MAY International school

DESIGN AND IMPLEMENT OF MAY INTERNATIONAL SCHOOL NETWORK WITH 2 BRANCHES

Agdenda

1-Topology, Ip, subnetting, basic configuration
2-OSPF and static routing
3-HSRP (Hot Standby Router Protocol)
4- DHCP Relay agent
5-STP

Agdenda

6-Access Control Lists (ACLs)

7-Additional services like DNS, web servers, Syslog, and NTP

8-Ethernet channel

9- Vlans

10-Advanced Security

MAY International school

Introduction

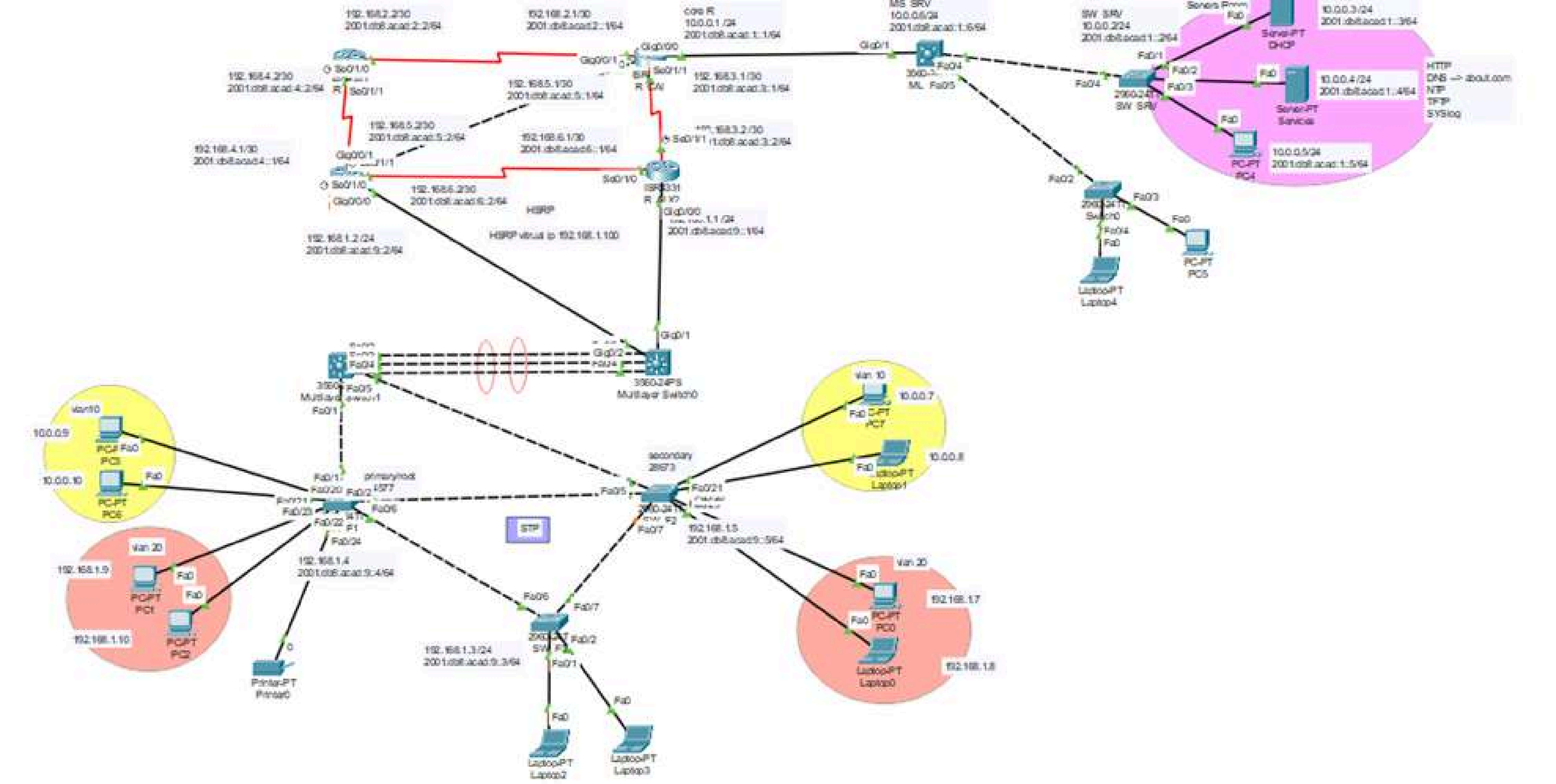
- This project aims to design and implement an advanced network for MAY International School, covering both branches and addressing current needs while planning for future expansion.

