رواد مصر الرقمية

وزارة الاتصـــالات
وتكنولوجيا المعلومات

Advanced Full Network Design and Deployment for a 2 Branch Bank

Prepared by:

NetNinjas

(ONL1_ISS2_S1e)

- شريف ثابت احمد يعقوب
- محمود السيد عبد الحميد شريف
- شادي عادل طرخان
- حسين محسن عبد الرحمن
- اية خالد محمد

Supervised by :

Eng . Amr Reda

FINAL PROJECT LLD

Table of Contents

1. Introduction

1.1 Document Control

Document Information

Document Title : Advanced Full Network Design and Deployment for a 2 Branch Bank
Document Owner : NET NINJAS TEAM

1.2 Document Purpose

The purpose of this document is to provide a comprehensive overview of the network architecture, hardware and software requirements, and security protocols for a two-branch network project. Each branch consists of three floors, and this document serves as a guide for the successful implementation of a scalable, secure, and reliable network infrastructure. It ensures that all stakeholders understand the project scope, technical specifications, and key objectives necessary for effective communication and data management across both branches

2. Technical Solution Overview

2.1 Details of the solution

2.1.1 Overview & Purpose of the project

The project aims to implement wired infrastructure with the latest technology elements.

2.2 Solution Components

I. Network Solution:

a. Core switches

4 x Cisco Catalyst WS-C3650-24PS-S

b. Servers Aggregator Switches:

2 x Catalyst 2960-24TT-L for UTP Servers Connectivity

c. OOB & Interconnection Switches:

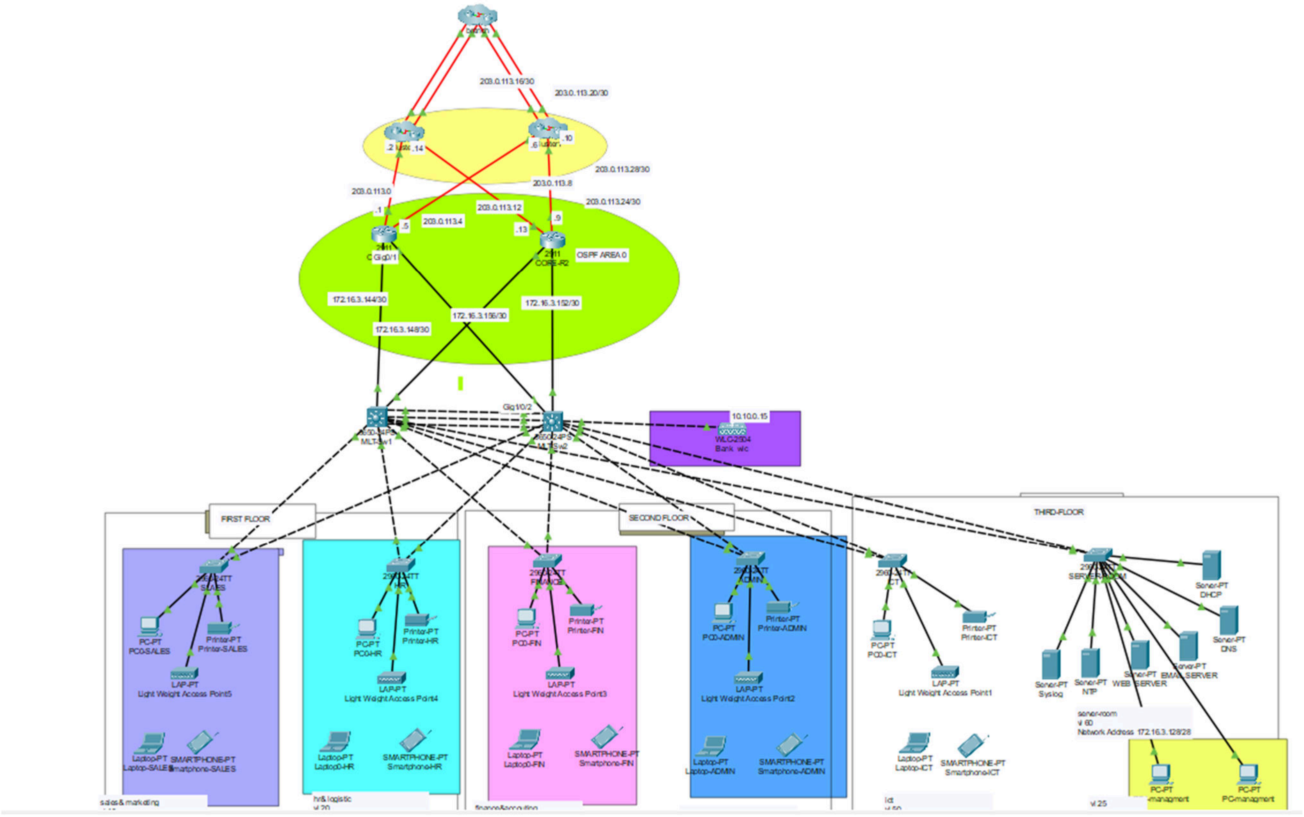
10 x Catalyst 2960-24TT-L for OOB Management & FW Interconnection

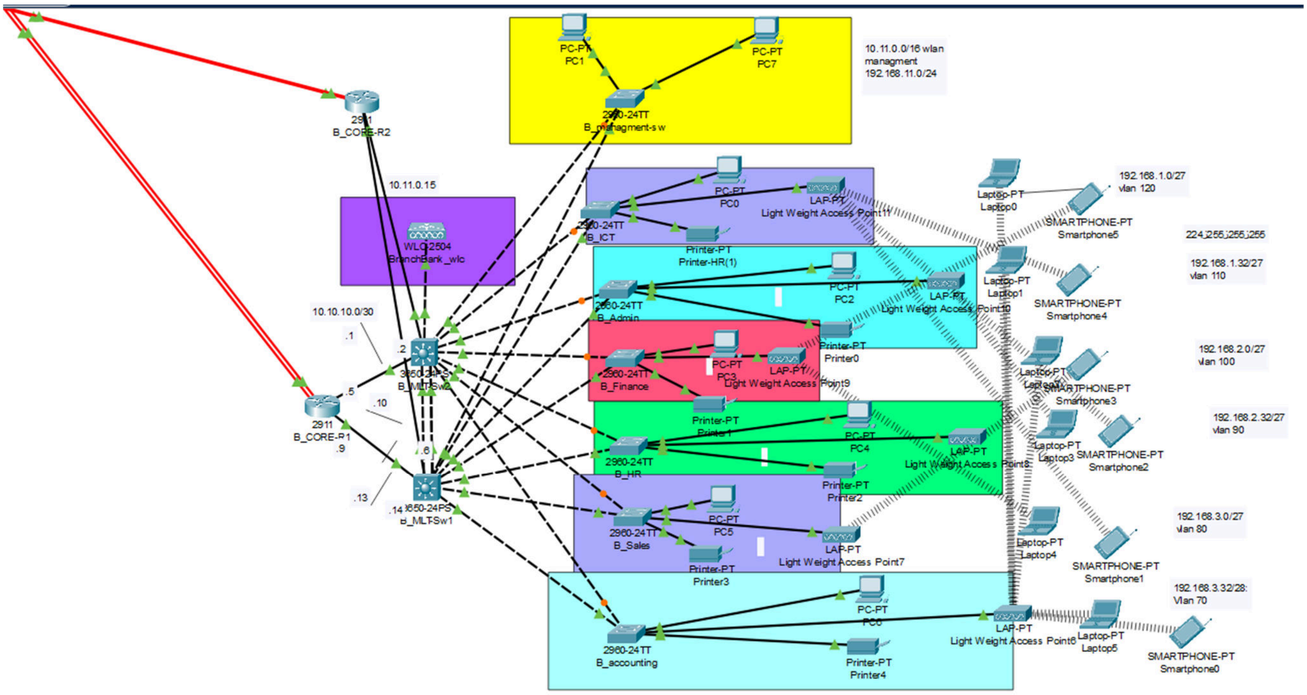
d. Routers:

