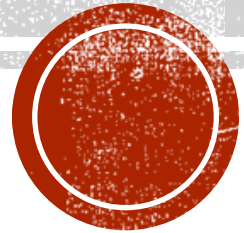
SWITCHING

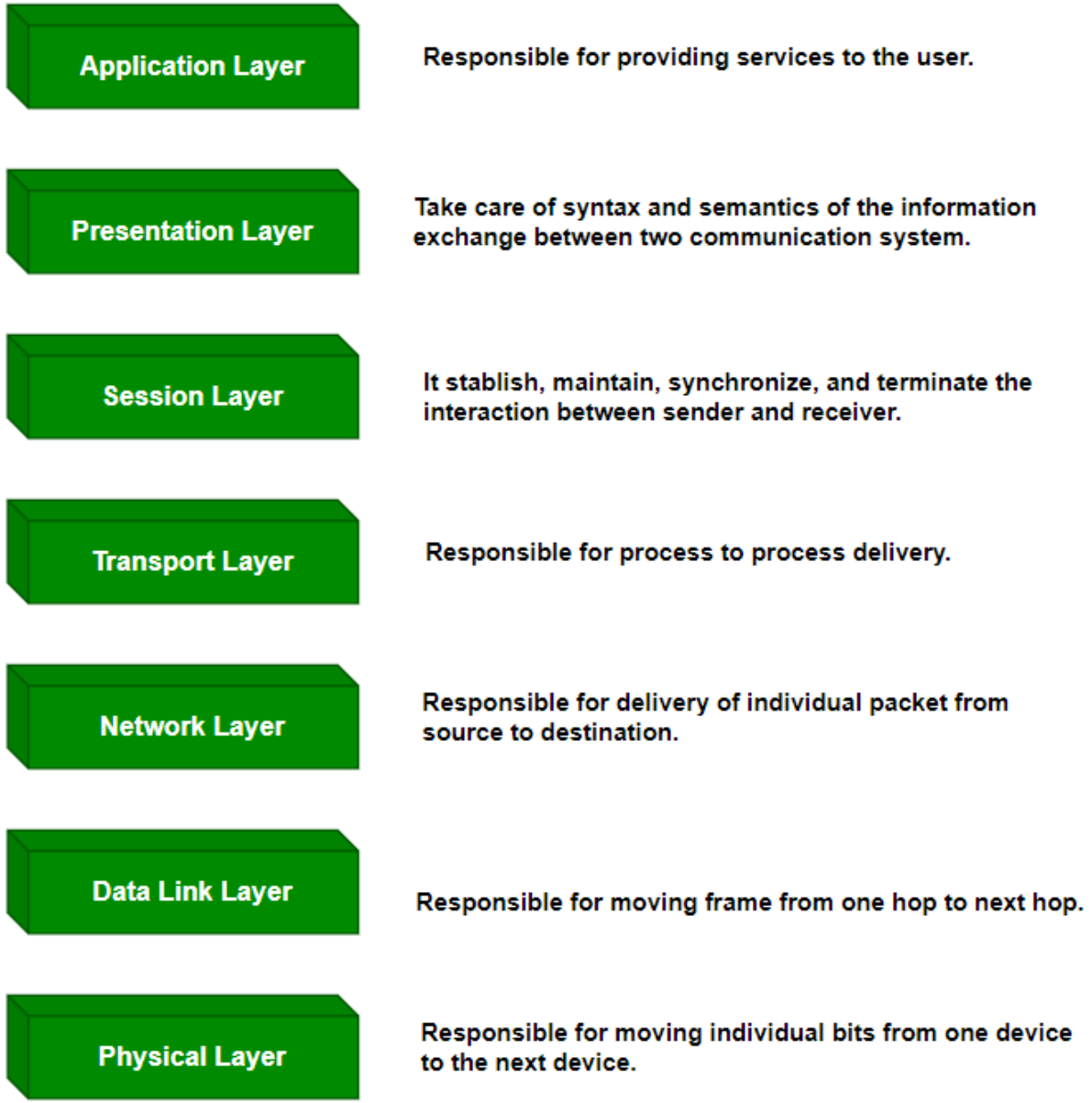


By

Jitendra Singh Tomar || Jeetu

OSI LAYERS

- Open System Interconnect (OSI) model.
- OSI is used to define how data is sent from one computer to another through network.
- Introduced by International Organization for Standardization (ISO) in 1984.
- It contains 7 layers.



OSI LAYERS

All

People

Should

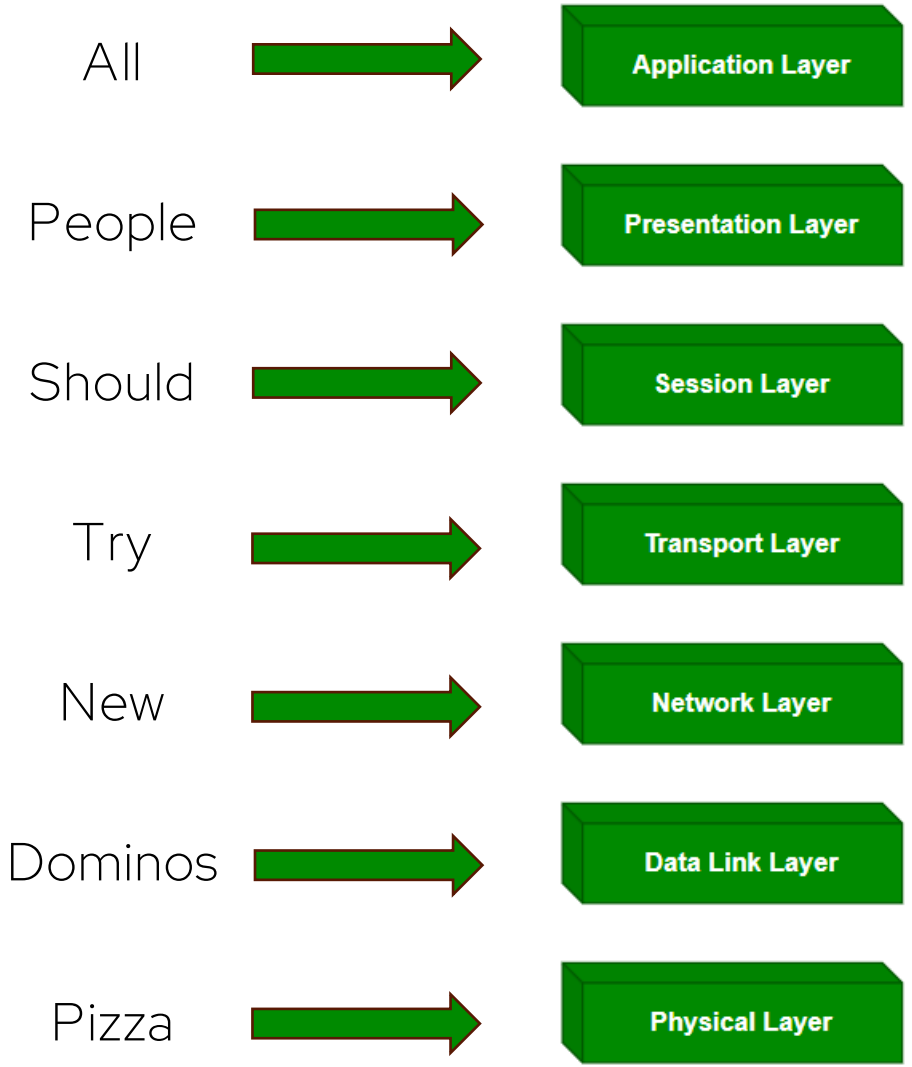
Try

New

Dominos

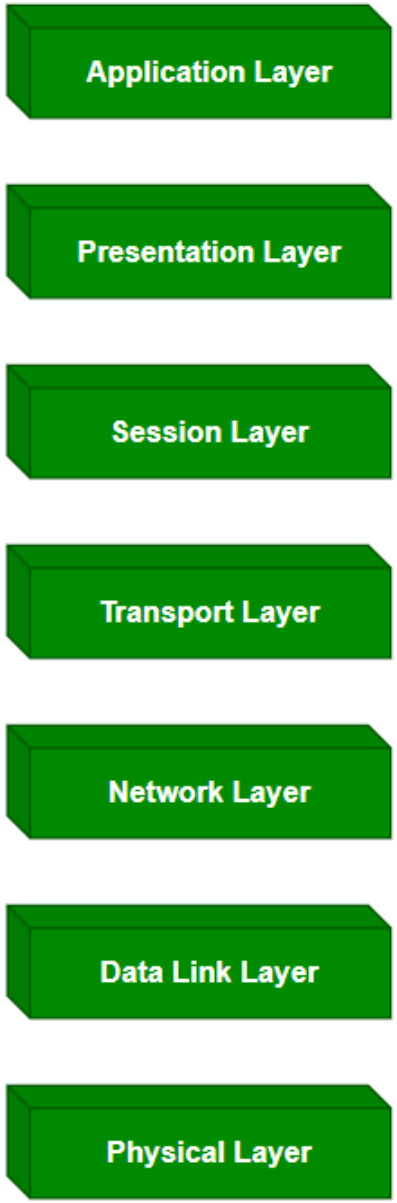
Pizza

OSI LAYERS

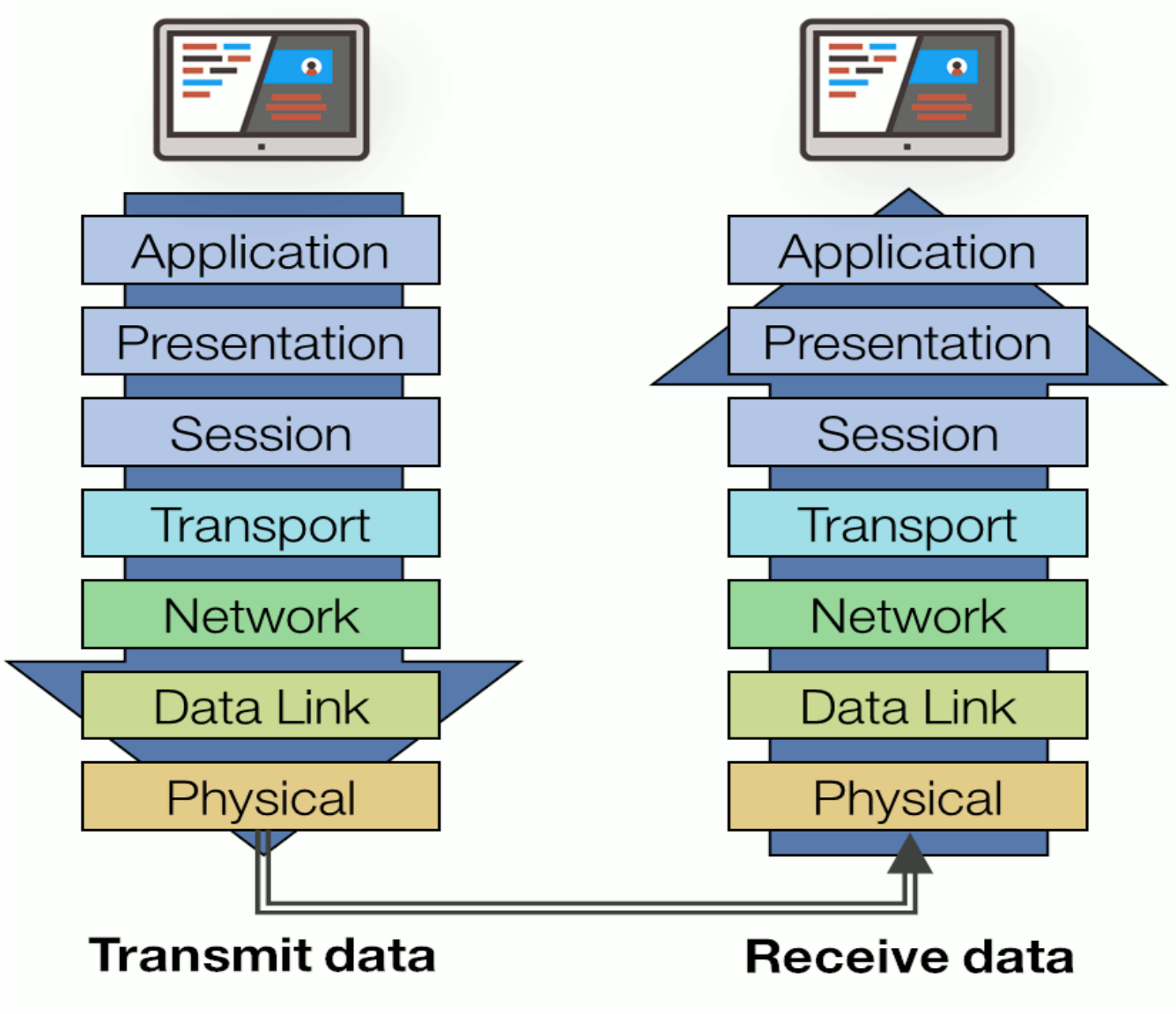

All
Application Layer
People
Presentation Layer
Should
Session Layer
Try
Transport Layer
New
Network Layer
Dominos
Data Link Layer
Pizza
Physical Layer

OSI LAYERS

- Application Layer: Applications create the data.
- Presentation Layer: Data is formatted, compressed and encrypted.
- Session Layer: Connections are established and managed.
- Transport Layer: Data is broken into segments for reliable delivery.
- Network Layer: Segments are packaged into packets and routed.
- Data Link Layer: Packets are framed and sent to the next device.
- Physical Layer: Frames are converted into bits and transmitted physically.



