Network Device and Configuration

Chapter Four

Switch (LAN) Configuration

Mar 2024

Content addressable memory (CAM) table

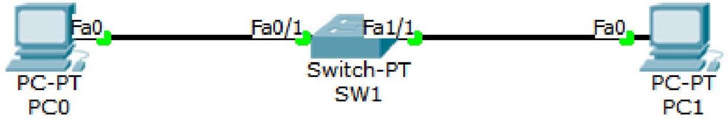
- **MAC table**, **filter table**, or **Content addressable memory** (**CAM**) table refers to a dynamic table in an network switch that maps MAC addresses to ports.
- It is the essential mechanism that separates network switches from network hubs.
- An Ethernet switch's role is to copy Ethernet frames from one port to another.
- Without a functional **CAM table**, all frames received by a network switch would be echoed back out to all other ports, much like an Ethernet hub.

Content Addressable Memory (CAM) Table

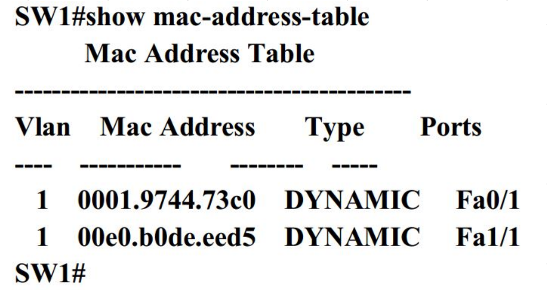
- A switch should only emit a frame on the port where the destination network device resides (**uncast**), unless the frame is for all nodes on the switch (**broadcast**) or multiple nodes (**multicast**).
- **CAM table** is a system memory construct used by Ethernet switch logic to dereference Media Access Control (MAC) addresses of stations to the ports on which they connect to the switch.
- The **CAM table** is consulted to make the frame forwarding decision.
- Switches learn MAC addresses from the source address of Ethernet frames on the ports, such as **Address Resolution Protocol** response packets.
- CAM tables are often the target of layer 2 network attacks in a local area network to set up man-in-the-middle attacks.

Content Addressable Memory (CAM) Table

- **Example:** PC 0 and PC 1 can communicate each other since both have IP and MAC addresses.



- To see MAC address in the switch CAM table, you have to use show mac-address-table command.



```
SW1#show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0001.9744.73c0    DYNAMIC     Fa0/1
   1    00e0.b0de.eed5    DYNAMIC     Fa1/1
SW1#
```

Port Security

- A switch that does not provide port security allows an attacker to attach a system to an unused, enabled port and to perform information gathering or attacks.
- Thus, an attacker could collect traffic that contains usernames, passwords, or configuration information about the systems on the network.
- **Port security** limits the number of valid MAC addresses allowed on a port.
- When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.
- A security violation occurs when the MAC address of a workstation attempting to access the port is different from any of the identified secure MAC addresses.

Secure MAC Address Types

- **There are a number of ways to configure port security.**

Static secure MAC addresses

- MAC addresses are manually configured by using the switchport port-security mac-address interface configuration command.
- MAC addresses configured in this way are stored in the address table and are added to the running configuration on the switch.

Dynamic secure MAC addresses

- MAC addresses are dynamically learned and stored only in the address table.
- MAC addresses configured in this way are removed when the switch restarts.

Secure MAC Address Types

Sticky secure MAC addresses

- Sticky secure MAC addresses are a hybrid.
- They are learned dynamically from the devices connected to the switchport, are put into the address table AND are entered into the running configuration as a static secure MAC address (sometimes referred to as a static sticky MAC address).
- Like a static secure MAC address, these MAC addresses will be lost unless saved to the startup configuration.

Characteristics of Sticky secure MAC addresses

- **Enable sticky learning on an interface:** interface converts all dynamic secure MAC addresses to sticky secure MAC addresses adds all sticky secure MAC addresses to running configuration
- **Disable sticky learning:** by using **no switchport port-security mac-address**; sticky secure MAC addresses remain part of running configuration but are removed from address table.
- **Port security is disabled:** sticky secure MAC addresses remain in running configuration.
- **Disable sticky learning enter switchport port-security mac-address sticky mac-address configuration command:** error message appears, sticky secure MAC address is not added to running configuration.

Security Violation Modes

- It is a security violation when either of these situations occurs:
  - The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
  - An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

Security Violation Modes

- Way to configure interface for Security Violation Modes.

