



# Graduation Project

*Documentation File*

## Implementing a Secure Multi-Branch Office Network

**Cisco Cybersecurity Engineer**

**(ONL2_ISS5_S2)**

**Made by**

Ahmed Mohamed Gharib

Abdul Rahman Mohammed Hamed

Hassan Muhammed Abdelnabi

Muhammed Samy Elhamzawy

Muhammed Mustafa Gomaa

**Supervised by**

Eng. Amr Adel

# Table of Contents

# 1. Introduction

## 1.1 Document Control

**Document Title:** Multi-Branch Enterprise Network Infrastructure with Secure VPN Integration

**Document Owner:** Group 01 -- ONL2_ISS5_S2

## 1.2 Document Purpose:

The objective of this project is to design and implement a reliable, secure, and scalable network infrastructure that connects a main office with three branch offices. The network is intended to:

- Ensure reliable and encrypted communication between all sites through site-to-site VPN tunnels.
- Segment internal networks using VLANs for better traffic management, security, and departmental isolation.
- Implement robust firewall rules and security mechanisms to protect against external and internal cyber threats.
- Centralize essential network services to simplify administration and improve resource efficiency.
- Monitor and log network activities for auditing and threat detection purposes.
- Provide internet access to all offices while ensuring controlled traffic flow.

## 1.3 Key Features

1. **VLAN Segmentation:**
   The network utilizes VLANs to separate different departments (e.g., HR, Finance, Sales) in each office. This segmentation improves performance and security while allowing tailored access controls and policies for each VLAN.
2. **Site-to-Site VPN (IPsec):**
   Encrypted VPN tunnels are established between the main office and each of the three branch offices using IPsec. This ensures secure data transmission over public networks and preserves the confidentiality and integrity of inter-office communication.
3. **Hierarchical Topology:**
   The network follows a hierarchical topology including routers, Layer 3 switches, Layer 2 access switches, firewalls, and secure links to internal servers and the internet. Each site has its own LAN infrastructure and is connected to the main office via VPN.
4. **Firewall Integration:**
   Firewalls are deployed at all offices to enforce security policies, block unauthorized traffic, and provide NAT for internet access. Rules are tailored to allow only approved inter-VLAN and inter-site communications.
5. **Centralized Services:**
   Core services such as DHCP, DNS, Syslog, and FTP servers are hosted at the main office and accessed securely by the branches. This centralization improves manageability and resource allocation.

6. **Security Measures:**
   The network devices are hardened through best practices including password policy enforcement, disabling unused ports, and firmware updates. Intrusion Detection and Prevention Systems (IDS/IPS) are implemented for proactive threat detection and response.
7. **Monitoring and Logging:**
   All network activities are logged via Syslog servers and monitored using dedicated tools. This allows real-time performance evaluation, anomaly detection, and supports post-event investigations.

---

## 1.4 Offices Table

| Office | Role |
|---|---|
| Main Office | Headquarters |
| Branch Office 1 | Small Branch |
| Branch Office 2 | Small Branch |
| Branch Office 3 | Small Branch |

---

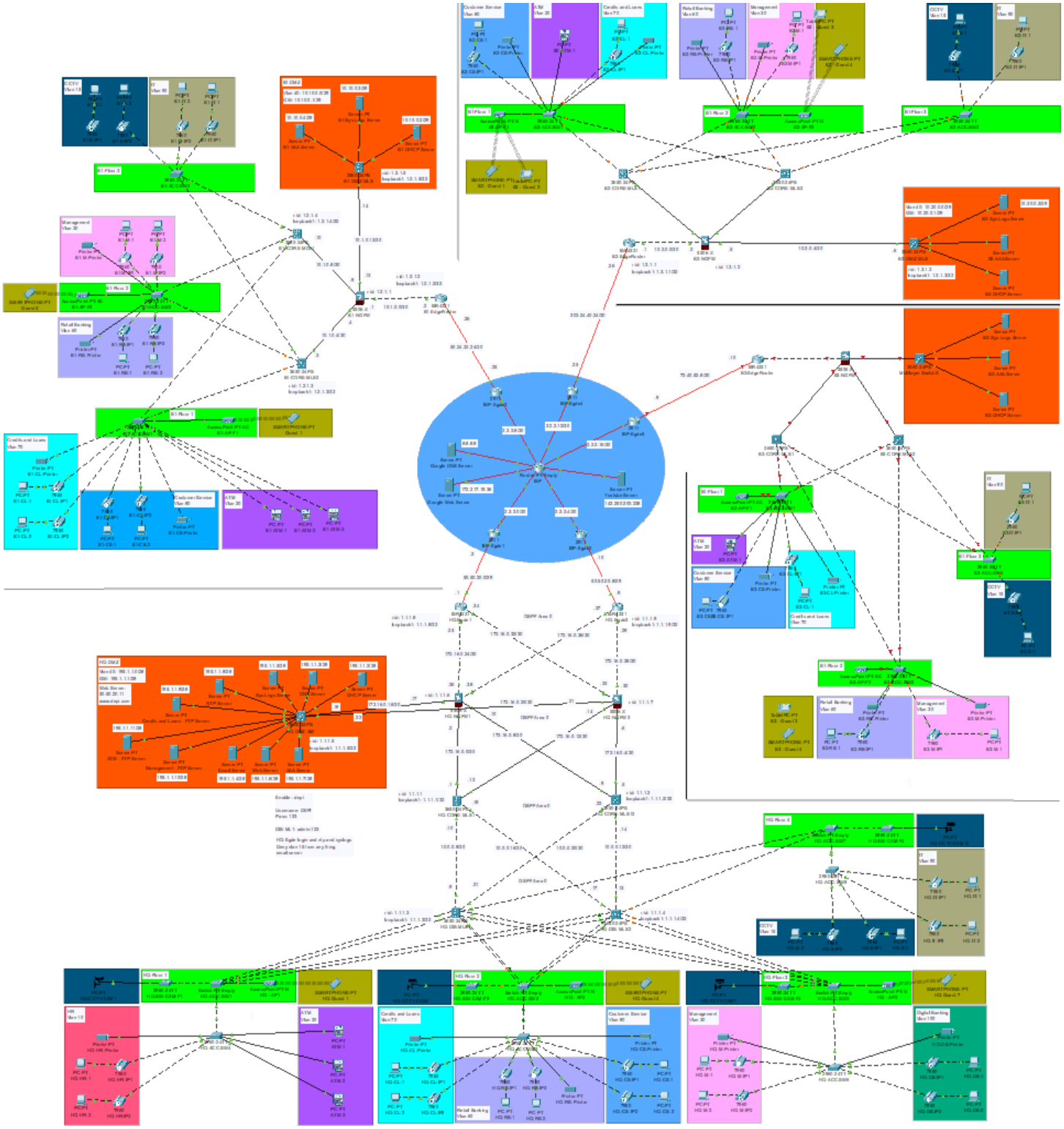
# 2. Network Architecture

## 2.1 Topology Description

| Main Office | | | | | |
|---|---|---|---|---|---|
| **Device** | **Number** | **Model** | **Device** | **Number** | **Model** |
| **Router** | 2 | ISR 4331 | **Server** | 8 | Sys-Logs Server |
| | | | | | Email Server |
| **MLS** | 5 | 3650-24PS | | | DNS Server |
| **ASA** | 2 | 5506-X | | | DHCP Server |
| **Access Point** | 3 | Stand Alone Access Point 802.11n | | | AAA Server |
| | | | | | Web Server |
| **Switch** | 8 | 2960 | | | NTP Server |
| | 4 | 2960-24TT +POE | | | FTP Server |

| Each Branch Office | | | | | |
|---|---|---|---|---|---|
| **Device** | **Number** | **Model** | **Device** | **Number** | **Model** |
| **Router** | 1 | ISR 4331 | **Server** | 3 | Sys-Logs Server |
| | | | | | AAA Server |
| **ASA** | 1 | 5506-X | | | DHCP Server |
| **MLS** | 2 | 3650-24PS | **Access Point** | 2 | Stand Alone Access Point 802.11n |
| | 1 | 3660-24PS | | | |

## 2.2 Network Topology Diagram:



## 2.3 Hierarchical Network Design:

**Why Hierarchical Design?**

- **Scalability:** Easily accommodate new branches or VLANs without redesigning the entire network.
- **Fault Tolerance:** Contain failures to a single layer, preventing widespread impact.
- **Performance:** Distribute traffic load across distinct layers (Core, Distribution, Access) to reduce congestion and improve throughput.

| Layer | Key Devices | Responsibilities |
|---|---|---|
| **Core Layer** | HQ-CORE-R1,<br>HQ-CORE-R2,<br>MLS1, MLS2 | Provide a high-speed, low-latency backbone |
| **Distribution Layer** | HQ-DIS-MLS1,<br>HQ-DIS-MLS2 | Inter-VLAN routing<br>Enforce ACLs and QoS policies |
| **Access Layer** | HQ-ACC-SW1,<br>HQ-ACC-SW2,<br>HQ-ACC-SW3,<br>APs | Connect end-users and devices<br>VLAN membership and port security<br>PoE for wireless APs |

# 3. Naming Convention and IP Scheme

## 3.1 Naming Convention:

We will adopt a standardized naming convention for network devices to simplify identification, management, and troubleshooting, using a consistent naming schema across all infrastructure components.

# Main Office:

| Hostname | IP address |
|---|---|
| HQ-Edge1 | 172.16.0.25 / 172.16.0.34 |
| HQ-Edge2 | 172.16.0.29 / 172.16.0.37 |
| HQ-NGFW1 | 172.16.0.2 / 172.16.0.10 |
| HQ-NGFW2 | 172.16.0.6 / 172.16.0.14 |
| HQ-DMZ-MLS | 195.1.1.1 |
| HQ-CORE-MLS1 | 192.168.200.16 |
| HQ-CORE-MLS2 | 192.168.200.17 |
| HQ-DIS-MLS1 | 192.168.200.2 |
| HQ-DIS-MLS2 | 192.168.200.3 |
| HQ-ACC-SW1 | 192.168.200.4 |
| HQ-ACC-SW2 | 192.168.200.6 |
| HQ-ACC-SW3 | 192.168.200.8 |
| HQ-ACC-SW4 | 192.168.200.5 |
| HQ-ACC-SW5 | 192.168.200.7 |
| HQ-ACC-SW6 | 192.168.200.9 |
| HQ-ACC-SW7 | 192.168.200.14 |
| HQ-ACC-SW8 | 192.168.200.10 |
| HQ-SW-CAM-F1 | 192.168.200.11 |
| HQ-SW-CAM-F2 | 192.168.200.12 |
| HQ-SW-CAM-F3 | 192.168.200.13 |
| HQ-SW-CAM-F4 | 192.168.200.15 |

# Branch 1:

| Hostname | IP address |
|---|---|
| B1-EdgeRouter | 10.1.0.2 |
| B1-NGFW | 10.1.0.1 |
| B1-DMZ-MLS | 10.1.0.14 |
| B1-CORE-MLS1 | 192.168.200.2 |
| B1-CORE-MLS2 | 192.168.200.3 |
| B1-ACC-SW1 | 192.168.200.4 |
| B1-ACC-SW2 | 192.168.200.5 |
| B1-ACC-SW3 | 192.168.200.6 |
| B1-SW-CAM-F1 | 192.168.200.7 |
| B1-SW-CAM-F2 | 192.168.200.8 |
| B1-SW-CAM-F3 | 192.168.200.9 |

# Branch 2:

| Hostname | IP address |
|---|---|
| B2-EdgeRouter | 10.2.0.1 |
| B2-NGFW | 10.2.0.2 |
| B2-DMZ-MLS | 10.2.0.6 |
| B2-CORE-MLS1 | 192.168.200.2 |
| B2-CORE-MLS2 | 192.168.200.3 |
| B2-ACC-SW1 | 192.168.200.4 |
| B2-ACC-SW2 | 192.168.200.5 |
| B2-ACC-SW3 | 192.168.200.6 |
| B2-SW-CAM-F1 | 192.168.200.7 |
| B2-SW-CAM-F2 | 192.168.200.8 |
| B2-SW-CAM-F3 | 192.168.200.9 |

