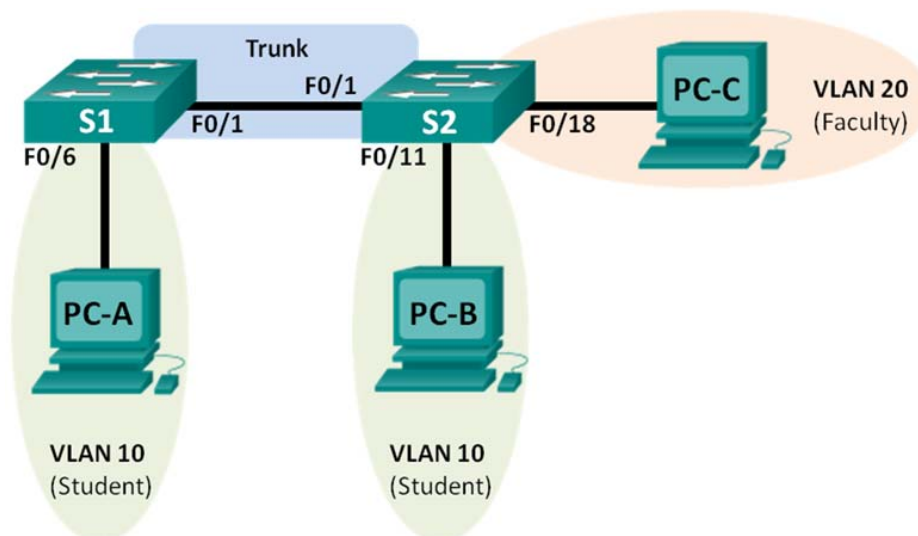


Lab 4 – Configuring VLANs and Trunking

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.1.11	255.255.255.0	N/A
S2	VLAN 99	192.168.1.12	255.255.255.0	N/A
PC-A	NIC (P-to-p)	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC (P-to-p)	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC (P-to-p)	192.168.20.3	255.255.255.0	192.168.20.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Maintain VLAN Port Assignments and the VLAN Database

Part 4: Configure an 802.1Q Trunk between the Switches

Part 5: Delete the VLAN Database

Background / Scenario

Modern switches use virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones. VLANs can also be used as a security measure by controlling which hosts can communicate. In general, VLANs make it easier to design a network to support the goals of an organization.

VLAN trunks are used to span VLANs across multiple devices. Trunks allow the traffic from multiple VLANs to travel over a single link, while keeping the VLAN identification and segmentation intact.

In this lab, you will create VLANs on both switches in the topology, assign VLANs to switch access ports, verify that VLANs are working as expected, and then create a VLAN trunk between the two switches to allow hosts in the same VLAN to communicate through the trunk, regardless of which switch the host is actually attached to.

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and switches.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Initialize and reload the switches as necessary.

Step 3: Configure basic settings for each switch.

1. Disable DNS lookup.
2. Configure device name as shown in the topology.
3. Assign **class** as the privileged EXEC password.
4. Assign **cisco** as the console and vty passwords and enable login for console and vty lines.
5. Configure **logging synchronous** for the console line.
6. Configure a MOTD banner to warn users that unauthorized access is prohibited.
7. Configure the IP address listed in the Addressing Table for VLAN 99 on both switches.
8. Administratively deactivate all unused ports on the switch.
9. Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 5: Test connectivity.

Verify that the PC hosts can ping one another.

Note: It may be necessary to disable the PCs firewall to ping between PCs.

Can PC-A ping PC-B? Why or why not?

Can PC-A ping PC-C? Why or why not?

Can PC-A ping S1? Why or why not?

Can PC-B ping PC-C? Why or why not?

Can PC-B ping S2? Why or why not?

Can PC-C ping S2? Why or why not?

Can S1 ping S2? Why or why not?

Part 2: Create VLANs and Assign Switch Ports

In Part 2, you will create Student, Faculty, Guest and management VLANs on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan** command is used to verify your configuration settings.

Step 1: Create VLANs on the switches.

