

**NETWORK DIZAJN DIJAGRAM**

| **Klijent :** | Delcourt |
| --- | --- |
|  |  |
| **Tip sistema :** | Mrežni sistem |
|  |  |
| **Status dokumenta** | Spreman i dozvoljen za izradu |
|  |  |
| **Document Reference** | Delcourt.word |
|  |  |
| **Numeracija Verzije:** | Verzija 1 |
|  |  |
| **Autor :** | Vladimir Cvetković |
|  |  |

**Sadržaj**

[**1.**](#_heading=h.gjdgxs) **Uvod** 3

[**2.**](#_heading=h.30j0zll) **Ciljevi projekta** 3

[**3.**](#_heading=h.1fob9te) **Poslovni zahtevi i ograničenja** 4

[**4. Tehnički zahtevi i ograničenja** 5](#_heading=h.3znysh7)

[**5. Aplikacije i njihovi prioriteti odrzavanja** 6](#_heading=h.2et92p0)

[**6. Logičke izmene na mrežnom sistemu** 7](#_heading=h.2s8eyo1)

[**6.1 Wireless mreža i bezbednost** 7](#_heading=h.17dp8vu)

[**6.2 Routing i Switching protokoli** 7](#_heading=h.3rdcrjn)

[**6.3 Bezbednost Mreže** 7](#_heading=h.26in1rg)

[**7. VLAN (Virtual Local Area Network)** 8](#_heading=h.lnxbz9)

[**7.1 VLAN- ovi i njihov adress pool: Organizacija sedišta kompanije** 8](#_heading=h.35nkun2)

[**8. WAN** 9](#_heading=h.44sinio)

[**9. Redudance i VRF Protokol** 10](#_heading=h.2jxsxqh)

[**10. Network dizajn i novi mrežni uredjaji** 10](#_heading=h.z337ya)

[**11. Data center**](#_heading=h.3j2qqm3) [10](#_heading=h.z337ya)