# Branch 3:

| Hostname | IP address |
|---|---|
| B3-EdgeRouter | 10.3.0.1 |
| B3-NGFW | 10.3.0.2 |
| B3-DMZ-MLS | 10.3.0.6 |
| B3-CORE-MLS1 | 192.168.200.2 |
| B3-CORE-MLS2 | 192.168.200.3 |
| B3-ACC-SW1 | 192.168.200.4 |
| B3-ACC-SW2 | 192.168.200.5 |
| B3-ACC-SW3 | 192.168.200.6 |
| B3-SW-CAM-F1 | 192.168.200.7 |
| B3-SW-CAM-F2 | 192.168.200.8 |
| B3-SW-CAM-F3 | 192.168.200.9 |

## 3.2 IP Addressing scheme

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

# Main Office:

| HQ | | | | |
|---|---|---|---|---|
| **Default Gateway** | **Host** | **Subnet** | **VLAN Name** | **VLAN Number** |
| 192.168.10.1 | 30 | 192.168.10.0/27 | HR | 10 |
| 192.168.150.1 | 30 | 192.168.150.0/27 | CCTV | 15 |
| 192.168.20.1 | 30 | 192.168.20.0/27 | ATM | 20 |
| 192.168.30.1 | 30 | 192.168.30.0/27 | Management | 30 |
| 192.168.40.1 | 254 | 192.168.40.0/24 | Voice | 40 |
| 192.168.50.1 | 254 | 192.168.50.0/24 | Guest | 50 |
| 192.168.60.1 | 62 | 192.168.60.0/26 | Retail Banking | 60 |
| 192.168.70.1 | 30 | 192.168.70.0/27 | Credits and Loans | 70 |
| 192.168.80.1 | 30 | 192.168.80.0/27 | Customer Service | 80 |
| 192.168.90.1 | 30 | 192.168.90.0/27 | IT | 90 |
| 192.168.100.1 | 30 | 192.168.100.0/27 | Digital Banking | 100 |
| 192.168.200.1 | 30 | 192.168.200.0/27 | Manage | 200 |

- **HR**: Around 15 devices (HR staff computers and printers).
- **CCTV**: Around 25 devices (security cameras and NVRs).
- **ATM:** About 6 devices (one for each ATM machine).
- **Management:** Around 8 devices (executive laptops and desktops).
- **Voice:** About 251 devices (IP phones across departments).
- **Guest:** Approximately 251 devices (visitor and employee mobile devices via Wi-Fi).
- **Retail Banking:** Around 40 devices (tellers, front desk systems).
- **Credits and Loans:** Roughly 20 devices (loan officers and support staff).
- **Customer Service:** About 25 devices (support agents and service counters).
- **IT:** Around 15 devices (engineer workstations, testing equipment, maybe small servers).
- **Digital Banking:** Around 10 devices (development team workstations).
- **Manage**: Around 16 devices (network/admin management consoles).

## Branch 1:

| Branch 1 | | | | |
|---|---|---|---|---|
| **Default Gateway** | **Host** | **Subnet** | **VLAN Name** | **VLAN Number** |
| 192.168.151.1 | 30 | 192.168.151.0/27 | CCTV | 15 |
| 192.168.21.1 | 14 | 192.168.21.0/28 | ATM | 20 |
| 192.168.31.1 | 14 | 192.168.31.0/28 | Management | 30 |
| 192.168.41.1 | 254 | 192.168.41.0/24 | Voice | 40 |
| 192.168.51.1 | 254 | 192.168.51.0/24 | Guest | 50 |
| 192.168.61.1 | 14 | 192.168.61.0/28 | Retail Banking | 60 |
| 192.168.71.1 | 14 | 192.168.71.0/28 | Credits and Loans | 70 |
| 192.168.81.1 | 14 | 192.168.81.0/28 | Customer Service | 80 |
| 192.168.91.1 | 14 | 192.168.91.0/28 | IT | 90 |
| 192.168.200.1 | 6 | 192.168.200.0/29 | Manage | 200 |

- **CCTV**: Around 25 devices (security cameras and NVRs).
- **ATM:** About 4 devices (one for each ATM machine).
- **Management:** Around 3 devices (executive laptops and desktops).
- **Voice:** About 251 devices (IP phones across departments).
- **Guest:** Approximately 251 devices (visitor and employee mobile devices via Wi-Fi).
- **Retail Banking:** Around 8 devices (tellers, front desk systems).
- **Credits and Loans:** Roughly 10 devices (loan officers and support staff).
- **Customer Service:** About 8 devices (support agents and service counters).
- **IT:** Around 3 devices (engineer workstations, testing equipment, maybe small servers).
- **Manage**: Around 9 devices (network/admin management consoles).

## Branch 2:

| Branch 2 | | | | |
|---|---|---|---|---|
| **Default Gateway** | **Host** | **Subnet** | **VLAN Name** | **VLAN Number** |
| 192.168.152.1 | 30 | 192.168.152.0/27 | CCTV | 15 |
| 192.168.22.1 | 14 | 192.168.22.0/28 | ATM | 20 |
| 192.168.32.1 | 14 | 192.168.32.0/28 | Management | 30 |
| 192.168.42.1 | 254 | 192.168.42.0/24 | Voice | 40 |
| 192.168.52.1 | 254 | 192.168.52.0/24 | Guest | 50 |
| 192.168.62.1 | 14 | 192.168.62.0/28 | Retail Banking | 60 |
| 192.168.72.1 | 14 | 192.168.72.0/28 | Credits and Loans | 70 |
| 192.168.82.1 | 14 | 192.168.82.0/28 | Customer Service | 80 |
| 192.168.92.1 | 14 | 192.168.92.0/28 | IT | 90 |
| 192.168.200.1 | 6 | 192.168.200.0/29 | Manage | 200 |

- **CCTV**: Around 25 devices (security cameras and NVRs).
- **ATM:** About 4 devices (one for each ATM machine).
- **Management:** Around 3 devices (executive laptops and desktops).
- **Voice:** About 251 devices (IP phones across departments).
- **Guest:** Approximately 251 devices (visitor and employee mobile devices via Wi-Fi).
- **Retail Banking:** Around 8 devices (tellers, front desk systems).
- **Credits and Loans:** Roughly 10 devices (loan officers and support staff).
- **Customer Service:** About 8 devices (support agents and service counters).
- **IT:** Around 3 devices (engineer workstations, testing equipment, maybe small servers).
- **Manage**: Around 9 devices (network/admin management consoles).

## Branch 3:

| Branch 3 | | | | |
|---|---|---|---|---|
| **Default Gateway** | **Host** | **Subnet** | **VLAN Name** | **VLAN Number** |
| 192.168.153.1 | 30 | 192.168.153.0/27 | CCTV | 15 |
| 192.168.23.1 | 14 | 192.168.23.0/28 | ATM | 20 |
| 192.168.33.1 | 14 | 192.168.33.0/28 | Management | 30 |
| 192.168.43.1 | 254 | 192.168.43.0/24 | Voice | 40 |
| 192.168.53.1 | 254 | 192.168.53.0/24 | Guest | 50 |
| 192.168.63.1 | 14 | 192.168.63.0/28 | Retail Banking | 60 |
| 192.168.73.1 | 14 | 192.168.73.0/28 | Credits and Loans | 70 |
| 192.168.83.1 | 14 | 192.168.83.0/28 | Customer Service | 80 |
| 192.168.93.1 | 14 | 192.168.93.0/28 | IT | 90 |
| 192.168.200.1 | 6 | 192.168.200.0/29 | Manage | 200 |

- **CCTV**: Around 25 devices (security cameras and NVRs).
- **ATM:** About 4 devices (one for each ATM machine).
- **Management:** Around 3 devices (executive laptops and desktops).
- **Voice:** About 251 devices (IP phones across departments).
- **Guest:** Approximately 251 devices (visitor and employee mobile devices via Wi-Fi).
- **Retail Banking:** Around 8 devices (tellers, front desk systems).
- **Credits and Loans:** Roughly 10 devices (loan officers and support staff).
- **Customer Service:** About 8 devices (support agents and service counters).
- **IT:** Around 3 devices (engineer workstations, testing equipment, maybe small servers).
- **Manage**: Around 9 devices (network/admin management consoles).

# 4. Network Design Notes and Configuration

## 4.1 Layer-2 Fundamentals

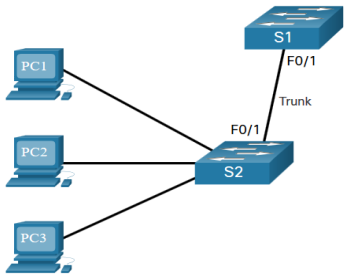
Below is a detailed breakdown of each Layer-2 technology used in our design.
For each, we provide

(a) A brief overview
(b) Example configuration steps
(c) Verification commands.

---

### 4.1.1 VLANs and Trunking

**Overview:**




- Virtual LANs (VLANs) logically segment broadcast domains at Layer 2.
- Trunk links carry multiple VLANs between switches using IEEE 802.1Q tagging, preserving separation across the network.

**Configuration:**

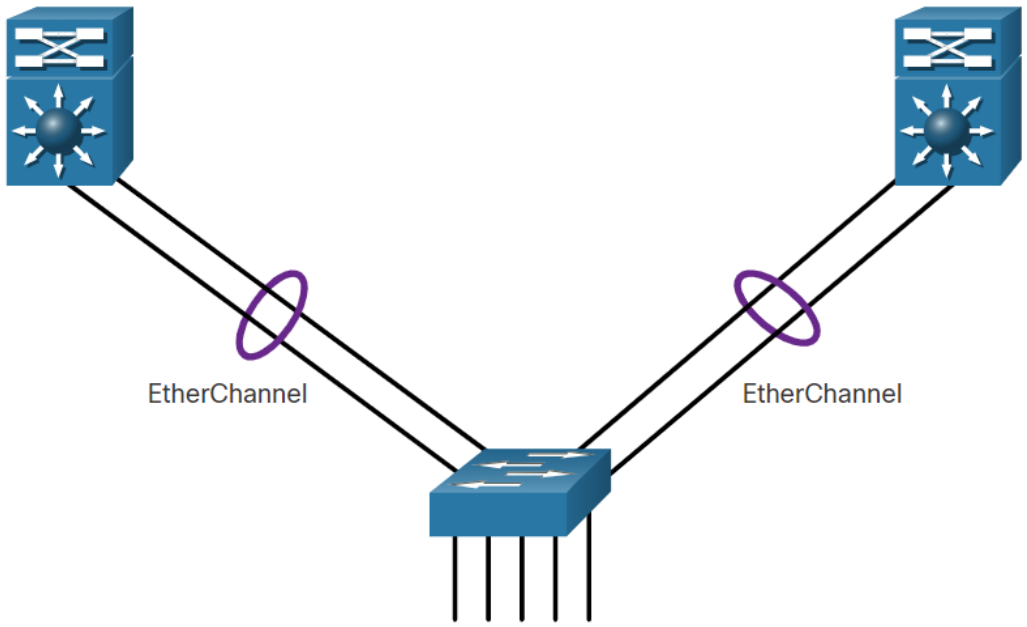
```
! Create your VLANs on each switch:
vlan 10
  name HR
vlan 15
  name CCTV

! Configure a trunk port between Switch 1 and Switch 2:
interface fa0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 10,15,20,30,40,50
```

**Verification:**

```
show vlan brief
show interfaces fa0/1 trunk
```

## 4.1.2 Port-Aggregation (**EtherChannel**)

**Overview:**




EtherChannel bundles multiple physical links into one logical interface, increasing bandwidth and providing link redundancy. We use **static mode** ("mode on") for full administrative control.

