Ministry of Communications and Information Technology

Digital Egypt Pioneers Initiative

Final Project Report

Design and Implement of MAY international school network with 2 branches

Made By:

- **Alaa Hassan Ali Melook**
- **Aya Tarek Ali**
- **Mai Eltaher Abobakr Sroor**
- **Mohamed Taher Abdelquader**
- **Yumna Medhat Anter**

Supervisors: ENG: WAEL SAMIR

Table of Contents

Abstract

In the modern educational environment, advanced networks are the foundation for the success of any institution. By providing efficient and reliable communication between devices and users, networks allow schools to deliver educational services more effectively while ensuring the protection of sensitive data and information. This project aims to design and implement an integrated and advanced network for MAY International School, a two-branch institution, meeting its current needs while allowing for future expansion.

The project will involve a detailed analysis of the school's requirements in terms of connected devices and the number of users, ensuring the design of a flexible network that fulfills these needs. Key technologies will be implemented to safeguard the network from cyber threats, ensuring a secure learning environment across both branches.

Additionally, the new network will provide high-speed connectivity between different departments and classrooms, enhancing the ease of data and resource sharing among teachers, students, and staff. Network monitoring systems will be deployed to ensure continuous efficiency and to detect and resolve any issues quickly.

Through this project, we aim to establish a fully integrated technical environment that boosts the educational experience, minimizes system downtime, and provides the necessary infrastructure for future growth. Building a strong and secure network is a crucial step in enabling MAY International School to achieve its educational goals and thrive in a fast-evolving digital world.

List of Figures

List of Tables

project Specification

The project aims to design and develop an integrated network for MAY International School, a two-branch institution, providing secure and efficient communication across both branches' departments and classrooms. This network will include connections between computers, printers, servers, and secure internet access, utilizing modern security technologies to protect students' and staff's data and ensure a safe learning environment.

The network design will incorporate several key elements to ensure scalability, efficiency, and security:

1. Topology, IP addressing, subnetting, and basic configuration will form the foundation of the network's structure.
2. OSPF and static routing will be implemented for dynamic and static route management, ensuring reliable data traffic flow.
3. HSRP (Hot Standby Router Protocol) will provide redundancy, minimizing downtime and maintaining high availability.
4. Ethernet channel technology will be used to enhance bandwidth and reliability between switches.
5. Inter VLAN routing will segregate network traffic to enhance performance and security across different departments.
6. DHCP relay agent will handle IP address allocation dynamically for efficient device management.

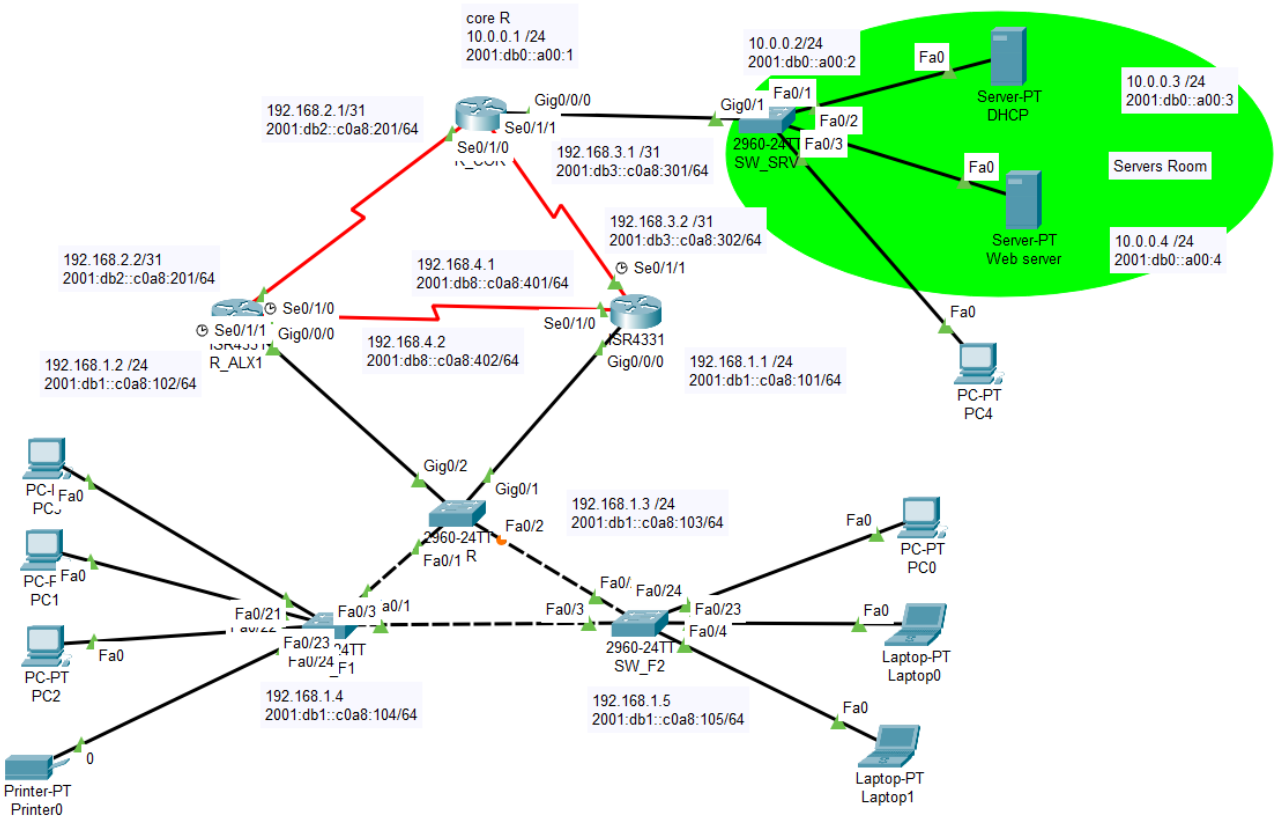
- **To secure the network:**
  7. Access Control Lists (ACLs) will be deployed to manage traffic and secure internal communications.
  8. Advanced security measures, including SSH, VLAN security, STP security, Switch security, Port security, and DHCP security, will safeguard against unauthorized access and threats.
  9. Additional services like DNS, web servers, Syslog, and NTP will ensure smooth network operations and time synchronization across the infrastructure.

- **The project will also include:**

- A detailed report and presentation to document the network design, configuration, and security policies.

This comprehensive network solution will provide the company with a robust, scalable infrastructure, supporting growth and ensuring business continuity with a high level of security and performance.

