Projekat univerzitetske mreže

Dejan Brdareski

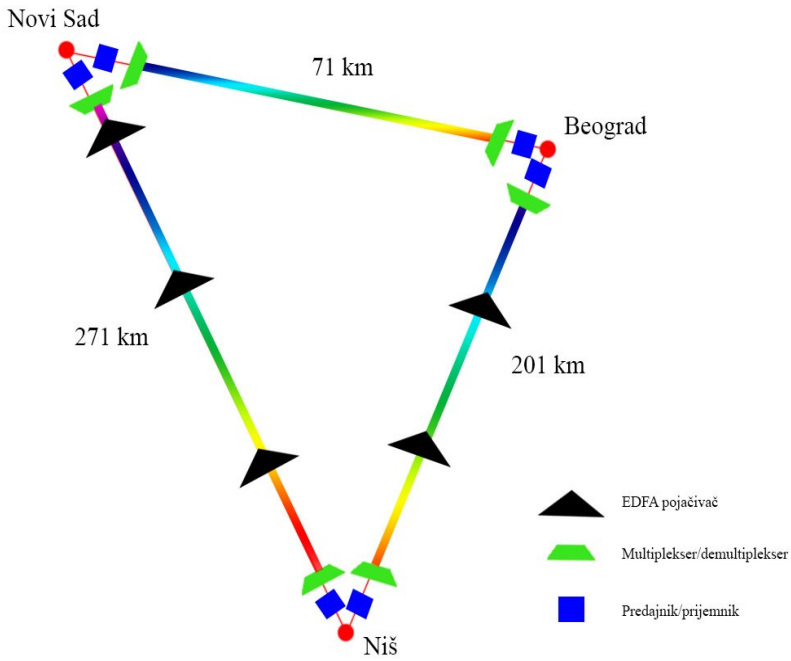
Sadržaj - Ovaj projekat bavi se planiranjem računarske mreže koja spaja sve univerzitete u Srbiji. Topologije lokacija dizajnirane su po hijerarhijskom modelu kompanije Cisco, koji uključuje tri sloja - jezgro mreže (*core* layer), sloj distribucije i sloj pristupa. Razlozi za ovakav dizajn su pouzdanost, skalabilnost, kao i manja cena implementacije. *Core* layer je okosnica mreže, uključuje svičeve i kablove. Ne bavi se rutiranjem unutar LAN-ova, već se bavi brzinama i omogućava pouzdan prenos paketa. Sloj distribucije bavi se pravilnim rutiranjem saobraćaja između podmreža i VLAN-ova unutar mreže. Pristupni sloj povezuje korisničke uređaje i bavi se pravilnom dostavom paketa ka njima.

Ključne reči – Projektovanje mreže, Optičke komunikacije, *Triple Play* mreže

I. Optička mreža

Između velikih lokacija (Beograd, Novi Sad, Niš) projektovan je optički prsten koji čini okosnicu univerzitetske mreže. Predviđene brzine prenosa između ovih lokacija su 10 Gbps, koje se dobijaju multipleksiranjem talasnih dužina iz C- opsega. Talasna dužina koja se koristi za prenos je 1552,52 nm (kanal 31, DWDM C31). U slučaju potrebe za proširenjem propusnog opsega, moguće je uvesti dodatne talasne dužine od kojih bi svaka podržavala 10 Gbps. Razmak između talasnih dužina je 100 Ghz, ili 0,8 nm. S obzirom na udaljenost između lokacija, potrebno je postaviti EDFA pojačivače na pravcu Beograd-Niš i Novi Sad-Niš. Pojačivači se postavljaju na udaljenosti od 80km. Na pravcu Beograd-Niš postavljena su 2 pojačivača, dok su na pravcu Novi Sad-Niš postavljena 3 pojačivača. Predviđene brzine za srednje lokacije su 2.5Gbps, dok su za male lokacije određene brzine od 1Gbps. Svaka lokacija poseduje redundante linkove od 1Gbps u slučaju otkazivanja glavnog linka. Za prenos podataka u kompletnoj optičkoj mreži koriste se *Non-zero dispersion shifted* vlakna oznake G.655. Upravne zgrade i zgrade fakulteta su međusobno povezane optičkim vlaknima. Unutar zgrada, koriste se UTP kablovi kategorije 5. STP kablovi se koriste na velikim lokacijama, tačnije u *data* centru zbog mogućnosti pojave velikog broja smetnji. Topologije su povezane po modelu redundantnih trouglova.

Dejan Brdareski, Računarski fakultet, Knez Mihailova 6, 11000 Beograd, Srbija (e-mail: dbrdareski12@raf.edu.rs)