- The network will ensure high-speed connectivity for smooth communication and resource sharing across classrooms and departments. It will also include robust security measures to protect against cyber threats, creating a safe and secure learning environment.

- With network monitoring systems in place, the school will maintain efficient operations and quickly resolve any issues. This network will provide a strong foundation for the school’s growth and enhance the educational experience for students and staff.

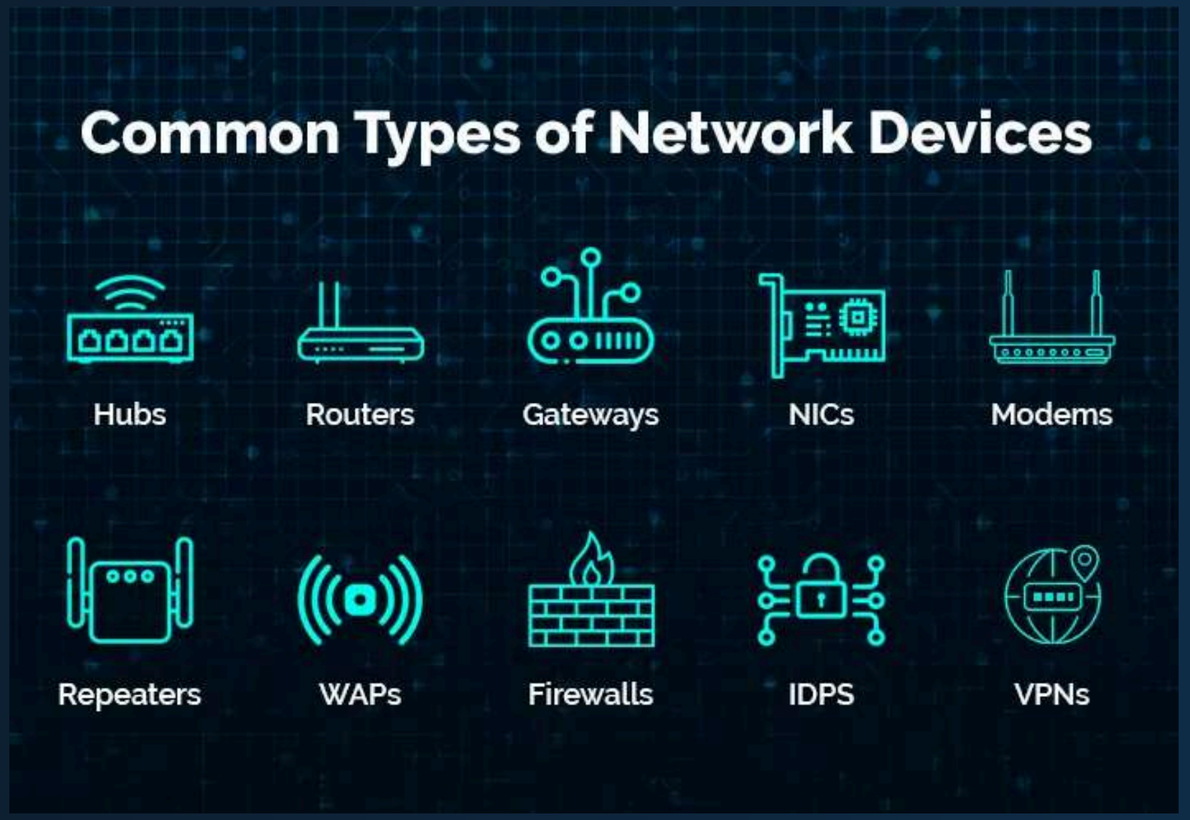
Topology, Ip, subnetting, basic configuration