Figure1: The first implementation for network (primary designs)



week	Work
1	Topology, network requirement, subnetting
2	VLANs and Inter-VLAN Routing and Network Security Implementation, OSPF
3	HSRP, EtherChannel, DHCP, ACL
4	Final Testing and Reporting, troubleshooting, Servers

Table 1 Week work

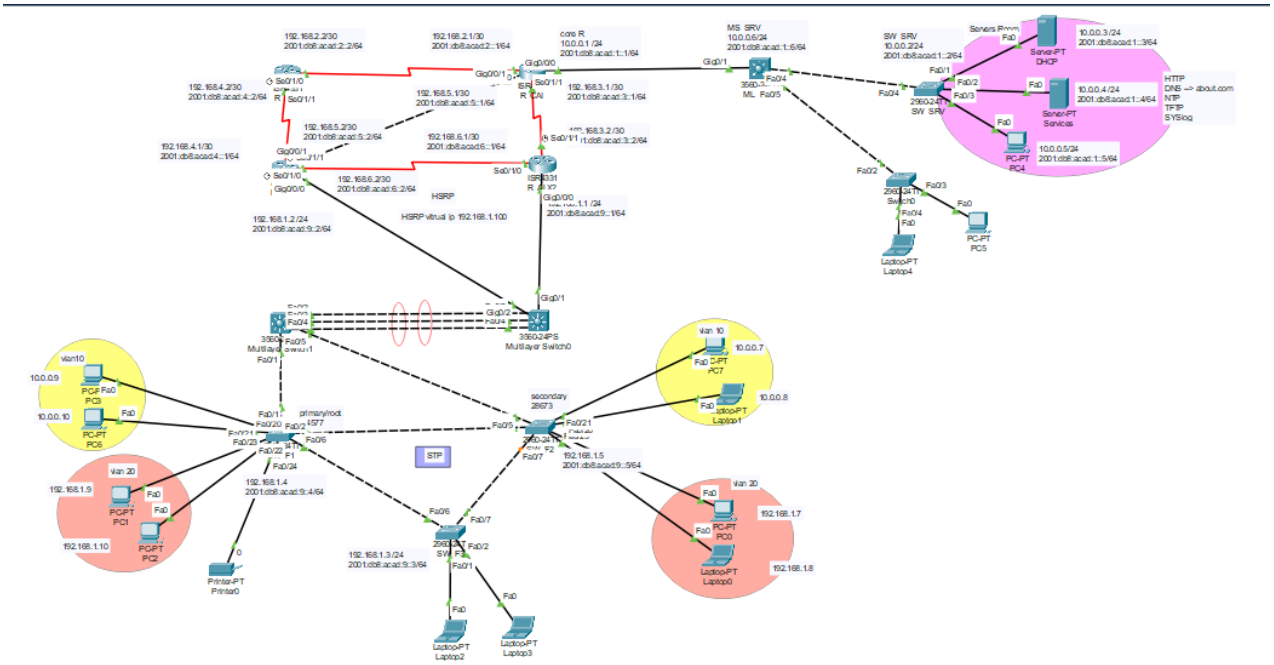
- Alaa Hassan Ali Melook
  - ACL, DNS, webserver, Sys log, NTP
- Aya Tarek Ali
  - OSPF , static routing - HSRP
- Mai Eltaher Abobakr Sroor
  - Security
    - Vlan security
    - STP security
    - Switch security
    - Port security
    - DHCP security
- Mohamed Taher Abdelquader
  - Topology, Ip, subnetting, basic configuration, STP ,relay agent , ssh
- Yumna medhat
  - ethernet channel, vlan

Part 1: Topology, Ip, subnetting, basic configuration

1.1 Topology and Ips

The network topology for this project is designed to support efficient communication across all departments within the company while ensuring scalability, Fault tolerance and security. The chosen topology allows for easy troubleshooting and centralized management.

FIG1.1 TOPOLOGY



Network Devices and Layout

- 5 switches
- 3 multi-layer switches
- 4 routers
- 2 servers
- End: Pcs & laptops vary

The following devices have been selected for the network:

- **Routers**: Two routers will handle interdepartmental communication and provide external internet access.
- **Multilayer Switches**: Deployed at the distribution layer, these switches facilitate both Layer 2 switching and Layer 3 routing, enabling efficient inter-VLAN routing while minimizing the need for additional routing devices.
- **Switches**: Additional Layer 2 switches will be used in the access layer to connect end devices within each department, ensuring high-speed connectivity for the department's devices.
- **Servers**: Centralized servers for DNS, DHCP, NTP, and web services will be placed in the core of the network.
- **End Devices**: Employee PCs, printers, and other peripherals are connected through the access layer switches.

IP Addressing Plan

The IP addressing scheme uses the private IP. Each department is assigned its own subnet to ensure proper segmentation and to simplify the management of network traffic. Subnetting is used to efficiently allocate IP addresses and optimize routing performance.

The gateway for each subnet will be the first IP address in each range (e.g., 192.168.1.1). The rest of the IP addresses will be allocated dynamically through the DHCP server for employee devices, with some reserved for critical devices such as routers, switches, and servers.

R_CAI	G/0/0/0 10.0.0.1 /24 2001:db8:acad:1::1/64	G/0/0/1 192.168.5.1/30 2001:db8:acad:5::1/64	S0/1/1 192.168.3.1/30 2001:db8:acad:3::1/64	S0/1/0 192.168.2.1/30 2001:db8:acad:2::1/64
R_BCP			S0/1/1 192.168.4.2/30 2001:db8:acad:4::2/64	S0/1/0 192.168.2.2/30 2001:db8:acad:2::2/64
R_ALX2	G0/0/0 192.168.1.1 /24 2001:db8:acad:9::1/64		S0/1/1 192.168.3.2 /30 2001:db8:acad:3::2/64	S0/1/0 192.168.6.1/30 2001:db8:acad:6::1/64
R_ALX1	G0/0/0 192.168.1.2 /24 2001:db8:acad:9::2/64	G0/0/1 192.168.5.2 2001:db8:acad:5::2/64	S0/1/1 192.168.4.1/30 2001:db8:acad:4::1/64	S0/1/0 192.168.6.2/30 2001:db8:acad:6::2/64
ML_SRV	10.0.0.6/24 2001:db8:acad:1::6/64			
SW_SRV	10.0.0.2/24 2001:db8:acad:1::2/64			
SW_F3	192.168.1.3 /24 2001:db8:acad:9::3/64			
SW_F1	192.168.1.4 2001:db8:acad:9::4/64			
SW_F2	192.168.1.5 2001:db8:acad:9::5/64			
DHCP Server	10.0.0.3 /24 2001:db8:acad:1::3/64			
Services server	10.0.0.4 /24 2001:db8:acad:1::4/64	HTTP DNS --> about.com NTP TFTP SYSlog		

Table 1.1 Ip addressing

1.2 Basic Configurations

The basic configuration of the network devices is crucial for establishing secure and efficient communication within the company. This process involves setting up the routers and switches with necessary security measures, enabling remote access, and ensuring that the network operates smoothly. The following configuration steps are essential for achieving these goals:

Router Configuration:

- Assigned IPv4 and IPv6 addresses to interfaces, including serial and Gigabit interfaces, based on the subnet for the connected department.
- Configured passwords for **enable**, **console**, and **auxiliary** lines to secure access.
- Enabled SSH version 2 for secure remote access and configured a banner message for security and identification.
- Opened necessary ports and enabled remote access on VTY lines 0 to 4, setting passwords for secure access.

