

DIZAJN RAČUNARSKE MREŽE

Kompanija: Helvetia

Pripremio: Jovan Stanković

SADRŽAJ

UVOD	3
APLIKACIJE	4
POSLOVNI I TEHNIČKI ZAHTEVI, POSLOVNA I TEHNIČKA OGRANIČENJA	5
HIGH-LEVEL DIJAGRAM	6
DIZAJN I REDIZAJN	6
IP ADRESIRANJE, VLAN KONFIGURACIJA I RUTIRANJE.....	8
POBOLJŠANJA SISTEMA	10
SYSTEM DEPLOYMENT	11

UVOD

Računarska mreža privatne bolnice Helvetia više nije u stanju da pordži poslovne procese u kompaniji. Kompanija planira da pored postojećih u sledeće dve godine uvede nove poslovne procese, kao i novi WiFi sistem i Video IP nadzor.

Na njihov zahtev potrebno je uraditi redizajn računarske mreže, koji će biti predstavljen u ovom dokumentu.

Za ovaj redizajn će se koristiti Top-Down metoda:

1. **Analiza zahteva:** Analizirati tehničke i poslovne zahteve i ograničenja, analizirati postojaću mrežu i protok saobraćaja.
2. **Logički dizajn mreže:** Dizajnirati mrežu, podesiti adresiranje, imena, izabrati svičing i ruting protokole i razviti bezbednost.
3. **Fizički dizajn:** Izabrati tehnologiju i uređaje za campus i enterprise mrežu.
4. **Testiranje, optimizacija i dokumentacija**

APLIKACIJE

Ime aplikacije	Tip aplikacije	Bitnost
Google aplikacije	E-mail, Web pretraga	Bitno
BKarton	Aplikacija za potrebe kompanije	Veoma bitno
Finansije	Aplikacija za potrebe kompanije	Veoma bitno
Adobe Suit	Programi za dizajn, video editovanje, ...	Bitno
Pacijenti	Aplikacija za potrebe kompanije	Veoma bitno

U tabeli su prikazane aplikacije potrebne za rad kompanije.

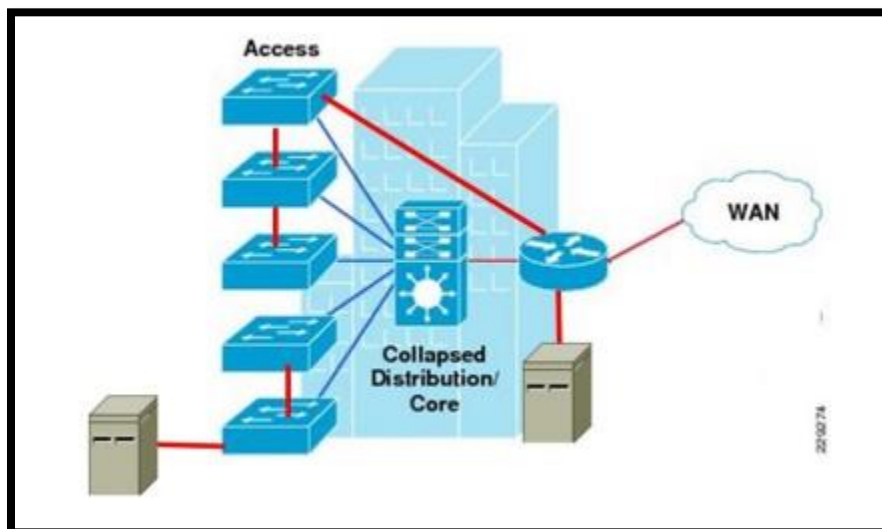
POSLOVNI I TEHNIČKI ZAHTEVI, POSLOVNA I TEHNIČKA OGRANIČENJA

POSLOVNI ZAHTEVI	POSLOVNA OGRANIČENJA
REDIZAJN POSTOJEĆE RAČUNARSKE MREŽE	KOMPANIJA IMA OGRANIČEN BUDŽET
MOGUĆNOST UVOĐENJA NOVIH POSLOVNIH PROCESA	ROK ZA ZAVRŠETAK PROJEKTA JE 4 MESECA
	U IT ODELJENJU SU ZAPOSLENI SAMO 1 INŽENJER (POČETNIK) I 2 TEHNIČARA