[**12. E-comerc modul**](#_heading=h.3j2qqm3) 10

**13.IP Telefonija** 11

**14.QoS** 11

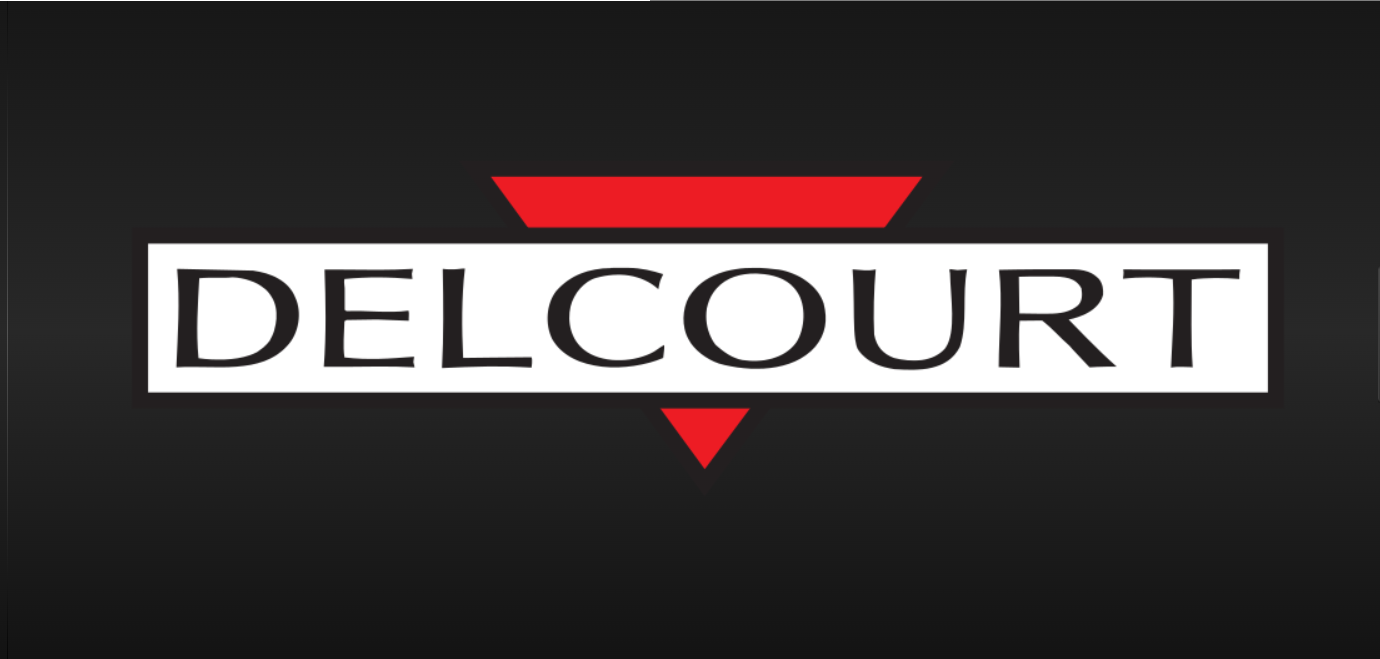
**14.1 CWVFQ Tabela** 11

**14.2 DSCP Tabela** 11

[**15. Metodologija izrade projekta**](#_heading=h.1y810tw) 12

[**16. Implementacioni plan projekta**](#_heading=h.4i7ojhp) 12

1. **Uvod**



Delcourt je porodična firma koja se razvila u poslednjih 100 godina do jedne od najvećih izdavačkih kuća za osnovne i srednje škole u Francuskoj. Zbog velikih uspeha u sferi biznisa unutar Francuske Delcourt planira da proširi svoj biznis van granica države i izabrala je nas zbog prethodno uspešnog redizajna sistema koji im je omogućio tehnički deo uspeha.

1. **Ciljevi projekta**

* Otvaranje novih centara u glavnim gradovima drugih država kao đto su : Berlin, London i Budimpešta
* Uvodjenje IP telefonije u novi sistem.
* Uvodjenje novog VPN modula za remote acces i site-to-site tipove VPN-a.
* Uvodjenje novog E-comerc modula
* Uvodjenje novog WAN modul\
* Dizajn nogog data centra

[**3.** **Poslovni zahtevi i ograničenja**](#_heading=h.1fob9te)

| **Poslovni zahtevi kompanije**  **i ograničenja** | **Poslovna ograničenja i njigova rešenja** |
| --- | --- |
| Klijent planira da korisnicima online omogući upotrebu svojih usluga tako da se mora obezbediti način e-comerc servisa za biznis klijenta | Potrebno je instalirati public servere unutar zasebne DMZ zone koji će služiti kao bezbedan kontakt sa spoljnim mrežama bez narušavanja naše privatne infrastructure. Takodje je potrebno obezbediti prevoznika za naručena dobra koji će isporučivati kupcima njihove proizvode unutar Francuske. Zbog proširenja mora se uzeti u obzir internacionalni faktor slanja dobara. |
| Zbog veličine projekta planirani budžet je limitiran po lokacijama, i treba obratiti dodatnu pažnju na ovu tačku. | Kako bi napravio što bolji novi mrežni sistem, arhitekta bi koristio najbolje i skuplje uredjaje. Medjutim uz dato ograničenje mora da se prilagodi planiranom budžetu kao i cenama ovih uredjaja na različitim lokacijama novih centara. |
| Rok za izradu projekta je 10 meseci; | Autor projekta mora za vrlo kratak vremenski period da isplanira veći broj identičnih sistema za centralne lokacije u novim gradovima. To uslovljava da autor projekta mora biti neko sa velikim iskustvom u mrežnom dizajnu kao i poznavanju tržišta mrežnih uredjaja u tim zemljama. |
| Zapošljavanje istog tima za IT rešenja, u vrlo kratom roku uz pomoć HR-a | Kako bi sistemi na novim lokacijama bili identični bitno je da zaposleni koji su uvodili inovacije na sistemu u Parizu budu uključeni u izradu sistema na novim lokacijama. |

