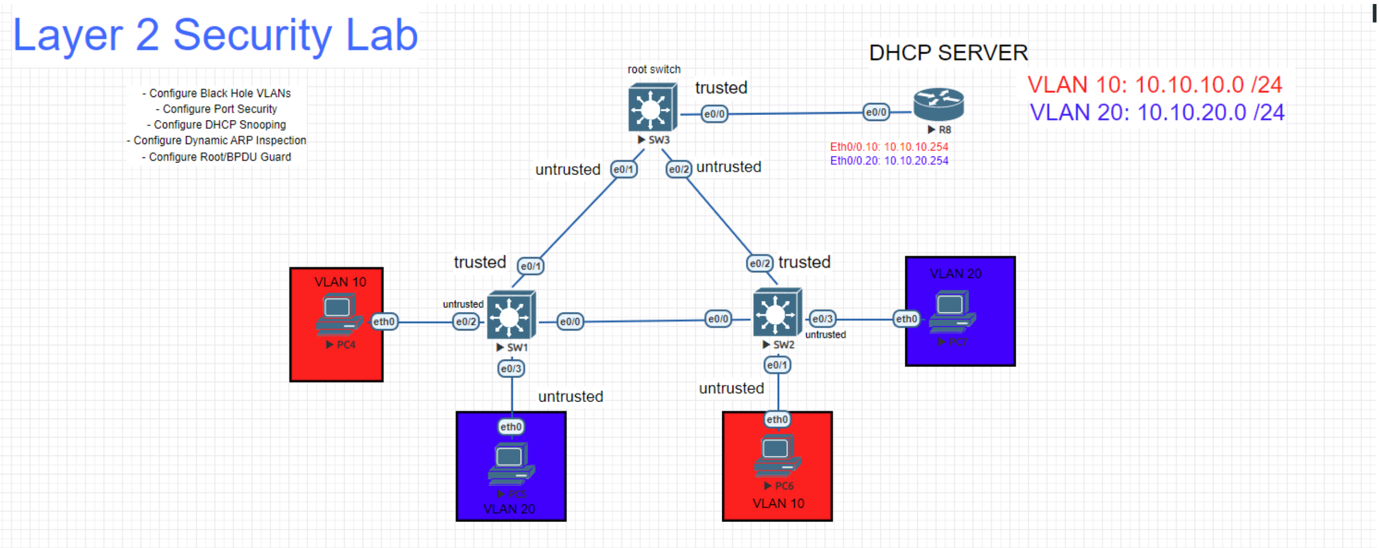
BPDUGuard and Root Guard

- The spanning-tree protocol is a Layer 2 Control plane protocol that prevents switching loops by electing a root bridge and placing switchport into a Forwarding or blocking state. Cisco switches will send Bridge Protocol Datagram Units per VLAN to elect a root switch, which all other switches will forward traffic too.

- STP is also vulnerable to Layer 2 attacks like Superior BDPU's, and malicious users creating a broadcast storm by flooding the switched architecture with BPDU's.

- Rootguard will prevent the manipulation of root bridge elections by placing protecting the root bridge from receiving superior BPDU's.


Layer 2 Security Lab

- Configure Black Hole VLANs
- Configure Port Security
- Configure DHCP Snooping
- Configure Dynamic ARP Inspection
- Configure Root/BPDU Guard

