UNIVERZITET U ZENICI

POLITEHNIČKI FAKULTET

ODSJEK: SOFTVERSKO INŽENJERSTVO

PREDMET: OSNOVE RAČUNARSKIH MREŽA



Projekat

Implementacija hotelske mreže

Studenti: Aida Terzić, Selma Škulj

Zenica, juni 2025.

SADRŽAJ

1. UVOD.................................................................................................3
2. TOPOLOGIJA MREŽE..........................................................................4
3. OPIS MREŽNE OPREME I NJENA ULOGA............................................5
4. KONFIGURACIJA MREŽE.....................................................................7
5. TESTIRANJE MREŽE…........................................................................10
6. ZAKLJUČAK……………….......................................................................11

**1.UVOD**

U savremenom poslovnom okruženju, efikasna i sigurna komunikacija predstavlja ključni faktor uspjeha svake organizacije, uključujući i hotelsku industriju. Moderne hotelske usluge zahtijevaju pouzdanu i stabilnu mrežnu infrastrukturu koja omogućava brzu razmjenu podataka između različitih odjeljenja, kao i pristup internetu i drugim mrežnim resursima.

Lokalne mreže (LAN - Local Area Network) igraju vitalnu ulogu u osiguravanju povezanosti unutar hotela, omogućavajući neometanu komunikaciju između recepcije, uprave, logistike, finansija i ostalih sektora. Dizajn i implementacija takve mreže zahtijevaju pažljivo planiranje, izbor odgovarajuće mrežne opreme i primjenu sigurnosnih mjera kako bi se garantovala pouzdanost, skalabilnost i zaštita podataka.

Ovaj projekat se fokusira na dizajn i implementaciju moderne hotelske mreže za **Diem Hotel** , koji se prostire na tri sprata, pri čemu svaki sprat ima tri odjeljenja sa različitim funkcijama. Mreža je konstruisana korištenjem VLAN-ova za segmentaciju mreže, OSPF protokola za dinamičko rutiranje, DHCP servera za automatsku dodjelu IP adresa te SSH za sigurnu udaljenu administraciju mrežnih uređaja. Za realizaciju projekta korišten je Cisco Packet Tracer kao alat za simulaciju mreže, što omogućava detaljno testiranje i optimizaciju prije same implementacije u stvarnom okruženju.

Cilj ovog rada je osigurati stabilnu i sigurnu mrežnu infrastrukturu koja će podržavati poslovne procese hotela, omogućiti internu i eksternu komunikaciju, te povećati efikasnost rada različitih odjeljenja kroz pouzdanu i organizovanu mrežu.

