

UNIVERZITET SINGIDUNUM

-MASTER STUDIJSKI PROGRAM-

SAVREMENE INFORMACIONE TEHNOLOGIJE

Danilo Jovanović

Zaštita i realizacija kampus i virtuelne privatne računarske mreže

Mentor:

Prof dr Mladen Veinović

Student:

Danilo Jovanović

Univerzitet Singidunum

Beograd, 2013.

Sažetak

Zaštita i realizacija kampus i virtuelne private računarske mreže

Ovaj master rad opisuje način realizacije kampus i virtuelne privatne mreže i uključuje detaljne opise tehnologija zaštite računarsih mreža, mrežne opreme, kriptoloških uređaja, VPN uređaja, kablova, načina kabliranja unutar svih objekata, kabliranja kampus mreže sa konstantnim protokom od 1 Gbps, VoIP mreže, mreže IP kamera za nadzor, servera, IP adresiranja i potrebnog ljudstva. Cilj projekta je realizacija kvalitetne, isplative, dugotrajne, pouzdane i nadogradive kampus i virtuelne privatne mreže. U projektu je korišćena najnovija mrežna oprema koja koristi modernu softversku mrežnu tehnologiju koja omogućava konstanti protok velike količine podataka.

Abstract

Protection and implementation of campus computing and virtual private networks

This master thesis describes the way of kampus network realization and includes detailed descriptions of nertwork security, network equipment, criptology equipment, VPN devices, cabling, wiring methods within all buildings, campus network wiring with a constant flow rate of 1 Gbps, VoIP network, network IP surveillance cameras, servers, IP addressing and the required manpower. The project objective is the realization of high-quality, cost effective, durable, reliable and upgradeable campus and virtual private network. The latest network equipment that uses modern software networking technology which allows the constant flow rate of large amounts of data is used in the project.

Sadržaj

Uvod ..... - 1 -
1 Metodologija istraživačkog projekta ..... - 2 -
1.1 Uvodne napomene i obrazloženje rada ..... - 2 -
1.2 Predmet istraživanja ..... - 2 -
1.3 Ciljevi i zadaci istraživanja ..... - 2 -
1.4 Istraživačke hipoteze ..... - 3 -
1.5 Metodi istraživanja i tok istraživačkog procesa ..... - 3 -
2 Organizacija ..... - 4 -
3 Mrežna infrastruktura ..... - 4 -
3.1 Mrežna oprema ..... - 4 -
3.1.2 Kanalice ..... - 12 -
3.2 Svičevi (komutatori) ..... - 13 -
3.3 Ruteri ..... - 16 -
3.4 Bežični (*WiFi*) ruteri ..... - 16 -
3.5 Kriptološki uređaji ..... - 17 -
4 Implementacija sistema ..... - 19 -
4.1 Marketing i menadžment ..... - 20 -
4.1.1 Sektor za dizajn ..... - 20 -
4.1.2 Odnosi sa javnošću ..... - 21 -
4.1.3 Računovodstvo ..... - 21 -
4.1.4 Menadžment ..... - 22 -
4.1.5 Ostali mrežni priključci ..... - 22 -
4.2 Nabavka i distribucija ..... - 23 -
4.2.1 Sektor za nabavke i distribuciju ..... - 24 -
4.2.2 Magacin ..... - 24 -
4.2.3 Ostali mrežni priključci ..... - 25 -
4.3 Prodaja ..... - 25 -
4.3.1 Sektor prodaje ..... - 26 -
4.3.2 Maloprodaja ..... - 26 -

4.3.3 Veleprodaja - 27 -
4.3.4 Ostali mrežni priključci - 28 -
4.4 Servis - 28 -
4.4.1 Prijem robe - 29 -
4.4.2 Popravka - 29 -
4.4.3 Ostali mrežni priključci - 30 -
4.5 IT sektor - 31 -
4.5.1 Server soba - 32 -
4.5.2 IT Administracija - 34 -
4.5.3 Ostali mrežni priključci - 35 -
5 Administracija - 36 -
5.1 IP Adresni plan - 36 -
6 Zaštita sistema i bezbednost podataka - 38 -
6.1 Potencijalni napadi na savremene računarske mreže i mogući načini odbrane - 41 -
6.2 Primeri napada na savremene računarske mreže - 42 -
6.2.1 Krađa identiteta - phishing - 42 -
6.2.2 Prisluškivanje - 43 -
6.2.3 Modifikacija podataka - 43 -
6.2.4 Identity spoofing (IP address spoofing) - 43 -
6.2.5 Napadi na lozinke - 43 -
6.2.6 Denial-of-service napad - 44 -
6.2.7 Man-in-the-middle napad - 44 -
6.2.8 Napad kompromitacije ključa - 44 -
6.2.9 Sniffer napad - 45 -
6.2.10 Napad na aplikativnom nivou - 45 -
7 Tehnologije zaštite savremenih računarskih mreža - 46 -
7.1 Primena kriptografskih metoda zaštite u informacionom sistemu - 46 -
7.1.1 Simetrični kriptografski algoritmi - 46 -
7.1.2 Blok šifarski sistemi - 47 -
7.1.3 Sekvencijalni šifarski sistemi - 49 -
7.1.4 Komparativna analiza blok i sekvencijalnih šifarskih sistema - 52 -
7.1.5 Asimetrični kriptografski algoritmi - 52 -

7.1.6 PKCS#1 standard ..... - 53 -
7.1.7 Primena kriptografskih algoritama u informacionim sistemima ..... - 55 -
7.2 Višeslojna arhitektura sistema zaštite savremenih računarskih mreža ..... - 56 -
7.2.1 Zaštita na aplikativnom nivou ..... - 57 -
7.2.2 Zaštita na transportnom nivou ..... - 59 -
7.2.3 SSL ..... - 60 -
7.2.4 Zaštita na mrežnom nivou ..... - 60 -
7.2.5 IPSec ..... - 61 -
7.2.6 VPN ..... - 62 -
7.2.7 Wi-Fi Protected Access (WPA) - Wi-Fi Protected Access II (WPA2) ..... - 63 -
7.2.8 IDS-IPS sistemi ..... - 64 -
7.2.9 IDS (Intrusion detection system) ..... - 64 -
7.2.10 IPS (Intrusion prevention system) ..... - 64 -
8 Softverska zaštita celokupnog mrežnog sistema ..... - 66 -
8.1 Zaštitni zid ..... - 66 -
8.2 Antivirus softver ..... - 67 -
9 Održavanje i unapređivanje sistema ..... - 68 -
9.1 Potrebe sistema ..... - 68 -
9.1.1 IT osoblje ..... - 68 -
9.2 Održavanje sistema ..... - 70 -
9.3 Unapređivanje sistema ..... - 70 -
Zaključak ..... - 71 -
Literatura ..... - 73 -

Uvod

Kraj XX i početak XXI veka obeležila je velika ekspanzija informacionih tehnologija zahvaljujući kojoj su računari postali neizostavni deo svakodnevnog života, kako sa poslovnog tako i sa privatnog aspekta.

Kako su računari postali neophodni u svakodnevnom poslovanju, firme današnjice imaju sve veći broj radnih stanica (najčešće personalnih računara). Skoro svaka firma ili organizacija ima bar jedan računar za svakog zaposlenog. Toliki broj računara direktno je doveo do znatnog porasta u potrebi za računarskim mrežama u srednjim i velikim firmama. Mogućnost brze razmene velikih količina podataka između mrežnih klijenata, zajednički mrežni resursi (serveri, internet...) i VoIP telefonija, samo su nekolicina čestih razloga za uvođenje računarske mreže.

Male i srednje firme najčešće poseduju LAN (Local Area Network) mreže. LAN mrežu čini skup računara koji su povezani u jednu celinu, na relativno malom prostoru. Ova mreža može da broji dva i više računara koji su povezani na određen način. Neki periferni uređaji kao što su štampači, modemi i sl., takođe se ubrajaju u ovu mrežu. LAN mreža obično je postavljena u kancelariji, kući ili poslovnoj ispostavi.

Sa druge strane univerziteti, vojne baze, proizvodni pogoni, velike firme i organizacije najčešće imaju potrebu za međusobnim spajanjem više LAN mreža na manjem ograničenom geografskom području (zbog velikog broja mrežnih klijenata, više objekata...). Takva mreža naziva se kampus mreža.

Sve gore navedene vrste računarskih mreža spadaju u savremene računarske mreže koje se uglavnom baziraju na Internet tehnologijama i protokolima za koje se zna da su podložni mogućim napadima koji ugrožavaju bezbednost podataka i identiteta subjekata. Ključni problem leži u činjenici da podaci kruže i egzistiraju u elektronskom obliku koji nije neposredno vidljiv i zbog toga postaju izloženi novim vrstama napada. Shodno tome je razvijena potpuno nova grana IT industrije koja se bavi isključivo zaštitom i bezbednošću sistema i podataka.

Ovaj rad u sebi objedinjuje nekoliko krucijalnnih aspekata računarskih mreža, počevši od organizacije i administracije kampus i virtuelne privatne mreže, do zaštite sistema i bezbednosti podataka.

Organizacija mreže se bavi hardverskim i softverskim rešenjima koja su potrebna da bi se mreža realizovala po zahtevima korisnika. Administraciju mreže čine njeno održavanje, nadgledanje i unapređivanje kako bi ona bila dugotrajna i efikasna, te na taj način zadovoljavala najviše IT standarde. Zaštitu sistema i bezbednost podataka čine sva hardverska i softverska rešenja neophodna da spreče i otklone potencijalne pretnje po sigurnost i bezbednost sistema.

1 Metodologija istraživačkog projekta

1.1 Uvodne napomene i obrazloženje rada

Master rad ima za cilj da definiše pojmove koji se koriste kada se govori o kampus i virtualnim privatnim mrežama kroz arhitekturu, protokole i bezbednosne aspekte vezane za ovu vrstu mreža.

Rad se pored planiranja, organizacije, implementacije bavi i zaštitom celokupne mreže i podataka uključujući i virtualnu privatnu mrežu zasnovanu na VPN tehnologiji.

Master rad je izrađen korišćenjem teoretskih i praktičnih znanja iz domena računarskih mreža i zaštite informacija.

1.2 Predmet istraživanja

Predmet istraživanja bile su kampus i virtuelna privatna mreža i njihova zaštita. Dakle planiranje mreže radi kvalitetne realizacije po zahtevima korisnika, administrativni aspekt iste, opisi i specifikacije mrežne infrastrukture, te njihova namena, primena i implementacija u sistemu, softverskim rešenjima koja omogućavaju rad mreže i na kraju zaštita sistema i bezbednost podataka pomoću hardverskih i softverskih rešenja.

1.3 Ciljevi i zadaci istraživanja

Ovaj rad je namenjen pre svega profesionalcima u oblasti računarskih mreža, kao i IT menadžerima koji treba da urade studiju izvodljivosti uvođenja kampus i virtuelne privatne mreže u neku kompaniju. Potrebno je da ovi profili IT stručnjaka imaju dobru osnovu u poznavanju mrežnih tehnologija ali nije nužno da detaljno ulaze u funkcionisanje protokola kao i način rada pojedinih uređaja koji se koriste u kampus i virtualnim privatnim mrežama.

Cilj ovog master rada je da se realizuje kvalitetan projekat mreže koji objedinjuje i pokriva sve ključne aspekte kamups i virtuelne privatne mreže, od planiranja mrežne infrastrukture do potpune zaštite sistema i informacija, kako bi se omogućila laka i efikasna realizacija iste.

1.4 **Istraživačke hipoteze**

Opšta hipoteza

Od samog početka težište istraživanja je na klasičnim kampus i virtualnim privatnim mrežama. Tokom istraživanja ukazalo se da su takve mreže krajnje kompleksne i da njihovo loše planiranje i implementacija mogu ugroziti ceo sistem i to ne odmah nakon njihovog aktiviranja već posle određenog upotrebnog veka.

Najviše problema čini skoro nemoguće testiranje mreže u virtuelnim uslovima pre implementacije sistema, te se posebna pažnja mora obratiti na razne primere iz literature i sa interneta kako bi se došlo do proverenog i sigurnog rešenja.

Drugi problem, tiče se direktno bezbednosti. Mreže koje imaju veliki broj klijenata, a pored toga poseduju i VPN konekcije veoma su izložene velikom broju mogućnosti za ugrožavanje sigurnosti i bezbednosti podataka i samog sistema. Da bi se ovakav problem rešio efikasno potrebno je realizovati kvalitetan i siguran sistem bezbednosnog softvera i hardvera.

Radna hipoteza

Ni jedna trenutno dostupna tehnologija ne omogućava potpuno rešenje svih navedenih problema. Međutim korišćenjem različitih i proverenih aplikacija i tehnologija moguće je postići visoko kvalitetnu, isplativu i funkcionalnu mrežu koja garantuje funkcionalnost i bezbednost u radu.

1.5 **Metodi istraživanja i tok istraživačkog procesa**

Metodologija istraživanja svela se na korišćenje pre svega Interneta ali i na korišćenje ozbiljnih knjiga koje se bave oblašću kampus i virtualnih privatnih mreža.

Na Internetu, a i u literaturi uopšte mnogo je manje informacija koje se tiču organizacije kampus i virtualnih privatnih mreža nego informacija o tehnologijama koje se za to koriste. Kada su u pitanju informacije o bezbednosnim rešenjima, veći deo čine radovi na temu pojedinačnih sigurnosnih rešenja nasuprot siromašnim informacija o kombinacijama hardvera, softvera i protokola koji se koriste u te svrhe. Svaka od informacija koja se nalazi u ovom radu proverena je obavezno na više mesta u literaturi da bi se dokazalo da je relevantna.

Ideja je da ovaj rad pomogne IT stručnjacima da dobiju informacije o planiranju, tehnologijama i implementaciji mreža i mrežnih sistema kao i informacije o tehnologijama koje pružaju kvalitetnu i efikasnu zaštitu u svakodnevnom prenosu podataka.

2 Organizacija

Firma poseduje pet objekata u kojima se realizuje mreža, to su:

1) Marketing i menadžment
2) Nabavka i distribucija
3) Prodaja
4) Servis
5) IT sektor

U svakom od ovih objekata potrebno je realizovati mrežu koja zadovoljava potrebe datog sektora. Objekat u kome se nalazi prodaja fizički je odvojen od ostatka mreže i pristupa istoj preko VPN (virtual private network) konekcije.

IP kamere unutar objekta imaju sopstvenu mrežu sa manjim protokom podataka (oko 100 Mbps) koja je povezana direktno preko mrežnih čvorišta objekata na kampus mrežu. Razlog ovakvog strukturiranja je rasterećenje glavne mreže objekta od konstantnog opterećenja mreže koje IP kamere stvaraju usled konstantnog emitovanja video signala u vidu paketa podataka koji se šalju na sigurnosni (eng. *Security*) server.

3 Mrežna infrastruktura

3.1 Mrežna oprema

U mrežnu opremu spada sav hardver koji čini jedan mrežni sistem. U ovom poglavlju navešćemo samo one koji se upotrebljavaju u ovom projektu a to su:

1) Kablovi
2) Svičevi
3) Load balancer ruteri
4) Bežični ruteri
5) Kriptološki uređaji

3.1.1 Kablovi

3.1.1.1 Kabliranje objekata

Najvažniji deo svake mreže čini njen sistem kablova koji sprovode različite vrste signala i međusobno povezuju sve mrežne klijente sa mrežnom opremom i serverima. Ukoliko mreža nije adekvatno i kvalitetno kablirana i sam kvalitet iste nikako ne može biti zagarantovan.

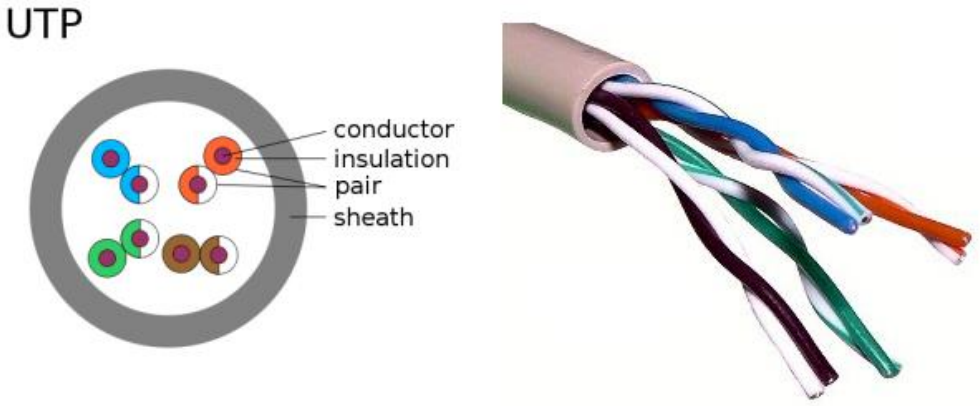
3.1.1.2 Vrste kablova

Zbog veličine i potreba ovog projekta koriste se dve potpuno različite vrste kablova, optički i bakarni (UTP, STP).

3.1.1.3 Vrste bakarnih mrežnih kablova koji se koriste u projektu

3.1.1.3.1 Nezaštićeni kablovi sa upredenim paricama (*UTP - Unshielded Twisted Pair*)

UTP kablovi se sastoje od zaštitne obloge (najčešće od PVC-a) i 4 para bakarnih žica koje su međusobno upletene kako bi se smanjio uticaj elektro-magnetnog zračenja koje nastaje usled protoka struje unutar samog kabla kao i spoljnog EM zračenja koje emituju električni vodovi, mašine...



Slika 1: Poprečni presek i izgled UTP kabla

Na tržištu postoje različite vrste UTP kablova koji se međusobno razlikuju u kvalitetu signala, brzini protoka podataka (eng. *bandwith*), zaštiti od elekltro-magnetnog zračenja i veku trajanja. Trenutno su najprisutnije dve kategorije UTP kablova:

1) Cat5e

10/100/1000BASE-T Ethernet
max dužina 100 metara

Specifikacije kabla ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:

UTP kabl kat. 5E Draka UC300 24 4P - testiran do 300MHz

UC300 24 Cat.5e U/UTP 4P PVC

UTP kabl kat. 5E DRAKA tip UC300 24 4P FRNC testiran do 300MHz, sertifikati DELTA & 3P - 'Wall', 4 parice punog preseka, FRNC / LSOH (omotač bez halogena, nezapaljiv i ne ispušta dim); ostali sertifikati ISO9001, ISO14001, RoHS

2) Cat6
10/100/1000BASE-T Ethernet
max dužina 100 metara
10GBASE-T Ethernet
max dužina 55 metara

Specifikacije kabla ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:

UTP kabl kat. 6 Draka tip UC400 23 4P FRNC - testiran do 400MHz, bez halogena

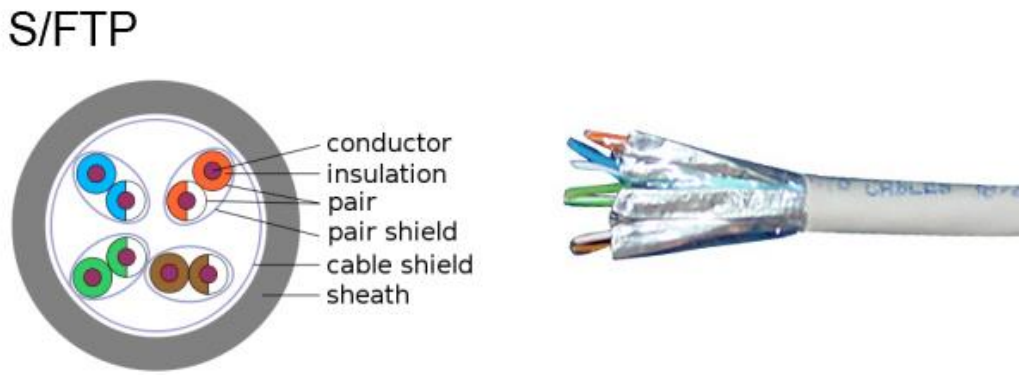
UC400 23 Cat.6 U/UTP 4P LSHF

UTP kabl kat. 6 DRAKA tip UC400 24 4P FRNC testiran do 400MHz, sertifikati DELTA & 3P - 'Wall', 4 parice, pun presek, krstast element između parica, kutije 305m i koturi 500m, FRNC (omotač bez halogena, nezapaljiv i ne ispušta dim), DELTA / EU sertifikovan; ostali sertifikati ISO9001, ISO14001, RoHS

3.1.1.3.2 **Zaštićeni kablovi sa upredenim paricama (*STP - Shielded Twisted Pair*)**

STP kablovi se sastoje od zaštitne obloge (najčešće od PVC-a), dodatne zaštite od EM zračenja koja je u potpunosti obmotana oko žica i 4 para bakarnih žica. Najisplativija (odnos cena/performanse) verzija STP kablova su S/FTP (*Screened Foiled Twisted Pair*) kablovi koji

imaju zaštitnu foliju koja u potpunosti obavija svaki par žica. Zaštitna folija zbog svoje visoke impendanse reflektuje spoljne EM signale.



Slika 2: Poprečni presek i izgled S/FTP kabla

Kao i kod UTP kablova na tržištu postoji veliki izbor različitih vrsta STP kablova gde se osim osnovnih merila (kvalitet signala, brzina protoka podataka,...) postoji i merilo zaštite od EM signala.

S/FTP kabl ima iste specifikacije kao i UTP Cat6 kabl osim što je njegova zaštita od EM signala neuporedivo veća kao i mogućnost prenosa podataka brzinom od 10Gbps na razdaljinu od 100m .

Class F

10/100/1000BASE-T Ethernet
10GBASE-T Ethernet
max dužina 100 metara

Specifikacije kabla ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:

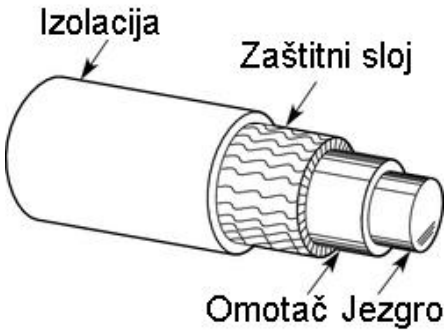
SFTP kabl kat. 6 Draka tip UC400 HS23 4P FRNC/LS0H - testiran do 400MHz, bez halogena

UC400 HS23 Cat.6 S/FTP 4P LSHF

SFTP kabl kat. 6 DRAKA tip UC400 HS23 4P FRNC testiran do 400MHz, sertifikati DELTA, 3P & GHMT - 'Wall', 4 parice, pun presek, širm oko parica, umesto krstastog elementa između parica je u cik-cak postavljena metalna folija što daje bolje karakteristike od standardnog FTP/SFTP kat. 6 kabla, FRNC (omotač bez halogena, nezapaljiv i ne ispušta dim); ostali sertifikati ISO9001, ISO14001, RoHS

3.1.1.4 **Vrste optičkih kablova koji se koriste u projektu**

Optički kablovi koji se koriste za umrežavanje računarskih sistema se sastoje od izolacije, zaštitnog sloja, povećivača savitljivosti, omotača i jezgra.



Slika 3: Izgled optičkog kabla

Optička vlakna se mogu sastojati od tanjih (eng. *singlemode*) koji sadrže jedno vlakno i debljih (eng. *mulitmode*) koji sadrže više vlakana. Singlemode vlakna mogu poslati samo jedan svetlosni signal pa time imaju i manji protok podataka ali mogu postići veću razdaljinu između izvora i prijemnika svetlosti (lasera i foto senzora). *Multimode* vlakna mogu poslati više svetlosnih signala odjednom pa samim tim imaju i drastično veći protok podataka ali je razdaljina između izvora i prijemnika znatno manja.