1. Create the VLANs on S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
```

Lab 4 – Configuring VLANs and Trunking

```
S1(config-vlan)# name Management
S1(config-vlan)# end
```

2. Create the same VLANs on S2.
3. Issue the **show vlan** command to view the list of VLANs on S1.

```
S1# 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	Student	active
20	Faculty	active
99	Management	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
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
99	enet	100099	1500	-	-	-	-	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
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
---------	-----------	------	-------

What is the default VLAN? What does default VLAN mean?

What ports are assigned to the default VLAN?

Step 2: Assign VLANs to the correct switch interfaces.

1. Assign VLANs to the interfaces on S1.
 - Assign PC-A to the Student VLAN.

Lab 4 – Configuring VLANs and Trunking

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

- Move the switch IP address to interface VLAN 99.

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end
```

2. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

```
S1# show vlan brief
```

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
10	Student	active	Fa0/6
20	Faculty	active	
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

3. Issue the **show ip interfaces brief** command.

What is the status and protocol of VLAN 99? Why?

4. Use the Topology to assign VLANs to the appropriate ports on S2.
5. Remove the IP address for interface VLAN1 on S2.
6. Configure an IP address for interface VLAN99 on S2 according to the Addressing Table.
7. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

```
S2# show vlan brief
```

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, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/11
20	Faculty	active	Fa0/18

Lab 4 – Configuring VLANs and Trunking

```
99   Management          active
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

Is PC-A able to ping PC-B? Why or why not?

.....

Is S1 able to ping S2? Why or why not?

.....

.....

Part 3: Maintain VLAN Port Assignments and the VLAN Database

In Part 3, you will change VLAN assignments to ports and remove VLANs from the VLAN database.

Step 1: Assign a VLAN to multiple interfaces.

1. On S1, assign interfaces F0/11 – 24 to VLAN 10.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```
2. Reassign F0/11 and F0/21 to VLAN 20.
3. Issue the **show vlan brief** command to verify that VLAN assignments are correct.

Step 2: Remove a VLAN assignment from an interface.

1. Use the **no switchport access vlan** command to remove the VLAN 10 assignment to F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```
2. Verify that the VLAN change was made.
Which VLAN is F0/24 is now associated with? Why?

Step 3: Remove a VLAN ID from the VLAN database.

1. Add VLAN 30 to interface F0/24 without issuing the VLAN command.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Note: Current switch technology no longer requires that the **vlan** command be issued to add a VLAN to the database. By assigning an unknown VLAN to a port, the VLAN adds to the VLAN database.

2. Verify that the new VLAN is displayed in the VLAN table.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8

Lab 4 – Configuring VLANs and Trunking

10	Student	active	Fa0/9, Fa0/10, Gi0/1, Gi0/2 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
30	VLAN0030	active	Fa0/24
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

What is the default name of VLAN 30? _____

3. Use the **no vlan 30** command to remove VLAN 30 from the VLAN database.

```
S1(config)# no vlan 30
```

```
S1(config)# end
```

4. Issue the **show vlan brief** command. F0/24 was assigned to VLAN 30.

After deleting VLAN 30, what VLAN is port F0/24 assigned to?

What happens to the traffic destined to the host attached to F0/24?

```
S1# show vlan brief
```

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, Gi0/1, Gi0/2
10	Student	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

5. Issue the **no switchport access vlan** command on interface F0/24.

6. Issue the **show vlan brief** command to determine the VLAN assignment for F0/24.

To which VLAN is F0/24 assigned? Why?

Note: Before removing a VLAN from the database, it is recommended that you reassign all the ports assigned to that VLAN.

Why should you reassign a port to another VLAN before removing the VLAN from the VLAN database?

Part 4: Configure an 802.1Q Trunk Between the Switches

In Part 4, you will configure interface F0/1 to use the Cisco Dynamic Trunking Protocol (DTP) to allow it to negotiate the trunk mode. After this has been accomplished and verified, you will disable DTP on interface F0/1 and manually configure it as a trunk.

Step 1: Use DTP to initiate trunking on F0/1.

The default DTP mode of a 2960 switch port is dynamic **auto**. This allows the interface to convert the link to a trunk if the neighboring interface is set to trunk or dynamic **desirable** mode.