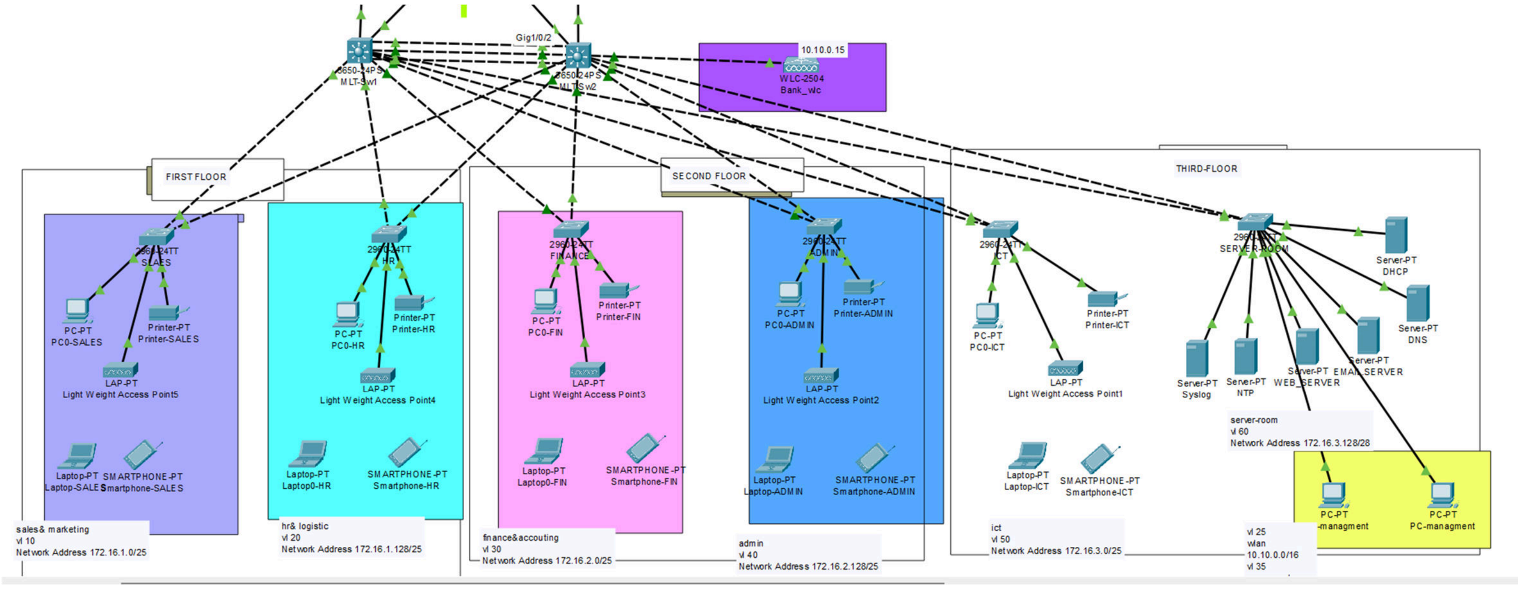
4 x CISCO2911/K9 2911 Router

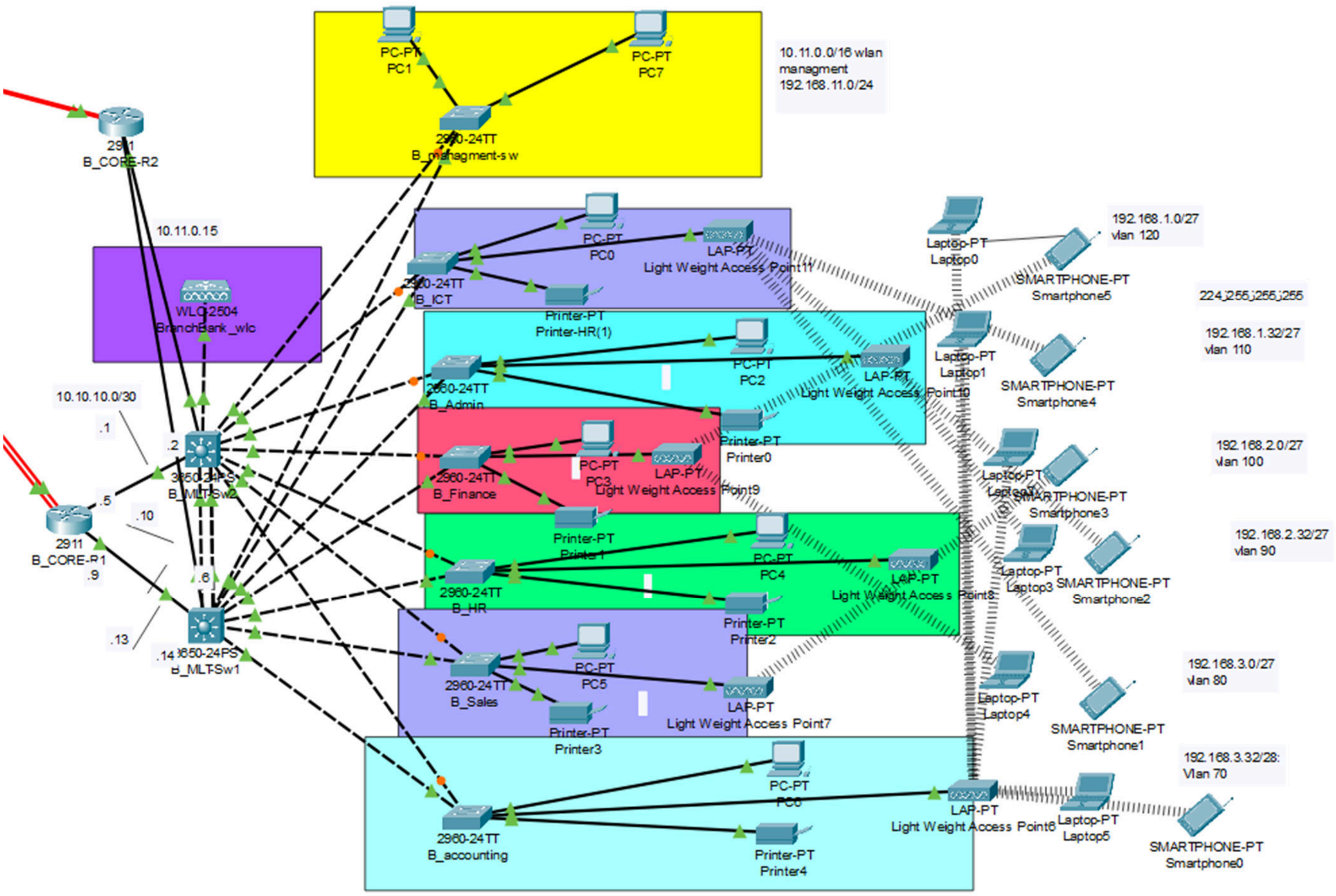
3. Network Architecture

3.1 Physical Topology






Gig1/0/2
3650-24PS
MLT-Sw1
3650-24PS
MLT-Sw2
10.10.0.15
WLC-2504
Bank_wlc
FIRST FLOOR
SECOND FLOOR
THIRD-FLOOR
2960-24TT
SALES
PC-PT
PC0-SALES
Printer-PT
Printer-SALES
LAP-PT
Light Weight Access Point5
Laptop-PT
Laptop-SALE
SMARTPHONE-PT
Smartphone-SALES
sales& marketing
vl 10
Network Address 172.16.1.0/25
2960-24TT
HR
PC-PT
PC0-HR
Printer-PT
Printer-HR
LAP-PT
Light Weight Access Point4
Laptop-PT
Laptop0-HR
SMARTPHONE-PT
Smartphone-HR
hr& logistic
vl 20
Network Address 172.16.1.128/25
2960-24TT
FINANCE
PC-PT
PC0-FIN
Printer-PT
Printer-FIN
LAP-PT
Light Weight Access Point3
Laptop-PT
Laptop0-FIN
SMARTPHONE-PT
Smartphone-FIN
finance&accouting
vl 30
Network Address 172.16.2.0/25
2960-24TT
ADMIN
PC-PT
PC0-ADMIN
Printer-PT
Printer-ADMIN
LAP-PT
Light Weight Access Point2
Laptop-PT
Laptop-ADMIN
SMARTPHONE-PT
Smartphone-ADMIN
admin
vl 40
Network Address 172.16.2.128/25
2960-24TT
ICT
PC-PT
PC0-ICT
Printer-PT
Printer-ICT
LAP-PT
Light Weight Access Point1
Laptop-PT
Laptop-ICT
SMARTPHONE-PT
Smartphone-ICT
ict
vl 50
Network Address 172.16.3.0/25
2960-24TT
SERVER-ROOM
Server-PT
DHCP
Server-PT
DNS
Server-PT
Syslog
Server-PT
NTP
Server-PT
WEB_SERVER
Server-PT
EMAIL SERVER
server-room
vl 60
Network Address 172.16.3.128/28
PC-PT
-managment
PC-PT
PC-managment
vl 25
wlan
10.10.0.0/16
vl 35