**4. Tehnički zahtevi i ograničenja**

| **Tehnički zahtevi kompanije**  **i ograničenja** | **Tehnička ograničenja i njigova rešenja** |
| --- | --- |
| Iako je brzina slanja podataka u novom sistemu već bila poboljšana zbog dodavanja novih lokacija postalo je nužno da se obezbedi jos veća brzina kako bi se jos brže dolazilo do potrebnih rešenja izmedju komunikacije sa inostranim centrima. | Trenutna kablovka infrastruktura je  bila ograničena sa budžetom prošlog projekta iako je ispunjavala tadašnje zahteve, novim uspesima klijenta i budžet se povećao pa arhitekta ima veću slobodu u izboru novije i skuplje opreme. |
| Nabavka i konfigurisanje rutiranja unutar novog sistema. | Rutiranje mora da se ponovo konfigurise zbog dodatka novih centralnih lokacija i klijent je izrazio želju za BGP protokolom.. |

| Uvodjenje E-comerca kao načina poslovanja za inostrane kupce i njegove mrežne i softwerske potrebe. | Kako bi se vršila komunikacija izmedju Main offica i stranih korisnika potrebno je stvoriti bezbednu zonu sa E-comerc serverim a(DMZ zona). Servere je potrebno nabaviti po što boljoj ceni. Softwerska strana ovog dela jeste pravljenje websajta preko koga ce se porudžbine praviti kao i način naplate za domace i inostrane kupce po novom dizajnu. |
| --- | --- |
| Povezanost WAN vezom izmedju centralnih lokacija. | Na svim centralnim lokacijama će raditi isti tim ljudi koji je radio u Parizu što će biti vrlo zamarajuća okolnost i njhovo povezivanje će morati da se uradi preko zahtevne tehnike HBS-poke-a. |

**5. Aplikacije i njihovi prioriteti odrzavanja**

| **Aplikacije** | **Prioriteti odrzavanja** |
| --- | --- |
| Google aplikacije | High Importance |
| Oracle Baza podataka | High importance |
| Microsoft office | Medium importance |
| Finansijski software | High importance |
| Adobe suit | Low importance |
| Oracle HCM cloud | Medium importance |
| Oracle Field Service cloud | Medium importance |
| Marketing software | Medium importance |
| Time schedule software | Low importance |

**6. Logičke izmene na mrežnom sistemu**

**6.1 Wireless mreža i bezbednost**

WiFi-i koristi WPA2 i koji je bezbedniji za upotrebu. Takodje, uvedeni su SSID za zaposlene i goste kompanije. Zaposleni koriste 2-step authentification code kako bi im pristup internetu bio dozvoljen.

**6.2 Routing i Switching protokoli**

Ruting protokol za sistem ostaje isti bez ikakvih promena. Zbog veličine enterprajz sistema i previše prostorija koje “single area OSPF” zona ne može sama da obuhvati, u novom sistemu ćemo koristiti “**multiarea OSPF” protokol**.

Kao eksterni protokol koristićemo EBGP koji će nas sistem predstaviti kao autonomni sistem (AS) i obezbediti komunikaciju sa drugim AS-ovima izvan naše mreže. Redistribucija izmedju OSPF-a i EBGP-a vršiće se preko gateway rutera.

Za L2 protokol koristimo RSTP koji nam omogućava više logicking topologija za odgovarajuće VLAN-ove na jednoj fizičkoj topologiji, kao i sprečava infinity loop-ove i broadcast stormove.

**6.3 VPN modul**

U novom sistemu postoje zasebni ruteri za VPN konekcije kao i E-comerc i Internet ruteri koji obezbedjuju redudansu u sistemu. Osim ovoga uveden je veći broj firewall uredjaja u sistem, na kojima su konfigurisani NAT i PAT kao i acces liste adresa koje smeju da pridju sistemu.VPN modul je razvrstan u 2 grane Remote acces i Site-to-Site Remote.Za Remote Access koristimo IP-sec grupu protokola kao nas VPN koja omogućava bezbednu i enkriptovanu vezu našim outsorce zaposlenima kojima je potrebna autentifikacija sa NAS uredjajem pre nego sto se povezu na sistem kompanije.Site-to-Site konekcija je takodje omogućena IP-sec vezom izmedju dve udaljene lokacije.