The network topology is designed for efficient communication, focusing on **security**, **scalability** and **fault tolerance**. It ensures reliable performance, easy expansion, and resilience, while also supporting simple troubleshooting and centralized management.


HSRP
HSRP virtual ip 192.168.1.100
STP
HTTP
DNS --> abcd.com
NTP
TFTP
SYSlog
Multilayer Switch0
Multilayer Switch1
Server-PT DHCP
Server-PT Services
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
PC-PT PC6
PC-PT PC7
Printer-PT Printer0
Laptop0
Laptop1
Laptop2
Laptop3
Laptop4

Network Devices and Layout

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



IP

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			

Addressing

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		

Router Configuration:

- Assigned IPv4/IPv6 to interfaces.
- Set passwords for enable, console, and auxiliary.
- Enabled SSH v2 and added a security banner.
- Opened VTY lines with passwords.

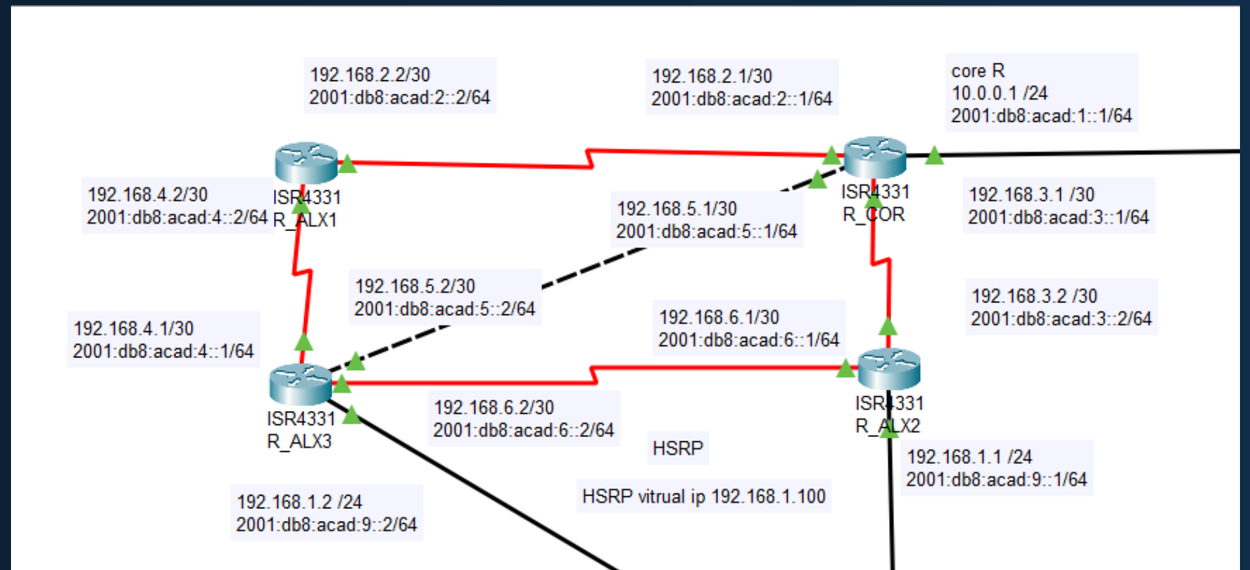
Switch Configuration:

- Assigned static IPs for management.
- Configured VLAN 10 for management.
- Set passwords and enabled SSH v2.
- Opened ports and set VLANs for traffic.

ospf and static routing

Overview of OSPF

the OSPF (Open Shortest Path First) in my network 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).



