci mogu proći na mreži. Dijametar u hijerarhijskom modelu iznosi 6, mada se u nekim slučajevima računa i kao 7 (zbog eventualnog dodavanja uređaja).

Nekoliko fizičkih portova se može agregirati u jedan virtuelni port čiji je propusni opseg jednak proizvodu broja portova i propusnog opsega pojedinačnog porta. Tehnologija se zove Link Aggregation, a u Ciscovoj implementaciji EtherChannel. Protokoli koje svič treba da podrži su PAgP (Cisco vlasnički protokol) ili LACP (IEEE standard).

**Redundantnim vezama** i komponentama se postiže veća pouzdanost i dostupnost mreže. Cilj svake mreže je obezbediti da mreža bude dostupna preko 99.999% vremena (odnosno smanjiti MTBF – mean time between failures).

**Konvergencija mreže** je pojam kojim se ukazuje na osobinu savremenih mreža da prenose različite tipove saobraćaja, za koje su ranije korišćene različite mreže, a koji na ovakvoj mreži predstavljaju konkurenciju jedni drugima za propusnim opsegom na mreži. Na primer, istovremeni prenos glasa, video-materijala i datoteka.

**+4. Ethernet i prosleđivanje frejmova: half i full duplex mod, tehnike baferovanja i lokacije bafera.**

Pod dupleks komunikacijom podrazumeva se smer prostiranja podataka između dva uređaja. Postoji **poludupleksna** i **punodupleksna** komunikacija.

* Kod **poludupleksne** komunikacije, oba uređaja mogu da primaju i predaju podatke na medijumu, ali to ne mogu raditi istovremeno. Ovaj režim se koristi u zastarelim topologijama magistrale (bus topology) i sa Eternet habovima. WLAN-ovi takođe rade u poludupleksu. Poldupleks dopušta samo jednom uređaju da šalje i prima podatke u jednom trenutku.
* Kod **punodupleksne** komunikacije, oba uređaja mogu da primaju i predaju podatke istovremeno. Sloj veze podataka pretpostavlja da je medijum dostupan za ransmisiju za oba čvora u bilo kom trenutku. Eternet svičevi rade u punodupleksnom režimu po podrazumevanim podešavanjima, ali mogu raditi i u poludupleksnom režimu ukoliko se povezuju na uređaj kao što je hab.

Važno je da sa obe strane linka budu isti režimi dupleksne komunikacije.

Konfiguracija se obavlja na interfejsu. Na primer, port FastEthernet 0/1 može se podesiti u “automatski” režim rada na sledeći način.

S# configure terminal

S(config)# interface f0/1

S(config-if)# duplex auto

S(config-if)# end

Tehnike za prosleđivanje frejmova kroz svičeve su sledeće.

* **Store-and-forward**. Ceo frejm se pamti u bafer prilikom dolaska frejma, računa se CRC, pa tek ako je CRC u redu, onda se prosleđuje frejm. Na ovaj način se ne opterećuje drugi kolizioni domen ako dođe do bilo kakve , ali je s duge strane veća latencija.
* **Cut-through**. Svič počinje da šalje frejm čim dobije odredišnu MAC adresu i proveri MAC tabelu. Latencija se ovime smanjuje, ali postoji mogućnost prosleđivanja neispravnih frejmova.
* **Fragment free.** predstavlja kompromis. Baferuju se samo prva 64 bajta. Na ovaj način se ne proverava sve, a sprečava prosleđivanje u slučaju nastanka kolizije.

Postoje dve tehnike baferovanja:

* **Port-based memory.** Frejmovi se čuvaju u redovima koji su povezani na određene ulazne i izazne portove.
* **Shared memory.** Svi frejmovi se čuvaju u zajedničkom baferu koji dele svi portovi.

**+5. Kontrola toka pri komunikaciji uređaja na portovima sa različitom brzinom asimetričnog sviča.**

Asimetrični svičevi obično imaju jedan ili dva porta koji su mnogo brži od ostalih. Preko njih se povezuju sa ostatkom mreže, dok se oni od 100 Mb/s koriste za korisnike.

Server počinje da šalje podatke brzinom od 1 Gb/s. Međutim, svič ima konačne bafere – kada se oni prepuni, frejmovi počinju da se gube. Svič ni na koji način ne vodi računa o tome: nema mehanizam oporavka. Kada se frejm izgubi, traži se rertransmisija i tada se smanjuje veličina prozora, a samim tim i brzina. Frejmovi će biti gubljeni sve dok se veličina prozora ne smanji toliko da brzine bude 100 Mb/s, iako je mreža gigabitna.

Dakle, neusaglašenost brzine se rešava TCP protokolom.

**+6. Pristup i zaštita od neovlašćenog pristupa.**

Podešavanje konzolne šifre od korisnika zahteva njen unos prilikom povezivanja na uređaj preko konzole. Ovo ne predstavlja apsolutnu zaštitu jer postoje metode za oporavak šifre koje napadač može da iskoristi ukoliko ima fizički pristup uređaju.

S# config terminal

S(config)# line console 0

S(config-line)# password cisco

S(config-line)# login

Zaštita pristupa preko telneta zahteva podešavanja VTY (Virtual Terminal Line) šifre. Na ovaj način se aktivira telnet server na ređaju.

S# config terminal

S(config)# line vty 0 4

S(config-line)# passord cisco

S(config-line)# login

Zaštita privilegovanog moda obavlja se komandom enable password, jer se u privilegovani mod ulazi pomoću komande enable. Ukoliko ova šifra nije podešena, nije mouguće telnetovati se na uređaj (bez obzira na to što je podešena IP adresa i VTY linije).

S(config)# enable secret cisco

Sve šifre je moguće videti prilikom listanja konfiguracije naredbom show run. Zato je dobro enkriptovati šifre.

S(config)# service password-encryption

Međutim, telnet šalje podatke u izvornom obliku i nije bezbedan protokol. Napadač može prislušktivati mrežu i otkriti sve naredbe koje se šalju, zajedno sa šiframa i drugim osetljivim informacijama. Zato se preporučuje korišćenje SSH protokola.

S(config)# ip domain-name cisco

S(config)# crypto key generate rsa

S(config)# ip ssh version 2

S(config)# line vty 0 15

S(config-line)# transport input ssh

Komanda transport input ssh će isključiti mogućnost pristupa putem telneta. Ako treba da rade i SSH i telnet paralelno, treba iskoristiti komandu transport input all.

+7. Primeri napada: MAC spoofing i floding, i DHCP spoofing.

Postoje tri najčešća napada.

* Kod **MAC spoofing** napada, napdač može poslati lažan frejm sa proizvoljnom MAC adresom u polju za izvorište. Na ovaj način može da se predstavi kao neki drugi računar.
* Čak i ako ne zna nijednu MAC adresu, može da pošalje veliki broj frejmova sa nasumice generisanim MAC adresama i time preplavi MAC tabelu u svičevima, odnosno prepuni memoriju. Zbog toga se ovaj napad zove **MAC flooding**. Kada se memorija prepuni, svič počinje da se ponaša kao hab što znači da će se svi paketi brodkastovati na sve izlazne portove. Ovo ne samo da usporava mrežu, već i omogućuje napadaču da prisluškuje svaki vid komunikacije na mreži.
* **DHCP spoofing.** Napadač može konfigurisati DHCP server na mreži. U tom slučaju, kad korisnik zahteva adresu od DHCP servera, lažni DHCP može da odgovori pre pravog (što se postiže brzim iscrpljivanjem adresa sa pravog servera kako on višene bi odgovarao na zahteve) i time napadač ima kontrolu nad IP konfiguracijom korisnika. Ovo znači da može podesiti adresu napadača kao default gateway i time presretne sve pakete. Kao odbrabeni mehanizam, portovi sviča se mogu podesiti kao bezbeni i nebezbedni (koji mogu da šalju DHCP zateve/odgovore i koji to ne mogu da rade). Ovo se aktivira komandom ip dhcp snooping

**+8. Bezbednost na nivou svič-porta.**

Portove sviča treba zaštiti tako da mogu da im pristupe samo ovlašćeni korisnici. Na primer, može se podesiti koja adresa je dozovljena na jednom portu, ili koliko različitih adresa je dozvoljeno na njemu.

Postoji tri načina za zadavanje statičkih MAC adresa:

• **Ručno ili statičko** podešavanje MAC adrese je najjednostavnije ali i najmukotrpnije. Treba ručno upisati MAC adresu ulaskom na port.

• Dozvoljene MAC adrese je moguće konfigurasati i **dinamički** ukoliko postoji server na mreži koji vodi računa o tome ko gde može da pristupi, a adrese se dinamički uče na portu.

• Najčešći način konfiguracije je lepljivi (**sticky**). MAC adrese se po pristupu dinamički lepe za port. Kada svič nauči MAC adresu, on je snimi u svoju running konfiguraciju, isto kao da je statički zadata. U praksi se ovo primenjuje tako što se ovaj režim ostavi na oko nedelju dana sa ograničenjem 100 da bi se osiguralo da su se svi redovni korisnici barem jednom nakačili na mrežu, a zatim se maksimalan broj MAC adresa smanji da odgovara broju za to vreme naučenih adresa.

Ima nekoliko načia na koji svič može da reaguje kada dođe do prekršaja na portovima.

• **Protected** jednostavno ignoriše saobraćaj. Ne prosleđuje ga, ne beleži prekršaje, i ne gasi port.

• **Restrict** obaveštava adminisratora o tome da je došlo do prekršaja, ali svič nastavlja da radi nomalno.

• **Shutdown** ne samo da alarmira administraciju o nastalom prekršaju, već i gasi port.

Na primer, podešavanje lepljivog porta sa najviše 50 dozvoljenih MAC adresa je dato u nastavku.

S(config)# interface f0/0

S(config-if)# switchport mode access

S(config-if)# switchport port-security

S(config-if)# switchport port-security max 50

S(config-if)# switchport port-security mac-address sticky

Obratiti pažnju da je pored zadavanja parametara, zaštitu neophodno i aktivirati.

**+9. Brotkast domeni i razdvajanje brotkast domena**

Brodkast domen je pojam koji definiše veličinu jedne lokalne mreže. To je skup mrežnih uređaja do kojih se prostire brodkast poruka poslata sa nekog od njih. Brodkast domeni se poistovećuju sa lokalnom mrežnom zbog ARP-a.

Pretpostavimo da jedan računar pinguje drugi. Kada ping krene sa aplikativnog nivoa naniže, u jednom trenutku dolazi do sloja 3. Ping se obavlja po IP adresi, ali za spuštanje paketa na sloj 2 neophodna je MAC adresa. Da bi se saznala MAC adresa odredišta, neophodno je poslati brodkast zahtev (ARP). Sve dokle se “čuje” ovaj ARIP zahtev, ima misla pričati o lokalnoj mreži.

Da bi se paketi rutirali između mreža, neophodan je **ruter**.

Problem sa velikim brodkast domenima jeste to što hostovi mogu da generišu mnogo brodkasta, što može negativno uticati na mrežu. Rešenje kojim se smanjuje veličina mreže i prave se manji brodkast domeni jeste kreiranje podmreža. Na primer, mrežu 172.16.0.0/23 možemo podeliti na dve podmreže, 172.16.0.0/24 i 172.16.1.0/24.

Međutim, ukoliko je potrebno da korisnici na različitim lokacijama pripadaju istom brodkast domenu, teško je takvu mrežu projektovati na “klasičan” način. Iz operativnog sistema upravljivih mrežnih svičeva, moguće je administrativno razdvojiti portove u različite brodkast domene. Ovime se kreiraju **virtuelne mreže** – to je administrativno definisani skup portova na svičevima koji pripadaju istom brodkast domenu. Ipak, i ovako razddvojeni brodkast domeni mogu imaju međusobnu komunikaciju jedino preko rutera.

**+10. Označavanje, tipovi i namena VLAN-ova.**

Postoji normalni i prošireni opseg ID brojeva koji se mogu dodeliti VLAN-ovima. Brojevi od 1 do 1005 prpadaju normalnom opsegu. Vlanovi sa rednim brojevima 1, 1002, 1003, 1004 i 1005 se automatski kreiraju i nije ih moguće obrisati. Čuvaju se u datoteci vlan.dat u fleš memoriji. Brojevi od 1006 do 4094 su dizajnirani za uslužitelje i imaju manje opcija nego normalni vlanovi. Čuvaju se u konfiguracionoj datoteci.

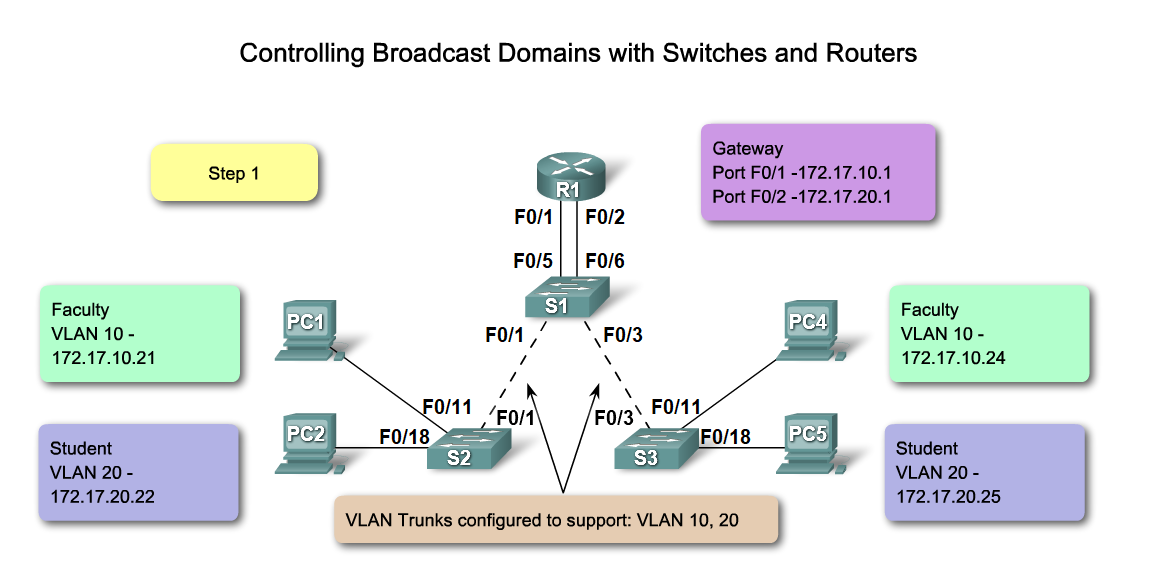
**11. Modovi za dodelu porta sviča VLAN-u.**

**Statički** - Administrator dodeljuje koji port je na kom broadcast domenu

**Dinamički** - Imamo server koji pamti preslikavanja (Mac adresa i vlan kome uređaj pripada), dinamički se prilikom dolaska uređaja na mrežu port se postavlja na određen vlan koji mu server odredi. Korisno na veliku mrežu sa puno switch-eva.

**Voice** - Specijalan tip, nalaze se na jednom portu 2 vlana , jedan za podatke a drugi za voice.

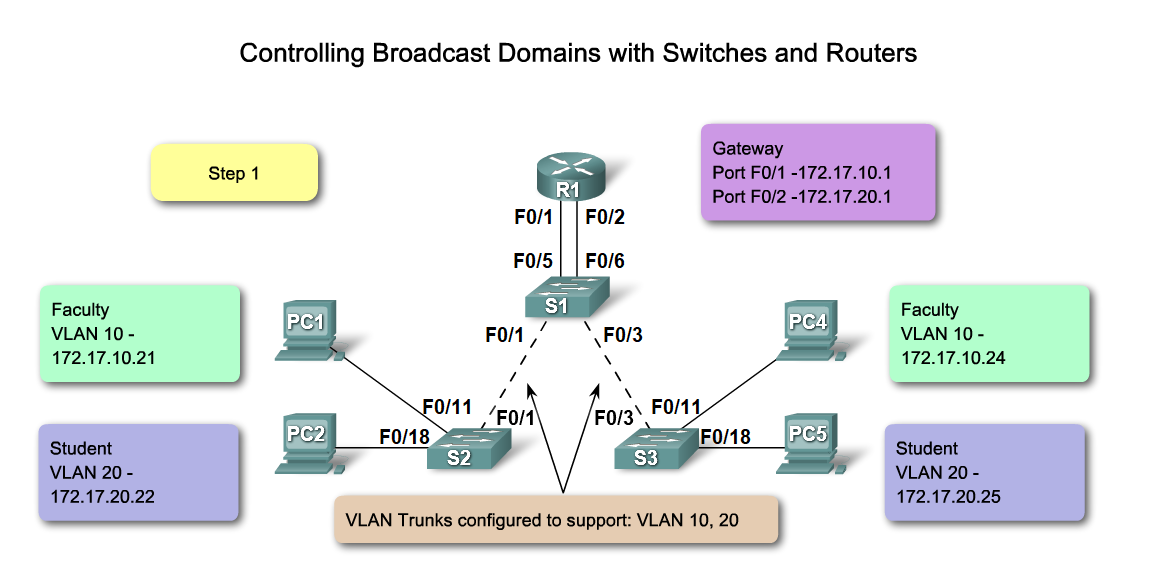
**12. Na proizvoljno izabranom primeru objasniti komunikaciju računara na istom VLAN-u, ako su računari na različitim svičevima (intra-VLAN).**



U ovoj slici PC1 želi da komunicira sa PC4. PC1 i PC4 su zajedno u VLAN 10.

1. PC1 u VLAN10 šalje ARP request paket (broadcast) na S2. Switch s2 i s1 šalju ARP request paketna sve portove VLAN-a 10. Switch S3 šalje ARP paket do PC4 koji je u VLAN 10.
2. Switch-evi u mreži prosleđuju nazad ARP reply paket do PC1. PC1 prihvati reply koji sadrži MAC adresu PC4
3. PC1 sada sadrži MAC adresu od PC4 i koristi ga da napravi unicast okvir sa PC4 MAC adresom kao njegovo odredište. Switchevi S2, S1 i S3 prosleđuju frame do PC4.

**13. Na proizvoljno izabranom primeru objasniti komunikaciju računara na različitim VLAN-ovima (inter-VLAN).**



U ovoj slici PC1 u VLAN 10 želi da komunicira sa PC5 koji je na VLAN 20.

1. PC1 u VLAN 10 želi da komunicira sa PC5 koji je na VLAN 20. PC1 šalje ARP request frame da dobije MAC adresu gateway-a R1.
2. Ruter R1 odgovara sa ARP reply frame sa svog interface-a koji je na VLAN 10. Svi Switchevi proslede ARP reply i PC1 ga primi. ARP odgovor sadrži MAC adresu default gateway-a
3. PC1 kreira ethernet frame sa MAC adresom default gateway-a kao odredište. Frame prolazi kroz switch S2 i S1.
4. Ruter R1 šalje ARP request frame na VLAN 20 da dobije MAC adresu PC5. Switch-evi S1, S2, S3 šalju arp request na sve portove koji su konfigurisani za VLAN 20. PC5 prima request frame od R1 rutera.
5. PC5 na VLAN 20 šalje ARP reply frame na S3. S3 i S1 prosleđuju ARP reply do rutera R1.
6. Ruter R1 šalje Ethernet frame koji je primio od PC1 kroz Switch S1 i S3 do PC5 na VLAN 20.

+**14. L3 svičevi.**

-2 uređaja odjednom (ruter i switch)

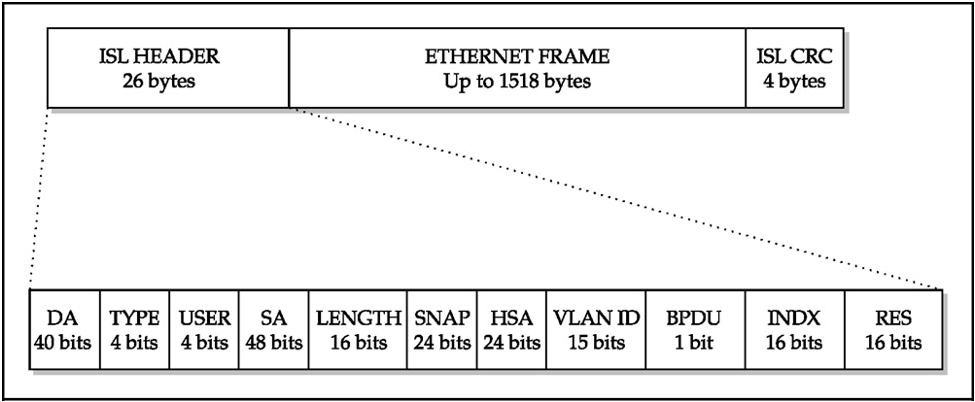
-sadrži Switch virtual interface, tj samo je IP adresa na određenom VLAN-u. Svakom vlanu je moguće dodeliti IP adresu.

-L3 switch formira routing tabelu.

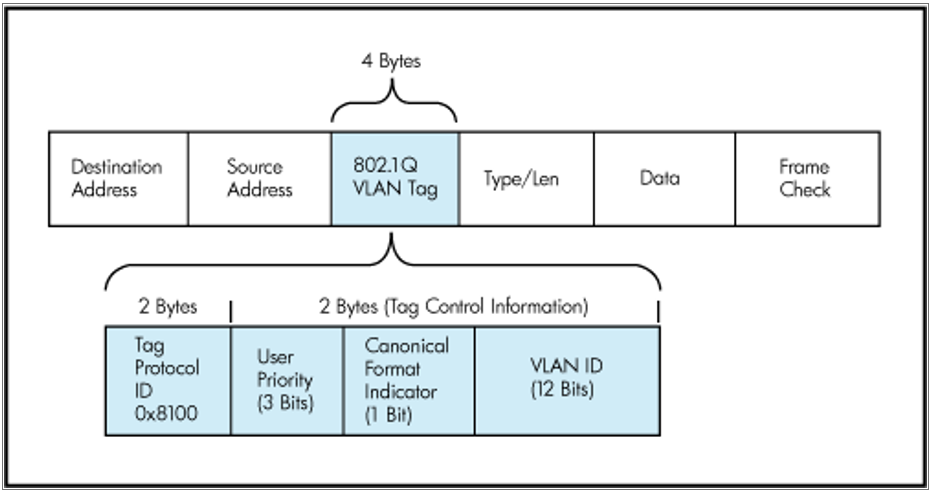
Kod L3 sviča, IP adresa se podešava na nivou VLAN-a.

