Individual Assessment Coversheet

To be attached to the front of the assessment.

Campus: Tygervalley

Faculty: Information Technology

Module Code: ITNAA2-34

Group: 1

Lecturer's Name: Grant Samson

Student Full Name: Valmy Kalombo

Student Number: EDUV4981741

Indicate	Yes	No
Plagiarism report attached		x

Declaration:

I declare that this assessment is my own original work except for source material explicitly acknowledged. I also declare that this assessment or any other of my original work related to it has not been previously, or is not being simultaneously, submitted for this or any other course. I am aware of the AI policy and acknowledge that I have not used any AI technology to generate or manipulate data, other than as permitted by the assessment instructions. I also declare that I am aware of the Institution's policy and regulations on honesty in academic work as set out in the Conditions of Enrolment, and of the disciplinary guidelines applicable to breaches of such policy and regulations.

Signature	Date
valmykalombo	21/11/2025

Lecturer's Comments:

Marks Awarded:	%

Signature	Date

TABLE OF CONTENTS

1. Introduction

This research-based report presents the planning, configuration, and verification of an integrated enterprise network for Gijima Trading, a medium-sized organization operating across Johannesburg, Bloemfontein, Cape Town, and Durban. The purpose of this project was to design a scalable, secure, and centrally administered network using Cisco Packet Tracer. Through the implementation of switching, routing, VLAN segmentation, inter-VLAN communication, DHCP allocation, RIP v2 routing, wireless technologies, and external web services, the network demonstrates full operational readiness. The report provides both the technical reasoning and practical configuration steps carried out, along with screenshots showing successful implementation.

2. Scenario Overview

Gijima Trading's legacy network relied on ad hoc and isolated configurations, causing poor performance, frequent downtime, and a lack of central management. The IT Manager has requested new integrated architecture connecting all four branches using point-to-point leased lines and a centralized DHCP and email service hosted in Bloemfontein.

Key requirements included:

- 2960 switches across all branches.
- Must create VLANs 10, 20 & 30 in JHB and VLANs 100 & 200 in CPT network.
- A Central DHCP and DNS in Bloemfontein.
- RIP v2 as the routing protocol.
- Full connectivity between sites through point-to-point serial interfaces.
- Inter-VLAN routing on JHB_R1 and CPT_R1.
- Corporate and guest wireless networks.
- A public web server hosted in an internet cluster reachable from all internal networks.

3. Question 1 – Packet Tracer Network Implementation

1.1. Network Design in Packet Tracer

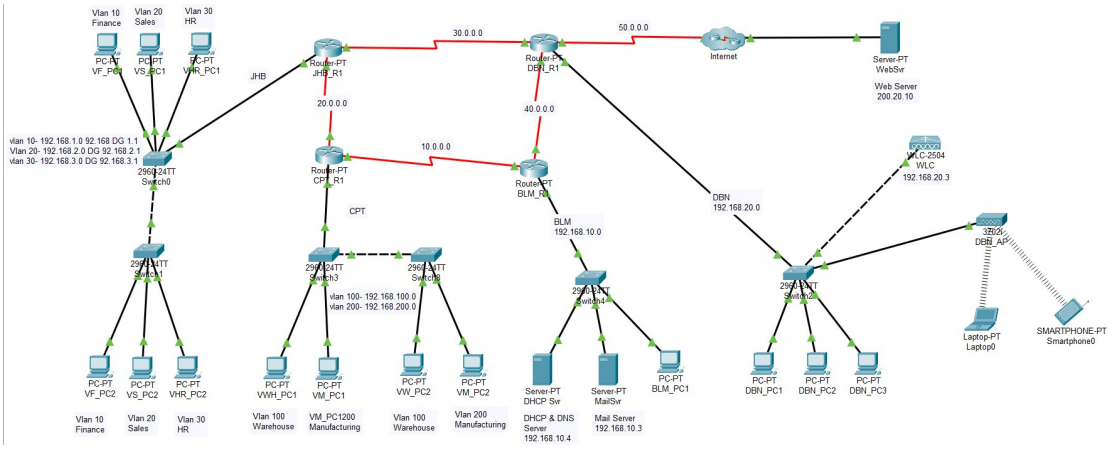
The network topology was designed exactly as specified in the scenario using the following devices:

- Cisco 2811 routers (one per city)
- 2960-24TT switches at each branch
- Serial point-to-point connections for WAN links
- A dedicated internet cluster containing an ISP Router and a switch
- A central DHCP & DNS server - 192.168.10.4
- A Mail Server - 192.168.10.3
- VLAN-based PCs across all locations
- Wireless LAN Controller (WLC)
- Lightweight Access Point (LAP)
- Laptop
- Smartphone

Design Steps Included:

- Dragging and placing routers, switches, servers, APs, WLC, PCs, Laptop and Smartphone.
- Connecting WAN routers using Serial DCE/DTE cables.
- Connecting LAN devices using Copper Straight-Through cables.
- Creating the Internet Cluster and Web Server.

Figure 1: Completed Enterprise Network Topology

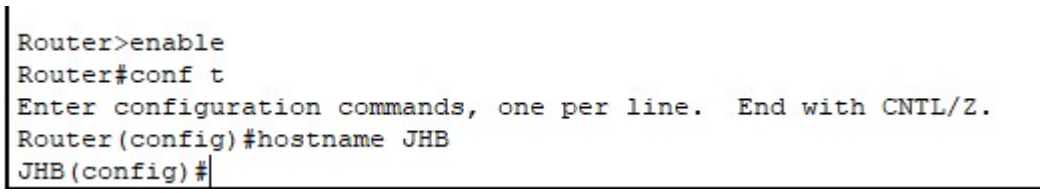


1.2. Router Renaming

All routers were renamed using global configuration mode:

Router(config)# hostname JHB
Router(config)# hostname BLM
Router(config)# hostname CPT
Router(config)# hostname DBN
Router(config)# hostname Internet

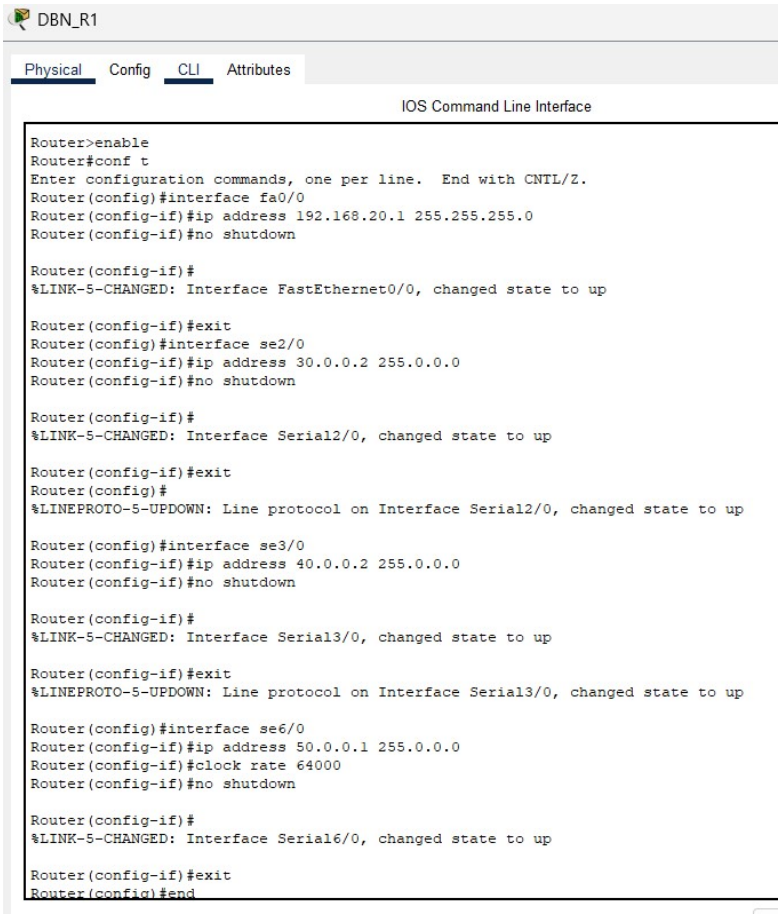
Figure 2: Renaming JHB router.



