Unit - 3
IPv4 Routing & LAN Switching

Introduction: Ipv4 Routing

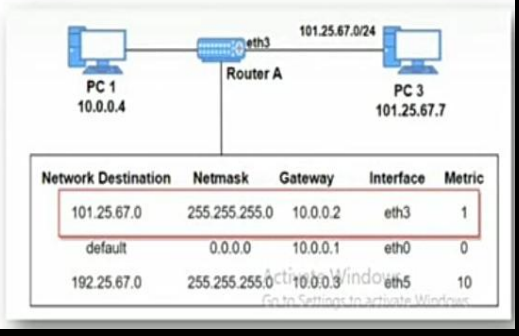
Router: A router is a networking device that forwards data packets between computer networks. It determines the optimal path for data to travel from the source to the destination.

Routing: Routing is the process of selecting paths in a network along which to send data packets. This involves determining the best route based on various metrics such as hop count, bandwidth, and latency.

- Computer Network is made of many machines called nodes or connected paths.
- Network layer convert data into packets.
- Routing algorithms are used to determine most efficient path for data to travel without any congestions.
- They use various metrics such as distance, traffic and available bandwidth.
- It make accurate routing decisions and optimize network performance.

➢ **Routing Algorithms:**

1. Static Routing (Non-Adaptive Routing)
2. Dynamic Routing (Adaptive Routing)
3. Distance Vector Routing
4. Link State Routing



Routing Table

Routing table is the collection of all the routes learned by the router.

It can be:

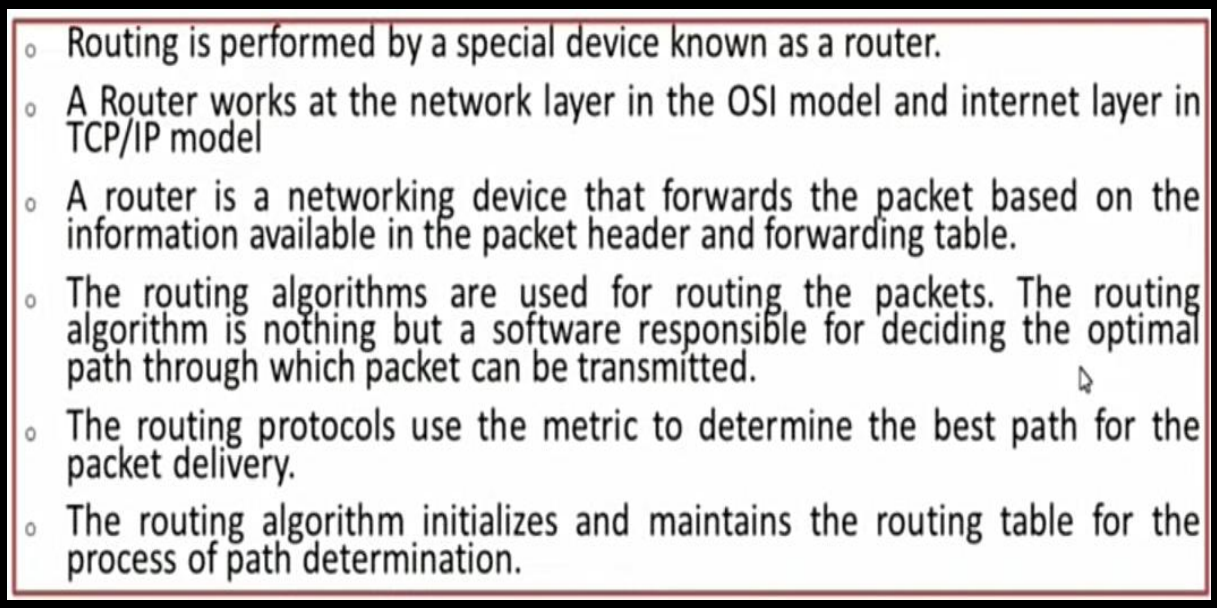
- Directly connected routes (C)
- Statically configured routes by the network admin (S)
- Dynamically learned routes using routing protocols (R, D, O etc.)

The best available path or paths to a destination network are listed in router's routing table and will be used for forwarding traffic.

OR

A **routing table** is a data structure stored in a router or a networked device that contains information about how to forward packets to their destination. It is essential for network routing and ensures that data is transmitted efficiently across networks.

Routers maintain routing tables, which store information about known networks and the best paths to reach them.



Types:

Routing tables can be either:

- Static: Manually configured by network administrators.
- Dynamic: Updated automatically by routing protocols that exchange routing information between router

Why is routing so important?

Routing is really important because in big networks like the internet, there are many different paths that data can take to reach its destination. As networks grow larger and are used for important tasks, routing becomes more complicated.

By understanding the different paths that data takes within a network, both inside and outside, network admins can find out where delays (called latency) are happening. This helps them fix issues and make the network run more smoothly.

Routing Protocols

- Routing protocols are used by routers to exchange routing information and build routing tables.
- Routing protocols can be classified as interior gateway protocols (IGPs) or exterior gateway protocols (EGPs).
- IGPs are used within an autonomous system (AS), while EGPs are used between ASs.

Intra-Domain Routing Protocols (IGPs):

- **RIP (Routing Information Protocol):**
  - A distance-vector routing protocol.
  - Uses hop count as the routing metric.
  - Updates are broadcasted every 30 seconds.
  - Limited to a maximum hop count of 15.
  - Simple to configure, but not suitable for large networks.
  - **RIPv2:** Version 2 of RIP, allows for VLSM and authentication.

- **OSPF (Open Shortest Path First):**
  - A link-state routing protocol.
  - Uses Dijkstra's algorithm to calculate the shortest path.
  - Uses cost as the routing metric, which is based on link bandwidth.
  - Updates are triggered by network changes.
  - Scalable and suitable for large networks.