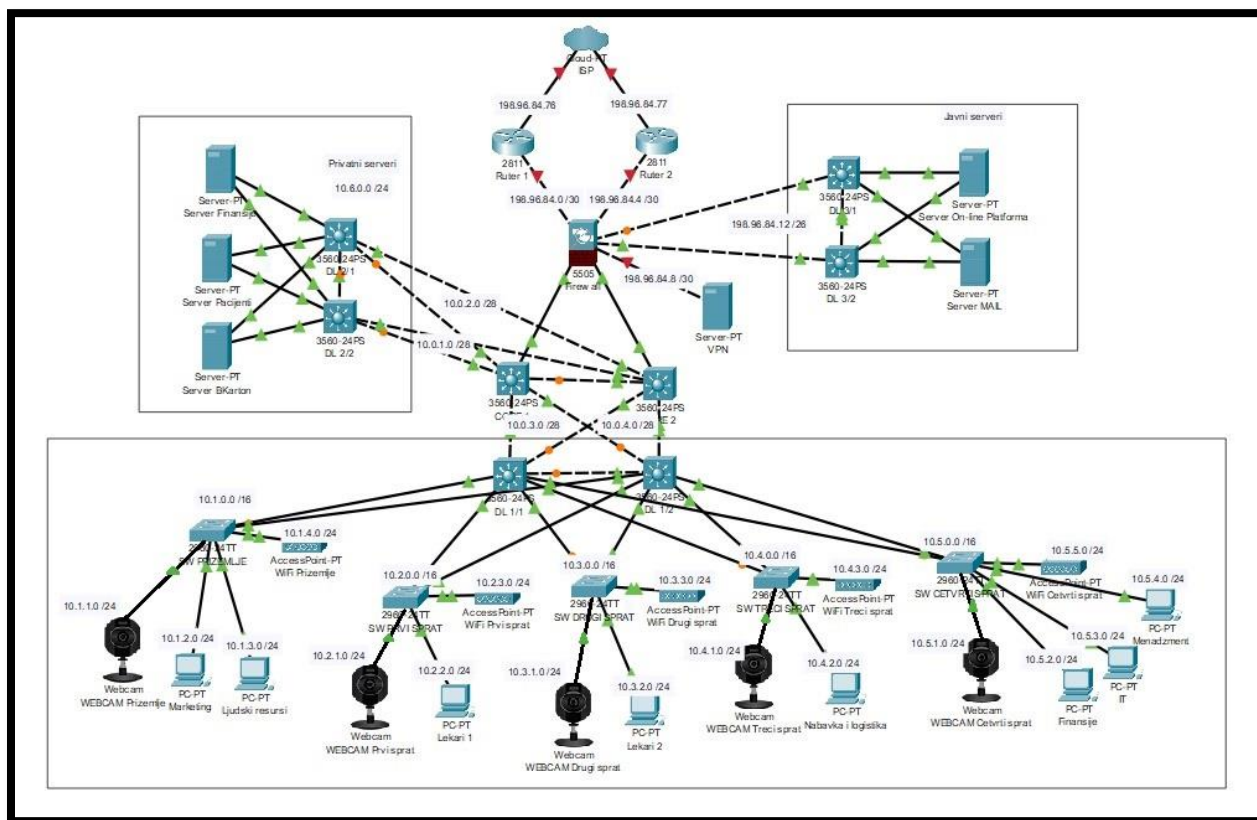
TEHNIČKI ZAHTEVI	TEHNIČKA OGRANIČENJA
KONFIGURISATI WIFI MREŽU	SPOR RAD APLIKACIJA U PERIODU OD 12-16h
KONFIGURISATI SISTEM ZA IP NADGLEDANJE	INTERNET KONEKCIJA POVREMENO NE FUNKCIONIŠE KAKO TREBA
POBOLJŠATI ZAŠTITU SISTEMA	MALI KAPACITET LINKOVA
PODESITI RUTIRANJE I VLAN-OVE	JEDNA ISP KONEKCIJA KOJA KORISTI DSL TEHNOLOGIJU
UVODJENJE 15 NOVIH VPN KONEKCIJA	SAMO 1 RUTER
OSPOSOBLJAVANJE MREŽE DA FUNKCIONIŠE ZA VEĆI BROJ ZAPOSLENIH	
OSPOSOBLJAVANJE MREŽE ZA UVODJENJE NOVOG E-COMMERCE MODULA	
APLIKACIJA BKarton MORA DA RADI U REALNOM VREMENU	