PC-PT
PC1
PC-PT
PC7
2960-24TT
B_managment-sw
10.11.0.0/16 wlan
managment
192.168.11.0/24
2911
B_CORE-R2
10.11.0.15
WLC-2504
BranchBank_wlc
10.10.10.0/30
.1
.2
.5
.10
.6
.9
.13
.14
2911
B_CORE-R1
3650-24PS
B_MLT-Sw2
3650-24PS
B_MLT-Sw1
2960-24TT
B_ICT
PC-PT
PC0
LAP-PT
Light Weight Access Point11
Printer-PT
Printer-HR(1)
2960-24TT
B_Admin
PC-PT
PC2
LAP-PT
Light Weight Access Point10
Printer-PT
Printer0
2960-24TT
B_Finance
PC-PT
PC3
LAP-PT
Light Weight Access Point9
Printer-PT
Printer1
2960-24TT
B_HR
PC-PT
PC4
LAP-PT
Light Weight Access Point8
Printer-PT
Printer2
2960-24TT
B_Sales
PC-PT
PC5
LAP-PT
Light Weight Access Point7
Printer-PT
Printer3
2960-24TT
B_accounting
PC-PT
PC6
Printer-PT
Printer4
LAP-PT
Light Weight Access Point6
Laptop-PT
Laptop0
SMARTPHONE-PT
Smartphone5
192.168.1.0/27
vlan 120
224,255,255,255
Laptop-PT
Laptop1
SMARTPHONE-PT
Smartphone4
192.168.1.32/27
vlan 110
Laptop-PT
Laptop2
SMARTPHONE-PT
Smartphone3
192.168.2.0/27
vlan 100
Laptop-PT
Laptop3
SMARTPHONE-PT
Smartphone2
192.168.2.32/27
vlan 90
Laptop-PT
Laptop4
SMARTPHONE-PT
Smartphone1
192.168.3.0/27
vlan 80
Laptop-PT
Laptop5
SMARTPHONE-PT
Smartphone0
192.168.3.32/28:
Vlan 70

4. Naming Convention and IP scheme

4.1 Naming Convention

We will use a standard naming convention to name all network infrastructure equipment. This facilitates device identification and management during the day-to-day administration activities as well as problem troubleshooting.

According to network Infrastructure naming convention, we are going to use the following naming schema for our network devices:

Hostname	IP address	Subnet Mask	Purpose/Description
		HQ	
MLT-Sw2	172.16.3.153	255.255.255.252	Link to router (WAN interface)
MLT-Sw2	172.16.3.157	255.255.255.252	Link to another router (WAN interface)
MLT-Sw1	172.16.3.145	255.255.255.252	Link to router (WAN interface
MLT-Sw1	172.16.3.149	255.255.255.252	Link to another router (WAN interface
CORE-R1	172.16.3.146	255.255.255.252	Main router for internal network communication
CORE-R2	172.16.3.154	255.255.255.252	Main router for internal network communication
Bank_Wlc	10.10.0.15	255.0.0.0	Wireless controller
		Servers	
Server-PT DHCP	172.16.3.132	255.255.255.240	Assigns IP addresses to devices on a network automatically.
Server-PT DNS	172.16.3.131	255.255.255.240	Translates domain names to IP addresses for accessing websites and services.
Server-PT EMAil	172.16.3.130	255.255.255.240	Manages and stores emails for users
Server-PT WEB	172.16.3.129	255.255.255.240	Hosts websites and serves web pages to users
Server-PT NTP	172.16.3.133	255.255.255.240	Synchronize clocks across network devices to a single time source
Server-PT Syslog	172.16.3.134	255.255.255.240	Collects and stores log data from various devices for monitoring aand analysis

Branch 2

B_MLT-Sw1	10.10.10.6	255.255.255.252	IP interface
B_MLT-Sw1	10.10.10.14	255.255.255.252	IP interface
B_MLT-Sw2	10.10.10.2	255.255.255.252	Layer 3 Switch - Routing between VLANs
B_MLT-Sw2	10.10.10.10	255.255.255.252	Router connection for network routing
B_CORE-R1	10.10.10.13	255.255.255.252	Internal interface for NAT (inside)
B_CORE-R1	10.10.10.9	255.255.255.252	Internal interface for NAT (inside)
B_CORE-R1	203.0.113.29	255.255.255.252	External interface for public access (NAT outside)
B_CORE-R1	203.0.113.25	255.255.255.252	External interface for public access
B_CORE-R1	172.16.3.133	N/A	NTP synchronization
B_CORE-R1	172.16.3.134	N/A	Remote logging server
B_CORE-R2	10.10.10.1	255.255.255.252	Internal interface for NAT
B_CORE-R2	10.10.10.5	255.255.255.252	Internal interface for NAT (inside)
B_CORE-R2	203.0.113.21	255.255.255.252	External interface for public access (NAT outside)
B_CORE-R2	203.0.113.17	255.255.255.252	External interface for public access
B_CORE-R2	172.16.3.133	N/A	NTP synchronization
B_CORE-R2	172.16.3.134	N/A	Remote logging server
BranchBank_wlc	10.11.0.15	255.255.0.0	Wireless LAN controller

4.2 IP Addressing Scheme

The following is the IP schema that will be implemented at building Infrastructure:

VLAN Number	VLAN Name	Subnet	Default gateway
HQ			
10	Sales	172.16.1.0/25	172.16.1.50
20	HR	172.16.1.128/25	172.16.1.140
25	wlan	10.10.0.0/16	10.10.0.1
30	Finance	172.16.2.0/25	172.16.2.50
35	management	192.168.10.0/24	192.168.10.1
40	admin	172.16.2.128/25	172.16.2.140
50	ict	172.16.3.0/25	172.16.3.50
60	server-room	172.16.3.128/28	172.16.3.140
Branch 2			
25	WLAN	10.11.0.0/16	10.11.0.1
35	Management	192.168.11.0/24	192.168.11.1
70	accounting	192.168.3.32/27	192.168.3.33
80	sales	192.168.3.0/27	192.168.3.1
90	HR	192.168.2.32/27	192.168.2.33
100	finance	192.168.2.0/27	192.168.2.1
110	admin	192.168.1.32/27	192.168.1.33
120	ict	192.168.1.0/27	192.168.1.1

Table 1 - IP VLAN Scheme

5. Port Mapping

Device	Port	Peer Device
	HQ Core SW	
MLT-Sw2	Gig 1/0/1	Router B -core R2
MLT-Sw2	Gig 1/0/2	Router B -core R1
MLT-Sw2	Gig 1/0/3	SW-Sales
MLT-Sw2	Gig 1/0/4	SW- HR
MLT-Sw2	Gig 1/0/5	SW-Finance
MLT-Sw2	Gig 1/0/6	SW-Admin
MLT-Sw2	Gig 1/0/7	SW-ICT
MLT-Sw2	Gig 1/0/8	SERVER-Room
MLT-Sw2	Gig 1/0/9	Bank_WLC
MLT-Sw2	Gig 1/0/10	MLT-Sw **1**
MLT-Sw 1	Gig 1/0/1	Router B -core R1
MLT-Sw 1	Gig 1/0/2	Router B -core R2
MLT-Sw 1	Gig 1/0/3	SW-Sales
MLT-Sw 1	Gig 1/0/4	SW- HR
MLT-Sw 1	Gig 1/0/5	SW-Finance
MLT-Sw 1	Gig 1/0/6	SW-Admin
MLT-Sw 1	Gig 1/0/7	SW-ICT
MLT-Sw 1	Gig 1/0/8	SERVER-Room
MLT-Sw 1	Gig 1/0/10	MLT-Sw2
	Branch 2 Core SW	
B_MLT-SW1	Gig 1/0/1	B_ICT
B_MLT-SW1	Gig 1/0/2	B_Admin
B_MLT-SW1	Gig 1/0/3	B_Finance
B_MLT-SW1	Gig 1/0/4	B_HR
B_MLT-SW1	Gig 1/0/5	B_Sales
B_MLT-SW1	Gig 1/0/6	B_accounting
B_MLT-SW1	Gig 1/0/7	B_CORE-R2
B_MLT-SW1	Gig 1/0/8	B_CORE-R1
B_MLT-SW1	Gig 1/0/9	B_managment
B_MLT-SW1	Gig 1/0/11	**B_MLT-SW2**
B_MLT-SW2	Gig 1/0/1	B_ICT
B_MLT-SW2	Gig 1/0/2	B_Admin
B_MLT-SW2	Gig 1/0/3	B_Finance
B_MLT-SW2	Gig 1/0/4	B_HR

B_MLT-SW2	Gig 1/0/5	B_Sales
B_MLT-SW2	Gig 1/0/6	B_accounting
B_MLT-SW2	Gig 1/0/7	B_CORE-R2
B_MLT-SW2	Gig 1/0/8	B_CORE-R1
B_MLT-SW2	Gig 1/0/9	BranchBank_wlc
B_MLT-SW2	Gig 1/0/10	B_managment