Switch Configuration:

- Assigned static IP addresses to the management interface of each switch.
- Configured a dedicated VLAN (e.g., VLAN 10) for management purposes, allowing centralized management of the switches and improving security.
- Configured passwords for **enable**, **console**, and **auxiliary** lines.
- Enabled SSH version 2 and configured a banner message.
- Opened necessary ports and configured additional VLANs to ensure proper segmentation of traffic within the switch network.

Testing Connectivity:

- Basic tests such as `PING & Tracert` between devices in different subnets are conducted to ensure interdepartmental connectivity.

Router Configuration Settings:

- **Enable Password**: `enpass`
- **Console Password**: `conpass`
- **Auxiliary Password**: `auxpass`
- **Domain Name**: `google.com`
- **Default Gateways**:
  - For the **10.0.0.0/24** network: `10.0.0.1`
  - For the **192.168.1.0/24** network: `192.168.1.1`
- **SSH Configuration**:
  - **Username**: `admin`
  - **SSH Password**: `sshpass`

Switch Configuration Settings:

- **Enable Password**: `enpass`
- **Console Password**: `conpass`
- **Auxiliary Password**: `auxpass`
- **SSH Configuration**:
  - **Username**: `admin`
  - **SSH Password**: `sshpass`

Part 2: OSPF and static routing

2.1. Overview of OSPF

In my network, I implemented **OSPF (Open Shortest Path First)** to ensure efficient routing and dynamic adaptation to network changes. OSPF is a link-state routing protocol that uses the **Dijkstra algorithm** to compute the shortest path between routers. It is designed for larger networks and operates within an **Autonomous System (AS)**.

2. Why Do We Need OSPF?

In large networks, static routing is not scalable due to the following reasons:

- Manual updates to routing tables are needed every time the topology changes.
- It lacks automatic adaptation to network changes, making it unreliable for high availability.
- **OSPF** addresses these challenges by:
    - Dynamically learning network routes and recalculating the best path whenever changes occur.
    - Supporting hierarchical design through **areas** that reduce the size of routing tables.
    - Enabling load balancing over multiple equal-cost paths.

How OSPF Works

- OSPF routers maintain an identical database of the network's topology.
- OSPF uses **link-state advertisements (LSAs)** to share information about network changes.
- Each router computes the best path to each destination in the network by constructing a **Shortest Path Tree (SPT)**.
- OSPF supports **Classless Inter-Domain Routing (CIDR)** and **Variable Length Subnet Masking (VLSM)**, making it flexible for large-scale networks.
- OSPF forms an **adjacency** with neighboring routers to share information about routes.

OSPF Network Types and Areas

- **OSPF Areas**: OSPF uses areas to scale efficiently in larger networks.
    - **Area 0**: Backbone area that interconnects all other areas.
    - **Non-backbone areas**: Other areas connect to Area 0 to simplify routing tables.
- **Network Types**:
    - **Broadcast**: Routers elect a **Designated Router (DR)** and a **Backup Designated Router (BDR)** to reduce OSPF traffic.
    - **Point-to-Point**: Direct communication between two routers.
    - **Non-broadcast**: Similar to broadcast but requires manual configuration.

OSPF Neighbor Command
The show ip ospf neighbor command is used to verify OSPF neighbor relationships in the topology.

- **Router Name: R_ALX2**
- **Neighbors: R_ALX1, R_BCP, and R_CAI**
- **Subnet Information: Multiple subnets connected via OSPF with IP addresses ranging from 192.168.x.x.**

R_ALX2 has three OSPF neighbors:

- 192.168.6.2 via **Serial0/1/0**
- 192.168.3.1 via **Serial0/1/1**
- 192.168.1.2 via **GigabitEthernet0/0/0**

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.6.2       1   FULL/DR         00:00:34    192.168.1.2     GigabitEthernet0/0/0
192.168.5.1       0   FULL/  -        00:00:34    192.168.3.1     Serial0/1/1
192.168.6.2       0   FULL/  -        00:00:34    192.168.6.2     Serial0/1/0
R_ALX2#
R_ALX2#show ip route ospf
     192.168.2.0/30 is subnetted, 1 subnets
O       192.168.2.0 [110/128] via 192.168.3.1, 00:11:15, Serial0/1/1
     192.168.4.0/30 is subnetted, 1 subnets
O       192.168.4.0 [110/65] via 192.168.1.2, 00:42:44, GigabitEthernet0/0/0
     192.168.5.0/30 is subnetted, 1 subnets
O       192.168.5.0 [110/2] via 192.168.1.2, 00:42:44, GigabitEthernet0/0/0

R_ALX2#show ip ospf
 Routing Process "ospf 1" with ID 192.168.6.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 7. Checksum Sum 0x03abaa
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

The `show ip ospf neighbor` command is used to verify OSPF neighbor relationships in the topology.

- **Router Name**: R_CAI
- **Neighbors**: R_ALX1, R_ALX2, and R_BCP
- **Subnet Information**: Multiple subnets connected via OSPF with IP addresses ranging from 192.168.x.x.

