VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Packet Tracer Layer 2 Security

Information Security Management

Team Members:

18BCE0941 - Harshith Chukka

18BCE0393-Robin Raj

18BCE0395- Aditya Raj

18BIS0147- Mrinmay Date

18BCE0958- Ritvik Baghel

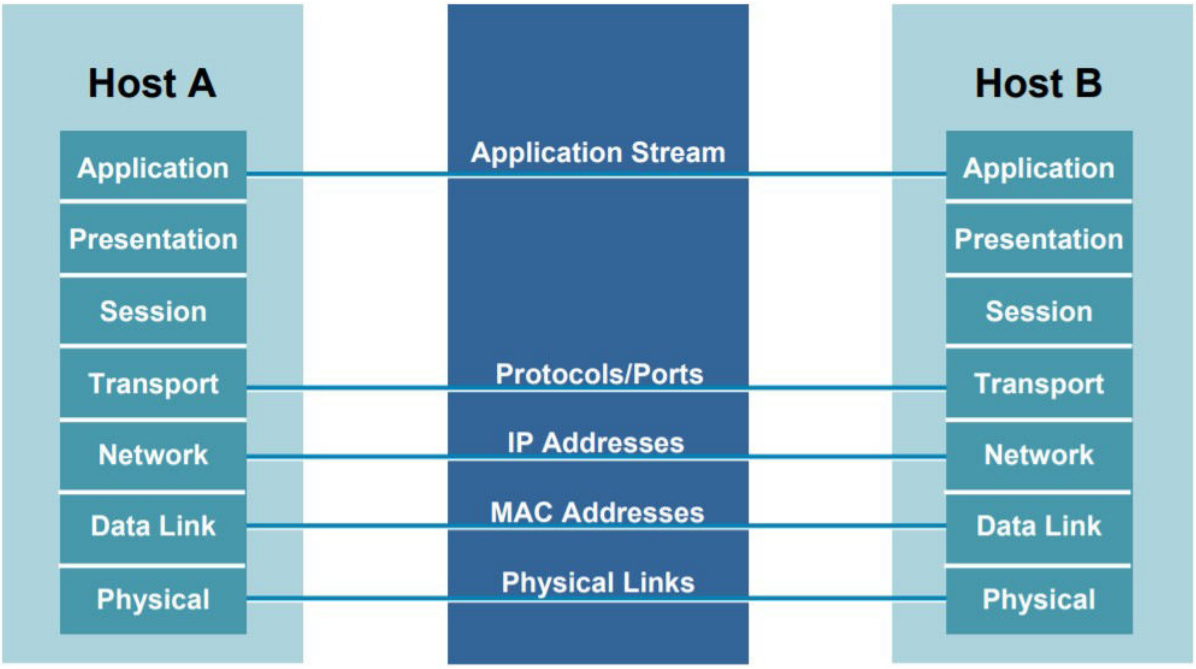
Professor: **Dr.Lavanya K**

1. Introduction

Cisco Packet Tracer- Layer 2 Security

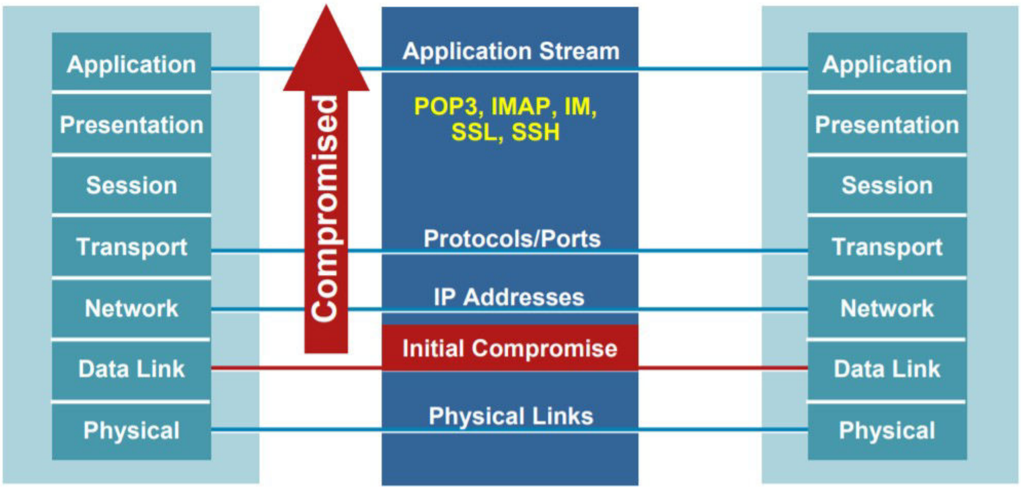
All attacks and mitigation techniques assume a switched Ethernet network running IPv4 All testing was done on Cisco Ethernet Switches Ethernet switching attack resilience varies widely from vendor to vendor This is not a comprehensive talk on configuring Ethernet switches for security or NAC or IEEE 802.1x: the focus is mostly access L2 attacks and their mitigation

OSI Was Built to Allow Different Layers to Work Without the Knowledge of Each Other therefore, its sequrity is needed.



