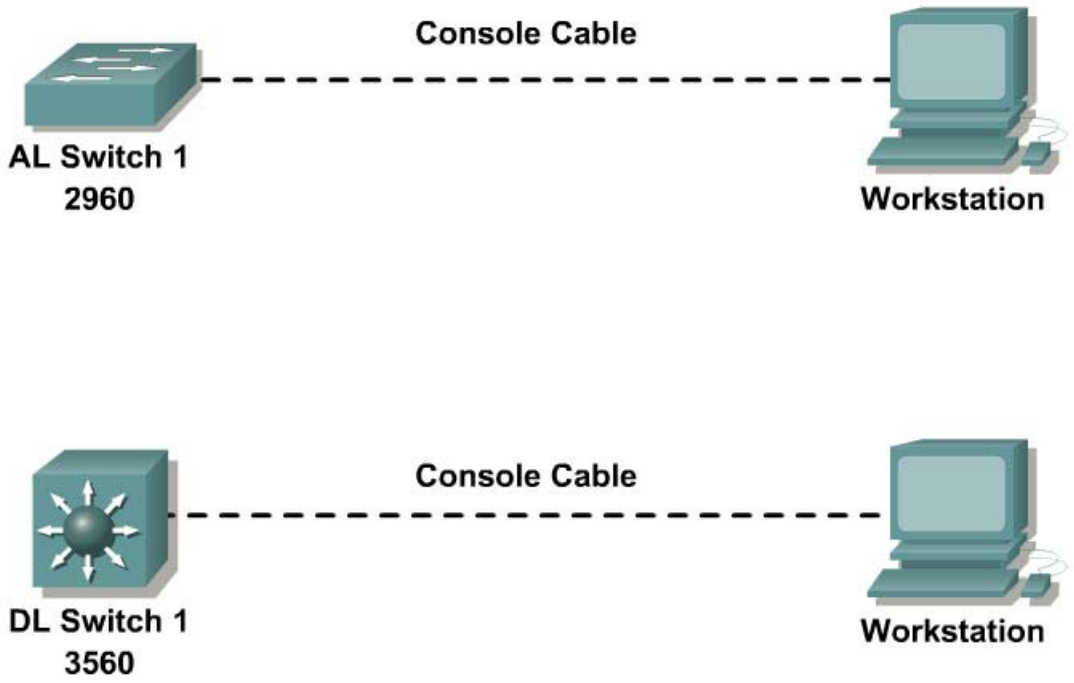
CISCO NETWORKING ACADEMY PROGRAM

CCNP:
Building Multilayer Switched Networks v5.0

Student Lab Manual

Lab 2-0a Clearing a Switch



Objective

The purpose of this lab is to clear a switch and prepare it for a new lab.

Scenario

Prepare a Catalyst 2960 or 3560 switch to be used in a lab.

Step 1

Connect to the switch that you want to clear with a console cable. You get a console prompt that includes the switch's hostname, followed by a ">" or "#".

```
Switch>
```
Or
```
Switch#
```

If the prompt ends with a ">", you are not currently in privileged mode. To enter privileged mode, type **enable**. This may require a password. If you are in a configuration mode, type **exit** or **end**.

If not enabled:
```
Switch>enable
Switch#
```


If in a configuration mode:

```
Switch(config)#exit
Switch#
```

Step 2

Once in privileged mode, type **delete vlan.dat** and press Return. If you are asked to confirm, press Return to confirm until you are back to the original prompt.

```
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#
```

Step 3

After deleting the vlan.dat file, you can erase the startup configuration on the switch by typing **erase startup-config**. You again have to press Return to confirm.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Step 4

After clearing the switch configuration, reload the switch by typing **reload** and pressing Return. If you asked whether you want to save the current configuration, answer no. Press Return to confirm. The switch starts reloading. Your output may look different depending on the switch model you are using. This step may take a few minutes, because the switch needs time to reload.

```
Switch#reload

System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]

1d20h: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
Base ethernet MAC Address: 00:0a:b8:a9:d7:80
Xmodem file system is available.
The password-recovery mechanism is enabled.
Initializing Flash...
flashfs[0]: 349 files, 5 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 15998976
flashfs[0]: Bytes used: 7909888
flashfs[0]: Bytes available: 8089088
flashfs[0]: flashfs fsck took 9 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs) installed, fsid: 3
done.
Loading "flash:c3560-ipservices-mz.122-25.SEB4/c3560-ipservices-mz.122-
25.SEB4.bin"...@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "flash:c3560-ipservices-mz.122-25.SEB4/c3560-ipservices-mz.122-25.SEB4.bin"
uncompressed and installed, entry point: 0x3000
executing...

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, C3560 Software (C3560-IPSERVICES-M), Version 12.2(25)SEB4, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 30-Aug-05 14:19 by yenanh
Image text-base: 0x00003000, data-base: 0x00E7EBC8

Initializing flashfs...

flashfs[1]: 349 files, 5 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 15998976
flashfs[1]: Bytes used: 7909888
flashfs[1]: Bytes available: 8089088
flashfs[1]: flashfs fsck took 1 seconds.
flashfs[1]: Initialization complete....done Initializing flashfs.

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC PortASIC interface Loopback Tests : Begin
POST: CPU MIC PortASIC interface Loopback Tests : End, Status Passed

POST: PortASIC RingLoopback Tests : Begin
POST: PortASIC RingLoopback Tests : End, Status Passed

POST: Inline Power Controller Tests : Begin
POST: Inline Power Controller Tests : End, Status Passed
```



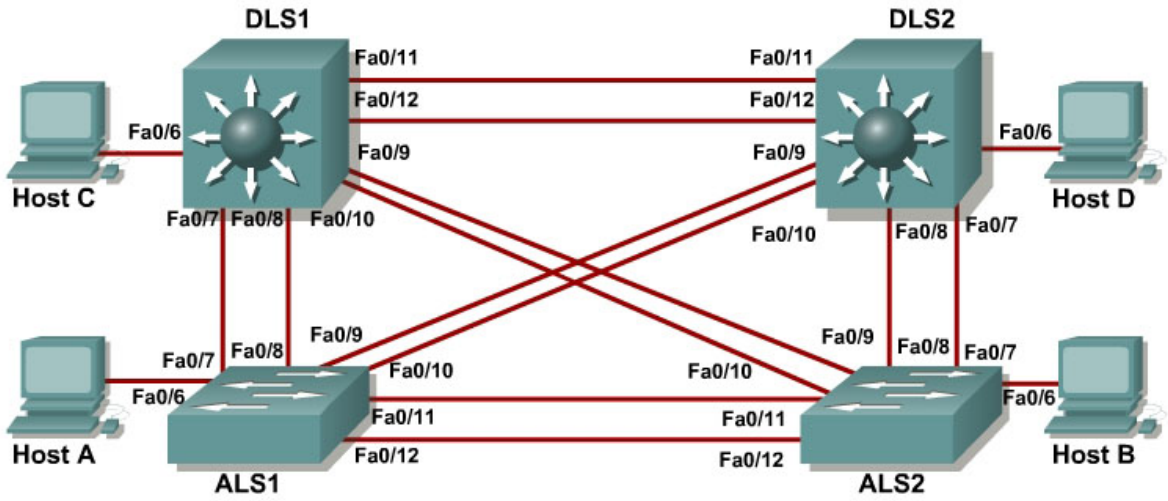
```
POST: PortASIC CAM Subsystem Tests : Begin
POST: PortASIC CAM Subsystem Tests : End, Status Passed

POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed

Waiting for Port download...Complete

cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with 118784K/12280K bytes of
memory.
Processor board ID CAT1026RMCJ
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:0A:B8:A9:D7:80
Motherboard assembly number     : 73-9673-09
Power supply part number        : 341-0029-05
Motherboard serial number       : CAT10266M51
Power supply serial number      : LIT10230AYW
Model revision number           : P0
Motherboard revision number     : A0
Model number                    : WS-C3560-24PS-E
System serial number            : CAT1026RMCJ
Top Assembly Part Number        : 800-26380-04
Top Assembly Revision Number    : B0
Version ID                      : V06
CLEI Code Number                : COM1100ARC
Hardware Board Revision Number  : 0x01


Switch   Ports  Model              SW Version            SW Image
------   -----  -----              ----------            ----------
*    1   26     WS-C3560-24PS      12.2(25)SEB4          C3560-IPSERVICES-M



Press RETURN to get started!
```

Step 5

The switch may log messages to the console, such as interfaces coming up and down. When you see the “Press RETURN to get started!” message, press Return. If you are asked whether you want to terminate auto-install, press Return to say yes.

If you are asked to enter an initial configuration dialog, type no, and you are placed at the exec prompt. If you accidentally type yes, you can break out of the initial configuration dialog at any time by pressing Ctrl-C. That concludes how to reset a switch for a lab.

Lab 2-0b Clearing a Switch Connected to a Larger Network



Objective

The purpose of this lab is to clear a switch that is connected to other switches and prepare it for a new lab.

Scenario

Prepare a Catalyst 2960 or 3560 switch to be used in a lab.

Step 1

This lab assumes that you have read Lab 2.0a “Clearing a Switch.”

Step 2

Once in privileged mode, type **delete vlan.dat** and press Return. If you are asked to confirm, press Return to confirm until you are back to the original prompt.

```
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#
```

Step 3

After deleting the vlan.dat file, you can erase the startup configuration on the switch by typing **erase startup-config**. You again have to press Return to confirm.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```


Step 4

The difficulty with clearing a switch that is networked to other switches is that even though you can easily remove the configuration file, it is more difficult to remove the VLANs. When the switch is finished reloading, it is possible for it to re-learn VLANs from another networked switch that is in server mode.

To determine if this has happened, use the **show vlan** command:

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                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
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

In this sample output, the switch has not learned any VLANs from another switch. You are finished clearing the switch of both its configuration and its VLANs.

If, however, you issue the **show vlan** command and you see VLANs after having deleted the vlan.dat file, your switch has learned these dynamically from another switch to which it is networked.

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                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
10   green                            active
20   blue                             active
30   yellow                           active
40   purple                           active
50   red                              active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```


Step 5

To eliminate these VLANS, do the following:

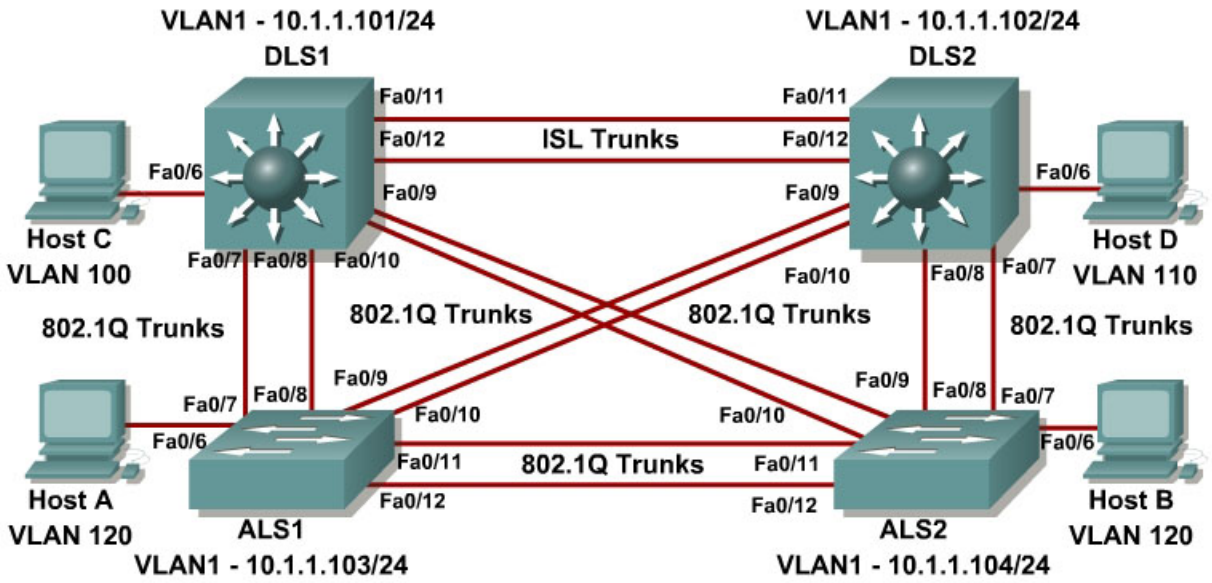
```
Switch(config)#interface range FastEthernet 0/1 -24
Switch(config-if-range)#shutdown
Switch(config-if-range)#
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
15:44:06: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
15:44:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
15:44:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down
15:44:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to down
15:44:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down
15:44:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down
15:44:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to down
Switch(config-if-range)#interface range GigabitEthernet 0/1 -2
Switch(config-if-range)#shutdown
Switch(config-if-range)#
15:45:59: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
15:45:59: %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
Switch(config-if-range)#exit
Switch(config)#no vlan 2-50
Switch(config)#exit
Switch#show vlan
15:48:39: %SYS-5-CONFIG_I: Configured from console by console

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                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
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Step 6

Now that both the configuration and the VLANs have been erased, you are ready to start a new lab. Use the **no shutdown** command on the links that are administratively down in your new lab. If you want to do some configuration before your switch learns VLANs from the network, put it into transparent mode until you are ready:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#^Z
Switch#
```


Lab 2-1 Catalyst 2960 and 3560 Series Static VLANS, VLAN Trunking, and VTP Domain and Modes



Objective

Set up a VTP domain, create and maintain VLANs, and use Inter-Switch Link (ISL) and 802.1Q trunking on Cisco Catalyst 2960 and 3560 series Ethernet switches using command-line interface (CLI) mode.

Scenario

VLANs must logically segment a network by function, team, or application, regardless of the physical location of the users. All end stations in a particular IP subnet are often associated with a specific VLAN. VLAN membership on a switch that is assigned manually for each interface is known as static VLAN membership.

Trunking, or connecting switches, and the VLAN Trunking Protocol (VTP) are used to segment the network. VTP manages the addition, deletion, and renaming of VLANs on the entire network from a single central switch. VTP minimizes configuration inconsistencies that can cause problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Step 1

Power up the switches and use the standard process for establishing a HyperTerminal console connection from a workstation to each switch in your pod. If you are connecting remotely to your switches, follow the instructions that have been supplied by your instructor.

Prepare for the lab by removing all VLAN information and configurations that may have been previously entered into you switches. Refer to Lab 2.0 “Clearing a Switch” and Lab 2.0b “Clearing a Switch Connected to a Larger Network.”

Step 2

To differentiate between the devices, give the switches names using the **hostname** command. We will also put IP addresses on the management VLAN according to the diagram. By default, VLAN 1 is used as the management VLAN.

The following is a sample configuration for the 3560 switch DLS1.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname DLS1
DLS1(config)#interface vlan 1
DLS1(config-if)#ip address 10.1.1.101
DLS1(config-if)#no shutdown
DLS1(config)#end
DLS1#
```

Repeat these steps on the other pod switches according to the diagram.

Step 3

Use the **show vlan** command from privileged mode on any switch. The following output is for a 2960 switch.

```
ALS1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                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
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```


The following output is for a 3560 switch.

```
DLS1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 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
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Note that the default VLAN numbers, names, associated types, and all switch ports are automatically assigned to VLAN 1.

You can use the **show vlan** command to determine the mode of a port. Ports configured for a particular VLAN are shown in that VLAN. Ports configured to trunk mode do not appear in any of the VLANs.

Step 4

A VTP domain, also called a VLAN management domain, consists of trunked or interconnected switches that are under the administrative responsibility of a switch or switches in server VTP mode. A switch can be in only one VTP domain with the same VTP domain name. The default VTP mode for the 2960 and 3560 switches is server mode. VLAN information is not propagated until a domain name is specified and trunks are set up between the devices.

The following table describes the three VTP modes.

VTP Mode	Description
VTP Server	This is the default VTP mode. VLANs can be created, modified, and deleted. Other configuration parameters

	may be specified for all switches in the VTP domain. VTP servers advertise VLAN configurations to other switches in the same VTP domain and synchronize VLAN configurations with other switches based on advertisements received over trunk links. In VTP server mode, VLAN configurations are saved in NVRAM.
VTP Client	The switch learns VLANs from the switch in server mode, without the ability to create, change, or delete VLANs. In VTP client mode, VLAN configurations are not saved in NVRAM.
VTP Transparent	Switches do not participate in VTP. The switch does not advertise its VLAN configuration and does not synchronize its configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive from other switches from their trunk interfaces. Therefore, local VLANs may be created, modified, and deleted on a switch in the transparent mode. In VTP transparent mode, VLAN configurations are saved in NVRAM, but they are not advertised to other switches.

Use the **show vtp status** command on any of the switches. The output should be similar to the following sample for DLS1.

```
DLS1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 10.1.1.250 on interface Vl1 (lowest numbered VLAN
interface found)
```

Since no VLAN configurations were made, all settings are the defaults. Notice that the VTP mode is server. The number of existing VLANs is the five built-in VLANs. The 3560 switch supports 1005 maximum VLANs locally. The 2960

switch supports 255. The configuration revision is zero, and the VTP version is 2. All switches in the VTP domain must run the same VTP version.

The importance of the configuration revision number is that the switch in VTP server mode with the highest revision number propagates VLAN information over trunked ports. Every time VLAN information is modified and saved in the VLAN database or vlan.dat file, the revision number is increased by one when the user exits from VLAN configuration mode.

Multiple switches in the VTP domain can be in VTP server mode. These switches can be used to manage all other switches in the VTP domain. This is suitable for small-scale networks where the VLAN information is small and easily stored in all switches. In a large network, the administrator must determine which switches make the best VTP servers. The network administrator should set aside some of the more powerful switches and keep them as VTP servers. The other switches in the VTP domain can be configured as clients. The number of VTP servers should be consistent based on the amount of redundancy desired in the network.

Step 5

Change the VTP domain name on DLS1 to SWLAB using the **vtp domain** command. The following is an example configuration from DLS1.

```
DLS1(config)#vtp domain SWLAB
Changing VTP domain name from NULL to SWLAB
DLS1(config)#end
```

Set up the switches so that the DL switches are in VTP server mode, and the AL switches are in VTP client mode. The following are example configurations for DLS1 and ALS1.

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#vtp mode server
Device mode already VTP SERVER.
DLS1(config)#end
```

```
ALS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#vtp mode client
Setting device to VTP CLIENT mode.
ALS1(config)#end
```

Note that since the default mode is server, we receive a message on DLS1 stating that the device mode is already VTP server.

Use the **show vtp status** command on either of the AL switches. The output should be similar to the following sample for ALS1.

```
DLS1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
```



```
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 10.1.1.250 on interface Vl1 (lowest numbered VLAN
interface found)
```

Notice that we do not see the VTP domain name we set up on DLS1. Since we do not have any trunks set up between the switches, they have not started to distribute any VLAN information.

Step 6

The **show interfaces switchport** command lists the configured mode of each port in detail. The following partial sample output is for a 2960 switch on FastEthernet 0/1.

```
ALS1#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Ports on the 2960 and 3560 are set to dynamic auto by default. This means that they do not try to negotiate a trunk unless manual configuration is performed on either side of the trunk to begin the negotiation. This can be done by configuring one end of the trunk using the **switchport mode trunk** command. On the 3560

switches, you also need to configure the trunk encapsulation with the **switchport trunk encapsulation** command. The 3560 switch can use either ISL or 802.1Q encapsulation, whereas the 2960 only supports 802.1Q.

Check the lab diagram for which ports to set up as trunks and their encapsulation types.

Configure only the interfaces on DLS1 and ALS1 with the **switchport mode trunk** command, and leave DLS2 and ALS2 as the default port types for interfaces FastEthernet 0/9 – 0/12. FastEthernet 0/7 and 0/8 of DLS2 also need to be configured for the trunks connecting DLS2 and ALS2.

The 2960 and 3560 switches have a **range** command that you can use to designate multiple individual ports or a continuous range of ports for an operation.

Use the **interface range** command to configure all trunk ports at once for trunking.

The following is a sample configuration for the ISL and 802.1Q trunk ports on DLS1.

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#interface range fastEthernet 0/7 - 10
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#end

DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#interface range fastEthernet 0/11 - 12
DLS1(config-if-range)#switchport trunk encapsulation isl
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#end
```

The following is a sample configuration for the trunk ports on ALS1.

```
ALS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#interface range FastEthernet 0/11 - 12
ALS1(config-if)#switchport mode trunk
ALS1(config-if)#end
```

The following is a sample configuration for the trunk ports on DLS2.

```
DLS2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)#interface range fastEthernet 0/7 - 8
DLS2(config-if-range)#switchport trunk encapsulation dot1q
DLS2(config-if-range)#switchport mode trunk
DLS2(config-if-range)#end
DLS2#
```

Step 7

Verify the trunking configuration of each switch using the following commands.

Use the **show interfaces fa0/7 switchport** command on both ALS1 and ALS2.

The following is a sample from ALS2.

```
ALS2#show interfaces fa0/7 switchport
Name: Fa0/7
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Notice that administrative mode on Fa0/7 of ALS2 is still the default dynamic auto. FA0/7 on ALS2 is operating as a trunk, because port Fa0/7 of DLS2 was configured using the **switchport mode trunk** command. Once this command was issued, trunking was negotiated between the two switch ports.

Use the **show interfaces trunk** command on DLS1.

```
DLS1#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           isl            trunking      1
Fa0/12      on           isl            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       1,100,110,120
Fa0/8       1,100,110,120
Fa0/9       1,100,110,120
Fa0/10      1,100,110,120
Fa0/11      1,100,110,120

Port        Vlans allowed and active in management domain
Fa0/12      1,100,110,120

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/7       1,100,110,120
Fa0/8       1,100,110,120
Fa0/9       1,100,110,120
Fa0/10      1,100,110,120
Fa0/11      1,100,110,120
Fa0/12      none
```

Use the **show interfaces trunk** command on DLS2.

```
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       auto         n-802.1q       trunking      1
Fa0/10      on           802.1q         trunking      1
Fa0/11      auto         n-isl          trunking      1
Fa0/12      auto         n-isl          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       1,100,110,120
Fa0/8       1,100,110,120
Fa0/9       1,100,110,120
Fa0/10      1,100,110,120
Fa0/11      1,100,110,120

Port        Vlans allowed and active in management domain
Fa0/12      1,100,110,120

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/7       1,100,110,120
Fa0/8       1,100,110,120
Fa0/9       1,100,110,120
Fa0/10      1,100,110,120
Fa0/11      1,100,110,120
Fa0/12      1,100,110,120
```

Notice in the highlighted output from DLS2 under the mode and encapsulation columns that these ports became trunks by negotiation. The connected ports of the respective switches were configured using the **switchport mode trunk** command.

Step 8

The Fast Ethernet ports connected to the hosts on the network can be set up as static access because they are not to be used as trunk ports. We use the **switchport mode** command to accomplish this task.

Use the **switchport mode ?** command for interface FastEthernet 0/6 in interface configuration mode.

The following command is for a 2960 switch.

```
ALS1#config terminal

ALS1(config)#interface FastEthernet 0/6
ALS1#(config-if)#switchport mode ?
  access   Set trunking mode to ACCESS unconditionally
  dynamic  Set trunking mode to dynamically negotiate access or trunk mode
  trunk    Set trunking mode to TRUNK unconditionally
```

The following command is for a 3560 switch.

```
DLS1#config terminal
DLS1(config)#interface FastEthernet 0/6
DLS1(config-if)#switchport mode ?
  access        Set trunking mode to ACCESS unconditionally
  dot1q-tunnel  set trunking mode to TUNNEL unconditionally
  dynamic       Set trunking mode to dynamically negotiate access or trunk mode
  private-vlan  Set the mode to private-vlan host or promiscuous
  trunk         Set trunking mode to TRUNK unconditionally

Switch(config-if)#switchport mode ?
  access        Set trunking mode to ACCESS unconditionally
  dot1q-tunnel  Set trunking mode to DOT1Q TUNNEL unconditionally
  dynamic       Set trunking mode to dynamically negotiate access or trunk
                  mode
  trunk         Set trunking mode to TRUNK unconditionally
```

A port on the 2960 switch can operate in one of three modes, and a port on the 3560 switch can operate in one of five modes.

Use the **switchport mode access** command to set a single port to the access mode. This is shown in the following example, which uses the FastEthernet 0/6 port.

Use this command on FastEthernet 0/6 port on all four switches in the pod.

The following is a sample configuration for the access port on ALS1.

```
ALS1#config terminal
ALS1(config)#interface FastEthernet 0/6
ALS1(config-if)#switchport mode access
ALS1(config-if)#^Z
```

Use the **show interfaces** command again for FastEthernet 0/6 on your switches.

The following command is for a 3560 switch.

```
DLS1#show interfaces fa0/6
Name: Fa0/6
Switchport: Enabled
```



```
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Note that administrative mode has now changed to static access, and that negotiation of trunking is off. The FastEthernet 0/6 ports on all four switches are now statically set to connect to a host device.

Step 9

Verify VTP configuration within the domain before configuring VLANs.

Use the **show vtp status** command on ALS1 and ALS2.

The following sample output is from ALS1.

```
ALS1#show vtp stat
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : SWPOD
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xC2 0x7A 0x7C 0xAC 0xA0 0xEA 0x85 0xEB
Configuration last modified by 10.1.1.101 at 3-1-93 04:55:43
```

The following sample output is from ALS2.

```
ALS2#show vtp stat
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : SWPOD
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
```



```
VTP Traps Generation            : Disabled
MD5 digest                      : 0xC2 0x7A 0x7C 0xAC 0xA0 0xEA 0x85 0xEB
Configuration last modified by 10.1.1.101 at 3-1-93 04:55:43
```

At this point, all switches in our pod are in VTP domain SWPOD, and have five existing VLANs. DLS1 and DLS2 are configured as VTP servers, and ALS1 and ALS2 are configured as clients.

Step 10

There are a few different ways that VLANs can be configured on a switch, depending on the type of switch used and the Cisco IOS version. An older way to configure VLANs is to use the VLAN database. This method is being deprecated and is no longer recommended. However, the VLAN database is still accessible for those who choose to use it.

The following command is for a 3560 switch.

```
DLS1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.
```

A more current way to create a VLAN is to assign a port to a VLAN that does not yet exist. The switch automatically creates the VLAN to the port that it has been assigned to.

VLAN 1 is the management VLAN by default. Therefore, all ports are automatically assigned to VLAN 1, and all ports are in access mode. There is no need to create a VLAN 1, assign ports to it, or to set the mode of each port.

VLANs 100, 110, and 120 must be created, and port 6 must be assigned to each VLAN according to the diagram. We will create VLANs 100 and 110 on the distribution switches using the port assignment method, and we will create VLAN 120 on the access switches using global configuration commands and then assign ports to those VLANs.

Use the **switchport access vlan** command to assign port 6 on DLS1 and DLS2 according to the diagram. Port FastEthernet 0/6 of DLS1 will be assigned to VLAN 100, and FastEthernet 0/6 on DLS2 will be assigned to VLAN 110.

The following command is for the 3560 switches.

```
DLS1#config terminal
DLS1(config)#interface FastEthernet 0/6
DLS1(config-if-range)#switchport access vlan 100
% Access VLAN does not exist. Creating vlan 100
Switch(config-if-range)#^z
```

VLAN 100 was created at the same time port 6 was assigned to it.

Configure DLS2 in the following manner, similar to DLS1, but this time using VLAN 110.

```
DLS2#config terminal
```



```
DLS2(config)#interface FastEthernet 0/6
DLS2(config-if-range)#switchport access vlan 110
% Access VLAN does not exist. Creating vlan 110
Switch(config-if-range)#^z
```

Issue a **show vlan** command on DLS1 to verify that VLANs 100 and 110 have been created. The output should be similar to the following sample output.

```
DLS1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/10, 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  VLAN0100                         active    Fa0/6
110  VLAN0110                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
110  enet  100110     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Since VLAN 100 and 110 were not named, the switch automatically assigns default names, which are VLAN0100 and VLAN0110.

Note that on DLS1 port fa0/6 is active in VLAN 100. A **show vlan** command issued on DLS2 should show port fa0/6 active in VLAN 110.

Step 11

Another way of creating VLANs is to create them in configuration mode without assigning port membership.

A VLAN can be created in global configuration mode using the **VLAN** command. Since ALS1 and ALS2 are configured for VTP client mode, and it is not possible to create a VLAN when a switch is in client mode, it is necessary to create the

VLAN on the switch that is acting as a server for the network. The VLAN then propagates to the other switches that are in client mode.

Issue the VLAN command in global configuration mode on DLS1.

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#vlan 120
DLS1(config-vlan)#end
```

Ports still need to be assigned to VLAN 120. Port assignment to a VLAN is an interface configuration operation.

Use the **switchport access vlan** command on FastEthernet 0/6 of ALS1 and ALS2 to configure those ports for VLAN 120.

```
ALS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#interface fastEthernet 0/6
ALS1(config-if)#switchport access vlan 120
ALS1(config-if)#end

ALS2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)#interface fastEthernet 0/6
ALS2(config-if)#switchport access vlan 120
ALS2(config-if)#end
```

Use the **show vlan** command to verify the creation of VLAN 120, with port Fa0/6 assigned to it. The output should be similar to the following.

```
ALS1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, 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  VLAN0100                         active
110  VLAN0110                         active
120  VLAN0120                         active    Fa0/6
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
110  enet  100110     1500  -      -      -        -    -        0      0
120  enet  100120     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1003 tr    101003     1500  -      -      -        -    srb      0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
```



```
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Step 12

The VLANs have not been named yet. Naming VLANs can help network administrators identify the functionality of those VLANs. To add names, use the **name** command in VLAN configuration mode.

The following is a sample configuration for naming the three VLANs created in the domain.

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#vlan 100
DLS1(config-vlan)#name Server-Farm-1
DLS1(config-vlan)#exit
DLS1(config)#vlan 110
DLS1(config-vlan)#name Server-Farm-2
DLS1(config-vlan)#exit
DLS1(config)#vlan 120
DLS1(config-vlan)#name Net-Eng
DLS1(config-vlan)#exit
DLS1(config)#end
```

Use the **show vlan** command on DLS1 to verify that the new names have been added.

```
DLS1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, 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  Server-Farm-1                    active    Fa0/6
110  Server-Farm-2                    active
120  Net-Eng                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
110  enet  100110     1500  -      -      -        -    -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
120  enet  100120     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
```



```
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------
```

Step 13

Prepare for the next lab by removing all the VLAN information and configurations. The VLAN database and startup configuration need to be deleted. Refer to lab 2.0a or 2.0b.

Note	Traffic between VLANs must be routed. Inter-VLAN routing will be covered in a later lab.

Show the running configuration on DLS1:

```
DLS1#show run
!
hostname DLS1
!
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/11
 switchport trunk encapsulation isl
 switchport mode trunk
!
interface FastEthernet0/12
 switchport trunk encapsulation isl
 switchport mode trunk
!
!
interface Vlan1
 ip address 10.1.1.101 255.255.255.0
!
!
End
```


Show the running configuration on DLS2:

```
DLS2#show run
!
hostname DLS2
!
!
interface FastEthernet0/6
 switchport access vlan 110
 switchport mode access
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
!
interface Vlan1
 ip address 10.1.1.102 255.255.255.0
 shutdown
!
!
end
```

Show the running configuration on ALS1:

```
ALS1#show run
!
hostname ALS1
!
!
interface FastEthernet0/6
 switchport access vlan 120
!
interface FastEthernet0/7
 switchport mode trunk
!
interface FastEthernet0/8
 switchport mode trunk
!
interface FastEthernet0/9
 switchport mode trunk
!
interface FastEthernet0/10
 switchport mode trunk
!
interface FastEthernet0/11
 switchport mode trunk
!
interface FastEthernet0/12
 switchport mode trunk
!
!
```

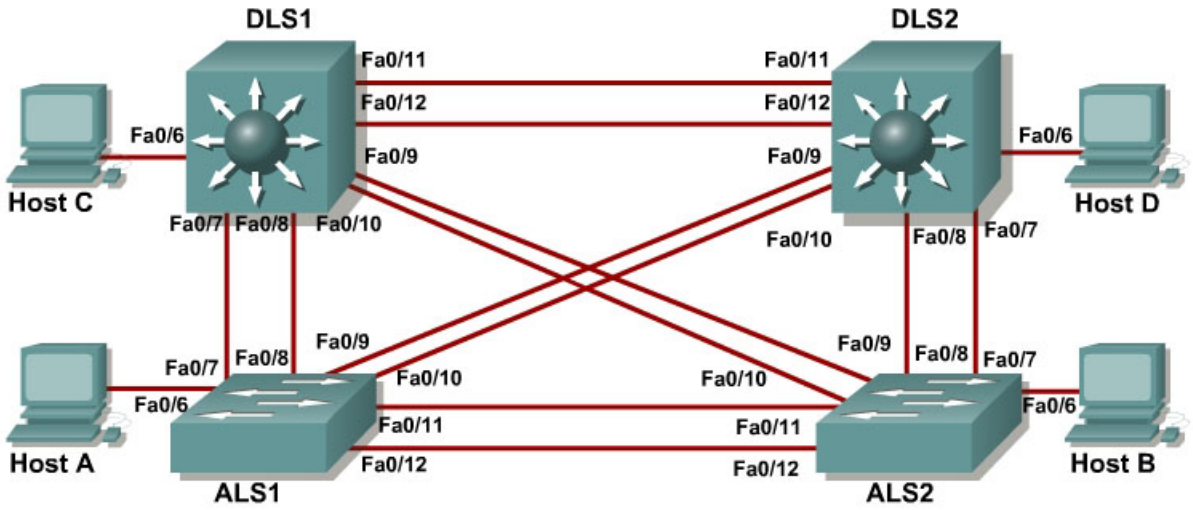


```
interface Vlan1
 ip address 10.1.1.103 255.255.255.0
 no shutdown
!
end
```

Show the running configuration on ALS2:

```
ALS2#show run
!
hostname ALS2
!
!
interface FastEthernet0/6
 switchport access vlan 120
!
!
interface Vlan1
 ip address 10.11.1.104 255.255.255.0
 no shutdown
!
end
```


Lab 3-1 Spanning Tree Protocol (STP) Default Behavior



Objective

The purpose of this lab is to observe the default behavior of STP.

Scenario

Four switches have just been installed. The distribution layer switches are Catalyst 3560s, and the access layer switches are Catalyst 2960s. There are redundant uplinks between the access layer and distribution layer. Because of the possibility of bridging loops, spanning tree logically removes any redundant links. In this lab, you will observe what spanning tree does and why.

Step 1

Refer to Lab 2.0 “Clearing a Switch” to prepare all four switches for this lab. Cable the equipment as shown. If you are accessing your equipment remotely, ask your instructor for instructions on how to do this. Configure the four switches as shown in the diagram with a hostname, password, and console security. Connect to DLS1 and enter the following commands:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname DLS1
DLS1(config)#enable secret class
DLS1(config)#line console 0
DLS1(config-line)#password cisco
DLS1(config-line)#login
```

Connect to DLS2 and enter the following commands:


```
Switch>enable
Switch#configure terminal
Switch(config)#hostname DLS2
DLS2(config)#enable secret class
DLS2(config)#line console 0
DLS2(config-line)#password cisco
DLS2(config-line)#login
```

Connect to ALS1 and enter the following commands:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname ALS1
ALS1(config)#enable secret class
ALS1(config)#line console 0
ALS1(config-line)#password cisco
ALS1(config-line)#login
```

Connect to ALS2 and enter the following commands:

```
Switch>enable
Switch# configure terminal
Switch(config)#hostname ALS2
ALS2(config)#enable secret class
ALS2(config)#line console 0
ALS2(config-line)#password cisco
ALS2(config-line)#login
```

Step 2

After the cables are connected and the switch detects the redundant links, spanning tree is initiated.

By default, spanning tree runs on every port. When a new link becomes active, the port goes through the listening, learning, and forwarding states before it becomes active. During this period, the switch discovers if it is connected to another switch or an end-user device.

If another switch is detected, the two switches begin creating a spanning tree. One of the switches is elected as the root of the tree. Then an agreement is established as to which links to keep active and which links to disable if multiple links exist.

1. What type of frame does STP use to communicate with other switches?

Note	The results in this lab will vary. Spanning tree operation is based on the MAC address of the switches.

Observe the LEDs on the switch to check the status of the link. A bright green light indicates an active link. An amber light indicates an inactive link.

Step 3

Verify STP with the **show spanning-tree** command on DLS1:

```
DLS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000a.b8a9.d680
              Cost        19
              Port        13 (FastEthernet0/11)
              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.d780
             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
```

Verify STP with the **show spanning-tree** command on DLS2:

```
DLS2#show spanning-tree

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
```

Verify STP with the **show spanning-tree** command on ALS1:

```
ALS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
```



```
              Address     000a.b8a9.d680
              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     0019.0635.5780
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost
1d22h: %SYS-5-CONFIG_I: Configured from console by console    Prio.Nbr
       Type
---------------- ---- --- --------- -------- --------------------------
       --
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
Fa0/11           Desg FWD 19        128.13   P2p
Fa0/12           Desg FWD 19        128.14   P2p
```

Verify STP with the **show spanning-tree** command on ALS2:

```
ALS2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000a.b8a9.d680
              Cost        19
              Port        9 (FastEthernet0/7)
              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
1d22h: %SYS-5-CONFIG_I: Configured from console by console   Prio.Nbr
       Type
---------------- ---- --- --------- -------- --------------------------
       --
Fa0/7            Root FWD 19        128.9    P2p
Fa0/8            Altn BLK 19        128.10   P2p
Fa0/9            Altn BLK 19        128.11   P2p
Fa0/10           Altn BLK 19        128.12   P2p
Fa0/11           Altn BLK 19        128.13   P2p
Fa0/12           Altn BLK 19        128.14   P2p
```

Notice that between two switches, one of the two ports is set to blocking. Blocking could occur on the access layer switch or the distribution layer switch. If all ports have their default setting, the higher interface number of the two ports is set to blocking.

The switch port is in blocking state because it detected two links between the same switches. This would result in a bridge loop if the switch logically disables one link.

Note	Your output may differ, because all switches have the default bridge priority of 32769 and selection of the root bridge is based upon the lowest switch MAC address. The sample output below may also differ from those in your lab, because they were generated with a different set of switches.

```
DLS2#show spanning-tree

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
```

After reviewing the spanning tree output, answer the following questions.

1. Which switch is the root of the spanning tree?

2. How can the root switch be identified?

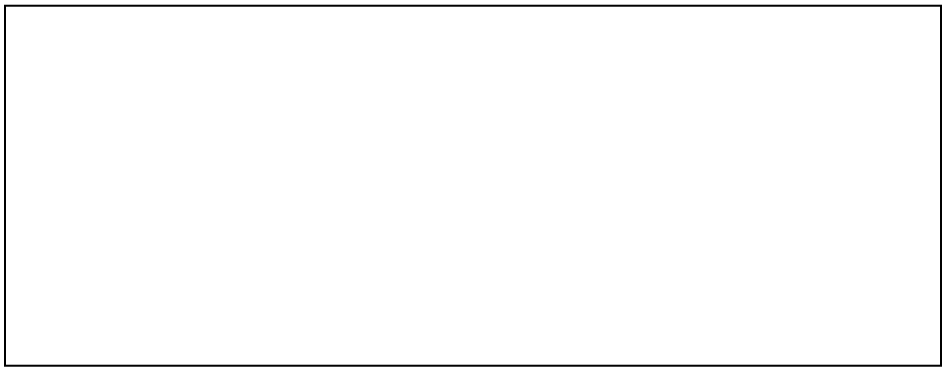
3. Why was that switch selected as the root?

4. What caused one port to be in blocking state over another?

5. What caused one link to be blocked over another?

Step 4

Create a diagram of the spanning tree topology for VLAN 01. With Cisco Catalyst switches, there is a different spanning tree state for each VLAN. Identify the root bridge, root ports, and designated ports.



In this lab, the default operation of spanning tree was observed. Since no bridge priorities were specified, the switch with the lowest MAC address was elected as the root. Since no link priorities were changed, the link with the lowest cost was chosen as the active link. If costs were equal, the tie was broken by the lowest port number.

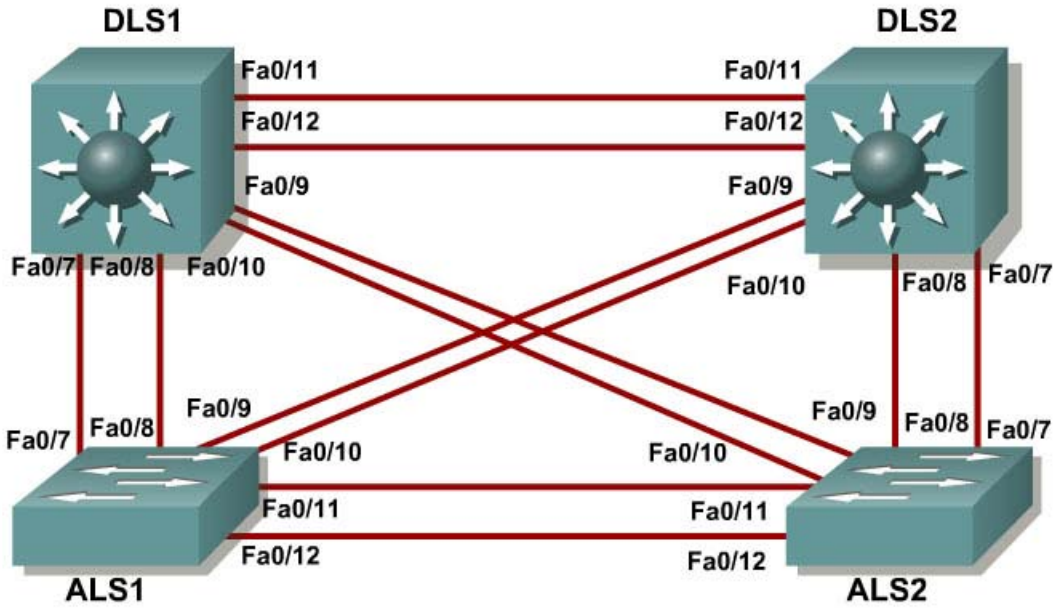
In a later lab, the default STP behavior will be modified so that spanning tree works according to specifications.

Challenge

Try to guess how your topology would look if you completely removed the root switch. Remember that the switch with the lowest MAC address becomes the root.

Now, shut down all the ports on your current root switch. Use the **show spanning-tree** command on the other switches. Did the topology converge the way you thought it would?

Lab 3-2 Modifying Default Spanning Tree Behavior



Objective

The purpose of this lab is to observe what happens when the default spanning tree behavior is modified.

Scenario

Four switches have just been installed. The distribution layer switches are Catalyst 3560s, and the access layer switches are Catalyst 2960s. There are redundant uplinks between the access layer and distribution layer. Because of the possibility of bridging loops, spanning tree logically removes any redundant links. In this lab, you will see what happens when the default spanning tree behavior is modified.

Step 1

Start by deleting vlan.dat, erasing the startup configuration, and reloading your switches. After reloading the switches, give them hostnames. You can find detailed instructions in Lab 2.0.

Step 2

Use the **show spanning-tree** command to check how your non-configured switches created a spanning tree. Verify which switch became the root bridge. In the topology used in this lab, DLS2 is the root bridge.


```
DLS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             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.d780
             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

DLS2#show spanning-tree

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

ALS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             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     0019.0635.5780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
```



```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------------
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
Fa0/11           Desg FWD 19        128.13   P2p
Fa0/12           Desg FWD 19        128.14   P2p

ALS2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             Cost        19
             Port        9 (FastEthernet0/7)
             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
---------------- ---- --- --------- -------- ----------------------------
Fa0/7            Root FWD 19        128.9    P2p
Fa0/8            Altn BLK 19        128.10   P2p
Fa0/9            Altn BLK 19        128.11   P2p
Fa0/10           Altn BLK 19        128.12   P2p
Fa0/11           Altn BLK 19        128.13   P2p
Fa0/12           Altn BLK 19        128.14   P2p
```

Troubleshooting: If you receive the following message:

```
Switch#show spanning-tree

No spanning tree instance exists.
```

Then issue the following commands:

```
Switch#conf t
Switch(config)#interface range FastEthernet 0/1-24
Switch(config-if-range)#no shutdown
Switch(config-if-range)#^Z
Switch#show spanning-tree
```

Now that your switch is communicating with the other switches in the topology, you should receive spanning tree output.

Step 3

Now, we will configure other switches to be the primary root and secondary root. Because DLS2 is the root switch in this topology, we change DLS1 to the primary root and ALS1 to the secondary. Do the same in your topology, regardless of which switch is the initial root. On one of the switches that you are not changing,

you can use the **debug spanning-tree events** command to monitor topology changes. To change the spanning tree root status, use the global configuration commands **spanning-tree vlan** *vlan_number* **root primary** and **spanning-tree vlan** *vlan_number* **root secondary**. On a switch that you are not going to be modifying, put the debug command and then watch the output.

First, debug DLS2:

```
DLS2#debug spanning-tree events
Spanning Tree event debugging is on
```

Then change DLS1 to the primary root:

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#spanning-tree vlan 1 root primary
```

Then change ALS1 to the secondary root:

```
ALS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#spanning-tree vlan 1 root secondary
```

You can see the topology changes on the switch that you enabled debugging on (your output may vary depending on your initial topology):

```
DLS2#
00:10:43: STP: VLAN0001 heard root 24577-000a.b8a9.d780 on Fa0/11
00:10:43:     supersedes 32769-000a.b8a9.d680
00:10:43: STP: VLAN0001 new root is 24577, 000a.b8a9.d780 on port Fa0/11, cost 19
00:10:43: STP: VLAN0001 sent Topology Change Notice on Fa0/11
00:10:43: STP: VLAN0001 Fa0/12 -> blocking
00:10:53: STP: VLAN0001 sent Topology Change Notice on Fa0/11
00:10:53: STP: VLAN0001 Fa0/9 -> blocking
00:10:53: STP: VLAN0001 Fa0/10 -> blocking
```

Notice the timestamps on the debugs to see the difference between changes caused by the commands done in both steps.

If you look at the running configuration for the two switches you made into roots, you see a different command than the one you entered. This is because **spanning-tree vlan** *vlan_number* **root** is a command that sets the priority number on that VLAN automatically rather than typing in a specific priority number. The priority number of a VLAN can be between 0 and 61440 in increments of 4096. If you want to manually set the specific priority number, use the **spanning-tree vlan** *vlan_number* **priority** *priority_number* command.

```
DLS1#show running-config
Building configuration...
!
hostname DLS1
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
ALS1#show running-config
Building configuration...
!
```



```
hostname ALS1
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 28672
```

The command **spanning-tree vlan** *vlan_number* **root primary** sets the priority to 24576 instead of the default (32768). Given this information, would a lower or higher priority number result in a switch becoming the root bridge?

You can also observe the priority modification with the **show spanning-tree** command:

```
DLS1#show span

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000a.b8a9.d780
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
              Address     000a.b8a9.d780
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 15

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
```

Step 4

With spanning tree, you can also modify port priorities to determine which ports are forwarding and which are blocking. To choose which port becomes the root on a non-root switch when faced with redundant root paths, the switch looks at the port priorities first. If the port costs are the same, and the port priorities are the same, the switch picks the port with the lowest port number. On the link between DLS1 and DLS2, the default forwarding port is f0/11 because it is lower, and the default blocking port is f0/12 because it is higher. The two ports have equal costs because they are the same speed. We will look into modifying this later. You can verify this using the **show spanning-tree** command on the non-root switch, which is DLS2.

```
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    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            Altn BLK 19        128.11   P2p
Fa0/10           Altn BLK 19        128.12   P2p
Fa0/11           Root FWD 19        128.13   P2p
Fa0/12           Altn BLK 19        128.14   P2p
```

For comparison, here is **show spanning-tree** on DLS1. Notice that all ports are forwarding because it is the root switch.

```
DLS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000a.b8a9.d780
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     000a.b8a9.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

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
```

Port priorities range from 0 to 240, in increments of 16. The default priority is 128, and a lower priority is preferred. To change port priorities, you change them on the switch closer to the root. If we want to make DLS2 f0/12 the root port, and f0/11 block, we change it on DLS1 with the interface-level command **spanning-tree port-priority** *priority*.

```
DLS1(config)#int f0/12
DLS1(config-if)#spanning-tree port-priority 112
```

Now, look at which port is blocking on DLS2.

```
DLS2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
```



```
  Root ID    Priority    24577
             Address     000a.b8a9.d780
             Cost        19
             Port        14 (FastEthernet0/12)
             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 15

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            Altn BLK 19        128.11   P2p
Fa0/10           Altn BLK 19        128.12   P2p
Fa0/11           Altn BLK 19        128.13   P2p
Fa0/12           Root FWD 19        128.14   P2p
```

Although the root port has changed, the port priorities have not. On DLS1, you can see the port priorities have changed, although all ports are still forwarding (because this is the root switch).

```
DLS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000a.b8a9.d780
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     000a.b8a9.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

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        112.14   P2p
```

Using the above output, how does DLS2 know which port to change to the root port, without changing the port priorities on DLS2?

Step 5

Another feature of spanning tree is portfast. Portfast allows you to bypass the normal phases of spanning tree and move a port to the forwarding state as soon as it is turned on. This is useful when connecting hosts to a switch, because they can start communicating on the VLAN instantly rather than waiting for spanning tree. There is no danger of creating a spanning tree loop because you are not connecting to another switch. A client that runs DHCP as soon as it starts up

benefits, because the DHCP requests could be ignored if the port was not in the correct spanning tree state. Portfast works only on ports in non-trunking mode, and must be used carefully to avoid creating spanning tree loops. To demonstrate the difference portfast makes, use one of your host connections to a switch and put it in access mode. Enable spanning tree debugging with the **debug spanning-tree events** command. Shut down the port using the **shutdown** command. Then turn the port back up using the **no shutdown** command. You see the port go through all the spanning tree stages before going to the forwarding stage.

Here is a demonstration with a host attached to ALS1. The host is attached on port f0/6. Look at what happens when the port is brought up (the port starts in the shutdown state). Set the switchport mode to access. Your output may vary.

```
ALS1#debug spanning-tree events
Spanning Tree event debugging is on

ALS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#interface f0/6
ALS1(config-if)#switchport mode access
ALS1(config-if)#end
ALS1#

22:32:23: set portid: VLAN0001 Fa0/6: new port id 800D
22:32:23: STP: VLAN0001 Fa0/6 -> listening
22:32:25: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to up
22:32:26: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
       changed state to up
22:32:38: STP: VLAN0001 Fa0/6 -> learning
22:32:53: STP: VLAN0001 Fa0/6 -> forwarding
```

Shut down the port again for the next part. Now, activate portfast on that port with the interface-level command **spanning-tree portfast**. The switch warns you about the possibility of creating switching loops.

```
ALS1#configure terminal
ALS1(config)#interface f0/6
ALS1(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 FastEthernet0/6 but will only
 have effect when the interface is in a non-trunking mode.
```

Now, bring up the port by issuing the **no shutdown** command on the interface.

```
ALS1(config-if)#no shutdown

22:43:23: set portid: VLAN0001 Fa0/6: new port id 800D
22:43:23: STP: VLAN0001 Fa0/6 ->jump to forwarding from blocking
22:43:25: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to up
22:43:26: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
       changed state to up
```


You can shut the port down again if you want. Be sure to turn off debugging before continuing:

```
ALS1(config-if)#end
ALS1#
22:55:23: %SYS-5-CONFIG_I: Configured from console by console
ALS1#undebug all
All possible debugging has been turned off
```

Why could enabling portfast on redundant switch access links be a bad idea?

Step 6

Another way of changing which port becomes the root is to modify the port costs using the interface command **spanning-tree cost** *cost*. The default cost for a gigabit Ethernet port is 4, Fast Ethernet is 19, and 10baseT Ethernet is 100. Lower cost is preferred. For this scenario, I am changing the cost of ports f0/11 and 12 on ALS1 and ALS2. First, look at the current port costs using the **show spanning-tree** command:

```
ALS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000a.b8a9.d780
             Cost        19
             Port        9 (FastEthernet0/7)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28673  (priority 28672 sys-id-ext 1)
             Address     0019.0635.5780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/7            Root FWD 19        128.9    P2p
Fa0/8            Altn BLK 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

ALS2#show spanning-tree

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
---------------- ---- --- --------- -------- --------------------------------
Fa0/7            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
Fa0/11           Altn BLK 19        128.13   P2p
Fa0/12           Altn BLK 19        128.14   P2p
```

Now, change the port cost to 10 on both ALS1 and ALS2:

```
ALS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#interface range f0/11 - 12
ALS1(config-if-range)#spanning-tree cost 10
```

Perform the same commands on ALS2. Verify the change with the **show spanning-tree** command:

```
ALS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000a.b8a9.d780
             Cost        19
             Port        9 (FastEthernet0/7)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28673  (priority 28672 sys-id-ext 1)
             Address     0019.0635.5780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

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

ALS2#show spanning-tree

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
---------------- ---- --- --------- -------- ----------------------------
Fa0/7            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
Fa0/11           Altn BLK 10        128.13   P2p
Fa0/12           Altn BLK 10        128.14   P2p
```

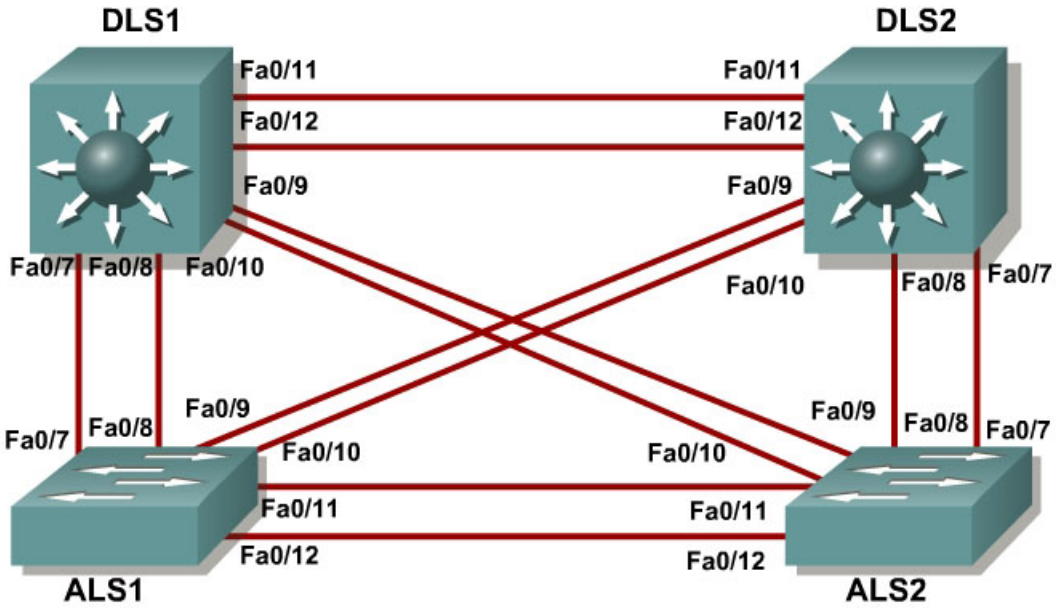
END OF LAB FINAL CONFIGS

```
DLS1#show running-config
!
hostname DLS1
!
!
spanning-tree vlan 1 priority 24576
!
!
interface FastEthernet0/12
 spanning-tree port-priority 112
!
!
end

DLS2#show running-config

!
hostname DLS2
!
!
end

ALS1#show running-config

!
hostname ALS1
!
!
spanning-tree vlan 1 priority 28672
!
!
interface FastEthernet0/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
!
interface FastEthernet0/6
 switchport mode access
 spanning-tree portfast
!
```



```
!
interface FastEthernet0/11
 switchport mode access
 spanning-tree cost 10
!
interface FastEthernet0/12
 spanning-tree cost 10
!
end

ALS2#show running-config

!
hostname ALS2
!