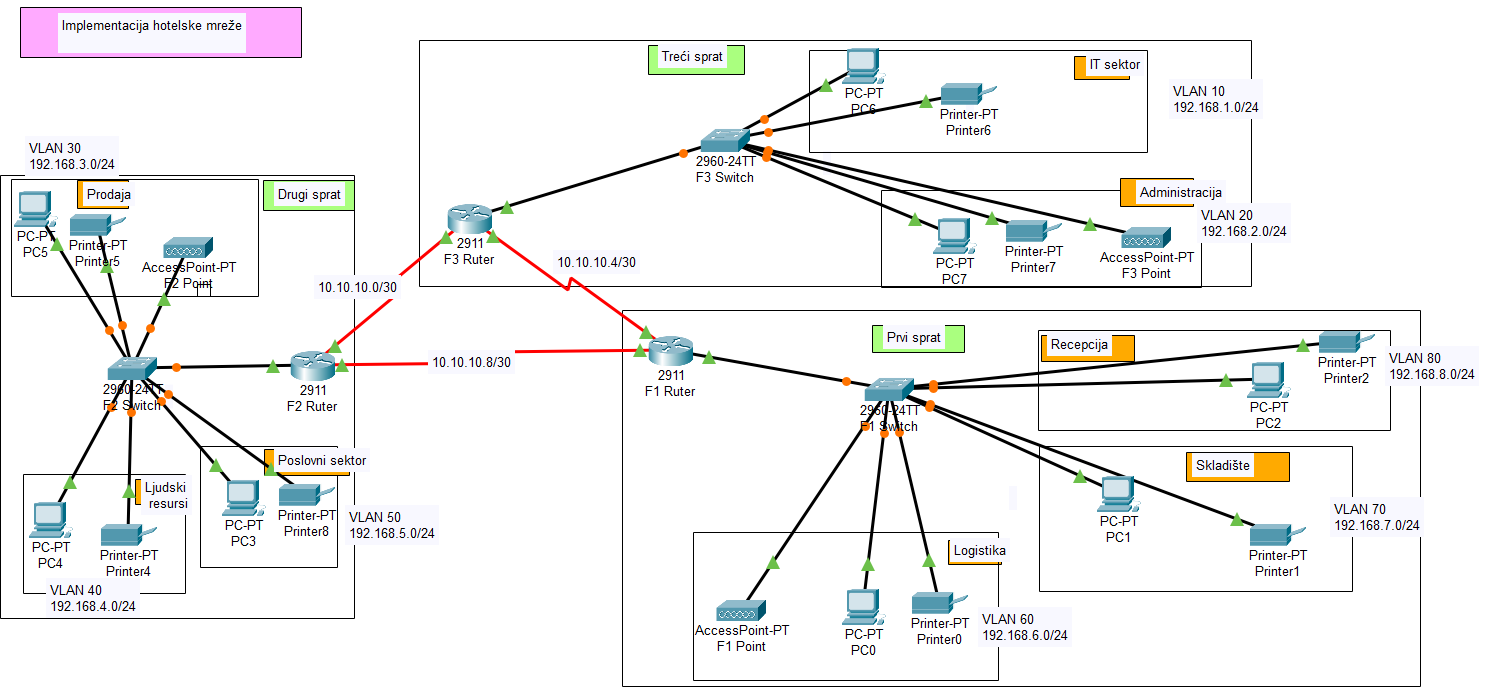
**2.TOPOLOGIJA MREŽE**

Mreža hotela Diem dizajnirana je kao složeni LAN sistem koji pokriva tri sprata, pri čemu svaki sprat sadrži tri zasebna odjeljenja. Svaki sprat ima svoj glavni switch koji povezuje uređaje unutar tog sprata, dok su svi switch-evi povezani na centralne rutere koji omogućavaju međusobnu komunikaciju i pristup internetu.

Topologija je hijerarhijska i segmentirana kroz korištenje VLAN-ova, čime se postiže veća sigurnost i bolja organizacija mreže. Svako odjeljenje pripada zasebnom VLAN-u, što omogućava izolaciju mrežnog saobraćaja između odjeljenja i smanjuje mogućnost neželjenih pristupa.

Za povezivanje spratova korištene su serijske veze između rutera (serijski DC kablovi) sa brzinom od 10 Mbps. Ruteri koriste OSPF protokol za dinamičko rutiranje, što omogućava automatsko upravljanje rutama i prilagođavanje promjenama u mreži.

Na svakom spratu su postavljene pristupne tačke (Access Points) koje omogućavaju bežičnu konekciju za laptopove i mobilne uređaje. Mreža također uključuje DHCP servere konfigurirane na ruterima, koji automatski dodjeljuju IP adrese uređajima unutar različitih VLAN-ova.



