



UNIVERZITET SINGIDUNUM
-MASTER STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE

- Master rad -

**Idejni projekat „Campus mreža Medicinskog
fakulteta Univerziteta u Beogradu“**



UNIVERZITET SINGIDUNUM
-MASTER STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE

Mentor:

Prof. dr Ranko Popović

Kandidat:

Nenad Džambasević

Beograd, 2011.

Sadržaj

1	UVOD.....	2
1.1	PROJEKTNII ZADATAK.....	3
2	METODOLOGIJA NAUČNOG ISTRAŽIVANJA.....	5
2.1	PREDMET ISTRAŽIVANJA.....	5
2.2	CILJ ISTRAŽIVANJA.....	5
2.3	METODE ISTRAŽIVANJA.....	6
3	FIZIČKA STRUKTURA CAMPUS MREŽE.....	7
4	LOGIČKA STRUKTURA CAMPUS MREŽE.....	13
4.1	POSTOJEĆA STRUKTURA MREŽE.....	17
4.2	REALIZOVANO REŠENJE.....	19
4.2.1	<i>Centralno čvorno mesto.....</i>	<i>20</i>
4.2.2	<i>Pristupni svičevi.....</i>	<i>23</i>
4.3	POVEZIVANJE PRISTUPNIH SVIČEVA SA CENTRALNIM ČVORIŠTEM.....	27
4.4	POVEZIVANJE SA AKADEMSKOM MREŽOM.....	29
4.5	RUTIRANJE U CAMPUS MREŽI.....	29
5	MREŽNI PROTOKOLI I SERVISI.....	31
5.1	PROTOKOLI ZA RUTIRANJE.....	31
5.2	HSRP.....	33
5.3	NTP.....	35
5.4	SNMP I MONITORING.....	37
6	BEZBEDNOST.....	40
6.1	FIREWALL.....	40
6.2	PROXY.....	45
6.3	SYSLOG.....	48
6.4	DHCP SNOOPING.....	50
6.5	SSH.....	51
7	SERVERSKA INFRASTRUKTURA.....	52
7.1	POSTOJEĆA INFRASTRUKTURA.....	52
7.2	BLADE ARHITEKTURA.....	53
7.3	VIRTUELIZACIJA.....	55
7.4	TEHNIČKE SPECIFIKACIJE REŠENJA ZA NOV DATA CENTAR.....	57
7.4.1	<i>Blejd server rešenje.....</i>	<i>57</i>
7.4.2	<i>Sistem za skladištenje podataka za blejd server rešenje.....</i>	<i>57</i>
7.4.3	<i>Rek ormar za smeštanje opreme.....</i>	<i>58</i>
7.4.4	<i>Softver za virtuelizaciju servera.....</i>	<i>58</i>
7.5	REALIZOVANO REŠENJE.....	60
8	TELEKOMUNIKACIJE.....	61
8.1	POSTOJEĆA INFRASTRUKTURA.....	61
8.2	REALIZOVANO REŠENJE.....	63
9	MERE ZAŠTITE BEZBEDNOSTI I ZDRAVLJA NA RADU.....	66
9.1	OPASNOSTI I PRETNJE I PREDVIĐENE MERE ZA NJIHOVO OTKLANJANJE.....	66
9.2	OPŠTE NAPOMENE I OBAVEZE.....	68
10	PREDMER I PREDRAČUN.....	70
11	ZAKLJUČAK.....	76
12	LITERATURA.....	77

SAŽETAK

U ovom radu je opisan projekat campus mreže Medicinskog fakulteta Univerziteta u Beogradu. Rad je koncipiran tako, da na osnovu postojeće strukture campus mreže, se izvrši nadogradnja opreme i servisa u cilju poboljšanja ICT infrastrukture i pripremanja same mreže za implementaciju novih servisa. Korišćen je model dizajna campus mreže srednje veličine koja obuhvata do 2000 korisnika.

Ključne reči: campus mreže, ICT, layer 3 svičevi, bezbednost, redundansa, visoka dostupnost, SNMP, blade serveri, virtuelizacija, VoIP

ABSTRACT

This paper describes project of Medical Faculty – University of Belgrade campus network. The paper is structured based on existing campus network, an upgrade of existing equipment and services can be made, to improve ICT infrastructure and prepare the network for implementation of new services. Medium-sized campus network model was used, which includes up to 2000 users.

Keywords: campus networks, ICT, layer 3 switches, security, redundancy, high availability, SNMP, blade servers, virtualization, VoIP

1 UVOD

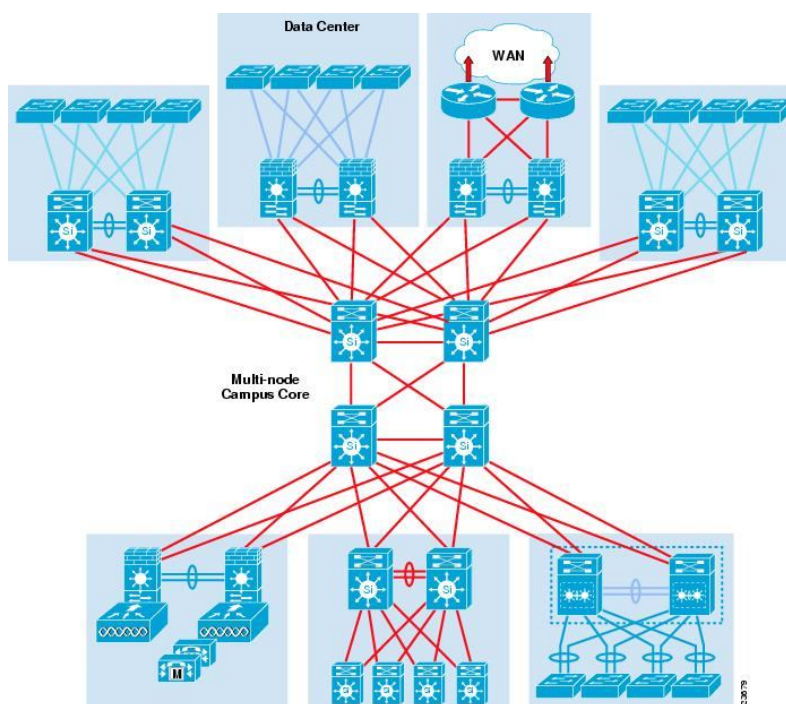
Moderna medicina u velikoj meri se oslanja na računarske i na telekomunikacione servise. Novi medicinski aparati u najvećem broju slučajeva imaju fabrički ugrađene komunikacione interfejsse koji im obezbeđuje jednostavno povezivanje u mrežu. Da bi ovakvi servisi bili mogući, neophodna je komunikaciona infrastruktura koja će da obezbedi prenos svih podataka od interesa.

Ovaj rad je nastao kao potreba za poboljšanjem jedinstvene računarsko-komunikacione infrastrukture koja povezuje sve objekte i institute Medicinskog fakulteta.

Na osnovu trenutnog stanja campus mreže Medicinskog fakulteta, predstavljene u drugom projektnom zadatku, projektni zadatak ovog rada predstavlja predlog nadogradnje i reorganizacije campus mreže Medicinskog fakulteta Univerziteta u Beogradu. U okviru projekta koristiće se postojeće trase položenih optičkih kablova, pomoću kojih su povezani udaljeni objekti Medicinskog fakulteta, takođe obuhvata i reorganizaciju logičke i dela fizičke strukture postojeće mreže, izgradnju novog datacentra, realizaciju backup lokacije centralnog čvornog mesta, implementacija novih bezbednosnih rešenja radi povećavanja bezbednosti campus mreže kako od spoljnih tako i od unutrašnjih napada, realizacija nove serverske infrastrukture u zajedno sa softverskom platformom za virtuelizaciju, kao i realizacija nove telekomunikacione infrastrukture sa implementacijom VoIP tehnologije.

1.1 Projektni zadatak

Projekat treba da sadrži predlog izmene svih aktivnih mrežnih uređaja sa novim uređajima, kao i predlog nadogradnje mreže menjajući samo aktivne mrežne uređaje na centralnim čvornim mestima. Pored menjanja samih mrežnih uređaja biće dat predlog izgradnje nove serverske infrastrukture, zasnovane na blade tehnologiji i virtuelizaciji, i predlog implementacije novih mrežnih protokola i servisa.



Slika 1. – Campus mreža sa više jezgara

Idejni projekat se sastoji iz 10 poglavlja. Prvo poglavlje je uvod u kome je napisano koji su osnovni zadaci koji su postavljeni za izradu ovog projekta.

Poglavlje broj dva sadrži opis metoda i ciljeva korišćenih pri izradi ovog projekta. Poglavlje broj tri sadrži opis fizičke strukture mreže koji se sastoji od opisa trasa polaganja kablova i tehnologija koja će se za to koristiti.

Kako bi se realizovala redundansa u centralnim čvorištima u četvrtom poglavlju je dat predlog nabavke i postavljanja novog centralnog layer 3 sviča. Pored same implementacije redundanse u vidu novog čvorišta, u četvrtom poglavlju je dat i predlog nabavke novih pristupnih layer 2 svičeva. Imajući u vidu da se implementacijom novih servisa i tehnologija, javlja

potreba za većim brzinama na pristupnim svičevima i trunk linkovima i uzimajući u obzir da trenutno standardne brzine iznose 1Gbps za pristupne (access) portove i 10Gbps za trunk portove, dat je predlog nabavke pristupnih svičeva i centralnog sviča koji ispunjavaju gore navedene uslove. Pri samom kreiranju predloga uočeno je da na određenim čvorištima postoje grupisani svičevi. Kako bi se kreirala redudansa i na nivou pristupnih svičeva iskorišćena je tehnologija u vlasništvu Cisco-a, FlexStack, koja nam pruža mogućnost da više svičeva grupišemo u jednu logičku celinu, što nam dodatno pruža mogućnost jednostavnijeg upravljanja i monitoringa istih.

Obzirom da trenutno postoji samo jedan link ka RCUB-u (Računarski Centar Univerziteta u Beogradu), potrebno je realizovati rezervni link, koji bi bio fizički odvojen od trenutnog linka, ka nekom od drugih čvorišta AMRESA-a.

U petom poglavlju je dat opis protokola koje je potrebno implementirati u okviru ove campus mreže i koji predstavljaju grupu osnovnih protokola potrebnih za neometano funkcionisanje i monitoring iste.

Šesto poglavlje predstavlja skup rešenja koje svojom implementacijom pružaju bezbednost kako od spoljnih tako i od unutrašnjih malicioznih korisnika. Pri implementaciji firewall rešenja potrebno je naglasiti da je samo definisanje dozvoljenih servisa kojima mogu da pristupaju korisnici campus mreže izvedeno tako da se blokiraju P2P saobraćaj i SMTP pristup udaljenim serverima, sem mail serveru Medicinskog fakulteta lociranom u RC-u Elektrotehničkog fakulteta, dok je pristup ostalim servisima dozvoljen samo korišćenjem implementiranog proxy rešenja, u vidu Squid 3 web cache proxy-ja. Pored centralnog rešenja za pristup web sadržaju, dat je predlog implementacije log rešenja kako bi se, u slučaju kršenja pravilnika eksploatacije mreže Medicinskog fakulteta ili prestanka funkcionisanja određenog uređaja ili servisa došlo do uzroka istog.

Sedmo poglavlje sadrži opis načina povezivanja postojećih telekomunikacionih centrala pomoću VoIP protokola i postojeće mrežne infrastrukture.

Poglavlje broj osam sadrži analizu i predlog implementacije nove telekomunikacione infrastrukture zasnovane na IP/PABX rešenju.

Poglavlje broj devet predstavlja prilog o merama zaštite bezbednosti i zdravlja na radu. U okviru desetog poglavlja se nalaze predmer i predračun za prethodno opisanu opremu i radove potrebne za implementaciju.

Pri samom definisanju mrežne opreme korišćena je isključivo profesionalna mrežna oprema visokih performansi i kapaciteta i ostavljena je opcija da se implementira i amaterska oprema, što se ne preporučuje u campus mrežama ove dimenzije a posebno u sklopu potreba i zahteva Medicinskog fakulteta.

2 METODOLOGIJA NAUČNOG ISTRAŽIVANJA

2.1 Predmet istraživanja

Predmet ovog istraživanja su *campus* mreže, njihov dizajn, njihov način funkcionisanja, eksploatacija, problemi uočeni pri korišćenju istih i rešenja za uklanjanje istih.

2.2 Cilj istraživanja

Ostvarivanje cilja istraživanja biće zasnovano na naučnim činjenicama definisanim i publikovanim u radovima i projektima eminentnih stručnjaka, ali će u radu biti prezentovana i iskustva autora.

Naučni cilj ovoga rada je sistematizacija znanja o *campus* mrežama, njihov dizajn i primena u dizajnu fakultetske mreže i primenjeno tehničko rešenje.

Društveni cilj ovoga rada je udovoljanje potreba fakulteta pri dizajnu i implementaciji mrežne računarske infrastrukture.

Osnovni pojmovi koji su bitni u ovom radu su:

- Ethernet;
- Layer 3 svičing;
- Security;
- Datacenter;

- Dostupnost (High Availability);
- Optički kablovi;
- Telekomunikacije.

2.3 Metode istraživanja

Uzimajući u obzir specifičnosti proučavanog predmeta istraživanja korišćene su različite metode, kako bi se zadovoljili osnovni metodološki zahtevi - objektivnost, pouzdanost, opštost i sistematičnost.

Istraživana su naučno-teorijska saznanja, relevantna literatura i savremena poslovna praksa sledećim metodama i tehnikama:

- deduktivna i induktivna metoda;
- metod analize i sinteze;
- metod apstrakcije
- komparativna metoda
- analiza sadržaja.

3 FIZIČKA STRUKTURA CAMPUS MREŽE

Fizička struktura mreže predstavlja trase optičkih kablova između objekata i način njihovog povezivanja u cilju uspostave linkova. Imajući u vidu strukturu prostora u delu grada gde se radi mreža, nije bilo moguće kopati i postavljati novu kablovsku kanalizaciju za postavljanje optičkih kablova. S druge strane, u delu koji pripada Kliničkom centru Srbije postoje tehnički kanali koji se koriste za postavljanje toplovodne i kablovske instalacije. Svi tehnički kanali su prohodni i omogućavaju da radnici mogu da prođu i postave regale za postavljanje optičkih kablova.

Što se tiče samih optičkih okosnica, postoje dva oblika:

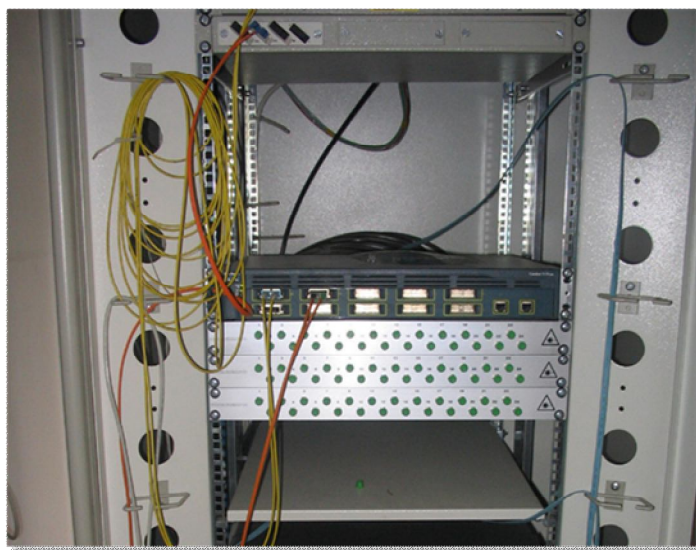
- prvi je u vidu glavnih optičkih čvorišta, gde su optički kablovi terminisani na *patch*–panelima unutar razvodnih RACK ormana, u kojima će se pored optičkih i LAN *patch* – panela ugrađivati i aktivna oprema, kao i UPS zaštitni uređaji.
- Drugi oblik predstavlja veliki broj optičkih kablova terminisanih u jednu ili više završnih optičkih kutija(ZOK), koje se nalaze na istom mestu unutar nekog objekta koji predstavlja lokalno čvorište. U njima se ne ugrađuje nikakva aktivna oprema, pa im nije potrebno napajanje, već se samo optičkim *patch* kablovima prespajaju optički linkovi.

Postoje dva glavna optička čvorišta. Prvo se nalazi u zgradi Dekanata Medicinskog fakulteta, a drugo u zgradi Silos (Institut za socijalnu medicinu i statistiku). Ova dva čvorna mesta potrebno je povezati pomoću optičkog kabla sa 24 *singlemode-nih*(SM) vlakana.

Trasa 1, dužine 160m, povezuje objekat Dekanata Medicinskog fakulteta sa objektom Interne B klinike. Na ovoj trasi postavljen je optički kabl sa 24 *singlemode-nih* vlakana. Postojeći optički kabl postavljen je unutar objekta Dekanata Medicinskog fakulteta do samog krova objekta, a zatim je vođen kao vazdušni samonosivi optički kabl do objekta Interne B klinike. Na strani objekta Dekanata Medicinskog fakulteta, kao i na strani objekta Interne B klinike postojeći optički kabl terminiran je na *patch* panelu.

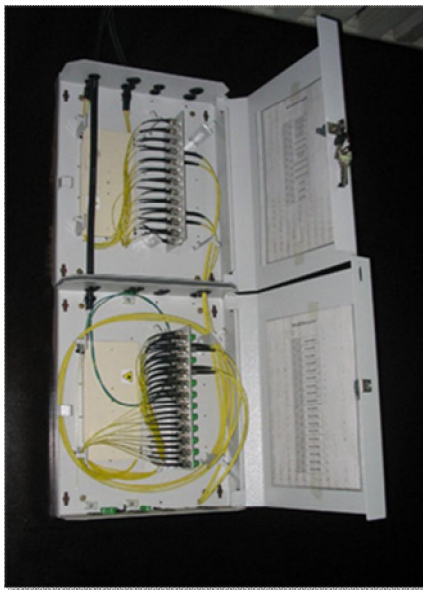
Trasa 2, dužine 138m, povezuje objekat Interne B klinike sa objektom Amfiteatra "Silos". Na ovoj trasi postavljen je optički kabl sa 24 *singlemode*-nih vlakana. Počevši od objekta Interne B klinike optički kabl je postavljen unutar objekta a zatim pasarelom do ulaska u objekat Amfiteatra "Silos". Na strani oba objekta postojeći optički kabl terminiran je na *patch* panelu.

Ostala čvorna mesta povezana su sa centralnim čvornim mestom pomoću optičkog *singlemode*-nog kabla za unutrašnju/spoljnu upotrebu.



Slika 5. – Glavno optičko čvorište u zgradi Dekanat

Pored već opisanog glavnog čvorišta, postoje i sporedna. Njihova glavna karakteristika po kojoj se razlikuju od glavnih čvornih mesta, jeste da se optički kablovi ne terminišu na *patch* – panelima, već na završnim optičkim kutijama, tzv. ZOK-ovima. Ako se, kojim slučajem, terminišu na *patch* – panelima, onda su to *patch* – paneli lokalnih LAN mreža, koji se nalaze unutar manjih RACK ormana. Ako su optički kablovi terminisani u ZOK-ovima, u tom slučaju, takva čvorišta služe samo za prespajanje kablova, tako da se saobraćaj samo preusmerava ka nekim drugim objektima, odnosno ka drugim RACK ormanima u kojima se nalazi adekvatna aktivna oprema sa kojom se vrši administriranje navedene mreže.