OSI LAYERS – SENDER & RECEIVER



LAYER 7: APPLICATION LAYER

- The Application layer is the highest layer of the OSI model.
- It provides the interface between the network protocol and the software running on the computer.
- This layer is used by "networking applications" like:
  - Google Chrome, Firefox, Skype, Teams, Etc.…
- It facilitates data formatting and translation for application use.
- It uses common protocols like:
  - HTTP, FTP, SMTP, DNS, Telnet, SSH, IMAP, POP, SNMP, etc.

LAYER 6: PRESENTATION LAYER

- This layer receives data from application layer in form of characters & numbers.
- This layer converts these characters into binary format & is called "translation".
- Here, data is compressed which requires less size to transmit which could be useful in scenarios like video streaming.
- It also encrypts the data by using SSL for secured transmission.
- It supports protocols like: SSL/TLS, JPEG, MPEG, ASCII
- It performs:
  - Data translation (into binary)
  - Data encryption/decryption (for security)
  - Data compression (for reduced size)

LAYER 5: SESSION LAYER

- The session layer manages sessions or connections between applications.
- It establishes, manages, and terminates sessions, ensuring that the data exchange between systems is synchronized.
- This layer is responsible for:
  - Authentication (who you are?)
  - Authorization (do you have permission?)
  - Placement of header information in a packet (where a message starts and where it ends)
- It supports protocols like: NetBIOS, RPC, SOCKS, L2TP, SDP, H.245, NFS, etc.
- Controls whether the data being exchanged in a session are transmitted as full or half duplex messages.

LAYER 4: TRANSPORT LAYER

- The Transport Layer ensures that messages are delivered error-free, in sequence and with no loss or duplication.
- It controls reliability of communication through:
  - Segmentation (divides data into small data units called segments)
  - Flow control (controls amount of data flow)
  - Error control (Automatic repeat request in case of transmission lost)
- This layer has:
  - Transmission Control Protocol (TCP) – Connection Oriented transmission
  - User Datagram Protocol (UDP) – Connection-less transmission

TCP VS UDP

UDP	TCP
- No feedback	- Send feedback
- Faster than TCP	- Slower in nature
- Example:	- Example:
- DNS	- World Wide Web
- Online games	- File Transfer Protocol (FTP)
- Online video streaming	- Emails
- Radio	

LAYER 3: NETWORK LAYER (INTERNET LAYER)

- Transport layer sends segments to this layer. Here, data units are called "Packets".
- This layer is primarily responsible for establishing the paths used for transfer of data packets between nodes on the network. This is the layer that routers operate on.
- Path determination (finding best path of delivery).
- This layer is responsible for:
  - Logical addressing (IP addresses)
  - Packet forwarding (routing through different routers)
  - Fragmentation and reassembly of packets
  - Handling traffic control (congestion management)

LAYER 3: NETWORK LAYER (INTERNET LAYER)

- The network layer also takes care of mapping logical (IP) addresses to physical (MAC) addresses that are used in the Data Link layer.
- Supported protocols:
  - IP (Internet Protocol) - IPv4 & IPv6
  - ICMP (Internet Control Message Protocol)
  - RIP (Routing Information Protocol)
  - OSPF (Open Shortest Path First)
  - BGP (Border Gateway Protocol)
  - MPLS (Multiprotocol Label Switching)

LAYER 2: DATA LINK LAYER

- At the Data Link layer, data packets are encoded into bits.
- This layer is responsible for establishing, maintaining, and terminating a link between two directly connected nodes.
- It ensures error-free transmission between devices on the same network and controls how data is placed on the physical medium.
- MAC address of sender & receiver is assigned to packet to create a frame.
  - MAC address is a 12 digit, alpha-numeric number embedded on NIC by manufacturer.
- Supported protocols: ARP, PPP, Token ring, L2TP, etc

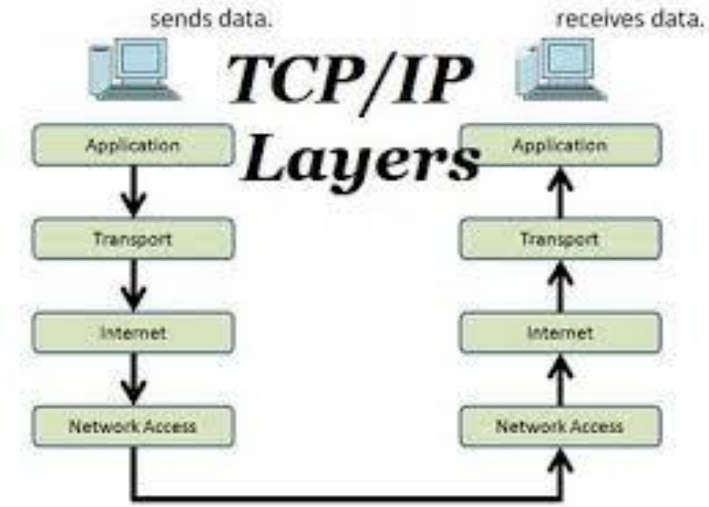
LAYER 1: PHYSICAL LAYER

- This layer converts data from data link layer into signals.
- This layer is the lowest layer of the OSI model and consists of the functionality that interacts with the actual hardware and signaling mechanism.
- This layer is responsible for:
  - Defines the physical characteristics of the network (cables, connectors, voltage levels).
  - Handles the transmission of binary data (0s and 1s) as electrical, optical, or radio signals.
  - Manages the data rate and synchronization of bit-level communication.
- Supported protocols: Ethernet, USB, Bluetooth, Infrared,

TCP/IP MODEL

OSI Model	TCP/IP (4 layer)	TCP/IP (5 layer)
Application	Application	Application
Presentation		
Session		
Transport	Transport	Transport
Network	Network	Internet layer
Data Link	Network Access	Data link
Physical		Physical layer

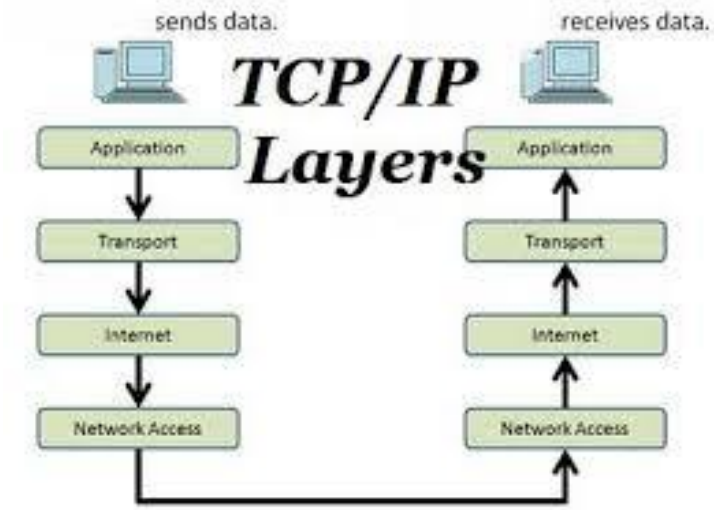
TCP/IP MODEL - APPLICATION LAYER



- The TCP/IP model is a fundamental framework for computer networking.
- It consists of four layers: *the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer*.
- Each layer has specific functions that help manage different aspects of network communication, making it essential for understanding and working with modern networks.
- The main work of TCP/IP is to transfer the data of a computer from one device to another.
- The TCP/IP model is used in the context of the real-world internet, where a wide range of physical media and network technologies are in use.

TCP/IP MODEL - APPLICATION LAYER

- This model defines how data is transmitted over networks, ensuring reliable communication between devices.
- This layer corresponds to the Application, Presentation, and Session layers of the OSI model.
- This layer:
  - Provides protocols that allow software applications to send and receive data over the network.
  - Manages the formatting, encryption, and compression of data for use by applications.
  - Supports the establishment, maintenance, and termination of communication sessions between applications.



TCP/IP – APPLICATION LAYER

- This protocol supports:
  - HTTP/HTTPS (Hypertext Transfer Protocol/Secure) – Web browsing.
  - FTP (File Transfer Protocol) – File transfers.
  - SMTP (Simple Mail Transfer Protocol) – Email transmission.
  - DNS (Domain Name System) – Resolving domain names to IP addresses.
  - Telnet, SSH (Secure Shell) – Remote access to servers.
  - SNMP (Simple Network Management Protocol) – Network management.

TCP/IP - TRANSPORT LAYER

- The Transport Layer ensures reliable data transfer between devices.
- It is responsible for maintaining the end-to-end communication, error-checking, and data flow control.
- Functionalities of this layer:
  - Establishes, maintains, and terminates connections between devices.
  - Segments and reassembles data into a format that can be transmitted over the network.
  - Provides flow control to prevent network congestion and ensures that data is delivered in sequence.
  - Offers error-checking mechanisms to detect and recover from data transmission errors.

TCP/IP - TRANSPORT LAYER

- Standard protocols used here are:
  - TCP (Transmission Control Protocol) - Ensures reliable, connection-oriented communication.
  - UDP (User Datagram Protocol) - Supports fast, connectionless communication with no guarantee of delivery.

TCP/IP - INTERNET LAYER

- The Internet Layer is responsible for routing data across networks and ensuring that it reaches its destination.
- It is equivalent to the Network Layer in the OSI model.
- In this layer:
  - Logical addressing (IP addresses) to identify devices across different networks.
  - Routing of data packets from the source network to the destination network, possibly across multiple networks.
  - Fragmentation and reassembly of data packets if the data exceeds the size limit of a network.
- This protocol supports: IP, ICMP, IGMP, IPSec

TCP/IP - NETWORK INTERFACE LAYER (LINK LAYER)

- The Network Interface Layer is responsible for the physical transmission of data over a network. It corresponds to the combination of the Physical and Data Link layers in the OSI model.
- In this layer, it:
  - Defines how data is sent over the physical medium (cables, radio waves).
  - Handles hardware addressing (MAC addresses) and error detection within the local network.
  - Manages frame placement on the network and ensures data reaches its immediate destination within the same network.

TCP/IP - NETWORK INTERFACE LAYER (LINK LAYER)

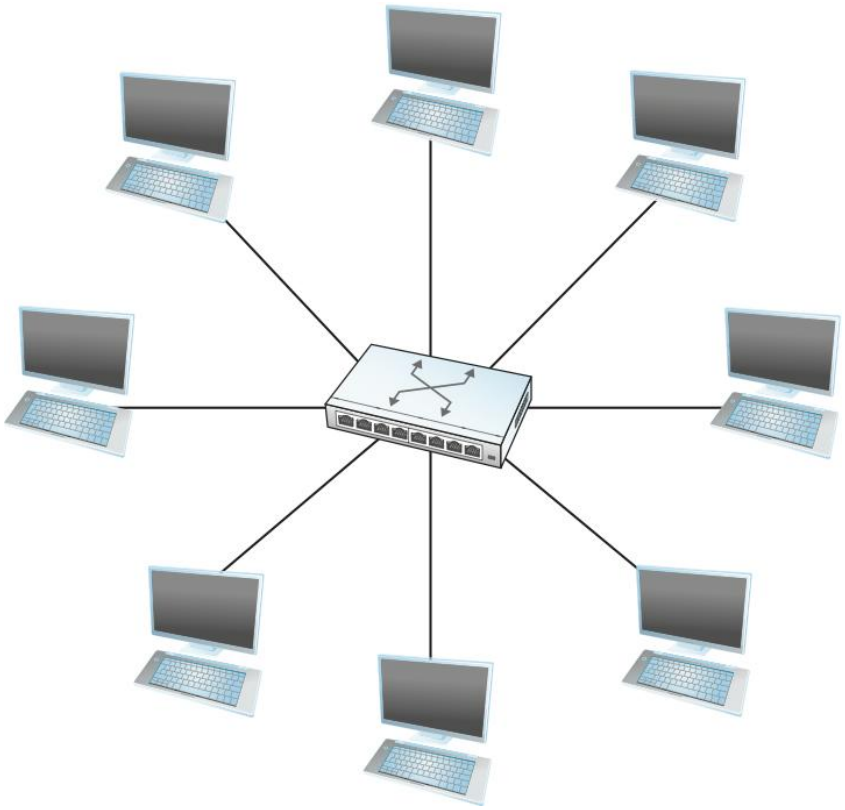
- This layer supported protocols/standards:
  - Ethernet
  - Wi-Fi (IEEE 802.11)
  - ARP (Address Resolution Protocol)
  - PPP (Point-to-Point Protocol)

OSI – TCP/IP IN A NUTSHELL

TCP/IP	OSI Layer	Functions	PDUs	Protocols	Devices
Application Layer	Application	User layer	Data	HTTP, FTP, SMTP	App FW, VPN, SSL, Proxies
	Presentation	Encrypt, Compress, Converts		ASCII, JPEG, DOC	
	Session	Open & Closes session		RPC, TLS	
Transport	Transport	Ensures Delivery	Segments	TCP, UDP	LB, N/W Firewall
Network	Network	Control Routing	Packet	IP, IPSec	Routers Layer 3 Switches
Physical Layer	Data Link	Error free data transfer	Frame	Ethernet, MAC	NIC, Switches
	Physical Layer	BITS			RJ45

BASICS OF SWITCHING

- A switch is a mechanism that allows you to interconnect links to form a larger network.
- A switch is a multi-input, multi-output device that transfers packets from an input to one or more outputs.
- A switch's primary job is to receive incoming packets on one of its links and to transmit them on some other link.
  - This function is sometimes referred to as either switching or forwarding, and in terms of the Open Systems Interconnection (OSI) architecture, it is considered a function of the network layer.



