
FAKULTET ZA INFORMATIKU I MENADŽMENT

Ana Milentijević

**UNIVERZITETSKA MREŽA
SA CISCO UREĐAJIMA**

- Diplomski rad -

FAKULTET ZA INFORMATIKU I MENADŽMENT

**UNIVERZITETSKA MREŽA
SA CISCO UREĐAJIMA**

– Diplomski rad –

Mentor:
prof. Mladen Veinović

Student:
Ana Milentijević
111-2005

Beograd, 2010.

FAKULTET ZA INFORMATIKU I MENADŽMENT

UNIVERZITET SINGIDUNUM
FAKULTET ZA INFORMATIKU I MENADŽMENT
Beograd, Danijelova 32

Broj: _____/2010

Kandidat: Ana Milentijević

Broj indeksa: 111/2005

Smer: Projektovanje i programiranje

Tema: Univerzitetska mreža sa Cisco uređajima

Zadatak: Realizovati i opisati rad univerzitetske mreže korišćenjem Cisco uređaja i Cisco patentiranih protokola.

MENTOR

Prof. dr Mladen Veinović

Datum odobrenja teme:
10.06.2009.
Beograd

DEKAN

Prof. dr Mladen Veinović

Sadržaj

Sažetak.....	8
Uvod.....	9
Arhitektura velike računarske mreže.....	9
Model hijerarhijske računarske mreže.....	9
Model složene računarske mreže.....	10
Model univerzitetske mreže	12
Internet protokol	13
Protokoli rutiranja	15
Enhanced Interior Gateway Routing Protocol	16
EIGRP metrika i odabir putanje.....	17
Raspoređivanje opterećenja saobraćaja.....	17
Nabitijske odlike EIGRP	18
Poređenje sa OSPF.....	18
Podešavanje EIGRP.....	18
Pravljenje VLAN-ova	21
Pravljenje VLAN-ova u opštem modu podešavanja	21
Pridruživanje portova VLAN-ovima	22
Provera VLAN podešavanja	22
VLAN Trunking	23
Podešavanje sabirne veze (Trunk Link)	23
VLAN-ovi dozvoljeni preko sabirne veze.....	24
VLAN Trunking Protocol (VTP)	25
VTP domeni.....	25
VTP režimi	25
VTP orezivanje (VTP Pruning).....	26
Podešavanje VTP.....	26
Spanning Tree Protocol.....	28
Agregiranje veza komutatora.....	31
EtherChannels	31
MeđuvLAN rutiranje (InterVLAN Routing)	34
InterVLAN rutiranje pomoću Multilayer Switch-eva	34
Layer 3 SVI.....	35
Layer 3 Redundancy	36
Hot Standby Router Protocol (HSRP)	37
Podešavanje HSRP	37
Gateway Load Balancing Protocol (GLBP)	39
Obezbeđivanje univerzitetske mreže	41
Plavljenje MAC adresama - MAC Address Flooding	42
Obezbeđivanje porta (Port Security).....	42
Pristupne liste.....	44
Port access control list (PACL).....	44
Router access control list (RACL).....	45
Standardne pristupne liste.....	45
Proširene pristupne liste.....	45
Imenovane pristupne liste.....	46
VLAN access control list (VACL).....	46

Dodatne napomene pri pisanju pristupnih lista.....	48
Napadi na VLAN	49
Imitiranje Switch-a – Switch Spoofing	49
Ublažavanje napada.....	50
DHCP osluškivanje	50
Zaštita IP izvora.....	51
Dinamička ARP provera.....	52
Obavezne mere zaštite.....	53
Zaključak.....	55
Literatura.....	56
Prilozi.....	57

Sažetak

Ovaj dokument opisuje preporučeni način projektovanja univerzitetske mreže, i uključuje opis topologije, protokola rutiranja, načina podešavanja i druge stvari vezane za projektovanje veoma dostupne i pouzdane univerzitetske mreže. Korišćeni su Cisco uređaji i Cisco patentirani protokoli naspram standardnih gde god je to bilo moguće. Mreža je projektovana prema *Enterprise Composite Network Model*-u sa ugrađenom redundancošću u svakom delu radi postizanja velike dostupnosti. Mreža je veoma skalabilna i lako je ugraditi i dodati nove funkcionalnosti (VoIP, bežičnu mrežu i sl).

This document presents recommended designs for the campus network, and includes descriptions of topology, routing protocols, configuration guidelines, and other considerations relevant to the design of highly available and reliable campus networks. Cisco devices and Cisco proprietary protocols were used where ever it was possible. The network was designed according to *Enterprise Composite Network Model* with maximum redundancy for high availability. The network is very scalable and it is easy to implement new functionalities (VoIP, wireless etc).

Uvod

Arhitektura velike računarske mreže

Model hijerarhijske računarske mreže

Cisco je godinama koristio troslojni hijerarhijski model računarske mreže. Ovaj stariji oblik računarskih mreža je predstavljao sliku o tome kako treba da izgleda pouzdana računarska mreža, ali je bio uglavnom konceptualan jer nije pružao nikakve smernice.

Na slici 1 je prototip hijerarhijske računarske mreže. *Layer3 switch* (komutator 3. sloja) se koristi za svaku zgradu univerzitetskog kompleksa i povezuje *access switch-eve* (komutatore pristupa) koji se nalaze na spratovima zgrada. Komutatori jezgra povezuju različite zgrade i različite blokove mreže.

Pristupni uređaji su komutatori 2. sloja i biraju se prema potrebnom broju portova. Pristupni komutatori se koriste za povezivanje krajnjih korisnika sistema u računarsku mrežu i za dodeljivanje virtualnih LAN mreža (VLAN).

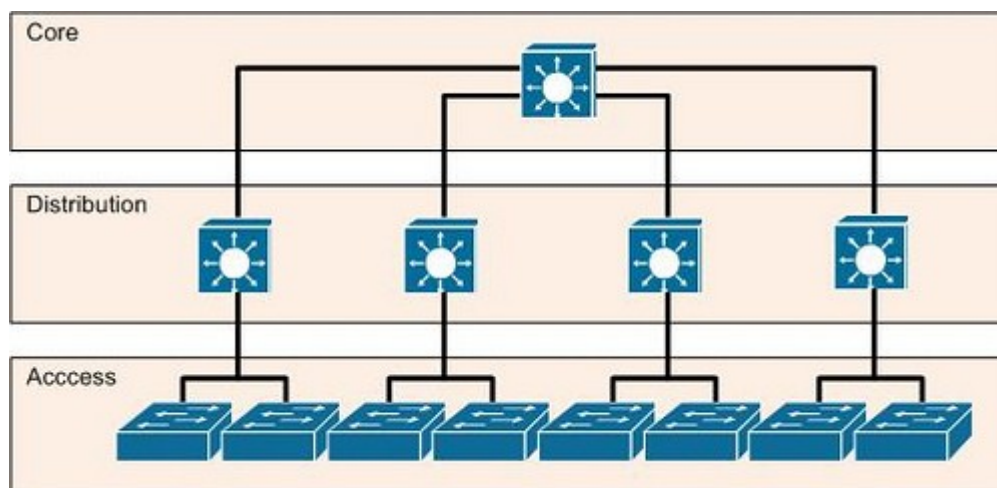
Distribicioni uređaji su komutatori 3. sloja i koriste se kao posrednici koji usmeravaju saobraćaj između VLAN mreža i pomoću kojih se primenjuju ograničenja (polise) koje se odnose na mrežni saobraćaj, npr. odabir putanja, firewall, QoS, ACL.

Uređaji jezgra (*core/backbone*) obezbeđuju veze velikih brzina između distribucionih uređaja.

Distribicioni sloj je mesto odakle se uspešno upravlja računarskom mrežom. Postavljanje polise na pristupnim uređajima bi povećalo složenost i troškove tih uređaja i usporilo bi njihov rad, i bilo bi veoma teško upravljati velikim brojem uređaja. Postavljanje polise na sloju jezgra bi usporilo uređaje čija je osnovna namena brzo usmeravanje mržnog saobraćaja.

Ovaj model je dobra polazna tačka, ali nije mogao uspešno da reši osnovne probleme, kao što su:

- gde postaviti redundantne uređaje
- gde uklopiti bežične uređaje
- gde ugraditi internet pristup i kako ga kontrolisati
- gde dozvoliti udaljeni pristup, kao što je dial-up i VPN



Slika 1: Troslojeni model hijerarhijske mreže

Model složene računarske mreže

Noviji Cisco model je znatno složeniji i teži da ispravi propuste hijerarhijskog modela time što izričito propisuje kako i gde treba da se postave određene mrežne opcije.

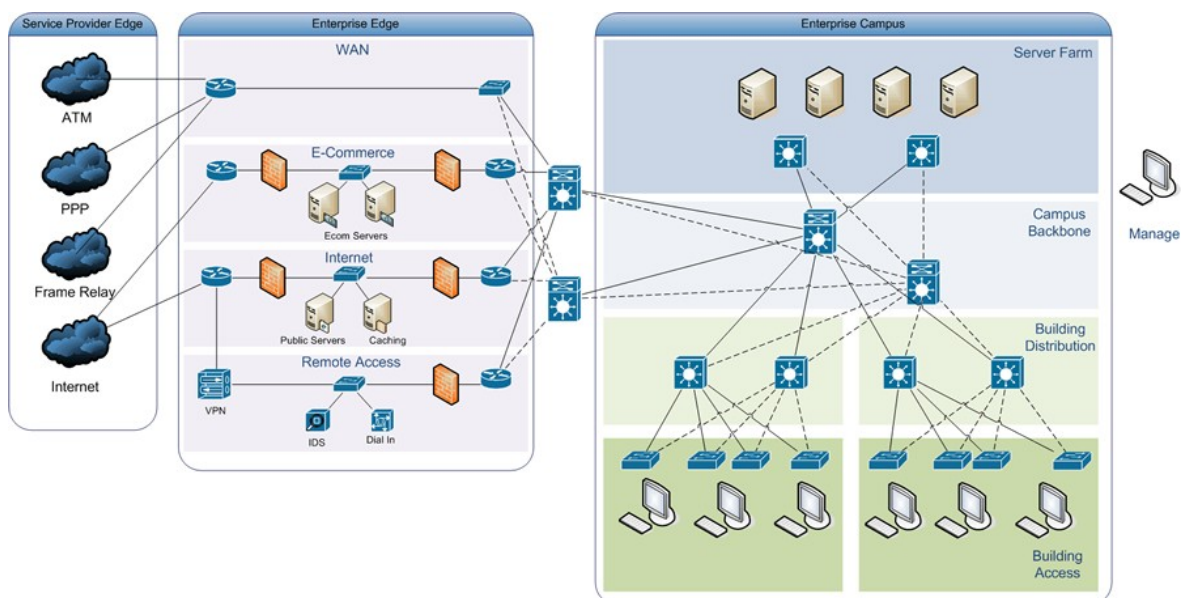
Univerzitetska računarska mreža se može logički projektovati, koristeći modularni pristup. Svaki sloj modela se može podeliti u osnovne funkcionalne jedinice. Veličina tih jedinica (modula) se može pravilno odrediti i potom povezati, vodeći računa o budućoj skalabilnosti i proširivosti mreže.

Model složene računarske mreže se može podeliti u sledeće osnovne delove:

- **Komutacijski blok** (*switch block*) – komutatori sloja pristupa zajedno sa komutatorima distribucionog sloja
- **Blok jezgra** (*core block*) – glavna računarska mreža

Ostali moduli koji ne čine srž mreže, a mogu se po potrebi dodati su:

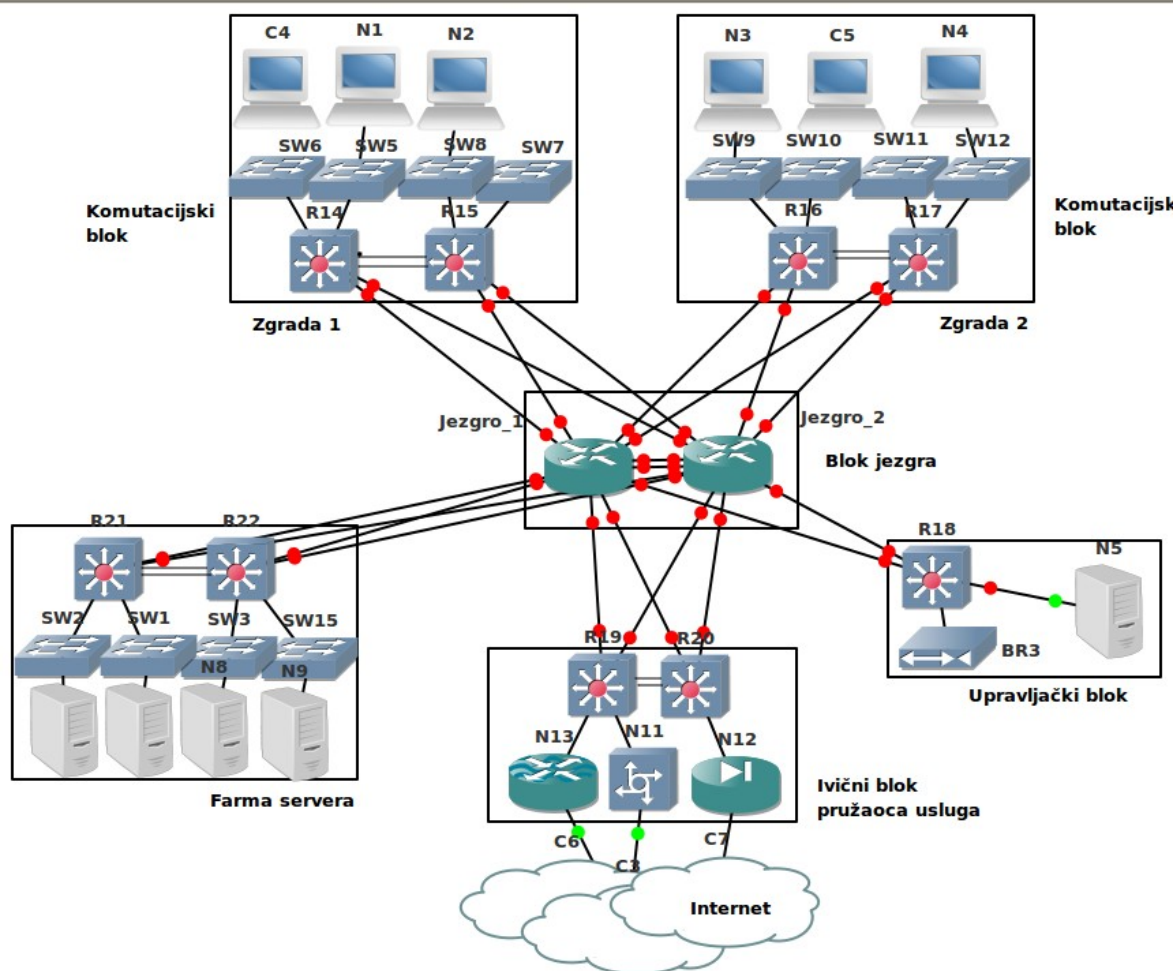
- **Blok farme servera** (*Server farm block*) – Grupa servera zajedno sa njihovim komutatorima sloja pristupa distribucije
- **Upravljački blok** (*Management block*) – Uređaji za upravljanje računarskom mrežom zajedno sa njihovim komutatorima sloja pristupa distribucije
- **Ivični blok velike mreže** (*Enterprise edge block*) – deo mreže koji je u kontaktu sa javnim mrežama (internetom)
- **Ivični blok provajdera usluga** (*Service provider edge block*) – Usluge preko kojih ivični blok mreže uspostavlja vezu sa javnim mrežama



Slika 2: Model složene računarske mreže

Na slici 2 je prikazana osnovna struktura velike mreže. Svaki blok je povezan sa blokom jezgra.

