Root Guard
BPDU Guard
802.1X

Sumayyah Alahmadi sfa8135@rit.edu

Lab partner: Mugdha Deshmukh, mud5545@rit.edu

CSEC.744.01

Professor Jonathan Weissman

Table of contents

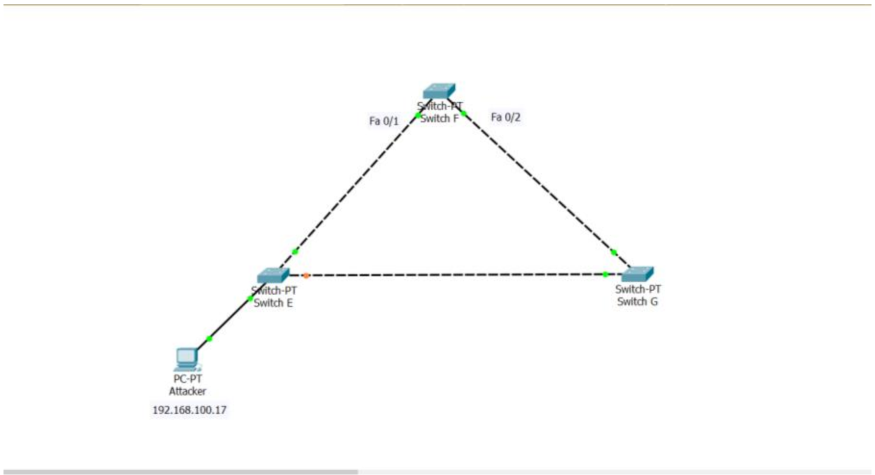
Root Guard

The attacker want to be the root so that all the traffic will go pass by him and perform man in the middle attack. The concept behind the root guard is that it prevents the attacker from sending superior BPDU to the port when he try to become a root. The root guard feature is disable by default. To enable it use the following per-port based command

- Switch(config-if)# **spanning-tree guard root**

If the port received superior BPDU after enabling the root guard it will go to root-inconsistant STP state which wont block the port, it will keep listening to the upcoming BPDU but without sending and receiving actual data in that port. Eventually, the port will go back to its normal state if the attacker stopped sending superior BPDU.

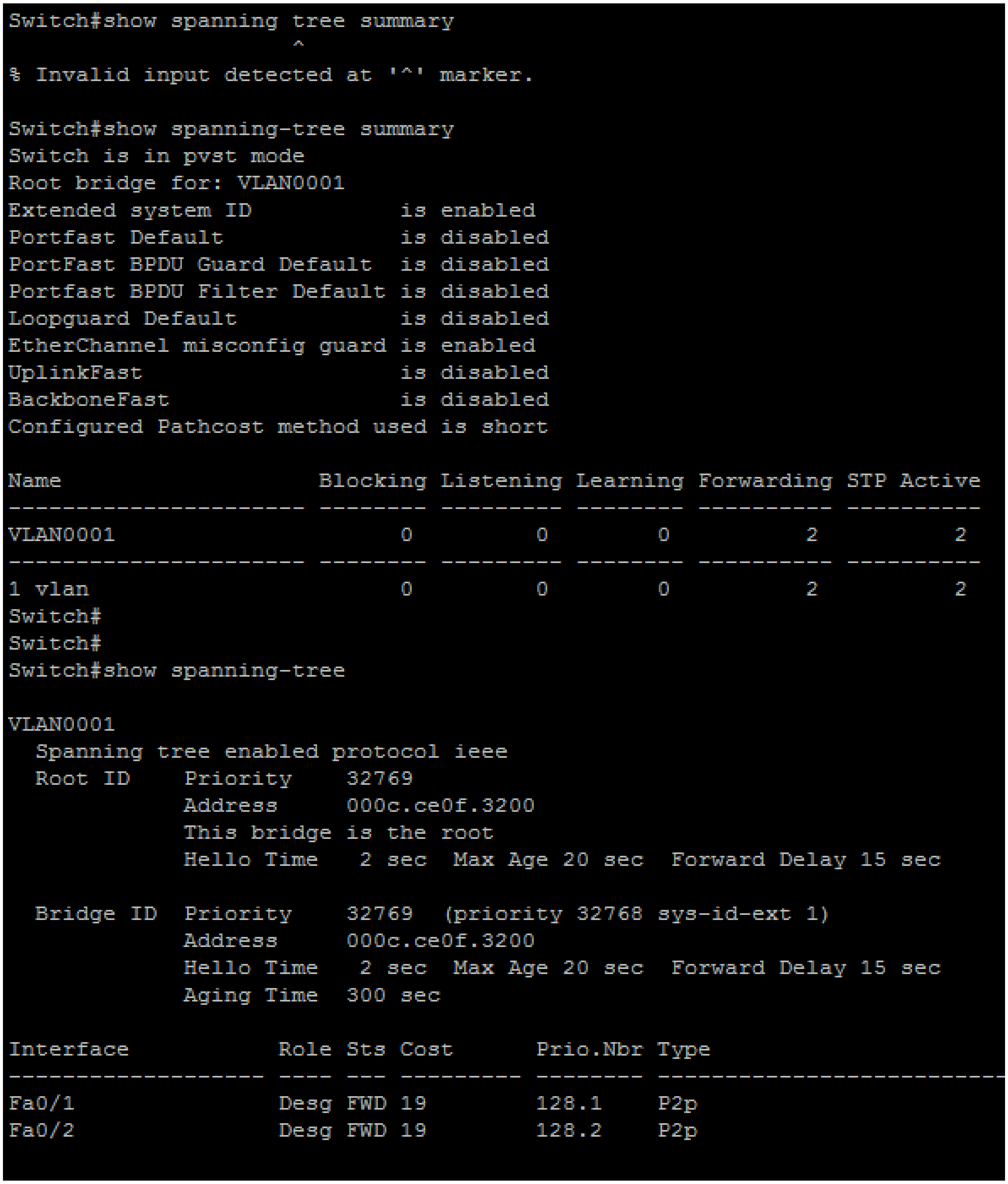
Topology :



Implementation:

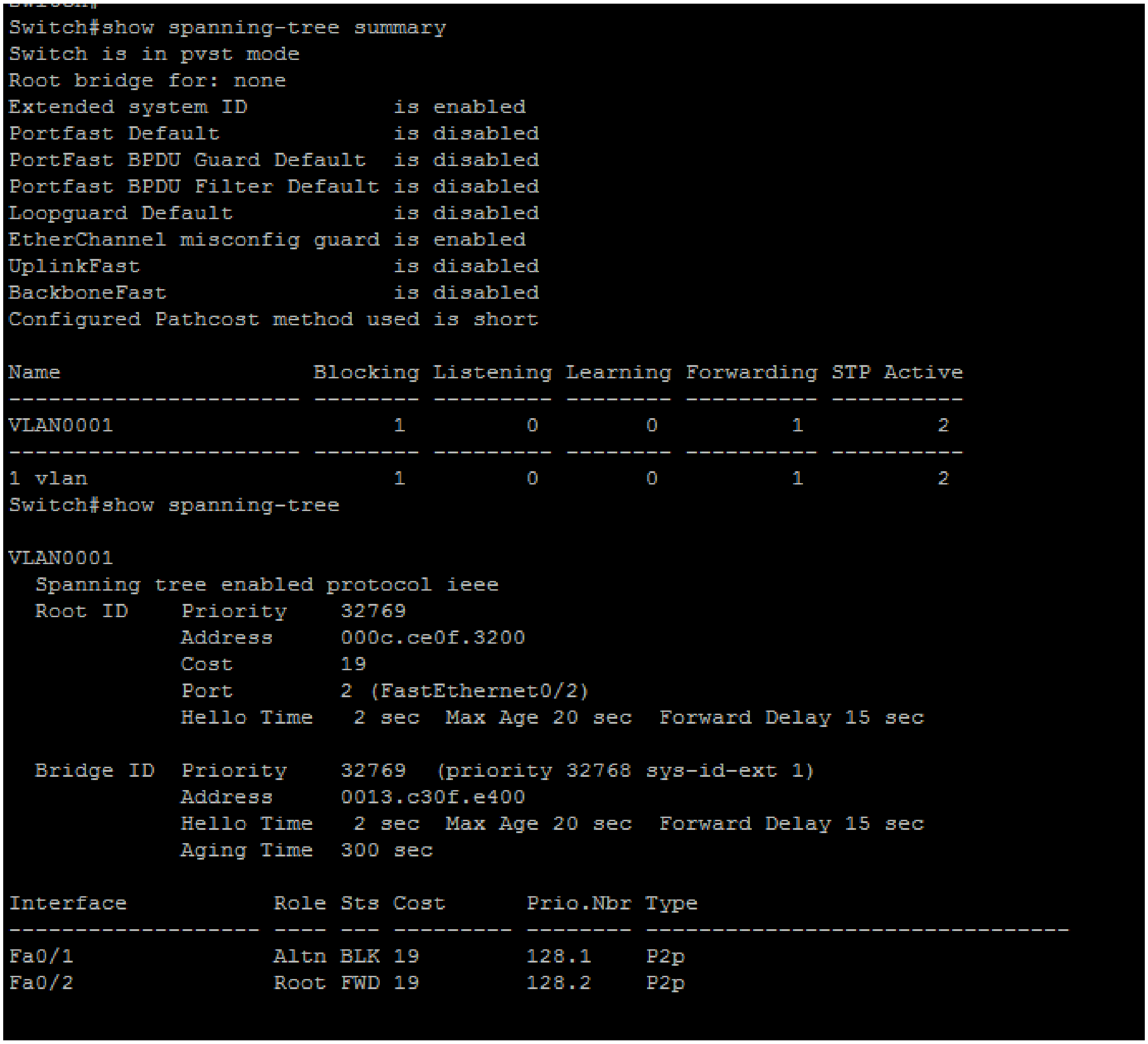
First we configure three switches and one PC as an attacker. The three switches are: E,F,G where F is the root. Switch E connect to a PC in the same subnet with an IP address 192.168.100.17. here is th configuration for the three switches along with Kali machine the attacker.

Switch F the root:



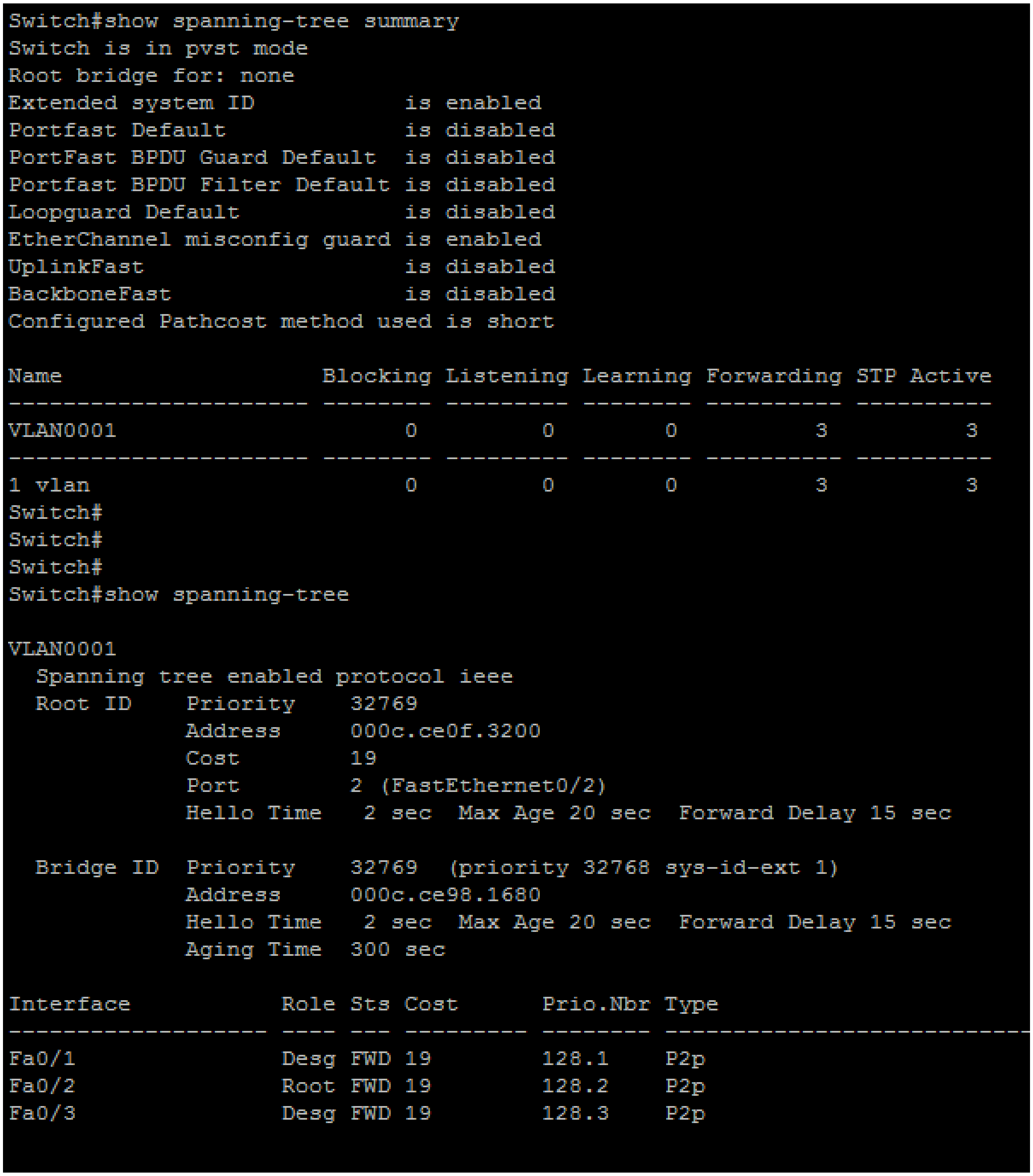
```
Switch#show spanning tree summary
                     ^
% Invalid input detected at '^' marker.

Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        0          2          2
---------------------- -------- --------- -------- ---------- ----------
1 vlan                       0         0        0          2          2
Switch#
Switch#
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce0f.3200
             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.ce0f.3200
             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
```