HOW DOES A NETWORK SWITCH WORK?

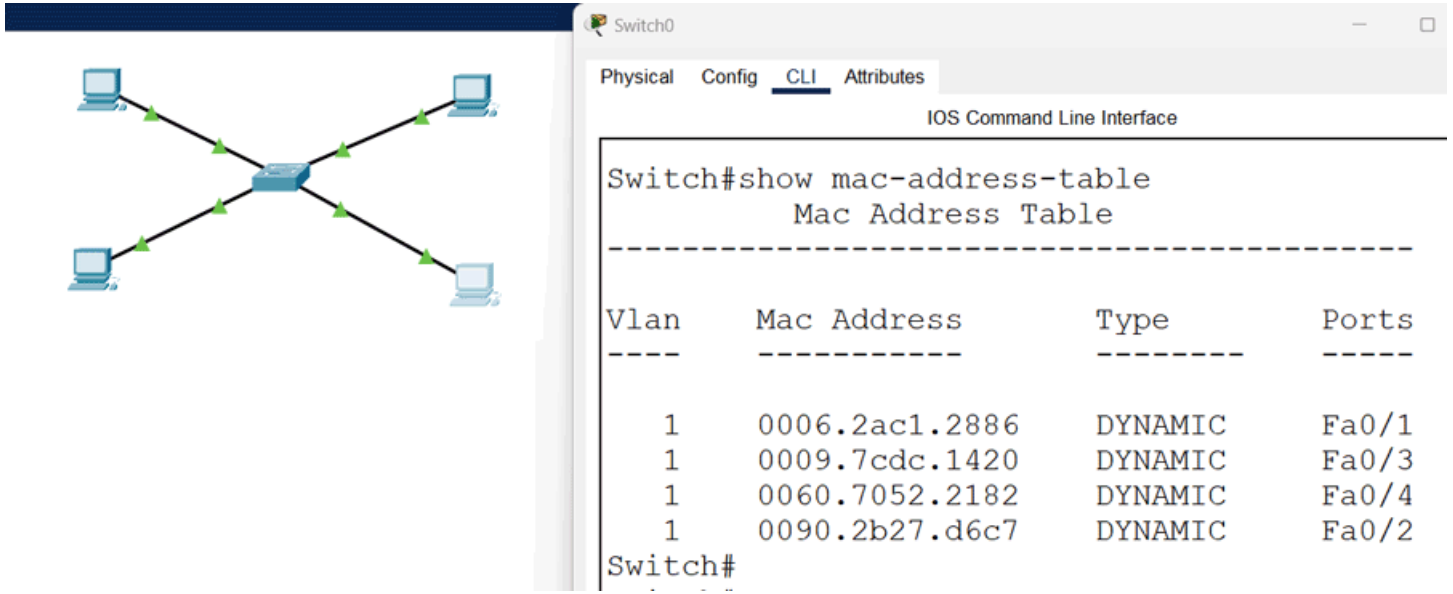
- A network switch can work in three ways:
  - Edge switches, also known as access switches: They handle traffic entering and departing the network. Edge switches link various devices, including personal computers and access points.
  - Aggregation switches: Switches for aggregation are located within an optional intermediary layer. These connect to edge switches, which may transmit traffic from one switch to another or up to the core switches.
  - Core switches: The network's backbone is made up of these switches. Core switches link edge or aggregation switches, device or consumer edge networks to networks at data centers, and routers to organizational LANs.

MAC/CAM TABLE

- Content Addressable Memory / Media Access Control
- Ethernet switches store the MAC addresses of all connected devices in a table known as CAM or MAC address table and use it to make forwarding decisions.
- The CAM table is also known as
  - MAC forward table,
  - MAC filter table,
  - MAC address table,
  - Switching table, or
  - Bridging table.

MAC/CAM TABLE

- A CAM table uses entries to store information in two ways
  - Static & Dynamic.
- In the static method, we manually add entries to the CAM table.
- In the dynamic method, the switch automatically adds entries to the CAM table.



COMPONENTS OF SWITCH

- Switching Fabric:
  - The switching fabric is the internal connection that allows data to be transferred between ports. It determines the switch's capacity to handle data traffic.
- Ports:
  - These are the physical interfaces where network cables connect. Ports can support different speeds like 10/100/1000 Mbps (Ethernet) or even 10 Gbps.
- MAC Address Table (Content Addressable Memory - CAM):
  - This table stores the MAC addresses of devices connected to the switch along with the corresponding port numbers. It allows the switch to forward frames to the correct destination.
- Central Processing Unit (CPU):
  - The CPU controls the switch's operations, including processing management tasks, running the switch’s firmware, and managing data traffic.

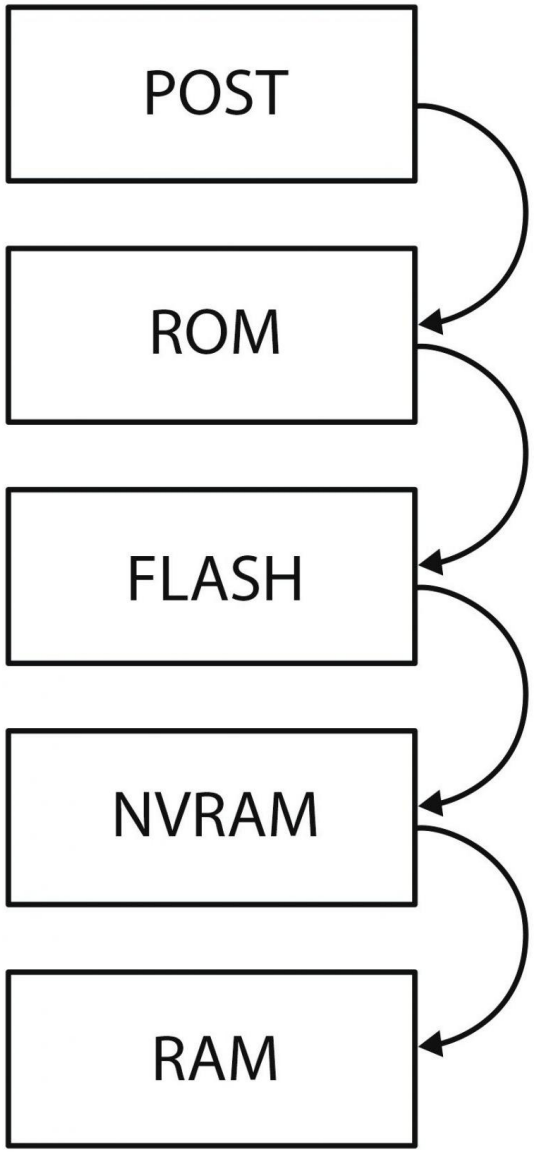
COMPONENTS OF SWITCH

- Memory (RAM and Flash):
  - RAM is used for running the switch’s operating system and for temporarily storing data during operations.
  - Flash memory stores the switch's operating system, configuration files, and other essential data.
- Power Supply:
  - The power supply provides the necessary power to all the internal components of the switch.
- Cooling System:
  - Switches often have fans or heat sinks to dissipate heat generated by the internal components.

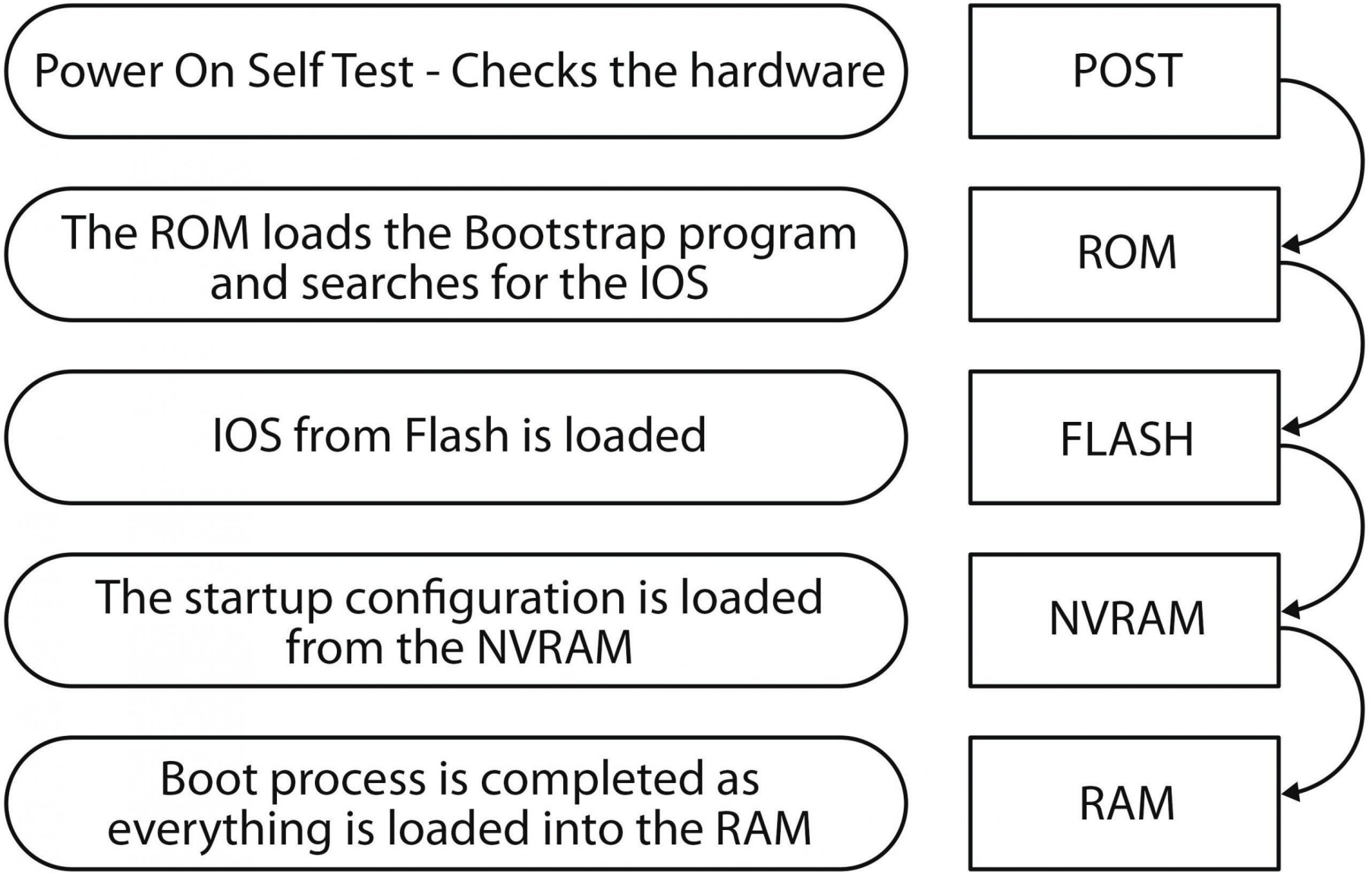
COMPONENTS OF SWITCH

- Application-Specific Integrated Circuits (ASICs):
  - These specialized chips are designed to handle the data forwarding process at high speeds, enabling the switch to perform at wire-speed without burdening the CPU.
- Network Interface Cards (NICs):
  - These cards are responsible for managing the physical network connections and converting data from the switch to the appropriate network media (e.g., copper, fiber).
- Management Interface:
  - includes both hardware and software components that allow network administrators to configure, monitor, and manage the switch, often through a web interface, CLI, or SNMP.