Slika 6. – Sporedno čvorno mesto (ZOK)

Svaki objekat mora imati terminisana dva para optičkih kablova kako bi se u slučaju prestanka funkcionisanja jednog glavnog čvornog mesta obezbedila redundansa i visoka dostupnost mreže. Obzirom da su svi optički linkovi između objekata već postavljeni i aktivni potrebno je samo realizovati link između objekata Dekanata i Silos.

Što se tiče fizičke strukture lan mreža povezanih objekata kao jedino rešenje nameće se strukturno kabliranje. Moderne računarske mreže sve više se sastoje od nekoliko desetina, pa i stotina radnih mesta (računara, terminala) koje treba povezati u računarsku mrežu. Ovakva kompleksnost zahtevala je rešavanje nekih problema koji su pri tome nastali, a ti su:

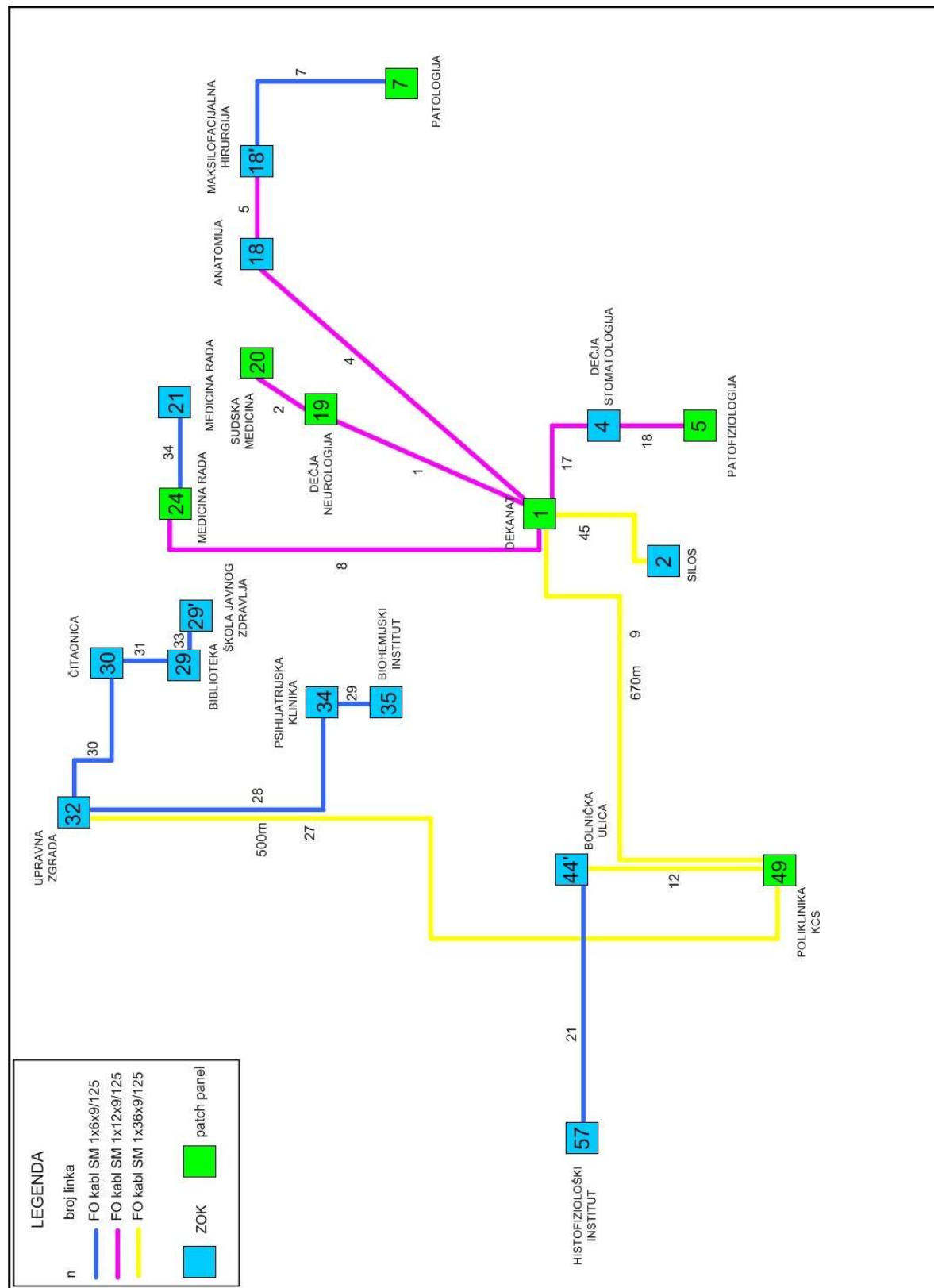
- veliki broj kablova koje je teško kontrolisati,
- stalno povećanje potrebne brzine prenosa podataka,
- povećanje cene održavanja velikih kablovskih sistema i
- potreba za velikom fleksibilnošću kablovskog sistema.

Strukturno kabliranje rešava sve gore navedene probleme i ispunjava zahteve koji se javljaju pri definisanju rešenja računarskih mreža u poslovnim zgradama, kompleksima poslovnih zgrada ili industrijskim kompleksima. Kablovski sistem koji je rešen po standardima koji opisuju strukturno kabliranje ima sledeće osobine:

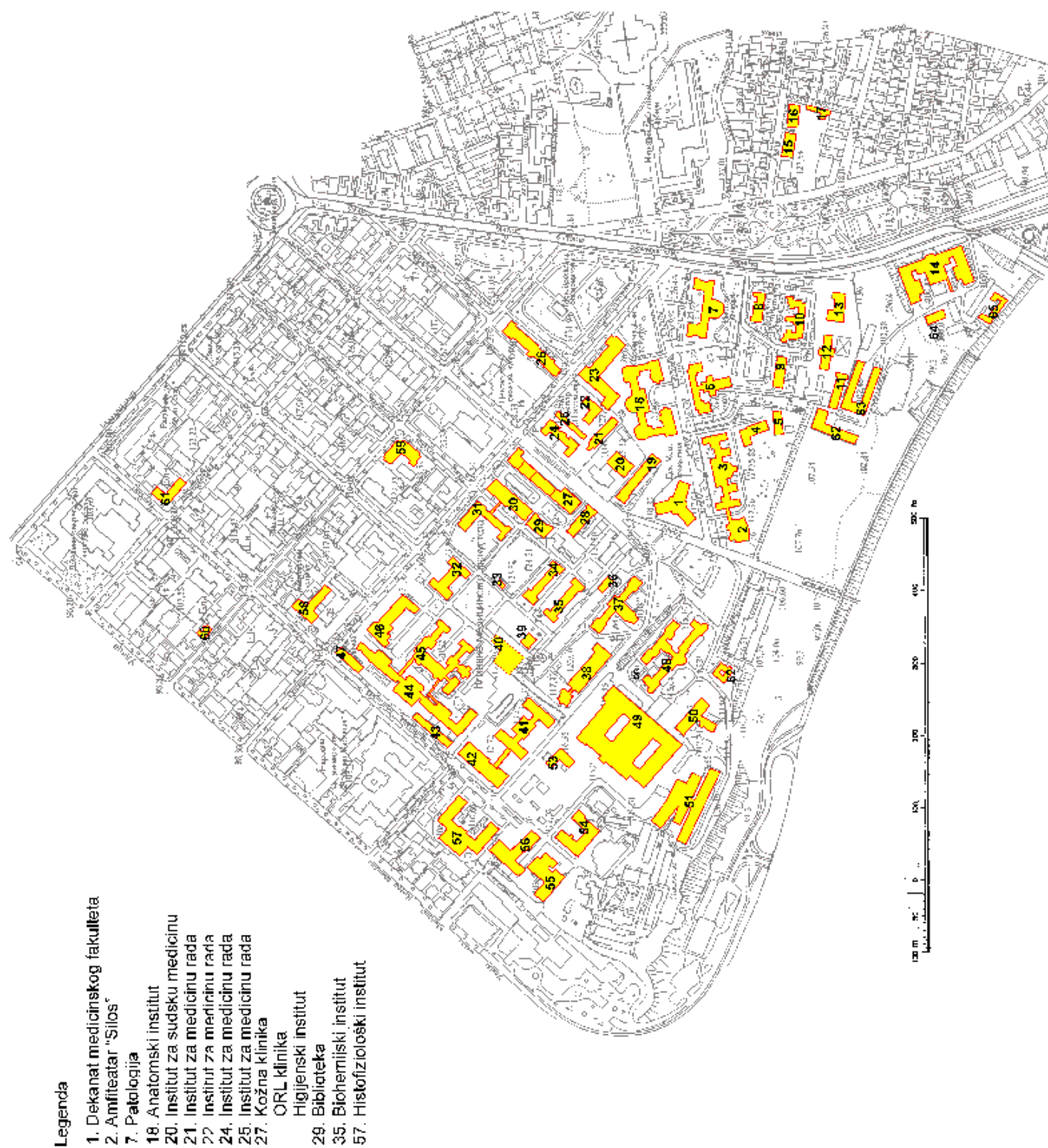
- oslanja se na važeće svetske standarde propisane za kablove, utičnice i distributivne elemente koji se koriste,
- smanjuje troškove održavanja,
- olakšava širenje i modifikacije računarske mreže i
- omogućava korišćenje telefona, računara i terminala u celoj zgradi.

Rešenje strukturnog kablovskog sistema obezbeđuju sledeći standardi:

- TIA/EIA-568 Commercial Building Telecommunications Cabling Standard
- TIA/EIA-569 Commercial Building Standard for Telecommunications Pathways and Spaces
- TIA/EIA-606 Administration Standard for Telecommunications Infrastructure of Commercial Building



Slika 3. – Blok šema campus mreže



Slika 4. – Objekti Medicinskog fakulteta

4 LOGIČKA STRUKTURA CAMPUS MREŽE

Za realizaciju campus mreže predviđeno je korišćenje gigabit ethernet tehnologije u kombinaciji sa tehnologijom layer 3 svičing-a. Ovakvo rešenje obezbeđuje visoke performanse celokupne mrežne infrastrukture uz mogućnost podrške svih trenutno aktuelnih mrežnih servisa. Aktivna mrežna oprema mora da podrži standardna i savremena rešenja za podršku informaciono komunikacionim tehnologijama (ICT), kao i specifična rešenja koje uslovljava delatnost zdravstvenih i naučnih ustanova.

Da bi se kreirala redundansa i obezbedila neprekidna dostupnost i funkcionalnost campus mreže potrebno je kreirati drugo centralno čvorno mesto. Za to centralno mesto je odabrana zgrada Instituta za socijalnu medicinu i statistiku (Silos). Obzirom da su mrežni servisi i aplikacije sve zahtevnije, i uzimajući u vid da postojeća fizička infrastruktura može da podrži, novo centralno čvorište mora da podrži sledeće protokole i tehnologije:

- 848 Gbps svičing kapacitet with 250 Mpps of throughput,
- 4 neblokirajuća 10 Gigabit Ethernet uplinka [SFP+],
- SFP podrška na uplinkovima,
- Maksimalno 384 neblokirajućih portova 10/100/1000,
- PoEP (30W) simultano mogućnosti na svim portovima, po jednoj kartici,
- UPOE (60W)mogućnosti na svim karticama,
- Energy Efficient Ethernet (IEEE 802.3az),
- 196 neblokirajućih portova Gig SFP,
- 100 portova 10G SFP+ (4 Uplink porta + 96 portova na karticama),
- 128K Flexible NetFlow zapisa u hardware-u,
- Podrška za eksternu USB and SD memoriju,
- 256K routing zapisa kako bi se omogućio brzi pristup campus mreži,
- IPv6 podrška u hardware-u, omogućeno wire-rate prosleđivanje paketa za IPv6 mreže,
- Dinamička hardverska tabela prosleđivanja kako bi se olakšala migracija sa IPv4-na-IPv6 ,

- Skalabilno rutiranje (IPv4, IPv6, and multicast) tabele, Layer 2 tabele, i Pristupne liste (ACL) i QoS upisi radi iskorišćenja 8 upita po jednom portu i sveobuhvatne bezbednosne polise po jednom portu.
- *Spanning Tree Protocol*,
- *Rapid Spanning Tree Protocol*,
- IEEE 802.1p *class-of-service (CoS) prioritization*,
- IEEE 802.1Q *VLAN tagging* na svim portovima,
- podrška za minimalno 4095 VLAN-ova,
- IEEE 802.3ad *Link Aggregation Control Protocol (LACP)*,
- SNMPv1 i SNMPv2,
- IGMP *snooping* V1 i V2,
- *DHCP Relay*,
- 1. Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) ili Gateway Load Balancing Protocol (GLBP)
- OSPF v2 i OSPF v3 protokol rutiranja,
- *access* liste za filtriranje saobraćaja koje imaju mogućnost kontrole saobraćaja do nivoa portova kod TCP i UDP paketa, i to kako u odlaznom tako i u dolaznom smeru,
- garantovanje QoS za multimedijalne i aplikacije za rad u realnom vremenu,
- DiffServ,
- klasifikaciju i reklasifikaciju saobraćaja za stanovišta QoS parametara,
- *wirespeed Layer 3 IP routing*,
- IEEE 802.1Q *VLAN tagging*,
- SSH za pristup preko mreže,
- kontrolu protoka po portu,
- SNMPv2c,
- podršku za rutiranje *multicast* saobraćaja,
- Maksimalna otpornost sa redundantnim komponentama, Nonstop Forwarding/Stateful Switchover (NSF/SSO), i podrška za In-Service Software Upgrade (ISSU),
- Virtuelizaciju mreže radi Layer 3 segmentacije,
- Automatizaciju pomoću AutoQoS i Auto SmartPorts radi brzog rezervisanja, dijagnostike i izveštavanja.

Aktuelne *svičing hub*-ove u mreži potrebno je zameniti novim koji moraju da podržavaju sledeće standarde za svaki port:

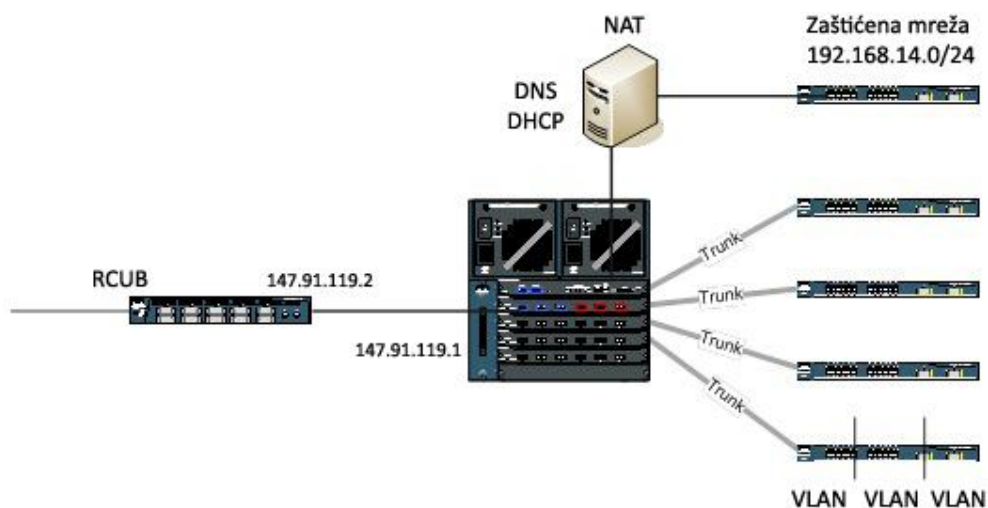
- IEEE 802.1x,
- IEEE 802.3x *full duplex* na 1000Base-T portovima,
- IEEE 802.1D *Spanning-Tree Protocol*,
- IEEE 802.1p *class-of-service (CoS) prioritization*,
- IEEE 802.1Q VLAN *tagging*,
- podrška za minimalno 255 VLAN-ova pri čemu VLANID mora da bude konfigurabilan u granicama od 1 do 4095,
- IEEE 802.3ad *Port Trunking*
- IEEE 802.3 10Base-T
- IEEE 802.3u 100Base-TX
- IEEE 802.3ab 1000Base-T,
- IEEE 802.3z 1000Base-X,
- 10GBASE-LR, SR, LRM, CX1 SFP+ portove,
- SNMPv2,
- ne blokirajuću komutaciono polje (*non-blocking svičing fabric*),
- IGMP *snooping*,
- *broadcast storm control*.

Redni broj	Ime	Lokacija
1.	Switch4506	Dekanat
2.	Cisco2960	Dekanat
3.	Cisco2960	Dekanat
4.	CiscoExpress500	Dekanat
5.	AT8024	Dekanat
6.	CiscoExpress500	Dekanat
7.	CiscoExpress500	Dekanat
8.	Cisco2950	Silos
9.	Cisco2950	Silos
10.	Cisco2950	Silos
11.	HP2524	Higijena
12.	Cisco2950	Cibid
13.	LinksysSRW2024G4	Citaonica
14.	Linksys SLM2008	Silos
15.	Linksys SLM2008	Dekanat
16.	Cisco2950	Histologija
17.	HP2524	Histologija
18.	HP2524	Fiziologija
19.	HP2524	Fiziologija
20.	CiscoExpress500	Histologija
21.	CiscoExpress500	Fiziologija
22.	LinksysSRW2024G4	Histologija
23.	LinksysSRW2024G4	Fiziologija
24.	HP2524	Biohemija
25.	HP2524	Biohemija
26.	HP2524	Anatomija
27.	HP2524	Anatomija
28.	HP2524	Patologija
29.	HP2524	Mikrobiologija
30.	HP2524	Patologija
31.	HP2524	Patologija
32.	LinksysSRW2024G4	Farmakologija
33.	LinksysSRW2024G4	Patofiza
34.	HP2524	Sudska medicina
35.	HP2524	Sudska medicina
36.	HP2524	Skola javnog zdravlja

Tabela 1. – Spisak trenutnih upravljivih svičing hub-ova i njihova lokacija

4.1 Postojeća struktura mreže

U centralnom čvorištu trenutno se nalazi jedan *Layer 3* svič Cisco Catalyst 4506 koji obavlja funkciju rutiranja saobraćaja između u campus mreži. Na slici 5. je data postojeća logička struktura campus mreže Medicinskog fakulteta.



Slika 5. – Izvedeni izgled mreže

Centralni *Layer 3* svič koji se trenutno koristi u ovoj *campus* mreži ima sledeće karakteristike:

- modularni uređaj sa redundantnim napajanjem,
- neblokirajuće komutaciono polje,
- propusna moć *backplane*-a minimalno 64Gb/s,
- propusna moć uređaja pri rutiranju paketa na IP nivou minimalno 48Mpps,
- 14 portova tipa 1000BaseLX dometa minimalno 10km po monomodnom optičkom vlaknu (portovi moraju da budu u realizaciji sa GBIC ili SFP modulima),
- 8 portova tipa 1000Base-SX za rad na multimodnom vlaknu (portovi moraju da budu u realizaciji sa GBIC ili SFP modulima),
- 1 port tipa 1000BaseT,
- mogućnost proširenja uređaja do minimalno 32 *gigabit ethernet* portova (ukupno u celom uređaju).