6. Network Design Notes & Configurations

6.1 Layer 2 technologies

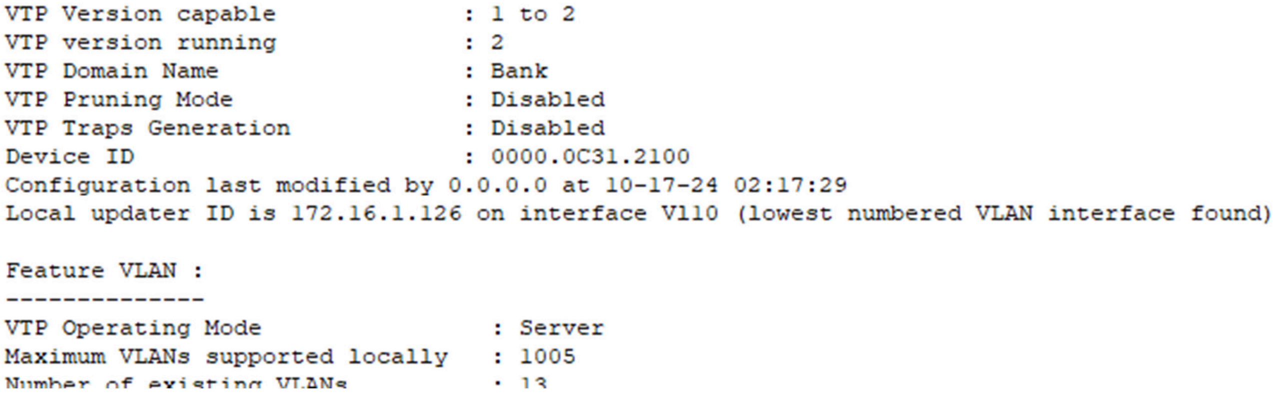
- Spanning Tree is configured in order to protect against physical and logical misconfigurations and a possibility to erroneously create L2 loops. Spanning tree is used in RPVST+ mode.
- Spanning tree root is configured to be on the core with priority 0 for all Vlans.
- Dot1q will be the protocol used for trunking for all uplinks.
- VLANs carried over the trunking link between the core and the switches.

- Hosts & Server ports on edges are configured as spanning tree port fast to exclude them from the spanning tree protocol decreasing the time these ports take to be up. Unless it is configured as trunk and these ports are explicitly configured as trunk.
- All switches must be managed in a secure a manner by using SSH, authentication mechanism and set privilege levels for different users if needed.
- SNMP V2 is used to manage the switches using different read and read/write community strings.
- BPDU filter will be applied globally on all switches to protect the network from miss connection of switches to the network, which could lead to network loops.

6.1.1 VTP and Vlan Configuration

VTP is a Layer 2 messaging protocol that allows managing, the addition, deletion, and renaming of VLANs on a network-wide basis. In the current setup it is recommended that all Catalysts are in VTP transparent mode. In other words we don’t want those switches to listen to VTP updates and share VLAN database between them. Such approach requires more configuration work, because all VLANs should be configured on every switch. This will avoid simple but critical VLAN configuration mistakes being propagated via VTP.

6.1.1.1 VTP Configuration



```
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : Bank
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0000.0C31.2100
Configuration last modified by 0.0.0.0 at 10-17-24 02:17:29
Local updater ID is 172.16.1.126 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 13
```

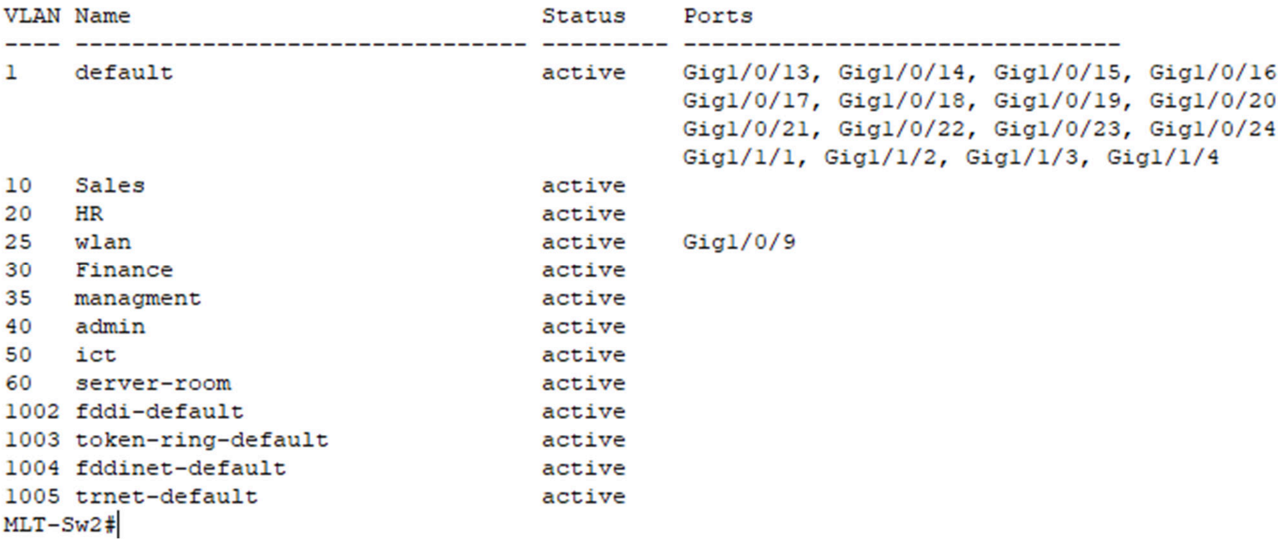
VTP Configuration

- VTP mode will be configured as transparent on all switches to avoid network outages due to miss-configured switches being added to the network or user miss-configuration that could be propagated to the entire network.

6.1.1.2 Vlan Configuration

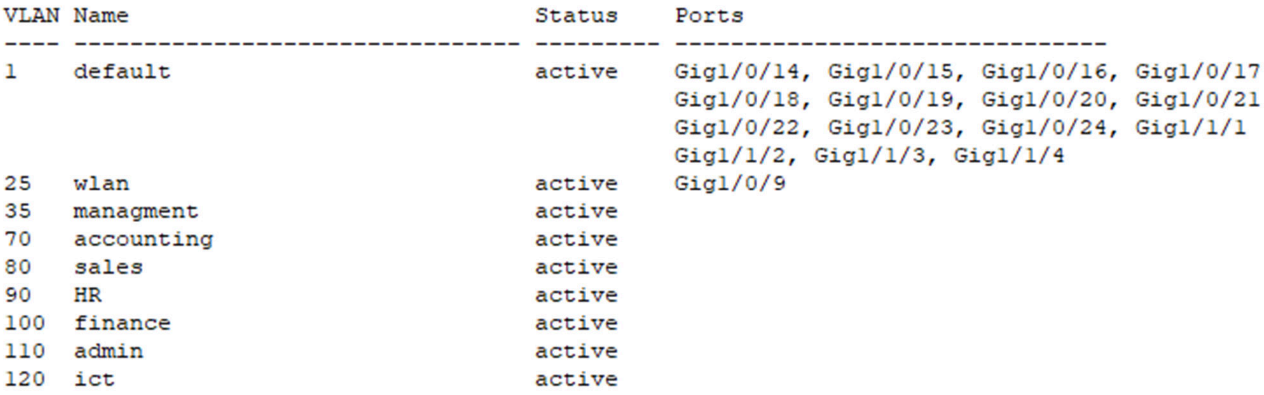
- VLANs will be statically assigned to DC Switches.
- The Vlans would be created as per table 1.

BRANCH 1



```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/13, Gig1/0/14, Gig1/0/15, Gig1/0/16
                                                Gig1/0/17, Gig1/0/18, Gig1/0/19, Gig1/0/20
                                                Gig1/0/21, Gig1/0/22, Gig1/0/23, Gig1/0/24
                                                Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
10   Sales                            active
20   HR                               active
25   wlan                             active    Gig1/0/9
30   Finance                          active
35   managment                        active
40   admin                            active
50   ict                              active
60   server-room                      active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
MLT-Sw2#
```

BRANCH 2



```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17
                                                Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21
                                                Gig1/0/22, Gig1/0/23, Gig1/0/24, Gig1/1/1
                                                Gig1/1/2, Gig1/1/3, Gig1/1/4
25   wlan                             active    Gig1/0/9
35   managment                        active
70   accounting                       active
80   sales                            active
90   HR                               active
100  finance                          active
110  admin                            active
120  ict                              active
```

6.1.2 Spanning-tree

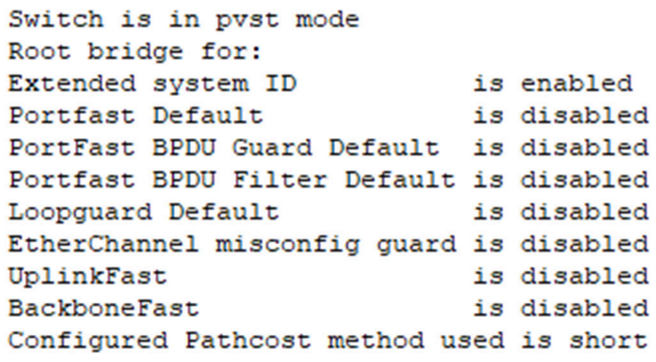
STP is a Layer 2 link-management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The STP algorithm calculates the best loop-free path throughout a switched Layer 2 network. Layer 2 LAN ports send and receive STP frames at regular intervals. Network devices do not forward these frames, but use the frames to construct a loop-free path.