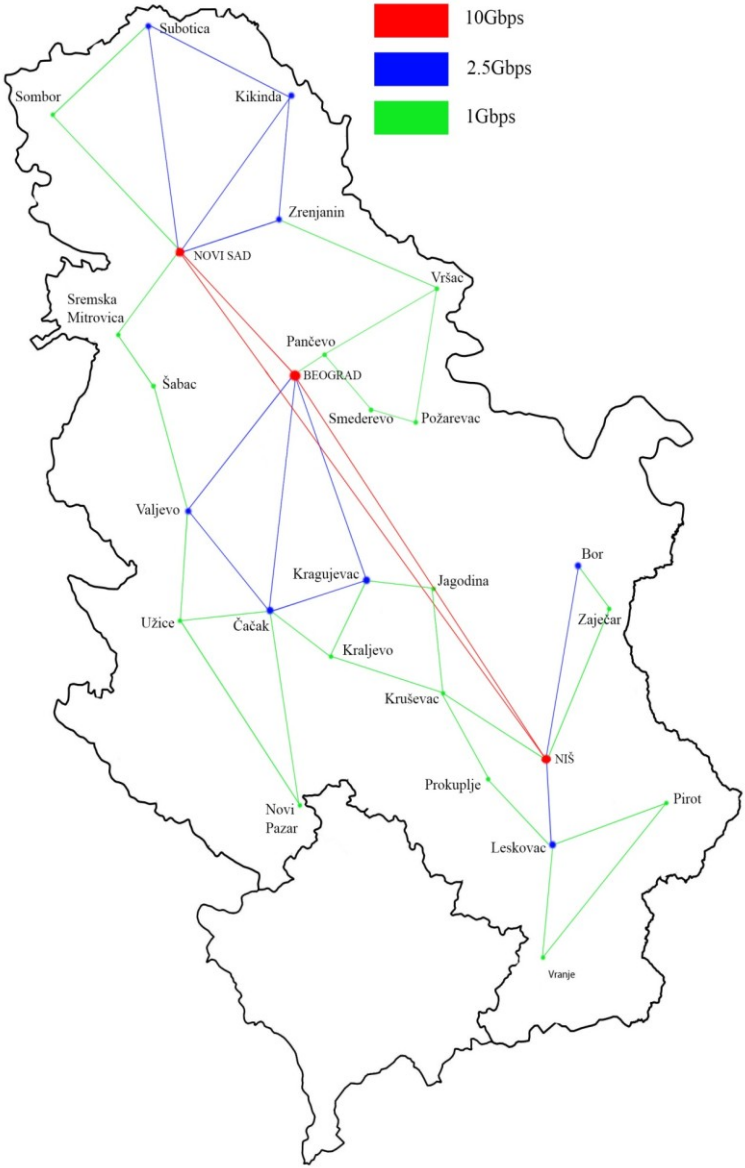
Sl. 1 Optička mreža

A. ADRESNI PROSTOR

Univerzitetska mreža koristi adrese iz opsega 172.16.0.0 sa mrežnom maskom 255.255.255.0 ili /24. To znači da svaka mreža sadrži 254 validne korisničke adrese. Među dodeljene adrese za svaki grad uračunat je i mogući porast broja korisnika od 50%.

B. INTERNET KONEKCIJA I ZAŠTITA

Velike lokacije su direktno povezane sa Internet linkom provajdera, sa po četiri linka brzina 1Gbps, dok se na srednjim lokacijama nalaze linkovi od 1Gbps. Male lokacije pristupaju Internetu preko srednjih lokacija. Za pristup Internetu koristi se NAT, tačnije opseg javnih adresa koje dodeljuje provajder. *Mail*, *web* i FTP serveri poseduju statičke adrese radi lakšeg pristupa sa Interneta. Svi serveri kojima je moguće pristupiti sa Interneta nalaze se u demilitarizovanoj zoni, koja je sa obe strane zaštićena *firewall* uređajima, kao i uređajima za prevenciju upada.



Sl. 2 Prostiranje optičkih linkova

Kako bi se automatizovao proces kontrole mreže i umanjila potreba za administrativnim održavanjem mreže, koriste se BGP ruting polise. Ruting polise su, u stvari, skup ruting filtera i mapa. Ruting filteri kontrolišu koje se rute oglašavaju i primaju, dok ruting mape kontrolišu metriku na tim rutama kako bi se odredilo koje će se rute koristiti, a koje bi trebalo promeniti i prilagoditi. Polise obuhvataju sledeća podešavanja:

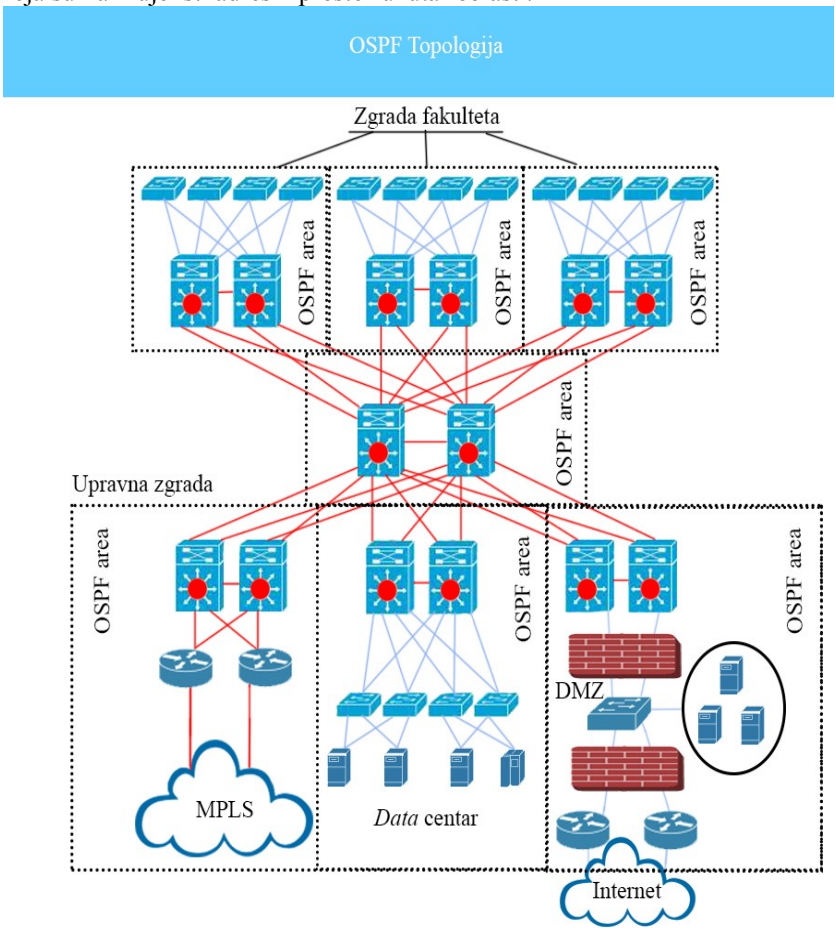
- Rute koje se koriste unutar mreže ne oglašavaju se van mreže, tj. ka Internet provajderu, već samo unutar mreže
- Ograničen je broj unosa u ruting tabele kako bi se izbeglo zagušenje rutera
- Ograničen je broj prefiksa koji se primaju od strane suseda radi smanjenja količine ažurnih BGP informacija
- Koristi se agregacija ruta, kako bi se smanjila količina prefiksa koji se oglašavaju
- *Flap Damping* - ne oglašavaju se rute koje su nestabilne, kako bi se umanjila šansa pojave treperenja i gubitka paketa kod osetljivih aplikacija. Funkcioniše po principu kaznenih bodova. Kada broj kaznenih bodova neke rute dostigne određeni nivo, ruta postaje nedostupna
- *Export filtering* - sprečava lica van mreže da pristupaju internim resursima tako što su konfigurisani filteri BGP oglašavanja ka destinacijama koje ne bi trebalo da su dostupne van mreže. Na primer, filtriraju se IP adrese koje se koriste za interfejse rutera. Takođe se filtriraju adrese uređaja na kojima se koristi softver za nadzor mreže
- Kao mera odbrane od DoS napada, na ruterima je podešen maksimalni broj prefiksa za jednu BGP sesiju, pa ukoliko dođe do prekoračenja tog broja sesija se gasi
- Konfigurisane su tzv. crne rupe (*blackhole routes*). Ukoliko dođe do prijema ogromne količine podataka, sav saobraćaj se preusmerava ka crnim rupama, bez obaveštavanja izvora da saobraćaj nije dostigao destinaciju

II. PROTOKOLI

A. OSPF

Za rutiranje unutar univerzitetske mreže koristi se OSPF protokol. Segmenti mreže su hijererhijski podeljeni u oblasti (*area*) u zavisnosti od geografske ili funkcionalne pripadnosti. Svaka zgrada fakulteta, kao i upravna zgrada je zasebna *area*. *Data* centar je zasebna *area*. Oblasti su podešene na *stub* mod operacije kako bi se umanjio broj neželjenih servisnih informacija. Oblastima su dodeljeni adresni prostori do 50% veći od trenutnih potreba kako bi se obezbedilo dovoljno adresa za budući rast broja korisnika. Na svim lokacijama oblasti sadrže po 2 ABR-a (Area Border

Router). Takav raspored koristi se radi redundanse pošto svaki ABR čuva kopiju baze podataka za svaku oblast sa kojom je povezan. Putanje unutar oblasti su sumarizovane kako bi se umanjio broj zapisa unutar tabela rutiranja, smanjio broj *type* 3 LSA (Sumarizacioni LSA - informacije o procesu sumarizacije ruta) i sačuvali resursi procesora rutera. Pošto svaka oblast sadrži više ABR-ova, na svakom je podešena sumarizacija. Kako bi se izbegle tzv. crne rupe rutiranja, između dva ABR-a postoji po jedna putanja koja sumarizuje isti adresni prostor unutar oblasti.



Sl. 3 OSPF Topologija

Razmena paketa između rutera u svakoj oblasti zaštićena je lozinkom. U korisničkim oblastima, tj. unutar zgrada fakulteta podešena je *Plain Text*

autentikacija koja koristi jednostavne lozinke. U upravnim zgradama i data centrima podešena je MD5 autentikacija koja koristi kriptografske lozinke radi poboljšane bezbednosti.