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_ALX3, and R_COR
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

OSPF Route Information - Router R_CAI

Command: show ip route ospf

OSPF Routes:

- 192.168.4.0/30(1 subnet)
- Learned via 192.168.2.2 on Serial0/1/0

192.168.6.0/30(1 subnet)

- Learned via 192.168.3.2 on Serial0/1/1

```
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
```

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.**

HSRP

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.

show standby brief

- Interface: **Gig0/0/0**
- Group (Grp): **1**
- Priority (Pri): **120** (higher priority router is selected as the active router)
- State: **Active (local router is currently active)**
- Standby Router: **192.168.1.2**
- Virtual IP: **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
```

HSRP Group and Roles

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.

DHCP relay agent

- **Routers don't forward broadcast messages, so a DHCP Relay Agent forwards client DHCP requests to the server located on a different network.**

- **It centralizes DHCP management, reducing the need for a server on each subnet, which simplifies the network and lowers costs.**

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.

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 10.0.0.3
```

STP (Spaning Tree Protocol)

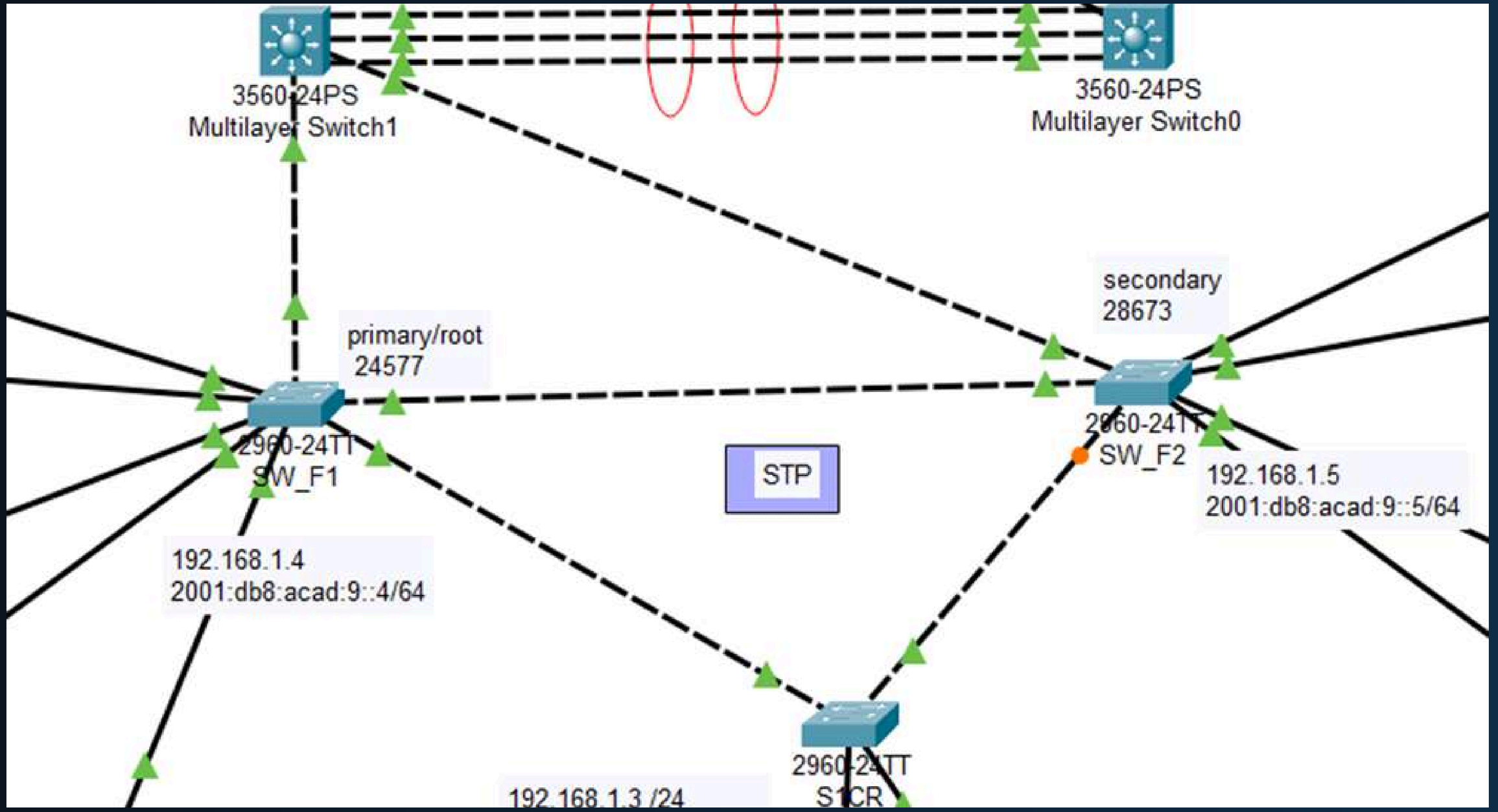
STP

- A network layer 2 protocol that prevents loops in Ethernet networks, ensuring a loop-free topology.
- Ensures redundancy and reliability in network design.
- Loops can cause broadcast storms, multiple frame copies, and congestion, but STP blocks redundant paths to maintain network stability