**7. VLAN (Virtual Local Area Network)**

U novom sistemu instalirani su VLAN-ovi koji služe da razdvoje jedan LAN na više virtualnih mreža i samim time smanje broadcast domen unutar te mreže.

**7.1 VLAN- ovi i njihov adress pool: Organizacija sedišta kompanije**

| **VLAN-Naziv** | **Ip adress range** |
| --- | --- |
| VLAN 5 (Warehouse) - Operacije i Logistika | 10.0.0.1/26-10.0.0.128/25 |
| VLAN 10  (Production Plant) - Administracija | 10.0.0.131/27-10.0.1.2/25 |
| VLAN 15 (Head-office) - Prodaja | 10.0.1.5/25-10.0.0.128/25 |
| VLAN 20 (Head-office) - Distribucija | 10.0.1.131/25-10.0.1.255/25 |
| VLAN 25 (Head-office)- Finansije | 10.0.2.2/27-10.0.2.32/27 |
| VLAN 30 (Head-office) - Menadžment | 10.0.2.35/28-10.0.2.49/28 |
| VLAN 35 (Head-office) - IT support i server room | 10.0.2.51/27-10.0.2.81/27 |
| VLAN 40 (Head-office) - Naručivanje i Pomoć Klijenta | 10.0.2.83/26-10.0.2.145/26 |
| VLAN 45 (Head-office) - Održavanje | 10.0.2.148/27-10.0.2.178/27 |
| VLAN 50 (Head-office) -  IP kamere | 10.0.2.181/25-10.0.3.50/25 |
| VLAN 55 (Head-office) -  Access pointi | 10.0.3.53/25-10.0.3.175/25 |
| VLAN 60(Data Center Servers) | 10.0.3.177/25-10.0.4.47/25 |
| VLAN 65(Head-office)-IP telefonija | 10.0.4.50/24-10.0.5.209/24 |
| VLAN 70 (Mail Servers) - DMZ  Zona i public server | 20.20.20.1/25-20.20.20.126/25 |
| VLAN 75(E-comerc DMZ)E-comerc Serveri (UK) | 30.30.30.1/25-30.30.30.126/25 |
| VLAN 75(E-comerc DMZ)E-comerc Serveri (Budapest) | 31.31.31.1/25-31.31.31.126/25 |
| LAN 75(E-comerc DMZ)E-comerc Serveri (Berlin) | 90.90.90.1/25-90.90.90.126/25 |

**8. WAN**

Tehnologija za koju se arhitekta novog sistema odlučio je MPLS, tačnije MPLS L3 - VPN. Kod MPLS VPN-a veza se stvara pomoću MPLS oblaka koji pruža usluge, a ne javne internet infrastrukture. Za razliku od internet VPN-ova site-to-site u kojima kompanija koristi svoju infrastrukturu, MPLS VPN koristi vlasničku infrastrukturu u vlasništvu VPN-a. Ova MPLS mreža, uključujući svoj oblak, funkcioniže kao tunel kojim kompanija stvara virtualne veze izmedju udaljenih lokacija. MPLS VPN-ovi ističu se po kvaliteti usluge i jednostavnosti postavljanja. Korišćenje oznaka za prosledjivanje podataka sprečava potrebu za dodatnim informacijama zaglavlja koje većina VPN-ova koristi za enkripciju. Novi sistem se sastoji od više VAN edge rutera što obezbedjuje redudansu u slučaju otkaza jednog od njih. QoS polisa je definisana na VAN edge ruterima. Osim VAN edge rutera dodat je i voice gateway ruter koji omogućava protok IP telefonije.

**9. Redudance i VRF Protokol**

Za redudansu koristimo HSRP gde je više rutera predstavljeno kao jedan virtualni (jedan ruter je postavljen kao gate-way ostali čekaju njegov otkaz, funkciju preuzima onaj koji ima najveći prioritet posle otkaza već postojećeg). Osim HSRP-a koristi se i Enthern channel izmedju L3 switcheva kao i linkova sa velikim opterećenjem kako bi se obezbedio load balancing i jednu grupu fizičkih linkova prikazao kao jedan virtualni link.

