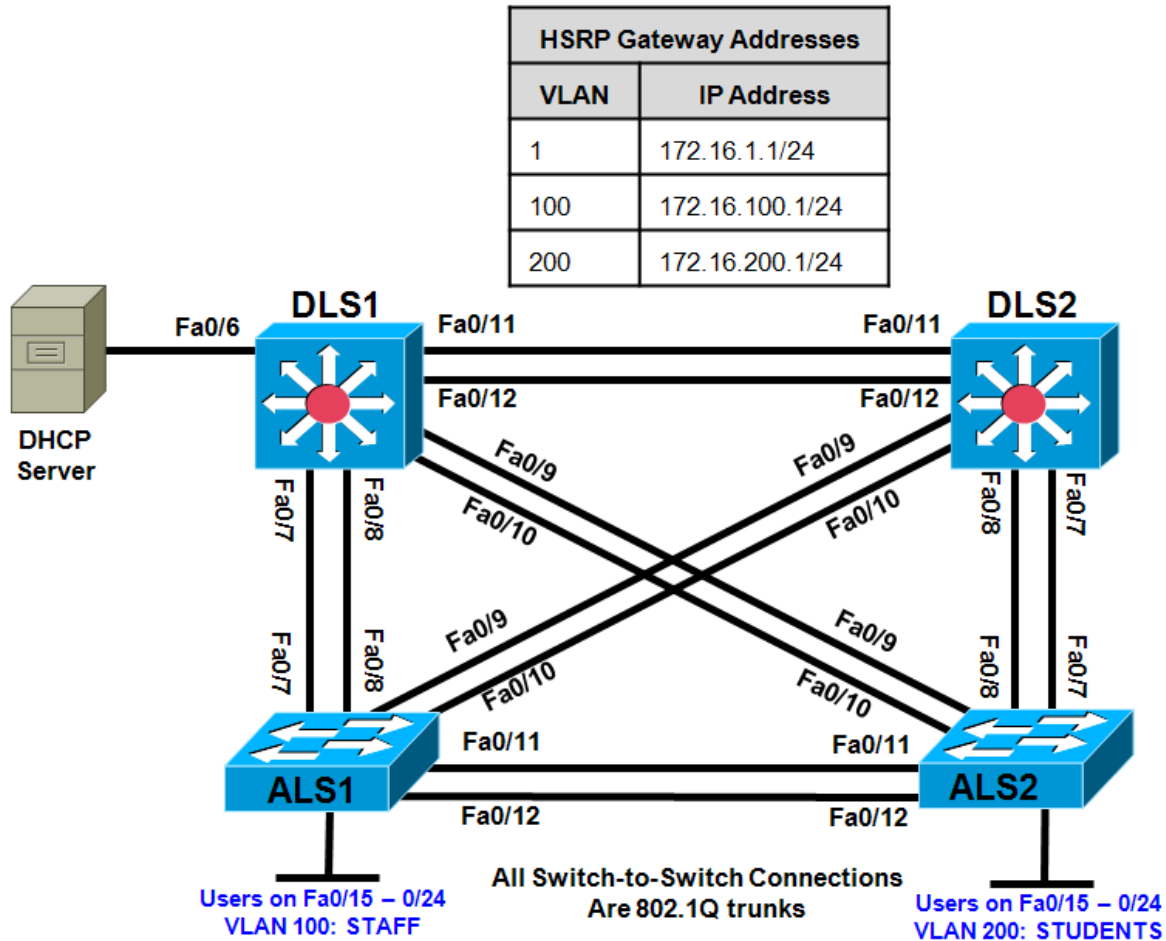


## Chapter 6 Lab 6-2, Securing Spanning Tree Protocol

### Topology



### Objectives

- Secure the Layer 2 spanning-tree topology with BPDU guard.
- Protect the primary and secondary root bridge with root guard.
- Protect switch ports from unidirectional links with UDLD.

### Background

This lab is a continuation of Lab 6-1 and uses the network configuration set up in that lab.

