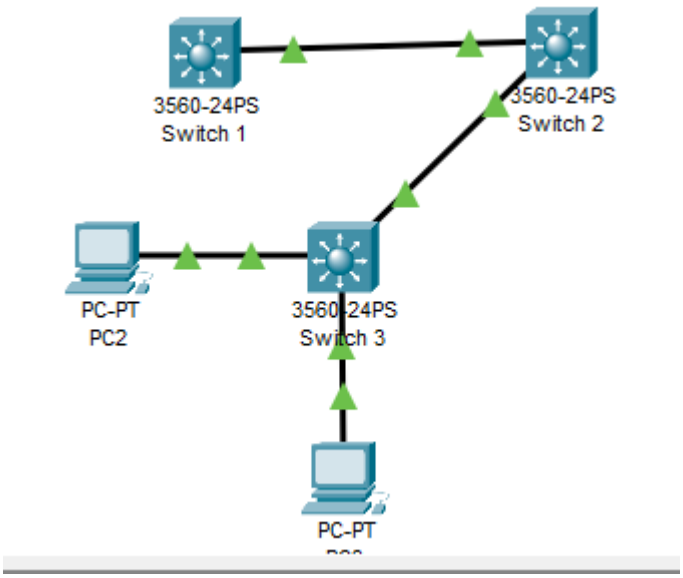
Name: Miftahul Huq
Course: Network Security
Course Prefix: CSEC 744
Section: 01
Root & BPDU Guard
Date: 03/04/2024

Initial Topology

Description: Switch 1 is the root switch



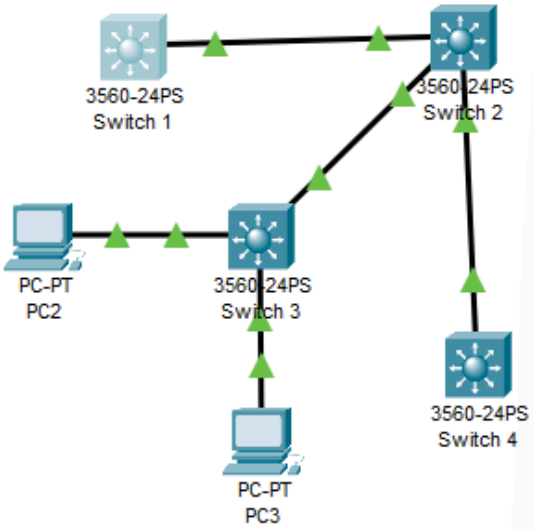
Another switch, Switch 4, will be the attacker.

Root Guard

Mitigation Description: This root guard mitigation control where candidate root bridges can be connected and found on a network. Basically, a switch learns the current root bridge's bridge ID. if another switch advertises a superior BPDU, or one with a better bridge ID, on a port where root guard is enabled, the local switch will no allow the new switch to become the root, and the port will be blocked.

Attack description: Sending BPDU message from attacker to force spanning tree recalculation to make the attacker the root switch. Basically making the priority of the attackers switch to be lower than the priority of the root switch. This can allow a Man-in-the-middle attack.

Attack Demo:
Switch 1 is the root switch and has root guard enable on the where switch 2 is connected



Switch 1

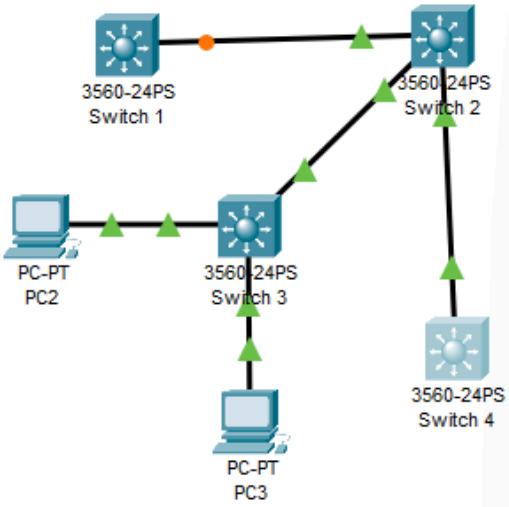
```
Switch#show spanning-tree vl
Switch#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0001.9677.3BE1
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0001.9677.3BE1
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/2            Desg FWD 4         128.26   P2p

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int g0/2
Switch(config-if)#span
Switch(config-if)#spanning-tree gu
Switch(config-if)#spanning-tree guard root
Switch(config-if)#
```

When I was trying to make switch 4 the root switch, it made the switch 1 root guard to activate and block the port where switch 2 is connected to.



Switch 4

```
Switch(config)#spanning-tree vlan 1 priority 0
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#span
Switch#show spa
Switch#show spanning-tree vla
Switch#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     0007.EC59.A7EC
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1  (priority 0 sys-id-ext 1)
              Address     0007.EC59.A7EC
              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

Switch#
```

BPDU Guard

Mitigation Description: The BPDU Guard feature automatically disables if unexpected BPDUs are received on a port where BPDUs should not be received. This feature was developed to further protect the integrity of switch ports that have portfast enabled. If any BPDU is received on a port where BPDU Guard is enabled, that port immediately is put into an errdisable state. The port is shut down in a error condition and can be either manually re-enabled or automatically recovered through the errdisable timeout function.

Attack Description: Basically you can inject STP bridge protocol data units into switch ports of VLANs, and can disrupt a stable, loop-free topology.

Attack Demo:
I have enabled BPDU Guard on all ports for switch 3.

Switch 3

```
Switch(config)#spanning-tree portfast bpduguard default
Switch(config)#
```

When I try to connect switch 4 to switch 3, it goes into err disable mode. As soon as the port on which switch 4 is connected, the port is shut down.