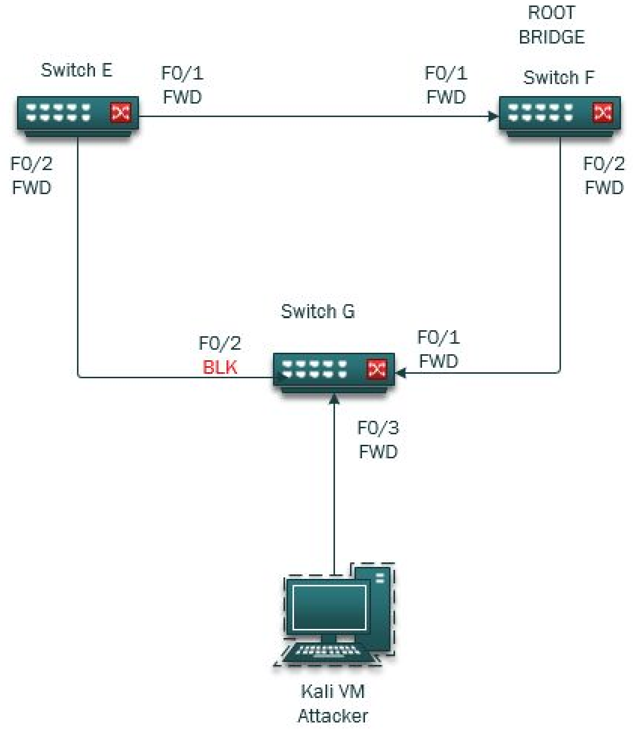
BPDU Guard

Overview:

Attack→ STP is a network protocol which prevents network loops. Layer 2 devices will use BPDU (bridge protocol data units) to share STP Priority Numbers and MAC Addresses to determine bridge ID’s.The lowest bridge ID becomes the root bridge. By Injecting spoofed BPDU’s with a fake bridge ID’s based on lower mac addresses, the topology changes and elects a new Root Bridge. From that point, traffic being sent within this compromised VLAN topology can now be eavesdropped upon.

Mitigation→ BPDU Guard is a spanning tree security feature that helps protect against layer 2 spanning tree DoS/overflow & MITM attacks. BPDU guard disables the port upon BPDU reception if PortFast is enabled on the port. This denies devices connected to these ports from participating in the STP.

LAB Topology

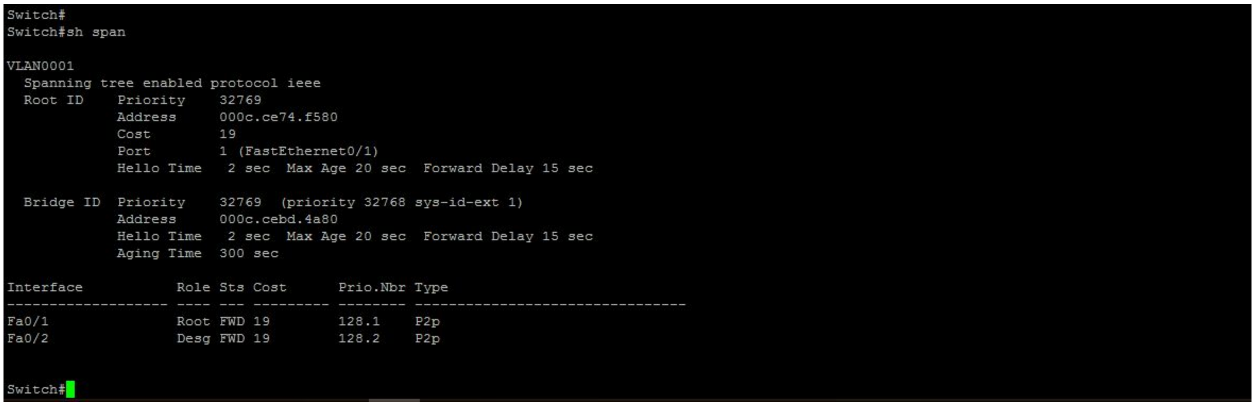


PART 1: Initial Setup

Step 1 - show spanning-tree [for switch E, F & G] to view current STP topology
Step 2 - configure spanning-tree debug messages [for switch E, F & G] to follow changes made

Step 1 - show spanning-tree [for switch E, F & G] to view current STP topology

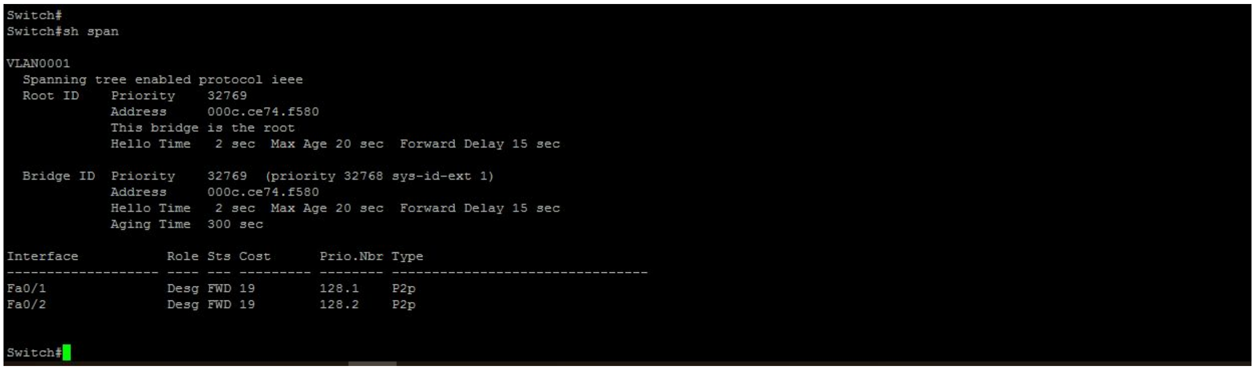
[Switch E] sh spanning-tree



```
Switch#
Switch#sh span

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce74.f580
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.cebd.4a80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p
Fa0/2               Desg FWD 19        128.2    P2p


Switch#
```

