** **

Univerzitet u Zenici Politehnički fakultet 2023/24

*Računarske mreže 1*

*Prva godina I. ciklus*

Dokumentacija projekta

Simulacija bankovnog sistema koristeći Cisco Packet Tracer

**Članovi tima:**

Ibrahim Bišić

Lamija Arnaut

Esada Durmić

Danis Đuhera

**UVOD**

Bankovni sistem predstavlja okosnicu moderne ekonomije, omogućavajući razmjenu dobara i usluga, čuvanje štednje, kreditiranje, te mnoge druge financijske operacije koje su ključne za funkcionisanje društva. Tehnološki napredak u bankarstvu doveo je do digitalizacije i automatizacije mnogih procesa, čineći poslovanje bržim, sigurnijim i efikasnijim.

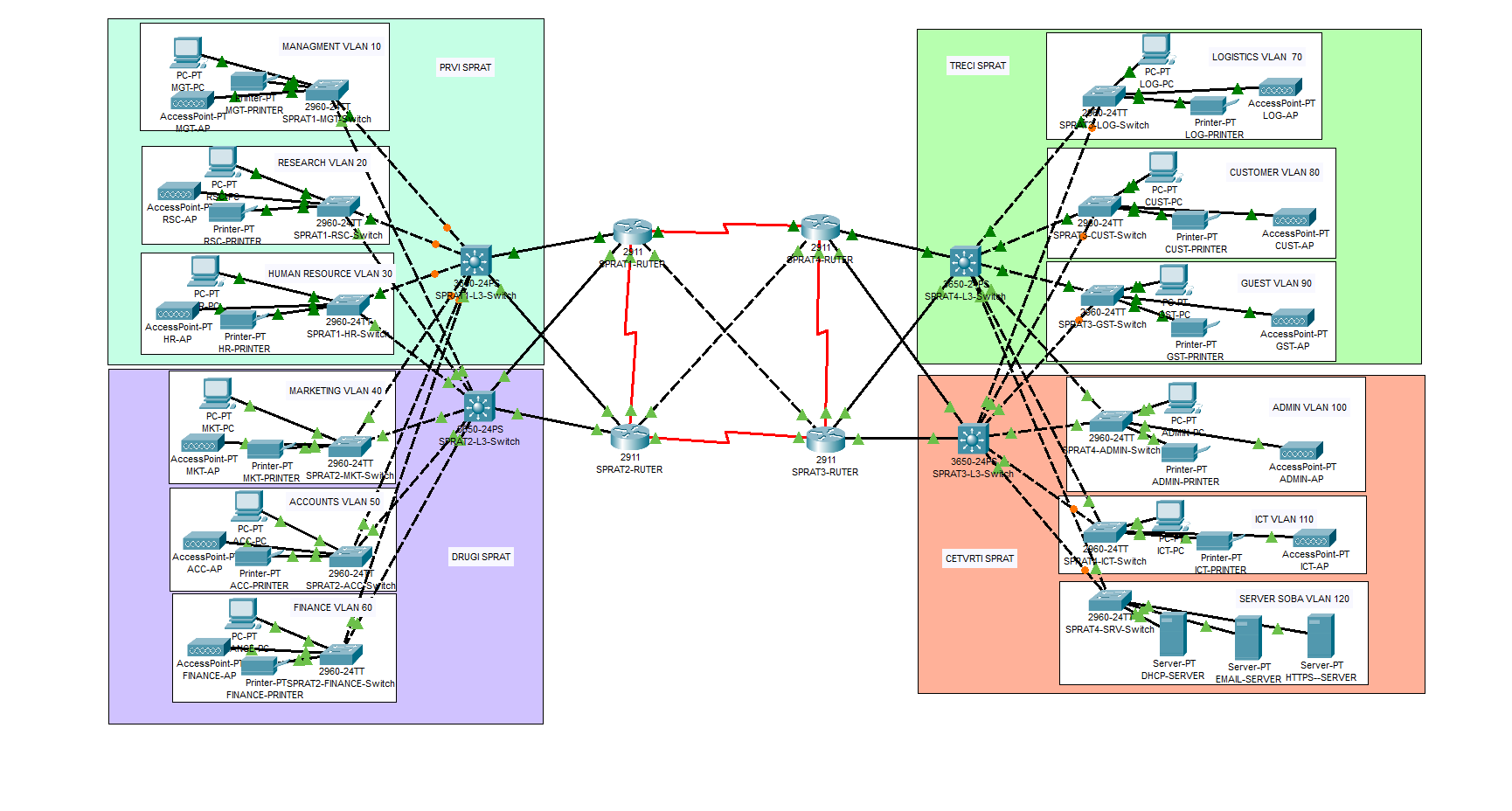
Jedan od ključnih aspekata modernog bankarstva je implementacija sigurnih i pouzdanih mrežnih infrastruktura koje omogućavaju neometan protok informacija i podataka. Upravo zbog toga, mrežno modeliranje i simulacije postaju sve značajniji alati u dizajniranju i održavanju bankovnih sistema. Cisco Packet Tracer, kao jedan od vodećih softverskih alata za simulaciju mreža, omogućava detaljno modeliranje mrežnih topologija, testiranje različitih scenarija i otkrivanje potencijalnih problema prije nego što se implementacija provede u stvarnom okruženju.