**Configuration:**

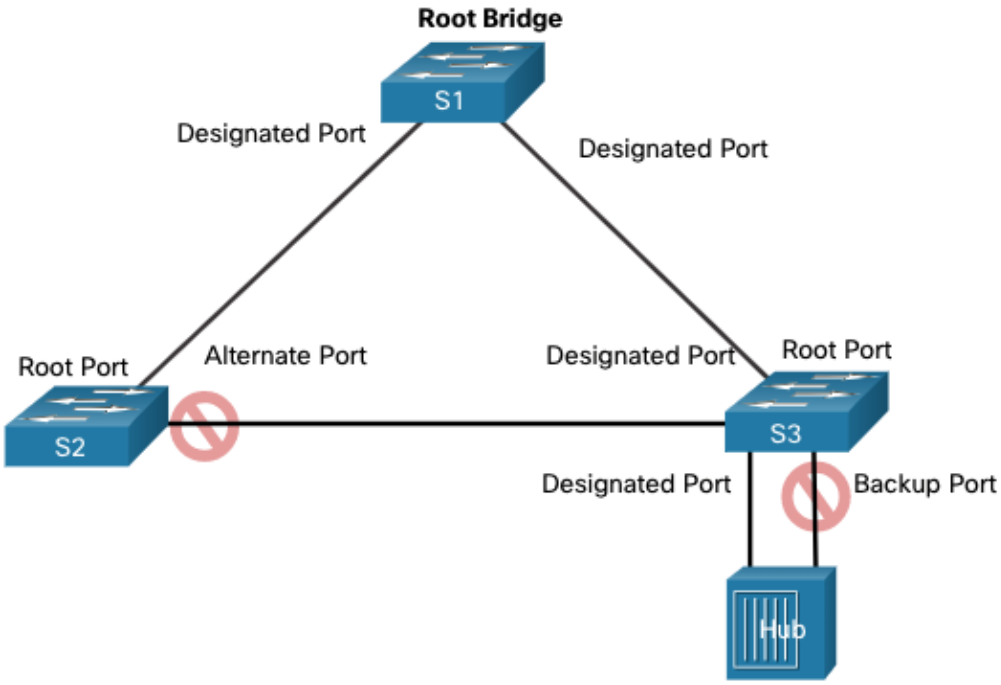
```
! On each switch in the channel:
interface range GigabitEthernet1/0/1 - 2
  switchport mode trunk
  channel-group 1 mode on

! Define the Port-Channel:
interface Port-channel1
  switchport trunk encapsulation dot1q
  switchport mode trunk
```

**Verification:**

```
show etherchannel summary
```

## 4.1.3 Spanning-Tree (**STP**)

**Overview:**




Rapid PVST+ provides fast convergence of spanning-tree topology changes on a per-VLAN basis. We enable **PortFast** on edge ports and **BPDU-Guard** to protect against inadvertent loops.

**Configuration:**

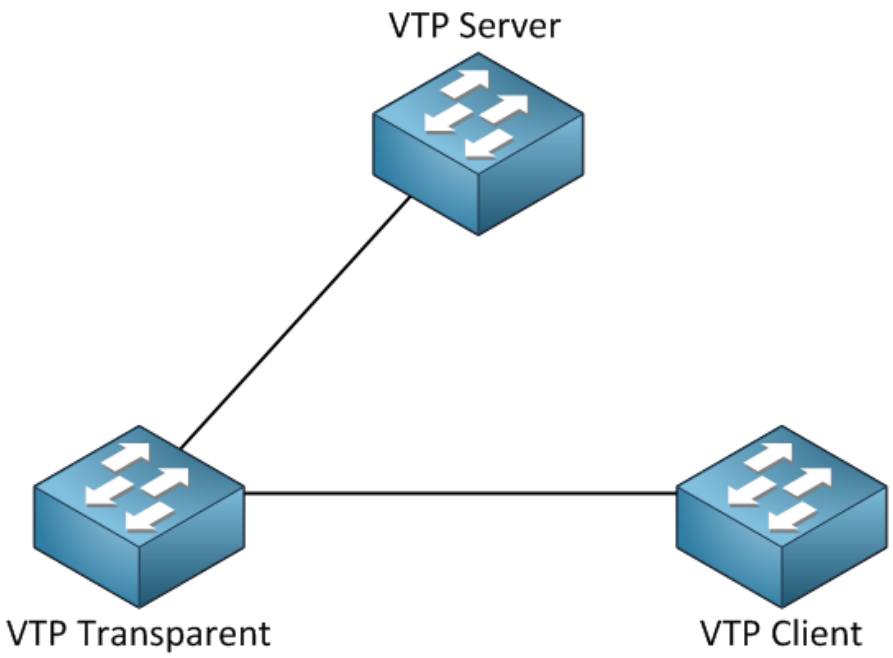
```
 !Global STP settings:
spanning-tree mode rapid-pvst
spanning-tree extend system-id

 !Edge-port optimization:
interface range FastEthernet0/1 - 10
  spanning-tree portfast
  spanning-tree bpduguard enable
```

**Verification:**

```
show spanning-tree summary
show spanning-tree active
```

## 4.1.4 VLAN Trunking Protocol (**VTP**)

**Overview:**




VTP manages VLAN propagation across a Cisco campus. We run **transparent** mode to avoid unintended VLAN changes; all VLANs are created manually.

**Configuration:**

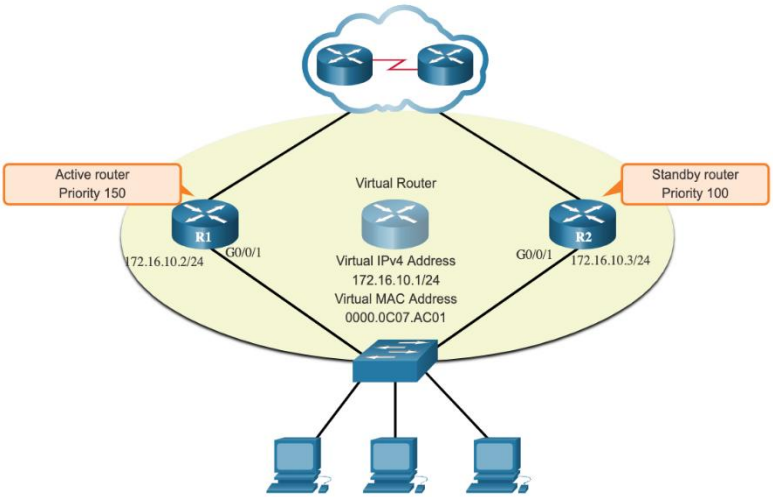
```
 !Global VTP settings:
vtp version 2
vtp domain DEPI
vtp password 123
vtp mode (server, transparent, client)
```

**Verification:**

```
show vtp status
show vlan brief
```

## 4.1.5 FHRP (**HSRP**)

**Overview:**




The Hot Standby Router Protocol (HSRP) provides gateway redundancy. Two routers share a virtual IP; in the event of failure, standby takes over without interrupting traffic.

**Configuration:**

```
! On Primary router:
interface Vlan10
  ip address 172.16.10.2 255.255.255.0
  standby 10 ip 172.16.10.1
  standby 10 priority 150
  standby 10 preempt

! On Secondary router:
interface Vlan10
  ip address 172.16.10.3 255.255.255.0
  standby 10 ip 172.16.10.1
```

**Verification:**

```
show standby brief
show standby
```

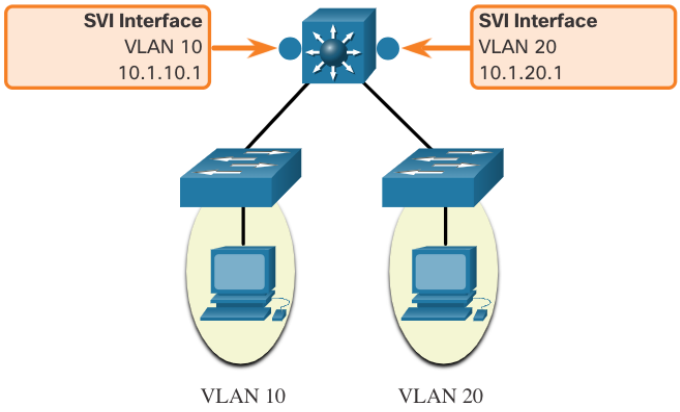
## 4.2 Layer-3 Fundamentals

Below are the Layer-3 services in our hierarchical design. Each subsection includes an overview, example configuration, and verification commands.

---

### 4.2.1 Inter-VLAN Routing

**Overview:**




- Inter-VLAN routing enables traffic exchange between VLANs. We implement this on a Layer-3 switch using Switched Virtual Interfaces (SVIs).

**Configuration:**

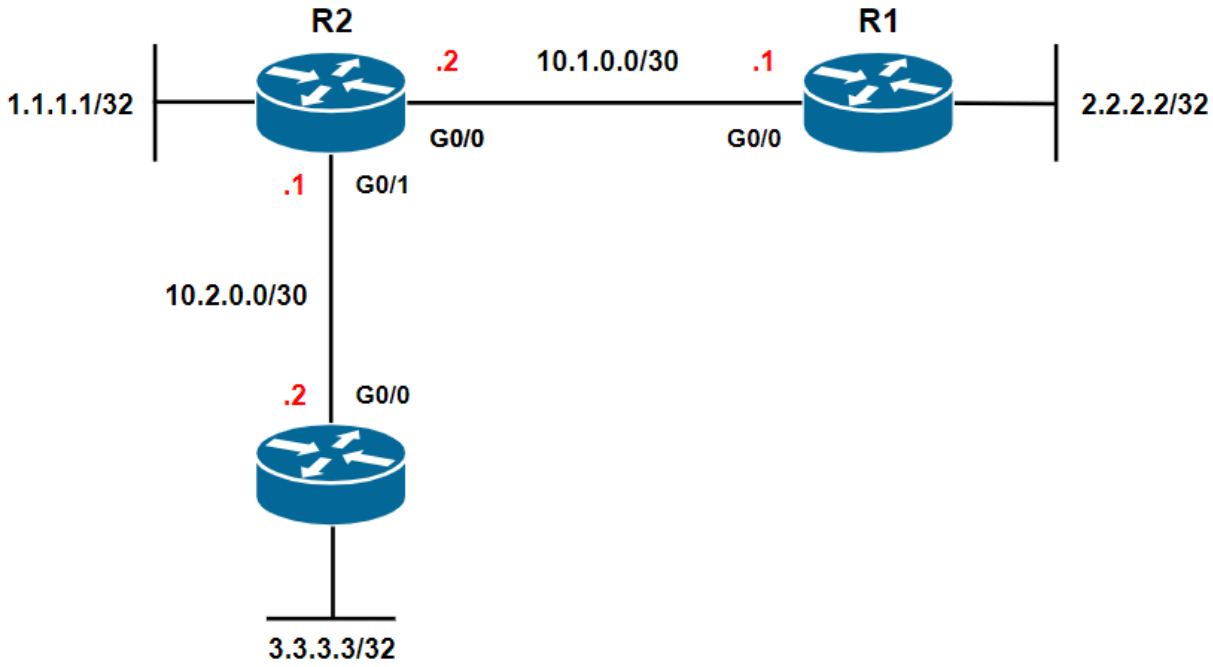
```
! Enable IP routing globally
ip routing

! Create SVIs for each VLAN
interface Vlan10
  ip address 10.1.10.1 255.255.255.0
interface Vlan20
  ip address 10.1.20.1 255.255.255.0
```

**Verification:**

```
show ip interface brief          ! SVIs status
ping 10.1.20.1                   ! Test routing from VLAN10 to VLAN20
```

## 4.2.2 Static & Default Static Routing

**Overview:**




- Implement static and default static routing to provide fixed and controlled paths for traffic forwarding, especially useful in small or hub-and-spoke topologies where routing decisions are predictable.