Then switch G



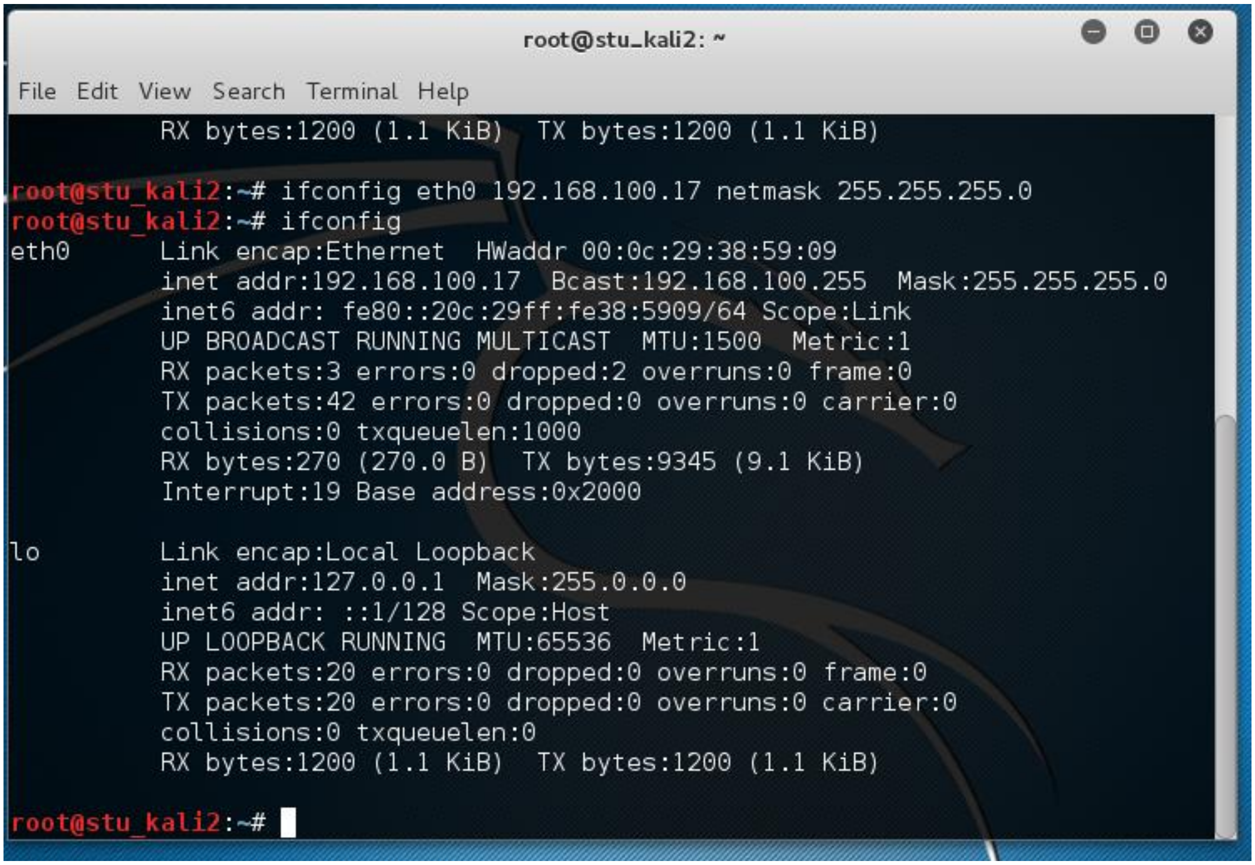
```
Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     1         0        0          1          2
---------------------- -------- --------- -------- ---------- ----------
1 vlan                       1         0        0          1          2
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce0f.3200
             Cost        19
             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     0013.c30f.e400
             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 E which is connected to the attacker machine



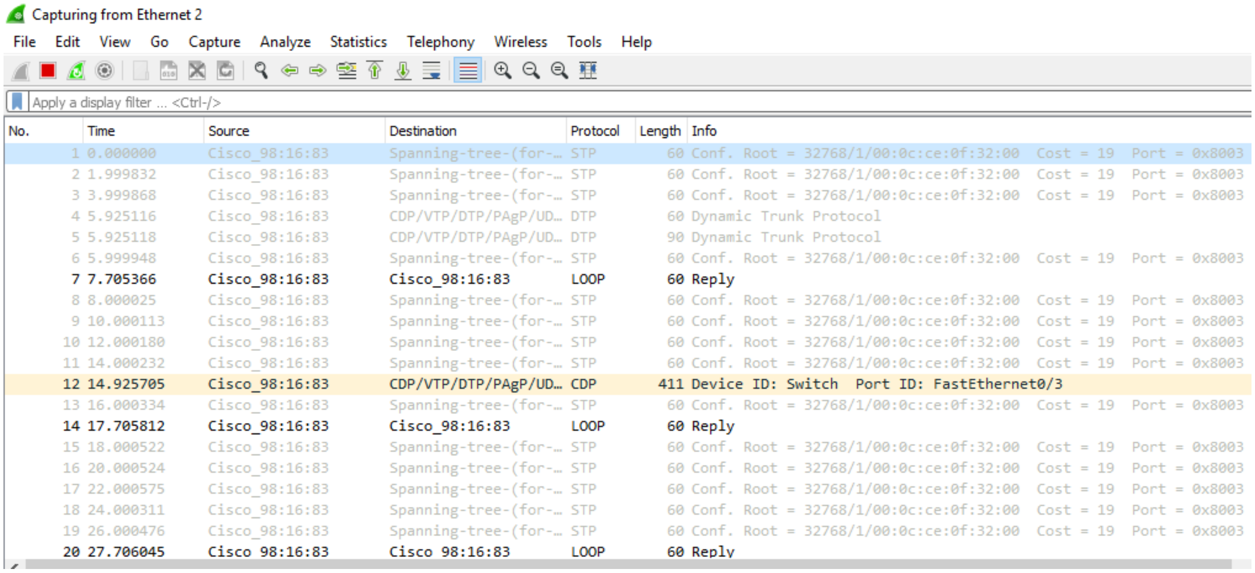
```
Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        0          3          3
---------------------- -------- --------- -------- ---------- ----------
1 vlan                       0         0        0          3          3
Switch#
Switch#
Switch#
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce0f.3200
             Cost        19
             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.ce98.1680
             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               Root FWD 19        128.2    P2p
Fa0/3               Desg FWD 19        128.3    P2p
```

Then configure the attacker machine



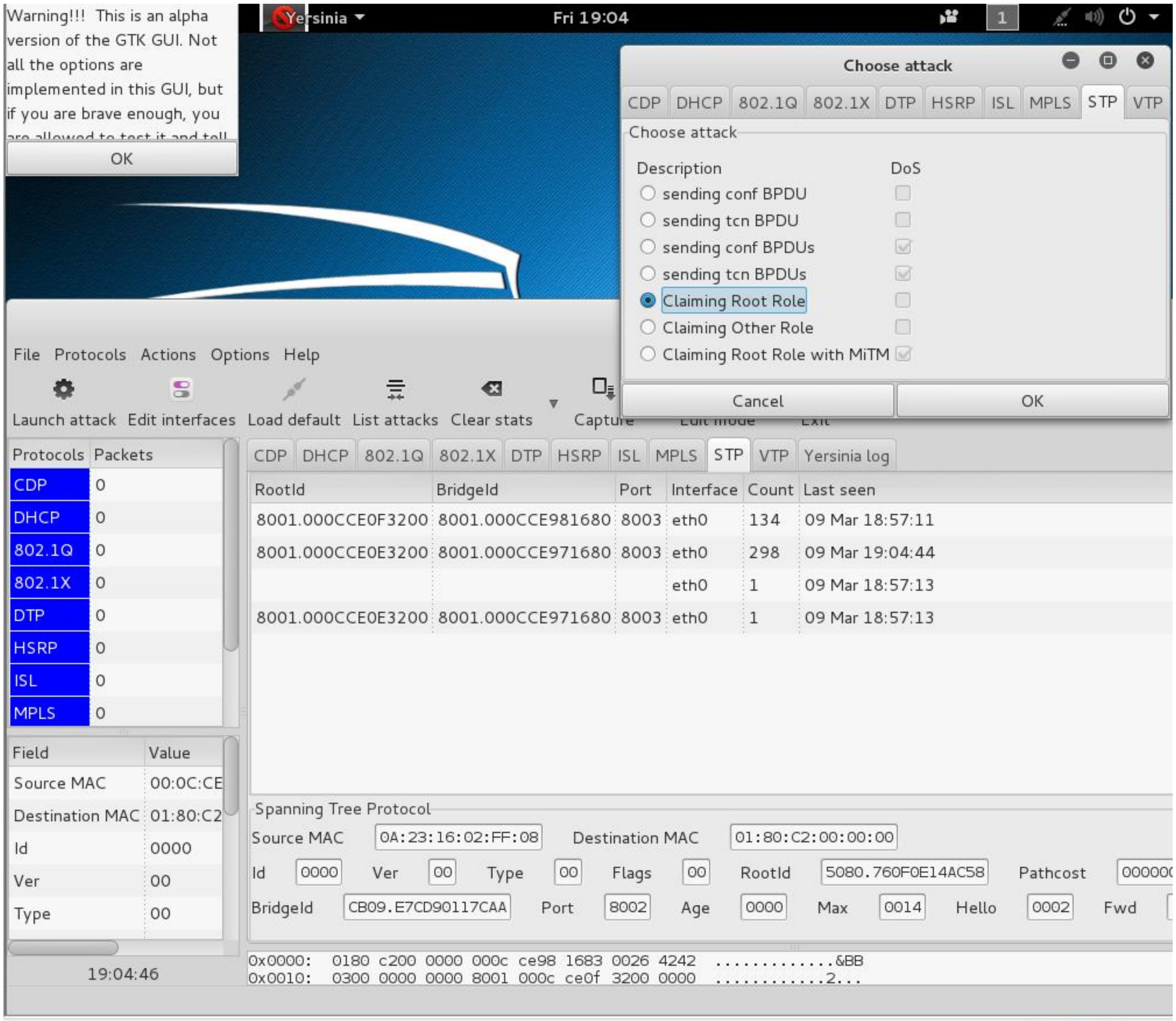
```
          RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)

root@stu_kali2:~# ifconfig eth0 192.168.100.17 netmask 255.255.255.0
root@stu_kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:38:59:09
          inet addr:192.168.100.17  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe38:5909/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:2 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:270 (270.0 B)  TX bytes:9345 (9.1 KiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)