Ovaj seminarski rad će istražiti ulogu i značaj Cisco Packet Tracera u simulaciji bankovnih mrežnih sistema. Detaljno ćemo analizirati osnovne funkcionalnosti ovog alata, prikazati primjer konkretnih mrežnih topologija specifičnih za bankovne sisteme. Demonstrirat ćemo kako se mogu unaprijediti sigurnost i efikasnost bankovnih mreža, te kako se pomoću ovog alata može optimizirati mrežna infrastruktura u skladu sa specifičnim potrebama bankovnog sektora.

**IMPLEMENTIRANE TEHNOLOGIJE**

1. Kreranje mrežne topologije koristeći Cisco Packet Tracer
2. Hijerarhalni Mrežni Dizajn
3. Povezivanje mrežnih uređaja sa ispravnim kablovima
4. Konfigurisanje osnovih postavki uređaja
5. Kreiranje VLAN-ova i dodavanje portova VLAN-ovima
6. Subnetiranje i IP adresiranje
7. Konfigurisanje Inter-VLAN rutrianja na Multilejerske switcheve
8. Konfigurisanje DHCP server uređaja da pruže dinamičku IP alokaciju
9. Konfigurisanje SSH kao sigurni udaljeni pristup
10. Konfigurisanje OSPF kao ruting protocol
11. Konfigurisanje swtichport security ili Port-Security na switch-evima
12. Konfigurisanje WLAN ili wireless mrežu
13. Host Device konfiguracija
14. Testiranje i verifikacija komunikacije unutar mreže (simulacija)

**KREIRANJE MREŽNE TOPOLOGIJE**



Mrežnu topologiju smo podijelili na vise djelova odnosno layera. Imamo *Core layer* koji predstavljaju 4 rutera u sredini, zatim *Access layer* koji predstavljaju switcheve nakon Host layera i *Distribution layer* predstavljaju samo odsjeci koji se nalaze u banci.

Za povezivanje uređaja unutar mrežne topologije koristili kablove:

*Serial DCE* koji smo koristili za povezivanje rutera u Core layeru, *Copper Cross-over* koji smo koristili unutar Core layer-a za povezivanje izmedju dijagonalnih rutera

Za ostalo smo koristili opciju da nam automatski izabere vrtu konekcije.

Što se tiće osnovne konfiguracije topologije za početak smo uključili svaki interfejs unutar *Core layer* dijela, nakon toga smo otišli u *Access layer* switcheve gdje smo ubacili AC-POWER-SUPPLY modul koji nam, naravno, daje energiju.

Podijelili smo topologiju na 4 sprata.

Prvi sprat ima 3 odsjeka: Management, Research, Hr

Drugi sprat: Marketing, Accounts, Finance

Treći sprat: Logistics, Customer, Guest

Četvrti sprat: Admin, ICT I Server sobu

Svaki odsjek ima svoj VLAN broj, pa npr. Management ima VLAN 10, Research ima VLAN 20, te Server soba ima VLAN 120.