**Configuration:**

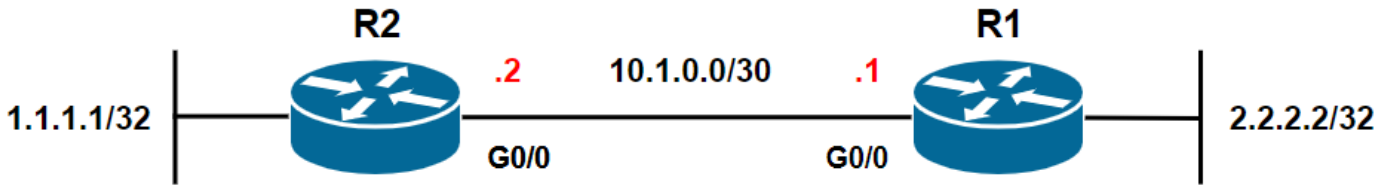
```
! R1 (Default Static Route - Gateway of Last Resort)
ip route 0.0.0.0 0.0.0.0 10.1.0.2

! R3 (Default Static Route - Gateway of Last Resort)
ip route 0.0.0.0 0.0.0.0 10.2.0.1

! R2 (Static Route)
ip route 2.2.2.2 255.255.255.255 10.1.0.1
ip route 3.3.3.3 255.255.255.255 10.2.0.2
```

**Verification:**

```
show ip route
ping 1.1.1.1
```

## 4.2.3 Dynamic Routing (**OSPF**)

**Overview:**




- OSPF provides fast, loop-free convergence and supports hierarchical area design. We place all links and SVIs in Area 0.

**Configuration:**

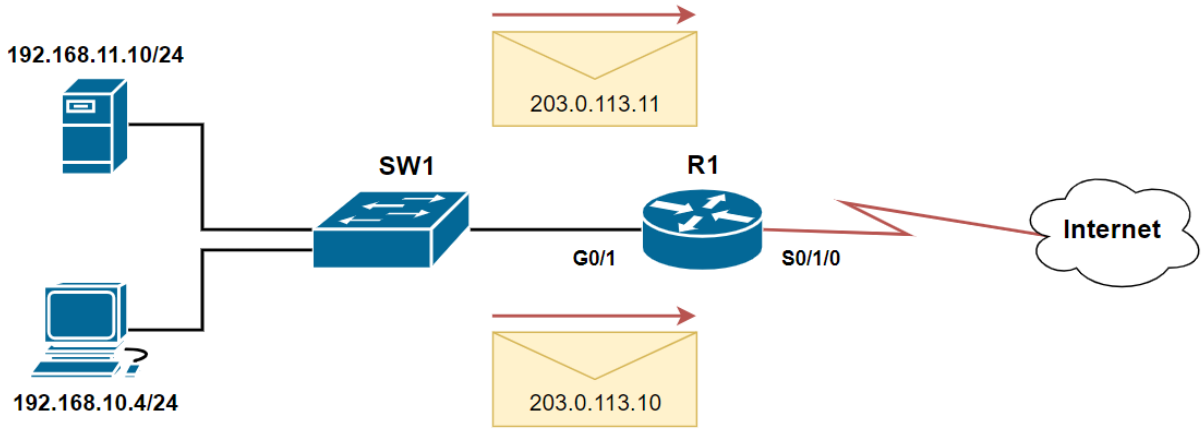
```
! R1
router ospf 1
  router-id 2.2.2.2
  network 10.1.0.0 0.0.0.3 area 0          ! Link to R2
  network 2.2.2.2 0.0.0.0
  passive-interface default
  no passive-interface G0/0                ! Active Link to R2

! R2
router ospf 1
  router-id 1.1.1.1
  network 10.1.0.0 0.0.0.3 area 0          ! Link to R1
  network 1.1.1.1 0.0.0.0
  passive-interface default
  no passive-interface G0/0                ! Active Link to R1
```

**Verification:**

```
show ip ospf neighbor
show ip route ospf
```

## 4.2.4 Network Address Translation (**NAT**)

**Overview:**




NAT allows private IP addresses to be translated to public addresses.

- **Static NAT** for one-to-one mappings (e.g., servers).
- **PAT** (overload) for many-to-one dynamic translations (Internet access).

**Configuration:**

```
! Define inside/outside interfaces
interface S0/0/0
  ip nat outside
interface G0/1
  ip nat inside

! Static NAT for a server
ip nat inside source static 192.168.11.10 203.0.113.11

! PAT for all internal networks
access-list 10 permit 192.168.10.0 0.0.0.255
ip nat inside source list 10 interface GigabitEthernet0/1 overload
```

**Verification:**

```
show ip nat statistics
show ip nat
```

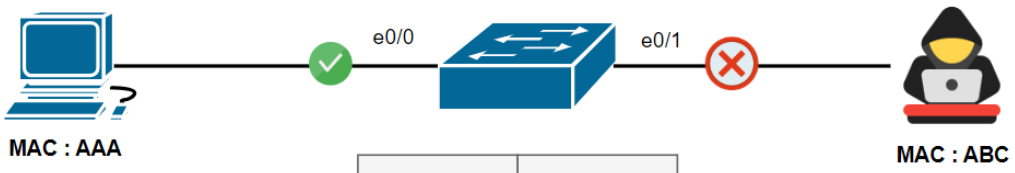
## 4.3 Security Implementation (Layer 2 & Layer 3)

This section will document all the **security technologies** you applied to protect your network, including:

---

### 4.3.1 Port Security

**Overview:**




| Port | Allowed MAC |
|---|---|
| e0/0 | AAA |
| e0/1 | BBB |

- Port Security restricts access to the switch ports based on MAC addresses, protecting against unauthorized devices.

**Configuration Steps:**

- Set port as an access port.
- Enable port security.
- Define maximum MAC addresses.
- Specify violation mode (protect, restrict, or shutdown).

**Configuration:**

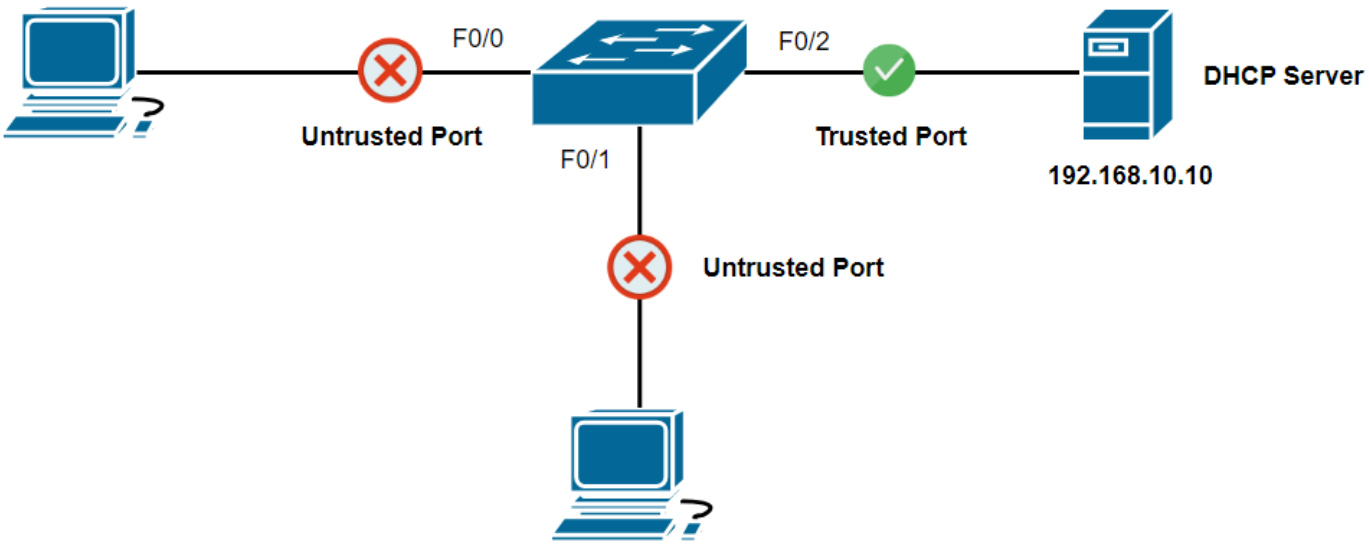
```
interface range e0/1 - 24
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation restrict
 switchport port-security mac-address sticky
```

**Verification:**

```
show port-security
show port-security interface e0/1
```

## 4.3.2 DHCP Snooping

**Overview:**




- DHCP Snooping prevents rogue DHCP servers from offering IP addresses on the network.
- To protect the network from rogue DHCP servers.

**Configuration Steps:**

- Enable DHCP snooping globally.
- Enable it on specific VLANs.
- Trust ports connected to authorized DHCP servers.

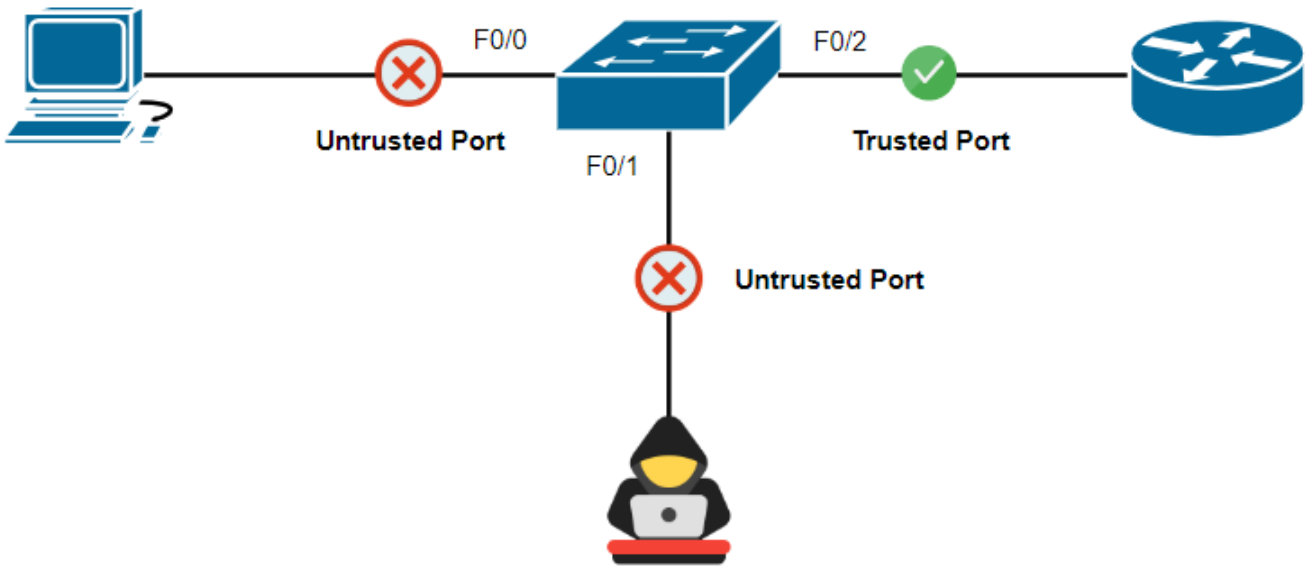
```
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40,50


interface F0/2
 ip dhcp snooping trust


interface range F0/0 - 1
 ip dhcp snooping limit rate 10
```

**Verification:**

```
Show ip dhcp snooping
```

## 4.3.3 Dynamic ARP Inspection (**DAI**)

**Overview:**




- DAI protects against ARP spoofing attacks by validating ARP packets based on DHCP snooping binding table.
- To prevent ARP spoofing attacks.