BOOTING PROCESS OF SWITCH



BOOTING PROCESS OF SWITCH



BOOTING PROCESS OF SWITCH

After a Cisco switch is powered on, it goes through the following boot sequence:

- First, the switch loads a power-on self-test (POST) program stored in ROM.
  - POST checks the CPU subsystem.
  - It tests the CPU, DRAM, and the portion of the flash device that makes up the flash file system.
- Next, the switch loads the boot loader software.
  - The boot loader is a small program stored in ROM and is run immediately after POST successfully completes.

BOOTING PROCESS OF SWITCH

- The boot loader performs low-level CPU initialization.
  - It initializes the CPU registers, which control where physical memory is mapped, the quantity of memory, and its speed.
- The boot loader initializes the flash file system on the system board.
- Finally, the boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.

BOOTING PROCESS OF SWITCH

IOS Command Line Interface

```
C2950 Boot Loader (C2950-HBOOT-M) Version 12.1(11r)EA1, RELEASE SOFTWARE (fc1)
Compiled Mon 22-Jul-02 18:57 by miwang
Cisco WS-C2950T-24 (RC32300) processor (revision C0) with 21039K bytes of memory.
2950T-24 starting...
Base ethernet MAC Address: 0050.0FCE.1740
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 3058048
flashfs[0]: Bytes available: 60958336
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2950-i6q4l2-mz.121-22.EA4.bin"...
################################################################################ [OK]
              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706
```

TYPES OF SWITCHES

- Virtual Switches: Virtual Switches are the switches that are inside Virtual Machine hosting environments.
- Routing Switches: These are the switches that are used to connect LANs. They also have the work of performing functions in the Network Layer of the OSI Model.
- Unmanaged Switches: Unmanaged Switches are the devices that are used to enable Ethernet devices that help in automatic data passing. These are generally used for home networks and small businesses.

TYPES OF SWITCHES

- Managed Switches: Managed Switches are switches having more complex networks. SNMP (Simple Network Management Protocol) can be used for configuring managed switches.
- LAN Switches: LAN (Local Area Network) Switches are also called ethernet switches or data switches. LAN switches always try to avoid overlapping of data packets in the network just by allocating bandwidth in such a manner.
- PoE Switches: Power over Ethernet(PoE) are the switches used in Gigabit Ethernets. PoE help in combining data and power transmission over the same cable so that it helps in receiving data and electricity over the same line.

TYPES OF SWITCHES

- Smart Switches: Smart Switches are switches having some extra controls on data transmissions but also have extra limitations over managed Switches. They are also called partially managed switches.
- Stackable Switches: Stackable switches are connected through a backplane to combine two logical switches into a single switch.
- Modular Switches: These types of switches help in accommodating two or more cards. Modular switches help in providing better flexibility.

BASIC CONFIGURATION(CLI)

- Working with "User EXEC mode":

```
Switch>enable
Switch#?
Exec commands:
  clear          Reset functions
  clock          Manage the system clock
  configure      Enter configuration mode
  connect        Open a terminal connection
  copy           Copy from one file to another
  debug          Debugging functions (see also 'undebug')
  delete         Delete a file
  dir            List files on a filesystem
  disable        Turn off privileged commands
  disconnect     Disconnect an existing network connection
  enable         Turn on privileged commands
  erase          Erase a filesystem
```

BASIC CONFIGURATION(CLI)

- Disabling "User EXEC mode" & then enabling configuration terminal:

```
Switch#disable
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#?
Configure commands:
  access-list         Add an access list entry
  banner              Define a login banner
  boot                Boot Commands
  cdp                 Global CDP configuration subcommands
  clock               Configure time-of-day clock
  crypto              Encryption module
  default             Set a command to its defaults
```

BASIC CONFIGURATION(CLI)

- Changing the banner on Cisco IOS:

```
Switch(config)#banner motd #
Enter TEXT message.  End with the character '#'.
THis is a limited access area.
#
```

```
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#exit



Switch con0 is now available



Press RETURN to get started.



THis is a limited access area.

Switch>
```

CONFIGURING PASSWORD

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#exit
```

On next login,

```
Press RETURN to get started.



User Access Verification

Password:

Switch>
```

CONFIGURING USERNAME AND PASSWORD

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#line console 0
Switch(config-line)#login local
Switch(config-line)#exit
Switch(config)#
Switch(config)#username jeetu password singh
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#exit
```

On next login,

```
User Access Verification

Username: jeetu
Password:

Switch>
```

CONFIGURING SECRET

- It's the alternative of password in Cisco environment.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#enable secret ?
  0       Specifies an UNENCRYPTED password will follow
  5       Specifies an ENCRYPTED secret will follow
  LINE    The UNENCRYPTED (cleartext) 'enable' secret
  level   Set exec level password
Switch(config)#enable secret cisco

Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show running-config | include secret
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
Switch#exit
```

```
User Access Verification

Username: jeetu
Password:

Switch>en
Password:
Password:
Password:
Switch#
Switch#
```

CONFIGURING PASSWORD PERMANENTLY

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#wr
Building configuration...
[OK]
Switch#
```

On next login,

```
User Access Verification

Username: jeetu
Password:

Switch>enable
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

- Username: **Jeetu**
- Password: **singh**
- Admin mode pwd: **cisco**

CONFIGURING TELNET ACCESS AND PASSWORD

```
Username: jeetu
Password:

Switch>en
Password:
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#no shut

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#ip add 192.168.10.10 255.255.255.0
Switch(config-if)#exit
Switch(config)#
Switch(config)#line vty 0 4
Switch(config-line)#password joker
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#enable secret joker
Switch(config)#
Switch(config)#
Switch(config)#
```

```
Switch#telnet 192.168.10.10
Trying 192.168.10.10 ...Open

User Access Verification

Password:
Switch>sh run
          ^
% Invalid input detected at '^' marker.

Switch>en
Password:
Password:
Switch#sh run
Building configuration...

Current configuration : 1235 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$W9QOfSPLczXr.bamhg.yv/
!
!
!
!
username jeetu privilege 1 password 0 singh
!
!
```

SHOWING MAC ADDRESS TABLE

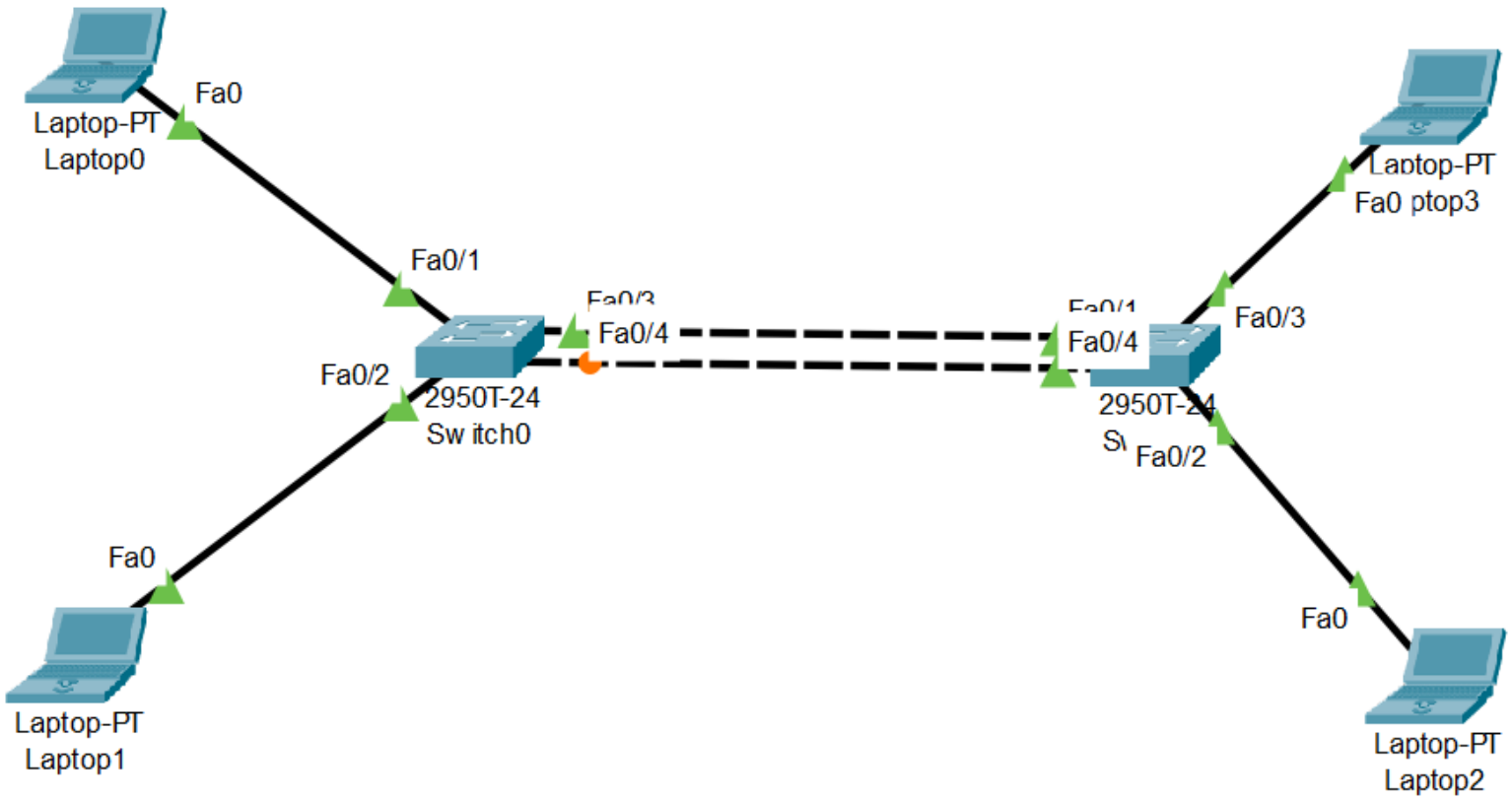
Before pinging switch & PC

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Switch#
```

After pinging switch & PC

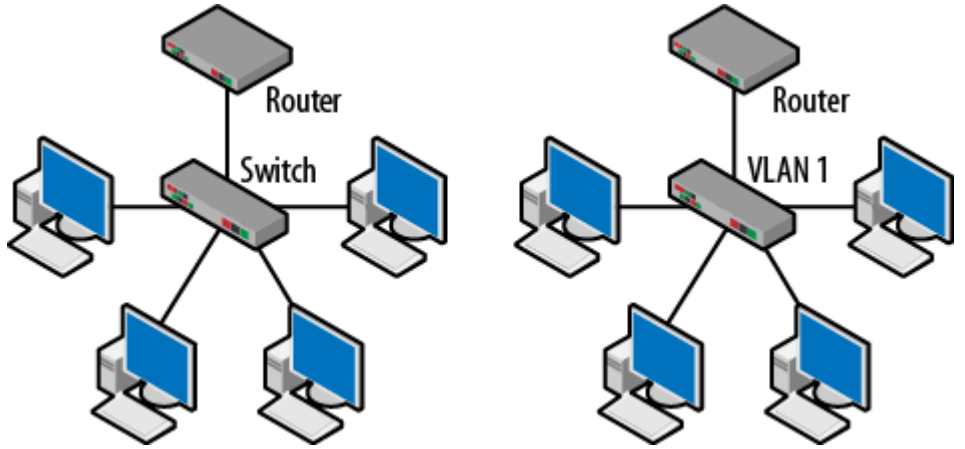
```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c77c.1371    DYNAMIC     Fa0/1
```

TASK


Laptop-PT
Laptop0
Fa0
Fa0/1
Fa0/2
2950T-24
Sw itch0
Fa0/4
Fa0/4
Fa0/3
Laptop-PT
Fa0 ptop3
2950T-24
Fa0/2
Fa0
Laptop-PT
Laptop1
Fa0
Laptop-PT
Laptop2

VLAN

- A VLAN is a group of end stations in a switched network that is logically segmented by function or application, without regard to the physical locations of the users.
- VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment.
- Under IEEE 802.1Q, the maximum number of VLANs on a given Ethernet network is 4,094.
- VLANs provide a number of advantages including
  - ease of administration,
  - confinement of broadcast domains,
  - reduced network traffic, and
  - enforcement of security policies.