DHCP SERVER

VLAN 10: 10.10.10.0 /24
VLAN 20: 10.10.20.0 /24

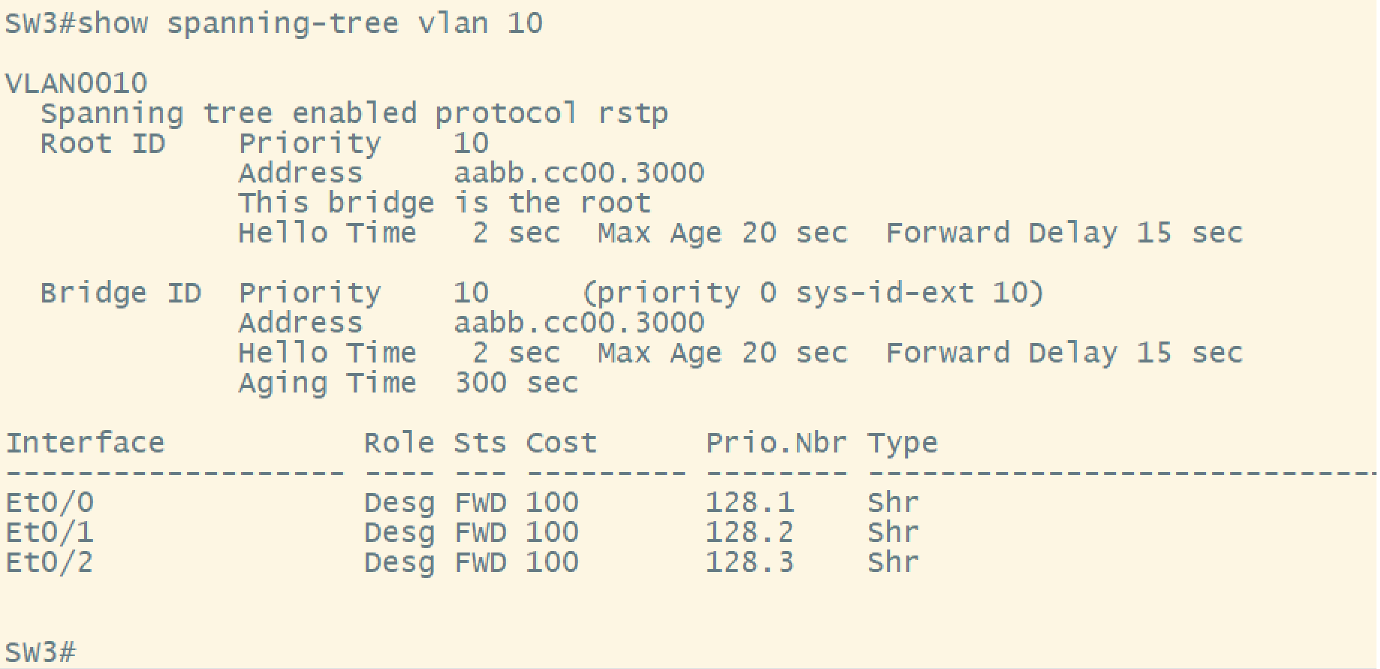
Eth0/0.10: 10.10.10.254
Eth0/0.20: 10.10.20.254

- For this How To we will configure rootguard on the root switches trunk ports.

`SW3(config)#interface range eth0/1 - 2` # This command brings you into the sub-configuration mode for a range of interfaces.

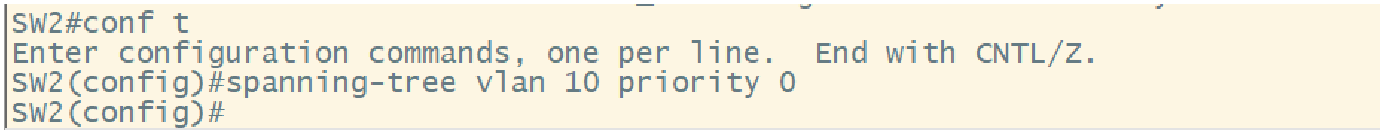
`SW3(config-if-range)#spanning-tree guard root` # This command will place a designated port on the root bridge into a "blocking" state

- Verification. Now lets see what happens to our topology once we apply rootguard and attempt to send a superior BPDU to SW3