✓ **Link-state vs. Distance-vector:**

- Distance-vector protocols (like RIP) share their entire routing table with neighbours.
- Link-state protocols (like OSPF) share information about their directly connected links with all routers in the area.

➢ **Inter-Domain Routing Protocols (EGPs):**

- **BGP (Border Gateway Protocol):**
  - A path-vector routing protocol.
  - Used to exchange routing information between ASs.
  - Uses path attributes to determine the best path.
  - Highly scalable and used for Internet routing.
  - **Path-vector:** BGP shares the path of AS numbers that a route traverses, allowing for policy based routing.

Routing Process

The routing process involves the following steps:

1. Receiving the Packet: A router receives a data packet on one of its interfaces.

2. Decoding the Packet: The router examines the packet's destination IP address.
3. Consulting the Routing Table: The router looks up the destination IP in its routing table to determine the best next-hop address and the corresponding interface.
4. Forwarding the Packet: The packet is forwarded to the next-hop router or the destination device via the selected interface.

Static Routing and Dynamic Routing

Static Routing: Routes are manually configured by network administrators. This method is simple but lacks scalability and adaptability to network changes.

Dynamic Routing: Routers automatically learn and adjust routes using routing protocols, allowing for scalability and adaptability to network topology changes.

1. Static Routing

- **Definition:** Manually configuring routing entries in the routing table by Network Admin.
- **Advantages:**
    - Simple to configure for small, stable networks.
    - Provides predictable paths and is fast.
    - Enhanced security as paths are explicitly defined.

- **Disadvantages:**
    - Requires manual updates for network changes.

- Not scalable for large or dynamic networks.
- Prone to errors if not configured correctly.

- **Configuration:**
  - Command-line interface (CLI) commands to add static routes.
  - Specifying the destination network, subnet mask, and next-hop IP address or exit interface.
  - Example:

- ip route 192.168.2.0 255.255.255.0 192.168.1.2

2. Dynamic Routing

- **Definition:** Routers automatically learn and update routing information using routing protocols.
- **Advantages:**
  - Adapts to network changes automatically.
  - Scalable for large and complex networks.
  - Reduces administrative overhead.

- **Disadvantages:**
  - Requires more processing power and memory.
  - Can be more complex to configure and troubleshoot.
  - Potential for routing loops or instability.

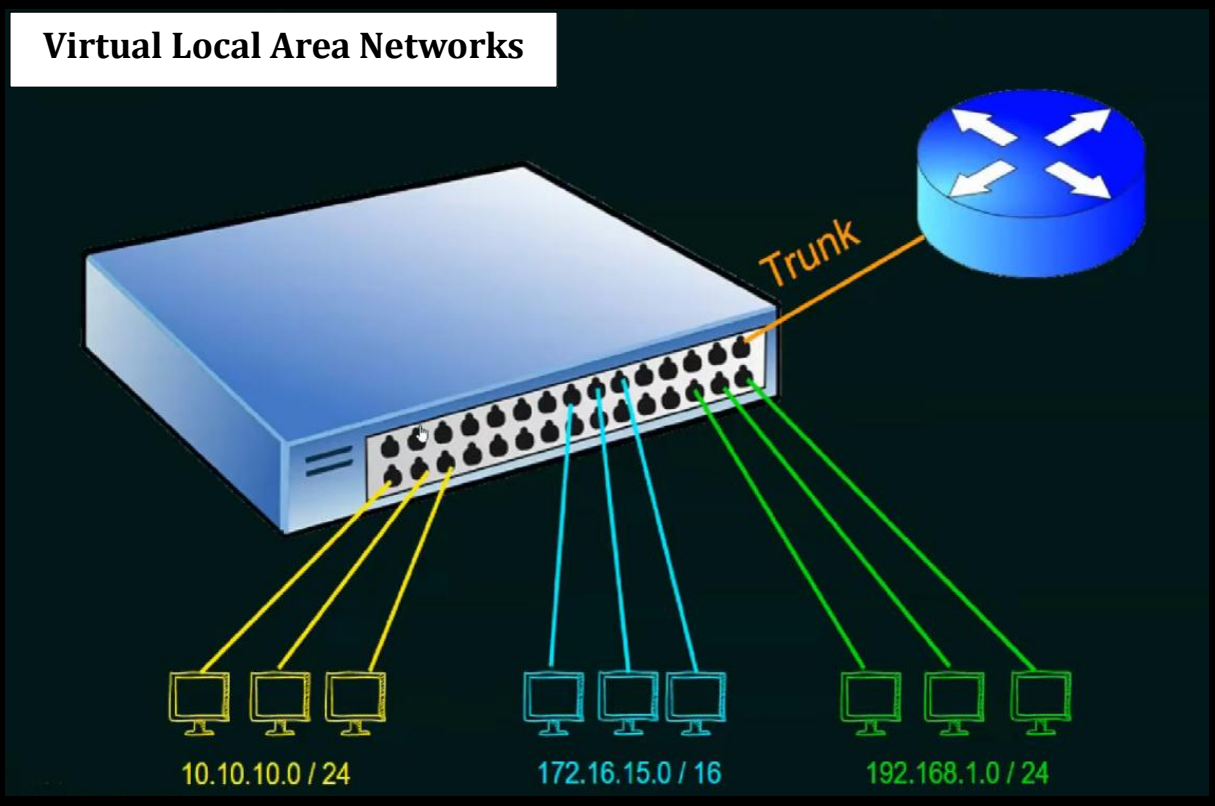
- **Routing Protocols:**
  - **RIP (Routing Information Protocol):** Distance-vector protocol, uses hop count as metric.
  - **OSPF (Open Shortest Path First):** Link-state protocol, uses cost as metric.