root@stu_kali2:~# 
```

Testing the STP connection before performing the attack


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
2	1.999832	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
3	3.999868	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
4	5.925116	Cisco_98:16:83	CDP/VTP/DTP/PAgP/UD...	DTP	60	Dynamic Trunk Protocol
5	5.925118	Cisco_98:16:83	CDP/VTP/DTP/PAgP/UD...	DTP	90	Dynamic Trunk Protocol
6	5.999948	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
7	7.705366	Cisco_98:16:83	Cisco_98:16:83	LOOP	60	Reply
8	8.000025	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
9	10.000113	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
10	12.000180	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
11	14.000232	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
12	14.925705	Cisco_98:16:83	CDP/VTP/DTP/PAgP/UD...	CDP	411	Device ID: Switch Port ID: FastEthernet0/3
13	16.000334	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
14	17.705812	Cisco_98:16:83	Cisco_98:16:83	LOOP	60	Reply
15	18.000522	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
16	20.000524	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
17	22.000575	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
18	24.000311	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
19	26.000476	Cisco_98:16:83	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/00:0c:ce:0f:32:00 Cost = 19 Port = 0x8003
20	27.706045	Cisco_98:16:83	Cisco_98:16:83	LOOP	60	Reply

Then trying to perform the attack using Yersinia



Warning!!! This is an alpha version of the GTK GUI. Not all the options are implemented in this GUI, but if you are brave enough, you are allowed to test it and tell

Choose attack

CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP

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	☑

Cancel
OK
File Protocols Actions Options Help
Launch attack
Edit interfaces
Load default
List attacks
Clear stats
Capture
Edit mode
Exit
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log

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

RootId	BridgeId	Port	Interface	Count	Last seen
8001.000CCE0F3200	8001.000CCE981680	8003	eth0	134	09 Mar 18:57:11
8001.000CCE0E3200	8001.000CCE971680	8003	eth0	298	09 Mar 19:04:44
			eth0	1	09 Mar 18:57:13
8001.000CCE0E3200	8001.000CCE971680	8003	eth0	1	09 Mar 18:57:13

Field	Value
Source MAC	00:0C:CE
Destination MAC	01:80:C2
Id	0000
Ver	00
Type	00

19:04:46

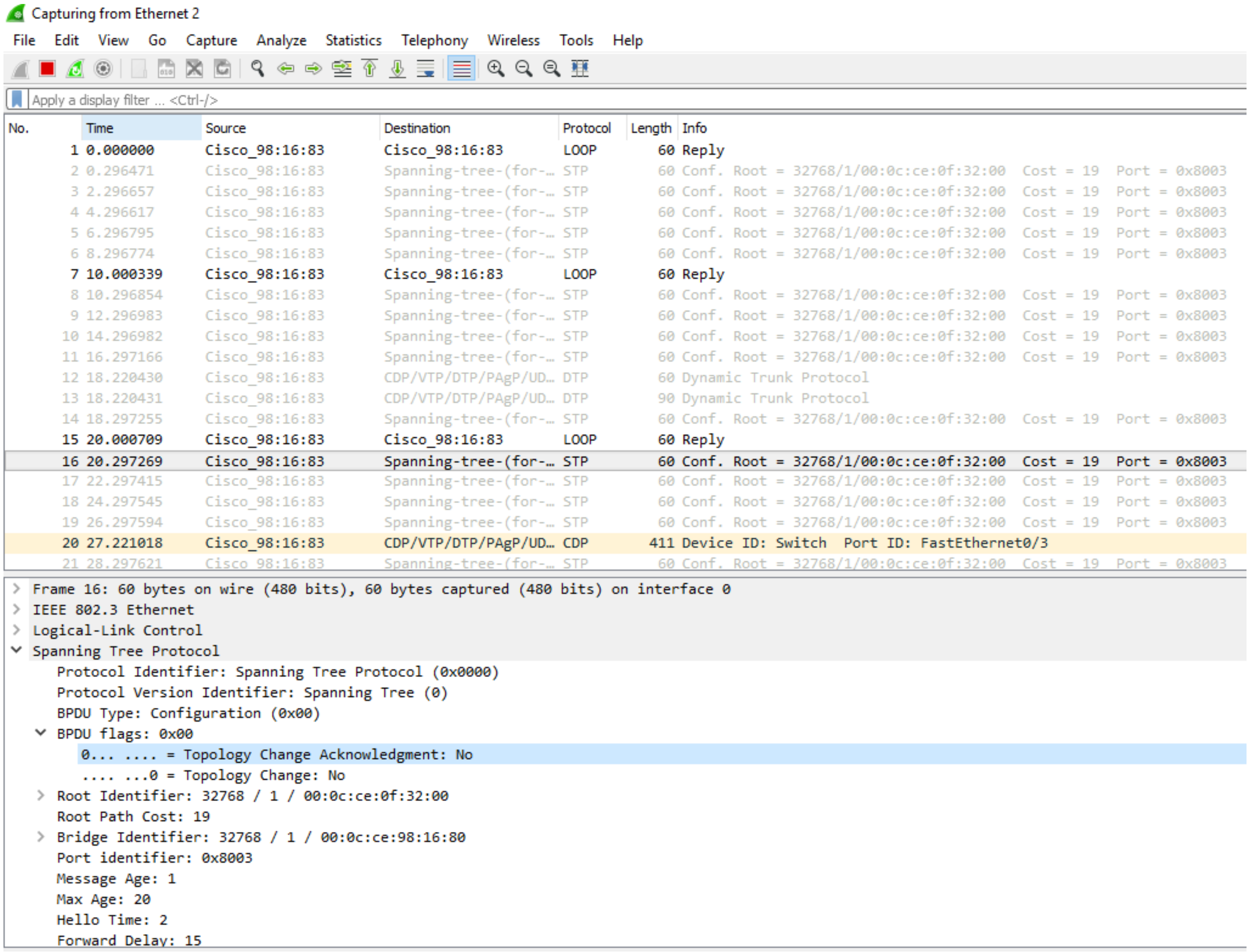
Spanning Tree Protocol

Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00

Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 000000

BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd

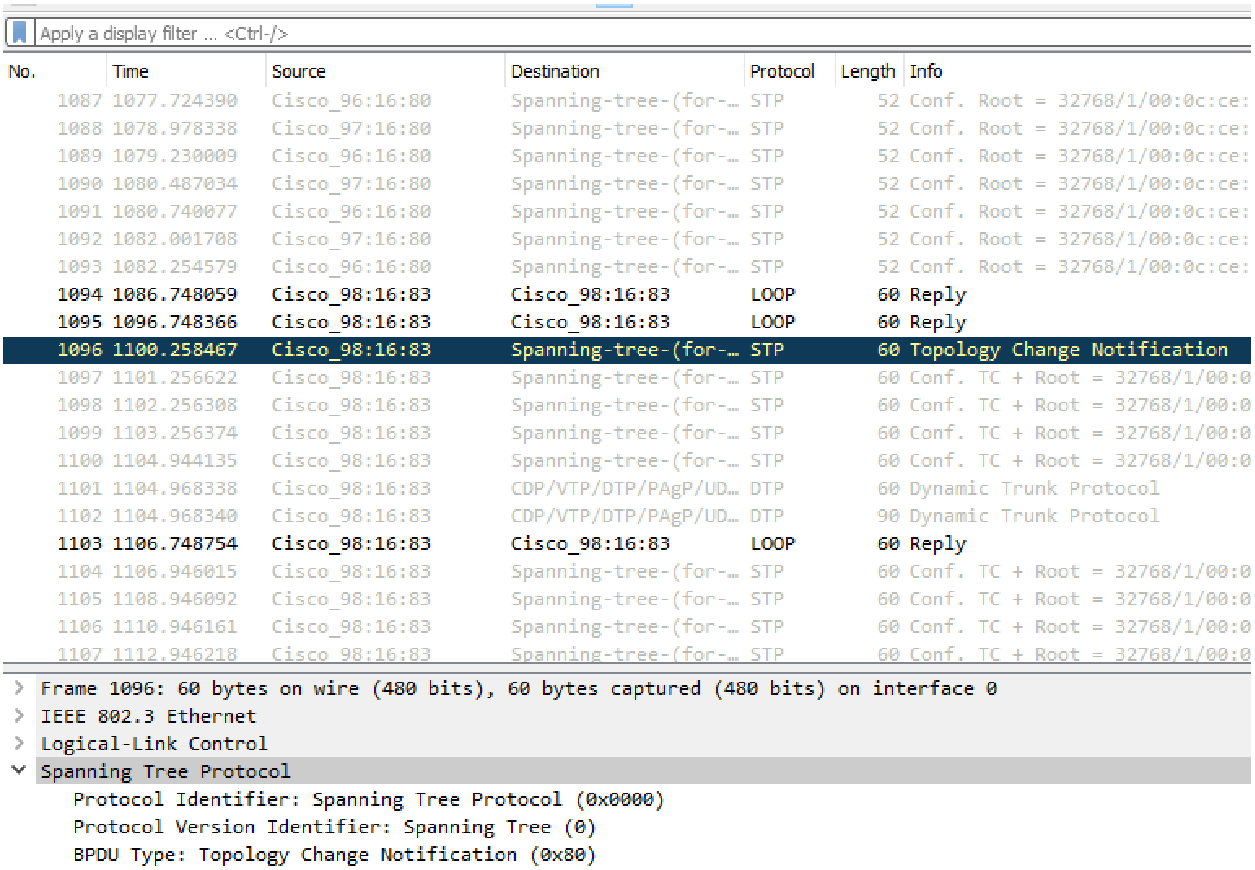
```
0x0000:   0180 c200 0000 000c ce98 1683 0026 4242   .............&BB
0x0010:   0300 0000 0000 8001 000c ce0f 3200 0000   ............2...
```


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source           Destination          Protocol Length Info
   1 0.000000   Cisco_98:16:83   Cisco_98:16:83       LOOP       60 Reply
   2 0.296471   Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
   3 2.296657   Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
   4 4.296617   Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
   5 6.296795   Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
   6 8.296774   Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
   7 10.000339  Cisco_98:16:83   Cisco_98:16:83       LOOP       60 Reply
   8 10.296854  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
   9 12.296983  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
  10 14.296982  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
  11 16.297166  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
  12 18.220430  Cisco_98:16:83   CDP/VTP/DTP/PAgP/UD… DTP        60 Dynamic Trunk Protocol
  13 18.220431  Cisco_98:16:83   CDP/VTP/DTP/PAgP/UD… DTP        90 Dynamic Trunk Protocol
  14 18.297255  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
  15 20.000709  Cisco_98:16:83   Cisco_98:16:83       LOOP       60 Reply
  16 20.297269  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
  17 22.297415  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
  18 24.297545  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
  19 26.297594  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
  20 27.221018  Cisco_98:16:83   CDP/VTP/DTP/PAgP/UD… CDP       411 Device ID: Switch  Port ID: FastEthernet0/3
  21 28.297621  Cisco_98:16:83   Spanning-tree-(for-… STP        60 Conf. Root = 32768/1/00:0c:ce:0f:32:00  Cost = 19  Port = 0x8003
```

```
> Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> IEEE 802.3 Ethernet
> Logical-Link Control
v Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Spanning Tree (0)
    BPDU Type: Configuration (0x00)
  v BPDU flags: 0x00
      0... .... = Topology Change Acknowledgment: No
      .... ...0 = Topology Change: No
  > Root Identifier: 32768 / 1 / 00:0c:ce:0f:32:00
    Root Path Cost: 19
  > Bridge Identifier: 32768 / 1 / 00:0c:ce:98:16:80
    Port identifier: 0x8003
    Message Age: 1
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
```