1.3. Router IP Addressing & Connectivity Tests

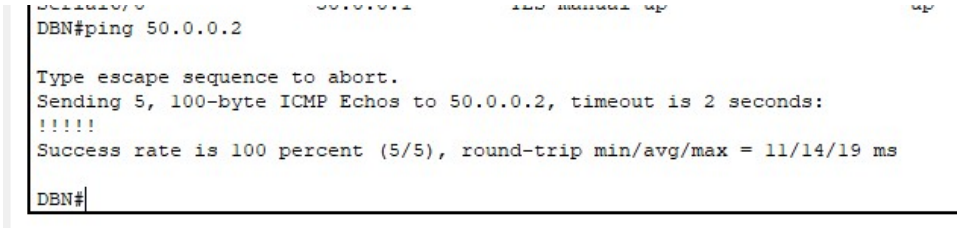
All routers were configured using the IP addressing table which I used and all routers were configured using, WAN serial interfaces (se2/0, se3/0, se6/0) links and uses /8 network addresses while LAN interface (fa0/0) segments uses /24 subnets. Connectivity was tested using the ping command over every Point-to-Point connection.

For example on DBN_R1, I configured the interfaces as shown below:



After configuration, connectivity was tested using ping:

Figure 3: Successful ping request on DBN_R1.



All of the routers responded successfully to the ping request.

Figure 4: Successful configuration of IP address on DBN_R1.

```
DBN>enable
DBN#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES manual administratively down down
GigabitEthernet1/0     192.168.20.1    YES manual up                    up
Serial2/0              30.0.0.2        YES manual up                    up
Serial3/0              40.0.0.2        YES manual up                    up
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
Serial6/0              50.0.0.1        YES manual up                    up
DBN#
```

1.4. DHCP Server Configuration

The DHCP server in Bloemfontein was given a static IP address (192.168.10.4). I created about seven pools and were configured as:

For the BLM site:

BLM_Default
Network: 192.168.10.0/24
Gateway: 192.168.10.1
DNS: 192.168.10.4

For the Johannesburg VLANs I created separate VLANs for instance:

VLAN10
Network: 192.168.1.0/24 (Finance)

VLAN20
Network: 192.168.2.0/24 (Sales)

VLAN30
Network: 192.168.3.0/24 (HR)

For the Cape Town VLANs:

VLAN100
Network: 192.168.100.0/24 (Warehouse)

VLAN200
Network: 192.168.200.0/24 (Factory)

For the Durban pool:

DBN_Pool
Network: 192.168.20.0/24

All pools provide DNS, default gateways, and subnet masks as per design, and all PCs across all sites successfully pulled IP addresses from the BLM DHCP server.

Figure 5: DHCP pools for VLANS.

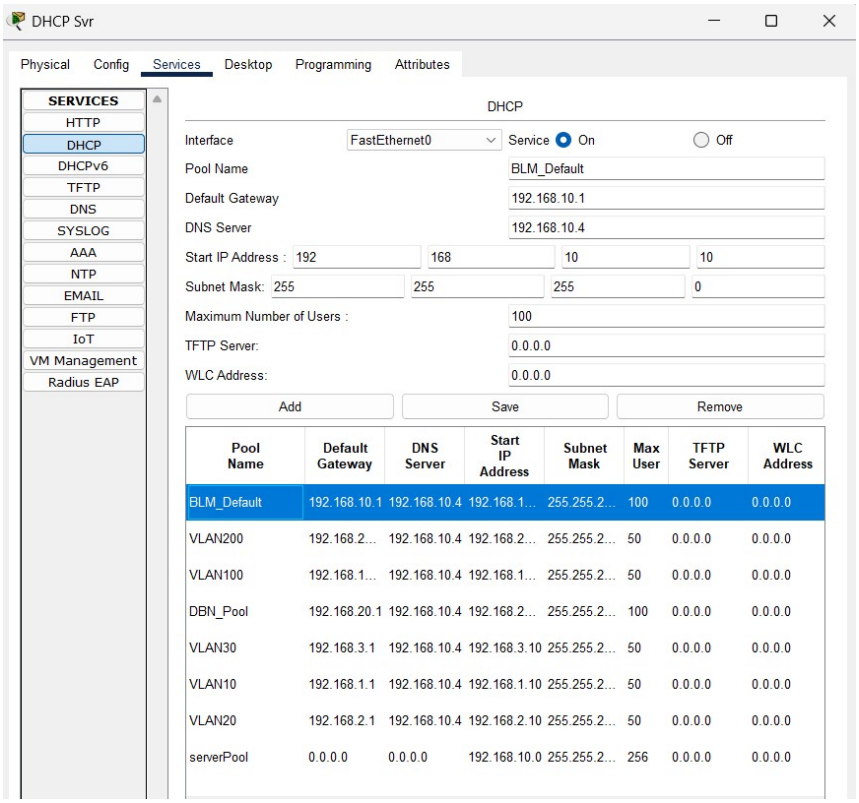
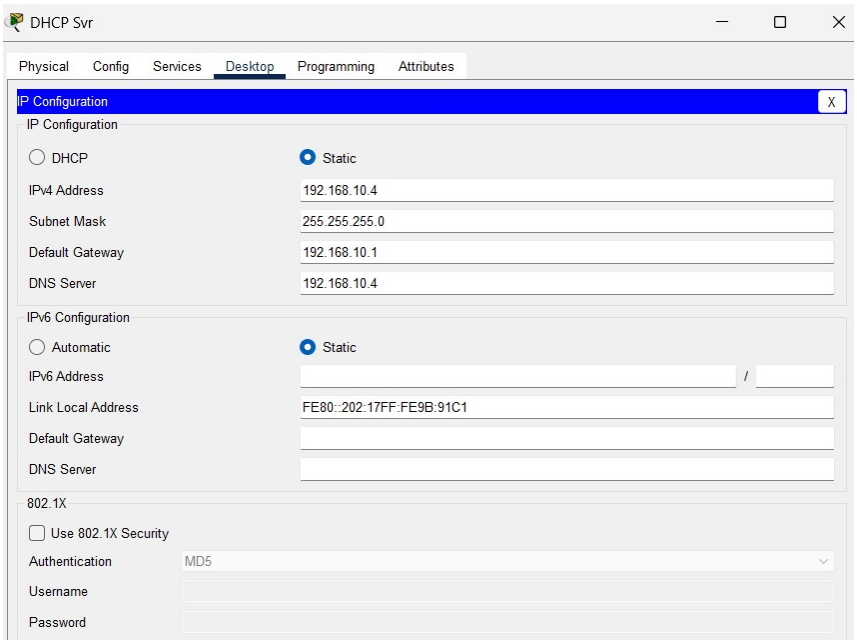