**10. Network dizajn i novi mrežni uredjaji**

Zbog većeg broja zaposlenih kao i zahteva da se obezbedi pregledan i redudantan mrežni sistem odlučeno je da isti bude konfigurisan po Hijerarhijskom modelu. Ovo je značilo da celu mrežnu arhirekturu podelimo na 3 dela (Acces, Distribucija, Core). Osim ovih delova dodata je i server farma sa novim kupljenim serverima kao i DMZ zona (svi serveri imaju po 2x mrežne kartice što obezbedjuje redudansu). Ovakav dizajn zahtevao je implementaciju većeg broja L3 i L2 uredjaja poput: L2 switcheva, MPLS-a, Firewall, rutera, servera. Naravno, pri implementaciji novog network dizajna uzet je u obzir i ograničen budžet pa je kupljena oprema sa najboljim odnosom cena/kvalitet.

**11. DATA CENTER**

Usled ekspanzije biznisa došlo je do povečanog opterećenja kojim su serveri bili izloženi, što je dovelo do potrebe za izgradnjom nove infrastrukture u vidu data centra. Metodologija izrade data centra jeste hijerarhijski model od tri sloja:

* Acces layer - uloga ovog sloja je da omogući što veću fizičku port gustinu za agregacije i core različitih servera u data centru
* Agregacioni layer - njegova glavna uloga je spajanje i slanje podatak izmedju acces layera i cora unutar data centra
* Core layer (back bone) mreže ima ulogu u minimiziranju kašnjenja slanja podataka i odgovornosti za brzo i pouzdano slanje podataka unutar mreže.

Data centar se povezuje na campus core preko dva L3 switch-a u distribucionom sloju.

**12. E-comerc modul**

Poslovanje van granica Francuske i priliv novih internacionalnih klijenata uslovili su izgradnju zasebne DMZ zone sa svojim zasebnim serverima. Zbog komunikacije sa klijentima i načinom plaćanja puten e - bankinga IP adrese datih servera su javnog tipa. Ovi serveri su direktno povezani na firewall što ih izoluje od ostatka mreže i time ne dovodi do ugrožavanja bezbednosti celokupnog sistema sa privatnim IP adresama.

**13. IP telefonija**

Kao što je klijent traio uvedena je IP telefonija korišćenjem PSTN-a. Javna komutirana telefonska mreža ili PSTN je telefonska usluga koja povezuje različite stanovnike i kompanije putem podzemnih bakrenih žica. Ova vrsta telefonske usluge naziva se i obična stara telefonska usluga (POTS), fiksni i fiksni telefoni. U našem dizajnu Trust Boundary je stavljen na Switchevima. Voice menager device upravlja dolaznim pozivima u svim centralnim lokacijama i on je zadužen za razdvajanje prioriteta voice-a od aplikacija. QoS je postavljen na WAN ruteru zato čto se koristi MPLS kao rečenje za WAN modul koji sam u semi ima ugradjen QoS sa 3 najveća pravila. Koraci ka osposobljavanju QoS-a unutar MPLS-a. PSTN pruža opciju redundantnosti aktivnog/pasivnog ili aktivnog/aktivnog balansiranja opterećenja na SIP trank grupama. Preporučuje se implementacija u aktivnoj/aktivnoj grupi tranka. Aktivno/aktivno balansiranje opterećenja omogućuje nam da osiguramo da svaki edge može prihvatiti pozive našeg PSTN Provajdera

**14. QoS**

Kako smo izabrali da koristimo VAN MPLS tehnologiju moramo koristiti i MPLS polisu. MPLS QoS podržava IP QoS. Za MPLS pakete EXP vrednost je mapirana u internu DSCP tabelu tako da PFC moše da upotrebi marking i policing NON MPLS QoS paketima. Za javnu i internu polisu odluke o MPLS markingu i policingu donose se na van interfejsima. MOdel QOS-a za koji smo se odlučili jeste DIFF Serv. U ovom modelu mreža prepoznaje specijalne klase QOS-a. U ovom modelu QoS polisa nameće različite tretmane toka saobraćaja unutar mreže. Mi kao arhitekta biramo nivo važnosti servisa za svaku klasu. Tehnika za queuing and congestion upotrebljena u dato sistemu jeste CVWFQ.Ova metoda omogućava klasifikaciju saobraćaja po želji arhitekte sistema,mana je u tome što je moguć kašnjenje glasovnog saobraćaja.