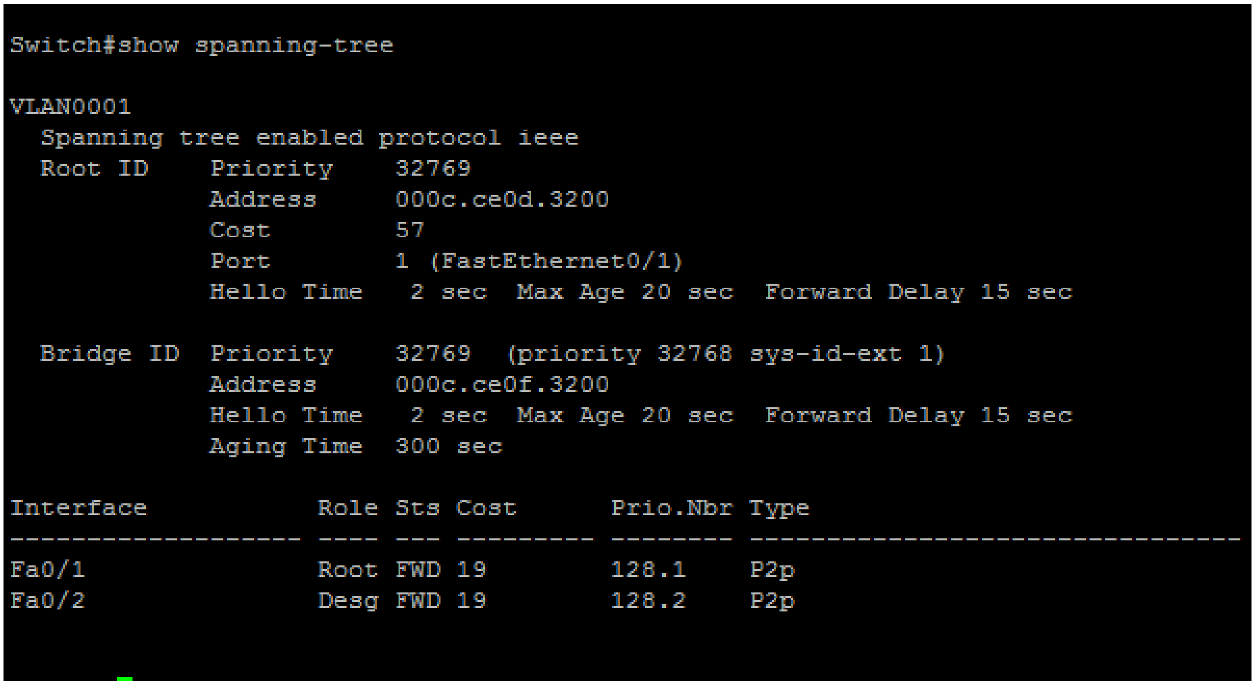
Capturing topology change notification



No.	Time	Source	Destination	Protocol	Length	Info
1087	1077.724390	Cisco_96:16:80	Spanning-tree-(for-…	STP	52	Conf. Root = 32768/1/00:0c:ce:
1088	1078.978338	Cisco_97:16:80	Spanning-tree-(for-…	STP	52	Conf. Root = 32768/1/00:0c:ce:
1089	1079.230009	Cisco_96:16:80	Spanning-tree-(for-…	STP	52	Conf. Root = 32768/1/00:0c:ce:
1090	1080.487034	Cisco_97:16:80	Spanning-tree-(for-…	STP	52	Conf. Root = 32768/1/00:0c:ce:
1091	1080.740077	Cisco_96:16:80	Spanning-tree-(for-…	STP	52	Conf. Root = 32768/1/00:0c:ce:
1092	1082.001708	Cisco_97:16:80	Spanning-tree-(for-…	STP	52	Conf. Root = 32768/1/00:0c:ce:
1093	1082.254579	Cisco_96:16:80	Spanning-tree-(for-…	STP	52	Conf. Root = 32768/1/00:0c:ce:
1094	1086.748059	Cisco_98:16:83	Cisco_98:16:83	LOOP	60	Reply
1095	1096.748366	Cisco_98:16:83	Cisco_98:16:83	LOOP	60	Reply
1096	1100.258467	Cisco_98:16:83	Spanning-tree-(for-…	STP	60	Topology Change Notification
1097	1101.256622	Cisco_98:16:83	Spanning-tree-(for-…	STP	60	Conf. TC + Root = 32768/1/00:0
1098	1102.256308	Cisco_98:16:83	Spanning-tree-(for-…	STP	60	Conf. TC + Root = 32768/1/00:0
1099	1103.256374	Cisco_98:16:83	Spanning-tree-(for-…	STP	60	Conf. TC + Root = 32768/1/00:0
1100	1104.944135	Cisco_98:16:83	Spanning-tree-(for-…	STP	60	Conf. TC + Root = 32768/1/00:0
1101	1104.968338	Cisco_98:16:83	CDP/VTP/DTP/PAgP/UD…	DTP	60	Dynamic Trunk Protocol
1102	1104.968340	Cisco_98:16:83	CDP/VTP/DTP/PAgP/UD…	DTP	90	Dynamic Trunk Protocol
1103	1106.748754	Cisco_98:16:83	Cisco_98:16:83	LOOP	60	Reply
1104	1106.946015	Cisco_98:16:83	Spanning-tree-(for-…	STP	60	Conf. TC + Root = 32768/1/00:0
1105	1108.946092	Cisco_98:16:83	Spanning-tree-(for-…	STP	60	Conf. TC + Root = 32768/1/00:0
1106	1110.946161	Cisco_98:16:83	Spanning-tree-(for-…	STP	60	Conf. TC + Root = 32768/1/00:0
1107	1112.946218	Cisco_98:16:83	Spanning-tree-(for-…	STP	60	Conf. TC + Root = 32768/1/00:0

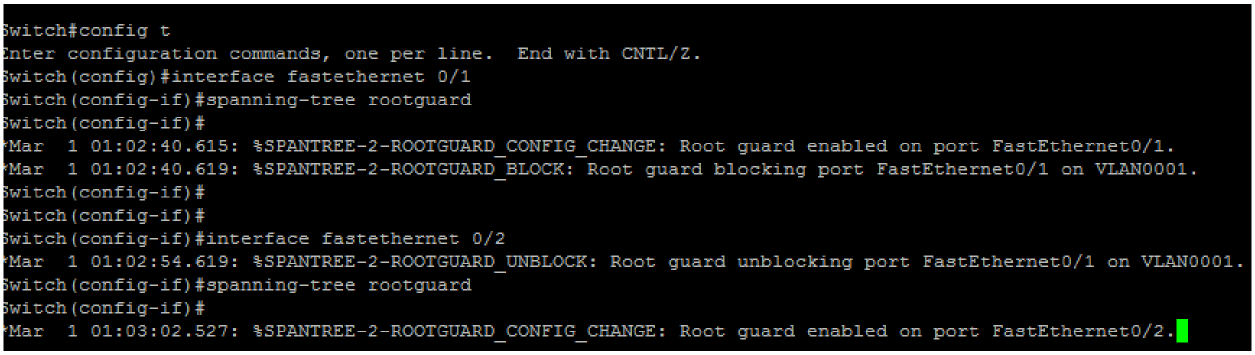
```
> Frame 1096: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> IEEE 802.3 Ethernet
> Logical-Link Control
v Spanning Tree Protocol
     Protocol Identifier: Spanning Tree Protocol (0x0000)
     Protocol Version Identifier: Spanning Tree (0)
     BPDU Type: Topology Change Notification (0x80)
```

After the attack we notice that the switch F is not a root anymore



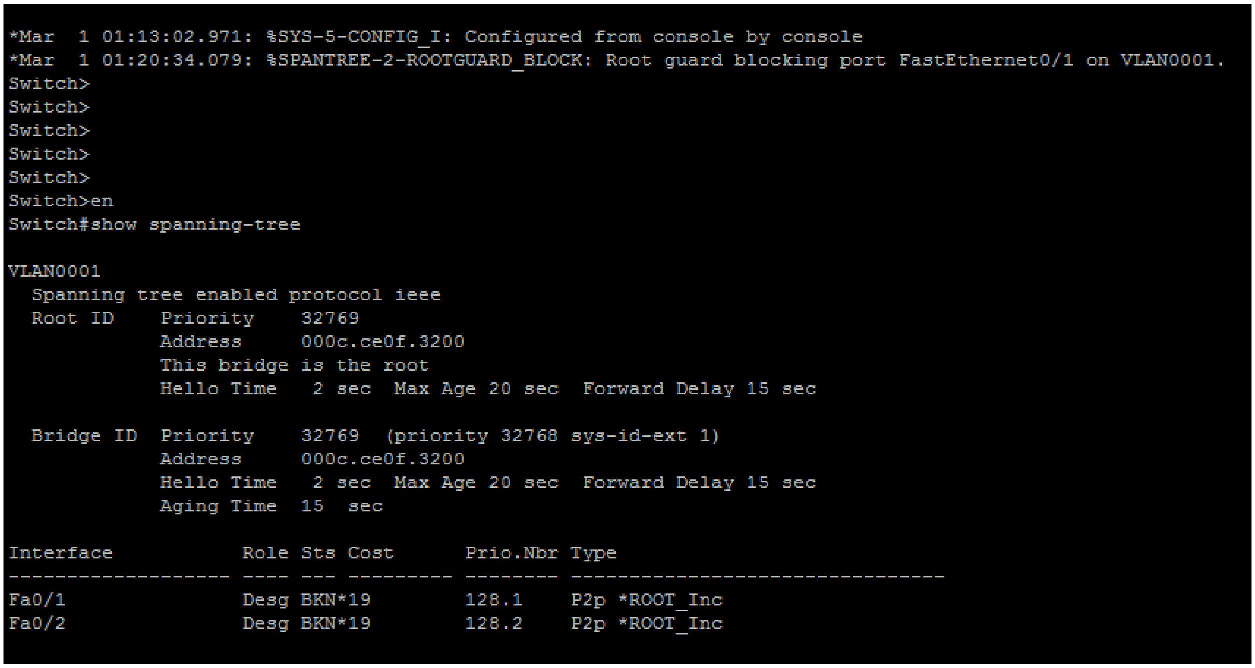
```
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce0d.3200
             Cost        57
             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.ce0f.3200
             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
```

Performing mitigation



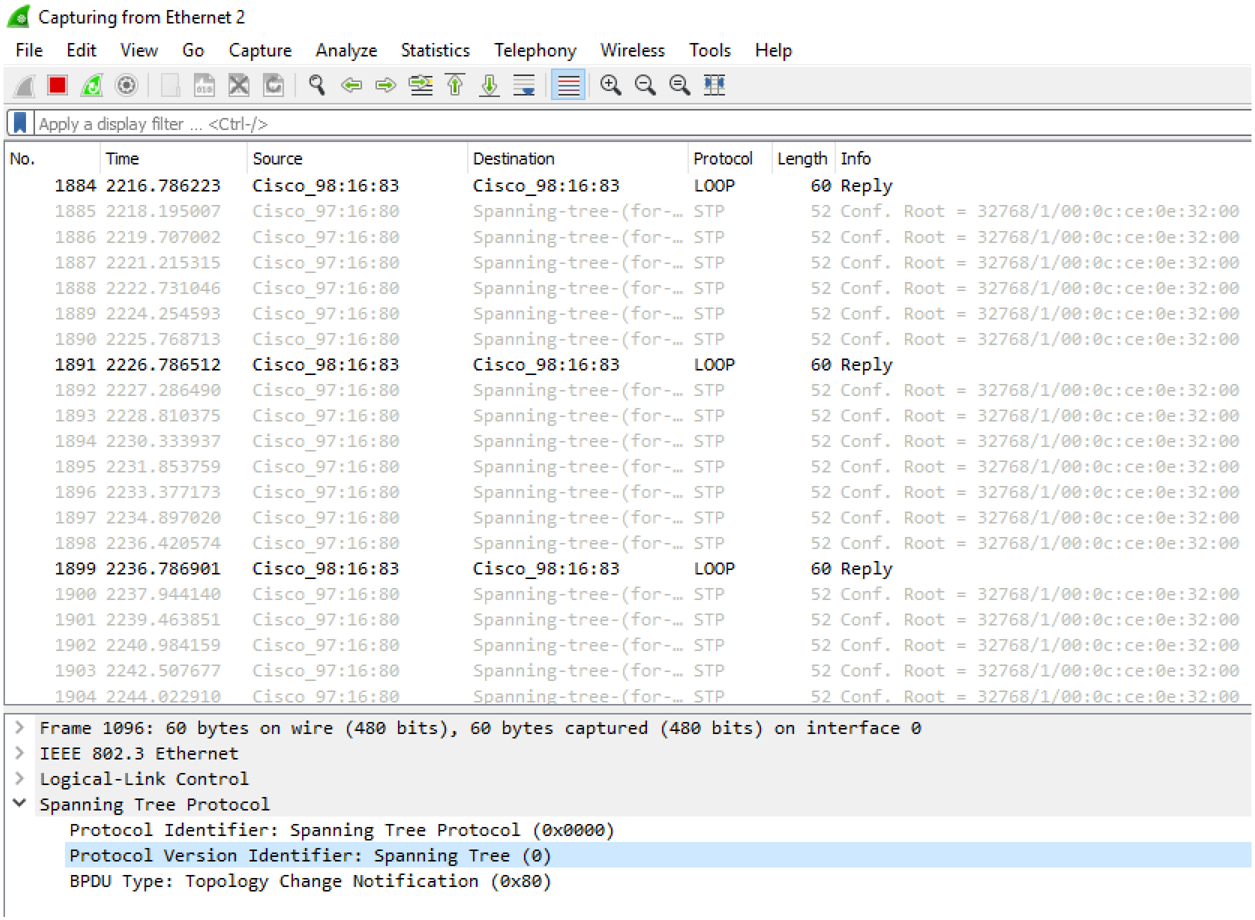
```
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#spanning-tree rootguard
Switch(config-if)#
*Mar  1 01:02:40.615: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port FastEthernet0/1.
*Mar  1 01:02:40.619: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/1 on VLAN0001.
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#interface fastethernet 0/2
*Mar  1 01:02:54.619: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/1 on VLAN0001.
Switch(config-if)#spanning-tree rootguard
Switch(config-if)#
*Mar  1 01:03:02.527: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port FastEthernet0/2.
```

After mitigation we perform the root again and we notic that the switch f still the root



```
*Mar  1 01:13:02.971: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 01:20:34.079: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/1 on VLAN0001.
Switch>
Switch>
Switch>
Switch>
Switch>
Switch>en
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce0f.3200
             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.ce0f.3200
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Desg BKN*19        128.1    P2p *ROOT_Inc
Fa0/2               Desg BKN*19        128.2    P2p *ROOT_Inc
```

Analyzing the traffic after the mitigation using wireshark


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time         Source          Destination            Protocol  Length Info
 1884 2216.786223  Cisco_98:16:83  Cisco_98:16:83         LOOP        60 Reply
 1885 2218.195007  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1886 2219.707002  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1887 2221.215315  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1888 2222.731046  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1889 2224.254593  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1890 2225.768713  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1891 2226.786512  Cisco_98:16:83  Cisco_98:16:83         LOOP        60 Reply
 1892 2227.286490  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1893 2228.810375  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1894 2230.333937  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1895 2231.853759  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1896 2233.377173  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1897 2234.897020  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1898 2236.420574  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1899 2236.786901  Cisco_98:16:83  Cisco_98:16:83         LOOP        60 Reply
 1900 2237.944140  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1901 2239.463851  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1902 2240.984159  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1903 2242.507677  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
 1904 2244.022910  Cisco_97:16:80  Spanning-tree-(for-…   STP         52 Conf. Root = 32768/1/00:0c:ce:0e:32:00
```