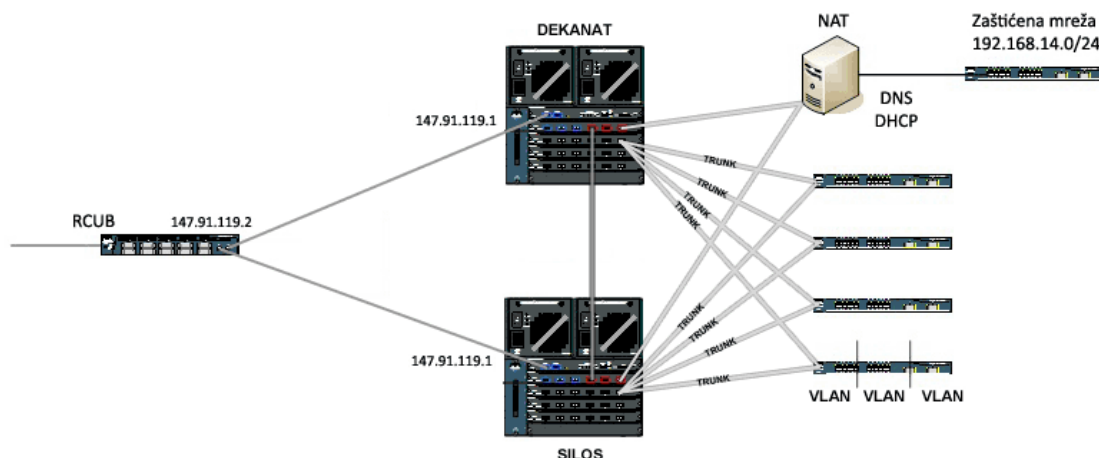
Osnovne funkcije i protokoli koje ima softver za rutiranje i prosleđivanje saobraćaja u uređaju su:

- *Spanning Tree Protocol*,
- *Rapid Spanning Tree Protocol*,
- IEEE 802.1p *class-of-service* (CoS) *prioritization*,
- IEEE 802.1Q *VLAN tagging* na svim portovima,
- podrška za minimalno 4095 VLAN-ova,
- IEEE 802.3ad *Link Aggregation Control Protocol* (LACP),
- SNMPv1 i SNMPv2,
- IGMP *snooping* V1 i V2,
- DHCP *Relay*,
- OSPF v2 protokol rutiranja,
- *access* liste realizovane u hardveru za filtriranje saobraćaja koje imaju mogućnost kontrole saobraćaja do nivoa portova kod TCP i UDP paketa, i to kako u odlaznom tako i u dolaznom smeru - minimalni broj pravila po jednoj *access* listi mora da bude 100 (sto),
- garantovanje QoS za multimedijalne i aplikacije za rad u realnom vremenu,
- DiffServ,
- klasifikacija saobraćaja za stanovišta QoS parametara,
- *wirespeed Layer 3 IP routing*,
- SSH protokol verzija 2 za pristup preko mreže,
- podršku za rutiranje *multicast* saobraćaja (PIM protokol).

Aktuelni centralni layer 3 svič trenutno podržava trankove do 1Gbps, što po današnjim standardima dizajna campus mreža predstavlja standardnu brzinu pristupa korisničkih radnih stanica. Takođe u postojećem dizajnu mreže, prilikom ispadanja iz rada centralnog čvornog mesta ne postoji redundantno čvorište koje bi preuzelo funkciju rutiranja tako da sam layer 3 switch predstavlja *single point of failure*. Jedini vid redudanse u centralno čvornom mestu predstavlja redundantno napajanje layer 3 sviča.

4.2 Realizivano rešenje

Kako bi se obezbedila visoka pouzdanost i dostupnost kompletne campus mreže potrebno je izgraditi sekundarno centralno čvorno mesto (*multi-node campus core - Slika 1.*) koje bi obezbedilo redundansu u postojećoj infrastrukturi. Postojeće rešenje takođe obuhvata premeštanje trenutnog layer 3 sviča.



Slika 6. – Predložena struktura campus mreže

Aktivna mrežna oprema u glavnim i lokalnim čvorištima mora da bude priključena na uređaj za neprekidno napajanje (UPS). UPS-evi moraju da budu on-line tipa sa priključkom na računarsku mrežu za remote management.

Obzirom da su nova IT rešenja kao što su *Cloud computing*, *video streaming*, *VoIP* i *video konferencije* dosta zahtevne po pitanju protoka, potrebno je da trunk linkovi ka *access* svič-evima budu 10Gbps dok je na samim *access* svič-vima potrebno da pristupni portovi podržavaju brzinu od 1Gbps.

4.2.1 Centralno čvorno mesto

Rešenje koje u potpunosti zadovoljava prethodno navedene kriterijume za nov *layer 3* *svič* je u Cisco-vom modularnom *svič-u* Cisco 4500 serije (Slika 7.). Centralni deo ovog sistema predstavlja *Cisco Catalyst 4500E Supervisor Engine 7-E* čije karakteristike su date u *Tabeli 2*, zajedno sa *Cisco Catalyst 4506-E Switch* šasijom u koju se postavlja. Od modularnih kartica potrebno je ugraditi 3 kartice *WS-X4712-SFP+E*. Predloženi SFP moduli za povezivanje na optičku infrastrukturu su *Cisco SFP-10G-SR(multi-mode)* i *Cisco SFP-10G-LR(single-mode)* čije karakteristike su prikazane u *Tabeli 3.* Napajanje samog *svič-a* je pomocu dva redundantna napajanja snage 1400W, koje je moguće menjati bez gašenja samog *svič-a* (*hot swappable*) i čija karakteristika je data u *Tabeli 4.*



Slika 7. – Cisco 4506-E *svič*

Feature and Description	Supervisor Engine 7-E
Centralized Switching Capacity	848 Gbps
Per-Slot Switching Capacity	48 Gbps
Throughput	• 250 Mpps for IPv4 • 125 Mpps for IPv6
IPv4 Routing Entries	256,000
IPv6 Routing Entries	128,000
Multicast Routes	16,000 (Available with Cisco IOS XE 3.1.0 SG) 32,000 (Available with Cisco IOS XE 3.2.0 SG or later)
CPU	Dual Core 1.5 GHz
CPU Queues	64
Synchronous Dynamic RAM (SDRAM)	2 GB upgradable to 4 GB
NVRAM	1G
Security and QoS Hardware Entries	128,000
Cisco Network Admission Control (NAC) and Dynamic Host Configuration Protocol (DHCP) Snooping Entries	12,000
MAC addresses	55,000
Active VLANs	4,094
ARP Entries	46,000
Spanning Tree Protocol Instances	10,000
Switched Virtual Interfaces (SVIs)	4,094
Switched Port Analyzer (SPAN)	Maximum of 8 sessions: ingress and/or egress

Tabela 2. – Karakteristike Cisco Catalyst 4500E Supervisor Engine 7-E modula

Cisco SFP+	Talasna Dužina (nm)	Tip kabla	Veličina jezgra (Mikrona)	Propusni opseg (MHz * km)	Dužina kabla
Cisco SFP-10G-SR	850	MMF	62.5	160	26m
			62.5	200	33m
			50.0	400	66m
			50.0	500	82m
			50.0	2000	300m
Cisco SFP-10G-LR	1310	SMF	G.652	-	10km

Tabela 3. – Karakteristike SFP+ modula

Power Supply	1400W AC
Integrated PoE	No (data only)
Input current (rated)	16A at 100 VAC, 7A at 240 VAC
Output current (data)	• 12V at 113.4A • 3.3V at 12.2A
Output power redundant mode (data)	1360W + 40W
Output power combined mode (data)	2473W
Heat dissipation	1048 Btus per hour
Holdup time	20 ms
Hot swappable	Yes

Tabela 4. – Karakteristike napajanja

Radne karakteristike navedenog Cisco svič-a su:

- Radna temperatura 0 do 40°C,
- Skladištena temperatura -40 do 75°C,
- Relativna vlažnost vazduha 10% do 90% bez kondenzovanja,
- Nadmorska visina -60m do 3000m.

4.2.2 Pristupni svičevi

Potrebno je razmatrati dve opcije pri implementaciji novih layer 2 svičeva. Prva opcija je da su računarska i telekomunikaciona infrastruktura skroz odvojene tj. da nije potrebno implementirati VoIP rešenje, dok se u drugoj opciji podrazumeva da se objedine podaci, zvuk i video (*data+voice+video*).



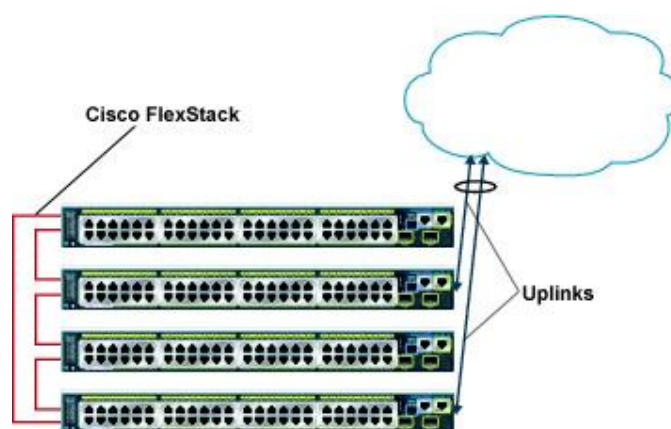
Slika 8. - Cisco Catalyst 2960S-24TD-L svič

Za prvi slučaj u kojem nije potrebno implementirati VoIP rešenje, odabran je Cisco Catalyst 2960S-24TD-L svič (karakteristike prikazane u *Tabeli 5.*) u potpunosti ispunjava postavljenu specifikaciju. Na lokacijama kao što su Histofiziološki institut, Institut za sudsku medicinu, Institut za socijalnu medicinu i statistiku i Anatomski institut gde se više svičeva nalazi u jednom rack ormanu Cisco FlexStack opcija koju nudi ovaj model olakšava održavanje i monitoring same mrežne infrastrukture. Naime Cisco FlexStack tehnologija nam omogućuje da se grupiše više layer 2 svičeva, koji se povezuju pomoću CAB-STK-E-0.5M FlexStack kabla. Tako povezani uređaji čine jednu logičku jedinicu i omogućavaju lakše održavanje i konfiguraciju mrežnih uređaja na datoj lokaciji.

	Catalyst 2960-S
Forwarding bandwidth	88 Gbps
Switching bandwidth	176 Gbps
Flash memory	64 MB
Memory DRAM	128 MB
Max VLANs	255
VLAN IDs	4000
Maximum transmission unit (MTU)	9198 bytes
Jumbo frames	9216 bytes

Forwarding Rate: 64-Byte Packet Cisco Catalyst 2960-S			
Cisco Catalyst 2960S-24TD-L	65.5 mpps		
Resource: Cisco Catalyst 2960-S and 2960	Default	QoS	Dual
Unicast MAC addresses	8000	8000	8000
IPv4 IGMP groups	255	255	255
IPv4 MAC QoS access control entries (ACEs)	128	384	0
IPv4 MAC security ACEs	384	128	256
Standards	• IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS Prioritization • IEEE 802.1Q VLAN • IEEE 802.1s • IEEE 802.1w • IEEE 802.1X • IEEE 802.1ab (LLDP) • IEEE 802.3ad • IEEE 802.3af • IEEE 802.3ah (100BASE-X single/multimode fiber only) • IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification		
	• 100BASE-BX (SFP) • 100BASE-FX (SFP) • 100BASE-LX (SFP) • 1000BASE-BX (SFP) • 1000BASE-SX (SFP) • 1000BASE-LX/LH (SFP) • 1000BASE-ZX (SFP) • 1000BASE-CWDM SFP 1470 nm • 1000BASE-CWDM SFP 1490 nm • 1000BASE-CWDM SFP 1510 nm • 1000BASE-CWDM SFP 1530 nm • 1000BASE-CWDM SFP 1550 nm • 1000BASE-CWDM SFP 1570 nm • 1000BASE-CWDM SFP 1590 nm • 1000BASE-CWDM SFP 1610 nm • 10GBASE-LR (SFP+) • 10GBASE-SR (SFP+) • 10GBASE-LRM (SFP+) • 10GBASE-CX1 (SFP+) • RMON I and II standards • SNMP v1, v2c, and v3		

Tabela 5. – Karakteristika Cisco Catalyst 2960S-24TD-L sviča



Slika 9. – Cisco FlexStack

Ukoliko se kao opcija odabere da se implementira kompletno VoIP rešenje potrebno je postaviti svičeve koji podržavaju PoE (*Power-Over-Ethernet*) standard, IEEE 802.3af-2003 i IEEE 802.3af-2009 standard poznatiji kao PoE+ (*Power-Over-Ethernet+*). Pored VoIP-a ovi svičevi omogućavaju i dodavanje uređaja koji podržavaju PoE standard kao što su IP Security kamere, mrežne web kamere, zidni satovi sa podrškom za NTP protokol, wireless access points, senzori (temperatura, vlažnost, kretanje, itd.) i drugi uređaji. Uređaj koji zadovoljava navedene karakteristike je Cisco WS-C2960S-24PD-L *layer 2* svič (specifikacija prikazana u *Tabeli 6.*) i kao i prethodno navedeni model takođe podržava Cisco FlexStack tehnologiju.

Cisco Catalyst 2960-S Switch Model	Description	Uplinks	Available PoE Power
Cisco Catalyst 2960S-24PD-L	24 Ethernet 10/100/1000 PoE+ ports	2 Ten Gigabit Ethernet SFP+ or 2 One Gigabit Ethernet SFP ports	370W
	Maximum Number of PoE+ (IEEE 802.3af) Ports*	Maximum Number of PoE (IEEE 802.3af) Ports*	Available PoE Power
Cisco Catalyst 2960S-24PD-L	12 ports up to 30W	24 ports up to 15.4W	370W
	Catalyst 2960-S		

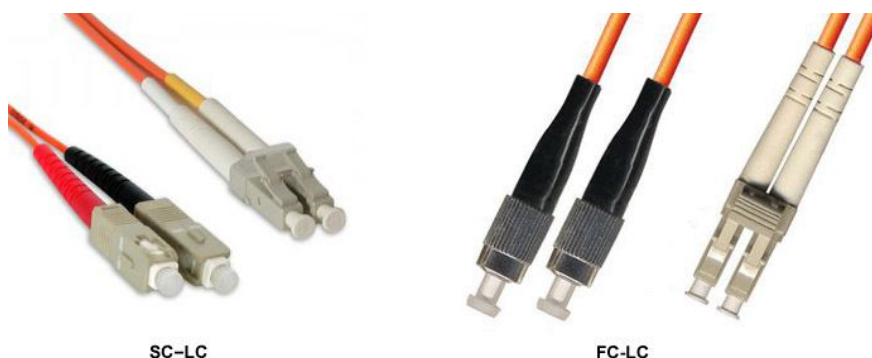
Forwarding bandwidth	88 Gbps		
Switching bandwidth	176 Gbps		
Flash memory	64 MB		
Memory DRAM	128 MB		
Max VLANs	255		
VLAN IDs	4000		
Maximum transmission unit (MTU)	9198 bytes		
Jumbo frames	9216 bytes		
Forwarding Rate: 64-Byte Packet Cisco Catalyst 2960-S			
Cisco Catalyst 2960S-24TD-L	65.5 mpps		
Resource: Cisco Catalyst 2960-S and 2960	Default	QoS	Dual
Unicast MAC addresses	8000	8000	8000
IPv4 IGMP groups	255	255	255
IPv4 MAC QoS access control entries (ACEs)	128	384	0
IPv4 MAC security ACEs	384	128	256
Standards	• IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS Prioritization • IEEE 802.1Q VLAN • IEEE 802.1s • IEEE 802.1w • IEEE 802.1X • IEEE 802.1ab (LLDP) • IEEE 802.3ad • IEEE 802.3af • IEEE 802.3ah (100BASE-X single/multimode fiber only) • IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • 100BASE-BX (SFP) • 100BASE-FX (SFP) • 100BASE-LX (SFP) • 1000BASE-BX (SFP) • 1000BASE-SX (SFP) • 1000BASE-LX/LH (SFP) • 1000BASE-ZX (SFP) • 1000BASE-CWDM SFP 1470 nm • 1000BASE-CWDM SFP 1490 nm • 1000BASE-CWDM SFP 1510 nm • 1000BASE-CWDM SFP 1530 nm • 1000BASE-CWDM SFP 1550 nm • 1000BASE-CWDM SFP 1570 nm • 1000BASE-CWDM SFP 1590 nm • 1000BASE-CWDM SFP 1610 nm • 10GBASE-LR (SFP+) • 10GBASE-SR (SFP+) • 10GBASE-LRM (SFP+)		

	• IEEE 802.3ab 1000BASE-T specification • IEEE 802.3z 1000BASE-X specification	• 10GBASE-CX1 (SFP+) • RMON I and II standards • SNMP v1, v2c, and v3
--	---	---

Tabela 6. – Specifikacija Cisco WS-C2960S-24PD-L sviča

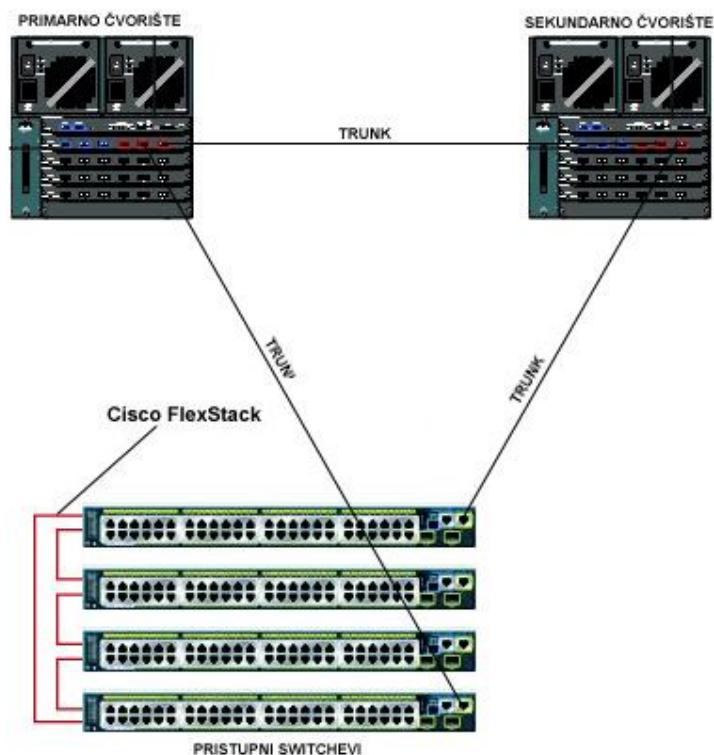
4.3 Povezivanje pristupnih svičeva sa centralnim čvorištem

Na Slici 6. prikazana je nova struktura campus mreže dobijena izgradnjom još jednog centralnog čvornog mesta. Premeštanjem postojećeg layer 3 sviča i postavljanjem novog dobija se redundantnost u radu same mreže. Fizičko povezivanje na optičku infrastrukturu u novom centralnom čvorištu se vrši pomoću SFP+ modula koji podrazumevaju da jedan kraj fiber optičkog kabla je terminiran na LC konektore dok je drugi kraj u zavisnosti od patch panela na koji se vrši konekcija terminiran na SC ili FC konektore (Slika 10.).