- **EIGRP (Enhanced Interior Gateway Routing Protocol):** Cisco proprietary, hybrid protocol.
- **BGP (Border Gateway Protocol):** Path-vector protocol, used for inter-domain routing.

IPv4 Routing and LAN Switching:

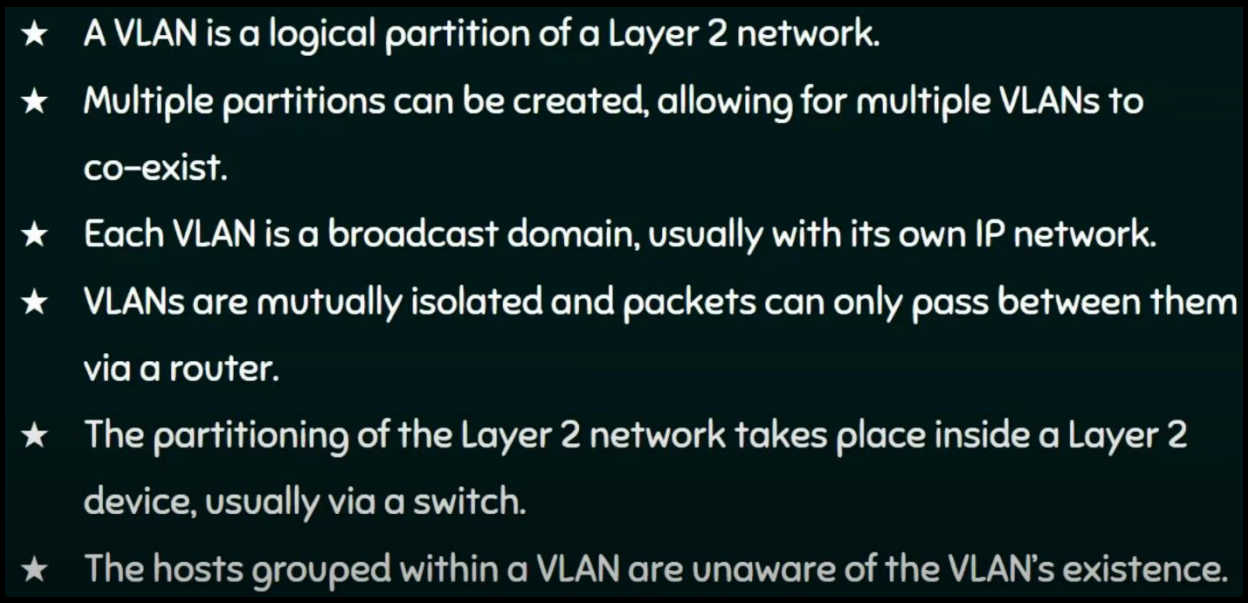
- **IPv4 Routing**: Involves forwarding packets based on the destination IP address using routing tables and protocols.
- **LAN Switching**: Uses switches to forward data within a local area network (LAN) based on MAC addresses, operating at the data link layer (Layer 2).

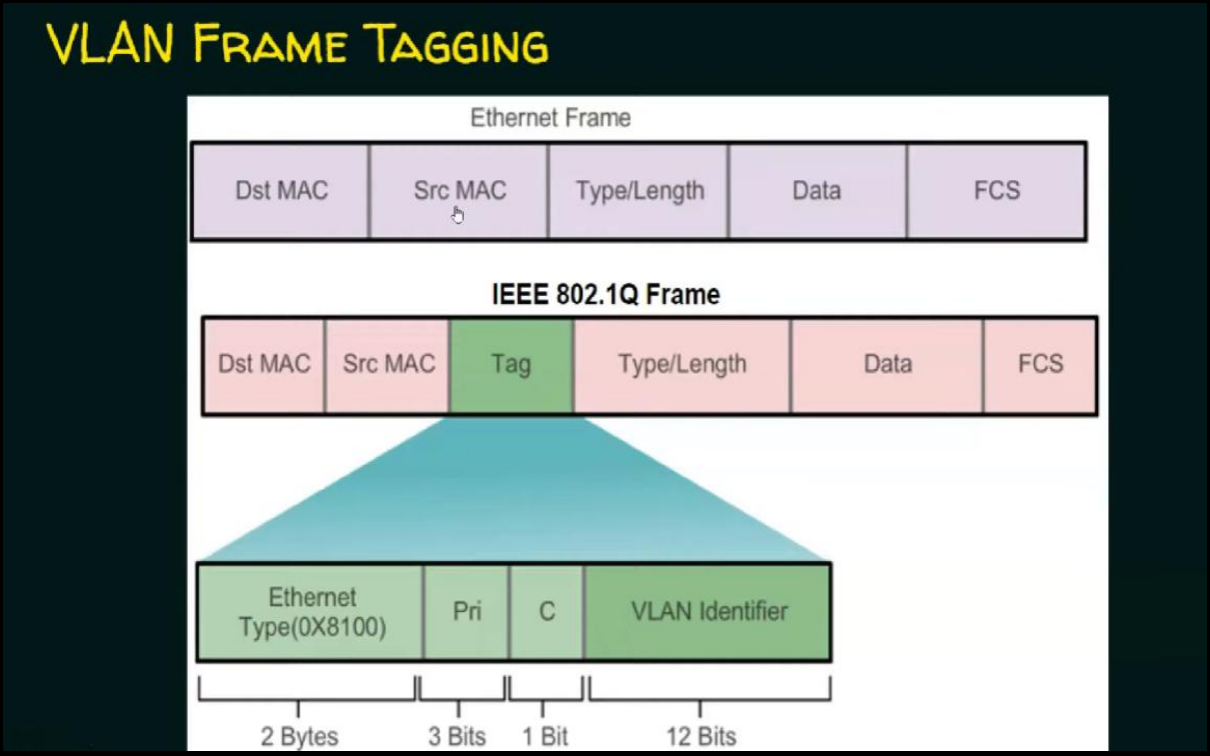
Introduction: LAN Switching



- **Definition:** VLANs are used to logically segment a physical network into multiple virtual networks. VLAN is the process of allowing devices in different VLANs to communicate with each other. VLANs split a network into separate broadcast domains, but without routing, they can't talk to each other.