**Configuration Steps:**

- Enable DAI globally and per VLAN.
- Trust ports manually

**Configuration:**

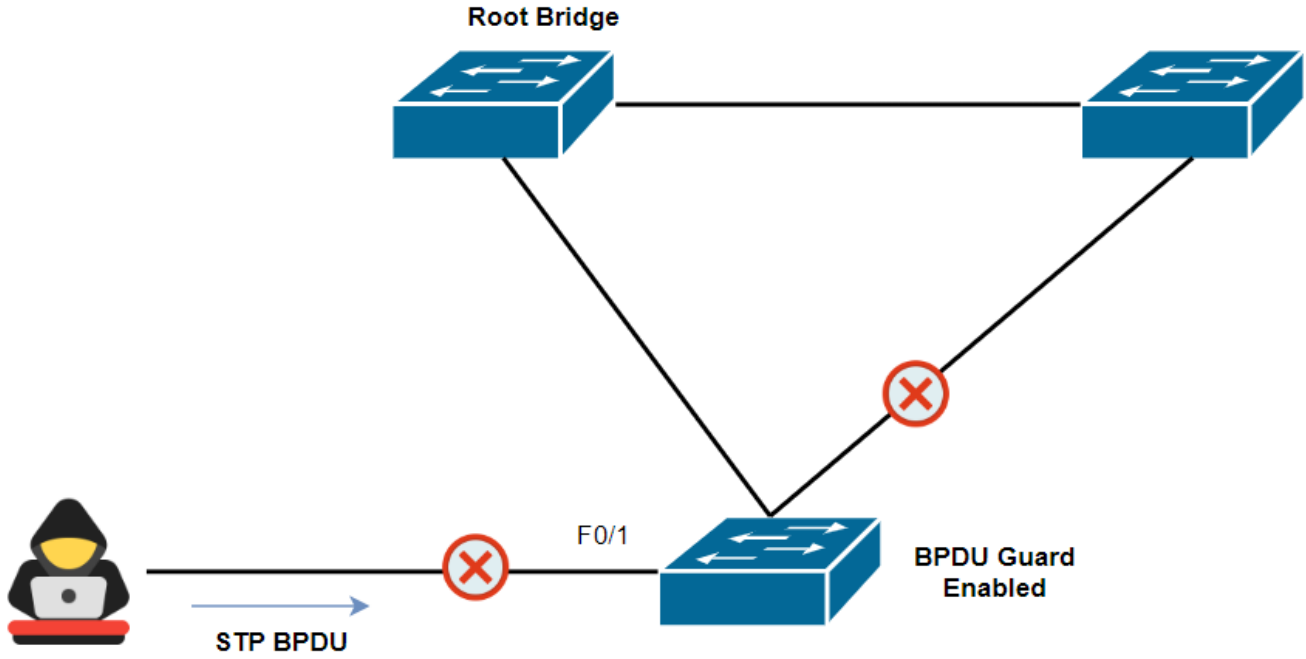
```
ip arp inspection vlan 10,20,30,40,50


interface F0/1
 ip arp inspection trust
```

**Verification:**

```
show ip arp inspection
show ip arp inspection statistics
```

## 4.3.4 BPDU Guard

**Overview:**




- Configure and verify BPDU Guard to protect edge ports from receiving unexpected BPDUs, preventing potential Layer 2 topology changes or STP attacks.
- This ensures network stability by disabling ports that receive unauthorized bridge protocol data units.

**Configuration Steps:**

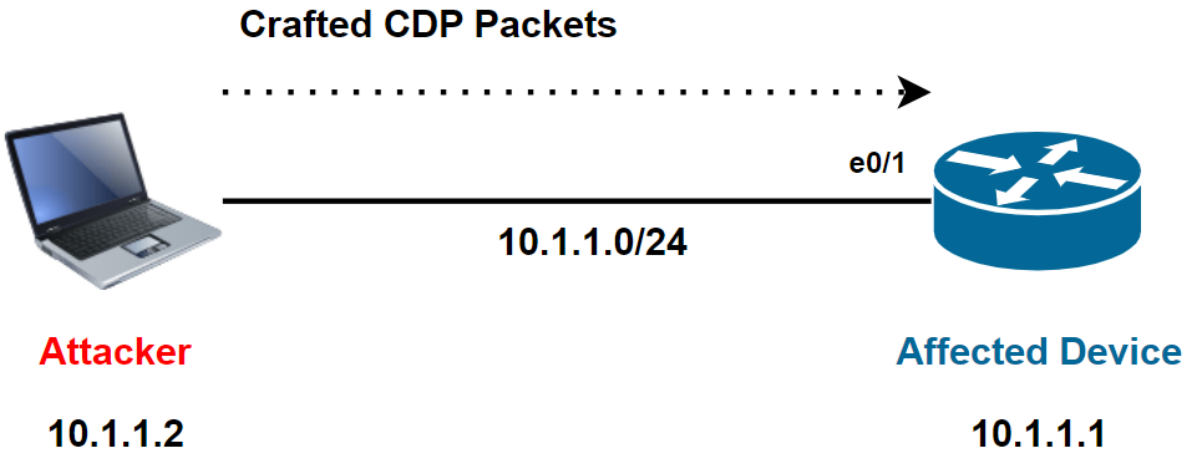
```
interface FastEthernet0/1
 spanning-tree portfast default
 spanning-tree portfast bpduguard default
```

**Verification:**

```
show running-config | begin span
show spaning-tree summary
```

## 4.3.5 CDP Mitigation

**Objective:**




- Disable CDP on unnecessary or user-facing interfaces to prevent information disclosure and network mapping.
- This protects the network from CDP-based reconnaissance attacks and limits visibility of device details like IP, platform, and ports.

**Configuration Steps:**

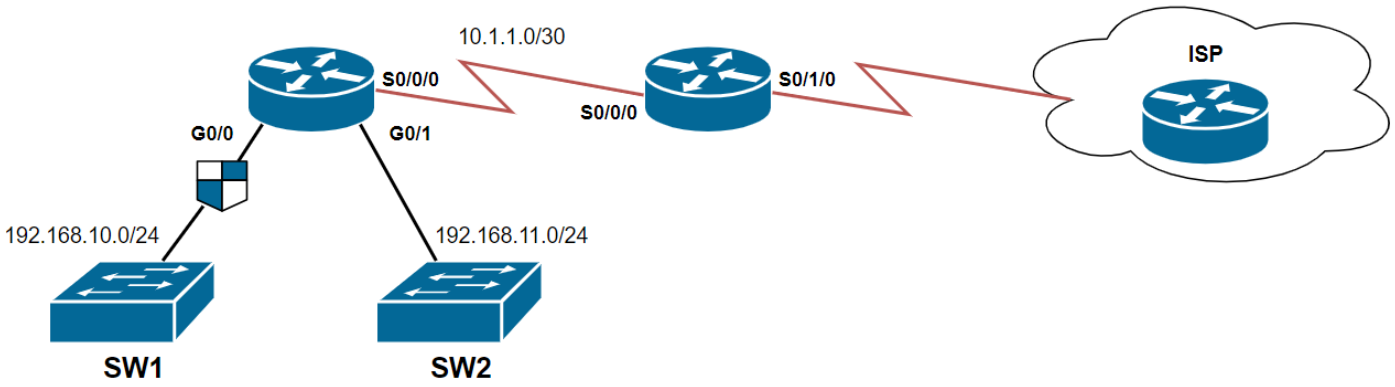
```
interface e0/1
  no cdp enable

! Globally Disable CDP
  no cdp run
```

**Verification:**

```
show cdp interface

! Globally Disable CDP
show cdp
```

## 4.3.6 Access Control Lists (**ACLs**)

**Overview:**




- ACLs are used to filter and control traffic between VLANs, and between LAN and WAN.
- To filter and control traffic flow based on IP addresses and protocols.

**Types Used:**

- Standard ACLs (based on source IP)
- Extended ACLs (based on source/destination IP and protocol)

**Configuration Steps:**

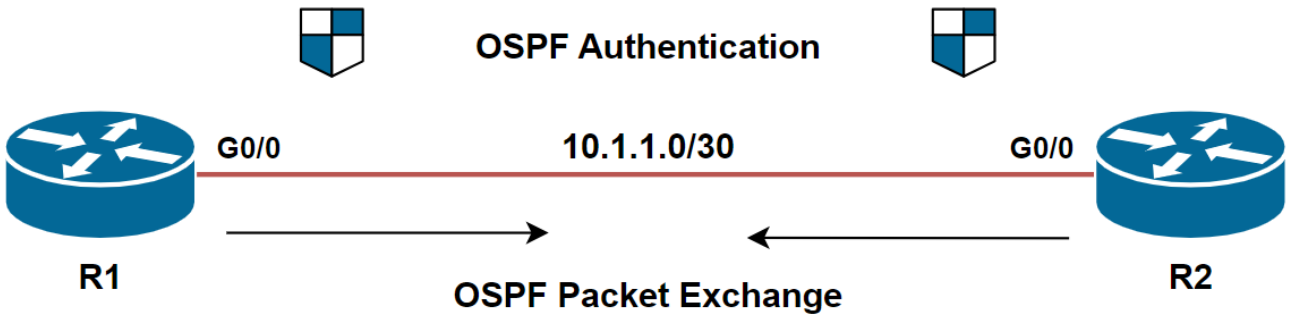
```
! Extended ACL
ip access-list extended SURFING
   permit tcp 192.168.10.0 0.0.0.255 any eq 80
   permit tcp 192.168.10.0 0.0.0.255 any eq 443
interface G0/0
   ip access-group SURFING in
```

**Verification:**

```
show access-lists
show ip interface G0/0
```

## 4.3.7 OSPF Authentication

**Objective:**




- Enable OSPF authentication to protect routing updates from tampering or spoofing.
- This ensures only trusted routers with the correct key can participate in OSPF neighbor relationships.

**Configuration Steps:**

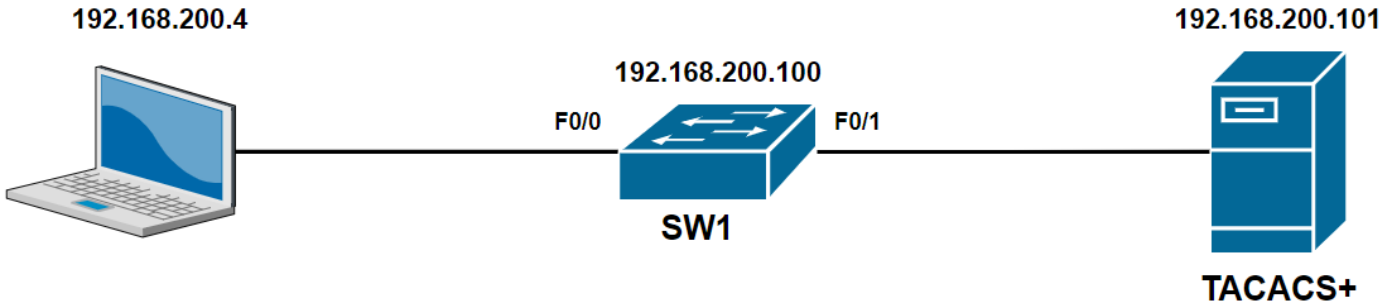
```
interface G0/0
   ip ospf message-digest-key 1 md5 DEPI
   ip ospf authentication message-digest

router ospf 1
   network 10.1.1.0 0.0.0.3 area 0
   area 0 authentication message-digest
```

**Verification:**

```
show ip ospf interface G0/0
show ip ospf neighbor
```

## 4.3.8 AAA (**TACACS+**) & Secure Remote Access (**SSH**)

**Objective:**




- Implement centralized user authentication, authorization, and accounting using TACACS+ to enhance security and maintain audit trails across network devices.