VLAN RANGES

- VLAN 0, 4095: These are reserved VLAN which cannot be seen or used.
- VLAN 1: It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.
- VLAN 2-1001: This is a normal VLAN range. We can create, edit and delete these VLAN.
- VLAN 1002-1005: These are CISCO defaults for FDDI and token rings. *These VLAN can't be deleted.*
- VLAN 1006-4094: This is the *extended range* of VLAN.

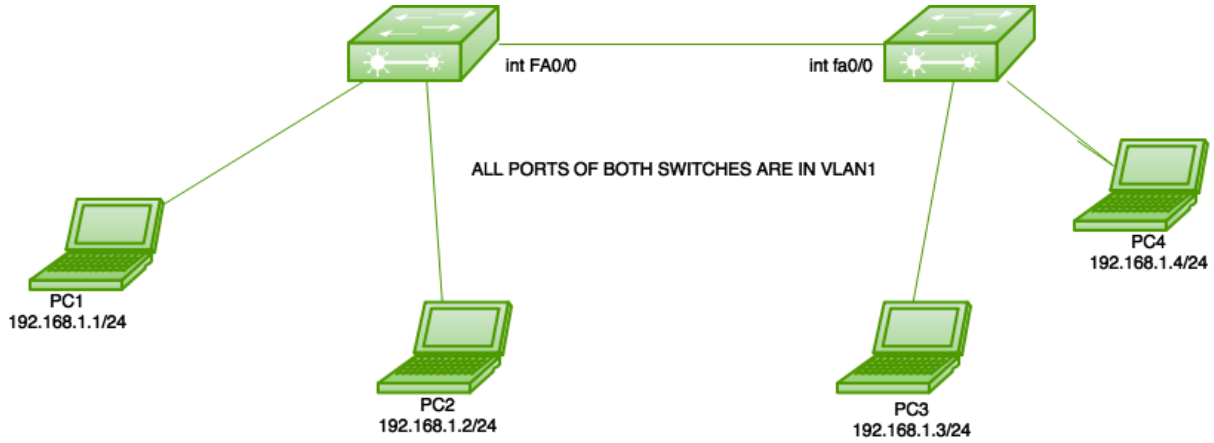
KEY FEATURES OF VLANS

- VLAN tagging: VLAN tagging is a way to identify and distinguish VLAN traffic from other network traffic. This is typically done by adding a VLAN tag to the Ethernet frame header.
- VLAN membership: VLAN membership determines which devices are assigned to which VLANs. Devices can be assigned to VLANs based on port, MAC address, or other criteria.
- VLAN Trunking: VLAN Trunking allows multiple VLANs to be carried over a single physical link. This is typically done using a protocol such as IEEE 802.1Q.
- VLAN management: VLAN management involves configuring and managing VLANs, including assigning devices to VLANs, configuring VLAN tags, and configuring VLAN Trunking.

VLAN - ACCESS PORTS

Types of connections in VLAN:

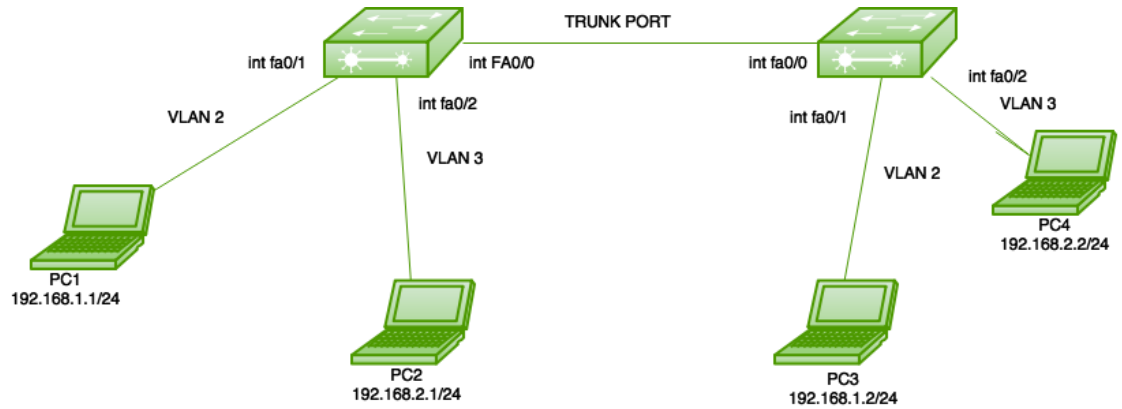
- Access link –
  - It connects PC/Laptops and Switches together.
  - Its part of single VLAN.



VLAN - TRUNK PORTS

Types of connections in VLAN:

- Trunk Link –
  - It connects 2 or more switches together.
  - It allows 2 VLANs of different switches to communicate to each other.



TO SHOW VLAN

- Command:
  - # show vlan

```
SW1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, 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, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

TO CREATE VLAN

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#
SW1(config)#vlan 10
SW1(config-vlan)#vl
SW1(config-vlan)#v
SW1(config-vlan)#v
SW1(config-vlan)#nam
SW1(config-vlan)#name marketing
SW1(config-vlan)#exit
```

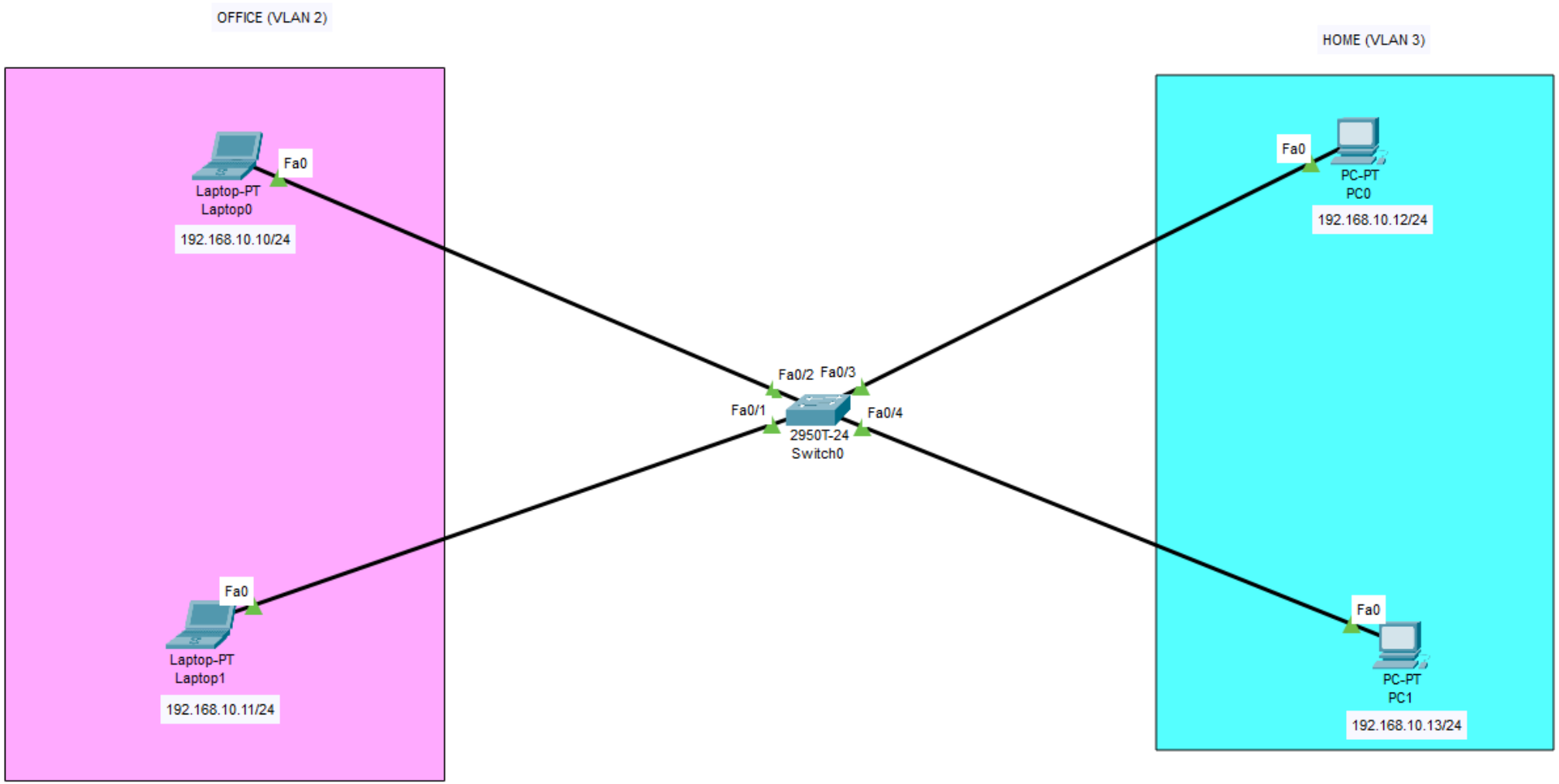
```
SW1(config)#exit
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, 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, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   marketing                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW1#
```

DELETING VLAN

```
SW1(config)#
SW1(config)#no vlan 10
```

```
SW1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, 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, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

HOME-OFFICE VLAN



HOME-OFFICE VLAN - COMMANDS

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name
% Incomplete command.
Switch(config-vlan)#
Switch(config-vlan)#name office
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 3
Switch(config-vlan)#name home
Switch(config-vlan)#exit
```

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#
Switch(config)#interface fastethernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#
Switch(config)#interface fastethernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#
Switch(config)#exit
Switch#
```

HOME-OFFICE VLAN – VERIFY

```
Switch#show vlan

VLAN Name                                Status
---- ----------------------------------- ---------
1    default                             active
2    office                              active
3    home                                active
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.10.13

Pinging 192.168.10.13 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	Laptop1	ICMP		0.000	N	0	(edit)	
	Failed	Laptop0	PC1	ICMP		0.000	N	1	(edit)	
	Successful	PC0	PC1	ICMP		0.000	N	2	(edit)	

DYNAMIC TRUNKING PROTOCOL (DTP)

- Dynamic Trunking Protocol (DTP) is *a proprietary Cisco protocol* used to manage trunk links between Cisco switches.
- It automates the negotiation of trunking on a link between two devices and manages the trunking mode on that link.
- Trunk links allow multiple VLANs to pass through a single physical connection.
- The main purpose of DTP is to dynamically configure and establish trunk links between switches without manual intervention.

DTP OPERATIONAL MODES

Mode	Description
Access	Forces the port to operate in access mode (no trunking).
Trunk	Forces the port to operate as a trunk, carrying multiple VLANs.
Dynamic Desirable	Actively tries to negotiate a trunk link.
Dynamic Auto	Passively waits for the other side to initiate trunking negotiation.
Nonegotiate	Disables DTP; the port operates in static mode (either access or trunk).

DYNAMIC TRUNKING PROTOCOL (DTP)

- Manual commands (not recommended)
  - # switchport mode access
  - # switchport mode trunk
- DTP configuration:
  - Switchport mode dynamic auto
  - Switchport mode dynamic desirable
  - Switchport nonegotiate

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
```

```
Switch>en
Switch#sh int fa0/1 sw
Switch#sh int fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 2 (office)
Trunking Native Mode VLAN: 1 (default)
```

DYNAMIC TRUNKING PROTOCOL (DTP)

- Switchport mode dynamic auto
  - It will form a trunk if the neighbor switch port is set to trunk or desirable.
  - Trunk will not be formed if both sides are set to auto.
  - Default on newer switches.
- Switchport mode dynamic desirable
  - Will form a trunk if the neighbour switch port is set to trunk, desirable or auto.
  - Default on older switches.
- Switchport nonegotiate
  - Disabled DTP

DYNAMIC TRUNKING PROTOCOL (DTP)

For new switch (default)

```
Switch#show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

After changing

```
Switch(config)#
Switch(config)#int fa0/1
Switch(config-if)#switchport mode dy
Switch(config-if)#switchport mode dynamic des
Switch(config-if)#switchport mode dynamic desirable
Switch(config-if)#
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Verify:

```
Switch#show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

For 2 switches connected together

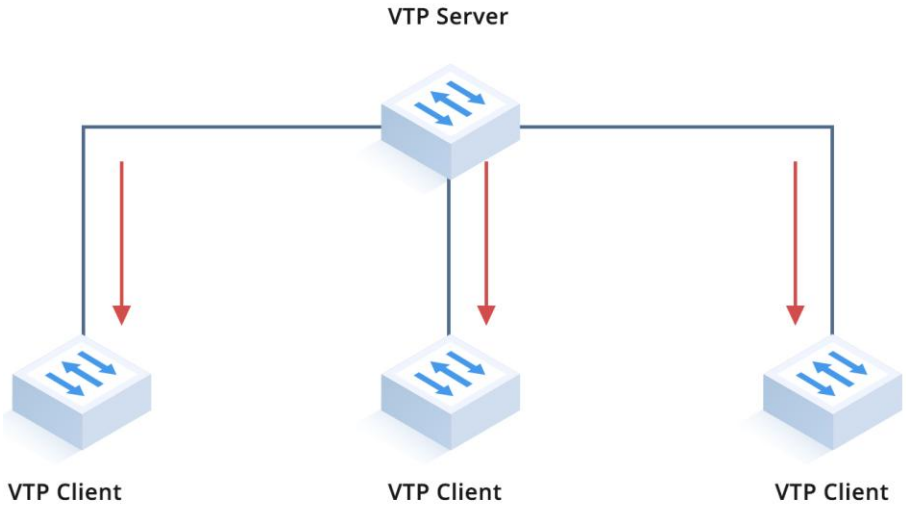
DTP – MODE COMBINATIONS

Local Port Mode	Remote Port Mode	Result
Trunk	Trunk	Trunk
Trunk	Dynamic Auto	Trunk
Trunk	Dynamic Desirable	Trunk
Dynamic Desirable	Dynamic Desirable	Trunk
Dynamic Auto	Dynamic Desirable	Trunk
Dynamic Auto	Dynamic Auto	Access (trunk not negotiated)
Nonegotiate	Any Mode	No trunking; operates in static mode.