Protect

- When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses.
- When using this mode, no notification message is sent when this violation occurs.

Restrict

- When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses.
- However, unlike the protect violation type, a message is also sent indicating that a violation has occurred.

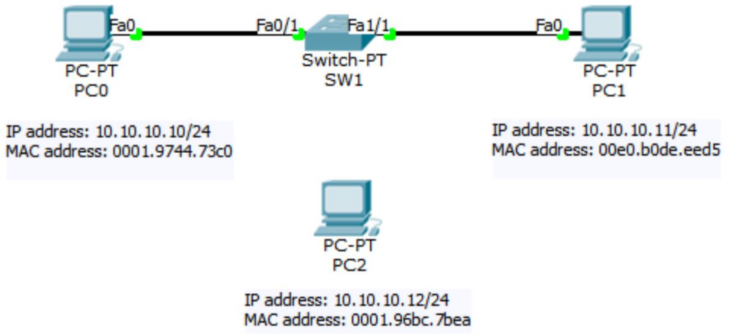
Security Violation Modes

shutdown

- When a violation occurs in this mode, the switchport will be taken out of service and placed in the err-disabled state.
- It also sends an SNMP trap, logs a syslog message, and increments the violation counter.
- The switchport will remain in this state until manually removed; this is the default switchport security violation mode.

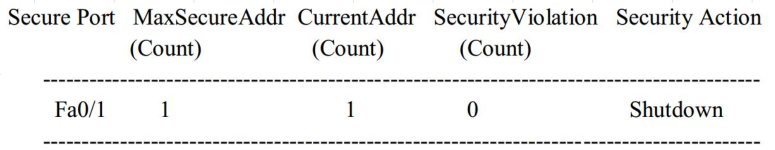
Security Violation Modes

- **Example:** Configure port security on the switch fa0/1 interface with default max. vlaue.


Fa0
Fa0/1
Fa1/1
Fa0
PC-PT
PC0
Switch-PT
SW1
PC-PT
PC1
IP address: 10.10.10.10/24
MAC address: 0001.9744.73c0
IP address: 10.10.10.11/24
MAC address: 00e0.b0de.eed5
PC-PT
PC2
IP address: 10.10.10.12/24
MAC address: 0001.96bc.7bea

Security Violation Modes

- SW1(config)#int fa0/1
- SW1(config)#switchport mode access
- SW1(config)#switchport port-security
- SW1(config)#switchport port-security mac-address sticky
- SW1(config)#switchport port-security maximum 1
- SW1(config)#switchport port-security violation shutdown
- SW1(config)#show port-security



```
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)        (Count)         (Count)
        ----------------------------------------------------------------------
   Fa0/1        1               1            0                  Shutdown
        ----------------------------------------------------------------------
```

Introduction to VLANs

- A virtual local area network (**VLAN**) is a virtualized connection that connects multiple devices and network nodes from different LANs into one logical network.
- Using VLANs it is possible to be free of the limitations of the physical architecture (geographic constraints, addressing constraints, etc) by defining logical segmentation based on a grouping together of machines using criteria (MAC addresses, port numbers, protocol, etc).

Types of VLAN

- Several types of VLAN are defined, depending on switching criteria and the level at which the VLAN is conducted:

Level 1 VLAN

- It is also called a **Port Based VLAN** defines a virtual network according to the connection ports on the switch;

Level 2 VLAN

- It is also called a **MAC Address-Based VLAN** comprises of defining a virtual network according to the MAC addresses of the stations.
- This type of VLAN is much more flexible than the port based VLAN because the network is independent from the location of the station.

Types of VLAN

Level 3 VLAN

- There are several types of level 3 VLANs:
  - **Network Address Based VLAN:** subnets according to the source IP address of the datagrams.
    - This type of solution provides great flexibility in so far as the configuration of the switches changes automatically when a station is moved.
  - **Protocol Based VLAN:** makes it possible to create a virtual network by protocol type (for example TCP/IP, IPX, AppleTalk, etc.).
    - Therefore grouping together all the machines using the same protocol on the same network.