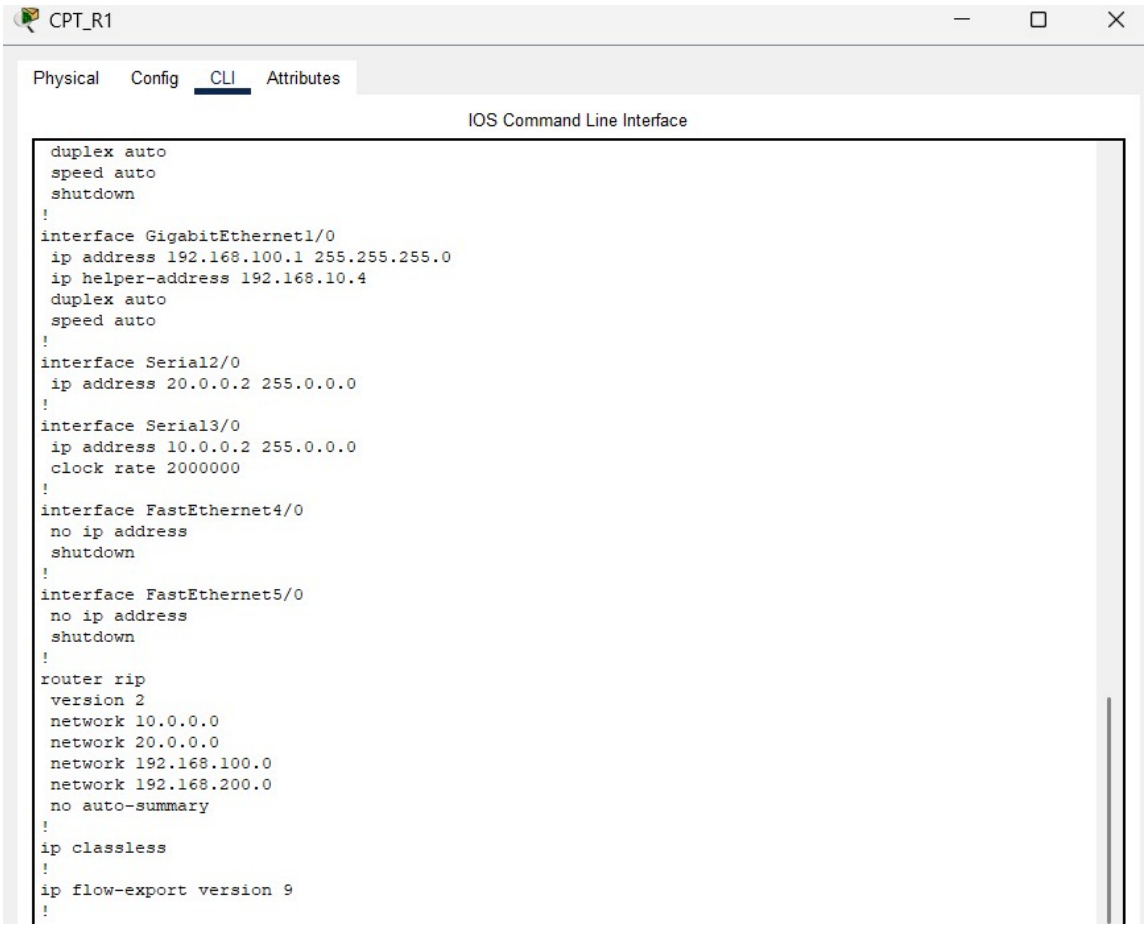
Figure 6: DHCP Static IP configuration.



1.5. RIP v2 Routing Protocol Configuration

All routers were configured with RIP version 2 using the network statements matching the WAN and LAN networks. Auto-summary was disabled to ensure accurate route propagation.On each router I configured the RIP v2 Protocol as shown below:

Figure 7: RIP v2 configuration on all routers.



Doing this allowed dynamic routing across all WAN links.

1.6. Route Verification

The command ***'show ip route rip***' was executed on each router to verify that they correctly learned and advertised routes across the network.

All routes appeared as *R* (RIP-learned), confirming successful routing propagation between all branches.

Figure 8: RIP v2 configuration on all routers.

```
DBN>enable
DBN#show ip route rip
R    10.0.0.0/8 [120/1] via 40.0.0.1, 00:00:03, Serial3/0
R    20.0.0.0/8 [120/1] via 30.0.0.1, 00:00:30, Serial2/0
R    192.168.1.0/24 [120/1] via 30.0.0.1, 00:00:30, Serial2/0
R    192.168.2.0/24 [120/1] via 30.0.0.1, 00:00:30, Serial2/0
R    192.168.3.0/24 [120/1] via 30.0.0.1, 00:00:30, Serial2/0
R    192.168.10.0/24 [120/1] via 40.0.0.1, 00:00:03, Serial3/0
R    192.168.100.0/24 [120/2] via 30.0.0.1, 00:00:30, Serial2/0
                      [120/2] via 40.0.0.1, 00:00:03, Serial3/0
R    192.168.200.0/24 [120/2] via 30.0.0.1, 00:00:30, Serial2/0
                      [120/2] via 40.0.0.1, 00:00:03, Serial3/0


DBN#
```

4. QUESTION 2 – ADVANCED CONFIGURATION

2.1. DHCP Reachability for All Devices

DHCP relay (ip helper-address) was configured on JHB, DBN, and CPT routers to forward DHCP discover messages to the server in Bloemfontein. The verification on the PCs confirmed that the PCs across all VLANs received correct IP addresses.