Slika 3: Model univerzitetske mreže korišćen u projektu.



Slika 3: Model univerzitetske mreže

Model univerzitetske mreže

Model univerzitetske mreže je urađen prema *Enterprise Composite Network Model-u*.

Krajnji korisnici mreže se mogu podeliti u dve velike grupe: zaposlene i studente.

Studenti su neprivilegovana grupa, imaju pristup samo internetu (i to *www*) i određenom *file serveru* radi preuzimanja predavanja. Zaposleni imaju pristup različitim delovima mreže u zavisnosti od njihovih ovlašćenja i radnog mesta. Radi lakšeg rukovanja korisnicima, svi su podeljeni u VLANove. Korisnici su povezani preko *Layer 2 switch*-eva koji spadaju u pristupni deo mreže (*access layer*). Svaki korisnik je priključen preko jednog porta i tako dobija namenski deo opsega. Korisnici se priključuju Ethernet ili FastEthernet vezom.

Svaki *switch* pristupnog sloja je povezan sa uređajima na sloju distribucije. Ovde se koriste ruteri ili *Layer 3 switch*-evi radi obezbeđivanja rutiranja, QoS, ACL i sl. VLAN i STP se ne prostiru dalje od ovog sloja. Veza između pristupnog i distribucionog sloja treba biti minimum FastEthernet ili GigabitEthernet.

Više uređaja distribucije se povezuju u uređaje jezgra preko GigabitEthernet ili 10 GigabitEthernet veze. Ovde je najpogodnije koristiti ruterte ili višeslojne *switch*-eve.

Ne bi li mreža bila otporna na otkaze (*fault tolerant*) i uvek dostupna (*high availability*), redundantnet veze i uređaji se koriste na pristupnom i distribucionom sloju. Rezervne veze nisu isključene, već se koriste za balansiranje mrežnog saobraćaja.

Farma servera se sastoji od aplikacionih, *web*, *mail*, *file* i drugih servera koje koriste različiti korisnici. Ukoliko se nekima pristupa preko interneta, moraju biti smešteni u DMZ i primeniti posebne vrste ograničenja. Serveri su povezani preko distribucionog sloja na mrežu, jer se tako najlakše omogućava skalabilnot. Radi veće dostupnosti (*high availability*) preporučljivo je svaki server povezati duplom vezom sa mrežom (*dual-homing*).

Aplikacije za upravljanje i nadgledanje računarskom mrežom su grupisane u jedan komutacijski blok. One namerno nisu deo bloka farme servera, jer njegove resurse ne koriste većina korisnika, već samo IT administratori. I ovde je dostupnost veoma bitna, te je rezervna veza i dupli *switch* poželjno.

Uspostavljanje veze sa provajderom usluga (*ISP*) radi pristupa spoljašnjim resursima (internetom) se obavlja sa jednog mesta preko nezavisnog komutacijskog bloka i to se naziva ivice računarske mreže (*Service provider edge block*). Usluge koje spadaju u ovu kategoriju su: pristup internetu, udaljeni pristup (*remote access*) i VPN, elektronska prodaja, WAN access, telefonske usluge (POTS).

Simulacija je urađena u programu GNS3 verzija 0.7 koristeći dva *image-a* rutera, c2691-advipservicesk9-mz.124-15.T6.bin i c3725-adventerprisek9-mz.124-15.T8.bin.

Internet protokol

IP (internet protokol) (*Internet Protocol*) je protokol trećeg sloja OSI referentnog modela (sloja mreže). Sadrži informacije o adresiranju, čime se postiže da svaki mrežni uređaj (računar, server, radna stanica, interfejs rutera) koji je povezan na internet ima jedinstvenu adresu i može se lako identifikovati u celoj internet mreži, a isto tako sadrži kontrolne informacije koje omogućuju paketima da budu prosleđeni (rutirani) na osnovu poznatih IP adresa. Ovaj protokol je dokumentovan u RFC 791 i predstavlja sa TCP protokolom jezgro internet protokola, TCP/IP stek protokola (*Transmission Control Protocol/Internet Protocol*).

IP ne zahteva prethodno upostavljanje veze u trenutku slanja podatka, već računar koji šalje podatke pokušava sve dok ne prosledi poruku - *best effort* model. Prenos podataka je relativno nepouzdan, što znači da nema gotovo nikave garancije da će poslati paket zaista i doći do odredišta nakon što je poslat. Sam paket u procesu prenosa se može promeniti, zbog različitih osnovnih prenosnih pravaca, može se dogoditi da segmenti ne stižu po redosledu, mogu se duplirati ili potpuno izgubiti tokom prenosa. Ukoliko aplikacija zahteva pouzdanost, koriste se mehanizmi TCP protokla u sloju iznad samog IP protokola. TCP protokol je zadužen i za definisanje redosleda paketa koji stižu (sekvence).

S obzirom da je sam koncept IP protokola oslobođen mehanizama koji osiguravaju pouzdanost, sam proces usmeravanja (rutiranja) paketa unutar mreže je relativno brz i jednostavan. Skrenula bih pažnju na razliku između pojmova *rutirani protokol* i *protokol rutiranja*. Protokoli rutiranja (*routing protocols*) služe za saznavanje topologije mreže (RIP, BGP...), a rutirani protokoli (*routed protocols*) su zapravo podaci koji se šalju preko mreže u određenom obliku (IP). IP je danas najkorišćeniji protokol 3. sloja OSI modela. IPv6 je njegov naslednik, a IPX i AppleTalk su se koristili kratko vreme.

Za adresiranje računara i uređaja unutrašnje mreže korišćen je opseg 192.168.0.0/16. IP adrese ne treba dodeljivati nasumično, već planski. Najveća prednost toga je sumiranje koje se može primeniti. Sumiranjem se smanjuje broj putanja koje ruter pamti, a time i CPU i memorija koju koristi. Pretraživanje tabele je lakše, broj objava manji, a konvergencija brža.

Studenti pristupaju mreži preko računara koji se nalaze u dve sale. Svaka sala se nalazi u posebnom VLAN-u, a IP adrese se dodelju dinamički.

Za studente je predviđen opseg 192.168.10.0/24 podeljen u dve podmreže. Studenti se nalaze u *switch block 1* (komutacijskom bloku 1) koji je sumiran u tabeli rutiranja u 192.168.10.0/24.

	Sala 1	Sala 2
Mreža	192.168.10.0/25	192.168.10.128/25
IP računara	192.168.10.1-126	192.168.10.129-253
Opšta adresa	192.168.10.127	192.168.10.254
Vlan ID	10 – SALA_1	11 – SALA_2

Zaposleni su svrstani u više grupa prema poslu kojim se bave. Svi IP su vezani za MAC adresu radi povećanja bezbednosti. Koriste opseg 192.168.20.0/24 podeljen u 5 podmreža. Poslednji opseg 192.168.20.224/27 nije dodeljen i ostavljen je za novu grupu. Zaposleni se nalaze u *switch block 2* (komutacijskom bloku 2) koji je sumiran u tabeli rutiranja u 192.168.20.0/24.

	Profesori	Stud. Služ.	Admin.	IT
Mreža	192.168.20.0/25	192.168.20.128/27	192.168.20.160/27	192.168.20.192/27
IP računara	192.168.20.1-126	192.168.20.129-158	192.168.20.161-190	192.168.20.193-222
Opšta adresa	192.168.20.127	192.168.20.159	192.168.20.191	192.168.20.223
Vlan ID	20 – PROF	21 – STUDSL	22 - ADMIN	23 - IT

Portovi jezgra su smešteni u 192.168.30.0/24, farma servera u 192.168.40.0 i tako redom za svaki blok uređaja radi lakše sumarizacije i skalabilnosti.

Prva komanda koju treba uneti pre dodeljivanja bilo koje IP adrese je ip subnet-zero koja omogućava korićenje prve i poslednje podmreže (npr. 192.168.0.x i 192.168.255.x). Ova komanda je automatski aktivna počev od verzije 12.4.

Protokoli rutiranja

Protokol rutiranja je jedna od prvih stvari na koju se pomisli kad se razmišlja o postavljanju računarske mreže. Protokoli rutiranja ne služe za rutiranje poruka, već služe da ruteri nauče kako izgleda topologija mreže i kako da naprave putanje bez petlji. Zadatak rutera je da prosledi paket od izvorišta do određene adrese uz što manje zadržavanja i odbacivanja paketa. Protokol rutiranja mu mnogo pomaže u tome.

Stariji protokoli za rutiranje (RIP¹, IGRP²) su spori jer periodično šalju kompletne kopije svoje baze i zauzimaju značajan deo propusnog opsega. Savremeni protokoli za rutiranje šalju ažurirane podatke samo kad se stanje promeni, dok pozdravne poruke (*hello messages*) šalju često i pomoću njih se brzo može uočiti promena stanja u mreži.

Unicast Routing Protocols Comparison					
	RIP	EIGRP	OSPF	IS-IS	BGP
Type	Distance Vector	Distance Vector	Link State	Link State	Path Vector
Algorithm	Bellman-Ford	DUAL	Dijkstra	Dijkstra	Path Selection
Admin Distance	120	90/170 (external)/5 (summary)	110	115	20/200 (IBGP)
Standard	RFCs 2080, 2453	Cisco proprietary	RFCs 2328, 5340	ISO 10589, RFC 1142	RFC 4271
Supported Protocols	IPv4, IPv6	IPv4, IPv6, IPX, Appletalk	IPv4, IPv6	IPv4, IPv6, CLNP	IPv4, IPv6
Transport	UDP/520	IP/88	IP/89	Layer 2	TCP/179
Authentication	Plain, MD5	MD5	Plain, MD5, AH (v3)	Plain, MD5	MD5
Multicast Address	224.0.0.9	224.0.0.10	224.0.0.5-6	N/A	N/A

Slika 4: Poređenje protokola rutiranja

1 Routing Internet Protocol

2 Interior Gateway Routing Protocol

Enhanced Interior Gateway Routing Protocol

Enhanced Interior Gateway Routing Protocol (EIGRP) je Cisco-v vlasnički besklasni protokol vektora udaljenosti zasnovan na IGRP i DUAL (*Diffusing Update Algorithm*). Protokol EIGRP brzo konvergira jer, kao i protokol OSPF, šalje odvojene pouzdane poruke, poruke ažuriranja i održavanja veze.

Četiri osnovne komponente protokola EIGRP su:

- **Moduli koji ne zavise od protokola** (*Protocol-independent modules* (PDM)) – EIGRP podržava nezavisno korišćenje nekoliko protokola. Moduli su dodaci (*plugins*) za IP, IPX, i AppleTalk. IPv4 i IPv6 su dva protokola koja se danas najviše koriste.
- **Pouzdan prenos** (*The Reliable Transport Protocol* (RTP)) – EIGRP vodi računa o poslatim porukama i prati odgovore suseda koristeći Cisco-v patentirani RTP.
- **Otkrivanje i oporavljanje suseda** (*Neighbor discovery and maintenance*) – EIGRP koristi pozdravne poruke kako bi brzo otkrio postojanje suseda i da li sused radi.
- **Prošireni algoritam ažuriranja** - (*Diffusing update algorithm* (DUAL)) – DUAL služi za pronalaženje putanja bez petlji (loop free) i za izračunavanje alternativnih putanja bez čekanja na odgovore od suseda.

EIGRP omogućava pozdano ažuriranje tako što svoje pakete šalje preko IP 88. Za komunikaciju se koriste: *hello*, *update*, *ack*, *query* i *reply* poruke. Susedi se otkrivaju slanjem *multicast* poruka na 224.0.0.10. Direktno priključeni ruteri koji imaju isti AS broj i k vrednosti³ se smatraju susedima.

EIGRP pravi i održava 3 tabele:

- **Tabela suseda** (*Neighbor table*) – pravi se na osnovu pozdravnih poruka i služi za periodično obaveštavanje suseda da ruter još uvek radi.
- **Tabela topologije** (*Topology table*) – sadrži topologiju mreže na osnovu koje je izračunata putanja za svako odredište i njene alternative.
- **Tabela rutiranja** (*Routing table*) – odabrane najbolje putanje iz tabele topologije se smeštaju u tabelu rutiranja i koriste.