Ako imamo trunkove, delimo bendvit i svi vlanovi dele jedan isti kabl, što je loše što se tiče bendvita (brže je ako svako ima zaseban). Jedan interfejs po vlanu nam teba ako nemamo trunkove.

**+15. ISL i IEEE 802.1q format frejmova.**



ISL (InterSwitch Link) ima zaglavlje i rep koji omeđuju Eternet frejm. U svom headeru sadrži VLAN ID polje. Ako swtich ne podržava VLAN-ove, ne ume da pročita ovaj frejm i on se odbacuje.



IEEE 802.1q zadržava ethernet frame ali ubacuje 802.1Q vlan tag polje. Podržava svaki switch

**+16. DTP protokol.**

Eternet trunk interfejsi podržavaju različite režime trunkovanja. Interfejs se može podesiti tako da bude trunk, ne-trunk ili da pregovara trunkovanje sa susedom. Pregovorima u vezi s trunkovima upravlja dinamicki protokol za trunkove (DTP, Dynamic Trunking Protocol), koji radi na nivou veze izmeu dva uređaja.

U pitanju je je vlasnicki protokol kompanije Cisco. Na svim portovima je DTP podrazumevano uključen. Portovi preko kojih su međusobno povezani susedni switch-evi periodično razmenjuju DTP pakete. Prilikom razmene paketa, switch može doći do određenih zaključaka neophodnih da sam inicira promenu režima u kom se port nalazi.

Režimi u kom se port kod DTP protokola može naći:

* **Pristupni režim** (access mode) je klasican režim porta switch-a. Interfejs je u ne-trunk režimu i pregovara sa suprotnom stranom da link promeni u ne-trunk. Ovaj interfejs postaje ne-trunk, nezavisno od toga šta je podešeno s druge strane.
* U **dinamičnom automatskom režimu** (dynamic automatic mode), interfejs može da se pretvori u trunk ako je susedni interfejs podešen u trunk ili poželjni režim. Ovo je podrazumevani režim za sve portove na Cisco-vim switch-evima.
* U **dinamičkom poželjnom režimu** (dynamic desirable mode), interfejs aktivno pokušava da pretvori vezu u trunk. Interfejs postaje trunk ako je susedni interfejs postavljen na trunk, poželjni ili automatski režim. Ovo je nekada bio podrazumevani režim za Cisco-ve switch-eve.
* **Trunk režim** (trunk port) karakteriše interfejs koji je u trajnom trunk režimu i pregovara sa susedom, u pokušaju da ga prevede u trunk. Interfejs postaje trunk cak i ako susedni nije.

|  | auto | desirable | trunk | access |
| --- | --- | --- | --- | --- |
| auto | access | trunk | trunk | access |
| desirable | trunk | trunk | trunk | access |
| trunk | trunk | trunk | trunk | Not good |
| access | access | access | Not good | access |

Tabela podrazumeva da je DTP uključen na obe strane

**+18. Router-on-a-Stick topologija i rutiranje.**

Tradicionalni nacin rutiranja nije praktičan za velike mreže, jer ruteri cesto nemaju mnogo fizicnih interfejsa. Alternativa za ovakve mreže jeste korišcenje trankova i podinterfejsa. Podinterfejsi su softverski implementirani virtuelni interfejsi. Svaki podinterfejs se podešava nezavisno IP adresom i maskom podmreže. Ovako je omogućeno da jedan fizički interfejs istovremeno bude deo više logickih mreža.

Kada se inter-VLAN rutiranje konfiguriše ovim modelom, fizički interfejs na koji je ruter povezan mora biti u trunk režimu. Svakom interfejsu se dodeljuje IP adresa specifična za tu podmrežu (tj. taj VLAN) i konfiguriše se tako da označava frejmove za taj VLAN. Na ovaj nacin, saobraćaj sa razlicith interfejsa je razdvojen.

Funkcionalno, router-on-a-stick topologija je identična tradicinalnom načinu rutiranja, izuzev toga što, umesto više fizičkih interfejsa, koristi samo jedan fizički interfejs koji je softverski podeljen na više virtuelnih. Ovako je smanjen broj portova koji se zauzima na switch-u za konfiguraciju mreže sa više VLAN-ova.

Na switch se konfiguracija blago razlikuje. Interfejs na koji je dovedena veza koja vodi do rutera treba biti trunk.

S1(config)# vlan 10

S1(config-vlan)# vlan 30

S1(config-vlan)# interface f0/5

S1(config-if)# switchport mode trunk

S1(config-if)# end

Na ruteru treba napraviti podinterfejse, podesiti im odgovarajuću enkapsulaciju i ukljuciti fizicki interfejs.

R1(config)# interface g0/0.10

R1(config-subif)# encapsulation dot1q 10

R1(config-subif)# ip address 172.17.10.1 255.255.255.0

R1(config-subif)# interface g0/0.30

R1(config-subif)# encapsulation dot1q 30

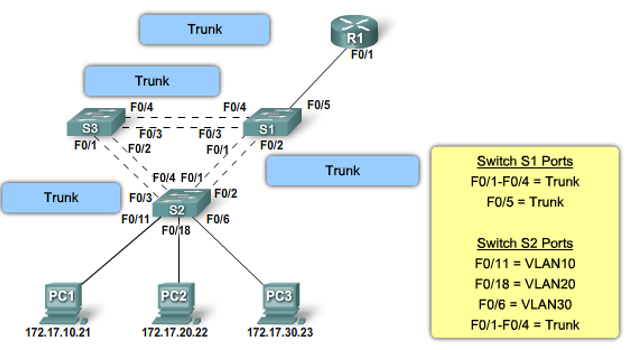
R1(config-subif)# ip address 172.17.30.1 255.255.255.0

R1(config-subif)# interface g0/0

R1(config-if)# no shutdown

Potvrda konfiguracije se na ruteru obavlja komandama *show vlan i show ip route.*

**19. Na proizvoljnoj router-on-a-stick topologiji detaljno objasniti inter-VLAN komunikaciju, počev od ARP zahteva.**



1. PC1 u VLAN 10 želi da komunicira sa PC2 koji je na VLAN 20. PC1 šalje ARP request frame da dobije MAC adresu gateway-a R1 za svoj Vlan.
2. Ruter R1 odgovara sa ARP reply frame sa svog virtuelnog interface-a koji je na VLAN 10. Svi Switchevi proslede ARP reply i PC1 ga primi. ARP odgovor sadrži MAC adresu default gateway-a virtualnog interfejsa na ruteru.
3. PC1 kreira ethernet frame sa MAC adresom default gateway kao odredište. Frame prolazi kroz switch S2 i S1.
4. Ruter R1 šalje ARP request frame na virtuelni interfejs koji je namenjen za VLAN 20 da dobije MAC adresu PC2. Switch-evi S1, S2, S3 šalju arp request na sve portove koji su konfigurisani za VLAN 20. PC2 prima request frame od R1 rutera.
5. PC2 na VLAN 20 šalje ARP reply frame na S2. S2 i S1 prosleđuju ARP reply do virtuelnog interfejsa na ruter R1.
6. Ruter R1 šalje Ethernet frame koji je primio od PC1 kroz Switch S1 i S3 do PC2 na VLAN 20.

**20. Razlozi za i protiv sinhronizacije virtualnih mrežama na grupi svičeva.**

Automatska sinhronizacija baza sa VLAN-ovima nam ubrzava postupak manipulacije sa VLAN-ovima i garantuje da svi switch-evi u administrativnom domenu imaju iste VLAN-ove.

Ako su switch-evi različitih proizvođača onda svaki od njih ima različit protokol za automatsku sinhronizaciju, moraće da se sinhronizacija radi ručno.

**+21. VTP terminologija i komponente.**

**VTP domen**: Skup Switch-eva koji razmenjuju informacije i cije se baze VLAN-ova sinhronizuju.

**VTP paketi**: Paketi koje razmenjuju Switch-evi u okviru VTP domena.

**VTP modovi:** Switch-evi VTP domenu mogu biti u jednom od režima: server, klijent, transparentni.

**VTP odsecanje:** VTP automatski može da zabrani VLAN na tranku ako detektuje da nema potrebe sladi brodkast “na tu stranu mreže” jer tamo nema racunara koji pripadaju tom VLAN-u. Po podrazumevanim podešavanjima, odsecanje je iskljuceno. Ukljucuje se komandom vtp prunning u globalnom konfiguracionom modu, na serveru.

**+22. Princip rada VTP protokola.**

Na Cisco-vom switch-u 2960, podrazumevana konfiguracija je sledeca:

S1# show vtp status

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 255

Number of existing VLANs : 5

VTP Operating Mode : Server

VTP Domain Name :

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generations : Disabled

MD5 digest : ...

Configuration last modified by 0.0.0.0 at 3-1-93 00:14:07

Ukoliko do switch-a koji nema podešen VTP domen dođe VTP advert, switch će prihvatiti ime domena iz adverta.

VTP sadrži sledece globalne informacije:

* ime VTP domena,
* identifikator switch-a koji vrši ažuriranje i vreme,
* MD5 potpis za zaštitu integriteta poruke (nije obavezno) i
* oznaku tipa frejma.

U paketu sa sadržani VLAN ID, ime, tip, status i dodatne specificke informacije o VLAN-u.

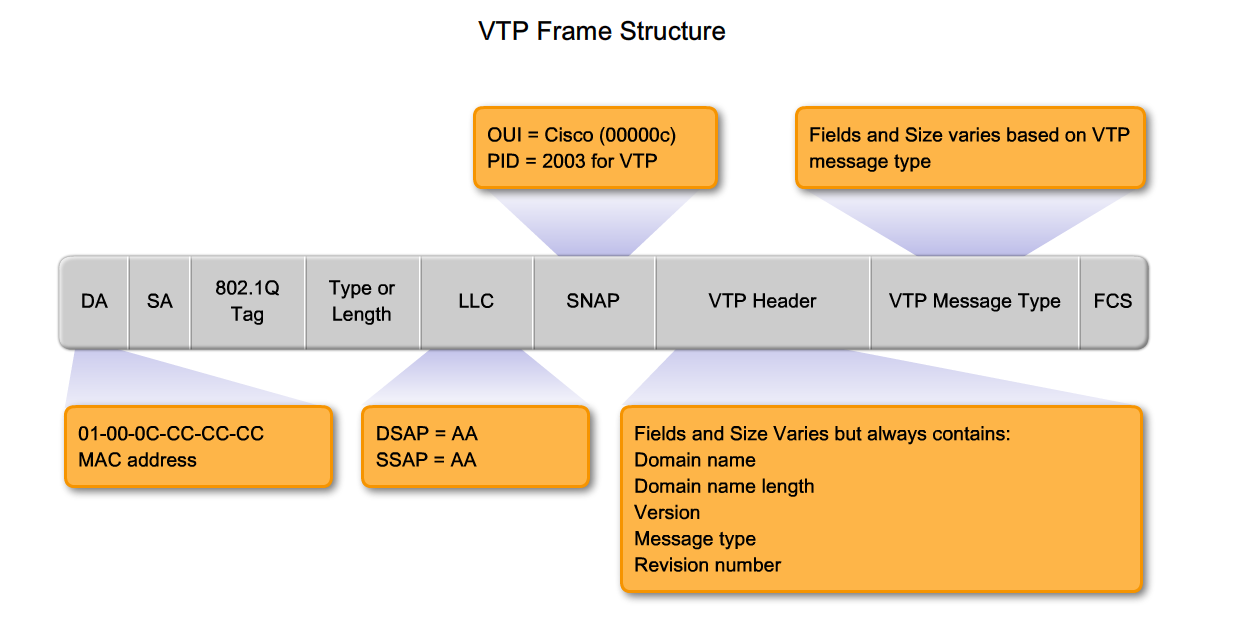
**Broj revizije** baze se koristi za sinhronizaciju baza VLAN-ova n svim switch-evima. Ukoliko primalac VTP poruke utvrdi da ima bazu sa nižim brojem revizije, od pošiljaoca zahteva “dopunu” informacija. Podrazumevana vrednost na nekonfigurisanom switch-u je 0. Broj revizije se inkrementira svakom manipulacijom sa VLAN-ovima: dodavnje, brisanje, promena imena.

Postoje tri tipa VTP paketa:

* Paket koji sadrži generalne informacije o bazi VLAN-ova, kao što je broj revizije, naziva se **sažetak** (**summary**). Šalje se na svakih pet minuta, kao i pirlikom izmene podataka o VLAN-ovima.
* Ukoliko primalac ustanovi da ima niži broj revizije, šalje paket tipa **zahtev** (**request**) od svog broja revizije do trenutne revizije.
* **Podskup** (**subset**) je paket koji sadrži zakrpu sa svim izmenama koje su se desile izmeu dve revizije: revizije koju ima primalac i revizije koju ima server.

**23. Struktura VTP frejma.**

VTP frejm sadrži VTP header polje i VTP poruka polje.



VTP frejm enkapsuliran kao 802.1Q frejm nije statičan. Switch koji prima VTP gleda specifilna polja i podatke u frejmu da zna šta da procesira. Prisutna su sledeća ključna polja:

* **Destination MAC adress:** Ova adresa je postavljena na 01-00-0C-CC-CC-CC, koji je rezervisan kao multicast adresa za sve VTP poruke
* **LLC polje**: Logical Link Control polje sadrži destination service access point i source service access point koji su postavljeni na vrednost AA
* **SNAP polje:**  Subnetwork access Protocol, polje koji identifikacioni broj je postavljen na AAAA i tip postavljen na 2003 (za VTP)
* **VTP header field:** Sadržaj se razlikuje u zavisnosti od tipa VTP poruke ali uvek sadrži ova VTP polja
  + Domain name
  + Domain name length
  + Version
  + Configuration revision number
* **VTP message polje:** Razlikuje se od zavisnosti tipa poruke

VTP Message sadržaj:

VTP sadrži sledeće globalne informacije:

* Ime VTP domena
* Identifikator sviča koji vrši update i vreme (timestamp)
* MD5 potpis za zaštitu integriteta poruke (opciono)
* Oznaku tipa frejma

Informacije o VLAN-u sadržane u VTP paketu

* VLAN ID
* Ime
* Tip
* Status
* Dodatne specifične informacije o VLAN-u

**24. VTP modovi i podrazumevana podešavanja.**

Postoji tri režima rada VTP-a: *server, klijent i transparentni.*

**Server** služi za upravljanje domenom i konfiguracijom VLAN-ova. Ucestvuje u procesu odgovora na VTP adverte. Globalna konfiguracija se cuva u NVRAM-u, pa je dostupna i nakon restartovanja switcha. switch koji radi u ovmo režimu može da ažurira druge switcheve na kojima je ukljucen VTP.

**Klijent** ne može da menja konfiguraciju VLAN-ova. Takoe ucestvuje u procesu odgovara na VTP adverte. Globalna konfiguracija se cuva u RAM-u, što znaci da nije dostupna nakon restartovanja switcha. Kao i server,switch koji radi u klijentskom režimu može da ažurira druge switcheve.

Switchevi koji rade u **transparentnom** režimu rada mogu da upravljaju lokalnom VLAN konfiguracijom, ali se ona ne propagira kroz ostatak VTP mreže. Ovakvi switchevi samo prosleuju VTP adverte koji stignu do njih. Samo se lokalna konfiguracija VLAN-ova cuva u NVRAM-u, što znaci da globalna konfiguracija nije dostupna nakon restartovanja ovog switcha. Ovaj switch ne može da ažurira druge VTP switcheve.

Na Cisco-vom switch-u 2960, podrazumevana konfiguracija je sledeca:

S1# show vtp status

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 255

Number of existing VLANs : 5

VTP Operating Mode : Server

VTP Domain Name :

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generations : Disabled

MD5 digest : ...

Configuration last modified by 0.0.0.0 at 3-1-93 00:14:07

Iz izlaza komande se vidi sledece:

* Verzija VTP protokola je 1.
* Ime VTP domena nije definisano (null).
* Režim rada je server.
* Redni broj revizije konfiguracije je 0.
* Ima 0 VLAN-ova.

**+25. MD5 kriptografski potpis za zaštitu integriteta VTP poruka.**

VTP paketi se šalju u režimu “obicnog teksta” (plain text), pa je prisluškivanjem jednostavno saznati ime domena. Ukoliko napdač zna ime domena, može zlonamerno dodati novi svic na mrežu, podesiti mu domen i obrisati sve VLAN-ove s mreže. U tom slucaju, svicevi reaguju kao kod brisanja VLAN-ova – gase sve portove koji su dodeljeni obrisanom VLAN-u.

Da se ova situacija ne bi desila, VTP svicevima se može zadati šifra za razmenu paketa. Šifra koju zadaje administrator se koristi za formiranje kriptografskog potpisa paketa. Poruke se i dalje prenose kao obican tekst.

**+26. Klasno i besklasno adresiranje.**

Adresa je klasna ako se samo na osnovu njene IP adrese može odrediti kojoj mreži pripada.

Ako to nije moguce, vec je neophodno poznavati i masku podmreže, adresa je besklasna.

Mada trajno rešenje za ocuvanje adresnog prostora postoji (IPv6), privremeno rešenje ukljucuje dve tehnike:

* **VLSM i CIDR** (1993) – Variable Length Subnet Masking i Classless Inter-Domain Routing.
* **NAT** (Network Address Translation, 1994) i privatno adresiranje (1996). Konvencijom je usvojeno da su privatne adrese: 10.0.0.0/8, 172.16.0.0/22 i 192.168.0.0/16.

**VLSM** dozvoljava da mrežni deo adrese bude proizvoljne velicine (a ne na granicama bajta). Ovo znaci da se mrežna adresa ne može odrediti bez maske podmreže. KOd VLSM-a, bitovi najvece težine predvieni za hostove u klasnim adresama se “pozajmljuju” kako bi se mreža dodatno podelila na manje celine – podmreže.

Maska podmreže može se zapisati u tri oblika:

* binarni format: 11111111 11111111 11111111 11000000,
* dekadni format: 255.255.255.192 i
* prefiksni format: /26.

Kod besklasnih adresa, mreža se može odrediti operacijom AND primenjenom nad IP adresom i maskom podmreže. Ovakvu operaciju koristi ruter kako bi odredio na koji interfejs treba proslediti paket.

**+27. Projektovanje adresne šeme.**

Adresna šema se može projektovati na tri nacina.

* **Klasna šema** – Uz poštovanje pravila o velicina mreža i broju hostova za opsege mreža klase A, B i C. Ovim se postiže skroman ušteda IP adresa, dovoljna za potrebe osamdesetih godina prošlog veka, ali nedovoljno za nadašnje potrebe.
* **Besklasna sa fiksnom dužinom maske podmreže** – Sve mreže u okviru jednog administrativnog domena se projektuju tako da imaju istu masku podmreže, manju od klasne. Ovim se postiže dobra ušteda IP adresa.
* **Besklasna sa promenljivom dužinom maske podmreže (VLSM)** – Sve mreže se projektuju tako da imaju masku podmreže koja (u najboljem slucaju savršeno) odgovara broju hostova na mreži. Ovim se postiže maksimalna ušteda IP adresa.

Svaka tehnika projektovanja adresne šeme zahteva korišcenje odgovarajucih protokola za rutiranje. Klasna adresna šema ne zahteva da protokoli za rutiranje šalju masku podmreže uz adresu mrežu, dok besklasne adresne šeme to zahtevaju.

**+-28. Klasno i besklasno rutiranje. Klasifikacija ruting protokola.**

Adresa je **klasna** ako se samo na osnovu njene IP adrese može odrediti kojoj mreži pripada.

Ako to nije moguce, vec je neophodno poznavati i masku podmreže, adresa je **besklasna**.

Kod besklasnih adresa, mreža se može odrediti operacijom AND primenjenom nad IP adresom i maskom podmreže. Ovakvu operaciju koristi ruter kako bi odredio na koji interfejs treba proslediti paket.

Ako je adresna šema mreže projektovana po VLSM principu, u paketima koje ruteri razmenjuju je pored adrese mreže neophodna i maska podmreže. Protokoli za rutiranje koji ukljucuju i masku podmreže nazivaju se besklasni protokoli za rutiranje (Classless Routing Protocols), a proces rutiranja se zove besklasno rutiranje izmeu domena (Classless Inter-Domain Routing).

Protokoli za rutiranje se mogu podeliti u dve grupe: klase i besklasne. Klasni protokoli za rutiranje su RIPv1 i IGRP. Besklasni su: RIPv2, EIGRP, OSPF i IS-IS.

**+29. Podršla RIPv1 protokola za rad sa različitim tipovima adresnih šema.**

Klasni protokoli vrše sažimanje (sumarizaciju) podmreža na klasne granice pre slanja paketa.

Bez određenih “softverskih zakrpa”, klasni protokoli bi na mreži sa slike informacije o rutiranju razmenili na sledeci nacin:

* R1 sumarizuje rutu 172.16.1.0/24 i šalje je ka R1 kao 172.16.0.0 za koju se podrazumeva da je maska /16.
* R2 dobija paket sa mrežom 172.16.0.0 i brojem skokova 1.
* R2 odbacuje ovu informaciju kao nepotrebnu – on vec ima direktno povezanu mrežu 172.16.0.0, i to sa metrikom 0.

RIPv1 ima softversku zakrpu u vidu sledeceg pravila.