**KONFIGURISANJE TOPOLOGIJE**

Prvo što smo uradili jest konfigurisanje Hostname svim *Distribution layer* switchevima pomoću komande „hostname \_\_\_\_\_\_\_\_“. Nakon tog smo konfigurisali Banner Message pomoću komande „banner motd #\_\_\_\_\_\_\_\_\_#“. Nakon toga smo uradili line console sa komandom „line console 0”, te omogućili šifru pomoću “password \_\_\_\_\_\_”, gdje nam je šifra *cisco.*

Nakon toga smo koristili komandu „line vty 0 15“. Ova naredba služi za podešavanje virutelnih terminalnih linija. Omogućavaju daljinski pristup uređaju preko mreže kao što je SSH. Te opet pišemo komandu “password cisco”

Nakon toga smo autentifikovali pomoću “login”.

Konfiguracijom naredbe “no ip domain lookup” onemogućili smo funkcije pretraživanja DNS-a za nepoznate unose. Kada se unese nepoznata naredba uređaj neće pokušavati pretražiti DNS poslužitelj, čime se izbjegava nepotrebno kašnjenje. Poslije toga, naredbom “enable password cisco” omogućavamo samu šifru.

Za enkripciju svih lozinki koristili smo “service password-encryption”, kada je omogućena, ova naredba koristi tip 7 enkripciju (Cisco Proprietary Encryption) koja je relativno slaba, ali ipak pruža osnovnu razinu zaštite time što lozinke nisu pohranjene u običnom tekstu.

Svaku od ovih komandi smo konfigurisali u svim switchevima unutar Distribution i Access layera.

Konfigurišemo SSh na svim switchevima pomoću komandi “ip domain-n”, “ip domain-name cisco.net”, “ username cisco password cisco”, “crypto key generate rsa”, generisali smo 1024 bitni RSA ključ.

Komandom “login local” služi za omogućavanje autentifikacije korisnika koristeći lokalne korisničke račune definirane na uređaju.

“transport input ssh” koristi za omogućavanje pristupa uređaju putem SSH (Secure Shell) protokola na VTY (virtual terminal) linijama. Te smo spremili ovu konfiguraciju pomoću “do wr”.

Te smo SSH omogućili na svakom switchu unutar topologije.

**KONFIGURACIJA VLAN-a I SWITCHPORT SECURITY**

“int range fa0/1-2” koristi se za istovremenu konfiguraciju više sučelja (interface-a).

“switchport mode trunk” koristi se za konfiguriranje sučelja kao trunk portova. Trunk portovi mogu nositi promet za više VLAN-ova, što je korisno za povezivanje preklopnika ili povezivanje preklopnika s rutera ili drugim mrežnim uređajima koji trebaju komunicirati s više VLAN-ova.

“vlan 10” služi za učazak u konfiguracijski način rada za VLAN 10

“name \_\_\_\_\_” dodjeljivanje imena

“int range fa0/3-24” access portovi

“switchport mode access” ulazak u konfiguracijski način access-a

“switchport access vlan 10” dodjeljivane VLAN 10 access portu

“switchport port-security” konfiguriranje sigurnosnih značajki na sučelju kako bi se spriječilo neovlašteno povezivanje uređaja.

“switchport port-security maximum 2” postavljanje maksimalnog broja dopuštenih MAC adresa koje se mogu naučiti na određenom interfejsu.