!
interface FastEthernet0/11
 spanning-tree cost 10
!
interface FastEthernet0/12
 spanning-tree cost 10

!
end
```


Lab 3-3 Per-VLAN Spanning Tree Behavior



Objective

The purpose of this lab is to observe what happens when there is a separate spanning tree instance per VLAN. This lab also looks at changing spanning tree mode to rapid spanning tree.

Scenario

Four switches have just been installed. The distribution layer switches are Catalyst 3560s, and the access layer switches are Catalyst 2960s. There are redundant uplinks between the access layer and distribution layer. Because of the possibility of bridging loops, spanning tree logically removes any redundant links. In this lab, you will see what happens when spanning tree is configured differently for different VLANs.

Step 1

Start by deleting the vlan.dat file, erasing the startup config, and reloading all your switches. After reloading the switches, give them hostnames. Configure ports f0/7 through f0/12 to be trunks. On the 3560s, you first need to set the trunk encapsulation to dot1q. On the 2960s, only dot1q is supported, so it does not need to be set, but the mode still needs to be changed to trunk. If you do not set the mode of the ports to trunk, the links do not form trunks and remain access

ports (the default mode on a 3560 or 2960 is dynamic auto; the default mode on a 3550 or 2950 is dynamic desirable).

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#interface range f0/7 - 12
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
```

Step 2

Configure all switches with VTP mode transparent and VTP domain CISCO. Add VLAN 10 and 20 to all of them. Use the **show vlan brief** command to view the VLAN configurations.

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
DLS1(config)#vtp domain CISCO
Changing VTP domain name from NULL to CISCO
DLS1(config)#vlan 10,20
DLS1(config-vlan)#end
DLS1#
00:02:43: %SYS-5-CONFIG_I: Configured from console by console
DLS1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/9, Fa0/10
                                                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
10   VLAN0010                         active
20   VLAN0020                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

If you issue the **show spanning-tree** command on any of the four switches, you notice that instead of just one VLAN coming up, there are multiple VLANs.

```
DLS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             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.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

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


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000a.b8a9.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

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


VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     000a.b8a9.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

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
```

Step 3

You may notice that all the ports have identical spanning tree behavior for each VLAN. This is because all VLANs are running spanning tree with the default behavior. However, we can modify the default spanning tree behavior on a per-VLAN basis. For this lab, we assign DLS1 the root switch for VLAN 10, and DLS2

for VLAN 20. To change the priority for a given VLAN, use the **spanning-tree vlan** *number* **priority** *number* command.

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#spanning-tree vlan 10 priority 4096
```

Configure DLS2 similarly for VLAN 20. If you look at the output of **show spanning-tree** on the four switches, you see that the port states and root switches vary on a per VLAN basis.

```
DLS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             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.d780
             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


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     000a.b8a9.d780
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4106   (priority 4096 sys-id-ext 10)
             Address     000a.b8a9.d780
             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


VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    4116
```



```
              Address     000a.b8a9.d680
              Cost        19
              Port        13 (FastEthernet0/11)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     000a.b8a9.d780
              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

DLS2#show spanning-tree

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


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              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    32778  (priority 32768 sys-id-ext 10)
              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


VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    4116
             Address     000a.b8a9.d680
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4116   (priority 4096 sys-id-ext 20)
             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

ALS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             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     0019.0635.5780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
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
Fa0/11           Desg FWD 19        128.13   P2p
Fa0/12           Desg FWD 19        128.14   P2p


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     000a.b8a9.d780
             Cost        19
             Port        9 (FastEthernet0/7)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0019.0635.5780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
```



```
---------------- ---- --- --------- -------- ----------------------------
Fa0/7            Root FWD 19        128.9    P2p
Fa0/8            Altn BLK 19        128.10   P2p
Fa0/9            Altn BLK 19        128.11   P2p
Fa0/10           Altn BLK 19        128.12   P2p
Fa0/11           Desg FWD 19        128.13   P2p
Fa0/12           Desg FWD 19        128.14   P2p


VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    4116
             Address     000a.b8a9.d680
             Cost        19
             Port        11 (FastEthernet0/9)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0019.0635.5780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------------
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
Fa0/11           Desg FWD 19        128.13   P2p
Fa0/12           Desg FWD 19        128.14   P2p

ALS2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             Cost        19
             Port        9 (FastEthernet0/7)
             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
---------------- ---- --- --------- -------- ----------------------------
Fa0/7            Root FWD 19        128.9    P2p
Fa0/8            Altn BLK 19        128.10   P2p
Fa0/9            Altn BLK 19        128.11   P2p
Fa0/10           Altn BLK 19        128.12   P2p
Fa0/11           Altn BLK 19        128.13   P2p
Fa0/12           Altn BLK 19        128.14   P2p


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             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    32778  (priority 32768 sys-id-ext 10)
             Address     0019.068d.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
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
Fa0/11           Altn BLK 19        128.13   P2p
Fa0/12           Altn BLK 19        128.14   P2p


VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    4116
             Address     000a.b8a9.d680
             Cost        19
             Port        9 (FastEthernet0/7)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0019.068d.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

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

Step 4

Other spanning tree modes besides regular PVST (per-VLAN spanning tree) are available. One of these modes is RSTP (rapid spanning tree protocol), which greatly reduces the time between a port coming up and changing to forwarding while still preventing bridging loops. To change the spanning tree mode to rapid spanning tree, use the global configuration command **spanning-tree mode rapid-pvst**. Configure this on all four switches. During the transition period, rapid spanning tree falls back to regular spanning tree on the links that have regular spanning tree on one side.

```
DLS1(config)#spanning-tree mode rapid-pvst
```

After configuring all four switches with this command, use the **show spanning-tree** command to verify the configuration:

```
DLS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     000a.b8a9.d680
```



```
              Cost        19
              Port        13 (FastEthernet0/11)
              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.d780
              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 BLK 19        128.9    P2p
Fa0/8            Desg BLK 19        128.10   P2p
Fa0/9            Desg BLK 19        128.11   P2p
Fa0/10           Desg BLK 19        128.12   P2p
Fa0/11           Root FWD 19        128.13   P2p
Fa0/12           Altn BLK 19        128.14   P2p


VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    4106
              Address     000a.b8a9.d780
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4106   (priority 4096 sys-id-ext 10)
              Address     000a.b8a9.d780
              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


VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    4116
              Address     000a.b8a9.d680
              Cost        19
              Port        13 (FastEthernet0/11)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
              Address     000a.b8a9.d780
              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 BLK 19        128.9    P2p
Fa0/8            Desg BLK 19        128.10   P2p
Fa0/9            Desg BLK 19        128.11   P2p
Fa0/10           Desg BLK 19        128.12   P2p
Fa0/11           Root FWD 19        128.13   P2p
Fa0/12           Altn BLK 19        128.14   P2p
```


Challenge

1. On each switch, add VLANs 50, 60, 70, 80, 90, and 100. Configure ALS1 to be the root of VLANs 50, 60, and 70, and ALS2 to be the root of VLANs 80, 90, and 100. Configure the roots with a single line on each switch.

HINT: Use the question mark when you type the global configuration command **spanning-tree vlan ?**. Notice that you can modify spanning tree attributes in ranges.

2. Change the spanning tree cost of VLAN 20 on f0/11 and f0/12 between DLS1 and DLS2 to 15.

HINT: Use the question mark on the interface level command **spanning-tree vlan *number* ?**.

END OF LAB FINAL CONFIGS:

```
DLS1#show running-config
!
hostname DLS1
!
!
vtp domain CISCO
vtp mode transparent
!
!
!
!
spanning-tree vlan 10 priority 4096
!
!
vlan 10,20,50,60,70,80,90,100
!
!
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```



```
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree vlan 20 cost 15
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree vlan 20 cost 15
!

!
end
```

```
DLS2#show running-config
!
hostname DLS2
!
!
vtp domain CISCO
vtp mode transparent
!
!
!
!
spanning-tree vlan 20 priority 4096
!
!
vlan 10,20,50,60,70,80,90,100
!

!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree vlan 20 cost 15
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree vlan 20 cost 15
```

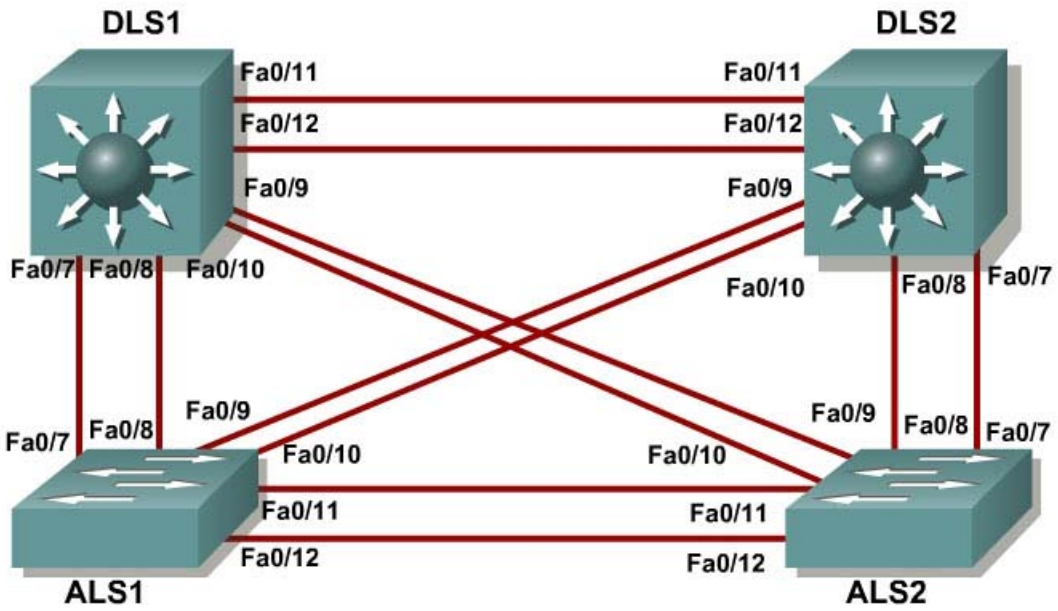


```
!

!
end

ALS1#show running-config
!
hostname ALS1
!
!
vtp domain CISCO
vtp mode transparent
!
!
!
spanning-tree vlan 50-70 priority 24576
!
!
vlan 10,20,50,60,70,80,90,100
!

!
interface FastEthernet0/7
 switchport mode trunk
!
interface FastEthernet0/8
 switchport mode trunk
!
interface FastEthernet0/9
 switchport mode trunk
!
interface FastEthernet0/10
 switchport mode trunk
!
interface FastEthernet0/11
 switchport mode trunk
!
interface FastEthernet0/12
 switchport mode trunk
!

!
end

ALS2#show running-config
!
hostname ALS2
!
!
vtp domain CISCO
vtp mode transparent
!
!
!
!
spanning-tree vlan 80,90,100 priority 24576
!
!
vlan 10,20,50,60,70,80,90,100
!

!
interface FastEthernet0/7
```



```
 switchport mode trunk
!
interface FastEthernet0/8
 switchport mode trunk
!
interface FastEthernet0/9
 switchport mode trunk
!
interface FastEthernet0/10
 switchport mode trunk
!
interface FastEthernet0/11
 switchport mode trunk
!
interface FastEthernet0/12
 switchport mode trunk
!

!
end
```


Lab 3-4 Multiple Spanning Tree



Objective

The purpose of this lab is to observe the behavior of MST (multiple spanning tree).

Scenario

Four switches have just been installed. The distribution layer switches are Catalyst 3560s, and the access layer switches are Catalyst 2960s. There are redundant uplinks between the access layer and distribution layer. Because of the possibility of bridging loops, spanning tree logically removes any redundant links. In this lab, we will group VLANs using MST so that we can have less spanning tree instances running at once to save switch CPU load.

Step 1

Start by deleting vlan.dat, erasing the startup configuration, and reloading your switches. After reloading the switches, give them hostnames. Configure ports f0/7 through f0/12 to be trunks. On the 3560s, you first need to set the trunk encapsulation to dot1q. On the 2960s, only dot1q is supported, so it does not need to be set, but the mode still needs to be changed to trunk. If you do not set the mode of the ports to be trunk, the links do not form trunks and remain access

ports (default mode on a 3560 or 2960 is dynamic auto; default mode on a 3550 or 2950 is dynamic desirable).

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#interface range f0/7 - 12
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
```

Step 2

Configure all switches with VTP mode transparent and VTP domain CISCO. Add VLANs 10, 20, 30, 40, 50, 60, 70, 80, 90 and 100 to all of them. Use the **show vlan brief** command to view the VLAN configurations.

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
DLS1(config)#vtp domain CISCO
Changing VTP domain name from NULL to CISCO
DLS1(config)#vlan 10,20,30,40,50,60,70,80,90,100
DLS1(config-vlan)#end
DLS1#show vlan brief
00:11:56: %SYS-5-CONFIG_I: Configured from console by console

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                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
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
50   VLAN0050                         active
60   VLAN0060                         active
70   VLAN0070                         active
80   VLAN0080                         active
90   VLAN0090                         active
100  VLAN0100                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Step 3

If you issue the **show spanning-tree** command on one of the switches, you see 11 spanning tree instances running.

```
DLS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             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.d780
             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


VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     000a.b8a9.d780
             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


VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     000a.b8a9.d780
             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

<output omitted>
```



```
VLAN0090
  Spanning tree enabled protocol ieee
  Root ID    Priority    32858
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32858  (priority 32768 sys-id-ext 90)
             Address     000a.b8a9.d780
             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    32868
             Address     000a.b8a9.d680
             Cost        19
             Port        13 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32868  (priority 32768 sys-id-ext 100)
             Address     000a.b8a9.d780
             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
```

Spanning tree is running a separate spanning tree instance for each VLAN we created, plus VLAN 1. This method assumes that each VLAN could be running on a differently shaped topology. However, in many networks, multiple VLANs follow the same physical topology, so multiple spanning-tree calculations for the same topologies can get redundant. MST (multiple spanning tree) lets you configure different spanning tree instances. Each instance can hold a group of VLANs and gets its own spanning tree calculation.

MST is convenient in that it is backward compatible with PVST. Two switches only run MST with each other if they are in the same MST region. An MST region is defined by switches having identical region names, revision numbers, and VLAN-to-instance assignments. If they differ by any single attribute, they are considered different MST regions and fall back to PVST.

Step 4

To configure MST, first use the global configuration command **spanning-tree mode mst** on all four switches.

```
DLS1(config)#spanning-tree mode mst
```

By default, all VLANs are assigned to instance 0, but can be moved around to different instances when MST is configured. Issue the **show spanning-tree** command and observe that there is only one spanning tree (instance 0) coming up. Also notice that the mode is listed as MSTP.

```
DLS1#show spanning-tree

MST00
  Spanning tree enabled protocol mstp
  Root ID    Priority    32768
             Address     000a.b8a9.d680
             Cost        0
             Port        13 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     000a.b8a9.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/7            Desg FWD 200000    128.9    P2p
Fa0/8            Desg BLK 200000    128.10   P2p
Fa0/9            Desg FWD 200000    128.11   P2p
Fa0/10           Desg FWD 200000    128.12   P2p
Fa0/11           Root FWD 200000    128.13   P2p
Fa0/12           Altn BLK 200000    128.14   P2p
```

If you use the **show spanning-tree mst configuration** command, you can see a switch's current MST configuration. Because you have not configured any MST region settings, the switch shows the default settings.

```
DLS1#show spanning-tree mst configuration
Name      []
Revision  0
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
---------------------------------------------------------------------------
```

Step 5

Now that MST has been enabled, we can configure the MST region settings to group VLANs. We use the region name CISCO and a revision number of 1. We put VLANs 20 through 50 into instance 1, and 80 and 100 into instance 2. The rest of the VLANs remain in instance 0, the default. To begin modifying the MST configuration, type the global configuration command **spanning-tree mst configuration**. Configuring MST is different from other switch configurations,

because changes are not applied until you are done, and you can abort changes if you want to.

Note: You must apply identical configurations on each switch for MST to work properly.

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#spanning-tree mst configuration
DLS1(config-mst)#
```

When you are in MST configuration mode, you can view the current configuration using the **show current** command. You do not need to leave configuration mode to execute this command. Notice that the output is identical to **show spanning-tree mst configuration**.

```
DLS1(config-mst)#show current
Current MST configuration
Name      []
Revision  0
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
---------------------------------------------------------------------------
```

Change the region name by typing **name** *name*. Change the revision number by typing **revision** *number*.

```
DLS1(config-mst)#name CISCO
DLS1(config-mst)#revision 1
```

The last configuration change you have to make is putting VLANs into instances. Use the command **instance** *number* **vlan** *vlan_range*. The instance number can be between 0 and 15. Remember that 0 is the default instance number.

```
DLS1(config-mst)# instance 1 vlan 20-50
DLS1(config-mst)# instance 2 vlan 80, 100
```

You can verify the changes you are about to make with the **show pending** command. Remember that the changes that you just entered are not committed until you type **exit**. If you do not like the changes you made, you can leave the prompt without committing them by typing **abort**. In the output below, notice the difference between **show current** and **show pending**.

```
DLS1(config-mst)#show current
Current MST configuration
Name      []
Revision  0
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
---------------------------------------------------------------------------

DLS1(config-mst)#show pending
Pending MST configuration
Name      [CISCO]
```



```
Revision  1
Instance  Vlans mapped
--------  ---------------------------------------------------------------
0         1-19,51-79,81-99,101-4094
1         20-50
2         80,100
-------------------------------------------------------------------------

DLS1(config-mst)#exit
```

If you enter the **show spanning-tree mst configuration** command, you can see that the current configuration reflects the changes you just committed. Remember to perform the same configuration on all four switches.

```
DLS1#show span mst configuration
Name      [CISCO]
Revision  1
Instance  Vlans mapped
--------  ---------------------------------------------------------------
0         1-19,51-79,81-99,101-4094
1         20-50
2         80,100
-------------------------------------------------------------------------
```

Why do the switches wait until you are finished making changes to MST to commit them, rather that changing MST as you enter commands (like most switch commands)?

Verify that you have separate instances of spanning tree running for each MST instance:

```
DLS1#show spanning-tree

MST00
  Spanning tree enabled protocol mstp
  Root ID    Priority    32768
             Address     000a.b8a9.d680
             Cost        0
             Port        13 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     000a.b8a9.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/7            Desg FWD 200000    128.9    P2p
Fa0/8            Desg FWD 200000    128.10   P2p
Fa0/9            Desg FWD 200000    128.11   P2p
Fa0/10           Desg FWD 200000    128.12   P2p
Fa0/11           Root FWD 200000    128.13   P2p
Fa0/12           Altn BLK 200000    128.14   P2p
```



```
MST01
  Spanning tree enabled protocol mstp
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             Cost        200000
             Port        13 (FastEthernet0/11)
             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.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/7            Desg FWD 200000    128.9    P2p
Fa0/8            Desg FWD 200000    128.10   P2p
Fa0/9            Desg FWD 200000    128.11   P2p
Fa0/10           Desg FWD 200000    128.12   P2p
Fa0/11           Root FWD 200000    128.13   P2p
Fa0/12           Altn BLK 200000    128.14   P2p


MST02
  Spanning tree enabled protocol mstp
  Root ID    Priority    32770
             Address     000a.b8a9.d680
             Cost        200000
             Port        13 (FastEthernet0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32770  (priority 32768 sys-id-ext 2)
             Address     000a.b8a9.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/7            Desg FWD 200000    128.9    P2p
Fa0/8            Desg FWD 200000    128.10   P2p
Fa0/9            Desg FWD 200000    128.11   P2p
Fa0/10           Desg FWD 200000    128.12   P2p
Fa0/11           Root FWD 200000    128.13   P2p
Fa0/12           Altn BLK 200000    128.14   P2p
```

Challenge

You can modify per-instance MST spanning tree attributes the same way you can modify per-VLAN attributes. Make DLS1 the root of instance 1 and DLS2 the root of instance 2.

HINT: Use a question mark on the global configuration command **spanning-tree mst ?**.

END OF LAB FINAL CONFIGS:

```
DLS1#show running-config
!
hostname DLS1
!
!
vtp domain CISCO
vtp mode transparent
!
!
!
!
!
spanning-tree mst configuration
 name CISCO
 revision 1
 instance 1 vlan 20-50
 instance 2 vlan 80, 100
!
spanning-tree mst 1 priority 24576
!
!
vlan 10,20,30,40,50,60,70,80,90,100
!
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
!
end



DLS2#show running-config
!
hostname DLS2
!
!
vtp domain CISCO
```



```
vtp mode transparent
!
!
spanning-tree mode mst
!
spanning-tree mst configuration
 name CISCO
 revision 1
 instance 1 vlan 20-50
 instance 2 vlan 80, 100
!
spanning-tree mst 2 priority 24576
!
!
vlan 10,20,30,40,50,60,70,80,90,100
!
!
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
!
end



ALS1#show running-config
!
hostname ALS1
!
!
vtp domain CISCO
vtp mode transparent
!
!
spanning-tree mode mst
!
spanning-tree mst configuration
 name CISCO
 revision 1
 instance 1 vlan 20-50
 instance 2 vlan 80, 100
```



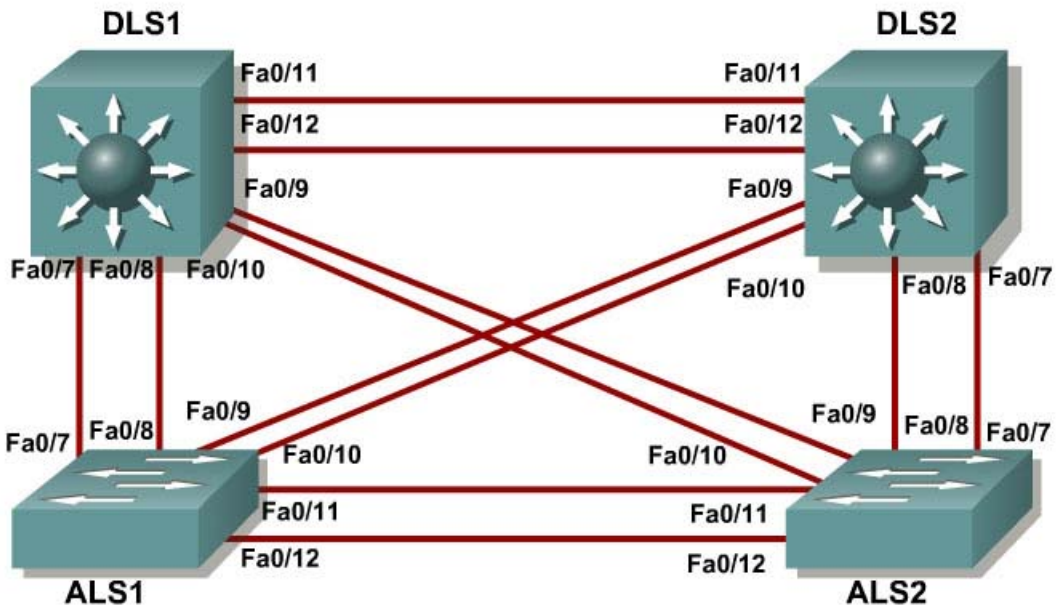
```
!
!
vlan 10,20,30,40,50,60,70,80,90,100
!
!
interface FastEthernet0/7
 switchport mode trunk
!
interface FastEthernet0/8
 switchport mode trunk
!
interface FastEthernet0/9
 switchport mode trunk
!
interface FastEthernet0/10
 switchport mode trunk
!
interface FastEthernet0/11
 switchport mode trunk
!
interface FastEthernet0/12
 switchport mode trunk
!
!
end
```

```
ALS2#show running-config
!
hostname ALS2
!
!
vtp domain CISCO
vtp mode transparent
!
!
spanning-tree mode mst
!
spanning-tree mst configuration
 name CISCO
 revision 1
 instance 1 vlan 20-50
 instance 2 vlan 80, 100
!
!
vlan 10,20,30,40,50,60,70,80,90,100
!
!
interface FastEthernet0/7
 switchport mode trunk
!
interface FastEthernet0/8
 switchport mode trunk
!
interface FastEthernet0/9
 switchport mode trunk
!
interface FastEthernet0/10
 switchport mode trunk
!
interface FastEthernet0/11
```



```
 switchport mode trunk
!
interface FastEthernet0/12
 switchport mode trunk
!
!
end
```


Lab 3-5 Configuring Etherchannel



Objective

The purpose of this lab is to configure and observe Etherchannel.

Scenario

Four switches have just been installed. The distribution layer switches are Catalyst 3560s, and the access layer switches are Catalyst 2960s. There are redundant uplinks between the access layer and distribution layer. Usually, only one of these links could be used, or a bridging loop might occur. However, this utilizes only half of the available bandwidth. Etherchannel allows up to eight redundant links to be bundled together into one logical link.

Step 1

Start by deleting vlan.dat, erasing the startup configuration, and reloading all your switches. After reloading the switches, give them hostnames. Configure ports f0/7 through f0/12 to be trunks. On the 3560s, you first need to set the trunk encapsulation to dot1q. On the 2960s, only dot1q is supported, so it does not need to be set, but the mode still needs to be changed to trunk. If you do not set the mode of the ports to trunk, the links do not form trunks and remain access ports (default mode on a 3560 or 2960 is dynamic auto; default mode on a 3550 or 2950 is dynamic desirable).

```
DLS1#configure terminal
```



```
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#interface range f0/7 - 12
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
```

Step 2

The first Etherchannel we create for this lab is aggregating ports f0/11 and f0/12 between ALS1 and ALS2. First, make sure that you have a trunk link active for those two links with the **show interfaces trunk** command.

```
ALS1#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

<output ommitted>
```

On both switches, add ports 11 and 12 to port-channel 1 with the **channel-group 1 mode desirable** command, where **mode desirable** indicates that you want the switch to actively negotiate to form a PAgP link. PAgP is an Etherchannel protocol.

```
ALS1(config)#interface range f0/11 - 12
ALS1(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
```

Now, you can configure the logical interface to become a trunk by first entering the **interface port-channel** *number* command, and then the **switchport mode trunk** command. Do this configuration on both switches.

```
ALS1(config)#interface port-channel 1
ALS1(config-if)#switchport mode trunk
```

Verify that Etherchannel is working by issuing the **show etherchannel summary** command on both switches. This command displays the type of Etherchannel, the ports utilized, and port states.

```
ALS1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```



```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         PAgP      Fa0/11(P)   Fa0/12(P)

ALS2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         PAgP      Fa0/11(P)   Fa0/12(P)
```

If the Etherchannel does not come up, you may want to try “flapping” the physical interfaces involved in the Etherchannel on both ends. This involves using the **shut** command followed by a **no shut** command a few seconds later on those interfaces.

The commands **show interfaces trunk** and **show spanning-tree** also show the port-channel as one logical link.

```
ALS1#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
Po1         on           802.1q         trunking      1

<output ommitted>

ALS1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.b8a9.d680
             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     0019.0635.5780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

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



```
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
Po1              Desg FWD 12        128.72   P2p
```

Step 3

Using the commands you have learned above, configure the link between DLS1 and ALS1 on ports f0/7 and f0/8 to be a LACP Etherchannel. You must use a different port-channel number on ALS1 than 1, because you already used that in the previous step. To configure a port-channel to be LACP, use the interface-level command **channel-group** *number* **mode active**. Active mode indicates that the switch actively tries to negotiate that link to be LACP (as opposed to PAgP).

```
ALS1(config)#interface range f0/7 - 8
ALS1(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
ALS1(config-if-range)#interface port-channel 2
ALS1(config-if)#switchport mode trunk
```

Apply a similar configuration on DLS1. Verify the configuration with the **show etherchannel summary** command.

```
ALS1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         PAgP      Fa0/11(P)   Fa0/12(P)
2      Po2(SU)         LACP      Fa0/7(P)    Fa0/8(P)
```

Step 4

In the previous steps, we configured Etherchannels as Layer 2 trunk connections between switches. We can also configure Etherchannels as Layer 3 (routed) connections on switches that can support it. Since DLS1 and DLS2 are both multilayer switches, they can support routed ports. Use the **no switchport** command on f0/11 and f0/12 to make them Layer 3 ports. Next, add them to the channel group with the **channel-group** *number* **mode desirable** command. Then, on the logical interface, type **no switchport** to make it a Layer 3 port. Add the IP address 10.0.0.1 for DLS1 and 10.0.0.2 for DLS2. Configure both with a /24 subnet mask.

```
DLS1(config)#interface range f0/11 - 12
```



```
DLS1(config-if-range)#no switchport
DLS1(config-if-range)#channel-group 3 mode desirable
Creating a port-channel interface Port-channel 3
DLS1(config-if-range)#interface port-channel 3
DLS1(config-if)#no switchport
DLS1(config-if)#ip address 10.0.0.1 255.255.255.0
```

Verify that you have Layer 3 connectivity by attempting to ping the other side of the link:

```
DLS1#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

If you look at the output of **show etherchannel summary**, you see that it lists the port channel as a routed port, not a switched port. RU in the parentheses next to the name means routed and up, as opposed to switched and up.

```
DLS1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
2      Po2(SU)         LACP      Fa0/7(P)    Fa0/8(P)
3      Po3(RU)         PAgP      Fa0/11(P)   Fa0/12(P)
```

Step 5

The switches can use different methods to load balance traffic going through a port channel. By default, they load balance using the source MAC address. You can view the current load-balancing configuration with the **show etherchannel load-balance** command:

```
DLS1#show etherchannel load-balance
EtherChannel Load-Balancing Operational State (src-mac):
Non-IP: Source MAC address
  IPv4: Source MAC address
  IPv6: Source IP address
```

Other methods of load balancing are based on the destination MAC address, both source and destination MAC addresses, source IP address, destination IP address, and both source and destination IP addresses. For this scenario, we

configure ALS1 to load balance by both source and destination MAC address using the global configuration command **port-channel load-balance** *method*, where the method is src-dst-mac.

```
ALS1(config)#port-channel load-balance src-dst-mac
```

Verify the configuration with the **show etherchannel load-balance** command:

```
ALS1#show etherchannel load-balance
EtherChannel Load-Balancing Operational State (src-dst-mac):
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination MAC address
  IPv6: Source XOR Destination IP address
```

Challenge

The topology still has redundant links that you can aggregate. Experiment with the other port-channel modes using the question mark on the interface-level command **channel-group** *number* **mode ?**. Look at the descriptions and implement some port channels in different manners. If you decide to use the “on” mode, you may want to take a look at the interface command **channel-protocol ?**. This mode statically sets the Etherchannel protocol without negotiation.

END OF LAB FINAL CONFIGS

```
DLS1#show running-config
!
hostname DLS1
!
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 no switchport
 ip address 10.0.0.1 255.255.255.0
!
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/11
 no switchport
 no ip address
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 no switchport
 no ip address
 channel-group 3 mode desirable
!
!
end

DLS2#show running-config
!
hostname DLS2
!
!
!
interface Port-channel3
 no switchport
 ip address 10.0.0.2 255.255.255.0
!
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
```



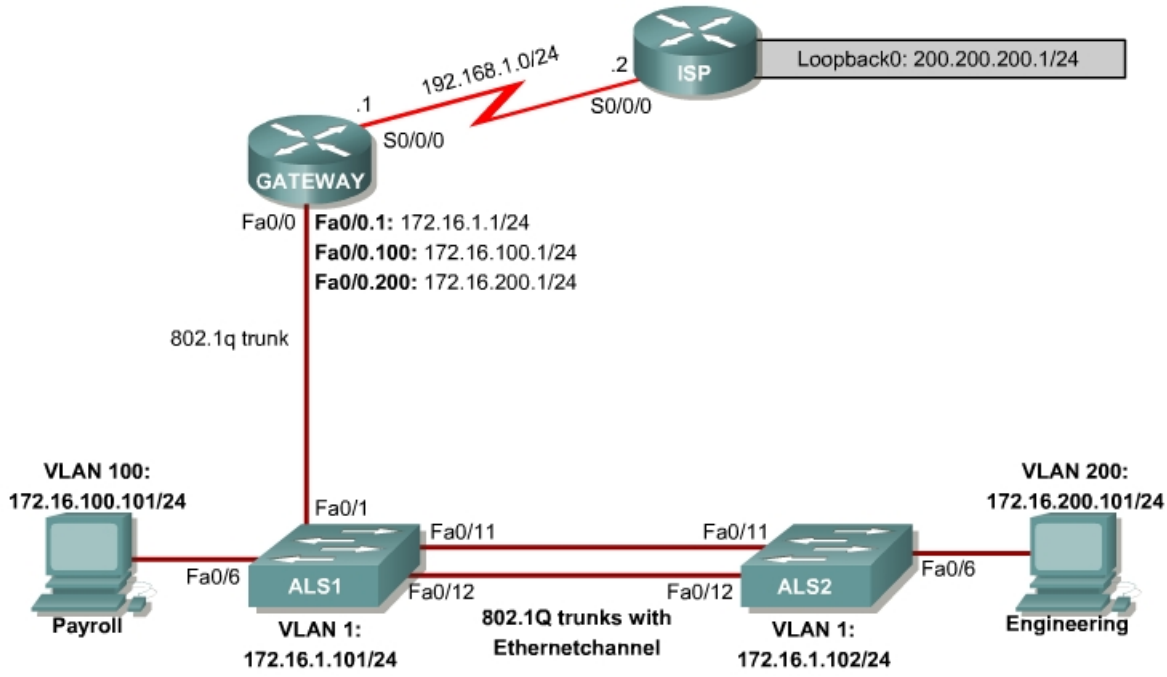
```
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/11
 no switchport
 no ip address
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 no switchport
 no ip address
 channel-group 3 mode desirable
!
!
end

ALS1#show running-config

!
hostname ALS1
!
!
port-channel load-balance src-dst-mac
!
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
!
interface FastEthernet0/7
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/8
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/9
 switchport mode trunk
!
interface FastEthernet0/10
 switchport mode trunk
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
 channel-group 1 mode desirable
!
```



```
!
end

ALS2#show running-config
!
hostname ALS2
!
!
interface Port-channel1
 switchport mode trunk
!
!
interface FastEthernet0/7
 switchport mode trunk
!
interface FastEthernet0/8
 switchport mode trunk
!
interface FastEthernet0/9
 switchport mode trunk
!
interface FastEthernet0/10
 switchport mode trunk
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
 channel-group 1 mode desirable
!
!
end
```


Lab 4-1 Inter-VLAN Routing with an External Router

Topology Diagram



Objective

This lab configures inter-VLAN routing using an external router, also known as a router-on-a-stick.

Scenario

Inter-VLAN routing using an external router can be a cost-effective solution when it is necessary to segment a network into multiple broadcast domains. In this scenario, we are splitting an existing network into two separate VLANs on the access layer switches, and using an external router to route between the VLANs. We are using a 802.1q trunk between the switch and the Fast Ethernet interface of the router for routing and management. Static routes are used between the gateway router and the ISP router.

Step 1

Power up the switches and use the standard process for establishing a HyperTerminal console connection from a workstation to each switch in your pod.

Remove all VLAN information and configurations that were previously entered into your switches. (Refer to Lab 2.0a or 2.0b if needed.)

Step 2

Configure the ISP router for communication with your Gateway router. The static route used for the internal networks provides a path for the local network from the ISP. In addition, configure a loopback interface on the ISP router to simulate an external network.

```
Router(config)# hostname ISP
ISP(config)# interface Loopback0
ISP(config-if)# ip address 200.200.200.1 255.255.255.0
ISP(config-if)# interface Serial0/0
ISP(config-if)# ip address 192.168.1.1 255.255.255.0
ISP(config-if)# clockrate 56000
ISP(config-if)# no shutdown
ISP(config-if)# exit
ISP(config)# ip route 172.16.0.0 255.255.0.0 192.168.1.2
```

Configure the Gateway router to communicate with the ISP router. Notice the use of a default static route here. The default route tells the router to send any unknown traffic within the network to the ISP router.

```
Router(config)# hostname Gateway
Gateway(config)# interface Serial0/0
Gateway(config-if)# ip address 192.168.1.2 255.255.255.0
Gateway(config-if)# no shutdown
Gateway(config-if)# exit
Gateway(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

1. Verify connectivity from the Gateway router using the **ping** command. Was this ping successful?

Step 3

To differentiate between the devices, name the two access layer switches using the **hostname** command. Configure the IP addresses on the management VLAN according to the diagram. By default, VLAN 1 is used as the management VLAN. Create a default gateway on both access layer switches using the **ip default-gateway** *ip_address* command. Set an enable secret password and configure the VTY lines for Telnet access to the switch.

The following is a sample configuration for the 2960 switch ALS1:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname ALS1
ALS1(config)# interface vlan 1
ALS1(config-if)# ip address 172.16.1.101 255.255.255.0
```



```
ALS1(config-if)# no shutdown
ALS1(config-if)# exit
ALS1(config)# ip default-gateway 172.16.1.1
ALS1(config)# enable secret cisco
ALS1(config)# line vty 0 15
ALS1(config-line)# password cisco
ALS1(config-line)# login
ALS1(config-line)# end
```

The following is a sample configuration for the 2960 switch ALS2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname ALS2
ALS2(config)# interface vlan 1
ALS2(config-if)# ip address 172.16.1.102 255.255.255.0
ALS2(config-if)# no shutdown
ALS2(config-if)# exit
ALS2(config)# ip default-gateway 172.16.1.1
ALS2(config)# enable secret cisco
ALS2(config)# line vty 0 15
ALS2(config-line)# password cisco
ALS2(config-line)# login
ALS2(config-line)# end
```

2. By default, how many lines are available for telnet on the access switches?

Step 4

Verify that the only existing VLANs are the defaults. Issue the **show vlan** command from privileged mode on both access layer switches.

```
ALS1# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                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
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
```



```
Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------
```

3. Which VLAN is the default management VLAN for Ethernet? What types of traffic are carried on this VLAN?

Step 5

Configure the access layer switches for trunking and Etherchannel.

Use the FastEthernet 0/11 and 0/12 ports of ALS1 and ALS2 to create an Etherchannel trunk between the switches.

Enter the following commands for ALS1:

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface range fastethernet 0/11 - 12
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 1 mode desirable
ALS1(config-if-range)# end
```

Enter the following commands for ALS2:

```
ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# interface range fastethernet 0/11 - 12
ALS2(config-if-range)# switchport mode trunk
ALS2(config-if-range)# channel-group 1 mode desirable
ALS2(config-if-range)# end
```

Verify the Etherchannel configuration using the **show etherchannel** command:

```
ALS1# show etherchannel 1 summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Fa0/11(P)   Fa0/12(P)
```


Step 6

Set up the VTP domain for the access layer switches in global configuration mode.

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# vtp domain SWLAB
Changing VTP domain name from NULL to SWLAB
ALS1(config)# end
```

Verify that ALS2 has learned of the new VTP domain using the **show vtp status** command on ALS2.

Step 7

Configure the switch access ports for the hosts according to the diagram. Statically set switchport mode to access, and use Spanning Tree Portfast on the interfaces. Assign the host attached to ALS1 FastEthernet 0/6 to VLAN 100, and the host attached to ALS2 FastEthernet 0/6 to VLAN 200.

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface fastEthernet 0/6
ALS1(config-if)# switchport mode access
ALS1(config-if)# switchport access vlan 100
% Access VLAN does not exist. Creating vlan 100
ALS1(config-if)# end

ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# interface fastEthernet 0/6
ALS2(config-if)# switchport mode access
ALS2(config-if)# switchport access vlan 200
% Access VLAN does not exist. Creating vlan 200
ALS2(config-if)# end
```

Use the **show vlan** command to verify that both access layer switches have VLAN 100 and VLAN 200.

Step 8

Configure the switch for trunking with the external router's Fast Ethernet interface according to the diagram.

The following is a sample for ALS1 port FastEthernet 0/1. This port connects to FastEthernet 0/1 of the Gateway router.

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface fastEthernet 0/1
ALS1(config-if)# switchport mode trunk
ALS1(config-if)# end
```


Step 9

Configure the Gateway router's Fast Ethernet interface for trunking for VLANs 1, 100, and 200.

The native VLAN cannot be configured on a subinterface for Cisco IOS releases that are earlier than 12.1(3)T. The native VLAN IP address must be configured on the physical interface. Other VLAN traffic is configured on subinterfaces. Cisco IOS releases 12.1(3)T and later support native VLAN configuration on a subinterface with the **encapsulation** {**dot1q** | **isl**} **native** command. This technique is used in the lab configuration.

Create a subinterface for each VLAN. Enable each subinterface with the proper trunking protocol and configure it for a particular VLAN with the **encapsulation** command.

Assign an IP address to each subinterface, which hosts on the VLAN can use as their default gateway.

The following is a sample configuration for the FastEthernet 0/0 interface:

```
Gateway# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway(config)# interface FastEthernet 0/0
Gateway(config-if)# no shut
```

The following is a sample configuration for the VLAN 1 subinterface:

```
Gateway(config)# interface fastethernet 0/0.1
Gateway(config-subif)# description Management VLAN 1
Gateway(config-subif)# encapsulation dot1q 1 native
Gateway(config-subif)# ip address 172.16.1.1 255.255.255.0
```

The following is a sample configuration for the VLAN 100 subinterface:

```
Gateway(config-subif)# interface fastethernet 0/0.100
Gateway(config-subif)# description Payroll VLAN 100
Gateway(config-subif)# encapsulation dot1q 100
Gateway(config-subif)# ip address 172.16.100.1 255.255.255.0
```

The following is a sample configuration for the VLAN 200 subinterface:

```
Gateway(config-subif)# interface fastethernet 0/0.200
Gateway(config-subif)# description Engineering VLAN 200
Gateway(config-subif)# encapsulation dot1q 200
Gateway(config-subif)# ip address 172.16.200.1 255.255.255.0
Gateway(config-subif)# end
```

Use the **show ip interface brief** command to verify the interface configuration and status:

```
Gateway# show ip interface brief
Interface            IP-Address      OK? Method Status                Protocol
FastEthernet0/0      unassigned      YES unset  administratively down down
```



```
FastEthernet0/1      unassigned      YES unset  up                    up
FastEthernet0/1.1    172.16.1.1      YES manual up                    up
FastEthernet0/1.100  172.16.100.1    YES manual up                    up
FastEthernet0/1.200  172.16.200.1    YES manual up                    up
Serial0/0/0          192.168.1.2     YES manual up                    up
Serial0/0/1          unassigned      YES unset  administratively down down
```

Use the **show vlan** command on the Gateway router:

```
Gateway# show vlan

Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/1.1

 This is configured as native Vlan for the following interface(s) :
FastEthernet0/1

   Protocols Configured:   Address:              Received:        Transmitted:
           IP              172.16.1.1                 198                 54
        Other                                           0                 29

   277 packets, 91551 bytes input
   83 packets, 15446 bytes output

Virtual LAN ID:  100 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/1.100

   Protocols Configured:   Address:              Received:        Transmitted:
           IP              172.16.100.1               0                   25

   0 packets, 0 bytes input
   25 packets, 2350 bytes output

Virtual LAN ID:  200 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/1.200

   Protocols Configured:   Address:              Received:        Transmitted:
           IP              172.16.200.1               0                   25

   0 packets, 0 bytes input
   25 packets, 2350 bytes output
```

Use the **show cdp neighbor detail** command on the Gateway router to verify that ALS1 is a neighbor. Telnet to the IP address given in the CDP information.

4. Was the telnet successful?

Step 10

Verify inter-VLAN routing on the Gateway router and the host devices.

5. Ping to the 200.200.200.1 ISP loopback interface from either host. Was this ping successful?

6. Telnet to the ALS2 VLAN 1 management IP address from the Engineering host. Was this telnet successful?

If either test failed, make any necessary corrections to the configurations for the router and switches.

Final Configuration

```
ISP# show run
!
hostname ISP
!
interface Loopback0
 ip address 200.200.200.1 255.255.255.0
!
interface Serial0/0/0
 ip address 192.168.1.1 255.255.255.0
 clockrate 64000
 no shutdown
!
ip route 172.16.0.0 255.255.0.0 192.168.1.2
!
end
```

```
Gateway# show run
!
hostname Gateway
!
interface FastEthernet0/0
 no shutdown
!
interface FastEthernet0/0.1
 description Management VLAN
 encapsulation dot1Q 1 native
 ip address 172.16.1.1 255.255.255.0
!
interface FastEthernet0/0.100
 description Finance VLAN
 encapsulation dot1Q 100
 ip address 172.16.100.1 255.255.255.0
!
interface FastEthernet0/0.200
 description Engineering VLAN
 encapsulation dot1Q 200
 ip address 172.16.200.1 255.255.255.0
!
interface Serial0/0/0
 ip address 192.168.1.2 255.255.255.0
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```



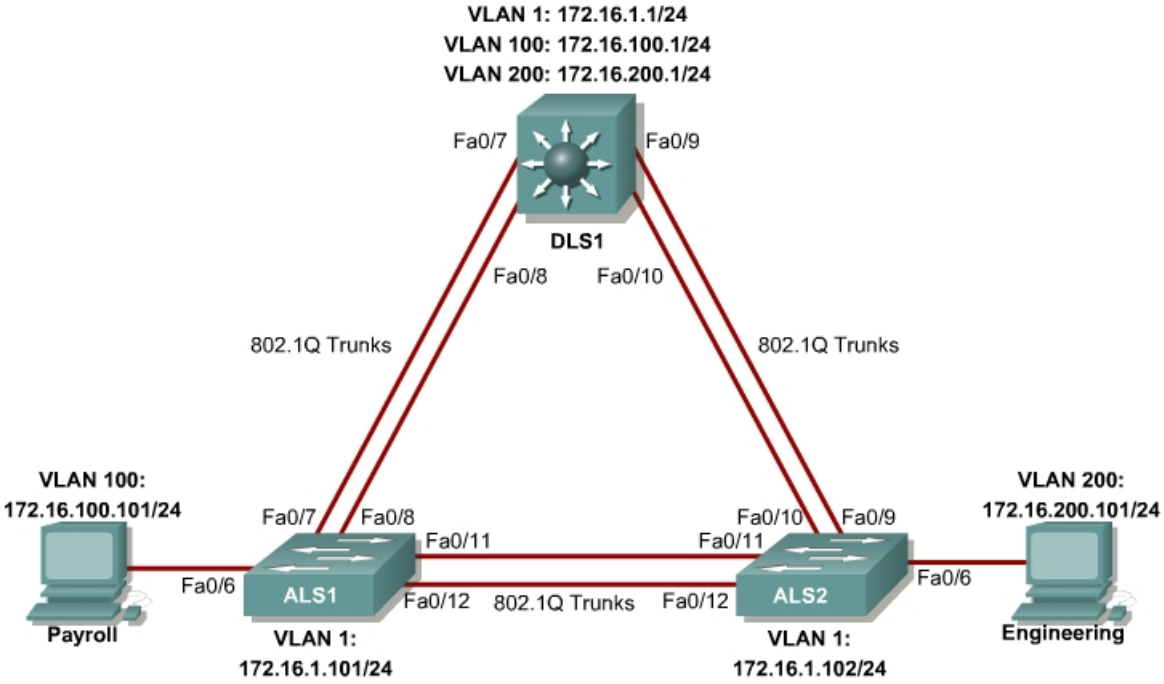
```
!
end


ALS1# show run
!
hostname ALS1
!
enable secret cisco
!
interface Port-channel1
 switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
 channel-group 1 mode desirable
!
interface Vlan1
 ip address 172.16.1.101 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end


ALS2# show run
!
hostname ALS2
!
enable secret cisco
!
interface Port-channel1
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 200
 switchport mode access
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
```



```
 channel-group 1 mode desirable
!
interface Vlan1
 ip address 172.16.1.102 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```


Lab 4-2 Inter-VLAN Routing with an Internal Route Processor and Monitoring CEF Functions

Topology Diagram



Objective

This lab routes between VLANs using a 3560 switch with an internal route processor using Cisco Express Forwarding (CEF).

Scenario

The current network equipment includes a 3560 distribution layer switch and two 2960 access layer switches. The network is segmented into three functional subnets using VLANs for better network management. The VLANs include Finance, Engineering, and a subnet for equipment management, which is the default management VLAN, VLAN 1. After VTP and trunking have been configured for the switches, Switched Virtual Interfaces (SVI) are used on the distribution layer switch to route between these VLANs, giving full connectivity to the internal network.

Step 1

Power up the switches and use the standard process for establishing a HyperTerminal console connection from a workstation to each switch in your pod. If you are remotely accessing your equipment, follow your teacher's instructions.

Remove all VLAN information and configurations that were previously entered into your switches. (Refer to Lab 2.0a or 2.0b if needed.)

Step 2

Cable the lab according to the diagram. Configure the hostname, password, and telnet access on each switch.

The following is a sample configuration for the 2960 switch ALS1:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname ALS1
ALS1(config)# enable secret cisco
ALS1(config)# line vty 0 15
ALS1(config-line)# password cisco
ALS1(config-line)# login
ALS1(config-line)# end
```

The following is a sample configuration for the 2960 switch ALS2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname ALS2
ALS2(config)# enable secret cisco
ALS2(config)# line vty 0 15
ALS2(config-line)# password cisco
ALS2(config-line)# login
ALS2(config-line)# end
```

The following is a sample configuration for the 3560 switch DLS1:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname DLS1
DLS1(config)# enable secret cisco
DLS1(config)# line vty 0 15
DLS1(config-line)#password cisco
DLS1(config-line)# login
DLS1(config-line)# end
```

Configure management IP addresses on VLAN 1 for all three switches according to the diagram.

The following is a sample configuration for the 2960 switch ALS1:

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface vlan 1
```



```
ALS1(config-if)# ip address 172.16.1.101 255.255.255.0
ALS1(config-if)# no shutdown
ALS1(config-if)# exit
```

The following is a sample configuration for the 2960 switch ALS2:

```
ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# interface vlan 1
ALS2(config-if)# ip address 172.16.1.102 255.255.255.0
ALS2(config-if)# no shutdown
ALS2(config-if)# exit
```

The following is a sample configuration for the 3560 switch DLS1:

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# interface vlan 1
DLS1(config-if)# ip address 172.16.1.1 255.255.255.0
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
```

Configure default gateways on the access layer switches. The distribution layer switch will not use a default gateway, because it acts as a Layer 3 device. The access layer switches act as Layer 2 devices and need a default gateway to send traffic off of the local subnet for the management VLAN.

The following is a sample configuration for the 2960 switch ALS1:

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# ip default-gateway 172.16.1.1
ALS1(config-line)# end
```

The following is a sample configuration for the 2960 switch ALS2:

```
ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# ip default-gateway 172.16.1.1
ALS2(config-line)# end
```

Step 3

Configure trunks and EtherChannels between switches.

To distribute VLAN and VTP information between the switches, trunks are needed between the three switches. Configure these trunks according to the diagram. EtherChannel is used for these trunks. EtherChannel allows you to utilize both Fast Ethernet interfaces that are available between each device, thereby doubling the bandwidth.

The following is a sample configuration for the trunks and EtherChannel from DLS1 to ASL1. The **switchport trunk encapsulation** [**isl** | **dot1q**] command is used because this switch also supports ISL encapsulation.


```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# interface range fastethernet 0/7 - 8
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1
```

The following is a sample configuration for the trunks and EtherChannel from DLS1 to ASL2:

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# interface range fastethernet 0/9 - 10
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2
```

The following is a sample configuration for the trunks and EtherChannel between ALS1 and DLS1, and for the trunks and EtherChannel between ALS1 and ALS2:

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface range fastethernet 0/11 - 12
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

ALS1(config-if-range)# exit
ALS1(config)# interface range fastethernet 0/7 - 8
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2
```

The following is a sample configuration for the trunks and EtherChannel between ALS2 and DLS1, and for the trunks and EtherChannel between ALS2 and ALS1.

```
ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# interface range fastethernet 0/11 - 12
ALS2(config-if-range)# switchport mode trunk
ALS2(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

ALS2(config-if-range)# exit
ALS1(config)# interface range fastethernet 0/7 - 8
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2
```


Verify trunking between DLS1, ALS1, and ALS2 using the **show interface trunk** command on all switches.

```
DLS1# show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1
Po2         on           802.1q         trunking      1

Port      Vlans allowed on trunk
Po1         1-4094
Po2         1-4094

Port        Vlans allowed and active in management domain
Po1         1
Po2         1

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1
Po2         1
```

Use the **show etherchannel summary** command on each switch to verify the EtherChannels.

The following is sample output from ALS1. Notice the two EtherChannels on the access layer switches.

```
ALS1# show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Fa0/11(P)   Fa0/12(P)
2      Po2(SU)         PAgP      Fa0/7(P)    Fa0/8(P)
```

1. Which ports are used for channel group 2?

Step 4

Change the VTP mode of ALS1 and ALS2 to client.

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```



```
ALS1(config)# vtp mode client
Setting device to VTP CLIENT mode.
ALS1(config)# end


ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# vtp mode client
Setting device to VTP CLIENT mode.
ALS2(config)# end
```

Verify the VTP changes with the **show vtp status** command.

```
ALS2# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xC8 0xAB 0x3C 0x3B 0xAB 0xDD 0x34 0xCF
Configuration last modified by 0.0.0.0 at 3-1-93 15:47:34
```

2. How many VLANs can be supported locally on the 2960 switch?

Step 5

Create the VTP domain on DLS1 and create VLANS 100 and 200 for the domain.

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# vtp domain SWPOD
DLS1(config)# vlan 100
DLS1(config-vlan)# name Finance
DLS1(config-vlan)# exit
DLS1(config)# vlan 200
DLS1(config-vlan)# name Engineering
DLS1(config-vlan)# end
```

Verify VTP information throughout the domain using the **show vlan** and **show vtp status** commands.

3. How many existing VLANs are in the VTP domain?

Step 6

Configure the host ports for the appropriate VLANs according to the diagram.

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface fastethernet 0/6
ALS1(config-if)# switchport mode access
ALS1(config-if)# switchport access vlan 100
ALS1(config-if)# end

ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# interface fastethernet 0/6
ALS2(config-if)# switchport mode access
ALS2(config-if)# switchport access vlan 200
ALS2(config-if)# end
```

4. Ping from the host on VLAN 100 to the host on VLAN 200. Was the ping successful? Why do you think this is the case?

5. Ping from a host to the VLAN 1 management IP address of DLS1. Was the ping successful? Why do you think this is the case?

Step 7

Create the Layer 3 VLAN interfaces to route between VLANs using the **interface vlan** *vlan-id* command. You do not need to set up VLAN 1 because this was done in Step 2.

The **ip routing** command is also needed to tell the switch that it acts as a Layer 3 device to route between these VLANs. Because the VLANs are all considered directly connected, a routing protocol is not needed at this time.

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# interface vlan 100
DLS1(config-if)# ip add 172.16.100.1 255.255.255.0
DLS1(config-if)# no shut
DLS1(config-if)# interface vlan 200
DLS1(config-if)# ip address 172.16.200.1 255.255.255.0
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# ip routing
DLS1(config)# end
```

Verify the configuration using the **show ip route** command on DLS1.


```
DLS1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.200.0 is directly connected, Vlan200
C       172.16.1.0 is directly connected, Vlan1
C       172.16.100.0 is directly connected, Vlan100
```

Step 8

Verify inter-VLAN routing by the internal route processor.

5. Ping from the Engineering host to the Finance host. Was the ping successful this time?

6. Telnet from a host to the VLAN 1 IP address of DLS1. Can this switch be remotely accessed from this host?

Example telnet from the Engineering host:

```
C:>telnet 172.16.1.1

User Access Verification

Password: <vty-password>

DLS1>
```

Step 9

Cisco Express Forwarding (CEF) implements an advanced IP lookup and forwarding algorithm to deliver maximum Layer 3 switching performance. CEF is less CPU-intensive than fast switching route caching.

In dynamic networks, fast switching cache entries are frequently invalidated because of routing changes. This can cause traffic to be process-switched using the routing table, instead of fast-switched using the route cache. CEF

uses the Forwarding Information Base (FIB) lookup table to perform destination-based switching of IP packets.