Ako mreža preko koje se šalje ima: istu masku podmreže kao i mreža o kojoj se razmenjuju informacije, i pripada istoj klasnoj mreži; onda se mreža šalje bez sumarizovanja na klasnu granicu.

Kada odredište dobije informacije o mreži koja nije na klasnoj granici, znace da je izvorište “primenilo” pomenuto pravilo, i u tom slucaju za masku podmreže se uzima maska podmreže interfejsa na koji je paket sa informacijom došao.

Tako na primer, na mreži sa slike RIPv1 radi bez problema iako mreža ima podmreže.

* R2 vidi da “nešto nije u redu” sa paketom jer nije na klasnoj granici.
* Pošto nema masku podmreže u paketu, R1 zakljucuje da je primenjeno goreopisano pravilo.
* Pošto izlazni interfejs na ruteru R1 i dolazni interfejs u R2 moraju da imaju istu masku podmreže, a R1 je primenio pravilo, R2 zakljucuje da je maska podmreže ista kao na njegovom interfejsu S0/0/0, tj. Da je /24.

Kaže se da mreža nema diskontinuitet ako je adresna šema takva da su sve mreže koje su podeljene na podmreže iz jedne klasne mreže susedne i sa istom maskom podmreže. RIPv1 radi samo na mrežama bez diskontinuiteta u adresnoj šemi.

+**30. IPv6.**

Šesta verzija IP protokola razvijena je 1998. godine od strane IETF-a i nastao je kako bi zamenio IPv4. IETF je uocio problem iskorišcenosti IPv4 adresnog prostora i predložio je dva privremena rešenja: CIDR (Classless Inter-Domain Routing) i NAT (Network Address Translation). IPv6 se zasniva na nedostacima svog prethodnika i u odnosu na njega ima: uprošceno zaglavlje, veci adresni prostor (2^128 razlicitih IPv6 adresa), efikasnije rutiranje, ugrađenu podršku za bezbednost podataka i bolji kvalitet servica (QoS).

IPv6 adrese se uglavnom zapisuju kao 8 grupa od po 16 bitova, u heksadekadnom brojevnom sistemu. Grupe se međusobno odvajaju pomocu simbola : . Na primer, IPv6 adresa može izgledati ovako:

2001:0DB8:0000:0000:0000:8A2E:0840:7334

Zapis se može skratiti ako se izbace vodece nule, kao i nule u susednim grupama.

2001:DB8::8A2E:840:7334

IPv6 adrese su sastavljene od dve celine: mrežnog dela i host dela.

**31. Tipovi IPv6 adresa.**

**Unicast** - jedinstvena adresa odredišta, koristi se u komunikaciji **jedan-na-jedan**,

* *Global unicast address* - Kao “javne” adrese kod IPv4, za sada se koriste samo adrese koje počinju sa 001 binarno. Posmartano kroz prvu heksa cifru, na početku je uvek 0010, što je 2 (npr. 2001::DB8::ACAD::1).
* *Link-local unicast address* (adrese sa prefiksom: FE80::/10) - Validne samo na jednom interfejsu. Jedan ruter može imati istu adresu na različitim (svojim) interfejsima, jer nemaju smisla “van” tog interfejsa (ne rutira ih ruter čak ni među svojim interfeejsima.
* *Site-local unicast address* (adrese sa prefiksom FEC0::/10 ) - Slično kao privatne IPv4 adrese
* *Specijalne IPv6 adrese* - Unspecified (::/128); Loopback adresa (::1);

**Anycast** - adresa grupe, koristi se u komunikaciji **jedan-na-jedan-iz-grupe**, odredište može biti bilo ko iz grupe, obično je topološki najbliži čvor.

**Multicast** - adresa grupe, koristi se u komunikaciji **jedan-na-više**,

**32. Primer podešavanja IPv6 interfejsa i rutiranja.**

//podesavanje ipv6 adrese

R1(config)# interface gigabitethernet 0/0

R1(config-if)# ipv6 address 2001:db8:acad:1::1/64

R1(config-if)# no shutdown

R1(config-if)# exit

//staticko rutiranje

R1(config)# ipv6 unicast-routing

R1(config)# ipv6 route 2001:db8:cafe:1::/64 2001:db8:cafe:2::1

R1(config)# ipv6 route ::/0 2001:db8:cafe:3::2

//RIPng

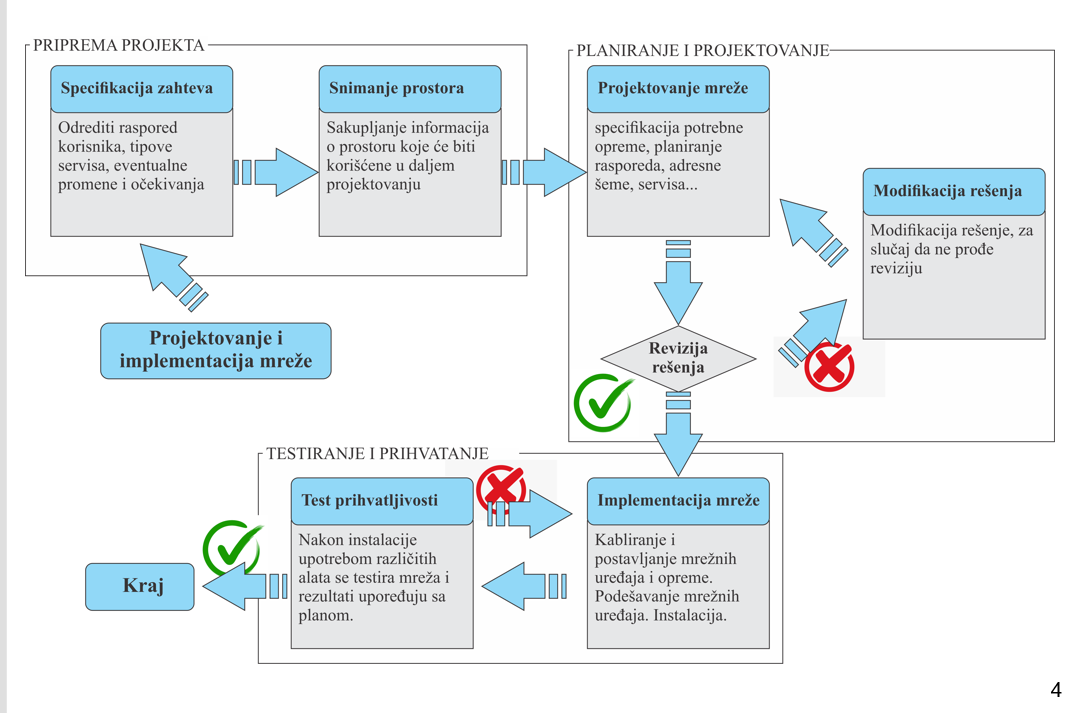
R1(config)# ipv6 unicast-routing

R1(config)# ipv6 router rip proc1

//ukljuciti rip na svaki interface

R1(config-if)# ipv6 rip proc1 enable

**33. Proces projektovanja i implementacije mreže.**



**34. Priprema projekta.**

Priprema projekta obuhvata specifikaciju zahteva i snimanje prostora.

Specifikacija zahteva podrazumeva komunikaciju sa korisnikom u cilju prikupljanja zahteva. Treba da se razjasne zahtevi i sagledati ciljevi.

Specifikacija zahteva obuhvata sledeće stvari

* Plan zgrade
* Broj i raspored uređaja
* Tipovi i namena uređaja
* Servisi koji će se najčvešće koristiti
* Nominalna brzina lokalne mreže
* Lokacija mrežne opreme
* Budžet
* Plan daljeg rasta i razvoja

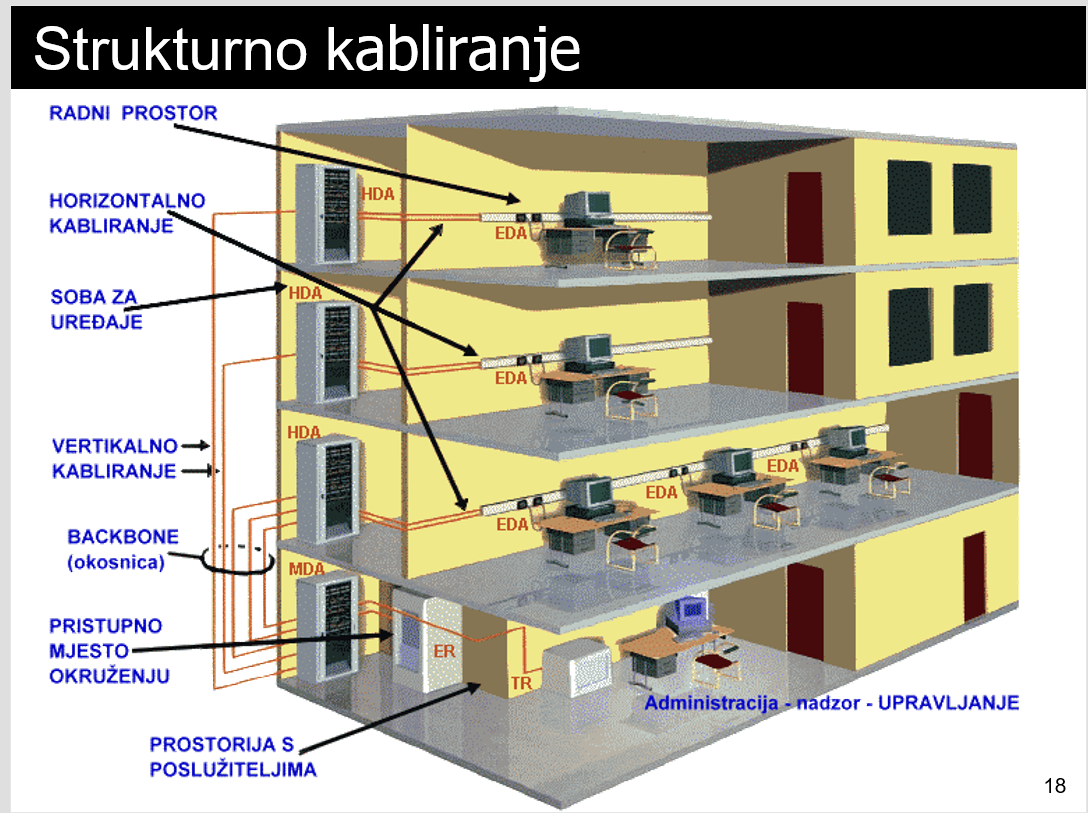
Snimanje prostora potrebno je evidentirate svih soba sa svim dimenzijama, tj da imamo plan projekta. Potrebno je i napraviti što više fotografija prostorije da se ponovo ne izlazi na teren. Obavlja se u prostoru gde će mreža biti implementirana, ako je objekat završen ili na osnovu građevinskih planova, ukoliko je projekat mreže sastavni deo projekta još uvek ne izvedenog objekta

**35. Planiranje i projektovanje fizočkog rasporeda uređaja.**

Planiranje fizičkog rasporeda zahteva strukturno kabliranje. Strukturno kabliranje je kablovska infrastruktura u zgradama i naseljima namenjena telekomunikacionim servisima, koja sadrži određeni broj standardizovanih manjih elemenata koje nazivamo podsistemima strukturnog kablovskog sitema.

Strukturno kabliranje možemo podeliti u šest podsistema

* Ulazne prostrojenja
  + Gde se unutrašnja infrastuktura povezuje sa sponjom
* Prostorije sa opremom
* Telekomunikacione sobe
  + U kojima se nalazi oprema koja povezuje magistrale kablovske sistema sa horizontalnim kablovskim sistemima
* Magistralno (Backbone) kabliranje
  + Povezuje ulazna prostrojenja, prostorije sa opremom i telekomunikacione sobe
* Horizontalno kabliranje
  + Povezuje telekomunikacione sobe i pojedinačne priključnice na spratu
* Krajnje komponente



Mrežna infrastruktura i fizički raspored uređaja se obično projektuju kao jedan od slojeva plana zgrada (električne instalacije, vodovodne instalacije itd.)

Infrastruktura i fizički raspored sadrže raspored

* Kablova
* Mrežnih priključaka
* Mrežne opreme
* Rek ormana
* Korisničkih uređaja

**36. Projektovanje kapaciteta mreže.**

Cilj projektovanja kapaciteta mreže je ispunjenje korisničkih zahteva u pogled brzine protoka podataka (throughput - realna brzina protoka podataka) na mreži

Treba razmotriti:

* Tipovi servisa koji će se koristiti
* Maksimalan protok
* Stepen konkurencije korisnika (koliko korisnika u isto vreme koriste) - Najvažnija stvar
* Tip krajnjih uređaja
* Tipovi, karakteristike i broj mrežnih uređaja

Bandwidth >= throughput = Broj korisnika \* stepen konkurencije \* throughput po korisniku

Stepen konkurencije je procenjen broj korisnika koji će istovremeno pristupiti mreži

Ovo mora da važi za svaku podmrežu i za svaku grupu uređaja

**+-37. Izbor mrežnih uređaja.**

Na izbor mrežnog uređaja uticu sledeci faktori.

* Nivo OSI modela na kome uređaji treba da se povežu. Ako se planira povezivanje lokalne mreže, u pitanju je drugi nivo, tj. radi se o switch-u. Ako se planira proširenje dometa mreže, u pitanju je prvi nivo, tj. uređaj je ripiter.
* Kašnjenje signala kroz uređaj se naziva latecija, a vreme potrebno da podatak stigne od izvora do odredišta je propagaciono kašnjenje.
* Dodatne specificne karakteristike izabrane po projektnim zahtevima.
* Cena.

Svi mrežni uređaji unose kašnjenje signala. **Repeater** i **Hub** unose najmanje kašenjenje, tipicno jedan ili nekoliko bitskih intervala. **Switch**, zavisno od tehnike baferovanja i brzine pretrage MAC tabele, tipično unosi kašnjenje od nekoliko do nekoliko stotina mikrosekundi. **Router** unosi par stotina mikrosekundi, a često i cele milisekunde. Kašnjenje unosi i **kabl**, i to oko 3 mikrosekunde po kilometru.

Zbog učestalih kolizija, na jednom kolizionom domenu se ne preporucuje više od nekoliko desetina uređaja. Za kolizione domene treba da važi pravilo 5-4-3.

Kod dašanjih mreža su za povezivanje uređaja dostupni switch-evi, i to po jedan port po uređaju. U tom slucaju kolizioni domen čine dve uređaja: port switcha i sam uređaj. Ovakva mreža se naziva mreža sa **mikrosegmentacijom**.

Po **fizičkim karakterstikama**, switchevi mogu podeliti na sledece grupe.

* Switch-evi sa **fiksnom** konfiguracijom (fixed-config) nemaju mogucnost dodavanja dodatnih komponenti u vidu dodatnih portova.
* U **Modularne** switch-eve(modular-config) mogu se dodavati razni moduli.
* Switch-evi sa mogućnošću **nadovezivanja** (stackable) se mogu nadovezivati jedan an drugi posebnim kablovima i protokolima.
* SFP port (Small Form-factor Pluggable) je poseban port koji mogu imati uređaji, a u koji se mogu priključiti posebni mrežni interfejsi, najcešce optika.

Po **performansi:**

* **Gustina portova**  odnosi se na broj portova.
* **Brzina prosleđivanja paketa** je ukupan broj frejmova koje switch može da obradi u jedinici vremena.

Dodatne mogućnosti:

* **Agregacija linkova** definiše maksimalni kapacitet veze
* **PoE** (Power over Ethernet) je napajanje preko UTP kabla.
* **L3 funkcije** uključuju mogućnosti rutiranja među VLAN-ovima.

**38. Testiranje i prihvatanje implementirane mreže.**

**Sertifikacija** je proces kojim se vrši testiranje svih postavljenih pasivnih elemenata infrastrukture: *priključnica i kablova*. Izlaz iz ove fate je dokument koji se naziva **sertifikat mreže**.

Sertifikat za svaki prikljucak na mreži sadrži merene karakteristike po kategorijama koje propisuje standard. Svaka karakteristika za svaki prikljčak mora da zadovolji uslove standarda. Ukoliko postoji negativno odstupanje, elementi koji ne ispunjavaju standard se uklanjaju i postavljaju se novi.

Postoji pet glavnih organizacija za standardizaciju: **EIA/TIA (SAD), ANSI, ISO/IEC, CENELC i IEEE.**

Uređaj za sertifikaciju meri karakteristike od utičnice do rek ormana. Ova sertifikacija ukljucuje dve kategorije:

* kvalitet pasivne opreme (utičnica i kablova) i
* kvalitet od strane proizvođača (spojevi, konektori), tj. kvalitet načina povezivanja uticnica, pec-panela i povezivanja u rek ormanu.

**+39. Projektna dokumentacija.**

Projekta dokumentacija treba da sadrži:

* Fizički raspored infrastrukturnih elemenata – Odnosi se na planove sa ucrtanim elementima.
* Specifickacija materijala i opreme – Predstavlja tabelarni prikaz opreme i karakteristika (kolicine i sl). Sadrži:
  + detaljnu specifikaciju pasivne mrežne opreme (kablovi, prikljucnice, rek-ormani, pec-paneli) i
  + detaljnu specifikaciju aktivne mrežne opreme (ripiteri, habovi, svicevi, ruteri, bežicne pristupne tacke, itd. sa svim oznakama, karakteristikama i opisima).
* Topologija mreže — Uključuje i fizičku i logičku topologiju mreže. Ističe nacin povezivanja ureaja, sa oznakama portova.
* Adresna šema i rutiranje.

**+40. Problemi sa redundansom na L2.**

Mnogim organizacijama je dostupnost mreže od presudnog znacaja; prema tome, redundantni dizajn infrastrukture nije nešto što treba zanemariti. Redundantnost mreže obuhvata alternative linkove i uređaje potkrepljenim protokolom kao što je *STP (Spanning Tree Protocol).*

Postoje izvesni problemi kod redundanse na prvom sloju.

* Eternet frejmovi nemaju TTL, što znaci da ne postoji mehanizam da se blokira kontinualna propagacija frejmova kroz mrežu, što je narocito izraženo tokom emisije paketa (nastaju takozvane emisione oluje).

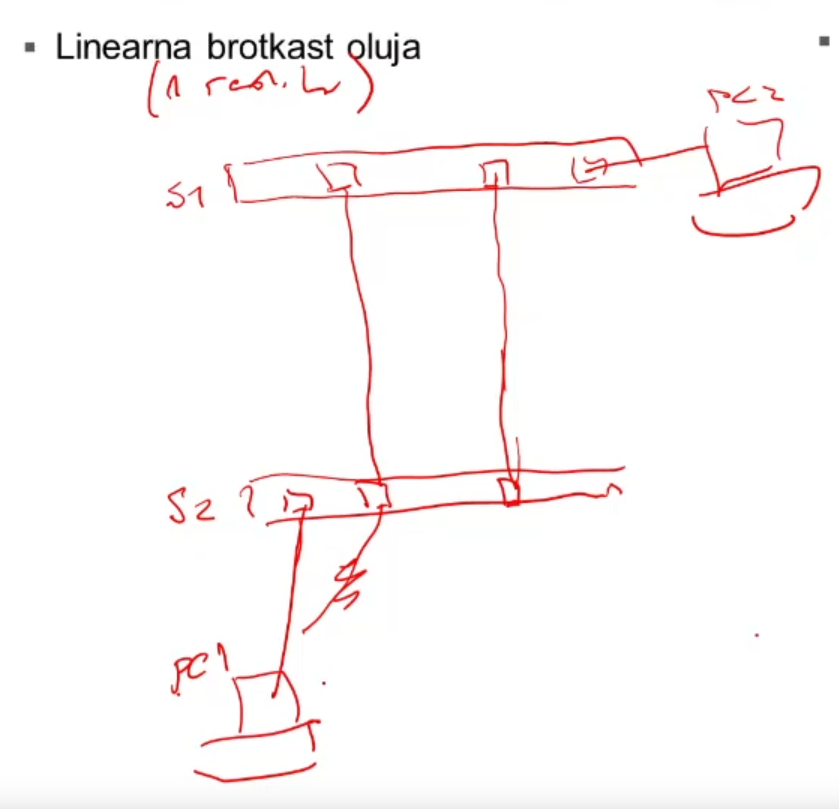
Ovo ne samo da izaziva **nestabilnost MAC tabele**, vec i opadaju **performanse**.

* Problem nisu samo emisije. I junikast paketi ce **dvaputa stici do odredišta** (a vecina protokola viših slojeva nije dizajnirana tako da prepozna duplikate).