EIGRP koristi 5 vrsta paketa za komuniciranje:

- **Pozdravna poruka** (*Hello*) – Služe za oglašavanje suseda, periodično se šalju kao znak da sused još uvek radi i na njih se ne šalje potvrda.
- **Ažuriranje** (*Update*) – Služe za objavljivanje putanja. Šalju se kao višesmerne poruke (*multicast*) i na njih se odgovara potvrdom.
- **Upit** (*Query*) – Služe za saznavanje da li postoje alternativne putanje do mreže kada je prethodno utvrđena najbolja putanja postala nevažeća.

³ K vrednosti su standardne i retko ih treba menjati.

- **Odgovor (Reply)** – Jednosmeran (*unicast*) odgovor na upit kojem obaveštava suseda o traženoj alternativnoj putanji ili obaveštenje da nema tu putanju.
- **Potvrдна poruka (Ack)** – Potvrda za prijem ažuriranih posdataka.

EIGRP šalje *pozdravne* poruke kako bi održao vezu sa susedima, a ažurirane informacije šalje samo kada se dogodi promena. Propusni opseg koristi mnogo štedljivije za razliku od starijih protokola.

Update, *query* i *reply* poruke se pouzdano šalju koristeći Ciscov RTP. Poruke su numerisane i susedi na njih odgovaraju jednosmernom potvrđnom porukom (*unicast*) ACK⁴. Ukoliko ruter ne primi potvrđnu poruku od suseda, nastavlja da mu šalje jednosmerne poruke (*unicast*). Posle 16 pokušaja, sused se proglašava nevažećim.

EIGRP metrika i odabir putanje

EIGRP ruter dobija obaveštenja od svakog suseda koja mu govore objavljenu udaljenost (*Advertised Distance* - AD) i predviđenu udaljenost (*Feasible Distance* - FD).

Advertised Distance (AD) je metrika od suseda do te mreže. **Feasible Distance** (FD) je metrika od rutera preko tog suseda do te mreže.

EIGRP koristi složenu metriku koja uzima u obzir propusni opseg, količinu mrežnog saobraćaja, pouzdanost i kašnjenje. Formula glasi:

$$metric = 256(k_1 \times \frac{10^7}{BW_{min}} + \frac{k_2 \times BW_{min}}{256 - load} + k_3 \times \sum delays) (\frac{k_5}{reliability + k_4})$$

K vrednosti su konstante njihove podrazumevane vrednosti su $k_1 = 1$, $k_2 = 0$, $k_3 = 1$, $k_4 = 0$ i $k_5 = 0$. Pošto je $k_5 = 0$, posledni deo formule se zanemara. BW je najmanje propusni opseg duž putanje. Delay je kašnjenje koje se javlja na svakom interfejsu i njihov zbir se uzima u računicu. Formula se može pojednostaviti na:

$$metric = 256(\frac{10^7}{BW_{min}} + \sum delays)$$

Lako je uočiti da je propusni opseg ima najveći uticaj na metriku.

Raspoređivanje opterećenja saobraćaja

EIGRP kao i većina protokola rutiranja automatski ravnomerno raspoređuje saobraćaj preko putanja sa jednakom metrikom. EIGRP je jedinstven po tome što omogućava nejednako deljenje mrežnog saobraćaja. Kod nejednakog deljenja se uzima najbolja predviđena udaljenost (FD)⁵ i množi se sa odstupanjem. Svaka putanja za koju je FD manja od dobijenog proizvoda se koristi prilikom deljenja saobraćaja. Veza od 256 kbps i 384 kbps se tako mogu zajedno koristiti, ali će EIGRP jednu vezu opteretiti sa 60% saobraćaja, a drugu sa 40%.

⁴ acknowledgement

⁵ Feasible distance

Nabitanije odlike EIGRP

- Brza konvergencija
- Podrška za VLSM
- Delimična ažuriranja čuvaju propusni opseg
- Podrška za IP, AppleTalk, and IPX
- Podrška za sve protokole i topologije 2 sloja
- Složena metrika koja omogućava nejednako srazmerno raspoređivanje saobraćaja (*load-balancing*)
- Korišćenje *multicast* (i *unicast* poruka gde je to potrebno) umesto *broadcast*.
- Lako se održava i podešava

Poređenje sa OSPF

Open Shortest Path First (OSPF) je standardizovani besklasni protokol stanja veze (*link state*). OSPF koristi kocept podele autonomnog sistema na zone (*area*) zarad veće skalabilnosti. OSPF verzije 2 je opisan u REC 2328 za IPv4, a OSPF verzije 3 u REC 5340 za IPv6.

U poređenju sa EIGRP, OSPF se složenije podešava i ne podržava nejednako raspoređivanje mrežnog saobraćaja.

U poređenju sa OSPF, EIGRP ne podržava zone (*area*) te nije zgodan za velike mreže. Čekajući suviše na odgovor suseda, ruter može da se „zaglavi u čekanju“ (*stack in active*). EIGRP je Cisco-v patentirani protokol i može se koristiti samo na Ciskovim uređajima.

Podešavanje EIGRP

EIGRP je pokrenut na svim Layer3 *switch*-evima i ruterima u jezgru. IP opsezi su sumirani na izlaznim vezama Layer3 *switch*-eva ka jezgru radi smanjenja tabele rutiranja. Layer3 *switch*-evi su proglašeni *EIGRP stub* radi stabilnijeg rada mreže. Protokol rutiranja na Layer3 *switch*-evima služi za međuVLAN rutiranje. U suprotnom bi taj posao obavljao ruter u jezgru, što nije poželjno.

EIGRP se pokreće jednostavnim komandama:

```
Jezgro_1(config)#router eigrp 1
Jezgro_1(config-router)#network 192.168.10.0
Jezgro_1(config-router)#network 192.168.20.0
Jezgro_1(config-router)#network 192.168.30.0
```

Ovako izgleda tabela rutiranja na ruteru Jezgro_1. EIGRP je prepoznao da je opseg 192.168.10.0 podeljen na dve podmreža, a 192.168.20.0 na četiri. One su sumirane, što je EIGRP ispisao pri kraju tabele. 192.168.30.0 je opseg u kome su smešteni *interface*-i Jezgra_1 prema svim uređajima i koriste masku /30 radi uštede adresnog prostora.

```
Jezgro_1#show ip route
```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

192.168.30.0/30 is subnetted, 14 subnets

D 192.168.30.52 [90/30720] via 192.168.30.17, 00:01:06, FastEthernet1/4
D 192.168.30.56 [90/30720] via 192.168.30.21, 00:01:08, FastEthernet1/5
D 192.168.30.36 [90/30720] via 192.168.30.1, 00:02:01, FastEthernet1/0
C 192.168.30.32 is directly connected, FastEthernet1/6
D 192.168.30.44 [90/30720] via 192.168.30.9, 00:02:33, FastEthernet1/2
D 192.168.30.40 [90/30720] via 192.168.30.5, 00:01:53, FastEthernet1/1
C 192.168.30.20 is directly connected, FastEthernet1/5
C 192.168.30.16 is directly connected, FastEthernet1/4
C 192.168.30.28 is directly connected, FastEthernet1/8
C 192.168.30.24 is directly connected, FastEthernet1/7
C 192.168.30.4 is directly connected, FastEthernet1/1
C 192.168.30.0 is directly connected, FastEthernet1/0
C 192.168.30.12 is directly connected, FastEthernet1/3
C 192.168.30.8 is directly connected, FastEthernet1/2

192.168.10.0/25 is subnetted, 1 subnets

D 192.168.10.128 [90/30720] via 192.168.30.5, 00:01:54, FastEthernet1/1

192.168.40.0/30 is subnetted, 2 subnets

D 192.168.40.0 [90/30720] via 192.168.30.17, 00:01:07, FastEthernet1/4
D 192.168.40.4 [90/30720] via 192.168.30.17, 00:01:07, FastEthernet1/4

192.168.20.0/27 is subnetted, 3 subnets

D 192.168.20.192 [90/30720] via 192.168.30.13, 00:02:23, FastEthernet1/3
D 192.168.20.160 [90/30720] via 192.168.30.13, 00:02:23, FastEthernet1/3
D 192.168.20.128 [90/30720] via 192.168.30.9, 00:02:34, FastEthernet1/2

Jezgro_1#

Jezgro_1#show ip protocols

Routing Protocol is "eigrp 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Default networks flagged in outgoing updates

Default networks accepted from incoming updates

EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

EIGRP maximum hopcount 100

EIGRP maximum metric variance 1

Redistributing: eigrp 1

EIGRP NSF-aware route hold timer is 240s

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

192.168.10.0

192.168.20.0

192.168.30.0

192.168.40.0

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

192.168.30.21	90	00:01:46
---------------	----	----------

192.168.30.17	90	00:01:44
---------------	----	----------

192.168.30.5	90	00:02:32
--------------	----	----------

192.168.30.1	90	00:02:40
--------------	----	----------

192.168.30.13	90	00:03:02
---------------	----	----------

192.168.30.9	90	00:03:13
--------------	----	----------

Distance: internal 90 external 170

Pravljenje VLAN-ova

VLAN-ovi se koriste da se velika mreža podeli na više logičnih celina. Direktna korist toga je smanjenje neusmerenog (*broadcast*) saobraćaja u svakoj celini.

VLAN⁶ je po definiciji emisioni domen koji je povezan fizičkom ili logičnom podmrežom. Fizička podmreža je grupa uređaja koji dele istu fizičku žicu. Logična podmreža je podmreža je grupa portova komutatora koji pripadaju istom VLAN-u bez obzira na njihovu stvarnu fizičku poziciju.

Postoje 2 vrste VLAN-ova:

- **VLAN od-kraja-do-kraja** – protežu se kroz celu komutiranu računarsku mrežu. Korisnici mogu biti pridruženi VLAN-ovima bez obzira na njihovu fizičku lokaciju. Distribucionni sloj treba da vodi računa o ovim VLAN-ovima.
- **Lokalne VLAN** – Korisnici su pridruženi VLAN-ovima na osnovu fizičke lokacije, kao što je zgrada ili sprat. Ruter opslužuje ove VLANove i oni se najčešće nalaze u sloju pristupa.

VLAN članstvo se dodeljuje statički po portu ili dinamički po MAC-u ili koristeći *VLAN Membership Policy Server* (VMPS).

VLAN-ovi bi trebalo da obuhvataju samo jedanu IP podmrežu. Jedino tako se može primeniti sumariizacija i ostvariti velike uštede. Pristupni portovi treba biti pridruženi samo jednom VLANu i treba da su Fast Ethernet ili brži. Portovi ka distribucionom sloju trebaju biti Gigabit Ethernet ili brži. Portovi sloja jezgra trebaju biti Gigabit Etherchannel ili 10-Gig Ethernet. Izlazne veze (*uplinks*) moraju da izdrže sav saobraćaj krajnjih korisnika.

Pravljenje VLAN-ova u opštem modu podešavanja

VLANovi se moraju napraviti pre nego što se mogu koristiti. Postoje 2 načina za pravljenje istih:

- U opštem načinu podešavanja (*global configuration mode*) se samo identifikuju i imenuju

```
switch(config)#vlan 10
switch(config-vlan)#name SALA_1
```

- Bazni način (*Database Mode*)

```
switch#vlan database
switch(vlan)#vlan 20 name SALA_2
```

6 Virtual local area network

Pridruživanje portova VLAN-ovima

Prilikom statičkog dodeljivanja portova VLAN, prvo se port proglasi pristupnim , a zatim dodeli VLANu.

```
switch(config)#int f0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 12
```

Dinamičko dodeljivanje je slično:

```
switch(config)#int f0/2
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan dynamic
```

Tada se mora uneti i IP adresa VMPS server

```
switch(config-if)#vmps server ip address
```

Provera VLAN podešavanja

Dat je primer *Layer2 switch-a* i podešenih VLAN-ova na njemu. Svaki pristupni port je ručno dodeljen VLAN-u kojem pripada. Svi portovi koji se ne koriste su dodeljeni VLANu koji se ne koristi.

Switch#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa1/0
10 SALA_1	active	Fa1/8, Fa1/9, Fa1/10, Fa1/11 Fa1/12, Fa1/13, Fa1/14
20 SALA_2	active	Fa1/1, Fa1/2, Fa1/3, Fa1/4 Fa1/5, Fa1/6, Fa1/7
100 NEKORISCEN		Fa1/15
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN Trunking

Sabirna veza (*trunk*) je veza koja nosi saobraćaj više od jednog VLAN. Sabirne veze povezuju komutatore i omogućavaju portovima na različitim komutatorima da pripadaju istom VLANu.

Postoje 2 načina obeležavanja VLANova preko sabirnih veza:

- **Inter-Switch Link (ISL)** – Cisco-v patentirani način očuvanja identifikacije izvorišne VLAN mreže. ISL identifikuje okvire na 2. sloju tako što svaki okvir enkapsulira između zaglavlja i kraja. Radi sa svim protokolima i može da prepozna *Cisco Discovery Protocol* (CDP) i *bridge protocol data unit* (BPDU) okvire.
- **802.1Q** – je standardizovan protokol koji ubacuje VLAN oznaku posle MAC polja u okviru.

ISL enkapsulira okvir sa 26 bajtova oznake i 4 bajta CRC⁷. Ako drugi kraj veze nije podešan za ISL, odbaciće okvir zbog prekoračenja MTU⁸ veličine. O tome se mora voditi računa.

Za razliku od ISL, oznaka (*tag*) VLAN kod 802.1q standarda je 4 bajta i okvir će biti normalno obrađen iako 802.1q nije uključen na drugom kraju veze.

Podešavanje sabirne veze (Trunk Link)

Portovi mogu postati sabirni ili statičkom dodelom ili dinamičkim pregovaranjem korišćenjem *Dynamic Trunking Protocol* (DTP).