1. Set F0/1 on S1 to negotiate trunk mode.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar 1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to down
*Mar 1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
S1(config-if)#
*Mar 1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
S1(config-if)#
*Mar 1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99,
changed state to up
*Mar 1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
```

You should also receive link status messages on S2.

```
S2#
*Mar 1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
S2#
*Mar 1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
S2#
*Mar 1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99,
changed state to up
*Mar 1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
```

2. Issue the **show vlan brief** command on S1 and S2. Interface F0/1 is no longer assigned to VLAN1. Trunked interfaces are not listed in the VLAN table.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/6, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Lab 4 – Configuring VLANs and Trunking

3. Issue the **show interfaces trunk** command to view trunked interfaces. Notice that the mode on S1 is set to **desirable** and the mode on S2 is set by default to **auto**.

S1# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,99

S2# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	auto	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,99

Note: By default, all VLANs are allowed on a trunk. The **switchport trunk** command allows you to control what VLANs have access to the trunk. For this lab, keep the default settings, which allow all VLANs to traverse F0/1.

4. Verify that VLAN traffic is traveling over trunk interface F0/1.

Can PC-A ping PC-B? Why or why not?

Can PC-A ping PC-C? Why or why not?

Can PC-C ping S2? Why or why not?

Can S1 ping S2? Why or why not?

Step 2: Manually configure trunk interface F0/1.

The **switchport mode trunk** command is used to manually configure a port as a trunk. This command should be issued on both ends of the link.

1. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

S1(config)# **interface f0/1**

S1(config-if)# **switchport mode trunk**

2. Issue the **show interfaces trunk** command to view the trunk mode. Notice that the mode changed from **desirable** to **on**.

S2# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
------	------	---------------	--------	-------------

Lab 4 – Configuring VLANs and Trunking

```
Fa0/1      on          802.1q      trunking      1

Port       Vlans allowed on trunk
Fa0/1      1-4094

Port       Vlans allowed and active in management domain
Fa0/1      1,10,20,99

Port       Vlans in spanning tree forwarding state and not pruned
Fa0/1      1,10,20,99
```

Why might you want to manually configure an interface to trunk mode instead of using DTP?

.....

.....

Part 5: Delete the VLAN Database

In Part 5, you will delete the VLAN Database from the switch. It is necessary to do this when initializing a switch back to its default settings.

Step 1: Determine if the VLAN database exists.

Issue the **show flash** command to determine if a **vlan.dat** file exists in flash.

```
S1# show flash
```

```
Directory of flash:/
```

```
 2  -rwx      1285   Mar 1 1993 00:01:24 +00:00  config.text
 3  -rwx     43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
 4  -rwx         5   Mar 1 1993 00:01:24 +00:00  private-config.text
 5  -rwx    11607161 Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-
2.SE.bin
 6  -rwx       736   Mar 1 1993 00:19:41 +00:00  vlan.dat
```

```
32514048 bytes total (20858880 bytes free)
```

Note: If there is a **vlan.dat** file located in flash, then the VLAN database does not contain its default settings.

Step 2: Delete the VLAN database.

1. Issue the **delete vlan.dat** command to delete the **vlan.dat** file from flash and reset the VLAN database back to its default settings. You will be prompted twice to confirm that you want to delete the **vlan.dat** file. Press Enter both times.

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#
```

2. Issue the **show flash** command to verify that the **vlan.dat** file has been deleted.

```
S1# show flash
```

```
Directory of flash:/
```

```
 2  -rwx      1285   Mar 1 1993 00:01:24 +00:00  config.text
 3  -rwx     43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
```

Lab 4 – Configuring VLANs and Trunking

```
4  -rwx          5  Mar 1 1993 00:01:24 +00:00 private-config.text
5  -rwx    11607161  Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-
2.SE.bin
```

32514048 bytes total (20859904 bytes free)

To initialize a switch back to its default settings, what other commands are needed?

.....
.....

Reflection

1. What is needed to allow hosts on VLAN 10 to communicate to hosts on VLAN 20?

.....
.....

2. What are some primary benefits that an organization can receive through effective use of VLANs?

.....
.....