DTP

Advantages	Disadvantages
Automates the process of establishing trunk links.	A malicious device can exploit DTP to gain access to VLANs on the trunk.
Allows for dynamic configuration, reducing manual errors.	Mitigation: Use "nonegotiate" mode and disable unused ports.

VLAN TRUNKING PROTOCOL



- VTP is a *Cisco proprietary protocol* that manages VLAN configurations across a network of switches.
- It helps in reducing misconfiguration of VLAN on multiple switches (say 10, 15, 30 or more switches) while trying to replicate the configuration.
- VTP helps you simplify the management of VLAN database across multiple switches.
- If you create VLAN on a single switch, then it gets replicated on all the switches by using VTP.
- Pre-requisites:
  - To make “trunk” on any 1 of the switch's interface, on another interface it will be created manually.

VTP COMMANDS

- # show vlan // list existing VLANs

```
Switch>show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Note:
Ensure to enable Trunking on all switches to work with VTP

switchport mode dynamic desirable

- Creating VTP:

```
Switch(config)#vtp domain newvtp1
Changing VTP domain name from NULL to newvtp1
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

VTP – CREATION & VERIFY

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
```

VTP STATUS – BY DEFAULT

```
Switch#show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

VTP STATUS – CHANGING ON SWITCH 1

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain testingVTP
Changing VTP domain name from NULL to testingVTP
Switch(config)#
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : testingVTP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x28 0x11 0x63 0xF6 0xB3 0x38 0xCA 0xE7
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

VTP STATUS – CHANGED ON SWITCH 2

Switch2

```
Switch>en
Switch#show vtp sta
Switch#show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : testingVTP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x28 0x11 0x63 0xF6 0xB3 0x38 0xCA 0xE7
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

CREATING VLAN USING VTP – SWITCH 1

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#vlan 100
Switch(config-vlan)#name vtplan1
Switch(config-vlan)#
```

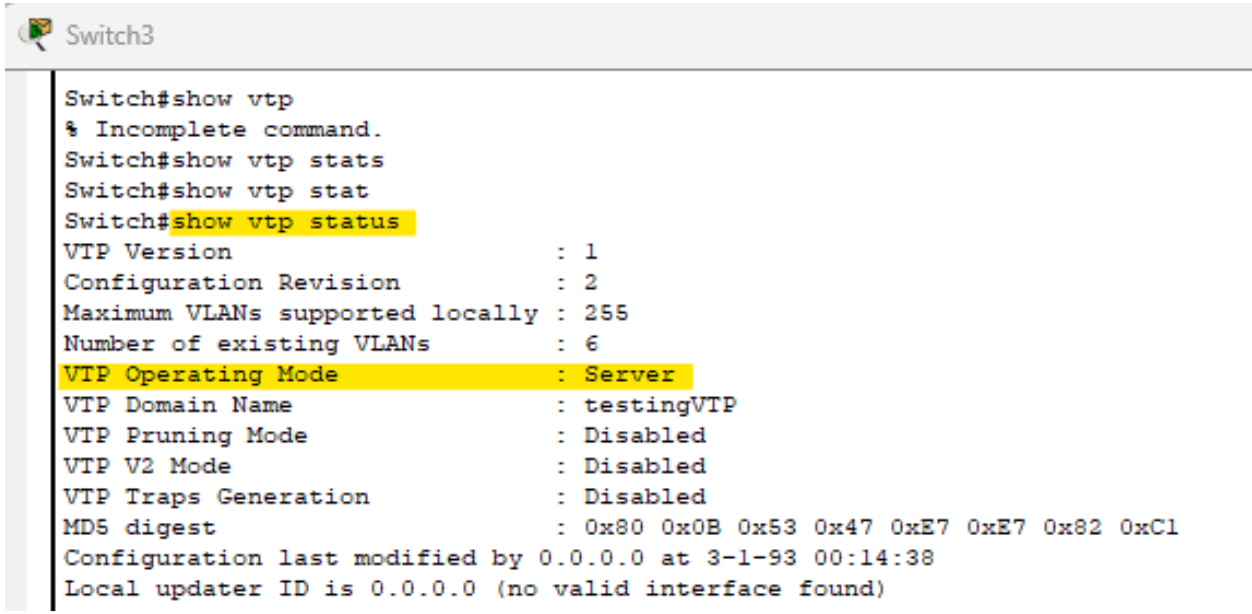
Checking on Switch 2

Switch3

```
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
100  vtplan1                    active
1002 fddi-default               active
1003 token-ring-default         active
1004 fddinet-default            active
1005 trnet-default              active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
 --More--
```

MODES OF VTP

- Client
  - Cannot create, change or delete VLANs.
  - Forwards advertisements to other switches.
  - Does not save VLAN configuration on NVRAM.
- Server (by default)
  - Creates, modifies and deletes VLANs.
  - Sends & Forwards advertisements to other switches.
  - Saves VLAN configuration in NVRAM. (filename: vlan.dat(flash file)
- Transparent
  - It forwards the advertisements to another switches but do not stores on that switches.



VTP VERSIONS

- VTP Version 1:
  - Basic VTP functionality, supports standard VLANs.
- VTP Version 2:
  - Adds support for Token Ring VLANs and other minor improvements.
- VTP Version 3:
  - Supports extended VLANs (VLANs above 1005).
  - Enhanced security and support for private VLANs.

CONFIGURING VTP

Switch1

```
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB0 0xC3 0xAD 0x29 0xC8 0x7C 0x16 0x0D
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain demo
Domain name already set to demo.
Switch(config)#vtp domain newdomain
Changing VTP domain name from demo to newdomain
Switch(config)#00:05:15 %DTP-5-DOMAINMISMATCH: Unable to perform trunk negotiation on
port Fa0/1 because of VTP domain mismatch.

00:05:45 %DTP-5-DOMAINMISMATCH: Unable to perform trunk negotiation on port Fa0/1
because of VTP domain mismatch.

00:06:15 %DTP-5-DOMAINMISMATCH: Unable to perform trunk negotiation on port Fa0/1
because of VTP domain mismatch.


Switch(config)#
```

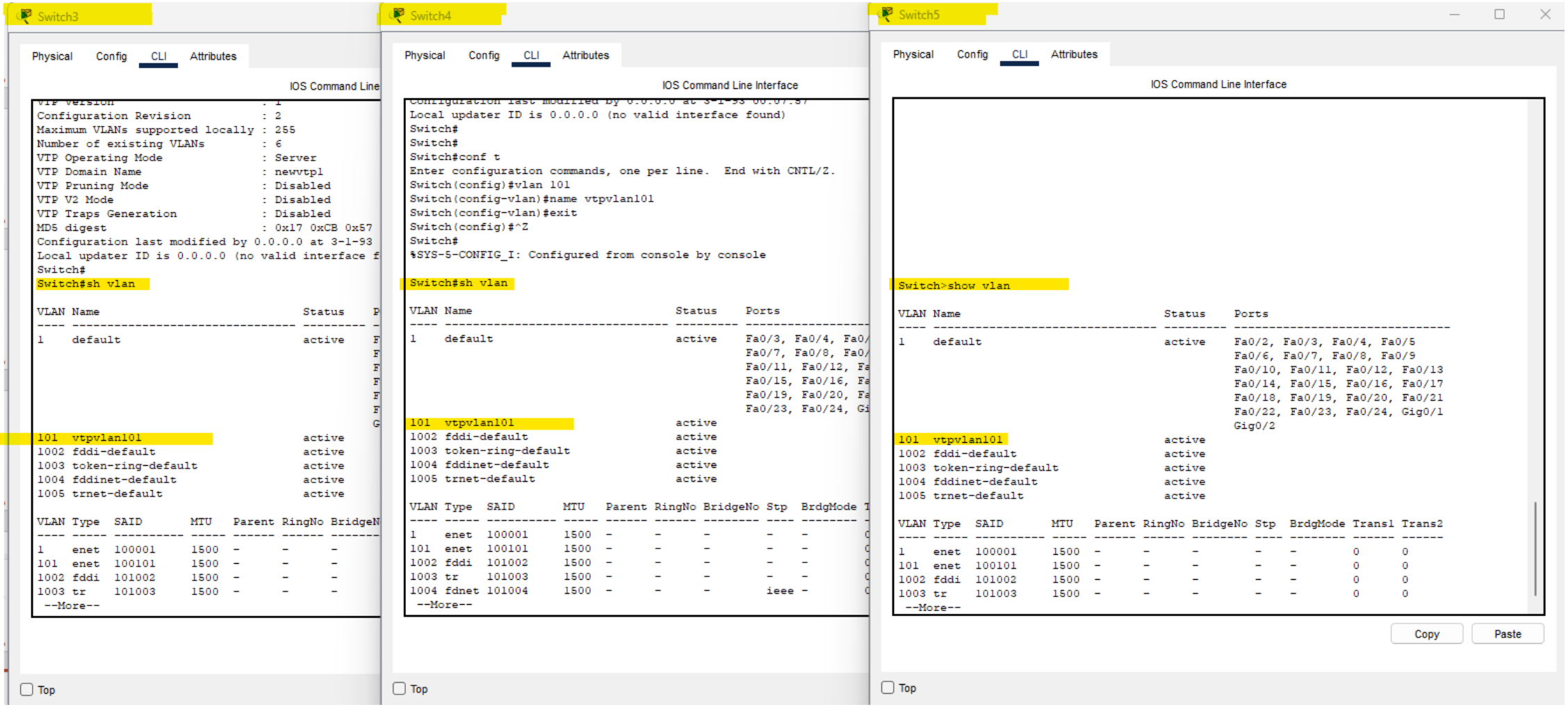
Copy Paste

VERIFY VTP – ON 1ST SWITCH

```
Switch#show vtp status
VTP Version                     : 1
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : newvtp1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
```