Kod upotrebe optičkih kablova u računarskim mrežama svaka veza zahteva dva vlakna, jedno za prijem a drugo za slanje podataka.

Vrsta optičkog kabla koji se koristi u projektu je MMF (*Multy-mode fiber*) OM3 50/125 kabl koji omogućava prenos podataka brzinom od 10Gbps na razdaljini od max 300 metara.

> Specifikacije kabla ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:
>
> Draka fiber kabl 24 vlakna 50/125 multimode indoor/outdoor, halogen free, nezapaljiv, sa zaštitom od glodara, U-DQ(ZN)BH 24G50

3.1.1.5 **Strukturno kabliranje**

Postoje tri hijerarhijske vrste strukturnog kabliranja:

1) Kabliranje kampusa (kabliranje između više zgrada)
2) Verikalno kabliranje (povezivanje spratova)
3) Horizontalno kabliranje (povezivanje unutar sprata)

3.1.1.6 **Kabliranje kampusa**

Po specifikacijama projekta postoji ukupno 5 objekata koji moraju biti međusobno umreženi i pritom ispunjavati zahtev maksimalnog protoka od 1 Gbps za svakog mrežnog klijenta kao i nesmetani protok VoIP komunikacije i IP kamera za nadzor.

Kako se ni jedan objekat ne nalazi na udaljenosti većoj od 250 metara kabliranje između zgrada firme bi trebalo obaviti pomoću optičkih kablova (MMF OM3) zbog njihovog protoka od 10 Gbps, kvaliteta signala i skoro neograničenog veka trajanja (nezapaljivi su i imaju zaštitu od glodara).

Postavljanje optičkih kablova treba obaviti na dubini od 1 metar unutar plastičnih cevi. Kablovi ni na jednom mestu ne smeju ostati otkriveni kako bi se umanjila mogućnost oštećenja i samim tim potreba za zamenom.

Pri ulasku kabla unutar objekta radi uspostavljanja konekcije sa ruterom treba obratiti pažnju da se optički kabl što pre prekine (spoji sa ruterom) kako bi se otklonila mogućnost fizičkog oštećenja.

Sve kablove koji dolaze ili odlaze od glavnog čvorišta treba povezati sa svičom preko peč (eng. *patch)* panela kako bi kabliranje bilo što urednije.



Slika 4: Primer sređenog rek ormana sa peč panelima

Zarad pune redundantnosti (dostupnosti mreže) svakom ruteru u kampus sistemu moramo pristupiti sa minimum 2 optičke konekcije od strane drugih rutera. Na taj način omogućavamo da mreža nastavi sa funkcionisanjem i usled gubitka jednog dela kampus mreže.

3.1.1.7 **Vertikalno kabliranje**

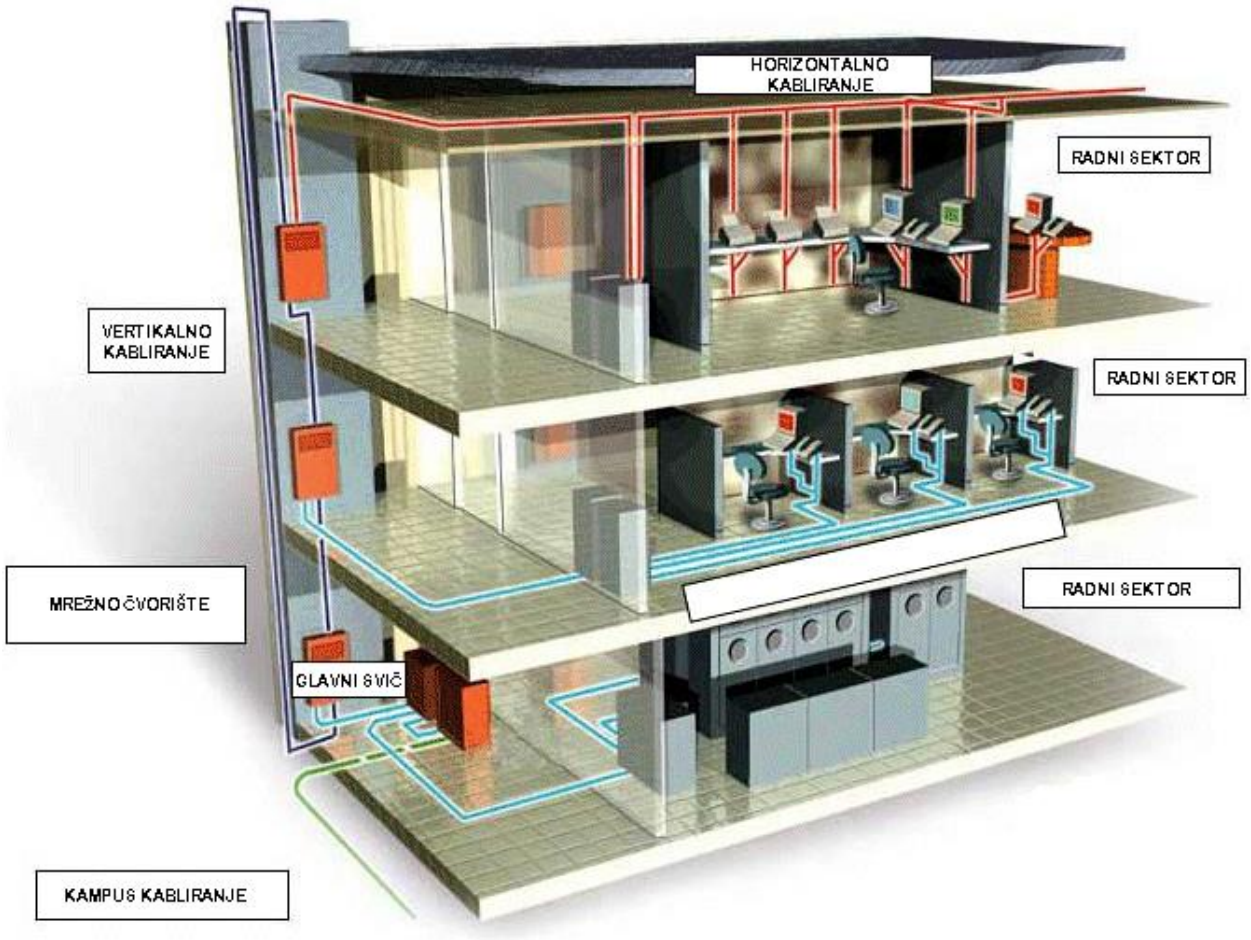
Da bi se realizovalo kvalitetno kabliranje između spratova objekta potrebno je obratiti pažnju na nekoliko stvari:

1) dužina kabla ne bi trebalo da pređe 500 metara, kablove treba voditi na razdaljini većoj od 25 cm od najbližeg električnog voda,
2) truditi se da je kablove što lakše zameniti i izbegavati vođenje kablova sa spoljne strane objekta.
3) Kablove u vertikalnom kabliranju treba povezati što je pre moguće sa mrežnom opremom na spratu/spratovima na kojima će se realizovati mreža.

3.1.1.8 **Horizontalno kabliranje**

Kod realizacije horizontalnog kabliranja (od spratnog svičera do utičnica u zidu) koristi se najveći broj kablova pa treba obratiti posebnu pažnju na sledeće stvari:

1) ukoliko postoji verovatnoća elektro-magnetnog zračenja treba koristiti SFTP kablove,
2) izbegavati vođenje kablova blizu električnih instalacija, u slučaju da nema mogućnosti vođenja kablova unutar zida ili "duplog" poda/plafona najbolje je koristiti zasebne kanalice kojima se kablovi vode do zidnih utičnica,
3) u svakom momentu mora postojati mogućnost lakog i brzog pristupa svim kablovima da bi se po potrebi (usled kvara ili potrebe za nadogradnjom sistema) mogli zameniti.
4) korišćenje peč (eng. *patch*) panela pri konekcijama zidnih kablova sa svičom



Slika 5: Primer strukturnog kabliranja

3.1.2 **Kanalice**

Kanalice se često koriste pri postavljanju svih vrsta mreža kako bi se kvalitetnije, lakše i lepše razvodili kablovi po objektu. Na tržištu postoji veliki broj različitih vrsta kanalica ali će se u projektu koristiti kanalice sledećih dimenzija i specifikacija:

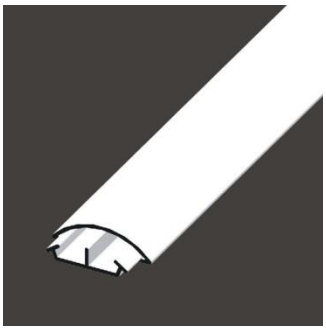
Sve kanalice moraju biti bez halogena, nezapaljive i ne smeju ispuštati dim.

1) 11 mm x 10 mm kanal sa poklopcem



Slika 6: Kanalica dimenzija 11mm x 10mm

2) 34 mm x 10,5 mm kanal sa poklopcem



Slika 7: Kanalica dimenzija 34mm x 10,5mm

3) 100 mm x 60 mm kanal sa poklopcem



Slika 8: Kanalica dimenzija 100mm x 60mm

3.2 **Svičevi (komutatori)**

Svič je jedan od najvažnijih delova svake mreže. Ovaj uređaj prosleđuje podatke od jednog mrežnog segmenta ka drugom. Podatke koje neki od mrežnih klijenata šalje se transmituje isključivo ka odredištu na koje je podatak poslat, za razliku od nekih drugih mrežnih uređaja koji podatke šalju na sve portove. Na ovaj način svič omogućava nesmetanu komunikaciju svih mrežnih klijenata u realnom vremenu (više uređaja može komunicirati istovremeno). Svič ovakvu mogućnost postiže uz pomoć MAC adresa koje upisuje u odgovarajuću internu tabelu iz koje kasnije iščitava adrese ka kojima su paketi poslati. Problemi koji se mogu pojaviti kod korišćenja sviča su preopterećenje portova koje nastaje ako isuviše veliki broj paketa treba da prođe kroz isti port. U tom slučaju dolazi do preopterećenja bafera (eng. *buffer*) i svič odbacuje višak paketa.

Postoji više vrsta svičeva, svičevi koji rade na drugom sloju OSI modela tj. u sloju veze podataka i oni koji rade na trećem sloju. Takođe postoje tzv. managed i unmanaged svičevi. Razlika između upravljivih (eng. *managed*) i neupravljivih (eng. *unmanaged*) svičeva je veoma važna za ovaj projekat. Upravljivi svič omogućava, za razliku od neupravljivog sviča, da mu se pristupi sa udaljene mrežne lokacije, pa samim tim i da se ručno izvrši kontrola protoka na svakom portu, ručno modifikuje brzina i propusna moć svakog od njime kontrolisanih komunikacionih kanala, kao i mogućnost popravke na daljinu. Time se postiže mogućnost visoke kontrole mrežnog saobraćaja i znatno veće brzine otklanjanja tekućih mrežnih problema (administratori ne moraju biti fizički prisutni da bi otklonili problem). L3 svičevi rade na trećem sloju OSI modela tj. u sloju mreže pa zbog toga mogu da korisniku priušte veću količinu brzih portova (10Gbps) i pametno rutiranje podataka ali je njihova tržišna cena i do 2 puta veća od L2 svičeva. U projektu L3 svičevi se moraju koristi na čvorištima između objekata.

Modeli svičeva koji se koristi u projektu:

DCN L3 switch DCRS-5750-28T

L3 managed switch

Portovi: 20 x 10/100/1000 RJ45 + 4 x Combo SFP/UTP+ 2 x 10G (XFP/SFP+)

MAC adresiranje: 8000 adresa

Switching: 128 Gbps

Specifikacije sviča ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:

L3 (statičko, RIP), Gigabit + 10-Gigabit Ethernet, Clustered stekabilni, performanse Cisco Catalyst 3560G serije

L3, upravljivi, 19"/1U, 20 x 10/100/1000 + 4 x dual 10/100/1000 - SFP + 2 slota za 10-Gigabit module + 1 x RJ-45 konzolni RS232 port, 256MB DRAM2 i 16MB flash, 128Gbps/96Mpps performanse, 8K MAK adresa, 4K PVLAN/GVRP/Voice VLAN-ova, Q-in-Q, LACP (128 trankova po 8 portova), UDLD loop zaštita, 9K jumbo frame podrška, STP/RSTP/MSTP sa 48 zapisa, IGMP v3 snooping, MRPP/VRRP/VRRP v3 tehnologija za uspostavljanje redundantnih linkova, 256 ruta (statičkio, RIP v1/v2) i 512 IP interfejsa, 802.1p prioritizacija (8 redova po 8 nivoa), Broadcast/Unicast/Multicast Storm zaštita, Load Balancing, Rate Limiting sa 64Kbps korakom, SP/WRR/SP+WRR, DifferServ, DSCP, 2K ACL, 802.1X i RADIUS/TACACS+, puna IPv6 podrška sa Dual-Stack protokolom, DHCP Server/Client/option 82/snooping, Clustered Stacking do 24 uređaja za upravljanje jednom IP adresom, HTTPS i SSL web interfejs, CLI SSH v2, SNMP v3, SysLog, N:1 Port Mirroring, LLDP, RMON, SNTP, sFlow, smart fan, AC + RPS (+12V) napajanje, DCN napredni DCBI-3000 Security Access Control i Accounting sistem (3D-SMP Ready) sa filtriranjem malicioznih paketa (Blaster, Zero-day, SQL slammer warm, ARP, Synflood, Smurf, ICMP napadi ...), garancija Lifetime

DCN L3 switch DCRS-5750-28T-DC

L3 managed switch

Portovi: 24 x Gigabit (20xUTP+4xCombo SFP/UTP) + 4 x 10G (XFP/SFP+)

MAC Adresiranje: 8000 adresa

Switching: 128 Gbps

Specifikacije sviča ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:

L3 (statičko, RIP), Gigabit + 10-Gigabit Ethernet, Clustered stekabilni, performanse Cisco Catalyst 3560G serije

L3, upravljivi, 19"/1U, 20 x 10/100/1000 + 4 x dual 10/100/1000 - SFP + 2 slota za 10-Gigabit module + 1 x RJ-45 konzolni RS232 port, 256MB DRAM2 i 16MB flash, 128Gbps/96Mpps performanse, 8K MAK adresa, 4K PVLAN/GVRP/Voice VLAN-ova, Q-in-Q, LACP (128 trankova po 8 portova), UDLD loop zaštita, 9K jumbo frame podrška, STP/RSTP/MSTP sa 48 zapisa, IGMP v3 snooping, MRPP/VRRP/VRRP v3 tehnologija za uspostavljanje redundantnih linkova, 256 ruta (statičkio, RIP v1/v2) i 512 IP interfejsa, 802.1p prioritizacija (8 redova po 8 nivoa), Broadcast/Unicast/Multicast Storm zaštita, Load Balancing, Rate Limiting sa 64Kbps korakom, SP/WRR/SP+WRR, DifferServ, DSCP, 2K ACL, 802.1X i RADIUS/TACACS+, puna IPv6 podrška sa Dual-Stack protokolom, DHCP Server/Client/option 82/snooping, Clustered Stacking do 24 uređaja za upravljanje jednom IP adresom, HTTPS i SSL web interfejs, CLI SSH v2, SNMP v3, SysLog, N:1 Port Mirroring, LLDP, RMON, SNTP, sFlow, smart fan, AC + DC (-48V) dual napajanje, DCN napredni DCBI-3000 Security Access Control i Accounting sistem (3D-SMP Ready) sa filtriranjem malicioznih paketa (Blaster, Zero-day, SQL slammer warm, ARP, Synflood, Smurf, ICMP napadi ...), garancija Lifetime

TP-Link TL-SG2216WEB

L2 managed switch

Portovi: 16 x 10/100/1000 RJ45 ports, 2 SFP expansion slots

Specifikacije sviča ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:

16-port Pure-Gigabit Web Smart Switch, 16 10/100/1000 RJ45 ports, 2 SFP expansion slots

TP-Link TL-SG2216WEB 16-port Gigabit Managed Switch 16x10/100/1000Mb/s+2xSFP slot, 802.1Q VLAN, QoS, Security, 19" rack, AC 100-240V / 50-60Hz

TP-Link TL-SG1008

L2 unmanaged switch

Portovi: 8 x 10/100/1000 RJ45

Wirespeed: 16Gb/s bandwith

Specifikacije sviča ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:

8-port Gigabit Switch, 8 10/100/1000M RJ45 ports, 1U rack-mountable steel case

TP-Link TL-SG1008 8-port Gigabit 10/100/1000Mb/s Switch, 19" rackmount, interno napajanje AC 100-240V / 50-60Hz, wirespeed 16Gb/s bandwidth

3.3 **Ruteri**

Ruteri za razliku od drugih mrežnih uređaja rade na trećem sloju OSI modela tj. na mrežnom sloju. Njihova glavna namena je usmeravanje paketa podataka ka njihovom odredištu. Način na koji ruter postiže ovu funkciju je odredišna adresa koja je smeštena u svakom paketu. Uz pomoć nje, ruter u svojoj tabeli rutiranja pronalazi gde su smešteni podaci i na koji port treba da se paket prosledi. Na taj način ruter određuje adresu sledećeg rutera na putu do adrese na koju paket treba da stigne. Naziv ovog procesa je *address lookup*. Posle završetka ovog procesa ruter vrši proces komutiranja (eng. *switching*) gde se paket prosleđuje sa ulaznog porta ka portu sa kog treba da se pošalje dalje. U projektu se ruter koristi kao čvorište između internet dobavljača i kampus mreže. U sebi mora da poseduje opciju *load balance* koja omogućava spajanje više internet konekcija i njihovu distribuciju ka mreži.

Model load balancera rutera koji se koristi u projektu:

MikroTik RouterBoard 1100AH

Specifikacije:

Portovi: 13 Gigabit LAN / WAN portova

Specifikacije rutera ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:

Ostale specifikacije: VPN ruter / Firewall / Bandwith manager, MPC8533 CPU 1066MHz, 2GB RAM, microSD card slot, RouterOS L6 (neograničen broj konekcija)

3.4 **Bežični (*WiFi*) ruteri**

Bežični ruteri imaju slične osobine kao i standardni ruteri osim što pružaju i opciju konekcije klijenata preko bežične (eng. *wireless*) mreže.

Model bežičnog (*WiFi*) rutera koji se koristi u projektu:

TP-Link TL-WR1043ND 300Mb/s wireless 2.4GHz firewall

Specifikacije:

1 x gigabit WAN + 4 x gigabit UTP LAN 10/100/1000Mb/s + 1 x USB2.0 storage, Atheros čip 100mW (20dBm), 3T3R MIMO, SST, CCA, 3 x antene RP-SMA

Specifikacije rutera ili njegov tržišni ekvivalent koji bi trebalo da se koristi u projektu:

Ultimate wireless 300Mb/s 802.11N Gigabit Router, Atheros, 3T3R, 2.4GHz, 1 WAN + 4 LAN Gigabit 10/100/1000Mb/s + 1 USB 2.0 Port (za deljenje podataka sa USB Flash diskova preko mreže), MIMO (Multiple Input, Multiple Output) tehnologija sa boljim prostiranjem signala i većim pokrivanjem uz stabilniju vezu, CCA tehnologija za izbegavanje konflikta kanala, SST za povećanje robustnosti i stabilnosti linka, UPnP, DDNS, VPN Pass-through, virtual server, DMZ host, SSID broadcast control, MAC access control list, 64/128/152-bit WEP, WPA standard(TKIP/AES), MIC, Firewall IP / MAC / URL filtering i sve ostale brojne softverske mogućnosti kao kod drugih TP-Link rutera, izlazna snaga 20dBm = 100mW, tri antene sa RP-SMA konektorom za opcione jače antene i još veće povećanje dometa

3.5 **Kriptološki uređaji**

Kriptološki uređaji služe kao osnovne delovi hardverske zaštite podataka koji se prenose putem računarski mreža. Njihova osnovna namena jeste da podatke koji se šalju preko mreže šifrira i kao takve prosledi dalje ka krajnjem primaocu koji ih zatim uz pomoć kriptološkog uređaja dešifruje a zatim i koristi. Na ovaj način stiče se bezbednost podataka koji su najranjiviji kada se šalju preko mreže i ponajviše interneta. U ovom projektu koriste se kao uređaji koji treba da zaštite VPN konekciju između matične mreže i objekta u kome se nalazi prodaja.

IP VPN Encryption HC-7845 Gigabit Version

Specifikacije uređaja:

Kriptologija i sigurnost:

Algoritam HCA-480, korisničko specifikovan šifarski algoritam; Korisničko kontrolisani profili algoritama CMP sa mogućnošću > 10^{506} ; Šema za međusobni dogovor oko ključeva za kratkoročne Komunikacione ključeve (CKs); Svaki enkripovani tunel koristi nezavisne komunikacione ključeve; Generator slučajnih brojeva vrhunsko kvaliteta.

Ključevi:

Korisničko definisani glavni komunikacioni ključevi (MCKs, za CK generisanje) se čuvaju u *tamper-proof* sigurnosnom modulu; Glavni komunikacioni ključevi i komunikacioni ključevi sa varijantama > 10^{38}

Upravljanje ključevima:

Ručni unos ključeva preko korisničkog interfejsa; Kopiranje i *backup* ključeva i instalacionih podataka putem *Security Data Carriers* (SDCs)

Offline sa SMC-1100 IP VPN i SDC, *Online* sa SMC-1100 IP VPN

Tamper-proof dizajn:

Role based access control; Block function; Emergency clear; Tamper evidence; Tamper detection & response (reset to ex-factory state); Metalno kućište sa mehaničkom bravom; Ugrađeni sigurnosni modul

Servisi:

Podržani servisi:

Unicast IP VPN tunnels (tunnel mode), Multicast IP VPN tunnels (tunnel mode), Throughput near wire-speed on world-side with 1500 byte IP packets > 2000 tunnels, Vrste saobraćaja: data/voice/video

DHCP server, DHCP klijent, Statičko rutiranje ili RIP-II, NAT support.