6.1.2.1 Spanning-tree Configuration

Spanning Tree is configured in order to protect against physical and logical misconfigurations and a possibility to erroneously create L2 loops. Spanning tree is used in RPVST+ mode.

We recommend to not enable Bpdu filter to avoid any loop.



```
Switch is in pvst mode
Root bridge for:
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
```

The following Spanning-tree features are enabled:

- In order to protect Spanning Tree from any misconfigurations STP PortFast BPDU guard is used. The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs from PortFast enabled port, the BPDU guard operation disables the port. The BPDU guard transitions the port into errdisable state
- Uplinkfast is enabled on the switches for fast convergence from indirect link failures.
- Spanning tree root is configured to be on the core switch with priority 0 for all Vlan

6.1.3 Err-disable recovery

If the configuration shows a port to be enabled, but software on the switch detects an error situation on the port, the software shuts down that port. In other words, the port is automatically disabled by the switch operating system software because of an error condition that is encountered on the port.

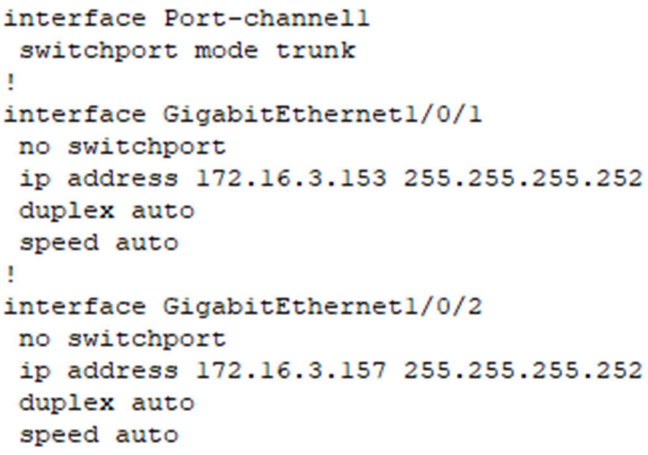
When a port is error disabled, it is effectively shut down and no traffic is sent or received on that port. The port LED is set to the color orange.

In network err-disable recovery will be disabled.

```
errdisable recovery cause
```

6.1.4 L2 Port configuration

6.1.4.1 Access Port Configuration



```
interface Port-channel1
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 172.16.3.153 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/2
 no switchport
 ip address 172.16.3.157 255.255.255.252
 duplex auto
 speed auto
```

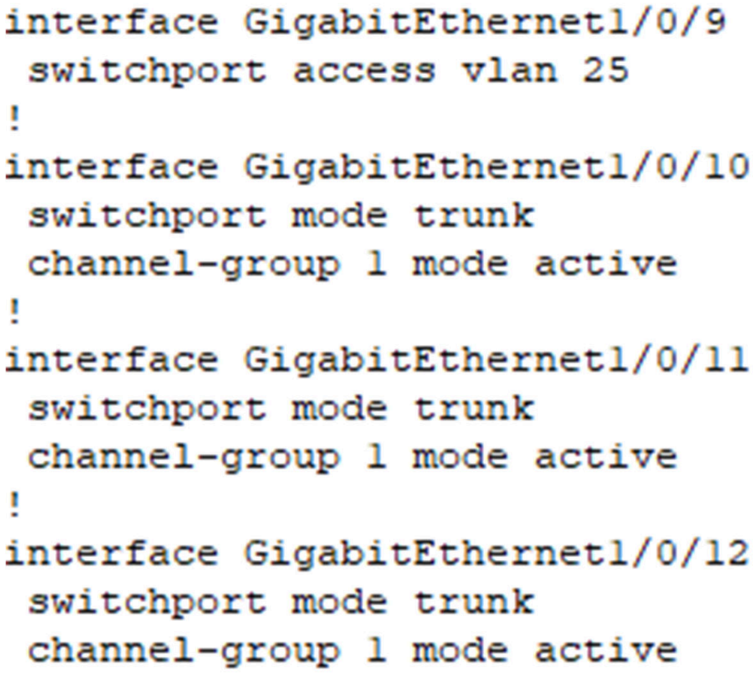
Access Port Configuration

- Portfast feature is enabled on all user and server ports to allow stable and fast L2 and spanning-tree convergence.
- Ports that are connected to the hosts are put in switchport access mode and are assigned to their corresponding Vlan using switchport commands.

6.1.4.2 Trunk port configuration

All uplink 10 gig Ethernet ports of the edge switches and the corresponding ports on the core are configured as dot1Q trunks.

All port channels are recommended to be LACP.



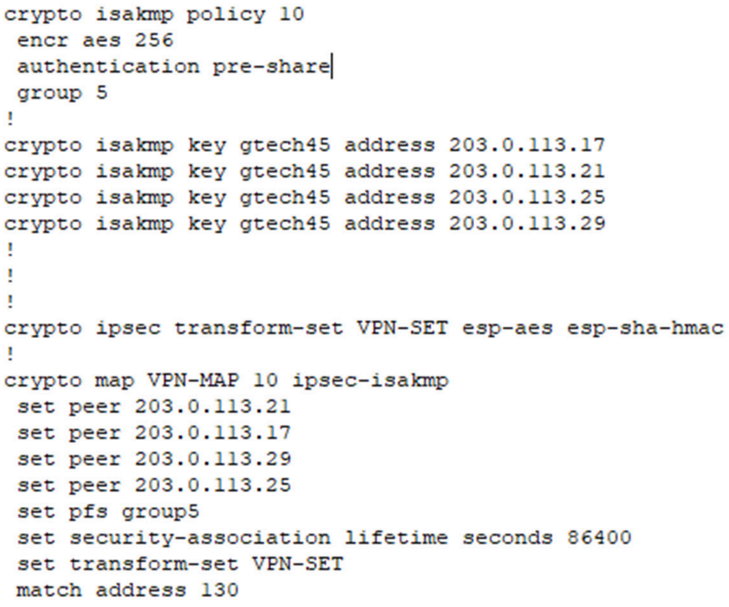
```
interface GigabitEthernet1/0/9
 switchport access vlan 25
!
interface GigabitEthernet1/0/10
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/11
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/12
 switchport mode trunk
 channel-group 1 mode active
```

Trunk Port Configuration

6.2 Layer 3 Technologies

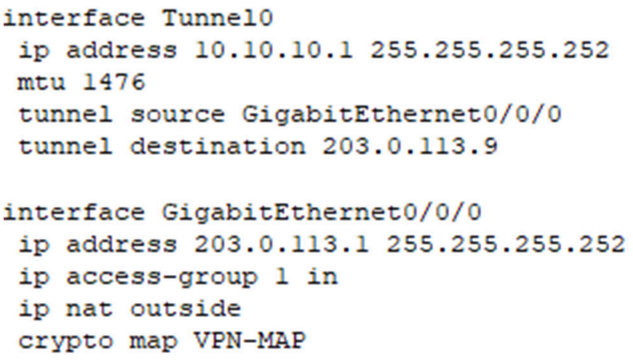
6.3 VPN Configuration:

This VPN configuration is designed to establish secure site-to-site connections using IPSec with AES encryption and SHA for authentication. It incorporates ISAKMP for key management, applies security policies, and ensures traffic between designated networks is encrypted. The setup includes the use of a crypto map, access lists for traffic control, and a GRE tunnel for encapsulation, providing robust security and performance for remote communications.



```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key gtech45 address 203.0.113.17
crypto isakmp key gtech45 address 203.0.113.21
crypto isakmp key gtech45 address 203.0.113.25
crypto isakmp key gtech45 address 203.0.113.29
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 203.0.113.21
 set peer 203.0.113.17
 set peer 203.0.113.29
 set peer 203.0.113.25
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set VPN-SET
 match address 130
```

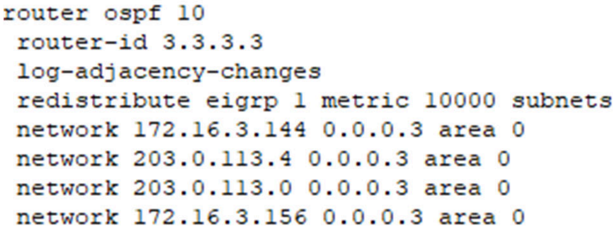
.



```
interface Tunnel0
 ip address 10.10.10.1 255.255.255.252
 mtu 1476
 tunnel source GigabitEthernet0/0/0
 tunnel destination 203.0.113.9

interface GigabitEthernet0/0/0
 ip address 203.0.113.1 255.255.255.252
 ip access-group 1 in
 ip nat outside
 crypto map VPN-MAP
```