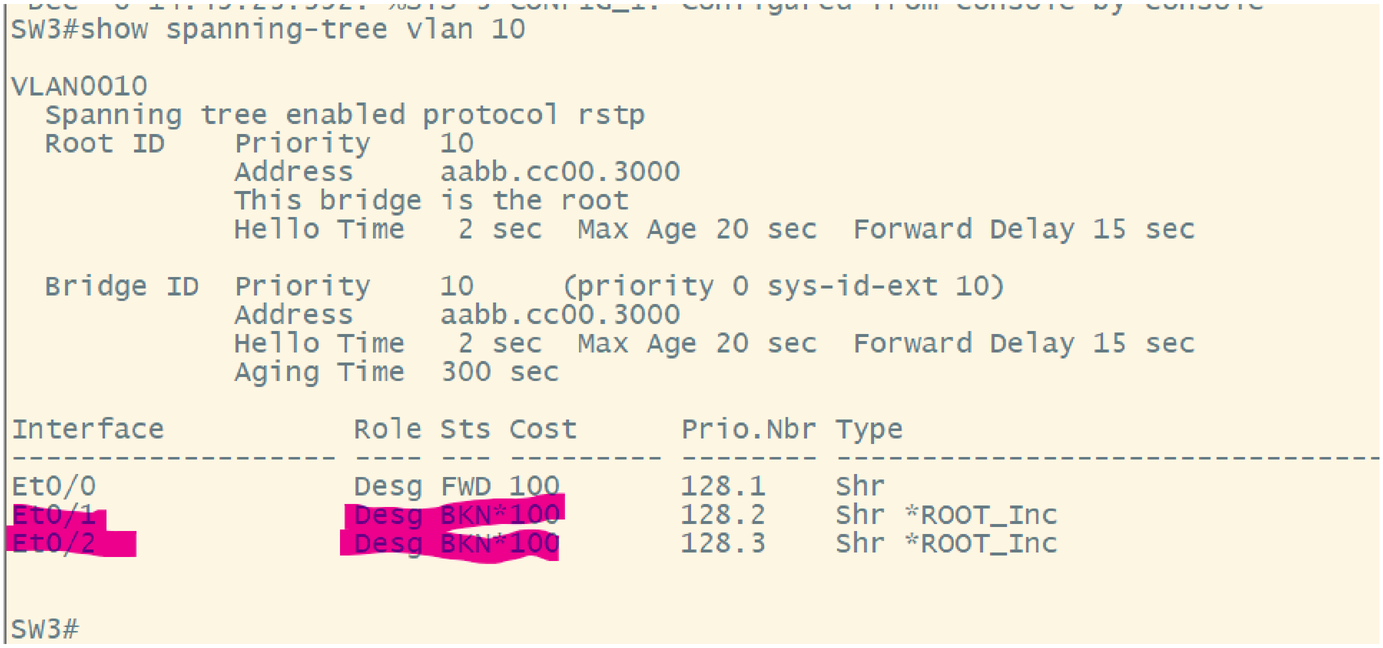


```
SW3#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    10
             Address     aabb.cc00.3000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    10     (priority 0 sys-id-ext 10)
             Address     aabb.cc00.3000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr


SW3#
```

- As you can see here SW3 is the rootbridge for VLAN. We have already configured rootguard. Now lets go to SW2 and try to make it the rootbridge and check what happens on SW3



```
SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#spanning-tree vlan 10 priority 0
SW2(config)#
```



```
*Dec  6 17:49:25.592: %SYS-5-CONFIG_I: Configured from console by console
SW3#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    10
             Address     aabb.cc00.3000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    10     (priority 0 sys-id-ext 10)
             Address     aabb.cc00.3000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg BKN*100       128.2    Shr *ROOT_Inc
Et0/2               Desg BKN*100       128.3    Shr *ROOT_Inc


SW3#
```

- As you can see now the two interfaces facing the other switches are in a blocking state. This is because SW2 tried to send a "superior BPDU" to SW3 from SW1 and from itself.

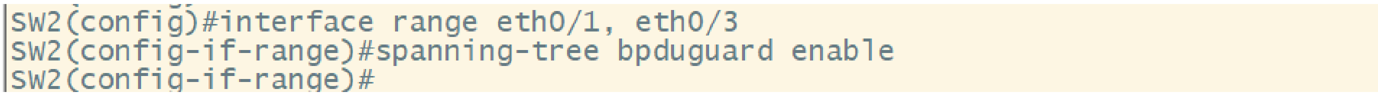
BPDUGuard

BPDUGuard is a feature we apply to our access ports to prevent the interfaces facing our users from processing BPDUs. This protects our switched architecture from BPDUs being flooded into the network.

`SW2(config)#interface range eth0/1, eth0/3` # This command brings you into the sub-configuration mode for a range of interfaces.