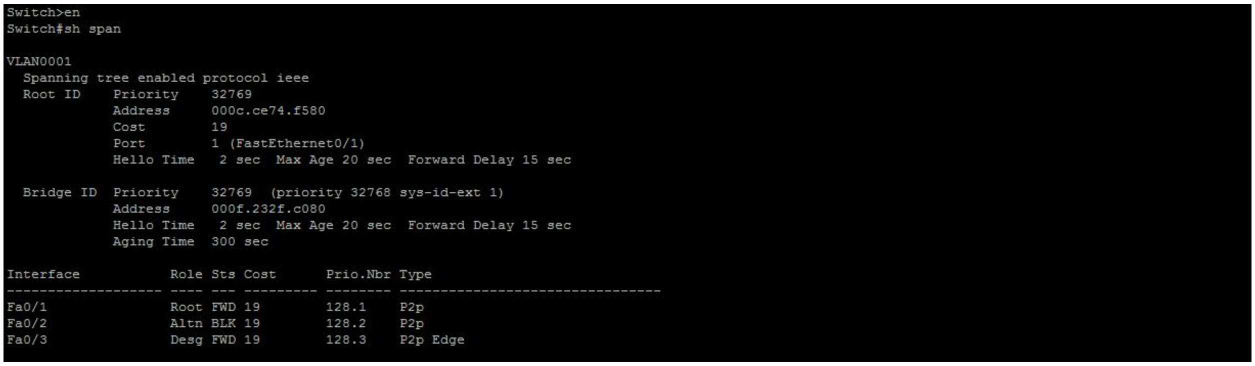
[Switch F] sh spanning-tree

NOTE: Switch F is the Root Bridge



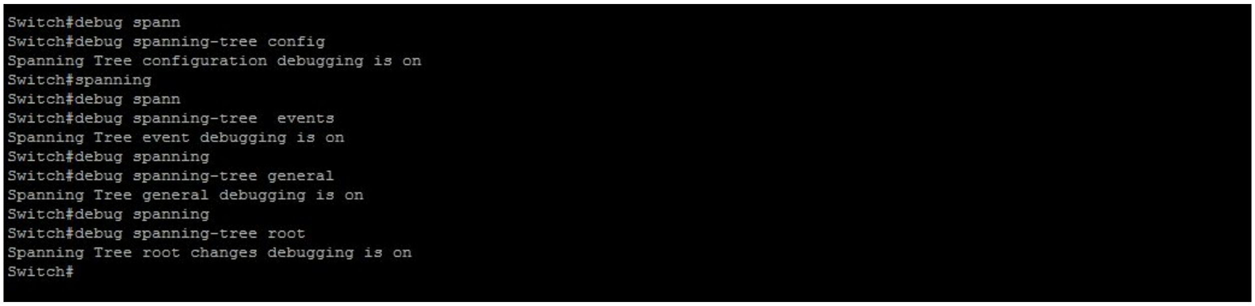
```
Switch#
Switch#sh span

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce74.f580
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.ce74.f580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Desg FWD 19        128.1    P2p
Fa0/2               Desg FWD 19        128.2    P2p


Switch#
```

[Switch G] sh spanning-tree



```
Switch>en
Switch#sh span

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce74.f580
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000f.232f.c080
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p
Fa0/2               Altn BLK 19        128.2    P2p
Fa0/3               Desg FWD 19        128.3    P2p Edge
```

Step 2 - Configure debug messages on [Switch E, Switch F & Switch G]
NOTE: Will allow us to see future changes made to the STP topology from each switch console



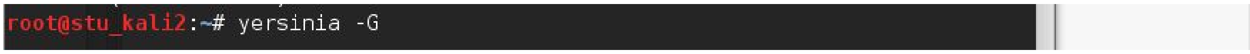
```
Switch#debug spann
Switch#debug spanning-tree config
Spanning Tree configuration debugging is on
Switch#spanning
Switch#debug spann
Switch#debug spanning-tree  events
Spanning Tree event debugging is on
Switch#debug spanning
Switch#debug spanning-tree general
Spanning Tree general debugging is on
Switch#debug spanning
Switch#debug spanning-tree root
Spanning Tree root changes debugging is on
Switch#
```

PART 2 : Launch Spanning Tree Attack

The basic steps to run exploit:

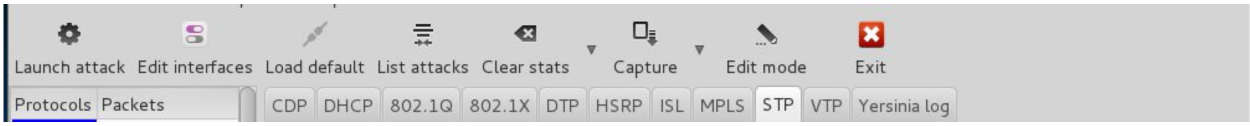
Step 1 - Open Yersinia from Kali VM command
Step 2 - Select STP & choose launch attack
Step 3 - Select ‘claiming root role’ and click ok to run attack
NOTE - Note that attack had begun, BPDU [Bridge Protocol Data Units] are being sent out
NOTE: BPDU flooding on Switch G, see console for debug messages