Lower Levels Affect Higher Levels

- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem
- Security is only as strong as the weakest link
- When it comes to networking, layer 2 can be a very weak link

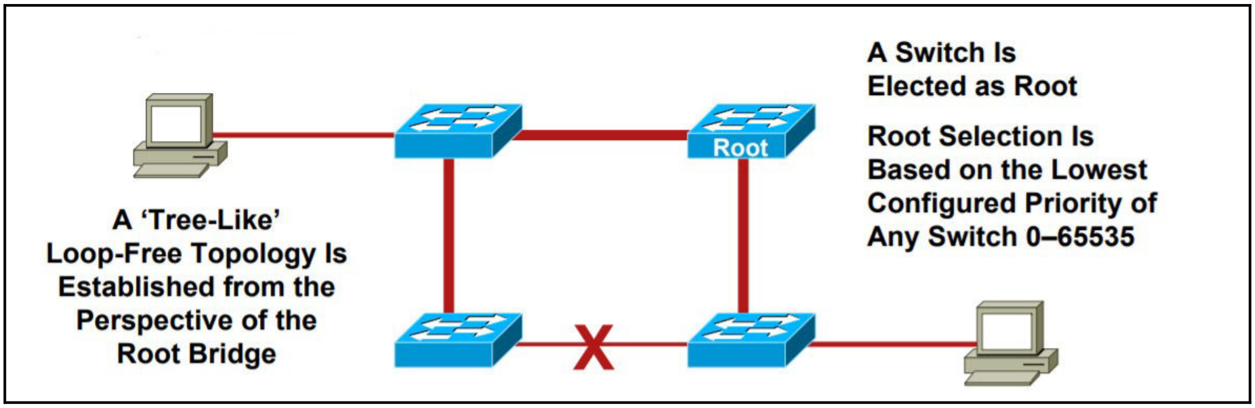


Types of layer 2 attacks and countermeasures:

1. MAC Attack:
   CAM table are the countermeasures for MAC Attack.The CAM table stores information such as MAC addresses available on physical ports with their associated VLAN parameters.Port Security Limits the Amount of MAC's on an Interface. Port security limits MAC flooding attack and locks down port and sends an SNMP trap.
2. DHCP Attack:
   Gobbler/DHCPx looks at the entire DHCP scope and tries to lease all of the DHCP addresses available in the DHCP scope This is a Denial of Service DoS attack using DHCP leases.Counter measure:Restrict the number of MAC addresses on an port with port security Else use option 82 option 82 of DHCP DHCP server can track which port has already got one IP address.
3. ARP Attack: Its countermeasure,Dynamic ARP Inspection, uses the information from the DHCP snooping binding table ,Looks at the MacAddress and IpAddress fields to see if the ARP from the interface is in the binding, it not, traffic is blocked.
4. Spoofing Attacks: Its Countermeasure,IP Source Guard ,Uses the information from the DHCP Snooping Binding table ,Looks at the MacAddress and IpAddress fields to see if the traffic from the interface is in the binding table, it not, traffic is blocked.
5. General Attack:

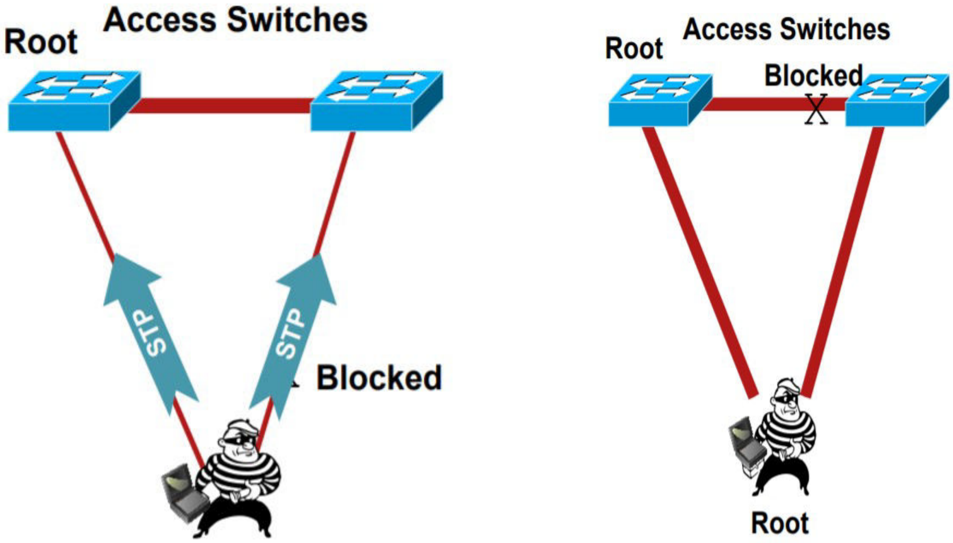
One of the most common attack is STP attacking:

STP Purpose: To maintain loop-free topologies in a redundant Layer 2 infrastructure



A Switch Is Elected as Root
Root Selection Is Based on the Lowest Configured Priority of Any Switch 0–65535
Root
A 'Tree-Like' Loop-Free Topology Is Established from the Perspective of the Root Bridge
X

Spanning Tree attack Example:



STP Attack Mitigation

- Try to design loop-free topologies where ever possible, so you do not need STP
- Don't disable STP, introducing a loop would become another attack Except in loop-free topologies (like layer 3 at access switch)
- BPDU guard
- Should be run on all user facing ports and infrastructure facing ports Disables ports using portfast upon detection of a BPDU message on the port

Other Types of attack includes VLAN Hopping,

- An end station can spoof as a switch with ISL or 802.1q
- The station is then a member of all VLANs

Counter Measures

- Disable trunking on all host ports (except phones)
- Never use VLAN 1 anywhere Specific VLAN for trunk native VLAN
- Disable VLAN tag on access ports
- Enforce VLAN tag on trunk ports

Layer 2, also known as the Data Link Layer, is the second level in the seven-layer OSI reference model for network protocol design. Layer 2 is equivalent to the link layer (the lowest layer) in the TCP/IP network model. Layer2 is the network layer used to transfer data between adjacent network nodes in a wide area network or between nodes on the same local area network.
At Layer 2, *unicast* refers to sending frames from one node to a single other node, whereas *multicast* denotes sending traffic from one node to multiple nodes, and *broadcasting* refers to the transmission of frames to all nodes in a network. A *broadcast domain* is a logical division of a network in which all nodes of that network can be reached at Layer 2 by a broadcast.
Layer 2 contains two sublayers:

- Logical link control (LLC) sublayer, which is responsible for managing communications links and handling frame traffic.
- Media access control (MAC) sublayer, which governs protocol access to the physical network medium. By using the MAC addresses that are assigned to all ports on a switch, multiple devices on the same physical link can uniquely identify one another.

The ports, or interfaces, on a switch operate in either access mode, tagged-access, or trunk mode:

- *Access mode* ports connect to a network device such as a desktop computer, an IP telephone, a printer, a file server, or a security camera. The port itself belongs to a single VLAN. The frames transmitted over an access interface are normal Ethernet frames. By default, all ports on a switch are in access mode.
- *Tagged-Access mode* ports connect to a network device such as a desktop computer, an IP telephone, a printer, a file server, or a security camera. The port itself belongs to a single VLAN. The frames transmitted over an access interface are normal Ethernet frames. By default, all ports on a switch are in access mode. Tagged-access mode accommodates cloud computing, specifically scenarios including virtual machines or virtual computers. Because several virtual computers can be included on one physical server, the packets generated by one server can contain an aggregation of VLAN packets from different virtual machines on that server. To accommodate this situation, tagged-access mode reflects packets back to the physical server on the same downstream port when the destination address of the packet was learned on that downstream port. Packets are also reflected back to the physical server on the downstream port when the destination has not yet been learned. Therefore, the third interface mode,

tagged access, has some characteristics of access mode and some characteristics of trunk mode:

- *Trunk mode* ports handle traffic for multiple VLANs, multiplexing the traffic for all those VLANs over the same physical connection. Trunk interfaces are generally used to interconnect switches to other devices or switches.

With native VLAN configured, frames that do not carry VLAN tags are sent over the trunk interface. If you have a situation where packets pass from a device to a switch in access mode, and you want to then send those packets from the switch over a trunk port, use native VLAN mode. Configure the single VLAN on the switch's port (which is in access mode) as a native VLAN. The switch's trunk port will then treat those frames differently than the other tagged packets. For example, if a trunk port has three VLANs, 10, 20, and 30, assigned to it with VLAN 10 being the native VLAN, frames on VLAN 10 that leave the trunk port on the other end have no 802.1Q header (tag). There is another native VLAN option. You can have the switch add and remove tags for untagged packets. To do this, you first configure the single VLAN as a native VLAN on a port attached to a device on the edge. Then, assign a VLAN ID tag to the single native VLAN on the port connected to a device. Last, add the VLAN ID to the trunk port. Now, when the switch receives the untagged packet, it adds the ID you specified and sends and receives the tagged packets on the trunk port configured to accept that VLAN.