- STP elects the root bridge based on the **lowest Bridge ID** (priority + MAC address, with a default priority of **32768**)
- The **root bridge is SW_F1**, with a priority of **24577**
- The **secondary bridge is SW_F2** with a priority of **28673**

STP Stages

1. Blocking: Does not forward frames; prevents loops.
2. Listening: Prepares to learn; processes BPDUs.
3. Learning: Learns MAC addresses; does not forward frames.
4. Forwarding: Actively forwards frames; learns MAC addresses.
5. Disabled: No participation in STP; does not forward frames.


3560-24PS
Multilayer Switch1
3560-24PS
Multilayer Switch0
primary/root
24577
secondary
28673
2960-24TT
SW_F1
2960-24TT
SW_F2
STP
192.168.1.5
2001:db8:acad:9::5/64
192.168.1.4
2001:db8:acad:9::4/64
2960-24TT
S1CR
192.168.1.3 /24

Access Control List (ACL)

Extended ACLs offer more flexibility and precision than standard ACLs, as they filter network traffic based on multiple parameters like source and destination IP addresses, protocol types, and port numbers, allowing for deeper understanding of data transmission.

Extended Access Control Lists (ACLs) in networking provide granular traffic filtering, specifying source and destination IP addresses, protocol type, and other parameters, enabling precise and effective security policies, typically used on routers.

Extended（ACL）

```
Extended IP access list 100
    10 deny tcp host 192.168.1.15 host 10.0.0.2 eq telnet
    20 deny udp host 192.168.1.15 host 10.0.0.4 eq domain
    30 deny tcp host 192.168.1.15 host 10.0.0.2 eq 22
    40 deny tcp host 10.0.0.15 host 10.0.0.6 eq telnet
    50 deny tcp host 192.168.1.15 host 10.0.0.6 eq telnet
    60 deny tcp host 192.168.1.15 host 10.0.0.6 eq 22
    70 deny tcp host 10.0.0.15 host 10.0.0.2 eq telnet
    80 permit ip any any
```