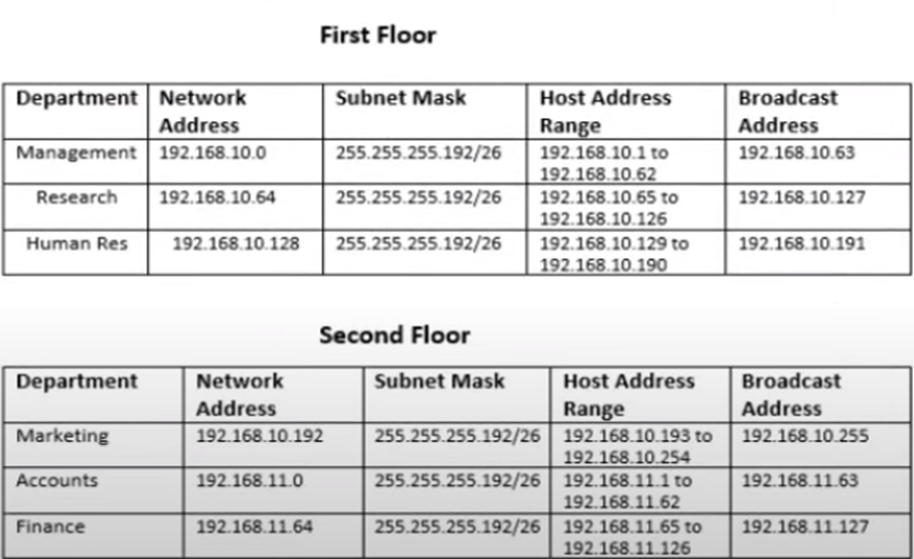
“switchport port-security mac-address sticky” konfiguriranje port-security značajke kako bi automatski naučio i zadržao MAC adrese svih uređaja koji se trenutno priključuju na sučelje

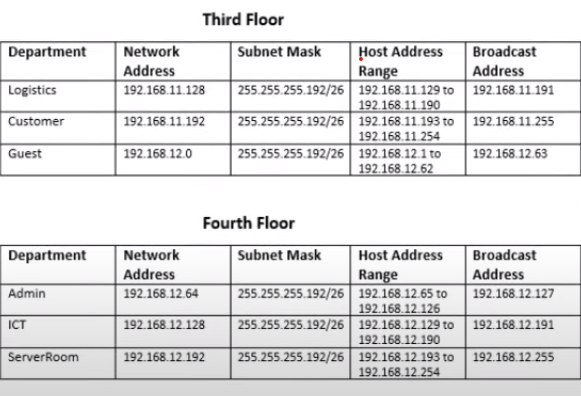
“switchport port-security violation shutdown” za konfiguriranje reakcije preklopnika u slučaju prekoračenja broja dopuštenih MAC adresa na sučelju s omogućenom port-security značajkom

Konfigurišemo na svaki switch koji imamo, samo mjenjamo VLAN broj.

**SUBNETIRANJE I IP ADRESIRANJE**

Dodali smo IP adrese na svaki odsjek.





Ovo su adrese za svaki sprat.

Konfigurisemo trunk portove swithevima unutar *Access layera* pomoću komandi

“int range gig1/0/3-8”

“switchport mode trunk”

Sada ćemo dodijeliti ip adrese

“int gig1/0/1”

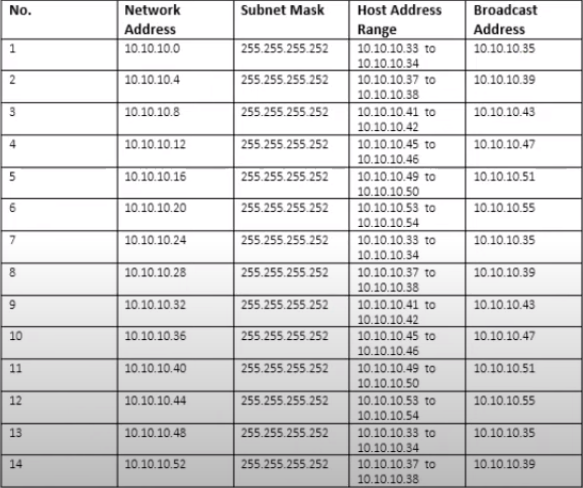
“ip address 10.10.10.1 255.255.255.252” “exit”

“int gig1/0/2”

“ip address 10.10.10.9 255.255.255.252”

I nastavljamo korititi iste komande, samo mijenjamo IP adresu za svaki Switch odnosno interfejs unutar Switch-a.

Ovo su IP adrese između Rutera I Layer3 Switcheva



Što se tiće serial portova unutar Rutera koji se nalaze u *Core layer-u* konfigurišemo ih pomoću interfejsa unutar configa.