**Configuration Steps:**

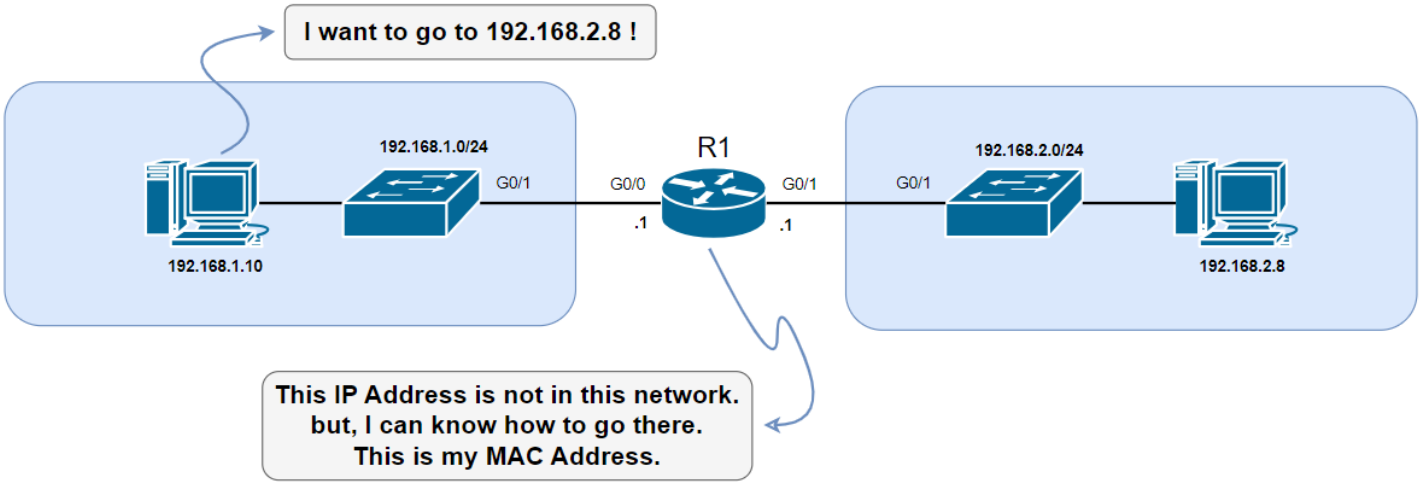
```
aaa new-model
tacacs-server host 192.168.200.101 key DEPI
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+

hostname SW1
ip domain-name SW1
crypto key generate rsa general-keys modulus 1024
ip ssh version 2

line vty 0 2
login authentication default
transport input ssh
```

**Verification:**

```
show ip ssh
show users
```

## 4.3.9 Proxy ARP Configuration & Verification

**Objective:**




- Proxy ARP is used when a router responds to ARP requests on behalf of another device, allowing devices in different subnets to communicate without the need for a router to change their IP addresses.
- This technique is commonly used when devices are not aware of the routers between them.

**Configuration Steps:**

```
interface GigabitEthernet0/1
ip proxy-arp
```

**Verification:**

```
show running-config interface G0/1
```

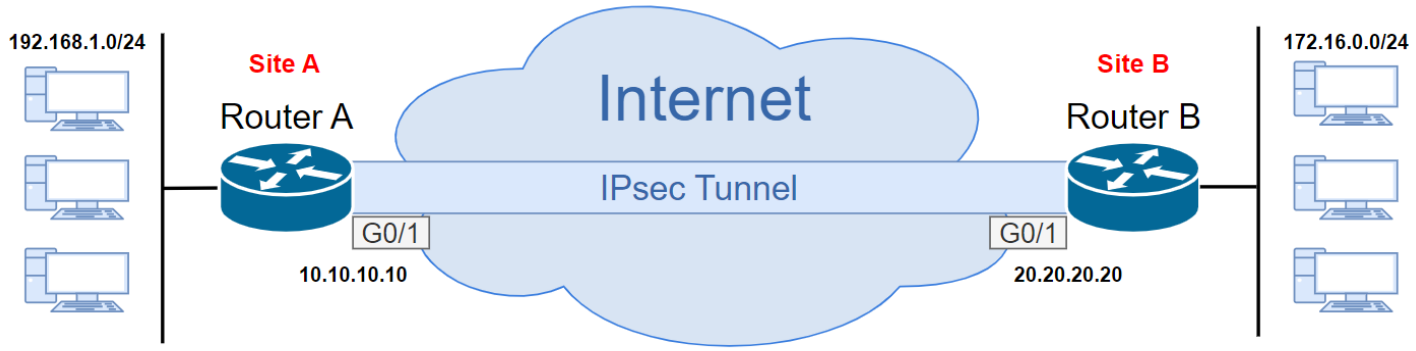
---

## 4.4 VPN Implementation

This section covers how we securely connect remote branches to the headquarters using **Site-to-Site VPN tunnels** over the Internet.

---

### 4.4.1 VPN Overview




#### 4.4.1.1 VPN Type

- **Site-to-Site VPN:** Connects entire networks across locations.
- **Remote Access VPN:** Connects individual users securely to the network.
- **SSL VPN:** Uses HTTPS for secure access, typically via a browser.
- **IPsec VPN:** Most commonly used for encrypted, site-to-site tunnels.

---

#### 4.4.1.2 VPN Tunnel Configuration Summary

- **Peer IP Address:** Remote router/firewall address.
- **IKE Phase 1 & 2 Parameters:** Encryption, hashing, DH group, lifetime.
- **IPsec Policies:** Transform sets (ESP, AES, SHA), access lists.
- **Tunnel Interface:** Defines the virtual interface and routing.

---

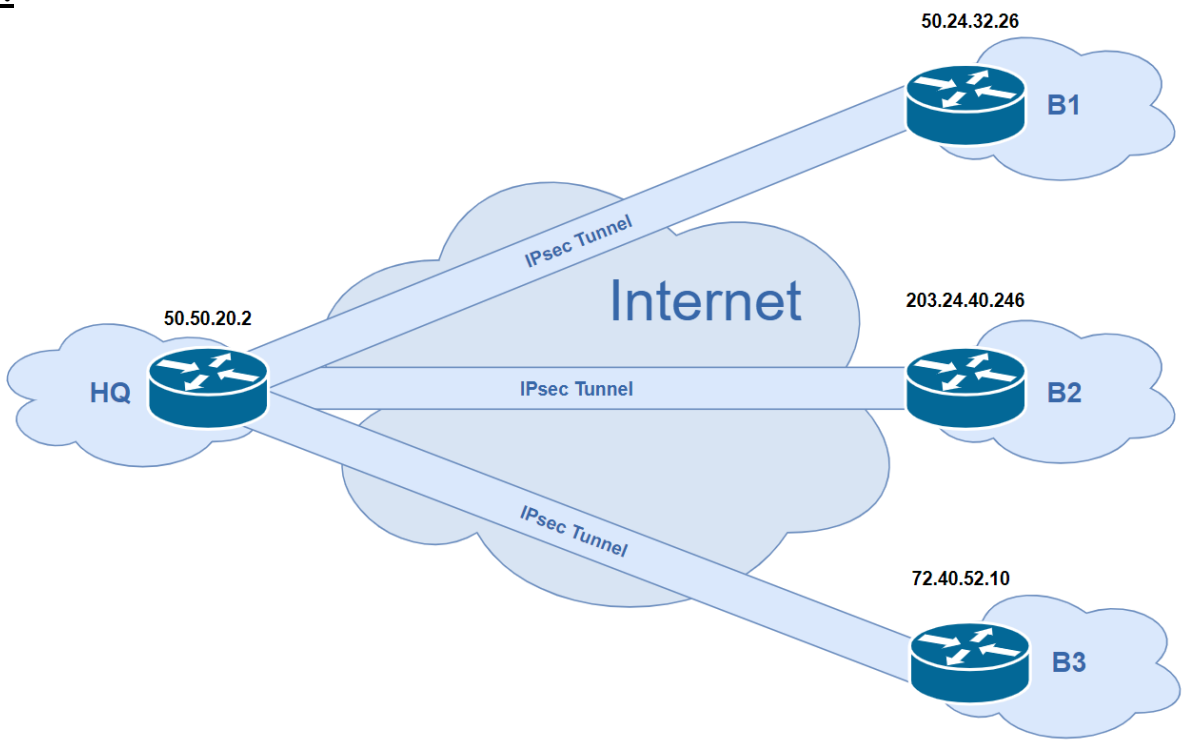
#### 4.4.1.3 VPN Security Measures

- Use strong encryption algorithms (AES-256, SHA-256).
- Apply authentication (Pre-Shared Key or digital certificates).
- Use ACLs to control which traffic is tunneled.
- Regularly update keys and tunnel settings.

---

## 4.4.2 Site-to-Site VPN Overview

**Objective:**




- A Site-to-Site VPN creates a secure connection between two or more locations, typically between head office and branch offices.
- Traffic between networks is encrypted and routed securely, making it appear as a single private network.

---

### 4.4.2.1 VPN Tunnel Configuration Summary

| VPN Endpoint | Remote Peer IP | Encryption | Authentication | Tunnel Type |
|---|---|---|---|---|
| HQ to Branch 1 | 50.24.32.26 | AES-256 | Pre-shared key | IPsec Tunnel |
| HQ to Branch 2 | 200.24.40.246 | AES-256 | Pre-shared key | IPsec Tunnel |
| HQ to Branch 3 | 72.40.52.10 | AES-256 | Pre-shared key | IPsec Tunnel |

---

### 4.4.2.2 Technologies Used

- IPsec Phase 1 (IKEv1 Policy)
- IPsec Phase 2 (Transform Set and Crypto Map)
- Pre-Shared Keys (PSK) Authentication
- Static Routing over VPN

---

### 4.4.3 VPN Configurations Steps

- **Define ISAKMP/IKE Phase 1 Policy**
  - Define encryption, hashing, authentication method, and Diffie-Hellman group.

    Example:

```
crypto isakmp policy 10
 encr aes
 hash sha
 authentication pre-share
 group 2
 lifetime 86400
```

- **Define Pre-shared Key**
  - Set a shared key for peer authentication.

    Example:

```
crypto isakmp key MY_SECRET_KEY address <peer-ip-address>
```

- **Configure IPsec Phase 2 Transform Set**
  - Define encryption and integrity methods used in IPsec tunnel.

    Example:

```
crypto ipsec transform-set Branch esp-aes esp-sha-hmac
```

- **Configure IPsec Phase 2 Transform Set**
  - Specify which traffic should be encrypted over the VPN.