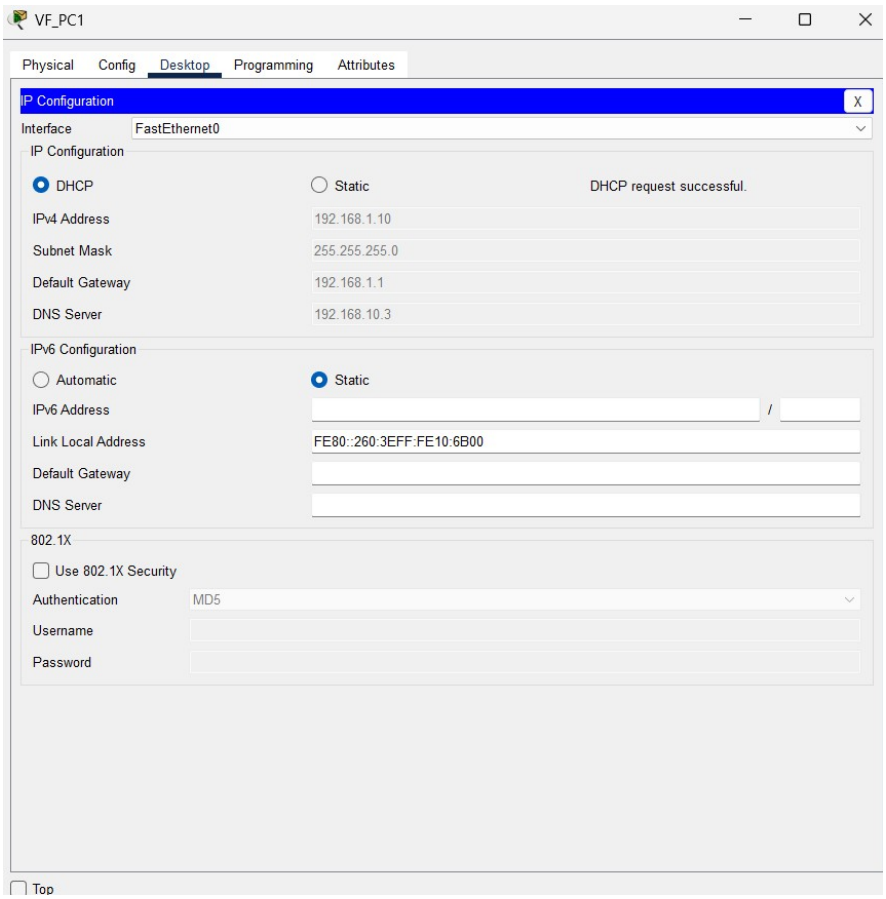
After adding router DHCP helper addresses:

interface fa0/0
ip helper-address 192.168.10.4

All branch devices received correct DHCP information, including:

- IP Address
- Subnet Mask
- Default Gateway
- DNS Server (192.168.10.4)

Figure 9: DHCP request success on PCs.



2.2. Inter-VLAN Communication

After configuring router in JHB and CPT, PCs in different VLANs successfully pinged each other.

Subinterfaces were created on JHB_R1 and CPT_R1:

interface fa0/0.10
encapsulation dot1Q 10
ip address 192.168.1.1 255.255.255.0

(Repeated for VLANs 20, 30, 100, 200)

Connectivity was verified using ping:

So, in the figure below it shows PC in VLAN 10 pinging PC in VLAN 20 and confirms it with a SUCCESS. I also pinged from a PC in CPT VLAN 100 to VLAN 200.

Figure 10: VLAN10 PC pinging VLAN20 PC.

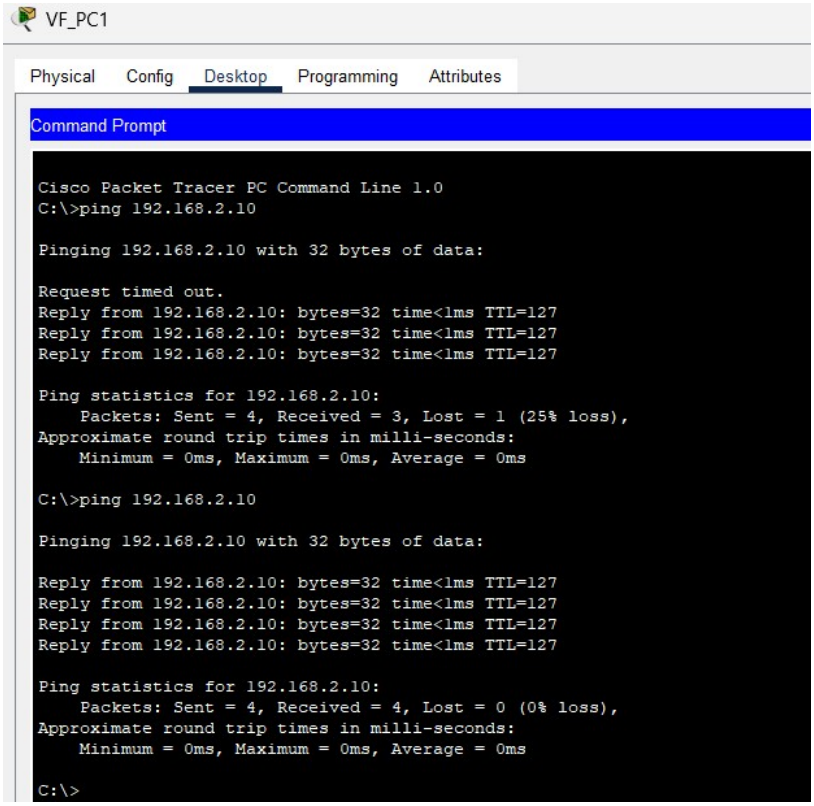
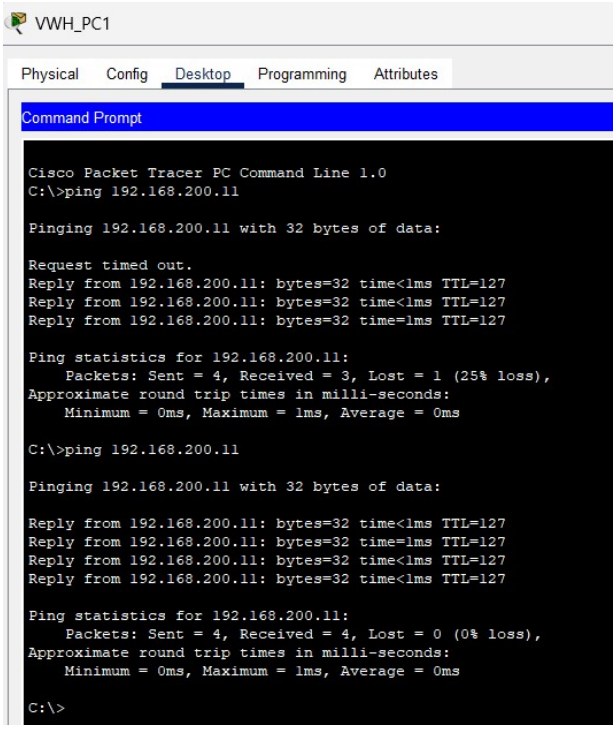


Figure 11: VLAN100 PC pinging VLAN200 PC.



2.3. VLAN Configuration & Port Assignments

VLANs 10, 20, and 30 were configured in Johannesburg, and VLANs 100 and 200 in Cape Town. Ports were assigned as per specification, and trunking was enabled on the Gigabit interfaces. Then the DHCP assignment and communication across VLANs were validated.