Advantages of the VLAN

- More flexibility in administration and changes to the network because all the architecture can be changed by simple parametering of the switches.
- Increase in security because information is encapsulated in an additional level and possibly analysed.
- Reduction in the broadcasting of traffic on the network

Configure VLAN

- Use config-vlan mode to configure normal-range VLANs (VLAN IDs 1 to 1005).
  - When VTP mode is transparent, to configure extended-range VLANs (VLAN IDs 1006 to 4094).
- When VTP mode is transparent, the VLAN and VTP configuration is saved in the running configuration file
  - We can save it to the switch startup configuration file by using the copy running-config startup-config privileged EXEC command.
- The configurations of VLAN IDs 1 to 1005 are saved in the VLAN database if VTP is in transparent or server mode.
- The extended-range VLAN configurations are not saved in the VLAN database.
- Enter the vlan vlan-id on global configuration command to access config-vlan mode:
  - Switch(config)# vlan 20
  - Switch(config-vlan)#

VLAN Links

- In VLAN there are three types of links that allows the access to connect to multiple switches or other simple network connections.

Access Links

- All network hosts connected to the switch's Access Links in order to gain access to the local network.
- These links are ordinary Port found on every switch. This switch port configured to carry only one VLAN.
- Any device connected to these links (port) is totally unaware of VLAN assigned to the port.

VLAN Links

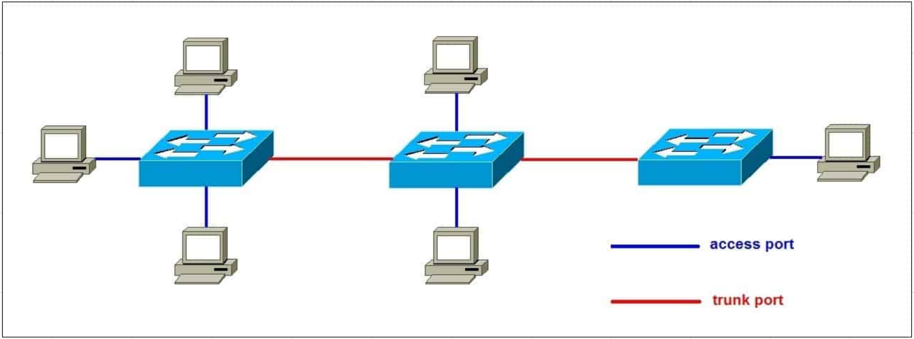
Trunk Link

- A trunk is an interface or link that can carry frames for multiple VLANs at once.
- A trunk is used to connect two switches or routers so that two VLANs in two separate networks can communicate with each other.
- But if there is only one VLAN to be connected, switches are connected at layer two using trunks.

Dynamic Link

- It sets trunking mode to dynamically negotiate access or trunk mode.

VLAN Links

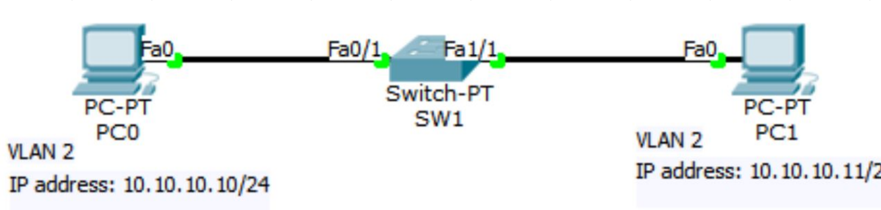


VLAN Tagging

- Frame tagging has been applied to trunk ports as links to other switches and routers within the wider network carry multiple VLANs.
  - This **tagging** is very important since it enables the VLANs to spread **Enterprise-wide** as the backbones take the bulk of network traffic and VLAN information.
- This is why VLANs need to operate across high-bandwidth trunked FDDI (802.10), Fast Ethernet (ISL and 802.1q) and ATM links (ATM LANE).

Creating VLAN

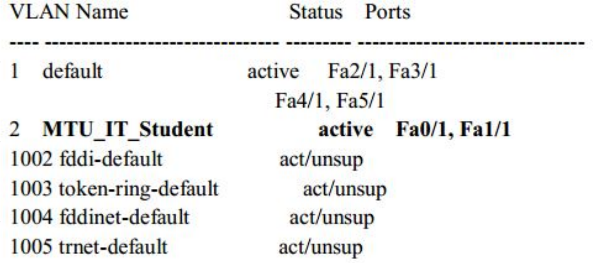
- Create VLAN 2 on the switch and add some ports in to this VLAN.