- **Important Concepts:**
  - **Inter-VLAN Routing:** Done using a router or a Layer 3 switch.
  - **Router-on-a-Stick**: A single router interface handles multiple VLANs using sub-interfaces.





VLAN FRAME TAGGING

★ Frame tagging is the process of adding a VLAN identification header to the frame.

★ It is used to properly transmit multiple VLAN frames through a trunk link.

★ Switches tag frames to identify the VLAN to that they belong. Different tagging protocols exist; IEEE 802.1Q is a very popular example.

★ The protocol defines the structure of the tagging header added to the frame.

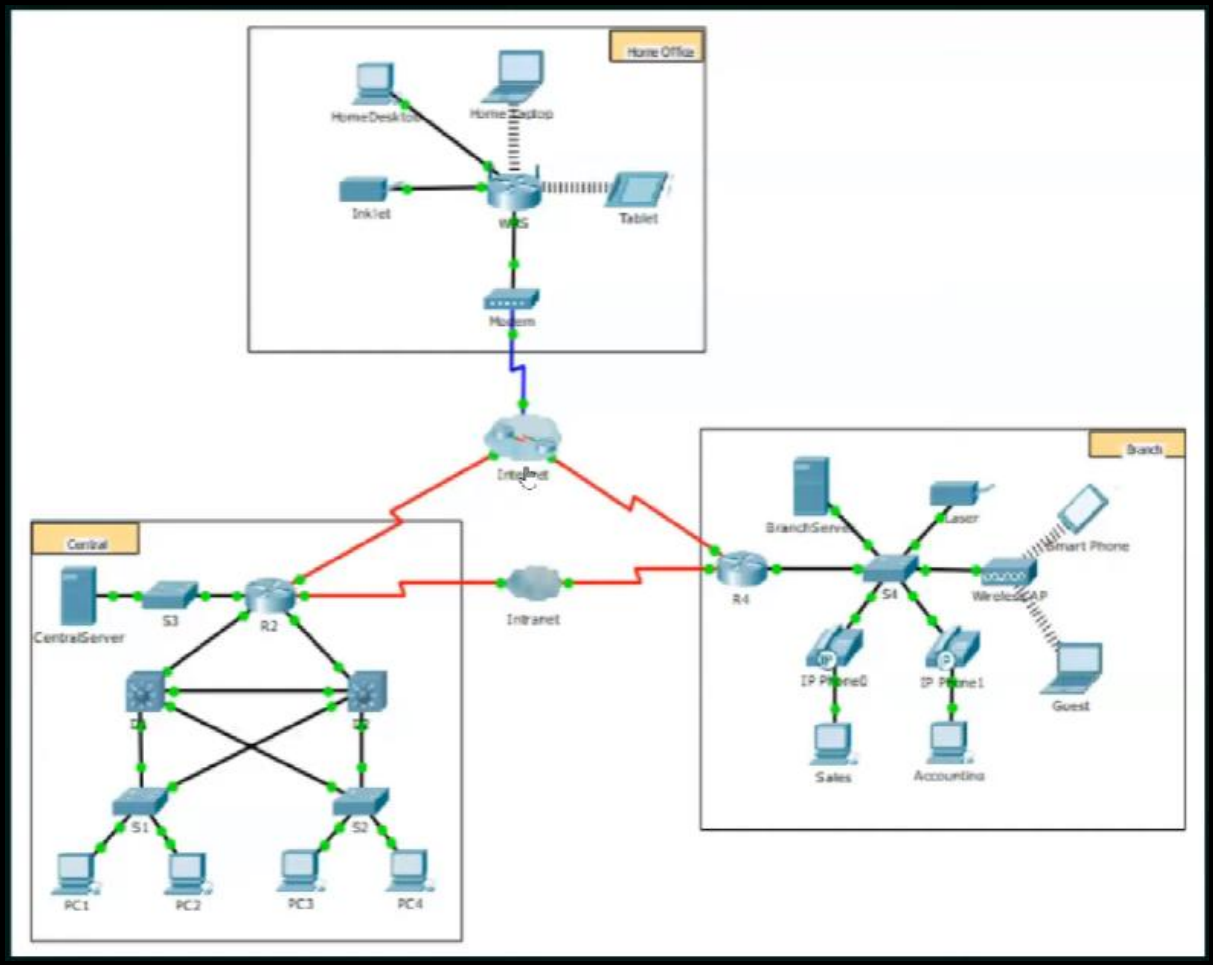
★ Switches add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports.