**41. Linearna i ekponencijalna brotkast oluja na L2.**

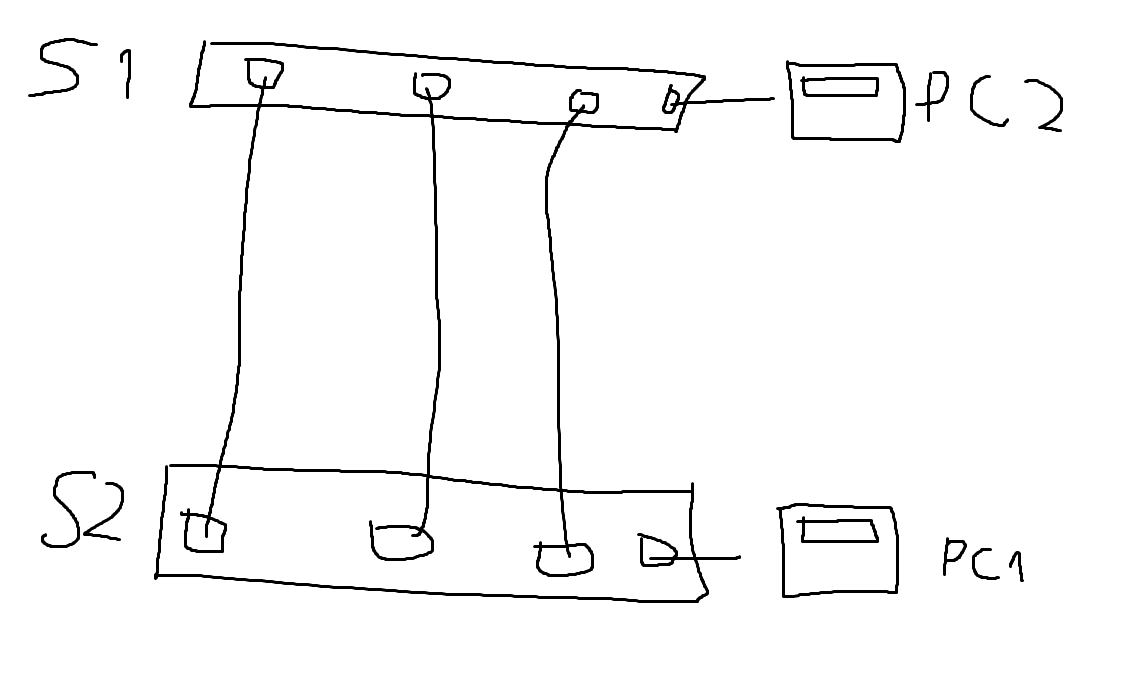
Brotkast oluja - previše brotkast paketa uhvaćenih u L2 petlji koji zauzimaju većinu ako ne ceo propusni opseg mreže, pa je mreža nedostupna za regularan saobraćaj

Razlikujemo 2 tipa brotkast oluje: Linearni i eksoponencijalni



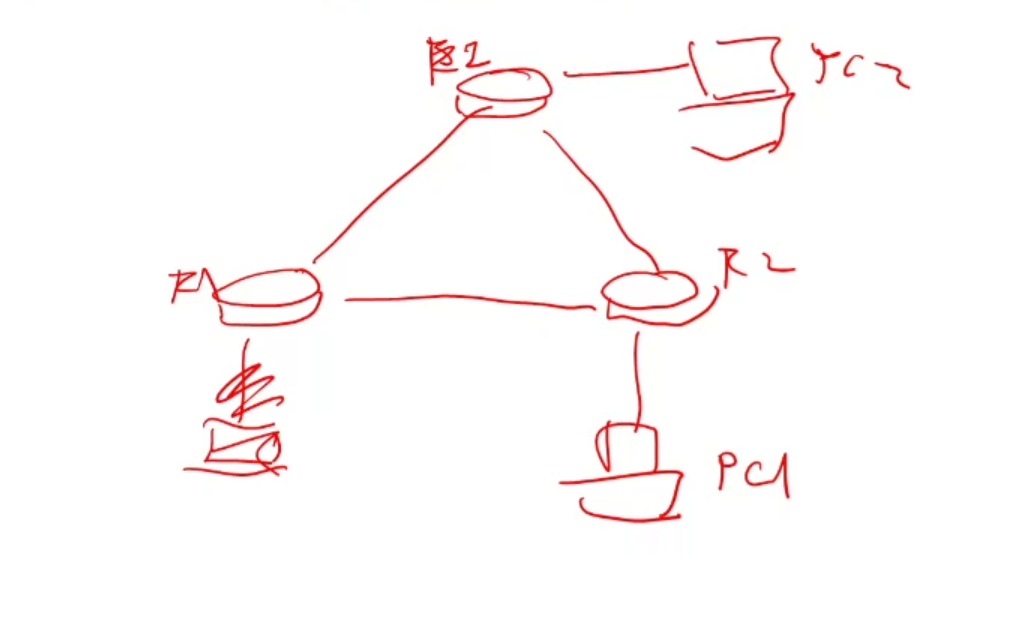
Na ovoj slici vidimo vezu između 2 pc koji smo dobili uz pomoć 2 switch-a. Na toj vezi dodamo još jednu redudnatnu vezu između linkova u slučaju da ta otkaže (bitna stvar oko linearne brotkast oluje).

PC1 šalje paket na S2 switch i S2 će proslediti broadcast na sve portove osim na onaj koji je dobio. Tako da će do S1 doći dupli frame od te dve veze. Nakon toga frame koji je dobio od leve veze proslediće na desnu vezu i na PC2, dok frame koji je dobio sa desne veze proslediće na levu vezu i ponovo na PC2. I to je prouzrokovalo da se 2 frame vratila nazad na S2. I s2 će ponoviti akcije S1 i da prosledi ponovo 2 frame-a ka S1. I tako dalje prouzrokovaće 2 frame koja se zaglavila u petlji. Tako da 1 broadcast pravi 2 broadcast-a koja će da kruže.



Kod eksponencijalne brotkast oluje kada pc1 pošalje paket pa pc2. S2 šalje paket na portove gde nije primio i onda će S1 da primi 3 duplikata i prouzrokovaće 6 koja se vraćaju i 3 koji idu ka PC2. Zato što S2 primi 6 paketa onda će nazad da poašalje 12 frejmova nazad. I tako u krug.

**42. Redundansa na L3.**



Ovde imamo redudansu sa R1 Ruterom. Administrator mora da doda lokalno mreže na svaki port gde je povezan sa ruterom, onda ili statički ili preko nekog routing protokola treba da inicira razmenu ruta svih rutera pa posle toga svaki router imaće po 5 stavki po routing tabeli. Nakon toga routing je moguće. Ako PC1 šalje paket pa PC2 onda paket prima R2 i bez problema zna da treba da šalje paket ka R2 drugom ruteru i doći će paket do PC2. Ako nestane veza između R2 rutera onda donji R2 router imaće 4 stavke u svojoj routing tabeli samo što će onda put do PC2 imati 2 hop-a. Što znači nema broadcast oluja jer ruteri ne uče od samog paketa koji je routirao nego je naučio informacije statički ili dinamički.

**+43. STP terminologija, komponente i algoritam.**

Uloge portova opisuju njihov odnos u mreži u odnosu na koreni most (root bridge), i daju informaciju o tome da li je kroz njih dozvoljen protok podataka.

* **Koreni portovi** (*root ports*) su portovi na svicevima koji su najbliži korenom mostu. Biraju se po switch-u.
* **Obeleženi portovi** (*designated ports*) su svi ne-koreni portovi kroz koje i dalje dozvoljen prenos podataka. Biraju se po tranku. Ako je na jednom kraju tranka koreni port, sa druge strane je obeležen port. Svi portovi korenog stabla su obeleženi.
* **Alternativni i rezervni portovi** (*alternate and backup ports*) se konfigurišu tako da budu u blokirajućem stanju kako bi onemogućili nastanak petlji. Biraju se samo na trankovima gde nijedan kraj nije koreni port. Uvek je samo jedan kraj tranka oznacen kao alternativni port. Ovo dozvoljava da se port brže prebaci u stanje u kome može da razmenjuje podatke kada za tim bude bilo potrebe.
* **Iskljuceni portovi** (*disabled ports*) su portovi svica koji su ugašeni.

Algoritam.

(1) **Bira se koreni most**. Kao koreni most bice izabran svic sa najmanjom vrednošcu prioriteta. Ukoliko je prioritet isti, bira se najniža MAC adresa.

Ovo se postiže razmenom BPDU paketa i poređenjem trenutnog identifikatora svica za koji se smatra da je koreni sa svojim identifikatorom. U pocetku svi svicevi misle da su koreni.

(2) **Određuje se najjeftiniji put do korena**. Podrazumevano se vezama izmeu sviceva dodeljuje cena na osnovu brzine veze. Na primer, za stomegabitne veze cena iznosi 19. Na cenu je moguce uticati programski, iz podešavanja za odgovarajuci interfejs na svicu. Na primer, za postavljanje cene 25, treba uneti komandu spanning-tree cost 25. Cena se vraca na podrazumevano podešavanje komandom no spanning-tree cost.

(3) **Gašenje nepotrebnih portova.** Koreni most automatski podešava sve portove kao obeležene. Drugi svicevi iz topologije sve ne-korene portove postavljaju na obeležene ili alternativne. Za obeleženi port se bira port sa nižim prioritetom (ili MAC adresom), a drugi kraj veze prelazi u alternativni port.

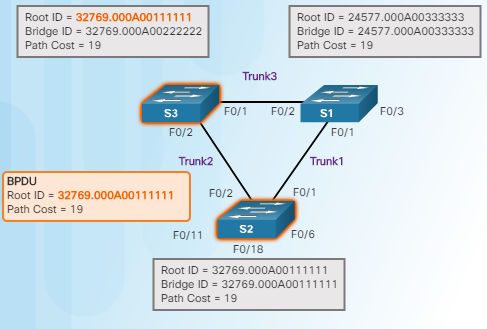
**44. Na primeru objasniti proces konvergencije Spanning Tree algoritma.**

Svaki svic u emisionom domenu prvo pretpostavlja da je on koren instance sprežnog stabla, tako da BPDU frejmovi koje šalje sadrže BID lokalnog svica kao ID korena. Po podrazumevanim podešavanjima, BPDU frejmovi se šalju na svake dve sekunde od kad se svic ukljuci. Podrazumevana vrednost Hello tajmera za BPDU frejmove je 2 sekunde. Svaki svic sadrži lokalne informacije o svom BID-u, ID-u korena i ceni puta do korena.

Kada susedni svicevi prime BPDU frejm, oni porede ID korena iz BPDU-a sa lokalnim ID-em korena. Ako je ID korena iz BPDU-a manji od lokalnog ID-a korena, svic ažurira i lokalni ID korena i ID u BPDU poruci. Ove poruke ukazuju na novi koren na mreži. Na rastojanje do korena ukazuje ažuriranje cena puta. Na primer, ako se dobije BPDU na Fast Ethernet portu svica, cena puta se povecava za 19. Ako je lokalni ID korena manji od ID-a korena dobijenog u BPDU frejmu, BPDU frejm se odbacuje.

Nakon što je ID korena ažuriran radi identifikacije novog korena, svi sledeci BPDU frejmovi koji se šalju od tog svica sadrže novi ID korena i ažuriranu cenu puta. Na taj nacin svi susedni svicevi mogu da u bilo kom trenutku vide najniži ID korena. Kako se BPDU frejmovi razmenjuju meu susednim svicevima, cena puta se neprekidno ažurira i ukazuje na ukupnu cenu do korena. Svaki svic u sprežnom stablu koristi cenu puta da identifikuje najbolji put do korena.

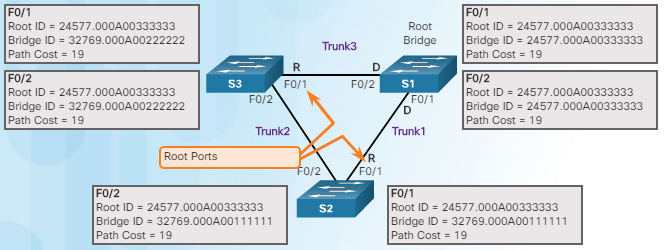
**45. STP BPDU propagacija i proces izbora Root bridža.**



1. Kada se svič uključi, (svaki) svič pretpostavlja da je baš on root bridge dok BPDU-ovi ne budu poslati i STP izračunavanja završena. Npr. S2 šalje BPDU…
2. S3 upoređuje svoj root ID sa BPDU dobijenom od S2. S2 ima manji BID pa S3 apdejtuje root ID.
3. S1 dobija istu informaciju od S2 i zato što S1 ima manji BID on ignoriše informaciju od S2.
4. S3 šalje svoj BPDU na sve portove sa naznakom da je S2 root bridge.
5. S2 upoređuje informacije dobijene od S3 pa S2 i dalje misli da je on root bridge.
6. S1 dobija iste informacije od S3 (da je S2 root bridge), pa pošto S1 ima manji BID, on ignoriše informacije iz BPDU.
7. 7. S1 šalje BPDU’-ove na sve svoje portove. BPDU sadrži informacije da je S1 root bridge.
8. S3 upoređuje informacije od S1 i S3 i sada vidi da je BID dobijen od S1 manji od njegovog zapamćenog root bridge polja koje trenutno pokazuje da je S2 root bridge. S3 menja root ID na informaciju dobijenu od S1.
9. S2 upoređuje informacije od S1 pa S2 sada vidi da je BID kod S1 manji od njegovog BID-a. S2 sada apdejtuje svoju informaciju i sada zna da je S1 root bridge.

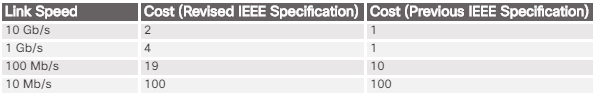
Nakon izbora root bridge-a uloge portova se mogu odrediti zato što se one određuju na osnovu ukupne cene puta do root bridge-a.

**46. STP proces izbora Root portova, Root Path Cost i Port Priority.**



Prvo se prolazi faza izbora root bridge-a pa onda kreće faza uloge dodele portovima.

Prvo Root bridge prebaci sve svoje portove u designated i šalje BPDU-ove. Za S3 primiće BPDU od S1 na oba porta ali odrediće da na port F0/1 je manja cena i on će postati root port dok drugi postaje designated port, isto to će uraditi i S2, od 2 porta bira onaj sa najmanjom cenom. I F0/1 postaje root dok drugi postaje designated. Nakon toga na designated portovima S2 i S3 primiće BPDU i moraće da se usaglase koji će biti Nondesiganted. Nondesignated biće onaj sa manjim prioritetom (U ovom slučaju S3)



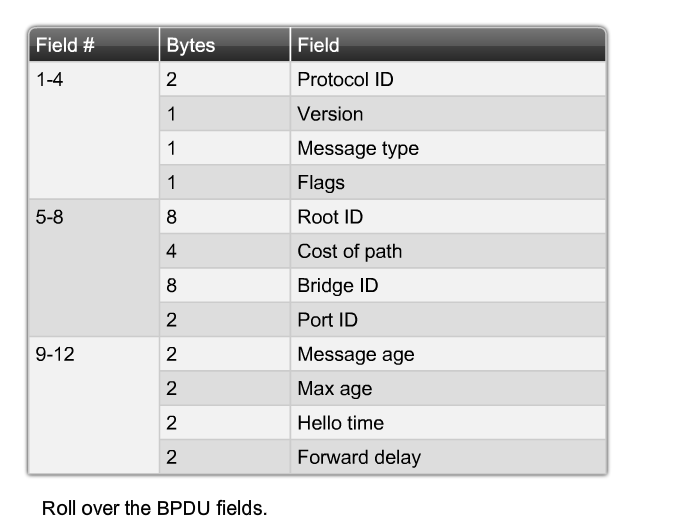
Root path cost se koristi kako bi se odredile uloge portova i da li se saobraćaj blokira (tj cena puta do root Bridge-a). Može se modifikovati naredbom spanning-tree cost.

Menjanjem Port Priority utiče isto kako biramo koji će root port za neki vlan. Naredba je spanning-tree vlan x port-priority y, port priority se menja u koraku od 16.

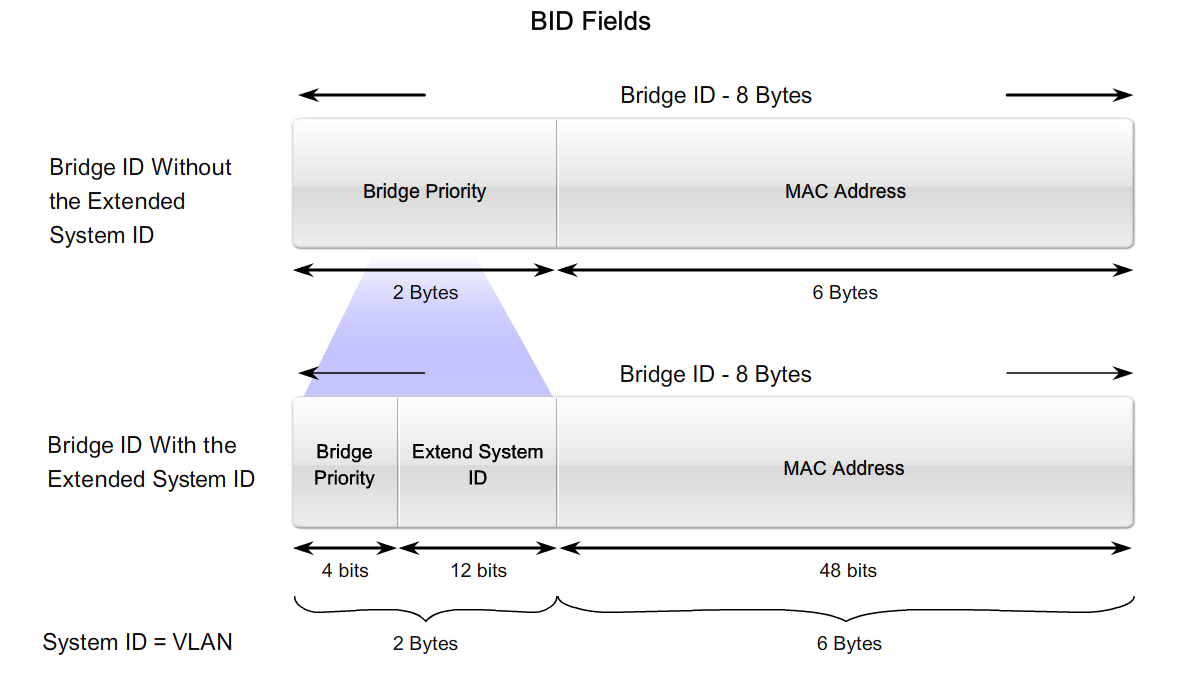
| Both parameters are used to determine which interface will be in forwarding state.  They have differences though:  If you want to affect how to the local switch elects the root port change the cost on the links. Cost is cumulative throughout the STP domain. The higher cost is the less preferred.  If you want to affect how downstream switch elects its root port change the priority. This is only local significant between the two directly connected switches. Highest priority is less preferred.  Going away from the root of the tree use priority whereas, when going towards the root of the tree use cost. |
| --- |

**47. STP BID i BPDU**.

BPDU frame sadžri 12 razlilčitih polja koja se koriste da prenesu informacije o putu i prioritetu koji STP koristi da odluči koji je root bridge i putanje do root bridge-a.



* Prva četiri polja služe da identifikuju protokol, verziju, tip poruke i statuse.
* Sledeća četri polja koriste se da identifikuju root bridge i cebu putanje do root bridge-va
* Poslednja četiri polja su svi polja sa tajmerima koja određuju koliko često BPDU poruke su postulate i koliko dugo se inforacije čuvaju koje su primljene kroz BPDU proces.



**Bridge ID (BID)**  se koristi da se odredi koji je root bridge u mreži. Sadržio 3 polja. Bridge Priority, Extended System Id i MAC adresu.

Bridge Priority je vrednost koju možemo promeniti koja uitiče koji siwthc ima da postane root bridge. Switch sa najnižim prioritetom postaje root bridge. Default vrednost je 32768.

**Extended System id**

Kao što je prikazano u primeru, prošireni ID sistema može biti izostavljen u BPDU okvirima u određenim konfiguracijama. Rana implementacija STP-a je dizajnirana za mreže koje nisu koristile VLAN. Postojalo je jedno zajedničko stablo za sve switch-eve. Kada su VLAN-ovi počeli da postaju uobičajeni za segmentaciju mrežne infrastrukture, STP je poboljšan da uključi podršku za VLAN. Kao rezultat, prošireno polje ID sistema sadrži ID VLAN-a sa kojim je BPDU povezan.

Kada se koristi Extentded System ID, on menja broj bitova dostupnih za vrednost prioriteta mosta, tako da se povećanje vrednosti prioriteta mosta menja sa 1 na 4096. Prema tome, vrednosti prioriteta mosta mogu biti samo višestruke od 4096.

Vrednost proširenog ID sistema se dodaje vrednosti prioriteta mosta u BID-u da bi se identifikovali prioritet i VLAN BPDU okvira.

**MAC adresa**

Kada su dva switch-a konfigurisana sa istim prioritetom i imaju isti prošireni ID sistema, switch sa MAC adresom sa najnižom heksadecimalnom vrednošću ima niži BID. U početku, svi prekidači su konfigurisani sa istom podrazumevanom vrednošću prioriteta. MAC adresa je tada odlučujući faktor koji će prekidač postati root bridge. Ovo rezultira nepredvidivim izborom za root bridge. Preporučuje se da konfigurišete željeni prekidač za root most sa nižim prioritetom kako biste bili sigurni da je izabran za root most. Ovo takođe osigurava da dodavanje novih prekidača u mrežu ne pokrene novi izbor sprežnog stabla, što bi moglo poremetiti mrežnu komunikaciju dok se bira novi root bridge.

**48. STP Extended System ID.**

Extended System id

Kao što je prikazano u primeru, prošireni ID sistema može biti izostavljen u BPDU okvirima u određenim konfiguracijama. Rana implementacija STP-a je dizajnirana za mreže koje nisu koristile VLAN. Postojalo je jedno zajedničko stablo za sve switch-eve. Kada su VLAN-ovi počeli da postaju uobičajeni za segmentaciju mrežne infrastrukture, STP je poboljšan da uključi podršku za VLAN. Kao rezultat, prošireno polje ID sistema sadrži ID VLAN-a sa kojim je BPDU povezan.

Kada se koristi Extentded System ID, on menja broj bitova dostupnih za vrednost prioriteta mosta, tako da se povećanje vrednosti prioriteta mosta menja sa 1 na 4096. Prema tome, vrednosti prioriteta mosta mogu biti samo višestruke od 4096.

Vrednost proširenog ID sistema se dodaje vrednosti prioriteta mosta u BID-u da bi se identifikovali prioritet i VLAN BPDU okvira.

**+49. Varijante i karakteristike STP protokola.**

Postoji nekoliko varijanti prvobitnog standarda IEEE 802.1D, među kojima su i sledeći.

**STP** – Ovo je prvobitna verzija IEEE 802.1D koja pruža topologiju bez petlji u mreži sa redundantnim vezama. Zajednicko sprežno stablo (CST, Common Spanning Tree) podrazumeva jednu instancu sprežnog stabla za celu mrežu sviceva, nezavisno od broja VLAN-ova.