Steps to see and understand results
Step 1 - Open Yersinia from Kali VM command

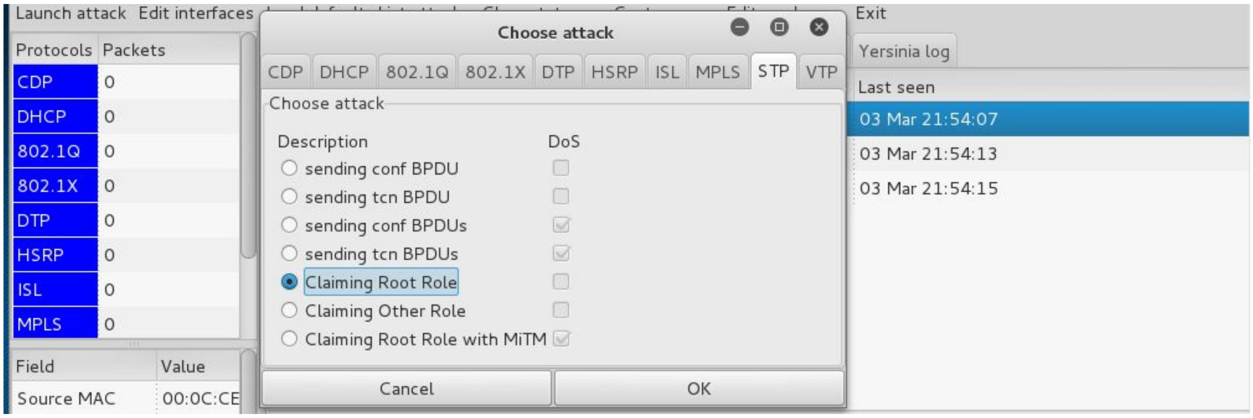


```
root@stu_kali2:~# yersinia -G
```

Step 2 - Select STP & choose launch attack



Step 3 - Select ‘claiming root role’ and click ok to run attack



Protocols	Packets
CDP	0
DHCP	0
802.1Q	0
802.1X	0
DTP	0
HSRP	0
ISL	0
MPLS	0

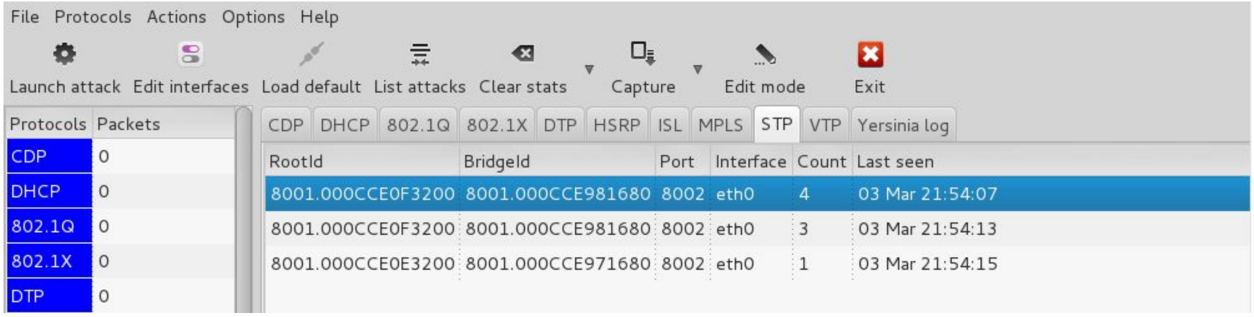
Field	Value
Source MAC	00:0C:CE

Choose attack

Description	DoS
○ sending conf BPDU	□
○ sending tcn BPDU	□
○ sending conf BPDUs	☑
○ sending tcn BPDUs	☑
● Claiming Root Role	□
○ Claiming Other Role	□
○ Claiming Root Role with MiTM	☑

Last seen
03 Mar 21:54:07
03 Mar 21:54:13
03 Mar 21:54:15

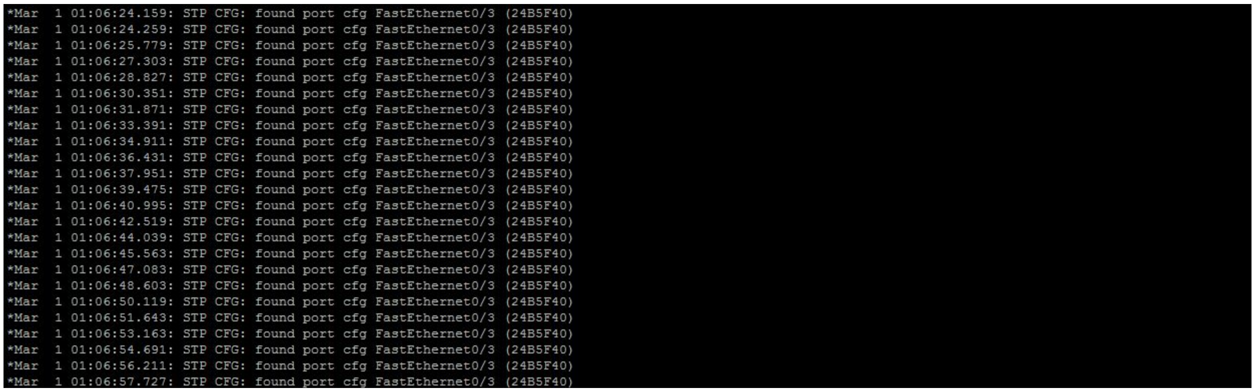
NOTE - Note that attack had begun, BPDU[Bridge Protocol Data Units] sent to switch G port 3



Protocols	Packets
CDP	0
DHCP	0
802.1Q	0
802.1X	0
DTP	0

RootId	BridgeId	Port	Interface	Count	Last seen
8001.000CCE0F3200	8001.000CCE981680	8002	eth0	4	03 Mar 21:54:07
8001.000CCE0F3200	8001.000CCE981680	8002	eth0	3	03 Mar 21:54:13
8001.000CCE0E3200	8001.000CCE971680	8002	eth0	1	03 Mar 21:54:15