CEF is enabled by default on the 3560 switch.

Use the **show ip cef** command to display the status of CEF.

```
DLS1# show ip cef
Prefix              Next Hop            Interface
0.0.0.0/32          receive
172.16.1.0/24       attached            Vlan1
172.16.1.0/32       receive
172.16.1.1/32       receive
172.16.1.101/32     attached            Vlan1
172.16.1.102/32     attached            Vlan1
172.16.1.255/32     receive
172.16.100.0/24     attached            Vlan100
172.16.100.0/32     receive
172.16.100.1/32     receive
172.16.100.255/32   receive
172.16.200.0/24     attached            Vlan200
172.16.200.0/32     receive
172.16.200.1/32     receive
172.16.200.255/32   receive
224.0.0.0/4         drop
224.0.0.0/24        receive
255.255.255.255/32  receive
```

Use the **show ip interface** command to verify that CEF is enabled on an interface. The following output shows that CEF is enabled on VLAN 100.

```
DLS1# show ip interface vlan 100
Vlan100 is up, line protocol is up
  Internet address is 172.16.100.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
```



```
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Use the **show ip cef summary** command to display the CEF table summary. The **show ip cef detail** command shows CEF operation in detail for the switch.

```
DLS1# show ip cef summary
IPv4 CEF is enabled for distributed and running
VRF Default:
 18 prefixes (18/0 fwd/non-fwd)
 Table id 0, 0 resets
 Database epoch: 1 (18 entries at this epoch)

DLS1# show ip cef detail
IPv4 CEF is enabled for distributed and running
VRF Default:
 18 prefixes (18/0 fwd/non-fwd)
 Table id 0, 0 resets
 Database epoch: 1 (18 entries at this epoch)

0.0.0.0/32, epoch 1, flags receive
  Special source: receive
  receive
172.16.1.0/24, epoch 1, flags attached, connected
  attached to Vlan1
172.16.1.0/32, epoch 1, flags receive
  receive
172.16.1.1/32, epoch 1, flags receive
  receive
172.16.1.101/32, epoch 1
  Adj source: IP adj out of Vlan1, addr 172.16.1.101
  attached to Vlan1
172.16.1.102/32, epoch 1
  Adj source: IP adj out of Vlan1, addr 172.16.1.102
  attached to Vlan1
172.16.1.255/32, epoch 1, flags receive
  receive
172.16.100.0/24, epoch 1, flags attached, connected
  attached to Vlan100
172.16.100.0/32, epoch 1, flags receive
  receive
172.16.100.1/32, epoch 1, flags receive
  receive
172.16.100.255/32, epoch 1, flags receive
  receive
172.16.200.0/24, epoch 1, flags attached, connected
  attached to Vlan200
172.16.200.0/32, epoch 1, flags receive
  receive
172.16.200.1/32, epoch 1, flags receive
  receive
172.16.200.255/32, epoch 1, flags receive
  receive
224.0.0.0/4, epoch 1
  Special source: drop
  drop
224.0.0.0/24, epoch 1, flags receive
  Special source: receive
```



```
  receive
255.255.255.255/32, epoch 1, flags receive
  Special source: receive
  receive
```

Final Configuration

```
DLS1# show run
!
hostname DLS1
!
enable secret cisco
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface Vlan1
 ip address 172.16.1.1 255.255.255.0
 no shutdown
!
interface Vlan100
 ip address 172.16.100.1 255.255.255.0
 no shutdown
!
interface Vlan200
 ip address 172.16.200.1 255.255.255.0
 no shutdown
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```



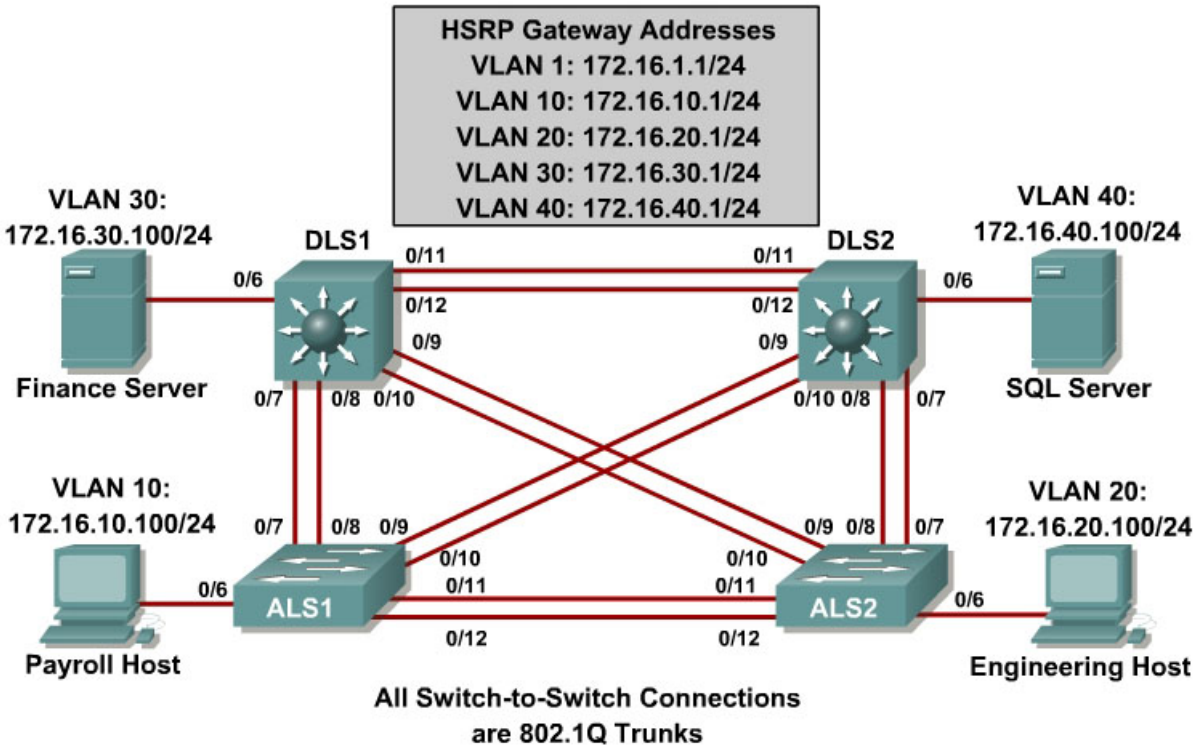
```
ALS1# show run
!
hostname ALS1
!
enable secret cisco
!
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/7
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/8
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
 channel-group 1 mode desirable
!
interface Vlan1
 ip address 172.16.1.101 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end


ALS2# show run
!
hostname ALS2
!
enable secret cisco
!
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
interface FastEthernet0/6
```



```
 switchport access vlan 200
 switchport mode access
!
interface FastEthernet0/9
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
 channel-group 1 mode desirable
!
interface Vlan1
 ip address 172.16.1.102 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```


Lab 5-1 Hot Standby Router Protocol

Topology Diagram



Objective

Configure inter-VLAN routing with HSRP to provide redundant, fault tolerant routing to the internal network.

Scenario

HSRP provides a transparent failover mechanism to the end stations on the network. This provides users with uninterrupted service to the network in the event of a router failure.

Step 1

Power up the switches and use the standard process for establishing a HyperTerminal console connection from a workstation to each switch in your pod.

Remove all VLAN information and configurations that were previously entered into your switches. (Refer to Lab 2.0a or 2.0b if needed.)

Step 2

Cable the lab according to the diagram.

Configure management IP addresses in VLAN 1, hostname, password, and telnet access on all four switches.

The following is a sample configuration for the 2960 switch ALS1:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname ALS1
ALS1(config)# enable secret cisco
ALS1(config)# line vty 0 15
ALS1(config-line)# password cisco
ALS1(config-line)# login
ALS1(config-line)# exit
ALS1(config)# interface vlan 1
ALS1(config-if)# ip address 172.16.1.101 255.255.255.0
ALS1(config-if)# no shutdown
ALS1(config-if)# end
```

The following is a sample configuration for the 2960 switch ALS2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname ALS2
ALS2(config)# enable secret cisco
ALS2(config)# line vty 0 15
ALS2(config-line)# password cisco
ALS2(config-line)# login
ALS2(config-line)# exit
ALS2(config)# interface vlan 1
ALS2(config-if)# ip address 172.16.1.102 255.255.255.0
ALS2(config-if)# no shutdown
ALS2(config-if)# end
```

The following is a sample configuration for the 3560 switch DLS1:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname DLS1
DLS1(config)# enable secret cisco
DLS1(config)# line vty 0 15
DLS1(config-line)# password cisco
DLS1(config-line)# login
DLS1(config-line)# exit
DLS1(config)# interface vlan 1
DLS1(config-if)# ip address 172.16.1.3 255.255.255.0
DLS1(config-if)# no shutdown
DLS1(config-if)# end
```

The following is a sample configuration for the 3560 switch DLS2.:

```
Switch# configure terminal
```



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname DLS2
DLS2(config)# enable secret cisco
DLS2(config)# line vty 0 15
DLS2(config-line)# password cisco
DLS2(config-line)# login
DLS2(config-line)# exit
DLS2(config)# interface vlan 1
DLS2(config-if)# ip address 172.16.1.4 255.255.255.0
DLS2(config-if)# no shutdown
DLS2(config-if)# end
```

Configure default gateways on the access layer switches. The distribution layer switchs will not use a default gateway, because they act as Layer 3 devices. The access layer switches act as Layer 2 devices and need a default gateway to send traffic off of the local subnet for the management VLAN.

The following is a sample configuration for the 2960 switch ALS1:

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# ip default-gateway 172.16.1.1
ALS1(config)# end
```

The following is a sample configuration for the 2960 switch ALS2:

```
ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# ip default-gateway 172.16.1.1
ALS2(config)# end
```

Step 3

Configure trunks and EtherChannels between switches according to the diagram. EtherChannel is used for these trunks. EtherChannel allows you to utilize both Fast Ethernet interfaces that are available between each device, thereby doubling the bandwidth.

The following is a sample configuration for the trunks and EtherChannel from DLS1 to the other three switches. The **switchport trunk encapsulation** [**isl** | **dot1q**] command is used because this switch also supports ISL encapsulation.

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# interface range fastethernet 0/7 - 8
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

DLS1(config-if-range)# interface range fastethernet 0/9 - 10
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2
```



```
DLS1(config-if-range)# interface range fastethernet 0/11 - 12
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# channel-group 3 mode desirable

Creating a port-channel interface Port-channel 3

DLS1(config-if-range)# end
```

The following is a sample configuration for the trunks and EtherChannels from DLS2 to the other three switches:

```
DLS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)# interface range fastethernet 0/7 - 8
DLS2(config-if-range)# switchport trunk encapsulation dot1q
DLS2(config-if-range)# switchport mode trunk
DLS2(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

DLS2(config-if-range)# interface range fastethernet 0/9 - 10
DLS2(config-if-range)# switchport trunk encapsulation dot1q
DLS2(config-if-range)# switchport mode trunk
DLS2(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2

DLS2(config-if-range)# interface range fastethernet 0/11 - 12
DLS2(config-if-range)# switchport trunk encapsulation dot1q
DLS2(config-if-range)# switchport mode trunk
DLS2(config-if-range)# channel-group 3 mode desirable

Creating a port-channel interface Port-channel 3

DLS2(config-if-range)# end
```

The following is a sample configuration for the trunks and EtherChannel from ALS1 and ALS2 to the other switches. Notice that no encapsulation type is needed because the 2960 supports only 802.1q trunks.

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface range fastethernet 0/7 - 8
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

ALS1(config-if-range)# interface range fastethernet 0/9 - 10
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2

ALS1(config-if-range)# interface range fastethernet 0/11 - 12
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 3 mode desirable

Creating a port-channel interface Port-channel 3
```



```
ALS1(config-if-range)# end
```

The following is a sample configuration from ALS2:

```
ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# interface range fastethernet 0/7 - 8
ALS2(config-if-range)# switchport mode trunk
ALS2(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

ALS2(config-if-range)# interface range fastethernet 0/9 - 10
ALS2(config-if-range)# switchport mode trunk
ALS2(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2

ALS2(config-if-range)# interface range fastethernet 0/11 - 12
ALS2(config-if-range)# switchport mode trunk
ALS2(config-if-range)# channel-group 3 mode desirable

Creating a port-channel interface Port-channel 3

ALS2(config-if-range)# end
```

Verify trunking between DLS1, ALS1, and ALS2 using the **show interface trunk** command on all switches.

```
DLS1# show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1
Po2         on           802.1q         trunking      1
Po3         on           802.1q         trunking      1

Port      Vlans allowed on trunk
Po1         1-4094
Po2         1-4094
Po3         1-4094

Port        Vlans allowed and active in management domain
Po1         1
Po2         1
Po3         1

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1
Po2         1
Po3         1
```

Issue the **show etherchannel summary** command on each switch to verify the EtherChannels. In the following sample output from ALS1, notice the three EtherChannels on the access and distribution layer switches. Your output may vary depending on which ports have been placed in blocking by the Spanning Tree Protocol.

```
ALS1# show etherchannel summary
Flags:  D - down        P - in port-channel
```



```
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
--
1      Po1(SU)         PAgP      Fa0/7(P)    Fa0/8(P)
2      Po2(SU)         PAgP      Fa0/9(P)    Fa0/10(P)
3      Po3(SU)         PAgP      Fa0/11(P)   Fa0/12(P)
```

1. Which EtherChannel negotiation protocol is in use here?

Step 4

Change the VTP mode of ALS1 and ALS2 to client.

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# vtp mode client
Setting device to VTP CLIENT mode.
ALS1(config)# end


ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# vtp mode client
Setting device to VTP CLIENT mode.
ALS2(config)# end
```

Verify the VTP changes with the **show vtp status** command.

```
ALS2# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xC8 0xAB 0x3C 0x3B 0xAB 0xDD 0x34 0xCF
Configuration last modified by 0.0.0.0 at 3-1-93 15:47:34
```

2. How many VLANs can be supported locally on the 2960 switch?

Step 5

Create the VTP domain on DLS1 and create VLANs 100, 200, 300, and 400 for the domain.

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# vtp domain SWPOD
DLS1(config)# vlan 10
DLS1(config-vlan)# name Finance
DLS1(config-vlan)# exit
DLS1(config)# vlan 20
DLS1(config-vlan)# name Engineering
DLS1(config-vlan)# exit
DLS1(config)# vlan 30
DLS1(config-vlan)# name Server-Farm1
DLS1(config-vlan)# exit
DLS1(config)# vlan 40
DLS1(config-vlan)# name Server-Farm2
DLS1(config-vlan)# end
```

Verify VTP information throughout the domain using the **show vlan** and **show vtp status** commands.

3. How many existing VLANs are in the VTP domain?

Step 6

Configure your hosts with IP addresses and default gateways according to the diagram.

Configure the host ports of all four switches. The following commands set up **access** as the switchport mode, place the port in the proper VLANs, and turn Spanning Tree Portfast on for the ports.

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# interface fastethernet 0/6
DLS1(config-if)# switchport mode access
DLS1(config-if)# switchport access vlan 30
DLS1(config-if)# spanning-tree portfast
DLS1(config-if)# end

DLS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)# interface fastethernet 0/6
DLS2(config-if)# switchport mode access
DLS2(config-if)# switchport access vlan 40
DLS2(config-if)# spanning-tree portfast
DLS2(config-if)# end
```



```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface fastethernet 0/6
ALS1(config-if)# switchport mode access
ALS1(config-if)# switchport access vlan 10
ALS1(config-if)# spanning-tree portfast
ALS1(config-if)# end

ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# interface fastEthernet 0/6
ALS2(config-if)# switchport mode access
ALS2(config-if)# switchport access vlan 20
ALS2(config-if)# spanning-tree portfast
ALS2(config-if)# end
```

4. Ping from the host on VLAN 10 to the host on VLAN 40. The ping should fail. Are these results expected at this point? Why?

Step 7

Hot Standby Router Protocol (HSRP) provides redundancy in the network. You can also load balance the VLANs by using the **standby** *group* **priority** *priority* command. The **ip routing** command is used on DLS1 and DLS2 to activate routing capabilities on the switch.

Each route processor can route between the various SVIs configured on its switch. Assign a third IP address in each subnet to be used as a virtual gateway address. HSRP negotiates and handles which switch accepts information forwarded to the virtual gateway IP address.

The **standby** command configures the IP address of the virtual gateway, sets the priority for each VLAN, and configures the router for preempt. Preemption allows the router with the higher priority to become the active router after a network failure has been resolved.

In the following configurations, the priority for VLANs 1, 10, and 20 is 150 on DLS1, making it the active router for those VLANs. VLANs 30 and 40 have a priority of 100 on DLS1, making DLS1 the standby router for these VLANs. DLS2 is configured to be the active router for VLANs 30 and 40 with a priority of 150, and the standby router for VLANs 1, 10, and 20 with a priority of 100.

HSRP configuration for DLS1:

```
DLS1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# ip routing
DLS1(config)# interface vlan 1
```



```
DLS1(config-if)# standby 1 ip 172.16.1.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 150
DLS1(config-if)# exit
DLS1(config)# interface vlan 10
DLS1(config-if)# ip address 172.16.10.3 255.255.255.0
DLS1(config-if)# standby 1 ip 172.16.10.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 150
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# interface vlan 20
DLS1(config-if)# ip address 172.16.20.3 255.255.255.0
DLS1(config-if)# standby 1 ip 172.16.20.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 150
DLS1(config-if)# exit
DLS1(config)# interface vlan 30
DLS1(config-if)# ip address 172.16.30.3 255.255.255.0
DLS1(config-if)# standby 1 ip 172.16.30.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 100
DLS1(config-if)# exit
DLS1(config)# interface vlan 40
DLS1(config-if)# ip address 172.16.40.3 255.255.255.0
DLS1(config-if)# standby 1 ip 172.16.40.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 100
DLS1(config-if)# end
```

HSRP configuration for DLS2:

```
DLS2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)# ip routing
DLS2(config)# interface vlan 1
DLS2(config-if)# standby 1 ip 172.16.1.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 100
DLS2(config-if)# exit
DLS2(config)# interface vlan 10
DLS2(config-if)# ip address 172.16.10.4 255.255.255.0
DLS2(config-if)# standby 1 ip 172.16.10.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 100
DLS2(config-if)# no shutdown
DLS2(config-if)# exit
DLS2(config)# interface vlan 20
DLS2(config-if)# ip address 172.16.20.4 255.255.255.0
DLS2(config-if)# standby 1 ip 172.16.20.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 100
DLS2(config-if)# exit
DLS2(config)# interface vlan 30
DLS2(config-if)# ip address 172.16.30.4 255.255.255.0
DLS2(config-if)# standby 1 ip 172.16.30.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 150
DLS2(config-if)# exit
DLS2(config)# interface vlan 40
DLS2(config-if)# ip address 172.16.40.4 255.255.255.0
DLS2(config-if)# standby 1 ip 172.16.40.1
DLS2(config-if)# standby 1 preempt
```



```
DLS2(config-if)# standby 1 priority 150
DLS2(config-if)# end
```

Step 8

Issue the **show standby** command on both DLS1 and DLS2.

```
DLS1# show standby
Vlan1 - Group 1
  State is Active
    5 state changes, last state change 00:02:48
  Virtual IP address is 172.16.1.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.228 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.1.4, priority 100 (expires in 7.207 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl1-1" (default)
Vlan10 - Group 1
  State is Active
    5 state changes, last state change 00:02:50
  Virtual IP address is 172.16.10.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.113 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.10.4, priority 100 (expires in 9.807 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl10-1" (default)
Vlan20 - Group 1
  State is Active
    5 state changes, last state change 00:02:55
  Virtual IP address is 172.16.20.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.884 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.20.4, priority 100 (expires in 9.220 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl20-1" (default)
Vlan30 - Group 1
  State is Standby
    4 state changes, last state change 00:02:45
  Virtual IP address is 172.16.30.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.413 secs
  Preemption enabled
  Active router is 172.16.30.4, priority 150 (expires in 8.415 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Vl30-1" (default)
Vlan40 - Group 1
  State is Standby
```



```
    4 state changes, last state change 00:02:51
  Virtual IP address is 172.16.40.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.826 secs
  Preemption enabled
  Active router is 172.16.40.4, priority 150 (expires in 7.828 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Vl40-1" (default)



DLS2# show standby
Vlan1 - Group 1
  State is Standby
    3 state changes, last state change 00:02:33
  Virtual IP address is 172.16.1.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.950 secs
  Preemption enabled
  Active router is 172.16.1.3, priority 150 (expires in 8.960 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Vl1-1" (default)
Vlan10 - Group 1
  State is Standby
    3 state changes, last state change 00:02:34
  Virtual IP address is 172.16.10.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.759 secs
  Preemption enabled
  Active router is 172.16.10.3, priority 150 (expires in 7.844 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Vl10-1" (default)
Vlan20 - Group 1
  State is Standby
    3 state changes, last state change 00:02:42
  Virtual IP address is 172.16.20.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.790 secs
  Preemption enabled
  Active router is 172.16.20.3, priority 150 (expires in 8.289 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Vl20-1" (default)
Vlan30 - Group 1
  State is Active
    2 state changes, last state change 00:02:52
  Virtual IP address is 172.16.30.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.549 secs
  Preemption enabled
```



```
  Active router is local
  Standby router is 172.16.30.3, priority 100 (expires in 9.538 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl30-1" (default)
Vlan40 - Group 1
  State is Active
    2 state changes, last state change 00:02:58
  Virtual IP address is 172.16.40.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.962 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.40.3, priority 100 (expires in 8.960 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl40-1" (default)
```

5. Which router is the active router for VLANs 1, 10, and 20? Which is the active router for 30 and 40?

6. What is the default hello time for each VLAN? What is the default hold time?

7. How is the active HSRP router selected?

Use the **show ip route** command to verify routing on both DLS1 and DLS2.

```
DLS1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.40.0 is directly connected, Vlan40
C       172.16.30.0 is directly connected, Vlan30
C       172.16.20.0 is directly connected, Vlan20
C       172.16.10.0 is directly connected, Vlan10
C       172.16.1.0 is directly connected, Vlan1
```


Step 9

Verify connectivity between VLANs using the **ping** command from the SQL Server (VLAN 40) to the other hosts and servers on the network.

The following is from the SQL Server to the Engineering host:

```
C:\> ping 172.16.20.100

Pinging 172.16.20.100 with 32 bytes of data:

Reply from 172.16.20.100: bytes=32 time=2ms TTL=255
Reply from 172.16.20.100: bytes=32 time=2ms TTL=255
Reply from 172.16.20.100: bytes=32 time=2ms TTL=255
Reply from 172.16.20.100: bytes=32 time=2ms TTL=255

Ping statistics for 172.16.20.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Step 10

Verify HSRP by disconnecting the trunks to DLS2. If you have physical access to the routers, unplug the cables to FastEthernet0/7 through FastEthernet0/12. If you do not have physical access, use the **shutdown** command on those interfaces.

```
DLS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)# interface range fastethernet 0/7 - 12
DLS2(config-if-range)# shutdown
DLS2(config-if-range)# end
```

Output to the terminal should reflect DLS1 becoming the active router for VLANs 30 and 40.

```
1w3d: %HSRP-6-STATECHANGE: Vlan30 Grp 1 state Standby -> Active
1w3d: %HSRP-6-STATECHANGE: Vlan40 Grp 1 state Standby -> Active
```

If the trunks are disconnected, reconnect the cables to FastEthernet0/7 through FastEthernet0/12 on DLS2. Repeat this step by disconnecting the trunks for DLS1 and use the **show standby** command to see the results.

Final Configurations

```
DLS1# show run
!
hostname DLS1
!
enable secret cisco
!
ip routing
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
```



```
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 300
 switchport mode access
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Vlan1
 ip address 172.16.1.3 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan10
 ip address 172.16.10.3 255.255.255.0
 standby 1 ip 172.16.10.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan20
 ip address 172.16.20.3 255.255.255.0
 standby 1 ip 172.16.20.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
```



```
!
interface Vlan30
 ip address 172.16.30.3 255.255.255.0
 standby 1 ip 172.16.30.1
 standby 1 preempt
 no shutdown
!
interface Vlan40
 ip address 172.16.40.3 255.255.255.0
 standby 1 ip 172.16.40.1
 standby 1 preempt
 no shutdown
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end


DLS2# show run
!
hostname DLS2
!
enable secret cisco
!
ip routing
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 400
 switchport mode access
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/10
```



```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Vlan1
 ip address 172.16.1.4 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 preempt
 no shutdown
!
interface Vlan10
 ip address 172.16.10.4 255.255.255.0
 standby 1 ip 172.16.10.1
 standby 1 preempt
 no shutdown
!
interface Vlan20
 ip address 172.16.20.4 255.255.255.0
 standby 1 ip 172.16.20.1
 standby 1 preempt
 no shutdown
!
interface Vlan30
 ip address 172.16.30.4 255.255.255.0
 standby 1 ip 172.16.30.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan40
 ip address 172.16.40.4 255.255.255.0
 standby 1 ip 172.16.40.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end


ALS1# show run
!
hostname ALS1
!
enable secret cisco
!
interface Port-channel1
```



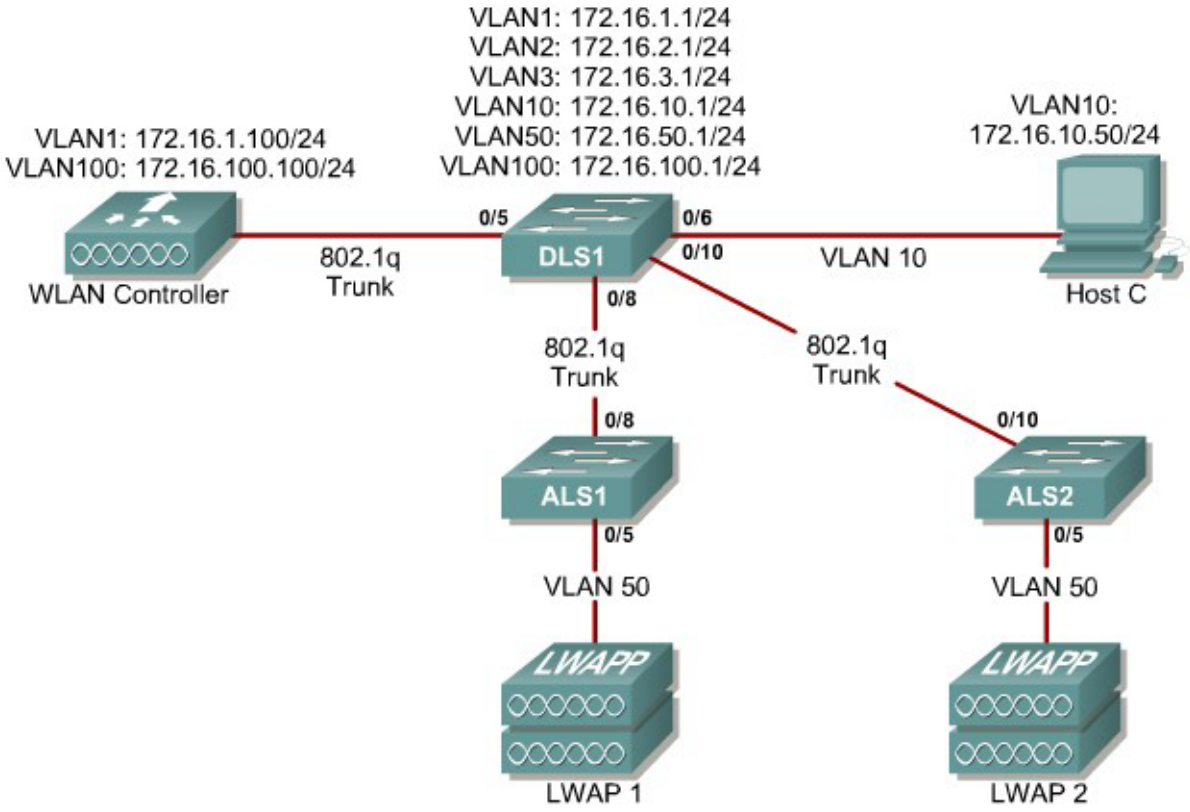
```
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
interface Port-channel3
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/7
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/8
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/9
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Vlan1
 ip address 172.16.1.101 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end


ALS2# show run
!
hostname ALS2
!
enable secret cisco
!
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
```



```
!
interface Port-channel3
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 200
 switchport mode access
!
interface FastEthernet0/7
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/8
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/9
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Vlan1
 ip address 172.16.1.102 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end
```


Lab 6-1 Configuring a WLAN Controller

Topology Diagram



Scenario

In the next two labs, you will configure a wireless solution involving a WLAN controller, two lightweight wireless access points, and a switched wired network. You will configure a WLAN controller to broadcast SSIDs from the lightweight wireless access points. If you have a wireless client nearby, connect to the WLANs and access devices from the inside of your pod to verify your configuration of the controller and access points.

Note: It is required that you upgrade the WLC firmware image to 4.0.206.0 or higher in order to accomplish this lab.

Step 1

Erase the startup-config file and delete the vlan.dat file from each switch. On the WLAN controller, use the **clear controller** command followed by the **reset system** command to reset them.

Step 2

Explanation of VLANs:
VLAN 1 – This VLAN is the management VLAN for the WLC
VLAN 2 and VLAN 3 – These VLANs are for hosts in the WLANs
VLAN 10 – The host is in this VLAN
VLAN 50 – The APs are in this VLAN
VLAN 100 – The AP-manager interface of the WLC is in this VLAN

Set up DLS1 as a VTP server, and ALS1 and ALS2 as clients. Put them in VTP domain CISCO. Set up the switch-to-switch links shown in the diagram as 802.1q trunks. Add VLANs 2, 3, 10, 50, and 100 to DLS1.

```
DLS1(config)# vtp mode server
DLS1(config)# vtp domain CISCO
DLS1(config)# vlan 2,3,10,50,100
DLS1(config-vlan)# interface fastethernet0/8
DLS1(config-if)# switchport trunk encapsulation dot1q
DLS1(config-if)# switchport mode trunk
DLS1(config-if)# interface fastethernet0/10
DLS1(config-if)# switchport trunk encapsulation dot1q
DLS1(config-if)# switchport mode trunk

ALS1(config)# vtp mode client
ALS1(config)# vtp domain CISCO
ALS1(config)# interface fastethernet0/8
ALS1(config-if)# switchport mode trunk

ALS2(config)# vtp mode client
ALS2(config)# vtp domain CISCO
ALS2(config)# interface fastethernet0/10
ALS2(config-if)# switchport mode trunk
```

Verify that VTP traffic has passed between the switch by comparing the non-zero VTP configuration revision between switches with the **show vtp status** command.

```
DLS1# show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 10
VTP Operating Mode              : Server
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x6A 0x6B 0xCA 0x3C 0xF0 0x45 0x87 0xAC
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:01
```



```
Local updater ID is 0.0.0.0 (no valid interface found)

ALS1# show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x6A 0x6B 0xCA 0x3C 0xF0 0x45 0x87 0xAC
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:01

ALS2# show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x6A 0x6B 0xCA 0x3C 0xF0 0x45 0x87 0xAC
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:01
```

Step 3

Configure all the switched virtual interfaces (SVIs) shown in the diagram for DLS1.

```
DLS1(config)# interface vlan 1
DLS1(config-if)# ip address 172.16.1.1 255.255.255.0
DLS1(config-if)# interface vlan 2
DLS1(config-if)# ip address 172.16.2.1 255.255.255.0
DLS1(config-if)# interface vlan 3
DLS1(config-if)# ip address 172.16.3.1 255.255.255.0
DLS1(config-if)# interface vlan 10
DLS1(config-if)# ip address 172.16.10.1 255.255.255.0
DLS1(config-if)# interface vlan 50
DLS1(config-if)# ip address 172.16.50.1 255.255.255.0
DLS1(config-if)# interface vlan 100
DLS1(config-if)# ip address 172.16.100.1 255.255.255.0
```

Step 4

DHCP gives out dynamic IP addresses on a subnet to network devices or hosts rather than statically setting the addresses. This is useful when dealing with lightweight access points, which usually do not have an initial configuration. The WLAN controller that the lightweight wireless access point associates with defines the configuration. A lightweight access point can dynamically receive an IP address and then communicate over IP with the WLAN controller. In this scenario, you will also use it to assign IP addresses to hosts that connect to the WLANs.

First, set up DLS1 to exclude the first 150 addresses from each subnet from DHCP to avoid conflicts with static IP addresses by using the global configuration command **ip dhcp excluded-address** *low-address* [*high-address*].

```
DLS1(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.150
DLS1(config)# ip dhcp excluded-address 172.16.2.1 172.16.2.150
DLS1(config)# ip dhcp excluded-address 172.16.3.1 172.16.3.150
DLS1(config)# ip dhcp excluded-address 172.16.10.1 172.16.10.150

DLS1(config)# ip dhcp excluded-address 172.16.50.1 172.16.50.150
DLS1(config)# ip dhcp excluded-address 172.16.100.1 172.16.100.150
```

To advertise on different subnets, create DHCP pools with the **ip dhcp pool** *name* command. After a pool is configured for a certain subnet, the IOS DHCP server processes requests on that subnet, because it is enabled by default. From the DHCP pool prompt, set the network and mask to use with the **network** *address /mask* command. Set a default gateway with the **default-router** *address* command.

VLAN 50 also uses the **option** command, which allows you to specify a DHCP option. In this case, option 43 is specified (a vendor-specific option), which gives the lightweight wireless access points the IP address of the WLAN controller AP Manager interface. It is specified in a hexadecimal TLV (type, length, value) format. F1 is the hardcoded type of option, 04 represents the length of the value (an IP address is 4 octets), and AC106464 is the hexadecimal representation of 172.16.100.100, which is going to be the AP manager address of the WLAN controller. DHCP option 60 specifies the identifier that access points will use in DHCP. This lab was written using Cisco Aironet 1240 series access points. If you are using a different access point series, consult http://www.cisco.com/univercd/cc/td/doc/product/wireless/aero1500/1500hig5/1500_axg.htm.

```
DLS1(config)# ip dhcp pool pool1
DLS1(dhcp-config)# network 172.16.1.0 /24
DLS1(dhcp-config)# default-router 172.16.1.1
DLS1(dhcp-config)# ip dhcp pool pool2
DLS1(dhcp-config)# network 172.16.2.0 /24
DLS1(dhcp-config)# default-router 172.16.2.1
DLS1(dhcp-config)# ip dhcp pool pool3
DLS1(dhcp-config)# network 172.16.3.0 /24
DLS1(dhcp-config)# default-router 172.16.3.1
DLS1(dhcp-config)# ip dhcp pool pool10
DLS1(dhcp-config)# network 172.16.10.0 /24
DLS1(dhcp-config)# default-router 172.16.10.1
DLS1(dhcp-config)# ip dhcp pool pool50
DLS1(dhcp-config)# network 172.16.50.0 /24
DLS1(dhcp-config)# default-router 172.16.50.1
DLS1(dhcp-config)# option 43 hex f104ac106464
DLS1(dhcp-config)# option 60 ascii "Cisco AP c1240"
DLS1(dhcp-config)# ip dhcp pool pool100
DLS1(dhcp-config)# network 172.16.100.0 /24
DLS1(dhcp-config)# default-router 172.16.100.1
```


Step 5

On all three switches, configure each access point's switchport with the **spanning-tree portfast** command so that each access point receives an IP address from DHCP immediately, thereby avoiding spanning-tree delays. Use VLAN 100 as the AP Manager interface for the WLAN controller. All control and data traffic between the controller and the lightweight wireless access points passes over this VLAN to this interface. Configure the ports going to the lightweight wireless access points in VLAN 50. DLS1 will route the traffic between the VLANs. Configure the interface on DLS1 that connects to the WLAN controller as an 802.1q trunk.

```
DLS1(config)# interface fastethernet0/5
DLS1(config-if)# switchport trunk encapsulation dot1q
DLS1(config-if)# switchport mode trunk

ALS1(config)# interface fastethernet0/5
ALS1(config-if)# switchport mode access
ALS1(config-if)# switchport access vlan 50
ALS1(config-if)# spanning-tree portfast

ALS2(config)# interface fastethernet0/5
ALS2(config-if)# switchport mode access
ALS2(config-if)# switchport access vlan 50
ALS2(config-if)# spanning-tree portfast
```

Step 6

You have a PC running Microsoft Windows attached to DLS1. First, configure the switchport facing the host to be in VLAN 10.

```
DLS1(config)# interface fastethernet0/6
DLS1(config-if)# switchport mode access
DLS1(config-if)# switchport access vlan 10
DLS1(config-if)# spanning-tree portfast
```

Next, configure the host with an IP address in VLAN 10, which will later be used to access the HTTP web interface of the WLAN controller.

In the **Control Panel**, select **Network Connections**.

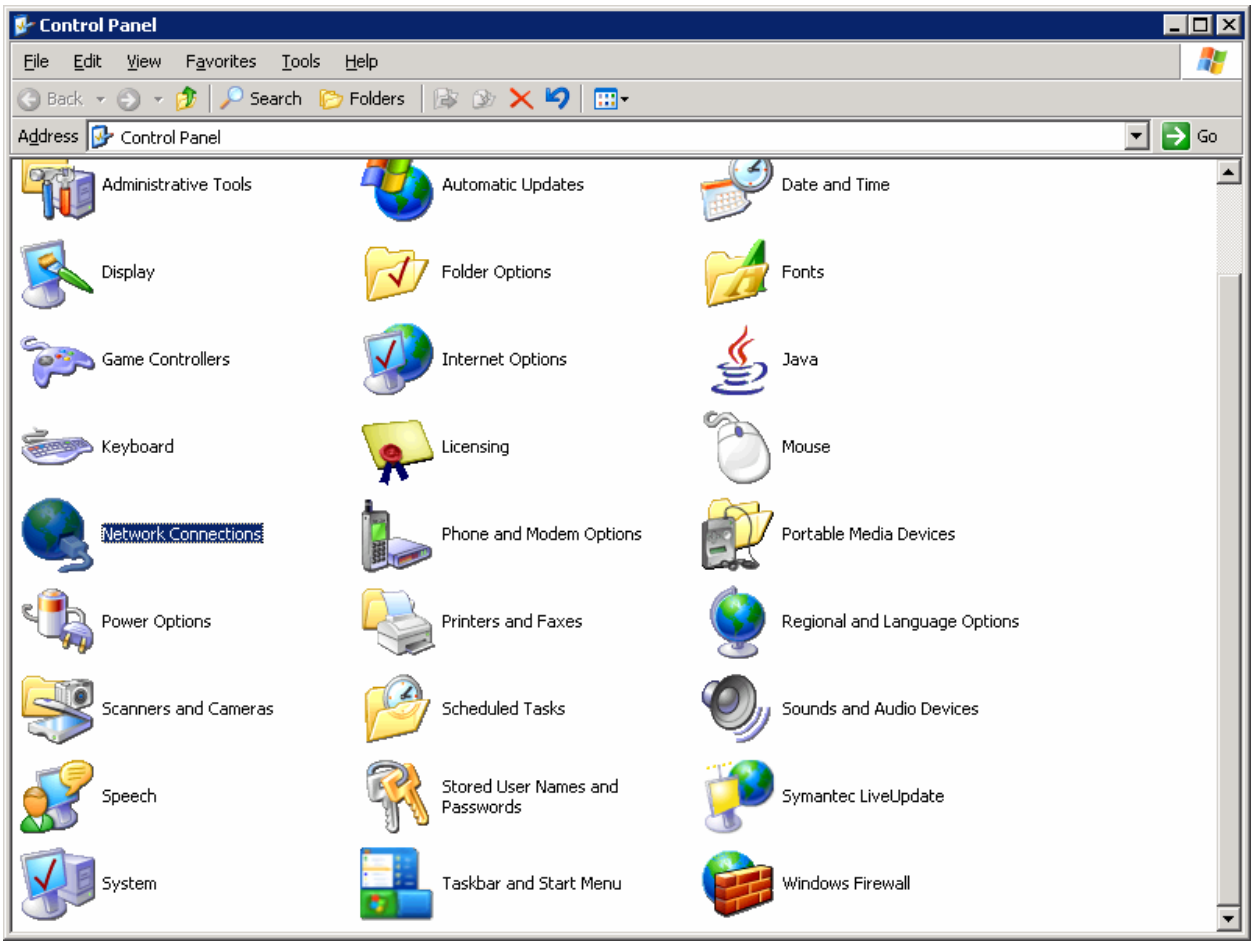


Figure 5-1: Microsoft Windows Control Panel

Right-click on the LAN interface that connects to DLS1, and select **Properties**. Select **Internet Protocol (TCP/IP)** and then click the **Properties** button.

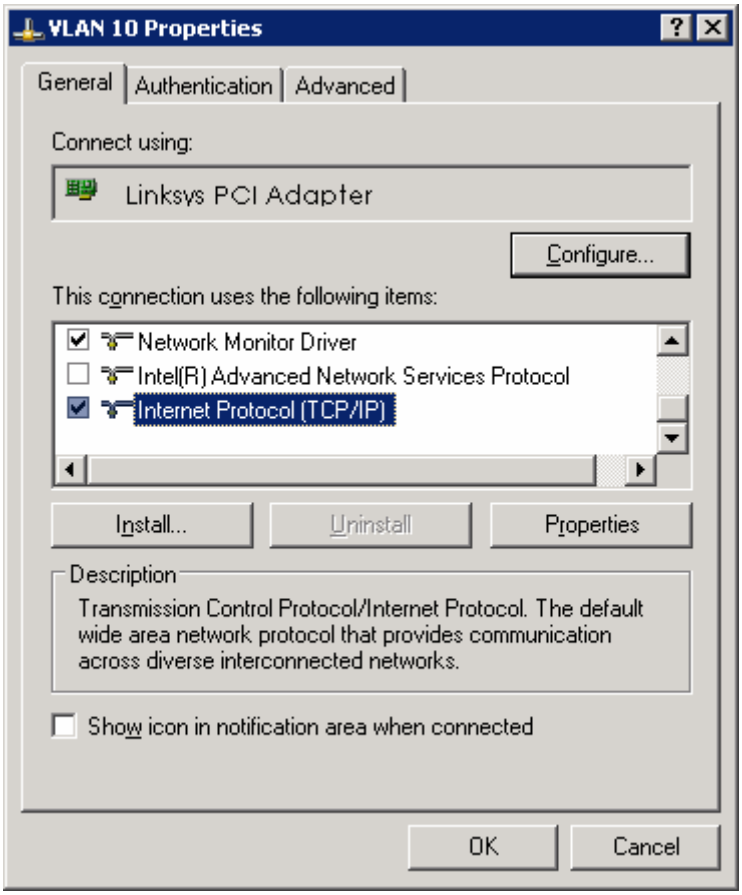


Figure 5-2: Modify the Properties for Interface on VLAN 10

Finally, configure the IP address shown in the diagram on the interface.

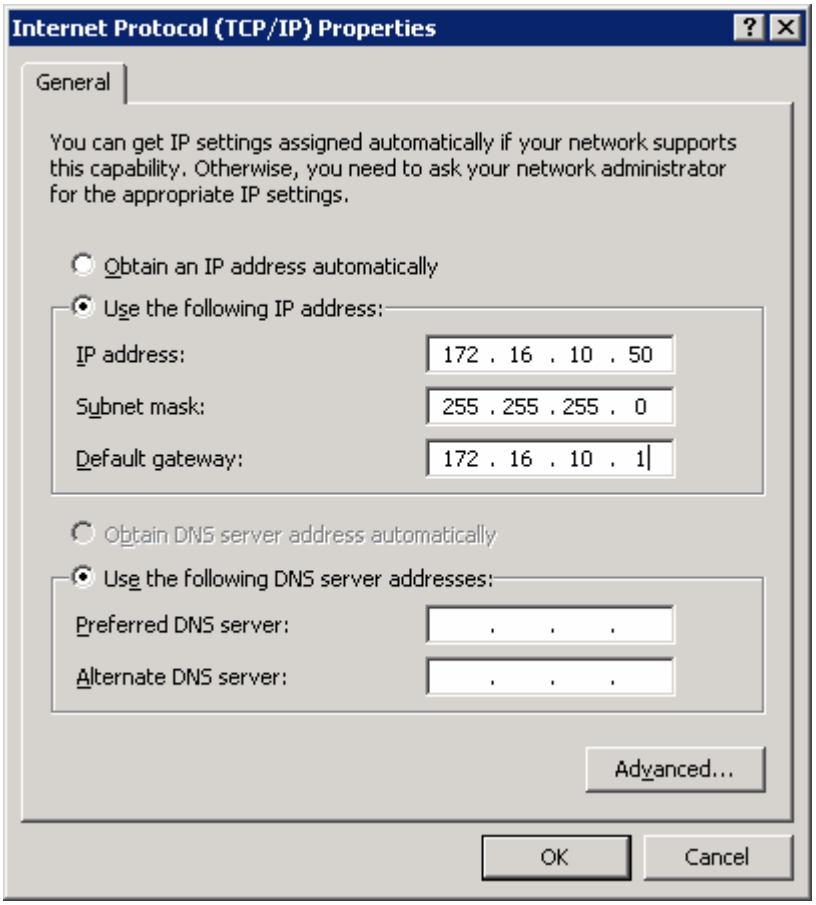


Figure 5-3: Configure IP Address, Subnet, and Gateway

Click **OK** to apply the TCP/IP settings, and then again to exit the configuration dialog box. From the Start Menu, click **Run**. Issue the **cmd** command and press the Return key. At the Windows command-line prompt, ping DLS1's VLAN 10 interface. You should receive responses. If you do not, troubleshoot, verifying the VLAN of the switchport and the IP address and subnet mask on each of the devices on VLAN 10.

```
C:\Documents and Settings\Administrator> ping 172.16.10.1

Pinging 172.16.10.1 with 32 bytes of data:

Reply from 172.16.10.1: bytes=32 time=1ms TTL=255
Reply from 172.16.10.1: bytes=32 time<1ms TTL=255
Reply from 172.16.10.1: bytes=32 time<1ms TTL=255
Reply from 172.16.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```


Step 7

Enable IP routing on DLS1. This lets DLS1 route between all subnets shown in the diagram. DLS1 can effectively route between all the VLANs configured because it has an SVI in each subnet. Each IP subnet is shown in the output of the **show ip route** command issued on DLS1.

```
DLS1(config)# ip routing

DLS1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 7 subnets
C       172.16.1.0 is directly connected, Vlan1
C       172.16.2.0 is directly connected, Vlan2
C       172.16.3.0 is directly connected, Vlan3
C       172.16.10.0 is directly connected, Vlan10
C       172.16.50.0 is directly connected, Vlan50
C       172.16.100.0 is directly connected, Vlan100
```

Step 8

When you first restart the WLAN controller, a configuration wizard prompts you to enter basic configuration attributes. You will know that you have entered the wizard interface when you see “Welcome to the Cisco Wizard Configuration Tool.” Pressing the Return key allows the default configuration options to be used. The default option will be in square brackets in the wizard prompts. If there is more than once choice in square brackets, it will be the option in capital letters.

The first prompt asks for a hostname. Use the default. Use “cisco” as both the username and password.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_49:43:c0]:
Enter Administrative User Name (24 characters max): cisco
Enter Administrative Password (24 characters max): <cisco>
```

Enter the management interface information. The management interface communicates with the management workstation in VLAN 1. The interface number is 1, because this is the port trunked from the controller to the switch. The VLAN number is 0 for untagged. It is untagged because VLAN 1 is the native 802.1q VLAN, and is therefore sent untagged through 802.1q trunks.

```
Management Interface IP Address: 172.16.1.100
Management Interface Netmask: 255.255.255.0
```



```
Management Interface Default Router: 172.16.1.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 172.16.1.1
```

Configure an interface to communicate with the lightweight access points. This will be in VLAN 100 and is tagged as such on the trunk.

```
AP Manager Interface IP Address: 172.16.100.100
AP Manager Interface Netmask: 255.255.255.0
AP Manager Interface Default Router: 172.16.100.1
AP Manager Interface VLAN Identifier (0 = untagged): 100
AP Manager Interface Port Num [1 to 4]: 1
AP Manager Interface DHCP Server (172.16.1.1): 172.16.100.1
```

Configure the virtual gateway IP address as 1.1.1.1 (this is acceptable because you are not using this for routing). The virtual gateway IP address is typically a fictitious, unassigned IP address, such as the address we are using here, to be used by Layer 3 Security and Mobility managers.

```
Virtual Gateway IP Address: 1.1.1.1
```

Configure the mobility group and network name as “ccnppod.” Allow static IP addresses by hitting enter, but do not configure a RADIUS server now.

```
Mobility/RF Group Name: ccnppod

Network Name (SSID): ccnppod
Allow Static IP Addresses [YES][no]:

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.

Please see documentation for more details.
```

Use the defaults for the rest of the settings. (Hit enter on each prompt).

```
Enter Country Code (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:

Configuration saved!
Resetting system with new configuration...
```

Step 9

When the WLAN controller has finished restarting, log in with the username “cisco” and password “cisco.”

```
User: cisco
Password: <cisco>
```


Change the controller prompt to WLAN_CONTROLLER with the **config prompt** *name* command. Notice that the prompt changes.

```
(Cisco Controller) > config prompt WLAN_CONTROLLER

(WLAN_CONTROLLER) >
```

Enable Telnet and HTTP access to the WLAN controller. HTTPS access is enabled by default, but unsecured HTTP is not.

```
(WLAN_CONTROLLER) > config network telnet enable

(WLAN_CONTROLLER) > config network webmode enable
```

Save your configuration with the **save config** command, which is analogous to the Cisco IOS **copy run start** command.

```
(WLAN_CONTROLLER) > save config

Are you sure you want to save? (y/n) y

Configuration Saved!
```

To verify the configuration, you can issue the **show interface summary**, **show wlan summary**, and **show run-config** commands on the WLAN controller.

How is the WLAN controller's **show run-config** command different than the Cisco IOS **show running-config** command?

Final Configurations

```
DLS1# show run
hostname DLS1
!
ip routing
ip dhcp excluded-address 172.16.1.1 172.16.1.150
ip dhcp excluded-address 172.16.2.1 172.16.2.150
ip dhcp excluded-address 172.16.3.1 172.16.3.150
ip dhcp excluded-address 172.16.10.1 172.16.10.150
ip dhcp excluded-address 172.16.50.1 172.16.50.150
ip dhcp excluded-address 172.16.100.1 172.16.100.150
!
ip dhcp pool pool2
   network 172.16.2.0 255.255.255.0
   default-router 172.16.2.1
!
ip dhcp pool pool3
   network 172.16.3.0 255.255.255.0
   default-router 172.16.3.1
!
ip dhcp pool pool10
   network 172.16.10.0 255.255.255.0
   default-router 172.16.10.1
!
```



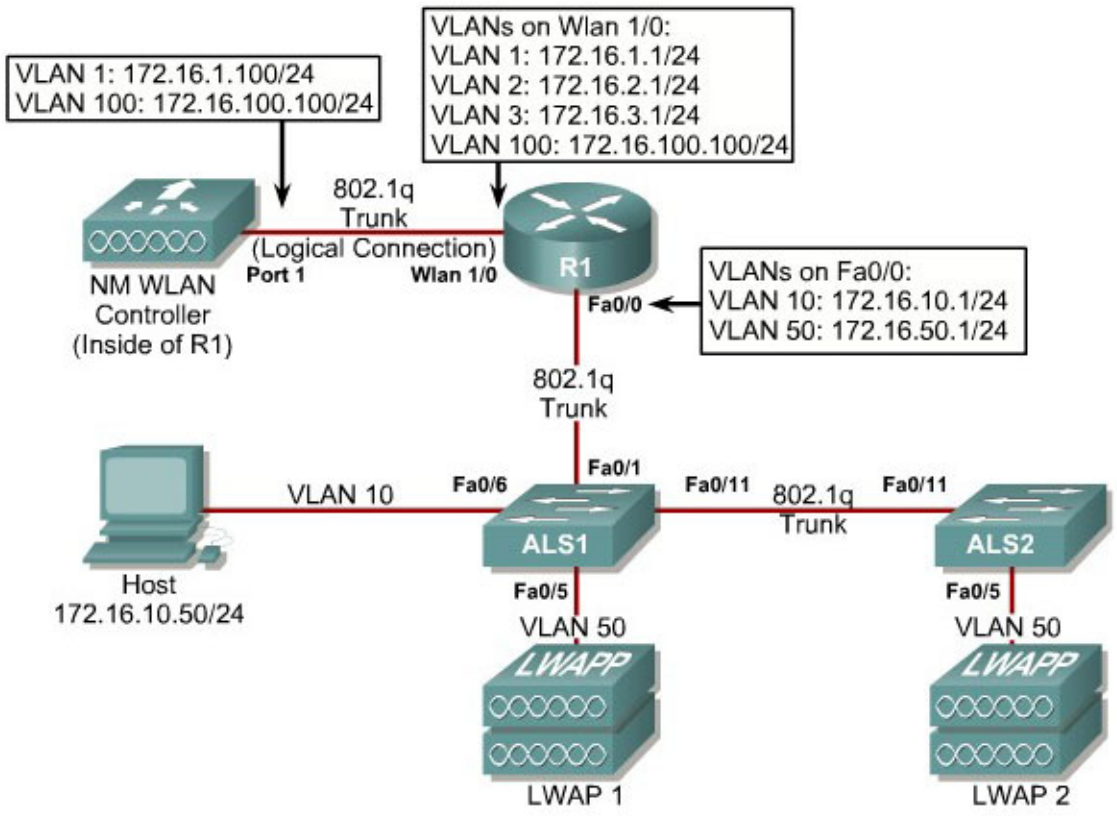
```
ip dhcp pool pool50
   network 172.16.50.0 255.255.255.0
   default-router 172.16.50.1
   option 43 hex f104ac106464
   option 60 ascii "Cisco AP c1240"
!
ip dhcp pool pool100
   network 172.16.100.0 255.255.255.0
   default-router 172.16.100.1
!
ip dhcp pool pool1
   network 172.16.1.0 255.255.255.0
   default-router 172.16.1.1
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan1
 ip address 172.16.1.1 255.255.255.0
 no shutdown
!
interface Vlan2
 ip address 172.16.2.1 255.255.255.0
 no shutdown
!
interface Vlan3
 ip address 172.16.3.1 255.255.255.0
 no shutdown
!
interface Vlan10
 ip address 172.16.10.1 255.255.255.0
 no shutdown
!
interface Vlan50
 ip address 172.16.50.1 255.255.255.0
 no shutdown
!
interface Vlan100
 ip address 172.16.100.1 255.255.255.0
 no shutdown
end

ALS1# show run
hostname ALS1
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
```



```
!
interface FastEthernet0/7
 switchport mode trunk
end

ALS2# show run
hostname ALS2
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport mode trunk
!
end
```


Lab 6-1 Configuring a WLAN Controller

Topology Diagram



Scenario

In the next two labs, you will configure a wireless solution involving a router with a built-in WLAN controller, two lightweight wireless access points, and a switched wired network. You will configure a WLAN controller to broadcast SSIDs from the lightweight wireless access points. If you have a wireless client nearby, connect to the WLANs and access devices from the inside of your pod to verify your configuration of the controller and access points.

Note: It is required that you upgrade the NM WLC firmware image to 4.0.206.0 or higher in order to accomplish this lab.

Step 1

Erase the startup-config file and delete the vlan.dat file from each switch, and erase the startup-config file on each router. Set hostnames on all of the devices.