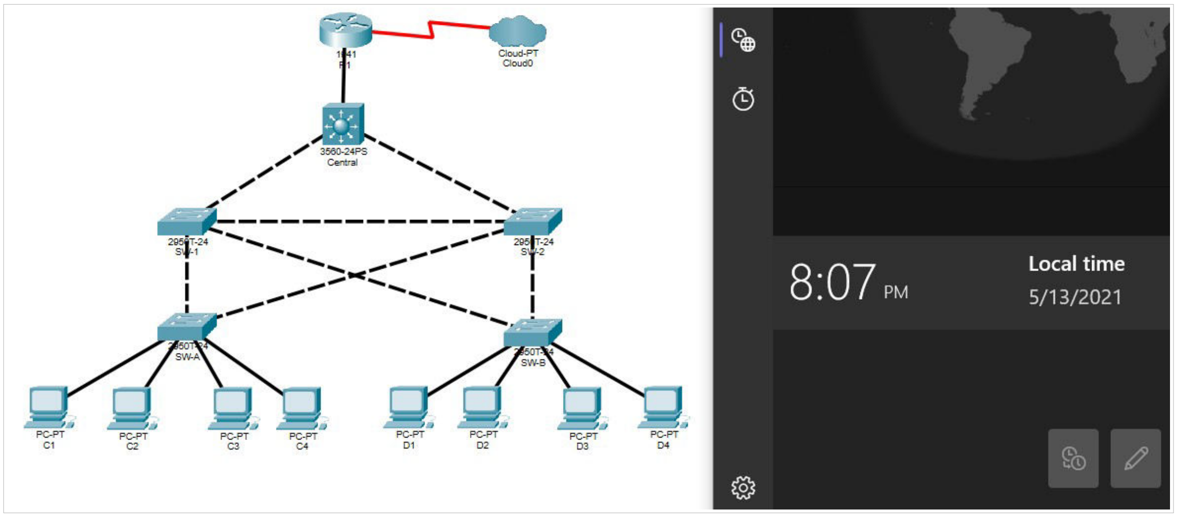
Including the sublayers, Layer 2 on the QFX Series supports the following functionality:

- Unicast, multicast, and broadcast traffic.
- Bridging.
- VLAN 802.1Q—Also known as *VLAN tagging*, this protocol allows multiple bridged networks to transparently share the same physical network link by adding VLAN tags to an Ethernet frame.
- Extension of Layer 2 VLANs across multiple switches using Spanning Tree Protocol (STP) prevents looping across the network.
- *MAC learning*, including per-VLAN MAC learning and Layer 2 learning suppression–This process obtains the MAC addresses of all the nodes on a network
- Link aggregation—This process groups of Ethernet interfaces at the physical layer to form a single link layer interface, also known as a *link aggregation group (LAG)* or LAG bundle

2. Frame of Diagram

Objectives

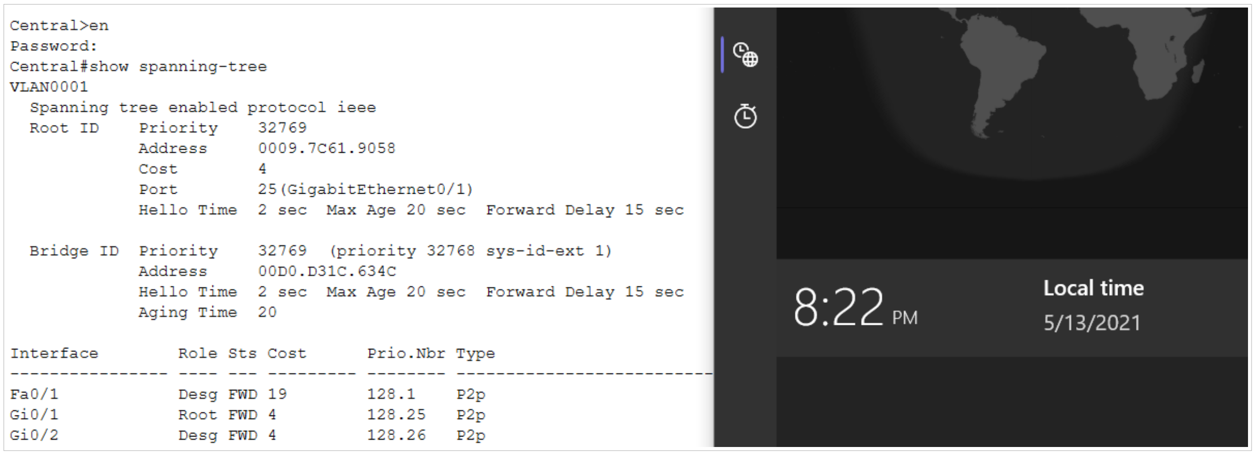
- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable port security to prevent CAM table overflow attacks.