    Example:

```
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

➢ **Create Crypto Map**

- Bind IPsec settings to the crypto map and link to the access list.

  Example:

```
crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
 set peer <peer-ip-address>
 set transform-set MY_TRANSFORM_SET
 match address 110
```

➢ **Bind Crypto Map to WAN Interface**

- Apply the crypto map to the outbound interface.

  Example:

```
interface GigabitEthernet0/0
 crypto map MY_CRYPTO_MAP
```

---

### 4.4.4 VPN Verification Commands

- Check tunnel status:

```
show crypto isakmp sa
show crypto ipsec sa
```

- Debugging if needed:

```
debug crypto isakmp
debug crypto ipsec
```

---

### 4.4.5 Security Measures for VPN

- Strong encryption algorithms (AES 256)
- SHA hashing for integrity
- Pre-Shared Keys with complexity
- Lifetime and session monitoring
- ACL to limit interesting traffic only
- Logging VPN events

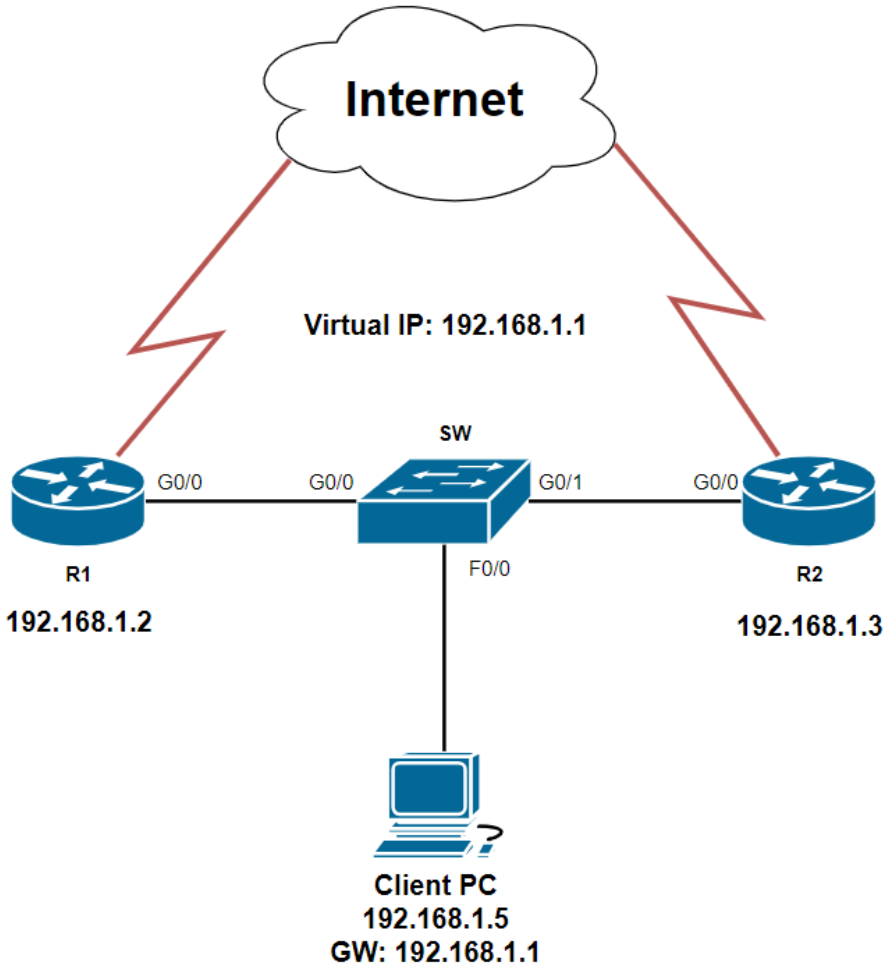
## 4.5 High Availability and Redundancy

In this section, we document the technologies that ensure **network reliability**, **failover capabilities**, and **link redundancy**.

---

### 4.5.1 HRSP (Hot Standby Router Protocol)

**Overview:**

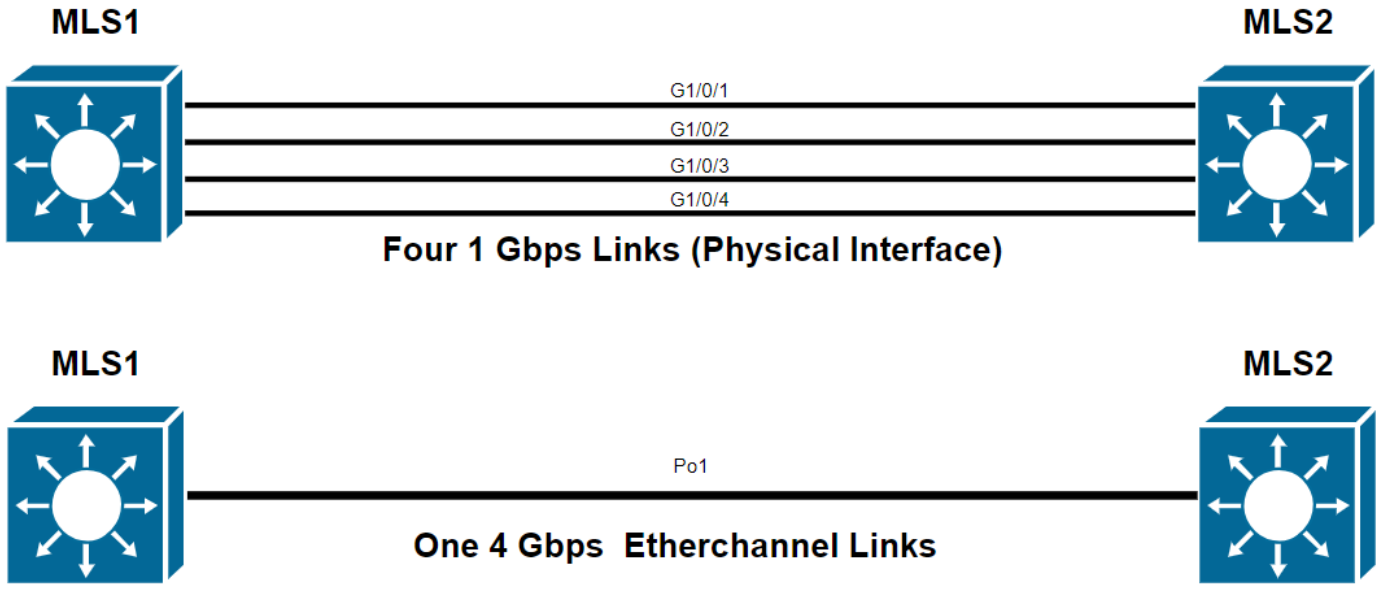



- HSRP provides a virtual IP address shared between two or more routers for gateway redundancy.
- If the active router fails, the standby router takes over seamlessly to maintain connectivity.

---

## 4.5.2 EtherChannel (Port Aggregation)

**Overview:**

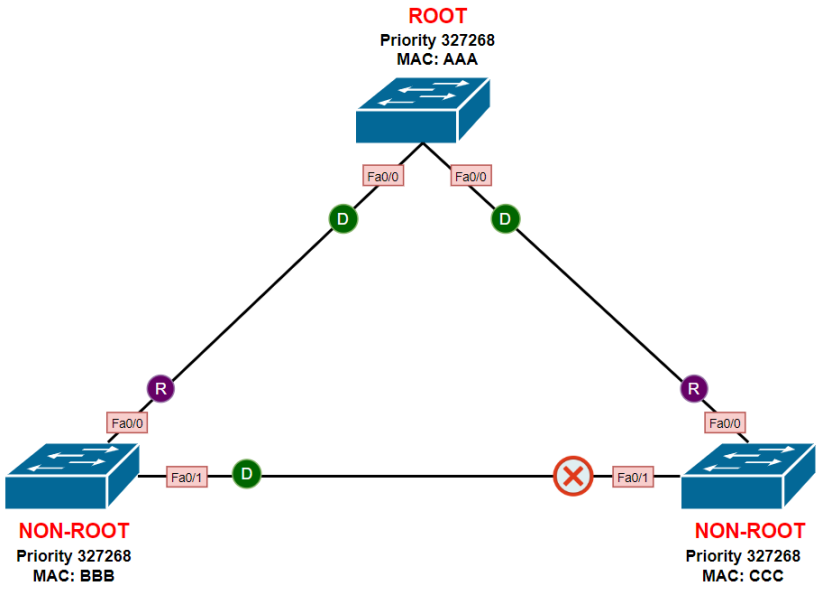



- EtherChannel groups multiple physical links into one logical link for increased bandwidth and redundancy.
- If one link fails, traffic continues to flow through the remaining active links without interruption.

---

## 4.5.3 Spanning Tree Protocol (Rapid-PVST)

**Overview:**

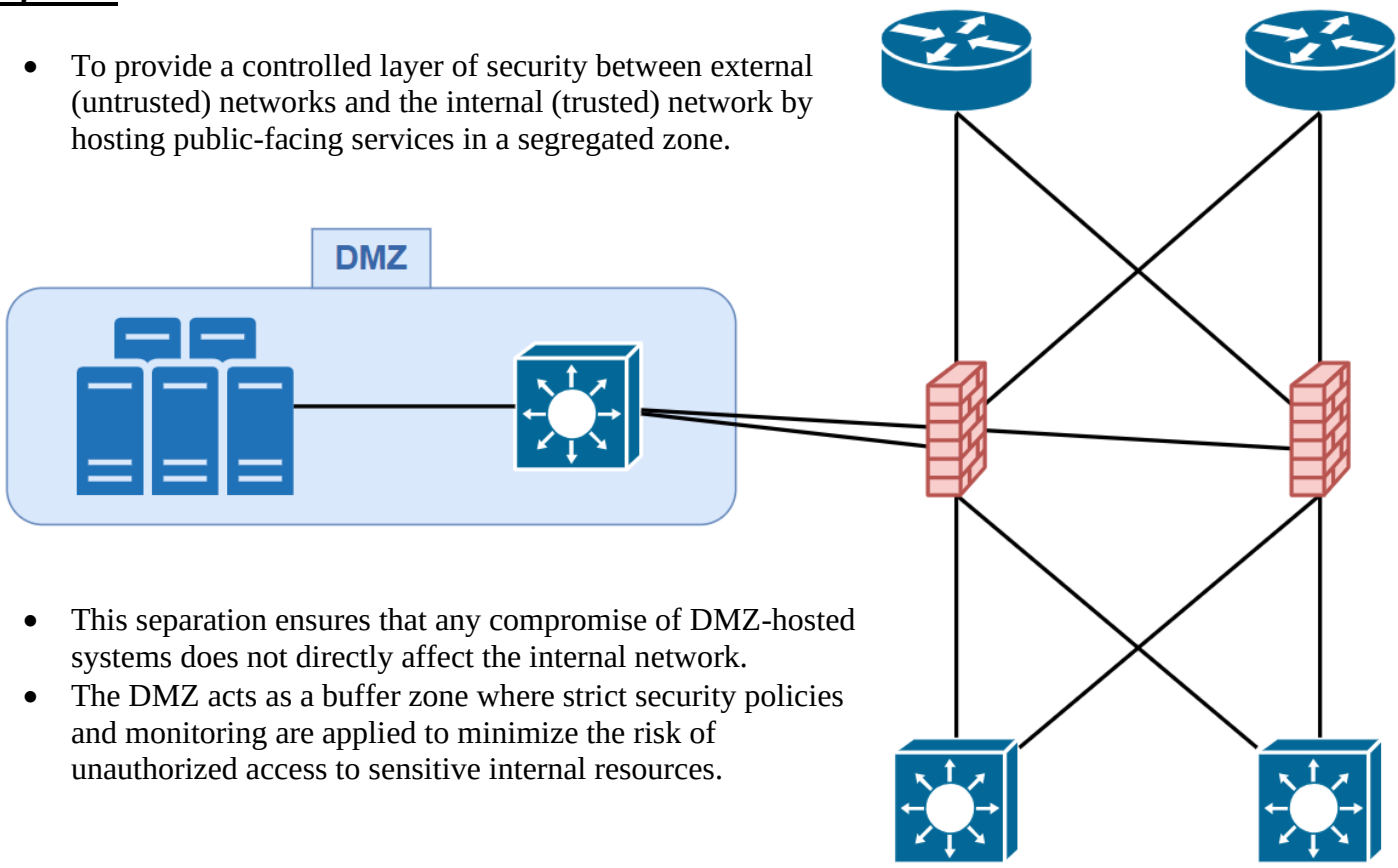



- EtherChannel groups multiple physical links into one logical link for increased bandwidth and redundancy.
- If one link fails, traffic continues to flow through the remaining active links without interruption.

## 4.6 DMZ (**Demilitarized Zone**) – Detailed Overview

**Objective:**

- To provide a controlled layer of security between external (untrusted) networks and the internal (trusted) network by hosting public-facing services in a segregated zone.




- This separation ensures that any compromise of DMZ-hosted systems does not directly affect the internal network.
- The DMZ acts as a buffer zone where strict security policies and monitoring are applied to minimize the risk of unauthorized access to sensitive internal resources.

---

### 4.6.1 What is a DMZ?

- A DMZ is a physical or logical subnetwork that contains and exposes an organization's external-facing services (like web servers, email servers, DNS, etc.) to the internet.
- It acts as a buffer zone between the internet and the internal LAN.

---

### 4.6.2 Services Commonly Placed in the DMZ

- Web Server (HTTP/HTTPS)
- Mail Server (SMTP)
- DNS Server
- DHCP Server
- NTP Server
- Syslog Server
- FTP Servers
- AAA Server

---

### 4.6.3 Traffic Flow Rules

- Inbound from Internet → DMZ: Allowed (with restrictions)
- DMZ → Internal LAN: Denied or highly restricted
- Internal LAN → DMZ: Allowed (to manage servers)
- DMZ → Internet: Allowed (for updates, etc.)

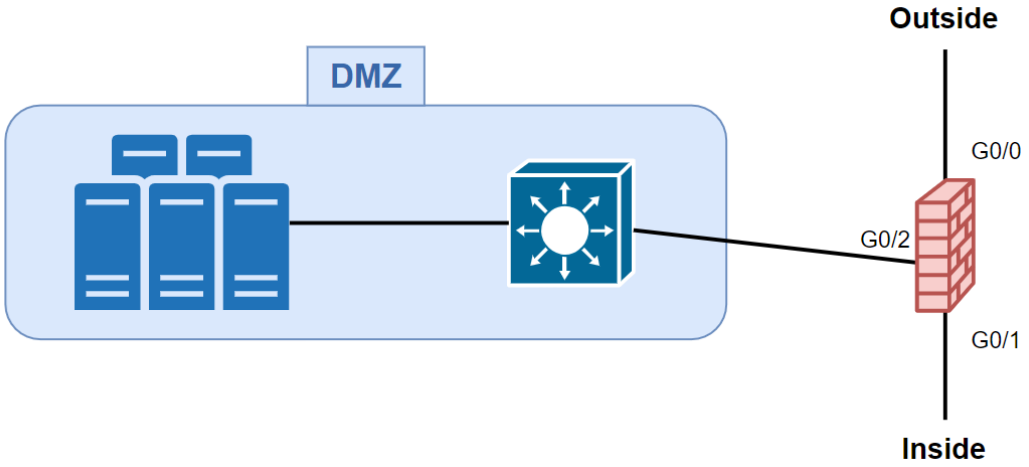
---

### 4.6.4 Security Measures for the DMZ

- Use stateful firewalls or NGFWs to inspect traffic.
- Apply strict ACLs or Zone-Based Policies.
- Use IPS/IDS to detect intrusions in the DMZ.
- Regularly patch and monitor DMZ systems.
- Use proxy servers and reverse proxies when needed.

---

### 4.6.5 Implementation Example (**CISCO ASA**)