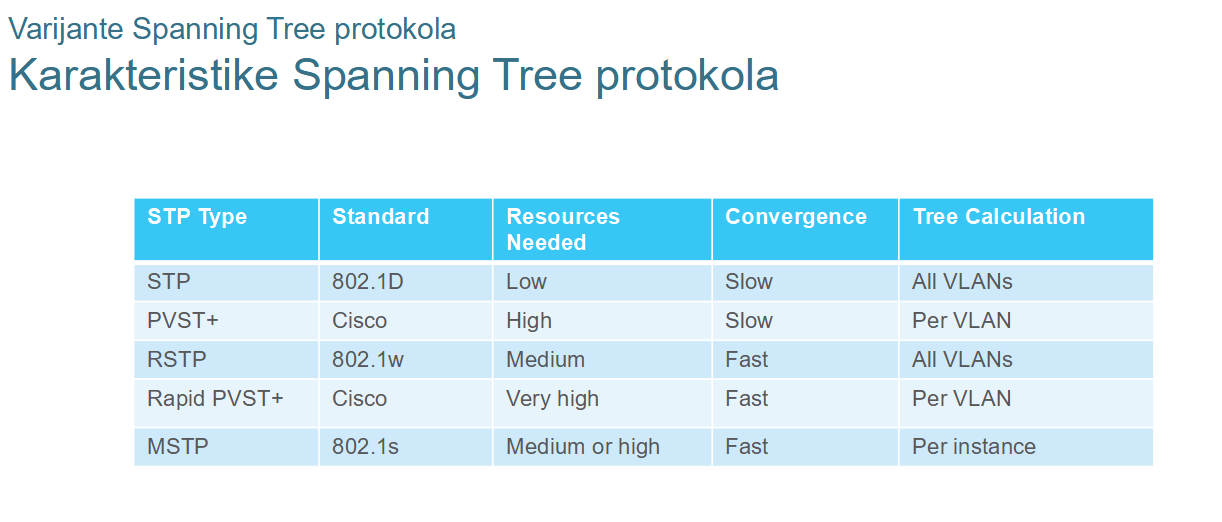
**PVST+** – Ovo je Cisco-ovo unapređenje STP-a koje pruža odvojene 802.1D instance sprežnih stabala za svaki VLAN konfigurisan na mreži. Odvojene instance podržavaju *PortFast, UplinkFast, BackboneFAst, BPDU guard, BPDU filter, root guard, i loop guard.*

**802.1D-2004** – Ovo je ažurirana verzija STP standarda; ukljucuje IEEE 802.1w

**Rapid Spanning Tree Protocol (RSTP)** ili **IEEE 802.1w** – Ovo je evolucija STP-a koja pruža bržu konvergenciju nego STP.

**Rapid PVST+** – Ovo je Cisco-vo unapređenje RSTP-a koje koristi PVST+. Rapid PVST+ pruža izdvojene instance standarda 802.1w po VLAN-u. Odvojene instance podržavaju PortFast, BPDU guard, BPDU filter, root guard i loop guard.

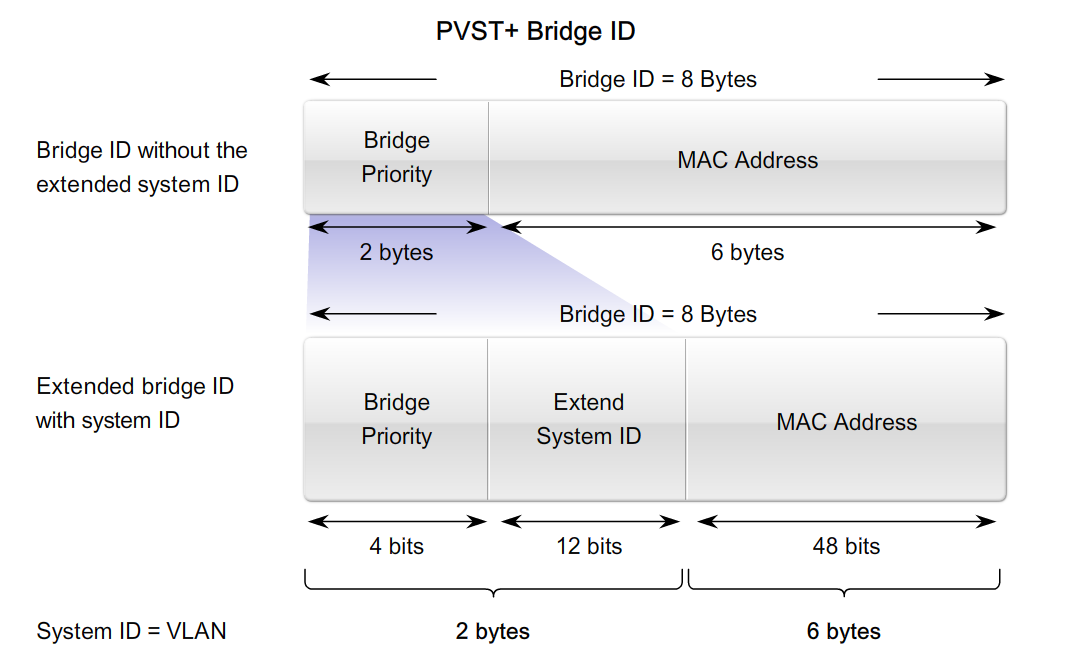
**Multiple Spanning Tree Protocol (MSTP)** – Ovo je IEEE standard inspirisan ranijom Cisco-vom implementacijom MISTP (Multiple Instance Spanning Tree Protocol). MSTP mapira više VLAN-ova na jednu instancu sprežnog stabla. Cisco-va implementacija MSTP-a je MST, koji omogućuje do 16 instanci RSTP-a i kombinuje više VLAN-ova sa istom fizickom i logickom topologijom u jednu instancu RSTP-a. Svaka instanca podržava *PortFast, BPDU guard, BPDU filter, root guard i loop guard.*

**

**50. PVST+ protokol.**

Origilani 802.1D standar definiše zajednićko sprežno stablo za sve VLAN-ove. Pravi se jedno stablo za celu mreži bez obzira na broj VLAN-ova. Nmea deljenje i balansiranje opterećenja i Blokirani port blokira sve VLANove. Nije zahtevan protokol.

PVST+ svaki VLAN ima svoju spanning tree instancu. Jedan port može blokirati jedna VLAN i istovremeno prosleđuje saobraćaj na drugom VLAN-u. Može da balansira opterećenje ali veoma je zahtevan ako se koristi veći broj VLAN-ova.



PVST+ zahteva da se za svaki VLAN pokrene posebna instanca sprežnog stabla. Da bi podržao PVST+, 8-bajtno BID polje je modifikovano da nosi VLAN ID (VID). Na slici, polje prioriteta mosta je smanjeno na 4 bita, a novo 12-bitno polje, prošireno polje ID

Sledeće pruža više detalja o PVST+ poljima:

* Bridge Priority – 4-bitno polje nosi prioritet bridge-a. Zbog ograničenog broja bitova, prioritet se prenosi u diskretnim vrednostima u koracima od 4096, a ne u diskretnim vrednostima u koracima od 1, kao što bi bili da je dostupno puno 16-bitno polje. Podrazumevani prioritet, u skladu sa IEEE 802.1D, je 32,768, što je vrednost srednjeg opsega.
* Extended System ID – 12-bitno polje koje nosi VID za PVST+.
* MAC adresa - 6-bajtno polje sa MAC adresom jednog switch-a.

MAC adresa je ono što čini BID jedinstvenim. Kada se prioritet i prošireni sistemski ID dodaju MAC adresi switch-a, svaki VLAN na switch-u može biti predstavljen jedinstvenim BID-om.

**51. Stanja STP portova, podrazumevana vremena, uticaj na dijametar mreže.**

Port ide od Blocking stanja pa do listening, pa Learning, Forwarding i Disabled stanju.

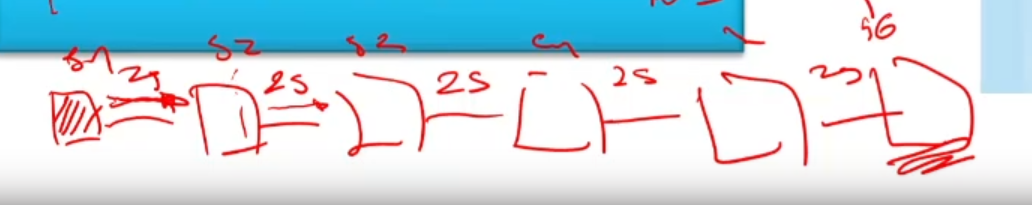
U stanju blocking port provede 20 sekundi i u tom stanju može da prima i procesira BPDU-ove

Nakon toga ide 15 sekunde na za listening za to vreme on i dalje sluša ove BPDU-ve i šalje BPDU-ove da bih učestvovao u izboru root bridge-a

Nakon toga je faza learning koji takođe traje 15 sekunde i u toj fazi sve je izabrano i počinje da uči MAC adrese da bih nakon toga presao u Forwarding stanje.

Disabled je administrativno disabled port.

Dijametar mreže utiče na vreme kada će svaki switch da nauči ko je root bridge. Na primer ako imamo 7 switch-a redno povezanih da je dijametar mreže jednak 7. Prvi switch šalje svoj hello packet drugom switch-u. Drugi switch u međuvremenu šalje svoj hello packet ali primiće hello packet od prvog switch-a i (u najgorem slučaju) moraće da čeka 2 sekunde pre nego što ponovo pošalje svoj hello packet na dalje. I tako će trebati svakom switch-u 2 sekunde da pošalje svoj hello packet pre nego što poslednji switch ne sazna ko je root switch. Ovaj deo će trajati oko 15 sekundi .Na kraju ove računice dodajemo 20 za blocking, 15 za listening i 15 za learning i trebaće nam sve ukupno 65 sekundi za ceo STP.



**52. Rapid PVST+**

Rapid PVST+ ubrzava STP rekalkulacije tako da protokol konvergira brže (Cisco-va verzija RSTP-a)

Rapid PVST+ uvodi 2 nova tipova portova

* Alternate Port - Ne mora da prođe kroz sve faze kao u PVST+ nego direktno iz Alternate port prelazi u Forwarding port. Postoji samo na P2P linkove. Eksplicitno se kaže koji je Alternate Port
* Backup port

RSTP (802.1w) koristi BPDU tipa 2, verzija 2, tako da RSTP bridge može da komunicira 802.1D na bilo kojoj deljenoj vezi ili sa bilo kojim switch-em koji koristi 802.1D. RSTP šalje BPDU-ove i popunjava bajt flagova na nešto drugačiji način nego u 802.1D:

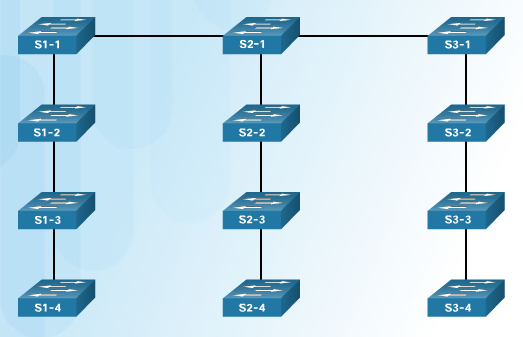
* Informacije o protokolu mogu odmah da se zastare na portu ako se hello ne primi tri uzastopna hello puta, podrazumevano 6 sekundi, ili ako istekne tajmer za maksimalnu starost.
* Pošto se BPDU-ovi koriste kao mehanizam za održavanje aktivnosti, tri uzastopno propuštena BPDU-a ukazuju na izgubljenu povezanost između mosta i njegovog susednog root ili designated bridge-a. Brzo starenje informacija omogućava brzo otkrivanje grešaka.

Sadrži i dva bitna Flaga koji se zovu Proposal i Agreement. Gde switch koji primeti pad salje BPDU switch-u koji sadriži proposal i kaže “predlažem da, pošto je druga strana pala da promeniš ulogu” i on mu odgovara sa BPDU koji sadrži Agreement i menja svoju ulogu

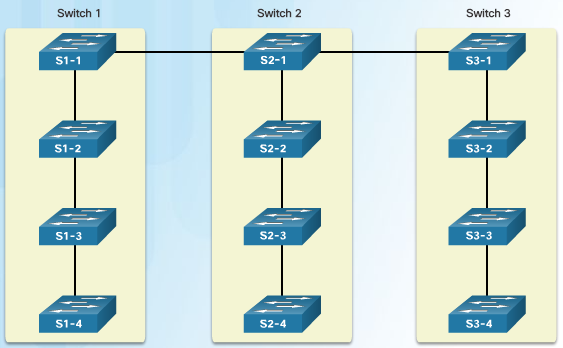
**53. Switch Stacking koncept i „Stek“ u STP stablu.**

Stack switcheva je povezivanje switcheva u daisy chain tako da nam se čini da radimo sa jednim velikim switch-em. Povezani su jedan sa drugim sa veoma brzim kablovima. Najbitnija stvar kod stacka jeste što imaju svoj master switch a stack ima samo 1 ip adresu i 1 konfiguraciju. Portovi se označavaju sa 3 broja. Prvi broj označava broj switch-a a drugi obično nula ba broj port-a.

Ukoliko je potrebno povezati više uređaja na access nivou. Nama ako treba na primer 100 portova. Mi ako normalno povežemo te switcheve nama će diameter mreže biti 9 pa bi trebao nam trebalo oko 20-25 sekundi da se izvrši STP. I plus 50 za blocking, listening i learning i trebaće nam više nego minut (75 sekundi) za celu konvergenciju.



Da to ne bi bio slučaj možemo povezati switcheve u stack Switcheva i da smanjimo dijametar mreže na 3.



**54. Definicije: defekt, greška, otkaz, pouzdanost, dostupnost, MTTF, MTBF.**

Defekt - uzrok kvara

Greška - pogrešan rezultat

Kvar/otkaz - stanje sistema u kom sistem može dati pogrešan izlaz ili prestati da funkcioniše. Mogu se klasifikovati po vremen trajanja (trajni, privremeni, povremeni) i efektima koja ima.

Pouzdanost - je verovatnoća u funkciji vremena, u oznaci R(t), koja ima vrednost u trenutku t jednaku verovatnoći da je sistem bez prekida bio ispravaon od t0 do trenutka t. Ova mera je pogodna za opis sistema kod kojih i trenutni prekid u radu sistema može imati velike posledice

MTTF- Mean Time to Failure, Prosečno vreme rada sistema do pojave otkaza

MTBF - Mean Time Between Failures, prosečno vreme između 2 otkaza, uključuje i vreme potrebno za oporavak sistema, MTTR - Mean time to Repair

MTBF = MTTF + MTTR

Dostupnost - funkcija vremena, u oznaci A(t), čija je vrednost jednaka prosečnom vremenu koje je sistem bio ispravan u vremenskom intervalu [0,t]. Ova mera je pogodna za sisteme gde konrinuirani rad nike toliko važan, kao ukupno vreme za koje je sistem bio dostupan.

Dugoročna dostupnost

A je jednako verovatnoći da je sistem ispravan u bilo kom vremenskom trenutku. Dugoročnu dostupnost ima smisla određivati samo kod sistema koji se mogu oporaviti od otkaza.

Dugoročna dostuponost može se računati kao

A = MTTF/MTBF = MTTF/(MTTF+MTTR)

Trenutna dostupnost je verovatnoća da je sistem dostupan u konkretnom trenutku t

**55. Mere dostupnosti i tipovi sistema.**

| Naziv | Nedostupno (min. po god.) | Dostupnost | Klasa |
| --- | --- | --- | --- |
| Unmanaged | 52560 (36 dana) | 90% | 1 |
| Managed | 5256 (3 dana) | 99% | 2 |
| Well-managed | 526 (9 sati) | 99.9% | 3 |
| Fault-tolerant | 53 | 99.99% | 4 |
| High-availability | 5 | 99.999% | 5 |
| Very high availabiliy | 0,5 | 99,9999% | 6 |
| Ultra High Availability | 0,05 | 99,99999% | 7 |

**56. Izvođenje MTTF iz stope otkaza.**

**Stopa otkaza** komponenti je najznačajniji parametar u analizi otkaza pojedinačnih komponenti. Predstavlja očekivani broj otkaza pojedinačnih komponenti u jedinici vremena za seriju proizvedenih komponenti. Zavisi od starosti komponente, fizičkih karakteristika, temperature u kojoj komponenta radi i dr.

Neka je:

1. Komponenta ispravna u trenutku t=0 i ispravna do trenutka otkaza
2. T vreme do otkaza
3. Otkaz trajan

Označimo sa f(t) funkciju gustine verovatnoće i sa F(t) kumulativnu distribuciju.

Veza između ovih funkcija je

,

U teoriji verovatnoće, funkcija gustine verovatnoće (engl. probability density function - PDF) je funkcija čija se vrednost u datom uzorku (ili tački) može protumačiti kao relativna verovatnoća da će vrednost slučajne promenljive biti jednaka tom uzorku. Drugim rečima, dok je apsolutna verovatnoća da kontinuirana slučajna promenljiva poprimi bilo koju određenu vrednost jednaka 0 (pošto postoji neograničen skup mogućih vrednosti), vrednost funkcije dva različita uzorka mogu se koristiti za izvođenje zaključka.

Uslovna verovatnoća otkaza je verovatnoća da će komponenta otkazati u narednom periodu , ako je ispravna u trenutku t.

Kako je , sledi

Ukoliko uslovna verovatnoća otkaza ne zavisi od starosti komponente, =

Rešenje dif. Jednačine je

Srednje vreme do otkaza MTTF za nepopravljive sisteme je jednako očekivanom vremenu života

Za konstantu stopu otkaza

**57. Jedinstvene tačke otkaza i redundantni sistemi**

Jedinstvena tačka otkaza je deo složenog sistema čiji otkaz dovodi do otkaza celokupnog sistema. Sistem se može učiniti robusnim i pouzdanim eleiminisanjem single points of failure.

Redundant sistemi se mogu dele na :

Hardverska redundansa

N-modularna redundansa je hardverska tehnika dodavanjem N komponenti gde svaka komponenta može preuzeti osnovnu funkciju u slučaju otkaza

Najpoznatiji sistemi su

* Dual modularna redundansa
  + Pogodna za multipliciranje celih sistema tako da ako jedan otkaže drugi može preuzeti rad
* Triple modularna redundansa
  + Pogodna za hardverske komponente na nivou logičkih komponenata, lako se može obezbediti oprovakav većinskim glasanjem

Informaciona redundansa

Specijalni kodovi koji se može rekonstruisati pogrešan/pogrešni bitovi

* Parity check
* CRC
* itd.

Disk sistemi

* RAID 1,2,3,4,5

Softverska redundnasna i

Redundansna mreža

* Redundansa na L1
  + Fizički postavljeni redundantni linkovi i komponente
* Redundansa na L2
  + Omogućena STP protokolom
* Redundansa na L3
  + Omogućena ruting protokolom i zavisi od brzine konvergencije protokola
* Redundansa na L4-L7
  + Load Balanseri

**58. Koncept „First Hop Redundancy“ protokola**

Ukoliko na istom VLAN-u imamo 2 ili više rutera, neophodan je mehanizam za preusmerenje saobraćaja u slučaju otkaza. Npr ako je neki ruter podešen kao gateway za pc i rutira pakete koji dolaze do njega. U slučaju otkaza Rutera neki drugi ruter bi mogao da preuzme ulogu prvog rutera jer postoji put, a i po IP adresama su na istom VLAN-U.

Za prevenciju SPoF može se podesiti “virtualni ruter”. Tako da računari imaju iluziju da je dostupan samo jedan ruter, a fizički ima 2 ili više rutera sa istom IP adresom i MAC adresom. Na celom segmentu hostovi imaju adresu virtualnog rutera podešen kao gateway.

Mogućnost da mreža samostalno odredi na osnovu otkaza da će uređaj raditi kao default gatewaz anziva se first-hop redundancy.

Kada aktivni ruter otkaže, redundancy protocol predaje standby ruteru aktivnu ulogu. Prvo standby ruter prestaje da dobija hello poruke od forwarding rutera. Nakon toga standby router preuzima ulogu forwarding rutera. S obzirom da novi forwarding ruter preuzima i IPv4 i MAC adrese virtuelnog rutera, hostovi ne primećuju prekid.

FHRP protokoli su:

Hot Standby Router Protocol - Cisco proprietary FHRP dizajniran da omogući transparentni failover gejtveja. Funkcija HSRP protokola je da prati rad HSRP grupe uređaja i brzo preda ulogu forvardovanja paketa u slučaju otkaza.

HSRP for IPv6 - Ista funkciolanost samo IPv6.

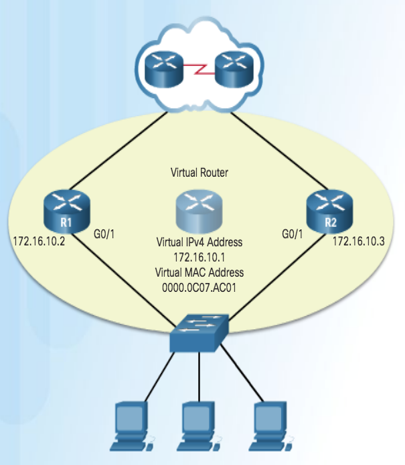
Virtual Router Redundacy Protocol version 2 - Non Proprietary protokol koji dinamički dodeljuje odgovornost jednom ili više virtuelnih rutera VRRP grupi na IPV6 Lan. Jedan ruter master, svi drugi backup.

VRRPv3 - Podrška za IPv4 i IPv6

Gateway load balancing protocol - Cisco-Proprietary FHRP koji omogućava balansiranje opterećenje između redundantnih rutera.