Konekcije:

IEEE 802.3 Ethernet, Transceiver SFP modules:

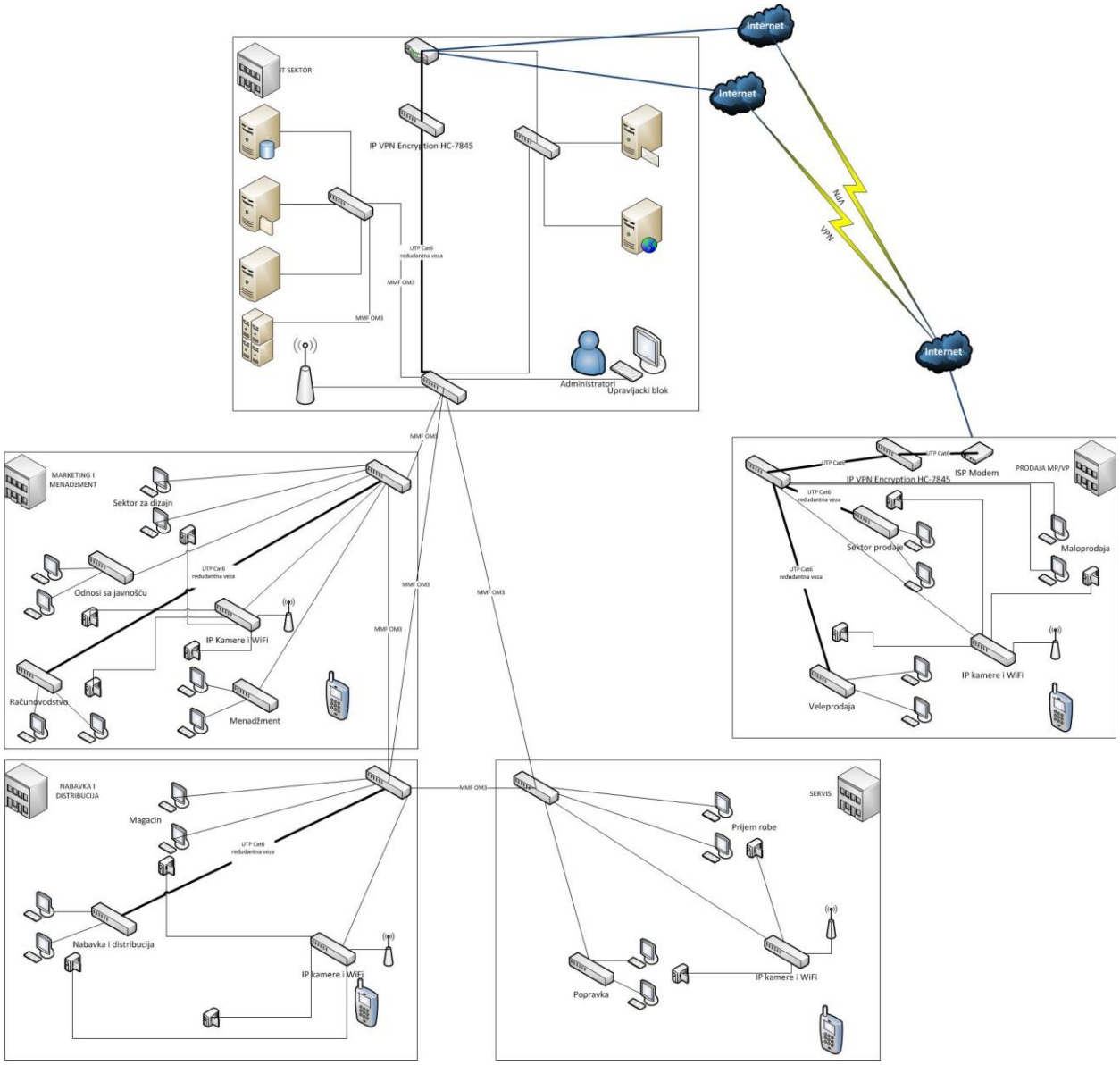
- RJ45, 10BASE-T/100BASE-TX/ 1000BASE-T

- ili optical LC, 1000BASE-SX, -LX, -ZX

4 Implementacija sistema

Firma poseduje pet objekata u kojima se realizuje mreža, to su:

1) Marketing i menadžment
2) Nabavka i distribucija
3) Prodaja (VPN konekcija)
4) Servis
5) IT sektor



Slika 9: Dijagram kampus mreže

4.1 **Marketing i menadžment**

Unutar ovog objekta postoje četiri pod sektora sa određenim brojem mrežnih klijenata:

1) Sektor za dizajn
2) Odnosi sa javnošću
3) Računovodstvo
4) Menadžment

Ukupan broj mrežnih klijenata u ovom objektu je 56 i to:

1) 26 x PC
2) 1 x Ploter
3) 22 x VoIP telefona
4) 6 x IP kamera
5) 1 x WiFi ruter

4.1.1 **Sektor za dizajn**

Mrežni klijenti:

1) 5 x PC
2) 1 x Ploter
3) 1 x VoIP telefona
4) 1 x IP kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 8 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 12 RJ45 zidnih priključaka. Zbog visoke cene rutera ovaj sektor bi trebalo direktno priključiti na DCN L3 switch DCRS-5750-28T svič koji se nalazi na čvorištu između objekta i kampus mreže. Kablove od sviča treba voditi najkraćim mogućim putem do zidnih utičnica i pritom paziti na vodove električnih instalacija. Kablove treba postaviti unutar kanalica dimenzija 100 mm x 60 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Na mestu gde treba odvojiti jedan ili više kablova da bi se sproveli do zidne utičnice treba koristiti kanalice dimenzija 11 mm x 10 mm koje treba postaviti vertikalno u odnosu na kanalicu glavnog voda. Zbog velike količine kablova koji su po pravilu povezani u snop (da bi im se lakše pristupilo u slučaju potrebe za zamenom) treba koristiti S/FTP class F kablove kako bi se izbeglo EM zračenje. Od utičnice do samih klijenata koriste se UTP Cat5e kablovi. Na ovaj način postiže se maksimalna brzina protoka podataka od 1Gbps za svakog od navedenih mrežnih klijenta.

4.1.2 **Odnosi sa javnošću**

Mrežni klijenti:

1) 5 x PC
2) 5 x VoIP Telefona
3) 1 x IP kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 11 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 15 RJ45 zidnih priključaka. Da bi se realizovao dovoljan broj mrežnih priključaka unutar sektora treba koristiti jedan TP-Link TL-SG2216WEB svič do kog će voditi jedan UTP Cat6 kabl od glavnog čvorišta objekta koje čini DCN L3 switch DCRS-5750-28T svič. Taj glavni "dovodni" kabl treba postaviti unutar kanalica dimenzija 11 mm x 10 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Razvodni TP-Link svič treba postaviti unutar rek ormana maksimalne veličine 4U koji se nalazi unutar sobe. Kablove (UTP Cat5e) od samog razvodnog sviča do zidnih utičnica treba voditi kanalicama dimenzija 11 mm x 10 mm ili po potrebi podnim kanalicama dimenzija 34 mm x 10,5 mm. Zbog male količine EM zračenja koje deluje na mrežne vodove mogu se koristiti samo UTP kablovi i na taj način se smanjuje visina cene projekta. Ovaj sektor nema potrebe za velikom količinom razmene podataka između servera i klijenata, a nasuprot tome veliku potrebu za razmenom velike količine VoIP podataka. Svaki VoIP klijent bi trebalo da ima pod najvećim opterećenjem lokalne mreže bar 10Mbps protka što je više nego dovoljno za nesmetani protok VoIP podataka.

4.1.3 **Računovodstvo**

Mrežni klijenti:

1) 10 x PC
2) 10 x VoIP Telefona
3) 1 x IP kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 21 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 28 RJ45 zidnih priključaka. Da bi se realizovao dovoljan broj mrežnih priključaka unutar sektora treba koristiti jedan DCN L3 switch DCRS-5750-28T svič od kog će voditi dva S/FTP kabla koji će omogućiti brzinu protoka od 2 Gbps do glavnog čvorišta objekta koje čini DCN L3 switch DCRS-5750-28T svič. Te glavne "dovodne" kablove treba postaviti unutar kanalica dimenzija 11 mm x 10 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Razvodni DCN

L3 switch DCRS-5750-28T svič treba postaviti unutar rek ormana maksimalne veličine 4U koji se nalazi unutar sobe. Kablove (UTP Cat5e) od samog razvodnog sviča do zidnih utičnica i bar jednog TP-Link TL-SG1008 sviča treba voditi kanalicama dimenzija 11 mm x 10 mm ili po potrebi podnim kanalicama dimenzija 34 mm x 10,5 mm. Zbog male količine EM zračenja koje deluje na mrežne vodove mogu se koristiti samo UTP kablovi i na taj način se smanjuje visina cene projekta. Na ovaj način optimalna brzina protoka podataka za svakog klijenta bi trebalo da iznosi 1Gbps.

4.1.4 **Menadžment**

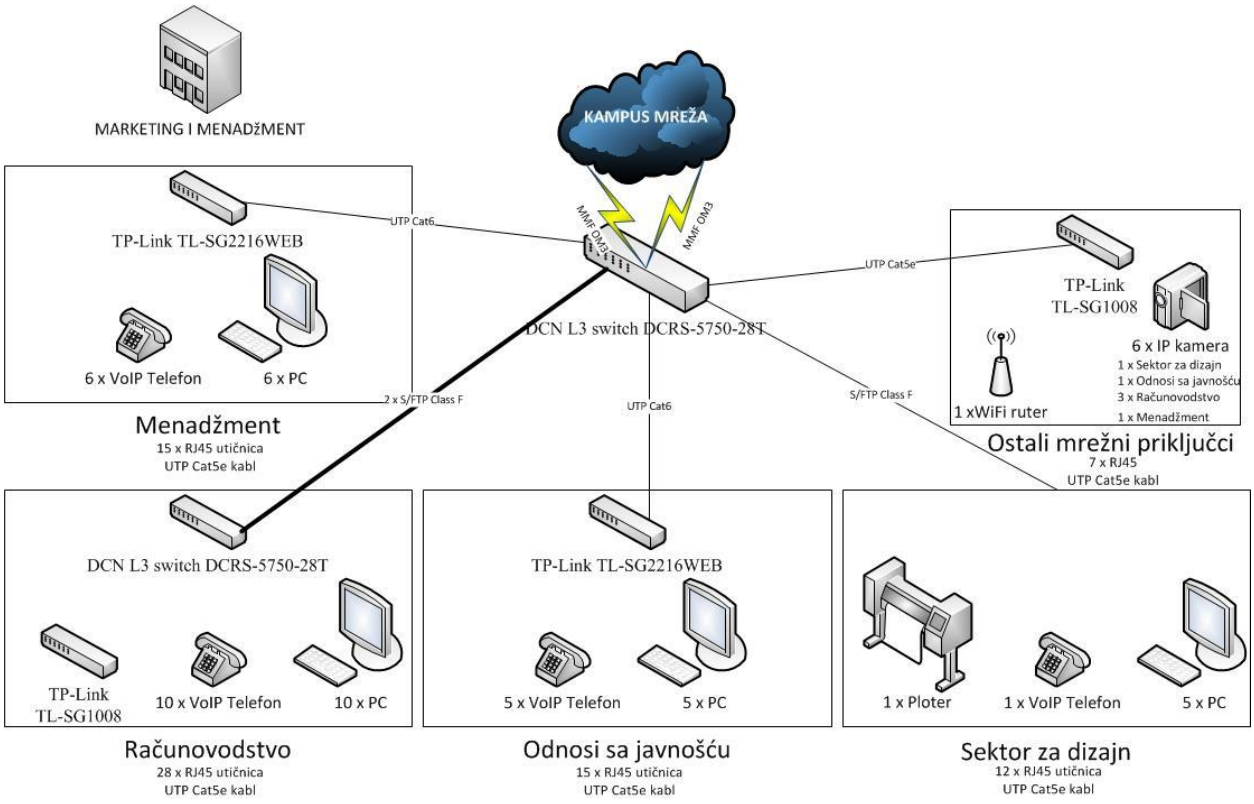
Mrežni klijenti:

1) 6 x PC
2) 6 x VoIP Telefona
3) 1 x IP Kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 12 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 15 RJ45 zidnih priključaka. Da bi se realizovao dovoljan broj mrežnih priključaka unutar sektora treba koristiti jedan TP-Link TL-SG2216WEB svič do kog će voditi jedan UTP Cat6 kabl od glavnog čvorišta objekta koje čini DCN L3 switch DCRS-5750-28T svič. Taj glavni "dovodni" kabl treba postaviti unutar kanalica dimenzija 11 mm x 10 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Razvodni TP-Link svič treba postaviti unutar rek ormana maksimalne veličine 4U koji se nalazi unutar sobe. Kablove (UTP Cat5e) od samog razvodnog sviča do zidnih utičnica treba voditi kanalicama dimenzija 11 mm x 10 mm ili po potrebi podnim kanalicama dimenzija 34 mm x 10,5 mm. Zbog male količine EM zračenja koje deluje na mrežne vodove mogu se koristiti samo UTP kablovi i na taj način se smanjuje visina cene projekta. Na ovaj način optimalna brzina protoka podataka za svakog klijenta bi trebalo da iznosi 1Gbps.

4.1.5 **Ostali mrežni priključci**

Direktno na DCN L3 switch DCRS-5750-28T svič koji se nalazi na glavnom čvorištu zgrade treba priključiti još jedan TP-Link TL-SG1008 svič na koji se priključuju sve IP kamere (kamere se povezuju preko UTP Cat5e kablova koji se postavljaju unutar kanalica dimenzija 11 mm x 10 mm) u objektu i jedan WiFi ruter. Svič TP-Link TL-SG1008 i WiFi ruter postavljaju se u blizini sviča i povezuju direktno UTP Cat5e kablom.



Slika 10: Dijagram LAN mreže u objektu MARKETING I MENADžMENT

4.2 **Nabavka i distribucija**

Unutar ovog objekta postoje dva pod sektora sa određenim brojem mrežnih klijenata:

1) Sektor za nabavke i distribuciju
2) Magacin

Ukupan broj mrežnih klijenata u ovom objektu je 39 i to:

1) 15 x PC
2) 15 x VoIP telefona
3) 6 x IP kamera
4) 1 x WiFi ruter

4.2.1 **Sektor za nabavke i distribuciju**

Mrežni klijenti:

1) 10 x PC
2) 10 x VoIP Telefona
3) 1 x IP Kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 21 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 28 RJ45 zidnih priključaka. Da bi se realizovao dovoljan broj mrežnih priključaka unutar sektora treba koristiti jedan DCN L3 switch DCRS-5750-28T svič od kog će voditi dva S/FTP kabla koji će omogućiti brzinu protoka od 2 Gbps do glavnog čvorišta objekta koje čini DCN L3 switch DCRS-5750-28T svič. Te glavne "dovodne" kablove treba postaviti unutar kanalica dimenzija 11 mm x 10 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Razvodni DCN L3 switch DCRS-5750-28T svič treba postaviti unutar rek ormana maksimalne veličine 4U koji se nalazi unutar sobe. Kablove (UTP Cat5e) od samog razvodnog sviča do zidnih utičnica i bar jednog TP-Link TL-SG1008 sviča treba voditi kanalicama dimenzija 11 mm x 10 mm ili po potrebi podnim kanalicama dimenzija 34 mm x 10,5 mm. Zbog male količine EM zračenja koje deluje na mrežne vodove mogu se koristiti samo UTP kablovi i na taj način se smanjuje visina cene projekta. Na ovaj način optimalna brzina protoka podataka za svakog klijenta bi trebalo da iznosi 1Gbps.

4.2.2 **Magacin**

Mrežni klijenti:

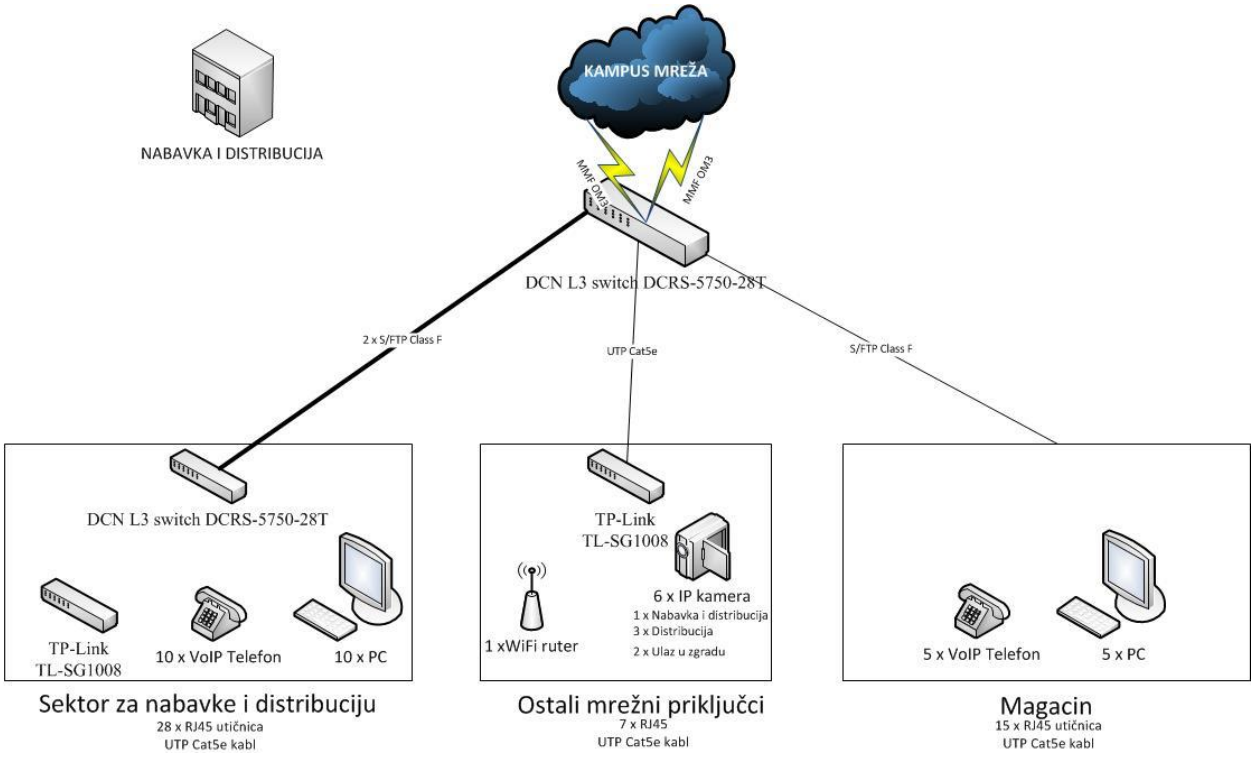
1) 5 x PC
2) 5 x VoIP Telefona
3) 3 x IP Kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 13 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 15 RJ45 zidnih priključaka. Zbog visoke cene rutera ovaj sektor bi trebalo direktno priključiti na DCN L3 switch DCRS-5750-28T svič koji se nalazi na čvorištu između objekta i kampus mreže. Kablove od sviča treba voditi najkraćim mogućim putem do zidnih utičnica i pritom paziti na vodove električnih instalacija. Kablove treba postaviti unutar kanalica dimenzija 100 mm x 60 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Na mestu gde treba odvojiti jedan ili više kablova da bi se sproveli do zidne utičnice treba koristiti kanalice dimenzija 11 mm

x 10 mm koje treba postaviti vertikalno u odnosu na kanalicu glavnog voda. Zbog velike količine kablova koji su po pravilu povezani u snop (da bi im se lakše pristupilo u slučaju potrebe za zamenom) treba koristiti S/FTP class F kablove kako bi se izbeglo EM zračenje. Od utičnice do samih klijenata koriste se UTP Cat5e kablovi. Na ovaj način postiže se maksimalna brzina protoka podataka od 1Gbps za svakog od navedenih mrežnih klijenta.

4.2.3 **Ostali mrežni priključci**

Direktno na DCN L3 switch DCRS-5750-28T svič koji se nalazi na glavnom čvorištu zgrade treba priključiti još jedan TP-Link TL-SG1008 svič na koji se priključuju sve IP kamere (kamere se povezuju preko UTP Cat5e kablova koji se postavljaju unutar kanalica dimenzija 11 mm x 10 mm) u objektu i jedan WiFi ruter. Svič TP-Link TL-SG1008 i WiFi ruter postavljaju se u blizini sviča i povezuju direktno UTP Cat5e kablom.



Slika 11: Dijagram LAN mreže u objektu NABAVKA I DISTRIBUCIJA

4.3 **Prodaja**

Unutar ovog objekta postoje tri pod sektora sa određenim brojem mrežnih klijenata:

1) Sektor prodaje
2) Maloprodaja
3) Veleprodaja

Ukupan broj mrežnih klijenata u ovom objektu je 54 i to:

1) 25 x PC
2) 22 x VoIP telefona
3) 6 x IP kamera
4) 1 x WiFi ruter

4.3.1 **Sektor prodaje**

Mrežni klijenti:

1) 10 x PC
2) 10 x VoIP Telefona
3) 1 x IP Kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 21 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 28 RJ45 zidnih priključaka. Da bi se realizovao dovoljan broj mrežnih priključaka unutar sektora treba koristiti jedan DCN L3 switch DCRS-5750-28T svič od kog će voditi dva S/FTP kabla koji će omogućiti brzinu protoka od 2 Gbps do glavnog čvorišta objekta koje čini DCN L3 switch DCRS-5750-28T svič. Te glavne "dovodne" kablove treba postaviti unutar kanalica dimenzija 11 mm x 10 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Razvodni DCN L3 switch DCRS-5750-28T svič treba postaviti unutar rek ormana maksimalne veličine 4U koji se nalazi unutar sobe. Kablove (UTP Cat5e) od samog razvodnog sviča do zidnih utičnica i bar jednog TP-Link TL-SG1008 sviča treba voditi kanalicama dimenzija 11 mm x 10 mm ili po potrebi podnim kanalicama dimenzija 34 mm x 10,5 mm. Zbog male količine EM zračenja koje deluje na mrežne vodove mogu se koristiti samo UTP kablovi i na taj način se smanjuje visina cene projekta. Na ovaj način optimalna brzina protoka podataka za svakog klijenta bi trebalo da iznosi 1Gbps.

4.3.2 **Maloprodaja**

Mrežni klijenti:

1) 5 x PC

2) 2 x VoIP Telefona
3) 3 x IP Kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 10 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 12 RJ45 zidnih priključaka. Zbog visoke cene rutera ovaj sektor bi trebalo direktno priključiti na DCN L3 switch DCRS-5750-28T svič koji se nalazi na čvorištu između objekta i kampus mreže, dok bi konektovanje IP Kamera trebalo obaviti preko TP-Link TL-SG1008 sviča koji treba direktno povezati sa glavnim DCN L3 svičom. Kablove od sviča treba voditi najkraćim mogućim putem do zidnih utičnica i pritom paziti na vodove električnih instalacija. Kablove treba postaviti unutar kanalica dimenzija 100 mm x 60 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Na mestu gde treba odvojiti jedan ili više kablova da bi se sproveli do zidne utičnice treba koristiti kanalice dimenzija 11 mm x 10 mm koje treba postaviti vertikalno u odnosu na kanalicu glavnog voda. Zbog velike količine kablova koji su po pravilu povezani u snop (da bi im se lakše pristupilo u slučaju potrebe za zamenom) treba koristiti S/FTP class F kablove kako bi se izbeglo EM zračenje. Od utičnice do samih klijenata koriste se UTP Cat5e kablovi. Na ovaj način postiže se maksimalna brzina protoka podataka od 1Gbps za svakog od navedenih mrežnih klijenta.