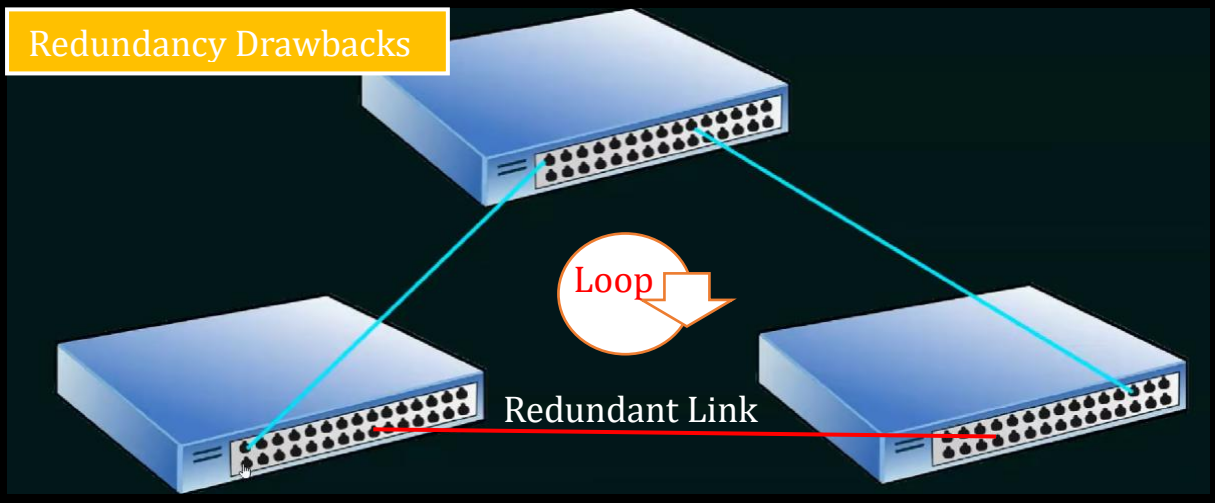
★ When properly tagged, the frames can transverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination.

STP (IEEE 802.1D Spanning Tree Protocol)

Redundancy is Good. Redundancy means having backup systems, pathways, and components to ensure continued operation even if a primary component fails, minimizing downtime and maintaining network reliability.

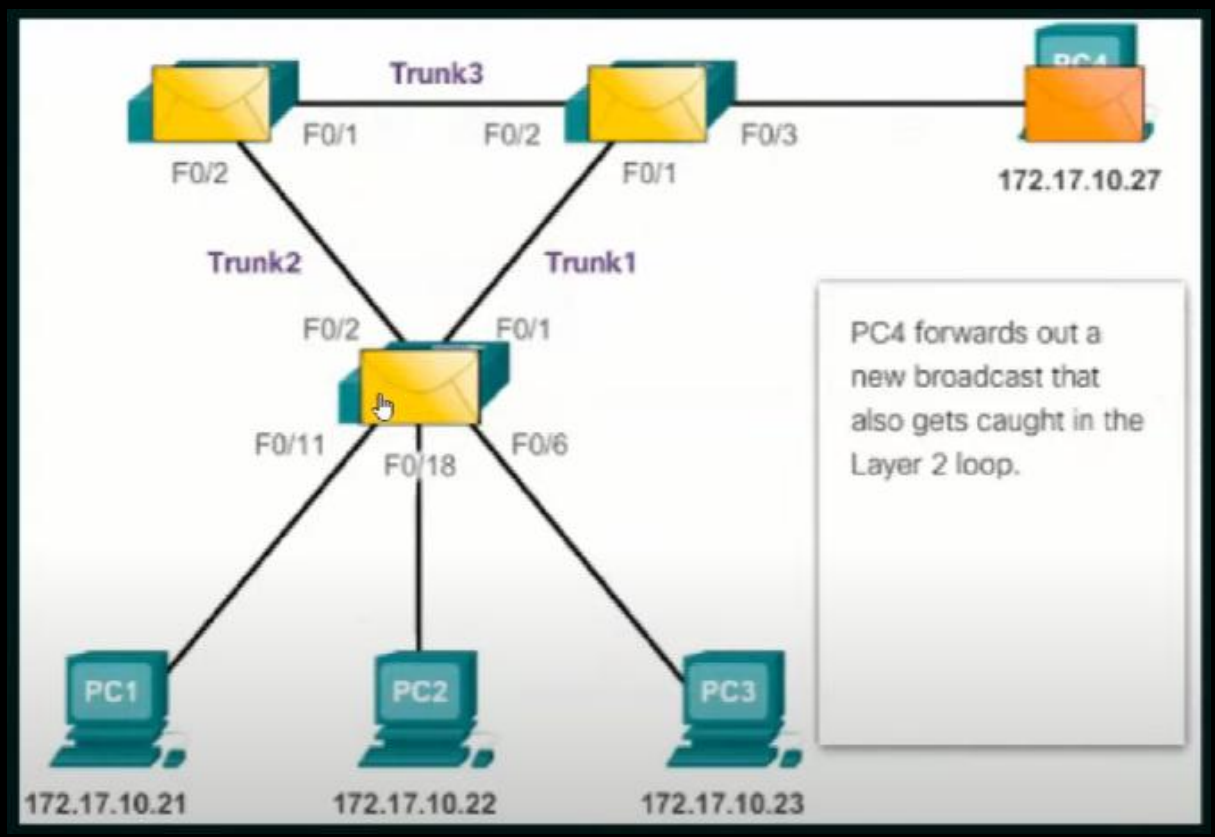
- ★ Enables users to access network resources, despite path disruption.
  - Improves reliability.
  - Improves availability.
- ★ In Technology, 2 is 1 and 1 is none. Single connection mean single point of failure.
  - Creating redundant links is very simple and is advisable.