R_CAI has three OSPF neighbors:

- **192.168.2.2** via Serial0/1/0 (R_BCP)
- **192.168.3.2** via Serial0/1/1 (R_ALX2)
- **10.0.0.2** via GigabitEthernet0/0/0 (Link to the SW_SRV)

```
R_CAI#show ip route ospf
     192.168.4.0/30 is subnetted, 1 subnets
O       192.168.4.0 [110/128] via 192.168.2.2, 00:19:33, Serial0/1/0
     192.168.6.0/30 is subnetted, 1 subnets
O       192.168.6.0 [110/128] via 192.168.3.2, 00:19:33, Serial0/1/1
```

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.4.2       0   FULL/  -        00:00:33    192.168.2.2     Serial0/1/0
10.0.0.6          1   FULL/BDR        00:00:33    10.0.0.6        GigabitEthernet0/0/0
192.168.6.1       0   FULL/  -        00:00:33    192.168.3.2     Serial0/1/1
```

```
R_CAI#show ip ospf
 Routing Process "ospf 1" with ID 192.168.5.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 7 times
        Area ranges are
        Number of LSA 7. Checksum Sum 0x03a7ac
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

2. Importance of OSPF in This Topology

- **OSPF is used to dynamically learn routes between routers in different subnets.**
- **This allows efficient routing without manually configuring static routes.**

2.2. Overview of Static Routing

Static routing involves manually configuring specific routes in a network, allowing traffic to follow predetermined paths. This method is particularly useful in small or stable networks where traffic patterns are predictable.

2. Why Use Static Routing?

- **Control:** Provides full control over traffic direction.
- **Simplicity:** Ideal for straightforward network designs.
- **No Overhead:** Eliminates CPU and bandwidth usage associated with dynamic routing protocols.

3.1 Configuration of Static Routing on Router (R_CAI)

I configured static routes on **R_CAI** to manage traffic effectively between subnets. The following static routes were implemented:

1. **To route traffic to the 192.168.1.0/24 network via 192.168.3.2:**

```
Ip route 192.168.1.0 255.255.255.0 192.168.3.2
```

3.2 Configuration of Static Routing on Router (R_ALX2)

I configured static routes on **R_ALX2** to manage traffic effectively between subnets. The following static routes were implemented:

2. **To route traffic to the 10.0.0.0/24 network via 192.168.3.1:**

```
Ip route 10.0.0.0 255.255.255.0 192.168.3.1
```

4. How It Works in My Topology

- Traffic destined for **192.168.1.0/24** is routed through **192.168.3.2**.
- Traffic targeting **10.0.0.0/24** is routed through **192.168.3.1**.

5. Verification

To verify these static routes, I used: **`show Ip route`**

This command confirms that both static routes are active in the routing table.

6. Conclusion

The configuration of static routes on **R_ALX2 , R_CAI** ensures controlled traffic flow within my network.

Mix with OSPF

In addition to static routing, **OSPF** (Open Shortest Path First) can be implemented for dynamic routing. OSPF adjusts routes automatically based on network changes, enhancing scalability and failover capabilities while static routes provide precise control where needed.

Part 3: HSRP (Hot Standby Router Protocol)

3.1. Overview of HSRP

In my network, **HSRP (Hot Standby Router Protocol)** was implemented to provide redundancy for the default gateway. HSRP ensures that if the primary (active) router fails, a secondary (standby) router takes over seamlessly, providing uninterrupted network access for devices.

---

2. Why Do We Need HSRP?

In a traditional network, a single default gateway presents a single point of failure. **HSRP** addresses this problem by:

- Providing **default gateway redundancy**, ensuring that hosts still have access to the network if one router goes down.
- Offering **seamless failover** between routers without affecting the network.
- Ensuring network reliability and high availability in critical environments.

3. Configuration on Router (R_ALX2)

I configured **R_ALX2** as the **Active Router** for HSRP, with **R_ALX1** as the **Standby Router**. The following settings were applied:

- **HSRP group 1** was created on both routers.
- A **virtual IP** was assigned to the group (192.168.1.100).

```
R_ALX2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0/0    1    120 P Active   local           192.168.1.2     192.168.1.100
```

```
R_ALX2#show standby
GigabitEthernet0/0/0 - Group 1
  State is Active
    5 state changes, last state change 00:00:28
  Virtual IP address is 192.168.1.100
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.055 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.2
  Priority 120 (configured 120)
  Group name is hsrp-Gig0/0/0-1 (default)
```

How HSRP Works

- **HSRP Group**: Multiple routers are grouped together to provide redundancy. These routers share a **virtual IP address** and **virtual MAC address**.
- **Roles**:
    - **Active Router**: Handles all traffic directed to the virtual IP address.

    - **Standby Router**: Monitors the active router. If the active router fails, the standby router takes over.
- **Priority**: The router with the highest priority becomes the **Active Router**.
- **Virtual IP**: Hosts are configured to use a single **virtual IP address** as their default gateway.
- **HSRP Timers**: HSRP uses two timers:
    - **Hello Timer**: How often Hello packets are sent.
    - **Hold Timer**: How long to wait for a Hello packet before assuming the active router is down.

HSRP Versions

- **HSRPv1**: Default virtual MAC is **0000.0C07.ACxx**, where **xx** is the HSRP group number.
- **HSRPv2**: Default virtual MAC is **0000.0C9F.Fxxx**, where **xxx** is the HSRP group number. HSRPv2 supports IPv6 and has faster convergence.

Advantages of HSRP

- **High Availability**: Provides redundancy to ensure network availability even if a primary router fails.
- **Load Sharing**: You can configure multiple HSRP groups to balance traffic across multiple routers.
- **Simplicity**: HSRP is easy to configure and does not require significant additional hardware or software.

Conclusion

- HSRP enhances network reliability and uptime by providing router redundancy.
- It’s commonly used in scenarios where high availability is critical, such as data centers and enterprise networks.

Part 4: Ethernet channel technology

4.1. EtherChannel technology

was originally developed by Cisco as a LAN switch-to-switch technique of grouping several Fast Ethernet or Gigabit Ethernet ports into one logical channel. When an EtherChannel is configured, the resulting virtual interface is called a port channel. The physical interfaces are bundled together into a port channel interface

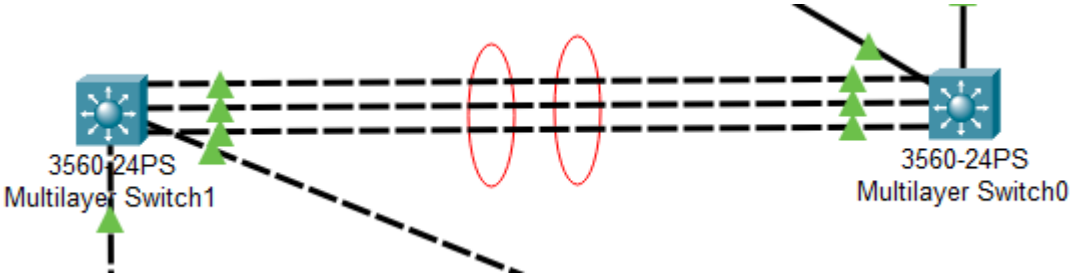
4.2 Error! Bookmark not defined.**PAgP Operation**

is a Cisco protocol that automatically creates EtherChannel links by sending packets between EtherChannel-capable ports to negotiate channel formation. It groups matched Ethernet links into an EtherChannel and adds it to the spanning tree as a single port. PAgP manages the EtherChannel, sending packets every 30 seconds, checking for configuration consistency and managing link additions and failures between switches. It ensures all ports have the same type of configuration. PAgP has three modes: On, Desirable, and Auto. Modes must be compatible on each side, and no negotiation between the two switches is possible. The on mode manually places the interface in an EtherChannel without negotiation, and no negotiation ensures all links in the EtherChannel are terminating on the other side.