3. Step by Step Screenshot

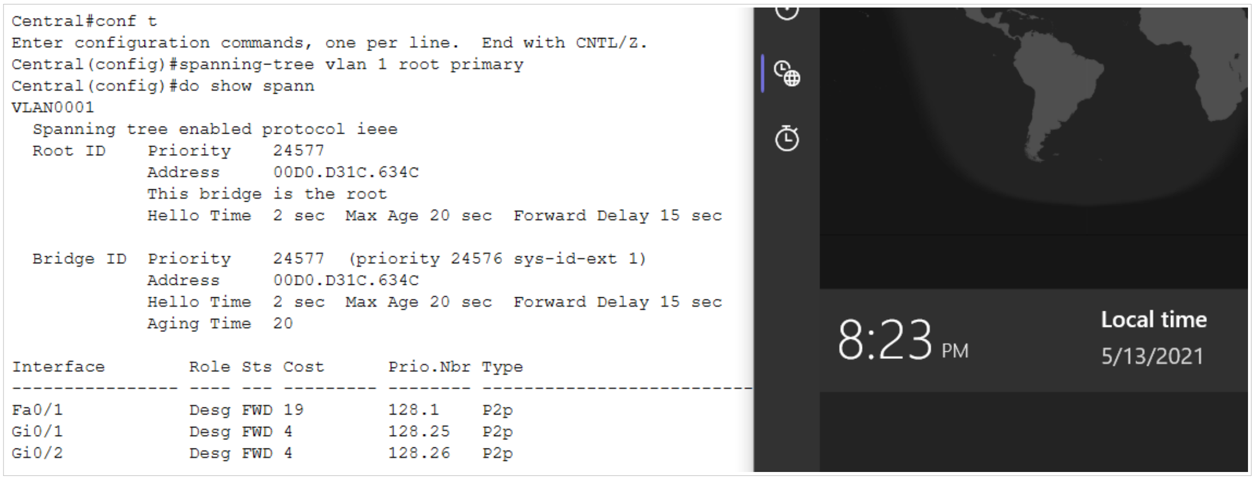
Step 1: Configure Root Bridge.

From Central, issue the **show spanning-tree** command to determine the current root bridge, to see the ports in use, and to see their status.



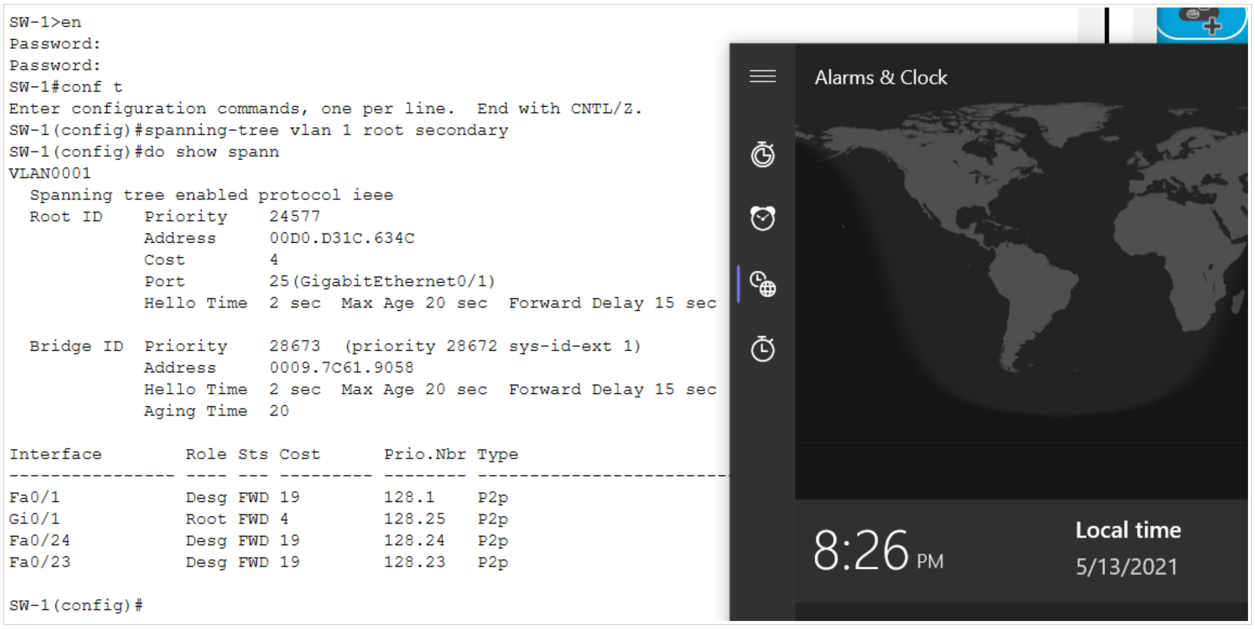
```
Central>en
Password:
Central#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0009.7C61.9058
             Cost        4
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.D31C.634C
             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
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

Using the **spanning-tree vlan 1 root primary** command, and assign Central as the root bridge.