Slika 10. – Tipovi konektora

Kako bi se obezbedila redundantnost potrebno je povezati pristupne svičeve sa oba centralna čvorna mesta, što je omogućeno aktiviranjem i povezivanjem rezervnih optičkih linija i povezivanjem samih layer 3 svičeva međusobno. U situaciji gde u jednom rack ormanu imamo postavljeno više layer 2 svičeva koji su međusobno povezani pomoću FlexStack tehnologije jedan od svičeva se preko svog *trunk* porta priključuje na primarno čvorno mesto dok se na jednom od ostalih svičeva vrši priključivanje sa sekundarnim čvornim mestom.



Slika 11. – Redudantni linkovi sa FlexStack redudansom

Cisco FlexStack tehnologija omogućava da se kao na Slici 11. svičevi međusobno povežu tako da u slučaju otkaza jednog od svičeva koji su povezani na centralno čvorište ostali svičevi ostaju povezani preko drugog sviča koji je povezan na sekundarno čvorište. Protokoli korišćeni za uspostavljanje redudantnosti mrežne infrastrukture su opisani u Poglavlju br. 5.

4.4 Povezivanje sa akademskom mrežom

Campus mreža Medicinskog fakulteta – Univerziteta u Beogradu je sastavni deo akademske mreže Srbije. Imajući to u vidu, neophodno je da campus mreža bude povezana kvalitetnim linkom na akademsku mrežu. Glavno čvorište akademske mreže je RCUB. Između RCUB-a i Dekanata Medicinskog fakulteta u Beogradu uspostavljen je optički link i preko njega je pušten gigabit *ethernet* link. Link je u Dekanatu Medicinskog fakulteta terminiran na Cisco Catalyst 3550-12G layer 3 svičing hub-u. Pošto navedeni uređaj ima samo 12 portova a prema logičkoj strukturi campus mreže, u čvorištu u Dekanatu se stiče 15 linkova, za ovo čvorište će biti neophodno obezbediti proširenje. Proširenje može da bude realizovano postavljanjem novom layer 3 svičing hub-a umesto postojećeg ili dodavanjem još jednog identičnog uređaja koji bi se sa postojećim vezao u stek. S obzirom na značaj i veličinu mreže Medicinskog fakulteta, postojanje samo jednog linka ka akademskoj mreži može da predstavlja problem sa stanovišta pouzdanosti rada. Zbog toga treba u budućnosti realizovati i rezervni link do nekog od čvorišta akademske mreže. Rezervni link treba da bude realizovan po posebnom optičkom kablju (ne sme da bude isti kabl kojim je realizovan sadašnji link ka akademskoj mreži niti sme da ide istom trasom).

4.5 Rutiranje u campus mreži

Mreža Medicinskog fakulteta predstavlja jednu celinu za sebe. S obzirom da je i adresni prostor tako definisan da je moguće izvršiti agregaciju, svi preduslovi za formiranje posebne oblasti u OSPF-u su prisutni.

Akadska mreža Srbije kao protokol za interno rutiranje koristi OSPF protokol. OSPF protokol celokupnu mrežu deli na oblasti u cilju pojednostavljenja u ubrzavanja rutiranja. U skladu sa tim bi i campus mreža Medicinskog fakulteta treba da bude jedna oblast u okviru OSPF-a. Imajući u vidu način numeracije oblasti koji se primenjuje na akademskoj mreži, oblast kojoj pripada fakultetu ima identifikaciju 147.91.112.0 (vodeći broj adresnog bloka koji je dodeljen Medicinskom fakultetu na korišćenje). Granični ruter (Area Border Router) za oblast 147.91.112.0 predstavlja layer 3 svičing hub Cisco Catalyst 3550-12G. Prema

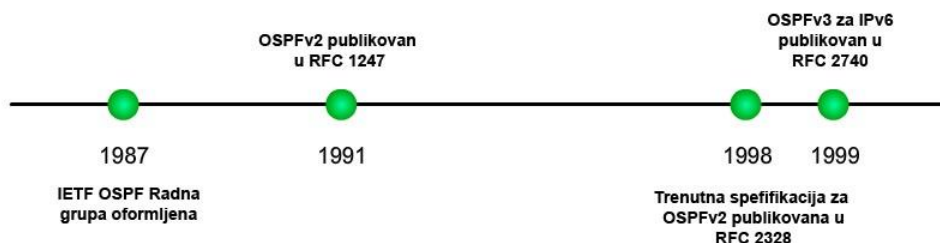
RCUB-u koji predstavlja backbone oblast za OSPF protokol, ovaj ruter će oglašavati agregirane rute. Unutar oblasti 147.91.112.0 koristiće se OSPF protokol između layer 3 svičing hub-ova koji će se nalaziti u lokalnim čvorištima. U mreži je na par mesta realizovana redundantna veza u cilju povećanja pouzdanosti rada cele mreže. OSPF protokol je zadužen da obezbedi korišćenje redundantnih linkova, kao u trenucima havarije tako i u vreme normalnog rada mreže.

5 MREŽNI PROTOKOLI I SERVISI

5.1 Protololi za rutiranje

OSPF (Open Shortest Path First) je link-state protokol koji je razvijen kao zamena za distance vector protokol RIP. RIP je predstavljao prihvatljivo rešenje u počecima umrežavanja i interneta, ali njegovo oslanjanje na hop count kao metriku za biranje putanja je ubrzo postalo neprihvatljivo u većim mrežama gde je bilo potrebno znatno bolje rešenje za rutiranje. OSPF je besklasni protokol za rutiranje koji koristi princip oblasti i skalabilnosti i koristi Dijkstrin SPF algoritam za odabir najbolje putanje.

Inicijalni razvoj OSPF-a je počeo 1987. godine od strane IETF (Internet Engineering Task Force) OSPF radne grupe. U to vreme Internet je u najvećem delu predstavljao akademsku i istraživačku mrežu finansiranu od strane vlade Sjedinjenih Američkih Država.



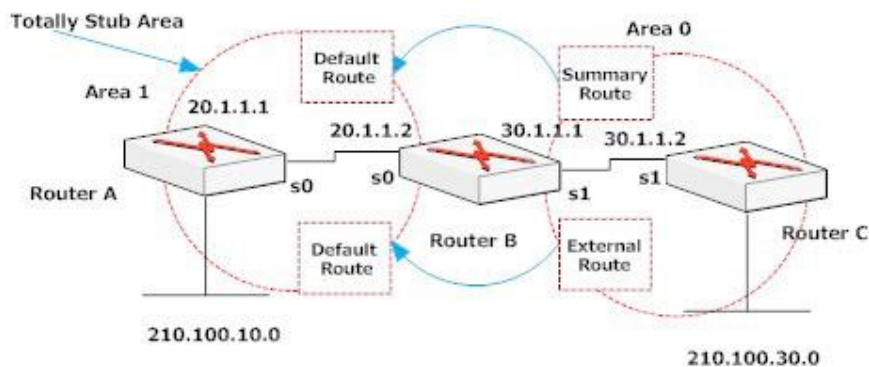
Slika 12. – Razvoj OSPF-a

Specifikacija za OSPFv1 je publikovana 1989.godine u RFC 1131. Specifikovane su dve implementacije OSPFv1, jedna za izvršavanje na ruterima a druga za izvršavanje na UNIX radnim stanicama. Kasnija implementacija UNIX verzije OSPF-a je postala naširoko rasprostranjen UNIX proces pod nazivom GATED. OSPFv1 je predstavljao eksperimentalni protokol za rutiranje i nikada nije doživeo punu primenu.

OSPFv2 je definisan u RFC 1247 od strane John Moy-a. Nova verzija OSPF je nudila znatna tehnička unapređenja u odnosu na OSPFv1. Trenutna specifikacija OSPFv2 protokola je definisana u RFC 2328.

U prethodnom poglavlju predstavljen je OSPF kao protokol za rutiranje koji se primarno koristi u Akademskoj mreži Srbije i koji je odabran kao protokol koji se koristi za rutiranje između campus mreže Medicinskog fakulteta i RCUB-a.

Uzimajući u obzir da trenutno campus mreža Medicinskog fakulteta predstavlja krajnju tačku u Akademskoj mreži Srbije javlja se mogućnost da se sama mreža pri rutiranju definiše kao kompletna stub oblast (*totally stubby area (TSA)*), čime bi se smanjilo opterećenje layer 3 svičeva pošto bi same ruting tabele bile manje. TSA kod OSPF-a se postiže tako što se na RCUB-ovom ruteru koji predstavlja granični ruter u ovoj mreži pri konfigurisanju oblasti (*area*) definiše da je to stub oblast i da se ne šalju informacije o rutama (*no-summary*). Umesto slanja paketa sa rutama u ruting tabelu *layer 3 sviča* se upisuje informacija o izlaznoj putanji (*gateway of last resort*), koja predstavlja putanju za sve pakete koji nisu namenjeni adresama iz adresnog opsega campus mreže (Slika 13.).



Slika 13. – Primer *totally stubby* oblasti

5.2 HSRP

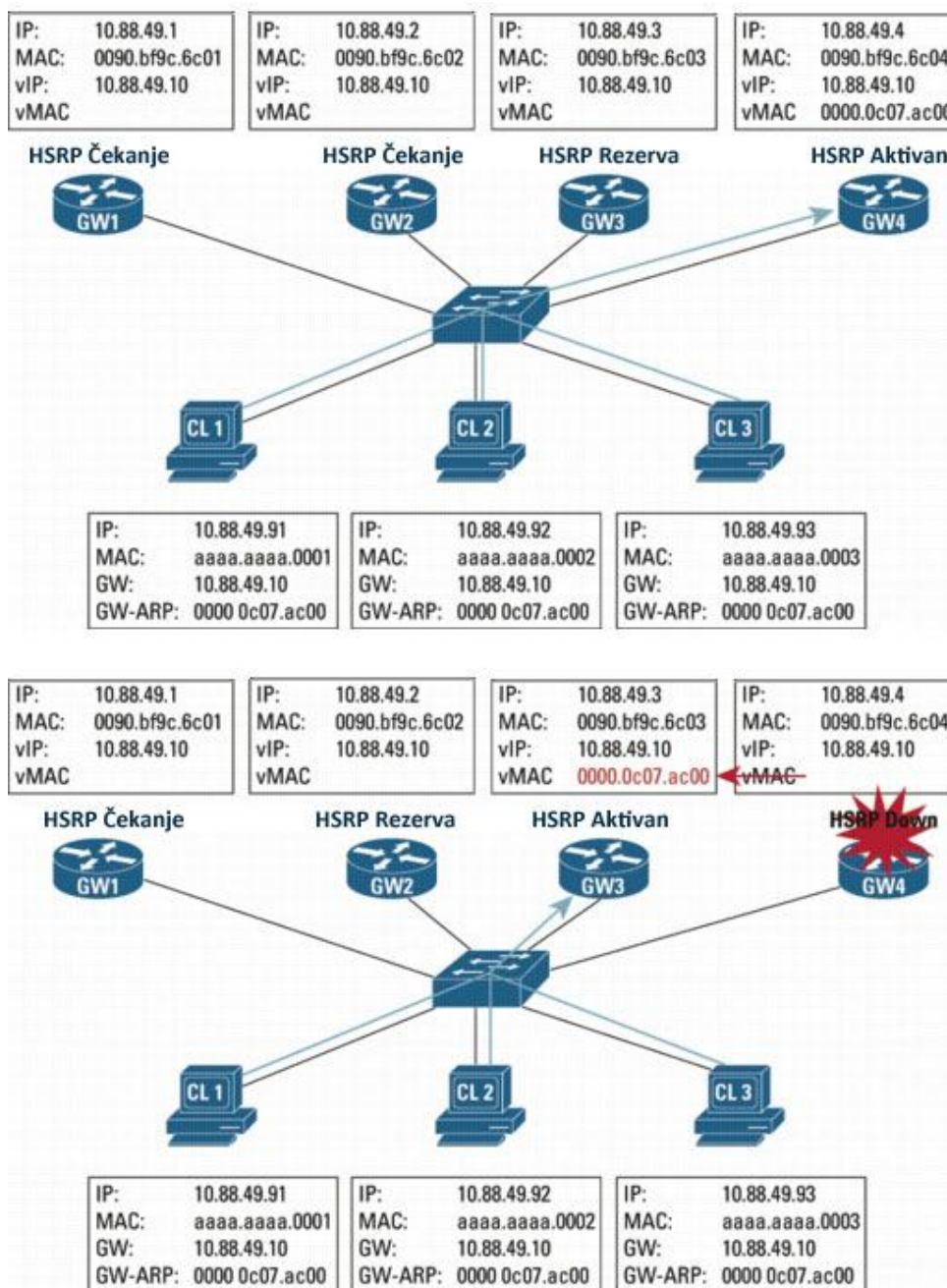
HSRP (*Hot Standby Router Protocol*) predstavlja Ciscov protokol koji se koristi za kreiranje redundantne u mrežama.

HSRP je Cisco patentirani protokol napravljen da omogući da nekoliko rutera poveže u logičku celinu koji se ponašaju kao jedan virtuelni ruter. RFC 2281 detaljnije opisuje protokol HSRP.

Pri samom kreiranju virtuelnog rutera (grupe) kojem pripadaju fizički ruteri definišu se virtuelna IP adresa i virtuelna MAC adresa. U samoj grupi ruter sa najvišim prioritetom dobija ulogu aktivnog rutera i svi paketi prosleđeni virtuelnoj IP adresi se obrađuju u ovom ruteru, sekundarni ruter je u stanju pripravnosti i u slučaju otkaza aktivnog rutera preuzima virtuelnu IP i MAC adresu i počinje da rutira pakete.

Logika koja omogućuje sekundarnom ruteru da zna kada je primarni postao nedostupan je zasnovana na tome da oba rutera razmenjuju *hello* poruke preko *multicast* adrese 224.0.0.2 po UDP portu 1985. Standardna podešavanja su da ruteri šalju poruke na 3 sekunde i ako nakon 10 sekundi ruter ne dobije *hello* poruku preuzima ulogu aktivnog rutera. Samo vreme od 10 sekundi u osetljivim mrežama u kojima se koriste video i zvuk (*voice*) predstavlja dugačak period za nedostupnost mreže. Ove vremenske intervale je moguće ručno konfigurisati ali sam proces otkrivanja neaktivnog rutera može dovesti do degradacije signala ili prekida aktivnih konekcija.

Na slici 14. prikazani su režimi rada rutera u konfigurisanoj HSRP grupi.



Slika 14. – Režimi rada rutera konfigurisanih pomoću HSRP-a

Sam način funkcionisanja HSRP-a se ogleda u tome da kada aktivni ruter u HSRP grupi postane nedostupan rezervni ruter preuzima virtuelnu IP i MAC adresu tako da klijentske mašine ne prekidaju aktivne konekcije nakon određenog perioda ne aktivnosti iste.

5.3 NTP

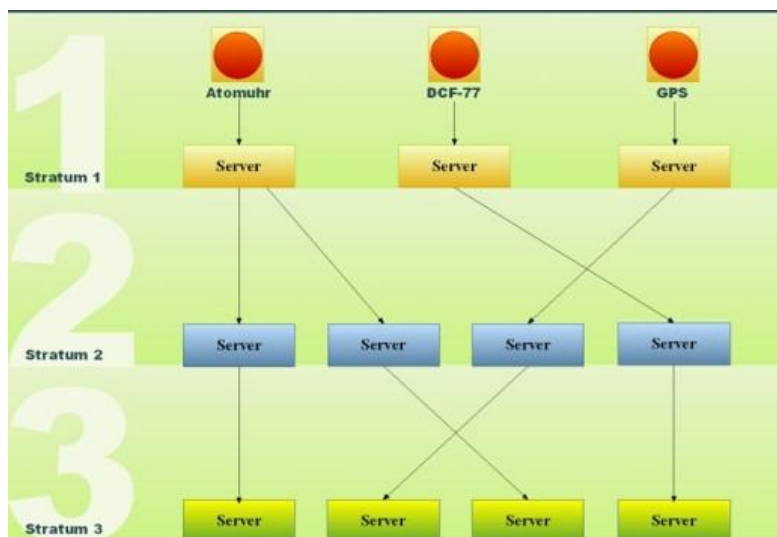
NTP (*Network Time Protocol*) predstavlja protokol i softversko rešenje za sinhronizaciju računarskih satova preko računarskih mreža. Sam protokol je prvi put definisan u RFC 958 dokumentu od strane Dejvida Milisa (*David L. Mills*), dok je poslednja verzija dokumentovana u RFC 5905. Logika na kojoj funkcioniše NTP protokol je zasnovana na Marculovom algoritmu (*Keith Marzullo*) i prestupnim sekundama. Sam protokol u sebi sadrži bufer za kašnjenje kako bi se sprečili efekti varjabilnog kašnjenja. NTP protokol koristi UDP port 123 za komunikaciju.

Sam sistem NTP servera se sastoji iz više stratuma (slojeva) vremenskih servera (Stratum 0, Stratum 1, Stratum 2).

Stratum-0 uređaji u suštini predstavljaju atomske, GPS ili radio časovnike. Sami uređaji nisu direktno povezani na mrežu već se preko RS232 sa PPS(*Pulse per signal*), signali koji se veoma precizno ponavljaju u vremenskom rasponu od 1 sekunde, portova povezuju na lokalni računar.

Stratum-1 serveri se obično nazivaju *time servers* (serveri sa kojih se sinhronizuje vreme). Ovi serveri preuzimaju informacije o vremenu od Stratum-0 uređaja i distribuiraju ih Stratum-2 uređajima.

Sami Stratum-2 uređaji čine lokalne radne stanice ili čak odvojeni NTP server u lokalnoj mreži. Sami Stratum-2 serveri preuzimaju informacije o vremenu od više Stratum-1 servera i u slučaju da se sa nekog servera šalju netačni podaci taj server se odbacuje.



Slika 15. – Hijerarhija stratum servera

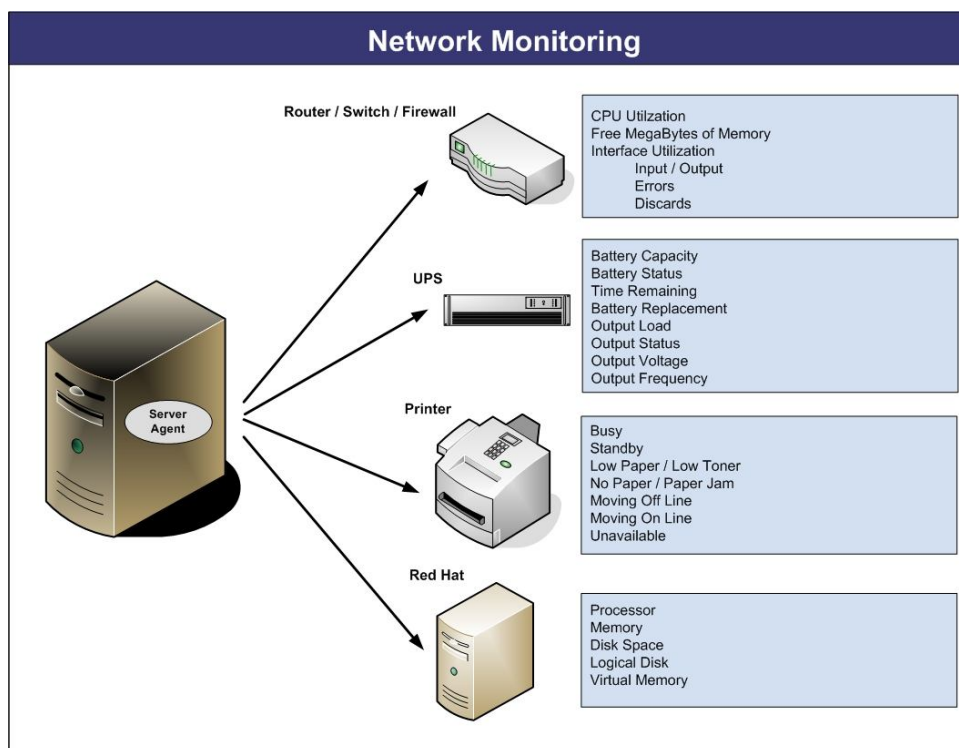
U campus mrežama NTP protokol je jedan od servisa koje je obavezno implementirati iz više razloga. Mnogi protokoli i servisi su osetljivi na razlike u vremenu podešenom npr. na klijentskom računaru i serveru. U slučaju gde je veliki broj radnih stanica i servera konfigurisati ručno oduzima mnogo vremena i nemoguće je veoma precizno podesiti vreme, kao primer može se uzeti gde usled pogrešno podešenog vremena na radnoj stanici, validan SSL sertifikat biva odbačen od strane softvera kao nevalidan. Pored radnih stanica i servera same mrežne uređaje u campus mreži je potrebno konfigurisati da uklađuju svoj časovnik sa lokalnim NTP serverom. U slučaju *firewall*-ova potrebno je konfigurisati da se vreme usklađuje sa NTP serverom ako npr. imamo situaciju gde se određena pravila aktiviraju u unapred definisanim vremenskim periodima. Takođe jedan od bitnijih razloga je što se javlja obaveza čuvanja *log* fajlova o kompletnoj komunikaciji u i van campus mreže za određeni vremenski period (3, 6 ili 12 meseci), pritom je potrebno da taj fajl sadrži i tačno vreme kada se određena komunikacija dogodila.