Step 2

Explanation of VLANs:
VLAN 1 – This VLAN is the management VLAN for the WLC
VLAN 2 and VLAN 3 – These VLANs are for hosts in the WLANs
VLAN 10 – The host is in this VLAN
VLAN 50 – The APs are in this VLAN
VLAN 100 – The AP-manager interface of the WLC is in this VLAN

Configure ALS1 and ALS2 to run VTP in transparent mode in the VTP domain "CISCO", and create VLANs 10 and 50 on them. Also, set up a trunk link between them as well as towards R1.

```
ALS1(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
ALS1(config)# vtp domain CISCO
Changing VTP domain name from NULL to CISCO
ALS1(config)# vlan 10,50
ALS1(config-vlan)# int fastethernet0/1
ALS1(config-if)# switchport mode trunk
ALS1(config-if)# int fastethernet0/11
ALS1(config-if)# switchport mode trunk

ALS2(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
ALS2(config)# vtp domain CISCO
Changing VTP domain name from NULL to CISCO
ALS2(config)# vlan 10,50
ALS2(config-if)# int fastethernet0/11
ALS2(config-if)# switchport mode trunk
```

Step 3

Configure the subinterfaces on R1 for both FastEthernet0/0 and wlan-controller1/0 ports shown in the diagram. Both will be configured as 802.1q trunks with a VLAN on each subinterface. Make sure you use the native VLAN on the physical wlan-controller1/0 interface, as you will not be able to connect to the controller unless there is an IP address on the physical interface. Don't forget to add **no shutdown** commands to both physical interfaces.

```
R1(config)# int fastethernet0/0
R1(config-if)# no shutdown
R1(config-if)# int fastethernet0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.16.10.1 255.255.255.0
R1(config-subif)# int fastethernet0/0.50
R1(config-subif)# encapsulation dot1q 50
```



```
R1(config-subif)# ip address 172.16.50.1 255.255.255.0
R1(config-subif)# int wlan-controller1/0
R1(config-if)# ip address 172.16.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# int wlan-controller1/0.2
R1(config-subif)# encapsulation dot1q 2

If the interface doesn't support baby giant frames
maximum mtu of the interface has to be reduced by 4
bytes on both sides of the connection to properly
transmit or receive large packets. Please refer to
documentation on configuring IEEE 802.1Q vLANs.

R1(config-subif)# ip address 172.16.2.1 255.255.255.0
R1(config-subif)# int wlan-controller1/0.3
R1(config-subif)# encapsulation dot1q 3
R1(config-subif)# ip address 172.16.3.1 255.255.255.0
R1(config-subif)# int wlan-controller1/0.100
R1(config-subif)# encapsulation dot1q 100
R1(config-subif)# ip address 172.16.100.1 255.255.255.0
```

Step 4

DHCP gives out dynamic IP addresses on a subnet to network devices or hosts rather than statically setting the addresses. This is useful when dealing with lightweight access points, which usually do not have an initial configuration. The WLAN controller that the lightweight wireless access point associates with defines the configuration. A lightweight access point can dynamically receive an IP address and then communicate over IP with the WLAN controller. In this scenario, you will also use it to assign IP addresses to hosts that connect to the WLANs.

First, set up R1 to exclude the first 150 addresses from each subnet from DHCP to avoid conflicts with static IP addresses by using the global configuration command **ip dhcp excluded-address** *low-address* [*high-address*].

```
R1(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.150
R1(config)# ip dhcp excluded-address 172.16.2.1 172.16.2.150
R1(config)# ip dhcp excluded-address 172.16.3.1 172.16.3.150
R1(config)# ip dhcp excluded-address 172.16.10.1 172.16.10.150
R1(config)# ip dhcp excluded-address 172.16.50.1 172.16.50.150
R1(config)# ip dhcp excluded-address 172.16.100.1 172.16.100.150
```

To advertise on different subnets, create DHCP pools with the **ip dhcp pool** *name* command. After a pool is configured for a certain subnet, the IOS DHCP server processes requests on that subnet, because it is enabled by default. From the DHCP pool prompt, set the network and mask to use with the **network** *address* /*mask* command. Set a default gateway with the **default-router** *address* command.

VLAN 50 also uses the **option** command, which allows you to specify a DHCP option. In this case, option 43 is specified (a vendor-specific option), which gives the lightweight wireless access points the IP address of the WLAN

controller AP Manager interface. It is specified in a hexadecimal TLV (type, length, value) format. F1 is the hardcoded type of option, 04 represents the length of the value (an IP address is 4 octets), and AC106464 is the hexadecimal representation of 172.16.100.100, which is going to be the AP manager address of the WLAN controller. DHCP option 60 specifies the identifier that access points will use in DHCP. This lab was written using Cisco Aironet 1240 series access points. If you are using a different access point series, consult http://www.cisco.com/univercd/cc/td/doc/product/wireless/aero1500/1500hig5/1500_axg.htm.

```
R1(config)# ip dhcp pool pool1
R1(dhcp-config)# network 172.16.1.0 /24
R1(dhcp-config)# default-router 172.16.1.1
R1(dhcp-config)# ip dhcp pool pool2
R1(dhcp-config)# network 172.16.2.0 /24
R1(dhcp-config)# default-router 172.16.2.1
R1(dhcp-config)# ip dhcp pool pool3
R1(dhcp-config)# network 172.16.3.0 /24
R1(dhcp-config)# default-router 172.16.3.1
R1(dhcp-config)# ip dhcp pool pool10
R1(dhcp-config)# network 172.16.10.0 /24
R1(dhcp-config)# default-router 172.16.10.1
R1(dhcp-config)# ip dhcp pool pool50
R1(dhcp-config)# network 172.16.50.0 /24
R1(dhcp-config)# default-router 172.16.50.1
R1(dhcp-config)# option 43 hex f104ac106464
R1(dhcp-config)# option 60 ascii "Cisco AP c1240"
R1(dhcp-config)# ip dhcp pool pool100
R1(dhcp-config)# network 172.16.100.0 /24
R1(dhcp-config)# default-router 172.16.100.1
```

Step 5

On both switches, configure all access points to bypass the spanning-tree port states with the **spanning-tree portfast** command. With this command, each access point receives an IP address from DHCP immediately, without worrying about timing out from DHCP. Configure the switchports going to the lightweight wireless access points in VLAN 50. R1 will route the tunneled WLAN traffic towards the WLAN controllers AP-manager interface.

```
ALS1(config)# int fastethernet0/5
ALS1(config-if)# switchport mode access
ALS1(config-if)# switchport access vlan 50
ALS1(config-if)# spanning-tree portfast

ALS2(config)# int fastethernet0/5
ALS2(config-if)# switchport mode access
ALS2(config-if)# switchport access vlan 50
ALS2(config-if)# spanning-tree portfast
```

Step 6

You have a PC running Microsoft Windows attached to ALS1. First, configure the switchport connecting to the host in VLAN 10 with portfast. Management

traffic from the host for the WLAN controller will be routed to R1 towards the management interface of the WLC.

```
ALS1(config)# int fastethernet0/6
ALS1(config-if)# switchport mode access
ALS1(config-if)# switchport access vlan 10
ALS1(config-if)# spanning-tree portfast
```

Next, configure the host with an IP address in VLAN 10, which will later be used to access the HTTP web interface of the WLAN controller later. Follow the procedure below to prepare the host to access the WLAN controller.

In the **Control Panel**, select **Network Connections**.

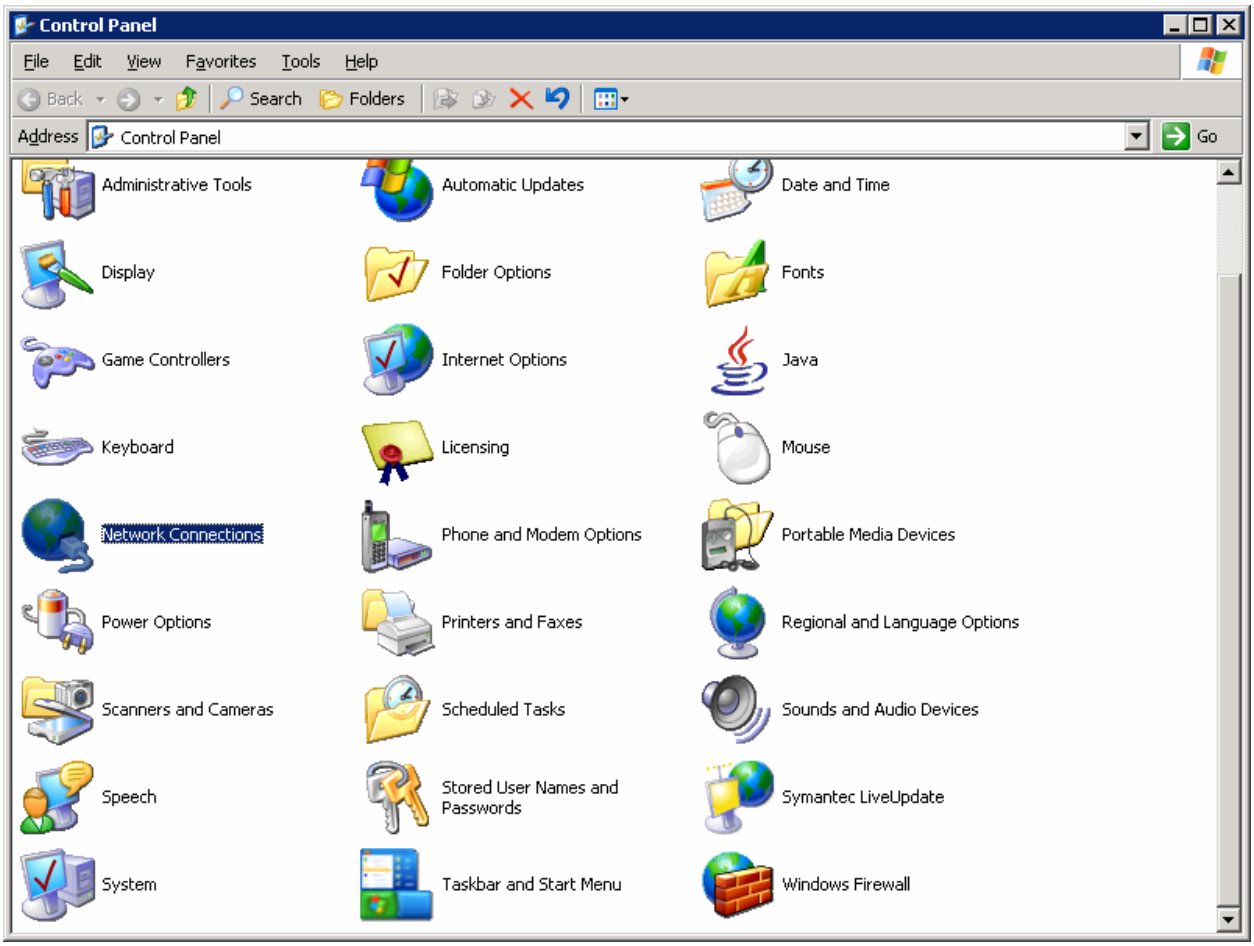


Figure 5-1: Microsoft Windows Control Panel

Right-click on the LAN interface that connects to ALS1, and select **Properties**. Select **Internet Protocol (TCP/IP)** and then click the **Properties** button.

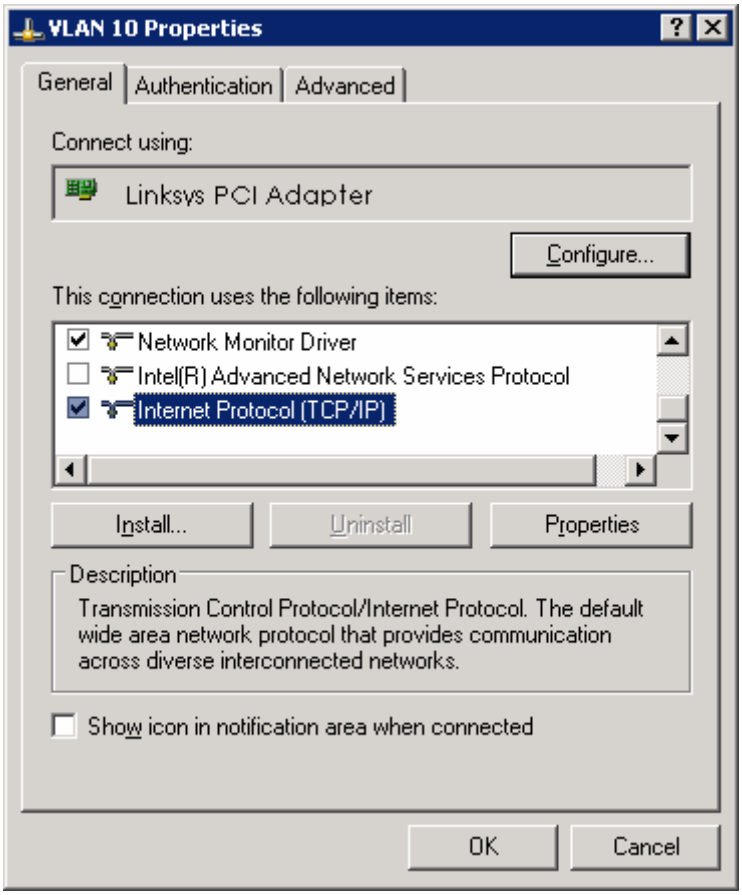


Figure 5-2: Modify the Properties for Interface on VLAN 10

Finally, configure the IP address shown in the diagram on the interface.

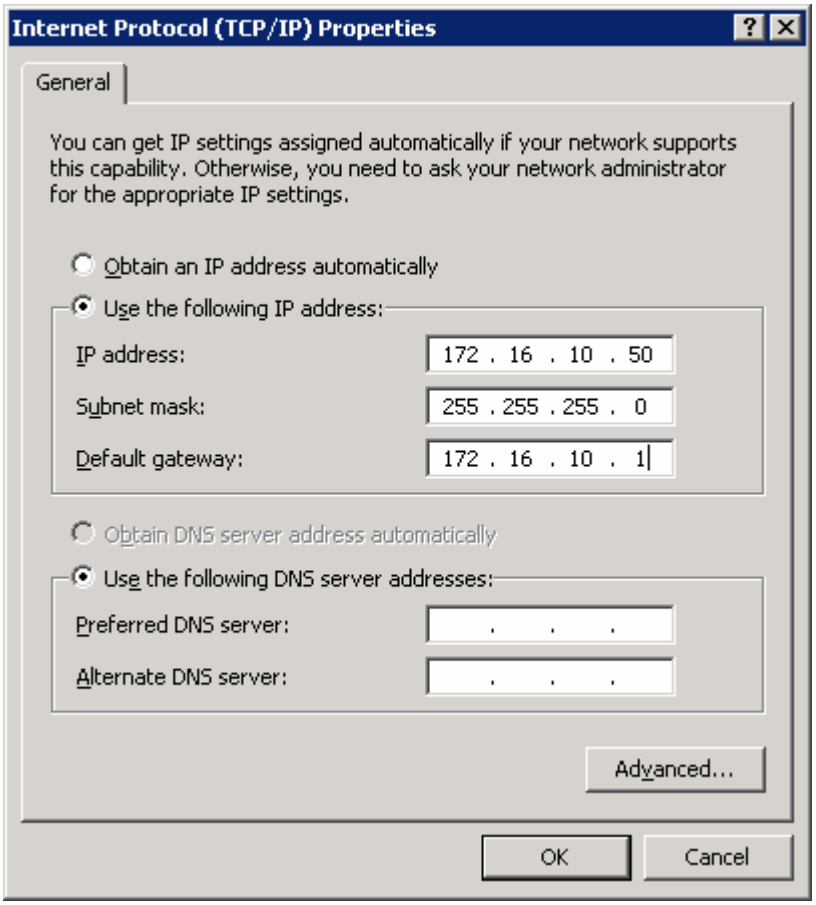


Figure 5-3: Configure IP Address, Subnet, and Gateway

Click **OK** to apply the TCP/IP settings, and then again to exit the configuration dialog box. From the Start Menu, click **Run**. Issue the **cmd** command and press the Return key. At the Windows command-line prompt, ping R1's VLAN 10 interface. You should receive responses. If you do not, troubleshoot, verifying the VLAN of the switchport and the IP address and subnet mask on each of the devices on VLAN 10.

```
C:\Documents and Settings\Administrator> ping 172.16.10.1

Pinging 172.16.10.1 with 32 bytes of data:

Reply from 172.16.10.1: bytes=32 time=1ms TTL=255
Reply from 172.16.10.1: bytes=32 time<1ms TTL=255
Reply from 172.16.10.1: bytes=32 time<1ms TTL=255
Reply from 172.16.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```


Step 7

R1 will route between all subnets shown in the diagram, because it has a connected interface in each subnet. Each IP subnet is shown in the output of the **show ip route** command issued on R1.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 6 subnets
C       172.16.50.0 is directly connected, FastEthernet0/0.50
C       172.16.10.0 is directly connected, FastEthernet0/0.10
C       172.16.1.0 is directly connected, wlan-controller1/0
C       172.16.2.0 is directly connected, wlan-controller1/0.2
C       172.16.3.0 is directly connected, wlan-controller1/0.3
C       172.16.100.0 is directly connected, wlan-controller1/0.100
```

Step 8

Now that the underlying network infrastructure is set up, you can set up the WLAN controller.

At R1's privileged exec prompt, you can control the state of the WLC inside R1. To see what types of commands you can execute, use the command **service-module *interface* ?**.

```
R1#service-module wlan-controller1/0 ?
  reload      Reload service module
  reset       Hardware reset of Service Module
  session     Service module session
  shutdown    Shutdown service module
  statistics  Service Module Statistics
  status      Service Module Information
```

After you review what you can do to the internal wlan-controller, reset it. Right after the line protocol comes back up on the controller, connect to it using the **session** argument for **service-module** as shown below.

```
R1#service-module wlan-controller1/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disc!
Do you want to reset?[confirm]
Trying to reset Service Module wlan-controller1/0.

R1#
*Feb 14 06:27:03.311: %LINEPROTO-5-UPDOWN: Line protocol on Interface wlan-
controller1/0, changed state to down
*Feb 14 06:27:23.311: %LINEPROTO-5-UPDOWN: Line protocol on Interface wlan-
controller1/0, changed state to up
R1#service-module wlan-controller1/0 session
```



```
Trying 172.16.1.1, 2066 ... Open
Cisco Bootloader Loading stage2...

    Cisco Bootloader (Version 4.0.206.0)


                     .o88b. d888888b .d8888.  .o88b.  .d88b.
                    d8P  Y8   `88'   88'  YP d8P  Y8 .8P  Y8.
                    8P         88    `8bo.   8P      88    88
                    8b         88      `Y8b. 8b      88    88
                    Y8b  d8   .88.   db   8D Y8b  d8 `8b  d8'
                     `Y88P' Y888888P `8888Y'  `Y88P'  `Y88P'

<OUTPUT OMITTED>
```

If you start up the WLC and it does not have a cleared configuration, you may use “Recover-Config” as the first username used to login after the NM has been restarted. If you are already at a command prompt for the WLC, use the **clear config** command followed by the **reset system** command.

Once connected to the WLAN controller with an erased configuration, a wizard starts to allow you to configure basic settings. Pressing the Return key allows the default configuration options to be used (whatever appears in square brackets will be the default, and if there are multiple entries in square brackets, the one in capital letters will be the default).

The first prompt asks for a hostname. Use the default. Use “cisco” as both the username and password.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_49:43:c0]:
Enter Administrative User Name (24 characters max): cisco
Enter Administrative Password (24 characters max): <cisco>
```

Enter the management interface information. The management interface communicates with the management workstation in VLAN 1. The interface number is 1, because this is the only interface on the NM WLC (it is the logical connection to R1’s wlan-controller1/0). The VLAN number is 0 for untagged. It is untagged it is the native 802.1q VLAN, and is going to be sent to the physical (non-subinterface) interface of R1.

```
Management Interface IP Address: 172.16.1.100
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 172.16.1.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1]: 1
Management Interface DHCP Server IP Address: 172.16.1.1
```

Configure an interface to communicate with the lightweight access points (tunneled access point traffic will be sent here). This will be in VLAN 100 and is tagged as such on the trunk.

```
AP Manager Interface IP Address: 172.16.100.100
```



```
AP Manager Interface Netmask: 255.255.255.0
AP Manager Interface Default Router: 172.16.100.1
AP Manager Interface VLAN Identifier (0 = untagged): 100
AP Manager Interface Port Num [1]: 1
AP Manager Interface DHCP Server (172.16.1.1): 172.16.100.1
```

Configure the virtual gateway IP address as 1.1.1.1 (this is acceptable because you are not using this for routing). The virtual gateway IP address is typically a fictitious, unassigned IP address, such as the address we are using here, to be used by Layer 3 Security and Mobility managers.

```
Virtual Gateway IP Address: 1.1.1.1
```

Configure the mobility group and network name as “ccnppod.” Allow static IP addresses by hitting enter, but do not configure a RADIUS server now.

```
Mobility/RF Group Name: ccnppod

Network Name (SSID): ccnppod
Allow Static IP Addresses [YES][no]:

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.

Please see documentation for more details.
```

Use the defaults for the rest of the settings by hitting enter, except for the time settings. Do not configure a time server, but do set the current time.

```
Enter Country Code (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 02/14/07
Enter the time in HH:MM:SS format: 02:17:00

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

Configuration saved!
Resetting system with new configuration...
```

Step 9

When the WLAN controller has finished restarting, log in with the username “cisco” and password “cisco.”

```
User: cisco
Password: <cisco>
```

Change the controller prompt to WLAN_CONTROLLER with the **config prompt** *name* command. Notice that the prompt changes.


```
(Cisco Controller) > config prompt WLAN_CONTROLLER

(WLAN_CONTROLLER) >
```

Enable Telnet and HTTP access to the WLAN controller. HTTPS access is enabled by default, but unsecured HTTP is not.

```
(WLAN_CONTROLLER) > config network telnet enable

(WLAN_CONTROLLER) > config network webmode enable
```

Save your configuration with the **save config** command, which is analogous to the Cisco IOS **copy run start** command.

```
(WLAN_CONTROLLER) > save config

Are you sure you want to save? (y/n) y


Configuration Saved!
```

To verify the configuration, you can issue the **show interface summary**, **show wlan summary**, and **show run-config** commands on the WLAN controller.

How is the WLAN controller's **show run-config** command different than the Cisco IOS **show running-config** command?

Final Configuration

```
R1#show run
hostname R1
!
ip dhcp excluded-address 172.16.1.1 172.16.1.150
ip dhcp excluded-address 172.16.2.1 172.16.2.150
ip dhcp excluded-address 172.16.3.1 172.16.3.150
ip dhcp excluded-address 172.16.10.1 172.16.10.150
ip dhcp excluded-address 172.16.50.1 172.16.50.150
ip dhcp excluded-address 172.16.100.1 172.16.100.150
!
ip dhcp pool pool1
   network 172.16.1.0 255.255.255.0
   default-router 172.16.1.1
!
ip dhcp pool pool2
   network 172.16.2.0 255.255.255.0
   default-router 172.16.2.1
!
ip dhcp pool pool3
   network 172.16.3.0 255.255.255.0
   default-router 172.16.3.1
!
ip dhcp pool pool10
   network 172.16.10.0 255.255.255.0
```



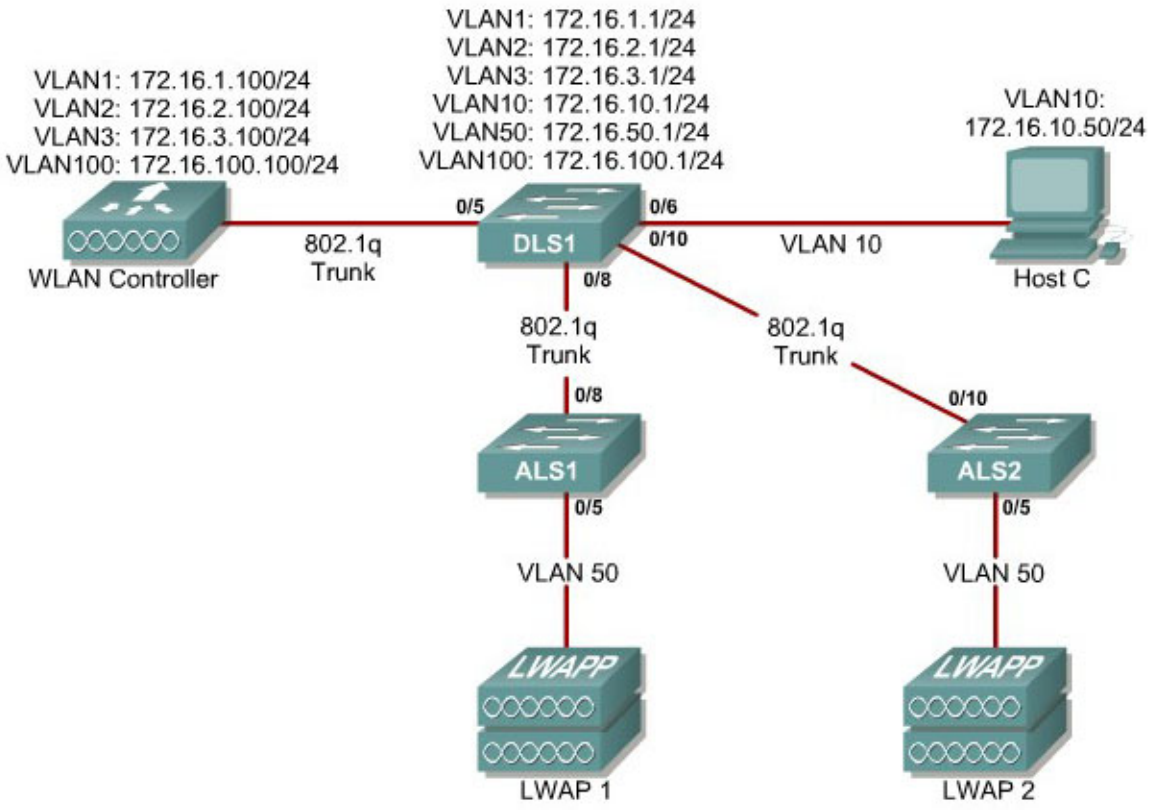
```
   default-router 172.16.10.1
!
ip dhcp pool pool50
   network 172.16.50.0 255.255.255.0
   default-router 172.16.50.1
   option 43 hex f104ac106464
   option 60 ascii "Cisco AP c1240"
!
ip dhcp pool pool100
   network 172.16.100.0 255.255.255.0
   default-router 172.16.100.1
!
interface FastEthernet0/0
 no shutdown
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.10.1 255.255.255.0
!
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 172.16.50.1 255.255.255.0
!
interface wlan-controller1/0
 ip address 172.16.1.1 255.255.255.0
 no shutdown
!
interface wlan-controller1/0.2
 encapsulation dot1Q 2
 ip address 172.16.2.1 255.255.255.0
!
interface wlan-controller1/0.3
 encapsulation dot1Q 3
 ip address 172.16.3.1 255.255.255.0
!
interface wlan-controller1/0.100
 encapsulation dot1Q 100
 ip address 172.16.100.1 255.255.255.0
end

ALS1#show run
hostname ALS1
!
vtp domain CISCO
vtp mode transparent
!
vlan 10,50
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport mode trunk
```