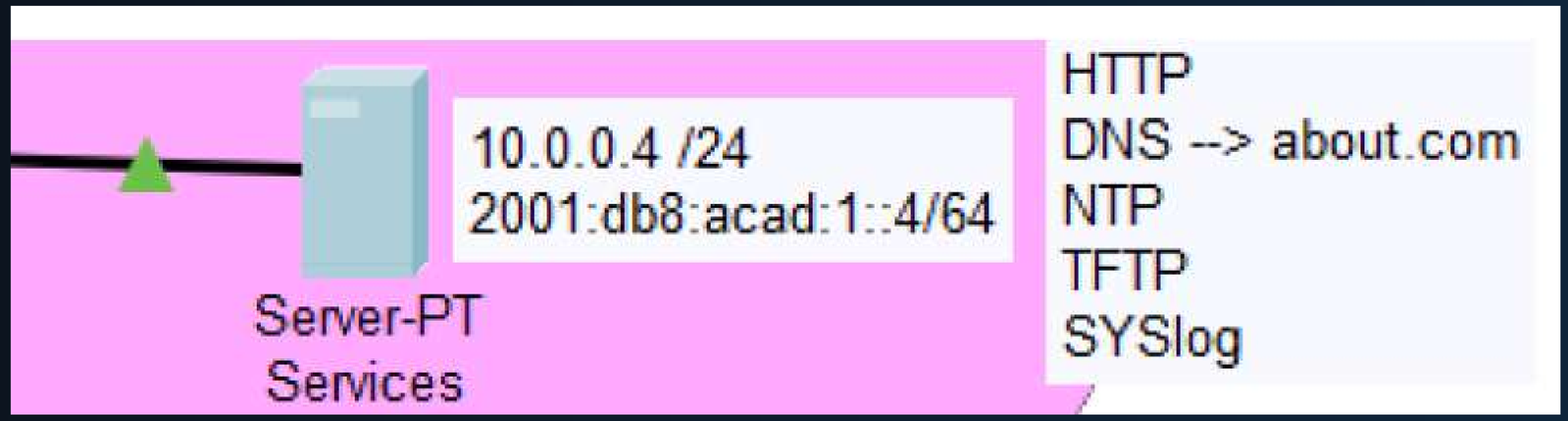
Additional services like DNS, web servers, Syslog, and NTP

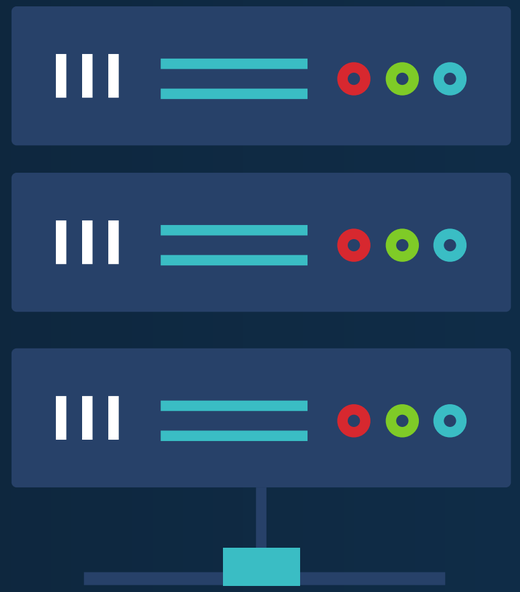
DNS Server: Domain Name System (DNS) servers translate human-readable domain names (like www.about.com) into IP addresses that computers use to locate and connect to each other. Think of it as the internet's phonebook.

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.





A DNS server translates domain names like www.about.com into IP addresses, ensuring browsers can locate the right server. An HTTP server, on the other hand, delivers web content to users by handling HTTP requests and sending back the appropriate responses. Both work hand-in-hand to make the web accessible and functional.