Port komutatora može biti u jednom od sledećih DTP stanja:

- **Access** – port je pristupni i pripada jednom VLANu
- **Trunk** – port pregovara o sabirnoj vezi sa portom na drugoj strani
- **Non-negotiate** – port je deo sabirne veze i ne pregovara sa drugom stranom o tome
- **Dynamic Desirable** – pregovara sa drugom stranom. Postaje sabirna veza ako je druga strana podešena na *trunk*, *dynamic desirable*, ili *dynamic auto mode*.
- **Dynamic Auto** – pasivno čeka da ga kontaktira druga strana. Postaje sabirna veza ako je druga strana podešena na *trunk* ili *dynamic desirable mode*.

Podešavanje porta u *interface configuration mode*:

```
switch(config-if)#switchport mode {dynamic {auto | desirable} | trunk}
```

U *dynamic mode*, DTP pregovara da li je sabirna veza i način enkapsulacije. Ako se koristi sabirna veza, mora se naznačiti vrsta enkapsulacija:

```
switch(config-if)#switchport trunk encapsulation {isl | dot1q | negotiate}
```

⁷ Cyclic redundancy check

⁸ Maximum transmission unit

VLAN-ovi dozvoljeni preko sabirne veze

Podrazumevano, sabirna veza prenosi sav saobraćaj za sve VLANove. Bezbednije je zadati koji se VLANovi mogu prenositi tom vezom. Time se ujedno i štedi propusni opseg jer se ne presnosi saobraćaj VLANova koji se neće koristiti. Mora se voditi računa da su isti VLANovi zadati sa obe strane veze.

```
switch(config-if)#switchport trunk allowed vlan vlangs
```

Podešavanje sabirne veze između 2 *Layer3 switcha* u bloku:

```
Zgrada1SW_1(config)#interface f1/15
Zgrada1SW_1(config-if)#shutdown
Zgrada1SW_1(config-if)#switchport trunk encapsulation isl
Zgrada1SW_1(config-if)#switchport trunk allowed vlan 1-2,1002-1005,10,20
Zgrada1SW_1(config-if)#switchport mode trunk
Zgrada1SW_1(config-if)#switchport trunk negotiate
Zgrada1SW_1(config-if)#no shutdown
```

```
Zgrada1SW_1>sh int f1/15 switchport
```

Name: Fa1/15

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: isl

Operational Trunking Encapsulation: isl

Negotiation of Trunking: Disabled

Access Mode VLAN: 0 ((Inactive))

Trunking Native Mode VLAN: 20 (SALA_2)

Trunking VLANs Enabled: 1,2,10,20,1002-1005

Trunking VLANs Active: 1,10,20

Protected: false

Priority for untagged frames: 0

Override vlan tag priority: FALSE

Voice VLAN: none

Appliance trust: none

```
Zgrada1SW_1>show int f1/15 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa1/15	on	isl	trunking	20
Port	Vlans allowed on trunk			
Fa1/15	1-2,10,20,1002-1005			
Port	Vlans allowed and active in management domain			
Fa1/15	1,10,20			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa1/15	1,10,20			

VLAN Trunking Protocol (VTP)

Upravljanje velikim brojem komutatora, VLAN mreža i VLAN prenosnicima može biti veoma složeno. Cisco je napravio protokol koji omogućava centralizovano dodavanje, uklanjanje i preimenovanje VLANova.

VTP domeni

VTP je organizovan u upravljačke domene (*managment domain*). Komutator može da pripada samo jednom VTP domenu i informacije deli sa grupom komutatora. Komutatori u različitim VTP domenima ne dele VTP informacije. VTP koristi objave:

- Svi komutatori šalju VTP obaveštenja svakih 5 min ili kada se baza izmeni (kada je VLAN napravljen, izmenjen ili izbrisan).
- VTP objave sadrže broj VTP revizije koji se povećava za 1 prilikom svake izmene.
- Kada komutator dobije VTP objave uporedi broj VTP revizije sa onim u bazi.
 - Ako je novi broj veći, komutator prepravi bazu sa novim VLAN informacijama i obavesti susede.
 - Ako je broj isti, objava se ignoriše.
 - Ako je broj niži, komutator odgovori sa informacijama koje on ima u bazi.

VTP režimi

Switch se može naći u jednom od sledećih režima:

- **Serverski** (*server mode*) – Podrazumevani režim rada. VTP serveri mogu da prave, izmene i obrišu VLANove u svojem domenu. Šalju VTP obaveštenja sa drugim komutatorima i sinhronizuju svoje baze sa njima. Svaki VTP domen mora da ima makar jedan server.
- **Klijentski** (*client mode*) – VTP klijenti ne mogu da prave, menjaju ili brišu VLANove. Oni samo osluškiju objave i u skladu sa njima prave izmene u svojoj bazi. Primeljenja obaveštenja prosleđuju dalje drugim komutatorima.
- **Transparentni** (*transparent mode*) – Transparentni VTP komutatori ne učestvuju u VTP. Oni mogu da prave, menjaju i brišu VLANove, ali te izmene se odnose samo na taj switch. Ne šalju svoja VTP obaveštenja, ali prenose tuđa.

Prilikom uključivanja novog komutatora na mrežu, njegov VTP broj revizije treba postaviti na nulu. Ukoliko se desi da je broj revizije veći od trenutnog, poslaće VTP objavu i izbrisati baze drugih komutatora bez obzira da li se sam nalazi u serverskom ili klijentskom režimu.

Radi veće bezbednosti domena, može se postaviti lozinka i to samo na VTP serverima i klijentima. Zadana lozinka se ne šalje, umesto toga se izračunava MD5 i taj heš (*hash*) se šalje u VTP objavama.

VTP orezivanje (VTP Pruning)

Switch-evi podrazumevano prosleđuju svima neusmerene (*broadcast*), višesmerne (*multicast*) i nepoznato usmerene (*unknown unicast*) okvire. Sabirna veza prenosi saobraćaj svih VLANova. Često se dešava da nemaju svi komutatori podešene portove za sve VLANove i slanje takvih okvira njima bespotrebno zauzima vezu.

VTP orezivanjem (*VTP Pruning*) komutator vodi evidenciju VLAN-ovima koje susedni komutator koristi. Propusni opseg sabirnih veza se štedi time što se ne šalje nepotreban saobraćaj njima.

Postoje 3 verzije VTP. Za korišćenje novijih verzija, svi komutatori u domeni moraju biti osposobljeni za njih. Dovoljno je podesiti jedan server na drugu verziju i informacija će se preneti svim komutatorima.

Podešavanje VTP

Svaki switch, podrazumevano, radi u serverskom VTP režimu za upravljački domen NULL (prazan string), bez lozinke ili bezbednosnog režima. Ukoliko switch preko sabirne veze od drugog switch-a dobije VTP objavu, onda automatski doznaje ime VTP domena, VLAN-ove i broj revizije podešavanja. Nije poželjno ostaviti sve komutatore u serverskom režimu rada.

VTP se podešava u opštem modu za podešavanje (*global config mode*)

```
switch(config)#vtp {server | client | transparent}
```

Podešavanje VTP ime domena:

```
switch(config)#vtp domain MREZA
```

Podešavanje VTP lozinke (svi komutatori moraju koristiti istu lozinku):

```
switch(config)#vtp password password
```

Podešavanje VTP Version 2:

```
switch(config)#vtp version 2
```

Uključivanje orezivanja:

```
switch(config)#vtp pruning
```

Preciziranje koji će VLANovi biti orezani:

```
switch(config-if)#switchport trunk pruning vlan {add | except | none | remove} vlan-list  
[,vlan[,vlan[, ,]]]
```

Podešavanja za *Layer3 switch* u komutacijskom bloku Zgrade 1:

```
Zgrada1SW_1(config)#vtp domain MREZA
```

Changing VTP domain name from NULL to MREZA

```
Zgrada1SW_1(config)#vtp version 2
```

```
Zgrada1SW_1(config)#vtp mode server
```

Device mode already VTP SERVER.

Zgrada1SW_1(config)#do show vtp status

VTP Version : 2

Configuration Revision : 3

Maximum VLANs supported locally : 36

Number of existing VLANs : 7

VTP Operating Mode : Server

VTP Domain Name : MREZA

VTP Pruning Mode : Enabled

VTP V2 Mode : Enabled

VTP Traps Generation : Disabled

MD5 digest : 0x5D 0x51 0x90 0x37 0xE9 0x77 0xC4 0xBC

Configuration last modified by 192.168.10.126 at 3-1-02 03:14:43

Local updater ID is 192.168.10.126 on interface Fa1/0 (first interface found)

Spanning Tree Protocol

U okruženju 3. sloja, protokoli rutiranja se koriste za praćenje redundantnih putanja do odredišta. Rutiranje na 3. sloju omogućava i raspoređivanje mrežnog saobraćaja preko više putanja. Ethernet tj. okruženje 2. sloja ne koristi nikakav protokol za rutiranje i redundante putanje nisu dozvoljene niti poželjne. Ukoliko bi one postojale, stvorile bi se petlje premošćavanja i ubrzo bi došlo beskonačnog umnožavanja saobraćaja i zagušenja (*broadcast storm*).

Spanning Tree je protokol koji sprečava nastajanje petlji tako što pronalazi redundantne veze i isključuje ih dok ne budu bile potrebne. Kada se aktivna veze prekine, saobraćaj će se brzo preusmeriti na redundantnu vezu. Opisan je u dokumentom IEEE 802.1D.

Svaki komutator, na osnovu informacija koje dobija od susednih komutatora, izvršava Spanning Tree algoritam. Algoritam bira referentnu tačku u računarsoj mtrži i izračunava sve redundantne putanje do referentne tačke. Pošto se pronađu sve redundantne putanje, Spanning Tree algoritam bira jednu putanju po kojoj će prosleđivati okvire, dok ostale redundantne putanje onemogućava ili blokira. Računarska mreža se nalazi u stanju kojem ne mogu nastati petlje premošćavanja. Ukoliko aktivni port prestane sa radom ili biva isključen, Spanning Tree algoritam ponovo izračunava topologiju mreže i uključuje jednu od redundantnih veza.

Spanning Tree Protocol (STP) odabira osnovni most (*root bridge*) i putanju bez petlji od njega do svakog komutatora. Putanje se biraju prema sledećim merilima:

1. Lowest root bridge ID (BID)
2. Lowest path cost to the root
3. Lowest sender bridge ID
4. Lowest sender port ID (PID)

STP podrazumevano blokira redundantne veze. Ali ako pokrenemo dva STP možemo iskoristiti obe izlazne veze.

```
Zgrada1SW_1(config)#spanning-tree vlan 10 root primary
% This switch is already the root of VLAN10 spanning tree
VLAN 10 bridge priority set to 8192
VLAN 10 bridge max aging time unchanged at 20
VLAN 10 bridge hello time unchanged at 2
VLAN 10 bridge forward delay unchanged at 15
```

```
Zgrada1SW_1(config)#spanning-tree vlan 20 root secondary
VLAN 20 bridge priority set to 16384
VLAN 20 bridge max aging time unchanged at 20
VLAN 20 bridge hello time unchanged at 2
VLAN 20 bridge forward delay unchanged at 1
```

Zgrada1SW_1#show spanning-tree brief

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 32768

Address c202.026a.0000

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address c202.026a.0000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Designated						
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID

FastEthernet1/1	128.42	128	19	FWD	0	32768 c202.026a.0000	128.42
FastEthernet1/14	128.55	128	19	FWD	0	32768 c202.026a.0000	128.55
FastEthernet1/15	128.56	128	19	FWD	0	32768 c202.026a.0000	128.56

VLAN10

Spanning tree enabled protocol ieee

Root ID Priority 32768

Address c202.026a.0001

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address c202.026a.0001

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Designated						
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID

FastEthernet1/14	128.55	128	19	FWD	0	32768 c202.026a.0001	128.55
FastEthernet1/15	128.56	128	19	FWD	0	32768 c202.026a.0001	128.56

VLAN20

Spanning tree enabled protocol ieee

Root ID Priority 8192

Address c203.026a.0002

Cost 19

Port 55 (FastEthernet1/14)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 16384

Address c202.026a.0002

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface				Designated				
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID		Port ID
FastEthernet1/14	128.55	128	19	FWD	0	8192 c203.026a.0002		128.55
FastEthernet1/15	128.56	128	19	BLK	0	8192 c203.026a.0002		128.56

Agregiranje veza komutatora

EtherChannels

Savremenim računarskim mrežama nikad dosta propusnog opsega. Cisco je osmislio način za skaliranje propusnog opsega veze tako što omogućava agregiranje, odn. grupisanje, paralelnih veza i tu tehnologiju nazvao EtherChannel. Od 2 do 8 veza tipa FastEthernet (FE), Gigabit Ethernet (GE) ili 10-Gigabit Ethernet (10GE) se grupišu u jednu logičku vezu, odn. FastEthernetChannel (FEC), Gigabit EthernetChannel (GEC) ili 10-Gigabit EthernetChannel (10GEC).

Grupisanje veza omogućava lako proširivanje kapaciteta veza između 2 komutatora i to do 1600Mbps sa 8FE, 16Gbps sa 8GE ili 160 Gbps sa 8 10GE.

Opterćenje preko pojedinačnih veza se određuje na osnovu izvorišne i/ili odredišne MAC ili IP adrese ili TCP/UDP porta. To znači da neće sve veze u grupi biti podjednako raspoređene. Podešava se u global configuration mode.:

```
switch(config)#port-channel load-balance type
```

Napomene:

- Veze (*interfaces*) u kanalu (*channel*) ne moraju biti fizički jedna do druge na modulu komutatora.
- Svi portovi moraju biti iste brzine i u dupleksu.
- Nijedan port ne sme biti SPAN⁹.
- IP adresa se dodeljuje logičkoj vezi koja se napravi, ne svakom fizičkom portu.
- Svi grupisani portovi moraju biti u istom VLANu, ili postati sabirna veza. Ako su svi koriste sabirnu vezu, moraju prenositi iste VLANove i koristiti isti režim sabirne veze.
- Podešavanje koja se unesi u *Port Channel interface-u* utiču na sav *EtherChannel*. Podešavanja koja se unesu u fizičkom (*physical interface*) utiču samo na taj port.

Za Layer 3 EtherChannel, potrebno je napraviti logički *interface* i dodeliti mu fizičke *interface*:

```
switch(config)#interface port-channel number  
switch(config-if)#no switchport  
switch(config-if)#ip address address mask
```

Zatim, na svakom portu koju je deo EtherChannel, uneti:

```
switch(config)#interface {number | range interface – interface}  
switch(config-if)#channel-group number mode {auto | desirable | on}
```

9 Switched Port Analyzer

Postavljanjem IP adrese na *Port Channel interface* pravi se *EtherChannel* trećeg sloja. Samo grupisnje *interfaces* pravi Layer 2 *EtherChannel*, i logički *interface* je automatski napravljen.

Ciscov patentirani *Port Aggregation Protocol* (PAgP) dinamički pregovara formiranje kanala. Postoje 3 PAgP režima:

- **On** (uključeno) – Bezuslovni kanal, port je deo grupe bez korišćenja PAgP pregovaranja.
- **Auto** – Pasivno osluškivanje i čekanje na poziv za pregovaranje
- **Desirable** – Aktivno pregovaranje sa drugom stranom veze. Kanal se formira ako je druga strana podešena na *Auto* ili *Desirable*.

Standardna nevlasnička verzija koja radi istu stvar je *Link Aggregation Control Protocol* (LACP) opisana IEEE 802.3ad dokumentom.