```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
```

```
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

```
interface GigabitEthernet0/2
 nameif dmz
 security-level 50
 ip address 172.16.1.1 255.255.255.0
```

```
access-list dmz_in extended permit tcp any host 172.16.1.10 eq 80
access-group dmz_in in interface dmz
```

## 4.7 Network Monitoring and Troubleshooting Procedures

This section details the procedures and tools used to monitor the network's performance and troubleshoot any arising issues proactively.

---

### 4.7.1 Network Monitoring Techniques

**Objective:**

- To ensure network health and detect anomalies early through proactive monitoring solutions.

**Tools and Technologies Used:**

- **Syslog:** Centralized logging system for network devices.
- **NTP:** Time sync for accurate device logs.

---

### 4.7.2 Syslog Configuration

**Purpose:**


- To send system logs from network devices to a centralized Syslog server for storage and analysis.

**Configuration:**

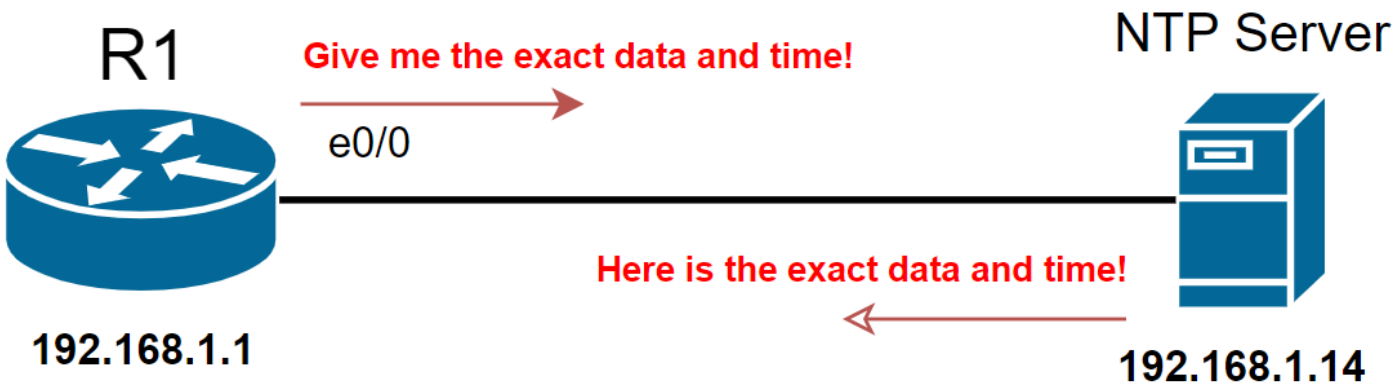
```
logging host 192.168.1.10
logging trap informational
service timestamps log datetime msec
```

**Verification:**

```
show logging
```

## 4.7.3 NTP Configuration

**Purpose:**




- Ensure all network devices maintain synchronized and accurate time.

**Configuration:**

```
ntp authentication-key 123 md5 cisco
ntp authenticate
ntp trusted-key 123
ntp server 195.1.1.8
```

**Verification:**

```
show ntp status
show ntp associations
```

---

## 4.7.4 Troubleshooting Commands

**Core Commands Used for Troubleshooting:**

| Purpose | Command |
|---|---|
| Verify interfaces | show ip interface brief |
| Verify VLANs | show vlan brief |
| Verify trunk ports | show interfaces trunk |
| Verify EtherChannel | show etherchannel summary |
| Verify STP states | show spanning-tree |

| Purpose | Command |
|---|---|
| Verify HSRP status | show standby |
| Verify routing table | show ip route |
| Verify OSPF neighbors | show ip ospf neighbor |
| Verify OSPF interfaces | show ip ospf interface |
| Verify static/dynamic routes | show running-config |
| Verify ARP entries | show ip arp |
| Check MAC address table | show mac address-table |
| Verify default gateway | show ip default-gateway |
| Check CDP neighbors | show cdp neighbors |
| Check NAT translations | show ip nat translations |
| Verify ACLs | show access-lists |
| Verify DHCP bindings | show ip dhcp binding |
| Check interface errors | show interfaces |
| Verify NTP status | show ntp status |
| Verify syslog configuration | show logging |
| Verify VPN tunnels | show crypto ipsec sa / show crypto isakmp sa |
| Debug VPN negotiation | debug crypto isakmp / debug crypto ipsec |

# 5. Security Policies

This section outlines the procedures, tools, and best practices implemented to secure the network infrastructure, protect against unauthorized access, and ensure the integrity of data and services across the network.

---

## 5.1 VLAN Security

- **Port Security**
  - Limit the number of MAC addresses per port (sticky MAC).
  - Automatically shutdown ports on violation.
  - Prevent unauthorized devices from connecting to the network.
- **BPDU Guard & Root Guard**
  - Enable BPDU Guard on access ports to prevent rogue switches.
  - Enable Root Guard on trunk ports to maintain the STP root bridge integrity.
- **Unused Ports**
  - Disable unused ports and assign them to an unused VLAN (e.g., VLAN 999).

---

## 5.2 Access Control Lists (ACLs)

- **Inter-VLAN ACLs**
  - Only allow necessary communication between VLANs.
  - Deny unnecessary traffic between user VLANs and DMZ.
- **Internet ACLs**
  - Allow only specific traffic to and from the Internet.
  - Block all unnecessary inbound traffic to protect internal resources.
- **VPN ACLs**
  - Allow only branch office subnets to communicate over VPN.
  - Deny all other traffic for enhanced VPN security.

---

## 5.3 Authentication & Management Security

- **SSH Access**
  - Secure remote device management via SSH (disable Telnet).
  - Use strong username/password combinations.

- **AAA (Authentication, Authorization, Accounting)**
    - Centralize user authentication using RADIUS or TACACS+ servers.
    - Log all administrative access for accountability.
- **Syslog Servers**
    - Forward logs from all critical devices to centralized Syslog servers.
- **NTP Servers**
    - Synchronize clocks across network devices for accurate logging and event correlation.

---

## 5.4 Firewall Policies

- **Inbound & Outbound Rules**
    - Inspect and filter incoming and outgoing traffic based on applications, ports, and protocols to block unauthorized access and ensure network security, while preventing attacks and controlling traffic flow.
- **DMZ Security**
    - Public servers (Web, FTP, DNS , etc..) placed in DMZ zone.
    - Strict firewall rules to isolate DMZ from internal network.
- **NAT/PAT Policies**
    - Hide internal IP addressing using NAT Overload for Internet traffic.
    - Static NAT for DMZ servers requiring external access.
- **Intrusion Prevention (IPS/IDS)**
    - Detect and block malicious traffic patterns.
    - Log security events for auditing and review.

---

# 6. Backup and Redundancy Strategy

## 6.1 Device Configuration Backup

- **Automated Scheduled Backups**
  - Set up scheduled backups for all critical network devices (switches, routers, firewalls).
  - Backup destinations: Secure FTP (SFTP) or TFTP servers.
- **Backup Policies**
  - Keep at least 3 versions of the latest configuration.
  - Store backups both locally (on-premises) and in secure cloud storage.
  - Encrypt configuration backups to prevent unauthorized access.
- **Manual Backup Before Major Changes**
  - Perform a manual backup before applying any critical updates or changes.

---

## 6.2 Redundancy Measures

- **Network Redundancy**
  - **HSRP** (Hot Standby Router Protocol) configured between core devices for default gateway redundancy.
  - **EtherChannel** aggregation provides redundancy at Layer-2 for important uplinks.
- **Internet Redundancy**
  - Dual WAN links at HQ using two different ISPs (future expansion plan).
- **Power Redundancy**
  - Critical devices connected to UPS (Uninterruptible Power Supplies).
  - Redundant power supplies (RPS) for key switches and firewalls.
- **Server Redundancy**
  - Internal servers (e.g., DHCP, DNS) designed with failover capabilities.

# 7. Maintenance and Troubleshooting Procedures

## 7.1 Regular Maintenance Activities

- **Firmware and IOS Updates**
  - Maintain latest stable firmware versions on network devices.
  - Schedule updates during off-peak hours to minimize downtime.
- **Device Health Monitoring**
  - Monitor CPU, memory, and interface statuses regularly.
  - Utilize SNMPv3 and NMS (Network Monitoring System) for real-time alerts.
- **Log Management**
  - Periodically review Syslog messages for anomalies.
  - Configure automatic log rotation and archival.
- **Security Patch Management**
  - Apply security patches promptly based on vendor advisories.

---

## 7.2 Troubleshooting Workflow

- **Network Troubleshooting Steps**
  1. **Identify the Problem**
     - Use ping, traceroute, and show commands to localize the issue.
  2. **Gather Information**
     - Check device logs, interface statuses, VPN tunnels, and routing tables.
  3. **Isolate the Fault**
     - Determine if the issue is with Layer-1 (cabling), Layer-2 (switching), or Layer-3 (routing).
  4. **Implement a Fix**
     - Apply corrective actions (restart interfaces, reroute traffic, reestablish tunnels).
  5. **Test and Validate**
     - Confirm the solution resolved the issue and no new problems occurred.
  6. **Document the Incident**
     - Log all troubleshooting steps and outcomes for future reference.