**3.OPIS MREŽNE OPREME I NJENA ULOGA**

### Ruteri (f1, f2, f3)

Ruteri su ključni uređaji u ovoj mreži jer omogućavaju usmjeravanje podataka između različitih spratova hotela, kao i između VLAN-ova unutar svakog sprata. U ovom projektu korišteni su tri rutera, označeni kao f1, f2 i f3, pri čemu svaki ruter upravlja mrežnim saobraćajem na svom spratu. Ruteri su konfigurirani za dinamičko rutiranje koristeći OSPF (Open Shortest Path First) protokol, koji omogućava efikasno pronalaženje najkraćeg i najoptimalnijeg puta za prijenos podataka između različitih mrežnih segmenata. OSPF protokol olakšava automatsku razmjenu rutnih informacija između rutera i omogućava mreži da se brzo prilagodi promjenama ili greškama u vezi.

Ruteri su također odgovorni za Inter-VLAN rutiranje, što znači da omogućavaju komunikaciju između uređaja koji se nalaze u različitim VLAN-ovima, čime se postiže segmentacija mreže i poboljšava sigurnost, a istovremeno zadržava mogućnost razmjene podataka između odjeljenja.

### Switch-evi

Na svakom spratu nalazi se jedan switch koji povezuje sve uređaje unutar tog sprata – računare, printere i druge mrežne uređaje. Switch-evi su konfigurirani sa više VLAN-ova, što omogućava logičku segmentaciju mreže unutar istog fizičkog uređaja. Svaki VLAN predstavlja zasebnu mrežnu grupu koja smanjuje broadcast saobraćaj i povećava sigurnost tako što izoluje odjeljenja i sprečava neautorizovanu komunikaciju između njih.

Pored toga, na switch-evima je implementirana i sigurnosna funkcionalnost poput port security-a, kojom se kontroliše pristup mreži na osnovu MAC adresa uređaja, čime se dodatno štiti mreža od neovlaštenih pristupa.

### Wi-Fi pristupne tačke

Na svakom spratu je instalirana bežična pristupna tačka (Access Point) koja omogućava mobilnim uređajima kao što su laptopovi, telefoni i tableti da se povežu na mrežu bez potrebe za žičanom vezom. Bežični pristup je konfiguriran sa sigurnosnim protokolima i lozinkama kako bi se spriječio neautorizovan pristup. Ove pristupne tačke su važan dio mreže jer omogućavaju zaposlenicima i gostima hotela fleksibilan i jednostavan pristup internetu i ostalim mrežnim resursima.

### Klijentski uređaji

Klijentski uređaji u mreži uključuju računare, telefone i printere koji su fizički povezani na switch-eve ili bežično na pristupne tačke. Svaki od ovih uređaja pripada određenom VLAN-u prema funkciji i odjeljenju u kojem se koristi, što osigurava pravilnu organizaciju i sigurnost mreže. Računari koriste DHCP za automatsko dobijanje IP adresa, čime se olakšava upravljanje mrežom i smanjuje mogućnost grešaka u konfiguraciji IP adresa. Printeri su također povezani u mrežu kako bi bili dostupni svim relevantnim korisnicima u njihovim VLAN-ovima.

Tabela korištene opreme

|  |  |  |
| --- | --- | --- |
| Tip uređaja | Količina (kom) | Opis funkcije |
| Router-PT (f1, f2, f3) | 3 | Ruteri koji povezuju VLAN-ove i omogućuju međusobnu komunikaciju putem OSPF-a |
| Switch-PT | 3 | Switch-evi na svakom spratu, za povezivanje krajnjih uređaja u VLAN-ovima |
| Switch-PT (Multilayer) | 3 | Omogućavaju inter-VLAN rutiranje na višem nivou |
| Wireless Router | 3 | Bežični pristup za goste i osoblje na svakom spratu |
| Server-PT (DHCP, DNS, HTTP) | 3–4 | Serveri za automatsku dodjelu IP adresa, web pristup i testiranje |
| PC-PT (klijenti) | ~10–12 | Krajnji uređaji smješteni po odjeljenjima i VLAN-ovima |
| Laptop / Tablet / Smartphone | 3–4 | Bežični uređaji povezani na Wi-Fi pristupne tačke |
| Printer-PT | 2–3 | Mrežni printeri dostupni putem VLAN-ova |
| Access Point | 3 | Za omogućavanje dodatne bežične pokrivenosti (putem Wireless Routera) |

**4.KONFIGURACIJA MREŽE**

4.1 VLAN konfiguracija

Za potrebe segmentacije mreže i povećanja sigurnosti, u okviru hotelske mreže implementirani su različiti VLAN-ovi (Virtual Local Area Networks). Svaki VLAN predstavlja zaseban logički mrežni segment, namijenjen različitim vrstama uređaja i funkcijama unutar objekta.