```
Central#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Central(config)#spanning-tree vlan 1 root primary
Central(config)#do show spann
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     00D0.D31C.634C
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     00D0.D31C.634C
             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
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

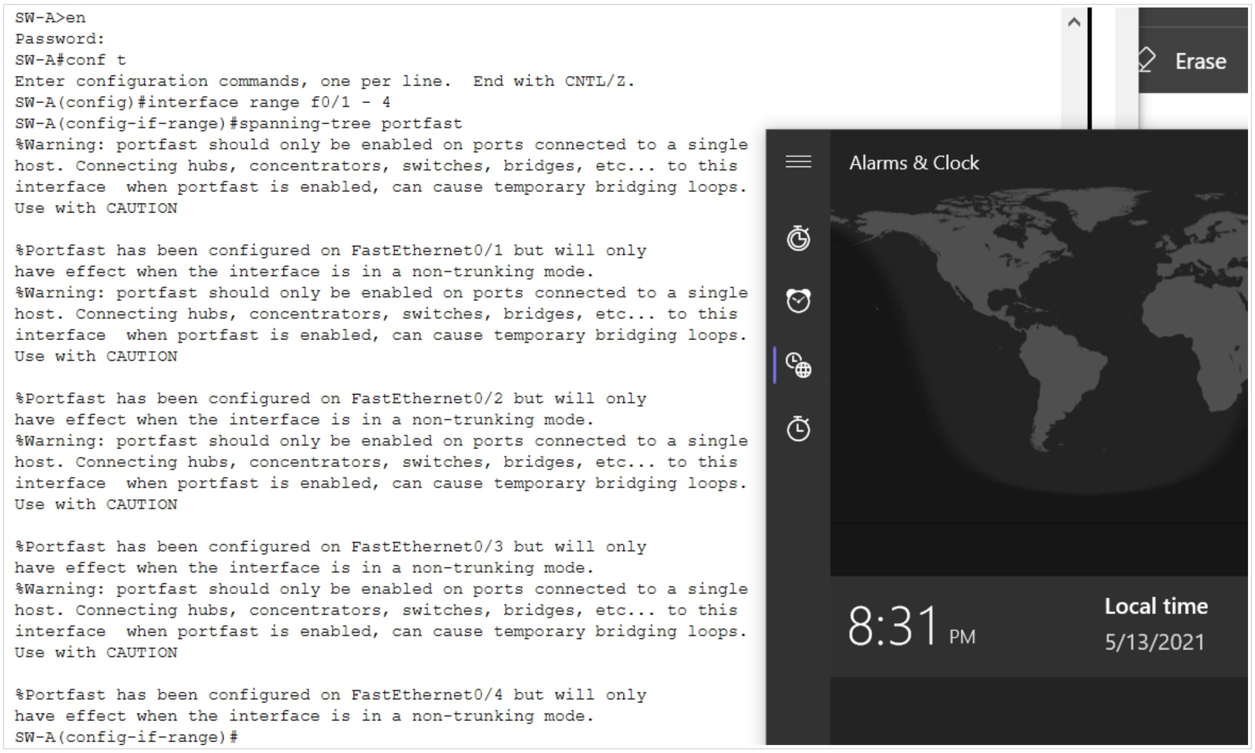
Assign SW-1 as the secondary root bridge using the **spanning-tree vlan 1 root secondary** command.



```
SW-1>en
Password:
Password:
SW-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#spanning-tree vlan 1 root secondary
SW-1(config)#do show spann
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     00D0.D31C.634C
             Cost        4
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28673  (priority 28672 sys-id-ext 1)
             Address     0009.7C61.9058
             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
Gi0/1            Root FWD 4         128.25   P2p
Fa0/24           Desg FWD 19        128.24   P2p
Fa0/23           Desg FWD 19        128.23   P2p

SW-1(config)#
```

Step 2: Enable PortFast on all access ports at both SW-A and SW-B.