Johannesburg Switches

- Ports 0–8 (VLAN 10)
- Ports 9–16 (VLAN 20)
- Ports 17–24 (VLAN 30)
- Gig ports (Trunk)

Cape Town Switches

- Ports 1–12 (VLAN 100)
- Ports 13–24 (VLAN 200)
- Gig ports (Trunk)

Figure 12: VLAN config confirmation on JHB switch0.

```
Switch>enable
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Gig0/1
                                                Gig0/2
10   Finance                          active    Fa0/1
20   Sales                            active    Fa0/2
30   HR                               active    Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Figure 13: VLAN config confirmation on CPT switch3.

```
Switch>enable
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig0/1, Gig0/2
100  Warehouse                        active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12
200  Factory                          active    Fa0/3, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

2.4. Web Server HTTP Configuration

The Internet-based Web Server (200.20.20.10) was configured to accept HTTP requests. Internal LAN devices accessed the webpage successfully, confirming firewall and routing compliance.

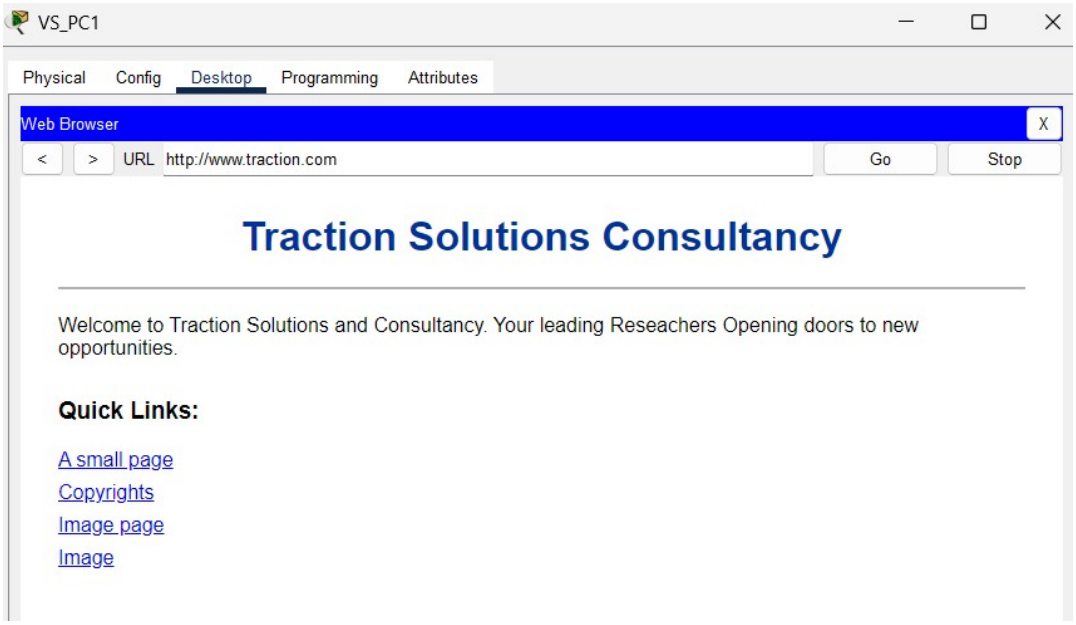
The web server was configured with:

- **Static IP:** 200.20.20.10
- **DNS enabled**
- **Web page created under HTML service**
- **Correct DNS A record: *www.traction.com*** → 200.20.20.10

Clients accessed the webpage successfully using:

http://www.traction.com

Figure 14: Webpage displaying of VS_PC1 in JHB network.



2.5. Wireless LAN Controller Setup

For me to centrally manage all wireless access points across the organization, a Cisco 2500 Series Wireless LAN Controller (WLC) was deployed in the Durban branch. I did this by first assigning the WLC a static management IP address as required by the scenario.

I used the following details were configured under the WLC's Management Interface:

- IP Address: 192.168.20.3
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.20.1

After assigning the management settings on the WLC, I used a PC from the internal network to access the WLC GUI via a web browser. Initially, HTTP was used to access:

http://192.168.20.3

This successfully loaded the Cisco 2500 Series Wireless LAN Controller setup page. During first-time setup, an admin account was created using:

- **Username:** EDUV4981741 (my student No.)
- **Password:** cisco@123

After completing the initial setup, the WLC enabled secure HTTPS access automatically. Attempting to reconnect using HTTP resulted in a “server reset connection” error due to the enforced encryption. Then I used the correct secure URL which was:

https://192.168.20.3

This gave me access to the WLC Login Portal, where the newly created administrator credentials were used to authenticate. I logged into the controller, and created two WLANs:

1. **STAFF-WIFI** – for employees
2. **GUEST-WIFI** – for visitors

These SSIDs were broadcast across the lightweight access point (LAP) deployed in the Durban network. A wireless laptop was successfully connected to **STAFF-WIFI**, and a smartphone connected to **GUEST-WIFI**, confirming proper SSID broadcasting and AP adoption by the WLC.

Figure 15: WLC creating admin webpage

Figure 16: Cisco WLC login success

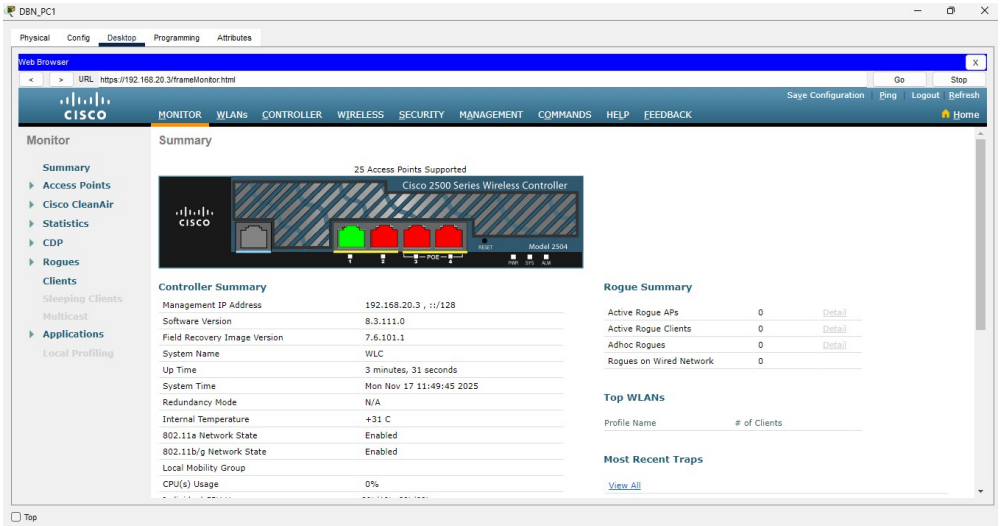
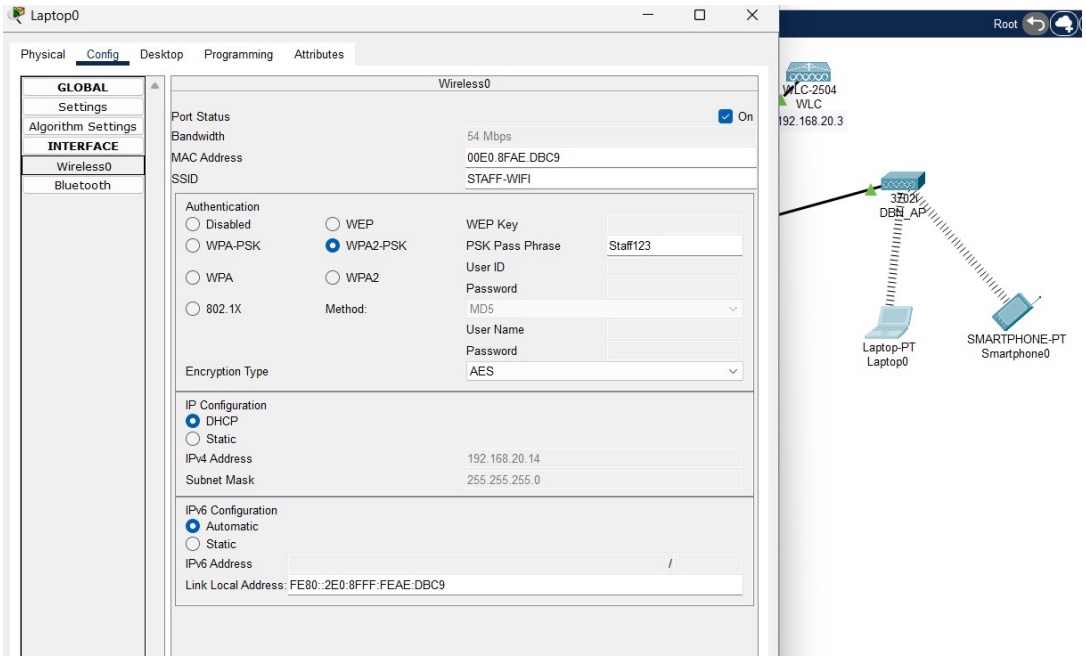