In this lab, you will secure the network against possible spanning-tree disruptions, such as rogue access point additions and the loss of stability to the root bridge by the addition of switches to the network. The improper addition of switches to the network can be either malicious or accidental. In either case, the network can be secured against such a disruption.

**Note:** This lab uses Cisco WS-C2960-24TT-L switches with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin, and Catalyst 3560-24PS switches with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. You can use other switches (such as 2950 or 3550) and Cisco IOS Software versions if they have comparable capabilities and features. Depending on the switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

## Required Resources

- 2 switches (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 12.2(46)SE C3560-ADVIPSERVICESK9-mz image or comparable)
- Ethernet and console cables

**Note:** Be sure to save your final device configurations to use with the next lab.

## Step 1: Load or verify the configurations from Lab 6-1.

- Verify that the configurations from Lab 6-1 are loaded on the devices by issuing the **show vtp status** command. The output should show that the current VTP domain is SWPOD, and VLANs 100 and 200 should be represented in the number of existing VLANs. The output from switch ALS2 is shown as an example. If the switches are not configured properly, erase the startup config, delete the vlan.dat file, and load the configurations saved at the end of lab 6-1.

**Note:** If you are loading the configurations from Lab 6-1, they do not include VLAN and VTP commands. You must first configure ALS1 and ALS2 as VTP clients and then create VLANs 100 (staff) and 200 (student) and the VTP domain name on DLS1. Refer to Lab 6-1 for assistance.

```
ALS1# show vtp status
VTP Version                : running VTP2
Configuration Revision      : 4
Maximum VLANs supported locally : 255
Number of existing VLANs    : 7
VTP Operating Mode          : Client
VTP Domain Name             : SWPOD
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Enabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x18 0x59 0xE2 0xE0 0x28 0xF3 0xE7 0xD1
Configuration last modified by 172.16.1.3 at 3-12-93 19:46:16
```

How many VLANs exist in the network? How many of these are defaults?

- Issue the **show vlan brief** command on DLS1. The student and staff VLANs should be listed in the output of this command.

```
DLS1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
100	staff	active	

```

200 student active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

```

Which ports are not listed for VLAN 1? Why is this?

---



---

- c. Issue the **show interfaces trunk** command on DLS2. If trunking was configured properly in Lab 6-1, interfaces Fast Ethernet 0/7–0/12 should be in trunking mode on all switches.

DLS2# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/7	on	802.1q	trunking	1
Fa0/8	on	802.1q	trunking	1
Fa0/9	on	802.1q	trunking	1
Fa0/10	on	802.1q	trunking	1
Fa0/11	on	802.1q	trunking	1
Fa0/12	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/7	1-4094
Fa0/8	1-4094
Fa0/9	1-4094
Fa0/10	1-4094
Fa0/11	1-4094
Fa0/12	1-4094

Port	Vlans allowed and active in management domain
Fa0/7	1,100,200
Fa0/8	1,100,200
Fa0/9	1,100,200
Fa0/10	1,100,200
Fa0/11	1,100,200

Port	Vlans allowed and active in management domain
Fa0/12	1,100,200

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/7	1,100,200
Fa0/8	1,100,200
Fa0/9	1,100,200
Fa0/10	1,100,200
Fa0/11	1,100,200
Fa0/12	1,100,200

Are any VLANs being pruned from these trunks? How can you tell?

---



---



---

- d. Issue the **show spanning-tree vlan 1** command on DLS2. The results from this command might vary, and DLS2 might not be the root in your topology. In the following output, this bridge is currently the root of the spanning tree.

```
DLS2# show spanning-tree vlan 1
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address    000a.b8a9.d680
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    000a.b8a9.d680
Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/7	Desg	FWD	19	128.9	P2p
Fa0/8	Desg	FWD	19	128.10	P2p
Fa0/9	Desg	FWD	19	128.11	P2p
Fa0/10	Desg	FWD	19	128.12	P2p
Fa0/11	Desg	FWD	19	128.13	P2p
Fa0/12	Desg	FWD	19	128.14	P2p

Where is the spanning-tree root in your lab network? Is this root bridge optimal for your network?