Implementacijom VLAN-ova omogućena je bolja kontrola saobraćaja, efikasnije upravljanje mrežom te povećana sigurnost jer se uređaji razdvajaju po logičkim grupama i međusobna komunikacija se kontroliše pomoću rutiranja i pristupnih pravila.

Tabela korištenih VLAN-ova

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN ID (VID) | Naziv | Mreža | Gateway |
| 10 | PC | 10.10.0.0/16 | 10.10.0.1 |
| 20 | AP | 10.20.0.0/16 | 10.20.0.1 |
| 30 | PRINTERI | 10.30.0.0/16 | 10.30.0.1 |
| 40 | VOICE | 10.40.0.0/16 | 10.40.0.1 |
| 50 | MGMNT | 10.50.0.0/16 | 10.50.0.1 |
| 70 | SERVERI | 10.70.0.0/16 | 10.70.0.1 |

### Opis VLAN-ova:

* **VLAN 10 – PC:** Koristi se za klijentske uređaje poput desktop računara i laptopa u različitim odjeljenjima hotela.
* **VLAN 20 – AP:** Namijenjen za pristupne tačke (Access Points) koje omogućavaju bežičnu mrežu za goste i osoblje.
* **VLAN 30 – PRINTERI:** Segment rezervisan za mrežne printere kako bi se osigurala dostupnost i kontrola pristupa.
* **VLAN 40 – VOICE:** Korišten za VoIP uređaje poput IP telefona. Odvojen VLAN za glasovne usluge smanjuje latenciju i poboljšava kvalitet poziva.
* **VLAN 50 – MGMNT:** Administratorski VLAN za upravljanje mrežnim uređajima poput rutera i switch-eva, te za pristup putem SSH-a.
* **VLAN 70 – SERVERI:** Posvećen mrežnim serverima (DHCP, DNS, HTTP) koji pružaju ključne mrežne servise svim ostalim VLAN-ovima.

Svaki switch je konfiguriran sa VLAN-ovima, pri čemu su odjeljenja podijeljena u različite VLAN-ove kako bi se omogućila sigurnost i kontrola pristupa:

|  |  |  |
| --- | --- | --- |
| VLAN | Odjeljenje | IP mreža |
| 10 | Recepcija | 192.168.1.0/24 |
| 20 | Administracija | 192.168.2.0/24 |
| 30 | IT | 192.168.3.0/24 |
| 40 | Finansije | 192.168.4.0/24 |
| 50 | Logistika | 192.168.5.0/24 |

### 4.2 DHCP serveri

U cilju automatizacije dodjele IP adresa unutar mreže, na svakom ruteru konfigurisan je DHCP server. Svaki DHCP pool definisan je zasebno za odgovarajući VLAN, pri čemu su uneseni sljedeći parametri:

* Podmreža (subnet)
* Gateway (default-router)
* DNS server
* IP adrese koje su dostupne za dodjelu (pool)

Nakon konfiguracije, testiran je proces automatske dodjele IP adresa putem DHCP protokola, a uređaji su uspješno dobili validne IP adrese u skladu sa svojim VLAN-ovima.

### 4.3 Inter-VLAN rutiranje i OSPF konfiguracija

Za omogućavanje komunikacije između različitih VLAN-ova korištena je tehnika **Inter-VLAN rutiranja** putem podinterfejsa (subinterfaces) na ruterima. Svaki podinterfejs je dobio odgovarajući VLAN ID i IP adresu gateway-a za tu mrežu.