4.3 Error! Bookmark not defined.**LACP Operation**

LACP is an IEEE specification that enables multiple physical ports to form a single logical channel, similar to PAgP with Cisco EtherChannel. It facilitates EtherChannels in multivendor environments and is now defined in the IEEE 802.1AX standard for local and metropolitan area networks. LACP provides negotiation benefits and helps create the EtherChannel link by detecting configurations on both sides. Modes for LACP include on, active, and passive. Both modes must be compatible for the EtherChannel link to form. LACP supports eight active links and eight standby links.

Fig4.1 Ethernet channel



Part 5: VLAN

5.1 Virtual LANs (VLANs)

- provide segmentation and organizational flexibility in a switched network. A group of devices within a VLAN communicate as if each device was attached to the same cable. VLANs are based on logical connections, instead of physical connections.
- A VLAN creates a logical broadcast domain that can span multiple physical LAN segments. VLANs improve network performance by separating large broadcast domains into smaller ones. If a device in one VLAN sends a broadcast Ethernet frame, all devices in the VLAN receive the frame, but devices in other VLANs do not.

5.2 Types of VLANs

- **Default VLAN**

The default VLAN on a Cisco switch is VLAN 1. Therefore, all switch ports are on VLAN 1 unless it is explicitly configured to be on another VLAN. By default, all Layer 2 control traffic is associated with VLAN 1.

Important facts to remember about VLAN 1 include the following:

- All ports are assigned to VLAN 1 by default.
- The native VLAN is VLAN 1 by default.
- The management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

- **Data VLAN**

Data VLANs are VLANs configured to separate user-generated traffic. They are referred to as user VLANs because they separate the network into groups of users or devices. A modern network would have many data VLANs depending on organizational requirements. Note that voice and network management traffic should not be permitted on data VLANs.

- **Native VLAN**

User traffic from a VLAN must be tagged with its VLAN ID when sent to another switch. Trunk ports support tagged traffic transmission, inserting a 4-byte tag in the Ethernet frame header. Untagged traffic may also be sent across a trunk link, placing it on the native VLAN, typically configured as an unused VLAN distinct from VLAN 1 and other VLANs.

- **Management VLAN**

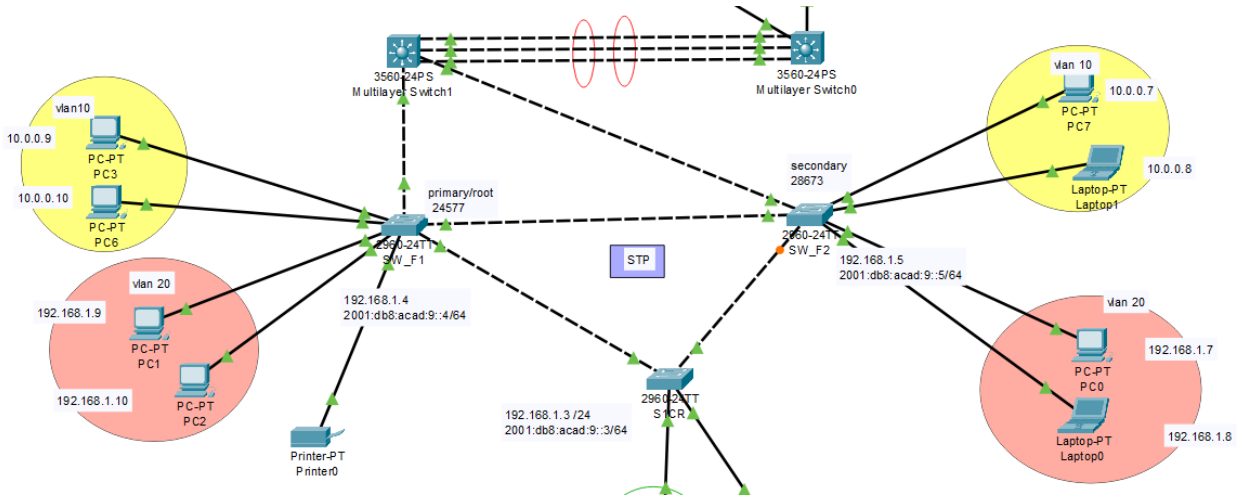
A management VLAN is a data VLAN configured specifically for network management traffic including SSH, Telnet, HTTPS, HTTP, and SNMP. By default, VLAN 1 is configured as the management VLAN on a Layer 2 switch.

- **Voice VLAN**

Voice over IP (VoIP) traffic needs its own separate VLAN with guaranteed bandwidth, priority

transmission, routing around congested areas, and less than 150 ms network delay.

Fig 5.1 Vlans


3560-24PS
Multilayer Switch1
3560-24PS
Multilayer Switch0
vlan10
10.0.0.9
PC-PT
PC3
10.0.0.10
PC-PT
PC6
primary/root
24577
2960-24TT
SW_F1
STP
secondary
28673
2960-24TT
SW_F2
192.168.1.5
2001:db8:acad:9::5/64
vlan 10
10.0.0.7
PC-PT
PC7
10.0.0.8
Laptop-PT
Laptop1
vlan 20
192.168.1.9
PC-PT
PC1
192.168.1.10
PC-PT
PC2
192.168.1.4
2001:db8:acad:9::4/64
Printer-PT
Printer0
192.168.1.3 /24
2001:db8:acad:9::3/64
2960-24TT
S1CR
vlan 20
192.168.1.7
PC-PT
PC0
Laptop-PT
Laptop0
192.168.1.8

Part 6: DHCP relay agent

6.1 DHCP Relay Agent Implementation

1. Overview of DHCP Relay Agent

In my network, the **DHCP Relay Agent** was necessary because the DHCP server is located on a different subnet from the clients. The DHCP Relay Agent ensures that DHCP requests from clients are forwarded to the correct DHCP server.

2. Why Do We Need a DHCP Relay Agent?

Routers do not forward broadcast messages, so if the DHCP server is on a different subnet, clients cannot reach it.