Ethernet channel

link aggregation technology

Etherchannel

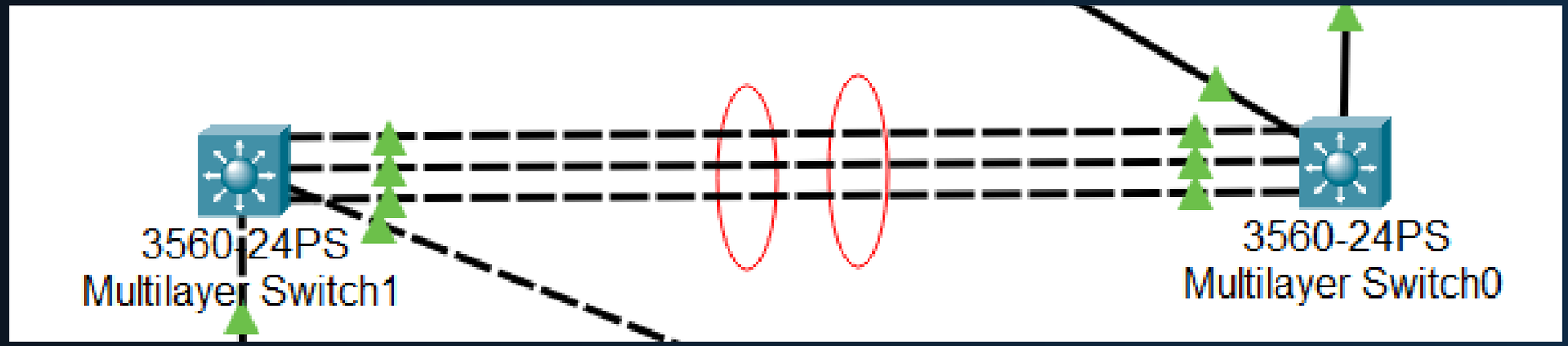
key benefits :

- **Increased Bandwidth:** By bundling multiple links, EtherChannel can significantly increase the available bandwidth2.
- **Redundancy:** If one link fails, traffic is automatically redistributed across the remaining links, ensuring continuous network availability3.
- **Simplified Network Management:** EtherChannel simplifies network management by treating multiple physical links as a single logical link4.

Etherchannel protocols

- **Port Aggregation Protocol (PAgP) –** is a Cisco proprietary EtherChannel protocol where we can combine a maximum of 8 physical links into a single virtual link.

- **Link Aggregation Control Protocol (LACP) –** is an IEEE 802.3ad standard where we can combine up to 8 ports that can be active and another 8 ports that can be in standby mode.



VLANs

Vlans

logical grouping of network devices

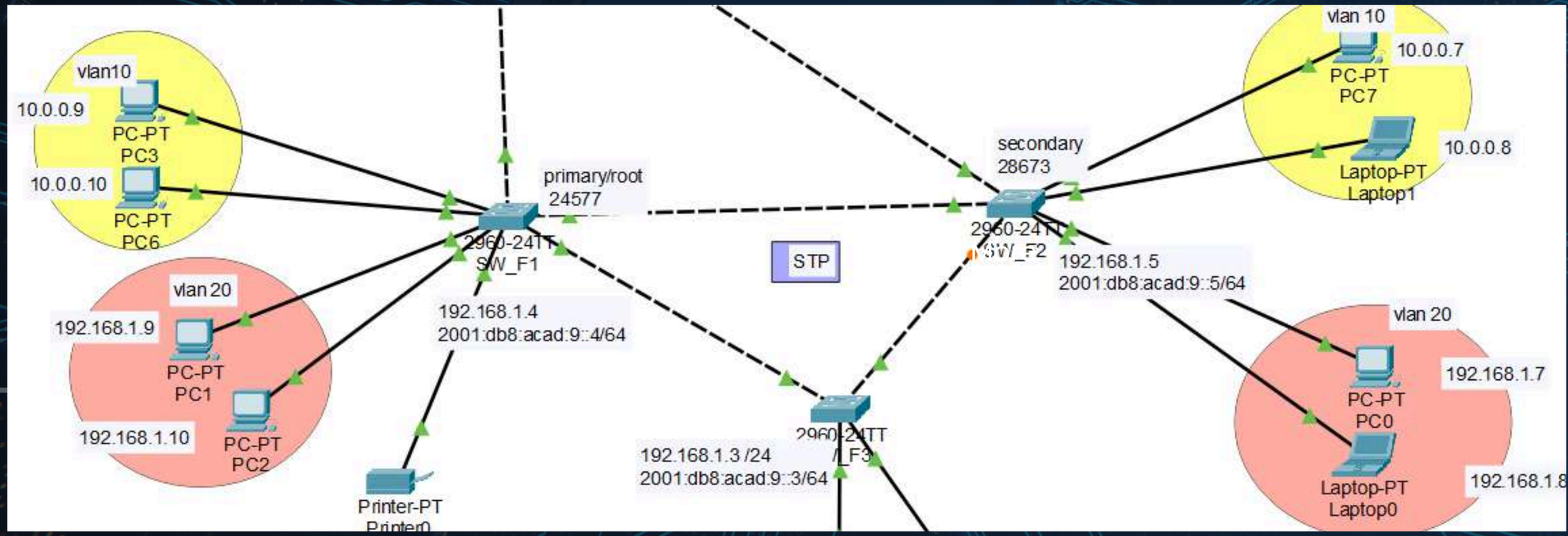
allows them to communicate as if they were on the same physical network, even if they are not. VLANs operate at the Data Link Layer (Layer 2) of the OSI model and help in segmenting a network to improve security, performance, and manageability.