NOTE: BPDU Flood on switch G, Port 3



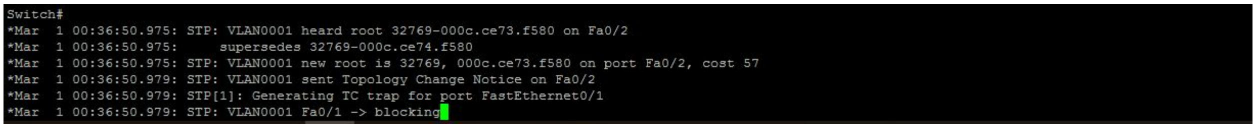
```
*Mar  1 01:06:24.159: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:24.259: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:25.779: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:27.303: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:28.827: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:30.351: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:31.871: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:33.391: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:34.911: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:36.431: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:37.951: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:39.475: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:40.995: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:42.519: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:44.039: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:45.563: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:47.083: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:48.603: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:50.119: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:51.643: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:53.163: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:54.691: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:56.211: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:06:57.727: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
```

View Attack Results:

Results A - view debug messages showing STP topology changes for [Switch E,F & G]
Results B - show spanning-tree [for switch E, F & G] to view current STP topology
Results C - see post attack lab topology

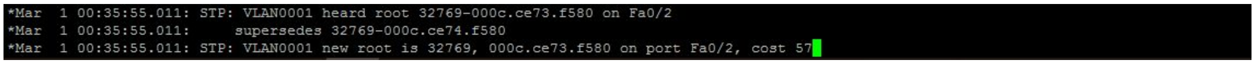
Step 1 - view debug messages showing STP topology changes for [Switch E,F & G]

[Switch E] debug topology change



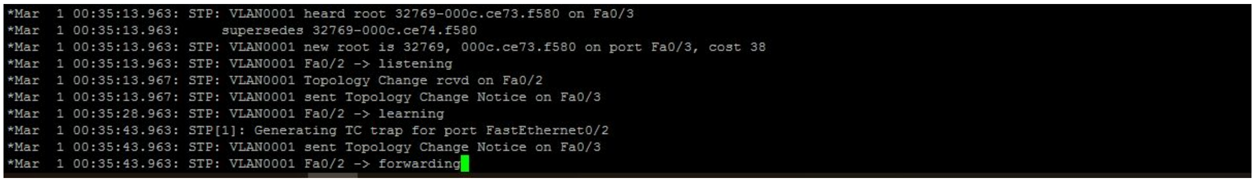
```
Switch#
*Mar  1 00:36:50.975: STP: VLAN0001 heard root 32769-000c.ce73.f580 on Fa0/2
*Mar  1 00:36:50.975:     supersedes 32769-000c.ce74.f580
*Mar  1 00:36:50.975: STP: VLAN0001 new root is 32769, 000c.ce73.f580 on port Fa0/2, cost 57
*Mar  1 00:36:50.979: STP: VLAN0001 sent Topology Change Notice on Fa0/2
*Mar  1 00:36:50.979: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar  1 00:36:50.979: STP: VLAN0001 Fa0/1 -> blocking
```

[Switch F] debug topology change



```
*Mar  1 00:35:55.011: STP: VLAN0001 heard root 32769-000c.ce73.f580 on Fa0/2
*Mar  1 00:35:55.011:     supersedes 32769-000c.ce74.f580
*Mar  1 00:35:55.011: STP: VLAN0001 new root is 32769, 000c.ce73.f580 on port Fa0/2, cost 57
```

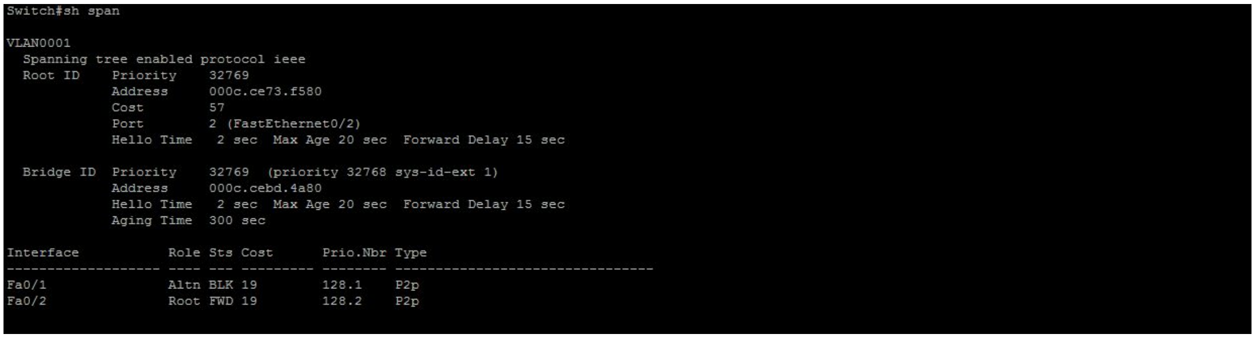
[Switch G] debug topology change



```
*Mar  1 00:35:13.963: STP: VLAN0001 heard root 32769-000c.ce73.f580 on Fa0/3
*Mar  1 00:35:13.963:     supersedes 32769-000c.ce74.f580
*Mar  1 00:35:13.963: STP: VLAN0001 new root is 32769, 000c.ce73.f580 on port Fa0/3, cost 38
*Mar  1 00:35:13.963: STP: VLAN0001 Fa0/2 -> listening
*Mar  1 00:35:13.967: STP: VLAN0001 Topology Change rcvd on Fa0/2
*Mar  1 00:35:13.967: STP: VLAN0001 sent Topology Change Notice on Fa0/3
*Mar  1 00:35:28.963: STP: VLAN0001 Fa0/2 -> learning
*Mar  1 00:35:43.963: STP[1]: Generating TC trap for port FastEthernet0/2
*Mar  1 00:35:43.963: STP: VLAN0001 sent Topology Change Notice on Fa0/3
*Mar  1 00:35:43.963: STP: VLAN0001 Fa0/2 -> forwarding
```