B. STP

Rapid Spanning Tree protokol koristi se kako bi se izbeglo formiranje petlji unutar mreže. Core svičevi podešeni su kao root bridge i secondary root bridge, koji će preuzeti tu ulogu u slučaju pada primarnog root-a. Implementiran je *LoopGuard* između svičeva sloja distribucije, kao i na portovima svičeva pristupnog sloja ka sloju distribucije. *RootGuard* je postavljen na portovima svičeva sloja distribucije koji su povezani sa pristupnim slojem. *UplinkFast* je implementiran na uplink portovima svičeva pristupnog sloja ka sloju distribucije. *PortFast* sa *BPDUGuard* postavljen je na portovima svičeva sloja pristupa koji su povezani sa krajnjim uređajima kako bi se omogućilo gašenje porta u slučaju prijema BPDU-a na tom interfejsu. *UniDirectional Link Detection* (UDLD) protokol omogućava uređajima da osmatraju fizičku konfiguraciju kablova i otkriju postojanje unidirekcionog linka (Link koji šalje podatke samo u jednom pravcu), te da isključe port koji je pogođen time. Svaki port podešen za UDLD šalje hello pakete susedima. Paketi sadrže informacije o susedima. Ukoliko sused ne primi svoje podatke neko vreme, smatra da je link postao unidirekcionalan. UDLD je podešen na *aggressive* mod operacije na svim interkonekcijama optičkih vlakana, što znači da će, u slučaju otkrivanja unidirekcionalnog linka, isključiti oba kraja konekcije, ne samo onaj na kom je otkriveno postojanje unidirekcionalnog linka. Koristi se *EtherChannel* na linkovima između core svičeva, kao i na linkovima koji povezuju *core* i sloj distribucije. EC se koristi radi omogućavanja redundantnih linkova i prevencije pojavljivanja *single point of failure*-a (Deo sistema koji, ukoliko otkaže, onemogućava funkcionisanje celokupnog sistema), te optimizacije svih *uplink*-ova za prenos saobraćaja i povećanja propusnog opsega. Koristi se u kombinaciji sa *Port Aggregation protocol*-om (PAgP), koji je kontrolni mehanizam za EC. Omogućava automatizovano formiranje redundantne konekcije između svičeva. Obe strane linka podešene su na *desirable* (pita se druga strana da li želi/može), što znači da se EC uspostavlja kada je konfigurisanje završeno. Pošto se u mreži koristi HSRP (*Hot Standby Router Protocol,* koji osigurava redundansu unutar mreže, kao i da će se korisnički saobraćaj momentalno oporaviti nakon neuspešnog prvog skoka), podešeno je da uređajima dodeljuje *default gateway* svič koji je ujedno i *root* STP-a za njihov VLAN. Ovo je veoma bitno zbog toga što, ukoliko HSRP nije usklađen sa STP-om, dolazi do neoptimizovanih putanja saobraćaja što vodi do zagušenja na linkovima.

C. MPLS

Lokacije unutar mreže povezane su pomoću MPLS tehnologije. MPLS podržava VPN-ove zasnovane na L2 i L3, servise kao što je ATM, *Frame Relay*, prenos glasa, kao i da se mogu konvergirati pomoću IP-a. Nudi mogućnost virtuelizacije mreže i uprošćavanje rukovođenja mrežom. Svaka manja virtuelizovana mreža može imati svoje QoS zahteve, korisničke zahteve, kao i bezbednosne zahteve koji su specifični za tu mrežu. Unutar MPLS/VPN arhitekture postoje 3 klase rutera: *provider* (P), *provider edge* (PE), i *customer edge* (CE). P su *core* ruteri, dok PE ruteri povezuju CR rutere sa ostatkom MPLS mreže. PE ruteri su demarkaciona tačka mreže između upravnih zgrada i zgrada fakulteta, i okosnice mreže. Na PE ruterima VRF *instance* (*Virtual routing and forwarding* - tehnologija koja omogućava da postoje višestruke ruting tabele na istom ruteru. Pomoću ovoga, iste IP adrese se mogu koristiti bez konflikata) odvajaju informacije o rutiranju kako bi se omogućilo korišćenje istih adresnih prostora. PE ruteri enkapsuliraju IP pakete pomoću dve nalepnice. P ruteri donose odluke o rutiranju na osnovu nalepnica. CE ruteri ne znaju za postojanje nalepnica i služe kao obični IP ruteri. Svaka VRF instanca sadrži po 2 CE rutera koji su po jednim linkom povezani sa PE ruterom. Iako *Label Distribution Protocol* (LDP) omogućava jednostavno rukovođenje mrežom, s obzirom da se distribucija u velikoj meri obavlja automatizovano, u mreži se koristi *Resource Reservation Protocol* (RSVP). RSVP podržava *Fast Re-Route* tehnologiju, koja je veoma bitna kada je prenos glasa i video zapisa u pitanju. FRR nakon otkrivanja nedostupnog linka ili uređaja omogućava trenutno preusmeravanje saobraćaja preko alternativnih putanja. Pomoću FRR-a mreža zadržava *real-time* performanse za prenos glasa i video zapisa u slučaju kvara u mreži. Upotrebom MPLS-a osigurava se da svaki paket ili podatak stigne na odredište, kao i da je svakom paketu dodeljen potreban prioritet. Koriste se servisne klase (*Classes of Service*, CoS) i prioritetno čekanje kako bi se označilo koji je saobraćaj najbitniji, i da bi se toj vrsti saobraćaja dodelio prioritet u odnosu na druge vrste saobraćaja. Ovo je posebno bitno s obzirom na prenos glasa i video zapisa u univerzitetskoj mreži. QoS/CoS se izvodi pomoću labela, tj. nalepnica koje MPLS dodeljuje saobraćaju, na osnovu kojih se određuje prioritet. Aplikacijama kao što su VoIP i prenos video zapisa dodeljeni su najviši prioriteti unutar mreže. Svi LSP ruteri koji podržavaju prenos video zapisa i glasa podešeni su tako da omogućavaju visoku dostupnost uz FRR i BFD (*Bidirectional Forwarding Detection* - veoma brzo otkrivanje nedostupnog linka ili uređaja). MPLS ima ključnu ulogu u *disaster recovery* planu univerzitetske mreže. Omogućava *data* centrima i ostalim bitnim lokacijama višestruke redundantne konekcije ka mreži, tj. ostalim lokacijama u mreži. Takođe, udaljene lokacije se brzo i lako

mogu ponovo povezati sa backup lokacijama ukoliko je potrebno. MPLS odlikuje mali broj izgubljenih paketa, što znači i brže funkcionisanje velikog broja aplikacija. Upotrebom MPLS-a poboljšava se i iskorišćavanje propusnog opsega. Pošto se različite vrste saobraćaja prenose istim linkom, moguće je da saobraćaj visokog prioriteta "pozajmi" propusni opseg od tokova saobraćaja niskog prioriteta ukoliko je potrebno. U obrnutom slučaju, ukoliko saobraćaj niskog prioriteta zahteva veći propusni opseg od uobičajenog, moguće je iskoristiti deo koji saobraćaj visokog prioriteta ne koristi.