---



---

What is the priority of the current root bridge?

---

## Step 2: Configure the primary and secondary root bridges for the VLANs.

In most cases, you must manually configure the spanning-tree root to ensure optimized paths throughout the Layer 2 network. This topic is covered in Module 3. For this scenario, DLS1 acts as the root for VLANs 1 and 100 and performs the secondary function for VLAN 200. In addition, DLS2 is the primary root bridge for VLAN 200 and secondary bridge for VLANs 1 and 100.

- a. Configure STP priority for the primary and secondary roots using the **spanning-tree vlan *vlan ID* root {primary | secondary}** command.

```
DLS1(config)# spanning-tree vlan 1,100 root primary
DLS1(config)# spanning-tree vlan 200 root secondary
```

```
DLS2(config)# spanning-tree vlan 1,100 root secondary
DLS2(config)# spanning-tree vlan 200 root primary
```

- b. Verify the configuration on both DLS1 and DLS2 using the **show spanning-tree** command.

```
DLS2# show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee
Root ID    Priority    24577
Address    000a.b8a9.d780
```

```

Cost          19
Port          13 (FastEthernet0/11)
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID Priority    28673 (priority 28672 sys-id-ext 1)
Address      000a.b8a9.d680
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time   300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/7	Desg	FWD	19	128.9	P2p
Fa0/8	Desg	FWD	19	128.10	P2p
Fa0/9	Desg	FWD	19	128.11	P2p
Fa0/10	Desg	FWD	19	128.12	P2p
Fa0/11	Root	FWD	19	128.13	P2p
Fa0/12	Altn	BLK	19	128.14	P2p

## VLAN0100

Spanning tree enabled protocol ieee

```

Root ID Priority    24676
Address    000a.b8a9.d780
Cost       19
Port       13 (FastEthernet0/11)
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID Priority    28772 (priority 28672 sys-id-ext 100)
Address      000a.b8a9.d680
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time   300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/7	Desg	FWD	19	128.9	P2p
Fa0/8	Desg	FWD	19	128.10	P2p
Fa0/9	Desg	FWD	19	128.11	P2p
Fa0/10	Desg	FWD	19	128.12	P2p
Fa0/11	Root	FWD	19	128.13	P2p
Fa0/12	Altn	BLK	19	128.14	P2p

## VLAN0200

Spanning tree enabled protocol ieee

```

Root ID Priority    24776
Address    000a.b8a9.d680
This bridge is the root
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID Priority    24776 (priority 24576 sys-id-ext 200)
Address      000a.b8a9.d680
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time   300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/7	Desg	FWD	19	128.9	P2p
Fa0/8	Desg	FWD	19	128.10	P2p

Fa0/9	Desg	FWD	19	128.11	P2p
Fa0/10	Desg	FWD	19	128.12	P2p
Fa0/11	Desg	FWD	19	128.13	P2p
Fa0/12	Desg	FWD	19	128.14	P2p

According to the output, what is the root for VLAN 100? For VLAN 200?

---

### Step 3: Configure root guard.

To maintain an efficient STP topology, the root bridge must remain predictable. If a foreign or rogue switch is maliciously or accidentally added to the network, the STP topology could be changed if the new switch has a lower BID than the current root bridge. Root guard helps prevent this by putting a port that hears these BPDUs in the root-inconsistent state. Data cannot be sent or received over the port while it is in this state, but the switch can listen to BPDUs received on the port to detect a new root advertising itself.

Root guard is enabled on a per-port basis with the **spanning-tree guard root** command. You should use root guard on switch ports where you would never expect to find the root bridge for a VLAN.

- a. In the topology diagram, Fast Ethernet ports 0/13 and 0/14 on each switch are not being used as trunk or access ports. It is possible that a switch could be accidentally or maliciously added to those ports. Configure root guard on these ports to ensure that if a switch is added, it is not allowed to take over as root.