Figure 17: Laptop0 successfully connected to the STAFF-WIFI from the AP.



2.6. Wireless Security Configuration

The STAFF-WIFI SSID was configured using **WPA2 security**. The security settings were implemented as follows:

- On the WLC:
  - **Layer 2 Security:** WPA + WPA2
- On the Access Point:
  - Where it says WLC I just put the IP address of the WLC and it connects.

GUEST-WIFI
The guest network was intentionally configured as an open network to allow easy visitor access:

- **Layer 2 Security:** None (Open Network)

Both wireless networks were fully tested using end-devices:

- A laptop successfully authenticated and connected to **STAFF-WIFI**.
- A smartphone connected to **GUEST-WIFI**.

Figure 18: WLC WLANs page

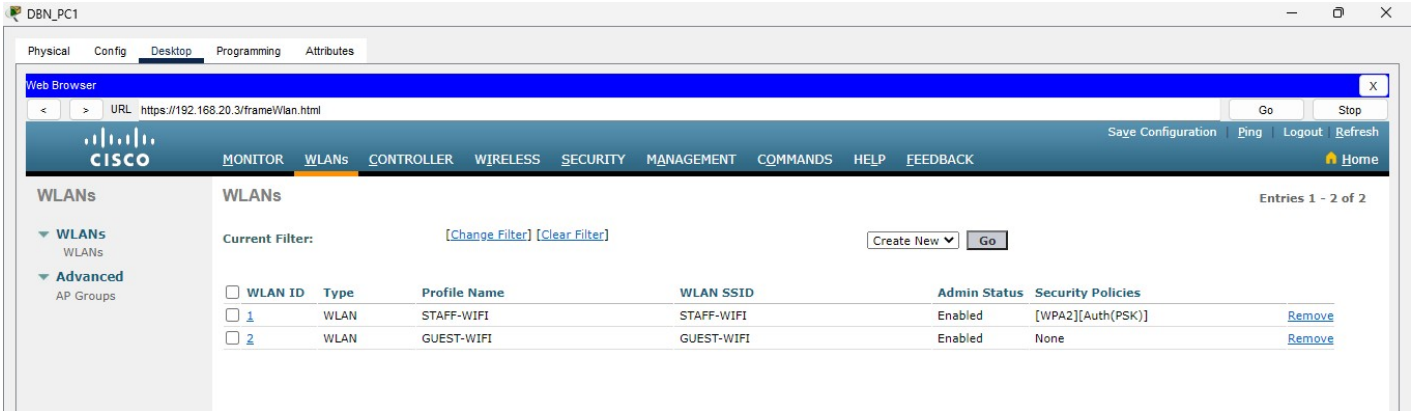


Figure 19: DBN AP located on the WLC page

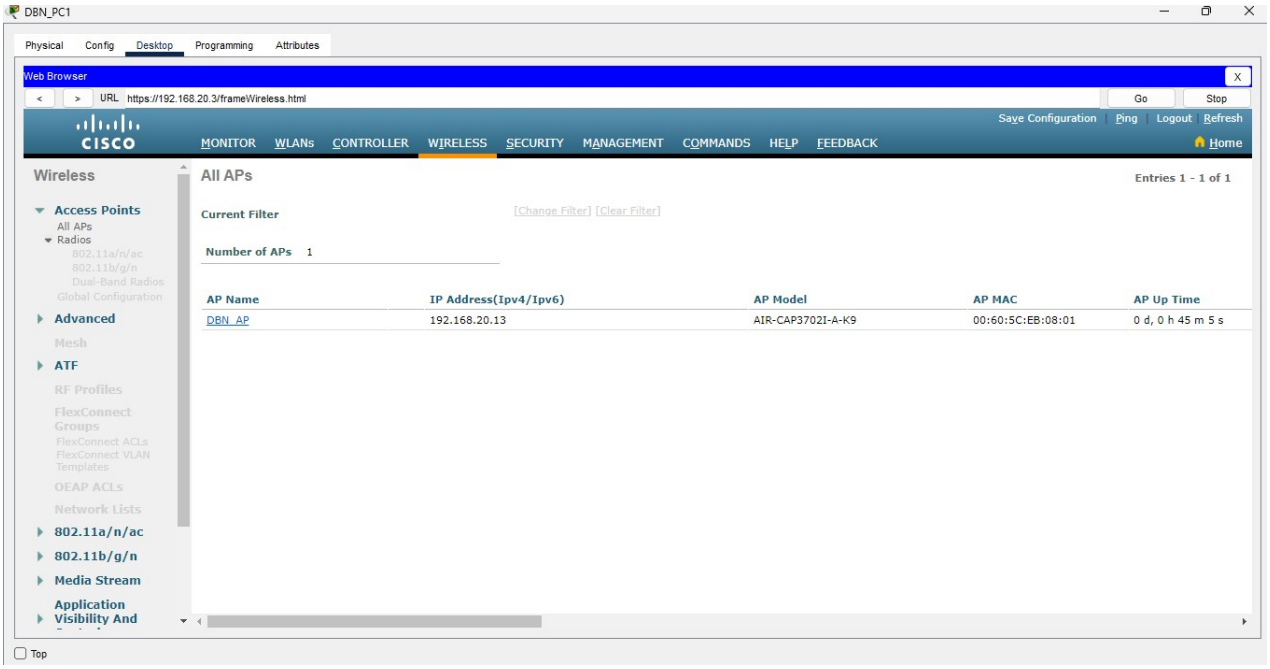


Figure 20: Security configurations for STAFF-WIFI

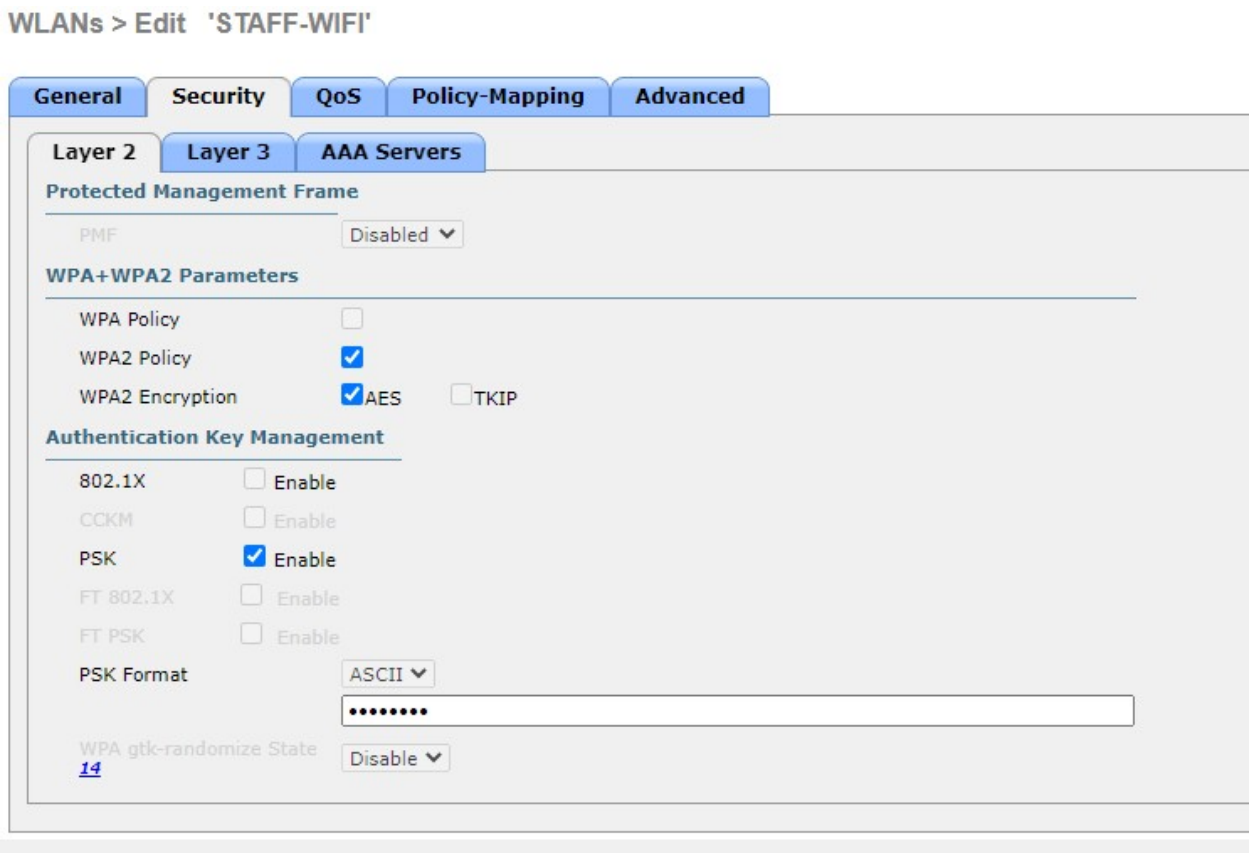