The **DHCP Relay Agent** solves this by:

- **Forwarding DHCP broadcasts** from clients to the DHCP server across different subnets.
- **Centralizing DHCP management**, eliminating the need for a server on each subnet, reducing complexity and costs.

3. Configuration on Router (R_ALX2)

To enable the DHCP Relay Agent, I configured it on the router **R_ALX2**, specifically on the **g0/0/0** interface. The following settings were applied:

- **IP Helper Address:**
  - The command `ip helper-address 10.0.0.3` was configured on the **g0/0/0** interface to relay DHCP requests to the server at **10.0.0.3**.

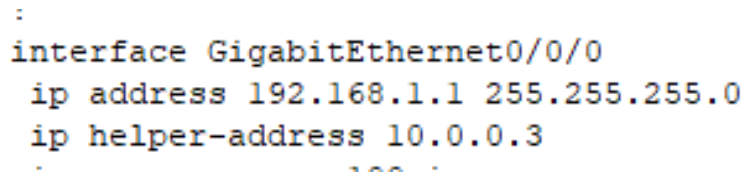
4. How It Works in My Topology

- DHCP clients broadcast a **DHCP Discover** message.
- The **R_ALX2** router, acting as the DHCP Relay Agent, intercepts the broadcast message on its **g0/0/0** interface.
- The message is forwarded as a unicast packet to the DHCP server at **10.0.0.3**.
- The DHCP server assigns an IP address, and the response is relayed back to the requesting client.

5. Verification

- The `show run or show int g 0/0/0` command is used to verify that the **R_ALX2** router is correctly forwarding DHCP requests to the DHCP server at **10.0.0.3**.

Fig 6.1 Relay agent configuration



Part 7: implementation of STP

7.1 Overview of Spanning Tree Protocol (STP)

The Spanning Tree Protocol (STP) is a network protocol that is used to prevent loops in Ethernet networks, ensuring a loop-free topology. Developed by Dr. Radia Perlman and standardized as IEEE 802.1D, STP is a critical component in network design, especially in environments where redundancy is necessary for reliability and performance.

Key Features of STP:

1. Loop Prevention:
    - STP prevents network loops that can occur when there are multiple active paths between switches. These loops can cause broadcast storms, multiple frame copies, and ultimately lead to network congestion and downtime.
2. Bridge Election:
    - STP designates one switch as the root bridge based on the lowest Bridge ID (bridge priority + MAC address (32768 Default)). The root bridge serves as the reference point for all other switches in the topology.
3. Port States and Roles:
    - Each port on a switch can be in one of several states: Blocking, Listening, Learning, or Forwarding. The roles of ports include Root Port (best path to the root), Designated Port (forwarding port for a segment), and Blocked Port (not forwarding to prevent loops).
4. Path Cost:
    - STP assigns a cost to each port based on the bandwidth of the link. It uses this cost to determine the best path to the root bridge. The lower the cost, the more preferred the path.
5. Convergence:
    - STP can take time to converge after a topology change (such as a link failure). During this period, some ports may transition between states, potentially leading to temporary connectivity issues.
6. Multiple Instances:
    - Variants of STP, such as Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w) and Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s), offer improvements in convergence times and allow for multiple spanning trees across VLANs.

Importance of STP in Network Design:

- Redundancy and Reliability: STP enables the creation of redundant links, providing alternative paths for data traffic. In case of a link failure, STP can quickly reconfigure the network to maintain connectivity.
- Efficient Resource Utilization: By preventing loops, STP ensures that network resources are utilized effectively, minimizing unnecessary traffic and reducing the risk of broadcast storms.
- Scalability: STP supports the addition of new switches and devices to a network while maintaining a stable and loop-free topology.

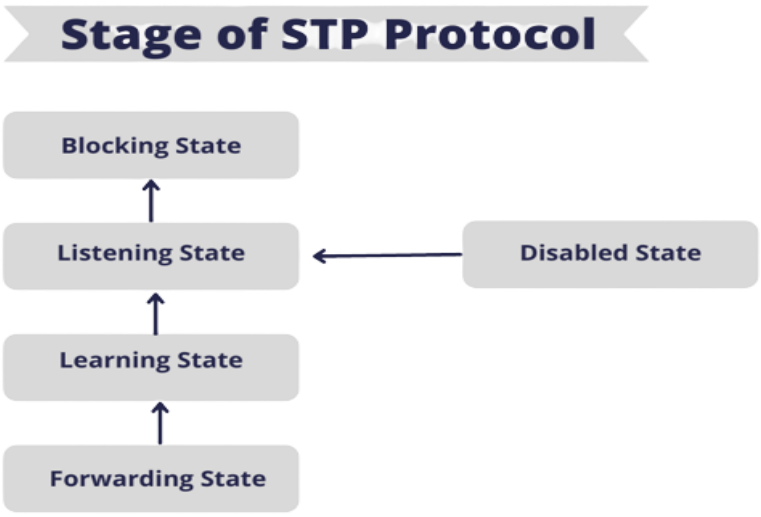
STP Advertising and Hello Protocol Steps

1. Hello Protocol Overview:
    - Hello BPDUs (Bridge Protocol Data Units) are used by switches to share network topology information.
2. Hello Time:
    - Default: 2 seconds
    - Switches send Hello BPDUs every 2 seconds.
3. Key BPDU Information:
    - Root ID: Identifies the root bridge.
    - Bridge ID: Identifies the sending bridge.

- Port ID: Identifies the port sending the BPDU.
- Path Cost: Cost to reach the root bridge.

4. Timers:
   - Hello Time:
     - Default: 2 seconds
     - Interval for sending Hello BPDUs.
   - Max Age:
     - Default: 20 seconds
     - Time before a BPDU is considered outdated if not refreshed.
   - Forward Delay:
     - Default: 15 seconds
     - Time spent in Listening and Learning states before transitioning to Forwarding.
   - Aging Time:
     - Default: 20 seconds
     - Time after which MAC addresses are removed from the MAC address table if not refreshed.

FIG7.1 STP stages



In summary, STP is an essential protocol in modern Ethernet networks, ensuring reliability, efficiency, and scalability by managing redundancy and preventing loops. Its proper implementation and monitoring are critical for maintaining optimal network performance.