III. E-MAIL

Korisnici proveru pošte vrše preko SSL protokola, kako bi se omogućila potrebna zaštita privatnosti. Tačnije, kompletno rešenje pristupa studentskom portalu, servisima i pošti izvode se preko SSL protokola. Koriste se digitalni sertifikati za enkripciju, bezbedan pristup serveru i razmenu informacija.

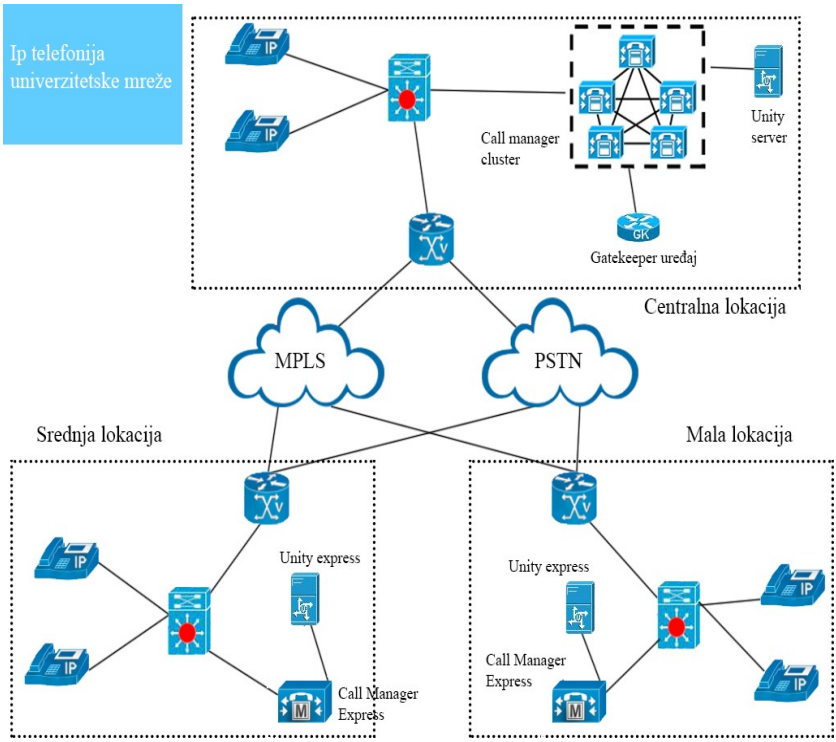
IV. IP TELEFONIJA

Rešenje za IP telefoniju koje se koristi je *Cisco Unified Communications Manager*, objedinjena platforma za kontrolu komunikacija. Nalaze se na velikim lokacijama, tačnije u *data* centrima, odakle pružaju usluge ostalim korisnicima. *Data* centar je prava lokacija za *call manager*, pošto poseduju najbolje uslove i najbezbedniji su u čitavoj mreži. Uređeni su u tzv. *cluster*-e, koji se sastoje iz više Cisco *CallManager* servera. Oni dele iste baze podataka i resurse. *Cluster* opcija omogućava neometano procesiranje poziva unutar mreže, podelu resursa i skalabilnost sistema. Na srednjim i malim lokacijama koriste se *Cisco Unified CallManager Express*, kao i *Cisco Unity Express*, koji pruža uslugu glasovne pošte. PSTN mreža (*Public switched telephone network*) koristi se u slučaju pada mreže IP telefonije, ili u slučaju prekoračenja propusnog opsega. Takođe se koriste i tzv. *Gatekeeper* uređaji, koji grupišu *gateway*-e u logičke zone i omogućavaju pozive između njih. Sprovode mrežni *dial* plan, tj. plan telefonskih brojeva, kao i *Call Admission Control*, koji sprečava zagušenje u mreži. *Gatekeeper* uređaj takođe prevodi E.164 tagove (Tj. brojeve telefona. Ovaj standard definiše generalni format telefonskih brojeva) u IP adrese za korišćenje unutar H.323 telefonske mreže (Standard koji definiše protokole za prenos audio-vizuelnih sesija unutar mreža sa komutacijom paketa).

V. IPTV/VOD

U Beogradu je lociran tzv. *Super Headend* ili *Super Hub Office*, iz kojeg se dalje u mrežu distribuiraju snimci uživo. Na lokaciji se nalaze *real-time*

enkoderi koji se koriste za emitovanje video zapisa, zajedno sa sistemima za distribuciju *on-demand* servisa. U data centrima u Novom Sadu i Nišu nalaze se tzv. *Video Headend Office*, na kojima se nalaze IPTV i VoD serveri. Na ovim lokacijama se nalazi većina video sadržaja koji se emituje on-demand. Kako bi korisnici neometano mogli da koriste ove servise, linkovi ka serverima imaju propusni opseg od 10Gbps.