```
DLS1(config)# interface range fastEthernet 0/13 - 14
DLS1(config-if-range)# spanning-tree guard root
```

- b. Configure root guard on the same ports for DLS2, ALS1, and ALS2.

What will happen if a switch is connected to Fa0/13 via a crossover cable?

---

---

### Step 4: Demonstrate root guard functionality.

Verify your configuration to make sure that root guard was not accidentally configured on a port that should hear root advertisements, such as a port on ALS2 that is connected to the root bridge.

- a. Use the **show spanning-tree vlan 1** command on ALS2 to look for a root port. In the following example, Fa0/9 is a root port for VLAN 1 on ALS2.

```
ALS2# show spanning-tree vlan 1
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000a.b8a9.d780
             Cost        19
             Port        11 (FastEthernet0/9)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0019.068d.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time   300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----------	------	-----	------	----------	------

```

-----
Fa0/5          Desg FWD 19          128.7    P2p
Fa0/7          Altn BLK 19          128.9    P2p
Fa0/8          Altn BLK 19          128.10   P2p
Fa0/9          Root FWD 19          128.11   P2p
Fa0/10         Altn BLK 19          128.12   P2p

```

- b. Configure root guard on the root port that you found. Note that this configuration is for teaching purposes only. This would *not* be done in a production network.

```

ALS2(config)# interface FastEthernet 0/9
ALS2(config-if)# spanning-tree guard root

```

Notice that as soon as you issue this command, you receive a message that root guard has been enabled and that the port is now in the blocking state for the specific VLANs configured. This port has been transitioned to this state because it receives a BPDU that claims to be the root.

```

1w4d: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port
FastEthernet0/9.
1w4d: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/9
on VLAN0001.

```

- c. Verify which ports are in this inconsistent state with the **show spanning-tree inconsistentports** command.

```

ALS2# show spanning-tree inconsistentports

```

Name	Interface	Inconsistency
VLAN0001	FastEthernet0/9	Root Inconsistent
VLAN0100	FastEthernet0/9	Root Inconsistent
VLAN0200	FastEthernet0/9	Root Inconsistent

Number of inconsistent ports (segments) in the system : 3

- d. Because this configuration is not intended for normal operation, remove it using the **no spanning-tree guard root** command.

```

ALS2(config)# interface FastEthernet 0/9
ALS2(config-if)# no spanning-tree guard root

```

When the configuration is removed, a message indicates that the port is being unblocked.

```

1w4d: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard disabled on port
FastEthernet0/9.
1w4d: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port
FastEthernet0/9 on VLAN0001.

```

## Step 5: Configure BPDU guard.

Because PortFast is enabled on all user access ports on ALS1 and ALS2, BPDUs are not expected to be heard on these ports. Any BPDUs that are heard could result in a disruption of the STP topology, so you should protect these ports from any type of accidental or malicious behavior which leads to BPDUs arriving at the port. If a rogue access point or switch is placed on these ports, BPDUs would most likely be heard.

BPDU guard protects ports from this type of situation by placing the interface in the error-disable state. The BPDU guard feature provides a secure response to invalid configurations because the network administrator must manually put the interface back in service.

- a. To enable BPDU guard on PortFast-enabled ports, use the **spanning-tree portfast bpduguard default** global configuration command.

```
ALS1(config)# spanning-tree portfast bpduguard default
```

```
ALS2(config)# spanning-tree portfast bpduguard default
```

- b. Verify your configuration using the **show spanning-tree summary** command.

```
ALS2# 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 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	5	0	0	2	7
VLAN0100	5	0	0	1	6
VLAN0200	5	0	0	1	6
3 vlans	15	0	0	4	19

Which action will be taken if a wireless access point sending BPDUs is connected to Fa0/15 on ALS1?

## Step 6: Enable broadcast storm control on trunk ports.

If a basic unmanaged switch is connected to an access port, a broadcast storm can result, which can lead to network failure. Implementing broadcast storm protection on trunk interfaces can help prevent this.

- a. Enable storm control for broadcasts on Fast Ethernet ports 0/7 and 0/8 on ALS1 with a 50 percent rising suppression level using the **storm-control broadcast** command. ALS1 trunk ports Fa0/7 and Fa0/8 are shown here as an example.