```
> Frame 1096: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> IEEE 802.3 Ethernet
> Logical-Link Control
v Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Spanning Tree (0)
    BPDU Type: Topology Change Notification (0x80)
```

BPDU Guard

The concept behind the BPDU Guard is basically preventing access port from sending BPDU. It's essential that switch not allow user to connect another switch to the network. So enabling BPDU port in the edge port is a significant security step we should always consider. In case the switch received a BPDU for an edge port that means that the user try to connect a switch to the network when it is not supposed to do that. Thus, the PBDU guard disable that port and put it in ERR-disable mode. It will also protect the spanning tree topology and limit and manipulation by an end station device that is likely an attacker try to get into the network. There are two ways to enable PBDU guard in the switch either globally using one command to enable it in all switch ports, or by writing one command per port.

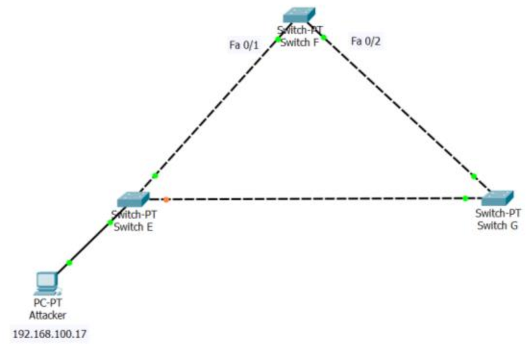
Switch(config)# **spanning-tree portfast bpduguard default**

Switch(config-if)# [**no**] **spanning-tree bpduguard enable**

After enabling the BPDU guard, if the switch port received a BPDU from an end station device, the port go to err-disable state. In order to make the port work again we have to options either by do shut/ no shut or we can specific time after and it set to enable mode automatically.

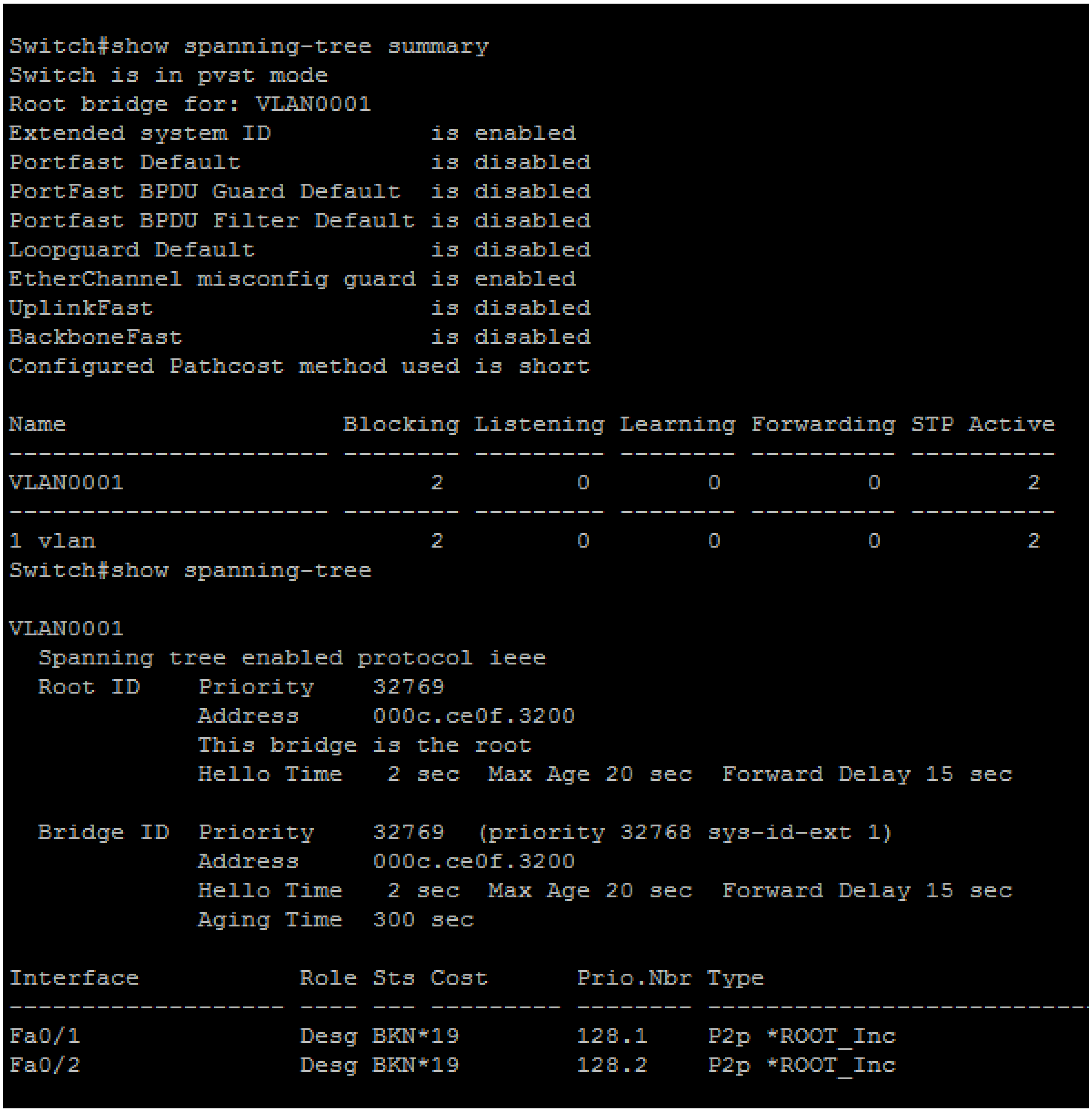
Topology:

We use the same topology as the previous one root guard



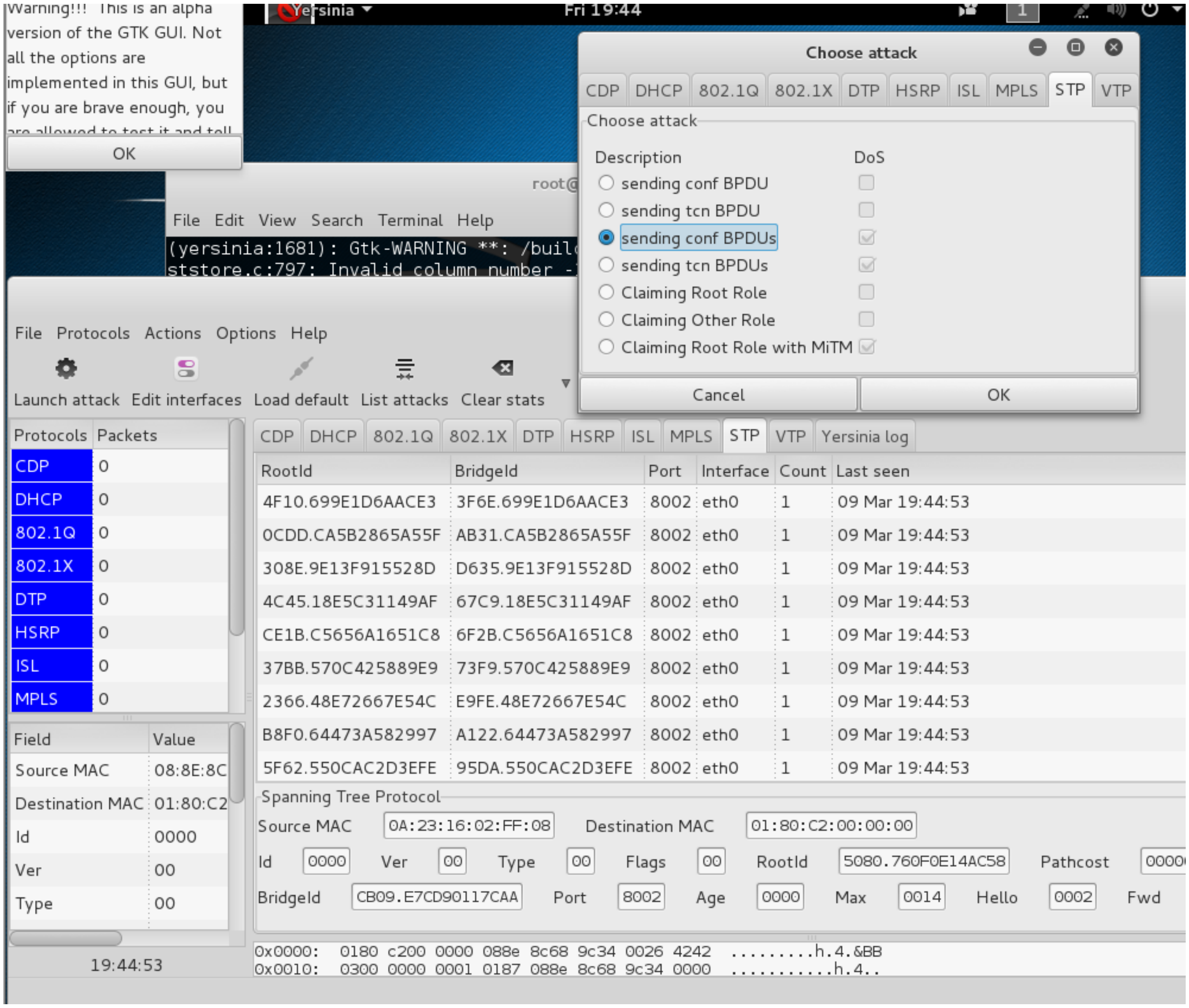
implementation:

starting configuration



```
Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      2         0        0          0          2
---------------------- -------- --------- -------- ---------- ----------
1 vlan                        2         0        0          0          2
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce0f.3200
             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.ce0f.3200
             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 BKN*19        128.1    P2p *ROOT_Inc
Fa0/2               Desg BKN*19        128.2    P2p *ROOT_Inc
```

Attacking using Yersinia


Warning!!! This is an alpha version of the GTK GUI. Not all the options are implemented in this GUI, but if you are brave enough, you are allowed to test it and tell
OK
Yersinia
Fri 19:44
root@
File Edit View Search Terminal Help
File Protocols Actions Options Help
Launch attack
Edit interfaces
Load default
List attacks
Clear stats
Choose attack
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP
Cancel
OK
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log
19:44:53