```
Jezgro_1(config)#interface port-channel 1
```

```
*Mar 1 00:03:28.827: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down
```

```
Jezgro_1(config)#interface range 1/14 - 15
```

```
Jezgro_1(config-if-range)#channel-group 1 mode on
```

```
Creating a port-channel interface Port-channel1
```

```
Jezgro_1(config-if-range)#
```

```
*Mar 1 00:38:34.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

```
Jezgro_1(config)#port-channel load-balance src-dst-ip
```

Balansiranje saobraća se odnosi na svaku vezu u grupi. Podešava se sledećom komadnom, podrazumevano je *src-dst-ip*.

```
Switch(config)# port-channel load-balance method
```

Drugi načini balansiranja su prema:

dst-ip — odredišnoj IP adresi.

dst-mac — odredišnoj MAC adresi.

src-dst-ip — XOR izvorne i odredišne IP adrese.

src-dst-mac — XOR izvorne i odredišne MAC adrese.

src-ip — izvornoj IP adresi.

src-mac — izvornoj MAC adresi.

```
Zgrada1SW_1#show running-config interface port-channel 1
```

```
Building configuration...
```

```
Current configuration : 31 bytes
```

```
!
```

```
interface Port-channel1
```

```
End
```

```
Zgrada1SW_1#show running-config interface f1/15
```

```
Building configuration...
```

```
Current configuration : 59 bytes
```

```
!
```

```
interface FastEthernet1/15
```

```
channel-group 1 mode on
```

```
End
```

```
Zgrada1SW_1#show int f1/15 etherchannel
```

```
Port state = Up Mstr In-Bndl
```

```
Channel group = 1 Mode = On/FEC Gcchange = 0
```

```
Port-channel = Po1 GC = 0x00010001 Pseudo port-channel = Po1
```

```
Port index = 1
```

```
Age of the port in the current state: 00d:00h:04m:00s
```

```
Zgrada1SW_1#show etherchannel 1 port-channel
```

```
Port-channels in the group:
```

```
-----
```

```
Port-channel: Po1
```

```
-----
```

```
Age of the Port-channel = 00d:00h:04m:52s
```

```
Logical slot/port = 8/0 Number of ports = 2
```

```
GC = 0x00010001 HotStandBy port = null
```

```
Port state = Port-channel Ag-Inuse
```

```
Ports in the Port-channel:
```

```
Index Port EC state
```

```
-----+-----+-----
```

```
0 Fa1/14 on
```

```
1 Fa1/15 on
```

```
Time since last port bundled: 00d:00h:04m:52s Fa1/15
```

MeđuVLAN rutiranje (InterVLAN Routing)

Računarska mreža na drugom sloju može postojati kao VLAN mreža unutar jednog ili više komutatora. VLAN mreže su međusobno izolovane tako da paketi jedne VLAN mreže ne mogu da pređu u drugu VLAN mrežu.

Da bi se paketi razmenjivali između VLAN mreža, mora se koristiti uređaj na trećem sloju. To je tradicionalno bila uloga rutera. Ruter mora imati logičku ili fizičku vezu sa svakom VLAN mrežom tako da između njih može da prosleđuje pakete. Za to se mogu koristiti odvojene fizičke veze ili jedna sabirna veza. To se naziva InterVLAN rutiranje.

Prednosti korišćenja spoljašnjeg rutera za međuVLAN rutiranje su:

- Jednostavno postavljanje
- Usluge trećeg sloja nisu potrebne na *switch-u*
- Ruter prosleđuje pakete između VLANova

Mane su :

- Ruter je jedinstveno mesto otkaza (*single point of failure*)
- Jedine putanje saobraćaja mogu postati zagušene
- Dolazi do kašnjenja jer paket odlazi od *switch-a* da bi se vratio nazad

Drugi način da se postigne međuVLAN rutiranje je korišćenje uređaja koji kombinuje rutiranje i komutiranje: višeslojni komutator (*Multilayer Switch*).

InterVLAN rutiranje pomoću Multilayer Switch-eva

Uobičajeno *switch* prebacuje (*switches*) okvire gledajući zaglavlje drugog sloja, a ruter prosleđuje (*routes*) gledajući treći. Višeslojni *switch* spaja zadatke *switch-a* i rutera u jedan uređaj time što prebacuje (*switches*) saobraćaj kad su izvorište i odredište u istom VLANu i preusmerava (*routes*) saobraćaj kad nisu.

Uloge portova:

- **Virtualni LAN** (*Virtual LAN* (VLAN)) port — Ponaša se kao komutatorski port drugog sloja sa VLAN.
- **Statički VLAN** (*Static VLAN*) — Koristi *switchport* komandu da identifikuje VLAN.
- **Dinamički VLAN** (*Dynamic VLAN*) – Koristi *VLAN Membership Policy Server* (VMPS)
- **Sabirni port** (*Trunk port*) — Koristi više VLANova koje razlikuje prema oznakama.

Layer 3 SVI

Switched Virtual Interface (SVI) je virtualni *interface* trećeg sloja koji se može uključiti za svaki VLAN koji postoji na *Layer 3 switch*-u. SVI VLAN-a obezbeđuje obradu saobraćaja trećeg sloja za sve pakete koji potiču sa portova iz tog VLAN-a. Samo jedan SVI može biti postavljen za jedan VLAN. SVI omogućava:

- podrazumevani mrežni prolaz (*gateway*) za VLAN tako da saobraćaj može da se rutira između VLAN-ova
- dostupnost na trećem sloju (IP) za *switch*
- podršku za protokl rutiranja

SVI je automatski uključen za podrazumevani VLAN (VLAN 1) da bi omogućio upravljanje sa udaljenog mesta. Dodatni SVI moraju biti izručito napravljeni.

```
Zgrada1SW_1(config)#ip routing
Zgrada1SW_1(config)#int vlan 10
Zgrada1SW_1(config-if)#ip add 192.168.10.1 255.255.255.128
Zgrada1SW_1(config-router)#int vlan 20
Zgrada1SW_1(config-if)#ip add 192.168.10.129 255.255.255.128
Zgrada1SW_1(config)#router eigrp 1
Zgrada1SW_1(config-router)#net 192.168.10.0
```

Druga vrsta portova na *switch*-u je rutirani port. To su portovi koji nisu povezani ni sa jednim VLAN-om i obavljaju obradu paketa na trećem sloju. Rutirani port se ponaša kao klasični port rutera, s tim što ne dozvoljava nikakve VLAN podinterfejse.

Na većini switch-eva portovi podrazumevano rade u drugom sloju. Rutirani port se postaje zadavanjem no switchport komande.

```
Zgrada1SW_1(config)#int f1/2
Zgrada1SW_1(config-if)#no switchport
Zgrada1SW_1(config-if)# ip address 192.168.30.1 255.255.255.252
Zgrada1SW_1(config-if)#
Zgrada1SW_1(config-if)#router eigrp 1
Zgrada1SW_1(config-router)#net 192.168.30.0
```

Layer 3 Redundancy

ARP je jedan od bitnijih protokola za uspešno i nesmetano funkcionisanje mreže. Služi za saznavanje MAC¹⁰ na osnovu IP adrese. U složenoj računarskoj mreži, dovoljno je paket proslati do najbližeg rutera ili podrazumevanog mrežnog prolaza. Oni su odgovorni za dalju isporuku paketa.

Podrazumevani mrežni prolaz služi kao izlazna tačka za sve pakete koji se šalju dalje od te podmreže i može biti samo jedan. Čak iako postoji više izlaznih tačaka, ne može se uneti *secondary gateway*. Postavljanjem podrazumevanog mrežnog prolaza (*gateway*), on postaje jedinstveno mesto otkaza (*single point of failure*). Ukoliko gateway prestane da radi, paketi se ne mogu isporučiti dalje od lokalne podmreže. Ne postoji način da se dinamički dobije adresa rezervnog mrežnog prolaza.

Proxy Address Resolution Protocol je jedan od načina da krajnji korisnici dinamički pronađu mrežne prolaze (*gateways*), ali nije preporučljiv za mreže od kojih se zahteva velika dostupnost (*highly-available environment*).

Sa Proxy ARP:

- Računari upućuju ARP zhteve u vezi svih odredišta, čak i za udaljeni pristup (*remote*).
- Ruteri šalju svoje MAC adrese kao odgovor.
- Problem: Spor oporavak od otkaza jer je potrebno minut da ARP zahtev zastari.

Umesto da računari sami biraju novi *gateway*, *Layer 3 redundancy protocol* dozvoljava da 2 ili više rutera dele MAC adresu. Ako primarni ruter prstane da radi, rezervni ruter počinje da obarađuje saobraćaj upućen na tu MAC adresu. Ovaj odeljak se odnosi na rutere, ali i *Layer 3 switch*-evi mogu primeniti *Layer 3 redundancy*.

10 Media Access Control

Hot Standby Router Protocol (HSRP)

HSRP je Cisco-v patentirani protokol napravljen da omogući da nekoliko rutera (ili višeslojnih svičeva) imaju jednu IP adresu mrežnog prolaza. RFC¹¹ 2281 detaljnije opisuje protokol HSRP.

HSRP pravi grupu rutera u pripravnosti, od kojih je samo jedan aktivan. Dva ili više uređaja čine virtualni ruter sa izmišljenom MAC adresom i jedinstvenom IP adresom. Računari koriste IP adresu kao podrazumevani mrežni prolaz, a MAC adresu u zaglavlju 2. sloja. Virtualna MAC adresa je 0000.0c07.ACxx, gde je xx HSRP grupa. Dozvoljeno je više grupa (virtualnih rutera).

Jedan od rutera se bira za primarni ili aktivni HSRP ruter, drugi ruter se bira za HSRP ruter u stanju pripravnosti (*standby*), a ostali su u stanju osluškivanja. Ruteri u pravilnim vremenskim razmacima razmenjuju HSRP poruke tako da znaju za postojanje drugih rutera i da li aktivan ruter radi. Prilikom otkaza aktivnog rutera, ruter u stanju pripravnosti počinje da odgovara na poruke poslate na IP i MAC adresu virtualnog rutera. Čitav proces se odvija neprimetno za krajnje korisnike i oni nastavljaju da rade bez prekida.

Aktivni ruter u grupi se bira prema najvišem HSRP prioritetu (podrazumevani je 100). Ukoliko jedan od rutera ima više HSRP prioritet, neće automatski preuzeti ulogu aktivnog rutera. To se postiže zadavanjem *preempt* komande.

Korišćenjem HSRP, korisnici ne smeju nipošto otkriti pravu MAC adresu rutera u grupi. Svi protokoli koji služe toj svrsi moraju biti isključeni. Pokretanjem HSRP na ruteru, automatski se isključuju ICMP preusmeravanja na tom *interface-u*.

HSRP aktivni i ruter u pripravnosti šalju UDP pozdravne poruke na višesmernu (*multicast*) adresu 224.0.0.2 na port 1985.

Podešavanje HSRP

Podešavanje HSRP počinje zadavanjem *standby group-number ip virtual-IP-address* komande u *interface configuration* režimu. Ruteri u istoj HSRP grupi moraju pripadati istoj podmreži, VLANu. Komanda se zadaje na *interface-u* koji povezuje tu podmrežu ili VLAN. Na primer, sledeća komanda postavlja ruter kao deo HSRP grupe 1 sa virtualnom IP adresom 192.168.10.3:

```
Zgrada1SW_1(config)#int vlan 10
Zgrada1SW_1(config-if)#standby 1 ip 192.168.10.3
```

HSRP se može dodatno podesiti sa opcijama: *Priority*, *Preempt*, *Timers*, i *Interface Tracking*.