5.4 SNMP i monitoring

SNMP (*Simple Network Management Protocol*) je deo TCP/IP seta protokola, čija osnovna funkcija je monitoring i menadžment radnih stanica, servera, svičeva, rutera i bezbednosnih rešenja u IP mreži. Aktuelne verzije SNMP-a su SNMPv2c i SNMPv3. Sam protokol je koncipiran tako da sadrži tri elementa i to su:

- Menadžeri - softver pomoću kojeg se vrši monitoring i menadžment mrežnih uređaja),
- Agenti - uređaji koji se monitoruju,
- MIBs (*Management Information Bases*) - koji predstavljaju skup definisanih informacija koje je moguće dobiti o agentima, na osnovu kojih menadžeri vrše upravljanje i monitoring.

Sam protokol funkcioniše na UDP portovima 161 i 162. Sama komunikacija između menadžera i agenta se vrši tako što menadžment softver šalje zahteve o informacijama agentu sa bilo kog izvornog porta na port 161, dok agent odgovara menadžment softveru na portu 162. U slučaju da se koristi TLS (*Transport Layer Security*) ili DTLS (*Datagram Transport Layer Security*) koriste se portovi 10161 i 10162.

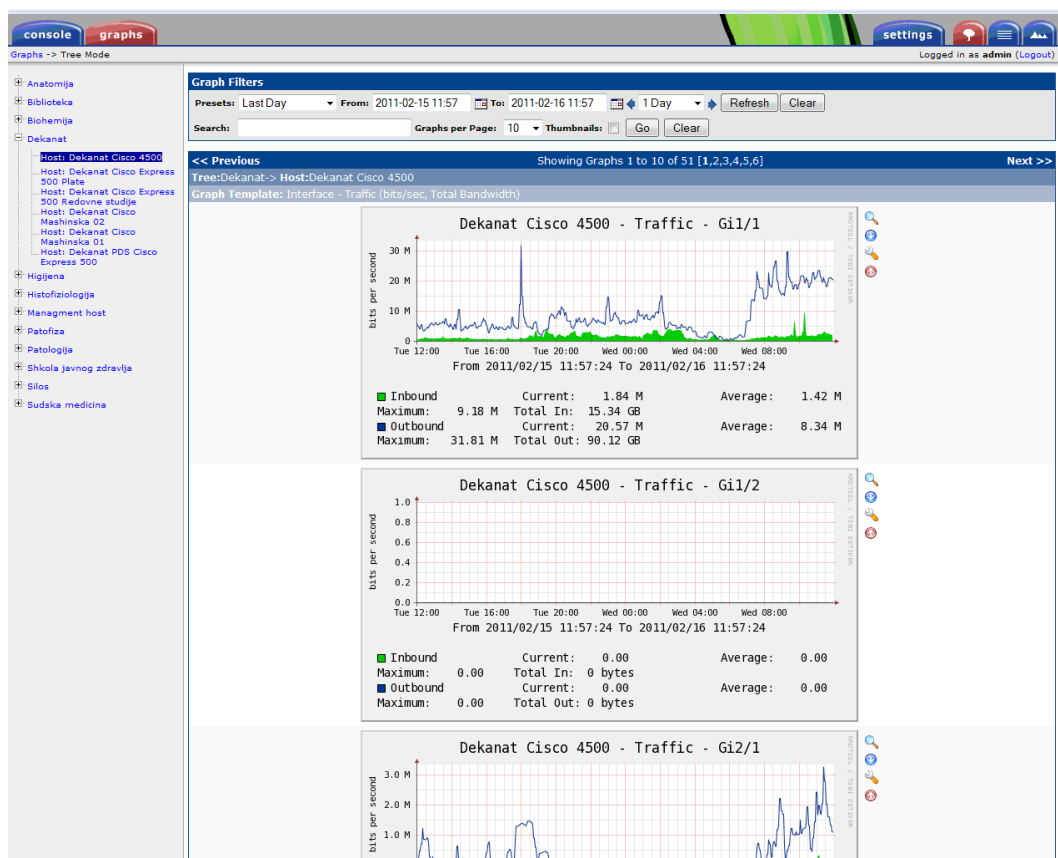


Slika 16. – SNMP monitoring

Campus mreža medicinskog fakulteta spada po veličini u srednje mreže sama kompleksnost iste iziskuje da se implementira SNMP rešenje za monitoring kako mrežnih uređaja tako i serverske infrastrukture, ups napajanja, u slučaju nabavke naprednijih rešenja za hlađenje data centra moguće je isto vršiti monitoring istih.

Kao rešenje za monitoring mrežnih resursa najjednostavnije rešenje, koje zadovoljava potrebe Medicinskog fakulteta, predstavlja alat po imenu Cacti dok za napredniji monitoring potrebno je implementirati rešenje poput Zenoss softvera za monitoring.

Cacti predstavlja kompletan grafički frontend za servis RRDTool, koji prikuplja sve neophodne informacije za kreiranje grafova i čuva ih u MySQL bazi podataka. Pored mogućnosti manipulacije i kreiranja grafova pomoću informacija iz određenih izvora Cacti nam omogućuje da sami definišemo način prikupljanja istih.



Slika 17. – Cacti grafovi

Ovaj alat nam omogućava da vršimo monitoring fakultetske mreže, kako aktivnih mrežnih uređaja kao što su ruteri i svičevi do samih servera i radnih stanica. Pri monitoringu aktivnih mrežnih uređaja možemo nadgledati svaki fizički interfejs na određenom ruteru i sviču, kao i saobraćaj na određenom VLAN-u. Pri manipulaciji grafovima moguće je pratiti informacije o promenama nastalim na sviču u vremenskom rasponu od jedne godine do jednog minuta. Sam alat ne pruža *realtime* informacije tako da je nemoguće npr. imati informaciju da li je istog trenutka određeni uređaj ili interfejs iz određenog razloga postao nedostupan.

Poput Cacti grafičkog alata, Zenoss nam pruža mogućnost da pratimo sve informacije vezane za mrežne uređaje nad kojima se vrši monitoring uz mogućnost proširenja MIB baze podataka kako bi se definisale dodatne informacije koje želimo da pratimo.

6 BEZBEDNOST

Krajem devedestih godina koncept bezbednosti računarskih mreža se zasnivao na odbrani od malicioznih korisnika čiji napadi potiču sa spoljne mreže, Interneta. U modernim mrežama veći deo napada potiče od unutrašnjih korisnika, kako zlonamernih tako i slučajnih. Kako bi se sprečila kompromitacija mreže i servisa koji se koriste unutar iste potrebno je implementirati više bezbednosnih rešenja.

6.1 Firewall

Rešenje koje je odabrano za implementaciju kao hardverski *firewall* u campus mreži Medicinskog fakulteta su dva Cisco ASA 5520 uređaja čije tehničke karakteristike su prikazane u Tabeli 7.

Cisco ASA 5500 Series Model/License	Cisco ASA 5520
Network Location	Internet Edge
Performance Summary	
Maximum Firewall throughput	450 Mbps
Maximum Firewall Connections	280,000
Maximum Firewall Connections/Second	12,000
Packets Per Second (64 byte)	320,000
Maximum 3DES/AES VPN Throughput	225 Mbps
Maximum Site-to-Site and IPsec IKEv1 Client VPN User Sessions	750
Maximum AnyConnect or Clientless VPN User Sessions	750
Bundled SSL VPN User Session	2
Technical Summary	
Memory	2 GB
Minimum System Flash	256 MB
Integrated Ports	4-10/100/1000, 1-10/100 +4-10/100/1000, 4 SFP (with 4GE SSM)
Maximum Virtual Interfaces (VLANs)	150
Expansion Capabilities	
SSC/SSM/ICs Expansion	1-SSM

SSC/SSM/ICs Supported	CSC SSM, AIP SSM, 4GE SSM
Intrusion Prevention	Yes (with AIP SSM)
Concurrent Threat Mitigation Throughput (Mbps) (Firewall + IPS Services)	225 (with AIP SSM-10) 375 (with AIP SSM-20) 450 (with AIP SSM-40)
Content Security (Anti-virus, Anti-Spyware, File Blocking)	Yes (with CSC SSM)
Maximum Number of Users for Anti-virus, Anti-spyware, File Blocking (CSC SSM only)	500 (CSC-SSM-10) 1000 (CSC-SSM-20)
Content Security Plus License features	Anti-spam, anti-phishing, URL filtering
Features	
Cisco Adaptive Security Appliance Software Version (latest)	8.4
Application-layer Firewall Services	Yes
Layer 2 Transparent Firewalling	Yes
Security Contexts (included/maximum)¹	2/20
GTP/GPRS Inspection¹	Yes
High-availability Support²	A/A and A/S
SSL and IPsec VPN Services	Yes
VPN Clustering and Load Balancing	Yes
Advanced Endpoint Assessment¹	Yes

Tabela 7. – Tehničke karakteristike Cisco ASA 5520 uređaja

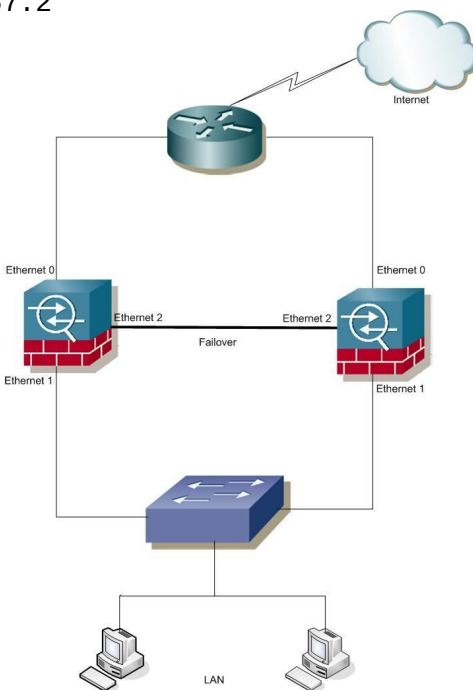
Cisco ASA podržava dva *firewall* režima rada i to su transparentni i rutirajući režim. U rutirajućem režimu rada *inside*(interfejs kad *campus* mreži) i *outside*(interfejs ka spoljnoj/internet mreži) imaju definisane IP adrese tj. uređaj funkcioniše na mrežnom nivou(layer 3). U ovom modu se takođe rutira saobraćaj između Cisco ASA-e i centralnog sviča fakultetske mreže i RCUB-ovog rutera/sviča. Da bi se smanjilo opterećenje Cisco ASA-e dodatnim rutiranjem pretežno se implementira statičko rutiranje. U transparentnom režimu rada Cisco ASA funkcioniše na nivou veze(layer 2) tj. *inside* i *outside* interfejsi nemaju definisane IP adrese. Ovaj režim rada je poznat i kao *stealth* ili *bump-in-a-wire* firewall zato što iako funkcioniše na nivou veze ovaj uređaj vrši inspekciju saobraćaja na mrežnom nivou tj. po IP adresama. Takođe u oba slučaja moguće je koristiti IP pristupne liste za definisanje dozvoljenog saobraćaja između fakultetske mreže i Internet-a.

VPN i NAT funkcionalnosti je moguće koristiti samo u rutirajućem režimu rada zato što je potrebno da uređaj ima definisane IP adrese na svojim interfejsima kako bi bio vidljiv sa spoljne mreže, tj. Internet-a. Kako bi se izbeglo dodatno opterećenje samih Cisco ASA uređaja VPN i NAT rešenja je potrebno implementirati kao odvojene servise u sklopu fakultetske mreže.

U *campus* mrežu Medicinskog fakulteta potrebno je postaviti dva Cisco ASA 5520 uređaja u *failover* režimu rada. Ovaj režim rada se konfiguriše da bi omogućio u slučaju otkaza

glavnog Cisco ASA uređaja da pomoćni uređaj preuzme ulogu aktivnog *firewall-a*. *Failover* se realizuje tako što se Cisco ASA-e povežu i definiše se određeni mrežni opseg u kojem su konfigurisani interfejsi preko kojih su ovi uređaji povezani. Postoje dva režima rada ovih uređaja u *failover* podešavanjima i to su *Active/Active* i *Active/Standby*. U *Active/Active* režimu rada oba uređaja su aktivna tj. propuštaju mrežni saobraćaj dok u *Active/Standby* režimu rada samo aktivni(primarni) uređaj propušta mrežni saobraćaj. Takođe postoje dva moda *failover-a* i to su *statefull* i *regular failover*. U *regular failover* modu pri prestanku rada primarnog uređaja sve konekcije se prekidaju, dok u *statefull failover* modu primarni uređaj konstantno šalje informacije o ostvarenim konekcijama sekundarnom uređaju kako u slučaju prestanka rada primarnog uređaja ne bi došlo do prekida konekcija. U sledećem primeru je prikazana konfiguracija *failover* opcije na Cisco ASA 5520 uređajima u fakultetskoj mreži:

```
ip address 147.91.119.3 255.255.255.240 standby 147.91.119.4
failover
failover lan unit secondary
failover lan interface Failover_int GigabitEthernet0/3
failover link Failover_int GigabitEthernet0/3
failover interface ip Failover_int 192.168.157.1 255.255.255.252
standby 192.168.157.2
```



Slika 17. – Realizacija failovera između dve Cisco ASA-e

Pri konfiguraciji pristupnih listi postoje dva tipa i to su *inside* i *outside* pristupne liste koje su u suštini produžene pristupne liste i postavljaju se na *inside* odnosno *outside* interfejs. Kao i u ruterima i svičevima na krajevima ovih listi se nalazi eksplicitno odbijanje kompletnog mrežnog saobraćaja.

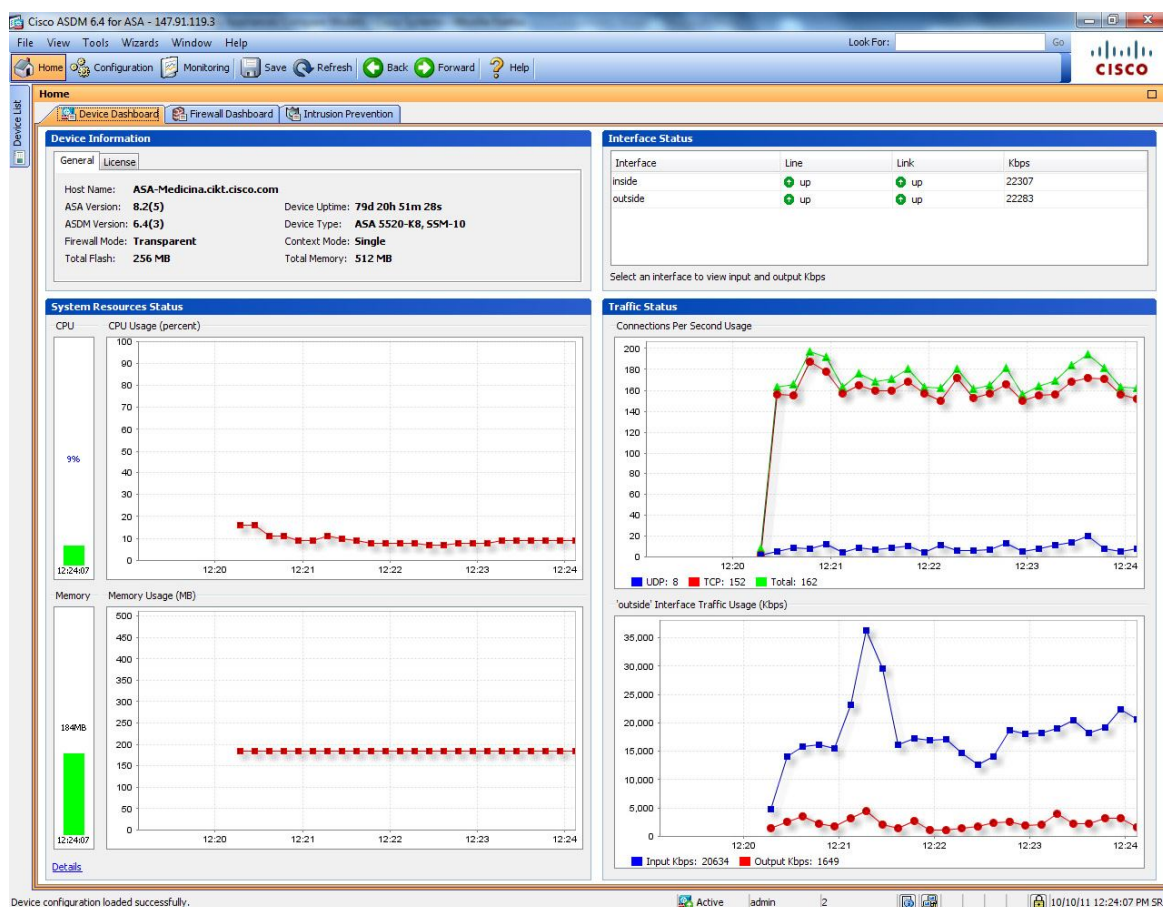
Pored samih pristupnih listi potrebno je implementirati i *real-time* bezbednosno rešenje u vidu IPS senzora koji se ugrađuje kao dodatni modul u sam Cisco ASA uređaj. Odabrano rešenje je Cisco ASA AIP SSM-10 čije tehničke karakteristike su prikazane u Tabeli 8.

Feature	Cisco ASA AIP SSM-10
	
Concurrent threat mitigation throughput (firewall and IPS services)	• 150 Mbps with Cisco ASA 5510 • 225 Mbps with Cisco ASA 5520
Global Correlation support	• Yes
Threat protection	• 25,000+ threats
Day-zero protection with anomaly detection	• Yes
Custom signature support	• Yes
Virtual sensors	• 4
Technical Specifications	
Memory	1 GB
Flash	256 MB

Tabela 8. – Tehničke karakteristike predloženog IPS modula

Sam modul se konfiguriše odvojeno od Cisco ASA uređaja tj. poseduje sopstvenu menadžment IP adresu.