6.4 OSPF Configuration:

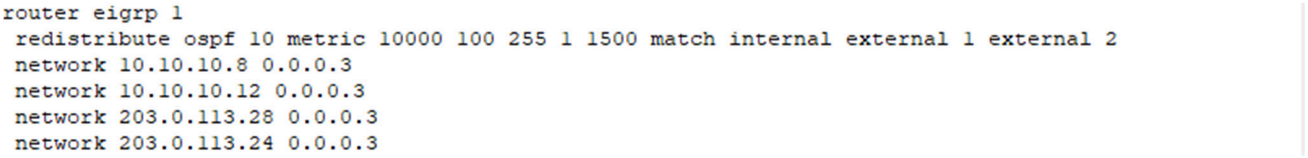
This configuration includes OSPF (Open Shortest Path First), a link-state routing protocol used to efficiently route IP traffic within an autonomous system. OSPF dynamically calculates the best paths between routers using the shortest path algorithm, allowing for fast convergence and scalability. It is widely used for its ability to handle large, complex networks by dividing them into areas and efficiently distributing routing information.



```
router ospf 10
 router-id 3.3.3.3
 log-adjacency-changes
 redistribute eigrp 1 metric 10000 subnets
 network 172.16.3.144 0.0.0.3 area 0
 network 203.0.113.4 0.0.0.3 area 0
 network 203.0.113.0 0.0.0.3 area 0
 network 172.16.3.156 0.0.0.3 area 0
```

6.5 EIGRP Configuration

This configuration includes EIGRP (Enhanced Interior Gateway Routing Protocol), a dynamic routing protocol developed by Cisco. EIGRP uses an advanced algorithm to quickly and efficiently route traffic within a network, providing fast convergence, load balancing, and support for both IPv4 and IPv6. It is widely used for its scalability and efficient use of bandwidth.

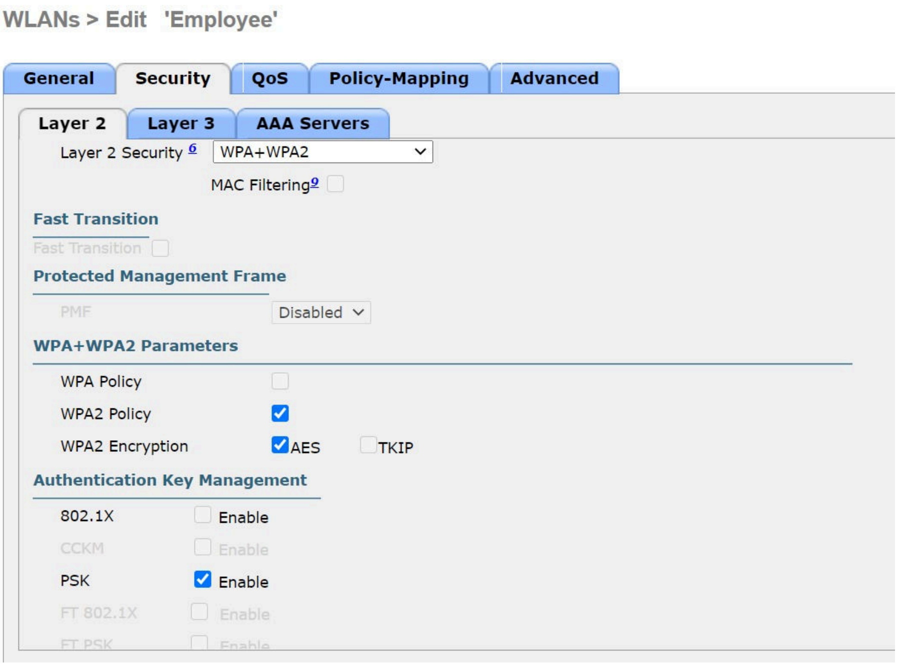


```
router eigrp 1
 redistribute ospf 10 metric 10000 100 255 1 1500 match internal external 1 external 2
 network 10.10.10.8 0.0.0.3
 network 10.10.10.12 0.0.0.3
 network 203.0.113.28 0.0.0.3
 network 203.0.113.24 0.0.0.3
```

6.6 Wan Configuration

In this section we are going to discuss the HQ WAN Router Setup.

- Router will be connected to an OOB & FW Management switch to Fortigate.
- Router will be connected to WAN Links & Microwave.
- Internet link to be hosted directly on the Fortigate FW for better network security
- Router will act as the Voice GW and the WAN RTR



WLANs > Edit 'Employee'

Layer 2 Security [6] WPA+WPA2

MAC Filtering[9] □

Fast Transition

Fast Transition □

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

Authentication Key Management

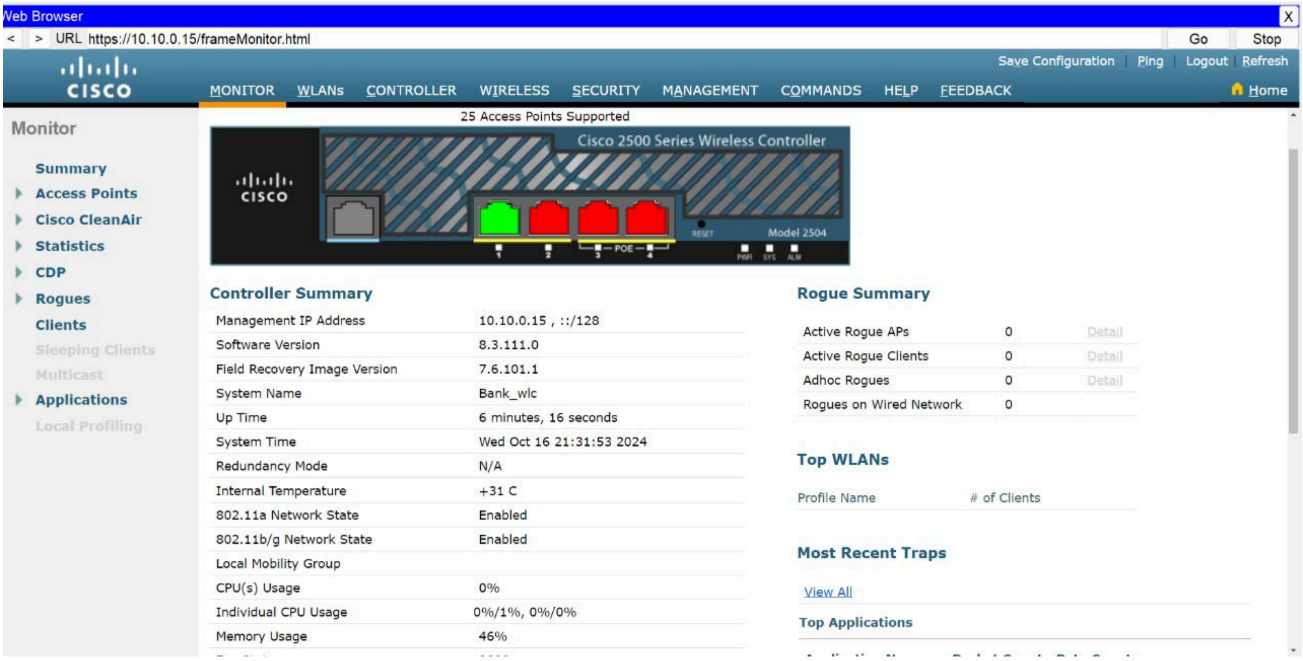
802.1X □ Enable

CCKM □ Enable

PSK ☑ Enable

FT 802.1X □ Enable

FT PSK □ Enable



URL https://10.10.0.15/frameMonitor.html

25 Access Points Supported

Controller Summary

Management IP Address	10.10.0.15 , ::/128
Software Version	8.3.111.0
Field Recovery Image Version	7.6.101.1
System Name	Bank_wlc
Up Time	6 minutes, 16 seconds
System Time	Wed Oct 16 21:31:53 2024
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/0%
Memory Usage	46%