Types of VLANs:

1. **Default VLAN:** The default VLAN on most switches, typically VLAN 1. It cannot be deleted or renamed.
2. **Native VLAN:** The VLAN that is used for untagged traffic on a trunk port. It's important for compatibility between different network devices.
3. **Extended VLAN:** VLANs with IDs ranging from 1006 to 4094. These are used when the normal VLAN range (1-1005) is exhausted.
4. **Trunk VLAN:** A VLAN that carries traffic from multiple VLANs across a single physical link. It uses tagging to distinguish between different VLANs.
5. **Access VLAN:** A VLAN assigned to a switch port, allowing devices connected to that port to communicate within the VLAN.

Benefits of VLANs:

- Improved Security
- Reduced Broadcast Traffic
- Enhanced Performance
- Simplified Network Managemen



Advanced Security

1 - VLAN Security

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

- **How to Implement VLAN Security?**

1- Change Native VLAN: Native VLANs can be vulnerable because they are untagged on Trunk ports. Changing it to an unused VLAN enhances security.

2- Disable DTP (Dynamic Trunking Protocol): Disabling DTP prevents ports from automatically switching to Trunk mode, reducing the risk of unauthorized access

3- Use Private VLANs: Private VLANs help isolate devices even within the same VLAN, preventing unwanted communication between them

```
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#
```

2- STP Security

The Spanning Tree Protocol (STP) prevents network loops in interconnected switches

How to Implement STP Security?

1-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.

2- Root Guard: Ensures that certain ports cannot become the root bridge of the STP, protecting the network's hierarchy

3- 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

3- Switch Security

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

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

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

4- 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.

How to Implement Port Security?

1- Limit the Number of Allowed Devices: Set a maximum number of devices allowed to connect to each port to prevent unauthorized access

2-Set Violation Action: Define what action the switch should take if the port security rules are violated (e.g., shutdown, restrict, or protect).

3- Set Static MAC Addresses: You can configure a port to only accept specific MAC addresses, ensuring only authorized devices can connect

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
```

5- 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.

How to Implement DHCP Security?

1- Enable DHCP Snooping: Enable DHCP Snooping on specific VLANs to monitor DHCP traffic and prevent unauthorized servers from distributing IP addresses

2- Trust Specific Ports: Configure trusted ports that are allowed to forward DHCP traffic from legitimate servers

3- Limit the Rate of DHCP Requests: Prevent DHCP starvation attacks by limiting the number of DHCP requests per second

Thank You

FOR YOUR ATTENTION