Radi dinamičkog pronalaska najboljeg puta za komunikaciju između mreža na različitim spratovima, implementiran je **OSPF (Open Shortest Path First)** protokol. Ruteri (f1, f2, f3) su konfigurisani da razmjenjuju informacije o dostupnim mrežama putem OSPF area 0.

Kompletna konfiguracija je testirana i potvrđeno je da uređaji iz različitih VLAN-ova mogu komunicirati međusobno, što ukazuje na ispravno funkcionisanje rutiranja i segmentacije mreže.

### 4.4 Serijske veze i clock rate

Za međusobno povezivanje rutera korišteni su serijski DCE kablovi, koji zahtijevaju konfiguraciju brzine takta na jednoj strani veze. Na serijskim interfejsima gdje se koristi DCE kraj, postavljen je **clock rate** vrijednosti **64000 bps**, kako bi se omogućila ispravna sinhronizacija i uspostava komunikacije.

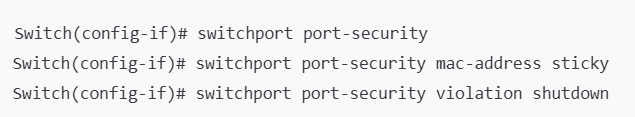
Ova konfiguracija je ključna za pravilno funkcionisanje serijske veze između rutera jer bez definisanog takta ne može doći do razmjene podataka. Nakon postavljanja clock rate vrijednosti i IP adresa na oba kraja veze, serijski link je uspješno aktiviran i testiran.

### 4.5 Sigurnosne postavke

U cilju povećanja sigurnosti mreže, implementirane su sljedeće mjere:

* Port Security: Na switch-evima je omogućena sigurnost portova. Svaki port prihvata saobraćaj samo od poznatih MAC adresa. Aktivirana je sticky opcija kojom se MAC adrese automatski zapisuju u konfiguraciju. U slučaju pokušaja neovlaštenog pristupa s druge MAC adrese, port ulazi u stanje shutdown, čime se sprječava neautorizovani pristup.
* SSH pristup: Za daljinsku administraciju rutera, konfigurisano je Secure Shell (SSH) umjesto nesigurnog Telnet protokola. Na svakom ruteru su podešeni:
  + hostname i domena
  + korisničko ime i lozinka
  + kripto ključevi (RSA) za sigurnu komunikaciju

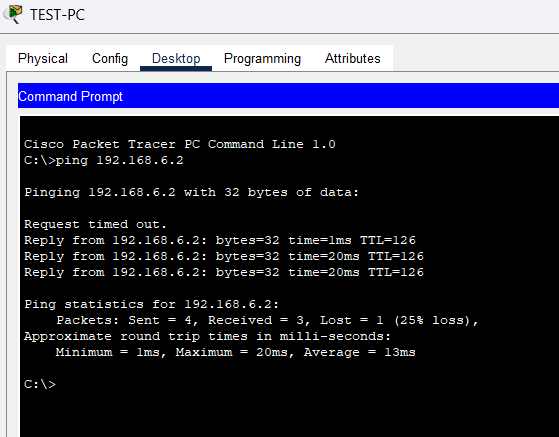
Nakon toga, uspješno je testiran pristup ruterima putem SSH sa udaljenih računara. Ova mjera omogućava sigurnu administraciju mrežnih uređaja, čak i kada im se pristupa putem javne mreže.