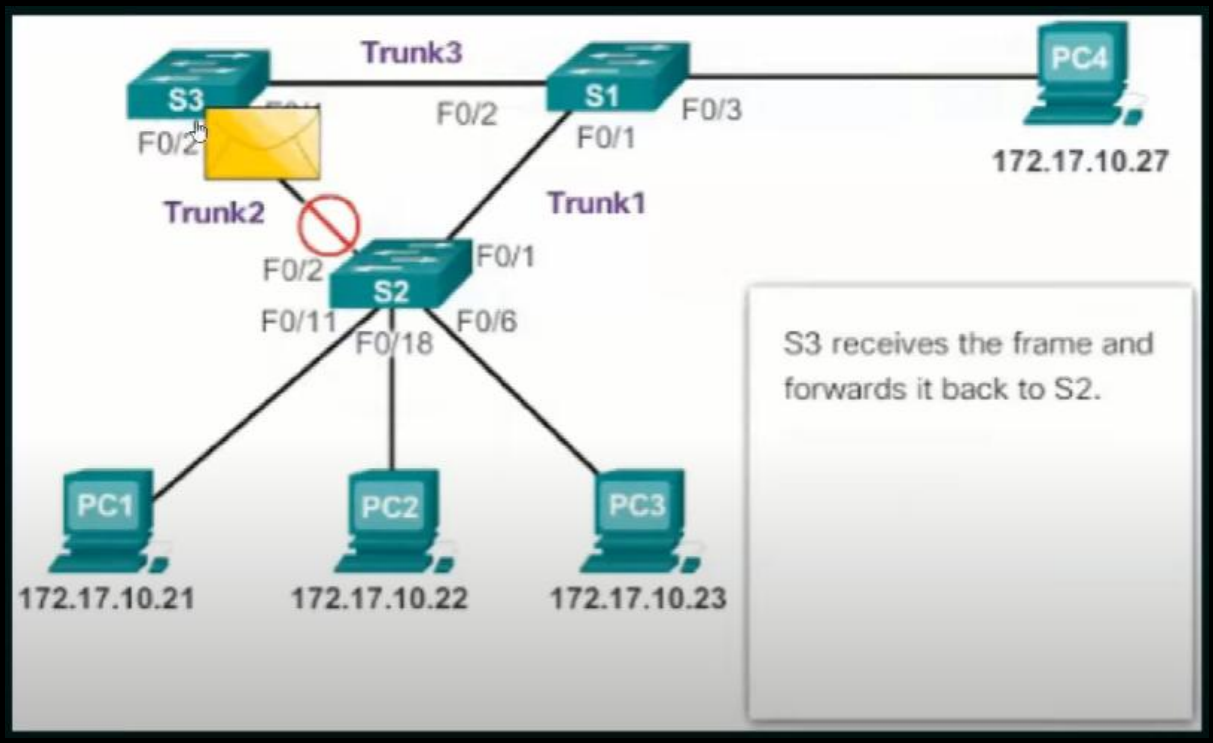




A broadcast storm in networking is an excessive amount of broadcast traffic that overwhelms a network, causing congestion and potential network disruptions. It often results from loops in the network or misconfigured devices, leading to continuous retransmission of broadcast packets.

STP (Spanning Tree Protocol) prevents Layer 2 loops in a switched network by blocking redundant paths. Purpose: Ensures a loop-free topology.





KEY FACTS - STP

★ Original STP (802.1D) was created to prevent loops.

★ Switches send probes message into the network to discover loops.

★ These probes are called as BPDU.

★ BPDU = Bridge Protocol Data Unit.

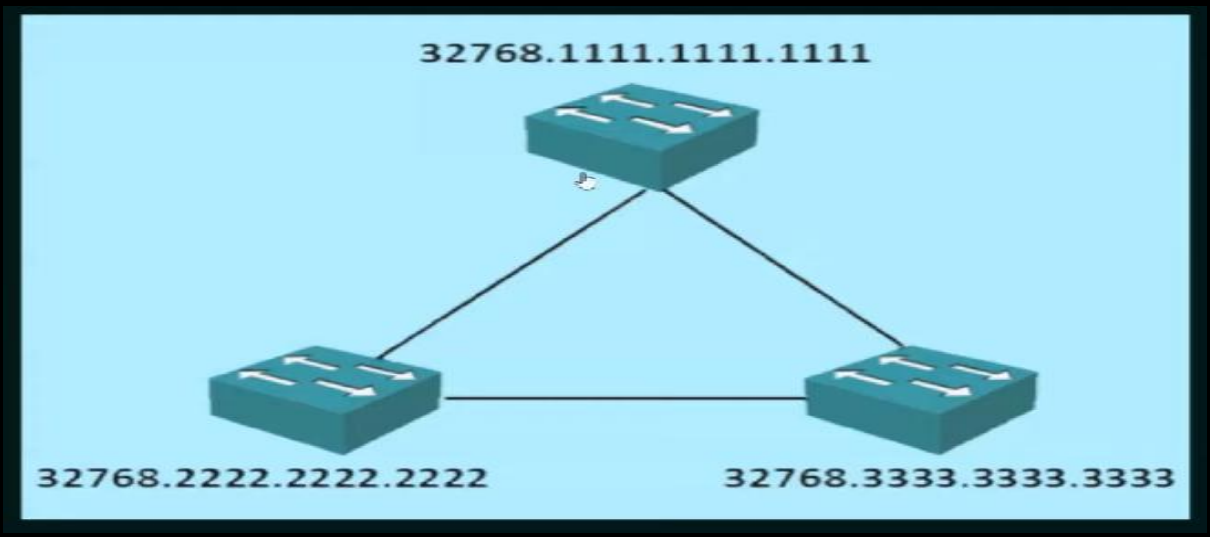
★ BPDU will have specific information about the switch.

★ Switch multicasts BPDU probes (every 2 seconds) and if it receives its own BPDU back, it means there is a loop in the network.

★ Also the BPDU probes helps to elect the root bridge.

★ All switches will find the best way to reach the root bridge and the redundant links will be blocked. (Port cost)

★ This redundant links will be active only if the existing links or ports goes down.