Jedna od prednosti korišćenja Cisco ASA uređaja je i mogućnost konfiguracije i monitoringa iste uz pomoć Cisco-vog softverskog rešenja Cisco ASDM (*Adaptive Security Device Manager*).



Slika 18.- Cisco Adaptive Security Device Manager

6.2 Proxy

Samo postavljanje hardverskog *firewall* rešenja nije dovoljno fleksibilno za kontrolisanje krajnjih korisnika campus mreže. Kako bi se omogućilo centralizovana kontrola web aktivnosti korisnika campus mreže Medicinskog fakulteta potrebno je prvo pomoću pristupnih listi na *firewall*-u zabraniti sav saobraćaj kad spoljnim mrežama a potom implementirati *proxy server*.

Proxy server predstavlja posrednika između klijentske mašine i resursa na udaljenoj mreži. Kada klijentska mašina pošalje zahtev za resursom sa udaljene lokacije, fajl, web stranica ili neki drugi resurs, server, u slučaju da je konfigurisan kao transparentni *proxy server*, presreće taj zahtev i u zavisnosti od predefinisanih pravila za filtriranje prosleđuje ga ili odbacuje. Prednosti korišćenja *proxy servera* su:

- Da se klijenti koji koriste *proxy server* ostanu anonimni pri slanju zahteva, najviše zbog bezbednosti,
- Da se ubrza pristup resursima (koristeći keširanje). Web *proxy*-ji se najčešće koriste za keširanje web stranica sa web servera,
- Da bi se primenila polisa pristupa mrežnim servisima ili sadržajima, npr. blokiranje pristupa određenim sajtovima,
- Da se prate aktivnosti korisnika na Internetu i pomoću istog generiše izveštaj,
- Da bi se skenirao prenešeni sadržaj u slučaju da sadrži maliciozni kod,
- Da se omogući skeniranje odlaznog saobraćaja u slučaju, kako bi se primera radi sprečilo curenje informacija iz organizacije.

Squid (web proxy server) je alat koji zadovoljava potrebe campus mreže ove veličine. *Squid* je prvenstveno keš *proxy server* namenjen kontroli pristupa Web-u i podržava protokole kao što su FTP, HTTP, HTTPS. Sam način funkcionisanja servera pomoću keširanja web sadržaja omogućava smanjivanje opterećenja spoljnog linka tako što kešira često posećivane sajtove i na taj način krajnjim korisnicima u lokalnoj mreži pruža dodatno brži pristup traženim resursima. U *Tabeli 9.* dat je primer konfiguracije *proxy servera Squid* koji je implementiran na nekoj od besplatno dostupnih Linux OS distribucija.

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl purge method PURGE
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
acl MEDNET src 147.91.112.0/20 192.168.0.0/22
acl SECNET src 192.168.14.0/24
acl SECNETDST dst 192.168.14.0/24
acl VPNNET src 192.168.13.0/24
acl ftp proto FTP
acl http proto HTTP
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow SECNET SECNETDST
http_access deny SECNETDST
http_access allow MEDNET
http_access allow SECNET
http_access allow VPNNET
http_access allow MEDNET ftp
http_access allow SECNET ftp
http_access allow VPNNET ftp
http_access allow MEDNET http
http_access allow SECNET http
http_access allow VPNNET http
http_access allow localhost
http_access deny all
http_reply_access allow all
icp_access deny all
http_access deny all
icp_access allow all
http_port 8080 transparent
hierarchy_stoplist cgi-bin ?
cache_mem 16 MB
maximum_object_size_in_memory 32 KB
cache_dir aufs /var/spool/squid 50000 16 256
access_log /var/log/squid/access.log squid
cache_store_log none
ftp_user proxy@med.bg.ac.rs
acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY
refresh_pattern ^ftp:      1440 20% 10080
refresh_pattern ^gopher:   1440 0% 1440
refresh_pattern .          0 20% 4320
```

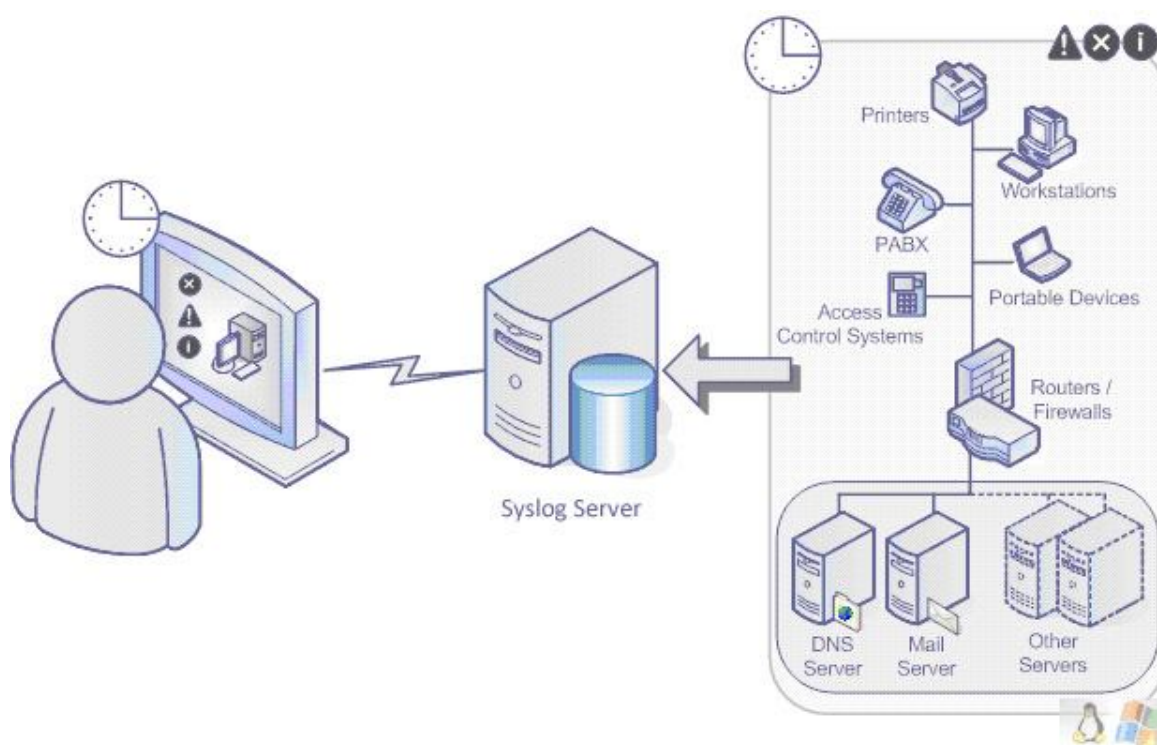
```
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
ie_refresh on
extension_methods REPORT MERGE MKACTION CHECKOUT
hosts_file /etc/hosts
coredump_dir /var/spool/squid
```

Tabela 9. – Primer konfiguracije proxy servera

6.3 Syslog

Zbog same kompleksnosti i broja korisnika potrebno je implementirati i rešenje pomoću kojeg bi se u slučaju nekih nepredvidljivih situacija poput otkaza nekog mrežnog uređaja, povrede pravila korišćenja računarske mreže, dokumentovao sam događaj. Rešenje koje nam pruža tu mogućnost predstavlja Syslog proces.

Sam proces se zasniva na tome da se važne informacije i opisi nekih dešavanja čuvaju lokalno na radnoj stanici, mrežnom uređaju ili na udaljenom serveru.



Slika 20. – Syslog server

Pored logovanja informacija vezanih za mrežne uređaje i protokole, dodatni razlog za uvođenje log servera je kako bi se na centralizovanoj lokaciji čuvali logovi vezani za određene aplikacije i servise dostupne u fakultetskoj mreži kako bi se u slučaju kompletnog prestanka funkcionisanja nekog od njih imao uvid u dešavanja koja su prethodila samom prestanku funkcionisanja.

Sam syslog protokol koristi UDP port 514, na aplikacionom nivou syslog server ne generiše odgovore na primljene poruke tako da sami uređaji konstantno šalju generisane log poruke bez obzira da li ih definisani server prihvata.

Moguće je identifikovati i koristiti osam različitih nivoa poruka od kojih najniži nivo (0) predstavlja najkritičniju poruku kao što je otkazivanje kompletnog sistema dok najviši nivo (7) predstavlja logovanje svih dešavanja na uređaju. Nivoi poruka koje je moguće koristiti su sledeći:

0 – *Emergency*, 1 – *Alert*, 2 – *Critical*, 3 – *Error*, 4 – *Warning*,

5 – *Notification*, 6 – *Informational*, 7 – *Debug*.

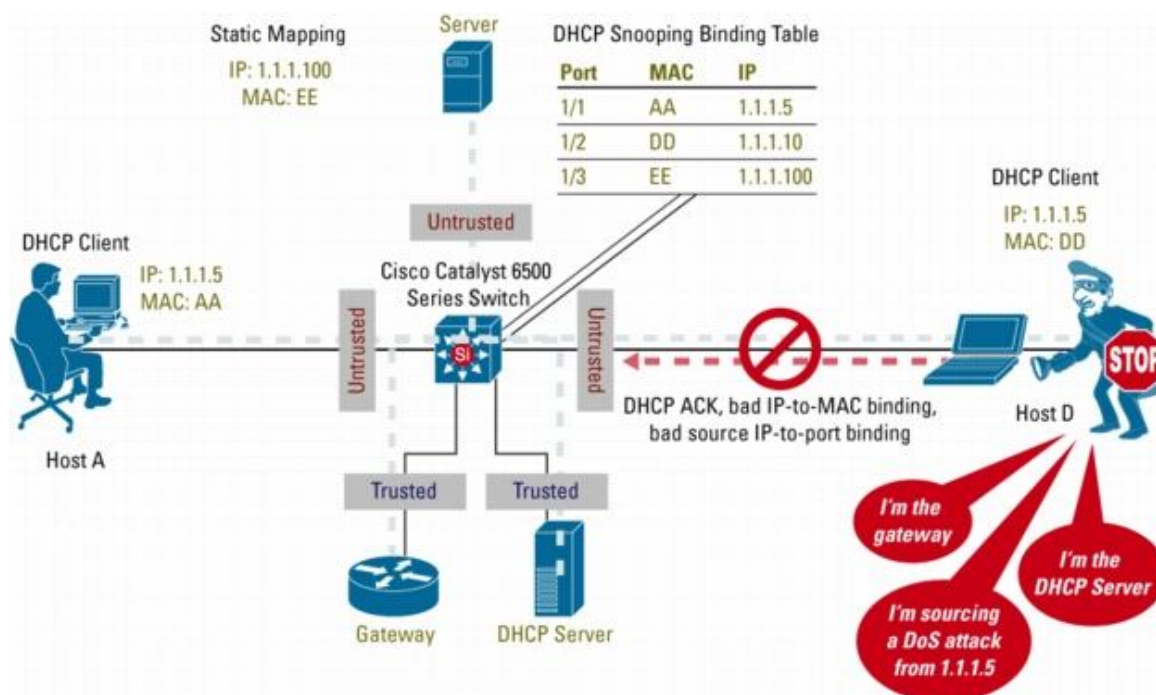
Format syslog poruka na Cisco-vim uređajima je sledeći:

mm/dd/yyyy:hh/mm/ss:facility-severity-MNEMONIC:Message-text