```
(yersinia:1681): Gtk-WARNING **: /buil
ststore.c:797: Invalid column number -
```

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	☑

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

Field	Value
Source MAC	08:8E:8C
Destination MAC	01:80:C2
Id	0000
Ver	00
Type	00

RootId	BridgeId	Port	Interface	Count	Last seen
4F10.699E1D6AACE3	3F6E.699E1D6AACE3	8002	eth0	1	09 Mar 19:44:53
0CDD.CA5B2865A55F	AB31.CA5B2865A55F	8002	eth0	1	09 Mar 19:44:53
308E.9E13F915528D	D635.9E13F915528D	8002	eth0	1	09 Mar 19:44:53
4C45.18E5C31149AF	67C9.18E5C31149AF	8002	eth0	1	09 Mar 19:44:53
CE1B.C5656A1651C8	6F2B.C5656A1651C8	8002	eth0	1	09 Mar 19:44:53
37BB.570C425889E9	73F9.570C425889E9	8002	eth0	1	09 Mar 19:44:53
2366.48E72667E54C	E9FE.48E72667E54C	8002	eth0	1	09 Mar 19:44:53
B8F0.64473A582997	A122.64473A582997	8002	eth0	1	09 Mar 19:44:53
5F62.550CAC2D3EFE	95DA.550CAC2D3EFE	8002	eth0	1	09 Mar 19:44:53

Spanning Tree Protocol

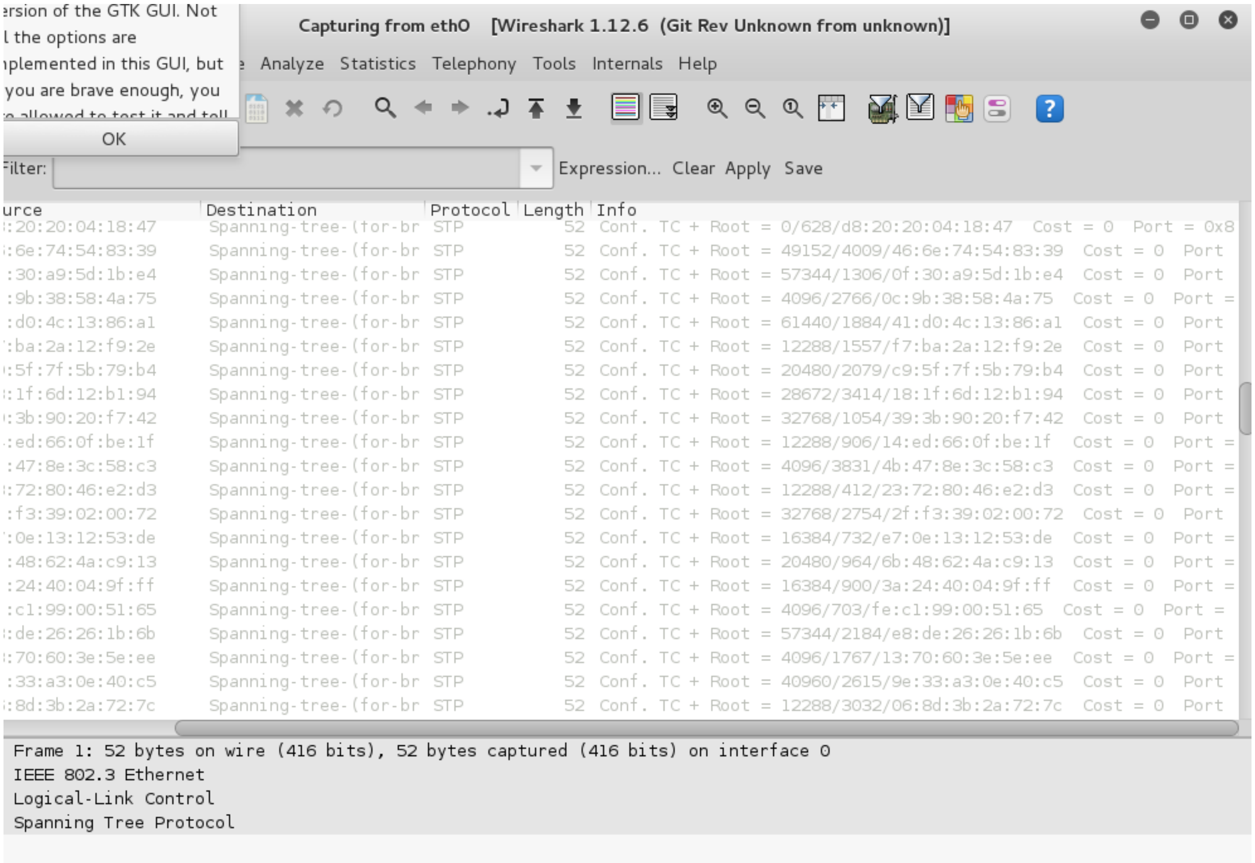
Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00

Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 0000

BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd

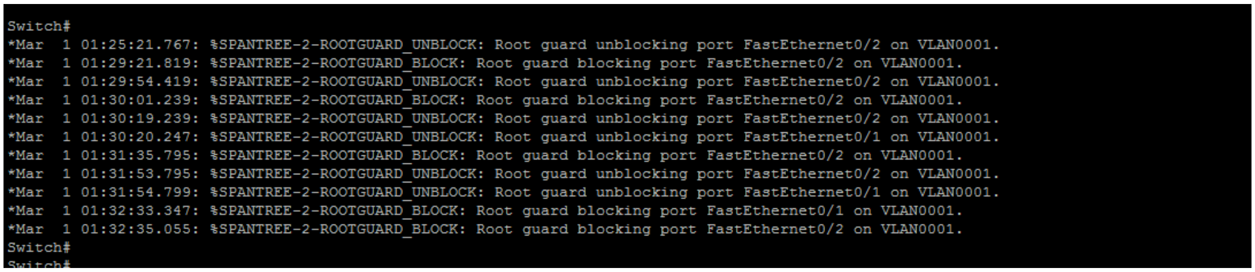
```
0x0000:   0180 c200 0000 088e 8c68 9c34 0026 4242   .........h.4.&BB
0x0010:   0300 0000 0001 0187 088e 8c68 9c34 0000   ...........h.4..
```

Analysis traffic


ersion of the GTK GUI. Not
l the options are
nplemented in this GUI, but
you are brave enough, you
e allowed to test it and tell
OK
Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
e Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

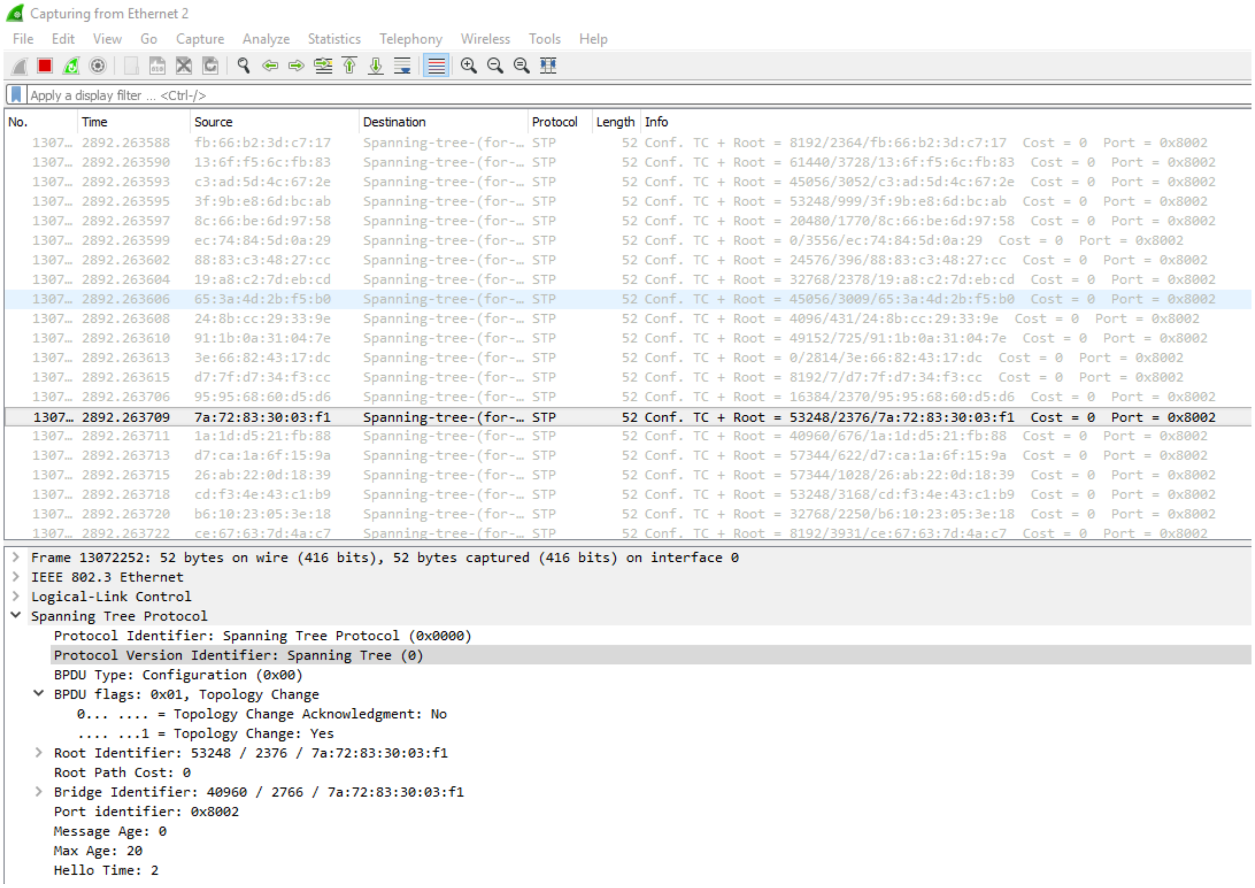
urce	Destination	Protocol	Length	Info
:20:20:04:18:47	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 0/628/d8:20:20:04:18:47 Cost = 0 Port = 0x8
:6e:74:54:83:39	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 49152/4009/46:6e:74:54:83:39 Cost = 0 Port
:30:a9:5d:1b:e4	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 57344/1306/0f:30:a9:5d:1b:e4 Cost = 0 Port
:9b:38:58:4a:75	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 4096/2766/0c:9b:38:58:4a:75 Cost = 0 Port =
:d0:4c:13:86:a1	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 61440/1884/41:d0:4c:13:86:a1 Cost = 0 Port
:ba:2a:12:f9:2e	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 12288/1557/f7:ba:2a:12:f9:2e Cost = 0 Port
:5f:7f:5b:79:b4	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 20480/2079/c9:5f:7f:5b:79:b4 Cost = 0 Port
:1f:6d:12:b1:94	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 28672/3414/18:1f:6d:12:b1:94 Cost = 0 Port
:3b:90:20:f7:42	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 32768/1054/39:3b:90:20:f7:42 Cost = 0 Port
:ed:66:0f:be:1f	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 12288/906/14:ed:66:0f:be:1f Cost = 0 Port =
:47:8e:3c:58:c3	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 4096/3831/4b:47:8e:3c:58:c3 Cost = 0 Port =
:72:80:46:e2:d3	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 12288/412/23:72:80:46:e2:d3 Cost = 0 Port =
:f3:39:02:00:72	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 32768/2754/2f:f3:39:02:00:72 Cost = 0 Port
:0e:13:12:53:de	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 16384/732/e7:0e:13:12:53:de Cost = 0 Port =
:48:62:4a:c9:13	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 20480/964/6b:48:62:4a:c9:13 Cost = 0 Port =
:24:40:04:9f:ff	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 16384/900/3a:24:40:04:9f:ff Cost = 0 Port =
:c1:99:00:51:65	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 4096/703/fe:c1:99:00:51:65 Cost = 0 Port =
:de:26:26:1b:6b	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 57344/2184/e8:de:26:26:1b:6b Cost = 0 Port
:70:60:3e:5e:ee	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 4096/1767/13:70:60:3e:5e:ee Cost = 0 Port =
:33:a3:0e:40:c5	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 40960/2615/9e:33:a3:0e:40:c5 Cost = 0 Port
:8d:3b:2a:72:7c	Spanning-tree-(for-br	STP	52	Conf. TC + Root = 12288/3032/06:8d:3b:2a:72:7c Cost = 0 Port

```
Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface 0
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol
```



```
Switch#
*Mar  1 01:25:21.767: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:29:21.819: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:29:54.419: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:30:01.239: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:30:19.239: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:30:20.247: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/1 on VLAN0001.
*Mar  1 01:31:35.795: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:31:53.795: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:31:54.799: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/1 on VLAN0001.
*Mar  1 01:32:33.347: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/1 on VLAN0001.
*Mar  1 01:32:35.055: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
Switch#
Switch#
```

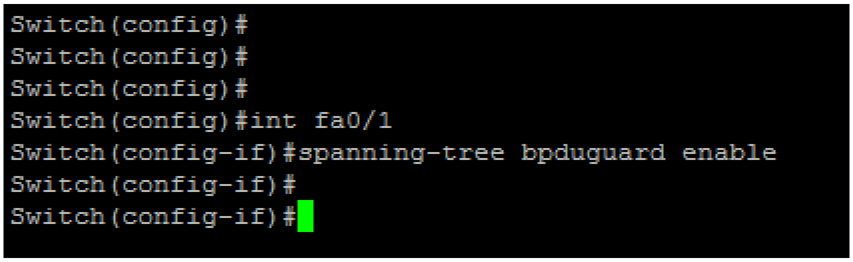
After the attck


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

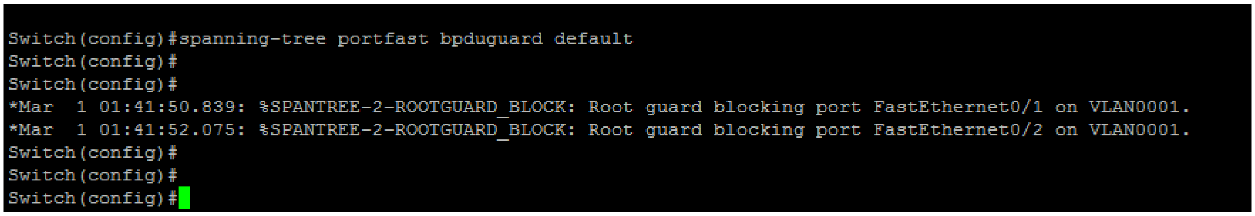
```
No.      Time          Source             Destination             Protocol  Length Info
 1307…   2892.263588   fb:66:b2:3d:c7:17  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 8192/2364/fb:66:b2:3d:c7:17  Cost = 0  Port = 0x8002
 1307…   2892.263590   13:6f:f5:6c:fb:83  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 61440/3728/13:6f:f5:6c:fb:83  Cost = 0  Port = 0x8002
 1307…   2892.263593   c3:ad:5d:4c:67:2e  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 45056/3052/c3:ad:5d:4c:67:2e  Cost = 0  Port = 0x8002
 1307…   2892.263595   3f:9b:e8:6d:bc:ab  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 53248/999/3f:9b:e8:6d:bc:ab  Cost = 0  Port = 0x8002
 1307…   2892.263597   8c:66:be:6d:97:58  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 20480/1770/8c:66:be:6d:97:58  Cost = 0  Port = 0x8002
 1307…   2892.263599   ec:74:84:5d:0a:29  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 0/3556/ec:74:84:5d:0a:29  Cost = 0  Port = 0x8002
 1307…   2892.263602   88:83:c3:48:27:cc  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 24576/396/88:83:c3:48:27:cc  Cost = 0  Port = 0x8002
 1307…   2892.263604   19:a8:c2:7d:eb:cd  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 32768/2378/19:a8:c2:7d:eb:cd  Cost = 0  Port = 0x8002
 1307…   2892.263606   65:3a:4d:2b:f5:b0  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 45056/3009/65:3a:4d:2b:f5:b0  Cost = 0  Port = 0x8002
 1307…   2892.263608   24:8b:cc:29:33:9e  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 4096/431/24:8b:cc:29:33:9e  Cost = 0  Port = 0x8002
 1307…   2892.263610   91:1b:0a:31:04:7e  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 49152/725/91:1b:0a:31:04:7e  Cost = 0  Port = 0x8002
 1307…   2892.263613   3e:66:82:43:17:dc  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 0/2814/3e:66:82:43:17:dc  Cost = 0  Port = 0x8002
 1307…   2892.263615   d7:7f:d7:34:f3:cc  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 8192/7/d7:7f:d7:34:f3:cc  Cost = 0  Port = 0x8002
 1307…   2892.263706   95:95:68:60:d5:d6  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 16384/2370/95:95:68:60:d5:d6  Cost = 0  Port = 0x8002
 1307…   2892.263709   7a:72:83:30:03:f1  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 53248/2376/7a:72:83:30:03:f1  Cost = 0  Port = 0x8002
 1307…   2892.263711   1a:1d:d5:21:fb:88  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 40960/676/1a:1d:d5:21:fb:88  Cost = 0  Port = 0x8002
 1307…   2892.263713   d7:ca:1a:6f:15:9a  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 57344/622/d7:ca:1a:6f:15:9a  Cost = 0  Port = 0x8002
 1307…   2892.263715   26:ab:22:0d:18:39  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 57344/1028/26:ab:22:0d:18:39  Cost = 0  Port = 0x8002
 1307…   2892.263718   cd:f3:4e:43:c1:b9  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 53248/3168/cd:f3:4e:43:c1:b9  Cost = 0  Port = 0x8002
 1307…   2892.263720   b6:10:23:05:3e:18  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 32768/2250/b6:10:23:05:3e:18  Cost = 0  Port = 0x8002
 1307…   2892.263722   ce:67:63:7d:4a:c7  Spanning-tree-(for-…    STP       52 Conf. TC + Root = 8192/3931/ce:67:63:7d:4a:c7  Cost = 0  Port = 0x8002
```