Sl. 4 IP Telefonija univerzitetske mreže

Definisana su tri tipa IPTV saobraćaja: *broadcast* TV (*real-time*), VoD preuzimanja (*non-realtime*), i *real-time* VoD. *Broadcast* TV se sastoji iz tradicionalne televizije, HDTV, i muzičkih kanala. Popularni VoD sadržaji nalaze se na serverima u VHO i šalju se korisnicima na zahtev. Novi sadržaji se iz SHO šalju ka VHO tokom perioda najmanjeg korišćenja sistema. Prebacivanje ovog sadržaja ne zahteva *real-time* podršku, pa ima minimalni uticaj na funkcionisanje same mreže. Međutim, očekivano je da se jedan deo *real-time* VoD sadržaja šalje korisnicima iz SHO. Za tu vrstu zahteva koristi se *unicast* dostava sadržaja. Kako bi se obezbedio brz oporavak servisa nakon

kvarova u mreži, koristi se FRR tehnologija, koja momentalno uspostavlja rezervnu rutu ukoliko otkrije kvar na primarnom linku.

VI. MULTICAST

Za preno *multicast* saobraćaja koristi se PIM *Source-specific Multicast* protokol. SSM je protokol koji odgovara *one-to-many* modelu operacije. U univerzitetskoj mreži koristi se uglavnom za prenos IPTV sadržaja. SSM je metod dostavljanja multicast paketa, s tim što se korisnicima dostavljaju isključivo paketi koje je korisnik zahtevao. Na taj način se ograničavaju izvori saobraćaja, umanjuje broj zahteva i poboljšava bezbednost same mreže. SSM zahteva od korisnika da precizno označe izvorišnu adresu sa koje žele da preuzmu sadržaj. Korisnici pomoću IGMPv3 protokola šalju zahtev za članstvo u određenim *multicast* grupama (S, G. S predstavlja IP adresu izvora, dok G predstavlja grupnu adresu), umesto (*, G) za članstvo u svim *multicast* grupama. Na taj način se samo zahtevani tokovi saobraćaja dostavljaju korisniku, a ujedno se i sprečavaju DoS napadi. Lažni saobraćaj ne stiže do korisnika i ne konzumira propusni opseg mreže. Za potrebe SSM protokola rezervisan je adresni prostor 232.0.0.0 - 232.255.255.255 (tzv. 232/8).

Pošto deo mreže odgovoran za *multicast* saobraćaj konvergira nakon dela za *unicast* rutiranje, potrebno je ručno podesiti tajmere ruting protokola kako bi se umanjilo vreme konvergencije u *edge* delu mreže (*dead-interval* na 1 sekundu, *hello* interval na 250ms. *Hello* paketi u OSPF protokolu šalju se susedima kako bi se održala veza sa njima. *Hello* interval je vremenski period između slanja dva *hello* paketa. Ukoliko ruter ne primi *hello* pakete od suseda u toku *dead* intervala, proglasiće susedni ruter kao ugašen). Takođe se ne koristi automatsko pregovaranje *trunk* linkova, što može umanjiti vreme konvergencije za nekoliko sekundi, dok su nekorišćeni VLAN-ovi manuelno uklonjeni (*pruned)*. Koristi se i IGMP *Snooping* kako bi se obezbedilo da samo zainteresovani korisnici primaju određeni tok saobraćaja, a ne svi korisnici koji su priključeni na isti svič.

VII. NTP

U Beogradu se takođe nalazi i jedan NTP uređaj pomoću kojeg se usklađuje vreme u celoj mreži.

VIII. OPORAVAK OD NESREĆE (DISASTER RECOVERY)

Replikacija tj. *backup* podataka obavlja se noću od 1h do 3h, kako ne bi došlo do gubitaka podataka u slučaju havarije. *Disaster recovery* lokacija se nalazi u Pančevu. Vrši se replikacija kompletnih sistema, uključujući

operativni sistem, aplikacije, baze podataka, podataka na disku, hardverskih drajvera, profila, podešavanja, registara, individualnih podataka i foldera, i smešta ih u jedinstvene *recovery point*-e kojima se lako rukuje.

IX. VLAN

Interne grupe korisnika su na svakoj lokaciji podeljene u VLAN-ove. Na svim lokacijama, dodeljeni VLAN za potrebe IP telefonije je 110. Takođe, *native* VLAN na svim lokacijama je 5. *Default* vrednost *native* VLAN-a na Cisco uređajima je 1, međutim upotreba tog VLAN-a ne preporučuje se zbog bezbednosti.

Koristi se model lokalnih VLAN-ova. Ovaj model implementacije jednostavniji je za administraciju i održavanje, pošto se stvaraju manji *broadcast* domeni. Na svim lokacijama dodeljene su iste vrednosti VLAN-ovima radi lakšeg snalaženja i konfiguracije. Podešeni su *trunk* linkovi između slojeva pristupa i distribucije. Koristi se 802.1Q standard. VLAN *Trunk Protocol* (VTP) je podešen na *transparent* mod kako bi se umanjile šanse za pojavu grešaka pri izračunavanju, dok je *Dynamic Trunk Protocol* (DTP) isključen, što znači da su svi *trunk* linkovi manuelno podešeni. Na trunk interfejsima su takođe manuelno uklonjeni (*prune*) nekorišćeni VLAN-ovi kako bi se umanjila *broadcast* propagacija.