GLBP for IPv6 - Podrška za IPv6

**59. HSRP protokol**



Jedan od rutera je izabran za aktivni ruter i preko njega se rutira saobraćaj.

Drugi ruter će postati standby ruter.

Ako aktivni ruter otkaže, standby ruter će preuzeti njegovu ulogu.

Na hostovima je podešena jedna default gateway adresa, i to VIRTUALNA adresa koji prepoznaju oba rutera.

Active i standby ruteri se određuju na osnovu procesa izbora (election process). Podrazumevano, ruter sa najvećom IPv4 adresom će biti izabran za aktivni ruter. Proces HSRP izbora će koristiti prioritet umesto adrese ako je podešen.

HSRP prioritet

Default HSRP priority: 100.

Opseg: 0 to 255

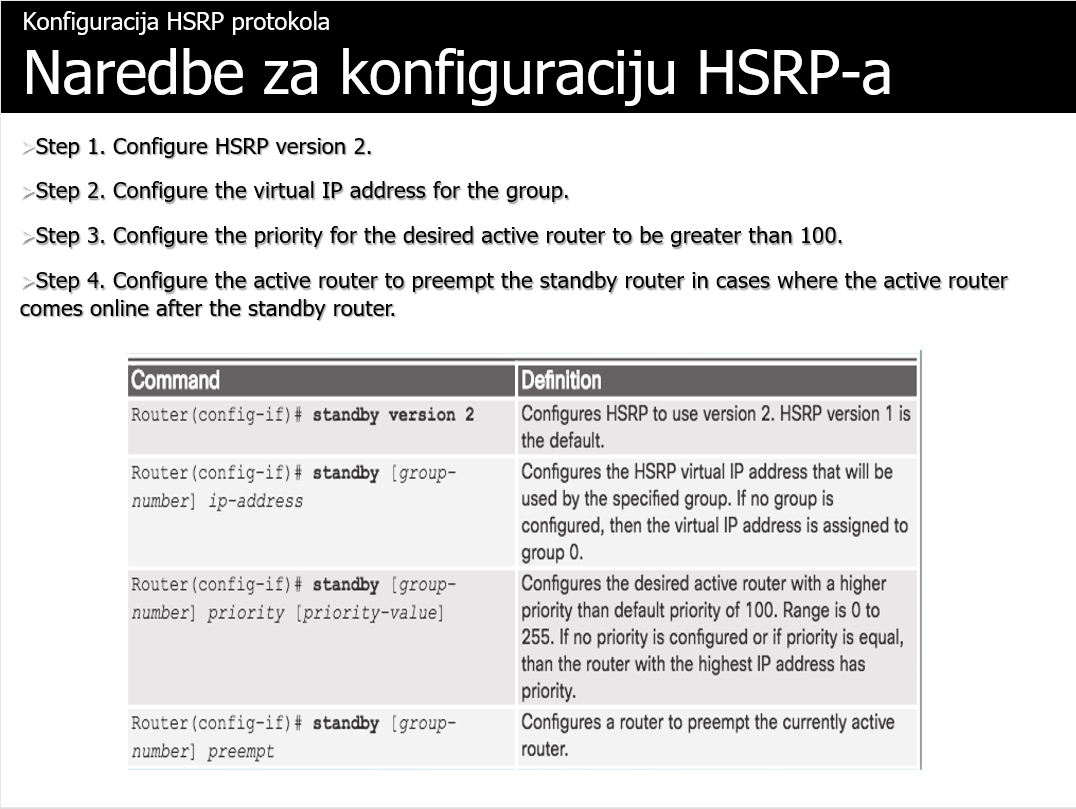
Veći broj, veći prioritet.

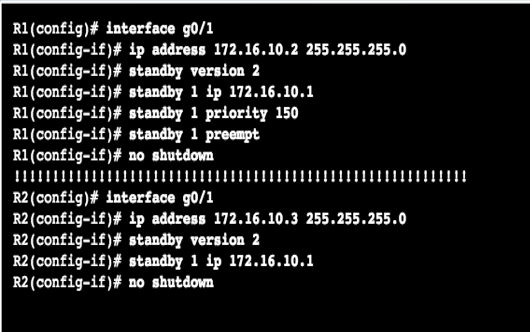
standby priority interface naredba.

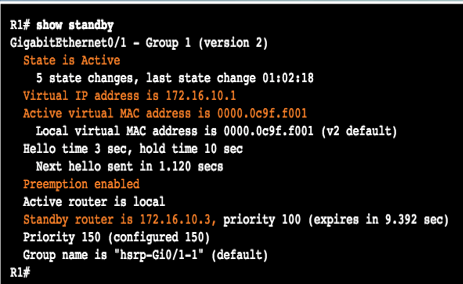
HSRP Preemption

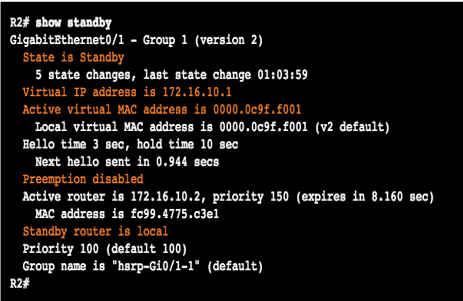
Preemption – mogućnost da se automatski pokrene Proces izbora novog rutera

Active i standby HSRP ruteri šalju hello pakete na multikast adresu HSRP-a na svake 3 sekunde po default-u. Standby ruter će postati aktivan ako ne dobije 3 sukcesivna hello paketa, t.j. nakon 10 sekundi



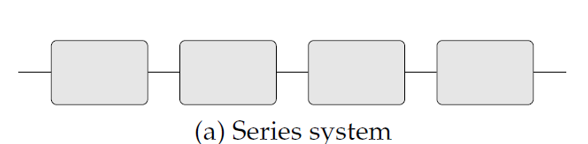




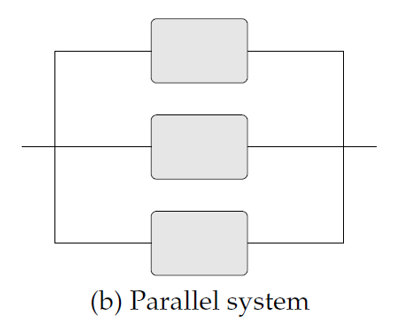


**60. Pouzdanost složenih sistema**

Pouzdanost složenih sistema se računa na sledeći način:



Ukoliko imamo rednu vezu sistema. Ukoliko znamo pouzdanost za svaki deo sistema onda računamo pouzdanost na sledeći način:



Sistem je neispravan ako su sva 3 dela sistema neispravna. Računa se na sledeći način: Da je bilo koji deo sistema neispravan računa se kao (1-R(t)). Da su svi istovremeno neispravni je proizvod tih verovatnoća. Ovaj proizvod je verovatnoća da sva 3 sistema su neispravna. A 1 minus ceo taj proizvod je verovatnoća da je taj sistem ispravan

Ako imamo sistem gde nije jasno odrediti šta je paralelno a šta je serijski.

**61. Odrediti dostupnost zadate mreže.**

//pogledajte T8.Vezbe

**62. Podela WLAN po veličini oblasti, razlika između WLAN i WiFi razvoj bežičnih mreža**

Wireless Local Area Network je lokalna mreža moja koristi bežične tehnologije

**WPAN** - Wireless personal area network, blisko okruženje korisnika uglavnom point to point tipa, pogodno za umrežavanje malih razmera

**WLAN** - Wireless Local Area Network, Koristi 2.4Ghz i 5Ghz frekventni opseg

* Fleksibilan Dizajn
* Glavne tehnologije: 802.11n/ac/ax (trenutno) 802.11a/b/g (ranije)

**WMAN** - Wireless Metropolitan Area Network - Uglavnom se koriste za kreiranje backbone mreža na većem području.

* Potrebna je dozvola za javno korišćenje
* Glavna Tehnologija 802.16

**WWAN** - Wireless Wide Area Network - Uglavnom se kriste kao backbone mreže za povezivanje udaljenih tačaka

* Glavne Tehnologije: 2G/3G/4G/5G, satelitska komunikacija, itd.

Termin WiFi je skraćenica od **Wireless Fidelity**.

Razlika između Wi-Fi i WLAN je u tome da je IEEE 802.11 WLAN standard, dok je Wi-Fi implementacija 802.11 standarda.

Razvoj:

1973 – Univerzitet na Hawaii kreirao AlohaNet koja je imala koncepte Metcalfe etherneta

1980 - MetCalfe predlaže standarde i kreira standarde 802 koja standardizuje sve mrežne standarde

1985 - Dodeljen je frekventni opseg za razvoj wireless mreža

1988 - Prvi put napravljen prototip bežične mreže s nazivom WaveLAN

1990 - Oformljen 802.11 koja se bavi isključivo bežičnom mrežom

1993 - Usvojen 2,4GHZ

1996 - John O’Sullivan dobija patent za WiFi

1997 - IEEE napravio standard koji direktno uticao na Patent John-a, Tražili su da se odrekne patenta da bi ta tehnologija mogla da se koristi javno. Reko ne.

1999 - Napravljena Wireless Alijansa

1999-2000 - Publikovani 802.11a i 802.11b

2000 - Kreiran Wi-Fi certified concept

2003 - Kreiran 802.11g

2004 – Kreiran 802.11i

2009 - kreiran 802.11n, najdominantniji

2013 - Kreiran 802.ac za telefone

2018 - usvojena Wi-Fi 4, WiFi 5, i WiFi 6

**63. Frekventni opsezi i bež. kom. sistem. Kodiranje i modulacija.**

Radio opseg je od 3kHZ do 300GHZ, delimo ga na 11 kategorije.

Imamo ELF (3 Hz do 30 Hz) - sonari, SLF (30 Hz do 300 Hz) - govor, ULF (300 Hz do 3 kHz) – bliske komunikacije, VLF (3 kHz do 30 kHz) - ultrazvuk, LF (30 kHz do 300 kHz) – međunarodni brotkast, MF (300 kHz do 3 MHz) – AM radio, HF (3 MHz do 30 MHz) – lične radio stanice, VHF (30 MHz do 300 MHz) – FM radio i TV, UHF (300 MHz do 3 GHz) – TV broadcast, bežične mreže, mikrotalasne peći, SHF (3 GHz do 30 GHz) – bežične mreže, radari, sateliti, EHF (30 GHz do 300 GHz) – radio astronomija, medicinski skeneri,…,

2.4Ghz (2,4000 - 2,4835GHZ) se nalazi na UHF opseg dok 5GH(5,15-5,35Ghz i 5,725 - 5,850 Ghz) se nalazi na SHF



Bežični komunikacioni sistem čine transmitter i receiver (prijemnik i predajnik). Svaki učesnik u komunikaciji mora da ima i predajnik i prijemnik da bi imao dvosmernu komunikaciju – primopredajnik (eng. transceiver).

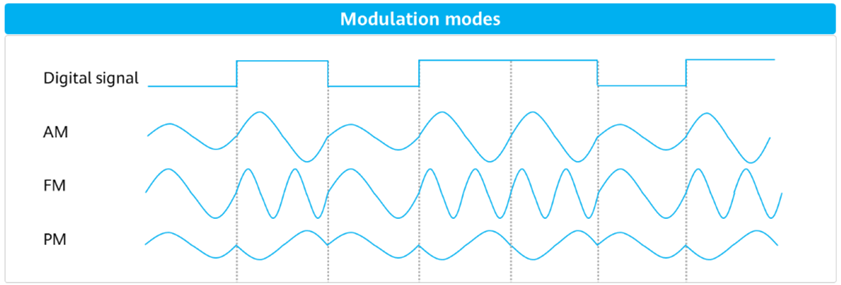
Predajnik vrši kodiranje (coding) i modulaciju signala (modulation), a prijemnik inverzne funkcije: demodulaciju i dekodiranje.

Source signal koji se kodira on se kodira u digitalni signal (digitalizacija signala) korišćenjem neke kodne šeme.

Source kodiranje se vrši u 2 podfaze

* Source coding
  + Predstavlja proces konverzije “raw” signala u digitalni signal korišćenje neke kodne šeme
* Channel coding
  + Dodavanje dodatnih informacija da bi signal bio otporniji da smetnje.

Dužina antene za emitovanje signala je direktno proporcionalna talasnoj dužini



Modulacija je tehnika kojom se korisni signal osnovne frekvencije integriše u signal više frekvencije koji je pogodan za prenos preko radio talasa

AM – amplitudna modulacija – amplituda visokofrekventnog signala se menja sa promenom amplitude baseband (korisnog) signala (tj kada je digitalni signal 0 onda su amplitude male dok kada je digitalni signal 1 onda su amplitude veće)

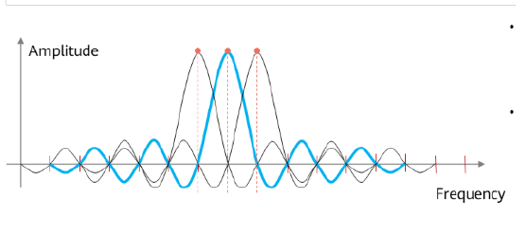
FM – frekventna modulacija – frekvencija visokofrekventnog signala se menja sa promenom amplitude baseband signala (tj kada je digitalni signal 0 onda je manjom frekvencom se prostire talas dok kada je digitalni signal 1 onda većom frekvencom se prostire)

PM – fazna modulacija - faza visokofrekventnog signala se menja sa promenom amplitude baseband signala. Npr. za digitalni signal 1 odgovara faznom pomeraju od 180 stepeni, dok 0 odgovara faznom pomeraju od 0 stepeni (slika)

**64. Noseći signal, OFDM. Kanali. Preklapanje kanala.**

Carrier signal - osnovni signal koji se moduliše korisnom informacijom. Tipično sinusoidnog oblika. Podaci se šalju preko nosećeg signala su male frekvencije.

OFDM (Orthogonal frequency-division multiplexing) tehnike vrši se modulacija nekoliko kanala istovremeno na jedan opseg. To nam daje da prenosimo više signala kroz jedan medijuma. Signali se utisnu u jedan drugi tako da množenjem signala, tj interferencija signala biće nula i neće se mešati i idealno mogu se razdvojiti jedan signal od drugog. Ako je vrh jednog signala u logičkom maksimumu onda svi ostali paralelni signali moraju da budu 0.



Kanal je frekventi opseg u kome je dozvoljena varijacija frekvencije da bi se preneo korisni signal. Na slici imamo prikazane sve kanale koji su na 2.4 Ghz Gde imamo ukupno 14 kanala, svaki je širine 20MHz i međusobno su pomereni za po 5Mhz. Ovde imamo ne preklapajuće kanale koji se neće mešati i neće praviti smetnje jednim drugim. To su kanali 1, 5, 9, 13. Može se koristiti paralelno bez ikakve smetnje. Kod 802.11b nepreklapajući kanali su 1,6,11 zato što su kanali širine 22MHz.



Preklapanje kanala je izuzetno bitno zbog interferencije. Kanala ima konačan broj. Broj pristupnih tačaka je izuzetno veliki. Ukoliko imamo 2 kanala koji rade na istoj frekvenciji. Oni će jednom drugom da naprave smetnje i u teoriji da idu na mnogo manjoj brzini iako standard dozvoljava da ide mnogo više. Zato postoji zagušenje kanala.

|  |  |
| --- | --- |

**65. 2.4 i 5GHz kanali. Grupisanje kanala. Spatial Stream. Single- Dual i Three radio**

2.4Ghz kanal: podeljen je na 14 preklapajućih kanal širine 20 MHz, centralna frekvencija se računa na sledeći način: 2412+(n-1)\*5Mhz. S tim da 14. se retko koristi. Kanali od 1 do 13 se koriste u većini sveta dok Severna Amerika koristi od 1 do 11.

5Ghz kanal: Svaki kanal je po 20MHz. Prvih 8 pripadaju prvoj grupi, Drugi opseg ima 12 kanala (nema ih u Kini) a treći opseg ima 5 kanalač. Tako da sve ukupno imamo 25 nepreklapajućih kanala

Jedan kanal jedan prenos. Mogu da se grupišu kanali da se ubrza prenos. Tako da ako imamo dva 20MHz kanal i spojimo ih u jedan 40MHz brzina se duplira. 802.11ac daje grupisanje 8 kanala u kanale od po 160MHZ.

Ukoliko radio-sistem šalje više signala istovremeno, svaki signal se naziva Spatial Stream. Broj antena je jednak broju prostornih prenosa. 802.11n je prvi standard koji maksimalno definiše 4 antene. Isto se označava kao 4x4 MIMO (multipli input multiple output) sistem.

Svaki access point može se naći u 3 različita režima rada. To su single-radio, Dual-radio ili Three-radio AP

Single radio je uređaj ima samo 1 antenu i može da se prenosi samo na 2.4 ili 5GHz. 20-25 bežičnih klijenta.

Dual radio ima mogućnost a poveže klijente ili na 2.4 ili na 5GHz istovremen. Broj klijenata je prešao na 40-50.

Three radio AP može da ima 1 radio na 2.4 i 2 na 5GHz i može da ima oko 70 korisnika.

**66. 802.11 standardi**

Bežicni ureaji imaju prijemnike i predajnike podešene na odreene frekventivne opseg radio-talasa. Sledeci opsezi su alocirani za 802.11 bežicne lokalne mreže:

2.4 GHz – 802.11b/g/n/ad

5 GHz (SHF) – 802.11a/n/ac/ad

60 GHz (EHF) – 802.11ad

IEEE 802.11 WLAN standard definiše kako se radio-frekvence u nelicenciranim ISM frekventnim opsezima koriste za fizicki sloj i MAC pod-sloj bežicnih veza.

Tokom godina postojale su razne implementacije standarda IEEE 802.11. Slede neke najvažnije:

802.11 – Stvoren 1997 i više se ne koristi. Ovo je prvobitna WLAN specifikacija koja je radila na opsegu od 2.4 GHz i pruža je brzine do 2Mb/s. Kada je objavljen, žicani LAN-ovi su radili na 10Mb/s, tako da nove bežicne tehnologije nisu bile prihvaćene s entuzijazmom. Bežicni uređaji imaju jednu antenu kojom šalju i primaju bežicne signale.

802.11a – Izdat 1999, radi na ne tako prepunom opsegu frekvencije 5 GHz i nudi brzine do 54Mb/s. Pošto ovaj standard radi na višim frekvencama, pokriva manju površinu i ima manju efektivnost u prolasku kroz zidove. Bežicni uređaji takođe imaju jednu antenu. Uređaji koji rade pod ovim standardom nisu interoperabilni sa 802.11b i 802.11g standardima.

802.11b – Izdat 1999, radi na frekventnom opsegu od 5 GHz i nudi brzine do 11Mb/s. Uređaji koji implementiraju ovaj standard pokrivaju veću površinu i bolji su u proboju prepreka nego uređaji bazirani na standardu 802.11a. Takođe imaju jednu antenu.

802.11g – Izdat 2003, radi na frekventnom opsegu od 2.4 GHz i nudi brzine do 54Mb/s. Prema tome, uređaji koji implementiraju ovaj standard rade na istim radio-frevencama kao i 802.11b, ali sa propusnim opsegom koji ima 802.11a. Imaju jednu antenu. Kompatibilan je sa 802.11b. Međutim, kada podržava klijenta koji ima 802.11b, ceo propusni opseg se smanjuje.

802.11n – Izdat 2009, radi na frekventnim opsezima od 2.4 GHz i 5 GHz i ovakvi uređaji se često nazivaju “dvoopsežni” uređaji. Protok podataka obicno iznosi između 150Mb/s i 600Mb/s, dok je domet na oko 70m. Međutim, da bi se postigle visoke brzine, pristupne tacke i bežicni klijenti moraju da imaju više antena i da koriste višeulaznu-višeizlaznu tehnologiju (MIMO). MIMO koristi veci broj antena i kao pošiljaoce i primaoce kako bi povecao performanse komuniacije. Podržano je do cetiri

antena. Kompatibilan je sa uređajima koji implementiraju 802,11a/b/g. Ipak, mešanje standarda imaće za posledicu slabiji protok podataka.

802.11ac – Izdat 2013, radi na frekventnom opsegu od 5 GHz i pruža brzinu od 450Mb/s do 1300Mb/s. Koristi MIMO tehnologiju za poboljšanje performansi komunikacije. Podržava do osam antena. Kompatibilan je sa 802.11a/n uređajima, ali mešanje standarda ima za posledicu manji protok podataka.

802.11ad – Izdat 2013, poznatiji kao “WiGig”. Koristi tri opsega: 2.4 GHz, 5 GHz i 60 GHz, a nudi teoretsku brzinu do 7Gb/s. Međutim, signal na frekveciji od 60 GHz ne može da penetrira kroz zidove, pa se ta brzina postiže samo ako su uređaji na veoma malim razdaljinama i bez prepreka među njima. Kada se korisnik kreće kroz prostor, protokol može da se prebaci na nižu frekvenciju (i samim tim manje protok), ali je moguća propagacija signala kroz zidove i druge prepreke.