Step 2 - show spanning-tree [for switch E, F & G] to view current STP topology

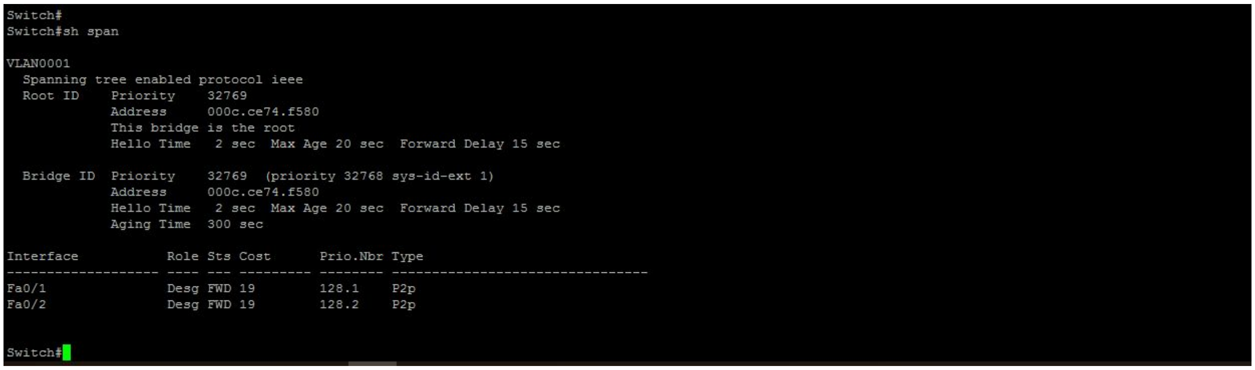
[Switch E] show spanning-tree



```
Switch#sh span

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce73.f580
             Cost        57
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.cebd.4a80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Altn BLK 19        128.1    P2p
Fa0/2               Root FWD 19        128.2    P2p
```

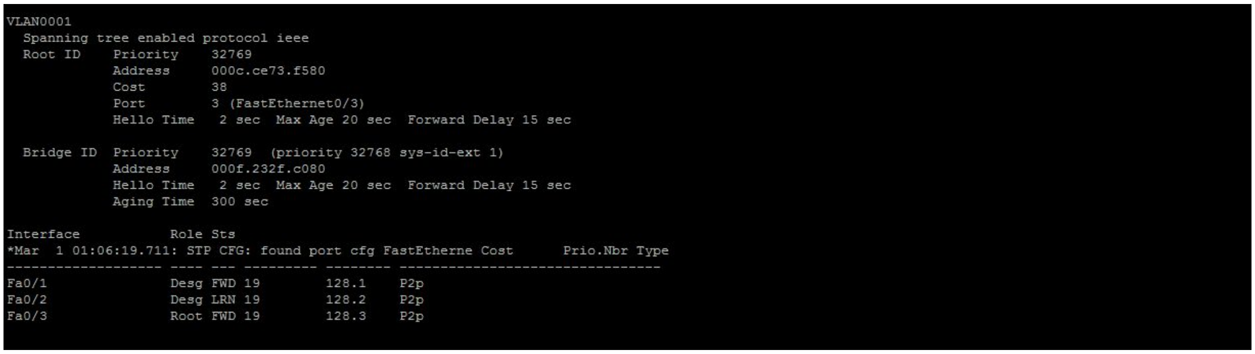
[Switch F] show spanning-tree

NOTE: No longer the Root Bridge | superior mac address has taken over



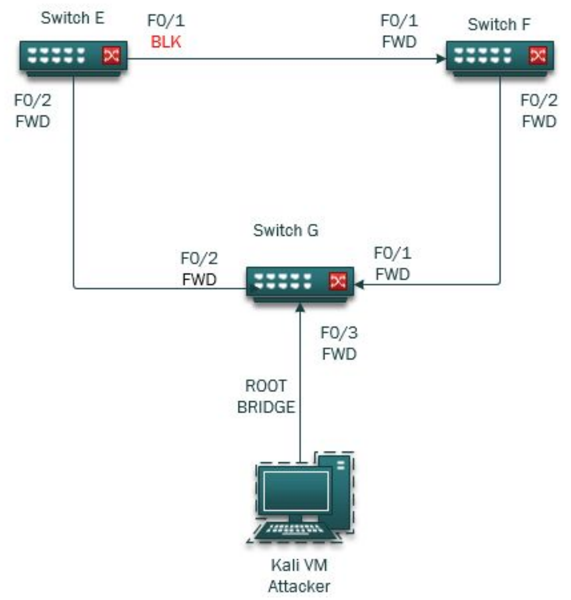
```
Switch#
Switch#sh span

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce74.f580
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.ce74.f580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Desg FWD 19        128.1    P2p
Fa0/2               Desg FWD 19        128.2    P2p


Switch#
```

[Switch G] show spanning-tree



```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce73.f580
             Cost        38
             Port        3 (FastEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000f.232f.c080
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts
*Mar  1 01:06:19.711: STP CFG: found port cfg FastEtherne Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Desg FWD 19        128.1    P2p
Fa0/2               Desg LRN 19        128.2    P2p
Fa0/3               Root FWD 19        128.3    P2p
```

Step 3 - See post attack Lab Topology
NOTE: The Blocked Port / Root Bridge has changed.



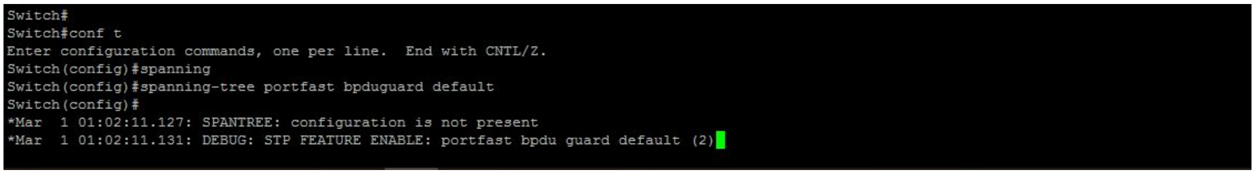
PART 3 : Attack Mitigation

Steps to mitigation:

Step 1 - Configure spanning-tree portfast bpduguard default on switch G
Step 2 - Set spanning-tree portfast on port 3 of switch G
NOTE: rerun Attack

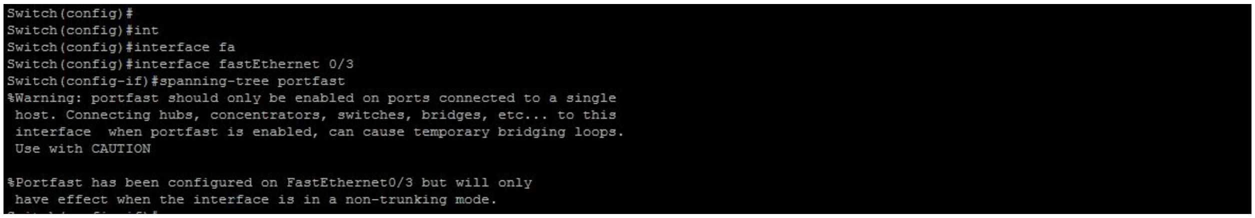
Results A: see BPDU error detected, block on switch G port 0/3
Results B: see err-disabled status
NOTE: Issue shutdown / No shutdown on switch G, Port 3 ro remove err-disable state

Step 1 - Configure spanning-tree portfast bpduguard default on switch G



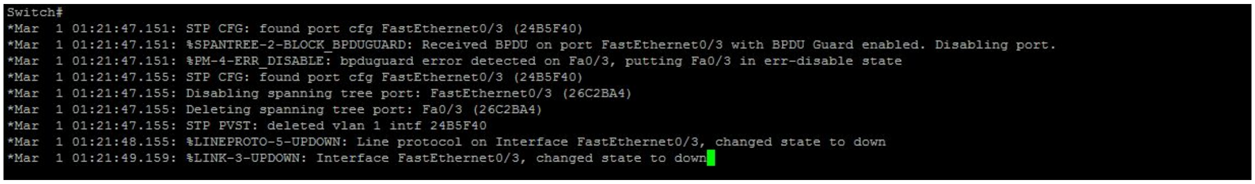
```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning
Switch(config)#spanning-tree portfast bpduguard default
Switch(config)#
*Mar  1 01:02:11.127: SPANTREE: configuration is not present
*Mar  1 01:02:11.131: DEBUG: STP FEATURE ENABLE: portfast bpdu guard default (2)
```

Step 2 - Set spanning-tree portfast on port 3 of switch G



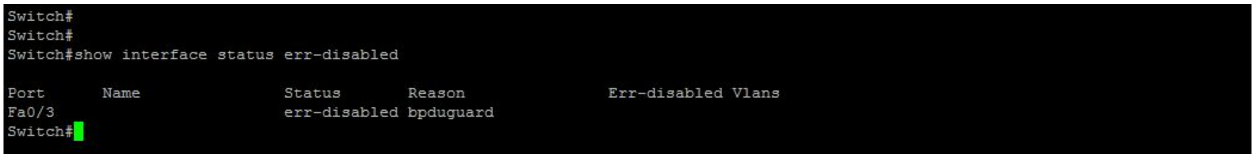
```
Switch(config)#
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
 have effect when the interface is in a non-trunking mode.
```

Results A: BPDU error detected, block on switch G port 3 Note: state changed to down



```
Switch#
*Mar  1 01:21:47.151: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:21:47.151: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/3 with BPDU Guard enabled. Disabling port.
*Mar  1 01:21:47.151: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/3, putting Fa0/3 in err-disable state
*Mar  1 01:21:47.155: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:21:47.155: Disabling spanning tree port: FastEthernet0/3 (26C2BA4)
*Mar  1 01:21:47.155: Deleting spanning tree port: Fa0/3 (26C2BA4)
*Mar  1 01:21:47.155: STP PVST: deleted vlan 1 intf 24B5F40
*Mar  1 01:21:48.155: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
*Mar  1 01:21:49.159: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
```

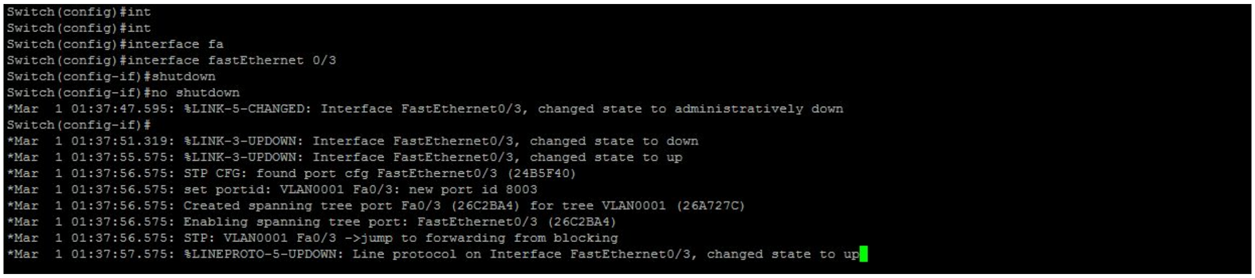
Results B: show interface status err-disabled on switch G



```
Switch#
Switch#
Switch#show interface status err-disabled

Port      Name               Status       Reason               Err-disabled Vlans
Fa0/3                        err-disabled bpduguard
Switch#
```

Reset: Issue shutdown / No shutdown on switch G, Port 3 ro remove err-disable state