7.2 Implementation of Spanning Tree Protocol (STP)

FIG7.2.1 STP implementation

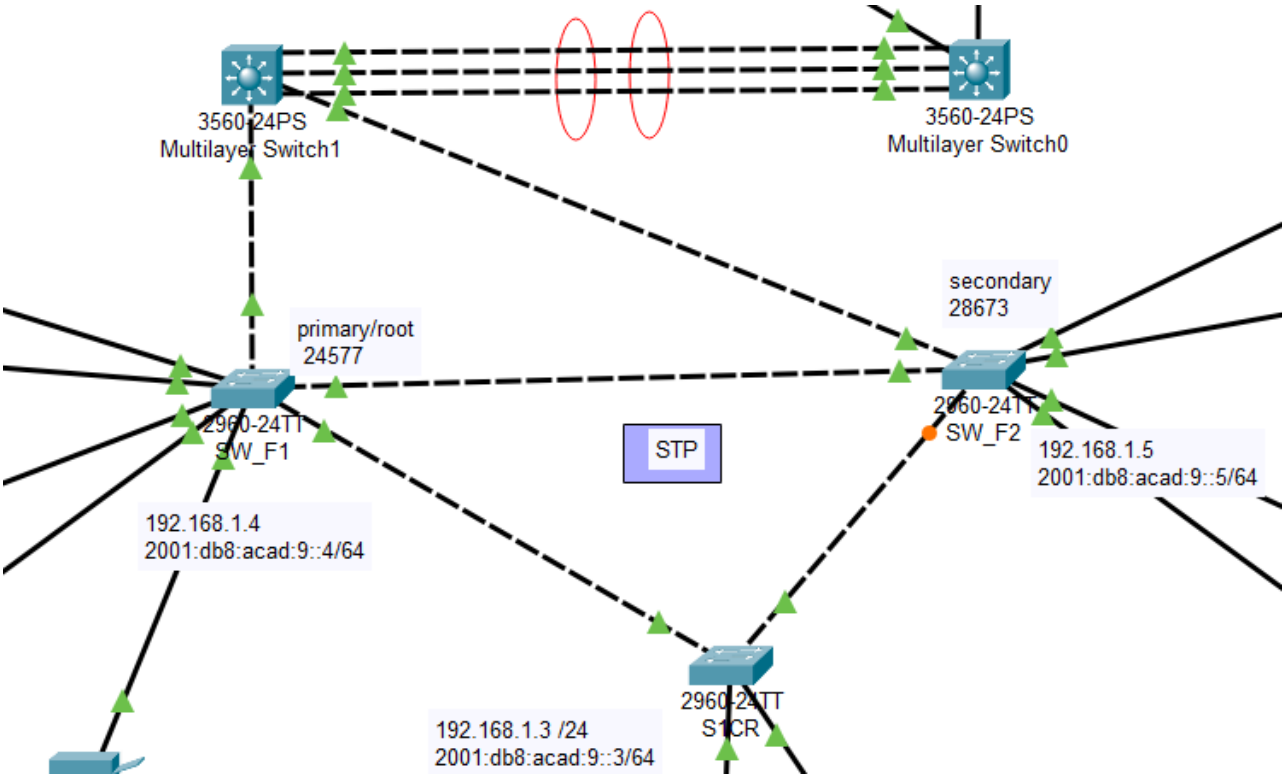


FIG7.2.2 SW_F1 (ROOT/primary)

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0001.42EC.E57A
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0001.42EC.E57A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/24           Desg FWD 19        128.24   P2p
```

Fig7.2.3 SW_F2 (secondary)

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0001.42EC.E57A
              Cost        38
              Port        5(FastEthernet0/5)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28673  (priority 28672 sys-id-ext 1)
              Address     0007.ECAA.828A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/5            Root FWD 19        128.5    P2p
Fa0/7            Altn BLK 19        128.7    P2p
```

1. Topology Overview

In my network topology, STP has been implemented on VLAN0001 to ensure a loop-free environment. This setup includes several switches, with one designated as the root bridge.

2. STP Configuration for VLAN0001

- Protocol Enabled:
  - Enabled STP using the IEEE protocol on VLAN0001.
- Root Bridge Configuration:
  - **Bridge Priority(SW_F1)**: The root bridge was configured with a priority of **24577.** This ensures that it is selected as the root bridge based on the lowest Bridge ID.
  - Root Bridge Address: The MAC address of the root bridge is `0001.42EC.E57A`.
- Bridge ID of the **Root Bridge(SW_F1):**
  - The Bridge ID for the root bridge is composed of the priority and the MAC address: 24577 (priority) + `0001.42EC.E57A` (MAC address).
- Bridge ID of the **Secondary Bridge(SW_F2):**
  - The secondary bridge has a Bridge ID of 28673 (priority) + `0007.ECAA.828A` (MAC address), ensuring that it does not compete to be the root bridge.

3. Timer Settings

The following timer settings are configured for STP in VLAN0001:

- Hello Time: 2 seconds
- Max Age: 20 seconds
- Forward Delay: 15 seconds
- Aging Time: 20 seconds

4. Monitoring and Verification

The STP status has been regularly verified using the show spanning-tree command to ensure that all ports are functioning correctly and that there are no loops in the network.

5. Troubleshooting

Continuous monitoring has been conducted to identify any STP-related issues. Any misconfigurations have been addressed promptly to maintain network stability.

Conclusion

The implementation of STP in my topology for VLAN0001 has successfully created a stable and loop-free environment, effectively managing data transmission within the network. By configuring bridge priorities and timer settings appropriately, I have ensured that the network remains efficient and reliable.

Part 8: Access Control List

Extended Access Control Lists (ACLs) in networking allow you to filter traffic with greater granularity than standard ACLs. They let you specify not just the source and destination IP addresses, but also the protocol type, source and destination ports, and other parameters. This level of detail helps you create more precise and effective security policies for your network. Extended ACLs are typically used on routers to control traffic flows and enforce security rules at different points in the network.

We use extended ACL because Standard ACLs filter network traffic by only examining the source IP address. They're simpler but offer less granularity. Extended ACLs, on the other hand, allow you to filter traffic based on multiple parameters including source and destination IP addresses, protocol types (like TCP or UDP), and port numbers. This makes extended ACLs more flexible and precise for controlling network traffic. In a nutshell, standard ACLs are about "who" is sending the data, while extended ACLs dig deeper into "what" the data is and where it's going.

Part 9: Advanced security

9.1 VLAN Security

9.1.1Why Do We Use VLAN Security?

VLAN Security is crucial for protecting Virtual Local Area Networks (VLANs) from attacks and unauthorized access. In large networks, VLANs are used to isolate and manage traffic more efficiently. However, without proper security measures, they can be vulnerable to attacks such as **VLAN hopping**, where attackers try to jump between VLANs to access sensitive resources. The purpose of VLAN Security is to enhance protection and reduce the risks associated with unwanted network traffic.