**67. 802.11 MAC: CSMA/CA. Hidden i Exposed nodovi.**

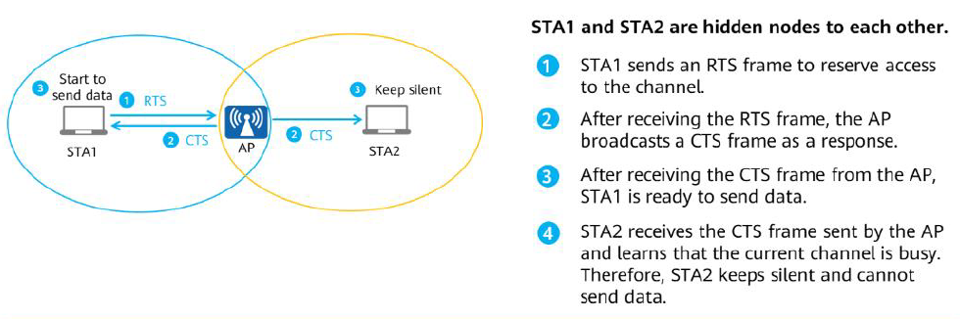
Za razliku od CSMA/CD koji imamo kod žičanih Ethernet mreža kao algoritam za pristup medijumu (Media Access Control – MAC algoritam), kod bežičnih mreža imamo CSMA/CA

CS – Pre slanja podataka STA proverava da li je kanal slobodan da bi smanjila šanse za koliziju

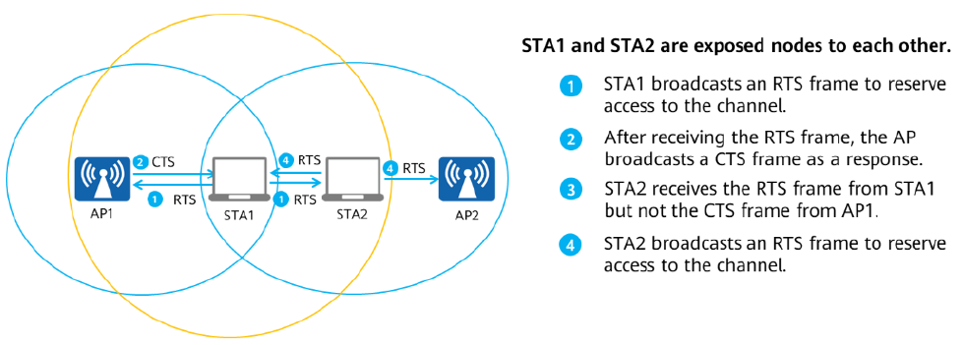
MA – Podaci koji se šalju mogu biti primljeni na više odredišta

CA – (Collision Avoidance) dizajniran za minimizira mogućnost pojave kolizije

„CA“ se postiže RTS/CTS (Request to send/ Clear to send) protokolom, koji rešava problem postojanja „skrivenih čvorova“ (hidden node problem)



Klijenti ne znaju za postojanje jednog drugog ali AP zna za njihovo postojanje uvek šalje broadcast CTS da onaj koji je tražio da šalje može da pošalje paket a drugi da ništa ne radi.



STA1 ima asocijaciju sa AP1 i šalje broadcast RTS koji će primiti i STA2. AP1 šalje CTS ka STA1 ali STA2 je čuo RTS ali nije čuo CTS i samim tim STA2 zaključuje da njegov medijum nije zauzet.

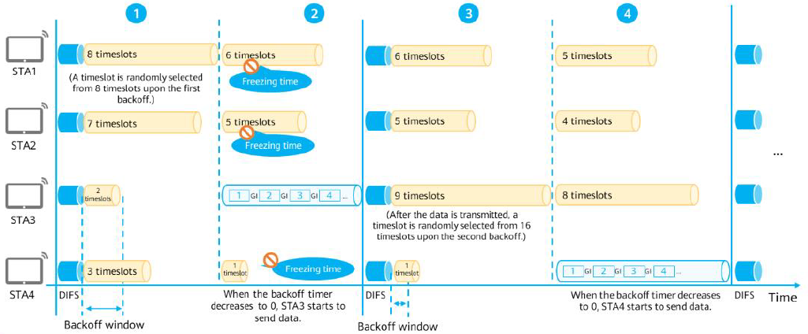
**68. 802.11 MAC: SIFS i DIFS. Binarni eksponencijalni backoff algoritam.**

IFS (Interframe Spacing) - vreme koje je potrebno sačekati između 2 frejma

SIFS (Short IFS) - Vreme koje je potrebno da jednoj stanici da prebaci režim rada iz slanja u prijem i obrnuto. Koristi se za pravljenje razmaka između 2 frejma

DIFS - (Distributed coordination Function IFS) - Je najduže vreme koje se čeka. Vreme za koje medijum treba da bude slobodan da bi stanica podrazumevala da niko ne prenosi ništa preko kanala i započne slanje svog frejma.

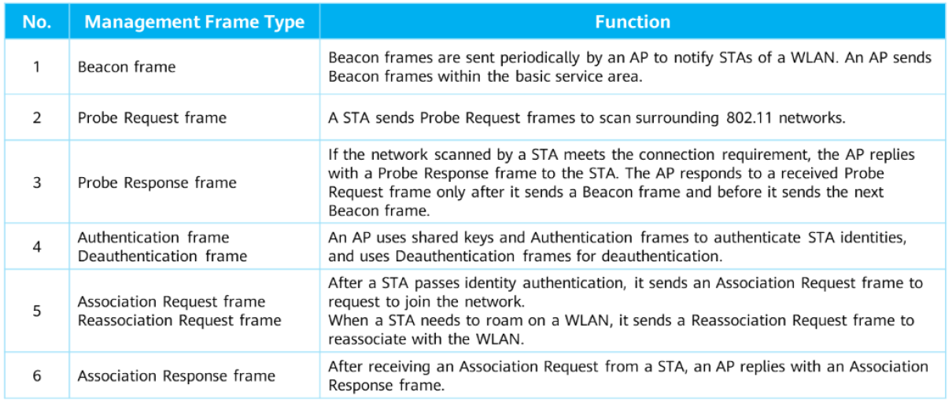
Binarni eksponencijalni backoff algoritam. U početku računar bira broj u opsegu 1 - 2^(2+i), dok je i broj iteracija. Za prvi slot bira se od 1 do 8. Kada broj slotova poraste do 255 (6 backoff-ova) vreme se više ne povećava

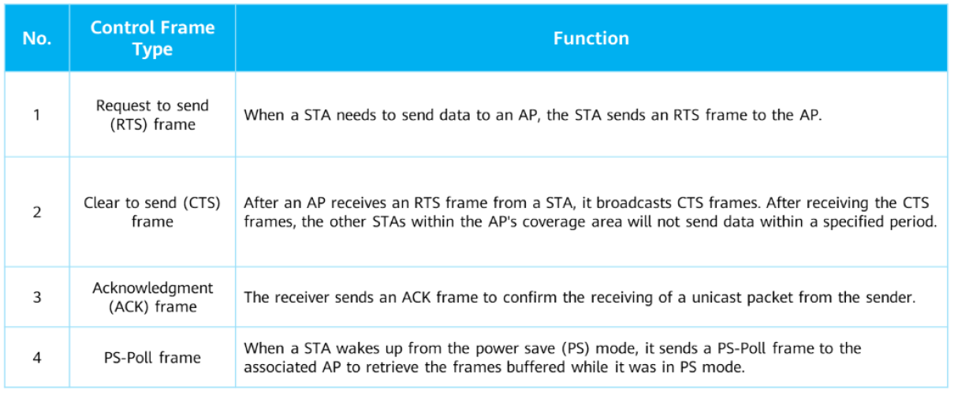


Na primeru sa slike: STA1 do 4 biraju random vreme za prvi slot (1 do 8). Nakon izbora vreme kreće da teče. Pošto je STA3 sa najmanjim brojem prvo će joj isteći vreme, pa počinje da prenosi. Za to vreme i ostalim stanicama je vreme skraćeno za po 2 slota. Dok STA3 prenosi, ostale stanice ne odbrojavaju. Nakon završetka prenosa, STA3 bira random vreme za sledeći prenos, i sve nastavljaju da odbrojavaju vreme dok prvoj ne istekne vreme (STA4 u ovom slučaju)…

**69. Tipovi frejmova 802.11 standarda.**

* Management frejmovi
  + Imaju supervizorsku ulogu.
  + Koriste se kada se STA povezuje na AP ili ga napušta, ili kada se vrši reasocijacija na drugi AP
* Control frejmovi
  + Carrier-sensing funkcije
  + Acknowledgment
  + Funkcije kontrole kanala
* Data frejmovi
  + Frejmovi koji prenose korisničke podatke





**70. Process povezivanja STA na AP.**

Da bi bežicni uređaji komunicirali preko mreže, moraju prvo da prođu kroz proces asocijacije sa pristupnom tackom ili sa bežicnim ruterom. Između uređaja se razmenjuju upravljački frejmovi kako bi se obavio sledeći trofazni proces:

* Otkrivanje novih bežicnih pristupnih tacaka.
* Autentifikacija sa pristupnom tackom.
* Asocijacija sa pristupnom tackom.

Da bi obavili proces asocijacije, klijent i pristupna tacka moraju da se slože oko nekih parametara. Najcešci parametri su:

Režim mreže – Misli se na 802.11 WLAN standarde. Pristupne tačke i bežični uređaji mogu da rade u mešovitom režimu, što znači da mogu da istovremeno koriste više standarda.

SSID – SSID je jedinstven identifikator koji bežični klijenti koriste da razlikuju različite bežične mreže koje se nalaze jedna blizu druge. Ako je emisija SSID-a uključena, ime SSID-a ce se nalaziti na listi dostupnih mreža na klijentu. U zavinsosti od konfiguracije, nekoliko pristupnih tacaka mogu da dele isti SSID.

Podešavanje kanala – Odnosi se na frekventne opsege koji se koriste za transmisiju. Bežicni ruteri i pristupne tačke mogu da biraju podešavanje kanala ili može da se podesi ručno ako postoji mešanje sa drugim bežicnim uređajima.

Režim bezbednosti – Odnosi se na podešavanja kao što su WEP, WPA ili WPA2. Za kućnu potrebu ili malu kancelariju, koristi se WPA1 Personal.

Enkripcija – WPA2 zahteva izbor enkripcije. Treba koristiti AES kada god je to moguce..

Šifra – Od bežicnog klijenta se zahteva da unese šifru kako bi se autentifikovao pristupnoj tacki. Omogućava kontrolisan pristup mreži.

Bežični uređaji moraju da otkriju i povežu se na pristupnu tacku ili bežican ruter. Povezivanje se obavlja procesom koji se naziva skeniranje ili pretraživanje (scanning, probing). Ovaj proces ima dva režima.

Pasivni režim. – Pristupna tačka otvoreno oglašava svoje usluge periodičnim slanjem signalinih frejmova (beacon frames) koji sadrže SSID, podržane standarde i podešavanja bezbednosti. Ovaj režim omogucava klijentima da pretraže koje su im mreže dostupne i izaberu neku da se prikače na nju.

Aktivni režim. – Bežicni klijent mora da zna ime SSID-a. On započinje postupak emisijom zahtevom za pretragu na više kanala. Zahtev za pretragom sadrži ime SSID-a i podržane standarde.

Standard 802.11 je prvobitno razvijen tako da podrži dva mehnizma za autentifikaciju.

Otvorena autentifikacija. Autentifikacija u suštini ne postoji: klijent kaže “autentifikuj me”, a pristupna tacka odgovara sa “da”.

Autentifikacija sa deljivim kljucem. Tehnika bazirana na ključu koji se unapred razmeni između klijenta i pristupne tacke.

Proces razmene frejmova radi autentifikacije obicno tece ovako:

(1) Klijent šalje frejm za autentifikaciju pristupnoj tački.

(2) Pristupna tačka odgovara izazovnim tekstom.

(3) Klijent enkriptuje poruku koristeći svoj deljivi kljuc i vraca enkriptovan tekst pristupnoj tacki.

(4) Pristupna tacka dekriptuje enkriptovan tekst koristeći svoj deljiv kljuc.

(5) Ako se dekriptovan tekst poklapa sa izazovom, klijent je uspešno autentifikovan. U suprotnom se pristup ne odobrava.

Zatim sledi faza asocijacije.

(1) Klijent šalje frejm sa zahtevom za asocijacijom koji sadrži njegovu MAC adresu.

(2) Pristupna tačka odgovara frejmom sa odgovorom koji sadrži BSSID pristupne tacke, tj. svoju MAC adresu.

(3) Pristupna tačka mapira logički port (identifikator asocijacije – AID) prema klijentu. AID je ekvivalentan portu na svicu.

**71. BSS, BSA, OBSS, SSID, BSSID, DS i EBS.**

**BSS** - Basic service set - Skup usluga koji pruža jedan access point

**BSA** - Basic Service Area - Access point sa njegovim klijentima, tj oblast koju pokriva jedan BSS

**OBSS** - Overlapping Basic Service Set - Preklapanje 2 BSA, za roaming se koristi gde ako klijent predje sa jednog AP-a na drugi, on će bez autentifikacije imati asocijaciju sa drugim AP-om

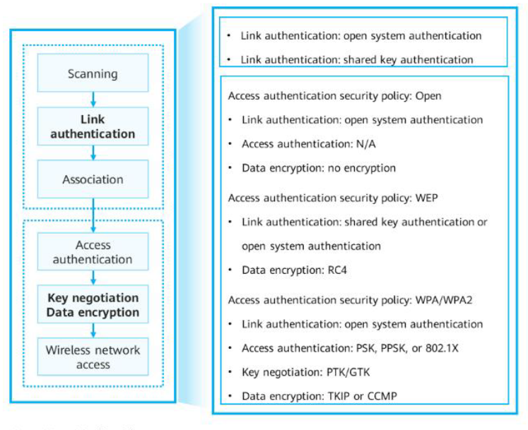
**SSID** - Service Set ID - najpotrebnija stvar za roaming, Naziv za AP-a 2 access point-a mogu imati isto ime

**BSSID**- Basic Service Set ID - Jedinstveno ime za AP koristi se od strane klijenta da bi znala sa kojim AP-om je uspostavljena veza.

**DS**- Distribution System - Veza između 2 BSS

**ESS**- Extended service set - je OBSS i AP imaju isti SSID da korisnici ne primećuju promene BSS-a

**72. 802.11i model, WEP, WPA/WPA2 i bezbednosne šeme**



802.11i je skup standarda koji se tiču bezbednosti uvodi: Access authentication i Key negotiation i Data encryption.

802.11i sadrži 2 autetifikiacije. *Link autentifikaciju* i *Access Authentifikaciju*. Link autentifikacije je samo autentifikacija veze AP i stanice. Dok access autnetifikacije je komunikacija sa serverom i AP-om, gde server sadži podatke korisnika. Nakon access autentifikacije ide Key negotiation Data encryption. Izvodjenje različitih ključeve za jedan AP.

Bez obzira da li se koristi Access Auth ili ne, faza link auth se ne preskače, već se u slučaju da se koristi AA, LA sprovodi kao open auth.

Link authetntification može da bude Open ili Shared key dok Access authentication može da bude ili Open, ili WEP ili WPA/WPA2.

WPA ima različite načine autentifikacije kao PSK (preshared key) gde svi korisnici imaju identičnu šifru, PPSK (Peruser Pre shared key) gde svaki korisnik ima svoju šifru za pristup, 802.1X je IEEE koji koristi externi server za authentifikacije.

Wired Equivalent Privacy (WEP) je originalni bezbednosni mehanizam IEEE 802.11 koji je prisutan u standardu praktično od samog nastanka.

Vrši funkciju zaštite mreže od neautorizovanog pristupa.

Koristi RC4 šifrator i statičke ključeve za enkripciju podataka.

Sve STA koriste isti ključ za pristup

WEP je kripotgrafski nebezbedan i postoje poznati napadi koji kriptoanalizom za desetak minuta dolaze do tačne šifre.

Da bi rešili problem nebezbednosti WEP-a, WiFi Alijansa je predložila Wi-Fi Protected Access (WPA).

WPA uz RC4 koristi bezbedniji TKIP algoritam/protokol za upravljanje ključevima i eliminiše nebezbedne statičke ključeve iz algoritma (Temporal Key Integrity Protokol).

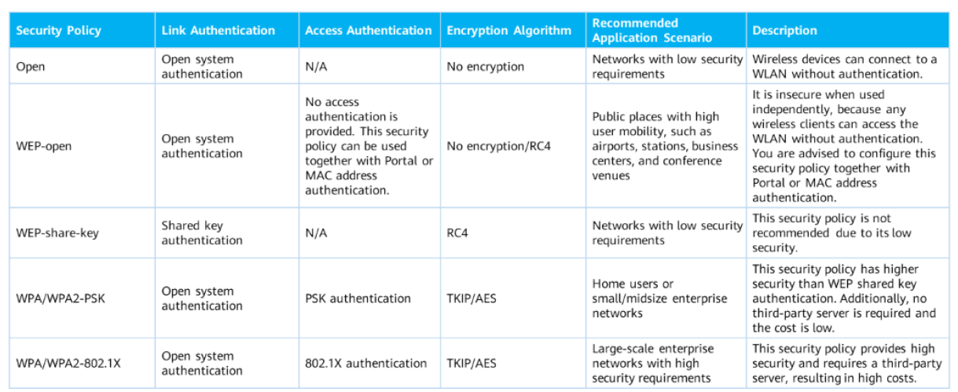
Na ovaj način je obezbeđena hardverska kompatibilnost između WEP i WPA/TKIP uređaja.

Pored TKIP, WPA može koristiti i noviji i bolji AES algoritam za enkripciju. (UVEK KORISTITI AES)

WPA/WPA2 ima personal i enterprise varijantu.

Personal: koristi preshared-key tehniku. Pogodna za male mreže

Enterprise: koristi 802.1X autentifikacioni model za autentifikaciju korisnika korisničkim imenom i šifrom preko RADIJUS (AAA) servera.



**73. 802.1X, EAP, AAA, RADIJUS**

AAA - Authentication, Authorization, and Accounting

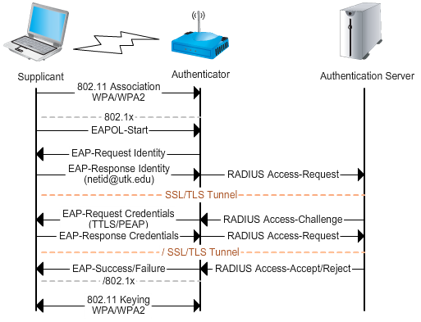
Authentification - Provera da li korisnik ima pravo da pristupi mreži

Authorisation - Autorizuje korisnika za korišćenje pojedinih servisa

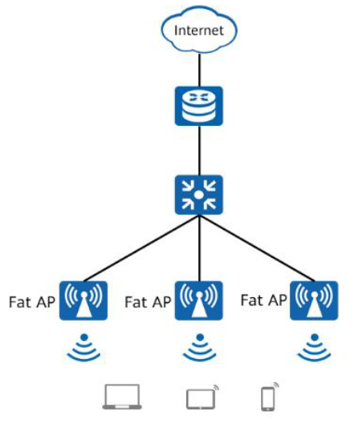
Accounting - Vođenje evidencije.

Na RADIUS server se implementira AAA. Radius koristi UDP protokol na portove 1812 i 1813 za AAA.

802.1X je model autentifikacije koji najčešće koristi RADIUS server za autentifikaciju. 802.1X Definiše EAP (Extensible Authentification Protocol) za razmenu podataka između STA, authentifikatora i servera za authentifikaciju.



**74. Fat AP arhitektura. WDS.**



Fat AP arhitektura naziva se i “autonomna” mrežna arhitektura, autonomna u smislu da AP-u nije potrebna podrška drugih uređaja da bi funkcionisao. Kompletna konfiguracija se vrši na AP.

Prednost: Lako se postavlja i cena koštanja je niska

Mane: Ako se pokriva veća površina svaki AP mora posebno da se konfiguriše. Nije dobar za veće mreže.

WDS (Wireless distribution system) je sistem koji omogućava bežičnu vezu između nekoliko AP-ova na IEE 802.11 mreži. Omogućava da BSA bude proširen korišćenjem više AP-ova bez potrebe postavljanja između njih. Root AP je jedini koji treba da ima bar jedan port povezan za žičanu mrežu.

Ovo je daleko lošije repenje od Fit AP + AC mreže.

Većina Fat AP-ova ima WDS mod. Nije više u upotrebi

**75. AC + Fit AP. CAPWAP.**

AC + Fit AP je trenutno de facto standard za velike WLAN mreže (pokrivanje cele zgrade jedne kompanije, hotela, stadiona, i sl.)

Access Controler (AC) je mrežni uređaj, vizuelno vrlo sličan običnom sviču, čija je uloga:

* Centralizovana konfiguracija svih AP-ova kroz konfiguraciju grupa AP-ova
* Kontrola pristupa WLAN-u
* Prosleđivanje korisničkog saobraćaja (poput proxy servera, ako je podešen da radi u tunnel modu)
* Prikupljanje statistike
* Konfiguracija i upravljanje AP-ovima
* Upravljanje roaming-om
* Upravljanje bezbednošću

Fit AP – nikakva podešavanja direkno se ne vrše na njemu.

* Dobija IP adresu AC-a i uspostavlja CAPWAP (Control and Provisioning of Wireless Access Points) tunel do njega.
* AC upravlja radom Fit AP-a
* Fit AP ima funkciju L1 uređaja: enriptuje i dekriptuje 802.11 frejmove.

CAPWAP - Control and Provisioning of Wireless Access Points, sam CAPWAP enkapsulira Korisničke i kontrolne informacije.