NOTE: The switch port is now up



```
Switch(config)#int
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
*Mar  1 01:37:47.595: %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
Switch(config-if)#
*Mar  1 01:37:51.319: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
*Mar  1 01:37:55.575: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Mar  1 01:37:56.575: STP CFG: found port cfg FastEthernet0/3 (24B5F40)
*Mar  1 01:37:56.575: set portid: VLAN0001 Fa0/3: new port id 8003
*Mar  1 01:37:56.575: Created spanning tree port Fa0/3 (26C2BA4) for tree VLAN0001 (26A727C)
*Mar  1 01:37:56.575: Enabling spanning tree port: FastEthernet0/3 (26C2BA4)
*Mar  1 01:37:56.575: STP: VLAN0001 Fa0/3 ->jump to forwarding from blocking
*Mar  1 01:37:57.575: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

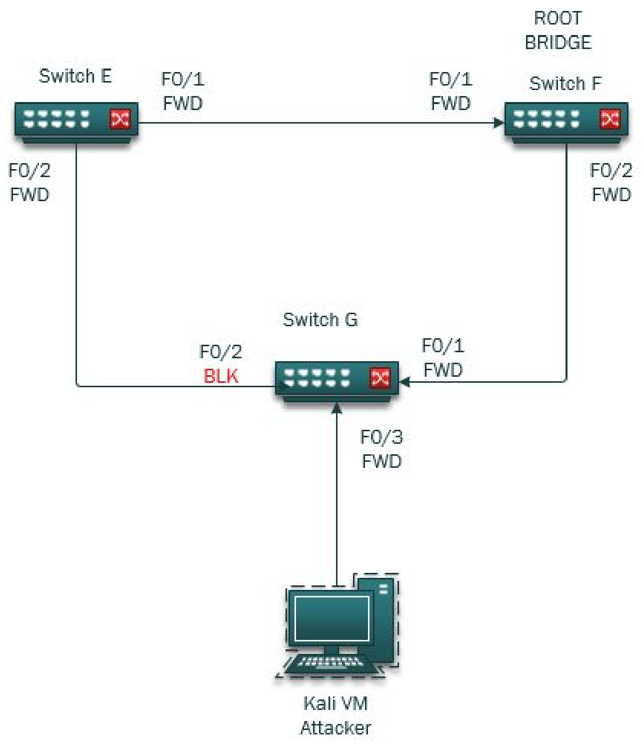
Root Guard

Overview:

Attack→. STP is a network protocol which prevents network loops. Layer 2 devices will use BPDU (bridge protocol data units) to share STP Priority Numbers and MAC Addresses to determine bridge ID's.The lowest bridge ID becomes the root bridge. By Injecting spoofed BPDU's with a fake bridge ID based on lower mac addresses, the topology changes and elects a new Root Bridge. From that point, traffic being sent within this compromised VLAN topology can now be eavesdropped upon.

Mitigation→ Root guard allows the device to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. Recovery occurs as soon as the offending device ceases to send superior BPDUs.

LAB Topology

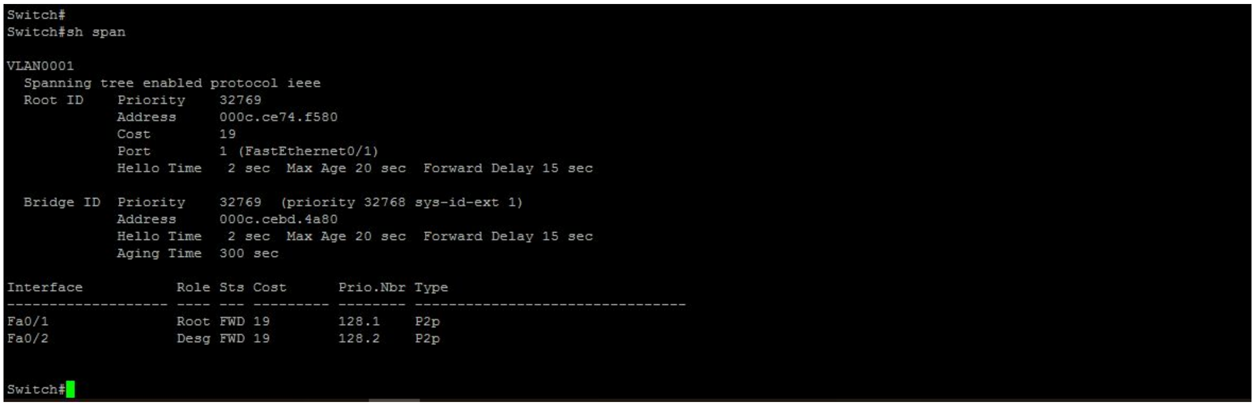


PART 1: Initial Setup

Step 1 - show spanning-tree [for switch E, F & G] to view current STP topology
Step 2 - configure spanning-tree debug messages [for switch E, F & G] to follow changes made

Step 1 - show spanning-tree [for switch E, F & G] to view current STP topology

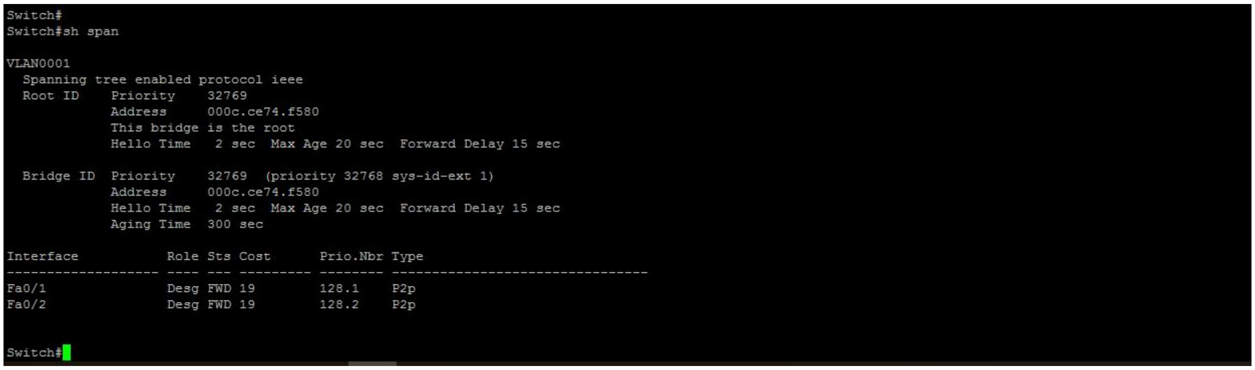
[Switch E] sh spanning-tree