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

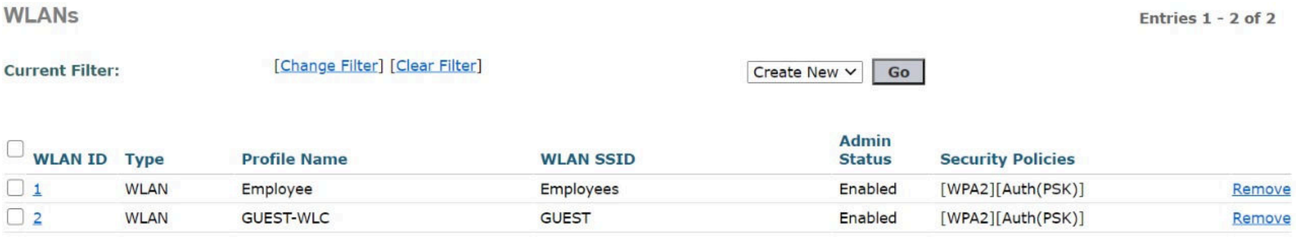
Top WLANs

Profile Name	# of Clients

Most Recent Traps

View All

Top Applications

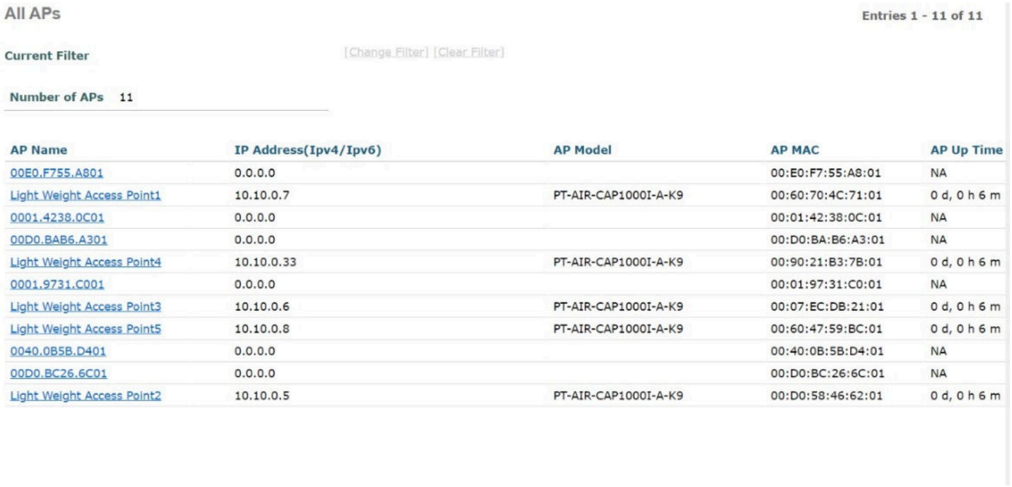


WLANs

Entries 1 - 2 of 2

Current Filter: [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
□ 1	WLAN	Employee	Employees	Enabled	[WPA2][Auth(PSK)]	Remove
□ 2	WLAN	GUEST-WLC	GUEST	Enabled	[WPA2][Auth(PSK)]	Remove



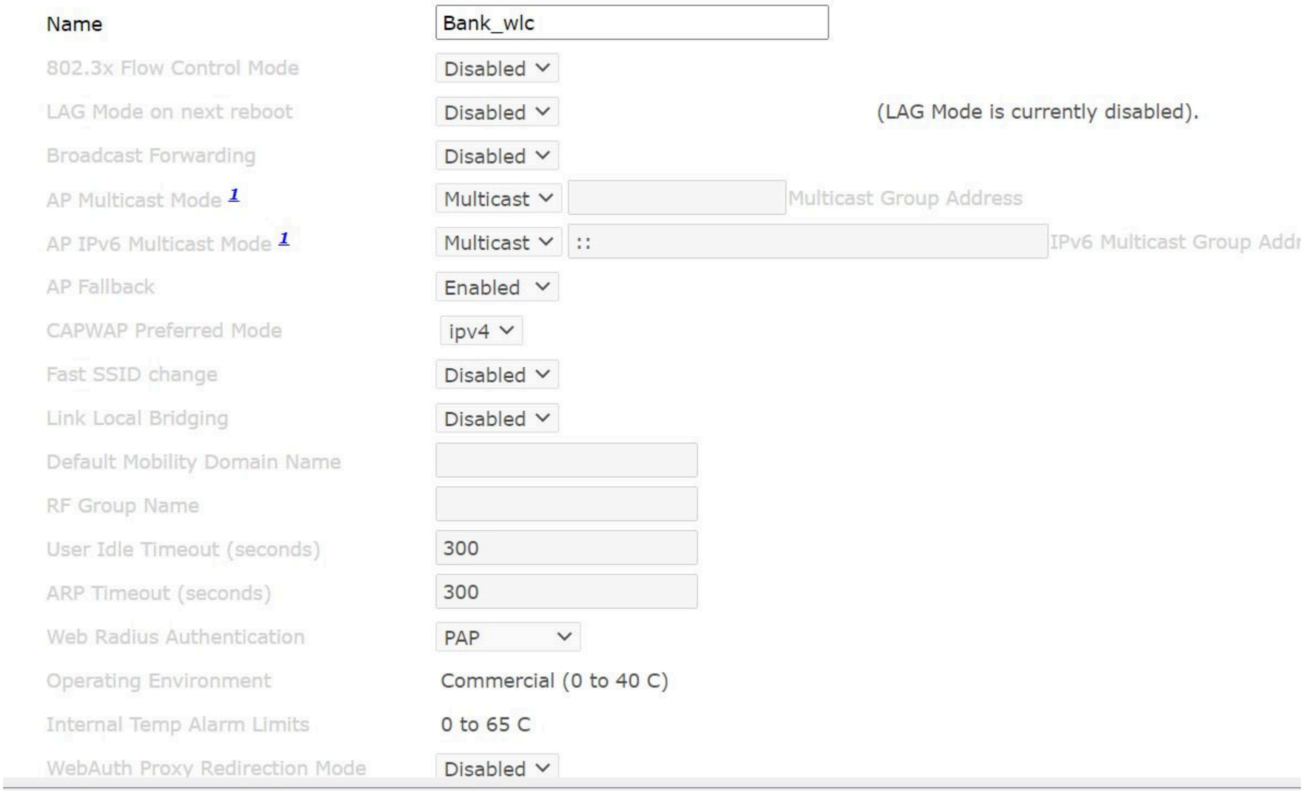
All APs

Entries 1 - 11 of 11

Current Filter [Change Filter] [Clear Filter]

Number of APs 11

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time
00E0.F755.A801	0.0.0.0		00:E0:F7:55:A8:01	NA
Light Weight Access Point1	10.10.0.7	PT-AIR-CAP1000I-A-K9	00:60:70:4C:71:01	0 d, 0 h 6 m
0001.4238.0C01	0.0.0.0		00:01:42:38:0C:01	NA
00D0.BAB6.A301	0.0.0.0		00:D0:BA:B6:A3:01	NA
Light Weight Access Point4	10.10.0.33	PT-AIR-CAP1000I-A-K9	00:90:21:B3:7B:01	0 d, 0 h 6 m
0001.9731.C001	0.0.0.0		00:01:97:31:C0:01	NA
Light Weight Access Point3	10.10.0.6	PT-AIR-CAP1000I-A-K9	00:07:EC:DB:21:01	0 d, 0 h 6 m
Light Weight Access Point5	10.10.0.8	PT-AIR-CAP1000I-A-K9	00:60:47:59:BC:01	0 d, 0 h 6 m
0040.0B5B.D401	0.0.0.0		00:40:0B:5B:D4:01	NA
00D0.BC26.6C01	0.0.0.0		00:D0:BC:26:6C:01	NA
Light Weight Access Point2	10.10.0.5	PT-AIR-CAP1000I-A-K9	00:D0:58:46:62:01	0 d, 0 h 6 m



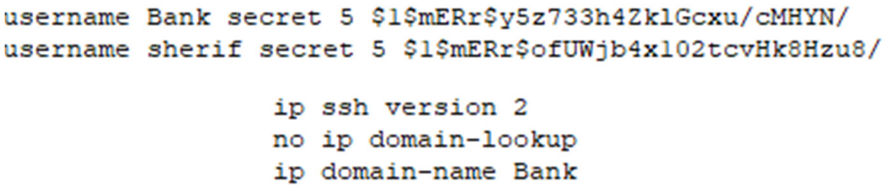
Name	Bank_wlc	
802.3x Flow Control Mode	Disabled	
LAG Mode on next reboot	Disabled	(LAG Mode is currently disabled).
Broadcast Forwarding	Disabled	
AP Multicast Mode [1]	Multicast	Multicast Group Address
AP IPv6 Multicast Mode [1]	Multicast	:: IPv6 Multicast Group Addr
AP Fallback	Enabled	
CAPWAP Preferred Mode	ipv4	
Fast SSID change	Disabled	
Link Local Bridging	Disabled	
Default Mobility Domain Name		
RF Group Name		
User Idle Timeout (seconds)	300	
ARP Timeout (seconds)	300	
Web Radius Authentication	PAP	
Operating Environment	Commercial (0 to 40 C)	
Internal Temp Alarm Limits	0 to 65 C	
WebAuth Proxy Redirection Mode	Disabled	