Ručno postavljanje aktivnog rutera se postiže postavljanjem prioriteta većeg od 100. U slučaju istog prioriteta, bira se onaj sa većom IP adresom.

```
Zgrada1SW_1(config-if)#standby 1 priority 150
```

¹¹ Request for comments

Jednom kad ruter preuzme ulogu aktivnog, zadržaće je i kad se pojavi drugi ruter sa većim prioritetom. Zadavanjem preempt neaktivni ruter će moći da preuzme ulogu aktivnog ako u nekom trenutku njegov prioritet postane veći od prioriteta koji aktivni već ima. Time se ujedno steče kontrola nad putanjom kojom saobraćaj može da krene. Druga komanda govori ruteru da sačeka 90 sekundi prilikom podizanja sistema da se mreža stabilizuje pre nego što pokrene HSRP.

```
Zgrada1SW_1(config-if)#standby 1 preempt
Zgrada1SW_1(config-if)#standby 1 preempt delay minimum 80
```

Podrazumevano HSRP šalje pozdravne poruke na 3 sekunde, a vreme delovanja je 10 sekundi. To znači da će korisnici čekati 10 sekundi pre nego što rezervni ruter preuzme saobraćaj. Vreme reagovanja se može smanjiti, ali to donosi dodatni saobraćaj i opterećenje ruteru, pa se odluka mora doneti pažljivo. Vreme slanja za *hello* i *dead* mora biti isto na svim uređajima u HSRP grupi.

```
Zgrada1SW_1(config-if)#standby 1 timers 2 7
```

HSRP može da prati stanje interfejsa i da na osnovu njih podešava svoj prioritet. Ukoliko Zgrada1SW_1 izgubi vezu sa Jezgro_1, više nije pogodan da bude aktivan ruter. Pošto su ICMP poruke isključene, ne postoji način da obavest Zgrada1SW_2 da treba da preuzme voćstvo. Automatskim snižavanjem ličnog prioriteta, ruter u pripravnosti će postati aktivan.

```
Zgrada1SW_1(config-if)#standby 1 track f1/3 50
Zgrada1SW_1(config-if)#standby 1 track f1/2 60
```

```
Zgrada1SW_1#sh standby vlan 10
Vlan10 - Group 1
State is Init (interface down)
Virtual IP address is 192.168.10.3
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 2 sec, hold time 7 sec
Preemption enabled, delay min 80 secs
Active router is local
Standby router is 192.168.10.4
Priority 150 (configured 150)
Track interface FastEthernet1/2 state Up decrement 60
Track interface FastEthernet1/3 state Up decrement 50
Group name is "hsrp-Vl10-1" (default)
```

```
Zgrada1SW_1#show standby brief
P indicates configured to preempt.
|
Interface  Grp  Pri P State  Active      Standby      Virtual IP
Vl10      1   150 P Active local      unknown      192.168.10.3
```

Gateway Load Balancing Protocol (GLBP)

Ravnomerno distribuiranje mrežnog saobraćaja možete da se postignete samo ako se konfiguriše da više HSRP grupa imaju više adresa virtualnih rutera. Svaka grupa klijenata mora da se pojedinačno podesi za odgovarajući virtualni ruter što može biti veoma naporno i sklono greškama.

Gateway Load Balancing Protocol GLBP je Ciscov protokol napravljen da bi se prevazišla ograničenja postojećih protokola redundantnih rutera. GLBP omogućava istovremenu upotrebu do 4 člana grupe - mrežna prolaza, koristeći maksimalno propusni opseg. I dalje se koristi jedna IP adresa, ali svaki ruter ima svoju virtualnu MAC adresu. Različite virtualne MAC adrese se naizmenično šalju kao odgovor na ARP.

Osobine GLBP:

- Ravnomerno raspoređivanje opterećenja (load sharing) – saobraćaj se raspoređuje među dostupnim ruterima
- Više virtualnih rutera – GLBP podržava do 1024 virtualna rutera (GLBP grupa) na svakom fizičkom interfejsu i do četiri virtualna prosleđivača (*virtual forwarder*).
- Preuzimanje voćstva (preemption) – Rezervni ruteri mogu postati glavni ako im prioritet postane veći u nekom trenutku
- Delotvornija upotreba sredstava – Bilo koji ruter u grupi služi kao rezervni, nijedan ne mora da se izričito proglašava takvim i svi aktivno učestvuju u prenošenju saobraćaja.

Opterećenje između članova može biti raspoređeno na 3 načina:

- ***Weighted load balancing*** – količina saobraćaja usmerena ka rutera zavisi od težine koju ruter oglašava.
- ***Host-dependent load balancing*** – računar šalje saobraćaj uvek preko istog rutera dok god on učestvuje u grupi.
- ***Round-robin load balancing*** – Na ARP zahtev se uvek šalje MAC adresa sledećeg rutera u grupi i tako u kurg.

GLBP ruteri odabiru *Active Virtual Gateway* (AVG). To je jedini ruter koji odgovara na ARP¹² zahteve. On s bira na osnovu najvišeg prioriteta, ili najviše IP adresa u slučaju da je nerešeno.

Ruter koji opslužuje saobraćaj poslat sa računara naziva se *Active Virtual Forwarder* (AVF). GLBP članovi grupe šalje višesmerne poruke (*multicast hellos*) na 3 sekunde preko IP adrese 224.0.0.102 na UDP port 3222. Ako jedan ruter postane nedostupan, sledeći počinje da odgovara na njegovu MAC adresu.

¹² Address resolution protocol

GLBP se podešava slično HSRP:

```
Zgrada2SW_1(config-if)#int vlan 20
Zgrada2SW_1(config-if)#ip add 192.168.20.1 255.255.255.128
Zgrada2SW_1(config-if)#glbp 1 ip 192.168.20.2
Zgrada2SW_1(config-if)#glbp 1 priority 150
Zgrada2SW_1(config-if)#glbp 1 preempt
Zgrada2SW_1(config-if)#glbp 1 timers msec 250 msec 750
```

Podrazumevani prioritet je 100.

Virtual Router Redundancy Protocol (VRRP) je IEEE standard za redundantnost na trećem sloju opisan u dokumentu RFC 2338. Ima slične osobine kao GLBP, izuzev što GLBP dozvoljava raspoređivanje saobraćaja (load-balancing).

Obezbeđivanje univerzitetske mreže

Na pomen obezbeđivanja mreže, najčešće se pomisli na korišćenje *firewall*-a i sprečavanje napada na trećem sloju i iznad. Svi se trude da zaštite mrežu od upada spolja, ostavljajući unutrašnje uređaje uglavnom nezaštićene. Problem je što se nedozvoljeni uređaji mogu lako prikačiti na mrežu i njihov upad može proći potpuno nezapaženo. Uređaji-uljezi mogu biti postavljeni zlonamerno ili od strane zaposlenog koji želi više *switch* portova ili bežični domet i sl. Najčešće se radi o:

- Bežičnim ruterima ili razvodnicima (*hub*)
- pristupni *switch*-evi
- razvodnici

Postoje četiri vrste napada na komutiranu mrežu:

- napadi zasnovani na MAC adresi, kao što je plavljenje MAC adresama (*MAC address flooding*)
- napadi zasnovani na VLANu, kao što je VLAN preskakanje (*VLAN hopping*) i napadi na uređaje u istom VLANu
- napadi obmane (*Spoofing attacks*), kao što je *DHCP spoofing*, *MAC spoofing*, *Address Resolution Protocol (ARP) spoofing*, i napadi na *Spanning Tree*
- Napadi na *switch*, kao što je izmena *Cisco Discovery Protocol (CDP)* poruka, *Telnet* napadi i *Secure Shell (SSH)* napadi

Plavljenje MAC adresama - MAC Address Flooding

Kod poplave MAC adresama, napadač teži da popuni *switch*-ov *Content Addressable Memory* (CAM) tabelu sa neispravnim MAC adresama. U situaciji kada *switch* ne zna koja MAC adresa se nalazi na kojem portu, podrazumevano počinje da šalje sve okvire na sve portove. Negativne posledice ovoga su stvaranje većeg saobraćaja nego što je potrebno i više posla za *switch*. Pošto se sav saobraćaj šalje na svaki port, napadač ima priliku da prisluškuje saobraćaj koji inače ne bi mogao da vidi i to sa svakog portu. Pošto napad prestane, zapisi u CAM tabeli zastare i popune se ispravnim MAC adresama i sve se nastavi da radi uobičajeno. Ovo se izvodi radi priključenja tuđeg saobraćaja ili kao deo *Denial of service* (DoS) napada. Obezbeđivanju porta i autentikacija na portu mogu da umanje MAC napade.

Obezbeđivanje porta (*Port Security*)

Obezbeđivanje porta je opcija na Catalyst switch-evima koja omogućava da samo određene MAC adrese mogu da šalju podatke preko porta. Ove adrese se mogu saznati dinamički ili ih statički uneti ručno.

Obezbeđivanje porta se ne može primeniti na sabirne (*trunk*) portove.

```
Switch(config-if)# switchport port-security ?
aging          Port-security aging commands
mac-address    Secure mac address
maximum        Max secure addresses
violation      Security violation mode
```

```
Switch(config-if)# switchport port-security
Switch(config-if)#^Z
```

Port security nije podrazumevano aktivno, već se mora uključiti na svakom portu zasebno.

```
Switch(config-if)# switchport port-security
```

Podrazumevano je dozvoljena samo jedna MAC adresa, ali se to može proširiti do 1024. Naučene MAC adrese nikad ne zasteravaju u tabeli za razliku od klasičnog načina rada. Ukoliko se koriste VoIP telefoni, vrednost mora biti najmanje 2.

```
Switch(config-if)# switchport port-security maximum 2
```

Ukoliko je broj unetih MAC adresa manji od broja dozvoljenih, *switch* će ostatak adrese zapamtiti dinamički kada se pojave na portu.

```
Switch(config-if)# switchport port-security mac-address mac_address
```

Kada se pojavi paket sa MAC adresom koja nije na listi dozvoljenih, *switch* može da:

- isključi port
- odbije paket sa tom MAC adresom i napravi unos u dnevniku (*log*)
- odbije paket sa tom MAC adresom bez unosa u dnevnik

Switch(config-if)# switchport port-security violation {protect | restrict | shutdown}

Switch# show port-security address
Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age
			(mins)	
1	0004.00d5.285d	SecureDynamic	Fa0/18	-

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024

Switch# **show port-security interface fa0/18**

```
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address     : 0004.00d5.285d
Security Violation Count : 0
```

Vezivanje porta za jednu MAC adresu pruža veliku sigurnost, ali je gotovo nemoguće ručno uneti sve te adrese u velikoj mreži. Za to postoji opcija *Sticky learning*. Prvu dinamički naučenu adresu pretvara u „lepljivu“ tj. smešta je podešavanja *switch*-a.

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

Ovu opciju je zgodno iskoristiti za podešavanje *switch*-eva na kojim se priključeni svi zaposleni.

Pristupne liste

Pristupna lista (ACL) je, u suštini, lista uslova koji kategorizuju pakete i služe za kontrolisanje mrežnog saobraćaja. Najčešća i najjednostavnije upotreba je za filtriranje neželjenih paketa kao deo bezbednosne polise. Mogu se koristiti i za kategorizovanje paketa u redu čekanja ili za QoS usluge, kontrolisanje koja vrsta saobraćaja sme da koristi ISDN vezu, kontrolisanje koje mreže će dinamički protokoli rutiranja oglašavati itd.

Pravila koja važe za sve ACL:

- Paket se upoređuje sa svakom linijom liste počevši od prve, pa sledećom redom.
- Paket se upoređuje dok se ne pronađe pravilo u koje se uklapa. Tada se izvrši to pravilo i ne upoređuje se sa ostatkom liste.
- Na kraju svake liste se nalazi podrazumevano odbijanje (*explicit deny*). Ako paket ne ispunjava uslov bilo koje od linija pristupne liste, on se odbacuje.

Pristupne liste nemaju nikakvog efekta dok se ne primene na interfejs. Saobraćaj na interfejsu ima dva smera, dolazni i odlazni. Posebne pristupne liste se mogu primeiti za oba.

- **Dolazne pristupne liste** (*inbound*) – Paketi dolaznog saobraćaja se filtriraju kroz pristupnu listu pre nego što se proslede na odlazni interfejs. Svaki paket koji je odbijen neće biti rutiran zato što se odbacuje pre nego što proces rutiranja započne.
- **Odlazne pristupne liste** (*outbound*) – Paketi se proslede na odlazni interfejs i filtriraju kroz pristupnu listu pre nego što se smeste u red čekanja za slanje.

Pristupne liste se dele na:

- **RACL** (*Router access control list*) se mogu primeniti na bilo koji rutirani *interface* (SVI ili rutirani port)
- **VACL** (*VLAN access control list*)
- **PACL** (*Port access control list*) se primenjuju na Layer 2 switch port, trunk port ili EtherChannel port

Port access control list (PACL)

PACL se mogu primeniti samo na fizičkom *interface*-u dolaznog smera (*inbound direction on Layer 2 physical interfaces*) na sviču. PACL obezbeđuju kontrolu pristupa za nerutirani saobraćaj ili saobraćaj drugog sloja. Zaštita IP izvora (*IP Source Guard*) koristi informacije sakupljene DHCP osluškivanjem (*DHCP snooping*) da dinamički napravi *port access control list* (PACL) na interfejsu drugog sloja i odbije saobraćaj koji potiče sa IP adresa koje nisu prijavljene u bazi.

Router access control list (RACL)

RACL se mogu primeniti na SVI (*switch virtual interface*) koji su zapravo virtualni interfejsi trećeg sloja za VLANove, na fizičke interfejse trećeg sloja (*physical Layer 3 interfaces*) i na *Layer 3 EtherChannel interfaces*.

RACL se dele na:

- **standardne** – koriste izvorišnu IP adresu za filtriranje
- **proširene** – koriste izvorišnu i odredišnu adresu i opcionalno protokol kao uslov filtriranja

Standardne pristupne liste

Standardne pristupne liste koriste samo izvorišnu IP adresu kao uslov testiranja. One dozvoljavaju ili odbijaju čitav komplet protokola jer ne prave razliku između vrsta saobraćaja, kao što je www, Telnet, UDP i sl. Postavljaju se najbliže moguće odredišnom računaru (tj. portu rutera). Najveća mana prilikom primene standardnih pristupnih lista je što se neželjeni paketi rutiraju i koriste propusni opseg, da bi bili odbačeni tek na odredišnom kraju mreže.

Standardne pristupne liste se označavaju brojevima 1-99 i 1300-1999.