Figure 21: Security configurations for GUEST-WIFI

5. Question 3 – Network Traffic Prioritization and QoS Implementation

3.1. Proposed Solution: Implement Quality of Service (QoS)

To address network congestion, VoIP delays, jitters, and video conferencing issues experienced by Traction Solutions, I propose implementing Quality of Service (QoS) across the entire network.
QoS is a set of techniques used to queue, and prioritize traffic, ensuring that time-sensitive apps like VoIP and Video Conferencing are given priority over general data traffic.

QoS provides the following benefits:

- Priority of real-time traffic
- Reduces delays
- Efficient bandwidth use
- High performance for critical apps (cisco, 2001).

3.2. Diagrams: How QoS Improves Traffic Management

Below are three explanatory diagrams showing how QoS works in the Traction Solutions network.

Diagram 1: Network Traffic Before QoS

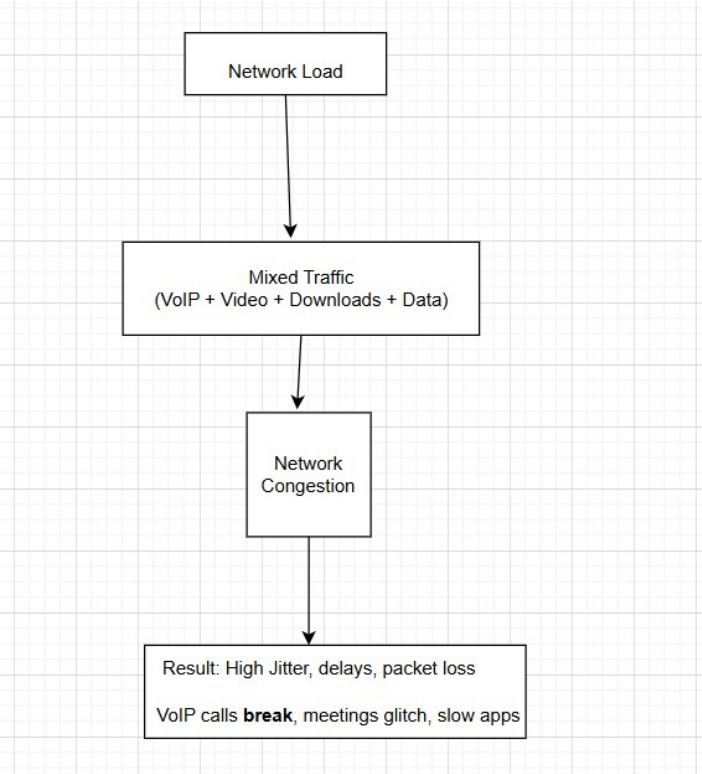
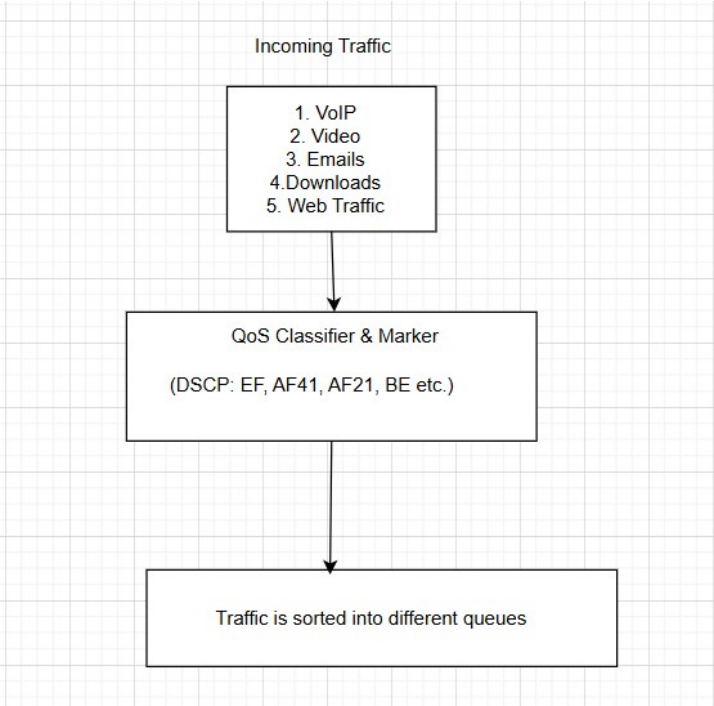