4.3.3 **Veleprodaja**

Mrežni klijenti:

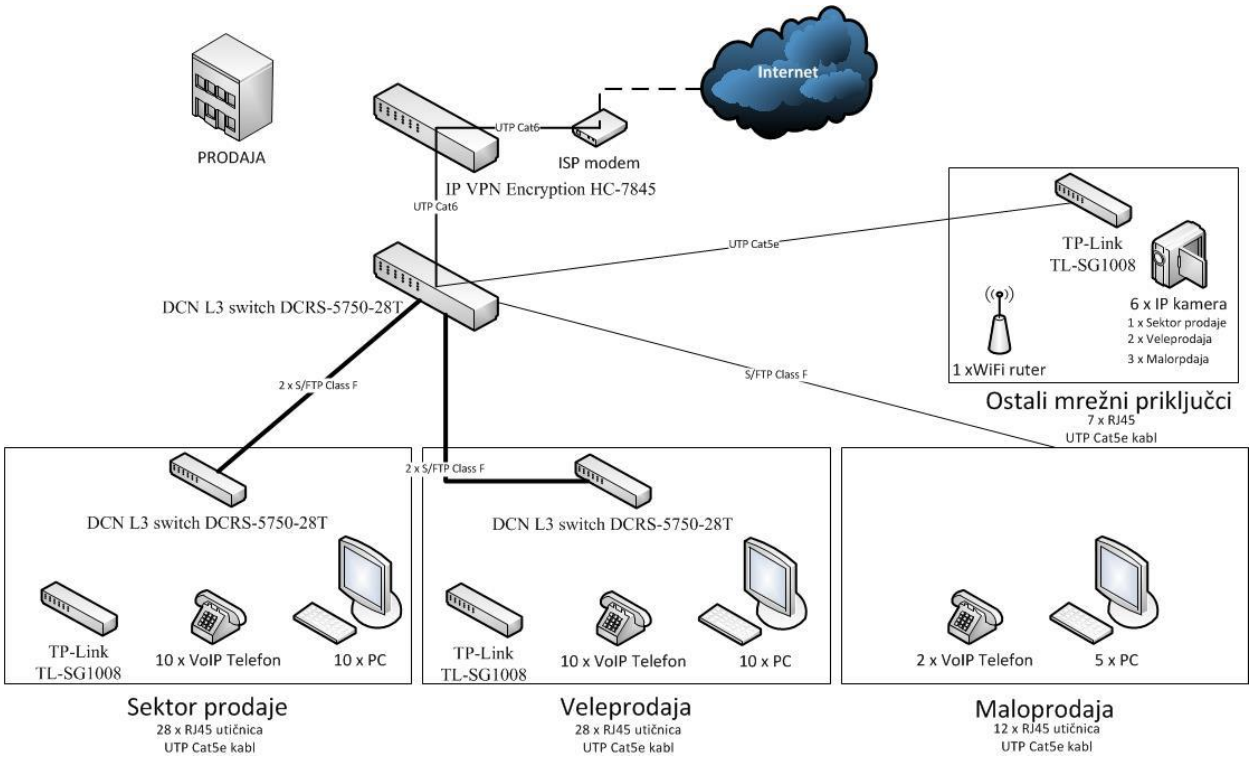
1) 10 x PC
2) 10 x VoIP Telefona
3) 2 x IP Kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 22 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 28 RJ45 zidnih priključaka. Da bi se realizovao dovoljan broj mrežnih priključaka unutar sektora treba koristiti jedan DCN L3 switch DCRS-5750-28T svič od kog će voditi dva S/FTP kabla koji će omogućiti brzinu protoka od 2 Gbps do glavnog čvorišta objekta koje čini DCN L3 switch DCRS-5750-28T svič. Te glavne "dovodne" kablove treba postaviti unutar kanalica dimenzija 34 mm x 10,5 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Razvodni DCN L3 switch DCRS-5750-28T svič treba postaviti unutar rek ormana maksimalne veličine 4U koji se nalazi unutar sobe. Kablove (UTP Cat5e) od samog razvodnog sviča do zidnih utičnica i bar jednog TP-Link TL-SG1008 sviča treba voditi kanalicama dimenzija 11 mm x 10 mm ili po potrebi podnim kanalicama dimenzija 34 mm x 10,5 mm. Zbog male količine EM zračenja koje deluje na mrežne vodove mogu se koristiti samo UTP kablovi i na taj način se smanjuje visina

cene projekta. Na ovaj način optimalna brzina protoka podataka za svakog klijenta bi trebalo da iznosi 1Gbps.

4.3.4 **Ostali mrežni priključci**

Direktno na DCN L3 switch DCRS-5750-28T svič koji se nalazi na glavnom čvorištu zgrade treba priključiti još jedan TP-Link TL-SG1008 svič na koji se priključuju sve IP kamere (kamere se povezuju preko UTP Cat5e kablova koji se postavljaju unutar kanalica dimenzija 11 mm x 10 mm) u objektu i jedan WiFi ruter. Svič TP-Link TL-SG1008 i WiFi ruter postavljaju se u blizini sviča i povezuju direktno UTP Cat5e kablom.



Slika 12: Dijagram LAN mreže u objektu PRODAJA

4.4 **Servis**

Unutar ovog objekta postoje dva pod sektora sa određenim brojem mrežnih klijenata:

1) Prijem robe
2) Popravka

Ukupan broj mrežnih klijenata u ovom objektu je 54 i to:

1) 12 x PC
2) 6 x VoIP telefona
3) 4 x IP kamera
4) 1 x WiFi ruter

4.4.1 **Prijem robe**

Mrežni klijenti:

1) 2 x PC
2) 4 x VoIP Telefona
3) 1 x IP Kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 7 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 10 RJ45 zidnih priključaka. Zbog visoke cene rutera ovaj sektor bi trebalo direktno priključiti na DCN L3 switch DCRS-5750-28T svič koji se nalazi na čvorištu između objekta i kampus mreže. Kablove od sviča treba voditi najkraćim mogućim putem do zidnih utičnica i pritom paziti na vodove električnih instalacija. Kablove treba postaviti unutar kanalica dimenzija 100 mm x 60 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Na mestu gde treba odvojiti jedan ili više kablova da bi se sproveli do zidne utičnice treba koristiti kanalice dimenzija 11 mm x 10 mm koje treba postaviti vertikalno u odnosu na kanalicu glavnog voda. Zbog velike količine kablova koji su po pravilu povezani u snop (da bi im se lakše pristupilo u slučaju potrebe za zamenom) treba koristiti S/FTP class F kablove kako bi se izbeglo EM zračenje. Od utičnice do samih klijenata koriste se UTP Cat5e kablovi. Na ovaj način postiže se maksimalna brzina protoka podataka od 1Gbps za svakog od navedenih mrežnih klijenta.

4.4.2 **Popravka**

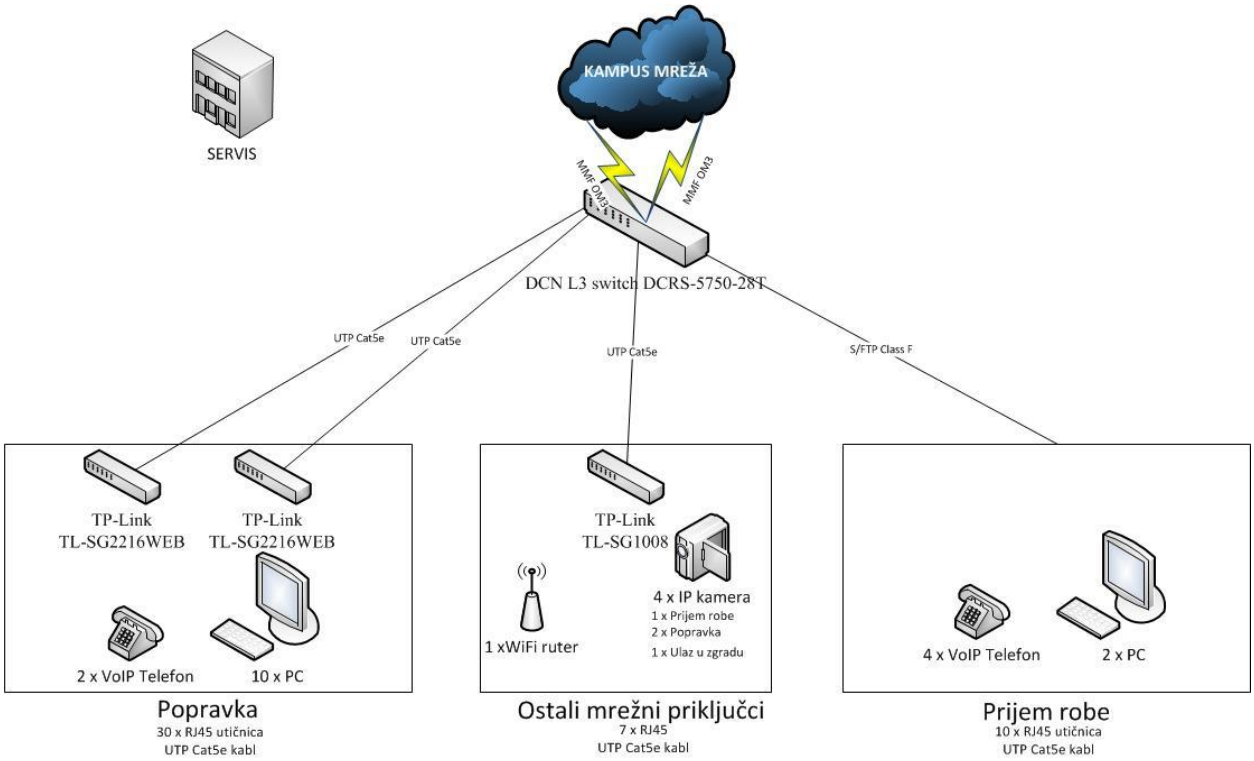
Mrežni klijenti:

1) 10 x PC
2) 2 x VoIP Telefona
3) 2x IP Kamera

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 14 ali da bi se u slučaju potrebe za proširenjem broja klijenata i konstantne potrebe za priključivanjem privremenih klijenata (zbog testiranja i popravke) otklonio problem kabliranja potrebno je realizovati bar 30 RJ45 zidnih priključaka. Da bi se realizovao dovoljan broj mrežnih priključaka unutar sektora treba koristiti dva TP-Link TL-SG2216WEB sviča do kojih će voditi po jedan UTP Cat6 kabl od glavnog čvorišta objekta koje čini DCN L3 switch DCRS-5750-28T svič. Te glavne "dovodne" kablove treba postaviti unutar kanalica dimenzija 11 mm x 10 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Razvodne TP-Link svič treba postaviti unutar rek ormana maksimalne veličine 4U koji se nalazi unutar sobe. Kablove (UTP Cat5e) od samog razvodnog sviča do zidnih utičnica treba voditi kanalicama dimenzija 11 mm x 10 mm ili po potrebi podnim kanalicama dimenzija 34 mm x 10,5 mm. Zbog male količine EM zračenja koje deluje na mrežne vodove mogu se koristiti samo UTP kablovi i na taj način se smanjuje visina cene projekta.

4.4.3 **Ostali mrežni priključci**

Direktno na DCN L3 switch DCRS-5750-28T svič koji se nalazi na glavnom čvorištu zgrade treba priključiti još jedan TP-Link TL-SG1008 svič na koji se priključuju sve IP kamere (kamere se povezuju preko UTP Cat5e kablova koji se postavljaju unutar kanalica dimenzija 11 mm x 10 mm) u objektu i jedan WiFi ruter. Svič TP-Link TL-SG1008 i WiFi ruter postavljaju se u blizini sviča i povezuju direktno UTP Cat5e kablom.



Slika 13: Dijagram LAN mreže u objektu SERVIS

4.5 **IT sektor**

Najvažniji sektor kampus mreže nalazi se u ovom objektu stoga posebnu pažnju treba obratiti na njegovu redudantnost.

Unutar ovog objekta postoje dva pod sektora sa određenim brojem mrežnih klijenata:

1) Server soba
2) IT Administracija

Mrežni klijenti:

1) Server baze podataka (*Data Base server*)
2) Fajl (*File*) server
3) Veb (*Web*) server
4) Server za elektronsku poštu (*Mail* server)
5) Sigurnosni (*Security*) server
6) Aplikativni (*Aplication*) server
7) Menadžment server
8) 4 x PC

9) 2 x NB
10) 2 x VoIP
11) 4 x IP Kamera
12) 1 x WiFi ruter
13) 2 x Internet modem
14) 1 x Load Balancer ruter

Ukupan broj mrežnih priključaka potrebnih u celom objektu je 21 ali da bi se omogućilo naknadno proširenje mreže treba obezbediti bar 30 RJ45 priključaka.

4.5.1 **Server soba**

Mrežni klijenti:

1) Server baze podataka (*Data Base server*)
2) Fajl (*File*) server
3) Veb (*Web*) server
4) Server za elektronsku poštu (*Mail* server)
5) Sigurnosni (*Security*) server
6) Aplikativni (*Aplication*) server
7) Menadžment server
8) Load balancer ruter
9) 2 x Internet modem
10) IP VPN Encryption HC-7845
11) 1 x IP Kamera

Ukupan broja klijenata u ovom sektoru je 12 pa je potrebno realizovati bar dvadeset RJ45 priključaka sa brzinom protoka na svakom portu koja ne sme biti ispod 1 Gbps.

Da bi se realizovao dovoljan broj priključaka sa velikom brzinom protoka podataka treba koristiti DCN L3 switch DCRS-5750-28T-DC svič na glavnom čvorištu objekta (unutar reka u server sobi) i kampus mreže na koji treba optičkim kablom MMF OM3 povezati DCN L3 switch DCRS-5750-28T svič koji se nalazi unutar server sobe. Na ovaj način dobijamo brzinu od 10 Gbps između čvorišta sobe i kampus mreže. Pri kabliranju optičkim kablovima unutar objekta treba obratiti pažnju na sledeće:

Kablove treba voditi najkraćim mogućim putem između klijenta.

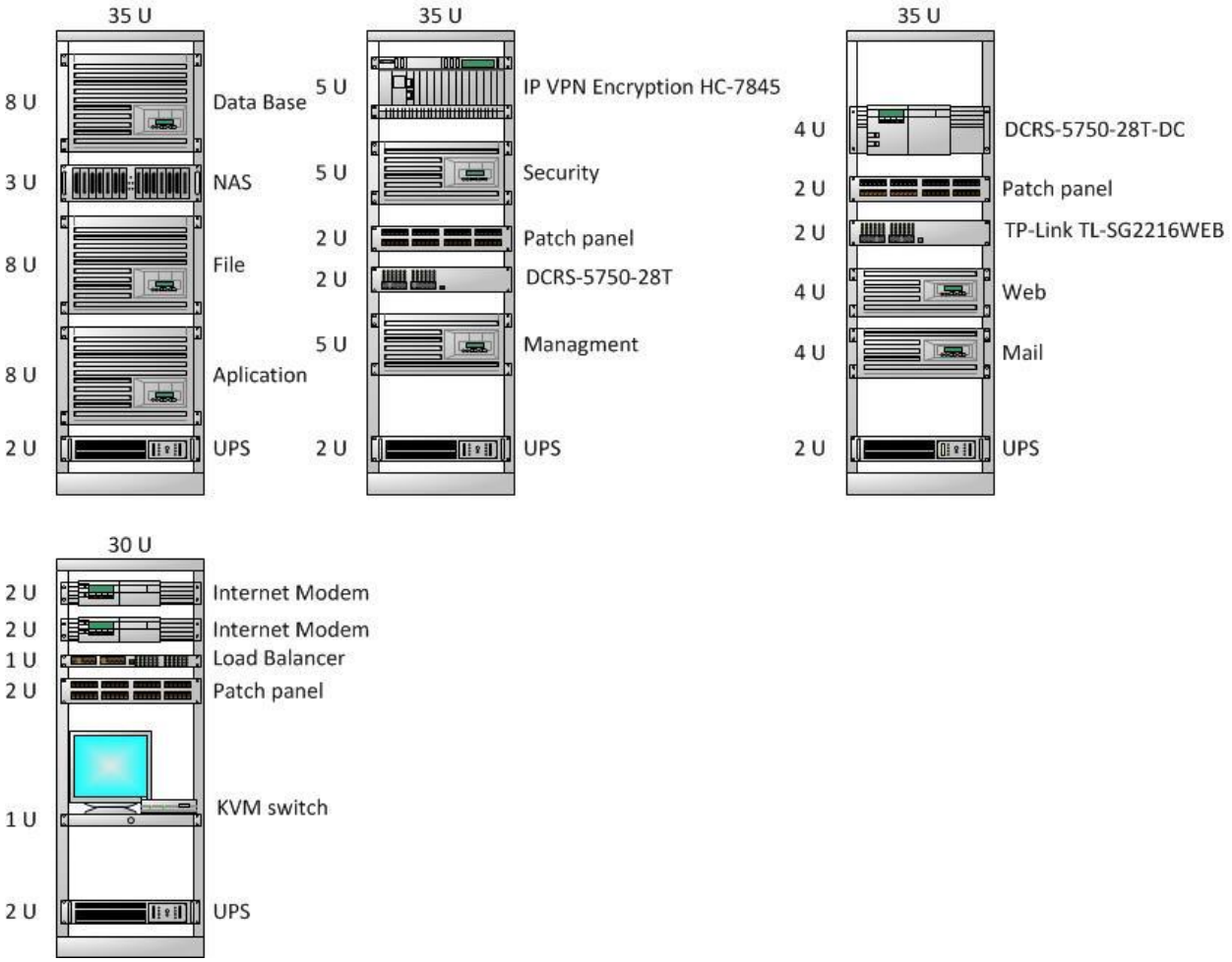
Posebna pažnja treba da se posveti zaštiti kablova od fizičkog oštećenja te ih treba postavljati unutar zidova ili u suprotnom unutar kanalica koje se nalaze na spojnom delu plafona i bočnog zida.

DCN L3 switch DCRS-5750-28T svič bi trebalo da se nalazi unutar server reka te se klijenti koji se na njega povezuju (*Backup NAS, DB, File, Managment i Secutiry server*) mogu

konektovati preko patch panel-a kako bi se vodilo računa o urednom kabliranju. Servere treba povezati sa ruterom putem UTP Cat6 kablova koji omogućuju protok od 1 Gbps. Aplikativni server se povezuje na DCN L3 switch DCRS-5750-28T svič putem OM3 MMF optičkog kabla i na taj način ostvaruje brzinu protoka podataka od 10 Gbps.

Mail i Web server treba povezati preko TP-Link TL-SG2216WEB sviča sa glavnim čvorišnim svičom DCN L3 switch DCRS-5750-28T-DC i sa *load balancer*-om koji se takođe nalazi unutar sever reka. Na ovaj način ovim serverima se može pristupiti unutar mreže i sa interneta. Konektovanje se vrši preko UTP Cat6 kablova.

Kako pristup mreže internetu omogućavamo preko dva različita internet provajdera (fizički preko dva internet modema) koji pojedinačno omogućavaju brzinu protoka podataka i do 16 Gbps (*download i upload*) moramo ih spojiti pomoću load balancer-a koji u sebi između ostalog poseduje i *firewall* te na taj način pruža zaštitu mreži od "spoljnog" napada. Load balancer se povezuje preko IP VPN Encryption HC-7845 (sa dva UTP Cat6 kabla, kako bi se omogućila redudantnost) i Cisco ASA 5515-X IPS uređaja (koji mrežu štiti od spoljnog i unutrašnjeg napada) na DCN L3 switch DCRS-5750-28T-DC svič preko kojeg se dalje internet konekcija distribuira unutar cele kampus mreže.



Slika14: Izgled rek ormana u server sobi

Direktan pristup svim serverima se omogućava preko KVM sviča: KVM switch CKL-16B 16 ports PS/2.

Da bi se serveri i mrežna oprema zaštitila od nestanka struje svaki od rek ormana mora da poseduje po jedan UPS uređaj:

Eaton Powerware 5125 1500i RM 1500VA/1350W UPS Line-interactive, rack 19"-2U

4.5.2 **IT Administracija**

Mrežni klijenti:

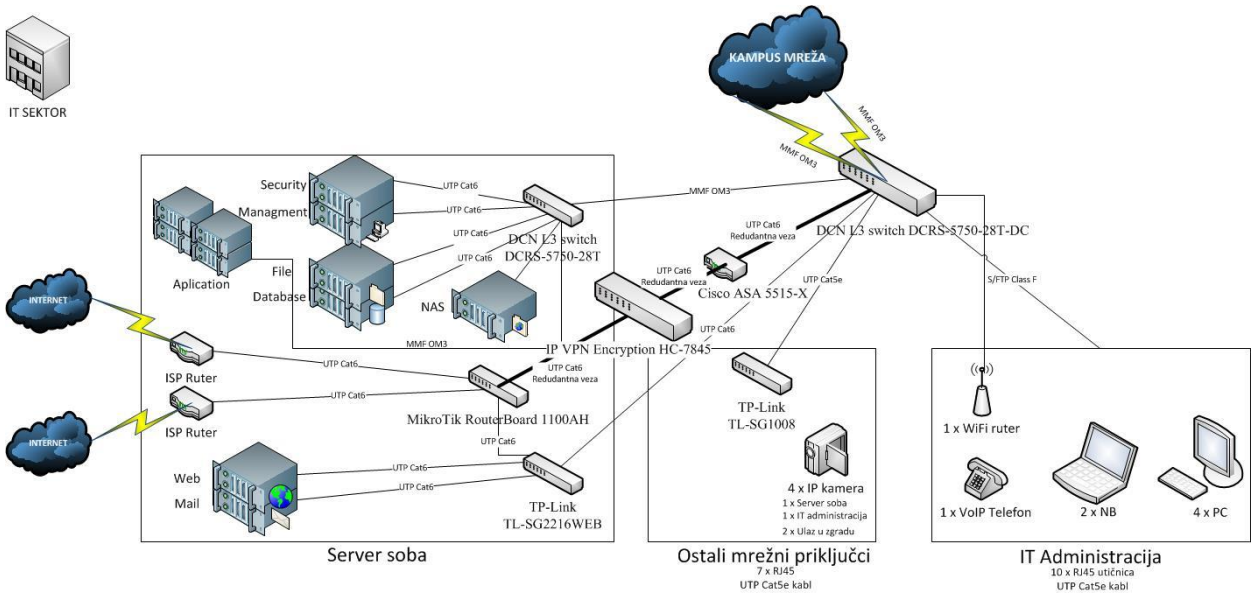
1) 4 x PC

2) 2 x NB
3) 1 x IP Kamera
4) 1 x VoIP telefona
5) 1 x WiFi ruter

Ukupan broj mrežnih priključaka potrebnih u ovom sektoru je 8 ali da bi se u slučaju potrebe za proširenjem broja klijenata otklonio problem kabliranja potrebno je realizovati bar 12 RJ45 zidnih priključaka. Zbog visoke cene rutera ovaj sektor bi trebalo direktno priključiti na DCN L3 switch DCRS-5750-28T-DC svič koji se nalazi na čvorištu između objekta i kampus mreže. Kablove od sviča treba voditi najkraćim mogućim putem do zidnih utičnica i pritom paziti na vodove električnih instalacija. Kablove treba postaviti unutar kanalica dimenzija 100 mm x 60 mm koje treba postaviti na spojnom delu plafona i bočnog zida sobe. Na mestu gde treba odvojiti jedan ili više kablova da bi se sproveli do zidne utičnice treba koristiti kanalice dimenzija 11 mm x 10 mm koje treba postaviti vertikalno u odnosu na kanalicu glavnog voda. Zbog velike količine kablova koji su po pravilu povezani u snop (da bi im se lakše pristupilo u slučaju potrebe za zamenom) treba koristiti S/FTP class F kablove kako bi se izbeglo EM zračenje. Od utičnice do samih klijenata koriste se UTP Cat5e kablovi, osim u slučaju povezivanja WiFi Rutera gde treba koristiti UTP Cat6 kablove. Stalni *notebook* klijenti se na mrežu (u zavisnosti od potreba) mogu povezati pomoću WiFi ili LAN konekcije.

4.5.3 **Ostali mrežni priključci**

Direktno na DCN L3 switch DCRS-5750-28T svič koji se nalazi na glavnom čvorištu zgrade treba priključiti još jedan TP-Link TL-SG1008 svič na koji se priključuju sve IP kamere (kamere se povezuju preko UTP Cat5e kablova koji se postavljaju unutar kanalica dimenzija 11 mm x 10 mm) u objektu. Svič TP-Link TL-SG1008 se postavlja u blizini sviča i povezuje direktno UTP Cat5e kablom.



Slika 15: Dijagram LAN mreže u objektu IT SEKTOR

5 Administracija

5.1 IP Adresni plan

Obzirom da je sistem u celosti realizovan uređajima baziranim na IP tehnologiji, uređajima je neophodno dodeliti IP-adresu (jedinstven 32-bitni broj predstavljen u decimalnoj notaciji).

Za ovaj sistem od interesa su samo privatne IP adrese, jer je projektovan kao zatvoren sistem.