Studenti ne treba da imaju pristup upravljačkom bloku, stoga ćemo zabraniti da njihov saobraćaj uopšte uđu u taj blok. Pristupna lista je primenjena na oba porta koja vode do jezgra na Layer3 switch-u R18 za dolazni saobraćaj.

```
Switch(config)#access-list 2 deny 192.168.0.0 0.0.0.255
Switch(config)#access-list 2 permit any
Switch(config)#int range f0/0 - 1
Switch(config-if)#ip access-group 2 in
Switch(config-if)#end
```

Standardna lista može biti veoma korisna za dozvoljavanje Telnet pristupa ruteru. Umesto mučne primene proširene liste pristupa na svakom portu rutera, dovoljno je odreti spisak adresa koje imaju dozvolu za pristup i primeniti ih direktno na VTY linije.

```
Jezgro_1(config)#access-list 3 permit 192.168.20.192 0.0.0.32
Jezgro_1(config)#access-list 3 deny any
Jezgro_1(config)#line vty 0 4
Jezgro_1(config-if)#access-class 3 in
Jezgro_1(config-if)#end
```

Proširene pristupne liste

Proširene pristupne liste (*Extended ACL*), sem izvorišne i odredišne IP adrese, gledaju i polje protokola u IP zaglavlju i broj porta u TCP zaglavlju. Bezbednosna ograničenja mogu biti detaljnije sprovedena, jer je moguće dozvoliti ili oduzeti pristup specifičnim uslugama (*services*). Podržani protokoli su: Authentication Header Protocol (**ahp**), Enhanced Interior Gateway Routing Protocol (**eigrp**), Encapsulation Security Payload (**esp**), generic routing encapsulation (**gre**), Internet Control Message Protocol (**icmp**), Internet Group Management Protocol (**igmp**), any Interior Protocol (**ip**), IP in IP tunneling (**ipinip**),

KA9Q NOS-compatible IP over IP tunneling (**nos**), Open Shortest Path First routing (**ospf**), Payload Compression Protocol (**pcp**), Protocol Independent Multicast (**pim**), Transmission Control Protocol (**tcp**), i User Datagram Protocol (**udp**).

Proširene pristupne liste se označavaju brojevima 100-199 i 2000-2799.

Studentski saobraćaj ka upravljačkom bloku je najbolje blokirati u distribucionom switch-u bliže izvoru saobraćaja i sprečiti nepotrebno zauzimanje opsega.

```
Switch(config)#access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
Switch(config)#access-list 100 permit ip any any
Switch(config)#int range f0/0 - 1
Switch(config-if)#ip access-group 100 out
Switch(config-if)#end
```

Imenovane pristupne liste

Usložnjavanjem bezbednosnih pollisa i korišćenjem velikog broja pristupnih lista, postaje veoma teško voditi računa o listama kada sve nose brojeve za imena. Cisco dozvoljava imenovanje kako standardnih tako i proširenih pristupnih listi. Njihova funkcionalnost ostalje ista, kao i podešavanja.

Primer proširena pristupne liste bi sada izgledao ovako:

```
Switch(config)#access-list dynamic BlokiraniStudenti
Switch(config-dyn-nacl)#192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
Switch(config-dyn-nacl)#permit any
Switch(config)#int range f0/0 - 1
Switch(config-if)#ip access-group BlokiraniStudenti out
Switch(config-if)#end
```

```
Zgrada1SW_1#show access-lists
Extended IP access list 100
  10 deny ip 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
  20 permit ip any any
```

VLAN access control list (VACL)

RACL utiče samo na pakete koji se razmenjuju između VLAN mreža. VLAN pristupne liste su filteri koji direktno utiču na obradu paketa unutar VLAN mreža.

VACL spiskovi se podešavaju kao VLAN mapa pristupa, u obliku koji nalikuje mapi rute. VLAN mapa pristupa se sastoji od jednog ili više iskaza, a svaki od njih ima ime. Prvo se definiše VACL pomoću sledeće komande:

```
Switch(config)# vlan access-map map-name[sequence-number]
```

Iskazi mape pristupa se obrađuju u nizu, prema rednim rednim brojevima (*sequence-number*). Svaki iskaz sadrži jedan ili više uslova za kojim sledi akcija.

Zatim se identifikuje mrežni saobraćaj koji treba filtrirati i spoji sa pristupnim listama koje se nezavisno prave.

```
Switch(config-access-map)# match ip address {1-199 | 1300-2699 | acl_name}  
Switch(config-access-map)# match ip address ipx address {800-999 | acl_name}  
Switch(config-access-map)# match ip address mac address acl_name
```

Zatim se definiše akcija:

```
Switch(config-access-map)# action forward | drop | redirect
```

VACL može da odbaci paket, prosledi ga ili preusmeri.

Zatim se VACL mora primeniti na VLAN da bi se filtrirao saobraćaj.

```
Switch(config)# vlan filter map_name vlan-list vlan_list
```

VACL spisak se primenjuje globalno na jednu ili više zadatih VLAN mreža, a ne na interfejs VLAN mreže (SVI). Interface VLAN mreže je mesto gde paketi ulaze i izlaze iz VLANa i nema mnogo smisla primenjivati listu na njega. Umesto toga, lista treba da se koristi unutar VLAN mreže, tamo gde nema odlaznog i doalznog mrežnog saobraćaja.

Saobraćaj zaposlenih u studentskoj službi nema potrebe da bude u VLANovi studenata. Blokirani je na sledeći način:

```
Zgrada1SW_1(config)#access-list 1 permit 192.168.20.128 0.0.0.32
```

```
Zgrada1SW_1(config)#vlan access-map BlokiraniStudSluz 5  
Zgrada1SW_1(config-access-map)#match ip address 1  
Zgrada1SW_1(config-access-map)#action drop  
Zgrada1SW_1(config-access-map)#vlan access-map BlokiraniStudSluz 10  
Zgrada1SW_1(config-access-map)#action forward  
Zgrada1SW_1(config)#vlan filter BlokiraniStudSluz vlan_list 10,20
```

```
Zgrada1SW_1# show vlan access-map BlokiraniStudSluz  
Vlan access-map "BlokiraniStudSluz" 1  
  match: ip address 1  
  action: drop
```

Dodatne napomene pri pisanju pristupnih lista

- Samo jedna pristupna lista može da se primeni po protokolu, po interfejsu i po smeru. Znači, kada se kreira IP pristupna lista, interfejs može da ima samo jednu pristupnu listu za dolazni i samo jednu za odlazni saobraćaj.
- Detaljniji i ograničavajući uslovi treba da se nalaze pri vrhu liste.
- Novi unosi u listu se uvek smeštaju na kraju liste. Za preuređivanje redosleda uslova u listi treba koristiti neki tekstualni editor.
- Nemoguće je ukloniti samo jednu liniju iz pristupne liste. Svaki pokušaj bi doveo do brisanja cele liste. Zato treba koristiti neki tekstualni editor.
- Imenovane pristupne liste dozvoljavaju brisanje pojedinačnih linija.
- Svi paketi će biti odbačeni ako ne ispunjavaju nijedan uslov liste osim ako se ona ne završava sa permit any. Svaka lista treba da ima makar jedan permit uslov, jer će u suprotnom sav saobraćaj biti odbijen.
- Pristupna lista mora biti primenjena na interfejs da bi filtrirala saobraćaj.
- Standardne pristupne liste se uvek smeštaju što je bliže moguće odredištu da se ne bi blokirao sav saobraćaj sa izvorišne adrese.
- Proširene pristupne liste se smeštaju što je bliže izvorištu. Pošto one izričito filtriraju saobraćaj po adresama i protokolima, nema potrebe da saobraćaj prolazi kroz čitavu mrežu i zauzima propusni opseg da bi bio odbijen.

Napadi na VLAN

U napade na VLAN spada VLAN hopping (VLAN skokovi), u kojem računar može da pristupi VLANu kojem ne pripada. Ovo se postiže obmanom switcha ili dvostrukom oznakom kod 802.1q.

Imitiranje Switch-a – Switch Spoofing

Switch spoofing predstavlja računar koji pregovara sabirnu vezu između sebe i switch-a. Podrazumevano svičevi dinamički pregovaraju o sabirnoj vezi koristeći *Dynamic Trunking Protocol* (DTP). Ako računar uspe da ostvari sabirnu vezu sa switch-om, dobiće saobraćaj svih VLANova koji su dozvoljeni na sabirnoj vezi. Podrazumevano, svi VLANovi su dozvoljeni na sabirnoj vezi.

Ovo se može ublažiti isključivanjem DTP na svim portovima koji ne treba da postanu sabirna veza., kao što je većina pristupnih portova, koristeći komandu `switchport nonegotiate`. Svaki port koji je pristupni treba podesiti sa `switchport mode access`. Sve ostale portove koji se ne koriste treba isključiti i smestiti ih u VLAN koji se ne koristi. Interfejsi 7 – 10 su smešteni u nekorišćeni VLAN i isključeni:

```
Zgrada1SW_1(config)#interface range f1/7 - 10
Zgrada1SW_1(config-if)#switchport mode access
Zgrada1SW_1(config-if)#switchport access vlan 100
Zgrada1SW_1(config-if)#shutdown
```

Ublažavanje napada

Zlonamerni korisnici ponekada šalju lažne informacije kako bi prevarili *switch*-eve ili druge računare ne bi li njihov računar koristili kao mrežni porlaz. Cilj napadača je da postane „posrednik“, i da navede korisnika da šalje podatke računaru koji se predstavlja kao ruter. Napadač tako može snimati podatke iz paketa koji su mu poslani pre nego što ih prosledi na odredište. Opisana su tri načina za ublažavanje *man-in-the-middle* napada.

DHCP osluškivanje

DHCP server klijentskom PC računaru pruža sve osnovne informacije koje su mu potrebne kako bi radio u računarskoj mreži, a to su IP adresa, maska pod mreže, IP adresa podrazumevanog mrežnog prolaza, DNS adresa itd.

Kod prevare DHCP (*DHCP spoofing*) napadač osluškuje pod mrežu za korisničke upite DHCP serveru. Zatim, korisniku šalje izmenjeni DHCP odgovor sa svojom IP adresom umesto adrese podrazumevanog mrežnog prolaza (*gateway*). Na taj način se napadač umetnuo u putanji (*man in the middle*) i pregledava sve pakete pre nego što ih šalje dalje (izmenjene ili neizmenjene) mrežnom prolazu.

DHCP osluškivanje (*DHCP snooping*) može da ublaži ovaj tip napada. Svi portovi na sviču se podele na one kojima se veruje i one kojima se ne veruje. Ispravni DHCP serveri se nalaze na portovima kojima se veruje, dok se svima drugima ne veruje.

Svič presreće sve DHCP zahteve na portovima kojima se ne veruje pre nego što ih pošalje u VLAN mrežu. Svaki DHCP odgovor koji dolazi sa porta kojem se ne veruje se odbacuje jer dolazi sa lažnog DHCP servera. Taj port se automatski zatvara prevođenjem u stanje *errdisable*.

Sem toga, DHCP osluškivanje, kada klijenti dobiju ispravne DHCP odgovore, prati broj ostvarenih povezivanja. Ta baza sadrži klijentske MAC adrese, IP adrese, vreme trajanja (*lease*) itd.

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10
```

Svim portovima se podrazumevano ne veruje, tako da se DHCP odgovori ne očekuju niti dozvoljavaju. Svim portovi na putanji do DHCP servera se može verovati jer su povezani sa drugim svičevima/ruterima i tu su manje šanse za prevaru.

```
Switch(config)#int f1/16
Switch(config-if)#ip dhcp snooping trust
```

Na portovima kojima se ne veruje se prihvata neograničen broj DHCP zahteva. Taj broj se može smanjiti i ograničiti sledećom komandom:

```
Switch(config-if)# ip dhcp snooping limit rate 10
```

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
10 20 30 40
Insertion of option 82 information is enabled.
Interface      Trusted      Rate limit (pps)
-----
FastEthernet1/1 yes        10
FastEthernet1/2 yes        none
Switch#
```

Zaštita IP izvora

Lažiranje IP adrese je tip napada koji je teško preduhitriti. Računaru je dodeljena IP adresa i od njega se očekuje da tu adresu koristi za mrežni saobraćaj koji šalje.

Kompromitovani računar ne mora da se ponaša po pravilima. Takav računara može koristiti ispravnu IP adresu, a može koristiti i lažne – adrese koje je uzeo drugim računarima ili nasumično ispisati neku. Lažne adrese se često koriste za prikrivanje izvora napada kojim se uskraćuje usluga (DoS - *denial of service*). Ukoliko izvorišna adresa ne postoji, povratni saobraćaj (koji napadaču ni ne treba) neće stići na izvoriste.

Ruteri i uređaji na trećem sloju mogu lako da otkriju lažne izvorišne adrese u paketima koji kroz njih prolaze. Ukoliko se u VLAN 10 koristi podmreža 192.168.10.0, paketi koji dolaze iz VLAN 20 ne smeju nikada da imaju adrese iz pomenute podmreže.

Međutim, lažne IP adrese je teško otkriti kada dolaze iz opsega kojem treba da pripadaju. Naprimjer, kada napadač koristi IP adresu računara iz istog VLANa.

Zaštita IP adrese se postiže korišćenjem DHCP baze podataka i nepromenljivih elemenata IP izvora. Sa uključenim DHCP osluškivanjem, svič saznaje MAC i IP adrese računara koji koriste DHCP, a zatim proverava sledeće:

- IP adresa mora biti jednaka onoj dobijenoj u DHCP odgovoru ili mora biti nepromenljiva. Na osnovu IP adrese koju je doznao, pravi se dinamička ACL i primenjuje na tom portu.
- Izvorna MAC adresa mora biti jednaka MAC adresi zapamćenoj na portu sviča i DHCP osluškivanjem. Za filtriranje mrežnog saobraćaja se koristi zaštita porta.

Ukoliko se adresa razlikuje od unete ili one koju je svič doznao, paket će biti odbacen.

Za korišćenje zaštite IP izvora, mora se koristiti DHCP osluškivanje. Za zaštitu od korišćenja lažnih MAC adresa mora se koristiti zaštita porta.