- **Creating VLAN 2**
  - SW1(config)#vlan 2
  - SW1(config-vlan)#name MTU_IT _Student
  - SW1(config-vlan)#int vlan 2
  - SW1(config-if)#

Creating VLAN

- **Assigning ports to VLAN 2**
  - SW1(config)#int fa0/1
  - SW1(config-if)#switchport mode access
  - SW1(config-if)#switchport access vlan 2
  - SW1(config-if)#
  - SW1(config-if)#int fa1/1
  - SW1(config-if)#switchport mode access
  - SW1(config-if)switchport access vlan 2
- **Check whether VLAN 2 is created or not**
  - SW1#show vlan



```
VLAN Name                              Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa2/1, Fa3/1
                                                Fa4/1, Fa5/1
2    MTU_IT_Student                   active    Fa0/1, Fa1/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Virtual Trunk Protocol (VTP)

- Protocol reducing the administration overhead and the possibility of error in any switched network environment.
- When a new VLAN is created and configured on a switch without the VTP protocol enabled, this must be manually replicated to all switches on the network so they are all aware of the newly created VLAN.
  - This means that the administrator must configure each switch separately, a task that requires a lot of time and adds a considerable amount of overhead depending on the size of the network.
- The configuration of a VLAN includes the VLAN number, name and a few more.
  - This information is then stored on each switch's NVRAM and any VLAN changes made to any switch must again be replicated manually on all switches.

Virtual Trunk Protocol (VTP)

- VTP allows you to add, delete and rename VLANs which is then propagated to other switches in the VTP domain.
    - VTP advertisements can be sent over 802.1Q, and ISL trunks.
- Currently, 3 different versions of the protocol exist, that is, version 1, 2 and 3, with the first version being used in most networks.
- It also operates in 3 different modes: Server, client and transparent mode

VTP Mode

VTP Server

- The default mode for all switches supporting VTP.
- Can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version) for the entire VTP domain.
- VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links.
- VLAN configurations are saved in NVRAM.

VTP Mode

VTP Client

- A switch using this mode can’t change its VLAN configuration.
- That means that a VTP client switch cannot create or delete VLANs.
- However, received VTP updates are processed and forwarded.

VTP Mode

VTP Transparent Mode

- Does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.