HIGH-LEVEL DIJAGRAM

DIZAJN I REDIZAJN



Stari dizajn



Novi dizajn

Na prvoj slici je predstavljen stari dizajn mreže. Predložen je novi dizajn (druga slika) koji treba da poboljša performanse. Novim sistemom posizemo bezbednost ubacivanjem firewall-a iza rutera.

Implementiramo core sloj koji omogućava svičovanje paketa velikim brzinama i visok stepen pouzdanosti i redundanse. Ovde se izbegavaju funkcije koje traže veće procesiranje kao što su inspekcija paketa i slični procesi. Time se osigurava brz rad aplikacija u kompaniji. Distribucionni sloj omogućava lako dodavanje novih svičeva ukoliko je to potrebno, takođe ovom implementacijom se prevazilazi single point of failure. Ovakva mreža je skalabilna. Po zahtevu korisnika instalirani su access point-i za wifi mrežu i IP kamere. Serverska farma je prikazana za core sloj radi bržeg prenosa podataka i manjeg zagušenja i radi zaštite od neautentifikovanog pristupa serverima. Ovako implementirani serveri mogu da obezbede siguran i brz rad novog kompanijskog softvera. VPN i ostali javni serveri su izolovani od “unutrašnje/privatne mreže”, kako neko ko pristupa njima ne bi mogao da upadne u sistem kompanije. Za internet rutere (gateway) se više ne koristi jedan, već dva zbog veće otpornosti na otkaz.

Svi uređaji u distribucionom i core sloju (L3 svičevi) su udvostručeni i duplo povezani iz istog razloga. Implementacija posebnog VPN servera omogućuje efikasniji i sigurniji pristup za zaposlene od kuće. Predložena je promena internet konekcije, pošto je sadašnja realizovana DSL tehnologijom koja je zastarela. Ovim bi se znatno poboljšala komunikacija sa spoljnim svetom zbog znatno većih brzina linkova koje nude druge tehnologije. Najbolje bi bilo koristiti optički link ukoliko je dostupan. Takođe, potrebno je zameniti linkove kojima su privatni povezani na svičeve zato što trenutna brzina konekcije nije idealna.

IP ADRESIRANJE, VLAN KONFIGURACIJA I RUTIRANJE

JAVNE IP ADRESE	
Ruter 1 – Internet	198.96.84.76
Ruter 2 - Internet	198.96.84.77
Ruter 1 - Firewall	198.96.84.0 /30
Ruter 2 - Firewall	198.96.84.4 /30
Firewall – MLS-ovi prema javnim serverima i javni serveri	198.96.84.12 /26
Firewall – VPN Server	198.96.84.8 /30

PRIVATNE IP ADRESE	
Firewall – CORE 1	10.0.5.0 /30
Firewall – CORE 2	10.0.6.0 /30
DL 2/1 – CORE 1,2	10.0.2.0 /28
DL 2/2 – CORE 1,2	10.0.1.0 /28
PRIVATNI SERVERI – DL 2	10.6.0.0 /24
DL 1/1 – CORE	10.0.3.0 /28
DL 1/2 - CORE	10.0.4.0 /24
DL 1/1,2 - Prizemlje	10.1.0.0 /16
DL 1/1,2 – Prvi sprat	10.2.0.0 /16
DL 1/1,2 – Drugi sprat	10.3.0.0 /16
DL 1/1,2 – Treci sprat	10.4.0.0 /16
DL 1/1,2 – Cetvrti sprat	10.5.0.0 /16