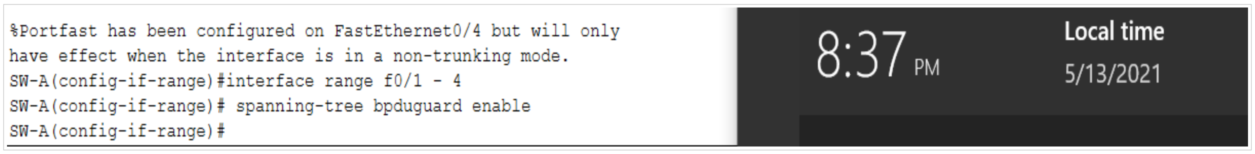
PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly. On the connected access ports of the SW-A and SW-B, use the **spanning-tree portfast** command.



```
SW-A>en
Password:
SW-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)#interface range f0/1 - 4
SW-A(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
SW-A(config-if-range)#
```

Step 3: Enable BPDU guard on all access ports.

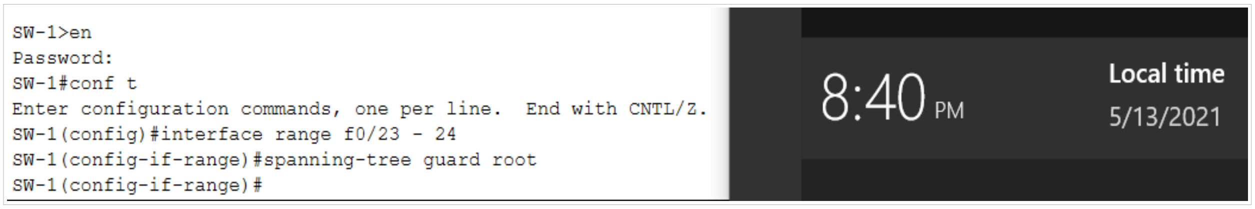
BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU guard on SW-A and SW-B access ports



```
%Portfast has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
SW-A(config-if-range)#interface range f0/1 - 4
SW-A(config-if-range)# spanning-tree bpduguard enable
SW-A(config-if-range)#
```

Step 4: Enable root guard.

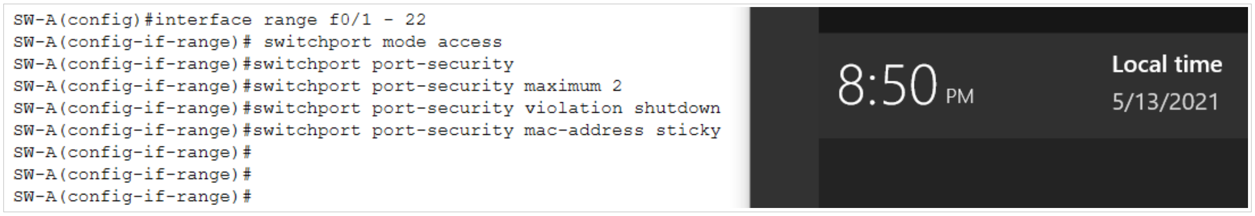
Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect to other non-root switches. Use the **show spanning-tree** command to determine the location of the root port on each switch.



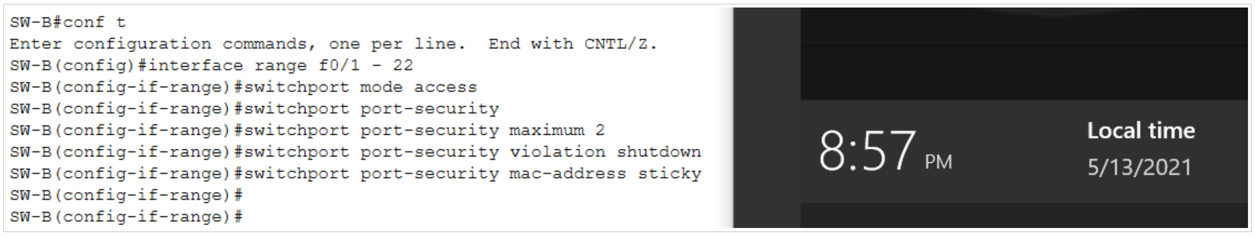
```
SW-1>en
Password:
SW-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#interface range f0/23 - 24
SW-1(config-if-range)#spanning-tree guard root
SW-1(config-if-range)#
```

Step 5: Configure basic port security on all ports connected to host devices.