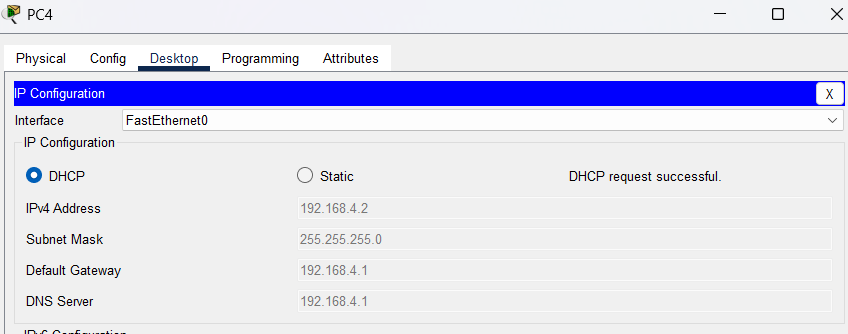


### 5.TESTIRANJE MREŽE

Nakon završene konfiguracije svih mrežnih komponenti, izvršeno je detaljno testiranje funkcionalnosti mreže kako bi se osiguralo da svi segmenti sistema pravilno komuniciraju i da sigurnosne postavke rade prema očekivanjima.

Testiranje je obuhvatilo sljedeće korake:

* **Testiranje međusobne komunikacije između VLAN-ova:** Korištena je komanda ping sa računara iz jednog VLAN-a prema računaru u drugom VLAN-u, kako bi se potvrdilo da je **Inter-VLAN rutiranje** uspješno konfigurisano i funkcionalno.
* **Validacija DHCP konfiguracije:** Na svim klijentskim uređajima je provjereno da li **DHCP serveri automatski dodjeljuju ispravne IP adrese**, uključujući gateway i DNS informacije, u skladu s VLAN-ovima kojima ti uređaji pripadaju.



* **Provjera SSH pristupa:** Sa lokalnog računara uspostavljena je sigurna veza sa ruterom putem ssh komande, čime je potvrđeno da su **SSH protokol, korisnički nalozi i kriptografski ključevi** ispravno konfigurisani.
* **Testiranje sigurnosti portova (port-security):** Na switch uređajima je povezan test uređaj na port koji je prethodno konfigurisan za prihvat samo poznatih MAC adresa. Prilikom povezivanja novog, neautorizovanog uređaja, port je automatski detektovao nepoznatu MAC adresu i **prešao u stanje gašenja (shutdown)**, čime je potvrđena ispravna implementacija sigurnosne politike.

Ovim testiranjem je potvrđeno da mreža ispravno funkcioniše u svim predviđenim segmentima, te da su sigurnosne postavke efektivne u zaštiti od neautorizovanog pristupa.

### ****6. ZAKLJUČAK****

Ovaj projekat je uspješno demonstrirao kompletan proces dizajna i implementacije složene mrežne infrastrukture prilagođene hotelskom okruženju. Kroz praktičan rad na simulaciji mreže korištenjem Cisco Packet Tracera, uspjeli smo uspostaviti pouzdanu i efikasnu komunikaciju između različitih spratova i odjeljenja koristeći VLAN-ove za segmentaciju mreže.

Implementacija DHCP servera na ruterima omogućila je automatsku dodjelu IP adresa krajnjim uređajima, što znatno olakšava upravljanje mrežom i smanjuje mogućnost grešaka u konfiguraciji. Korištenje OSPF protokola za dinamičko rutiranje osiguralo je optimalan i skalabilan prijenos podataka između mrežnih segmenata, što je posebno važno u većim mrežnim okruženjima kao što je hotel.

Posebna pažnja posvećena je sigurnosti mreže – implementacijom SSH pristupa omogućeno je sigurno daljinsko upravljanje mrežnim uređajima, dok je port-security na switch portovima spriječio neautorizovani pristup mreži i zaštitio resurse od mogućih prijetnji.

Ovaj projekat predstavlja izvrsnu praksu za buduće mrežne administratore i inženjere, jer obuhvata ključne aspekte dizajna, implementacije i sigurnosti mreža, kao i rješavanje problema koji se javljaju u realnim situacijama. Stečena znanja i vještine značajno doprinose pripremi za rad u profesionalnim mrežnim okruženjima.