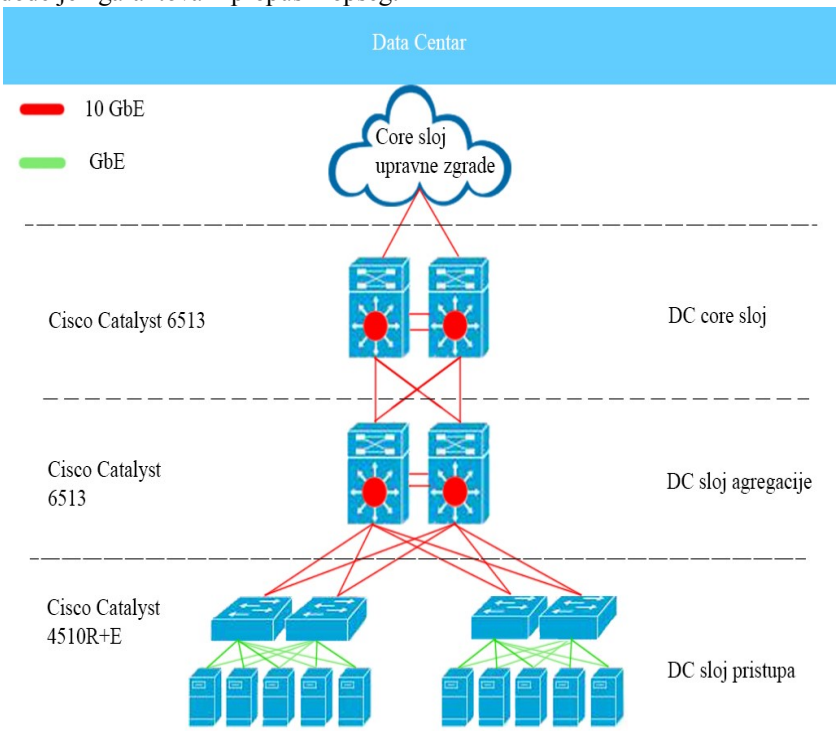
X. CENTAR PODATAKA (DATA CENTAR)

Data centar poseduje svoj *core* sloj iz nekoliko razloga. Uveden je kako bi se obezbedio dovoljan broj 10Gb *Ethernet* portova za povezivanje sloja distribucije i *data* centra. Služi kao *gateway* ka *core* sloju upravnih zgrada. Prisustvo 2 *core* sloja omogućava bolju i precizniju implementaciju bezbednosnih polisa, QoS-a, lakše održavanje i administraciju. DC core koristi OSPF protokol rutiranja. DC sloj agregacije povezuje core sloja sa slojem pristupa. Prikuplja saobraćaj sa sloja pristupa i šalje ga ka DC core sloju. Na ovom sloju se odvija STP procesiranje, *firewall*, kao i *load balancing (*Odabir između putanja sa istom administrativnom distancom*)*, modul za detekciju upada, analizatori mreže i sl. DC sloj pristupa je mesto gde su serveri fizički povezani sa mrežom. U data centru implementiran je *Rapid Spanning Tree protokol*, koji podržava *RootGuard*, *BPDUGuard* i *LoopGuard*, i omogućava veoma brzu konvergenciju.

XI. QOS I FIREWALL

U cilju smanjenja uskih grla unutar mreže, uvedena je redundansa od 4:1 između *core* sloja i sloja distribucije, kao i 20:1 za pristupni sloj. QoS je implementiran po principu *end-to-end* radi efikasnosti. *Queuing*, tj. čekanje je

omogućeno na svakom čvoru za koji postoji šansa da dođe do zakrčenja. *Low-Latency queuing* (LLQ) se koristi za označavanje saobraćaja koji se mora poslati bez kašnjenja i sa minimalnim treperenjem. *DiffServ* arhitektura se koristi za označavanje i deljenje saobraćaja na klase, te određivanje prioriteta za prenos. Saobraćaj je podeljen na četiri klase, a svakoj klasi je dodeljen garantovani propusni opseg:



Sl 5. Topologija Data Centra

- *Realtime* klasa 33% (Prenos glasa i video zapisa)
- *Critical Data* klasa (Aplikacije studentske službe – Indeks i Servis, kao i razmena podataka na studentskom portalu)
- *Best Effort* klasa 25% (Osnovna klasa za sav saobraćaj u mreži. Saobraćaj gubi best effort status jedino mu ako se dodeli prioritet neke druge klase)
- *Scavenger*/*Bulk* klasa 5% (FTP, e-mail, sinhronizacija baza podataka, replikacija podataka, bilo koji servis koji se odvija u pozadini, nije interaktivan i nije osetljiv na promene brzine)

Kako bi se olakšalo rukovanje QoS mehanizmima, koristi se Cisco AutoQos, koji omogućava administratorima jednostavno rukovanje makro programima i podešavanje željenih QoS parametara na određenim interfejsima ili za određene aplikacije.