VLAN-ovi	
Prvi sprat	
VLAN IPCamera1	10.1.1.0 /24
VLAN Marketing	10.1.2.0 /24
VLAN Ljudski Resursi	10.1.3.0 /24
VLAN WiFi1	10.1.4.0 /24
Drugi sprat	
VLAN IPCamera2	10.2.1.0 /24
VLAN Lekari	10.2.2.0 /24
VLAN WiFi2	10.2.3.0 /24
Treci sprat	
VLAN IPCamera3	10.3.1.0 /24
VLAN Lekari	10.3.2.0 /24
VLAN WiFi3	10.3.3.0 /24
Cetvrti sprat	
VLAN IPCamera4	10.4.1.0 /24
VLAN Nabavka i logistika	10.4.2.0 /24
VLAN WiFi4	10.4.3.0 /24

Peti sprat	
VLAN IPCamera5	10.5.1.0 /24
VLAN Finansije	10.5.2.0 /24
VLAN IT	10.5.3.0 /24
VLAN Menadzment	10.5.4.0 /24
VLAN WiFi5	10.5.5.0 /24

Javni serveri kao i ruteri dobijaju javne IP adrese. Svim javnim serverima su statički dodeljene IP adrese. Javni serveri su zaštićeni preko firewall-a. Za rutiranje prema internetu se koristi BGP protokol.

Sa druge strane imamo privatnu mrežu, gde firewall koristi PAT da pretvori javne u privatnu adresu. Za rutiranje u LAN-u i WAN-u se koristi OSPF protokol. IP adrese mrežnim uređajima u kompaniji se dodeljuju dinamički preko DHCP servera, svaki uređaj dobija pool adresa, dok su L2 i L3 svičevima statički dodeljene IP adrese.

Za svaki sprat konfigurisan je VLAN. VLAN-ovi su implementirani da bi se razdvojio protok saobraćaja npr. administracije i IT-ja (da se saobraćaj ne bi mesao). U svakom VLAN-u imamo dovoljan broj adresa za već povezane uređaje, ali imamo i neiskorišćene adrese u pool-u kako bi se dodavali novi uređaji.

U ovom redizajniranom sistemu će se koristiti cisco mrežni uređaji i oracle-based serveri. U nižim slojevima se koriste bežični i koaksijalni linkovi dok se u višim koriste optički. Propusni opseg nije svuda isti.

POBOLJŠANJA SISTEMA

ZAHTJEVI	KOMENTAR
SIGURNOST SISTEMA	SIGURNOST SISTEMA SE POSTIŽE IMPLEMENTIRANJEM FIREWALL-A, ODVAJANJEM JAVNIH OD PRIVATNIH SERVERA U DMZ I IMPLEMENTACIJOM VLAN-OVA
BRZINA	DODAVANJEM L3 SVIČEVA U DISTRIBUCIONOM SLOJU I NJIHOVOM DVOSTRUKOM POVEZANOŠĆU POSTIŽE SE VEĆI PRENOS PODATAKA IZMEĐU SVIČEVA NA RAZLIČITIM SPRATOVIMA
REDUDANTNOST	OTPORNOST NA OTKAZ SE OBEZBEĐUJE DUPLIRANJEM UREĐAJA U CL I DL I NJIHOVOM DVOSTRUKOM POVEZANOŠĆU
SKALABILNOST	IMPLEMENTACIJOM CL I DL SA ODGOVARAJUĆIM SUBNET IP ADRESAMA OMOGUĆUJE SE LAKO DODAVANJE NOVIH UREĐAJA
DOSTUPNOST	SISTEM MORA BITI DOSTUPAN 99.9% VREMENA

SYSTEM DEPLOYMENT

MESEC	OPIS
1. MESEC	Analiza trenutne mreže, aplikacija I Sistema
	Izvođenje tehničkih I poslovnih ciljeva
	Implementacija aplikacija
2. MESEC	Redizajniranje mreže
	IP adresiranje I konfiguracija VLAN-ova
	Konfiguracija protokola
3. MESEC	Testiranje aplikacija
	Testiranje povezanosti mrežnih uređaja
	Testiranje sistema
4. MESEC	Verifikacija I dokumentacija