- However, they will forward VTP advertisements as they are received from other switches.
- Can create, modify, and delete VLANs on a switch in VTP transparent mode.
- **Note**
  - A Transparent VTP switch will act as a VTP relay (forward all VTP information it receives, out its trunk ports) only when VTP version 2 is used in the network.
  - With VTP version 1, the transparent switch will simply ignore and discard any VTP messages received from the rest of the network.

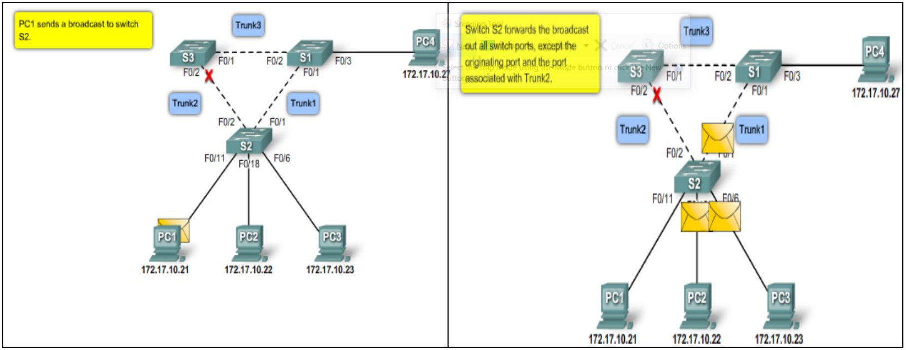
Spanning Tree Protocol(STP)

- Redundancy increases the availability of the network topology by protecting the network from a single point of failure, such as a failed network cable or switch.
- When redundancy is introduced into a Layer 2 design, loops and duplicate frames can occur.
- Loops and duplicate frames can have severe consequences on a network.
    - The Spanning Tree Protocol (STP) was developed to address these issues
- 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.

Spanning Tree Protocol(STP)

- 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 network traffic is prevented from entering or leaving that port.
- Blocking the redundant paths is critical to preventing loops on the network.
- 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.

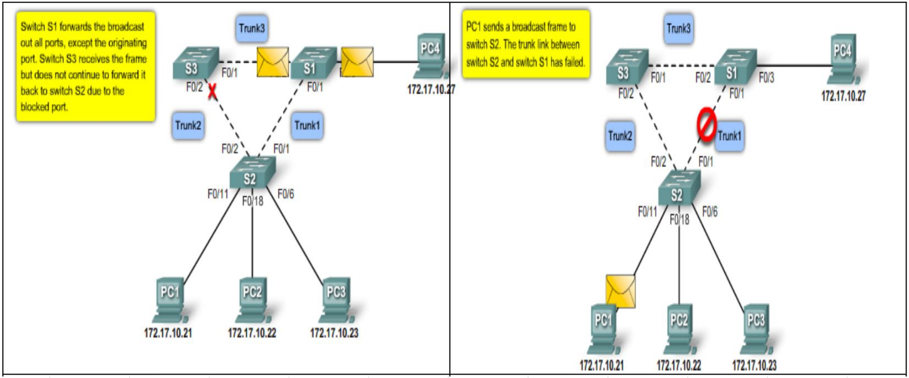
Spanning Tree Protocol(STP)



PC1 sends a broadcast to switch S2.

Switch S2 forwards the broadcast out all switch ports, except the originating port and the port associated with Trunk2.

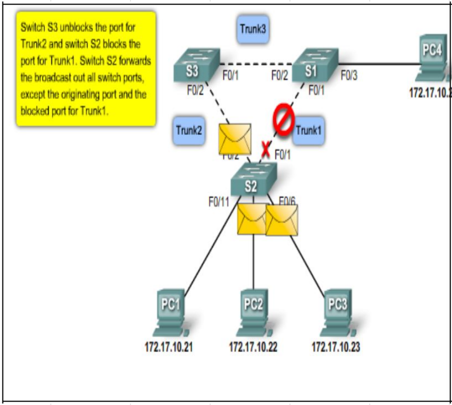
Spanning Tree Protocol(STP)



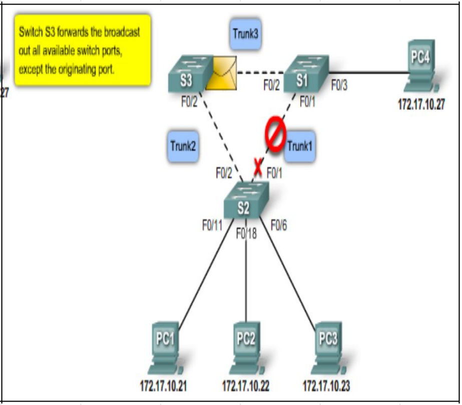
Switch S1 forwards the broadcast out all ports, except the originating port. Switch S3 receives the frame but does not continue to forward it back to switch S2 due to the blocked port.

PC1 sends a broadcast frame to switch S2. The trunk link between switch S2 and switch S1 has failed.

Spanning Tree Protocol(STP)

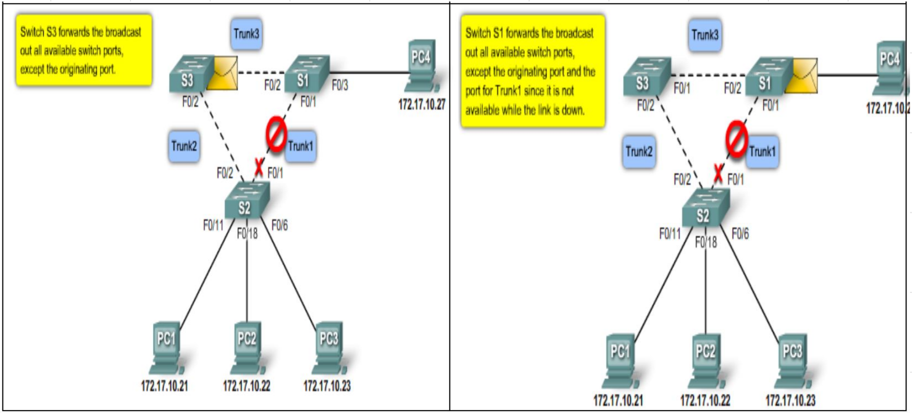


Switch S3 unblocks the port for Trunk2 and switch S2 blocks the port for Trunk1. Switch S2 forwards the broadcast out all switch ports, except the originating port and the blocked port for Trunk1.



Switch S3 forwards the broadcast out all available switch ports, except the originating port.

Spanning Tree Protocol(STP)



Switch S3 forwards the broadcast out all available switch ports, except the originating port.

Switch S1 forwards the broadcast out all available switch ports, except the originating port and the port for Trunk1 since it is not available while the link is down.

Thank You!