**OSPF KOFIGURACIJA**

Da bismo konfigurisali ospf koristit ćemo se komandama:

“router ospf 10” se koristi u konfiguracijskom načinu rada Cisco IOS uređaja za pokretanje OSPF (Open Shortest Path First) procesa s identifikatorom 10

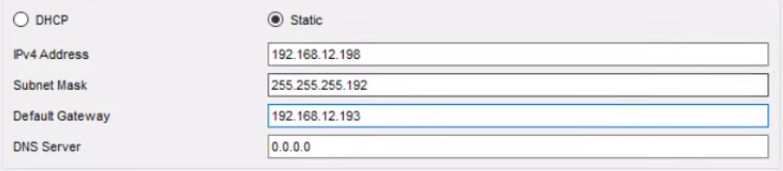
„network 10.10.10.0 0.0.0.3 area 0“ koristi unutar konfiguracijskog načina OSPF procesa (nakon što smo unutar "router ospf 10" konfiguracije) kako bismo omogućili OSPF na određenoj mreži i dodijelili je određenom području.

„do wr“ spremanje kofiguracije

Ponavljamo za svaki ruter unutar *Core Layer-a I switch unutar Access layer-a*

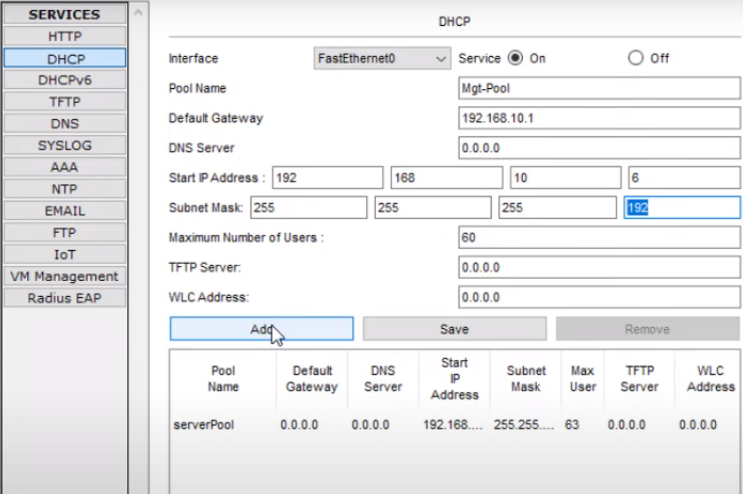
**STATIC IP ADRESA ZA SERVER SOBU**

Unutar server uređaja ulazimo u Desktop I nakon toga u IP konfiguraciju gdje pišemo u IPv4 “192.168.12.196”, sa subnet maskom “255.255.255.192” I Default Gateway “192.168.12.193”, te za druga dva servera unutar IPv4 mijenjamo samo zadnji broj, tj. dodajemo jedan.



**DHCP SERVER KONFIGURACIJA**

Da bismo konfigurisali DHCP konfigurisali DHCP ući ćemo unutar DHCP-SERVER uređaja te ćemo unutar services početi sa konfiguracijom



I dodajemo pool za svaki odsjek koji imamo unutar banke, mijenjamo samo default gateway, Startnu ip adresu i subnet masku.

**Inter-VLAN RUTIRANJE**

Kofigurišemo VLAN-ove od 10 do 60.

“int vlan 10”

“no shutdown”

“ip add 192.168.10.1 255.255.255.192”

“exit”

Nakon toga ulazimo u VLAN 20 I mijenjamo ip adresu “ip add 192.168.10.65”, te VLAN 30 “ip add 192.168.10.129”

“ip helper-address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_” koristi se kako bi se omogućilo preusmjeravanje određenih vrsta prometa prema odredišnom serveru, često DHCP serveru, na drugom mrežnom segmentu.

Konfigurisat ćemo na svaki L3 switch-eve od sprata 1 i 2. A što se tiće spratova 3 i 4 konfigurisat ćemo VLAN-ove 70 do 120, gdje ćemo koristiti iste komande sa blagim promjenama brojeva.

**WIRELESS NETWORK**

Ulazimo u neki AP I konfigurisemo tako što dodamo na port 1 mogućnost autentifikacije WPAK2-PSK I PSK Pass Phrase “Finance@2024” kao šifru. Pomoću nekog uređaja poput laptopa palimo internet te se pomoći šifre povezujemo na mrežu.