Prema dokumentu RFC 1918, opseg privatnih IP adresa je sledeći:

klasa A od 10.0.0.0 do 10.255.255.255

klasa B od 172.16.0.0 do 172.31.255.255

Klasa C od 192.168.0.0 do 192.168.255.255

Dodeljivanje IP adresa treba da se isplanira prema fizičkom rasporedu delova sistema i prema broju mrežnih uređaja u sistemu. Planom treba predvideti i buduće širenje sistema.

Tabela 1: IP adresiranje

OBJEKAT	SEKTOR	OPSEG	RASPOLOŽIVE IP ADRESE
MARKETING I MENADŽMENT		192.168.8.0/21	192.168.8.0 - .192.168.15.255
	IP KAMERE I WiFi RUTER	192.168.8.0/24	192.168.8.0 - 192.168.8.255
	DIZAJN	192.168.9.0/24	192.168.9.0 – 192.168.9.255
	ODNOSI SA JAVNOŠĆU	192.168.10.0/24	192.168.10.0 – 192.168.10.255
	RAČUNOVODSTVO	192.168.11.0/24	192.168.11.0 – 192.168.11.255
	MENADŽMENT	192.168.12.0/24	192.168.12.0 – 192.168.12.255
NABAVKA I DISTRIBUCIJA		192.168.16.0/22	192.168.16.0 – 192.168.19.255
	IP KAMERE I WiFi RUTER	192.168.16.0/24	192.168.16.0 - 192.168.18.255
	NABAVKE I DISTRIBUCIJA	192.168.17.0/24	192.168.17.0 – 192.168.17.255
	MAGACIN	192.168.18.0/24	192.168.18.0 – 192.168.18.255
PRODAJA		192.168.20.0/22	192.168.20.0 – 192.168.23.255
	IP KAMERE I WiFi RUTER	192.168.20.0/24	192.168.20.0 – 192.168.20.255
	PRODAJA	192.168.21.0/24	192.168.21.0 – 192.168.21.255
	MALOPRODAJA	192.168.22.0/24	192.168.22.0 – 192.168.22.255
	VELEPRODAJA	192.168.23.0/24	192.168.23.0 – 192.168.23.255
SERVIS		192.168.24.0/22	192.168.24.0 – 192.168.27.255
	IP KAMERE I WiFi RUTER	192.168.24.0/24	192.168.24.0 – 192.168.24.255
	PRIJEM ROBE	192.168.25.0/24	192.168.25.0 – 192.168.25.255
	POPRAVKA	192.168.26.0/24	192.168.26.0 – 192.168.26.255
IT SEKTOR		192.168.0.0/21	192.168.0.0 – 192.168.7.255
	IP KAMERE I WiFi RUTER	192.168.7.0/24	192.168.7.0 – 192.168.7.255
	SERVER SOBA	192.168.0.0./24	192.168.0.0 – 192.168.0.255
	IT ADMINISTRACIJA	192.168.1.0/24	192.168.1.0 – 192.168.1.255
POSEBNA OPREMA IT SEKTORA	LOAD BALANCER, ISP MODEMI,ENCRIPTION, IPS...	192.168.2.0/24	192.168.2.0 – 192.168.2.255

6 Zaštita sistema i bezbednost podataka

Savremene računarske mreže se uglavnom baziraju na Internet tehnologijama i protokolima koji su podložni mogućim napadima koji ugrožavaju bezbednost podataka i identiteta subjekata. Ključni problem leži u činjenici da podaci kruže i egzistiraju u elektronskom obliku koji nije neposredno vidljiv i zbog toga postaju izloženi novim vrstama napada, a osnovni razlozi za to leže u samim karakteristikama arhitekture računarskih mreža Internet-Intranet tipa:

- TCP/IP protokoli nisu projektovani da zadovolje zahteve za zaštitom informacija,
- Internet je mreža sa komutacijom paketa u kojoj se jednostavno pristupa informacijama koje se prenose i moguće je ubacivanje poruka nepoznatog porekla i sadržaja.

U cilju rešavanja navedenih problema, uporedo sa razvojem računarskih mreža, razvijaju se i specijalizovani softverski i hardverski sistemi zaštite. Danas u svetu postoji veliki broj proizvođača tehnološki kvalitetnih proizvoda za različite nivoe zaštite savremenih mreža. U ovim proizvodima su ugrađeni javni "de-facto" standardni kriptografski algoritmi. Ovi algoritmi obezbeđuju dovoljni nivo bezbednosti za većinu komercijalnih informacionih sistema i računarskih mreža.

Iako pomenuti proizvodi predstavljaju veoma kvalitetna rešenja sa stanovišta tehnologije realizacije, oni se ne preporučuju za primenu u TCP/IP računarskim mrežama sa bezbedno osetljivim podacima. Osnovni razlog je nepostojanje potpune sigurnosti u kriptografski kvalitet ovih rešenja, npr. ona se ne mogu verifikovati na nivou izvornog koda. Najkvalitetnija kriptografska rešenja koja se primenjuju u savremenim računarskim mrežama baziraju se na primeni simetričnih kriptografskih sistema za zaštitu tajnosti (u specijalnim slučajevima po mogućstvu uz korišćenje sopstvenih simetričnih algoritama višeg kriptografskog kvaliteta), tehnologije digitalnog potpisa na bazi asimetričnih kriptografskih sistema, digitalnih certifikata i hardverskih modula (smart kartice i kriptografski koprocesori). Ovakvi sistemi zaštite su projektovani da se uspešno odbrane od potencijalnih opasnosti i napada u cilju ugrožavanja bezbedno osetljivih resursa informacionih sistema.

Kriptografski algoritmi koji se primenjuju u sistemima zaštite Internet/Intranet računarskih mreža dele se u dve velike grupe:

- Simetrični kriptografski algoritmi,
- Asimetrični kriptografski algoritmi.

Podela je izvedena na osnovu posedovanja informacija neophodnih za šifrovanje i dešifrovanje. Primenom simetričnih kriptografskih algoritama se, kao i u tradicionalnim sistemima zaštite, ostvaruje funkcija zaštite tajnosti u savremenim informacionim sistemima. Sa druge strane, primenom asimetričnih kriptografskih algoritama i tehnologije digitalnog potpisa ostvaruju se sledeće funkcije u savremenim računarskim mrežama:

- Autentičnost strane koja je poslala digitalno potpisanu poruku,
- Zaštita integriteta podataka u poruci koja je poslata,
- Neporecivost elektronskog potpisnika za sadržaj date poruke.

Uporedo sa razvojem i implementacijom računarskih mreža Internet tipa, razvijaju se i različiti mehanizmi zaštite specijalizovani za odbranu od pojedinih vrsta napada.

U startu treba biti svestan da računarske mreže Internet tipa, pored toga što omogućavaju izuzetno povećanje efikasnosti rada i smanjenje troškova, predstavljaju kritičnu tačku bezbednosti date organizacije sa stanovišta bezbednosti informacija koje se u sistemu prenose.

U svetu postoji veliki broj različitih pregleda i analiza opasnosti korišćenja računarskih mreža na bazi Internet tehnologija izrađenih od strane relevantnih institucija. Prema jednom pregledu američkog instituta za zaštitu računara (Computer Security Institute (CSI)'s 2000 Computer Crime and Security Survey) koji je obuhvatao velike korporacije, 70% razmatranih subjekata je prijavilo detektovane neautorizovane pristupe u svojim mrežama u prethodnoj godini.

Takođe, prema istoj analizi, u prethodnih 5 godina, 66 razmatranih subjekata je prijavilo ukupan gubitak proizveden krađom osetljivih korporacijskih informacija u iznosu od $66 708 000, a 54 razmatrana subjekta su prijavila ukupan gubitak proizveden finansijskom proneverom u iznosu od $53 996 000 Ova analiza je takođe potvrdila sledeće trendove u korišćenju računarskih mreža Internet tipa u poslednje vreme:

- Razvoj sve šireg spektra mogućih napada.
- Napadi na korporacijske računarske mreže Internet tipa mogu biti eksterni i interni. Iako su prethodnih godina napadi na računarske mreže Internet tipa bili pretežno eksterni, novije analize (kao što je i prethodno pomenuta analiza CSI) pokazuju da mnogo veću štetu i finansijske gubitke nanosi širok spektar internih napada. Razlozi za to leže u samoj prirodi mreža Internet tipa u kojima interni učesnici nisu samo zaposleni u datoj korporaciji (za koje postoji određeni stepen poverenja), već i poslovni partneri, zaposleni u firmama podružnicama, kooperanti, dostavljači, itd., koji iz razloga jednostavnosti korišćenja i povećanja efikasnosti i produktivnosti rada imaju vrlo sličan, ako ne i isti, pristup korporacijskoj mreži kao i zaposleni u datoj korporaciji.
- U poslednje vreme su zabeleženi veoma veliki finansijski gubici prouzrokovani napadima na računarske mreže Internet tipa.
- Uočeno je da primena samo komercijalnih tehnologija zaštite informacija ne može uvek predstavljati pouzdano rešenje odbrane od potencijalnih napada već da se ponekad mora koncipirati i primeniti slojevita i sveobuhvatna politika zaštite koja će pored komercijalnih tehnologija zaštite obavezno uključiti i primenu kvalitetnijih, sopstveno realizovanih mehanizama zaštite, kao i mehanizama kontrole pristupa i organizacionih elemenata zaštite date računarske mreže Internet tipa.

Sa druge strane, SANS Institut je obavio istraživanja koja su rezultovala u definisanju tri liste osnovnih grešaka koje omogućavaju različite vrste napada na mreže Internet tipa i pojedinačne radne stanice u mreži.

Prva lista se odnosi na krajnje korisnike i definiše sledećih pet najvećih bezbednosnih grešaka:

- Otvaranje e-mail priloga (attachment) dobijenog od nepoverljivog izvora,
- Propust da se instaliraju bezbednosni patch-evi standardnih Internet programskih paketa, kao i novih definicija (upgrade) antivirusnih programa,
- Instaliranje i download-ovanje screen saver-a i igara od nepoverljivih izvora,
- Nekreiranje i netestiranje back-up operacija,
- Korišćenje modema dok ste vezani u lokalnoj računarskoj mreži (LAN).

Druga lista se odnosi na korporacijske uprave (management) i definiše sledećih sedam najvećih bezbednosnih grešaka koje utiču na slabosti korporacijske računarske mreže:

- Neobezbeđenje odgovarajućeg broja službenika koji treba da uspostave i održavaju sistem zaštite u okviru korporacije,
- Primena samo organizacionih vidova zaštite bez primene (i bez prihvatanja neophodnosti primene) mehanizama zaštite informacija,
- Rešavanje samo pojedinačnih bezbednosnih problema bez primene mera i stvaranja uslova za kreiranje kompletnog sistema zaštite koji bi osigurao rešenje najšireg spektra bezbednosnih problema,
- Korišćenje samo mrežnih barijera (firewall) u korporacijskoj računarskoj mreži,
- Neshvatanje koliko vrede intelektualno vlasništvo i poslovna reputacija firme,
- Primena kratkotrajnih rešenja pojedinačnih situacija što dovodi do brzog umnožavanja bezbednosnih problema,
- Pretvaranje da će se bezbednosni problemi rešiti sami od sebe ako se ignorišu.

Treća lista se odnosi na informatičke profesionalce i definiše sledećih deset najvećih bezbednosnih grešaka:

- Priključivanje računarskog sistema na Internet bez prethodne primene svih neophodnih bezbednosnih mera da se to učini,
- Priključivanje test i razvojnih sistema na Internet sa default lozinkama,
- Propust da se sistem ažurira sa rešenjima nekih bezbednosnih problema,
- Korišćenje nekriptovanih protokola za upravljanje sistemima, ruterima i firewall-ovima,
- Davanje korisnicima lozinki preko telefona i njihovo menjanje bez prethodne autentifikacije osobe koja zahteva izmenu,
- Propust pri održavanju i testiranju procedure back-up-a sistema,
- Korišćenje nepotrebnih Internet servisa,
- Primena mrežnih barijera sa pravilima koja ne osiguravaju bezbedno osetljivi dolazeći i odlazeći saobraćaj,
- Propust u implementaciji i ažuriranju softverskog paketa za detekciju virusa,
- Propust u edukaciji korisnika u odnosu na to šta je potrebno učiniti kada se uoči potencijalni bezbednosni problem.

Imajući u vidu prethodno rečeno, u nastavku su sumirani najčešći vidovi potencijalnih napada i moguće odbrane u okviru TCP/IP distribuiranih računarskih sistema

6.1 **Potencijalni napadi na savremene računarske mreže i mogući načini odbrane**

Najčešći vidovi napada na računarske mreže Internet/Intranet tipa su:

- Prisluškivanje – neovlašćeno pristupanje podacima u otvorenom obliku i lozinkama,
- Lažno predstavljanje – neautorizovani pristup podacima ili kreiranje neautorizovanih podataka,
- Napad tipa ukidanja servisa (denial-of-service) – onemogućavanje funkcionisanja mrežnih servisa i resursa,
- Ponavljanje poslatih poruka – neovlašćena kontrola komunikacije subjekata i ponavljanje, izmena ili sprečavanje prenosa podataka,
- Pogađanje lozinke – neovlašćeni pristup podacima uz pomoć otkrivene lozinke,
- Kriptoanaliza – otkrivanje tajnih ključeva – otkrivanje podataka u otvorenom obliku na bazi šifrata i otkrivenog tajnog ključa,
- Napadi tipa Trojanskog konja – distribucija zlonamernih programa na radne stanice,
- Virusi – uništenje podataka.

Iako pomenuti napadi nisu specifični samo za TCP/IP računarske mreže oni su tu najviše ispoljeni jer se daleko najveći broj računarskih mreža u svetu bazira na Internet tehnologijama.

Mogući načini odbrane od navedenih napada su sledeći:

- Šifrovanje – zaštita tajnosti podataka i lozinki,
- Primena tehnologije digitalnog potpisa – provera autentičnosti, zaštita integriteta podataka i obezbeđenje neporecivosti za sadržaj poslate poruke,
- Procedura jake autentifikacije – bezbedna međusobna autentifikacija strana u komunikaciji,
- Korišćenje jakih ključeva i česta izmena ključeva – sprečavanje metoda kriptoanalize,
- Zaštita adresa servera – zaštita od napada tipa ukidanje servisa,
- Korišćenje digitalnih certifikata kao jednoznačnih identifikacionih parametara subjekata u komunikaciji,
- Korišćenje smart kartica za generisanje digitalnog potpisa i bezbedno čuvanje ključeva i drugih kriptografskih parametara,
- Višenivoovska antivirusna zaštita.

U cilju odbrane od navedenih potencijalnih napada na mrežu, najsvrsishodnije je primeniti kombinovane metode zaštite koje se sastoje od većine gore navedenih metoda.

6.2 **Primeri napada na savremene računarske mreže**

Internet je uveo revoluciju u način na koji kompanije posluju s obzirom da je to izuzetno efikasan, jeftin i fleksibilan protokol. Međutim, postojeće metode koje se koriste za rutiranje paketa u mreži čine ih ranjivim u odnosu na veliki opseg bezbednosnih rizika, kao što su: spoofing, sniffing i session hijacking. Takođe, TCP/IP protokol ne obezbeđuje nikakvu formu neporecivosti za ugovorne i finansijske transakcije. Pored toga što moraju da obezbede interno okruženje, organizacije moraju da obezbede i komunikaciju između udaljenih kancelarija, poslovnih partnera, korisnika i zaposlenih koji putuju ili rade sa udaljenog mesta. Prenošenje poruka putem Interneta ili Intraneta do tih različitih entiteta predstavlja jedan očigledan rizik, imajući u vidu nedostatak zaštite u postojećoj Internet mreži. Kontrola i upravljanje bezbednošću i pristupom pomenutih entiteta u poslovnom okruženju kompanije je od izuzetnog značaja.

Bez primene bezbednosnih mehanizama, i javne i privatne mreže su ranjive na neovlašćeno nadgledanje i pristup. Interni napadi mogu biti rezultat minimalne ili nepostojeće Intranet bezbednosti. Rizici koji dolaze spolja u jednoj privatnoj mreži potiču od konekcija na Internet i ekstranet. Kontrola pristupa korisnika samo na bazi password-a ne može da zaštiti podatke koji se prenose kroz mrežu.

Bez primene kontrola i mera bezbednosti, podaci i sistemi mogu biti predmet napada. Neki napadi su pasivni u kojima se informacije samo monitorišu. Drugi napadi su aktivni i informacije se menjaju sa ciljem menjanja ili uništenja samih podataka ili same mreže putem koje se vrši prenos podataka. Mreže i podaci su ranjivi na bilo koji od tipova napada koji su navedeni u nastavku ukoliko nisu primenjene odgovarajuće bezbednosne mere.

Osnovne informacije i lista uobičajenih mrežnih napada koji se primenjuju na fiksne i mobilne TCP/IP računarske mreže:

- Krađa identiteta - phishing
- Prisluškivanje
- Modifikacija podataka
- Spoofing identiteta (IP address spoofing)
- Napadi na lozinke
- Denial-of-service (DoS) napad
- Man-in-the-middle napad
- Napad kompromitacije ključa
- Sniffer napad
- Napad na aplikativnom nivou

6.2.1 **Krađa identiteta - phishing**

To je jedan od danas najpopularnijih napada. U najkraćem, napad se ogleda u pretvaranju da se radi o validno web sajtu određene organizacije, kao i da se radi o validnoj aktivnosti

(resetovanje, neke administrativne aktivnosti, itd.) u vezi korisničkih tajnih parametara pristupa sistemu (credentials). U tom smislu, napadač traži od korisnika da dostavi napadaču svoje tajne parametre (brojeve kartica ili bilo šta drugo). Drugim rečima, phishing predstavlja simuliranje pravog bankarskog web sajta ili email adrese u cilju jednostavnog sakupljanja tajnih parametara krajnjih korisnika koji se zatim koriste za eventualnu krađu novca sa realnog web sajta.

Phishing predstavlja jednu novu vrstu Internet napada koji pre svega cilja korisnike bankarskih servisa. Phishing je jedan od prvih bezbednosnih napada koji omogućuje jednostavnu masovnu zloupotrebu, koja privlači organizovan kriminal.

6.2.2 **Prisluškivanje**

U opštem slučaju, veliki deo mrežnih komunikacija se realizuje u otvorenom obliku (nešifrovano), što omogućuje napadaču koji je pristupio putevima podataka u mreži da monitoriše i čita saobraćaj. Kada napadač prisluškuje komunikaciju, to se naziva sniffing ili snooping. Mogućnost da prisluškivač monitoriše mrežu je generalno najveći bezbednosni problem sa kojim se admnistratori susreću u jednoj organizaciji. Ukoliko se ne primene jaki kriptografski mehanizmi šifrovanja, podaci mogu biti čitani od strane neovlašćenih lica tokom prolaska kroz mrežu.

6.2.3 **Modifikacija podataka**

Nakon što napadač dođe u poziciju da može da čita podatke koji prolaze kroz računarsku mrežu organizacije, naredni logički korak je često da ih modifikuje. Često, napadač može menjati podatke u paketima na način da niti primalac niti pošiljalac mogu to primetiti.

6.2.4 **Identity spoofing (IP address spoofing)**

Većina mreža i operativnih sistema koristi IP adrese u cilju identifikacije validnog računara na mreži. U nekim slučajevima, moguće je da se zloupotrebi IP adresa od strane zlonamernog korisnika (napadača). Taj napad je poznat kao identity spoofing.

Napadač može koristiti specijalne programe da konstruiše IP pakete koji se pojavljuju na mreži kao da potiču sa validnih adresa u okviru Intranet-a (internet mreže) date organizacije. Nakon dobijanja pristupa mreži sa validnom IP adresom, napadač može modifikovati, rerutirati ili brisati podatke. Napadač takođe može sprovoditi i druge tipove napada, kao što je opisano u narednim sekcijama.

6.2.5 **Napadi na lozinke**

Uobičajena stvar u većini operativnih sistema i mrežnih bezbednosnih planova je korišćenje sistema kontrole pristupa na bazi lozinki. Naime, najčešće je pristup kako samom računaru tako i mrežnim resursima određen korisničkim imenom (user name) i lozinkom (password).

Ranije verzije komponenata operativnih sistema nisu uvek štitile informacije o identitetu korisnika tokom njihovog puta kroz mrežu u cilju validacije. To je moglo da omogući prisluškivaču da dobije validno korisničko ime i lozinku i da ih iskoristi da dobije pristup mreži kao validan korisnik. Kada napadač nađe i pristupi validnom korisničkom nalogu, on će imati ista prava kao i aktuelni korisnik. Na primer, ukoliko korisnik ima administratorska prava, napadač može kreirati dodatne naloge za kasniji pristup. Nakon što dobije pristup mreži sa validnim nalogom, napadač može realizovati bilo koju od sledećih aktivnosti:

- Da dobije liste validnih korisnika i imena računara, kao i mrežnih informacija,
- Da modifikuje konfiguracije servera i same računarske mreže, uključujući i kontrolu pristupa i ruting tabele,
- Da modifikuje, rerutira ili obriše podatke

6.2.6 **Denial-of-service napad**

Za razliku od napada na lozinke, Denial-of-Service (DoS) napad sprečava normalno korišćenje računara ili računarske mreže od strane validnih korisnika. Nakon što dobije pristup mreži, napadač može realizovati bilo koju od aktivnosti:

- Da prevari zaposlene informacionog sistema tako da oni nisu u mogućnosti da odmah detektuju napad. Na taj način, napadač ima mogućnost da kreira dodatne napade,
- Da šalje nevalidne podatke aplikacijama ili mrežnim servisima, prouzrokujući na taj način da se prekine rad aplikacija ili servisa ili da ne rade na uobičajen način,
- Da šalje veliku gomilu saobraćaja sve dok se računar ili čitava mreža ne ugase,
- Da blokira saobraćaj što rezultuje u nemogućnosti pristupa mrežnim resursima od strane autorizovani korisnika.

6.2.7 **Man-in-the-middle napad**

Man-in-the-middle napad se ostvaruje kada neko neovlašćeno, postavljen između dva validna korisnika koji komuniciraju, vrši aktivno monitorisanje, prihvatanje i kontrolu komunikacije i to bez znanja ovlašćenih korisnika.

Na primer, napadač može da dogovori/uspostavi ključeve za šifrovanje sa oba ovlašćena korisnika. Svaki korisnik tada šalje šifrovane podatke napadaču koji može da dešifruje podatke. Kada računari komuniciraju na niskim nivoima mrežnog sloja, računari mogu ne biti u mogućnosti da odrede sa kojim računarima u mreži oni u stvari razmenjuju podatke.

6.2.8 **Napad kompromitacije ključa**

Ključ predstavlja tajni kod ili broj koji se zahteva za šifrovanje, dešifrovanje ili validaciju zaštićenih informacija. Iako određivanje/rekonstrukcija ključa predstavlja jedan težak i računarski intenzivan proces za napadača, to je moguće realizovati.

Kada napadač dođe do ključa, taj ključ se posmatra kao kompromitovan ključ. Napadač koristi kompromitovan ključ da dobije pristup zaštićenoj komunikaciji pri čemu niti pošiljalac niti primalac nisu svesni da su predmet napada. Uz korišćenje kompromitovanog ključa, napadač može dešifrovati ili modifikovati podatke. Napadač takođe može pokušati da koristi kompromitovan ključ da izračuna dodatne ključeve koji mogu omogućiti pristup drugim zaštićenim komunikacijama.

6.2.9 **Sniffer napad**

Sniffer je aplikacija ili uređaj koji može da čita, monitoriše i preuzima podatke i pakete koji se razmenjuju u mreži. Ukoliko paketi podataka nisu šifrovani, sniffer program može imati potpun uvid u podatke koji su unutar paketa.