Benefiti ovog modela su:

* visoka skalabilnost,
* mogućnost više nivoa kvaliteta.

Slabosti ovakvog modela su :

* kompleksnost sistema,
* mogučnost eventualnog otkaza sistema.

**14.1 CVWFQ Tabela**

| Aplikacije i Servisi | Propusni opseg |
| --- | --- |
| Video aplikacije | 20% |
| Streming aplikacije | 15% |
| Audio aplikacije | 25% |
| Kriticne aplikacije | 28% |
| Sve ostalo | 22% |

**14.2 DSCP Tabela**

| Aplikacija | DSCP Value |
| --- | --- |
| Zvuk | 48 |
| Video | 44 |
| Audio Zapisi | 34 |
| Rutiranje | 42 |
| Switchovanje | 40 |
| Transakcije | 28 |

**15. Metodologija izrade projekta**

Za ovaj dizajn izbor je bio PPDIOO koja je prilagodjena za rok od 10 meseci. Ova metodologija se sastoji od šest faza usko povezanih: priprema, planiranje, dizajn, implementacija, rad, optimizacija.

**16. Implementacioni plan projekta**

Vremensko ograničenje projekta je **10meseci** pa je arhitekta projekta predložio plan implementacije po PPDO metodologiji za svaki mesec pojedinačno.

* **Realizacija plana u prvom mesecu**: Arhitekta i njegov tim održavaju redovne sastanke sa klijentom gde se razmatraju svi zahtevi koje je klijent predlagao kao i varijante novog sistema koje je IT konsultanska kuća predlagala. Ovo rezultuje predlogom idejnog resenja, konačnim tehničkim rešenjem sa specifikacijom potrebne opreme.
* **Realizacija plana u drugom mesecu:** Nakon usvajanja predloga tehničkog rešenja, počinje i rad na projektu. Tokom ovog meseca započinje nabavka potrebnog hardvera za sve predvidjene lokacije na kojima će se konstruisati identični mrežni sistemi kao u centrali u Parizu.
* **Realizacija** **plana u trećem mesecu**: Završetkom nabavke hardwar-a potrebna je i njegova postepena implementacija i konfiguracija na celoj infrastrukturi starog sistema.

U prvoj nedelji implementiraju se novi serveri koji se smeštaju na predvidjenim lokacijama u E-comerc DMZ zonu. U njih su ugradjene po 2 mrežne kartice radi redudanse.

U tri preostale nedelje vrši se nabavka i postavljanje servera u data centar.

* **Realizacija plana u četvrtom mesecu** : U ovom mesecu vršiće se instalacija servera u data centru i njegovo postepeno povezivanje sa campus corom. Dalje sledi postepena implementacija MPLS tehnologije.
* **Realizacija plana u petom i šestom mesecu** : U prvoj polovini planiranog vremena dovršava se implementacija MPLS tehnologije i započinje softversko definisanje MPLS L3 VPN-a.
* **Realizacija plana u sedmom i osmom mesecu** :Nakon potpune implementacije MPLs-a sve predvidjene lokacije se spajaju fullmesh topologijom. Fullmesh topologija podrazumeva spajanje lokacija svaka sa svakom. Ovakva topologija omogućava najbolju redudandu u slučaju narušene komunikacije sa bilo kojom od lokacija.
* **Realizacija plana u devetom mesecu** : Započinje uvodjenje IP telefonije preko PSTN tehnologije. Nakon uvodjenja IP telefonije dovršava se QoS polisa.
* **Realizacija plana u desetom mesecu** : Implementacijom prethodno navedenih faza projekta, pre zamene starog Sistema potrebno je uraditi detaljnu proveru svih konfiguracija kao i testiranje rada svih uredjaja. Vremenski period za testiranje i evaluaciju novog sistema iznosi četiri nedelje. Po završetku četvrte nedelje i poslednjih provera, novi mrežni sistem zamenjuje stari a projekat biva zaokružen.