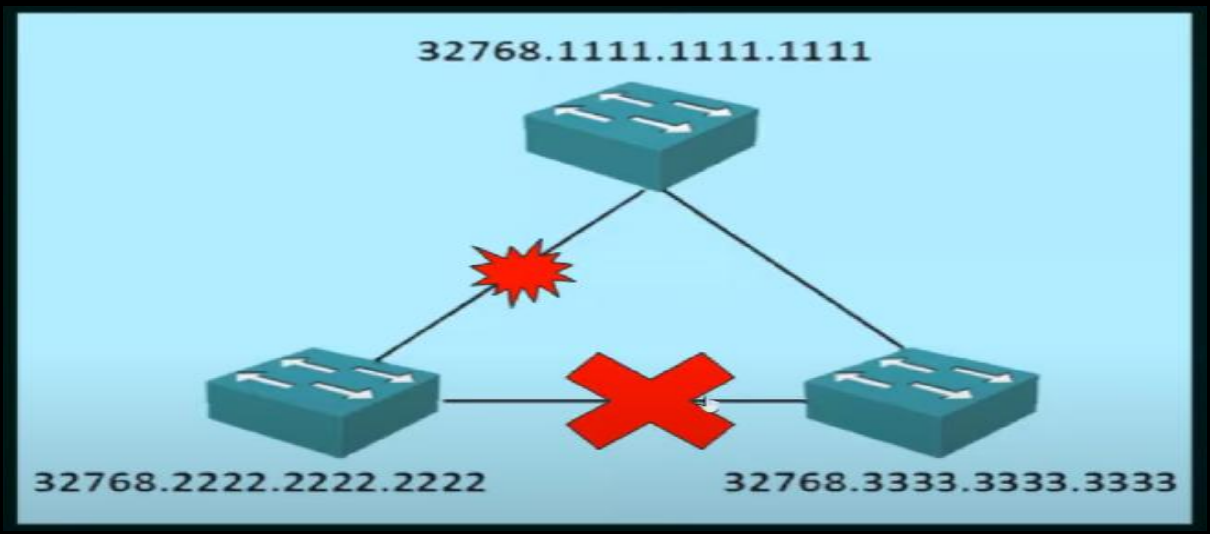
SPANNING TREE PROTOCOL

★ STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.

★ A port is considered blocked when user data is prevented from entering or leaving that port. This does not include bridge protocol data unit (BPDU) frames that are used by STP to prevent loops.

★ The physical paths still exist to provide redundancy, but these paths are disabled to prevent the loops from occurring.

★ If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.



VLAN Trunking Protocol (VTP)

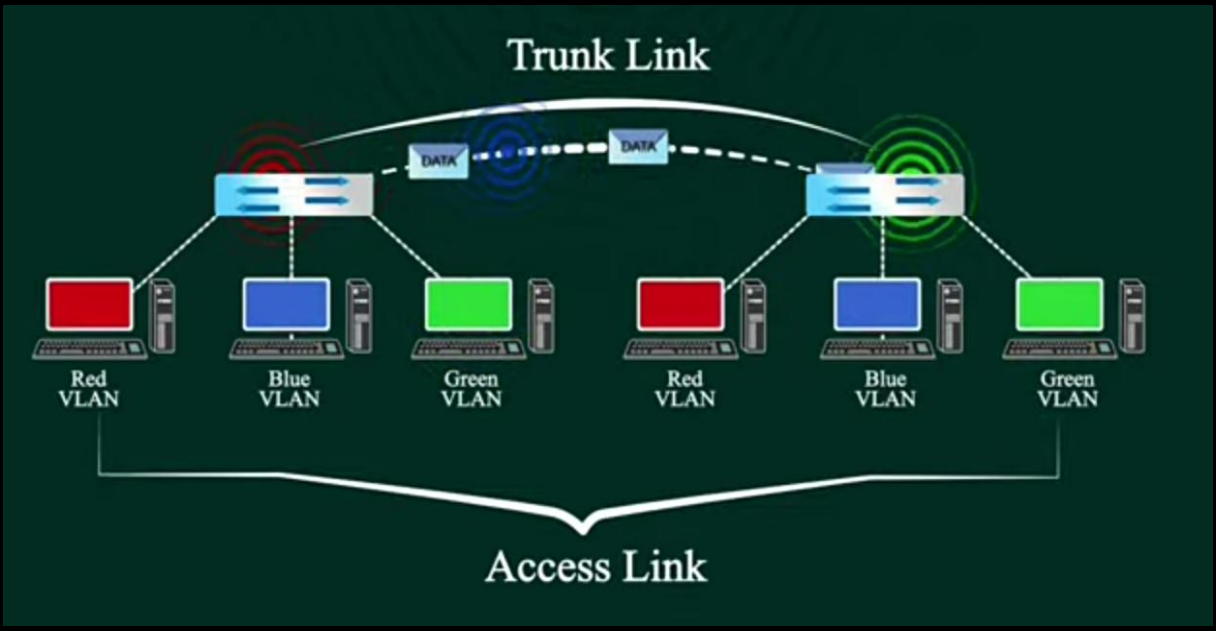
Trunk or Trunk Link:

A physical link between two or more Ethernet switch interfaces that carries traffic for multiple VLANs, allowing VLANs to be extended across an entire network.

A trunk is a point-to-point link, typically between switches or between a switch and a router, that is configured to carry traffic from multiple VLANs.

OR

A trunk is a physical link between two network devices (e.g., switches) that can carry multiple VLANs simultaneously.



Why is Trunking Important?

- Trunking allows for efficient use of network resources by carrying multiple VLANs over a single link.
- It enables the extension of VLANs across multiple switches, creating a more flexible and scalable network.
- By using trunks, you can avoid having multiple physical links between switches for each VLAN.

How it works:

Unlike access ports that carry traffic for only one VLAN, trunk ports are tagged with VLAN information (using protocols like 802.1Q) to identify the VLAN to which each frame belongs.