```
ALS1(config)# interface FastEthernet 0/7
ALS1(config-if)# storm-control broadcast level 50
ALS1(config-if)# interface FastEthernet 0/8
ALS1(config-if)# storm-control broadcast level 50
```

- b. Verify the configuration of interface Fa0/7 with the **show running-config** command.

```
ALS1# show running-config interface fastEthernet 0/7
Building configuration...
```

```
Current configuration : 155 bytes
!
interface FastEthernet0/7
  switchport mode trunk
  storm-control broadcast level 50.00
  ip dhcp snooping trust
end
```



## Step 7: Configure UDLD.

A unidirectional link occurs when traffic is transmitted between neighbors in one direction only. Unidirectional links can cause spanning-tree topology loops. UDLD allows devices to detect when a unidirectional link exists and shut down the affected interface.

You can configure UDLD on a per-port basis or globally for all fiber-optic gigabit interfaces. The **aggressive** keyword places the port in the error-disable state when a violation occurs on the port.

```
DLS1(config)# udld ?
    aggressive  Enable UDLD protocol in aggressive mode on fiber ports except
                  where locally configured
    enable      Enable UDLD protocol on fiber ports except where locally
                  configured
```

- a. Enable UDLD protection on Fast Ethernet ports 1–24 on all switches using the **udld port aggressive** command. Configure UDLD globally for all fiber-optic gigabit interfaces for future use using the **udld enable** command.

**Note:** This lab assumes the existence of fiber-optic gigabit ports, although this might not be the case with your lab equipment.

```
DLS1(config)# interface range FastEthernet 0/1 - 24
DLS1(config-if-range)# udld port aggressive
DLS1(config-if-range)# exit
DLS1(config)# udld enable
```

```
DLS2(config)# interface range FastEthernet 0/1 - 24
DLS2(config-if-range)# udld port aggressive
DLS2(config-if-range)# exit
DLS2(config)# udld enable
```

```
ALS1(config)# interface range FastEthernet 0/1 - 24
ALS1(config-if-range)# udld port aggressive
ALS1(config-if-range)# exit
ALS1(config)# udld enable
```

```
ALS2(config)# interface range FastEthernet 0/1 - 24
ALS2(config-if-range)# udld port aggressive
ALS2(config-if-range)# exit
ALS2(config)# udld enable
```

- b. Verify your configuration using the **show udld interface-id** command.

```
ALS2# show udld Fa0/15
```

```
Interface Fa0/15
```

```
---
```

```
Port enable administrative configuration setting: Enabled / in aggressive
mode
```

```
Port enable operational state: Enabled / in aggressive mode
```

```
Current bidirectional state: Unknown
```

```
Current operational state: Link down
```

```
Message interval: 7
```

```
Time out interval: 5
```

```
No neighbor cache information stored
```

What is the operation state of this interface?

---

**Note:** Although not configured in this lab, loop guard can be configured as an alternative or in addition to UDLD. The functionality overlaps, partly in the sense that both protect against STP failures caused by unidirectional links. Based on the various design considerations, you can choose UDLD or the loop guard feature or both. In regards to STP, the most noticeable difference between the two features is the absence of protection in UDLD against STP failures caused by problems in software. As a result, the designated switch does not send BPDUs. However, this type of failure is (by an order of magnitude) more rare than failures caused by unidirectional links. In return, UDLD might be more flexible in the case of unidirectional links on EtherChannel. In this case, UDLD disables only failed links, and the channel should remain functional with the links that remain. In such a failure, loop guard puts it into loop-inconsistent state to block the whole channel.

**Note:** Save your final device configurations for use with the next lab.