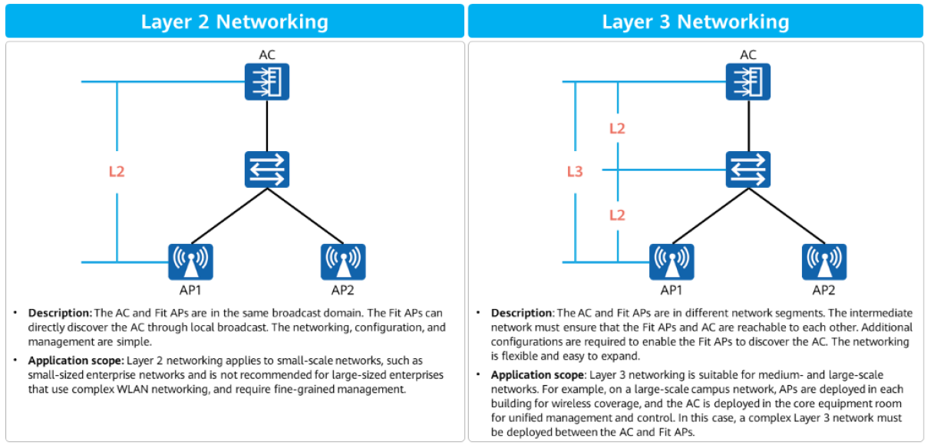
Omogućava AP-ovima da automatski (plug-and-play) otkriju za postojanje AC-a:

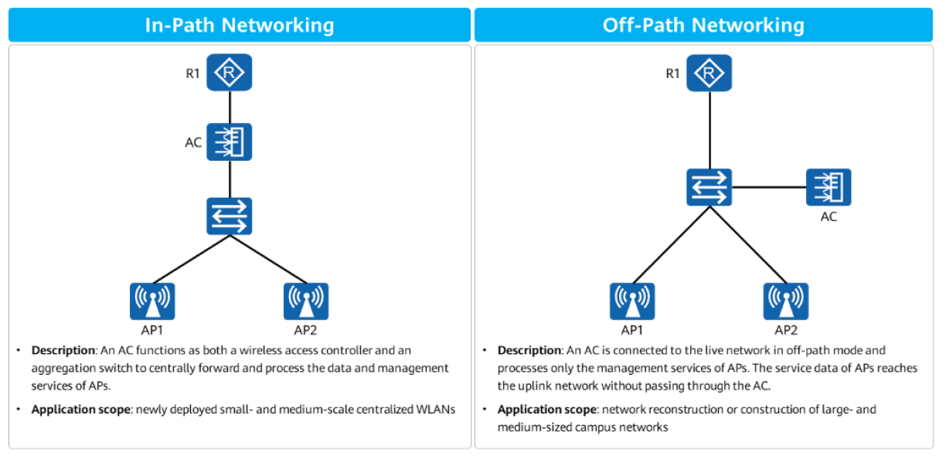
* Ukoliko su na istom brotkast domenu, nakon što Fit AP dobije adresu od DHCP servera, brotkastuje discovery paket
* Ukoliko nisu na stoj IP mreži, AP uz IP adresu treba da od DHCP-a dobije i IP adresu AC-a (preko DHCP opcije 43)

Održava konekciju između AC-a i AP-a keep alive mehanizmom

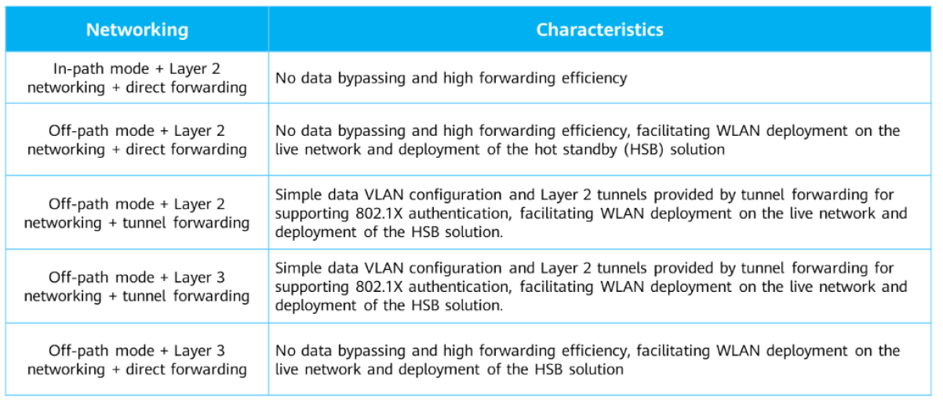
Omogućava da nakon uspostavljanja veze AC uploaduje konfiguraciju na AP

**76. Mrežni modovi WLAN arhitektura.**









Sve kombinacije ove 3 stvari mogu da se prave… Veoma obimno čudo mrzime da pišem sve.

**77. Planiranje VLAN-ova i IP adresa AC + Fit AP.**

VLAN na kome se ostvaruje CAPWAP i VLAN na kom su STA se može razlikovati kod AC+ Fit AP arhitekture. Bez obzira na mod u kom AC i AP rade.

AP uvek ima 2 VLAN-A jedan je za Management drugi je za Service i Management je obično na Native Vlan switch-a. AP neće znati koji su VLAN ovi i neće enkapsulirati i poslaće discovery na AC. Bitno je da je AC na Native VLAN-u.

Ako ima isti broj SSID-eva koliko i VLAN ova, to je jednostavniji roaming jer IP adresa STA Je validna prilikom prelaska ali je teže implementirati na većim mrežama. Dok ako imamo različite VLANo-ove na iste SSID-eve onda roaming jedino radi preko tunnel moda

**78. WLAN roaming i primeri prosleđivanja paketa.**

WLAN roaming omogućava da STA prelazi sa jednog na drugi AP bez prekida veze i servisa

Da bi roaming bio moguć:

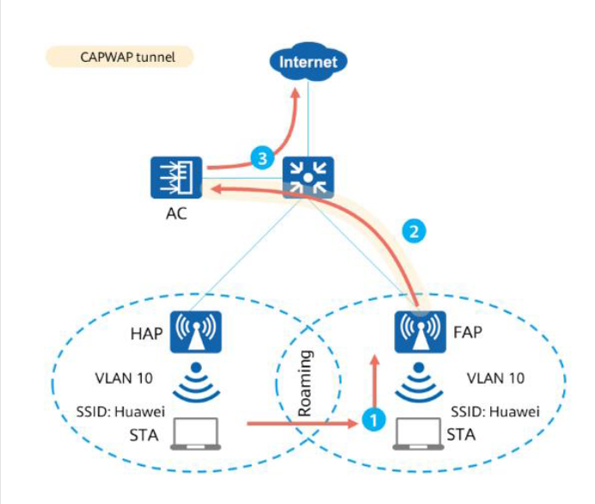
* SSID treba da je isti
* Scurity identičan
* Mod za autentifikaciju isti

Roaming je transparentan što se tiče korisnika i kod projektovanja DOMEN AP-a može da se preklapa. STA tokom roaming zadržava svoju IP adresu

Koraci:

1. STA detektuje da postoji AP sa istim SSID-jem koji ima jači signal od AP-a na koji je trenutno povezan
2. SSID je isti, BSSID se razlikuje
3. STA šalje zahtev na oba BSSID-a za reautentifikacijom
4. Raskida vezu sa jednim i vrši reasocijaciju (poseban 802.11 frejm) na drugi AP.

Postoje L2 i L3 roaming. Kod L2 svi AP su na istom VLAN-u dok kod L3 svaki AP može biti na različitom VLAN-u i arhitektura mora da bude u tunel modu.



Kod L2 roaming sa tunnel forwarding, pre roaming stanica šalje service paket do svog AP-a. Nakon primanje servisnih paketa, taj AP šalje ih do AC kroz CAPWAP tunnel. Na kraju AC prosleđuje servisne pakete do mreže kroz switch-a.

Nakon ovoga pomerimo stanicu do drugog udaljenog AP-a i povezuje se na njega. Napomena: Prvi AP i udaljeni AP moraju da budu na istom VLAN-u. Čim stanice se pomeri do udaljenog AP-a radi se isto kao kod svog domaćeg AP-a, tj Stanica šalje service pakete udaljenom AP-u. Nakon sto udaljeni AP primi servisni paket šalje ih do AC kroz CAPWAP tunel. I AC prosleđuje service pakete do mreže kroz switch

Najjednostavnija varijanta L2 roaming je sa Direct forwarding. Sada nam AC uopste nije bitan. Bitno je da je isti VLAN da oba AP-a. Pošto je Direct forwarding, stanica šalje direktno ka odredištu. Nakon prelaska u drugu AP zonu. Drugi AP će nastaviti direktno da šalje pakete direktno ka odredištu.

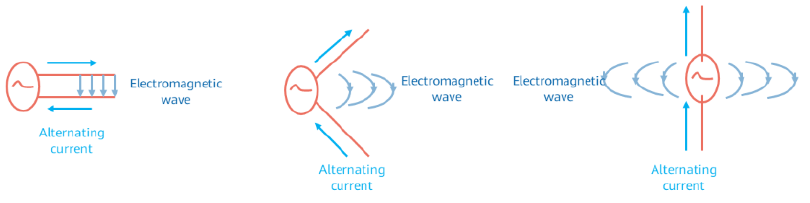
Najveća muka je L3 roaming. U ovom slučaju npr AC je negde na cloudu. Pre roaming stanica šalje pakete na domaći AP, domaći AP šalje pakete kroz CAPWAP tunel do AC-a i na kraju AC prosleđuje pakete kroz switch do odredišta. Nakon Roaming-a, stanica je došla do drugog AP-a koji je na skroz drugom vlan-u. Moraće bez obzira što koristimo Direct forwarding da se tunneluju paketi od udaljenog AP-a do AC-a kroz CAPWAP, dalje preko CAPWAP da AC vrati saobraćaj do domaćeg AP-a, gde je inicijalno stanica dobila IP adresu, i taj domaći AP da prosleđuje pakete direktno do odredišta na mreži

**79. Antene**

Radio talasi su elektromagnetni talasi koji se prostiru kroz prostor.

Signal radio frekvencije je elektromagnetni talas koji se prostire kroz prostor na frekvencijama između 300 kHz i 300 GHz. Mikrotalasi su talasi (prostiranje, zračenje) frefvencije od 300 MHz do 300 GHz

Kada su dva provodnika blizu jedan drugom, električno polje je ograničeno i zračenje je malo. Kada su dva provodnika daleko jedan od drugoga električno polje je povećano.

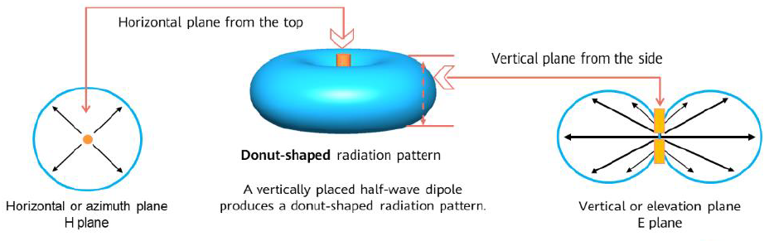


Npr ovde na slici vidimo da što su bliži provodnici koji idu u suprotnom smeru vidimo da su talasi sve manji. Dok kod ove kranje varijante imamo nešto što liči na antenu. Ovakvu antenu nazivamo omno-direkcione antene tj ne usmerene antene.

Antene možemo klasifikovati na sledeći način.

* Po usmerenosti
  + Omnidirectional
  + Directional
  + Smart antena
* Po polarizaciji
  + Jednostruko polarizovana
  + Dvostruko polarizovana
* Po izgledu
  + Štap
  + Pločasta
* Po lokaciji
  + Eksterna
  + Ugrađena

Oblast pokrivanja omni-antene



Ako gledamo po horizontalnom preseku vidimo da u kržnici idu talasi, tj prostiru se jednako i da je maksimalan domet u horizontali ravni. Sposobnost predaje antene i prijema je jednaka

Međutim ako se gleda vertikalni presek vidimo da nije skroz jednaka i da je energija zračenja antene u pravcu antene je 0.

Direkcione antene dobijamo tako što na suprotnoj strani gde želimo da se prostire talas stavimo reflektujuće ogledalo da šalje zrake gde treba.

Relativna snaga u logaritamskoj skali se izražava u decibelima i određuje na sledeći način:

Gde je A snaga čija se vrednost izražava u dB, B je referentna snaga.

Za jačinu signala uzima se jedinica dBm, gde je referentna snaga 1mW

Antene su pasivni elementi => antene ne pojačavaju signal

Gain (eng. dobit) je odnos snaga elektromagnetnog talasa koji emituje konkretna antena i hipotetička antena koja s uzima za refencu. Mi gain karakterišemo kao dobit ali u jednom smeru može samo da bude.



Npr na ovom primeru dobili smo gain u jednom smeru ( u ovom slučaju na domet ) ali izgubili smo na drugim smerovima (više ne ide na gore ili na dole).

Ili ako oko antene imamo perfektnu sferu kako se prostire elektromagnetni talas. Onda gain možemo dobiti tako što ćemo imati veći domet ali signal slabi gore i dole

Gain se izražava u decibelima.

Ukoliko se računa u odnosu na idealnu sferu jedinice su dBi

Ukoliko se raluna u odnosu na idealnu omni antenu jedinice su dBd.

Razlika između dBi i dBd je 2.15dB (dBd = dBi + 2,15dB)



**80. Prostorno planiranje WLAN mreža**

Treba da se prvo izvrši planiranje i projektovanje mreže. Koncept je isti kao i kod žičanih, treba da se izvši specifikacija zahteva i snimanje prostora, nakon čega ide iterativno projektovanje mreže, i na kraju implementacija mreže i testiranje mreže. Zahtevi se veoma razlikuju. Treba da se ispune zakonske regulative i dostupnost kanala. Npr za 2.4 Ghz je dozvoljeno bez posebnih dozvola ali samo ako je snaga manja od 100 mW. Treba da uzmemo nacrt zgrade za razgovor zahteva i očekivanja. Treba posebno pričati o porkivenost prostorija WiFi signalom. Treba specificirati:

1. Ključne oblasti - signal najbolji
2. Oblast nižeg ranga - očekuje da ima signal ali slablji
3. Oblasti gde nije potreban signal

Nakon toga ide specifikacija jačine signala. Slabljenje od -40 do -65dB sasvim odlično zadovoljava kvalitet bežične mreže. Preko -75dB mreža ne valja.

Broj uređaja je bitan da se zna koliko AP može biti na tom prostoru. Tipovi uređaja da se zna kolika brzina treba njima. Lokacija napajanja za AP-ove. I lokacija switch-eva AC-a.

Kada se dobije neki plan treba onda početi raspoređivanjem uređaja, treba znati tipična slabljenja. Npr ako ima neke prepreke koje oslabljuju signal. Što znači na nekim prostorijama mora da bude više AP-ova da bi mogli da pokriju celu prostoriju.

**81. Na kom rastojanju od AP-a će jačina signala za 2.4/5 GHz radio biti na granici jačine definisane za ključne oblasti, ako je predajna snaga AP-a x mW, gain antene y dBi/dBd, i između AP-a i STA prepreka od z debljine d cm.**

Jačina\_signala = 10\*log(x/1mW) + y - z - d

Treba da izacunamo gubljenje signala po udaljenosti d i to što ima zid debiljne z. I tada dobijamo Jačinu signala. Nominlna jačina je oko -40dB do -65dB, loša je oko -75dB

**+82. VoIP komunikacioni modeli.**

**POTS** je uobičajena oznaka za Plain Old Telephone Service. POTS prenosi kontrolni i audio signal preko iste parice. Oprema sadrži tri podsistema:

**Indikacija dolaznog poziva** (ringer ) – To je zvono ili svetlosna indikacija koja obaveštava korisnika o dolaznom pozivu.

**Povezivanje korisnika na centralu** (hookswitch) – U pitanju je podsistem koji detektuje da je korisnik podigao slušalicu, bilo da se javi na dolazni poziv ili da inicira poziv.

**Biranje brojeva** (dial) – Do 1960. godine u upotrebi je bio pulsni sistem baziran na rotacionim delovima. Broj impulsa je odreiđvao cifru, a cifre su bile odvojene kratkim pauzama. DTMF (Dual Tone Multi-Frequency) je zamenio pulsni sistem biranje brojeva. Kod DTMF-a, svaka cifra se predstavlja sa po dva čista tona. Pruža veću brzinu biranja brojeva.

**VoIP** (Vocie over Internet Protocol) predstavlja popularni naziv za više tehnologija koje omogućavaju prenos glasa preko internet mreže korišcenjem IP protokola.

Postoji nekoliko tipova komunikacionih modela:

**Internet-to-Internet** – Ovaj tip poziva uključuje one čiji je telefon povezan na internet i koji pozivaju one čiji je telefon takođe povezan na internet. Celokupan poziv se takođe rutira unutar interneta.

**Internet-to-PSTN** – Ovi pozivi zahtevaju da korisnik koji poziva ima telefon priključen na internet, dok korisnik koji prima poziv ima telefon povezan na PSTN (**Public Switched Telephone Network**). U ovom slucaju, pozivi prolaze kroz segmente PSTN mreže i kroz segmente interneta.

**PSTN-to-Internet** – U ovom slučaju, korisnik koji poziva ima telefon u PSTN mreži dok korisnik koji prima poziv ima telefon povezan na internet. Kao i u prethodnom modelu, ovde takođe pozivi prolaze i kroz segmente PSTN mreže i kroz segmente interneta.

**PST-to-PSTN preko interneta** – Ovo je slučaj gde se poziv stvara i završava na uređajima koji su povezani na PSTN mrežu, ali se samo rutiranje poziva obavlja preko interneta. Ovo se radi jer je komunikacija preko interneta jeftinija i obično se koristi za međunarodne pozive.

**Internet-toInternet preko PSTN-a** – Kod ovog modela pozivi se ostvaruju i završavaju na uređajima koji su povezani na internet, ali se deo rutiranja poziva vrši preko PSTN mreže. Ovo se radi kada se zna da PSTN mreža smanjuje kašnjenje u komunikaciji u odnosu na internet.

**+83. VoIP protokoli i arhitektura.**

Kako bi podržala VoIP komunikacione modele, arhitektura mora da zadovoljni sledece funkcionalne zahteve:

**Pronalaženje adrese** – Kada je poziv iniciran, potrebno je pronaći lokaciju odredišta. Odredište može da bude neki IP telefon cija adresa može biti IP adresa ili URI (Uniform Resuorce Identifier). Adresa takođe može biti jedinstveni korisnicki identifikator, kao što je slučaj u mnogim P2P VoIP aplikacijama. Za podržavanje PSTN telefona, doredište treba da bude broj telefona.

**Interoperabilnost ureaja** – VoIP uređaj treba da bude interoperabilan sa drugim uređajima korišcenjem istog protokola.

**Interoperabilnost sa PSTN telefonima** – Potrebno je omogućiti komunikaciju VoIP mreže i PSTN.

**Kontrola nivoa sesija** – Autorizacija, autentifikacija, itd, na nivou sesije.

**Funkcionalnosti nivoa medijuma** – Odnosi se na servise omogućene protokolima kao što je RTP, npr. mešanje poziva u konferencijskom pozivu.

**Interoperabilnost meu komponentama** – Sve funkcionalne komponente VoIP arhitekture treba da budu interoperabilne ako koriste standardne protokole kao što su SIP/H.232.

//VoIP signalizacija direktan pristup i preko registra

VoIP standardi tabele

**H.323** je skup protokola koji omogućuju osnove za audio, video i prenos podataka kroz mreže bazirane na IP protokolu. H323 je mrežno, platformski i aplikacijski zavisan. To je signalni standard koji je baziran na paketima i on omogucuje interoperabilnost između H.323 uređaja.

Komponente ove arhietekture su:

**Media gateway** – Konvertuje jedan medijum u drugi. Na primer, konvertovanje digitalnog paketa glasa u analogni signal.

**H.323 gateway** – Ponaša se kao most između PSTN i IP mreže. Ima mogućnost da izabere kodek (codec, od coder-decoder) za glasovnu kompresiju.

**Pozivni serveri** – Pozivni serveri primaju poruke za uspostavljanje poziva, utvrđuju status odredišnih uređaja i proveravaju autorizaciju korisnika. Takođe, prave i šalju potrebne poruke kako bi obradili zahteve za poziv.

**Gatekeeper** – Cuvar ima nekoliko funkcija u VoIP mrežama:

– omogućuje kontrolu poziva,

– omogućuje pristup medijumu,

– upravlja propusnim opsegom izmeu dve krajnje tačke,

– izvršava prevođenje aderse, kontrolu pristupa i kontorlu zone,

– koordiniše pristupom ka drugim serverima i upravlja rutiranjem poziva i

– mapira brojeve telefona odredišta u njihove IP adrese.

**IP terminali i klijenti** – To su krajnje tacke na mreži, kao što su “hard” ili “soft” telefoni.

**SIP** je protokol koji omogućuje krajnjim tačkama uspostavljanje sesije. SIP radi upravo ono što mu i ime pokazuje: omogućuje da dve (ili više) krajnje tačke inicijraju sesiju, kao što je telefonski poziv ili video konferencija. SIP koristi jezik za opis medijuma i ima strukturu sličnu HTTP-u, što znači da se lako čita i razume.

SIP poruka se šalju u prostom tekstom, kao i HTTP. Imaju sledeci format:

message = start-line

\*message-header CRLF

[message-body]

start-line = request-line | status-line

Postoje sledeci metodi:

* **INVITE,**
* **BYE,**
* **Options,**
* **CANCEL,**
* **REGISTER,**
* **INFO**

SIP u svom radu koristi niz drugih protokola aplikativnog nivoa da identifikuje uređaje i prenosi poruke. Identifikacija i pregovaranje o vezi postiže se pomoću protokola SDP (Session Description Protocol). Za prenos govora koristi se RTP (Real-time Transport Protocol), a za uspostavljanje bezbednih veza SRTP (Secure Real-time Transport Protocol). Za bezbedan prenos SIP poruka, enkripcija se vrši pomocu protokola TLS (Transport Layer Security).

Korisnici mogu komunicirati sa ili bez prethodne registracije.

Osnovni tok uspostavljanje SIP veze

Registracija korisnika.

SIP URL (Uniform Resource Locator) zavisi od toga da li je korisnik registrovan ili se poziv uspostavlja direktno između krajnjih tačaka. Registrovani korisnik može imati numeričku ili alfanumeričku ekstenziju, formata sip:ekstenzija@registrator, na primer sip:collins@home.net ili sip:334455789@telco.net. Neregistrovani poziv obavlja se u formatu sip:ipAdresa, na primer sip:169.33.32.5

**84. Unified Communication Manager.**

**85. Praćanje i analiza rada mreže.**

**86. Optimizacija rada mreže i kvalitet servisa.**

**87. Uvođenje pravila i oblikovanje saobraćaja.**