```
> Frame 13072252: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface 0
> IEEE 802.3 Ethernet
> Logical-Link Control
v Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Spanning Tree (0)
    BPDU Type: Configuration (0x00)
  v BPDU flags: 0x01, Topology Change
      0... .... = Topology Change Acknowledgment: No
      .... ...1 = Topology Change: Yes
  > Root Identifier: 53248 / 2376 / 7a:72:83:30:03:f1
    Root Path Cost: 0
  > Bridge Identifier: 40960 / 2766 / 7a:72:83:30:03:f1
    Port identifier: 0x8002
    Message Age: 0
    Max Age: 20
    Hello Time: 2
```

We perform two types of mitigation one in general for all ports by default and the other for specific port

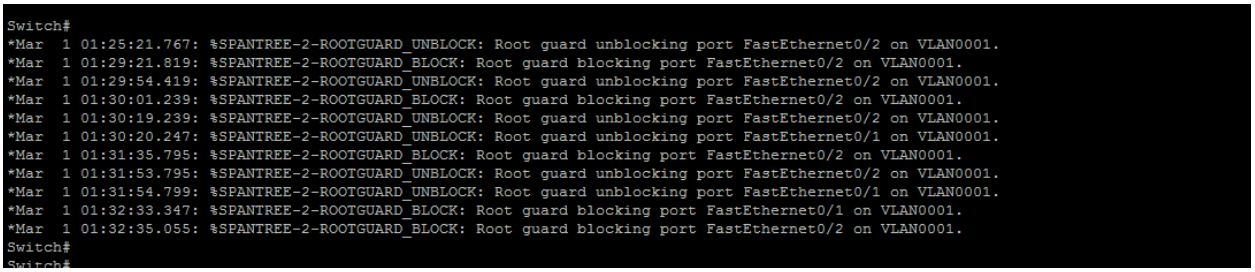


```
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#int fa0/1
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#
Switch(config-if)#
```

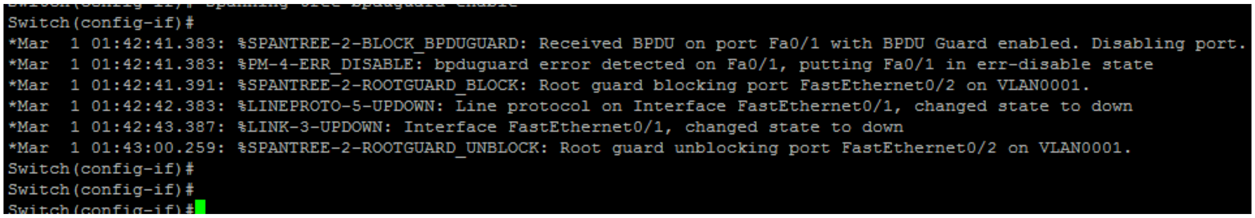


```
Switch(config)#spanning-tree portfast bpduguard default
Switch(config)#
Switch(config)#
*Mar  1 01:41:50.839: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/1 on VLAN0001.
*Mar  1 01:41:52.075: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
Switch(config)#
Switch(config)#
Switch(config)#
```

While the attack

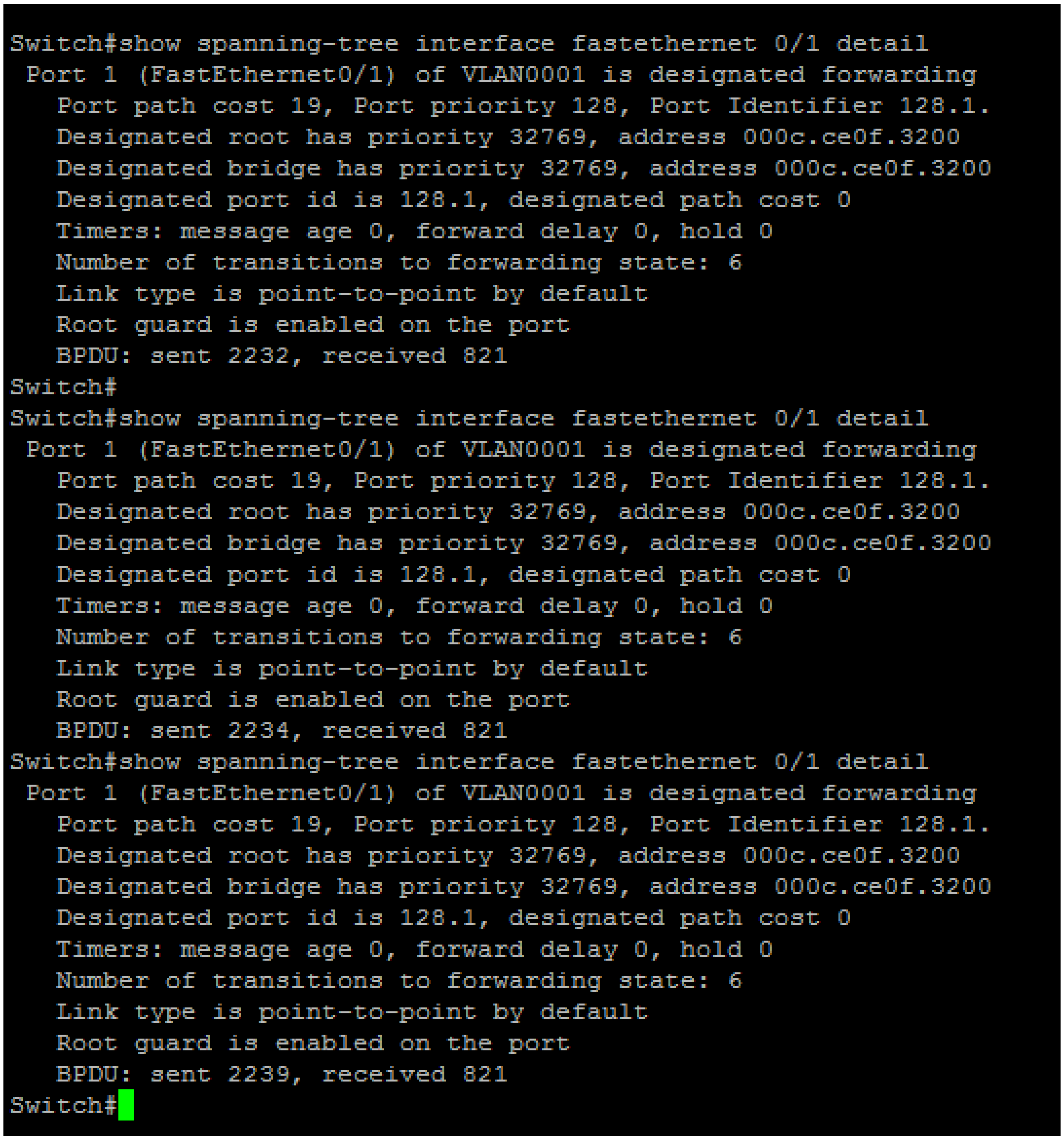