Zaštita IP adrese se pokreće komandom:

```
Switch(config-if)#ip verify source
```

Za proveru i MAC adrese treba dodati i port-security:

```
Switch(config-if)#ip verify source port-security
```

Dinamička ARP provera

ARP služi za saznavanje nepoznate MAC adrese na osnovu IP adrese radi prosleđivanja paketa na drugom sloju. Računar šalje ARP zahtev sa IP adresom uredišta na koji može odgovoriti računar sa tom IP adresom ili podrazumevani mrežni prolaz koji će dalje proslediti paket gde treba.

Slično DHCP osluškivanu, napadač i ovde osluškuje mrežu za ARP zahtevima i na njih odgovara sa svojom MAC adresom. I ovde se radi o *man-in-the-middle* napadu.

Ovakva vrsta napada se naziva ARP trovanje (*ARP poisoning*) ili ARP osluškivanje (*ARP spoofing*). Za njegovo ublažavanje se koristi dinamička ARP provera (*dynamic ARP inspection* – DAI).

DAI radi slično DHCP osluškivanju. Svi portovi se podele na one kojima se veruje i one kojima se ne veruje.

Kada na portu kojem se ne veruje pristigne ARP odgovor, svič proveraca da li se MAC i IP adresa u odgovoru slažu sa zapisima u bazi. Baza se popunjava statičkim ručno unetim informacijama ili dinamički korišćenjem DHCP osluškivanja.

Neispravne ARP poruke se odbacuju i pravi se unos u dnevnik (*log*).

DAI se pokreće na jednoj ili više klijentskih VLAN:

```
Switch(config)#ip arp inspection vlan 10
```

Svi portovima se podrazumevano ne veruje. Svi portovi koji vode do drugih svičeva se može verovati, jer se pretpostavlja da je i na njima pokrenuta DAI provera.

```
Switch(config)#int f1/16
```

```
Switch(config-if)#ip arp inspection trust
```

Obavezne mere zaštite

- **Korišćenje lozinki** – Lozinke na Cisco uređajima treba zadati sa enable secret komandom. Šifre će biti sačuvane kao heš (*hash*) vrednost u podešavanjima za razliku od komande enable password koja čuva lozinke u čitljivom formatu. Treba imati na umu da je od skora razbijena zaštita koju je Cisco koristio u enable secret komandi i da se programi za to mogu pronaći na internetu. Service password-encryption nalaže ruteru da šifrue sve šifre koje se nalaze u podešavanjima, Challenge Handshake Authentication Protocol (CHAP) šifre i sl.

```
Zgrada1SW_1(config)#enable secret singi
```

```
Zgrada1SW_1(config)#service password-encryption
```

- **Autentifikacija korisnika** - Za autentikaciju korisnika uvek treba koristiti specijalizovane spoljašnje AAA servere, npr RADIUS, Kerberos i sl. Centralizovano upravljanje korisnikima je mnogo skalabilnije rešenje od menjanja podešavanja na velikom broju svičeva i rutera.
- **Korišćenje banera** - Prilikom svakog pristupa sviču, korisnike (i poželjene i nepoželjne) treba upozoriti da se njihove aktivnosti snimaju i mogu biti osnov za krivično gonjenje. Pomoću komande banner motd se zadaje tekst. Nikako ne treba otkrivati dodatne informacije o mreži koje bi mogle biti zloupotrebene.
- **Isključivanje nepotrebnih i nebezbednih usluga** – Na nekim uređajima su podrazumevano uključene usluge koje više nisu bezbedne. Osnovno pravilo podešavanja glasi da treba isključiti sve usluge (*service*), osobine i protokole i uključiti samo one neophodne za rad. Neke od usluga koje treba isključiti su: no service finger, no service pad, no service tcp-small-servers, no service udp-small-servers, no ip bootp server, no ip identd, no ip source-route...
- **Obezbeđivanje konzole** - Najčešće se ruteri/svičevi nalaze u zaključanim oramnim i prostorijama. I pored toga neophodno je postaviti šife za konzolni i telnet pristup.

```
Zgrada1SW_1(config)#line console 0
Zgrada1SW_1(config-line)#pass
Zgrada1SW_1(config-line)#password singi
Zgrada1SW_1(config-line)#line vty 0 4
Zgrada1SW_1(config-line)#password singi
```
- **Pristupne liste** – Za veću sigurnost, moguće je postaviti pristupne liste ACL koje dozvoljavaju pristup samo određenim IP adresama, MAC adresama ili VLANovima. Primer je dat na strani 40.
- **Koristiti SSH** – Telnet je veoma star program koji se koristi za terminalni pristup preko mreže. Podaci koje šalje nisu šifrovani ni na koji način i lako ih je prisluškivati. Umesto njega bi trebalo koristiti SSH kad god je moguće i uvek poslednje verzije podržane.
- **Obezbedite SNMP** – SNMP je protokol kojim se mogu podešavati mrežni uređaji.

Najbolje bi bilo ne koristiti ga jer i on ima sigurnosne propuste. Ukoliko je neophodan, treba koristiti poslednju verziju podržanu.

- **Isključiti nekorišćenje portove** – Svi portovi koji se ne koriste treba isključiti shutdown komandom. To će sprečiti korisnike da se neprimetno priključe na *switch*. Osim toga, sve te portove treba smestiti u izolovani VLAN koji se ne koristi. Sve portove korisnika treba zadati da rade u switchport mode access režimu. Time će se sprečiti eventualnu korisnikov pokušaj postavljanje sabirne veze sa ruterom/svičom.
- **Isključiti CDP** – CDP¹³ objave se šalju svakih 60 sekundi i služe za otkrivanje susednih Cisco uređaja. CDP je koristan za podešavanje Cisco VoIP telefona, ali je jednako koristan i napadačima jer lako mogu sakupiti mnogo korisnih informacija o mreži. CDP treba obavezno isključiti na portovima na kojima su priključeni korisnici dok se portovi koji povezuju sa drugim (Cisco) ruterima smatraju bezbednim. CDP treba isključiti i na portovima koji komuniciraju sa ne-Cisco uređajima. Radi veće sigurnosti poželjno je potpuno isključiti CDP ukoliko ne postoji izričita potreba za njim komandom `No cdp enable`.

13 Cisco Discovery Protocol

Zaključak

Model univerzitetske mreže je urađen prema Cisco-voj preporuci za projektovanje mreža. Zbog ugrađene redundantnosti veza, rutera i svičeva, mreža je veoma dostupna (*high-availability*) i otporna na otkaze (*fault-tolerant*), ali i izuzetno skupa za sprovođenje. Preporučljivo je graditi mrežu na jednostavnijem modelu, i vremenom dodavati rezervne uređaje i veze. Bitno je pravilno postaviti uređaje po slojevima, ne bi li kasnija nadogradnja bila laka. Ovo je šema mreže kojoj treba težiti jer je izuzetno skalabilna i lako se njom upravlja.

Literatura

1. Campus Network for High Availability Design Guide
2. CCNP BSCI Official Exam Certification Guide, Fourth Edition, 2008 Cisco Press
3. CCNP BCMSN Official Exam Certification Guide, Fourth Edition, 2008 Cisco Press
4. CCNA Study Guide, Third Edition, 2005 Sybex
5. BCMSN Student Guide, 2006 Cisco Press
6. BSCI Student Guide, 2006 Cisco Press
7. www.cisco.com
8. www.wikipedia.com
9. http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094cb7.shtml
10. www.gns3.net

Prilozi

Priloženi su konfiguracioni fajlovi za *Layer3switch* u komutacijskom bloku Zgrade 1 i Jezgro_1 iz bloka jezgra. Ostali konfiguracioni fajlovi nisu priloženi jer su relativno slični.

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Zgrada1SW_1
!
boot-start-marker
boot-end-marker
!
enable secret 5!
$1$CdZ5$wV2vDO.OcsbGEIRrkjSyu.
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
!
spanning-tree vlan 20 priority 16384
!
archive
no ip domain lookup
log config
!
hidekeys
multilink bundle-name authenticated
!
!
!
!
```

```

vlan access-map BlokiraniStudSluz 5      !
  match ip address 1                      interface FastEthernet1/1
  action drop                             !
vlan access-map BlokiraniStudSluz 10     interface FastEthernet1/2
  action forward                          description veza sa Jezgro_1
vlan filter BlokiraniStudSluz vlan_list 10,20 no switchport
vlan internal allocation policy ascending ip address 192.168.30.1 255.255.255.252
!                                         ip access-group 100 out
!                                         ip summary-address eigrp 1 192.168.10.0
!                                         255.255.255.0 5
!                                         !
!                                         interface FastEthernet1/3
!                                         description veza sa Jezgro_2
!                                         no switchport
!                                         ip address 192.168.30.37 255.255.255.252
interface Port-channel1                  ip access-group 100 out
  switchport trunk allowed vlan 1,2,10,20,1002-1005 !
  switchport mode trunk                 interface FastEthernet1/4
!                                         !
interface FastEthernet0/0                interface FastEthernet1/5
  no ip address                         !
  shutdown                             interface FastEthernet1/6
  duplex auto                          !
  speed auto                           interface FastEthernet1/7
!                                         !
interface FastEthernet0/1                interface FastEthernet1/8
  no ip address                         !
  shutdown                             interface FastEthernet1/9
  duplex auto                          !
  speed auto                           interface FastEthernet1/10
!                                         !
interface FastEthernet1/0                interface FastEthernet1/11
  no switchport                        !
  no ip address                        interface FastEthernet1/12
```

```

!                               network 192.168.30.0
interface FastEthernet1/13      no auto-summary
!                               eigrp stub connected
interface FastEthernet1/14      !
description veza sa Zgrada1SW_2 ip forward-protocol nd
switchport trunk allowed vlan 1,2,10,20,1002-!
1005                             !
switchport mode trunk          ip http server
channel-group 1 mode on        no ip http secure-server
!                               !
interface FastEthernet1/15      access-list 1 permit 192.168.20.128 0.0.0.32
description veza sa Zgrada1SW_2 access-list 100 deny      ip 192.168.10.0
switchport trunk allowed vlan 1,2,10,20,1002-0.0.0.255 192.168.50.0 0.0.0.255
1005                             access-list 100 permit ip any any
switchport mode trunk          mac-address-table static c202.026a.0000
channel-group 1 mode on        interface FastEthernet1/14 vlan 10
!                               mac-address-table static 0000.0c07.ac01
interface Vlan1                 interface FastEthernet1/14 vlan 10
no ip address                   !
!                               !
interface Vlan10                !
ip address 192.168.10.1 255.255.255.128 !
standby 1 ip 192.168.10.3       !
standby 1 timers 2 7           !
standby 1 priority 150         control-plane
standby 1 preempt delay minimum 80 !
standby 1 track FastEthernet1/2 60 !
standby 1 track FastEthernet1/3 50 !
!                               !
interface Vlan20                !
ip address 192.168.10.129 255.255.255.128 !
!                               !
router eigrp 1                  !
network 192.168.10.0           !

```

```

!                               line vty 0 4
line con 0                     password 7 031752050106
exec-timeout 0 0              login
password 7 05180F012645      !
logging synchronous          !
line aux 0                    end

```

Konfiguracioni fajl za *router* u bloku jezgra Jezgro_1.

```

version 12.4                  !
service timestamps debug datetime msec !
service timestamps log datetime msec  !
no service password-encryption      !
!                                   !
hostname Jezgro_1                 !
!                                   !
boot-start-marker                 !
boot-end-marker                   !
!                                   !
enable                          secret 5!
#8$7dz5$wV2vDO.OcsbGEIRrkjS7u.  !
!                                   !
no aaa new-model                 !
memory-size iomem 5             !
ip cef                          !
!                                   !
!                                   !
!                                   !
!                                   !
no ip domain lookup              archive
ip auth-proxy max-nodata-conns 3 log config
ip admission max-nodata-conns 3  hidekeys
!                                   !
multilink bundle-name authenticated

```

```
! ip address 192.168.30.10 255.255.255.252
!
vlan internal allocation policy ascending
!
! ip address 192.168.30.14 255.255.255.252
!
!
! interface FastEthernet1/3
! description veza sa R17
! ip address 192.168.30.14 255.255.255.252
!
! interface FastEthernet1/4
! description veza sa R21
! ip address 192.168.30.18 255.255.255.252
!
interface Port-channel1
switchport mode trunk
!
! interface FastEthernet1/5
! description veza sa R22
! ip address 192.168.30.22 255.255.255.252
!
! interface FastEthernet1/6
! description veza sa R18
! ip address 192.168.30.34 255.255.255.252
!
! interface FastEthernet1/7
! description veza sa R19
! ip address 192.168.30.26 255.255.255.252
!
! interface FastEthernet1/8
! description veza sa R20
! ip address 192.168.30.30 255.255.255.252
!
! interface FastEthernet1/9
!
! interface FastEthernet1/10
!
! interface FastEthernet1/11
!
! interface FastEthernet1/12
!
! interface FastEthernet0/0
! no ip address
! shutdown
! duplex auto
! speed auto
!
! interface FastEthernet0/1
! no ip address
! shutdown
! duplex auto
! speed auto
!
! interface FastEthernet1/0
! description veza sa R14
! ip address 192.168.30.2 255.255.255.252
!
! interface FastEthernet1/1
! description veza sa R15
! ip address 192.168.30.6 255.255.255.252
!
! interface FastEthernet1/2
! description veza sa R16
```

```

!
interface FastEthernet1/13
!
!
interface FastEthernet1/14
!
description veza sa Jezgro_2
!
channel-group 1 mode on
control-plane
!
!
interface FastEthernet1/15
!
description veza sa Jezgro_2
!
channel-group 1 mode on
!
!
interface Vlan1
!
no ip address
!
!
router eigrp 1
!
network 192.168.10.0
!
network 192.168.20.0
line con 0
network 192.168.30.0
exec-timeout 0 0
network 192.168.40.0
password 7 34780F012645
auto-summary
logging synchronous
!
line aux 0
ip forward-protocol nd
line vty 0 4
!
password 7 731864050111
!
login
!
ip http server
!
no ip http secure-server
!
!
end
!

```