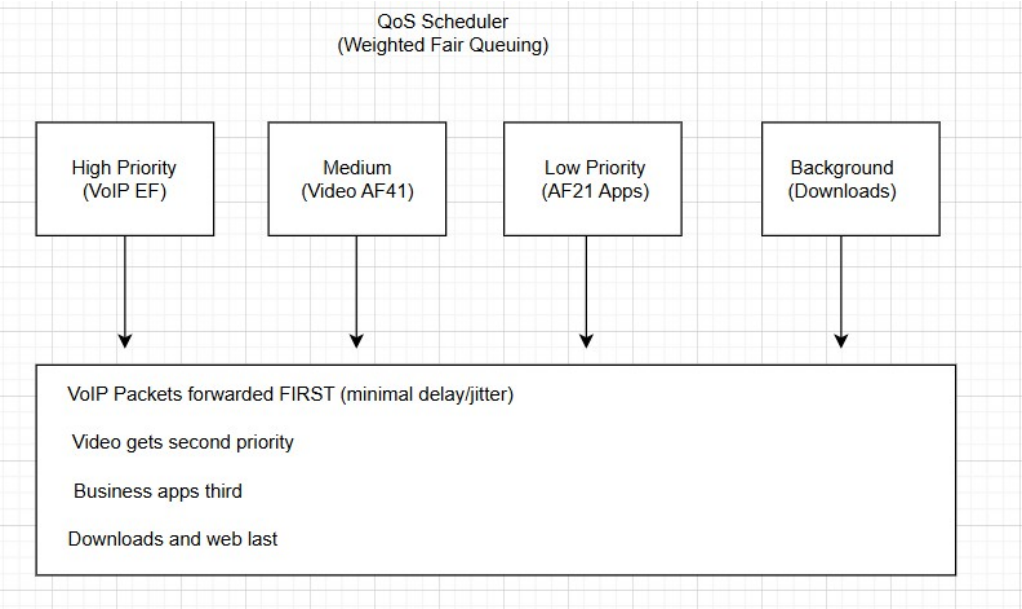
Diagram 2: Traffic Classification and Marking (QoS Enabled)



Example DSCP markings:

- **EF (Expedited Forwarding) –** VoIP
- **AF41 –** Video Conferencing
- **AF21 –** Business-critical traffic
- **Best Effort –** Downloads

Diagram 3: Prioritized Queuing on the Router/Switch



CLI Commands for Routers:

These commands are for example purposes; I have not configured them in my network design I created in Question 1. But I did test these commands and they work. The goal for these commands below is for voice to get priority, and video gets bandwidth share whilst bulk gets remaining.

Create ACLs:

```
ip access-list extended VOICE_ACL
 permit udp any any range 16384 32767 (RTP ports example)
 permit udp any any eq 5060 (SIP example)

ip access-list extended VIDEO_ACL
 permit udp any any range 30000 30100 (video RTP example)
```

Class-map & policy-map:

```
class-map match-any VOICE
 match access-group name VOICE_ACL

class-map match-any VIDEO
```

```
 match access-group name VIDEO_ACL

class-map match-any BULK
 match protocol ftp
 match protocol http (if you want specific)

policy-map WAN-OUT
 class VOICE
  priority 1500
 class VIDEO
  bandwidth percent 30
 class BULK
  bandwidth percent 20
 class class-default
  fair-queue
```

WAN link:

```
interface Serial6/0
 ip address 50.0.0.1 255.0.0.0
 service-policy output WAN-OUT
```

The priority command reserves strict priority queue with policing (use a large value enough for concurrent calls — e.g., 64K × expected simultaneous calls).

CLI Commands for Switches:

```
interface FastEthernet0/5
 switchport mode access
 switchport access vlan 10
 switchport voice vlan 20
 mls qos trust dscp
 spanning-tree portfast
```

How This Solves the Problem?

Under QoS:

- VoIP and Video Conferencing receive a **confirmed minimum bandwidth**
- Downloads are **rate-limited**
- Critical services no longer compete with non-essential traffic

- Network congestion is managed through **priority-based forwarding**

QoS ensures **consistent communication quality** and prevents performance degradation even at peak usage.

6. CONCLUSION

This project successfully demonstrated the complete design and deployment of a scalable and secure enterprise network for Gijima Trading. The network meets all organizational requirements, integrates all four branch locations, supports secure wireless, RIP v2 routing, centralized DHCP & DNS, and provides internet access through an ISP cluster. The final topology is fully operational, efficient, and aligned with industry's best practices.

7. References

Babiarz, J., Chan, K., & Baker, F. (2006, August). *Configuration Guidelines for DiffServ Service Classes.* Retrieved from RFC Informational: https://datatracker.ietf.org/doc/html/rfc4594

cisco. (2001). Quality of Service for Voice over IP. *cisco*. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html

cisco. (2022). Quality of Service Configuration Guide, Cisco IOS XE 17.x. *cisco*. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/qos/b-quality-of-service/m_qos-mrkg.html

cisco. (2025). Class-Based Weighted Fair Queueing. *cisco*. Retrieved from https://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/cbwfq.html

cisco. (2025). Compare Traffic Policy and Traffic Shape to Limit Bandwidth. *cisco*. Retrieved from https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

Juniper. (2025). Juniper Mist Wired Assurance Configuration Guide. *Juniper*. Retrieved from https://www.juniper.net/documentation/us/en/software/mist/mist-wired/topics/concept/wired-config-overview.html

Lammle, T. (2020). *CCNA Certification Study Guide* (Vol. 2).

Molenaar, R. (2013). CBWFQ not supported on Sub-Interfaces. *NetworkLessons*. Retrieved from https://networklessons.com/quality-of-service/apply-cbwfq-to-sub-interface

Molenaar, R. (2013). QoS LLQ (Low Latency Queueing) on Cisco IOS. *NetworkLessons*. Retrieved from https://networklessons.com/quality-of-service/qos-llq-low-latency-queueing-cisco-ios

packettracernetwork. (2024). Packet Tracer 8.2 - WLC configuration. *packettracernetwork*. Retrieved from https://www.packettracernetwork.com/tutorials/pt71-wlc-configuration.html