Example:

Imagine a network with multiple switches. Without trunking, each switch would need to be configured with the same VLANs, which is a time-consuming and error-prone process. With trunking and VTP, VLAN configurations can be managed centrally on one switch, and the other switches in the VTP domain will automatically synchronize their VLAN configurations.

Configuring the VLAN Trunking Protocol (VTP)

Configuring the VLAN Trunking Protocol (VTP) on Cisco switches involves setting up a VTP domain, defining the VTP mode (Server, Client, Transparent, or Off), and ensuring trunk links are properly established between switches.

Below is a step-by-step explanation of VTP configuration, including commands and considerations.

Understanding VTP Modes

Cisco switches support four VTP modes:

- **Server Mode**: Creates, modifies, and deletes VLANs, propagating changes to all switches in the VTP domain. Requires at least one server.
- **Client Mode**: Receives VLAN updates from a VTP server but cannot modify VLANs.
- **Transparent Mode**: Maintains its own VLAN database, does not sync with VTP but forwards advertisements.
- **Off Mode**: Disables VTP entirely, preventing participation and forwarding of VTP updates.

Prerequisites: Before configuring VTP, ensure the following:

- All switches have consistent domain names.
- Trunk links between switches are operational, as VTP advertisements are sent over trunk ports.
- If using VTP passwords, they must match across all switches in the domain.

Step-by-Step VTP Configuration

1. **Access Global Configuration Mode**
   Begin by entering privileged EXEC mode and then global configuration mode:

   ```
   Switch> enable
   Switch# configure terminal
   ```

2. **Set the VTP Domain Name**

   Define the VTP domain name to group switches that will share VLAN information. All switches in the same domain must have an identical domain name:

   ```
   Switch(config)# vtp domain [YourDomainName]
   ```
   Replace [YourDomainName] with your chosen domain name.

3. **Configure the VTP Mode**

   Select the appropriate VTP mode based on the switch's role:

   - **Server Mode**:
     Switch(config)# vtp mode server
   - **Client Mode**:
     Switch(config)# vtp mode client
   - **Transparent Mode**:
     Switch(config)# vtp mode transparent
   - **Off Mode**: Switch(config)# vtp mode off

4. **Set a VTP Password (Optional)**

   To enhance security, set a VTP password. This ensures that only switches with the correct password can join the VTP domain:

```
Switch(config)# vtp password [YourPassword]
Replace [YourPassword] with a secure password.
```

5. **Specify the VTP Version**

   Choose the VTP version to use. Version 2 supports Token Ring VLANs, while Version 3 offers enhanced features like support for extended VLANs and improved security:

```
Switch(config)# vtp version [1 | 2 | 3]
Select the version number based on your network requirements.
```

6. **Enable VTP Pruning (Optional)**

   VTP pruning reduces unnecessary VLAN traffic on trunk links by preventing broadcasts of VLAN information to switches that do not have ports in that VLAN:

```
Switch(config)# vtp pruning
```

7. **Configure Trunk Ports**

   VTP advertisements are transmitted over trunk links. Configure the relevant interfaces as trunk ports:

```
Switch(config)# interface [interface-id]
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
```

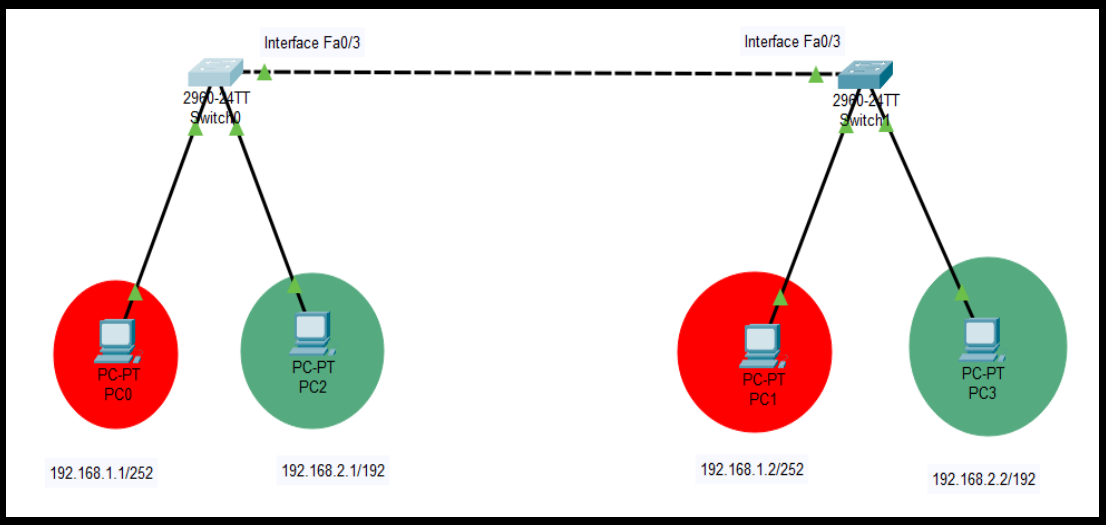
   Replace [interface-id] with the appropriate interface identifier, such as GigabitEthernet0/1.

8. **Verify VTP Configuration**

   After configuration, exit to privileged EXEC mode and verify the settings:

Switch# show vtp status
This command displays critical information

Example:



switch> enable
switch# conf t
switch(config)# int Fa0/3
switch(config-if)# switchport mode trunk

switch(config-if)# ex

switch(config)# vlan 100
switch(config-vlan)# name red

switch(config-if)# ex

switch(config)# vlan 200
switch(config-vlan)# name green

switch(config-vlan)# exit
switch(config)# exit
switch# exit

Or

Instead of typing exit three times, you can use end or CTRL+Z to exit all configuration modes at once and return to privileged EXEC mode (switch#).

switch# show vlan or show vlan brief