```
end

ALS2#show run
hostname ALS2
!
vtp domain CISCO
vtp mode transparent
!
vlan 10,50
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport mode trunk
end
```


Lab 6-2 Configuring a WLAN Controller via the Web Interface

Topology Diagram



Scenario

Continuing from the previous lab, you will now set up the WLAN controller through its web interface. Previously you configured it through the CLI.

Step 1

Set up all the switches as they were in the previous lab. Make sure that the WLAN controller and host also have the same configuration as before.

Step 2

On the host, open up Internet Explorer and go to the URL “https://172.16.1.100”. This is the secure method of connecting to the management interface of the WLAN controller. You can also use

"http://172.16.1.100" since we previously enabled regular insecure HTTP access in the CLI for Lab 6.1. If you connect to the secure address, you may be prompted with a security warning. Click **Yes** to accept it and you will be presented with the login screen for the WLAN controller. Click **Login** and an authentication dialog box will appear.

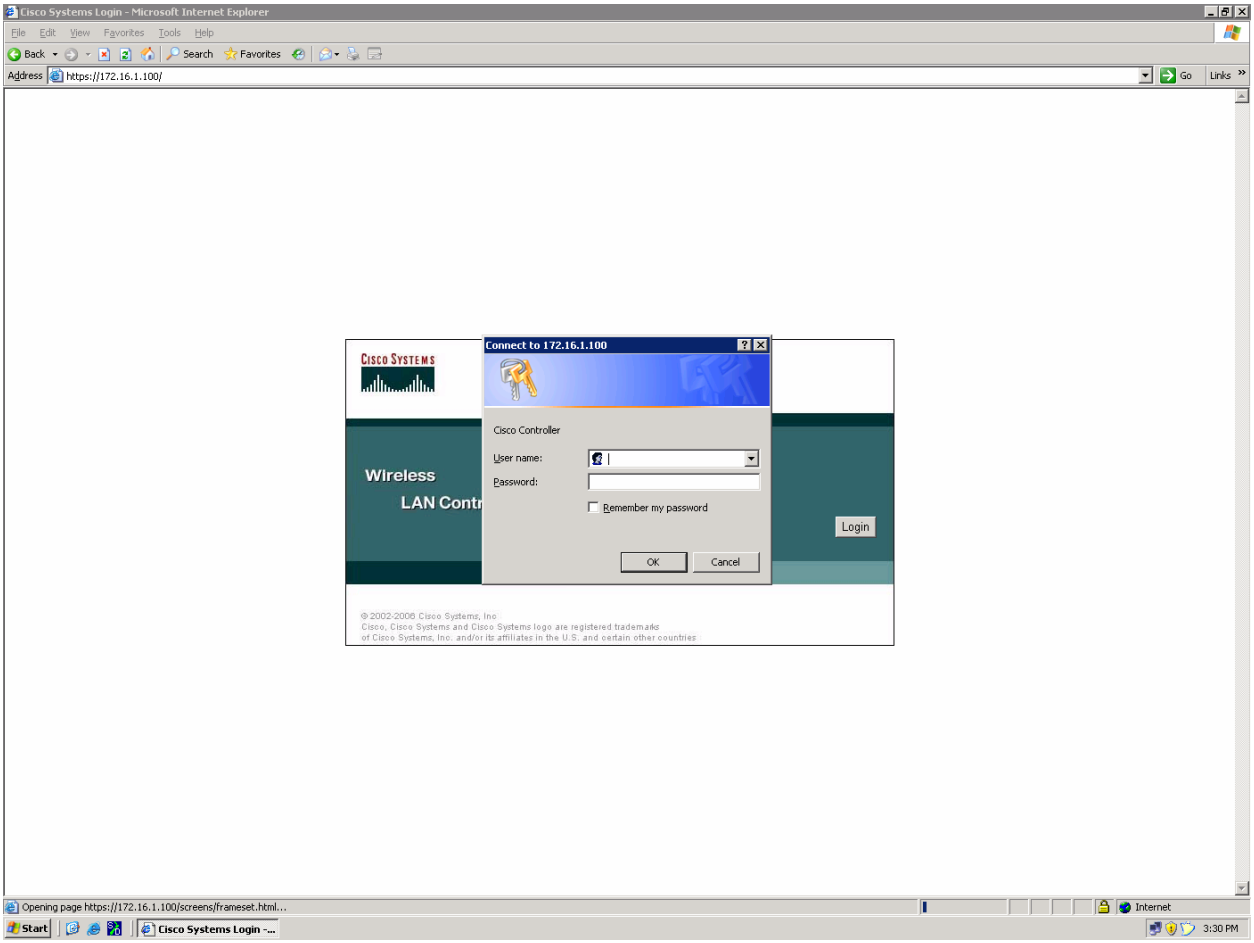


Figure 2-1: Authentication Dialog Box for WLAN Controller Web Access

Use "cisco" as both the username and password. You configured these in the previous lab. Click **OK** to get to the main page of the graphical user interface (GUI). You are then presented with the monitor page for the WLAN controller.

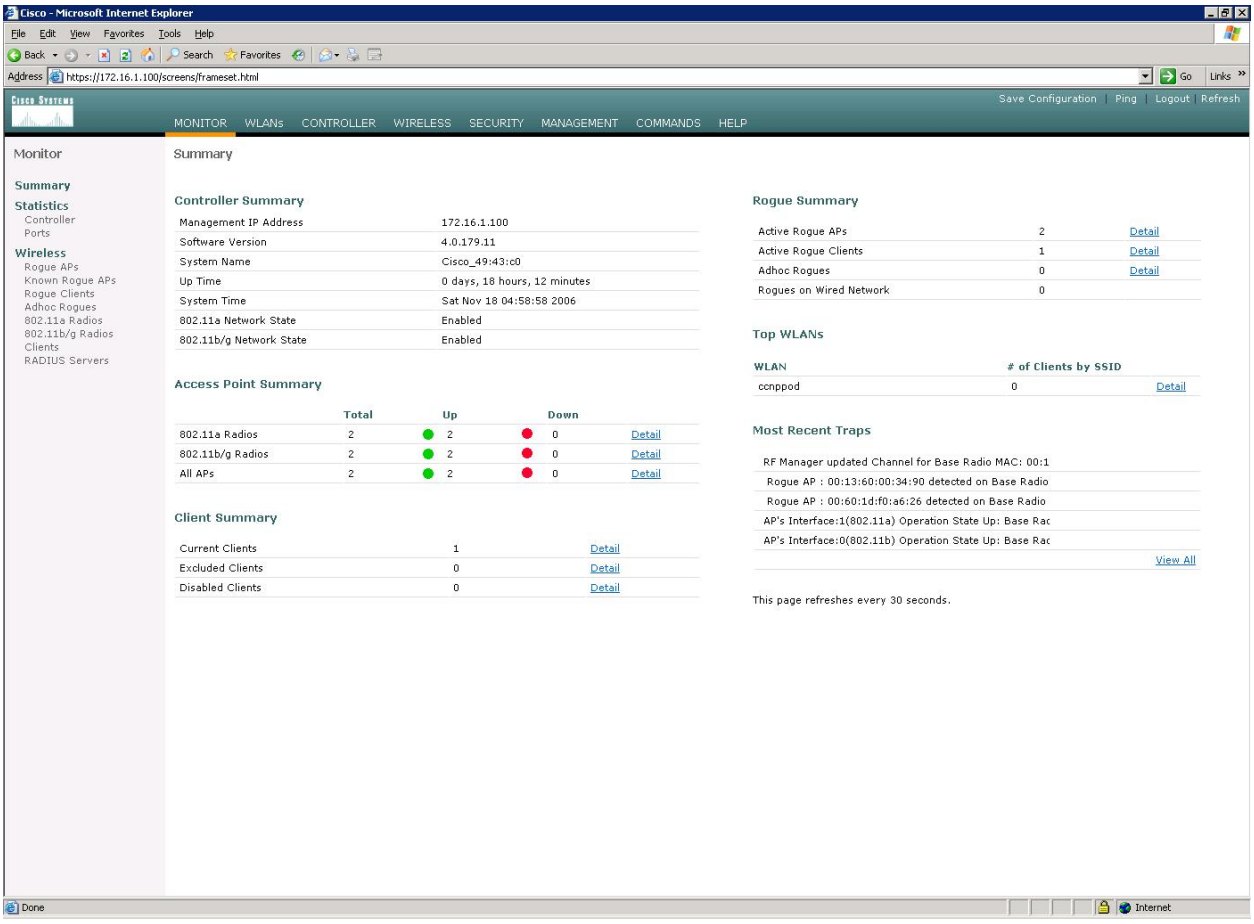


Figure 2-2: WLAN Controller Monitor Page

Make sure you see 2 access points under the “Access Point Summary” part of the page. You may also see it detecting rogue access points if your lab has other wireless networks around it; this behavior is normal. You can also see various port controller and port statistics by clicking their respective links on the left-hand menu on the screen.

Step 3

The next task in configuring WLANs is to add in the logical interfaces on the WLAN controller corresponding to VLANs 2 and 3. To do this, click the **Controller** link on the top of the web interface. Then, click **Interfaces** link on the left side bar.

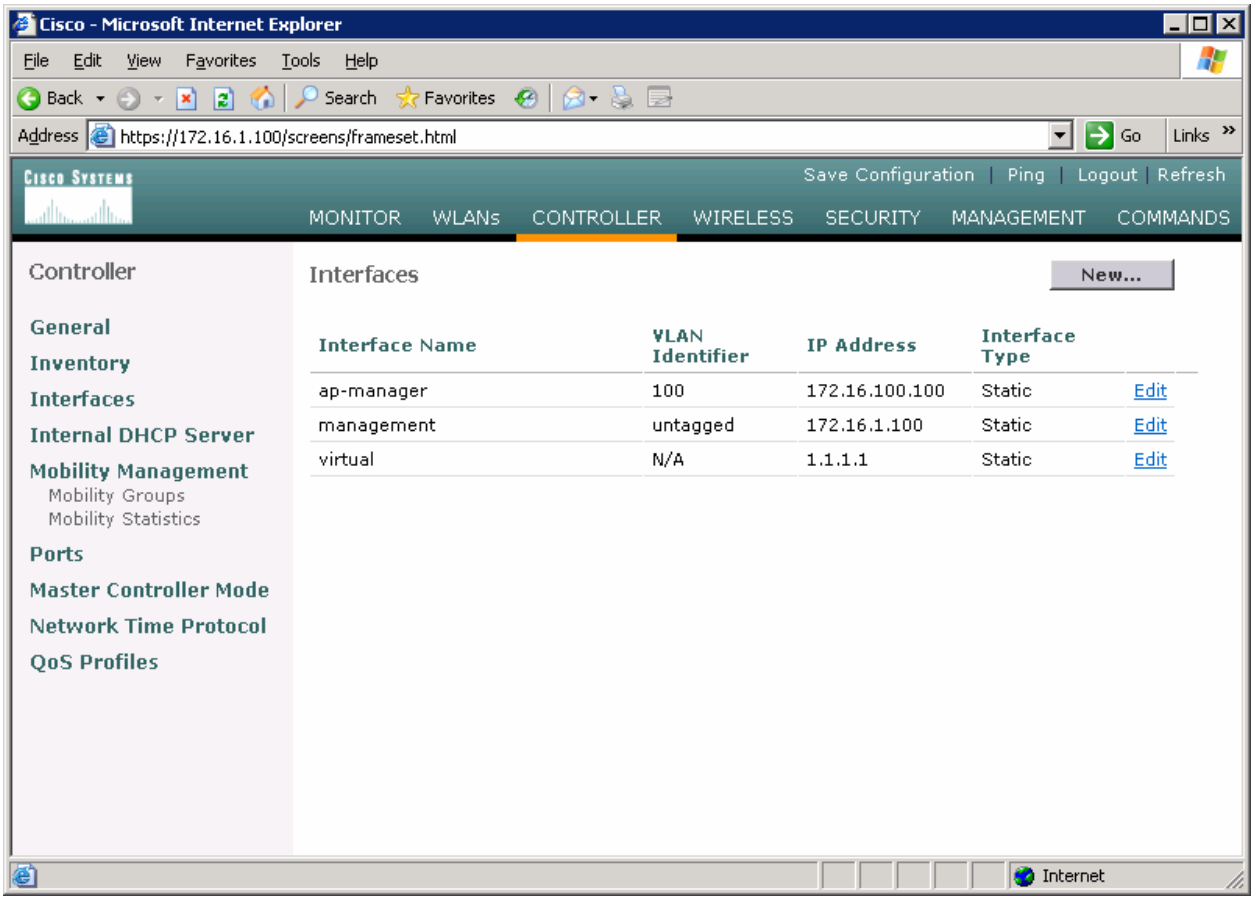


Figure 3-1: Interface Configuration Page

Click the **New...** link to create a new interface. Give the new interface a name of VLAN2 and VLAN number 2. Click **Apply** to submit the parameters.

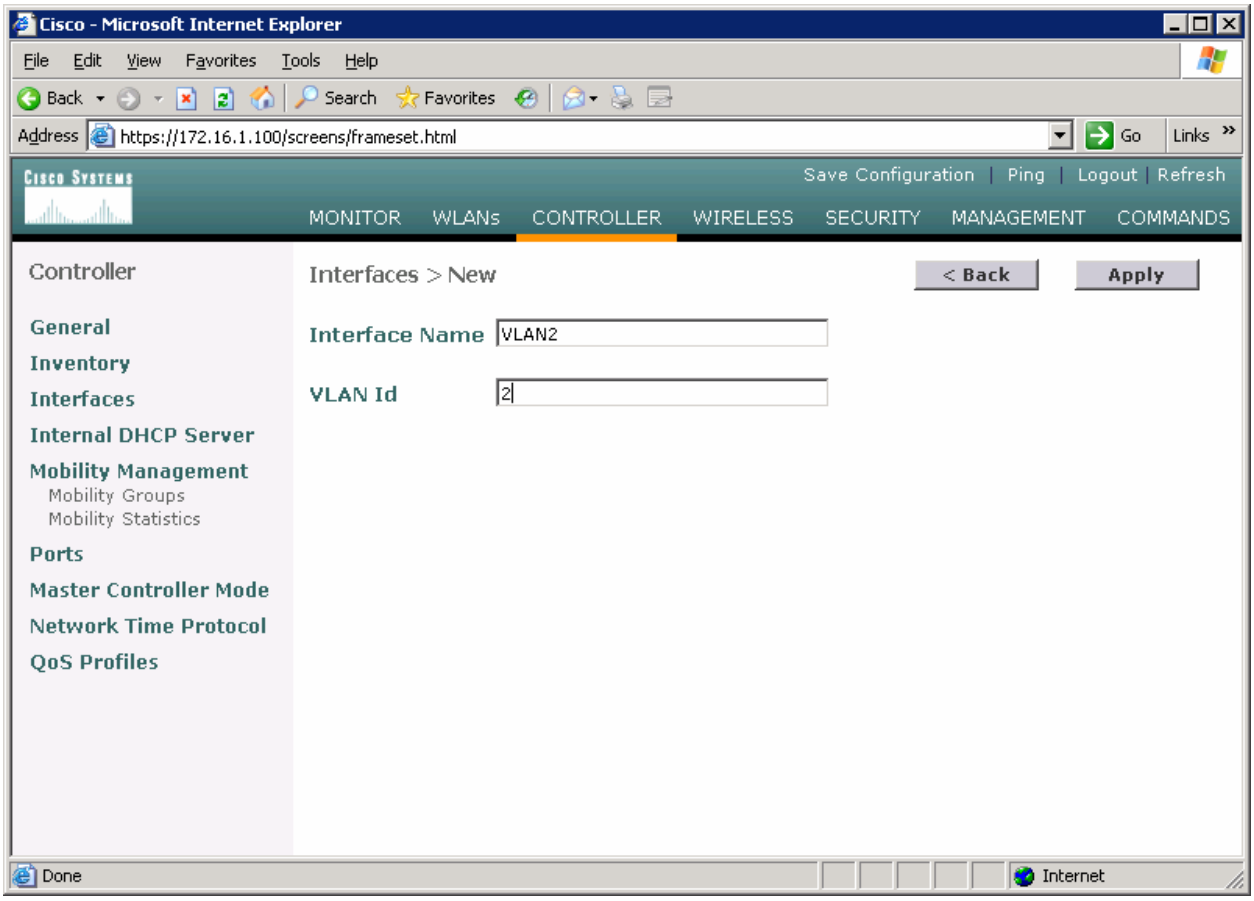


Figure 3-2: Creating a New VLAN Interface

On the next page, configure the IP address shown in the diagram. Also configure this on physical port 1, since that is the port trunked to the switch. After you have entered in all the changes, click **Apply**. Click **OK** to the warning box that comes up. This warning says that there may be a temporary connectivity loss on the APs while changes are applied.

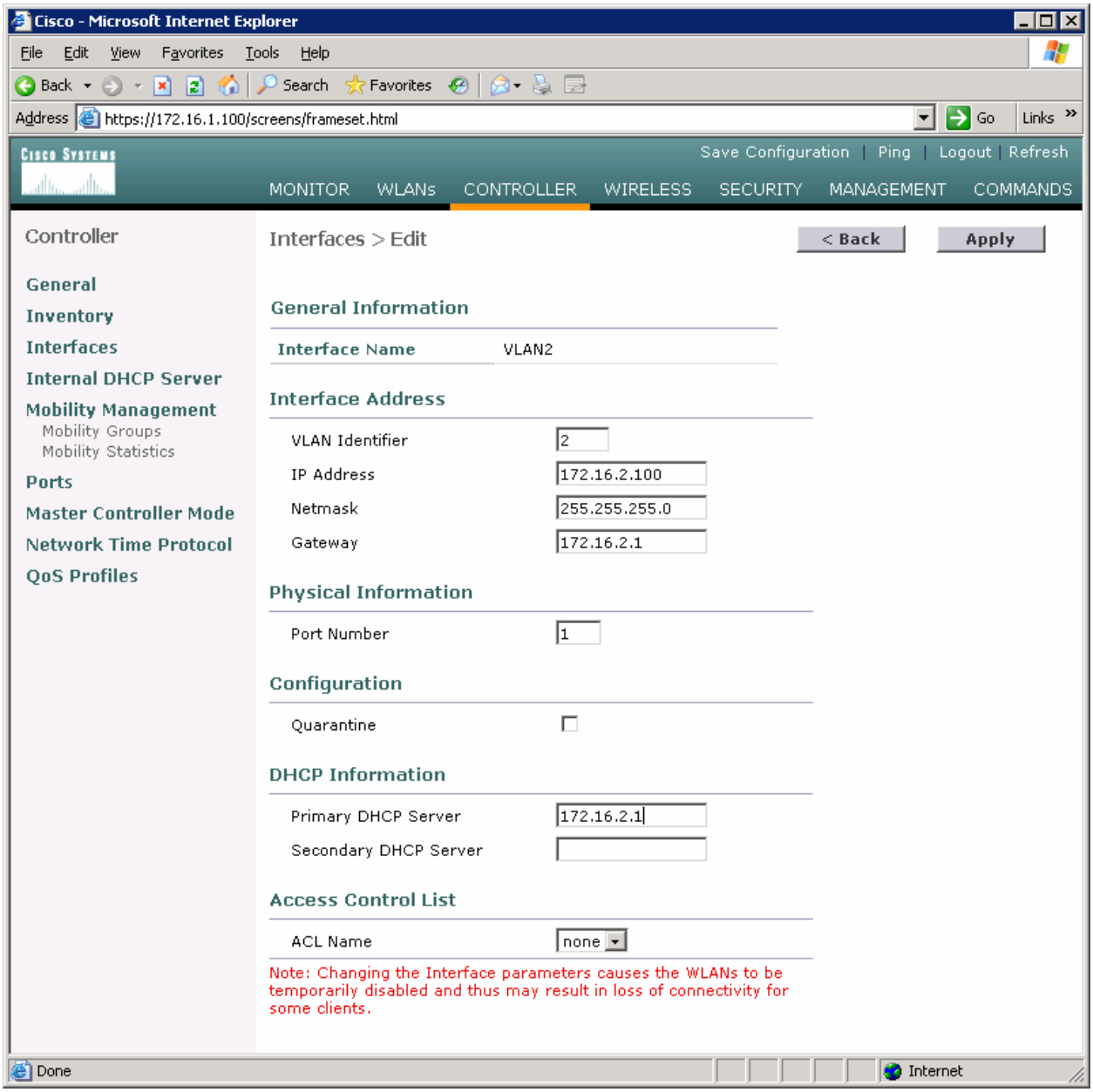


Figure 3-3: Configuring VLAN Interface Properties

The new interface should appear in the interfaces list. Do the same configuration steps for VLAN 3.

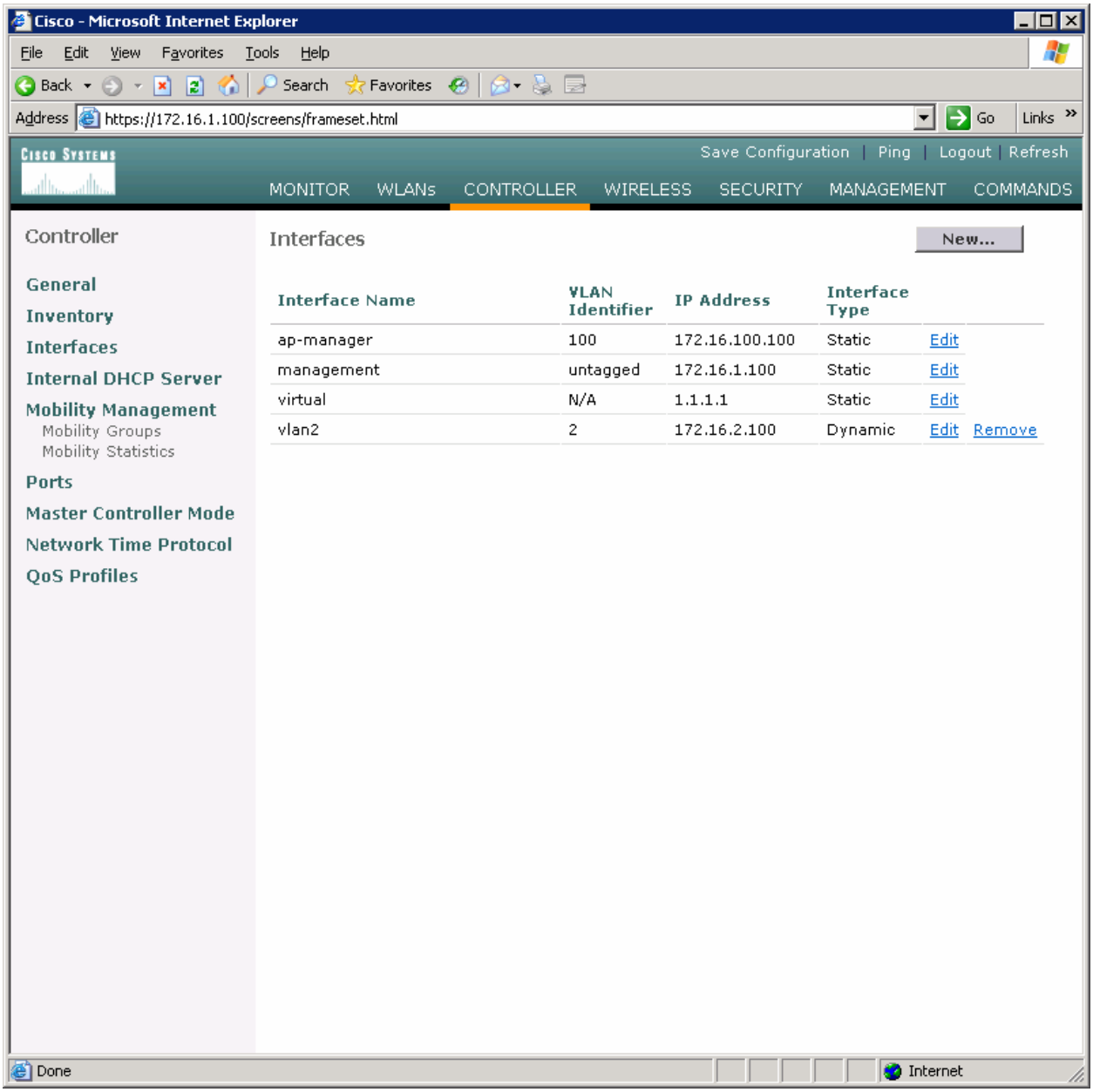


Figure 3-4: Verify Existing VLAN Interfaces

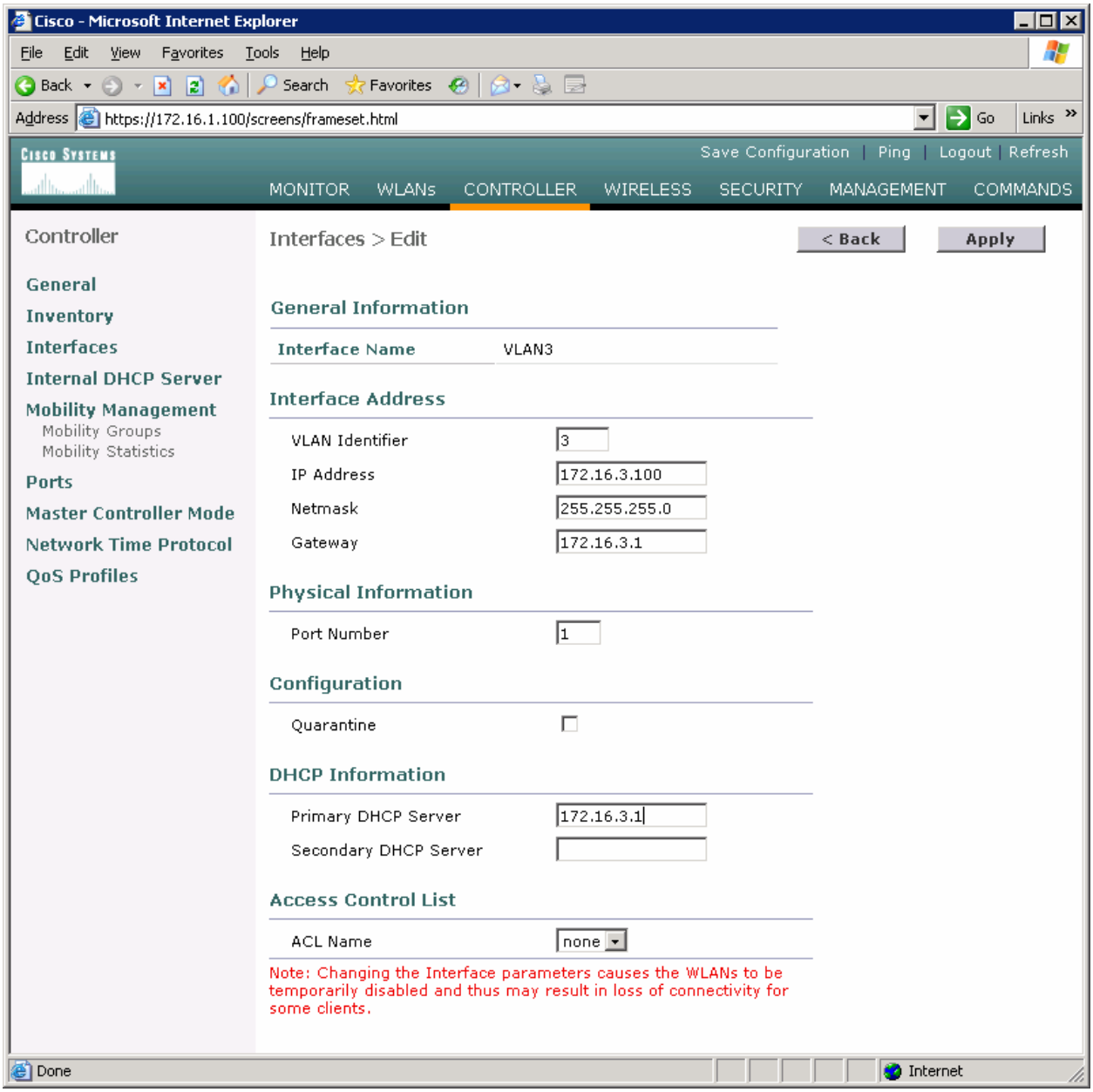


Figure 3-5: Configuring the VLAN 3 Interface

Make sure both interfaces appear in the interface table.

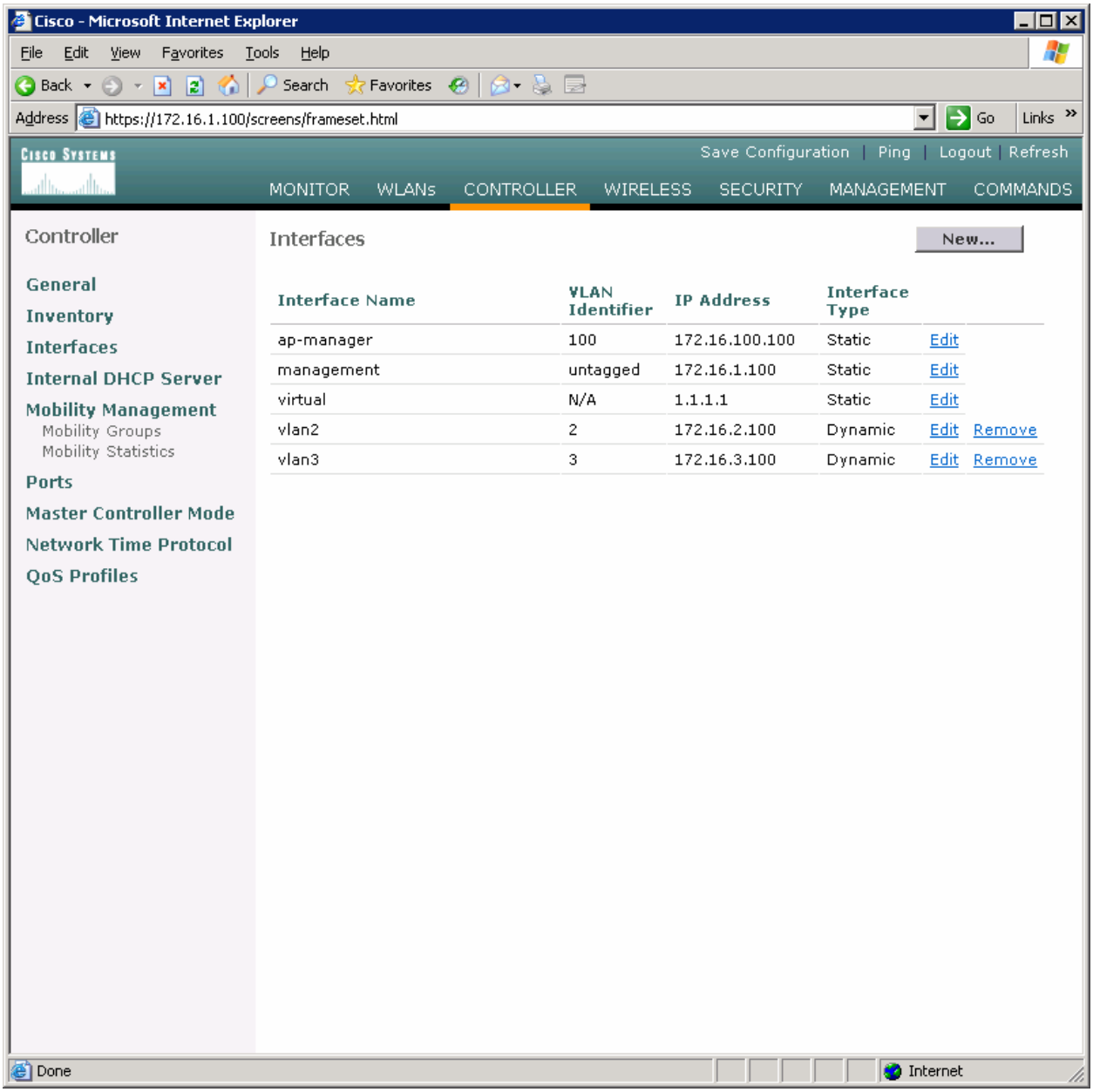


Figure 3-6: Verifying VLAN Interfaces on the WLAN Controller

Step 4

Now, you can configure the WLANs corresponding to these VLANs. To do this, first click the **WLANs** link at the top of the page. This will show you all configured WLANs.

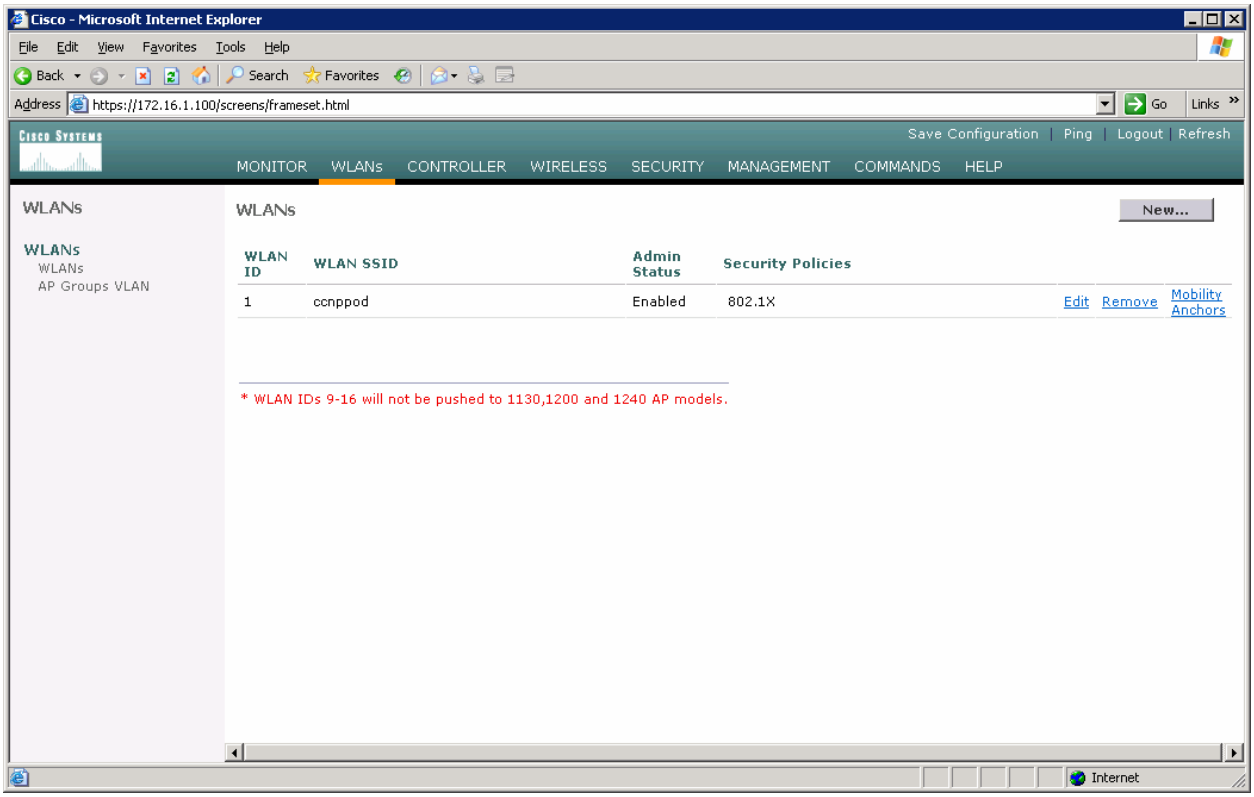


Figure 4-1: Viewing Existing WLANs

On the existing one, click **Edit** on the right of it. Remove the layer 2 security and change the interface to VLAN2. This will associate this WLAN with the correct VLAN.

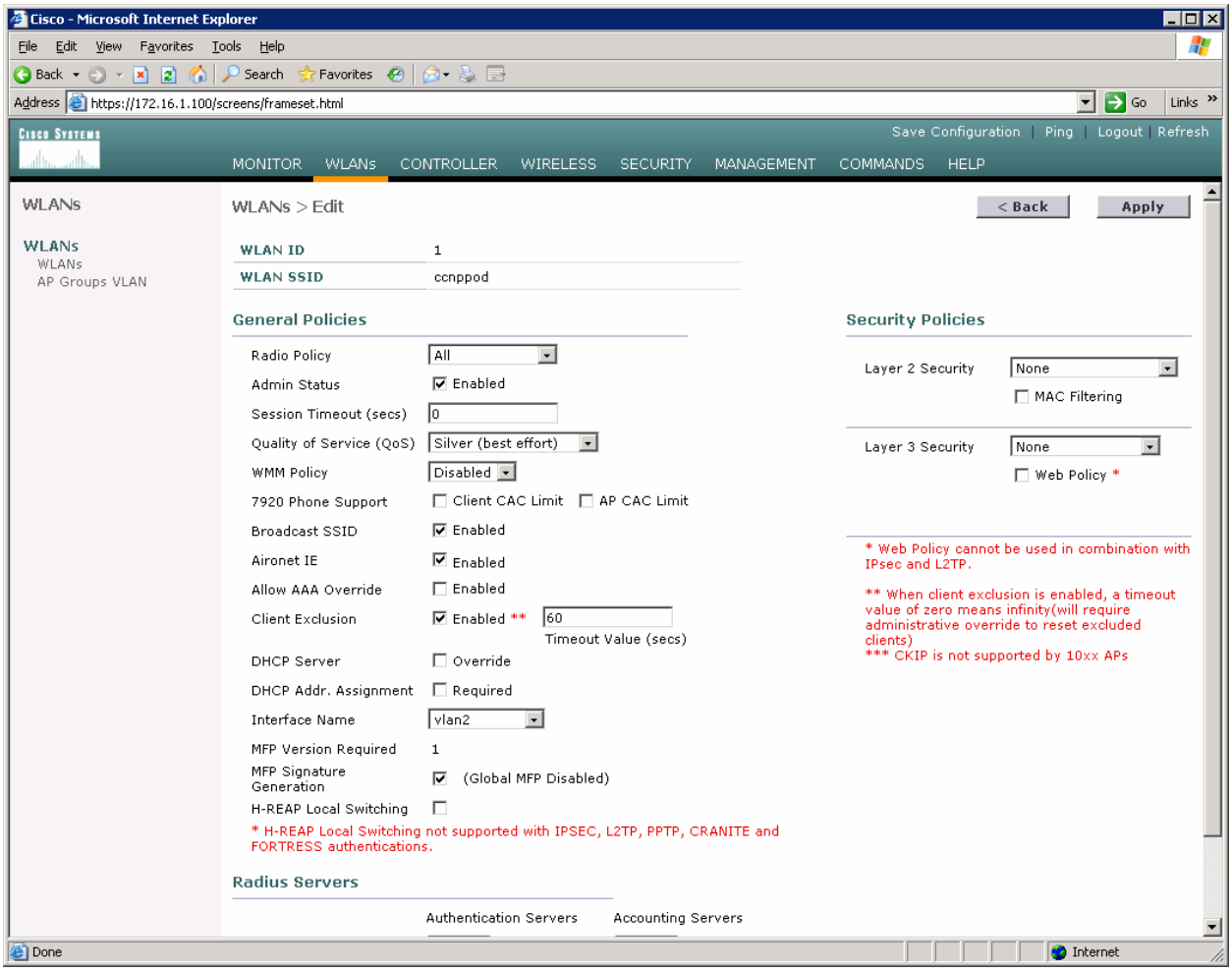


Figure 4-2: Edit the Configuration for WLAN 1

Click **Apply** and click **OK** to the warning box that comes up.

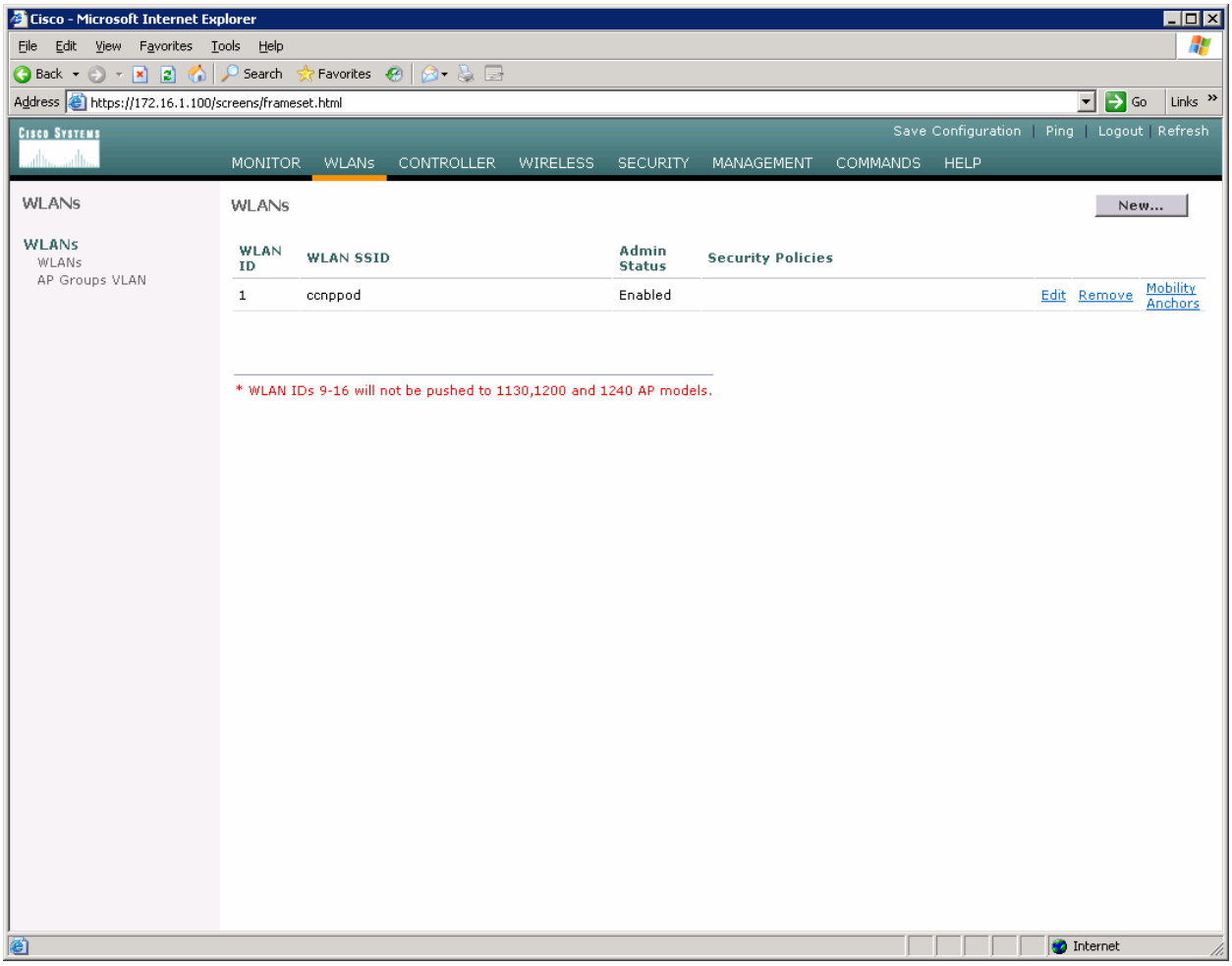


Figure 4-3: WLAN 1 without a Security Policy

Click **New...** and configure a WLAN for VLAN 3. Use the SSID “ccnplab”.

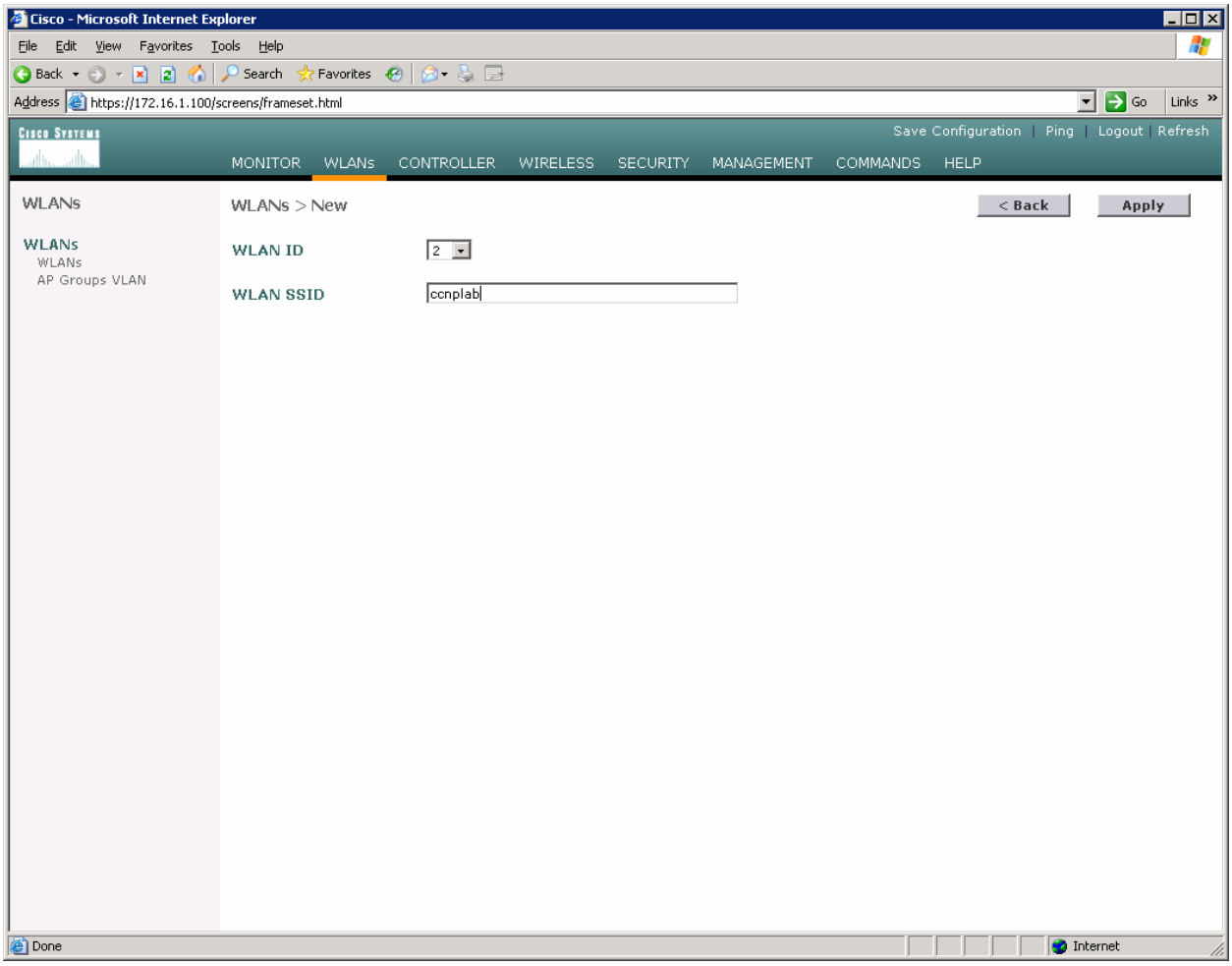


Figure 4-4: Adding a New SSID for WLAN 2

On this WLAN, configure the layer 2 security as Static WEP and use a 40 bit WEP key. Make the key index 2 and use a key of “cisco”. Also, set the administrative status of the WLAN to enabled and change the interface name to VLAN3. When you are done, click **Apply** and you should see both WLANs in the WLAN list.

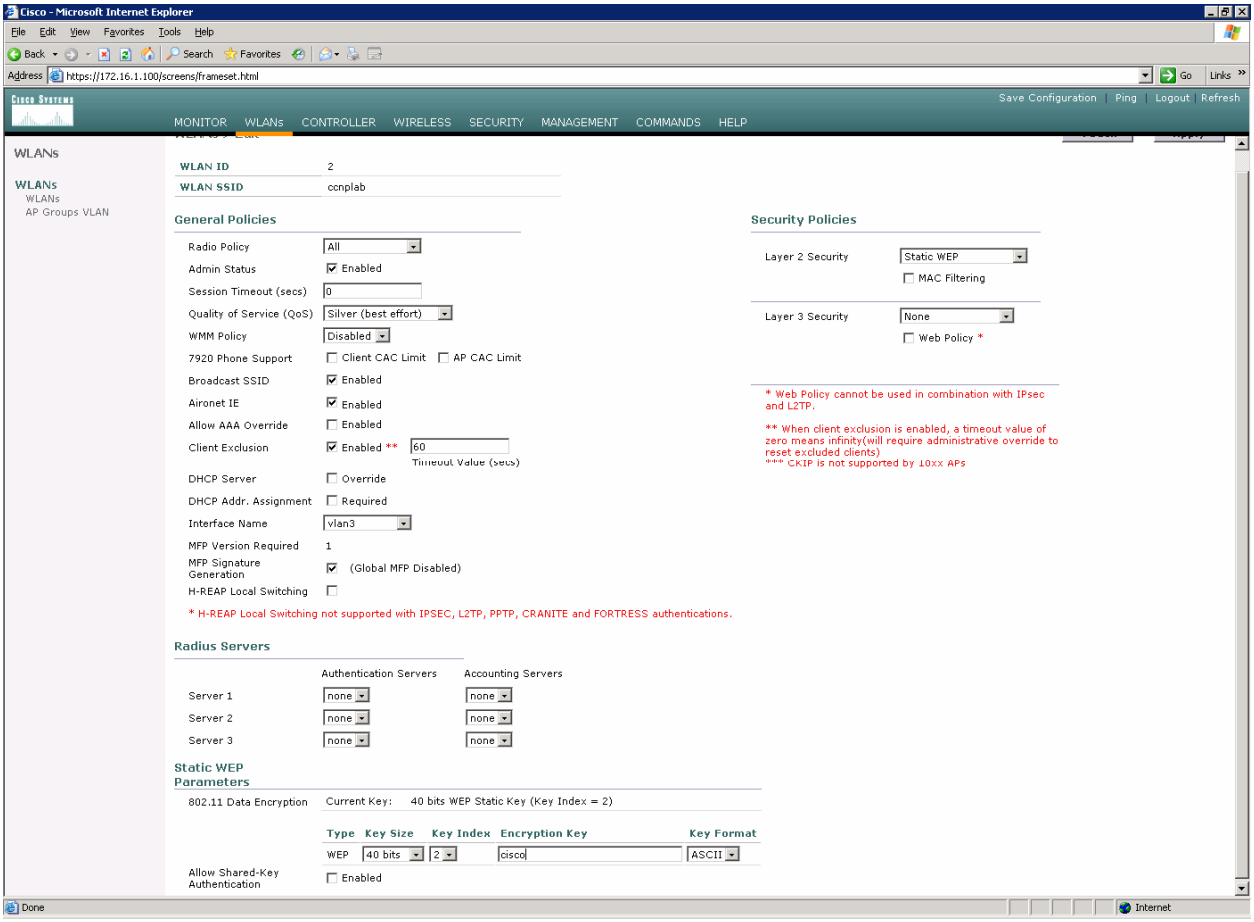


Figure 4-5: Configuring VLAN Association and Authentication for VLAN 3

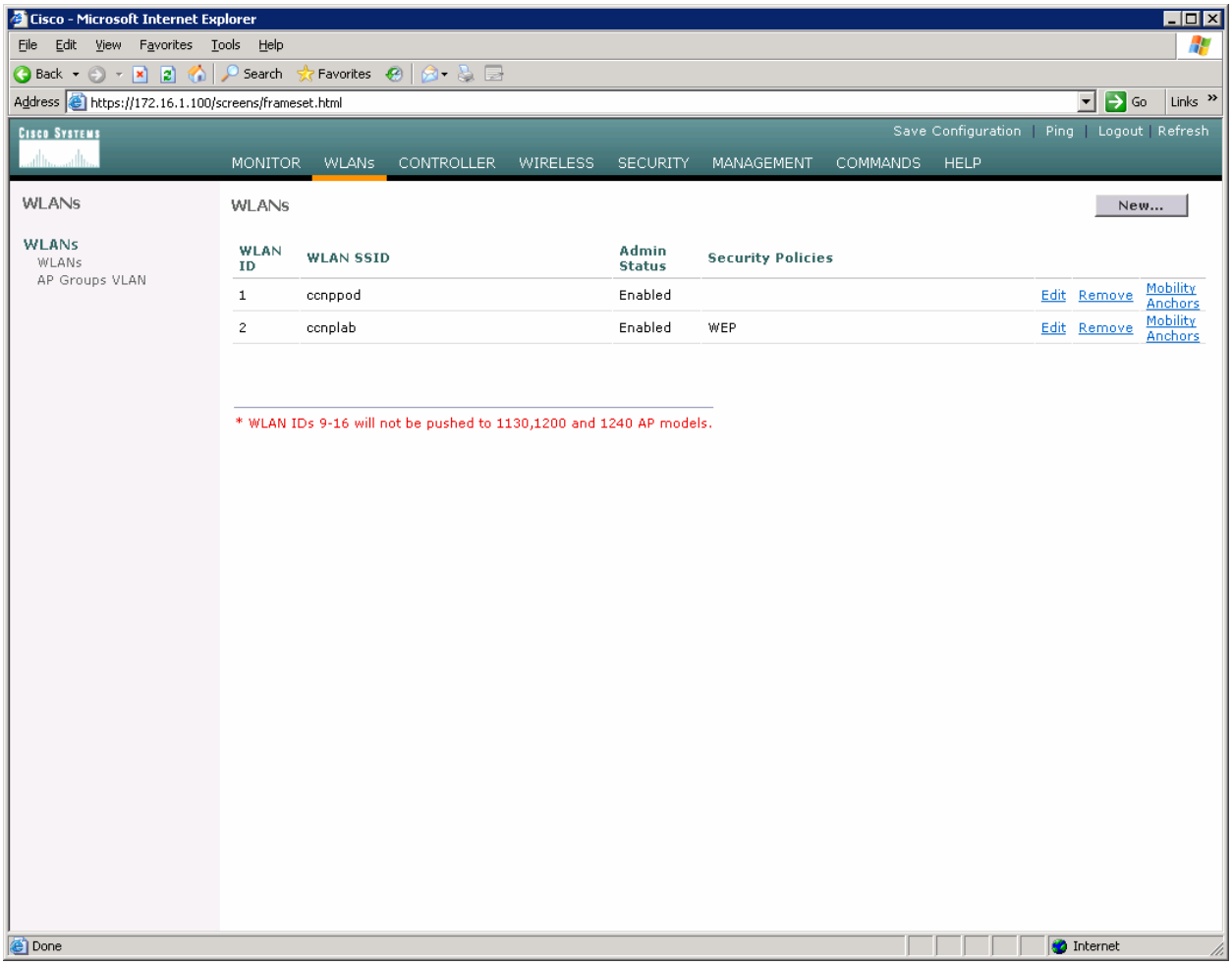
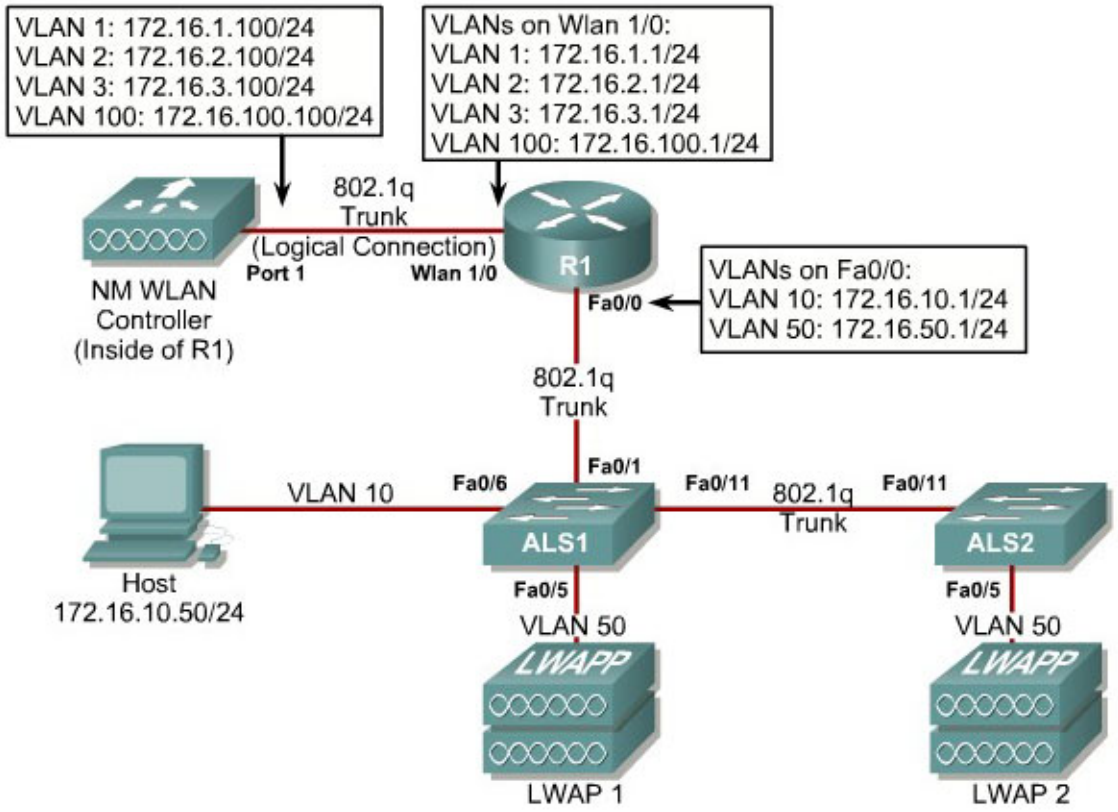


Figure 4-6: Verifying Final WLAN Configuration

At this point, if you have a computer with a wireless card installed you should be able to see both SSIDs and connect to the WLANs/VLANs associated with them. Notice that each WLAN exists in a separate subnet, because each WLAN is in a separate VLAN.

Lab 6-2 Configuring a WLAN Controller via the Web Interface

Topology Diagram



Scenario

Continuing from the previous lab, you will now set up the WLAN controller through its web interface. Previously you configured it through the CLI.

Step 1

Set up all the switches as they were in the previous lab. Make sure that the WLAN controller and host also have the same configuration as before.

Step 2

On the host, open up Internet Explorer and go to the URL “https://172.16.1.100”. This is the secure method of connecting to the management interface of the WLAN controller. You can also use

"http://172.16.1.100" since we previously enabled regular insecure HTTP access in the CLI for Lab 6.1. If you connect to the secure address, you may be prompted with a security warning. Click **Yes** to accept it and you will be presented with the login screen for the WLAN controller. Click **Login** and an authentication dialog box will appear.

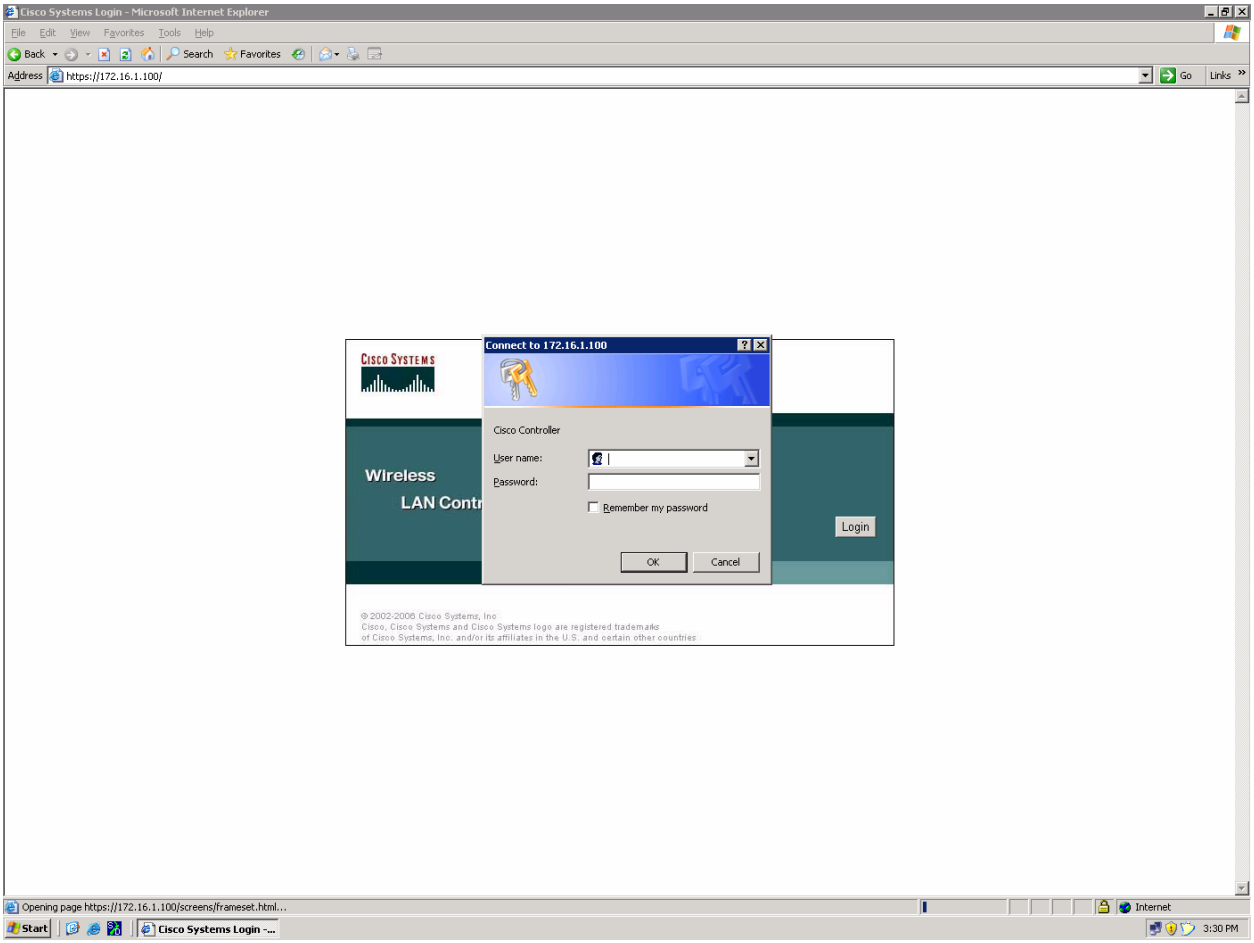


Figure 2-1: Authentication Dialog Box for WLAN Controller Web Access

Use "cisco" as both the username and password. You configured these in the previous lab. Click **OK** to get to the main page of the graphical user interface (GUI). You are then presented with the monitor page for the WLAN controller.

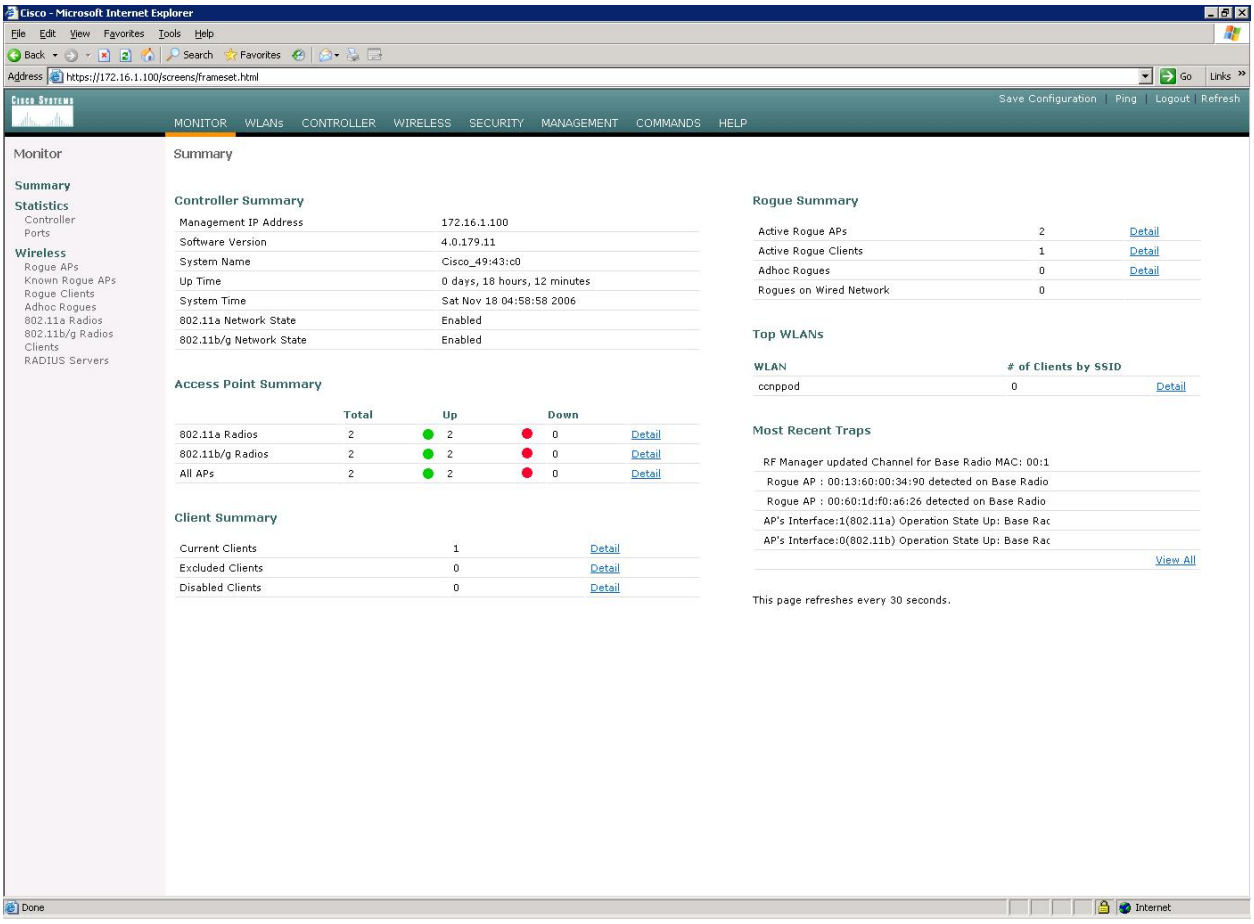


Figure 2-2: WLAN Controller Monitor Page

Make sure you see 2 access points under the “Access Point Summary” part of the page. You may also see it detecting rogue access points if your lab has other wireless networks around it; this behavior is normal. You can also see various port controller and port statistics by clicking their respective links on the left-hand menu on the screen.

Step 3

The next task in configuring WLANs is to add in the logical interfaces on the WLAN controller corresponding to VLANs 2 and 3. To do this, click the **Controller** link on the top of the web interface. Then, click **Interfaces** link on the left side bar.

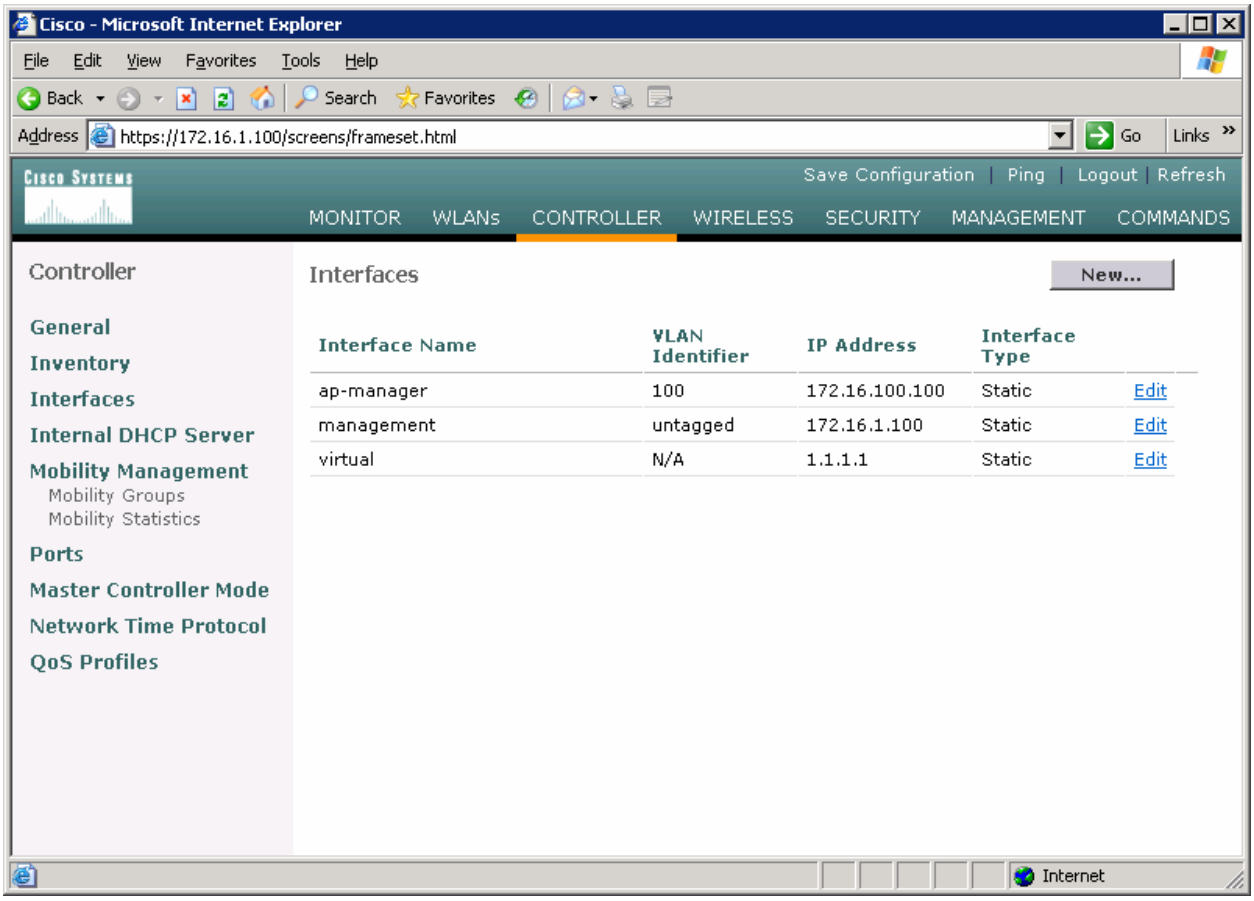


Figure 3-1: Interface Configuration Page

Click the **New...** link to create a new interface. Give the new interface a name of VLAN2 and VLAN number 2. Click **Apply** to submit the parameters.

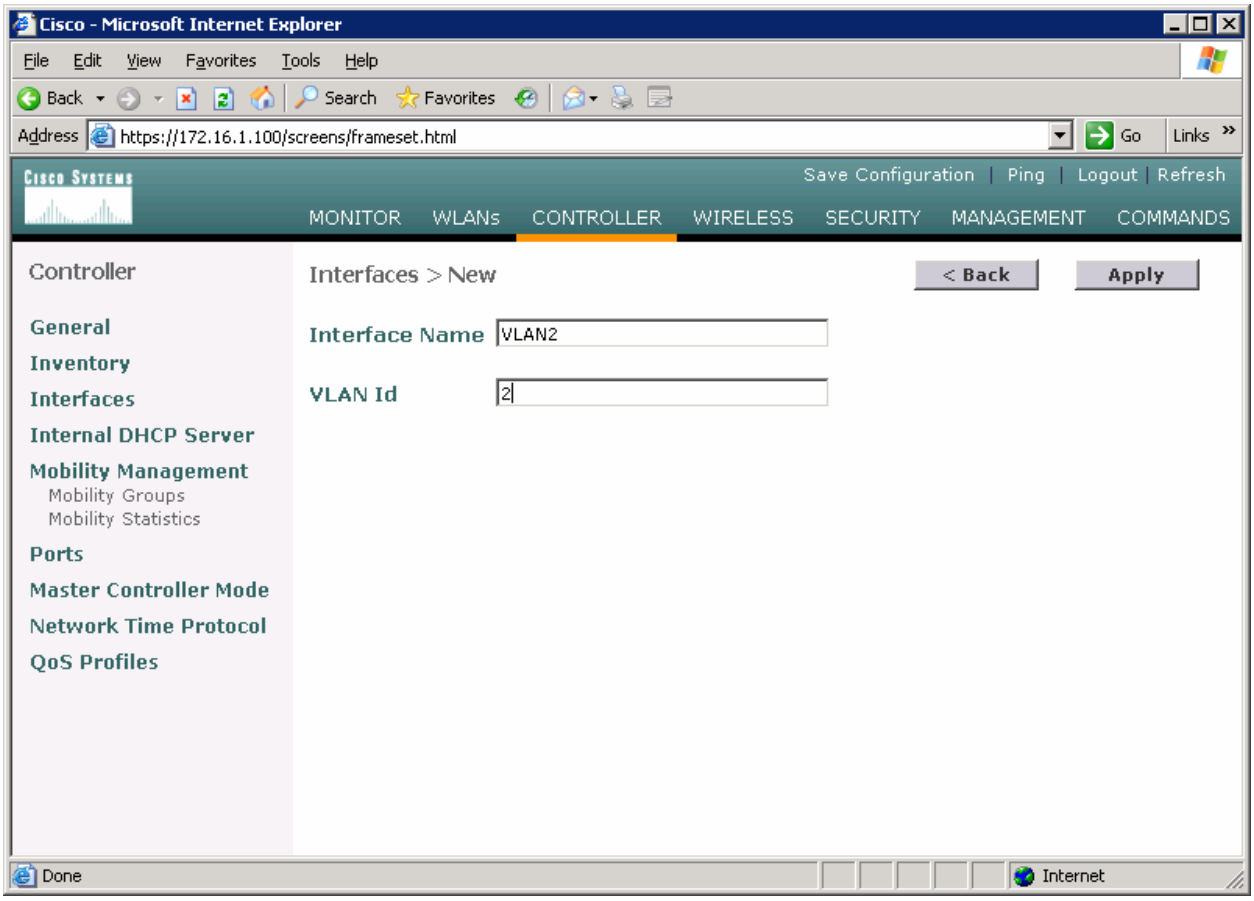


Figure 3-2: Creating a New VLAN Interface

On the next page, configure the IP address shown in the diagram. Also configure this on physical port 1, since that is the port trunked to the switch. After you have entered in all the changes, click **Apply**. Click **OK** to the warning box that comes up. This warning says that there may be a temporary connectivity loss on the APs while changes are applied.

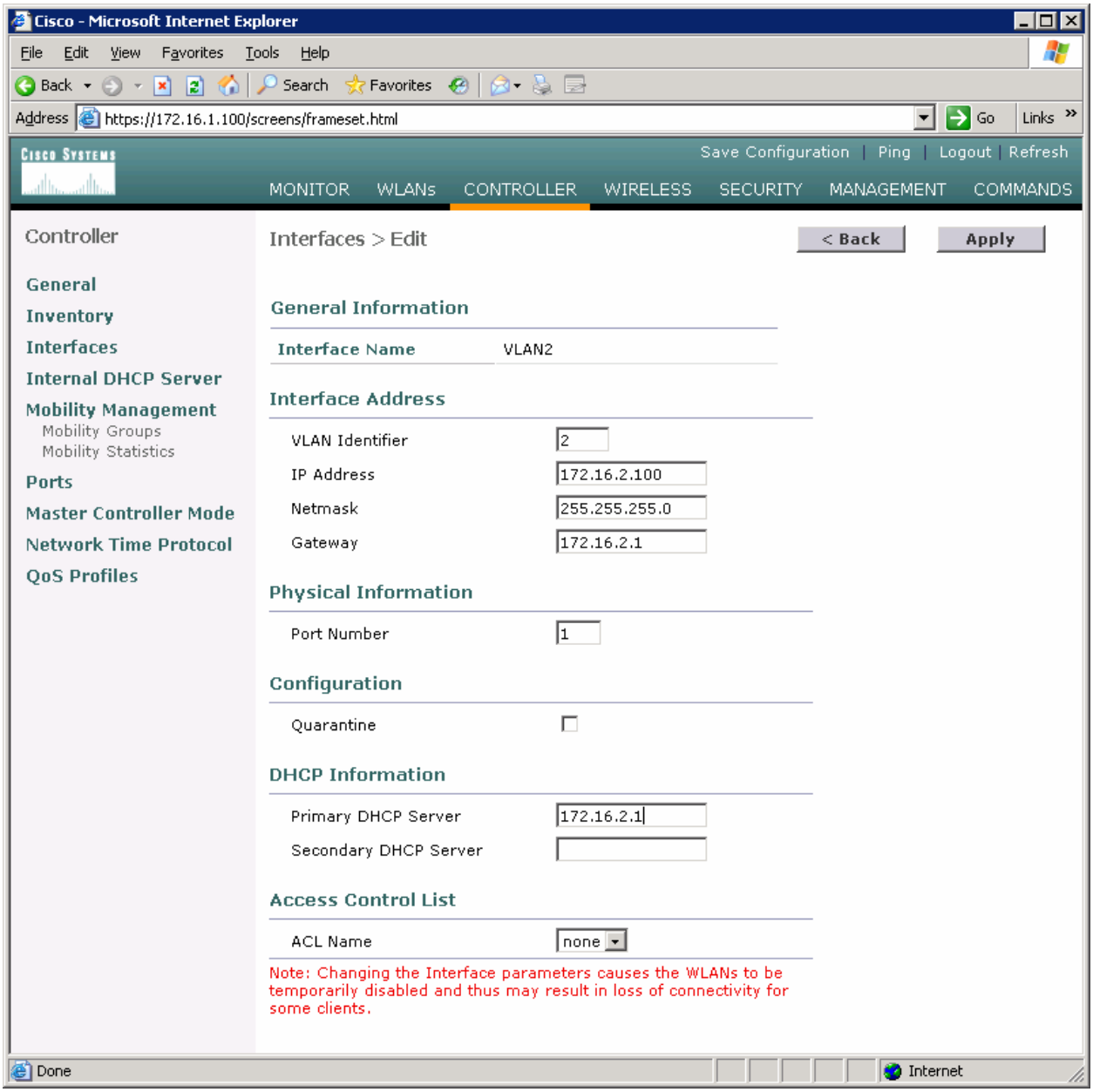


Figure 3-3: Configuring VLAN Interface Properties

The new interface should appear in the interfaces list. Do the same configuration steps for VLAN 3.

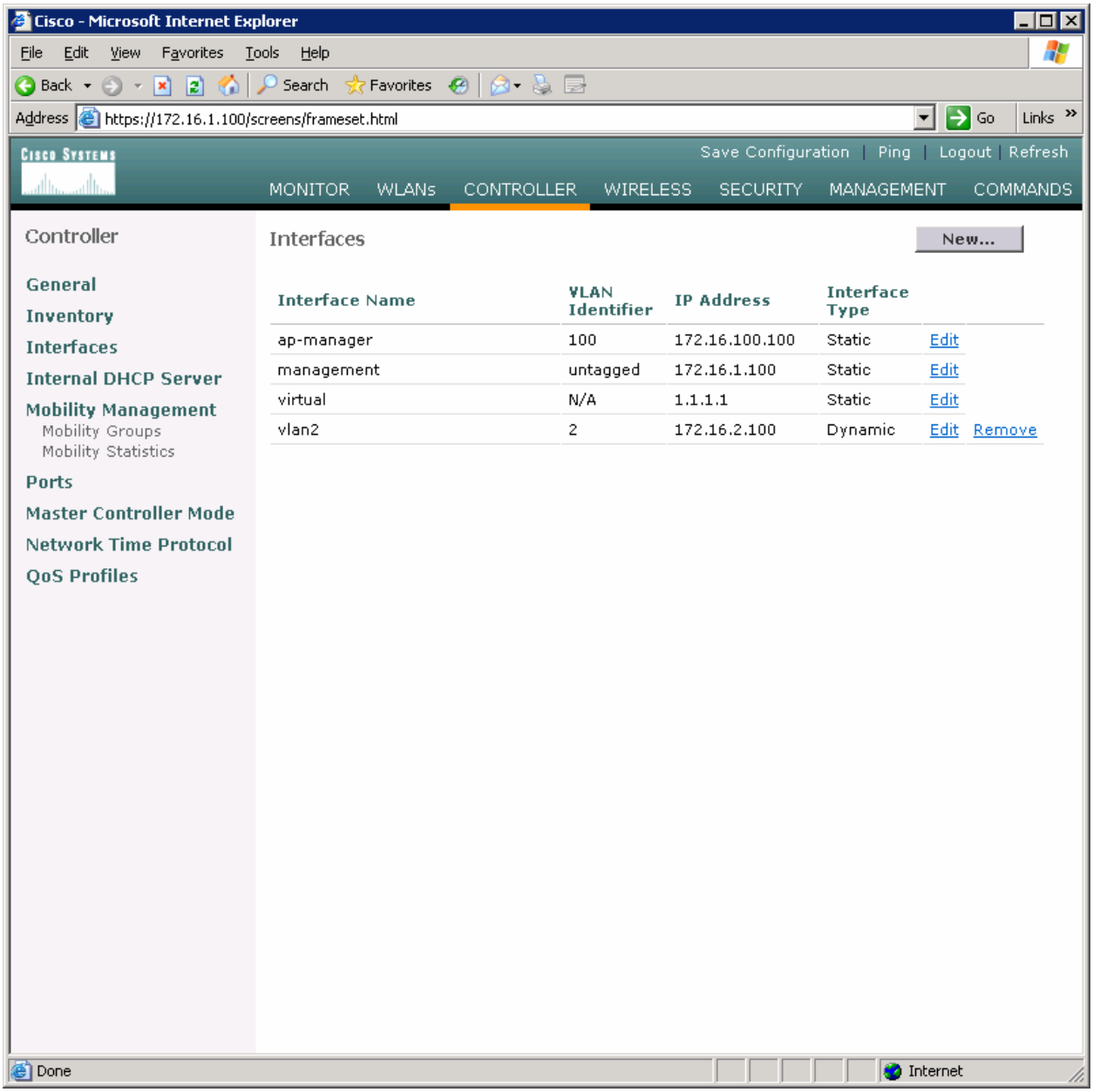


Figure 3-4: Verify Existing VLAN Interfaces

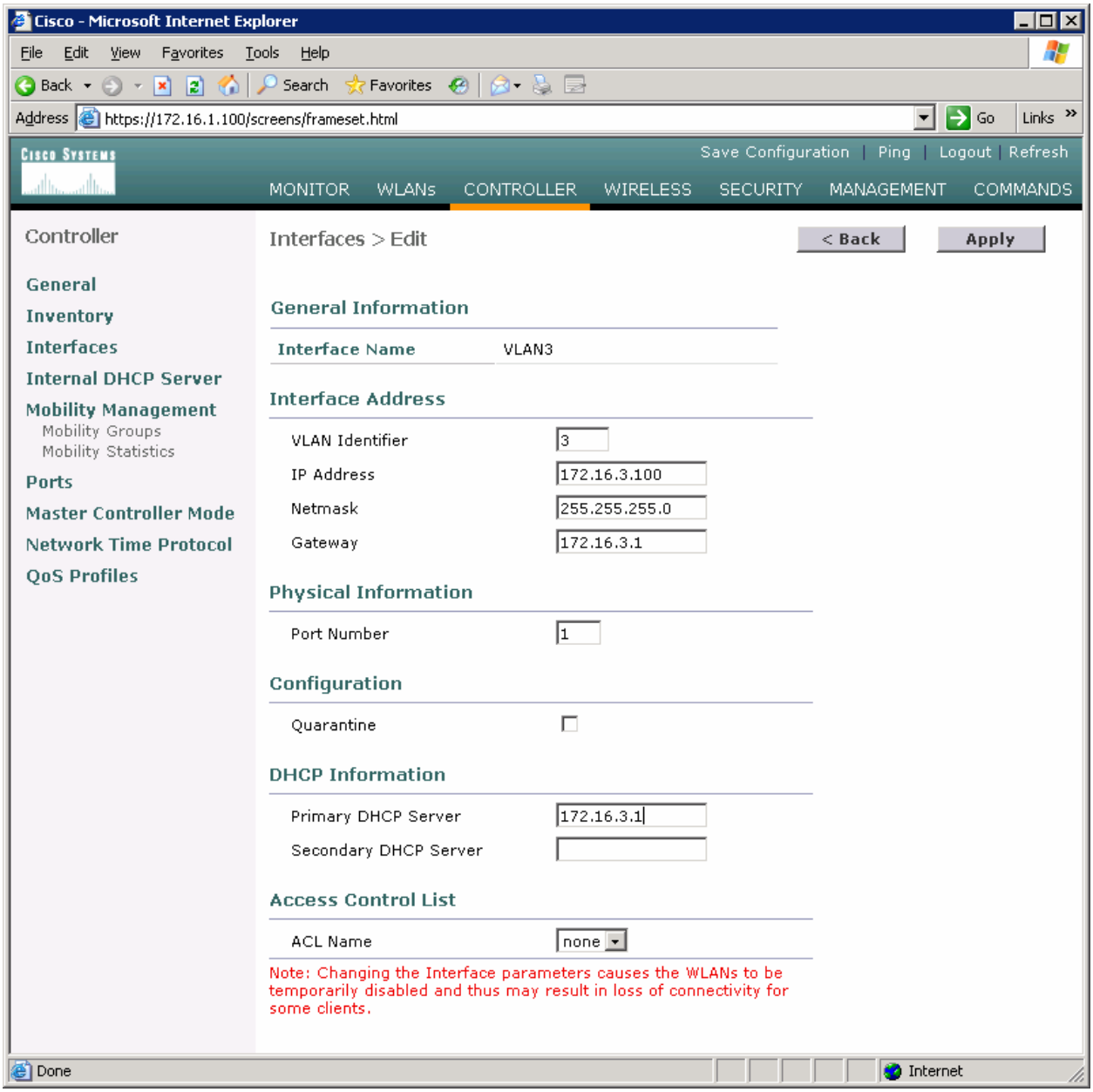


Figure 3-5: Configuring the VLAN 3 Interface

Make sure both interfaces appear in the interface table.

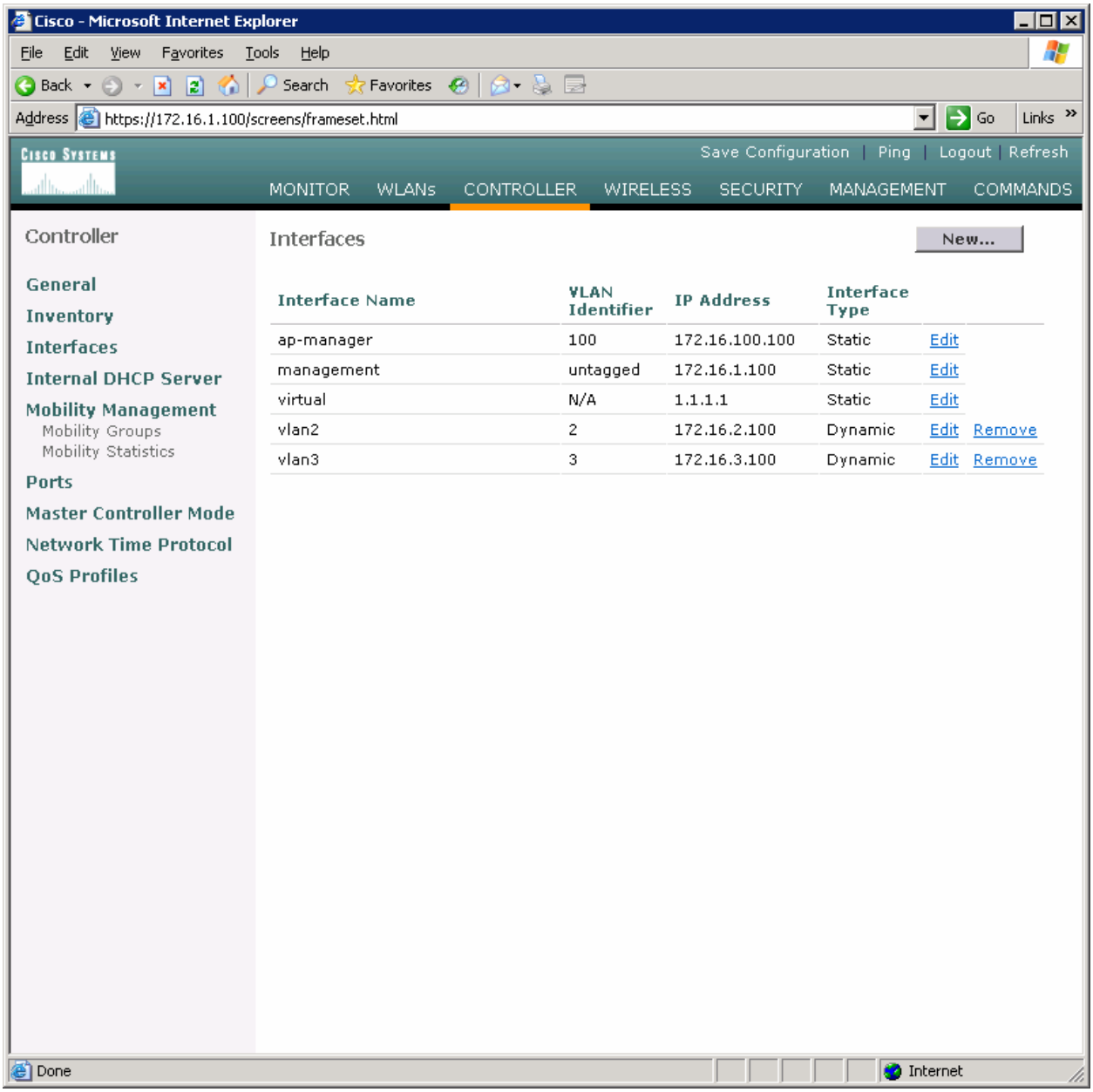


Figure 3-6: Verifying VLAN Interfaces on the WLAN Controller

Step 4