Korišćenjem sniffer programa, napadač može realizovati sledeće operacije:

- Analizirati mrežu i informacije o pristupu, eventualno prouzrokujući da mreža prestane da odgovara ili postane neispravna,
- Pristupiti i čitati privatnu komunikaciju.

6.2.10 **Napad na aplikativnom nivou**

Napad na aplikativnom nivou cilja aplikativne servere prouzrokujući grešku u operativnom sistemu servera ili aplikacijama. To može rezultovati da napadač dobije mogućnost da preskoči normalne kontrole pristupa. Napadač koristi prednosti takve situacije, zadobija kontrolu nad aplikacijom, sistemom ili mrežom i može sprovesti neku od sledećih operacija:

- Da čita, dodaje, briše ili modifikuje podatke ili operativni sistem,
- Da ubaci virus koji će koristiti računare i softverske aplikacije da kopira viruse kroz celu računarsku mrežu,
- Da uvede sniffer program u cilju analize mreže i da dobije informacije koje će eventualno moći da se koriste da se prouzrokuje da mreža prestane da odgovara ili postane neispravna,
- Da se na neuobičajen način prekine rad aplikacija ili operativnih sistema,
- Da se deaktiviraju druge bezbednosne kontrole da bi se omogućili budući napadi.

7 Tehnologije zaštite savremenih računarskih mreža

U cilju zaštite informacionih sistema i savremenih računarskih mreža od gore navedenih napada, neophodno je uspostaviti sistem bezbednosti u organizaciji u kome će se primenjivati sledeće tehnologije zaštite:

- Tehnologija digitalnog potpisa bazirana na asimetričnim šifarskim sistemima,
- Zaštita tajnosti podataka primenom simetričnih šifarskih sistema,
- Infrastruktura sistema sa javnim ključevima (PKI – Public Key Infrastructure).

7.1 Primena kriptografskih metoda zaštite u informacionom sistemu

Kriptografski algoritmi koji se primenjuju u sistemima zaštite Internet/Intranet računarskih mreža dele se u dve velike grupe:

- Simetrični kriptografski algoritmi,
- Asimetrični kriptografski algoritmi.

Podela je izvedena na osnovu posedovanja informacija neophodnih za šifrovanje i dešifrovanje.

7.1.1 Simetrični kriptografski algoritmi

Grupu simetričnih kriptografskih algoritama predstavljaju algoritmi kod kojih je ključ za šifrovanje identičan ključu za dešifrovanje. Algoritmi iz ove grupe se takođe nazivaju i algoritmi sa tajnim ključem jer je tajnost ključa koji se koristi i za šifrovanje i za dešifrovanje esencijalna za bezbednost poruka u sistemu.

Ovi sistemi predstavljaju osnovu tradicionalne kriptološke teorije i razvijaju se već veoma dugi niz godina. S obzirom da zaštita informacija glavnu primenu ima u poslovima vezanim za državne strukture (vojska, policija i diplomatija), ovi sistemi su bili isključivo tajni sistemi, namenski definisani i realizovani od strane nadležnih državnih institucija.



Slika 16: Simetrični kriptografski algoritmi

Sa porastom intenziteta i primene elektronskih oblika komunikacija javila se potreba za definisanjem javnih simetričnih kriptografskih algoritama pa je u poslednjih desetak godina definisano više javnih simetričnih kriptografskih algoritama za primenu u aplikacijama u kojima za to postoji potreba. Ovi algoritmi se uglavnom koriste u aplikacijama vezanim za sisteme poslovnih i finansijskih komunikacija. Imajući u vidu eksplozivni razvoj poslovnih i finansijskih sistema u poslednje vreme, javni simetrični kriptografski algoritmi su postali dominantni u pogledu korišćenja. Međutim, nijedan od njih nije usvojen kao generalni standard već pomenuti sistemi uglavnom koriste odgovarajuće liste mogućih kriptografskih algoritama. Na taj način, kao parametar komunikacije, bira se i identifikator simetričnog šifarskog algoritma koji će se koristiti pri datoj transakciji.

Iako je po masovnosti komercijalna upotreba simetričnih kriptografskih algoritama daleko prevazišla upotrebu u tajnom sektoru (vezanom za državne strukture), glavni teorijski rezultati se i dalje dešavaju u oblasti tajne kriptologije i tajnih sistema. Velika većina država ima specijalizovane organizacije koje se bave dizajniranjem i analizom raznih vrsta šifarskih sistema (npr. NSA u SAD). Stepeni dostignuća u toj oblasti najčešće nisu javno poznati i nalaze se u sferi pretpostavki.

Postoje dve osnovne vrste simetričnih šifarskih sistema:

- blok šifarski sistemi,
- sekvencijalni šifarski sistemi (stream cipher).

7.1.2 **Blok šifarski sistemi**

Blok šifarski sistemi procesiraju blokove nešifrovanog signala - otvorenog teksta (OT) i šifrovanog signala – šifrata (ST), obično u blokovima čija je veličina 64 bita ili više. Sekvencijalni šifarski sistemi procesiraju nizove bita, bajtova ili reči (16 ili 32 bita) OT i ST.

Ako se u toku procesa šifrovanja jedne poruke nekim blok šifarskim sistemom više puta pojavljuje isti blok otvorenog teksta (OT) rezultat će biti uvek isti blok šifrata (ST), što nije slučaj kod sekvencijalnih šifarskih sistema.

Kod sekvencijalnih šifarskih sistema verovatnoća da isti niz bita, bajtova ili reči OT pri svakom pojavljivanju u jednoj poruci proizvodi isti šifrat teži nuli ukoliko su niz za šifrovanje i otvoreni tekst nezavisni. Blok šifarski sistemi se veoma mnogo koriste u sistemima poslovnih i finansijskih transakcija, ali su njihove bezbednosne osobine dosta slabije od sekvencijalnih šifarskih sistema. I pored toga definisan je veliki broj javnih algoritama baziranih na blok šifarskim sistemima, kao što su DES, 3-DES, RC2, IDEA, i mnogi drugi koji su našli veoma široku primenu u savremenim informacionim sistemima.

U 2001. godini, NIST organizacija u SAD je usvojila novi standard AES (Advanced Encryption Standard). Kao primer jednog blok šifarskog algoritma, dat je kratak opis AES simetričnog blok kriptografskog algoritma.

7.1.2.1 **AES algoritam**

Kao što je već rečeno, u toku 2001. godine, NIST (National Institute of Standards and Technology) organizacija u SAD je objavila standard za simetrične kriptografske algoritme AES (Advanced Encryption Standard) koji je trebalo da zameni prethodni standard DES (Data Encryption Standard).

Nakon duge selekcione procedure, za AES algoritam izabran je Rijndael algoritam koga su realizovali Belgijski istraživači: Joan Daemen i Vincent Rijmen. Rijndael predstavlja blok šifarski algoritam koji podržava promenljivu dužinu bloka informacije (128, 192 i 256 bita) kao i promenljivu dužinu ključa (128, 192 i 256 bita).

Naime, poruke šifrovane DES algoritmom su se, zbog nedostataka u samom algoritmu (bezbednosni nedostaci u supstitucionim s-tabelama), male dužine ključa (56-bita) i povećane procesne moći računara, mogle dešifrovati za samo par časova. Nakon selekcione procedure, za realizaciju AES standarda izabran je Rijndael algoritam koga su realizovali belgijski matečatičari: Joan Daemen i Vincent Rijmen.

Rijndael je blok šifarski algoritam koji podržava promenljivu dužinu bloka otvorenog teksta (128, 192 i 256 bita) kao i promenljivu dužinu ključa (128, 192 i 256 bita). Rijndael algoritam je u odnosu na konkurentske algoritme (MARS, RC6, Serpent, Twofish) bio brži i zahtevao je manje operativne memorije u procesu šifrovanja i dešifrovanja poruka. Rijndael algoritam sa 128-bitnom dužinom ključa je brži za oko 2.5 puta u odnosu na 3-DES algoritam.

AES algoritam realizuje operacije šifrovanja i dešifrovanja bloka podataka u promenljivom broju ciklusa. Broj ciklusa zavisi od veličine ključa i iznosi 10/12/14 za veličinu

ključa 128/192/256 bita, respektivno. Pre početka šifrovanja ili dešifrovanja vrši se ekspanzija ključa.

7.1.3 **Sekvencijalni šifarski sistemi**

Sekvencijalni šifarski sistemi predstavljaju vrlo važnu klasu šifarskih algoritama. Oni transformišu pojedinačne karaktere (najčešće bite i bajtove otvorenog teksta) koristeći transformaciju koja pored ključa zavisi na određeni način i od vremenskog trenutka u kojem se primenjuje, za razliku od blokovskih šifarskih sistema koji transformišu blokove otvorenog teksta nepromenljivom transformacijom tokom šifrovanja cele poruke.

Kao i obično, u praksi, ova podela nije tako rigidna, postoje transformacije koje se mogu po svojim osobinama svrstati i u jedne i u druge. Tako na primer CFB i OFB modovi blokovskih šifarskih sistema imaju neke karakteristike sekvencijalnih šifarskih sistema. Sa druge strane sekvencijalni šifarski sistemi se mogu smatrati blokovskim kod kojih je dužina bloka jedan karakter (bit, bajt ili mašinska reč (word) dužine 16, 24 ili 32 bita).

Generalno govoreći sekvencijalni šifarski sistem sastoji se od generatora niza ključa (keystream generator) koji generiše niz jedinica ključa $k_1, k_2, ..., k_i, ...$ i funkcije f koja se primenjuje na niz jedinica OT: $p_1, p_2, ..., p_i$, proizvodeći niz jedinica ST: $c_1, c_2, ..., c_i$, na bazi sledeće relacije:

$$c_i = f(k_i, p_i)$$

Na drugom kraju komunikacije, primenom inverzne funkcije na parove jedinica šifrata i jedinica ključa dobijaju se jedinice poslatog OT. Naime:

$$p_i = f^{-1}(k_i, c_i)$$

jer je funkcija f tako odabrana da je

$$p_i = f^{-1}(k_i, f(k_i, p_i))$$

Zbog jednostavnosti obrade za f se najčešće koristi ekskluzivna disjunkcija (XOR operacija). Bezbednost nizovnog šifarskog sistema primarno je određena kriptološkim kvalitetom generatora niza ključa.

7.1.3.1 **Klasifikacija sekvencijalnih šifarskih sistema**

Klasifikacija sekvencijalnih šifarskih sistema se može vršiti po različitim kriterijumima, po načinu na koji se generiše niz ključa, po tipu primenjenog algoritma (sa javnim ili tajnim ključem), itd. Osnovna je podela po načinu na koji se generiše niz ključa. U tom smislu postoje sistemi sa slučajnim i pseudo-slučajnim nizom.

Sistemi sa slučajnim nizom – kod ovih sistema niz ključa se generiše na slučajan način, tako što se jedinice ključa generišu nezavisno i slučajno. Ako se prema prethodnim oznakama za funkciju *f* uzme ekskluzivna disjunkcija, tada se dobija takozvani "one time pad" sistem za koji se može teorijski pokazati da je apsolutno siguran, tj. da šifrat ne nosi nikakvu informaciju o otvorenom tekstu.

Sa druge strane taj sistem je i optimalan u smislu da koristi najkraći ključ kojim se postiže apsolutna sigurnost. Naime, Šenon je u svojim radovima pokazao da je neophodan uslov za apsolutnu bezbednost da entropija ključa bude veća ili jednaka od entropije poruke. Kako je kod ovog sistema entropija ključa jednaka dužini poruke, čija entropija ne može biti veća od njene dužine, to sledi da je ovo zbilja optimalan sistem u navedenom smislu.

Nedostatak ovog sistema je u činjenici da oba učesnika komunikacije moraju imati isti niz ključa koji mora biti tajan, što proizvodi, ponekad nepremostive, probleme u upravljanju ključevima jer treba obezbediti i dostaviti stranama u komunikaciji velike količine ključeva kako bi mogle nesmetano da komuniciraju.

Sistemi sa pseudoslučajnim nizom – kod ovih sistema se na osnovu inicijalne vrednosti i dogovorenog algoritma generiše niz jedinica ključa. Posedovanjem identične inicijalne vrednosti, obe strane u komunikaciji su u stanju da produkuju isti niz jedinica ključa i da ostvare bezbednu komunikaciju. Kako je generisanje jedinica ključa determinističko, niz ključa je u potpunosti definisan sa:

- Početnim unutrašnjim stanjem – inicijalna vrednost kojom se definiše početno stanje generatora ključa,
- Funkcijom narednog stanja – koja na bazi prethodnog unutrašnjeg stanja generiše novo unutrašnje stanje,
- Izlaznom funkcijom – koja na osnovu unutrašnjeg stanja generiše izlaznu jedinicu ključa.

Posledica činjenice da je niz ključa deterministički je da je on nužno periodičan. Iako su ovo na izgled činjenice koje ovakve sisteme značajno dezavuišu, stvari ne stoje tako loše, i ti problemi se mogu sasvim uspešno prevazići. Naime, bezbednost ovakvih sistema direktno zavisi od veličine inicijalnih podataka i kvaliteta dogovorenog algoritma. Dobro dizajnirani algoritmi ovog tipa pružaju zaštitu koja je po kvalitetu vrlo blizu apsolutno bezbednim sistemima.

Sekvencijalni šifarski sistemi sa pseudoslučajnim nizom se dele u dve velike grupe:

- Sinhroni sekvencijalni šifarski sistemi
- Samosinhronišući sekvencijalni šifarski sistemi

Sinhroni sekvencijalni šifarski sistemi su oni kod kojih se niz ključa generiše nezavisno od otvorenog teksta i šifrata

Kod ovih sistema niz ključa se generiše nezavisno od niza jedinica poruke. Na obe strane u komunikaciji se istovremeno generišu nizovi ključa. Učesnici u komunikaciji su u stanju da

razmenjuju poruke sve dotle dok su algoritmi za generisanje niza ključa sinhronizovani među sobom.

Ukoliko se desi gubitak ili umetanje jednog ili više jedinica tokom prenosa ST, dešifrovanje će biti nekorektno. U slučaju takvog događaja, generatori niza ključa na predajnoj i prijemnoj strani moraju se resinhronizovati, pre nego što nastave komunikaciju. Sa druge strane, u ovim sitemima se ne propagira greška i svaki pogrešan bit u prenosu ostaće i u dešifrovanom obliku pogrešan, ali ta greška neće uticati ni na prethodne ni na buduće bite za prenos.

Prethodno navedena osobina može poslužiti aktivnom protivniku kao osnova za različite vrste pokušaja kompromitovanja ovakvog sistema.

Samosinhronišući asinhroni sistemi su oni kod kojih je niz ključa dobija u funkciji inicijalne vrednosti, dogovorenog algoritma i izvesnog konstantnog broja prethodnih jedinica šifrata.

Kod ovih sistema moguće je ostvariti samosinhronizaciju zato što dešifrovanje zavisi samo od fiksnog broja prethodnih jedinica šifrata, tako da je moguće sinhronizaciju ponovo uspostaviti vraćanjem na određeni broj dobro primljenih znakova šifrata. Kod ovih sistema propagacija greške je takođe ograničena na fiksiran broj uzastopnih jedinica a posle toga se preostale jedinice šifrata mogu ispravno dešifrovati.

Sekvencijalni šifarski sistemi imaju veliku ulogu u zaštiti masovnih podataka zato što obezbeđuju kvalitetnu zaštitu a pri realizaciji obezbeđuju veliku brzinu obrade.

Teorija analize i sinteze sekvencijalnih šifarskih sistema sa pseudoslučajnim nizom je veoma razvijena i u glavnom jedna podstiče drugu na razvoj.

7.1.3.2 **RC4 algoritam**

RC4 je najkorišćeniji sekvencijalni algoritam i koristi se u popularnim protokolima kao što su SSL i WEP. Izvrstan je zbog jednostavnosti i brzine, ali je sa druge strane ranjiv na napade kada početak izlaznog niza nije odbačen ili kada se jedan ključ koristi dvaput.

RC4 je jednostavan za opis. Ima 256 *S-box*-ova. Ulazi su permutacija brojeva od 0 do 255, a permutacija je funkcija ključa promenljive dužine. Ima dva brojača, *i* i *j*, postavljena na 0. Za generisanje slučajnog bajta koristi se sledeći algoritam:

$i = (i + 1)\ mod\ 256$
$j = (j + S_i)\ mod\ 256$
zameni S_i i S_j
$t = (S_i + S_j)\ mod\ 256$
$K = S_t$.

Bajt K se XOR-uje sa otvorenim tekstom da bi se dobio šifrat ili XOR-uje sa šifratom da bi se dobio otvoreni tekst. Enkripcija je brza (oko 10 puta brža nego kod DES-a). Inicijalizacija *S-box*-ova je takođe lagana.

Prvo se popunjavaju linearno: $S_0 = 0$, $S_1 = 1$,..., $S_{255} = 255$.

Zatim se generiše drugi 256-bajtni niz ključa, ponavljajući ključ koliko je potrebno da se popuni ceo niz: K_0, K_1,..., K_{255}. Indeks *j* se postavlja na 0. Tada se izvršava sljedeća petlja:

for i = 0:255
$j = (j + S_i + K_i)$ *mod* 256
zameni S_i i S_j.

Algoritam je imun na diferencijalnu i linearnu kriptoanalizu i krajnje je nelinearan. Indeks *i* osigurava da se svaki element menja, a indeks *j* da se elementi menjaju slučajno.

7.1.4 **Komparativna analiza blok i sekvencijalnih šifarskih sistema**

Iako su blok i sekvencijalni šifarski sistemi veoma različiti, blok sistemi se mogu implementirati kao sekvencijalni sistemi i obrnuto. Razlike se najviše iskazuju u implementaciji ovih sistema. Naime, sekvencijalni šifarski sistemi koji šifruju i dešifruju svaku jedinicu OT nisu previše pogodni za softverske implementacije. Oni su pogodni za šifrovanje i dešifrovanje podataka u realnom vremenu, i to posebno ako su realizovani u hardveru.

Sa druge strane, blok šifarski sistemi su lakši za implementaciju u softveru zato što često izbegavaju vremenski zahtevne bitske manipulacije i zato što rade nad podacima u računarski podeljenim blokovima. Postoje neki specifični momenti gde šifrovanje jedinica OT može biti od interesa i u računarskim sistemima, kao na primer šifrovanje veze između tastature i procesora, ali i u tom slučaju blok koji se šifruje treba da bude najmanje širine magistrale podataka. U savremenom razvoju kriptologije svedoci smo sve intenzivnijeg korišćenja kako blok tako i sekvencijalnih šifarskih sistema. Savremene aplikacije finansijskih i poslovnih transakcija su prouzrokovale eksplozivan rast primena pomenutih šifarskih sistema i to: DEA, 3-DES, RC2, IDEA, AES, itd. kao blok šifarskih sistema, i RC4, i drugih, kao sekvencijalnih šifarskih sistema.

U savremenim softverskim i hardverskim proizvodima za zaštitu finansijskih, poslovnih i državnih računarskih mreža uglavnom se podržava čitav skup najviše korišćenih blok i sekvencijalnih algoritama (de facto standardnih algoritama).

7.1.5 **Asimetrični kriptografski algoritmi**

Asimetrični kriptografski algoritmi predstavljaju jedno od najvećih dostignuća kriptologije druge polovine dvadesetog veka. Otkriveni su u procesu rešavanja problema vezanih za zaštitu tajnosti i distribuciju ključeva koji je često bio aktuelan u primenama simetričnih kriptografskh algoritama.

Naime, u asimetričnim šifarskim sistemima se koriste različiti ključevi za šifrovanje i dešifrovanje, tzv. javni i tajni ključ, tako da ključ za šifrovanje može imati svako a samo posednik ključa za dešifrovanje može dešifrovati poruku.



Slika 17: Asimetrični kriptografski algoritmi

Međutim, visoka računarska zahtevnost ovih algoritama utiče na performanse sistema u kojima se primenjuju, tako da se ne preporučuje primena za zaštitu tajnosti informacija u sistemima sa velikim protokom informacija. Ovo naravno ne dezavuiše automatski ove algoritme jer način na koji je uz korišćenje ovakvih algoritama moguće ostvariti funkcije integriteta, autentičnosti i neporicanja ima nesumnjivu prednost nad tradicionalnim tehnikama.

U literaturi je opisano više algoritama sa javnim ključem ali sa stanovišta kvaliteta, otpornosti na razne vrste napada, efikasnost i lakoću implementacije te rasprostranjenost, nisu svi podjednako dobri. U tom smislu se kao prirodni izbor nameće RSA algoritam koji više od dvadeset godina odoleva svim teorijskim i tehnološkim napadima. Opis i način upotrebe ovog algoritma propisani su u standardu PKCS#1. Pored RSA algoritma moguće je koristiti i druga dva algoritma, DSA (Digital Signature Algorithm) i ECDSA (Elliptic Curve DSA), koja spadaju u standard digitalnog potpisa (NIST standard DSS (Digital Signature Standard).

7.1.6 **PKCS#1 standard**

PKCS#1 standard opisuje metode šifrovanja podataka korišćenjem RSA asimetričnog algoritma i najčešće se koristi za konstrukciju digitalnog koverta i digitalnog potpisa.

U slučaju digitalnog koverta, sadržaj poruke se prvo šifruje određenim simetričnim algoritmom (kao što su DES, 3-DES, RC2, RC4, IDEA, AES, ili neki namenski privatni algoritmi). Zatim se tajni ključ primenjenog simetričnog algoritma koji je upotrebljen za šifrovanje date poruke šifruje RSA algoritmom upotrebom javnog ključa korisnika kome je data poruka namenjena (RSA public key operacija). Tako šifrovan sadržaj poruke i tajni ključ kojim je ta poruka šifrovana zajedno predstavljaju digitalni koverat.

U slučaju digitalnog potpisa, sadržaj koji treba da se potpiše, poruka, prvo se redukuje u otisak poruke (message digest), primenom nekog od metoda za kreiranje otiska poruke, message-digest algoritma (kao što su na primer MD5 ili SHA-1 algoritmi), a zatim se dobijeni otisak poruke šifruje primenom, na primer, RSA algoritma koristeći privatni ključ potpisnika poruke (RSA private key operacija). Šifrovani otisak poruke predstavlja digitalni potpis date poruke, i postaje njen pridruženi deo. Kada ovakva poruka stigne do primaoca kojem je namenjena izvršava se postupak verifikacije digitalnog potpisa. Ovaj postupak se sastoji od dešifrovanja otiska dobijene poruke primenom RSA algoritma uz upotrebu javnog ključa pošiljaoca poruke. Po dešifrovanju digitalnog potpisa primalac poruke izvrši isti message digest postupak nad dobijenom porukom.

Ako je dobijeni otisak poruke, identičan sa dešifrovanom vrednošću otiska, verifikacija je uspela, u protivnom verifikacija je negativna. Ukoliko je verifikacija uspela, primalac poruke je siguran u sledeće:

- Autentičnost pošiljaoca – jer je uspešno dešifrovao otisak poruke primenom RSA algoritma sa javnim ključem datog pošiljaoca,
- Integritet poslate poruke – ako su izračunati i dešifrovani otisci date poruke identični zaključuje se da poruka na prenosnom putu nije menjana, i
- Nemogućnost da pošiljalac naknadno porekne da je tu poruku poslao jer je njegov digitalni potpis uspešno verifikovan i ukoliko je potpisnik koristio privatni ključ generisan na smart kartici.