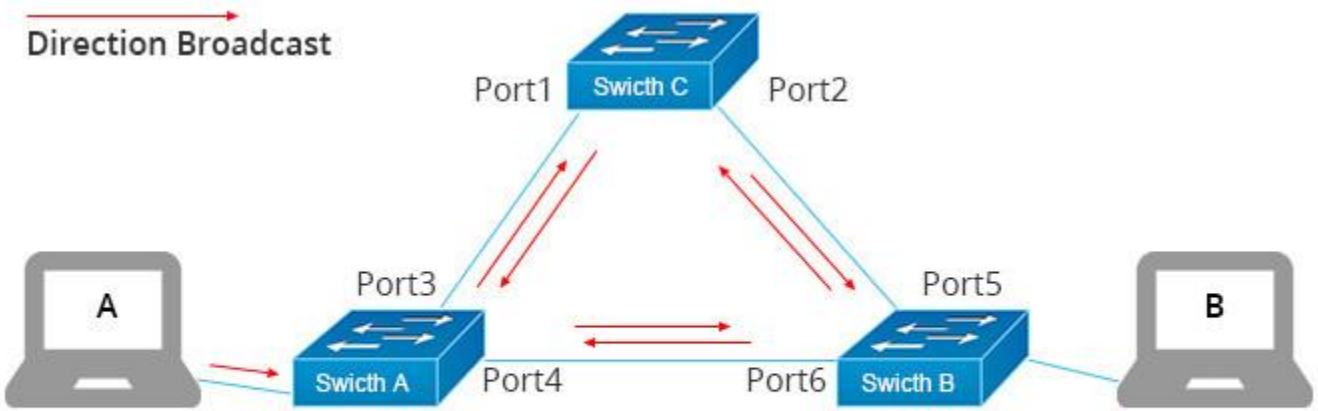
```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
101  vtpvlan101                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

VLAN REPLICATION TO ALL SWITCHES



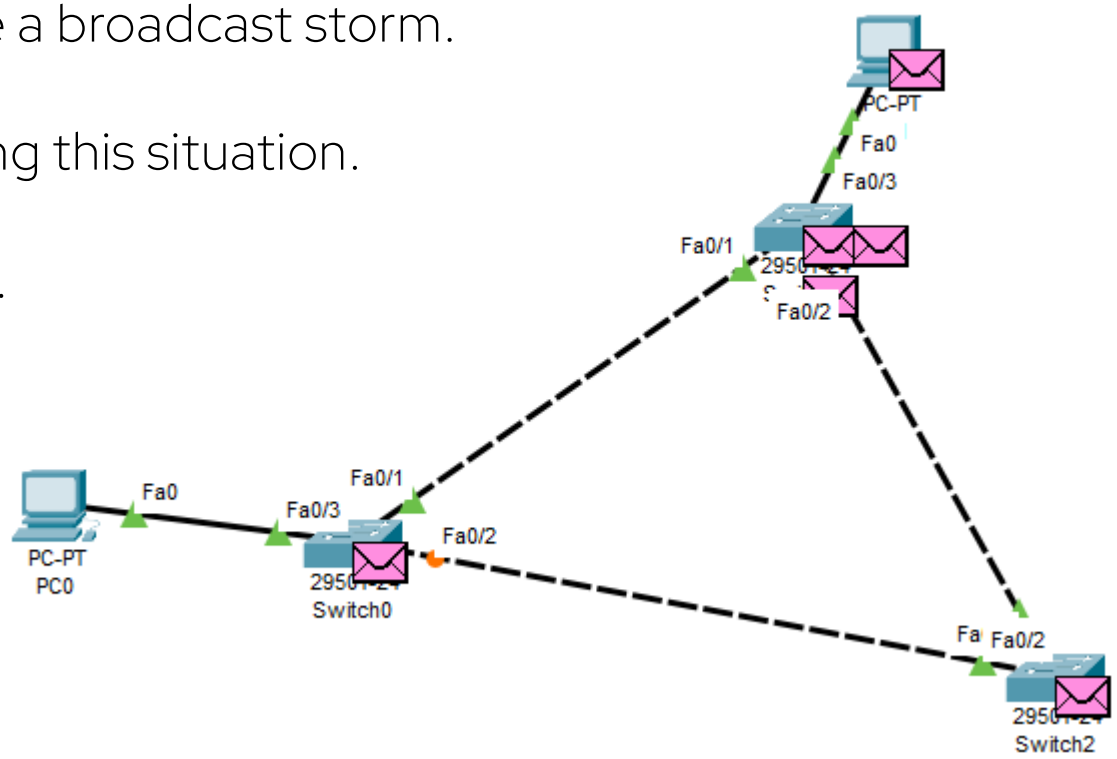
SPANNING TREE PROTOCOL (STP)

- It is a Layer 2 protocol that runs on bridges and switches.
- The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network.



STP

- When you have switches which keeps sending the broadcast messages, it creates a loop due to which the network could go down.
- This creates a situation called “Broadcast storm”.
- Extreme amounts of broadcast traffic constitute a broadcast storm.
- Spanning Tree Protocol (STP) is useful in handling this situation.
- STP prevents loop formation within the network.



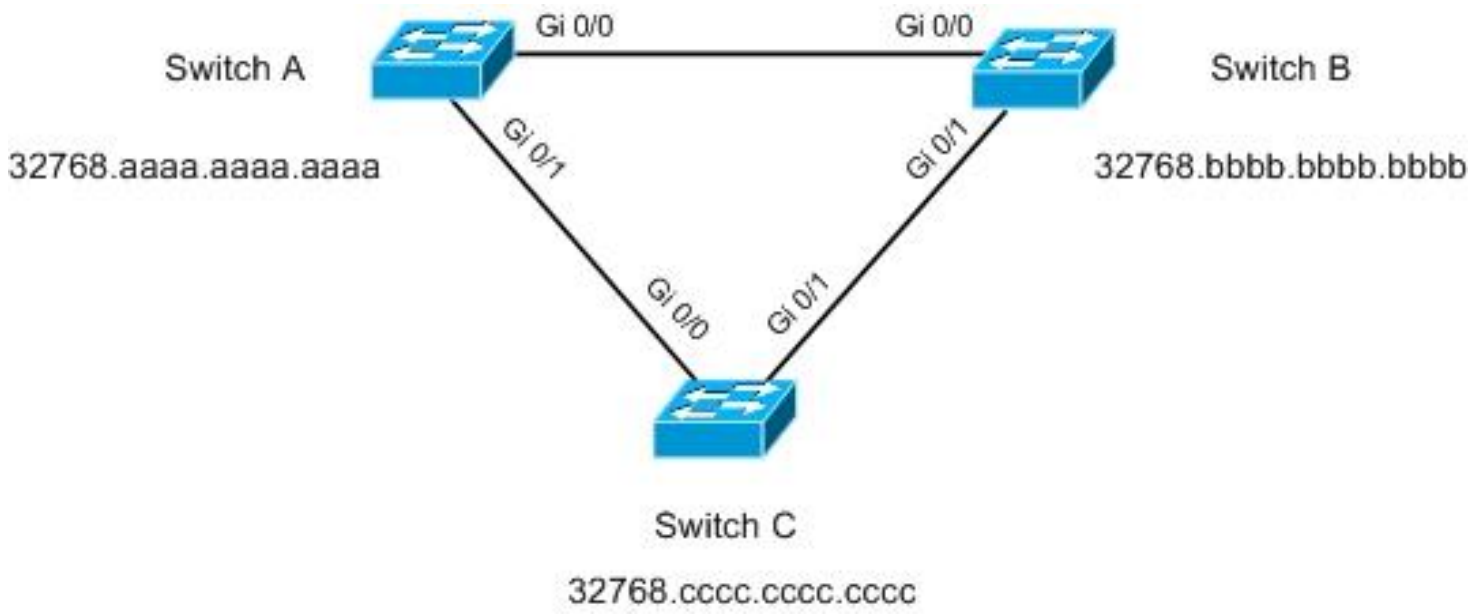
STP

- STP is known by IEEE 802.1D (original).
- Switches send probe into the network periodically to discover loops.
- The work of these probe messages is to detect the loops within network.
- It's detect the loops, when a switch receives the same broadcast message that was sent by itself earlier.
- These probes are called BPDU (Bridge Protocol Data Unit), that contains the details of a sender switch. Once a switch receives the same BPDU, it understands that theirs a loop in network.
- Switch multicasts this BPDU after every 2 seconds. And block if any redundant links.

STP – ROOT BRIDGE

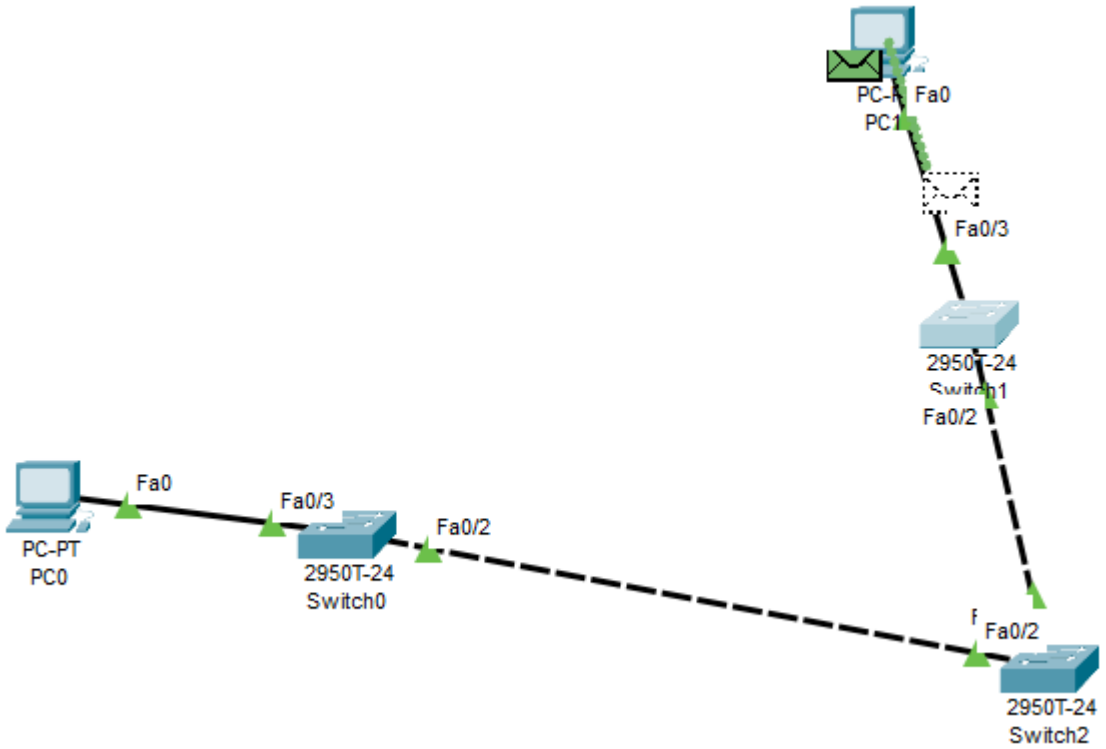
BPDU ID = Bridge Priority + MAC address.

- The switch with the lowest BPDU ID is elected as "root bridge".
- The bridge with the lowest MAC address will be root bridge.



BPDU = Bridge Protocol Data Unit

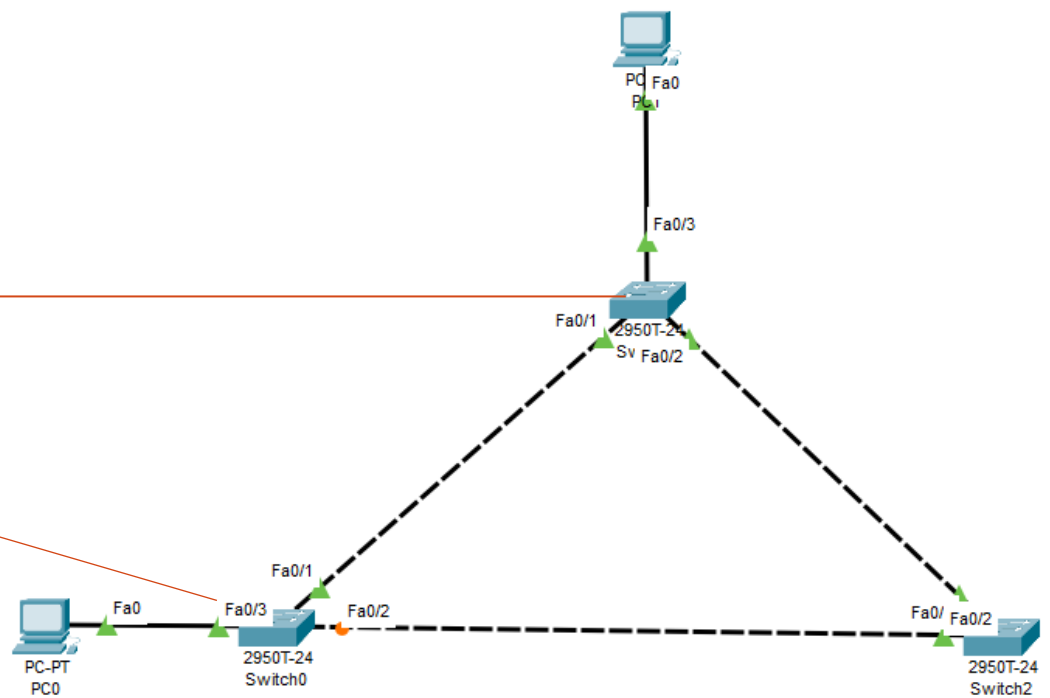
STP – LINK FAILURE



STP – LIST ROOT BRIDGE

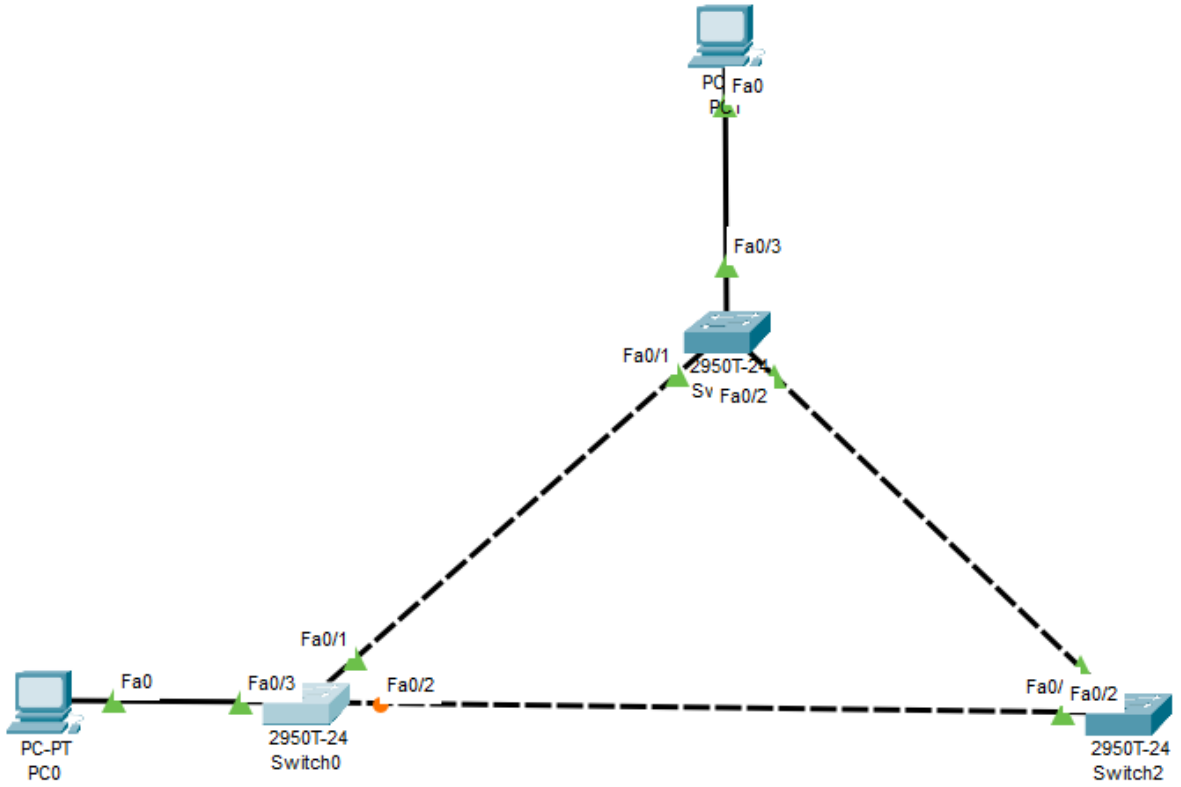
```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.64E1.6E4B
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.64E1.6E4B
              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
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.64E1.6E4B
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.F3DD.108E
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p