Now, you can configure the WLANs corresponding to these VLANs. To do this, first click the **WLANs** link at the top of the page. This will show you all configured WLANs.

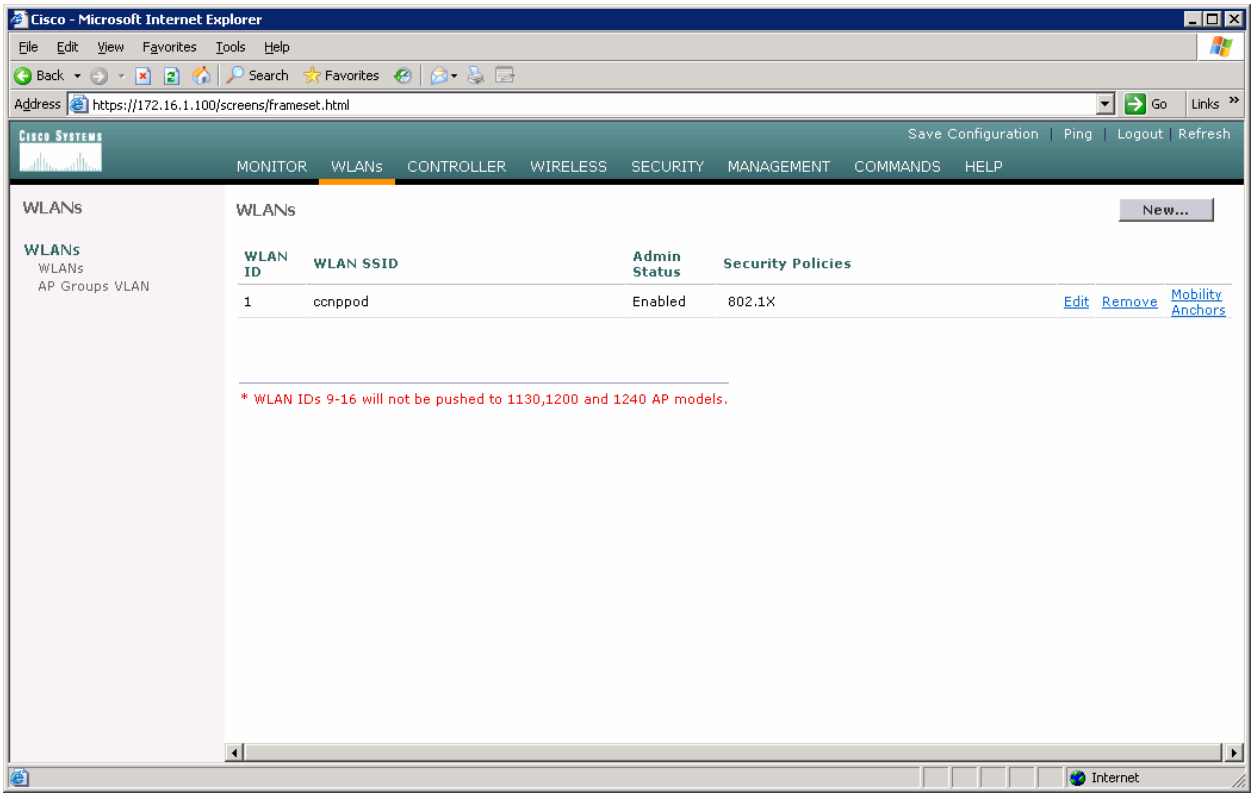


Figure 4-1: Viewing Existing WLANs

On the existing one, click **Edit** on the right of it. Remove the layer 2 security and change the interface to VLAN2. This will associate this WLAN with the correct VLAN.

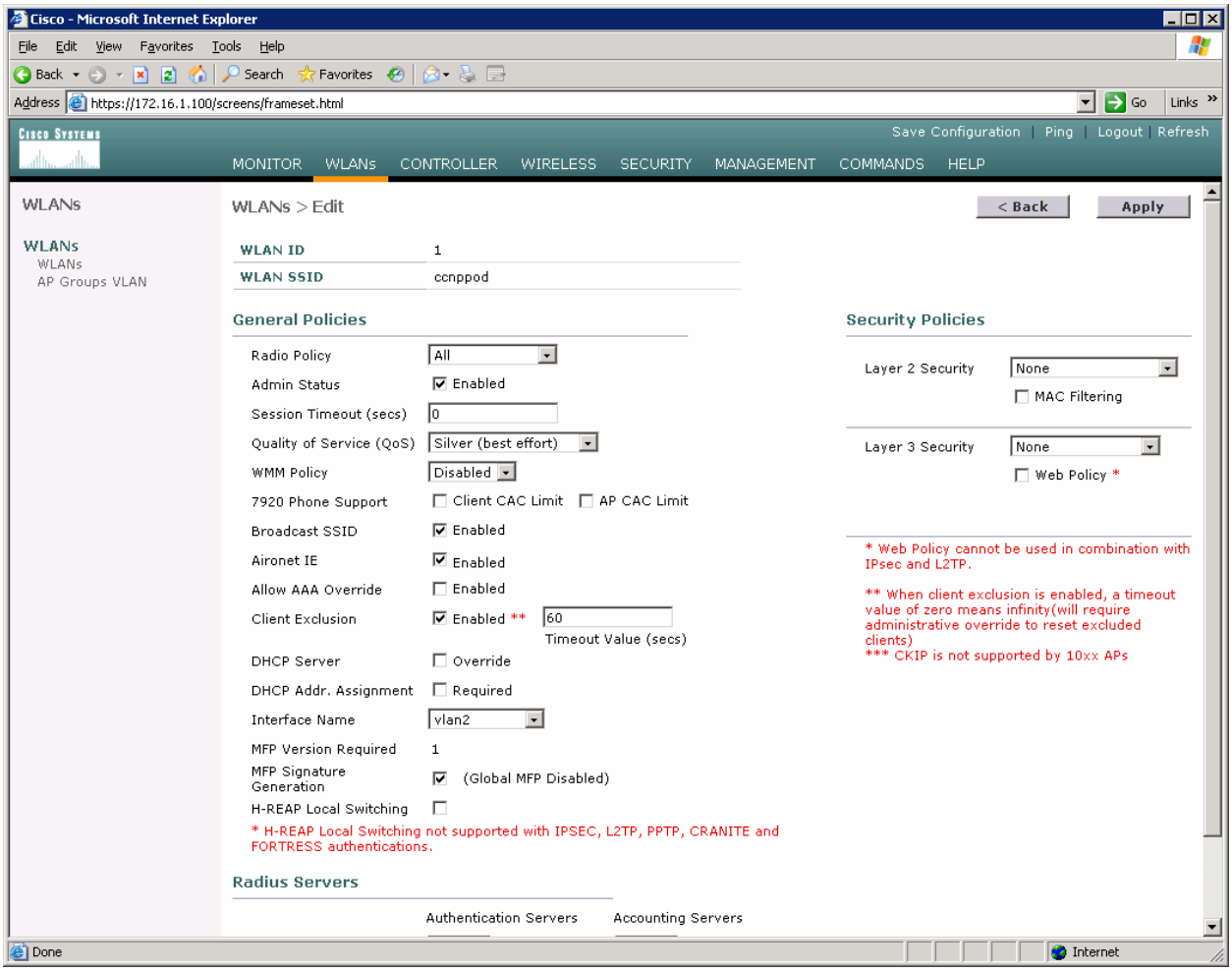


Figure 4-2: Edit the Configuration for WLAN 1

Click **Apply** and click **OK** to the warning box that comes up.

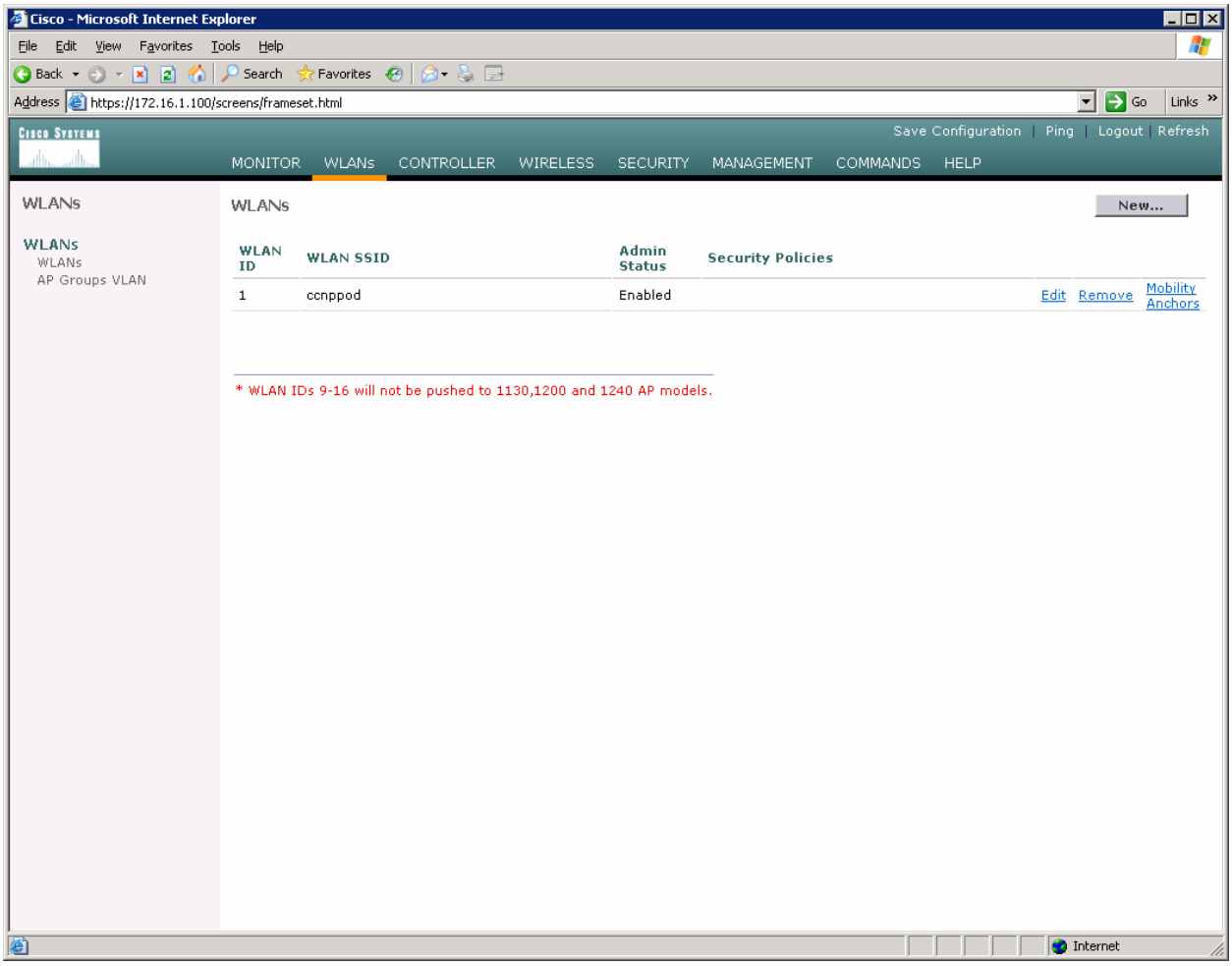


Figure 4-3: WLAN 1 without a Security Policy

Click **New...** and configure a WLAN for VLAN 3. Use the SSID “ccnplab”.

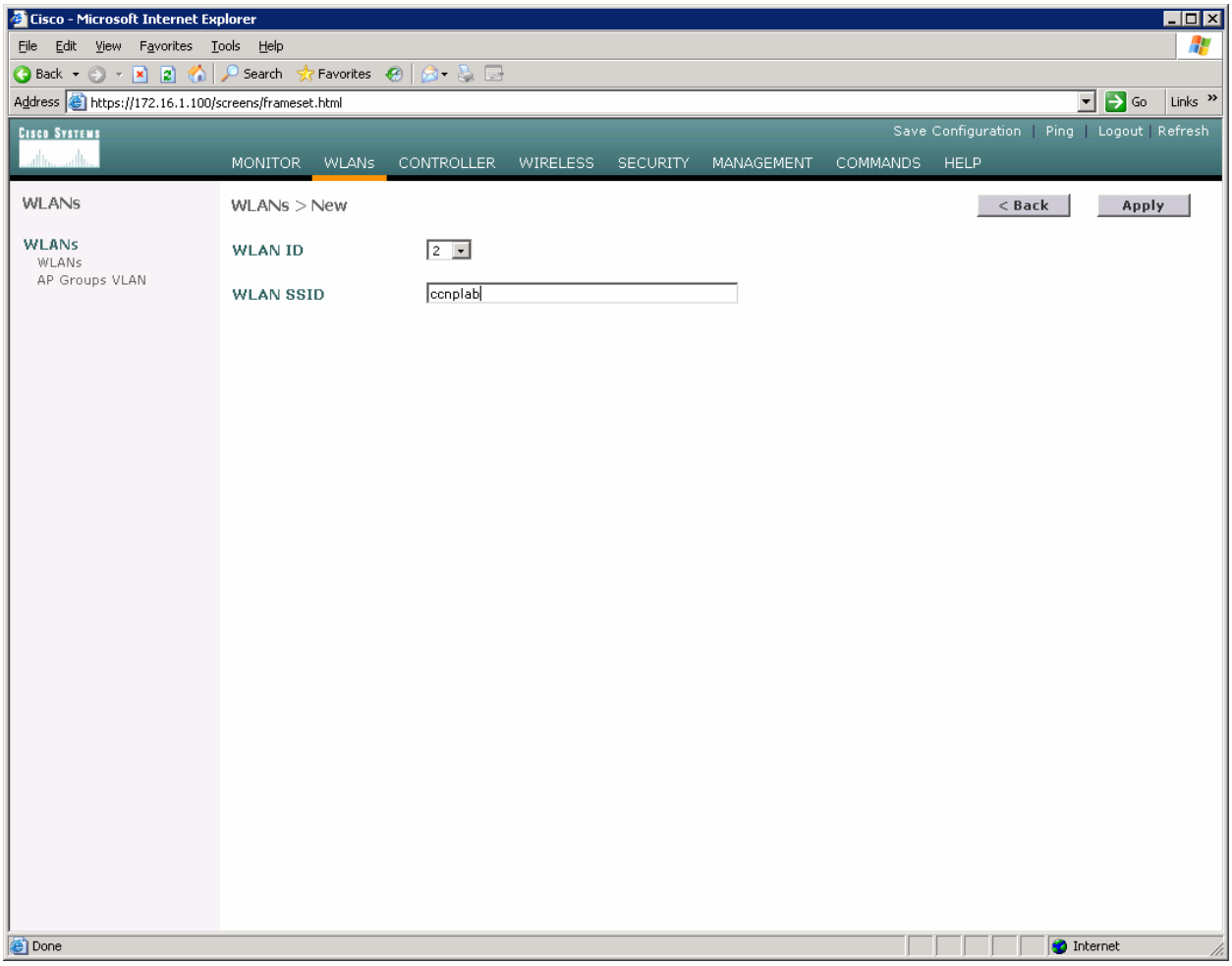


Figure 4-4: Adding a New SSID for WLAN 2

On this WLAN, configure the layer 2 security as Static WEP and use a 40 bit WEP key. Make the key index 2 and use a key of “cisco”. Also, set the administrative status of the WLAN to enabled and change the interface name to VLAN3. When you are done, click **Apply** and you should see both WLANs in the WLAN list.

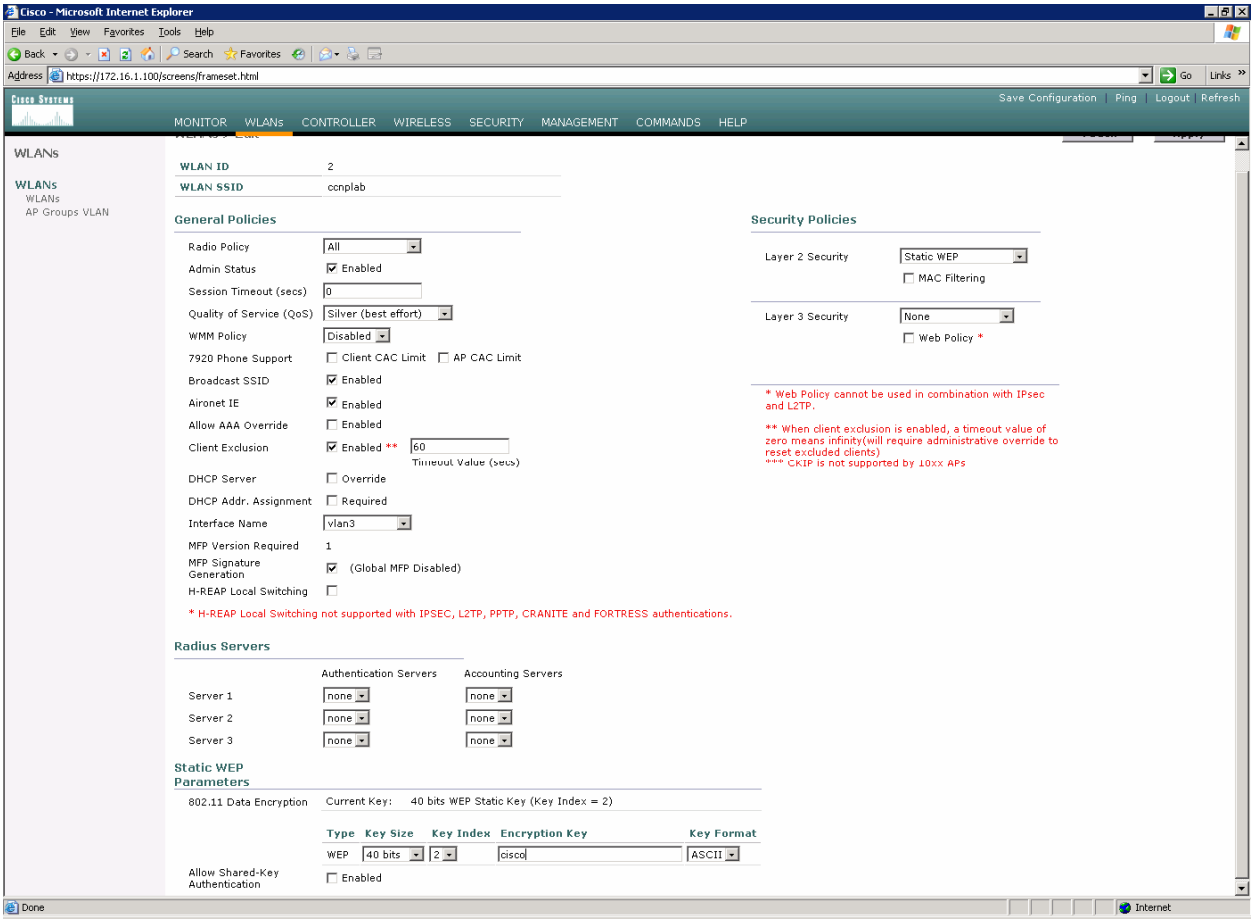


Figure 4-5: Configuring VLAN Association and Authentication for VLAN 3

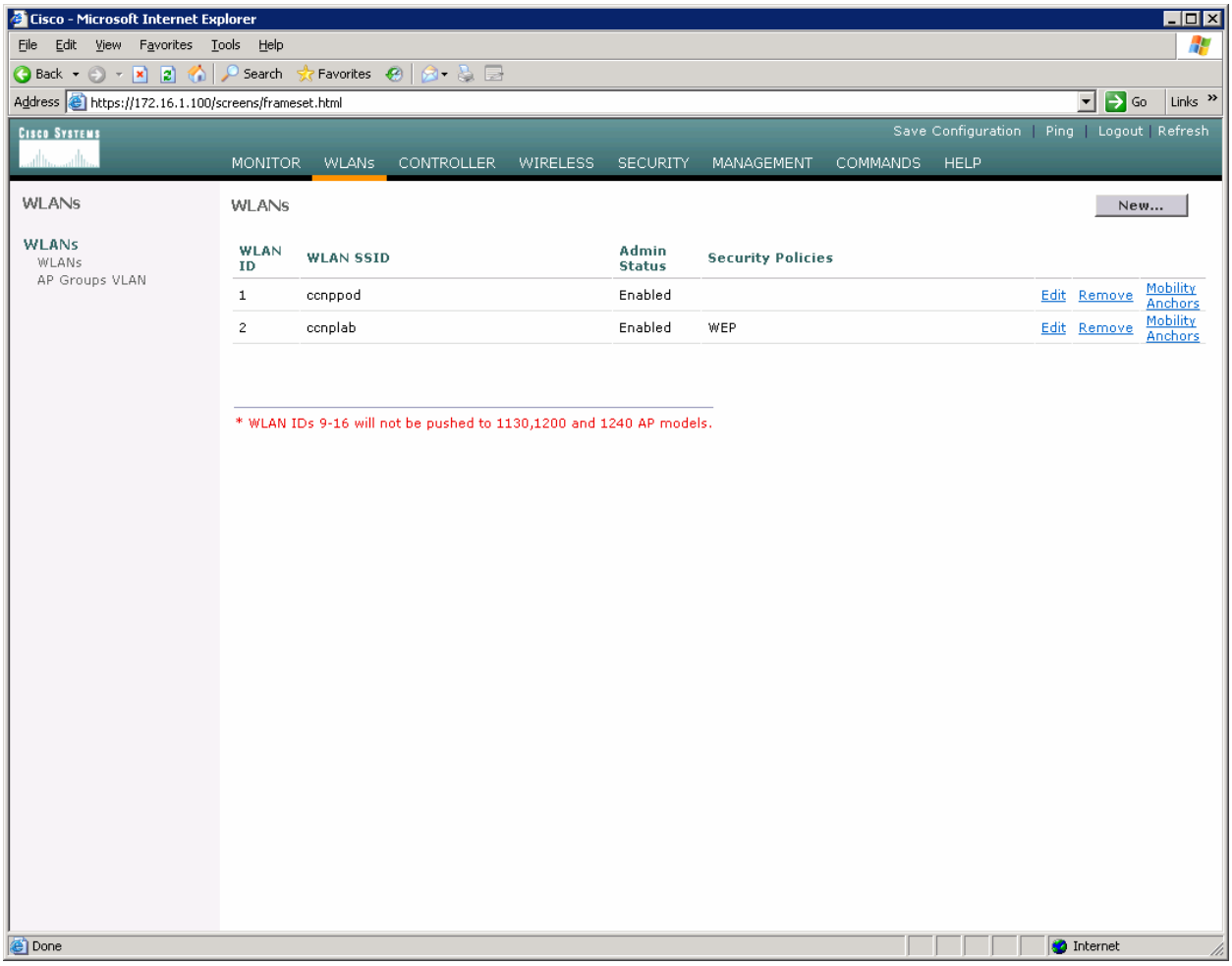
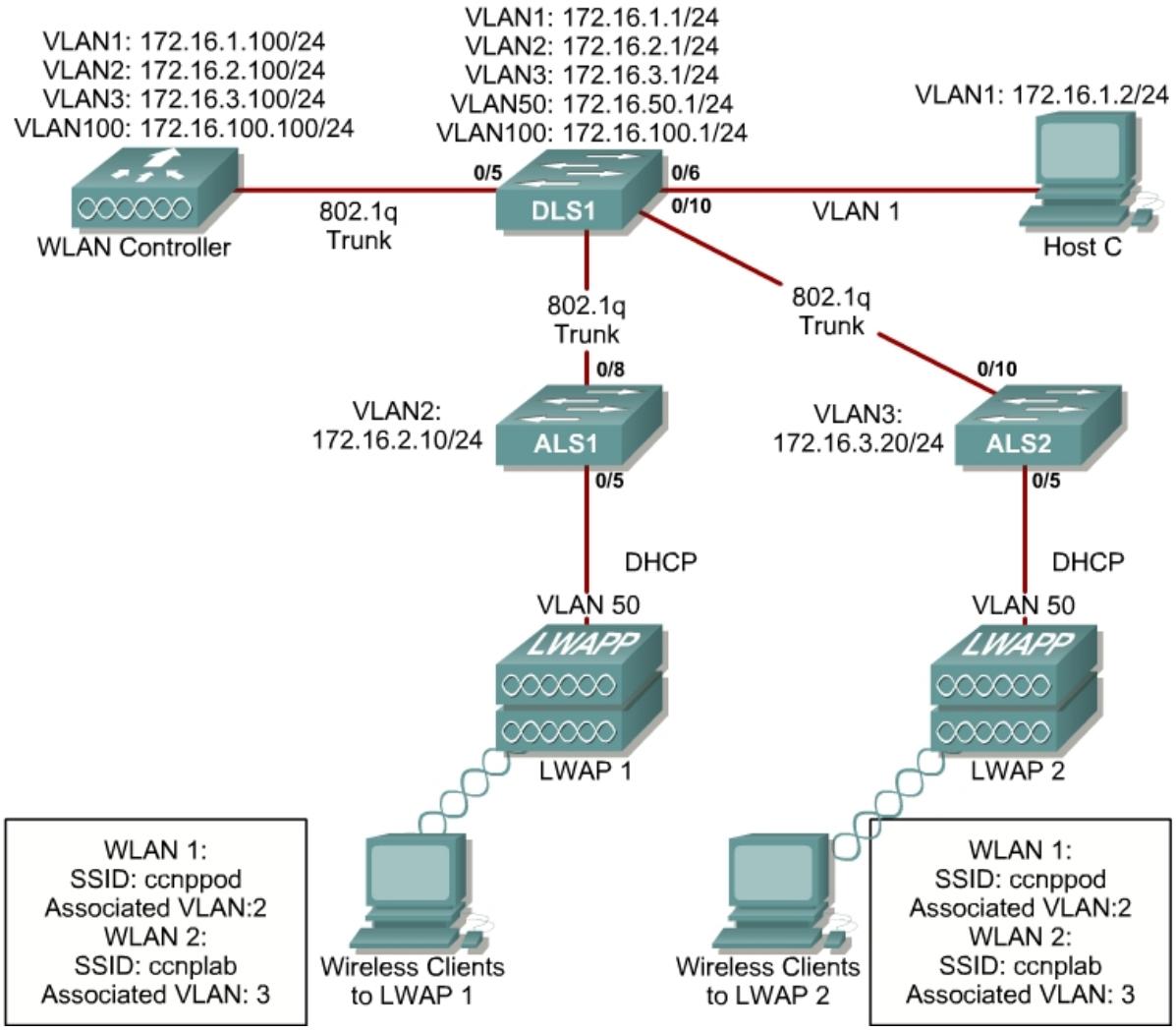


Figure 4-6: Verifying Final WLAN Configuration

At this point, if you have a computer with a wireless card installed you should be able to see both SSIDs and connect to the WLANs/VLANs associated with them. Notice that each WLAN exists in a separate subnet, because each WLAN is in a separate VLAN.

Lab 6-3 Configuring a Wireless Client

Topology Diagram



Scenario

In this lab, you will install a Cisco Aironet wireless PC card on a laptop. Then you will also configure the Cisco Aironet Desktop Utility (ADU) to connect to an access point.

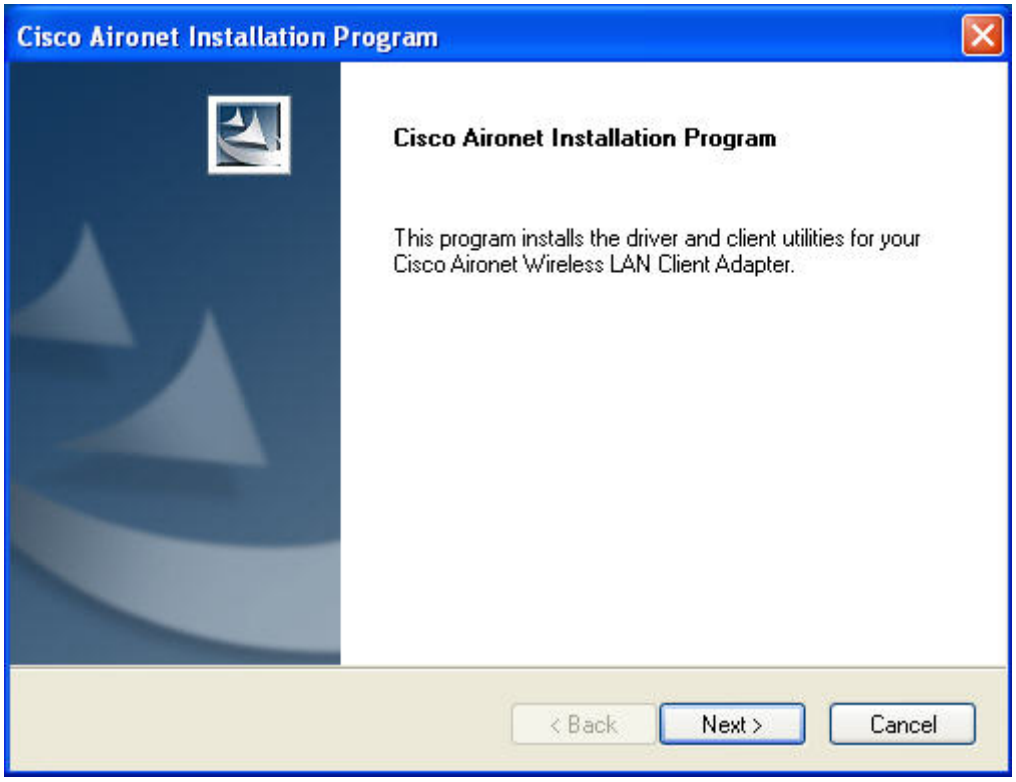
Step 1

Place the Cisco Aironet 802.11 a/b/g Wireless Adapter into an open NIC slot on your laptop.

Step 2

WinClient-802.11a-b-g-Ins-Wizard-v30

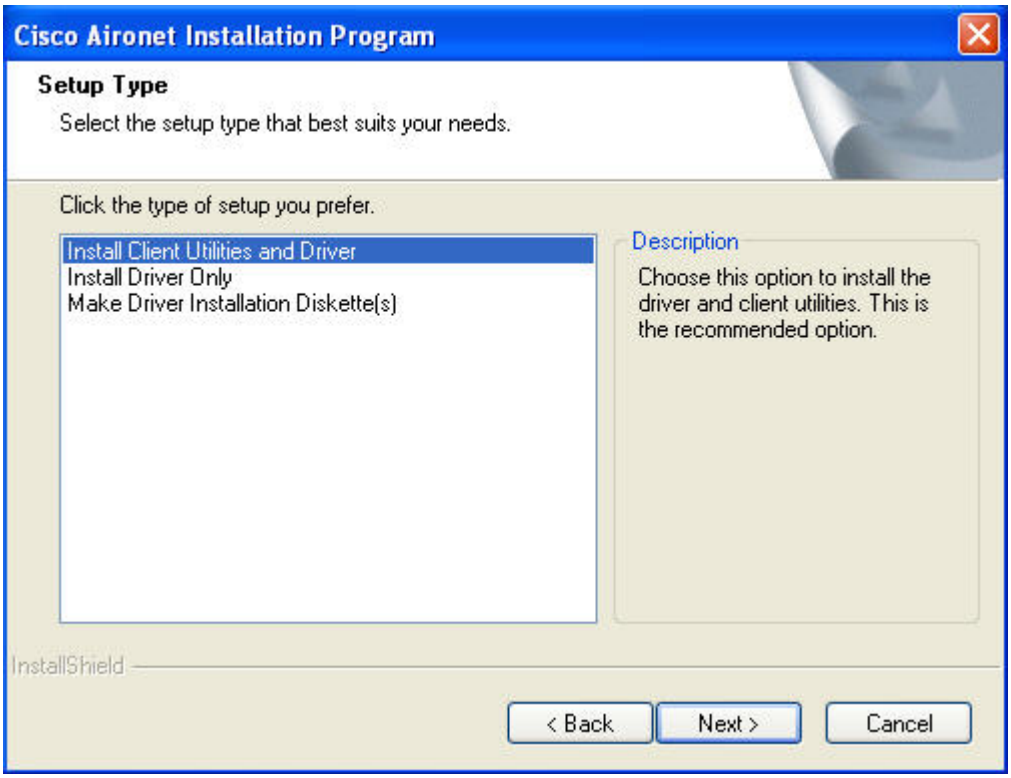
Once you have transferred the Installation Wizard software to your hard drive, double-click on it. The following is the first screen to appear.



First Page of the Cisco Aironet Installation Wizard

Step 3

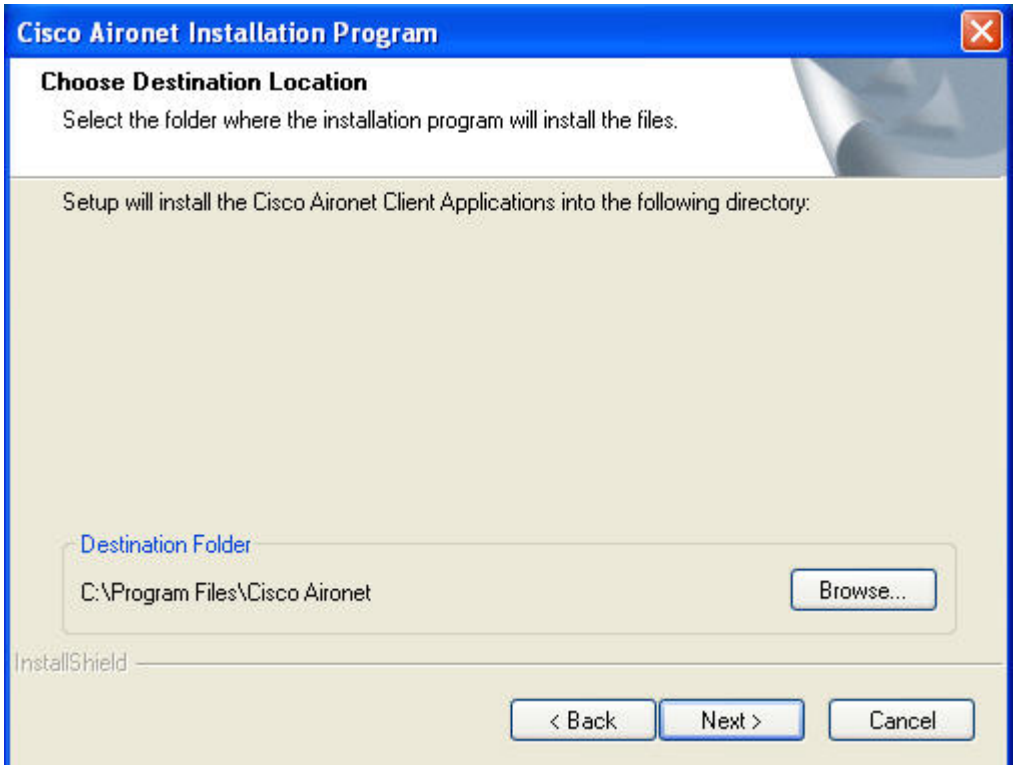
Click on Next. Then select **Install Client Utilities and Driver**. Click on **Next.**



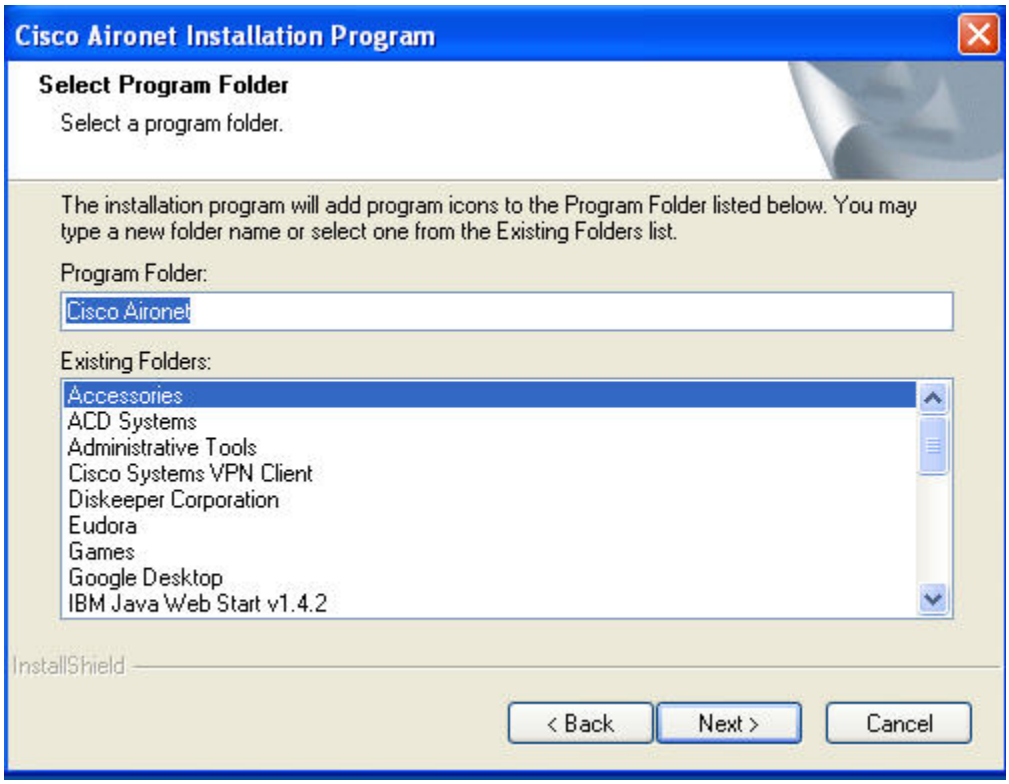
Choose Install Client Utilities and Driver

Step 4

On the next two screens, choose the default setting by clicking on **Next** unless instructed otherwise by your teacher.



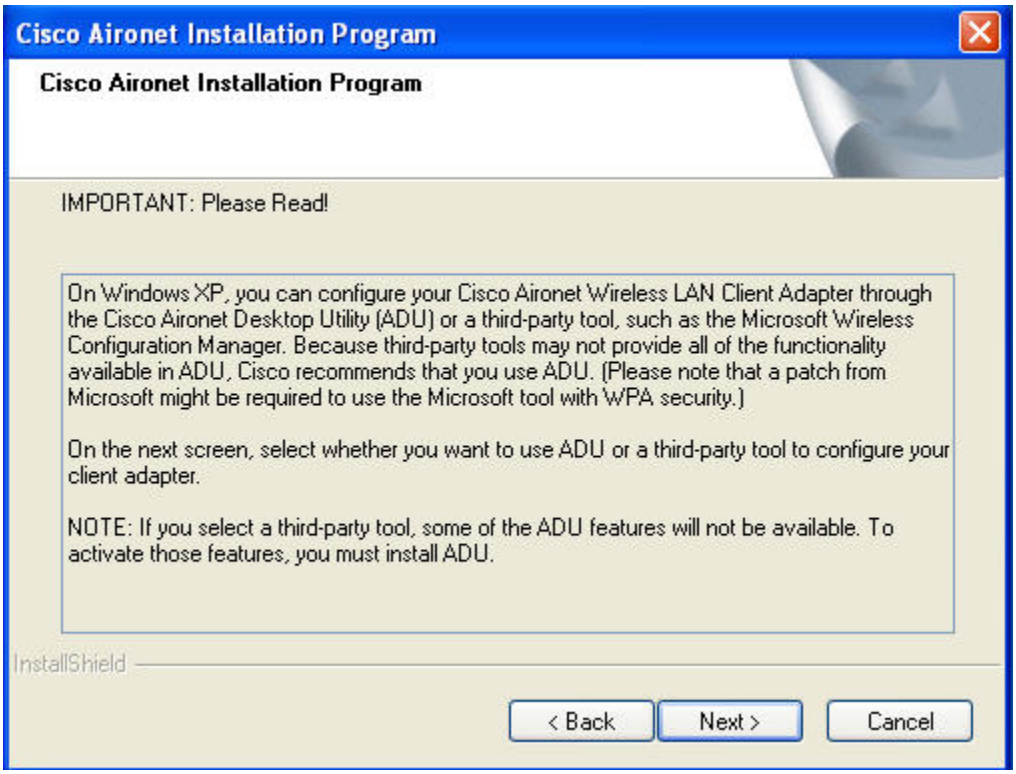
Choose Destination Location for Software Installation



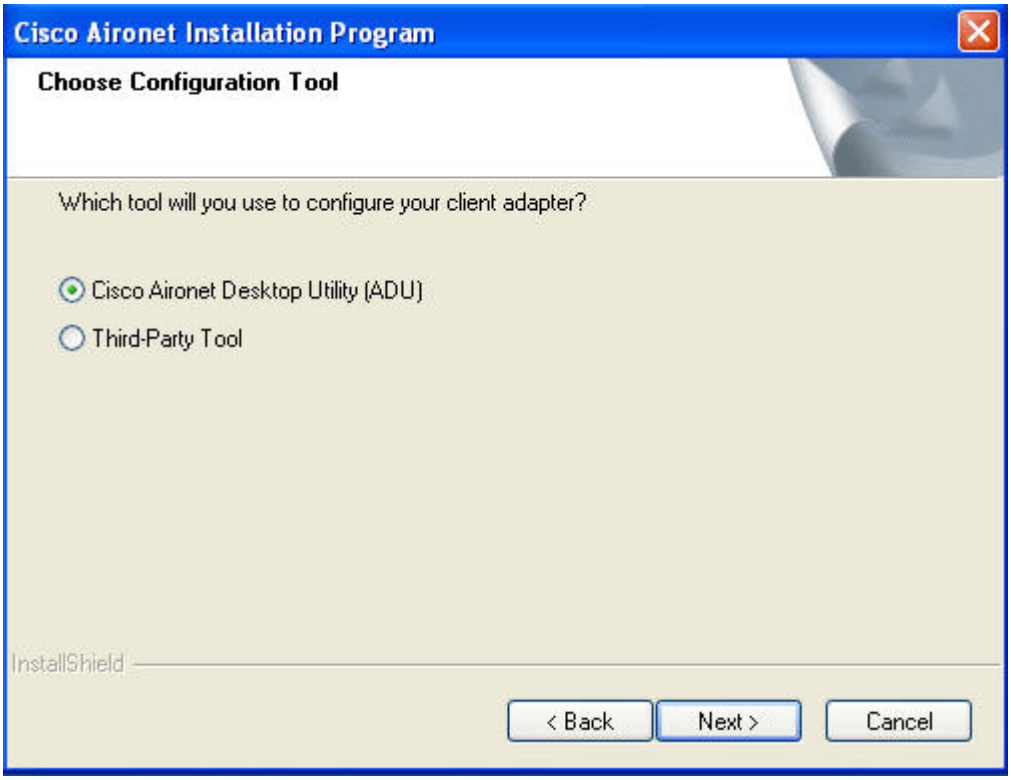
Select Program Folder for Software Installation

Step 5

If you are running Microsoft Windows XP, you get a warning about using the Cisco ADU rather than the default Microsoft Wireless Configuration Manager. After this screen, you have the option to choose between the two. Choose Cisco ADU, because it is more capable than the one from Microsoft.



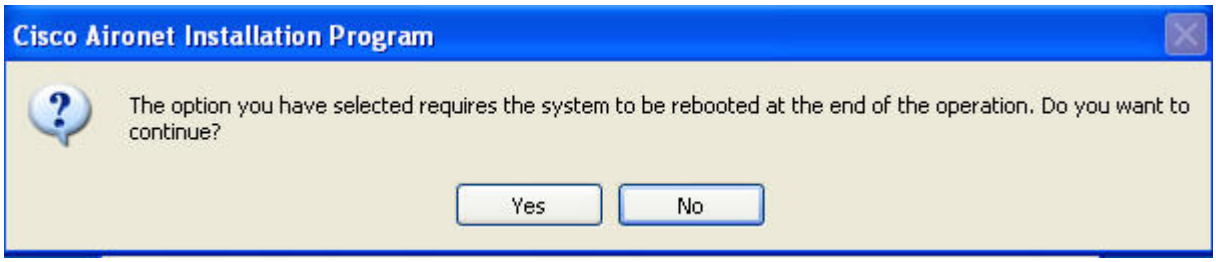
Windows XP Warning



Choose ADU as the Configuration Tool

Step 6

Click on **Yes** to reboot your system at the end of the operation. On the next screen click **OK**.

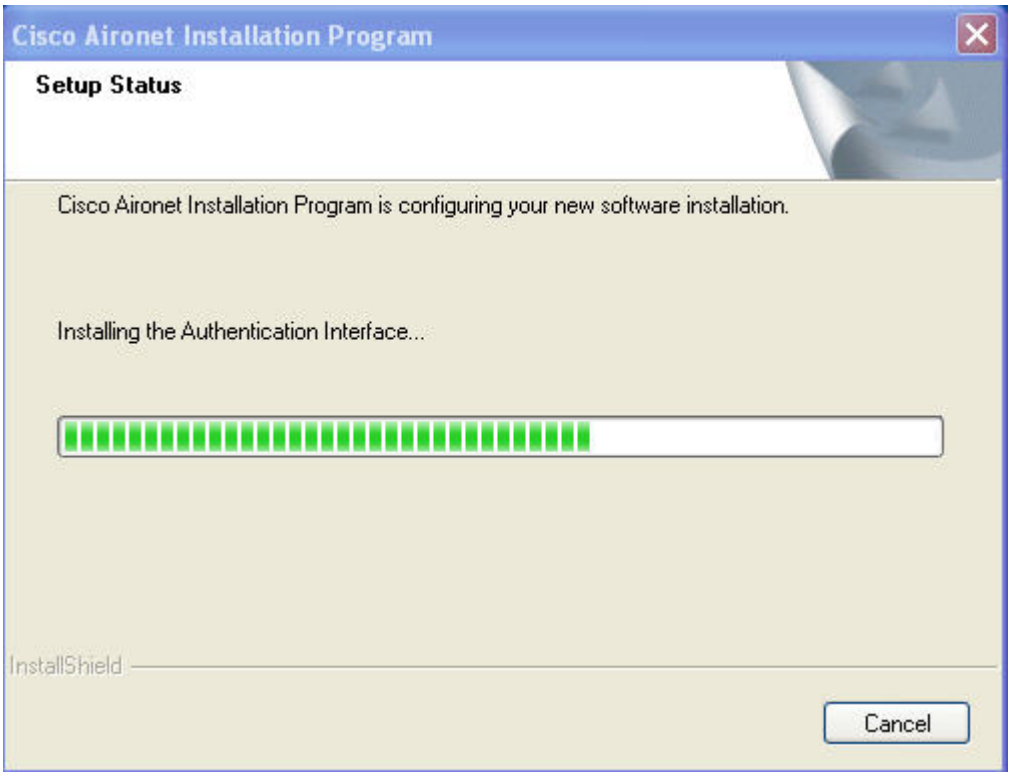


Reboot at the end of the operation

Click OK to Continue

Step 6

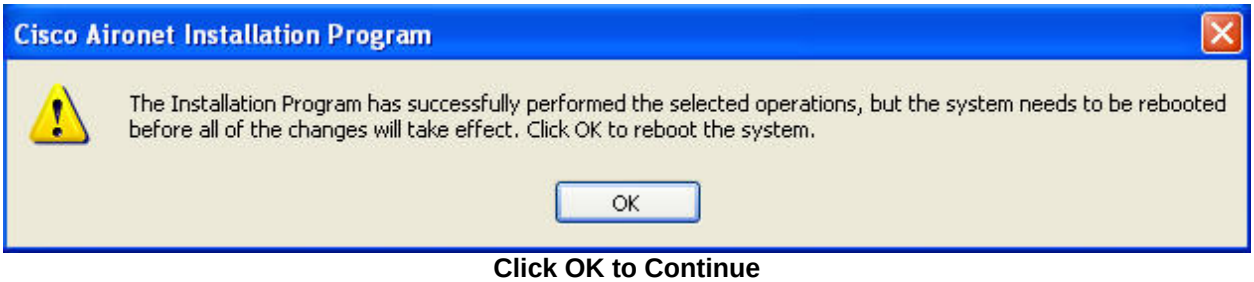
The **Setup Status** screen will show the status of the software installation.



Setup Status

Step 7

When Setup is complete, reboot the computer by clicking **OK**.



Click OK to Continue

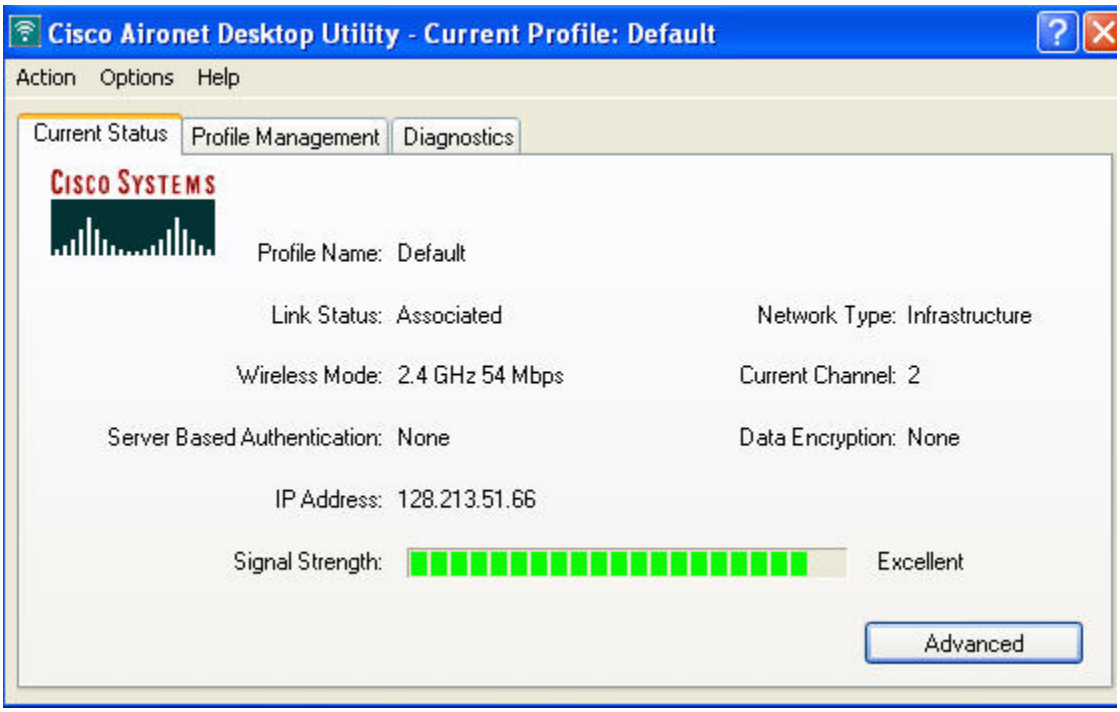
Step 8

After the computer has rebooted, click on the shortcut to the Aironet Desktop Utility (ADU).

Shortcut to Aironet Desktop Utility

Step 9

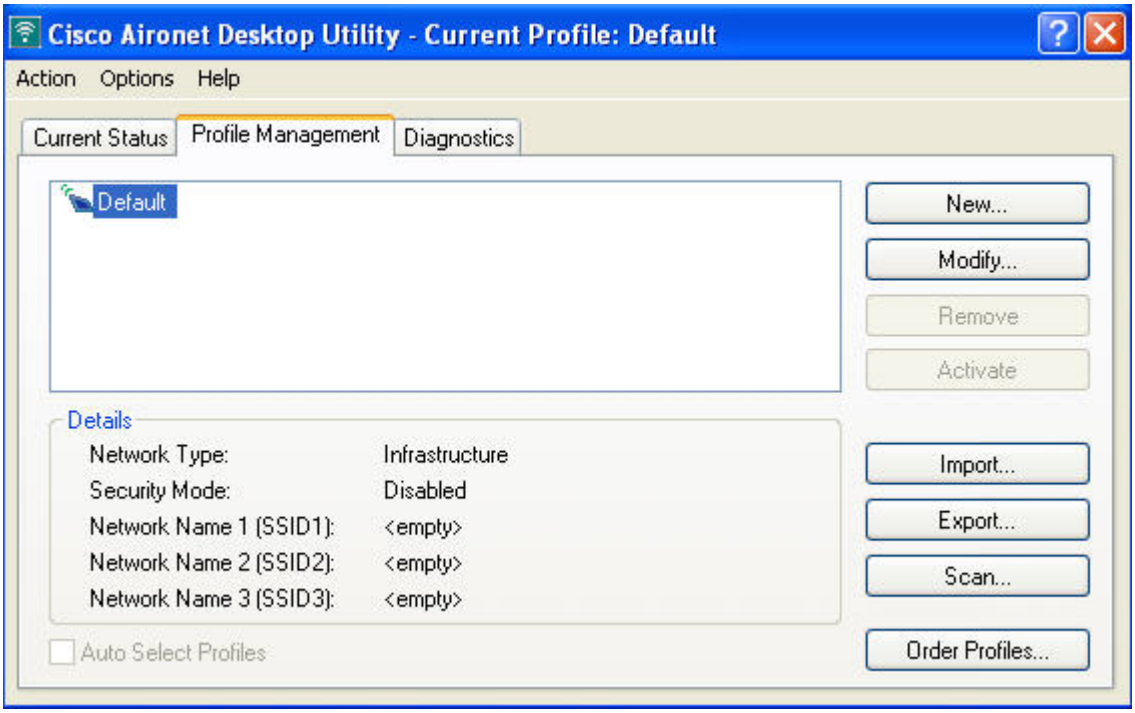
The **Current Status** screen appears by default. In the image below, the PC has found a production wireless network and associated with its access point. If your lab is close to a production wireless network, you may have a similar result. If your PC is not close to a production network, then your **Current Status** screen will look different.



Current Status Screen

Step 10

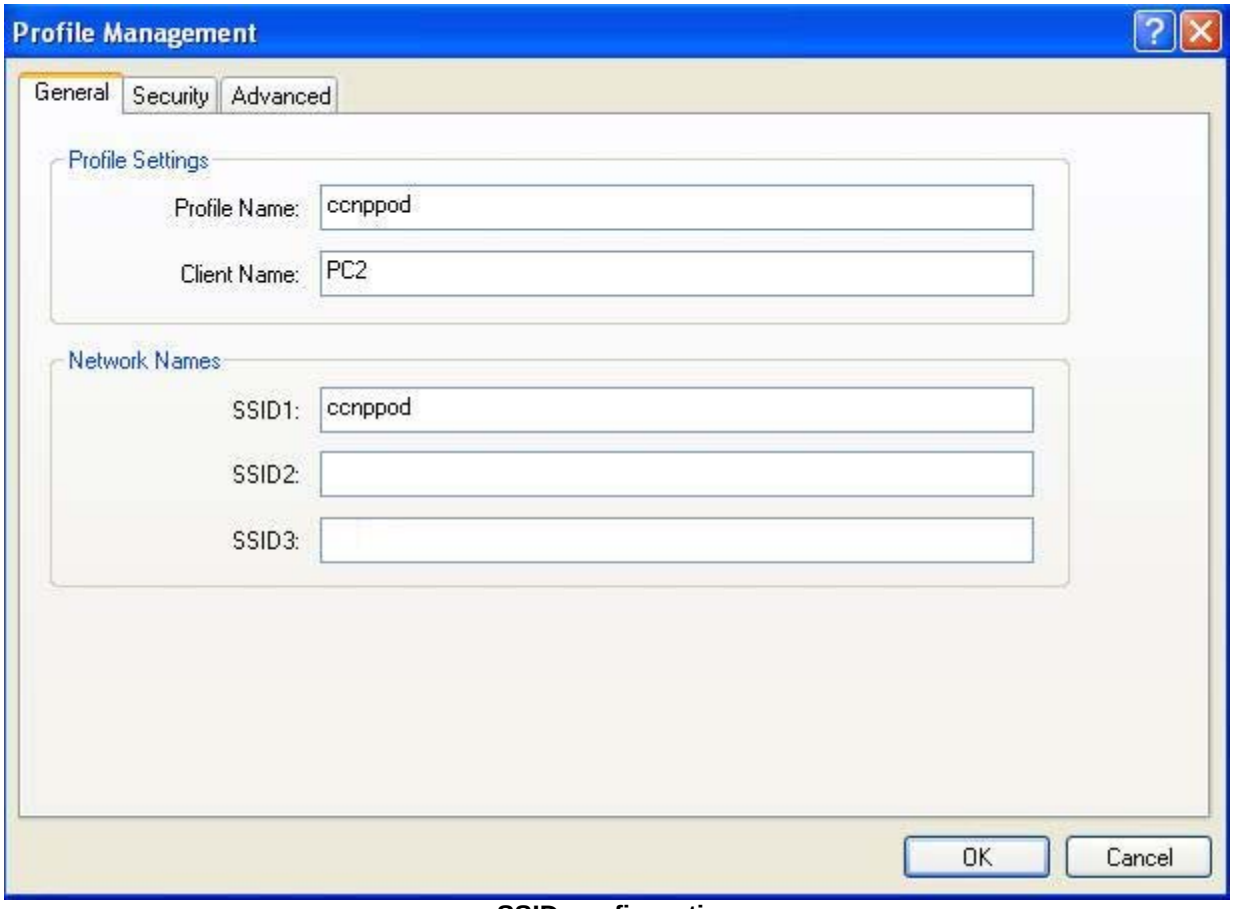
Whether or not you are connected to a production wireless network, you now want to connect to the lab network. Click on the **Profile Management** tab next to the **Current Status** tab. Then click on the **New** button in the upper right hand corner of the screen.



Profile Management Screen

Step 11

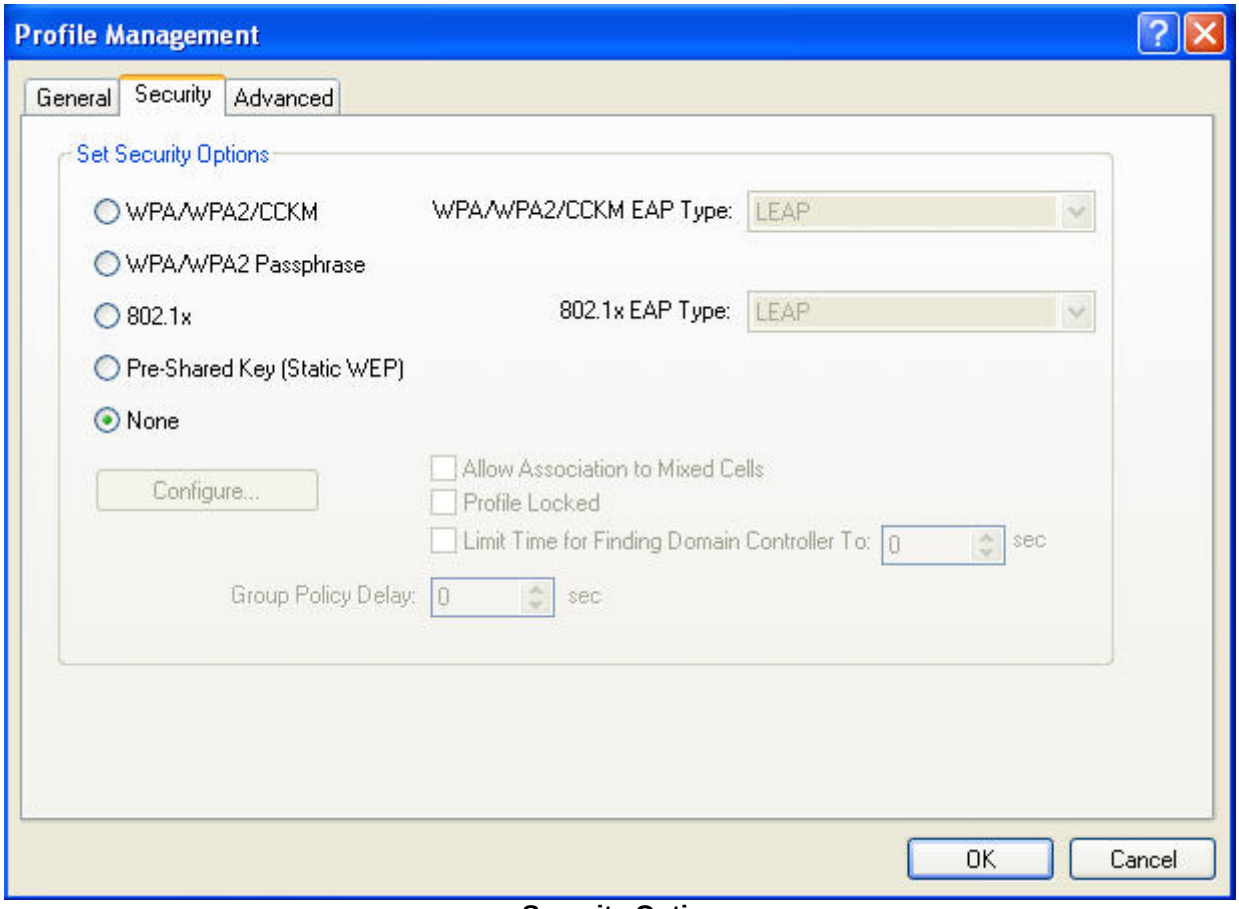
Enter the profile name “ccnppod.” Use the SSID of “ccnppod.”.



SSID configuration

Step 12

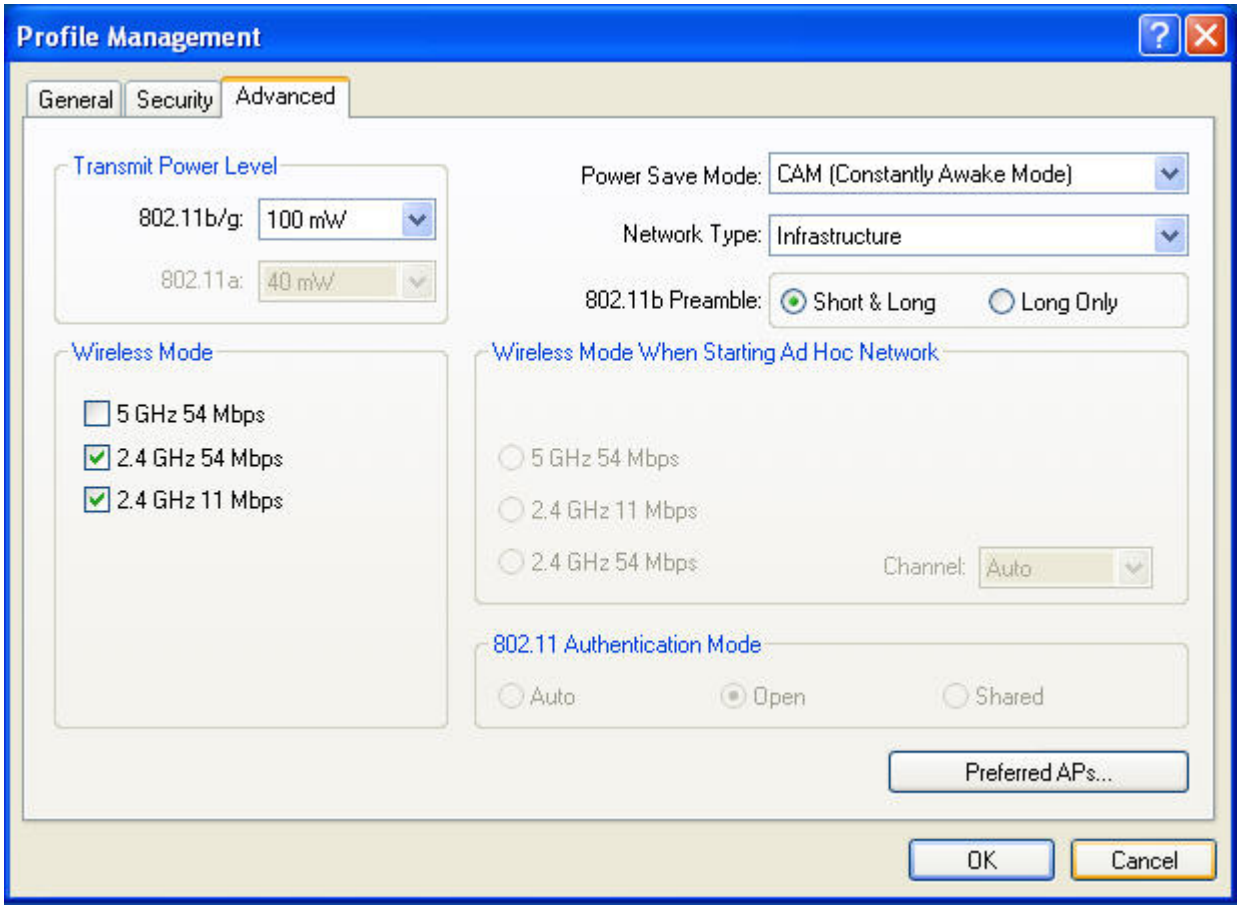
Select the **Security** tab. Select **None**.



Security Options

Step 13

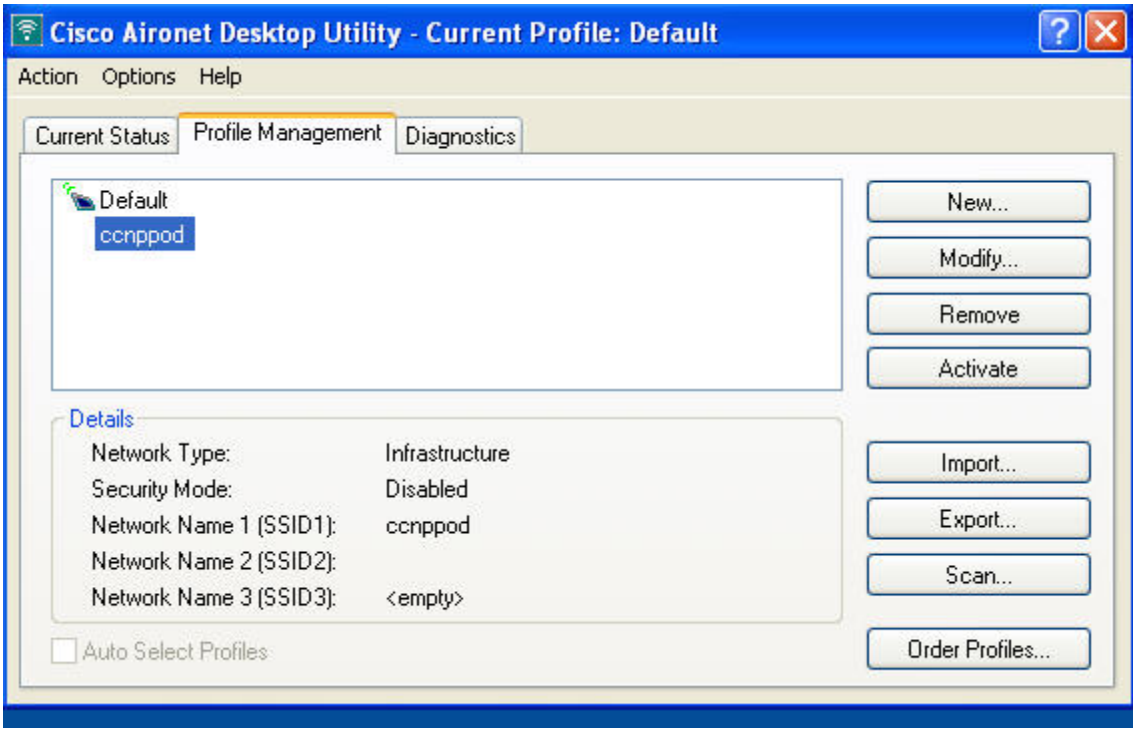
Select the **Advanced** tab. Uncheck **5GHz 54 Mbps** because you are not using 802.11a. Then click **OK**.



Advanced Configuration Options

Step 14

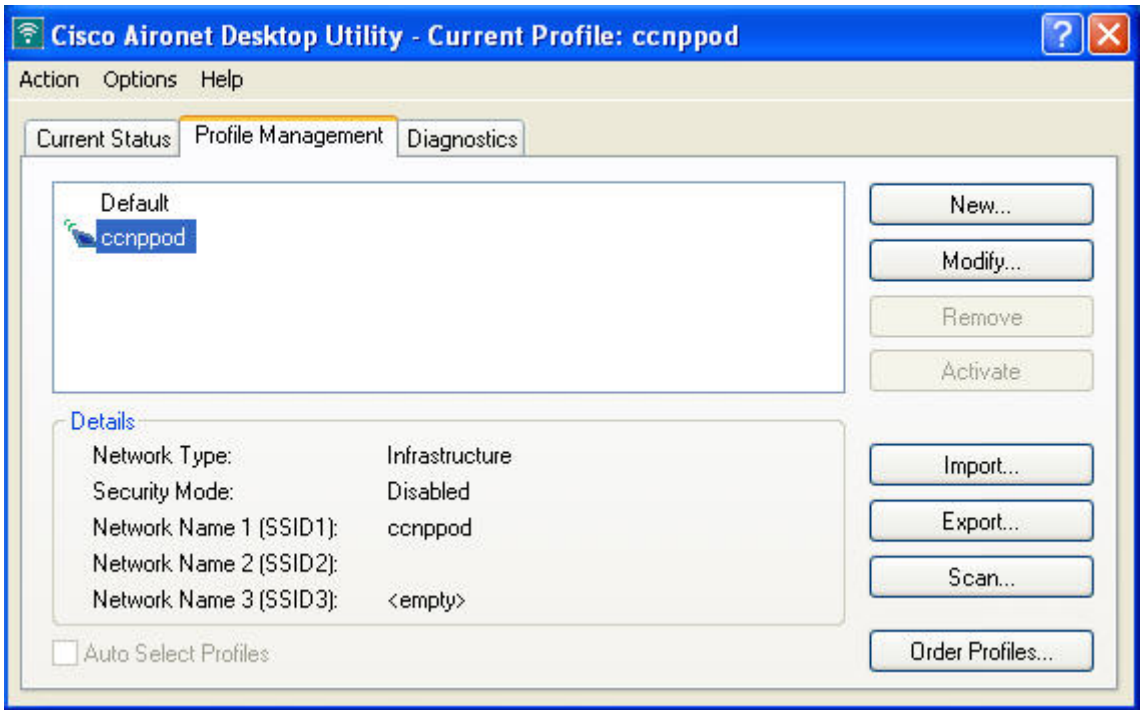
After you click on **OK**, you are returned to the **Profile Management** screen. In addition to the Default profile, there is now the ccnppod profile. Click the **Activate** button on the right hand side of the screen.



Click on the Activate Button

Step 15

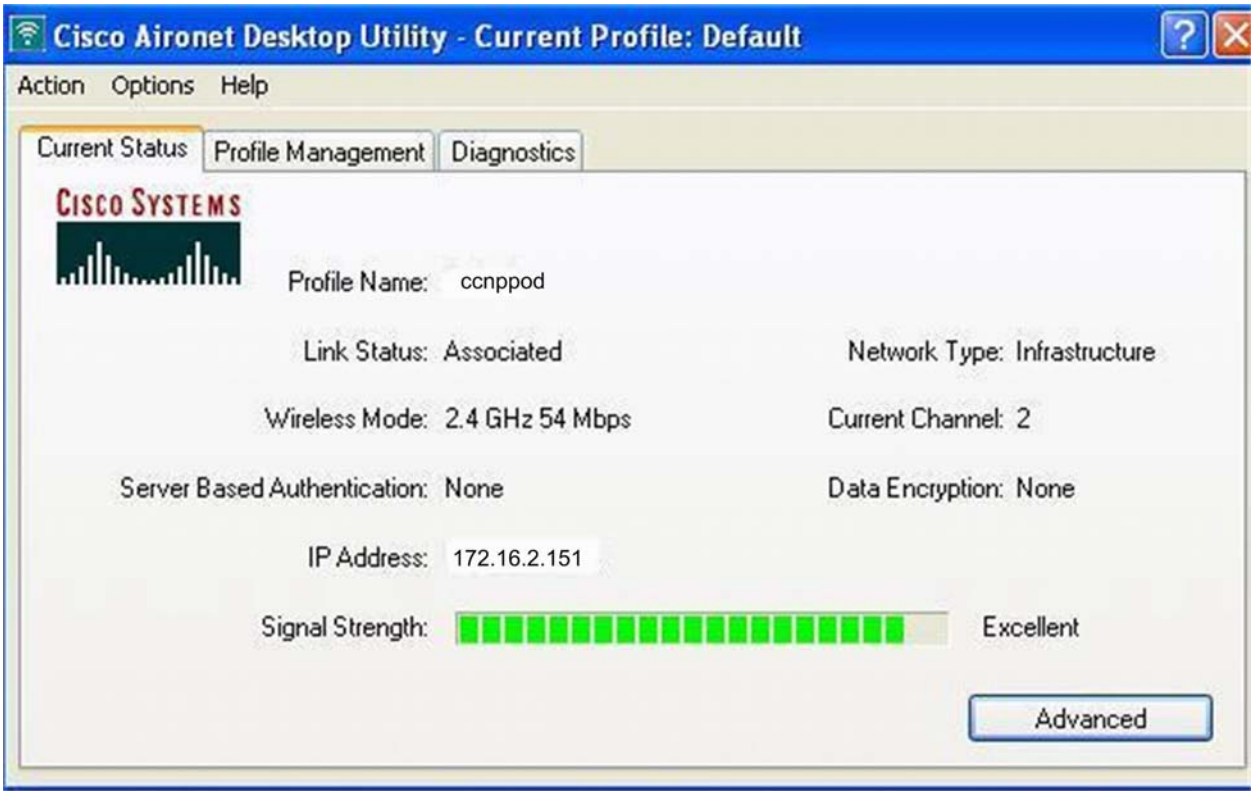
After clicking the **Activate** button, your screen will look like the image below.



ccnppod profile activated

Step 16

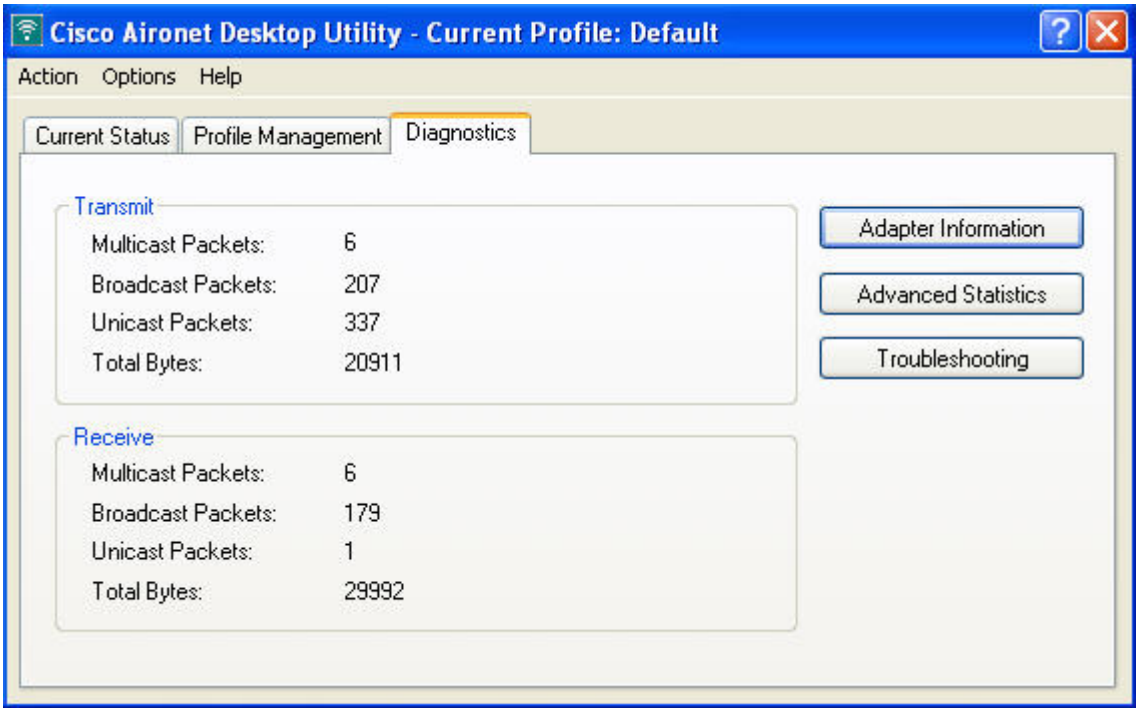
Click on the **Current Status** tab, and your screen will look similar to the image below.



Current Status of ccnppod profile

Step 17

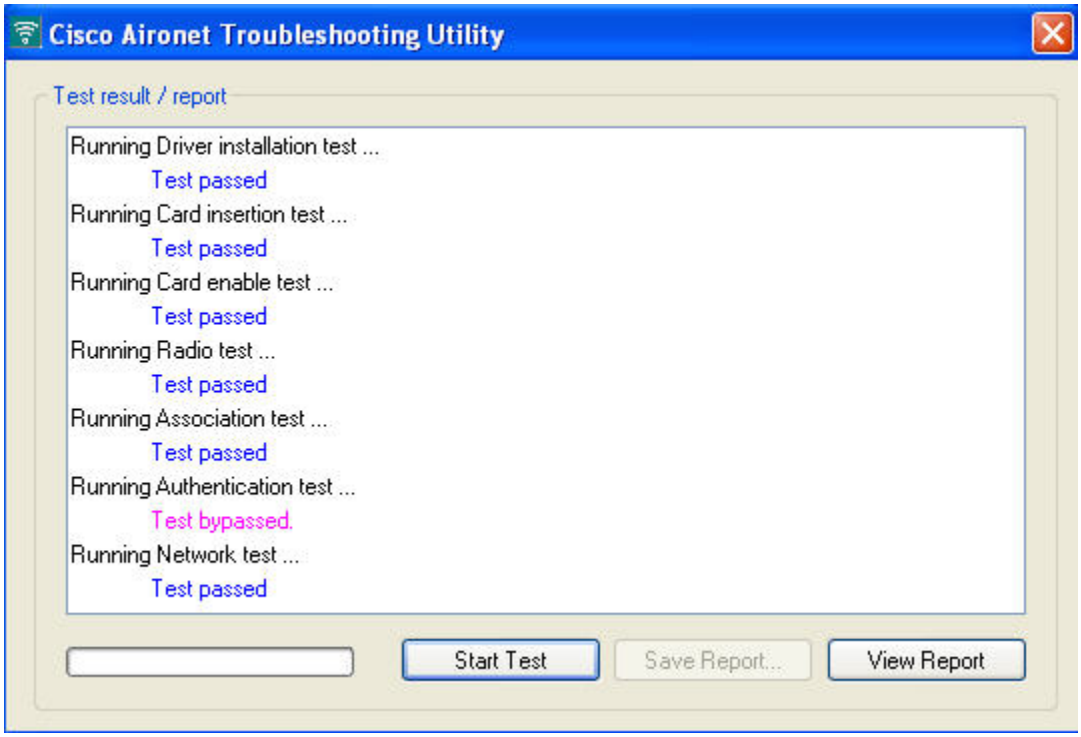
The **Diagnostics** tab shows transmit and receive data about the wireless connection.



Diagnostics Screen

Step 18

To run tests on the wireless card and see the results, click the **Troubleshooting** button.



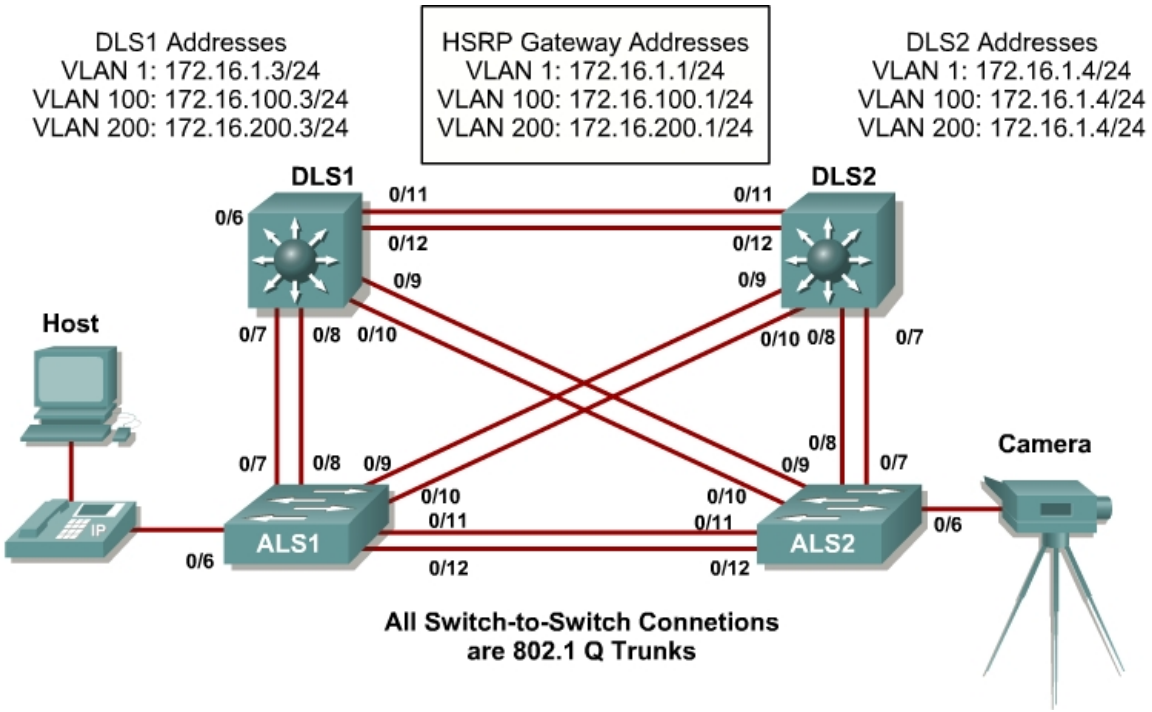
Running Troubleshooting Tests

Lab 7-1 Configuring Switches for IP Telephony Support

Learning Objectives

- Configure auto QoS to support IP phones
- Configure CoS override for data frames
- Configure the distribution layer to trust access layer QoS measures
- Manually configure CoS for devices that cannot specify CoS (camera)
- Configure HSRP for voice and data VLANS to ensure redundancy
- Configure 802.1Q trunks and EtherChannels for Layer 2 redundancy and load balancing

Topology



Scenario

IP phones have been deployed throughout the network. The phones are connected to access ports on a 2960 Cisco switch. Each user's PC is connected to the network via the phone's internal switch so that the phones can be deployed without additional wiring.

You must configure the access and distribution layer switches to trust the CoS mapping provided by the IP phone through Cisco Discovery Protocol (CDP). To ensure redundancy for the phones and user end stations, you must use HSRP on the distribution layer switches.

A camera for video is also deployed on the network, which requires that its access port on the 2960 be manually configured. It is not necessary to have a camera to successfully complete the lab.

Step 1

Power up the switches and use the standard process for establishing a HyperTerminal console connection from a workstation to each switch in your pod.

Prepare for the lab by removing all previous VLAN information and configurations. Refer to Lab 2.0, “Clearing a Single Switch,” or Lab 2.0b, “Clearing a Switch Connected to a Larger Network.”

Step 2

Cable the lab according to the diagram.

Configure the management IP addresses in VLAN 1, and the hostname, password, and telnet access on all four switches.

You also need to configure a default gateway on the access layer switches. The distribution layer switches act as Layer 3 devices and do not need default gateways.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname ALS1
ALS1(config)# enable secret cisco
ALS1(config)# line vty 0 15
ALS1(config-line)# password cisco
ALS1(config-line)# login
ALS1(config-line)# exit
ALS1(config)# interface vlan 1
ALS1(config-if)# ip address 172.16.1.101 255.255.255.0
ALS1(config-if)# no shutdown
ALS1(config-if)# exit
ALS1(config)# ip default-gateway 172.16.1.1
ALS1(config)# end
```