```
Switch#
*Mar  1 01:25:21.767: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:29:21.819: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:29:54.419: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:30:01.239: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:30:19.239: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:30:20.247: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/1 on VLAN0001.
*Mar  1 01:31:35.795: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:31:53.795: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:31:54.799: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/1 on VLAN0001.
*Mar  1 01:32:33.347: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/1 on VLAN0001.
*Mar  1 01:32:35.055: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
Switch#
Switch#
```



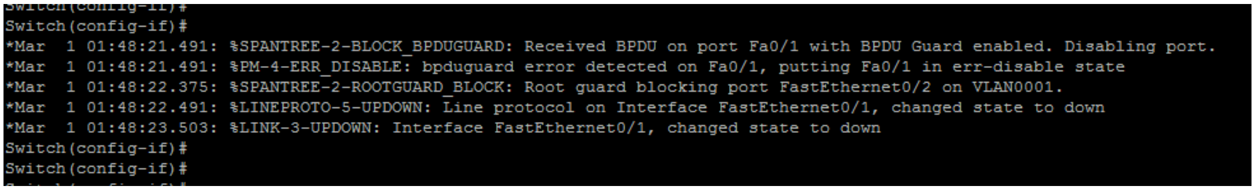
```
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)#
*Mar  1 01:42:41.383: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa0/1 with BPDU Guard enabled. Disabling port.
*Mar  1 01:42:41.383: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/1, putting Fa0/1 in err-disable state
*Mar  1 01:42:41.391: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:42:42.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  1 01:42:43.387: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
*Mar  1 01:43:00.259: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port FastEthernet0/2 on VLAN0001.
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
```

We notice after the attack the number or recived bpdu increased



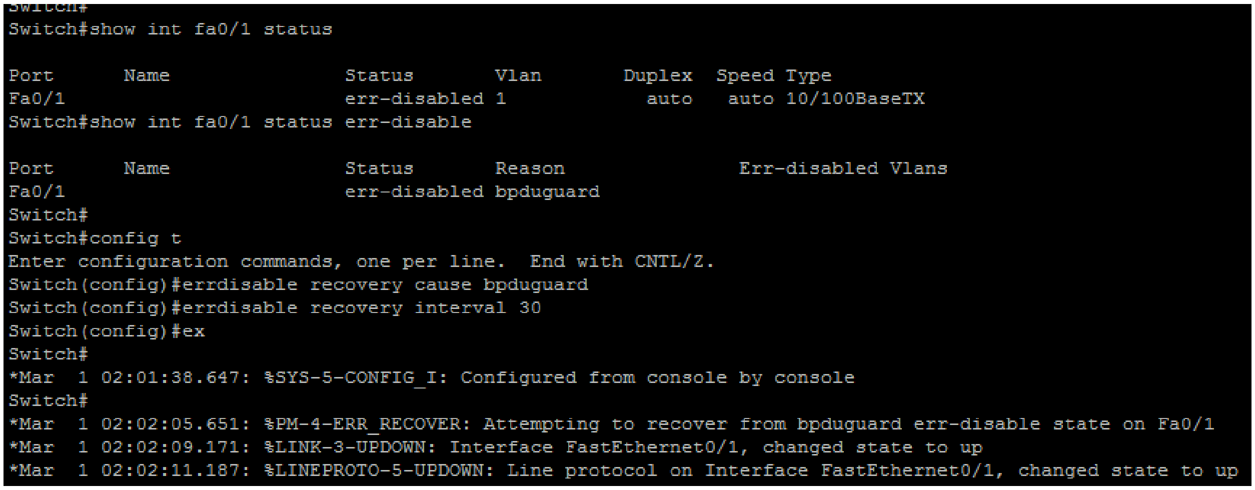
```
Switch#show spanning-tree interface fastethernet 0/1 detail
 Port 1 (FastEthernet0/1) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.1.
   Designated root has priority 32769, address 000c.ce0f.3200
   Designated bridge has priority 32769, address 000c.ce0f.3200
   Designated port id is 128.1, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 6
   Link type is point-to-point by default
   Root guard is enabled on the port
   BPDU: sent 2232, received 821
Switch#
Switch#show spanning-tree interface fastethernet 0/1 detail
 Port 1 (FastEthernet0/1) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.1.
   Designated root has priority 32769, address 000c.ce0f.3200
   Designated bridge has priority 32769, address 000c.ce0f.3200
   Designated port id is 128.1, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 6
   Link type is point-to-point by default
   Root guard is enabled on the port
   BPDU: sent 2234, received 821
Switch#show spanning-tree interface fastethernet 0/1 detail
 Port 1 (FastEthernet0/1) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.1.
   Designated root has priority 32769, address 000c.ce0f.3200
   Designated bridge has priority 32769, address 000c.ce0f.3200
   Designated port id is 128.1, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 6
   Link type is point-to-point by default
   Root guard is enabled on the port
   BPDU: sent 2239, received 821
Switch#
```

Attacking after mitigation will disable the port



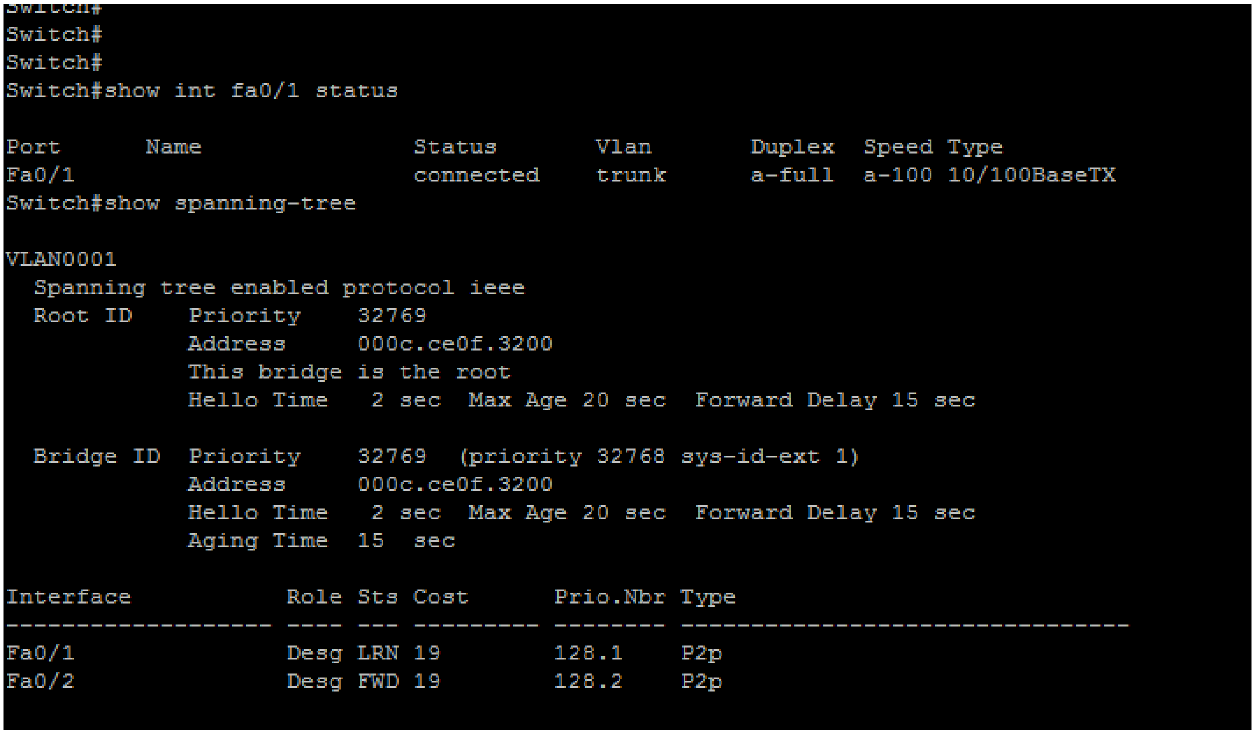
```
Switch(config-if)#
Switch(config-if)#
*Mar  1 01:48:21.491: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Fa0/1 with BPDU Guard enabled. Disabling port.
*Mar  1 01:48:21.491: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/1, putting Fa0/1 in err-disable state
*Mar  1 01:48:22.375: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/2 on VLAN0001.
*Mar  1 01:48:22.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  1 01:48:23.503: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
Switch(config-if)#
Switch(config-if)#
```

To recover after see the reason off rerr-disable is bpduguard

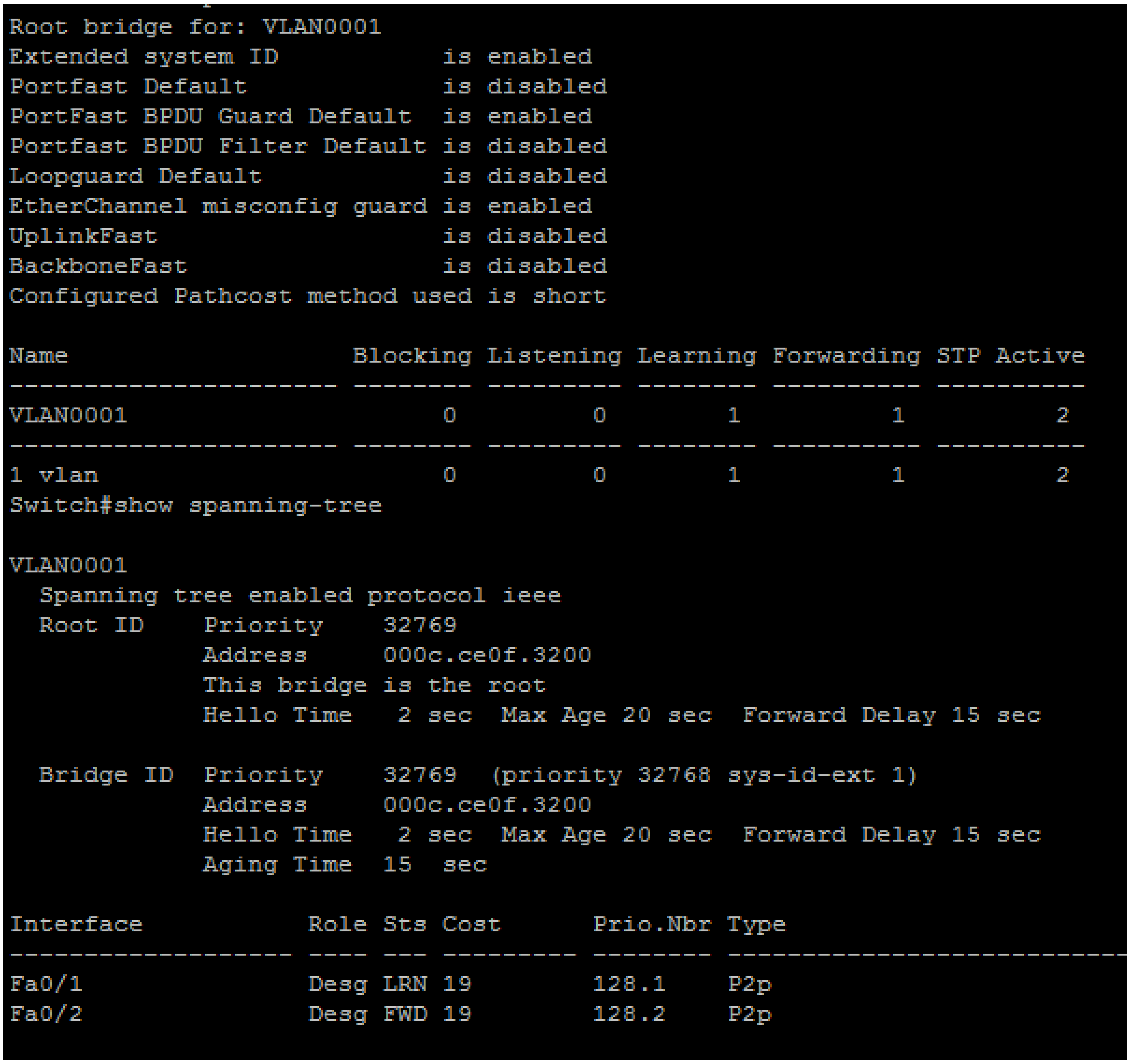


```
Switch#
Switch#show int fa0/1 status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        err-disabled 1            auto   auto 10/100BaseTX
Switch#show int fa0/1 status err-disable

Port      Name               Status       Reason               Err-disabled Vlans
Fa0/1                        err-disabled bpduguard
Switch#
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#errdisable recovery cause bpduguard
Switch(config)#errdisable recovery interval 30
Switch(config)#ex
Switch#
*Mar  1 02:01:38.647: %SYS-5-CONFIG_I: Configured from console by console
Switch#
*Mar  1 02:02:05.651: %PM-4-ERR_RECOVER: Attempting to recover from bpduguard err-disable state on Fa0/1
*Mar  1 02:02:09.171: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 02:02:11.187: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

And we make sure it is connected again



```
Switch#
Switch#
Switch#
Switch#show int fa0/1 status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    trunk      a-full  a-100 10/100BaseTX
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce0f.3200
             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.ce0f.3200
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

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



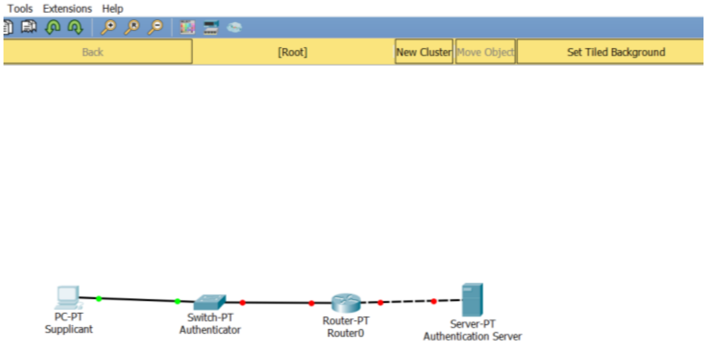
```
Root bridge for: VLAN0001
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        1          1          2
---------------------- -------- --------- -------- ---------- ----------
1 vlan                       0         0        1          1          2
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000c.ce0f.3200
             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.ce0f.3200
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

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

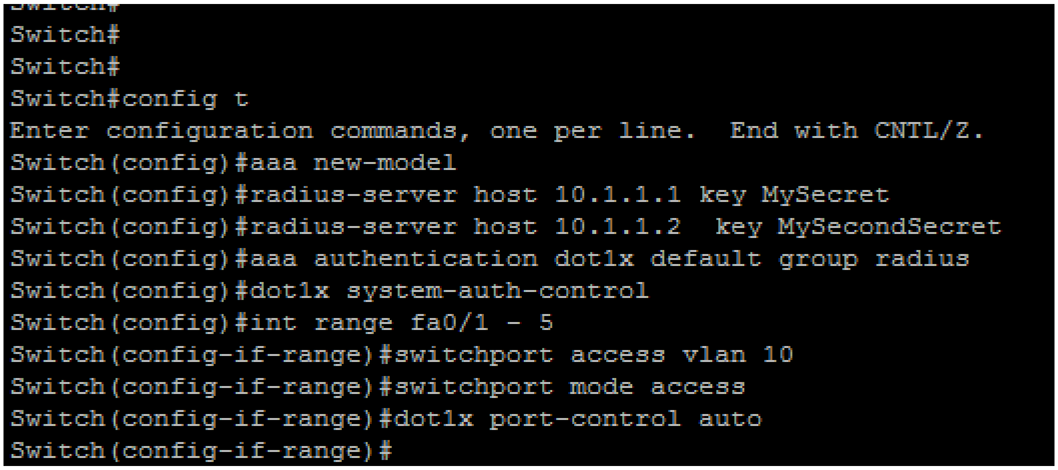
802.1X

Concept:

In previous lab, we studied port security and its great benefit of protecting the network from any intrusion or suspicious connection. However, port security might be a great tool to make sure verified certain machine by its mac address, we need another technique to verify the user behind the machine and make sure we are only allowing access to legitimate users. To verify and authenticate users, we use IEEE 802.1x standard which is combination of port security and AAA

(Authentication, Authorization, Accounting). In the main picture, there are three main party for 802.1x standard first is the supplicant which is the user who want to connect to the network. Then the authenticator which is a switch. The authenticator doesn’t really authenticate the user it just send the user credential to the authentication server where its get checked and then send it back to the switch with a result if the credintal is correct and allowed to access the system or invalid and rejected. There are a necessary setup for the switch and the authentication to be able to perform 802.1x because the supplicant and the switch communicate using Extensive Authentication Protocol over Lan (EAPoL). On the other hand the authenticator and the authentication service communicate using RADIUS -Remote Authentication Dial In User Service- and having the EAPol as a payload inside encrypted by TLS channel. The process step by step is as follow first we enabled AAA then define external server and the authentication method. Next, enable 802.1x with configuring every port that use it.





```
Switch#
Switch#
Switch#
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#aaa new-model
Switch(config)#radius-server host 10.1.1.1 key MySecret
Switch(config)#radius-server host 10.1.1.2  key MySecondSecret
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system-auth-control
Switch(config)#int range fa0/1 - 5
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#dot1x port-control auto
Switch(config-if-range)#
```

Conclusion:

In summary, switch security is significant for protecting data in the network. We have to protect the network from any intrusion like an attacker try to become a root so than he can break the confidentiality of the network and expose all the going through information. Also, performing the bpdu guard is important to make sure that all edge port protected and no attacker try o connect a switch from end station device. Lastly, authentication is a major port of security and IEEE standard 802.1x allow us to verify the user behind the machine and make sure who is who climes to be. Implementing these security feature is crucial to prevent any intrusion.

Reference:

[1] Spanning Tree Protocol Root Guard Enhancement. (2017, June 05). Retrieved March 09, 2018, from https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html

[2] Spanning Tree PortFast BPDU Guard Enhancement. (2017, May 11). Retrieved March 09, 2018, from https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10586-65.html

[3] Catalyst 6500 Release 12.2SX Software Configuration Guide - IEEE 802.1X Port-Based Authentication [Cisco Catalyst 6500 Series Switches]. (2016, July 07). Retrieved March 09, 2018, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html