```
*Mar    6  22:48:34.452 UTC: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Loopback0,changed state to up
```

6.4 DHCP Snooping

U jednu od mera unutrašnje bezbednosti mreže spada *DHCP snooping*. Unutrašnja bezbednost računarske mreže predstavlja trenutno visok prioritet za zaštitu iz same činjenice da do napada ili nefunkcionisanja same mreže može doći i iz neadekvatnog priključivanja mrežnih uređaja na fakultetsku campus mrežu, poput priključivanja *SOHO* rutera kojem na njegovom LAN portu i usled čega on počinje da deli neispravne DHCP odgovore. Sam servis nam pruža mogućnost da definišemo koji port na sviču može da odgovara/prosleđuje odgovore na DHCP zahteve. Portovi se u ovom slučaju dele na sigurne (*trusted*) i nesigurne (*untrusted*) portove. U slučaju da se na nesigurnom portu pojavi DHCP odgovor na poslato zahtev sistem automatski isključuje port.



Slika 21. – DHCP Snooping

Pri samoj konfiguraciji portova u mreži potrebno je obratiti pažnju da se pored porta na koji je povezan zvanični DHCP server, *trunk* portovi kad ostalim svičevima takođe definišu kao sigurni portovi kako bi prosleđivali DHCP odgovore.

6.5 SSH

Sa sve većom dostupnošću alata za analizu mrežnog saobraćaja potrebno je implementirati enkriptovanu komunikaciju na lokacijama na kojima presretanje komunikacije može da dovede do kompromitacije računarske mreže i servisa.

Potrebno je da na svim mrežnim uređajima i serverima omogućiti pristup samo pomoću protokola koji obezbeđuju dovoljan nivo zaštite od napadača.

Da bi se to ostvarilo potrebno je da svi uređaji podržavaju SSH protokol verzije 2. Prva verzija SSH protokola je razvijena od strane Tatu Ilonena (*Tatu Ylönen*), istraživača sa Helsinškog Tehnološkog Univerziteta, kao zamena za rlogin, telnet i rsh protokole koji nisu obezbeđivali dovoljan nivo autentifikacije i zaštite.

Jedan od glavnih razloga implementacije ovog protokola je kako bi se sprečilo „prisluškivanje“ komunikacije, poput konfiguracije udaljenih svičeva i servera ili prebacivanje log fajla na syslog server. Pri samoj implementaciji SSH-2 protokola potrebno je da pri kreiranju ključa (*key*) se koristi RSA algoritam čiji modul mora da iznosi minimalno 1024 bita.

Svi prethodno definisani uređaji i protokoli moraju da podrže i SSH-2 protokol.

7 SERVERSKA INFRASTRUKTURA

7.1 Postojeća infrastruktura

Analizom postojeće serverske infrastrukture na Medicinskom fakultetu javila se potreba za kreiranjem i implementacijom kompletno nove infrastrukture. Uzimajući u obzir da je u prethodnih 5 godina povećan obim servisa koji su dostupni zaposlenima i studentima u okviru fakulteta iz priložene Tabele 10. se vidi da trenutni kapaciteti, zastarelost i sama organizacija postojećih servera predstavlja potencijalni problem u daljoj implementaciji novih servisa i nadogradnji postojećih.

Uzimajući u obzir da trenutna infrastruktura je neefikasna u iskorišćenju postojećih resursa, samo rešenje se nalazi u implementaciji novih serverskih tehnologija u kombinaciji sa virtuelizacijom.

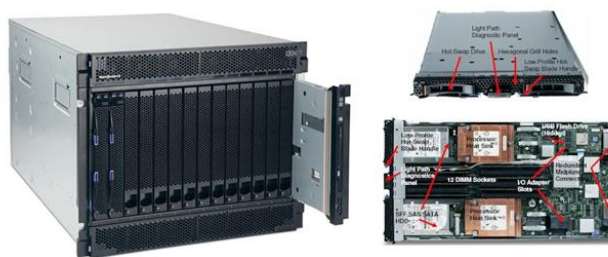
Proizvođač	Model	Broj CPU (jezgara)	CPU brzina GHz	Kapacitet RAM (GB)	Tip diskova SATA/SCSI	Broj diskova	Ukupan kapacitet diskova(GB)
HP	Proliant DL310 G5	1(2)	2.13	1	SATA	2	160
HP	Proliant DL310 G5	1(2)	2.13	1	SATA	2	160
HP	Proliant DL380 G5	1(4)	2.83	8	SAS	6	540
IBM	x3500	2(8)	1.6	8	SATA	6	500
Inspur	NF5520	2(8)	2.13	4	SATA	6	640
Inspur	NF5520	2(8)	2.13	4	SATA	6	640
Inspur	NF290D2	2(8)	2.33	16	SATA	4	500
Inspur	NF290D2	2(8)	2.33	16	SATA	3	500

Tabela 10. – Aktuelna serverska infrastruktura na Medicinskom fakultetu

7.2 Blade arhitektura

Blade serveri predstavljaju novi oblik organizacije serverske infrastrukture koji odlikuje visoka gustina servera, storage sistema i komunikacione opreme. Unapred odredjenje veze izmedju napajanja, hladjenja i komunikacionih uređaja značajno olakšavaju upravljanje infrastrukturom i donose uštede u toku održavanja sistema. Za razliku od klasičnih servera koji se postavljaju horizontalno, blade serveri se najčešće postavljaju vertikalno u blade šasiju. Blade šasija omogućava napajanje servera i njihovu interkonektivnost sa ostatkom računarske infrastrukture. Ovakav pristup omogućava jednostavno dodavanje novih servera u infrastrukturu uz minimalno učešće administratora sistema.

Pored navedenih prednosti koje se odnose na fizički sistem, veliku prednost blade serverima donosi i sistem objedinjenog upravljanja šasijom i svim komponentama koje se nalaze u njoj. Administrator kroz jedan interfejs može nadgledati sve komponente sistema i na taj način efikasnije upravljati sa infrastrukturom.



Slika 22. – Blade arhitektura

Ključne prednosti blade servera:

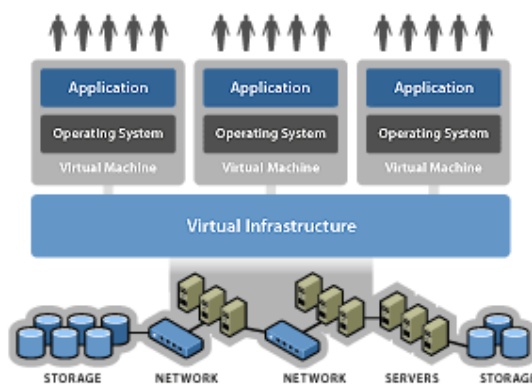
- Ušteda u prostoru koja omogućava veliku računarsku snagu u okviru malog prostora,
- Konsolidacija servera u cilju poboljšanja upravljivosti serverima i ključnim komponentama,
- Smanjenje kompleksnosti sistema uvođenjem modularnosti, jednostavnom integracijom, unapred prežičenim komponentama, deljenjem zajedničkih resursa (napajanje, hladjenje) itd.,
- Brzi povratak investicije kroz nižu ukupnu cenu troškova (nabavka + održavanje).

7.3 Virtuelizacija

Virtuelizacija pruža mogućnost da se na jednom serveru istovremeno izvršava više operativnih sistema. Svaki od ovih sistema je izolovan i ne ugrožava ostale sisteme. Na ovaj način se postiže konsolidacija velikog broja servera na malo hardvera. Pored očiglednih ušteda u hardveru koje se postižu na ovaj način, nastaju uštede u operativnim troškovima kao što su napajanje, hladjenje, održavanje i uštede u prostoru.

Iako je inicijalna ideja virtuelizacije bila ušteda u gore navedenim aspektima, danas se virtuelizacija koristi i za realizovanje sistema visoke dostupnosti. Kreiranje sistema visoke dostupnosti korišćenjem virtuelizacije je vrlo jednostavno i već je implementirano u skoro svakom virtuelizovanom okruženju.

Kreiranje novih virtuelnih mašina sa operativnim sistemom je daleko brže nego u slučaju fizičkih servera. Ovo omogućava IT službi da se brzo prilagodi zahtevima koje im rukovodstvo i biznis nalažu.



Slika 23. - Virtuelizacija

Ključne prednosti virtuelizacije:

- Konsolidacija resursa,
- Veća pouzdanost i kontinuitet u radu aplikacija,
- Visok nivo upravljivosti računarskim resursima.

Kombinacija blade servera i virtuelizacija pruža maksimalnu fleksibilnost u upravljanju infrastrukturom. Sa jedne strane unapredjeno i efikasno upravljanje u hardveru kroz blade servere, a sa druge strane mogućnost pokretanja operativnih sistema u okviru virtuelnog sistema. Komplementarnost ovih tehnologija je pravi katalizator u revolucionarnom unapredjivanju današnjih računarskih centara. Računarski resursi će biti dopremljeni kada budu potrebni, koliko god budu potrebni, na mestu na kom su potrebni i vrlo lako će se po zahtevu ukloniti. Primenom ovih tehnologija se uspostavlja novi, viši nivo kontrole računarskih resursa.

7.4 Tehničke specifikacije rešenja za nov Data Centar

7.4.1 Blejd server rešenje

Blejd sistem rešenje mora podržavati servere bazirane na x86-64 Intel i AMD procesorima, kao i servere sa podrškom za RISC procesore (npr. Itanium, POWER, SPARC itd.)

Rešenje mora inicijalno da podržava kapacitet za minimum 10 blejd servera pune visine (full-high) sa redundantnim signalnim konekcijama između blejd servera i blejd šasije.

Rešenje mora da bude u potpunosti opremljeno redundantnim komponentama sistema za napajanje i hlađenje za pun kapacitet blade sistema.

Rešenje mora da omogući funkcionisanje svih ethernet i SAS konekcija u svakom od blejd servera i njihovu povezanost sa eksternim uređajima van blejd šasije putem odgovarajućih ethernet i SAS svičeva. Ethernet svičevi moraju biti minimum gigabit ethernet, moraju imati eksterne RJ45 konektore i moraju podržavati 802.1q protokol. Ethernet i SAS svičevi moraju biti redundantni.

Rešenje inicijalno mora da sadrži minimum 3 blejd servera pune visine (full-height) sa redundantnim signalnim konekcijama i sa sledećom konfiguracijom (tehnički minimum):

- a) 2 x Intel Xeon 5620 ili ekvivalent,
- b) 6 x 2GB RAM DDR3,
- c) 6 x 4GB RAM DDR3,
- d) 4 x 1Gb Ethernet port,
- e) 2 x SAS port za povezivanje na storidž sistem,
- f) 1 x USB memorija sa preinstaliranim programskim rešenjem za virtuelizaciju servera.

7.4.2 Sistem za skladištenje podataka za blejd server rešenje

Rešenje mora sadržati sistem za skladištenje podataka koji ima ugrađena dva kontrolera sa po minimum 1GB cache memorije po kontroleru. Kontroleri moraju podržavati redundantni režim rada.

Takođe mora sadržati sistem za skladištenje podataka koji se putem SAS konekcija povezuje na blejd server sistem.

Sistem za skladištenje podataka mora posedovati mogućnost kreiranja RAID 1,5 i 10 nizova.

Sistem za skladištenje podataka mora sadržati minimum 24 6Gb SAS diska sa pojedinačnim kapacitetom od minimum 300GB koji rade na minimalnoj brzini obrtanja 10,000 rpm.

Sistem za skladištenje podataka mora biti proširiv do minimalno 192 diska.

Sistem za skladištenje podataka mora sadržati sve potrebne licence za povezivanje sa ponuđenim blejd serverima i ponuđenim softverom za virtuelizaciju.

7.4.3 Rek ormar za smeštanje opreme

Ormar mora biti minimalne visine 42U i minimalnih dimenzija osnove 600 x 1000 mm (ŠxD). Ormar mora imati i prednja i zadnja perforirana vrata, stim što prednja treba da imaju bravu. Ormar mora da bude takve konstrukcije da omogućava nesmetan pristup opremi i sa prednje i sa zadnje strane.

Sav ponuđeni hardver mora biti od istog proizvođača. Umesto navedene SAS konekcije za pristup sistemu za skladištenje podataka, ponuđač može ponuditi alternativno tehničko rešenje (npr. Fibre Channel ili 10Gb iSCSI).

7.4.4 Softver za virtuelizaciju servera

Potrebno je ponuditi licence za 6 fizičkih procesora sa po 4 procesorska jezgra i menadžment aplikacijom za minimum 3 fizička servera.

Tip ponuđenih licenci ne sme posedovati ograničenja u pogledu broja fizičkih procesora po jednom fizičkom serveru.

Softver mora posedovati hipervizor koji radi nezavisno od operativnog sistema (bare metal hypervisor).

Softver inicijalno treba da sadrži sledeće funkcionalnosti:

- a) Kreiranje virtualnih mašina sa 4 virtuelna procesora,
- b) Dodavanje hard diskova i mrežnih karti u virtuelnu mašinu u toku rada virtuelne mašine,
- c) Podešavanje sistema visoke dostupnosti virtualnih mašina – High Availability,
- d) Migracija virtualnih mašina sa servera na server bez isključivanja virtuelne mašine,
- e) Ušteda prostora na disku alociranjem prostora po potrebi – Thinprovisioning,

- f) Praćenje verzija softvera za virtualizaciju i automatsko ažuriranje u cilju povećanja bezbednosti i dodavanja novih funkcionalnosti,
- g) Softver za automatsko pravljenje sigurnosnih kopija(backup) virtualnih mašina u cilju sprečavanja gubljenja podataka. Sistem u startu mora posedovati ovu funkcionalnost za minimalno 100 virtuelnih mašina. Sistem mora sadržati i mogućnost uklanjanja duplo skladištenih podataka (deduplikacija). Softver mora podržavati opciju da se integriše sa menadžment okruženjem samog sistema za virtuelizaciju,
- h) Programski interfejs (API) za komunikaciju sa proizvođačima bekap softvera u cilju jednostavnije integracije.

Softversko rešenje i licence moraju posedovati mogućnost nadogradnje kako u pogledu količine procesorskih licenci i menadžment softvera, tako i u pogledu funkcionalnosti. Funkcionalnosti koje softver mora podržavati u naprednim verzijama su:

- a) Mogućnost nadogradnje rešenja sa funkcionalnostima dinamičkog upravljanja resursima kroz automatsko balansiranje opterećenja servera u slučaju preopterećenosti pojedinačnih servera,
- b) Mogućnost migracije fajlova virtuelnih mašina u toku rada virtuelne mašine,
- c) Mogućnost instalacije distribuiranog sviča u cilju jednostavnije administracije mrežnih resursa u virtualnom okruženju,
- d) Mogućnost unifikacije konfiguracija i provera usklađenosti konfiguracija virtuelizovanih servera.

Uz licence je potrebno isporučiti i uslugu godišnjeg održavanja softvera i tehničku podršku proizvođača softvera za minimalni period od jedne godine.

Rešenje treba da obuhvati i sledeće aktivnosti oko instalacije i puštanja u rad sistema na lokaciji korisnika:

- a) Isporuka, montaža i puštanje opreme u rad,
- b) Povezivanje isporučene opreme na postojeći UPS sistem u server sobi,
- c) Povezivanje sistema za skladištenje podataka sa blejd server rešenjem,
- d) Konfiguracija sistema za skladištenje podataka koja uključuje kreiranje logičkih diskova, mapiranje logičkih diskova na servere i podešavanje rezervnih diskova za slučaj otkaza,
- e) Povezivanje blejd server sistema u postojeću računarsku mrežu,
- f) Instalacija i konfiguracija softvera za virtuelizaciju uključujući instalaciju menadžment komponente, podešavanje sistema visoke dostupnosti, integracija sa postojećom računarskom mrežom, podešavanje potrebno za migraciju virtuelnih mašina i inicijalno postavljanje aplikacije za izradu sigurnosnih kopija virtuelnih mašina,
- g) Obuka korisnika za korišćenje blejd server sistema, sistema za skladištenje podataka i softvera za virtuelizaciju,

- h) Dokumentacija o izvršenoj isporuci opreme, izvršenim aktivnostima na instalaciji i puštanju u rad sistema i održanoj obuci korisnika.

7.5 Realizovano rešenje

Rešenje koje u potpunosti zadovoljava prethodno navede tehničke specifikacije i funkcionalnosti je u vidu IBM eServer BladeCenter H šasije koja podržava do 14 blejd servera pune veličine i potpuno redundantne komponente (napajanje,konekcije,hlađenje). Serveri IBM HS22 su u skladu sa navedenim specifikacijama za servere koje je potrebno implementirati u samu šasiju. Pored samih servera i šasije tu se nalaze i moduli poput:

- IBM BladeCenter SAS Connectivity Module,
- IBM BladeCenter H 2980W AC Power Modules w/Fan Pack,
- Multi-Switch Interconnect Module for IBM BladeCenter,
- Server Connectivity Module for IBM BladeCenter,
- IBM UltraSlim Enhanced SATA Multi-Burner.

Kako bi se ispunio uslov da sva oprema mora da bude od istog proizvođača, sistem za skladištenje podataka koji ispunjava sve karakteristike je IBM System Storage DS3524 u koji je potrebno ugraditi 24 SAS HDD-a 2,5“ kapaciteta 300GB. Zajedno sa IBM NetBAY rek ormanom, u koji se postavlja oprema, hardverska platforma je kompletirana.

Što se tiče softverske platforme za vitruelizaciju kompletnu funkcionalnost i ispunjenost prethodno navedenih specifikacija, ispunjava VMware vSphere 5 Standard i VMware vCenter Server 5 Foundation kao kompletno rešenje za virtuelizaciju.

8 TELEKOMUNIKACIJE

Ovo poglavlje predstavlja rezultat analize trenutnog stanja telefonske mreže Medicinskog fakulteta Univerziteta u Beogradu. U sledećim podsekcijama je dat kratak opis postojeće telefonske infrastrukture i predlog ugradnje nove centrale koja bi predstavljala centralno čvorište u telefonskoj mreži i mogućnosti za implementaciju CTI servisa koje podržava ista.

8.1 Postojeća infrastruktura

U Tabeli 11. je dat pregled telefonskih centrala koje se nalaze na Medicinskom fakultetu. Pored samih kućnih centrala navedenih u Tabeli 10. postoje i direktne telefonske linije koje ne idu preko navedenih centrala. Trenutno je prvih pet lokacija navedenih u Tabeli 10. povezano IP putem, međutim, treba na mesto centrale u Dekanatu (Panasonic KX-TDA200), postaviti novu i savremeniju centralu koja bi praktično trebala da predstavlja buduće čvorište telefonske mreže Medicinskog fakulteta, na koji bi se povezivali svi ostali delovi telefonske mreže. Pri tome da bi ova nova centrala bila adekvatna za duži niz godina ona bi trebala da bude softsvič koji omogućava priključenje kako starih telefona i TDM telefonskih centrala (starija generacija centrala baziranih na TDM komutaciji govora), tako i novih sistema (VoIP telefoni, media gejtveji – sistemi bazirani na paketskoj komutaciji).

Trenutna infrastruktura obuhvata devet lokacija prikazanih u Tabeli 11. od kojih na četiri lokacije su instalirane centrale novije generacije Aastra BP250, u Dekanatu je postavljena Panasonic TDA200 centrala, na Institutu za sudsku medicinu Panasonic TDA100.

Sve centrale imaju samostalne veze ka mreži Telekoma Srbija a.d., realizovane pomoću ISDN PRI ili CO. Aastra BP250 centrale i Panasonic TDA200 centrala u Dekanatu su povezane na telefonsku mrežu Telekoma Srbija pomoću pet ISDN PRI konekcija. Same Aastra BP250 centrale su povezane međusobno pomoću H.323 protokola dok je veza sa Panasonic TDA200 centralom lociranom u Dekanatu realizovana IP putem pomoću media gateway uređaja sa 4 FXS kanala.

Trenutno ne postoje realizovane veze ka drugim fiksnim i IP operaterima. Ka GSM mreži postoje četiri GSM gateway uređaja locirana u Dekanatu i jedan neaktivni BizLink, Telekom Srbija, na Histološkom institutu.

R.br.	Opis	Tip centrale	ISDN PRI	Modem	Numeracija lokala	IP Adresa	Ukupno portova
1	Dekanat	Panasonic TDA200	3636-300				158
2	Histofiziologija	Ericsson BP250	3607-000	3607-099	70xx do 71xx	147.91.126.121	260
3	Biohemija	Ericsson BP250	3643-200	3643-299	32xx	147.91.126.122	134
4	Biblioteka	Ericsson BP250	2062-200	2062-099		147.91.126.123	82
5	Patologija	Ericsson BP250	3643-300	3642-499	33xx	147.91.126.124	242
6	Anatomija	Alcatel 4200					40
7	Sudska medicina	Panasonic TDA100					48
8	Patofiziologija	Alcatel 4200					40
9	Silos	Direktne linije					0
	UKUPNO:						1004

Tabela 11. – Spisak trenutno aktivnih centrala

Prednosti koje umrežavanje postojećih centrala, zamena trenutne Panasonic TDA200 centrale u Dekanatu i kreiranje centralnog telekomunikacionog čvorišta su sledeće:

- Korišćenje postojećih resursa uz optimizaciju,
- Jedinствена telefonska mreža Fakulteta na IP/ISDN nivou,
- Novi IP/CTI servisi,