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname ALS2
ALS2(config)# enable secret cisco
ALS2(config)# line vty 0 15
ALS2(config-line)# password cisco
ALS2(config-line)# login
ALS2(config-line)# exit
ALS2(config)# interface vlan 1
ALS2(config-if)# ip address 172.16.1.102 255.255.255.0
ALS2(config-if)# no shutdown
ALS2(config-if)# exit
ALS2(config)# ip default-gateway 172.16.1.1
ALS2(config)# end
```



```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname DLS1
DLS1(config)# enable secret cisco
DLS1(config)# line vty 0 15
DLS1(config-line)# password cisco
DLS1(config-line)# login
DLS1(config-line)# exit
DLS1(config)# interface vlan 1
DLS1(config-if)# ip address 172.16.1.3 255.255.255.0
DLS1(config-if)# no shutdown
DLS1(config-if)# end


Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname DLS2
DLS2(config)# enable secret cisco
DLS2(config)# line vty 0 15
DLS2(config-line)# password cisco
DLS2(config-line)# login
DLS2(config-line)# exit
DLS2(config)# interface vlan 1
DLS2(config-if)# ip address 172.16.1.4 255.255.255.0
DLS2(config-if)# no shutdown
DLS2(config-if)# end
```

Step 3

Configure the trunks according to the diagram, and configure EtherChannels between the switches. Using EtherChannel for the trunks provides Layer 2 load balancing over redundant trunks.

The following is a sample configuration for the trunks and EtherChannel from DLS1 to the other three switches. Notice that the 3560 needs the **switchport trunk encapsulation** {**dot1q** | **isl}** command, because this switch also supports ISL encapsulation.

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# interface range fastethernet 0/7 - 8
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

DLS1(config-if-range)# interface range fastethernet 0/9 - 10
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2

DLS1(config-if-range)# interface range fastethernet 0/11 - 12
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# channel-group 3 mode desirable
```



```
Creating a port-channel interface Port-channel 3

DLS1(config-if-range)# end
```

The following is a sample configuration for the trunks and EtherChannels from DLS2 to the other three switches:

```
DLS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)# interface range fastethernet 0/7 - 8
DLS2(config-if-range)# switchport trunk encapsulation dot1q
DLS2(config-if-range)# switchport mode trunk
DLS2(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

DLS2(config-if-range)# interface range fastethernet 0/9 - 10
DLS2(config-if-range)# switchport trunk encapsulation dot1q
DLS2(config-if-range)# switchport mode trunk
DLS2(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2

DLS2(config-if-range)# interface range fastethernet 0/11 - 12
DLS2(config-if-range)# switchport trunk encapsulation dot1q
DLS2(config-if-range)# switchport mode trunk
DLS2(config-if-range)# channel-group 3 mode desirable

Creating a port-channel interface Port-channel 3

DLS2(config-if-range)# end
```

The following is a sample configuration for the trunks and EtherChannel from ALS1 and ALS2 to the other switches:

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface range fastethernet 0/7 - 8
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

ALS1(config-if-range)# interface range fastethernet 0/9 - 10
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2

ALS1(config-if-range)# interface range fastethernet 0/11 - 12
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 3 mode desirable

Creating a port-channel interface Port-channel 3

ALS1(config-if-range)# end
```

Sample configuration from ALS2:

```
ALS2# configure terminal
```



```
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# interface range fastethernet 0/7 - 8
ALS2(config-if-range)# switchport mode trunk
ALS2(config-if-range)# channel-group 1 mode desirable

Creating a port-channel interface Port-channel 1

ALS2(config-if-range)# interface range fastethernet 0/9 - 10
ALS2(config-if-range)# switchport mode trunk
ALS2(config-if-range)# channel-group 2 mode desirable

Creating a port-channel interface Port-channel 2

ALS2(config-if-range)# interface range fastethernet 0/11 - 12
ALS2(config-if-range)# switchport mode trunk
ALS2(config-if-range)# channel-group 3 mode desirable

Creating a port-channel interface Port-channel 3

ALS2(config-if-range)# end
```

Use the **show interfaces trunk** command on all switches to verify trunks.

1. Which VLANs are currently allowed on the newly created trunks?

Issue the **show etherchannel summary** command on each switch to verify your EtherChannels.

2. Which EtherChannel negotiation protocol is in use here?

Step 4

Change the VTP mode of ALS1 and ALS2 to client.

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# vtp mode client
Setting device to VTP CLIENT mode.
ALS1(config)# end
ALS1#

ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# vtp mode client
Setting device to VTP CLIENT mode.
ALS2(config)# end
```

Verify the VTP changes with the **show VTP status** command.

3. How many VLANs can be supported locally on the 2960 switch?

Step 5

Create the VTP domain on DLS1, and create VLANs 100 and 200 for the computer data and voice VLANs in the domain.

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# vtp domain SWPOD
DLS1(config)# vlan 100
DLS1(config-vlan)# name CP-Data
DLS1(config-vlan)# exit
DLS1(config)# vlan 200
DLS1(config-vlan)# name Voice
DLS1(config-vlan)# end
```

Verify the VTP information throughout the domain using the **show vlan** and **show vtp status** commands.

4. How many existing VLANs are in the VTP domain?

Step 6

Configure Hot Standby Router Protocol (HSRP) between the VLANs to provide redundancy in the network. To achieve some load balancing, issue the **standby** [*group*] **priority** command. Use the **ip routing** command on DLS1 and DLS2 to activate routing capabilities on the switch.

Each route processor will have its own IP address on each switched virtual interface (SVI), and also be assigned an HSRP virtual IP address for each VLAN. Devices connected to the VLAN 100 and VLAN 200 use the gateway IP address for the VLANs.

The **standby** command is also used to configure the IP address of the virtual gateway and configure the router for preempt. The **preempt** option allows for the active router with the higher priority to take over again after a network failure has been resolved.

Notice in the following configurations that the priority for VLANs 1 and 100 has been configured for 150 on DLS1, making DLS1 the active router for those

VLANs. VLAN 200 has been configured for a priority of 100 on DLS1, making DLS1 the standby router for this VLAN. Reverse priorities have been configured on the VLANs on DLS2. DLS2 is the active router for VLAN 200, and the standby router for VLANs 1 and 100.

HSRP configuration for DLS1:

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# ip routing
DLS1(config)# interface vlan 1
DLS1(config-if)# standby 1 ip 172.16.1.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 150
DLS1(config-if)# exit
DLS1(config)# interface vlan 100
DLS1(config-if)# ip address 172.16.100.3 255.255.255.0
DLS1(config-if)# standby 1 ip 172.16.100.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 150
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# interface vlan 200
DLS1(config-if)# ip address 172.16.200.3 255.255.255.0
DLS1(config-if)# standby 1 ip 172.16.200.1
DLS1(config-if)# standby 1 preempt
DLS1(config-if)# standby 1 priority 100
DLS1(config-if)# end
```

HSRP configuration for DLS2:

```
DLS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)# ip routing
DLS2(config)# interface vlan 1
DLS2(config-if)# standby 1 ip 172.16.1.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 100
DLS2(config-if)# exit
DLS2(config)# interface vlan 100
DLS2(config-if)# ip address 172.16.100.4 255.255.255.0
DLS2(config-if)# standby 1 ip 172.16.100.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 100
DLS2(config-if)# no shutdown
DLS2(config-if)# exit
DLS2(config)# interface vlan 200
DLS2(config-if)# ip address 172.16.200.4 255.255.255.0
DLS2(config-if)# standby 1 ip 172.16.200.1
DLS2(config-if)# standby 1 preempt
DLS2(config-if)# standby 1 priority 150
DLS2(config-if)# end
```

Enter the **show standby** command on both DLS1 and DLS2.

5. Which router is the active router for VLANs 1 and 100? Which is the active router for VLAN 200?

6. What is the default hello time for each VLAN? What is the default hold time?

7. How is the active HSRP router selected?

Verify routing using the **show ip route** command.

The following is a sample output from DLS1:

```
DLS1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.200.0 is directly connected, Vlan200
C       172.16.1.0 is directly connected, Vlan1
C       172.16.100.0 is directly connected, Vlan100
```

Step 7

The access layer switches will be the QoS trust boundaries for the network. Data coming in on the switchports will either have the CoS trusted or altered based on the information received on the ports.

Configure Fast Ethernet access ports 15 to 24 to trust the CoS for recognized IP phones on the network. The CoS of a Cisco IP phone is 5 by default. Any port that has a device other than a Cisco phone will not trust the CoS that is advertised. This configuration is accomplished by using the Cisco auto QoS features offered on these switches. Using a single command at the interface level, you can implement both trust boundaries and QoS features. Information obtained through CDP is used to determine when an IP phone is attached to the access port.

The following configuration also sets the voice VLAN on the interface with the **switchport voice vlan** *vlan-number* command.

Configure Fast Ethernet ports 15 through 24 on ALS1 and ALS2 using the **interface range** command:

```
ALS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)# interface range fastethernet 0/15 - 24
ALS1(config-if-range)# switchport access vlan 100
ALS1(config-if-range)# switchport voice vlan 200
ALS1(config-if-range)# auto qos voip cisco-phone
ALS1(config-if-range)# end


ALS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)# interface range fastethernet 0/15 - 24
ALS2(config-if-range)# switchport access vlan 100
ALS2(config-if-range)# switchport voice vlan 200
ALS2(config-if-range)# auto qos voip cisco-phone
ALS2(config-if-range)# end
```

Step 8

Verify the auto QoS configuration at the access layer using the **show mls qos interface** *interface-type interface-number* and the **show run** commands.

```
ALS1# show mls qos int fa 0/15
FastEthernet0/15
trust state: not trusted
trust mode: trust cos
trust enabled flag: dis
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: cisco-phone
qos mode: port-based


ALS1# show run interface fastethernet 0/15
interface FastEthernet0/15
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
```

8. What is the default CoS for a PC connected to these interfaces?

Step 9

Configure the distribution layer switches to trust the CoS information in the Layer 2 frames being sent from the access layer. Because the trust boundary is

at the access layer, frames being sent from this layer should be trusted into the distribution layer for optimal QoS.

The following are sample configurations for both DLS1 and DLS2:

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# mls qos
DLS1(config)# interface range fa0/7 - 12
DLS1(config-if-range)# auto qos voip trust
DLS1(config-if-range)# end
DLS1#

DLS2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)# mls qos
DLS2(config)# interface range fa0/7 - 12
DLS2(config-if-range)#  auto qos voip trust
DLS2(config-if-range)# end
DLS1#
```

Step 10

Verify auto QoS at the distribution layer on DLS1 and DLS2 using the **show auto qos interface** command.

```
DLS1# show auto qos interface
FastEthernet0/7
auto qos voip trust

FastEthernet0/8
auto qos voip trust

FastEthernet0/9
auto qos voip trust

FastEthernet0/10
auto qos voip trust

FastEthernet0/11
auto qos voip trust

FastEthernet0/12
auto qos voip trust
```

Use the **show mls qos interface fastethernet** *interface ID* command on DLS1 to verify QoS on the trunk interfaces:

```
DLS1# show mls qos interface fastethernet 0/7
FastEthernet0/7
trust state: trust cos
trust mode: trust cos
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```


Step 11

A camera needs to be moved from its current location in the network and connected to FastEthernet0/5 of ALS2.

Video traffic must have priority treatment within the network, because it has different requirements than voice traffic. Because the camera is not capable of setting its own CoS, assign a CoS of 3 to ensure that the video traffic is identified by other switches and routers within the network.

```
ALS1(config)# interface fastethernet 0/5
ALS1(config-if)# mls qos cos 3
```

Verify the configuration using the **show mls qos interface** command on ALS2.

```
ALS2# show mls qos interface fa0/5
FastEthernet0/5
trust state: not trusted
trust mode: not trusted
trust enabled flag: ena
COS override: dis
default COS: 3
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

9. Will other devices that are attached to this port get a CoS of 3? Explain.

Final Configurations

```
DLS1# show run
!
hostname DLS1
!
enable secret cisco
!
!
ip routing
!
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2  1
mls qos srr-queue input cos-map queue 1 threshold 3  0
mls qos srr-queue input cos-map queue 2 threshold 1  2
mls qos srr-queue input cos-map queue 2 threshold 2  4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3  3 5
mls qos srr-queue input dscp-map queue 1 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3  0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3  32
mls qos srr-queue input dscp-map queue 2 threshold 1  16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2  33 34 35 36 37 38 39 48
```



```
mls qos srr-queue input dscp-map queue 2 threshold 2  49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2  57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 3  3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3  2 4
mls qos srr-queue output cos-map queue 4 threshold 2  1
mls qos srr-queue output cos-map queue 4 threshold 3  0
mls qos srr-queue output dscp-map queue 1 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3  16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3  32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3  0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos



!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 1 mode desirable
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 1 mode desirable
```



```
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 3 mode desirable
!
!
interface Vlan1
 ip address 172.16.1.3 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan100
 ip address 172.16.100.3 255.255.255.0
 standby 1 ip 172.16.100.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan200
 ip address 172.16.200.3 255.255.255.0
 standby 1 ip 172.16.200.1
 standby 1 preempt
 no shutdown
!
!
line con 0
 password cisco
 login
line vty 0 4
```



```
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end


DLS1# show run
!
hostname DLS2
!
enable secret cisco
!
!
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2  1
mls qos srr-queue input cos-map queue 1 threshold 3  0
mls qos srr-queue input cos-map queue 2 threshold 1  2
mls qos srr-queue input cos-map queue 2 threshold 2  4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3  3 5
mls qos srr-queue input dscp-map queue 1 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3  0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3  32
mls qos srr-queue input dscp-map queue 2 threshold 1  16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2  33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2  49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2  57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 3  3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3  2 4
mls qos srr-queue output cos-map queue 4 threshold 2  1
mls qos srr-queue output cos-map queue 4 threshold 3  0
mls qos srr-queue output dscp-map queue 1 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3  16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3  32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3  0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
!
!
```



```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 1 mode desirable
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 1 mode desirable
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust cos
 auto qos voip trust
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
```



```
 mls qos trust cos
 auto qos voip trust
 channel-group 3 mode desirable
!
!
interface Vlan1
 ip address 172.16.1.4 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 preempt
 no shutdown
!
interface Vlan100
 ip address 172.16.100.4 255.255.255.0
 standby 1 ip 172.16.100.1
 standby 1 preempt
 no shutdown
!
interface Vlan200
 ip address 172.16.200.4 255.255.255.0
 standby 1 ip 172.16.200.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end

ALS1# show run
!
hostname ALS1
!
enable secret cisco
!
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2  1
mls qos srr-queue input cos-map queue 1 threshold 3  0
mls qos srr-queue input cos-map queue 2 threshold 1  2
mls qos srr-queue input cos-map queue 2 threshold 2  4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3  3 5
mls qos srr-queue input dscp-map queue 1 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3  0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3  32
mls qos srr-queue input dscp-map queue 2 threshold 1  16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2  33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2  49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2  57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3  5
```



```
mls qos srr-queue output cos-map queue 2 threshold 3  3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3  2 4
mls qos srr-queue output cos-map queue 4 threshold 2  1
mls qos srr-queue output cos-map queue 4 threshold 3  0
mls qos srr-queue output dscp-map queue 1 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3  16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3  32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3  0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
!
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
interface Port-channel3
 switchport mode trunk
!
!
interface FastEthernet0/7
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/8
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/9
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
 channel-group 3 mode desirable
!
!
interface FastEthernet0/15
 switchport access vlan 100
```



```
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
interface FastEthernet0/17
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
interface FastEthernet0/18
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
interface FastEthernet0/19
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
interface FastEthernet0/20
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
interface FastEthernet0/21
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
```



```
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
interface FastEthernet0/22
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
interface FastEthernet0/23
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
interface FastEthernet0/24
 switchport access vlan 100
 switchport voice vlan 200
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
!
!
interface Vlan1
 ip address 172.16.1.101 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end

ALS2# show run
!
hostname ALS2
!
enable secret cisco
!
!
mls qos map cos-dscp 0 8 16 26 32 46 48 56
```



```
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2  1
mls qos srr-queue input cos-map queue 1 threshold 3  0
mls qos srr-queue input cos-map queue 2 threshold 1  2
mls qos srr-queue input cos-map queue 2 threshold 2  4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3  3 5
mls qos srr-queue input dscp-map queue 1 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3  0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3  32
mls qos srr-queue input dscp-map queue 2 threshold 1  16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2  33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2  49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2  57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 3  3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3  2 4
mls qos srr-queue output cos-map queue 4 threshold 2  1
mls qos srr-queue output cos-map queue 4 threshold 3  0
mls qos srr-queue output dscp-map queue 1 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3  16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3  32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3  0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
!
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
interface Port-channel3
 switchport mode trunk
!
!
interface FastEthernet0/5
 mls qos cos 3
!
!
interface FastEthernet0/7
 switchport mode trunk
 channel-group 1 mode desirable
!
```



```
interface FastEthernet0/8
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/9
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/10
 switchport mode trunk
 channel-group 2 mode desirable
!
interface FastEthernet0/11
 switchport mode trunk
 channel-group 3 mode desirable
!
interface FastEthernet0/12
 switchport mode trunk
 channel-group 3 mode desirable
!
!
interface FastEthernet0/15
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface FastEthernet0/16
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface FastEthernet0/17
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface FastEthernet0/18
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface FastEthernet0/19
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface FastEthernet0/20
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
```



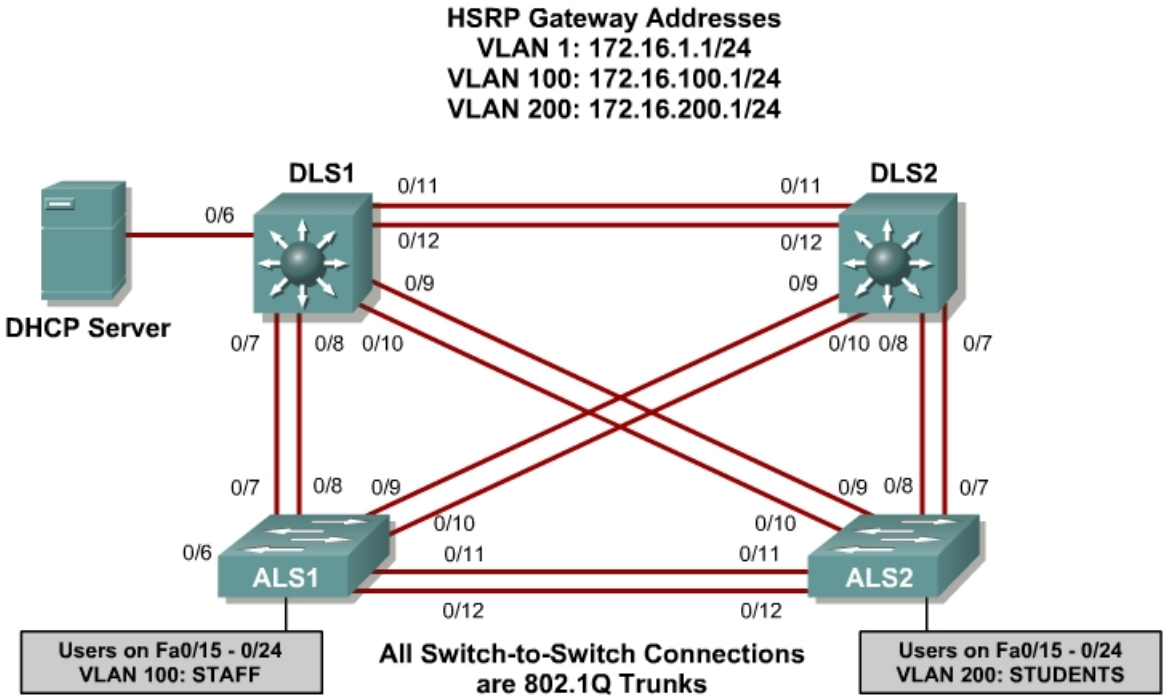
```
interface FastEthernet0/21
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface FastEthernet0/22
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface FastEthernet0/23
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface FastEthernet0/24
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
!
interface Vlan1
 ip address 172.16.1.102 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
 line vty 5 15
 password cisco
 login
!
end
```


Lab 8-1 Securing the Layer 2 Switching Devices

Learning Objectives

- Secure the Layer 2 network against MAC flood attacks
- Prevent DHCP spoofing attacks
- Prevent unauthorized access to the network using AAA and dot1x

Topology



Scenario

A fellow network engineer that you have known and trusted for many years has invited you to lunch this week. At lunch, he brings up the subject of network security and how two of his former co-workers had been arrested for using different Layer 2 attack techniques to gather data from other users in the office for their own personal gain in their careers and finances. The story shocks you because you have always known your friend to be very cautious with security on his network. His story makes you realize that your business network has been cautious with external threats, Layer 3–7 security, firewalls at the borders, and so on, but insufficient at Layer 2 security and protection inside the local network.

When you get back to the office, you meet with your boss to discuss your concerns. After reviewing the company's security policies, you begin to work on a Layer 2 security policy.

First, you establish which network threats you are concerned about and then put together an action plan to mitigate these threats. While researching these threats, you learn about other potential threats to Layer 2 switches that might not be malicious but could greatly threaten network stability. You decide to include these threats in the policies as well.

Other security measures need to be put in place to further secure the network, but you begin with configuring the switches against a few specific types of attacks, including MAC flood attacks, DHCP spoofing attacks, and unauthorized access to the local network. You plan to test the configurations in a lab environment before placing them into production.

Step 1

Power up the switches and use the standard process for establishing a HyperTerminal console connection from a workstation to each switch in your pod.

Remove all VLAN information and configurations that were previously entered into your switches. (Refer to Lab 2.0a or 2.0b if needed.)

Step 2

Cable the lab according to the diagram. Configure the management IP addresses in VLAN 1, and configure the hostname, password, and Telnet access on all four switches. HSRP will be used later in the lab, so set up the IP addressing for VLAN 1 on DLS1 and DLS2. Because 172.16.1.1 will be the virtual default gateway for this VLAN, use the .3 and .4 for the IP addresses on DLS1 and DLS2, respectively.

You also need to configure a default gateway on the access layer switches. The distribution layer switches act as Layer 3 devices and do not need default gateways.

Set up 802.1q trunking between the switches according to the diagram. The default trunking for the 2960 switch is dot1q, so you do not need to configure it.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname ALS1
ALS1(config)#enable secret cisco
ALS1(config)#line vty 0 15
ALS1(config-line)#password cisco
ALS1(config-line)#login
ALS1(config-line)#exit
ALS1(config)#interface vlan 1
```



```
ALS1(config-if)#ip address 172.16.1.101 255.255.255.0
ALS1(config-if)#no shutdown
ALS1(config-if)#exit
ALS1(config)#ip default-gateway 172.16.1.1
ALS1(config)#interface range fastethernet 0/7 - 12
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#end
ALS1#


Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname ALS2
ALS2(config)#enable secret cisco
ALS2(config)#line vty 0 15
ALS2(config-line)#password cisco
ALS2(config-line)#login
ALS2(config-line)#exit
ALS2(config)#interface vlan 1
ALS2(config-if)#ip address 172.16.1.102 255.255.255.0
ALS2(config-if)#no shutdown
ALS2(config-if)#exit
ALS2(config)#ip default-gateway 172.16.1.1
ALS2(config)#interface range fastethernet 0/7 - 12
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#end
ALS2#


Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname DLS1
DLS1(config)#enable secret cisco
DLS1(config)#line vty 0 15
DLS1(config-line)#password cisco
DLS1(config-line)#login
DLS1(config-line)#exit
DLS1(config)#interface vlan 1
DLS1(config-if)#ip address 172.16.1.3 255.255.255.0
DLS1(config-if)#no shutdown
DLS1(config-if)#exit
DLS1(config)#interface range fastethernet 0/7 - 12
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#end


Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname DLS2
DLS2(config)#enable secret cisco
DLS2(config)#line vty 0 15
DLS2(config-line)#password cisco
DLS2(config-line)#login
DLS2(config-line)#exit
DLS2(config)#interface vlan 1
DLS2(config-if)#ip address 172.16.1.4 255.255.255.0
DLS2(config-if)#no shutdown
DLS1(config-if)#exit
DLS1(config)#interface range fastethernet 0/7 - 12
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#end
```


Verify trunking and spanning tree operations using the **show interfaces trunk** and **show spanning tree** commands.