Switch#
```



STP – PORT RULES

- Root port (used to reach the root bridge)
- Designated Port (forwarding port)
- Blocking / Non-Designation Port (Loop)




```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.64E1.6E4B
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.F3DD.108E
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p

Switch#
```

TYPES OF STP

- STP / 802.1D (Original STP)
- Per VLAN Spanning Tree (PVST) + Cisco improvement of STP
- Rapid Spanning Tree Protocol (RSTP) / 802.1W (improved STP with fast convergence)
- RAPID PVST (Cisco improvement of RSTP)

PORT SECURITY

- To configure port security:
  1. Maximum – allows max number of MAC addresses allows on that port.
  2. MAC-Address – allows only specific MAC addresses on that port.
     1. Static – statically assigning MAC address
     2. Sticky – it learns the attached MAC address connected to that port.
- If the port security breaks the rules, it falls under VIOLATION:
  - Protect – it will drop all packets until MAC address is connect with no violation notification
  - Restrict – same as 'protect' but will receive notifications & increase counter with every violation.
  - Shutdown – it shutdown all the interface together.

PORT SECURITY

- Port Security on a Cisco switch is a security feature that controls access to individual switch ports by limiting and managing the devices that can connect to them.
- Port security is used to prevent unauthorized access to the network by restricting which devices can send data through specific ports on the switch.
- This is achieved by defining the number and specific MAC addresses that are allowed on a port, providing both control and enhanced security at the network access layer.

KEY FEATURES OF PORT SECURITY

- MAC Address Limiting
- MAC Address Learning
- Violation Modes
  - Protect
  - Restrict
  - Shutdown
- Aging and Relearning

PORT SECURITY – COMMAND - 1

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#inter
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#swi
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport port-se
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
  <cr>
```

If you get error, run : SW1(config-if)#**switchport port-security mac-address sticky**

PORT SECURITY – COMMAND - 2

```
  <cr>
Switch(config-if)#switchport port-security max
Switch(config-if)#switchport port-security maximum ?
  <1-132>  Maximum addresses
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address ?
  H.H.H   48 bit mac address
  sticky  Configure dynamic secure addresses as sticky
Switch(config-if)#switchport port-security mac-address 0000.0000.0001
Switch(config-if)#switchport port-security vio
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
Switch(config-if)#switchport port-security vio
Switch(config-if)#switchport port-security violation res
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#exit
Switch(config)#exit
```

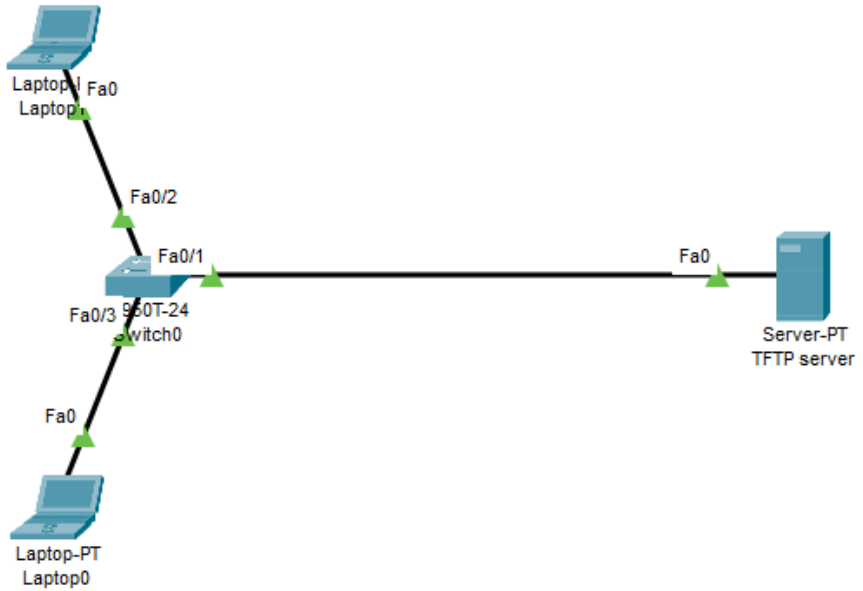
PORT SECURITY – VALIDATE

After adding a PC to the Switch


```
Switch#
Switch#show port-se
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)        (Count)
---------------------------------------------------------------------------
      Fa0/1         1             1                5          Restrict
---------------------------------------------------------------------------
```

BACKUP OF SWITCH

- Steps
  1. Create required environment (adding a TFTP server with a switch with some PCs).
     - Set IP address to all the PCs, switch & TFTP server.
  2. Display the current configuration
     - Switch# show running-config
  3. Run the following command to backup:
     - Switch# copy running-config tftp:




```
S1(config)#int
S1(config)#interface vlan
S1(config)#interface vlan 1
S1(config-if)#ip add
S1(config-if)#ip address 192.168.10.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#no shutdown
```

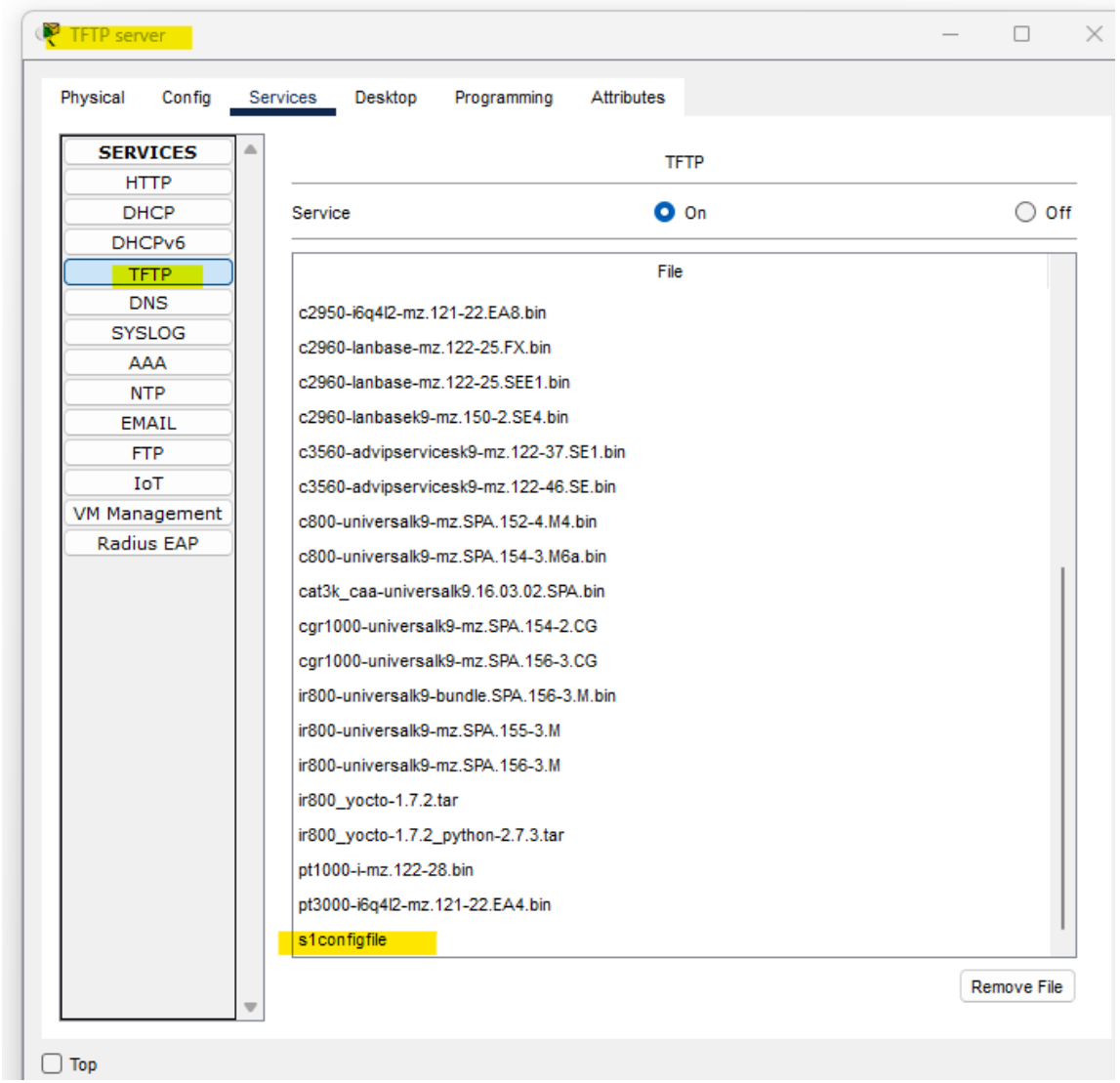
VIEW CURRENT SWITCH CONFIG

```
S1#show int vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0002.4a56.d8cb (bia 0002.4a56.d8cb)
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

TAKING BACKUP TO TFTP SERVER

```
S1#cop
S1#copy run
S1#copy running-config tf
S1#copy running-config tftp:
Address or name of remote host []? 192.168.10.10
Destination filename [S1-confg]? s1configfile

Writing running-config....!!
[OK - 1090 bytes]

1090 bytes copied in 3.001 secs (363 bytes/sec)
S1#
```

TO VERIFY ON TFTP SERVER



RECOVERING BACKUP FROM TFTP SERVER

- Change the IP address on the current configuration:

```
S1#con
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int
S1(config)#interface vla
S1(config)#interface vlan 1
S1(config-if)#ip addres
S1(config-if)#ip address 192.168.10.100 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- Verifying the IP address

```
S1#show interfaces vla
S1#show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0002.4a56.d8cb (bia 0002.4a56.d8cb)
  Internet address is 192.168.10.100/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

RECOVERING BACKUP FROM TFTP SERVER

```
S1#
S1#cop
S1#copy tftp run
S1#copy tftp running-config
Address or name of remote host []? 192.168.10.10
Source filename []? slconfigfile
Destination filename [running-config]?

Accessing tftp://192.168.10.10/slconfigfile....
Loading slconfigfile from 192.168.10.10: !
[OK - 1090 bytes]

1090 bytes copied in 3.007 secs (362 bytes/sec)
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Verifying the configuration

```
S1#show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0002.4a56.d8cb (bia 0002.4a56.d8cb)
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```