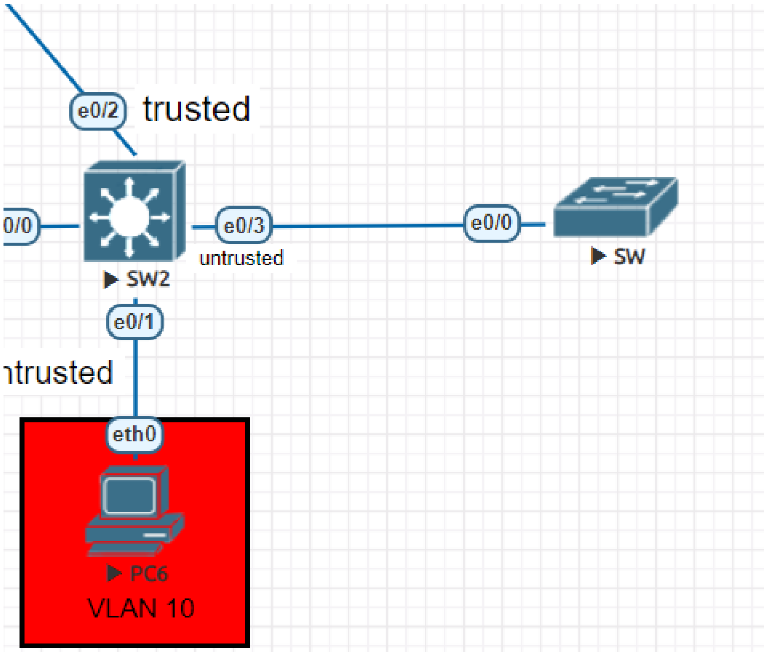
`SW2(config-if-range)#spanning-tree bpduguard enable` # This command will place a port into an **"err-disabled"** state if the port receives a BPDU

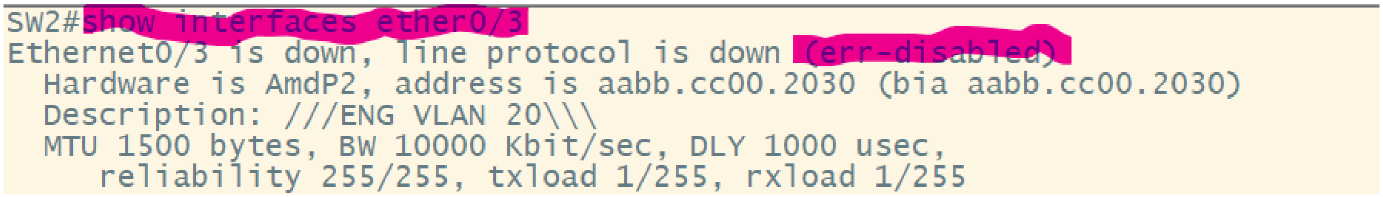
The full configuration is shown below



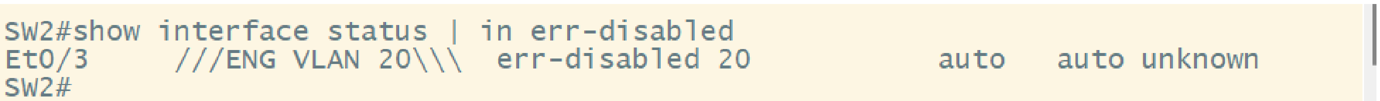
```
SW2(config)#interface range eth0/1, eth0/3
SW2(config-if-range)#spanning-tree bpduguard enable
SW2(config-if-range)#
```

Verification. Now let's attach a switch to the access ports and see how they respond. As we can see below with a switch connected and sending BPDU's the access port goes into a "err-disabled" state.





```
SW2#show interfaces ether0/3
Ethernet0/3 is down, line protocol is down (err-disabled)
  Hardware is AmdP2, address is aabb.cc00.2030 (bia aabb.cc00.2030)
  Description: ///ENG VLAN 20\\\
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```



```
SW2#show interface status | in err-disabled
Et0/3     ///ENG VLAN 20\\\  err-disabled 20          auto   auto unknown
SW2#
```