1. Which trunks are marked as designated for ALS1?

2. Is trunk negotiation being used here? Which mode are the trunks in?

Step 3

Set up the VLANs according to the diagram. Two VLANs are in use at this time: one for students, and one for faculty and staff. These VLANs will be created on DLS1, which is set up as a VTP server. DLS2 also remains in its default VTP mode and acts as a server as well. ALS1 and ALS2 are configured as VTP clients.

The user access ports for these VLANs also needs to be configured on ALS1 and ALS2. Set up these ports as static access ports and turn spanning tree portfast on. Configure these ports according to the diagram.

HSRP is a requirement for the network, and VLANs 100 and 200 are configured to use HSRP to provide redundancy at Layer 3. Use the **priority** command to make DLS1 the active router for VLANs 1 and 100, and DLS2 the active router for VLAN 200.

The following is an example for ALS1 and ALS2 for the VTP client changes:

```
ALS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#vtp mode client
Setting device to VTP CLIENT mode.
ALS1(config)#interface range fa0/15 - 24
ALS1(config-if-range)#switchport mode access
ALS1(config-if-range)#switchport access vlan 100
ALS1(config-if-range)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 10 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.

ALS1(config-if-range)#end
ALS1#
```



```
ALS2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)#vtp mode client
Setting device to VTP CLIENT mode.
ALS2(config)#interface range fa0/15 - 24
ALS2(config-if-range)#switchport mode access
ALS2(config-if-range)#switchport access vlan 200
ALS2(config-if-range)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 10 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.

ALS2(config-if-range)#end
ALS2#
```

The following are sample configurations for the VLAN setup and HSRP:

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#vtp domain SWPOD
DLS1(config)#vlan 100
DLS1(config-vlan)#name Staff
DLS1(config-vlan)#exit
DLS1(config)#vlan 200
DLS1(config-vlan)#name Student
DLS1(config-vlan)#exit
DLS1(config)#ip routing
DLS1(config)#interface vlan 1
DLS1(config-if)#standby 1 ip 172.16.1.1
DLS1(config-if)#standby 1 preempt
DLS1(config-if)#standby 1 priority 150
DLS1(config-if)#exit
DLS1(config)#int vlan 100
DLS1(config-if)#ip add 172.16.100.3 255.255.255.0
DLS1(config-if)#standby 1 ip 172.16.100.1
DLS1(config-if)#standby 1 preempt
DLS1(config-if)#standby 1 priority 150
DLS1(config-if)#no shutdown
DLS1(config-if)#exit
DLS1(config)#int vlan 200
DLS1(config-if)#ip add 172.16.200.3 255.255.255.0
DLS1(config-if)#standby 1 ip 172.16.200.1
DLS1(config-if)#standby 1 preempt
DLS1(config-if)#standby 1 priority 100
DLS1(config-if)#end


DLS2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)#ip routing
DLS2(config)#interface vlan 1
DLS2(config-if)#standby 1 ip 172.16.1.1
DLS2(config-if)#standby 1 preempt
DLS2(config-if)#standby 1 priority 100
DLS2(config-if)#exit
DLS2(config)#int vlan 100
```



```
DLS2(config-if)#ip add 172.16.100.4 255.255.255.0
DLS2(config-if)#standby 1 ip 172.16.100.1
DLS2(config-if)#standby 1 preempt
DLS2(config-if)#standby 1 priority 100
DLS2(config-if)#no shutdown
DLS2(config-if)#exit
DLS2(config)#int vlan 200
DLS2(config-if)#ip add 172.16.200.4 255.255.255.0
DLS2(config-if)#standby 1 ip 172.16.200.1
DLS2(config-if)#standby 1 preempt
DLS2(config-if)#standby 1 priority 150
DLS2(config-if)#end
```

Verify your configurations using the **show vlan**, **show vtp**, **show standby**, and **show ip route** commands.:

3. What is the active router for VLANs 1 and 100? What is the active router for VLAN 200?

4. How many VLANs are active in the VTP domain?

Step 4

The following table shows the appropriate verification methods and mitigation approaches for the attack types specified in the left column:

Attack Type	Verification	Mitigation
MAC address spoofing or flooding	Show CAM dynamic	MAC port security
DHCP spoofing	View DHCP leases for discrepancies	Configure DHCP snooping
Unauthorized LAN access	Verification is very difficult for this type of attack	Configure authentication using AAA

Step 5

To protect against MAC flooding or spoofing attacks, configure port security on the VLAN 100 and 200 access ports. Because the two VLANs serve different purposes—one for staff and one for students—configure the ports to meet the different needs.

The student VLAN must allow for MAC addresses assigned to a port to change, because most of the student use laptops and move around within the network. Set up port security so that only one MAC address is allowed on a port at a given time. (This type of configuration does not work on ports that need to service IP phones with PCs attached. In this case, there would be two allowed MAC addresses.) This can be accomplished using the **switchport port-security maximum <*# of MAC addresses*>** command.

The staff MAC addresses do not change often, because the staff uses desktop workstations provided by the IT department. In this case, you can configure the staff VLAN so that the MAC address learned on a port is added to the configuration on the switch as if the MAC address were configured using the **switchport port-security mac-address** command. This feature, which is called sticky learning, is available on some switch platforms. It combines the features of dynamically learned and statically configured addresses. The staff ports also allow for a maximum of two MAC addresses to be dynamically learned per port.

The following is a sample configuration for the student access ports on ALS2:

```
ALS2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)#interface range fastethernet 0/15 - 24
ALS2(config-if-range)#switchport port-security maximum 1
ALS2(config-if-range)#end
```

Note that the maximum number of MAC addresses allowed on FastEthernet 0/15 – 24 is one.

Verify your configuration for ALS2 using the **show port-security** *interface* command.

```
ALS2#show port-security interface fa0/15
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
```



```
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

The following is a sample configuration of the staff ports on ALS1:

```
ALS1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#interface range fastethernet 0/15 - 24
ALS1(config-if-range)#switchport port-security maximum 2
ALS1(config-if-range)#switchport port-security mac-address sticky
ALS1(config-if-range)#end
```

This time two MAC addresses are allowed. Both will be dynamically learned and then added to the running configuration.

Verify your configuration using the **show port-security** *interface* command.

```
ALS1# show port-security int fa0/15
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Step 6

DHCP spoofing is a “man-in-the-middle” type of attack in that an attacker gains access to information meant for another destination. The attacker replies to a DHCP request, claiming to have valid gateway and DNS information. A valid DHCP server may also reply to the request, but if the attacker’s reply reaches the requestor first, the invalid information from the attacker is used. The attacking device then receives the data before it is sent to the proper destination.

To help protect the network from such an attack, you can use DHCP snooping. DHCP snooping is a Cisco Catalyst feature that determines which switch ports are allowed to respond to DHCP requests. Ports are identified as trusted or untrusted. Trusted ports can source all DHCP messages, while untrusted ports can source requests only. Trusted ports host a DHCP server or can be an uplink toward a DHCP server. If a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is shut down. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as a DHCPOFFER, DHCPACK, or DHCPNAK.

The first step to configure DHCP snooping is to turn snooping on globally on all switches using the **ip dhcp snooping** command.

Second, you configure the trusted interfaces with the **ip dhcp snooping trust** command. By default, all ports are considered untrusted unless statically configured to be trusted. For this network, configure all trunk ports as trusted, as well as port FastEthernet 0/6 on DLS1, which connects to the DCHP server for the network.

Next we will configure a DHCP request rate limit on the user access ports to limit the amount of DHCP requests that are allowed per second. This is configured using the **ip dhcp snooping limit rate *<rate in pps>***. This is used to prevent DHCP starvation attacks by limiting the rate of the DHCP requests on untrusted ports.

Finally, configure the VLANs that will use DHCP snooping. DHCP snooping will be used on both the student and staff VLANs.

```
DLS1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#ip dhcp snooping
DLS1(config)#interface fastethernet 0/6
DLS1(config-if)#ip dhcp snooping trust
DLS1(config-if)#exit
DLS1(config)#interface range fastethernet 0/7 - 12
DLS1(config-if-range)#ip dhcp snooping trust
DLS1(config-if-range)#exit
DLS1(config)#ip dhcp snooping vlan 100,200
DLS1(config)#end
```

Verify your configuration using the **show ip dhcp snooping** command.

```
DLS1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
100,200
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/6              yes         unlimited
FastEthernet0/7              yes         unlimited
FastEthernet0/8              yes         unlimited
FastEthernet0/9              yes         unlimited
FastEthernet0/10             yes         unlimited
FastEthernet0/11             yes         unlimited
FastEthernet0/12             yes         unlimited
DLS1#
```

Configure DLS2 to trust DHCP information on the trunk links, enable DHCP snooping globally, and define the VLANs that will use DHCP snooping for this switch.

```
DLS2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
```



```
DLS2(config)#ip dhcp snooping
DLS2(config)#interface range fastEthernet 0/7 - 12
DLS2(config-if-range)#ip dhcp snooping trust
DLS2(config-if-range)#exit
DLS2(config)#ip dhcp snooping vlan 100,200
DLS2(config)#end
```

Configure ALS1 and ALS2 to trust DHCP information on the trunk ports only, and limit the rate that requests are received with the **ip DHCP snooping limit rate** command.

```
ALS1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#ip dhcp snooping
ALS1(config)#interface range fastethernet 0/7 - 12
ALS1(config-if-range)#ip dhcp snooping trust
ALS1(config-if-range)#exit
ALS1(config)#interface range fastethernet 0/15 - 24
ALS1(config-if-range)#ip dhcp snooping limit rate 20
ALS1(config-if-range)#exit
ALS1(config)#ip dhcp snooping vlan 100,200
ALS1(config)#end
```

```
ALS2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ALS2(config)#ip dhcp snooping
ALS2(config)#interface range fastethernet 0/7 - 12
ALS2(config-if-range)#ip dhcp snooping trust
ALS2(config-if-range)#exit
ALS2(config)#interface range fastethernet 0/15 - 24
ALS2(config-if-range)#ip dhcp snooping limit rate 20
ALS2(config-if-range)#exit
ALS2(config)#ip dhcp snooping vlan 100,200
ALS2(config)#end
```

Verify the configurations on ALS1 and ALS2 using the **show ip dhcp snooping** command.

```
ALS2# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
100,200
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/7              yes         unlimited
FastEthernet0/8              yes         unlimited
FastEthernet0/9              yes         unlimited
FastEthernet0/10             yes         unlimited
FastEthernet0/11             yes         unlimited
FastEthernet0/12             yes         unlimited
FastEthernet0/15             no          20
FastEthernet0/16             no          20
FastEthernet0/17             no          20
FastEthernet0/18             no          20
FastEthernet0/19             no          20
FastEthernet0/20             no          20
FastEthernet0/21             no          20
```



```
FastEthernet0/22            no          20
FastEthernet0/23            no          20
FastEthernet0/24            no          20
ALS2#
```

5. Will DHCP replies be allowed on access ports assigned to VLAN 200?

6. How many DHCP packets will be allowed on FastEthernet 0/16 per second?

Step 7

The authentication portion of AAA requires a user to be identified before being allowed access to the network. Authentication is configured by defining a list of methods for authentication and applying that list to specific interfaces. If lists are not defined, a default list is used.

For this network, it has been decided that AAA using 802.1x will be used to control user access for the staff VLAN using a local list of usernames and passwords. Once a radius server is added to the network, all user ports, including the student VLAN, will also be added to the configuration.

The IEEE 802.1x standard defines a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switchports. The authentication server authenticates each workstation that is connected to a switchport before making any services that are offered by the switch or the LAN available.

Until the workstation is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the workstation is connected. After authentication succeeds, normal traffic can pass through the port.

Use the **aaa new-model** command to turn on AAA authentication on ALS1. The **aaa authentication dot1x default local** command tells the switch to use a local database of usernames and passwords to authenticate the users. Users are assigned to the database using the **username** *username* **password** *password* command.

The Fast Ethernet interfaces used for VLAN 100 staff access are configured using the **dot1x port-control auto** command. The **auto** keyword allows the switchport to begin in the unauthorized state, and allows the negotiation

between the client and server to authenticate the user. Once authenticated, the user is allowed access to the network resources.

The following is a sample configuration for ALS1:

```
ALS1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#username janedoe password 0 cisco
ALS1(config)#username johndoe password 0 cisco
ALS1(config)#username joesmith password 0 cisco
ALS1(config)#aaa new-model
ALS1(config)#aaa authentication dot1x default local
ALS1(config)#int range fa 0/15 - 24
ALS1(config-if-range)#dot1x port-control auto
ALS1(config-if-range)#end
```

Verify your AAA configuration using the **show dot1x interface** command.

```
ALS1# show dot1x interface fa0/15
Supplicant MAC <Not Applicable>
   AuthSM State      = N/A
   BendSM State      = N/A
PortStatus        = N/A
MaxReq            = 2
MaxAuthReq        = 2
HostMode          = Single
PortControl       = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

7. If a user with a username frankadams attempts to connect to the staff VLAN access ports, will he be allowed access? Will the user be allowed access to the student VLAN ports?

8. How will the configuration need to be changed when a radius server is added to the network?

Final Configurations

```
DLS1# show run
Building configuration...
!
hostname DLS1
!
enable secret cisco
!
ip routing
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
!
interface FastEthernet0/6
 ip dhcp snooping trust
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface Vlan1
 ip address 172.16.1.3 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan100
 ip address 172.16.100.3 255.255.255.0
 standby 1 ip 172.16.100.1
```



```
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan200
 ip address 172.16.200.3 255.255.255.0
 standby 1 ip 172.16.200.1
 standby 1 preempt
 no shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end


DLS2# show run
Building configuration...
!
hostname DLS2
!
enable secret cisco
!
!
ip routing
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
```



```
 ip dhcp snooping trust
!
interface Vlan1
 ip address 172.16.1.4 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 preempt
 no shutdown
!
interface Vlan100
 ip address 172.16.100.4 255.255.255.0
 standby 1 ip 172.16.100.1
 standby 1 preempt
 no shutdown
!
interface Vlan200
 ip address 172.16.200.4 255.255.255.0
 standby 1 ip 172.16.200.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end


ALS1#show run
Building configuration...
!
hostname ALS1
!
enable secret cisco
!
username janedoe password 0 cisco
username johndoe password 0 cisco
username joesmith password 0 cisco
aaa new-model
aaa authentication dot1x default local
!
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
!
interface FastEthernet0/7
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport mode trunk
 ip dhcp snooping trust
```



```
!
interface FastEthernet0/10
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport mode trunk
 ip dhcp snooping trust
!
!
interface FastEthernet0/15
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/16
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/17
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/18
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/19
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/20
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
```



```
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/21
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/22
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/23
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/24
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
!
interface Vlan1
 ip address 172.16.1.101 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
line vty 5 15
 password cisco
!
end


ALS1# show run
Building configuration...
!
```



```
!
hostname ALS2
!
enable secret cisco
!
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
!
interface FastEthernet0/7
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport mode trunk
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport mode trunk
 ip dhcp snooping trust
!
!
interface FastEthernet0/15
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/16
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/17
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/18
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/19
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
```



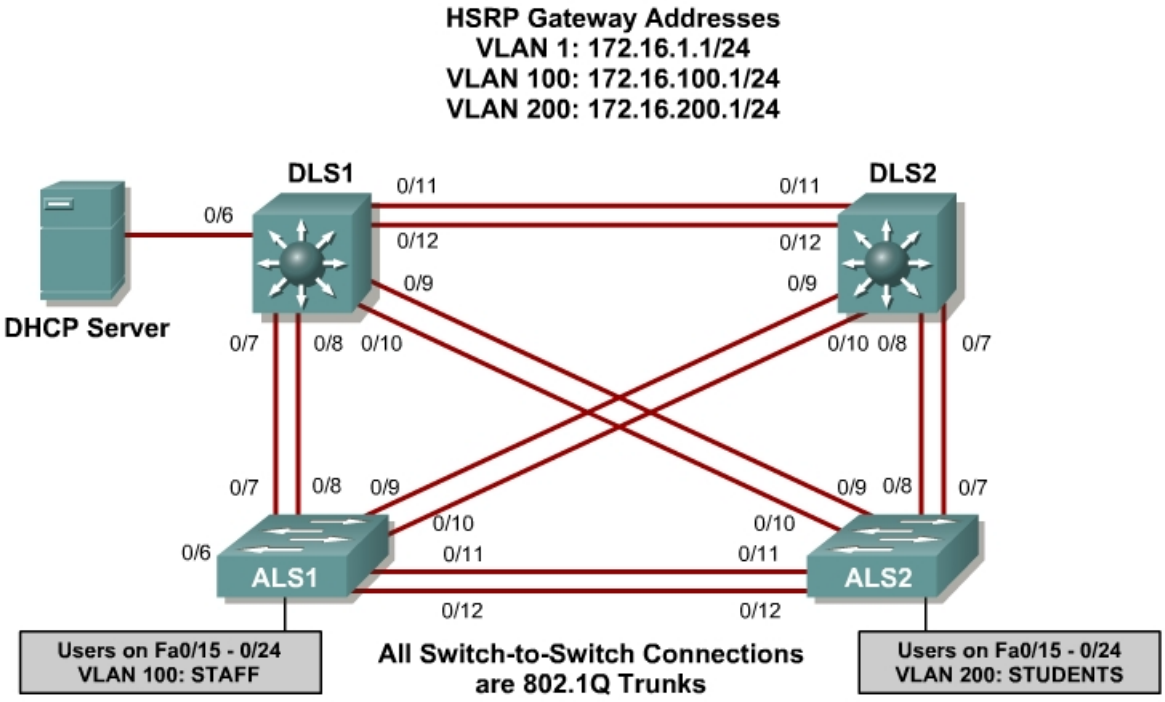
```
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/20
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/21
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/22
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/23
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/24
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
!
interface Vlan1
 ip address 172.16.1.102 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```


Lab 8-2 Securing Spanning Tree Protocol

Learning Objectives

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

Topology



Scenario

This lab is a continuation of Lab 8.1 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 with 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.

Step 1

Verify the configurations from Lab 8.1 by issuing the **show vtp status** command on ALS2. 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.

```
ALS2# show vtp status
VTP Version                     : 2
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                     : Disabled
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
ALS1#
```

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

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

```
DLS1# show vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
200  enet  100200     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```



```
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

DLS1#
```

2. Which ports are not showing as active for VLAN 1? Why is this?

Issue the **show interface trunk** command on DLS2. If trunking was configured properly in Lab 8.1, FastEthernet 0/7 – 0/12 should be in trunking mode on all switches.

```
DLS2# show int 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
DLS2#
```


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

Issue the **show spanning-tree vlan 1** command on DLS2. The results from this command may vary, and DLS2 may or may 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

DLS2#
```

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

5. What is the ID priority of the current bridge?

Step 2

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 for VLANs 1 and 100.

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

```
DLS1#config t
Enter configuration commands, one per line. End with CNTL/Z
DLS1(config)#spanning-tree vlan 1,100 root primary
DLS1(config)#spanning-tree vlan 200 root secondary
DLS1(config)#end


DLS2#config t
Enter configuration commands, one per line. End with CNTL/Z
DLS2(config)#spanning-tree vlan 1,100 root secondary
DLS2(config)#spanning-tree vlan 200 root primary
DLS2(config)#end
```

Verify your 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

DLS2#
```

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

Step 3

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 switchports where you would never expect to find the root bridge for a VLAN.

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. Set up root guard on these ports to ensure that if a switch is added, it is not allowed to take over as root.

```
DLS1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DLS1(config)#interface range fastEthernet 0/13 - 14
DLS1(config-if-range)#spanning-tree guard root
DLS1(config-if-range)#end
DLS1#
```

Configure the same on DLS2, ALS1, and ALS2.

7. What will happen if a switch is connected to FA0/13 via a crossover cable?

Step 4

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. 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
```

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#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#interface FastEthernet 0/9
ALS2(config-if)#spanning-tree guard root
ALS2(config-if)#end
```


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
VLAN0100.
1w4d: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/9 on
VLAN0200.
```

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
```

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

```
ALS2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#interface FastEthernet 0/9
ALS2(config-if)#no spanning-tree guard root
ALS2(config-if)#end
```

Once 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

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 disrupt the STP topology, so you should protect these ports from accidental or malicious behavior that could cause BPDUs. 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.

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

```
ALS1#config t
Enter configuration commands, one per line. End with CNTL/Z.
ALS1(config)#spanning-tree portfast bpduguard default
ALS1(config)#end

ALS2#config t
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#spanning-tree portfast bpduguard default
ALS2(config)#end
```

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
ALS2#
```

8. What action will be taken if a wireless access point sending BPDUs is connected to FA0/15 on ALS1?

Step 6

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 gigabit interfaces. The **aggressive** keyword places the port in the error-disable state when a violation occurs on the port.

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

```
DLS1#config t
Enter configuration commands, one per line. End with CNTL/Z.
DLS1(config)#interface range FastEthernet 0/1 - 24
DLS1(config-if-range)#udld port aggressive
DLS1(config-if-range)#exit
DLS1(config)#udld enable
DLS1(config)#end

DLS2#config t
Enter configuration commands, one per line. End with CNTL/Z.
DLS2(config)#interface range FastEthernet 0/1 - 24
DLS2(config-if-range)#udld port aggressive
DLS2(config-if-range)#exit
DLS2(config)#udld enable
DLS2(config)#end

ALS1#config t
Enter configuration commands, one per line. End with CNTL/Z.
ALS1(config)#interface range FastEthernet 0/1 - 24
ALS1(config-if-range)#udld port aggressive
ALS1(config-if-range)#exit
ALS1(config)#udld enable
ALS1(config)#end

ALS2#config t
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#interface range FastEthernet 0/1 - 24
ALS2(config-if-range)#udld port aggressive
ALS2(config-if-range)#exit
ALS2(config)#udld enable
ALS2(config)#end

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
```

Verify your configuration using the **show UDLD** *interface ID* command.

```
ALS2# show udld fa 0/15

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
```

9. What is the operation state of this interface?

Note: Keep all configurations from this lab for the next Layer 2 security lab.

Final Configurations

```
DLS1#show run
Building configuration...

Current configuration : 2928 bytes
!
!
hostname DLS1
!
enable secret cisco
!
!
udld enable
!
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1,100 priority 24576
spanning-tree vlan 200 priority 28672
!
!
interface FastEthernet0/1
 udld port aggressive
!
interface FastEthernet0/2
 udld port aggressive
!
interface FastEthernet0/3
 udld port aggressive
!
interface FastEthernet0/4
 udld port aggressive
!
interface FastEthernet0/5
 udld port aggressive
!
interface FastEthernet0/6
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/9
```



```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/13
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/14
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/15
 udld port aggressive
!
interface FastEthernet0/16
 udld port aggressive
!
interface FastEthernet0/17
 udld port aggressive
!
interface FastEthernet0/18
 udld port aggressive
!
interface FastEthernet0/19
 udld port aggressive
!
interface FastEthernet0/20
 udld port aggressive
!
interface FastEthernet0/21
 udld port aggressive
!
interface FastEthernet0/22
 udld port aggressive
!
interface FastEthernet0/23
 udld port aggressive
!
interface FastEthernet0/24
 udld port aggressive
!
interface GigabitEthernet0/1
!
```



```
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 172.16.1.3 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan100
 ip address 172.16.100.3 255.255.255.0
 standby 1 ip 172.16.100.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan200
 ip address 172.16.200.3 255.255.255.0
 standby 1 ip 172.16.200.1
 standby 1 preempt
 no shutdown
!

!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

```
DLS2#show run
Building configuration...

Current configuration : 2880 bytes
!
!
hostname DLS2
!
enable secret cisco
!
!
udld enable
!
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1,100 priority 28672
spanning-tree vlan 200 priority 24576
!
```



```
!
interface FastEthernet0/1
 udld port aggressive
!
interface FastEthernet0/2
 udld port aggressive
!
interface FastEthernet0/3
 udld port aggressive
!
interface FastEthernet0/4
 udld port aggressive
!
interface FastEthernet0/5
 udld port aggressive
!
interface FastEthernet0/6
 udld port aggressive
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/13
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/14
 udld port aggressive
 spanning-tree guard root
!
```



```
interface FastEthernet0/15
 udld port aggressive
!
interface FastEthernet0/16
 udld port aggressive
!
interface FastEthernet0/17
 udld port aggressive
!
interface FastEthernet0/18
 udld port aggressive
!
interface FastEthernet0/19
 udld port aggressive
!
interface FastEthernet0/20
 udld port aggressive
!
interface FastEthernet0/21
 udld port aggressive
!
interface FastEthernet0/22
 udld port aggressive
!
interface FastEthernet0/23
 udld port aggressive
!
interface FastEthernet0/24
 udld port aggressive
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 172.16.1.4 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 preempt
 no shutdown
!
interface Vlan100
 ip address 172.16.100.4 255.255.255.0
 standby 1 ip 172.16.100.1
 standby 1 preempt
 no shutdown
!
interface Vlan200
 ip address 172.16.200.4 255.255.255.0
 standby 1 ip 172.16.200.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
```



```
!
end



ALS1#show run
Building configuration...

Current configuration : 4682 bytes
!
!
hostname ALS1
!
enable secret cisco
!
username janedoe password 0 cisco
username johndoe password 0 cisco
username joesmith password 0 cisco
aaa new-model
aaa authentication dot1x default local
!
aaa session-id common
udld enable
!
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 udld port aggressive
!
interface FastEthernet0/2
 udld port aggressive
!
interface FastEthernet0/3
 udld port aggressive
!
interface FastEthernet0/4
 udld port aggressive
!
interface FastEthernet0/5
 udld port aggressive
!
interface FastEthernet0/6
 udld port aggressive
!
interface FastEthernet0/7
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport mode trunk
```



```
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/13
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/14
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/15
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/16
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/17
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/18
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
```



```
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/19
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/20
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/21
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/22
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/23
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/24
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
```



```
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 172.16.1.101 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!

!
radius-server source-ports 1645-1646
!
line con 0
 password cisco
line vty 0 4
 password cisco
line vty 5 15
 password cisco
!
end


ALS2#show run
Building configuration...

!
!
hostname ALS2
!
enable secret cisco
!
!
udld aggressive
!
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
!
spanning-tree mode pvst
spanning-tree portfast bpduguard default
!
!
interface FastEthernet0/1
 udld port aggressive
!
interface FastEthernet0/2
 udld port aggressive
!
interface FastEthernet0/3
 udld port aggressive
!
interface FastEthernet0/4
 udld port aggressive
!
interface FastEthernet0/5
 udld port aggressive
!
interface FastEthernet0/6
 udld port aggressive
!
```



```
interface FastEthernet0/7
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/13
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/14
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/15
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/16
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/17
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/18
 switchport access vlan 200
 switchport mode access
 udld port aggressive
```



```
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/19
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/20
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/21
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/22
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/23
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/24
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 172.16.1.102 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
```



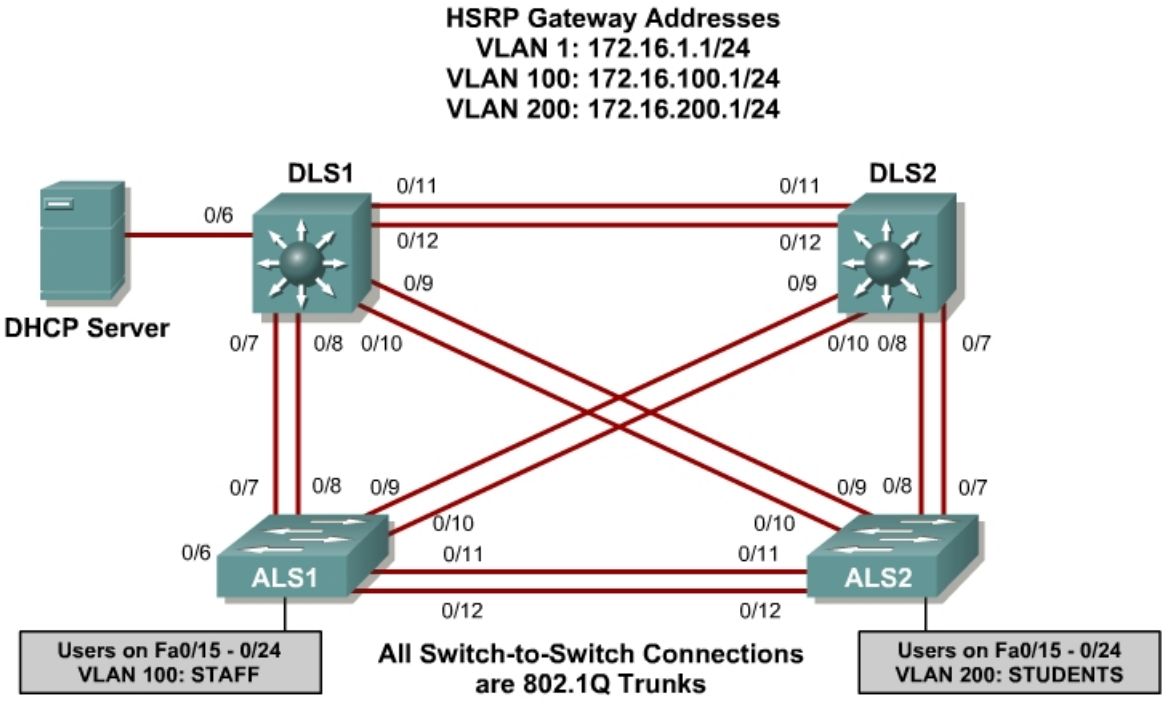
```
 password cisco
 login
!
end
```


Lab 8.3 Securing VLANs with Private VLANs, RACLs, and VACLs

Learning Objectives

- Secure the server farm using private VLANs
- Secure the staff VLAN from the student VLAN
- Secure the staff VLAN when temporary staff personnel are used

Topology



Scenario

In this lab, you will configure the network to protect the VLANs using router ACLs, VLAN ACLs, and private VLANs. First, you will secure the new server farm by using private VLANs so that broadcasts on one server VLAN are not heard by the other server VLAN. Service providers use private VLANs to separate different customers' traffic while utilizing the same parent VLAN for all server traffic. The private VLANs provide traffic isolation between devices, even though they may exist on the same VLAN.

Then, you will secure the staff VLAN from the student VLAN by using a RACL, which prevents traffic from the student VLAN from reaching the staff VLAN. This allows the student traffic to utilize the network and Internet services while keeping the students from accessing any of the staff resources.

Lastly, you will configure a VACL that allows a host on the staff network to be set up to use the VLAN for access but keeps the host isolated from the rest of the staff machines. This machine is used by temporary staff employees.

Step 1

Verify that the configurations from Labs 8.1 and 8.2 are loaded on the devices by issuing the **show vtp status** command on ALS1. 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.

```
ALS1#show vtp status
VTP Version                     : 2
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                     : Disabled
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
ALS1#
```

1. Will VLAN information be stored in NVRAM when this device is rebooted?

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

```
DLS1# show vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
200  enet  100200     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
```



```
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

DLS1#
```

2. How many of these VLANs are active by default on a 3560?

Issue the **show interface trunk** command on all switches in the lab. If trunking was configured properly in Labs 8.1 and 8.2, FastEthernet 0/7 – 0/12 should be in trunking mode on all switches.

```
DLS1# show int 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
DLS1#
```

3. What is the native VLAN for these trunk ports?

Use the **show standby brief** command on DLS2:

```
DLS2# show standby brief

Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl1         1   100  P Standby  172.16.1.3      local           172.16.1.1
Vl100       1   100  P Standby  172.16.100.3    local           172.16.100.1
Vl200       1   150  P Active   local           172.16.200.3    172.16.200.1
```

4. DLS2 is the active router for which VLANs?

Step 2

Within this server farm VLAN, all servers should be allowed access to the router or gateway but not be able to listen to each other's broadcast traffic. Private VLANs solve this problem. When you use a private VLAN, the primary VLAN (normal VLAN) can be logically associated with unidirectional, or secondary, VLANs. Servers or hosts on the secondary VLANs can communicate with the primary VLAN but not with another secondary VLAN. You can define the secondary VLANs as either isolated or community.

An isolated secondary VLAN can reach the primary VLAN, but not any other secondary VLAN. In addition, the host associated with the isolated port cannot communicate with any other device on the same isolated secondary VLAN. It is essentially isolated from everything except the primary VLAN.

A community VLAN cannot communicate with other secondary VLANs; however, it can communicate within the community. This lets you have workgroups within an organization while keeping them isolated from each other.

The first step is to configure the switches for the primary VLAN. Based on the topology diagram, VLAN 150 will be used for the new server farm.

On DLS1, add VLAN 150 to the configuration and name the VLAN.

```
DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#vlan 150
DLS1(config-vlan)#name server-farm
```



```
DLS1(config-vlan)#end
```

Add routing and HSRP information for the new VLAN on DLS1 and DLS2. Make DLS2 the primary router, and make DLS1 the standby router.

```
DLS1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#interface vlan 150
DLS1(config-if)#ip address 172.16.150.3 255.255.255.0
DLS1(config-if)#standby 1 ip 172.16.150.1
DLS1(config-if)#standby 1 priority 100
DLS1(config-if)#standby 1 preempt
DLS1(config-if)#end


DLS2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)#interface vlan 150
DLS2(config-if)#ip add 172.16.150.4 255.255.255.0
DLS2(config-if)#standby 1 ip 172.16.150.1
DLS2(config-if)#standby 1 priority 150
DLS2(config-if)#standby 1 preempt
DLS2(config-if)#end
DLS2#
```

Verify the HSRP configuration for VLAN 150 using the **show standby vlan 150 brief** command on DLS2.

```
DLS2# show standby vlan 150 brief

                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl150       1   150  P Active   local           172.16.150.3    172.16.150.1
```

The command output shows that DLS2 is the active router for the VLAN.

Now set up the primary and secondary VLAN information on DLS2. Because the new secondary VLANs are locally significant, configure DLS2 in transparent mode for VTP using the global configuration command **vtp mode transparent**.

```
DLS2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
DLS2(config)#end
```

Configure DLS2 to contain the new private VLANs. Secondary VLAN 151 is an isolated VLAN used for Fast Ethernet port 0/15, while secondary VLAN 152 is used as a community VLAN on Fast Ethernet ports 0/18 – 0/20. Configure these new VLANs in global configuration mode.

You also need to associate these secondary VLANs with primary VLAN 150.

```
DLS2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)#vlan 151
```



```
DLS2(config-vlan)#private-vlan isolated
DLS2(config-vlan)#exit
DLS2(config)#vlan 152
DLS2(config-vlan)#private-vlan community
DLS2(config-vlan)#exit
DLS2(config)#vlan 150
DLS2(config-vlan)#private-vlan primary
DLS2(config-vlan)#private-vlan association 151,152
DLS2(config-vlan)#exit
DLS2(config)#
```

Verify the creation of the secondary private VLANs and their association with the primary VLAN using the **show vlan private-vlan** command.

```
DLS2# show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------
150     151       isolated
150     152       community
```

5. Will hosts assigned to ports on private VLAN 151 be able to communicate directly with each other?

Next, configure the Fast Ethernet ports that are associated with the server farm private VLANs. Fast Ethernet port 0/15 is used for the secondary isolated VLAN 151, and ports 0/18 – 0/20 are used for the secondary community VLAN 152. Ports 0/16 and 0/17 are reserved for future use.

The **switchport private-vlan host-association** *primary-vlan-id secondary-vlan-id* command assigns the appropriate VLANs to the interface. The following is an example configuration on DLS2.

```
DLS2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)#interface fastethernet 0/15
DLS2(config-if)#switchport private-vlan host-association 150 151
DLS2(config-if)#exit
DLS2(config)#interface range fa0/18 - 20
DLS2(config-if-range)#switchport private-vlan host-association 150 152
DLS2(config-if-range)#end
```

6. As servers are added to Fast Ethernet 0/18 – 20, will these servers be allowed to hear broadcasts from each other?

Optional: If servers or hosts are available, connect them to the Fast Ethernet ports and try to ping between the new devices.

7. Which pings should succeed and which should fail?

Step 3

Configure an access control list to separate the student and staff VLANs. The staff VLAN can access the student VLAN, but the student VLAN does not have access to the staff VLAN for security purposes.

This can be achieved using a standard IP access list on DLS1 and DLS2, and assigning the access list to the appropriate VLAN interfaces. To deny the student subnet, use the **access-list** # **deny** *subnet-address wildcard-mask* command. Then assign the access list using the **access-group** # {**in** | **out**} command.

```
DLS1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#access-list 1 deny 172.16.200.0 0.0.0.255
DLS1(config)#interface vlan 100
DLS1(config-if)#ip access-group 1 out
DLS1(config-if)#end


DLS2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS2(config)#access-list 1 deny 172.16.200.0 0.0.0.255
DLS2(config)#interface vlan 100
DLS2(config-if)#ip access-group 1 out
DLS2(config-if)#end
DLS2#
```

Verify the configuration using the **show ip access-list** and **show ip interface vlan 100** commands:

```
DLS1# show ip access-lists
Standard IP access list 1
    10 deny   172.16.200.0, wildcard bits 0.0.0.255


DLS1# show ip int vlan 100
Vlan100 is up, line protocol is up
  Internet address is 172.16.100.3/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.2
  Outgoing access list is 1
  Inbound  access list is not set
```

After the access list has been applied, verify the configuration in one of the following ways:

Option1 – If available, set up hosts on the student and staff VLANs and ping the staff host from the student host. This ping should fail. Then ping the student host from the staff host. Does this ping succeed? Why?

Option 2 – Set up ALS1 as a host on VLAN 200 by creating a VLAN 200 interface on the switch. Give the interface an IP address in VLAN 200, and give it the default gateway of 172.16.200.1. Shut down the VLAN 1 interface. Now try to ping the interface of the gateway for the staff VLAN.

The following is a sample configuration and a sample ping from ALS1:

```
ALS1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#int vlan 1
ALS1(config-if)#shutdown
ALS1(config-if)#exit
ALS1(config)#int vlan 200
ALS1(config-if)#ip add 172.16.200.200 255.255
ALS1(config-if)#exit
ALS1(config)#ip default-gateway 172.16.200.1
ALS1(config)#end



ALS1#ping 172.16.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.100.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
ALS1#
```

8. What does a U signify in the output of the **ping** command?

Step 4

Configure the network so that the temporary staff host cannot access the rest of the staff VLAN, yet still be able to use the default gateway of the staff subnet to connect to the rest of the network and the Internet Service Provider (ISP). You can accomplish this task by using a VACL.

Because the temporary staff PC is located on DLS1's FastEthernet0/3, the VACL must be placed on DLS1.

First, configure an access list called temp-host on DLS1 using the **ip access-list extended** *name* command. This list is used to define the traffic between the host and the rest of the network. Then define the traffic using the **permit ip host** *ip-address subnet wildcard-mask* command.

```
DLS1#config t
```



```
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#ip access-list extended temp-host
DLS1(config-ext-nacl)#permit ip host 172.16.100.150 172.16.100.0 0.0.0.255
DLS1(config-ext-nacl)#exit
```

The VACL is defined using a VLAN access map. Access maps are evaluated in a numbered sequence. To set up an access-map, use the **vlan access-map** *map-name seq#* command.

The following configuration defines an access map named block-temp, which uses the **match** statement to match the traffic defined in the access list and denies that traffic. You also need to add a line to the access map that allows all other traffic. If this line is not added, an implicit deny catches all other traffic and denies it.

```
DLS1(config)#vlan access-map block-temp 10
DLS1(config-access-map)#match ip address temp-host
DLS1(config-access-map)#action drop
DLS1(config-access-map)#vlan access-map block-temp 20
DLS1(config-access-map)#action forward
DLS1(config-access-map)#exit
```

Define which VLANs the access map should be applied to using the **vlan filter** *map-name* **vlan-list** *vlan-ID* command.

```
DLS1(config)#vlan filter block-temp vlan-list 100
DLS1(config)#end
```

Verify the VACL configuration using the **show vlan access-map** command on DLS1.

```
DLS1# show vlan access-map
Vlan access-map "block-temp"  10
  Match clauses:
    ip  address: temp-host
  Action:
    drop
Vlan access-map "block-temp"  20
  Match clauses:
  Action:
    forward
```

Optional: If possible, connect a PC to the fa0/3 port of DLS1 and assign the host an IP address of 172.16.100.150/24. Try to ping to another staff host. The ping should not be successful.

Final Configurations

```
DLS1#show run
Building configuration...

Current configuration : 3462 bytes
!
!
hostname DLS1
!
enable secret cisco
```



```
!
!
ip routing
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
spanning-tree portfast default
spanning-tree vlan 1,100 priority 24576
spanning-tree vlan 200 priority 28672
!

!
vlan access-map block-temp 10
 action drop
 match ip address temp-host
vlan access-map block-temp 20
 action forward
vlan filter block-temp vlan-list 100
!

!
interface FastEthernet0/1
 udld port aggressive
!
interface FastEthernet0/2
 udld port aggressive
!
interface FastEthernet0/3
 udld port aggressive
!
interface FastEthernet0/4
 udld port aggressive
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
!
interface FastEthernet0/6
 switchport mode access
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/10
```



```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/13
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/14
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/15
 udld port aggressive
!
interface FastEthernet0/16
 udld port aggressive
!
interface FastEthernet0/17
 udld port aggressive
!
interface FastEthernet0/18
 udld port aggressive
!
interface FastEthernet0/19
 udld port aggressive
!
interface FastEthernet0/20
 udld port aggressive
!
interface FastEthernet0/21
 udld port aggressive
!
interface FastEthernet0/22
 udld port aggressive
!
interface FastEthernet0/23
 udld port aggressive
!
interface FastEthernet0/24
 udld port aggressive
!

!
interface Vlan1
 ip address 172.16.1.3 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
```



```
!
interface Vlan100
 ip address 172.16.100.3 255.255.255.0
 ip access-group 1 out
 standby 1 ip 172.16.100.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan150
 ip address 172.16.150.3 255.255.255.0
 standby 1 ip 172.16.150.1
 standby 1 preempt
 no shutdown
!
interface Vlan200
 ip address 172.16.200.3 255.255.255.0
 standby 1 ip 172.16.200.1
 standby 1 preempt
 no shutdown
!

!
ip access-list extended temp-host
 permit ip host 172.16.100.150 172.16.100.0 0.0.0.255
!
access-list 1 deny   172.16.200.0 0.0.0.255
!

!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

```
DLS2#show run
Building configuration...

Current configuration : 3520 bytes
!

!
hostname DLS2
!
enable secret cisco
!

!
vtp domain SWLAB
vtp mode transparent
udld enable
!
```



```
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!

!
spanning-tree vlan 1,100 priority 28672
spanning-tree vlan 200 priority 24576
!
vlan 100
 name staff
!
vlan 150
 name server-farm
  private-vlan primary
  private-vlan association 151-152
!
vlan 151
  private-vlan isolated
!
vlan 152
  private-vlan community
!
vlan 200
 name student
!
!
interface FastEthernet0/1
 udld port aggressive
!
interface FastEthernet0/2
 udld port aggressive
!
interface FastEthernet0/3
 udld port aggressive
!
interface FastEthernet0/4
 udld port aggressive
!
interface FastEthernet0/5
 udld port aggressive
!
interface FastEthernet0/6
 udld port aggressive
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
```



```
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/13
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/14
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/15
 switchport private-vlan host-association 150 151
 udld port aggressive
!
interface FastEthernet0/16
 udld port aggressive
!
interface FastEthernet0/17
 udld port aggressive
!
interface FastEthernet0/18
 switchport private-vlan host-association 150 152
 udld port aggressive
!
interface FastEthernet0/19
 switchport private-vlan host-association 150 152
 udld port aggressive
!
interface FastEthernet0/20
 switchport private-vlan host-association 150 152
 udld port aggressive
!
interface FastEthernet0/21
 udld port aggressive
!
interface FastEthernet0/22
 udld port aggressive
!
interface FastEthernet0/23
 udld port aggressive
!
interface FastEthernet0/24
 udld port aggressive
!

!
```



```
interface Vlan1
 ip address 172.16.1.4 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 preempt
 no shutdown
!
interface Vlan100
 ip address 172.16.100.4 255.255.255.0
 ip access-group 1 out
 standby 1 ip 172.16.100.1
 standby 1 preempt
 no shutdown
!
interface Vlan150
 ip address 172.16.150.4 255.255.255.0
 standby 1 ip 172.16.150.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!
interface Vlan200
 ip address 172.16.200.4 255.255.255.0
 standby 1 ip 172.16.200.1
 standby 1 priority 150
 standby 1 preempt
 no shutdown
!

!
access-list 1 deny   172.16.200.0 0.0.0.255
!

!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 loging
!
end
```

```
ALS1#show run
Building configuration...

Current configuration : 4747 bytes
!

!
hostname ALS1
!
enable secret cisco
!
username janedoe password 0 cisco
username johndoe password 0 cisco
username joesmith password 0 cisco
```



```
aaa new-model
aaa authentication dot1x default local
!
aaa session-id common
udld enable
!

!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!

spanning-tree portfast default
spanning-tree portfast bpduguard default
!

!

!
interface FastEthernet0/1
 udld port aggressive
!
interface FastEthernet0/2
 udld port aggressive
!
interface FastEthernet0/3
 udld port aggressive
!
interface FastEthernet0/4
 udld port aggressive
!
interface FastEthernet0/5
 udld port aggressive
!
interface FastEthernet0/6
 udld port aggressive
!
interface FastEthernet0/7
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/12
```



```
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/13
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/14
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/15
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/16
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/17
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/18
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/19
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/20
```



```
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/21
 switchport access vlan 100
 switchport trunk allowed vlan 10
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/22
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/23
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/24
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 udld port aggressive
 dot1x port-control auto
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
!
interface Vlan1
 ip address 172.16.1.101 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
radius-server source-ports 1645-1646
!
!
line con 0
 password cisco
line vty 0 4
 password cisco
```



```
line vty 5 15
 password cisco
!
end


ALS2#show run
Building configuration...

Current configuration : 3471 bytes
!
!
hostname ALS2
!
enable secret cisco
!
!
udld aggressive
!
!
ip dhcp snooping vlan 100,200
ip dhcp snooping
!
!
spanning-tree portfast default
spanning-tree portfast bpduguard default
!
!
interface FastEthernet0/1
 udld port aggressive
!
interface FastEthernet0/2
 udld port aggressive
!
interface FastEthernet0/3
 udld port aggressive
!
interface FastEthernet0/4
 udld port aggressive
!
interface FastEthernet0/5
 udld port aggressive
!
interface FastEthernet0/6
 udld port aggressive
!
interface FastEthernet0/7
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/8
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/9
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/10
 switchport mode trunk
```

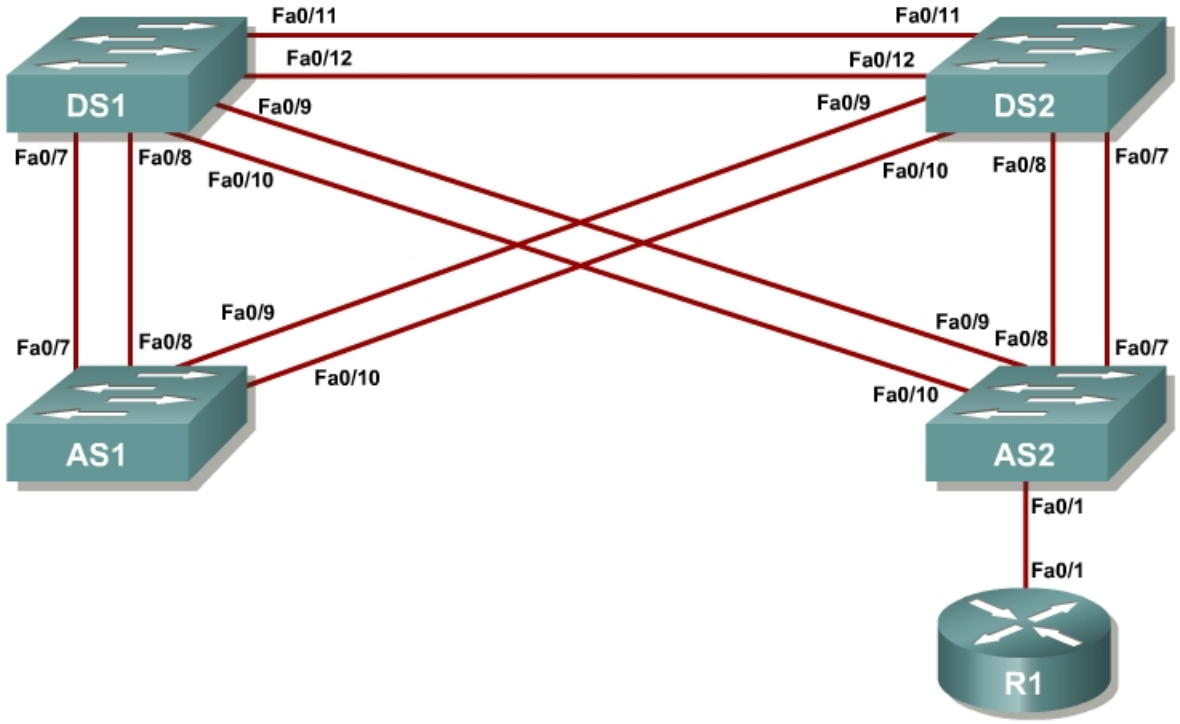


```
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/11
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/12
 switchport mode trunk
 udld port aggressive
 ip dhcp snooping trust
!
interface FastEthernet0/13
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/14
 udld port aggressive
 spanning-tree guard root
!
interface FastEthernet0/15
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/16
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/17
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/18
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/19
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/20
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
```



```
interface FastEthernet0/21
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/22
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/23
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet0/24
 switchport access vlan 200
 switchport mode access
 udld port aggressive
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
!
interface Vlan1
 ip address 172.16.1.102 255.255.255.0
 no shutdown
!
ip default-gateway 172.16.1.1
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```


Case Study 1 VLANs, VTP and Inter-VLAN Routing



VLAN	Name
10	Red
20	Blue
30	Orange
40	Green

Instructions

Plan, design, and implement the International Travel Agency switched network as shown in the diagram and described below. Implement the design on the lab set of switches. Verify that all configurations are operational and functioning according to the guidelines given.

Scenario

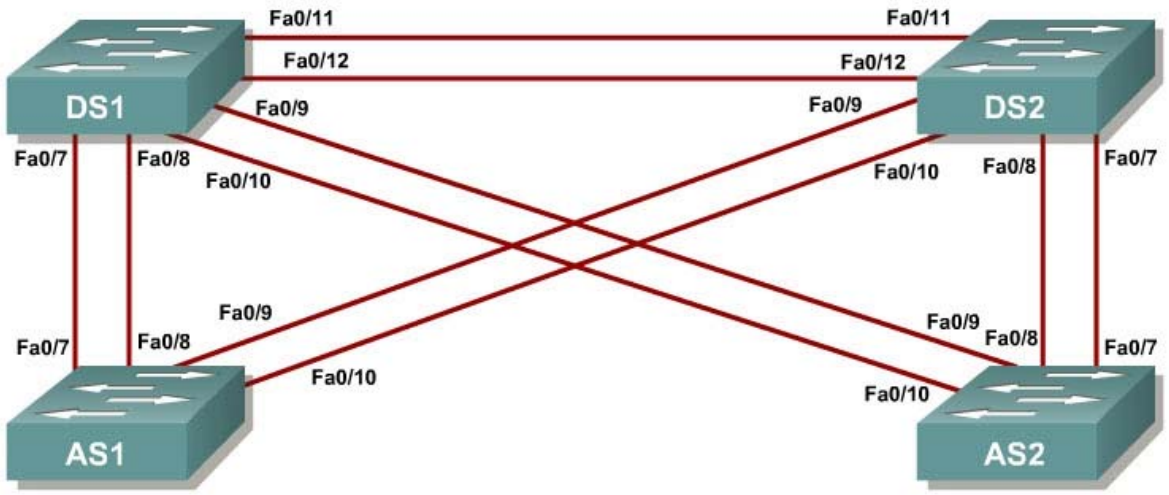
You will need to configure a group of switches for the International Travel Agency. It has two distribution switches, DLS1 and DLS2, and two access layer

switches, which are ALS1 and ALS2. You will have to design the addressing scheme to use here. The address space you can use is the 172.16.0.0/16 range. You may subnet it any way you want, although it is recommended for simplicity purposes to use /24 subnets.

- Disable the links between the access layer switches.
- Place all switches in the VTP domain CISCO. Make DLS1 the VTP server and all other switches VTP clients.
- Create the VLANs shown in the VLAN table and assign the names given. For subnet planning, allocate a subnet for each VLAN.
- Make DLS1 the primary spanning-tree root for all VLANs. Make DLS2 the backup root.
- Make F0/12 between DLS1 and DLS2 a layer 3 link and assign a subnet to it.
- Create a loopback interface on DLS1 and assign a subnet to it.
- Make F0/11 between DLS1 and DLS2 an ISL trunk link.
- Configure all other trunk links using 802.1q.
- Make sure that all inter-switch links are statically set as trunks.
- The links from DLS1 to each access switch must be bound together in an EtherChannel.
- Enable portfast on all access ports.
- Put F0/15 through F0/17 on ALS1 and ALS2 in VLAN 10. Place F0/18 and F0/19 on ALS1 and ALS2 in VLAN 20. Place F0/20 on ALS1 and ALS2 in VLAN 30.
- Create an 802.1q trunk link between R1 and ALS2. Allow only VLANs 10 and 40 to pass through the trunk.
- Give R1 subinterfaces in VLANs 10 and 40.
- Create an SVI interface on DLS1 in VLANs 20, 30 and 40. Create an SVI interface on DLS2 in VLAN 10, an SVI interface on ALS1 in VLAN 30, and an SVI interface on ALS2 in VLAN 40.
- Enable IP routing on DLS1. On R1 and DLS1, configure EIGRP for the whole major network (172.16.0.0/16) and disable automatic summarization.

Case Study 2 Voice and Security in a Switched Network

Topology Diagram



Instructions

Plan, design, and implement the International Travel Agency switched network as shown in the diagram and described below. Implement the design on the lab set of switches. Verify that all configurations are operational and functioning according to the guidelines.

Scenario

The International Travel Agency has two distribution switches, DLS1 and DLS2, and two access layer switches, ALS1 and ALS2. Configure a group of switches as follows:

- Disable the links between the access layer switches.
- Place all switches in the VTP domain CISCO and set them all to VTP mode transparent.
- Make sure that all inter-switch links are statically set as 802.1q links.
- Create VLANs 10 and 200 on all switches. Give DLS1 and DLS2 SVIs in VLAN 10 and assign addresses in the 172.16.10.0/24 subnet.
- Configure DLS1 and DLS2 to use HSRP on the 172.16.10.0/24 subnet. Make DLS1 the primary gateway, and enable preemption on both switches.
- Place ports Fa0/15 through Fa0/20 in VLAN 10 on both access layer switches.

- Enable PortFast on all access ports.
- Enable QoS on all switches involved in the scenario.
- Configure ALS1 F0/15 and F0/16 for using Cisco IP phones with a voice VLAN of 200 and trust the IP phone CoSes.
- Configure ALS1 F0/18 through F0/20 for port security. Allow only up to three MAC addresses to be learned on each port and then drop any traffic from other MAC addresses.
- Configure ALS2 F0/18 to only allow the MAC address 1234.1234.1234 and to shut down if a violation occurs.