9.1.2 How to Implement VLAN Security?

- **Change Native VLAN**: Native VLANs can be vulnerable because they are untagged on **Trunk** ports. Changing it to an unused VLAN enhances security.
- **Disable DTP (Dynamic Trunking Protocol)**: Disabling DTP prevents ports from automatically switching to **Trunk** mode, reducing the risk of unauthorized access
- **Use Private VLANs**: Private VLANs help isolate devices even within the same VLAN, preventing unwanted communication between them.

9.1.3 How to Verify the Implementation:

- To verify VLAN settings and ensure they're properly configured, use:

```
SW_F1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4, 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, Fa0/24, Gig0/1
                                                Gig0/2
10   hr                               active    Fa0/20, Fa0/21
20   sales                            active    Fa0/22, Fa0/23
999  VLAN0999                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW_F1#
```

9.2 STP Security

9.2 .1 Why Do We Use STP Security?

The **Spanning Tree Protocol (STP)** prevents network loops in interconnected switches. Without STP, loops can cause network congestion and downtime. However, STP is susceptible to attacks like **BPDU attacks**, where an attacker sends fake **BPDU** messages to manipulate the root bridge selection in the network. **STP Security** ensures that unauthorized devices cannot disrupt the network's topology.

9.2.2 How to Implement STP Security?

- **BPDU Guard**: Used to prevent ports from accepting unauthorized **BPDU** messages. If a BPDU is received on a port with BPDU Guard enabled, the port shuts down to protect the network.
- **Root Guard**: Ensures that certain ports cannot become the root bridge of the STP, protecting the network's hierarchy
- **Loop Guard**: Prevents loops caused by a sudden loss of **BPDU** messages. If the **BPDU** messages stop for a certain period, **Loop Guard** ensures the network remains stable

9.2.3 How to Verify the Implementation:

- To check the status of STP and ensure there are no problems, use:

```
show spanning-tree
```

- To verify **BPDU Guard** or **Root Guard** status on your ports

```
SW_F1#show spanning-tree inconsistentports
Name                 Interface            Inconsistency
-------------------- -------------------- ------------------

Number of inconsistent ports (segments) in the system : 0
SW_F1#
```

9.3 Switch Security

9.3.1 Why Do We Use Switch Security?

Switch security is vital to protect switches from unauthorized access and attacks. **Switch Security** involves a set of measures to safeguard switches from vulnerabilities, such as unauthorized logins or network disruptions. Securing switches ensures attackers can't exploit the network's backbone.

9.3.2 How to Implement Switch Security?

- **SSH Access**: Instead of using the insecure **Telnet** protocol, enable **SSH** to encrypt communications to and from the switch.

```
SW_F1#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
SW_F1#
```

- **Disable CDP (Cisco Discovery Protocol)**: Disabling CDP prevents the switch from broadcasting information about itself, which could be used by attackers.

- **Shutdown Unused Ports**: Unused ports should be disabled to reduce the attack surface for unauthorized devices.

9.3.3 How to Verify the Implementation:

- to verify the status of interfaces (enabled or disabled), use:

```
SW_F1#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    trunk      auto    auto  10/100BaseTX
Fa0/2                        connected    trunk      auto    auto  10/100BaseTX
Fa0/3                        notconnect   1          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        connected    1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        notconnect   1          auto    auto  10/100BaseTX
Fa0/10                       notconnect   1          auto    auto  10/100BaseTX
Fa0/11                       notconnect   1          auto    auto  10/100BaseTX
Fa0/12                       notconnect   1          auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       connected    10         auto    auto  10/100BaseTX
Fa0/21                       connected    10         auto    auto  10/100BaseTX
Fa0/22                       connected    20         auto    auto  10/100BaseTX
Fa0/23                       connected    20         auto    auto  10/100BaseTX
Fa0/24                       connected    1          auto    auto  10/100BaseTX
Gig0/1                       notconnect   1          auto    auto  10/100BaseTX
Gig0/2                       notconnect   1          auto    auto  10/100BaseTX

SW_F1#
```

9.4 Port Security

9.4.1 Why Do We Use Port Security?

Port Security is used to restrict and control the number of devices that can connect to a switch port. This protects against unauthorized devices trying to connect to the network. It also helps mitigate attacks such as MAC flooding, where a switch's MAC address table is overwhelmed, causing it to operate like a hub and broadcast traffic to all devices.

9.4.2 How to Implement Port Security?

- **Limit the Number of Allowed Devices**: Set a maximum number of devices allowed to connect to each port to prevent unauthorized access.
- **Set Violation Action**: Define what action the switch should take if the port security rules are violated (e.g., shutdown, restrict, or protect).
- **Set Static MAC Addresses**: You can configure a port to only accept specific MAC addresses, ensuring only authorized devices can connect.

9.4.3 How to Verify the Implementation:

- To check the port security status of a specific interface:

```
SW_F1#show port-security interface FastEthernet0/20
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0060.5C2E.D586:10
Security Violation Count   : 0
```

9.5 DHCP Security

9.5.1Why Do We Use DHCP Security?

DHCP Security protects the network from attacks that exploit the **DHCP** protocol, such as **DHCP Spoofing**, where an attacker sets up an unauthorized DHCP server to trick users into connecting to it. **DHCP Snooping** is a feature that helps mitigate these attacks by identifying trusted and untrusted ports and filtering DHCP messages.

9.5.2 How to Implement DHCP Security?

- **Enable DHCP Snooping**: Enable DHCP Snooping on specific VLANs to monitor DHCP traffic and prevent unauthorized servers from distributing IP addresses
- **Trust Specific Ports**: Configure trusted ports that are allowed to forward DHCP traffic from legitimate servers
- **Limit the Rate of DHCP Requests**: Prevent **DHCP starvation** attacks by limiting the number of DHCP requests per second.

9.5.3 How to Verify the Implementation:

- To verify that **DHCP Snooping** is enabled and functioning properly

```
SW_SRV#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            yes        70
SW_SRV#
```

Part 10: Additional services like DNS, web servers, Syslog, and NTP

DNS Server: Domain Name System (DNS) servers translate human-readable domain names (like www.about.com) into IP addresses that computers use to locate and connect to each other. Think of it as the internet's phonebook.

Web Servers: These servers store, process, and deliver web pages to users. When you type a URL into your browser, a web server fetches and serves the requested page. Popular examples include Apache and Nginx.

Syslog: This is a standard protocol used to send system log or event messages to a designated server called a syslog server. It helps in monitoring and analyzing network devices and systems for troubleshooting and security purposes.

NTP (Network Time Protocol): NTP is used to synchronize the clocks of computers to sometime reference. It ensures that all devices on a network have the same time, which is crucial for logging and security protocols.

Fig 10.1 Services server