- Integracija sa LAN/WAN servisima,
- Ušteda u telefoniranju i praćenje troškova,
- Jednostavna administracija i održavanje,
- Kreiranje osnova za dalji razvoj telefonskih resursa i usluga.

8.2 Realizovano rešenje

Instalacijom nove centrale u server sali, u objektu Dekanata, stvara se mogućnost da se postojeća Panasonic TDA200 centrala izmesti na Institut za anatomiju gde trenutna Alcatel 4200 centrala ne ispunjava trenutne potrebe instituta.

Kako bi se kreiralo centralno čvorište, potrebno je instalirati softsvič centralu, u sklopu server sale u Dekanatu. Predložena centrala je Aastra MX One TS sa sledećom konfiguracijom:

- 64 analognih lokala,
- 20 SIP lokala,
- 2 ISDN PRI linkova,
- 20 Analognih PTT veza sa CLIP,
- 2 SIP Trunk,
- 120 ISDNI Qsig kanala za umrežavanje.

Sama softsvič centrala ja zasnovana na HP Proliant serverskoj arhitekturi i Suse Linux operativnom sistemu na kojem se izvršava aplikacija koja i čini samu srž ovog telekomunikacionog sistema Aastra MX-ONE Manager.

Samom instalacijom ove centrala otvara se mogućnost implementacije naprednih CTI servisa poput:

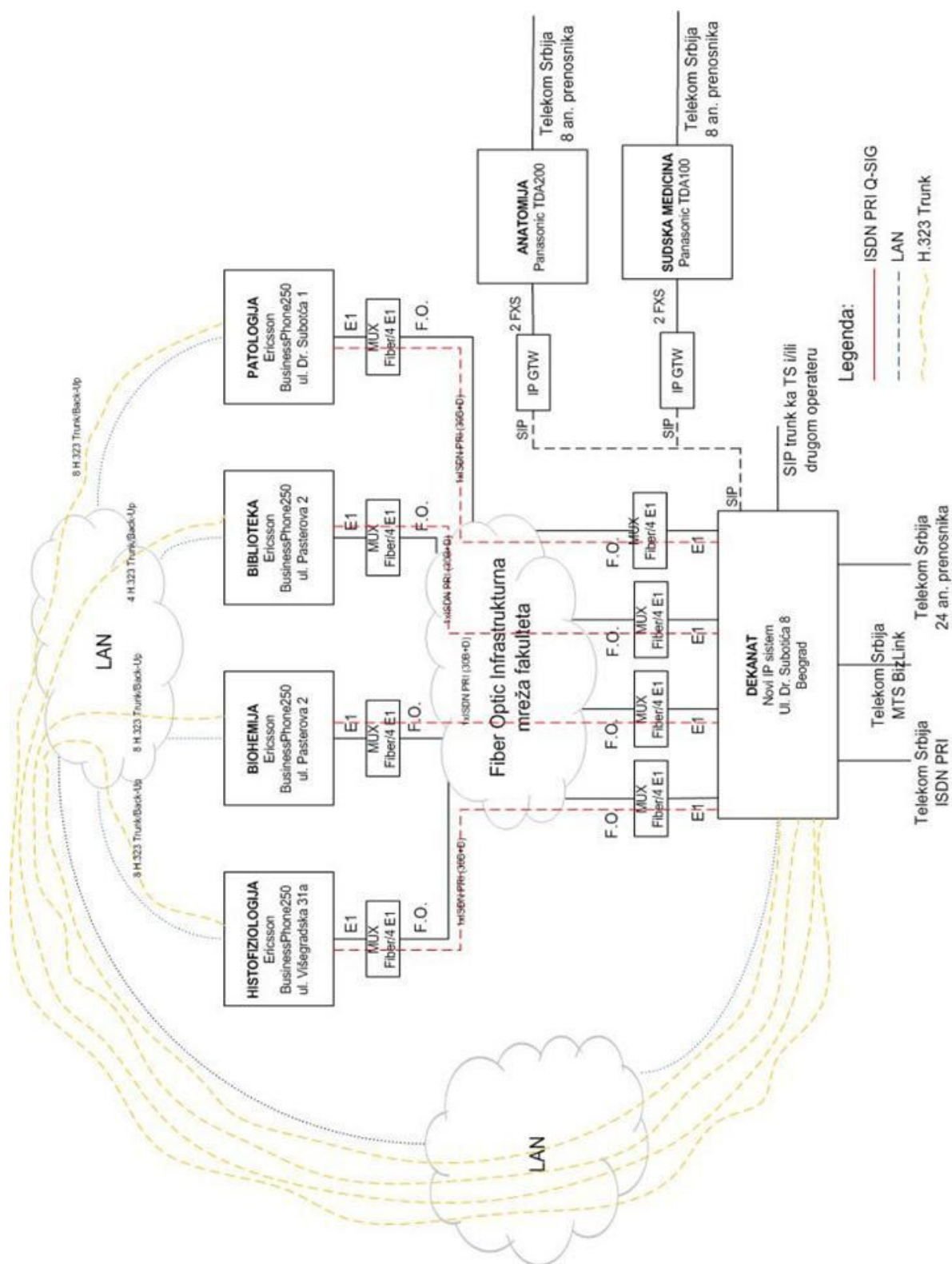
1. Fax servera – Novog mrežnog uredjaja na IP nivou, vezanog putem SIP na IP/PBX u Dekanatu, na kojem su mapirani svi FAX brojevi iz mreže putem DID brojeva u prolaznom biranju. Sam server pruža mogućnost slanja/primanja fax poruka na/sa mail-a, pri čemu je svaki fax broj uvezan sa mail adresom primaoca fax poruka i svaki mail nalog uvezan sa brojem fax-a u predstavljanju pošiljaocu.

2. Voice mail servera – Predstavlja novi mrežni uređaj na IP nivou koji je vezan putem SIP na IP/PBX u Dekanatu. Svaki lokal u celokupnoj mreži poseduje svoj nalog i jedinstveni način rutiranja poziva na voice mail u slučajevima nejavljanja, zauzeća ili direktnog rutiranja. Povezivanje Voice mail servera i mail Servera. Slanje primljenih voice poruka na e-mail vlasnika lokala kao audio file attachment. Pozdravne poruke i IVR kao nezavisni servis.
3. SIP Trunk/Ext - Mogućnost povezivanja ka alternativnim operaterima. Ušteda u ceni koštanja međunarodnih poziva. Povezivanje sa izdvojenim lokacijama. Aktivacija SIP korisnika i povezivanje putem VPN.
4. Umreženje sa GSM - Iskorišćavanje postojećeg, neaktivnog, BizLink-a Telekoma Srbija. Povezivanje na centralnu IP/PBX i mrežno korišćenje aktivnim rutiranjem GSM poziva pri pozivanju. Aktiviranje pristupa direktnim biranjem iz GSM mreže ka svakom lokalu po jedinstvenom broju. Skraćeno biranje svakog GSM broja iz CUG mreže Fakulteta. Ušteda u ceni minuta prema svim GSM operatorima.

Povezivanje postojećih centrala sa centralnim čvorištem u Dekanatu je moguće izvršiti na više dva načina i to (oba načina su prikazana na slici 24.):

1. Korišćenjem postojeće optičke infrastrukture i rezervnih optičkih linkova koji bi se terminirali na MUX modeme spojene na postojeće interfejsne module na PBX pri čemu bi postojeći H.323 linkovi bili ostavljeni kao aktivne backup veze.
2. Korišćenjem postojeće računarske mreže i postojećih H.323 linkova na lokacijama gde ne postoji rezerva u optičkim linkovima pri čemu je potrebno voditi računa da je na tim linkovima i VLAN-u koji je dodeljen za komunikaciju potrebno implementirati QoS (*Quality of Service*) kako ne bi došlo do zagušenja ili čak nedostupnosti servisa.

Samom implementacijom predložene centrale ostavlja se mogućnost implementacije kompletne VoIP tehnologije uz podršku za klasične telefonske tehnologije. Pored VoIP-a implementacijom ove centrale je postavljena i osnova za Unified Communications pri čemu se objedinjuju *voice*, *video* i *data* sa mogućnošću kompletne mobilnosti krajnjih korisnika.



Slika 24. – Predložena struktura telekomunikacione mreže

9 MERE ZAŠTITE BEZBEDNOSTI I ZDRAVLJA NA RADU

Prilog je urađen prema članu 7. Zakona o bezbednosti i zdravlju na radu (Sl.glasnik br.101/2005).

Preventivna mera zaštite je ukazivanje radnom osoblju na opasnosti koje im prete i primena odgovarajuće zaštite (zaštitna sredstva, postupci) od tih opasnosti. Osoblje treba da je obučeno za pružanje prve pomoći, a pribor za prvu pomoć mora biti uvek u kompletu uz radnu ekipu, odnosno uz ostala sredstva zaštite.

9.1 Opasnosti i pretnje i predviđene mere za njihovo otklanjanje

Tokom izvođenja radova na opremi predviđenom ovim projektom, potrebno je pridržavati se merama zaštite na radu. Ovde su nabrojane opasnosti i pretnje koje se mogu javiti pri izgradnji instalacija. O ovome treba da vodi računa Odgovorni Izvođač i Nadzorni organ.

	Opasnosti i pretnje	Predviđene mere
1.	Opasnost od slučajnog dodira delova pod naponom	Sva električna oprema predviđena za ugradnju u zid ili u ormane, zaštićena je kućištima i poklopcima, a vodovi su odgovarajuće konstrukcije zaštićeni izolacijama i plaštovima. Uvođenje kablova u razvodne ormane i zaštitna kućišta opreme, izvedeno je na pravilan način te je tako otklonjena opasnost od slučajnog dodira delova pod naponom.
2.	Opasnost od preopterećenja	Pravilnim izborom zaštitnih osigurača i prekidača centralnih uređaja onemogućena je pojava preopterećenja napojnih kablova i priključenih uređaja.

	Opasnosti i pretnje	Predviđene mere
3.	Opasnost od struje kratkog spoja	Pravilnim izborom opreme i pravilno dimenzionisanje kablova, na osnovu podataka o struji kratkog spoja izbegava se opasnost od pregorevanja kablova i opreme.
4.	Opasnost od previsokog napona dodira i napona koraka	Opasnost od previsokog napona dodira i napona koraka izbegava se pravilnim izborom opreme, uzemljenjem svih metalnih delova koji ne pripadaju strujnim kolima, sistemom sniženog napona i pravilnim izborom otpora uzemljivača. Opasnost od napona koraka otklonjena je izradom uzemljenja na koje su vezani centralni uređaji.
5.	Opasnost od prevelikog pada napona u instalaciji	Opasnost od prevelikog pada napona u instalaciji otklanja se pravilnim dimenzionisanjem preseka provodnika za sva strujna kola.
6.	Opasnost od nestanka napona	Centralni uređaji zaštićeni su od nestanka napona opremom za obezbeđenje neprekidnog napajanja ili dodatnog napajanja u određenom vremenskom intervalu.
7.	Opasnost od uticaja struje zemljospoja	Izvođenjem zajedničkog uzemljivača izbegnuta je opasnost od struje zemljospoja.
8.	Opasnost od mehaničkog oštećenja	Sva oprema je zaštićena kućištima od metala i locirana je na odgovarajućim mestima, a svi kablovi su položeni u zaštitne cevi i kanale, tako da ne može doći do slučajnih mehaničkih oštećenja.
9.	Opasnost od pogrešnog rukovanja	Štetnost od pogrešnog rukovanja uvek postoji za sve ugrađene uređaje, a može se otkloniti samo odgovarajućom obukom lica koja je koriste i zaštitom od neovlašćenog rukovanja opremom. Zaštita može biti mehanička (npr. zaključavanje ormara).
10.	Opasnost od požara	Pravilnim izborom opreme koja pri pravilnom rukovanju i održavanju ne može biti uzrok požara. Ugradnjom aparata za gašenje požara na električnim instalacijama tipa CO ₂ postavljenim na svim ulaznim vratima, izbegava se veće širenje požara.

	Opasnosti i pretnje	Predviđene mere
11.	Opasnost od uticaja vlage, prašine, eksplozivnih i zapaljivih materijala i hemijskih uticaja	Opasnost od ovih uticaja otklonjena je pravilnim izborom opreme, razvodnih tabli i ormana prema mestu ugradnje, nameni i uslovima u kojima rade.
12.	Opasnost od uticaja elektromagnetnog polja	Primenom zaštitnih mera prilikom paralelnog vođenja i ukrštanja sa energetskim kablovima i izvođenjem uzemljenja armature kablova na oba kraja otklonjen je uticaj elektromagnetnog zračenja.
13.	Opasnost od statičkog elektriciteta	Pravilnim izvođenjem uzemljenja svih uređaja i ormana izbegnuta je opasnost od statičkog elektriciteta.

9.2 Opšte napomene i obaveze

Sva oprema i materijali, predviđeni ovim projektom moraju da odgovaraju važećim tehničkim propisima i standardima.

Izvođač radova je obavezan da uradi poseban elaborat o uređenju gradilišta i radu na gradilištu.

Oruđa za rad na mehanizovan pogon moraju imati uputstvo za bezbedan rad i da imaju potvrdu da su na njima primenjene sve propisane mere i normativi zaštite na radu, odnosno da poseduju atesto primenjenim propisima zaštite na radu.

Izvođač radova je obavezan da 8 dana pre početka rada obavesti nadležni organ inspekcije rada o početku radova.

Izvođač radova je dužan da izvrši obučavanje radnika iz materije zaštite na radu i da upozna radnika sa uslovima rada, opasnostima i štetnostima u vezi sa radom i obavi proveru sposobnosti radnika za samostalan i bezbedan rad.

Izvođač radova je obavezna da utvrdi radna mesta sa posebnim uslovima rada ukoliko takva mesta postoje.

Prilikom nabavke oruđa za rad i uređaja iz dokumentacije, koja se prilaže uz oruđa za rad i uređaje, moraju se pribaviti i podaci o akustičkim osobinama iz kojih će se videti da li buka na radnim mestima i prostorijama ne prelazi dozvoljene vrednosti. Ako je za ispunjenje uslova o dopuštenim vrednostima potrebno preduzimnje posebnih mera (prigušivači buke, elastično podlaganje i dr.) u pomenutoj dokumentaciji moraju biti naznačene i te mere.

Izvođač je obavezan da izradi normativna akta iz oblasti zaštite na radu. Program za obučavanje i vaspitvanje radnika iz oblasti zaštite, Pravilnik o pregledima, ispitivanjima i održavanju oruđa, uređaja i alata, Program mera za unapređenje zaštite na radu i dr.

Sva postrojenja i održavanje istih moraju se uskladiti sa važećim propisima.

Svuda gde propisi zahtevaju, postaviti vidno označene natpise sa upozorenjima: visina napona, namena opreme, druga obaveštenja.

Pri izvođenju radova ili remonta postrojenja i opreme obavezno je postaviti opomensku tablicu u pogledu stanja uključenosti - isključenosti, zabrana, druga obaveštenja za rukovaoce i sevisere. Pri rukovanju opemom obavezna je primena zaštitne opreme i sredstava.

10 PREDMER I PREDRAČUN

U okviru predmera i predračuna date su budžetske cene za aktivnu i pasivnu opremu kao i za izvođenje radova.

Redni broj	Opis	Jedinica mere	Količina	Cena	Ukupno
1.	Optički kabl SM 24 vlakana 9/125, indoor/outdoor, halogen free, nezapaljiv, sa zaštitom od glodara	m	300	180,00	54.000,00
2.	Optički patch panel za 24 vlakna	kom	2	80.000,00	160.000,00
3.	Stojeći rek orman 42U	kom	1	180.000,00	180.000,00
4.	Optički SM patch kabl FC-LC duplex 2m	kom	20	3.260,00	65.200,00
5.	Optički SM patch kabl SC-LC duplex 2m	kom	20	3.260,00	65.200,00
6.	Radovi na postavljanju optičkog kabla	kom	300	350,00	105.000,00
7.	Sitan materijal i radovi	kom	1	75.000,00	75.000,00
8.	Projekat izvedenog stanja sa rezultatima merenja	kom	1	100.000,00	100.000,00
UKUPNO:					714.400,00

Tabela 12. – Predmer i predračun pasivne mrežne opreme

Redni broj	Opis	Jedinica mere	Količina	Cena	Ukupno
1.	Cisco Catalyst 4506-E chassis	kom	1	455.201,00	455.201,00
2.	Cisco Catalyst 4500E Supervisor Engine 7-E	kom	1	721.788,00	160.000,00
3.	Cisco WS-X4712-SFP+E kartica	kom	3	529.190,00	1.587.570,00
4.	Catalyst 4500 1400W AC napajanje	kom	2	64.960,00	129.920,00
5.	APC Smart-UPS 5000VA 230V Rackmount	kom	1	308.244,00	308.244,00
6.	Opcija 1: Cisco Catalyst 2960S-24TD-L	kom	40	121.982,00	5.196.800,00
	Opcija2: Cisco Catalyst 2960S-24TD-L (PoE Switch)	kom	40	156.122,00	6.244.880,00
7.	Cisco SFP-10G-LR modul	kom	42	36.089,00	1.515.738,00
8.	Cisco CAB-STK-E-0.5M	kom	40	4.260,00	170.040,00
9.	Montaža i puštanje u rad aktive	kom	1	200.000,00	200.000,00
10.	Sitan materijal i radovi	kom	1	50.000,00	50.000,00
UKUPNO(Opcija 1):					9.773.513,00
UKUPNO(Opcija 2):					10.821.593,00

Tabela 13. – Predmer i predračun aktivne mrežne opreme

Redni broj	Opis	Jedinica mere	Količina	Cena	Ukupno
BLADE ŠASIJA					
1.	IBM eServer BladeCenter(tm) H Chassis with 2x2980W PSU	kom	1	361.775,00	361.775,00
2.	IBM BladeCenter SAS Connectivity Module	kom	2	30.720,00	61.440,00
3.	IBM BladeCenter H 2980W AC Power Modules w/Fan Pack	kom	1	53.380,00	53.380,00
4.	Multi-Switch Interconnect Module for IBM BladeCenter	kom	2	75.283,00	150.566,00
5.	Server Connectivity Module for IBM BladeCenter	kom	4	153.031,00	612.126,00
6.	IBM UltraSlim Enhanced SATA Multi-Burner	kom	1	7.217,00	7.217,00
7.	2.8m, 200-240V, Triple 16A IEC 320-C20	kom	2	6.339,00	12.678,00
BLADE SERVERI					
8.	Intel Xeon 4C Processor Model E5620 80W 2.40GHZ/1066MHz/12 MB	kom	3	122.248,00	366.745,00
9.	4GB (1x4GB, 2Rx8, 1.5V) PC3-10600 CL9 ECC DDR3 1333MHz VLP RDIMM	kom	18	8.894,00	160.092,00
10.	2GB (1x2GB, 2Rx8, 1.5V) PC3-10600 CL9 ECC DDR3 1333MHz VLP RDIMM	kom	9	6.539,00	58.854,00
11.	2/4 1GB Port Ethernet Expansion Card (CFFh) For IBM SAS	kom	3	16.213,00	48.639,00

Redni broj	Opis	Jedinica mere	Količina	Cena	Ukupno
12.	Connectivity Card (CIOv) for IBM BladeCenter IBM USB	kom	3	5.973,00	17.919,00
13.	Memory Key for VMware ESXi 4.1	kom	3	5.253,00	15.760,00
SISTEM ZA SKLADIŠTENJE PODATAKA					
14.	IBM System Storage DS3524 Express Dual Controller Storage	kom	1	316.608,00	316.608,00
15.	300GB 2,5in 10K 6Gb SAS HDD	kom	24	12.904,00	309.714,00
16.	IBM 1m SAS Cable	kom	4	3.466,00	13.866,00
SOFTVER ZA VIRTUELIZACIJU					
17.	Academic VMware vSphere 5 Standard for 1 processor (with 32 GB vRAM entitlement per processor)	kom	6	51.950,00	311.703,00
18.	Academic Basic Support/Subscription for VMware vSphere Standard for 1 processor for 1 year	kom	6	12.157,00	72.944,00
19.	Academic VMware vCenter Server 5 Foundation for vSphere up to 3 Hosts	kom	1	78.056,00	78.056,00

Redni broj	Opis	Jedinica mere	Količina	Cena	Ukupno
20.	Academic Basic Support/Subscription for vCenter Server Foundation for vSphere	kom	1	31.803,00	31.803,00
	OSTALO				
21.	IBM NetBay S2 42U Standard rack cabinet	kom	1	87.988,00	87.988,00
22.	Aktivnosti oko instalacije i puštanja u rad kompletnog sistema	kom	1	180.000,00	180.000,00
UKUPNO:					3.329.873,00

Tabela 14. – Predmer i predračun opreme u okviru nove serverske infrastrukture

Redni broj	Opis	Jedinica mere	Količina	Cena	Ukupno
1.	Aastra MX-ONE Server	kom	1	1.093.769,00	1.093.769,00
2.	Aastra MX-ONE Media Gateway	kom	1	1.242.292,00	1.242.292,00
3.	Licenca za softver	kom	1	298.300,00	298.000,00
4.	Premeštanje postojeće centrale na Anatomski Institut	kom	1	100.000,00	100.000,00
5.	Postavljanje, povezivanje i konfigurisanje nove centrale	kom	1	50.000,00	50.000,00
6.	Sitan materijal i radovi	kom	1	50.000,00	50.000,00
UKUPNO:					2.834.061,00

Tabela 15. – Predmer i predračun opreme za novu telefonsku infrastrukturu

11 ZAKLJUČAK

Ovaj rad predstavlja idejni projekat nadogradnje postojeće računarsko-telekomunikacione infrastrukture Medicinskog fakulteta Univerziteta u Beogradu, opisane u drugom projektnom zadatku. Imajući to u vidu nije razmatrano kompletno postavljanje nove optičke infrastrukture već samo polaganje novog optičkog kabla koji se prostire trasom od objekta Dekanata preko Interne B klinike KCS-a do zgrade Silosa u kojem je realizovano rezervno čvorište i izmešten postojeći layer 3 svič.

Implementacijom novih mrežnih uređaja i kreiranjem mreže velikih brzina stvoreni su uslovi za postavljanje nove serverske infrastrukture zasnovane na IBM BladeCentrer rešenju u okviru koga je odabrana IBM Blade šasija sa 14 slotova za IBM Blade servere pune veličine i IBM i IBM sistem za skladištenje podataka koji čine kompletno hardversko rešenje na kojem se implementira VMware vSphere 5 i vCenter Server 5 softversko rešenje za virtuelizaciju. Ovim rešenjem se dostiže kompletna kontrola i visoka dostupnost servisa i informacionih sistema Medicinskog fakulteta kao i kompletna iskorišćenost resursa koje nudi samo rešenje.

Pored izgradnje nove računarsko-komunikacione infrastrukture, dat je i opisan predlog realizacija telekomunikacione infrastrukture u cilju postepenog prelaska sa klasične telefonije na nove tehnologije poput VoIP telefonije, do video konferencija, a sve sa ciljem da se postave osnove za buduće kompletno objedinjavanje *video*, *voice* i *data* komunikacije.

U ovom projektu je realizovana implementacija nove računarsko-telekomunikacione infrastrukture Medicinskog fakulteta, koja čini osnovu za uvođenje novih tehnologija i servisa sa ciljem da se ubrza i olakša dostupnost informacija u okviru samog fakulteta, uzimajući u obzir razuđenost objekata, i dalji razvoj i implementaciju novih ICT/CTI servisa koji bi činili nadogradnju postojeće infrastrukture a koji bi bili opisani i realizovani drugim radovima.

12 LITERATURA

- [1] *Glavni projekat mreže LOMED*, Mr. Nenad Krajinović, Elektrotehnički fakultet u Beogradu (2004).
- [2] *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide*, Richard Froom, Balaji Sivasubramanian, Erum Frahim (2010).
- [3] *CCNA Security - Implementing Network Security*, Cisco Learning Network(2009).
- [4] *CSU Telecommunications Design Standards*,
www.colostate.edu/~pburns/Standards/TelecomStandards.htm
- [5] *TIA/EIA Structured Cabling Standards*, www.linktionary.com/t/tia_cabling.html
- [6] *EIA/TIA-606-A Labeling Standard For Networks*
www.deepsurplus.com/s.nl/sc.2/category.349/
- [7] *Analiza postojeće telekomunikacione infrastrukture*, Mihajlo Lakićević, www.ericom.rs (2011).
- [8] *IBM System Storage Solutions Handbook*, Sangam Racherla, Libor Miklas, Thiago Montenegro, James M Mulholland (2011).
- [9] *IBM BladeCenter Products and Technology*, David Watts, Randall Davis, Ilia Kroutov (2011).
- [10] *Vmware vSphere 5 documentation*, <http://pubs.vmware.com/vsphere-50/>, (2011).
- [11] *Zakon o bezbednosti i zdravlju na radu*, Službeni Glasnik br.101/2005, (2005).
- [12] *E-Campus in Xiamen University: The Past, Present and The Hopeful Future*, Weisheng Xue, Guojun Ji, (2010).
- [13] *A Study of Efficiency- Campus Networks in Western Himalayan Universities of India*, Dharendra Sharma, Vikram Kumar, Marco Zennaro, Vikram Singh (2011).
- [14] *VCUHK: integrating the real into a 3D campus in networked virtual worlds*, Bin CHEN, Fengru HUANG, Hui LIN, Mingyuan HU (2010).