6.7 Management Technologies

6.7.1 AAA & Network Devices Access

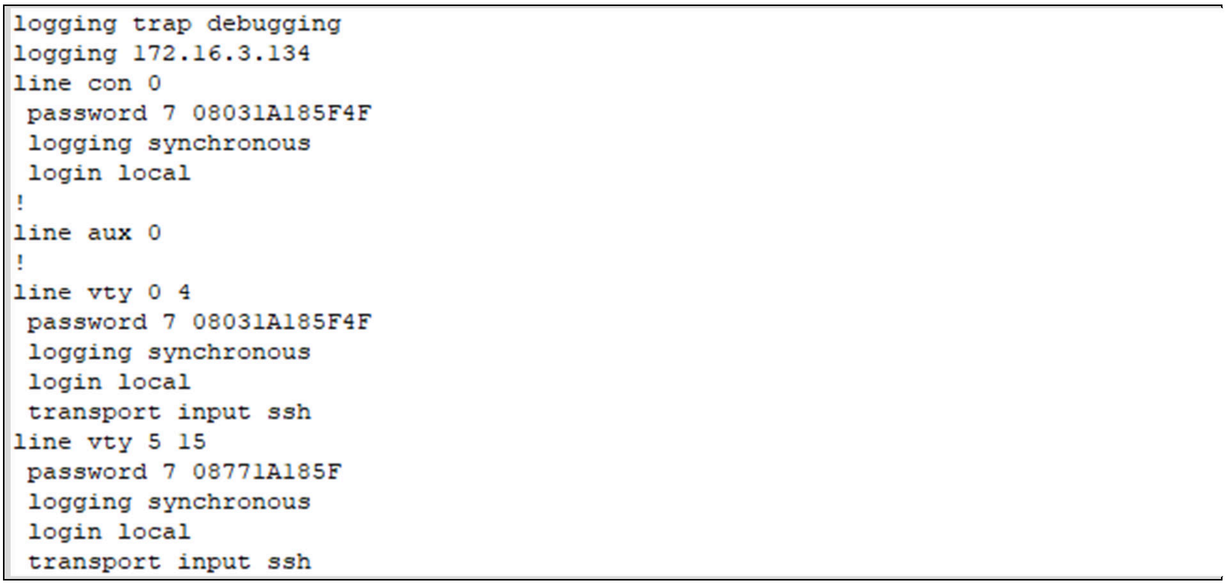
This point discuss method will be used for securing access to network devices through usernames, passwords, controlling access line parameters, controlling remote access protocols, and affecting privileges of users and commands.

SSH will be the only enabled remote access control protocol to secure the management traffic



```
username Bank secret 5 $1$mERr$y5z733h4Zk1Gcxu/cMHYN/
username sherif secret 5 $1$mERr$ofUWjb4x102tcvHk8Hzu8/

                ip ssh version 2
                no ip domain-lookup
                ip domain-name Bank
```

Local Users and SSH Configuration

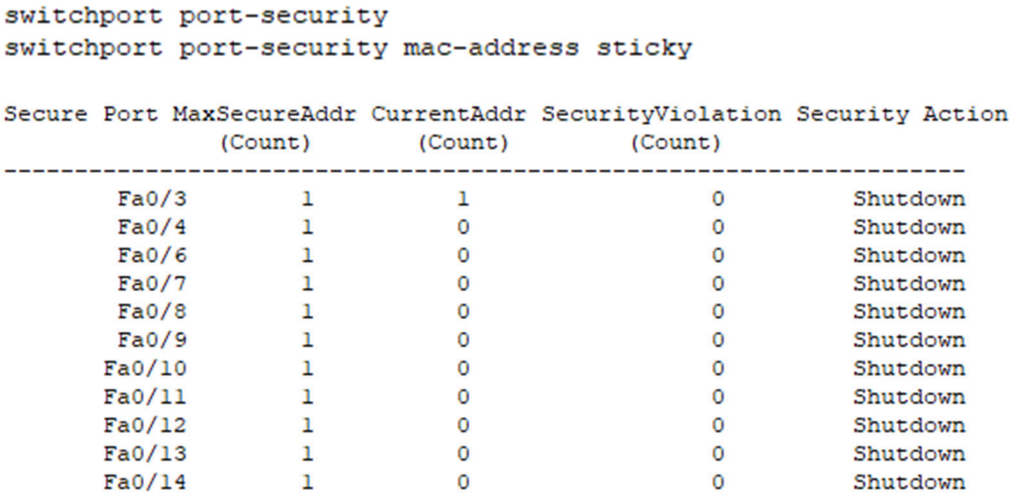


```
logging trap debugging
logging 172.16.3.134
line con 0
 password 7 08031A185F4F
 logging synchronous
 login local
!
line aux 0
!
line vty 0 4
 password 7 08031A185F4F
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 password 7 08771A185F
 logging synchronous
 login local
 transport input ssh
```

AAA Configuration

6.7.2 Port Security:

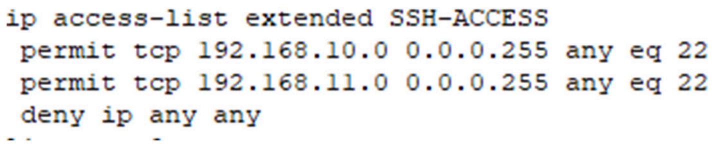
Port Security is a network feature used to restrict input to an interface by limiting and identifying MAC addresses of devices allowed to connect to that port



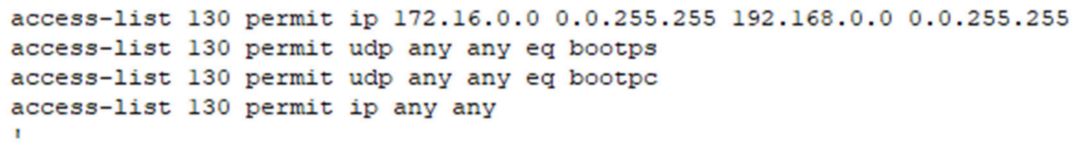
```
switchport port-security
switchport port-security mac-address sticky

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
----------------------------------------------------------------------
        Fa0/3        1           1                  0         Shutdown
        Fa0/4        1           0                  0         Shutdown
        Fa0/6        1           0                  0         Shutdown
        Fa0/7        1           0                  0         Shutdown
        Fa0/8        1           0                  0         Shutdown
        Fa0/9        1           0                  0         Shutdown
       Fa0/10        1           0                  0         Shutdown
       Fa0/11        1           0                  0         Shutdown
       Fa0/12        1           0                  0         Shutdown
       Fa0/13        1           0                  0         Shutdown
       Fa0/14        1           0                  0         Shutdown
```

6.7.3 Access Control List (ACL):

Access Control Lists (ACLs) are essential tools in networking used to control traffic flow and enhance security. They define rules that permit or deny traffic on network interfaces.



```
ip access-list extended SSH-ACCESS
 permit tcp 192.168.10.0 0.0.0.255 any eq 22
 permit tcp 192.168.11.0 0.0.0.255 any eq 22
 deny ip any any
```



```
access-list 130 permit ip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 130 permit udp any any eq bootps
access-list 130 permit udp any any eq bootpc
access-list 130 permit ip any any
!
```

SNMP Configuration

6.7.4 Disable unneeded services

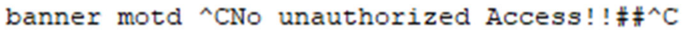
Disable Services that may be Involve Security risks as Bootp server, pad service, http server, https server and finger service.

```
service timestamps debug datetime msec local show
service timestamps debug datetime msec local time
no ip domain-lookup
```

Disable Unneeded Services

6.7.5 Banner

Banner message used to display a security warning for any one try to access network devices.



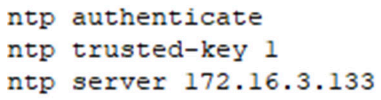
```
banner motd ^CNo unauthorized Access!!##^C
```

Banner Configuration

6.7.6 NTP and time

It is often extremely useful to be able to accurately pinpoint when a particular event occurred. You may want to compare network event messages from various routers on your network for fault isolation, troubleshooting, and security purposes. This is impossible if their clocks are not set to a common source. In fact, the problem is even worse than merely setting the clocks to a single common standard because some clocks run a little bit fast and others run a little bit slow. So they need to be continuously adjusted and synchronized.

Network Time Protocol (NTP) is a standard for protocol which we can use to achieve the previous requirements.



```
ntp authenticate
ntp trusted-key 1
ntp server 172.16.3.133
```

NTP Configuration

6.7.7 Logging

Logging is critical for fault notification, network forensics, and security auditing. Cisco equipment handles log messages in following ways:

- By default, the router sends all log messages to its console port. Only users that are physically connected to the router console port may view these messages, though. This is called console logging.
- Terminal logging is similar to console logging, but it displays log messages to the router’s VTY lines instead. This type of logging is not enabled by default, so if you want to use it, you need to need activate it for each required line.
- Buffered logging creates a circular buffer within the router’s RAM for storing log messages. This circular buffer has a fixed size to ensure that the log will not deplete valuable system memory. The router accomplishes this by deleting old messages from the buffer as new messages are added.
- The router can use syslog to forward log messages to external syslog servers for centralized storage. This type of logging is not enabled by default.

Logging Configuration