```
Switch#
Switch#sh span

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce74.f580
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.cebd.4a80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p
Fa0/2               Desg FWD 19        128.2    P2p


Switch#
```

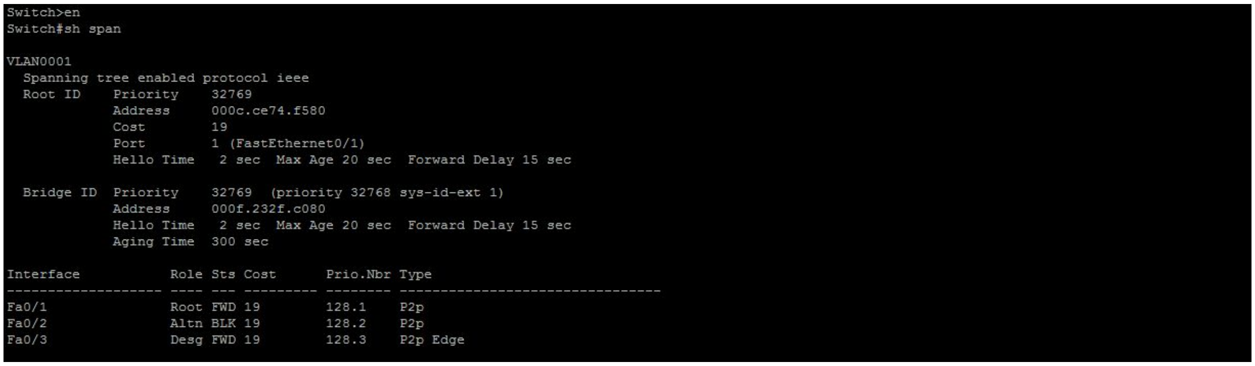
[Switch F] sh spanning-tree

NOTE: Switch F is the Root Bridge



```
Switch#
Switch#sh span

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce74.f580
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000c.ce74.f580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Desg FWD 19        128.1    P2p
Fa0/2               Desg FWD 19        128.2    P2p


Switch#
```

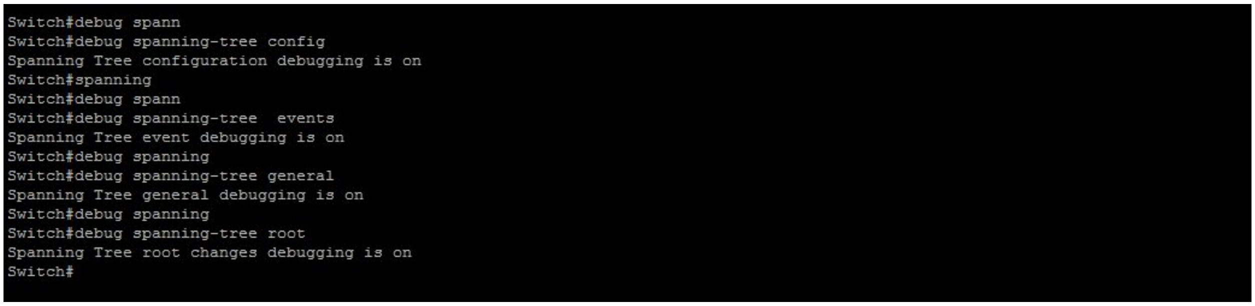
[Switch G] sh spanning-tree



```
Switch>en
Switch#sh span

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce74.f580
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000f.232f.c080
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p
Fa0/2               Altn BLK 19        128.2    P2p
Fa0/3               Desg FWD 19        128.3    P2p Edge
```

Step 2 - Configure debug messages on [Switch E, Switch F & Switch G]

NOTE: Will allow us to see future changes made to the STP topology from each switch console



```
Switch#debug spann
Switch#debug spanning-tree config
Spanning Tree configuration debugging is on
Switch#spanning
Switch#debug spann
Switch#debug spanning-tree  events
Spanning Tree event debugging is on
Switch#debug spanning
Switch#debug spanning-tree general
Spanning Tree general debugging is on
Switch#debug spanning
Switch#debug spanning-tree root
Spanning Tree root changes debugging is on
Switch#
```

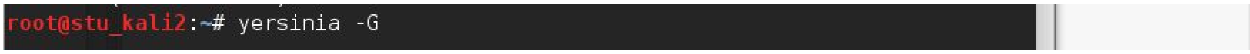
PART 2 : Launch Spanning Tree Attack

The basic steps to run exploit:

Step 1 - Open Yersinia from Kali VM command
Step 2 - Select STP & choose launch attack
Step 3 - Select ‘claiming root role’ and click ok to run attack
NOTE - Note that attack had begun, BPDU [Bridge Protocol Data Units] are being sent out
NOTE: BPDU flooding on Switch G, see console for debug messages

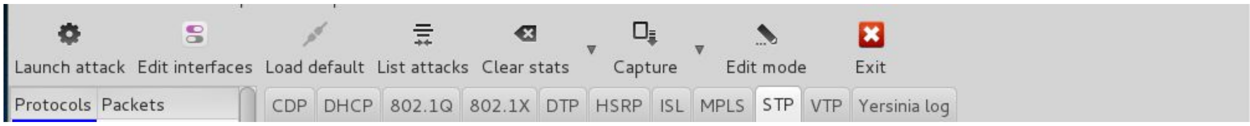
Steps to see and understand results

Step 1 - Open Yersinia from Kali VM command



```
root@stu_kali2:~# yersinia -G
```

Step 2 - Select STP & choose launch attack



Launch attack
Edit interfaces
Load default
List attacks
Clear stats
Capture
Edit mode
Exit
Protocols
Packets
CDP
DHCP
802.1Q
802.1X
DTP
HSRP
ISL
MPLS
STP
VTP
Yersinia log