Da bi dati primalac bio u mogućnosti da prima poruke od datog pošiljaoca i sprovede proces verifikacije digitalnog potpisa mora imati mogućnost pristupa javnom ključu pošiljaoca. Pristup i distribucija javnih ključeva se mogu organizovati na različite načine a najčešće se realizuju u procesu utvrđivanja identiteta putem razmene digitalnih certifikata.

PKCS#1 standardom se pored bezbednosnih mehanizama definiše i unutrašnja struktura validnih poruka čime se omogućava dodatni mehanizam verifikacije ispravnosti poruka. Naime, svaka poruka koja ima narušenu strukturu se smatra neispravnom i odbacuje se.

Treba posebno naglasiti da je trenutno aktuelan i važeći PKCS#1 standard verzije 2.1 i da su njime značajno izmenjene preporuke date u PKCS#1 standardu verzije 1.5, koje se odnose na format bloka podataka koji podleže operacijama šifrovanja i potpisivanja. Razlog za ovakve drastične promene leži u činjenici da prema verziji 1.5 pri formiranju bloka za šifrovanje postoji niz bita na početku bloka koji je uvek isti. To se može iskoristiti da se bez poznavanja tajnih informacija, samo uz poznavanje šifrata dođe do otvorenog teksta. Ovde treba naglasiti da ovim

nije kompromitovana bezbednost samog RSA algoritma već je, grubo govoreći, način njegove upotrebe bio takav da je pod određenim uslovima dolazilo do oticanja informacija.

U verziji 2.1 ovog standarda blok podataka koji se šifruje prethodno se kodira OAEP (Optimal Assymetric Encryption Padding) metodom koja ima dobre bezbednosne karakteristike tako da čak ni dva identična bloka podataka posle kodiranja ovim metodom ne daju isti rezultat. Time su izbegnute slabosti detektovane u verziji 1.5. PKCS#1 standard verzije 2.1 je neophodno primeniti u mehanizmima zaštite u specijalizovanim računarskim mrežama i informacionim sistemima.

7.1.7 **Primena kriptografskih algoritama u informacionim sistemima**

U prethodnom tekstu bilo je reči o kriptografskim tehnikama koje se mogu koristiti pri dizajniranju i realizaciji sistema za zaštitu informacija. Kriptografske tehnike koje se koriste smo svrstali u dve grupe, simetrične i asimetrične kriptografske sisteme. Sa stanovišta bezbednosnih usluga jasno je da se uz manje ili veće probleme pri realizaciji u svakom od ovih sistema može realizovati većina osnovnih bezbednosnih servisa.

U obe vrste sistema neosporno se može postići poverljivost podataka. Činjenica je da simetrični sistemi na bazi slučajnog i pseudoslučajnog niza pružaju viši nivo bezbednosti od asimetričnih sistema pri istim dužinama ključeva. Takođe, asimetrični sistemi su znatno sporiji od simetričnih sistema i neophodni su im ključevi znatno veće dužine. Sa druge strane kod simetričnih sistema u slučaju intenzivnog saobraćaja javlja se problem distribucije ključeva.

Što se tiče utvrđivanja autentičnosti i identiteta subjekta u komunikaciji to se izuzetno kvalitetno realizuje u asimetričnim sistemima korišćenjem tehnike digitalnog potpisa uz upotrebu digitalnih certifikata. U simetričnim sistemima takođe se mogu realizovati sistemi za autentifikaciju, najpoznatiji je Kerberos, ali sa stanovišta logike samog procesa autentifikacije tu postoji jedna nepremostiva teškoća. Naime u takvim sistemima uvek postoji treća strana od poverenja koja aktivno učestvuje u procesu autentifikacije, te kao takva predstavlja potencijalni izvor opasnosti.

Što se tiče zaštite integriteta podataka u oba sistema se pomenuti servis relativno lako realizuje a kao kriterijum se uzima uspešno dešifrovanje (struktura i sadržaj poruke).
Kod realizacije servisa neporicanja kod simetričnih sistema se javlja problem postojanja aktivne treće strane od poverenja koja u spornim situacijama vrši arbitražu. Prednost asimetričnih sistema u ovom slučaju je u tome što je subjekt sam u stanju da pruži dokaze učešća drugog entiteta u transakciji ukoliko su ostali bezbednosni mehanizmi sistema adekvatni (pasivna treća strana od poverenja).

Iz prethodnog izlaganja prirodno proističu zaključci o koncepciji sistema zaštite u savremenim informacionim sistemima i računarskim mrežama. Najjednostavnije i najlogičnije je formirati sistem koji koristi dobre strane i jednih i drugih kriptografskih algoritama, pogotovu što su oni po svojim dobrim osobinama komplementarni. Prema tome najefikasniji pristup u koncipiranju savremenih sistema zaštite je formiranje hibridnog sistema koji koristi dobre osobine i jednih i drugih sistema, pa tako za utvrđivanje autentičnosti, zaštite integriteta i

obezbeđenje neporicanja treba koristiti asimetrične sisteme a za zaštitu tajnosti podataka simetrične kriptografske algoritme.

Od algoritama sa javnim ključem prirodan izbor bi bio RSA algoritam zbog svoje robusnosti i činjenice da se isti algoritam koristi i za šifrovanje i za potpisivanje poruka. Rasprostranjenost ovog algoritma u primenama učinila ga je važećim de facto standardom u toj klasi.

7.2 Višeslojna arhitektura sistema zaštite savremenih računarskih mreža

U cilju optimalne odbrane informacionih sistema i savremenih računarskih mreža od potencijalnih opasnosti i raznovrsnih napada kojima se ugrožavaju različiti servisi i resursi, predlaže se arhitektura sistema zaštite koja se sastoji od mehanizama zaštite primenjenih na tri nezavisna bezbednosna nivoa koji su namenjeni za odbranu od različitih tipova napada.

Ovi nivoi su projektovani da minimizuju i ograniče moguću štetu tako što eventualno ugrožavanje jednog nivoa ne može kompromitovati ostale bezbednosne nivoe arhitekture sistema zaštite.

U tom smislu, mehanizmi zaštite informacionog sistema mogu da se sastoje od primenjenih mehanizama na sledeća tri nivoa:

- Zaštita "s kraja na kraj" (end-to-end security) na aplikativnom nivou koja se zasniva na primeni tehnologije digitalnog potpisa na bazi asimetričnih kriptografskih algoritama i zaštite tajnosti podataka primenom simetričnih kriptografskih algoritama. Primenom ovog nivoa zaštite globalno se obezbeđuje:
    - provera autentičnosti korisnika servisa kako u smislu komunikacije (end-user authentication) tako i (opciono) u smislu kontrole pristupa mreži (access control),
    - zaštita integriteta podataka koji se prenose,
    - zaštita od mogućnosti naknadnog poricanja odgovornosti za poslate podatke i
    - zaštita tajnosti podataka.

  Ovaj nivo zaštite generalno služi za odbranu od internih napada.
- Zaštita na transportnom nivou predstavlja zaštitu tajnosti podataka primenom simetričnih kriptografskih algoritama i autentifikacije čvorova komunikacionog segmenta mreže na transportnom nivou. Ovaj nivo štiti mrežu od eksternih napada primenom kriptografskih tunela (zaštićenih sesija) između čvorišta komunikacionog segmenta mreže na transportnom nivou na bazi simetričnih kriptografskih sistema i primenom procedure jake autentifikacije između čvorišta mreže čime se obezbeđuje provera autentičnosti strana u komunikaciji.
- Zaštita na mrežnom IP nivou obezbeđuje kriptografsku i logičku zaštitu na nivou IP paketa koji se razmenjuju između mrežnih čvorova i štiti čitavu mrežu od eksternih napada korišćenjem zaštitnih mehanizama koje pruža standardna komunikaciona oprema. Ova zaštita se bazira na ostvarivanju kriptografskih tunela na IP nivou na bazi IPSec

protokola zaštite putem koga se ostvaruju Virtuelne Privatne Mreže (VPN – Virtual Private Network).

Suština predloga primene višeslojne arhitekture zaštite je u preporuci korišćenja kombinovanih mehanizama zaštite na više različitih nivoa ISO/OSI modela. Dakle, ukoliko nije moguće koristiti mehanizme na svim nivoima, kao minimalna arhitektura, predlaže se primena kombinacije mehanizama na dva nivoa, i to:

- Zaštita na aplikativnom nivou (kao obavezna) i
- Dodatna zaštita na transportnom ili mrežnom nivou.

Na taj način, sistem se brani kako od internih (aplikativna zaštita) tako i od eksternih napada (transportna ili mrežna zaštita).

7.2.1 **Zaštita na aplikativnom nivou**

U cilju realizacije mehanizama zaštite na aplikativnom nivou u okviru informacionog sistema Organizacije, predlaže se primena digitalnog potpisa i digitalne koverte, na bazi smart kartica za korisnike.

Za realizaciju zaštite na aplikativnom nivou, neophodno je primeniti odgovarajuću kriptografsku biblioteku kako na klijentu, u okviru odgovarajuće klijentske aplikacije (standalone) ili Internet browser programa, tako i za primenu na odgovarajućem web ili aplikativnom serveru. Ove kriptografske biblioteke na klijentu i serveru su u potpunosti odgovorne za realizaciju kriptografskih funkcija na aplikativnom nivou.

Naime, klijentska offline aplikacija (standalone) sa ugrađenom kriptografskom bibliotekom (ili odgovarajućom ActiveX kontrolom) ili web pretraživački program iz koga se poziva odgovarajuća ActiveX kontrola (ili JAVA aplet u non-Windows baziranim aplikativnim sistemima), treba da ima sledeće kriptografske karakteristike:

- Primena mehanizmima zaštite na aplikativnom nivou kojima se obezbeđuju sledeće funkcije:
    - Autentičnost potpisnika (asimetrični kriptografski algoritam i tehnologija digitalnog potpisa),
    - Zaštita integriteta fajlova (asimetrični kriptografski algoritam i tehnologija digitalnog potpisa),
    - Obezbeđenje neporecivosti (asimetrični kriptografski algoritam i generisanje ključeva na samim smart karticama i tehnologija digitalnog potpisa),
    - Zaštita tajnosti podataka (simetrični kriptografski algoritam i tehnologija digitalne envelope).
- Koriste se tehnologije digitalnog potpisa i digitalne envelope.

- Univerzalnost u odnosu na smart kartice i čitače smart kartice. Ugrađena ActiveX kontrola na klijentu, kao i kriptografske biblioteke ugrađene na serveru, koristi odgovarajući middleware (koji se sastoji od: CSP (Cryptographic Service Provider), PKCS#11 biblioteke i token menadžera za administraciju smart kartice) za pristup smart karticama. Na ovaj način, klijentska i serverska aplikacija su nezavisne od konkretne smart kartice koja će biti korišćena a i prelaz na drugi tip kartice je u potpunosti direktan.
- Klijentska aplikacija (bilo standalone bilo da se koristi web pretraživački program) sa ugrađenom kripto kontrolom mora da obezbedi funkciju provere autentičnosti korisnika na bazi njegove smart kartice i odgovarajućeg PIN-a pre nego što se omogući korišćenje same aplikacije, tj. aplikacija ne može da se startuje bez korišćenja odgovarajuće smart kartice ovlašćenog korisnika. Pri tome, provera nije samo da li se određena kartica nalazi u čitaču kartica već se mora proveriti i sertifikat korisnika (proverom validnosti, da li je izdat od CA kome se veruje i provera statusa povučenosti).
- Bazira se na kriptografskim operacijama koje se izvršavaju na samoj smart kartici: digitalni potpis (tj. RSA private key encryption) i dešifrovanje simetričnog ključa kod digitalne envelope (digital envelope retrieval). Ostale kriptografske operacije (šifrovanje/ dešifrovanje simetričnim algoritmima, kreiranje hash vrednosti podataka koji se digitalno potpisuju, verifikacija digitalnog potpisa) se izvršavaju u klijentskom i serverskom softveru (softverski deo kripto komponenti na klijentu i serveru).
- Bazira se na PKCS de facto standardima za zaštitu, i to:

    - PKCS#1 za digitalni potpis i digitalnu envelopu,
    - PKCS#7 za format zaštićenih podataka,
    - PKCS#11 standardni interfejs za pristup smart karticama.

- Aplikacija treba da bude standardna u smislu formata digitalno potpisanih i šifrovanih podataka. U tom smislu, treba primeniti standarde: PKCS#7 (ili noviji Cades) ili XML DIGSIG standard (ili noviji Xades) za format zaštićenih fajlova.
- Aplikacija pri realizaciji bezbednosnih mehanizama treba da koristi standardne načine pristupa smart karticama: CSP (Cryptographic Service Provider) i PKCS#11 biblioteka, i stoga je nezavisna od konkretne smart kartice koja će biti korišćena tako da je prelaz na drugi tip kartice u potpunosti direktan.
- Klijentska standalone aplikacija, ili odgovarajuće stranice web aplikacije, treba da omoguće:

    - Izbor sertifikata potpisnika (koji stoje u Personal Store-u) ukoliko na datoj radnoj stanici postoji veći broj korisničkih sertifikata.
    - Izbor sertifikata (koji stoje u Other PeopleStore-u) namenjenog primalaca šifrovanog fajla, tj. lice/korisnik za koga se šifruje taj fajl nakon digitalnog potpisivanja. To može biti i sam server ukoliko se radi o šifrovanoj dostavi podataka do servera.
    - Prikaz informacija o podacima koji se digitalno potpisuju pre samog potpisivanja,
    - Prikaz informacija o rezultatima digitalnog potpisivanja i/ili šifrovanja datih podataka,
    - Prikaz informacija o rezultatima uspešne ili neuspešne verifikacije digitalnog potpisa i/ili uspešnog ili neuspešnog dešifrovanja datih podataka.

- Klijentska i serverska kripto komponenta treba da u ovom trenutku podrži sledeće kriptografske algoritme i pridružene dužine ključeva:

    - Asimetrični algoritmi – RSA algoritam (koji se izvršava na smart kartici) sa dužinom asimetričnog ključa od 2048 bita.
    - Hash algoritmi – SHA-1, SHA-224, SHA-256, SHA-384 ili SHA-512.
    - Simetrični algoritmi – 3DES algoritam sa dužinom ključa od 168 bita ili AES algoritam sa dužinama ključa od 128, 192 ili 256 bita.

- Aplikacija treba da bude otvorena za stalnu dogradnju kako novih algoritama tako i za zamenu onih algoritama za koje je utvrđeno da su kriptografski slabi za korišćenje. Takođe, aplikacija treba da obezbedi promenu dužina odgovarajućih kriptografskih ključeva ukoliko se ukaže potreba za tim.
- Aplikacija treba da bude otvorena za eventualnu ugradnju privatnih simetričnih algoritama kreiranih i verifikovanih od strane nadležne institucije za poslove kriptozaštite u zemlji, ukoliko postoje zahtevi za to.
- U okviru aplikacije (klijentske i serverske) treba obezbediti funkciju verifikacije digitalnog potpisa odgovarajućih podataka (koji se razmenjuju između korisnika i sistema ili podataka/dokumenata koji su arhivirani i pregledaju se u okviru sistema) koji se sastoji od sledeća dva koraka (tim redom):

    - Provera digitalnog potpisa podataka na osnovu javnog ključa iz digitalnog sertifikata potpisnika (koji je došao uz digitalno potpisane podatke u samoj formatiranoj poruci),
    - Provera samog digitalnog sertifikata. Ova provera se izvršava na sledeći način:

        - proverava se da li je dati sertifikat istekao,
        - proverava se da li je sertifikat izdat od CA (certification Authority) kome se veruje i
        - proverava se da li je sertifikat povučen, tj. da li se nalazi na važećoj CRL listi koje izdaje dato CA.

U okviru mehanizama zaštite na aplikativnom nivou mogla bi se integrisati i odgovarajuća challenge-response procedura jake autentifikacije korisnika na aplikativnom nivou.

Alternativa tome je da se za te potrebe iskoristi standardna procedura klijentske i serverske autentifikacije u okviru SSL protokola zaštite na transportnom nivou što je opisano u nastavku a što se i predlaže za primenu u okviru informacionog sistema Organizacije.

7.2.2 **Zaštita na transportnom nivou**

U vezi realizacije transportnih mehanizama zaštite, predlaže se primena standardnog SSL (Secure Sockets Layer) protokola (novija verzija je TLS (Transport Layer Security) protokol) između korisnika i web servera (ili web servisa).

7.2.3 **SSL**

U informacionom sistemu organizacije predlaže se primena:

- SSL protokola sa serverskom autentifikacijom – neophodan je SSL serverski sertifikat izdat za dati web server i
- SSL protokola sa klijentskom i serverskom autentifikacijom na bazi digitalnih sertifikata i smart kartica korisnika. U ovom slučaju je takođe neophodno da web server (ili odgovarajući web servis) ima SSL serverski sertifikat.

Naime, za potrebe autentifikacije korisnika informacionog sistema Organizacije, predlaže se primena zaštite na transportnom nivou i jake autentifikacije korisnika na bazi SSL protokola sa klijentskom i serverskom autentifikacijom.

Dakle, u ovom slučaju nije samo dovoljno da web server poseduje sertifikat (serverska autentifikacija) već je neophodno da u sistemu postoji/koristi se i odgovarajuće Sertifikaciono telo (CA) koje izdaje sertifikate klijentima na smart karticama. Na ovaj način se postiže da samo klijenti sa smart karticama i odgovarajućim digitalnim sertifikatima mogu da pristupe datom web serveru, a samim tim da izvršavaju poslovne procese u okviru informacionog sistema Organizacije.

7.2.4 **Zaštita na mrežnom nivou**

Umesto SSL protokola na transportnom nivou, ili dodatno njemu, mogu se koristiti i kriptografski mehanizmi zaštite na mrežnom nivou koji se najčešće baziraju na IPSec protokolu zaštite i uspostavi virtuelnih privatnih mreža (VPN – Virtual Private Network).

U zavisnosti od načina komunikacije kao i protokolima koji se koriste za komunikaciju, kriptografske VPN mreže se najčešće baziraju na čistom IPSec protokolu zaštite ili na kombinacijama PPTP/IPSec ili L2TP/IPSec.

U okviru informacionog sistema Organizacije generalno se predlaže primena IPSec protokola na bazi digitalnih sertifikata čvorova u računarskoj mreži (ili između klijenta i VPN servera).

U tom smislu, VPN mreža, koja se bazira na IPSec protokolu, može se uspostaviti između dva rutera ili rutera i firewall-a, ili između VPN klijenta i VPN koncentratora (ruter ili firewall uređaj) – opet na bazi digitalnih sertifikata.

Sa druge strane, neophodno je primeniti firewall uređaje u cilju podizanja sveukupne zaštite i kontrole pristupa sistemu.

Takođe, potrebno je razmotriti i primenu drugih „nekriptografskih“ mehanizama zaštite u Organizaciji, i to: antivirusne zaštite, patch management, web content filtriranja, Intrusion Prevention Sistema (IPS), end-point security mehanizama, itd.

7.2.5 **IPSec**

Internet Protocol Security (IPSec) koristi kriptografske bezbednosne servise da zaštiti komunikaciju preko Internet protokola (IP) mreža . IPsec podržava peer mreže na nivou podataka, autentifikaciju porekla, integritet podataka, tajnost podataka (enkripcija) i zaštitu od reprodukcije.

Raniji pristupi bezbednosti su implementirali bezbednost na nivou aplikacija modela komunikacije. Za IPsec se kaže da je posebno koristan za implementaciju virtuelne privatne mreže i za daljinski pristup korisnika preko internet konekcije na privatne mreže . Velika prednost IPsec je da mere bezbednosti ne zahtevaju promene u pojedinačnim računarima korisnika . Cisco je lider u predlaganju IPsec kao standarda (ili kombinacija standarda i tehnologija) i uključuje podršku za to u svoje mrežne rutere .

IPsec pruža dva izbora bezbednosnih servisa : *Authentication Header* (AH) , koji u suštini omogućava autentifikaciju pošiljaoca podataka, i *Encapsulating Security Payload* (ESP) , koji podržava i autentifikaciju pošiljaoca i enkripciju podataka. Specifične informacije u vezi sa svakom od ovih usluga se ubacuju u zaglavlje paketa koji sledi IP zaglavlje istog paketa.

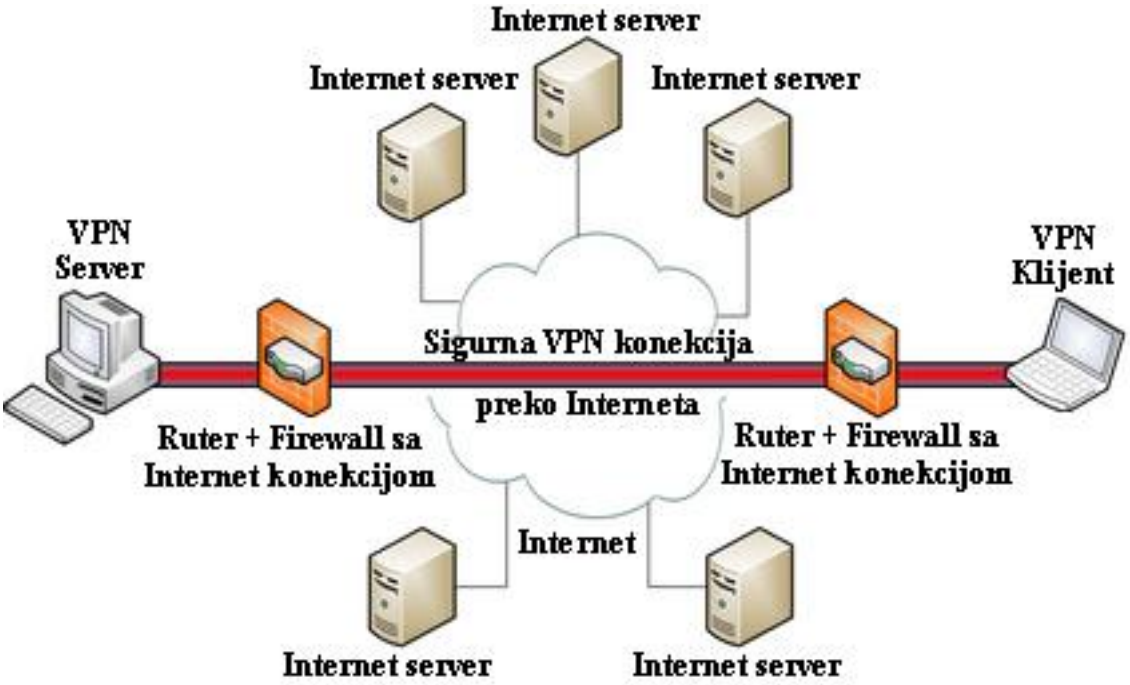
Ipsec protokol se koristi u „Tunelovanju" i u transportnom modu. Transportni mod obezbeđuje sigurnu vezu između dve krajnje tačke , jer sažima teret IP -a , dok u režimu tunela sažima ceo IP paket da obezbedi sigurnu virtuelnu konekciju između dva gejtveja . Ovo poslednje se koristi za formiranje tradicionalnog VPN tunela , gde se obično kreira bezbedni tunel preko nepouzdanog interneta.

Postavljanje IPsec konekcije obuhvata sve vrste kripto izbora , ali je to znatno pojednostavljeno i činjenica je da svaka data veza koristi najviše dva ili (retko) tri sigurnosna protokola odjednom. Autentifikacija izračunava *Integriti Check Value* (ICV) zbog sadržaja ima paketa i obično je izgrađen na osnovu *hash* funkcija kao što su MD5 ili SHA-1 . On sadrži tajni ključ poznat obema stranama, a to omogućava primaocu da izračuna ICV, na identičan način. Ukoliko primalac dobije istu vrednost, pošiljalac je efektivno autorizovan (oslanjajući se na sadržinu koja kriptografskog *hash*-a koji praktično ne može da se poništi). AH uvek obezbeđuje autentifikaciju , ESP i to radi po želji. Za šifrovanje koristi tajni ključ za enkripciju podataka pre slanja , a to krije stvarni sadržaj paketa od prisluškivača. Postoji dosta različitih algoritama koji se mogu koristiti, a neki od njih su: DES, 3DES, Blovfish, AES...