This procedure should be performed on all access ports on SW-A and SW-B. Set the maximum number of learned MAC addresses to 2, allow the MAC address to be learned dynamically, and set the violation to shutdown



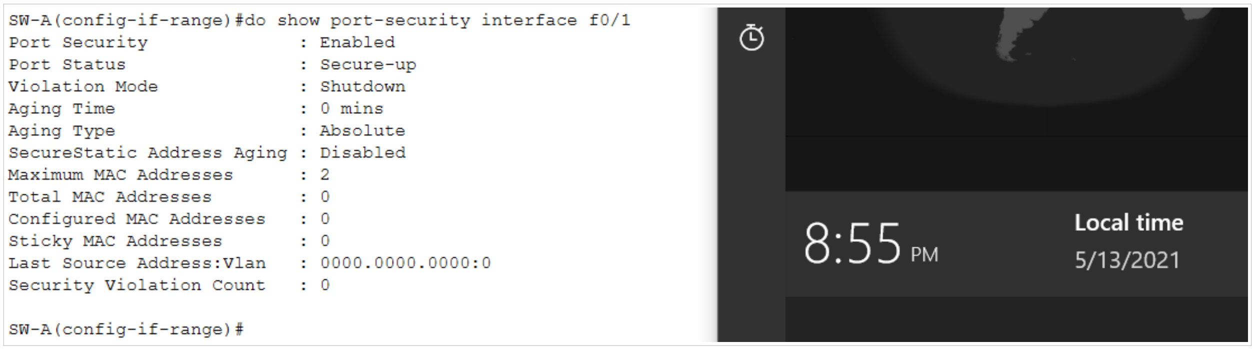
```
SW-A(config)#interface range f0/1 - 22
SW-A(config-if-range)# switchport mode access
SW-A(config-if-range)#switchport port-security
SW-A(config-if-range)#switchport port-security maximum 2
SW-A(config-if-range)#switchport port-security violation shutdown
SW-A(config-if-range)#switchport port-security mac-address sticky
SW-A(config-if-range)#
SW-A(config-if-range)#
SW-A(config-if-range)#
```



```
SW-B#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-B(config)#interface range f0/1 - 22
SW-B(config-if-range)#switchport mode access
SW-B(config-if-range)#switchport port-security
SW-B(config-if-range)#switchport port-security maximum 2
SW-B(config-if-range)#switchport port-security violation shutdown
SW-B(config-if-range)#switchport port-security mac-address sticky
SW-B(config-if-range)#
SW-B(config-if-range)#
```

Step 6: Verify port security.

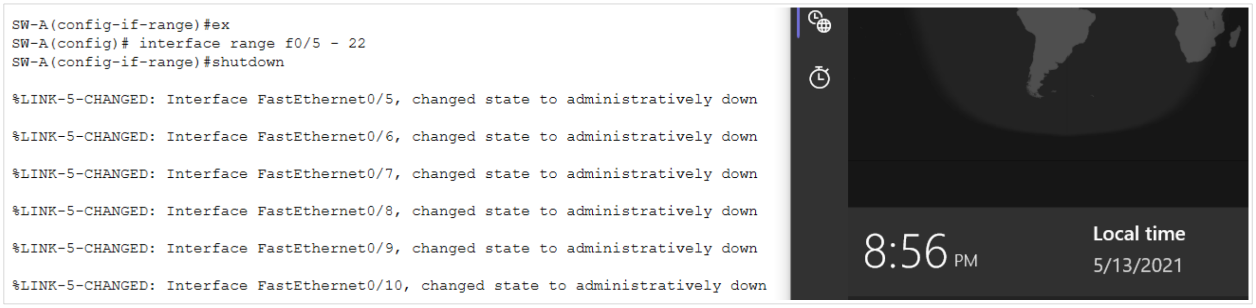
On SW-A, issue the command **show port-security interface f0/1** to verify that port security has been configured



```
SW-A(config-if-range)#do show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

SW-A(config-if-range)#
```

Step 7: Disable unused ports.

Disable all ports that are currently unused.



```
SW-A(config-if-range)#ex
SW-A(config)# interface range f0/5 - 22
SW-A(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
```

4. Result

Hence we were able to implement Layer-2 Security using Packet Tracer with central switch as the primary root bridge. To prevent spanning-tree manipulation attacks, we ensured that the STP parametres are secure and to prevent against CAM table flow attacks, we decided to limit the number of MAC addresses each switch port can learn to two.