Implementiran je *firewall* zasnovan na zonama (*Zone based policy firewall*). Bezbednosne polise se odnose na zone, a ne na interfejse, pa su interfejsi dodeljeni zonama. *Firewall* tako nadzire saobraćaj koji se razmenjuje između zona. Bezbednosna zona je postavljena na svakom mestu na kojem postoji potreba za kontrolom saobraćaja. Svi interfejsi unutar zone imaju isti nivo bezbednosti. Postoje 3 bezbednosne zone - Privatna, DMZ, i Internet. Privatna zona odnosi se na univerzitetsku mrežu. Dozvoljeni su sledeći tokovi saobraćaja, tzv. *zone pairs*:

- Iz privatne zone ka uređajima u DMZ
- Iz privatne zone ka Internetu
- Unutar privatne zone
- Sa Interneta ka uređajima u DMZ

Pošto je DMZ izložena Internetu, uređaji unutar ove zone mogu biti meta neželjenih aktivnosti neautorizovanih korisnika. Pomoću ZBF-a, korisnici unutrašnje mreže su zaštićeni od pristupa iz DMZ, osim ako nije specifično dodeljen pristup uređajima koji se nalaze u toj zoni. Na isti način je onemogućen pristup korisnicima sa Interneta koji žele da pristupe korisnicima unutar privatne mreže.

Univerzitetskoj mreži je moguće pristupiti preko Interneta, tačnije pomoću VPN modula. Kao rešenje koristi se IPSec tehnologija. Javna strana VPN-a postavljena je u DMZ i zaštićena *firewall*-om. Svi IPSec tuneli se završavaju kod *firewall*-a.

XII. SNMP

Kao alat za nadzor mreže koristi se SNMP protokol koji se koristi za nadzor raznih stavki unutar mreže, npr. da li su podaci stigli sa neočekivanog izvora, dodaje izvore na tzv. crnu listu, nadzire da li se krše odredbe zaštitne polise (maksimalni dozvoljeni broj poziva, maksimalni propusni opseg i sl.). Konkretno, koristi se set aplikacija Net-SNMP. To je skup alata koji se koristi za implementaciju SNMPv1, v2 i v3, sa podrškom za IPv4 i IPv6. SNMP *manager* se nalazi u data centru i koristi se za komunikaciju za ostalim računarima i uređajima na kojima je instaliran SNMP *Agent*. SNMP *Agent* je program koji je implementiran na mrežnim uređajima. Koristi se za prikupljanje informacija unutar mreže, koje dostavlja manager uređaju na zahtev administratora. Prikuplja razne informacije o stanju mreže i svojoj okolini koje mogu biti od značaja za funkcionisanje mreže. Svaki agent održava informacionu bazu podataka koja se sastoji od statističkih i

kontrolnih vrednosti, koje su definisane za uređaje u mreži. Podaci iz baze su vrednosti koje *manager* kontroliše u pomoću njih utvrđuje nepravilnosti unutar mreže. SNMP je nebezbedan protokol. Sistemi koji koriste SNMP Agent podešeni su da odbijaju zahteve od neautorizovanih *management* sistema. Takođe se koristi i IPSec kako bi se zaštitile SNMP poruke. To se postiže implementacijom filterskih specifikacija u odgovarajućim IP filter listama između SNMP *management* sistema i agenata.

Univerzitetska mreža poseduje dostupnost od 99.995%, što znači 27 minuta nedostupnosti na godišnjem nivou.

XIII. ZAKLJUČAK

Pravilno planiranje mreže je od velikog značaja. Potrebno je potrebe korisnika uskladiti sa brojnim standardima, bezbednosnim stavkama, kao i naći odgovarajući odnos između bezbednog protoka informacija i kvaliteta prenosa tih informacija. Takođe je neophodno obratiti pažnju na fizičku zaštitu samih uređaja u mreži, uz softversku bezbednost, jer je opasnost od neovlašćenog pristupa velika i može imati negativne posledice po funkcionisanje same mreže.

Veoma je bitno detaljno pristupiti projektovanju konvergirane mreže pošto prenos podataka, video, i audio zapisa zahteva neometan i bezbedan rad mrežne infrastrukture, pogotovo ako je reč o velikim mrežama kao što je univerzitetska mreža koja povezuje hiljade korisnika. Potreban je i konstantan nadzor mreže, kao i edukacija korisnika i administratora kako bi se mogućnost greške svela na minimum.

LITERATURA

[1] Student guide: Designing Cisco Network Service Architectures Volume 1 (ARCH), Version 2.0, Cisco Press, 2007
[2] Student guide: Designing Cisco Network Service Architectures Volume 2 (ARCH), Version 2.0, Cisco Press, 2007
[3] Ramaswami, R., Sivarajan, Kumar N., *Optical networks: A practical perspective*, second edition, 2002
[4] Hellberg, C., Greene, D., Boyes, T., *Broadband network architectures: Designing and deploying Triple-play services*, 2007
[5] Hens, Francisco J., Caballero, José M., *Triple play: Building the converged network for IP, VoIP and IPTV*, 2008
[6] Alwayn, V., *Optical network design and implementation*, Cisco Press, 2004
[7] Perros, Harry G., *Connection-oriented networks*, 2005
[8] www.ciscopress.com

[9] Moy, John T., *OSPF: Anatomy of an Internet Routing Protocol*, 19 98
[10] Veinović, M., Jevremović, A., *Računarske mreže*, 2011

ABSTRACT

Subject of this paper is careful and detailed planning of a computer network which would interconnect all universities in Serbia The backbone comprises of optical links which enable high speed data transfer. Network topologies of all the locations are designed per the Cisco's three layer hierarchical model (core, distribution, access) which enables reliability and scalability.

Keywords – Network design, Optical communications, Triple Play Networks

UNIVERSITY NETWORK DESIGN

Dejan Brdareski