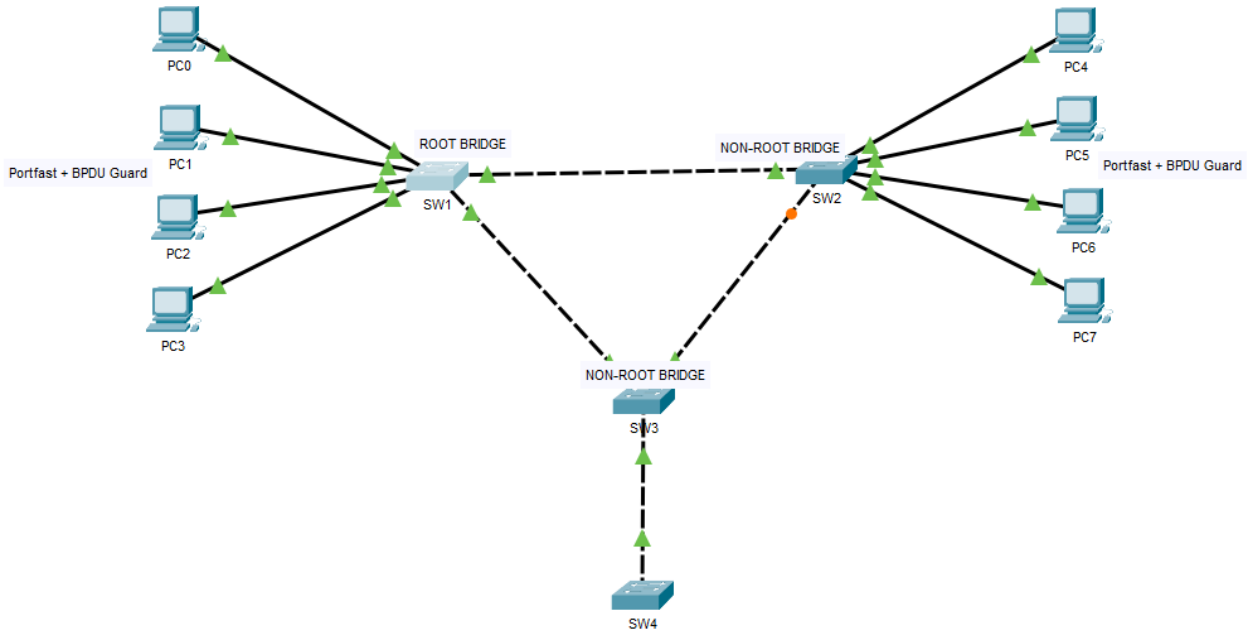
2024

STP Portfast, BPDU Guard, Root Guard Configuration

STP ATTACKS PREVENTION

INACIO ANDRE



- Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) are switching mechanisms that prevent a LAN with redundant links to forward Ethernet frames to loop in an indefinite time in a network. STP and RSTP have features that help the network work better and more securely, such as Portfast, BPDU Guard, and Root Guard.

- PortFast enables the switch to instantaneously transition from blocking state to forwarding state immediately through bypassing the listening and learning state. However, PortFast is highly recommended only on non-trunking access ports, such as edge ports, because these ports typically do not send nor receive BPDU.
- Because PortFast can be enabled on non-trunking ports connecting two switches, spanning-tree loops can occur because Bridge Protocol Data Units (BPDUs) are still being transmitted and received on those ports.

- Layer 2 loops in our network topology can be prevented by enabling another feature called PortFast BPDU Guard wherein it prevents the loop from happening by moving non-trunking switch ports into an errdisable state when the Bridge Protocol Data Unit (BPDU) is accepted on that port. Whenever STP BPDU guard is enabled on the switch, STP shuts down PortFast-configured interfaces on the switch that received Bridge Protocol Data Unit (BPDU) instead of putting them into STP blocking state.

- In a correct configuration, PortFast-configured ports do not receive BPDU. If a PortFast-configured interface receives a Bridge Protocol Data Unit (BPDU), a misconfiguration exists. BPDU guard provides a secure response to invalid configurations because the network engineer needs to manually put the interface in a forwarding state.

S1

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#int range f0/23-24
S1(config-if-range)#switchport mode trunk
```

```
S1(config-if-range)#exit
S1(config)#int range f0/1-22, g0/1-2
S1(config-if-range)#switchport mode access
S1(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
```

```
S1(config-if-range)#exit
S1(config)#spanning-tree portfast default
S1(config)#spanning-tree portfast bpduguard default
S1(config)#do wr
```

S2

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#int range f0/23-24
S2(config-if-range)#switchport mode trunk
```

```
S2(config)#int range f0/1-22, g0/1-2
S2(config-if-range)#switchport mode access
S2(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
```

```
S2(config)#spanning-tree portfast default
S2(config)#spanning-tree portfast bpduguard default
S2(config)#do wr
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0
```

S3

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#int range f0/23-24
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#exit
S3(config)#int f0/22
S3(config-if)#switchport mode trunk
S3(config-if)#spanning-tree guard root
S3(config-if)#exit
S3(config)#do wr
Building configuration...
```

```
S1#show spanning-tree summary
Switch is in pvst mode
Root bridge for: default
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      0         0        0          6          6

---------------------- -------- --------- -------- ---------- ----------
1 vlans                       0         0        0          6          6
```

```
S1#show spanning-tree interface f0/4 portfast
VLAN0001         enabled
```