Pošto obe strane komunikacionog kanala treba da znaju tajne vrednosti korišćene u hashiranom šifrovanju, tu je pitanje kako se ovi podaci razmenjuju. Ručni tasteri zahtevaju ručni unos tajnih vrednosti na oba kraja, pretpostavljajući da se prenos vrši nekim van opsežnim mehanizmom, a IKE (Internet Key Exchange) je sofisticirani mehanizam za tu vrstu prenosa ključeva online.

7.2.6 **VPN**

Cela svrha virtuelne privatne mreže je da se povežu dve proverene mreže preko nepouzdane posredne mreže, kao što bi postigli korišćenjem veoma dugog Ethernet kabla između njih . VPN se obično koristi za povezivanje filijala kompanije sa sedištem, što omogućava svim korisnicima da dele osetljive resurse bez straha od prisluškivanja.



Slika 18: VPN

Jasno je da siguran VPN zahteva i autentifikaciju i šifriranje. Mi znamo da je ESP jedini način da se obezbedi enkripcija, ali ESP i AH mogu da obezbede autentifikaciju: Ali koji mi treba da koristimo ?

Očigledno rešenje je pakovanje ESP-a unutar AH je tehnički moguće, ali u praksi se obično ne koristi zbog AH ograničenja u pogledu prevođenja mrežne adrese . Korišćenjem AH ESP , ovaj tunel nikada ne može uspešno proći kroz NAT uređaj. Umesto toga , ESP autentifikacija se koristi u režimu tunela da obuhvati u potpunosti saobraćaj na putu preko nepouzdane mreže , zaštićeni šifrovanjem i proverom identiteta u isto vreme. Saobraćaj zaštićeni na ovaj način daje skoro nikakve korisne informacije uljezu zbog činjenice da su dva sajta povezan sa VPN-om. Ova informacija može da pomogne napadaču da stekne uvid u odnose poverenja , ali ništa o samu saobraćaja ne biva otkriveno . Čak je i vrsta ugradjenog protokola (TCP, UDP ili ICMP) sakrivena od autsajdera. Ono što je posebno lepo u ovom režimu rada je da krajnji korisnici, domaćini uglavnom ne znaju ništa o VPN-u ili drugim merama bezbednosti koje se koriste.

7.2.7 **Wi-Fi Protected Access (WPA) - Wi-Fi Protected Access II (WPA2)**

WPA i WPA2 su bezbednosni protokoli i programi za sertifikaciju sigurnosti razvijeni od WiFi Alianse radi zaštite bežičnih računarskih mreža. Ovi protokoli su razvijeni kao odgovor na ozbiljne slabosti u prethodnom sistemu, WEP (Wired Equivalent Privacy)

Greška u funkciji koja je dodata u WiFi pod nazivom WiFi Protected Setup (WPS) omogućava da se WPA i WPA2 zaobiđu i budu efikasno probijeni u mnogim situacijama. WPA i WPA2 zaštita koja se koristi bez WPS funkcije ostaje sigurnosno neoštećena i samim tim neuporedivo sigurnija.

WPA

WPA protokol sadrži veliki deo IEEE802.11i standarda. Konkretno *Temporal Key Integrity Protocol* (TKIP) je usvojen za potrebe WPA. WEP koristi 40-bitni ili 104-bitni ključ za šifrovanje koji se mora ručno uneti na bežične pristupne uređaje i ne menja se. TKIP koristi *per-packet* ključ, što znači da dinamički generiše novi 128-bitni ključ za svaki paket i na taj način vrši prevenciju od napada koji su upotrebljavani za WEP.

WPA takođe uključuje i proveru integriteta poruke. Takva provera je dizajnirana da bi sprečila napadača da snima, menja i/ili ponovo šalje pakete poruka.

WPA2

WPA2 je zamenio WPA uvođenjem CCMP-a, nove AES bazirane enkripcije sa jakom bezbednošću.

Protokoli za enkripciju

TKIP

(*Temporal Key Integrity Protocol*) je RC4 lančana šifra koja se koristi sa 128-bitnim *per-packet* ključem, što znači da generiše novi ključ za svaki paket.

CCMP

Šifrovanje bazirano na AES-u koje je jače od TKIP-a. Prema specifikacijama 802.11n ovaj protokol za šifrovanje mora se koristiti za postizanje brzih 802.11n šema u suprotnom brzina prenosa ne prelazi 54 MBit/s.

7.2.8 **IDS-IPS sistemi**

7.2.9 **IDS (Intrusion detection system)**

Intrusion detection system (IDS) je uređaj ili softverska aplikacija koja prati aktivnosti na mreži ili sistemu u potrazi za zlonamernim aktivnostima ili nepoštovanjem pravila. Ovakvi sistemi obično generišu izveštaj i šalju administratoru sistema. Neki sistemi mogu pokušati da spreče pokušaj napada (upada u sistem), ali to nije njihova primarna funkcija pošto su oni prvenstveno sistemi za detekciju a ne za sprečavanje napada. Sistemi za otkrivanje i sprečavanje (IDPS) su pre svega usmereni na identifikaciju mogućih incidenata, pravljenje izveštaja i obaveštavanje o istina. Pored toga organizacije koriste IDPS i za druge namene kao što su identifikovanje problema sa bezbednosnim politikama, dokumentovanje postojećih pretnji i odvraćanje pojedinaca od kršenja bezbednosnih politika.

IDS obično dokumentuje informacije koje su u vezi sa posmatranim događajima i obaveštava administratore bezbednosti (*eng. security administrator*). Mnogi sistemi za detekciju i prevenciju od upada pokušavaju uz pomoć nekoliko tehnika npr. promenom podešavanja vatrenog zida ili promenom sadržaja napadnute informacije.

7.2.10 **IPS (Intrusion prevention system)**

Intrusion prevention system (IPS) čine mrežni sigurnosni uređaji koji prate aktivnosti na mreži i/ili u sistemu tražeći tragove bilo kakve zlonamerne aktivnosti. Osnovne funkcije sistema za sprečavanje upada u sistem (IPS-a) čine:

Identifikacija maliciozne aktivnosti

Prijavljivanje zlonamernih aktivnosti

Pokušavanje da se takva aktivnost blokira ili spreči

IPS se smatra za proširenje sistema za detekciju upada (IDS) jer oba vrše monitoring tj. nadgledanje mrežnog saobraćaja i/ili sistemske aktivnosti u potrazi za zlonamernom aktivnošću. Glavne razlike IPS-a u odnosu na IDS su u njegovom postavljanju unutar same mreže i mogućnosti da aktivno spreče/blokiraju upade koji su detektovani. Tačnije IPS može da pošalje alarm, prekine (*drop* eng.) zlonamerni paket, resetuje konekciju i/ili blokira saobraćaj sa sporne IP adrese. IPS takođe može da ispravi greške Ciklične Redudantne Provere (CRC), defragmentuje strimove paketa, spreči TCP sekvencijalne probleme i izvrši čišćenje neželjenog transporta i opcija na mrežnom sloju.

Klasifikacije IPS-a

Sistemi za sprečavanje upada mogu se klasifikovati u četiri različite vrste:

Mrežni sistemi za sprečavanje upada (NIPS) prate celu mrežu u potrazi za sumnjivim aktivnostima analizirajući aktivnosti mrežnih protokola.

Bežični sistemi za sprečavanje upada (WIPS) prate celu bežičnu mrežu u potrazi za sumnjivim aktivnostima analizirajući aktivnosti bežičnih mrežnih protokola.

Analiza ponašanja mreže (NBA) ispituje mrežni saobraćaj radi identifikacije pretnji koje stvaraju neuobičajene tokove mrežnog saobraćaja kao što su napadi distribuiranim uskraćivanjem usluga (DDoS), pojedini oblici malicioznog softvera i nepoštovanje pravila.

Sistem za sprečavanje upada bazirani na *Host-u* (HIPS) su instalirani softverski paketi koji nadgledaju jednog domaćina (*eng. Host*) radi pronalaženja sumnjivih aktivnosti putem analiziranja procesa koji se odvijaju u okviru tog *host-a.*

Metode detekcije:

Većina sistema za sprečavanje upada koriste jedu od tri metode detekcije:

Detekcija bazirana na obrascima: Ova metoda detekcije zasnovana je na obrascima napada koji su unapred podešeni i predodređeni. Ovakav sistem prati mrežni saobraćaj i traži podudaranja sa obrascima. Kada pronađe podudaranje IPS preduzima odgovarajuću akciju. Obrasci mogu biti bazirani na iskorišćavanju ili ranjivosti.

Detekcija bazirana na anomalijama: Ovaj metod detekcije zasniva se na prosečnim performansama mrežnog saobraćaja. Nakon uspostavljanja statistike performansi mrežnog saobraćaja uz pomoć prikupljanja uzoraka, sistem je u mogućnosti da uporedi bilo koji uzorak koji kako bi odredio da li se nalazi izvan određenih parametara. Ukoliko se bilo kakva aktivnost nalazi izvan željenih granica performansi, IPS preduzima odgovarajuću akciju. Ovakav sistem nadgleda korisnike i ponašanje mreže.

Detekcija bazirana na analizi protokola: Uz pomoć unapred određenih profila koji sadrže opšteprihvaćene definicije benigne aktivnosti ovaj metod identifikuje odstupanja protokola poređenjem zabeleženih događaja.

Specifikacije IPS uređaja ili njegovog tržišnog ekvivalenta koji se koristi u projektu

Cisco ASA 5515-X

Stateful Inspection throughput (max)	1.2 Gbps
Stateful Inspection throughput (multiprotocol)	600 Mbps
Next-Generation throughput[3] (multiprotocol)	350 Mbps
IPS throughput	400 Mbps
Concurrent sessions	250,000
Connections per second	15,000

Packets per second (64 byte)	500,000
3DES/AES VPN throughput	250 Mbps
Site-to-site and IPsec IKEv1 client VPN user sessions	250
AnyConnect or clientless VPN user sessions	250
Cisco Cloud Web Security users	250
VLANs	100
High-availability support	A/A and A/S
Integrated I/O	6-port 10/100/1000
Expansion I/O	6-port 10/100/1000 or 6-port GE (SFP)
Power	AC/DC

8 Softverska zaštita celokupnog mrežnog sistema

8.1 Zaštitni zid

Zaštitni zid (engl. Firewall, u prevodu vatreni zid) je hardver ili softver koji u sklopu računarske mreže ima mogućnost da spreči nepropisni ili neželjeni prenos podataka kao i pristup računaru preko mreže koji je zabranjen od strane sigurnosne politike postavljene na mreži.

Zaštitni zid ima zadatak da kontroliše protok podataka između različitih zona u računarskoj mreži. Zone se dele na osnovu količine poverenja u bezbednost nekog dela mreže. Obično se zona interneta smatra nesigurnom, dok se lokalna mreža smatra relativno sigurnom.

Najčešće, zaštitni zid se brine da sa globalne mreže, interneta, na računar ne dospe štetni kod (virus, crv itd) i da spreči nedozvoljeni pristup računaru ili mreži od strane drugog računara radi ilegalnog eksploatisanja. Većina firewall-ova pita za dozvolu koji program ce da pusti da izađe, pod kojim uslovima, koji protokol program koristi i na kojim portovima program komunicira. Naravno, isto se odnosi i na obrnuti smer, dakle na ulaznu komunikaciju.

Zaštitni zid ne može raditi sam, i najčešće zahteva iskusnijeg korisnika koji će odobravati ili zabranjivati pristup nekoj mrežnoj aktivnosti. Zaštitni zid je najosnovnija komponenta koja čini sigurnu računarsku mrežu i najčešće se implementira u mrežnim uređajima ili u paketu zajedno sa antivirus softverom.

Softverski zaštitni zid se nalazi na svakom računaru u mreži i time omogućava visoki stepen zaštite celog sistema.

8.2 Antivirus softver

Anti-virus program se sastoji od nekoliko računarskih programa koji pokušavaju da pronađu, spreče i uklone računarske viruse i ostali maliciozni softver (eng. malware).

Anti-virus program obično koristi dve tehnike da bi postigao svoju funkcionalnost:

1) Proverom (skeniranjem) fajlova, tražeći poznate viruse proverom definicija u rečniku virusa
2) Identifikacijom sumnjivog ponašanja od strane kompjuterskog programa, koji bi mogao ukazati na infekciju računara virusom. Takve analize obuhvataju analizu podataka, nadgledanje portova i druge metode.

Većina komercijalnih anti-virus programa koristi oba pristupa, sa naglaskom na metod provere poznatih virusa u rečniku virusa.

Antivirus program koji se koristi u projektu dolazi u paketu sa zaštitnim zidom i čini njegov sastavni deo.

Antivirus i zaštitni zid koji se koristi u projektu i njegov način rada.

Comodo Internet Security Complete 2013



Slika 19: Izgled UI-a Comodo IS 2013

Specifikacije:

Zaštitni zid

Comodo zaštitni zid se nalazi među najviše rangiranima u testovima IT industrije.

Defense+ Tehnologija

Proaktivna zaštita automatski izoluje pretnje od sumnjivih fajlova, tako da ne mogu izazvati štetu i na taj način ne samo da otkriva nego i sprečava infekcije.

Auto Sandbox Tehnologija

Da bi se smanjilo prekidanje korisnika u radu, nepoznati fajlovi se mogu pokrenuti u sigurnoj virtualnoj okolini u kojoj oni ne mogu da naškode operativnom sistemu, registru ili bilo kojim važnim podacima.

Minimalni Prekidi

Comodo Internet Security Complete 2013 u potpunosti oslobađa korisnika od obaveze da odlučuje da li da blokira ili dozvoli sumnjive podatke, on donosi odluke sam umesto korisnika.

Spyware Skeniranje

Spyware Scanner detektuje i čisti maliciozne infekcije u registru računara i njegovom tvrdom disku.

Cloud baziran Antivirus

Cloud bazirano antivirus skeniranje detektuje maliciozne podatke čak i kada virusne definicije nisu najnovije.

TrustConnect

Hot spot protekcija enkriptuje sve podatke koji se šalju preko bežične ili žične internet konekcije.

Kompatibilnost

Windows 7, Windows Vista and Windows XP.

9 Održavanje i unapređivanje sistema

9.1 Potrebe sistema

9.1.1 IT osoblje

Za kompletno održavanje mrežnog sistema potrebno je obezbediti osoblje sa sledećim znanjem:

1) *Senior network administrator*

a) Postavljanje i održavanje mrežne opreme (svičevi, ruteri, VoIP telefoni, kabliranje,...)

b) Planiranje kompjuterske mreže i njena realizacija

c) Instalacija, rad i održavanje Windows, Windows server i Linux server operativnih sistema

d) Postavljanje i održavanje domenske strukture

e) Administracija File, Aplication i Menadžment servera

2) *Senior database administrator*

a) Instalacija, nadogradnja i održavanje database servera

b) Rad sa SQL bazama podataka

c) Back-up baza podataka

3) *Security administrator*

a) Održavanje sistema za nadzor objekata (IP kamere i njihova mrežna struktura)

b) Rad u Linux operativnom sistemu

c) Praćenje i održavanje sigurnosti mreže i podataka

d) Zaštita od spoljnih i unutrašnjih napada na mrežu i mrežne klijente

4) *Desktop/network technician*

a) Softverska podrška mrežnih klijenata (PC, NB, Štampači...)

b) Hardverska podrška mrežnih klijenata (PC, NB, Štampači...)

c) Instalacija, nadogradnja i održavanje Windows i Linux operativnih sistema

d) Pomoć pri postavljanju i održavanju mrežne opreme (svičevi, ruteri, VoIP telefoni, kabliranje,...)

e) Rad u domenskoj strukturi

5) *Web administrator/Web* dizajner/*Postmaster*

a) Postavljanje i održavanje Web i Mail servera

b) Programiranje, realizacija i administracija web stranica

9.2 **Održavanje sistema**

Kako cela mreža poseduje više od 200 klijentskih računara postavlja se pitanje da li je osoblje u mogućnosti da na vreme i sa dovoljnom efikasnošću otkloni svaki hardverski i softverski problem. Moguće rešenje za brzo delovanje i otklanjanje softverskih (koji su i češći problemi) je da se klijentima pristupa preko remote desktop konekcije i na taj način otklone uobičajeni softverski problemi i to bez fizičkog pristupa administratora sistema. Uz pomoć ovakve vrste tehničke i desktop podrške proces popravki se drastično vremenski smanjuje. Kod hardverskih ili ozbiljnijih softverskih kvarova potrebna je fizička prisutnost administratora i treba obratiti posebnu pažnju da se kod takvih popravki ne dovede u pitanje rad celokupnog sistema.

9.3 **Unapređivanje sistema**

Po završetku implementacije celokupne računarske i mrežne infrastrukture sistem bi trebao da bude u potpunosti operativan i funkcionalan. Međutim, kao takav on ne može biti beskrajno upotrebljiv i stoga treba obratiti pažnju na unapređivanje elemenata u toku njegovog radnog veka.

Svaki objekat (mrežni sektor) u sistemu projektovan je tako da može da podrži proširenje u smislu dodavanja novih mrežnih klijenata. Dodavanjem novih ili zamenom prvobitnih mrežnih uređaja i klijenata povećava se i opterećenje na sam sistem te se mora obratiti pažnja da se sistem ni u jednom momentu ne dovede u stanje preopterećenosti. Posebna pažnja treba da se obrati na opterećenost sistema koja bi trebala da bude oko 75% od maksimalnih mogućnosti jer se na taj način omogućava maksimalna efikasnost sistema i sigurna primena njegovih mogućnosti. Sama mrežna infrastruktura projektovana je tako da u narednih 10 – 15 godina pruža dovoljan protok i brzinu prenosa podataka za nesmetani rad sistema. Posle tog perioda trebalo bi aktivno planirati zamenu mrežne opreme i kablova kako bi se sistem modernizovao i unapredio tako da može da podrži rastuće zahteve klijenata i sistema. Na ovaj način radni vek sistema može se prolongirati još 10 - 15 godina pod uslovom da ne dođe do ogromnih promena na polju informacionih tehnologija i mrežnih sistema gde bi u tom slučaju došlo do potrebe za zamenom celokupnog mrežnog sistema.

Konstantnim vođenjem evidencije, monitoringom sistema, planiranjem modernizacije i zamenom uređaja i opreme sistem može biti aktivan i isplativ sve dok za njim ima potrebe.

Zaključak

U ovom radu bilo je reči o organizaciji, implementaciji i zaštiti kampus i virtuelnih privatnih mreža. Na početku rada opisana je metodologija po kojoj je istraživanje sprovedeno kao i pored ostalog predmet istraživanja, ciljeve i zadatke istraživanja, istraživačke hipoteze, metode istraživanja i tok istraživačkog procesa.

U poglavlju o organizaciji u kratkom je dat opis mreže i koje su njene potrebe kako bi se master rad mogao lakše koncipirati.

U poglavlju mrežna infrastruktura opisana je sva mrežna oprema (kablovi, mrežni uređaji,...) korišćena u projektu kao i način na koji bi ona trebalo da bude implementirana prilikom realizacije sistema.

Poglavlje implementacija sistema sadrži detaljno opisan način, pravila i instrukcije kako postaviti i međusobno povezati mrežnu opremu i klijente koji zajedno čine kampus i virtuelnu privatnu mrežu. Opisani su načini kabliranja u svakom sektoru mreže, dati tačni dijagrami povezivanja opreme kao i moguća proširenja mreže unutar svakog sektora.

Poglavlje administracija daje uputstva za upravljanje sistemom i IP adresiranje mrežne opreme i mrežnih klijenata.

U poglavlju Zaštita sistema i bezbednost podataka data je kratka definicija savremenih mreža i IT sistema kao i rezultati istraživanja koje se bavi ugroženošću sigurnosti podataka u takvim sistemima. Takođe ovo poglavlje sadrži primere potencijalnih napada na savremene računarske mreže i moguće načini odbrane.

U poglavlju Tehnologije zaštite savremenih računarskih mreža detaljno su opisane različite vrste rešenja na polju zaštite kao što su Simetrični i Asimetrični kriptografski algoritmi, Višeslojna arhitektura sistema zaštite (zaštita na aplikativnom, transportnom i mrežnom sloju).

Poglavljem softverska zaštita celokupnog sistema, gde je objašnjen rad antivirusnog softvera i zaštitnog zida u smislu zaštite sistema od štetnih programa i zlonamernih spoljnih “napada” na sistem, finalizira se deo rada koji se bavi zaštitom podataka i sistema.

Rad se završava poglavljem o održavanju i unapređivanju sistema u kome je dat detaljan pregled potrebnog ljudstva, načina održavanja i ideje za unapređivanje sistema u budućnosti.

Uz pomoć celokupnog teksta čitaoc bi trebalo da je u mogućnosti da samostalno odabere načine i vrste implementacije sistema u smislu hardvera, softvera i zaštite koje bi trebalo primeniti kao osnovicu za siguran i bezbedan računarski sistem, a sve u zavisnosti od vrste i namene tog sistema. Dakle kao opširan rad na temu organizacije i zaštite velikih računarskih sistema ovaj tekst ne daje striktnu marginu po kojoj se treba voditi, već podatke koji mogu da pomognu IT stručnjaku da u „moru“ tehničkih rešenja pronađe ono odgovarajuće za projekat koji pokušava da realizuje.

Literatura

[1] Računarske mreže, Prof. dr Mladen Veinović, Dr Aleksandar Jevremović, 2011
[2] Uvod u računarske mreže, Prof. dr Mladen Veinović, Aleksandar Jevremović, 2008
[3] Kriptologija I, Prof. dr Mladen Veinović, M.Sc. Saša Adamović, 2013
[4] Kent, S.; Atkinson, R. (November 1998). IP Encapsulating Security Payload (ESP). IETF. RFC 2406.
[5] Thayer, R.; Doraswamy, N.; Glenn, R. (November 1998). IP Security Document Roadmap. IETF. RFC 2411.
[6] Kent, S.; Atkinson, R. (November 1998). IP Authentication Header. IETF. RFC 2402.
[7] Harkins, D.; Carrel, D. (November 1998). The Internet Key Exchange (IKE). IETF. RFC 2409.
[8] Kaufman, C., ed. IKE Version 2. IETF. RFC 4306
[9] Sakane, S.; Kamada, K.; Thomas, M.; Vilhuber, J. (November 1998). Kerberized Internet Negotiation of Keys (KINK). IETF. RFC 4430.
[10] Richardson, M. (February 2005). A Method for Storing IPsec Keying Material in DNS. IETF. RFC 4025.
[11] "Understanding WEP Weaknesses". Wiley Publishing. Retrieved 2010-01-10.
[12] Meyers, Mike (2004). Managing and Troubleshooting Networks. Network+. McGraw Hill. ISBN 978-0-07-225665-9.
[13] Zaštita računarskih i poslovnih sistema, Dr Milan Marković, (Januar 2009)
[14] Richardson, M. (February 2005). A Method for Storing IPsec Keying Material in DNS. IETF. RFC 4025.
[15] www.wikipedia.com
[16] www.cisco.com
[17] www.crypto.ch
[18] www.tp-link.com
[19] www.hp.com
[20] http://technet.microsoft.com