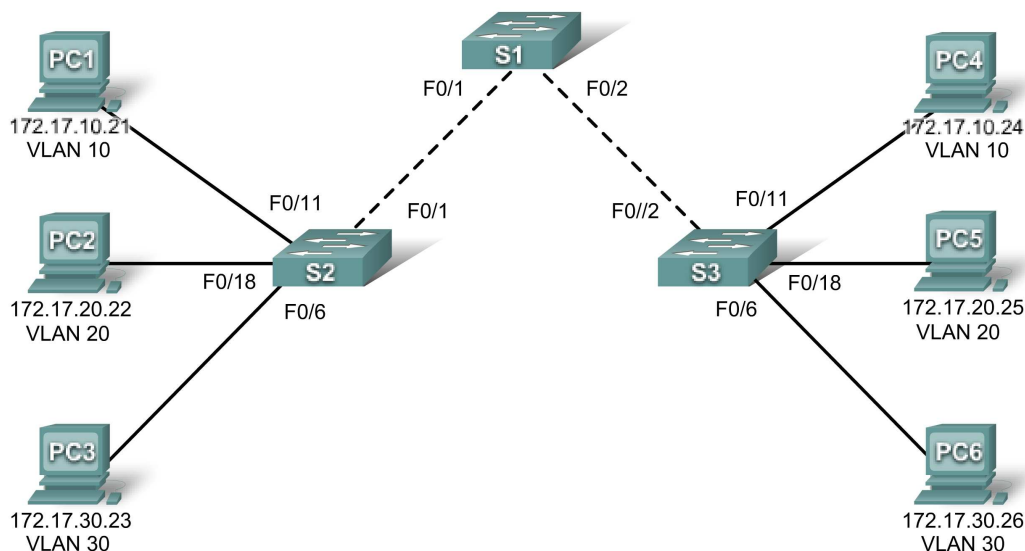


Lab 3.5.1: Basic VLAN Configuration (Instructor Version)

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a switch to the default state
- Perform basic configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 2900 or 2950 switches, the outputs may appear different. Also, certain commands may be different or unavailable.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

If necessary, refer to Lab 2.5.1, Appendix 1, for the procedure to clear switch configurations.

It is a good practice to disable any unused ports on the switches by putting them in shutdown. Disable all ports on the switches:

```
Switch#config term
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Task 2: Perform Basic Switch Configurations

Step 1: Configure the switches according to the following guidelines.

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2: Re-enable the user ports on S2 and S3.

```
S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
```

```
S2(config-if-range)#no shutdown

S3(config)#interface range fa0/6, fa0/11, fa0/18
S3(config-if-range)#switchport mode access
S3(config-if-range)#no shutdown
```

Task 3: Configure and Activate Ethernet Interfaces

Step 1: Configure the PCs.

You can complete this lab using only two PCs by simply changing the IP addressing for the two PCs specific to a test you want to conduct. For example, if you want to test connectivity between PC1 and PC2, then configure the IP addresses for those PCs by referring to the addressing table at the beginning of the lab. Alternatively, you can configure all six PCs with the IP addresses and default gateways.

Task 4: Configure VLANs on the Switch

Step 1: Create VLANs on switch S1.

Use the `vlan vlan-id` command in global configuration mode to add a VLAN to switch S1. There are four VLANs configured for this lab: VLAN 10 (faculty/staff); VLAN 20 (students); VLAN 30 (guest); and VLAN 99 (management). After you create the VLAN, you will be in `vlan` configuration mode, where you can assign a name to the VLAN with the `name vlan name` command.

```
S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#end
S1#
```

Step 2: Verify that the VLANs have been created on S1.

Use the `show vlan brief` command to verify that the VLANs have been created.

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, 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	faculty/staff	active	
20	students	active	
30	guest	active	
99	management	active	

Step 3: Configure and name VLANs on switches S2 and S3.

Create and name VLANs 10, 20, 30, and 99 on S2 and S3 using the commands from Step 1. Verify the correct configuration with the **show vlan brief** command.

What ports are currently assigned to the four VLANs you have created?

_____ none

Step 4: Assign switch ports to VLANs on S2 and S3.

Refer to the port assignment table on page 1. Ports are assigned to VLANs in interface configuration mode, using the **switchport access vlan** *vlan-id* command. You can assign each port individually or you can use the **interface range** command to simplify this task, as shown here. The commands are shown for S3 only, but you should configure both S2 and S3 similarly. Save your configuration when done.

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Step 5: Determine which ports have been added.

Use the **show vlan id** *vlan-number* command on S2 to see which ports are assigned to VLAN 10.

Which ports are assigned to VLAN 10?

_____ Fa0/11, Fa0/12, Fa0/13, Fa0/14,
Fa0/15, Fa0/16, Fa0/17

Note: The **show vlan name** *vlan-name* displays the same output.

You can also view VLAN assignment information using the **show interfaces** *interface* **switchport** command.

Step 6: Assign the management VLAN.

A management VLAN is any VLAN that you configure to access the management capabilities of a switch. VLAN 1 serves as the management VLAN if you did not specifically define another VLAN. You assign the management VLAN an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 is a bad choice as the management VLAN. You do not want an arbitrary user who is connecting to a switch to default to the management VLAN. Recall that you configured the management VLAN as VLAN 99 earlier in this lab.

From interface configuration mode, use the **ip address** command to assign the management IP address to the switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 99
```

```
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Assigning a management address allows IP communication between the switches, and also allows any host connected to a port assigned to VLAN 99 to connect to the switches. Because VLAN 99 is configured as the management VLAN, any ports assigned to this VLAN are considered management ports and should be secured to control which devices can connect to these ports.

Step 7: Configure trunking and the native VLAN for the trunking ports on all switches.

Trunks are connections between the switches that allow the switches to exchange information for all VLANs. By default, a trunk port belongs to all VLANs, as opposed to an access port, which can only belong to a single VLAN. If the switch supports both ISL and 802.1Q VLAN encapsulation, the trunks must specify which method is being used. Because the 2960 switch only supports 802.1Q trunking, it is not specified in this lab.

A native VLAN is assigned to an 802.1Q trunk port. In the topology, the native VLAN is VLAN 99. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. One of the IEEE 802.1Q specifications for Native VLANs is to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For the purposes of this lab, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

Use the **interface range** command in global configuration mode to simplify configuring trunking.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Verify that the trunks have been configured with the **show interface trunk** command.

```
S1#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99
Fa0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	1-4094
Fa0/2	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,30,99
Fa0/2	1,10,20,30,99

```
Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         1,10,20,30,99
Fa0/2         1,10,20,30,99
```

Step 8: Verify that the switches can communicate.

From S1, ping the management address on both S2 and S3.

```
S1#ping 172.17.99.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

S1#ping 172.17.99.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Step 9: Ping several hosts from PC2.

Ping from host PC2 to host PC1 (172.17.10.21). Is the ping attempt successful? _____ no

Ping from host PC2 to the switch VLAN 99 IP address 172.17.99.12. Is the ping attempt successful?
_____ no

Because these hosts are on different subnets and in different VLANs, they cannot communicate without a Layer 3 device to route between the separate subnetworks.

Ping from host PC2 to host PC5. Is the ping attempt successful? _____ yes

Because PC2 is in the same VLAN and the same subnet as PC5, the ping is successful

Step 10: Move PC1 into the same VLAN as PC2.

The port connected to PC2 (S2 Fa0/18) is assigned to VLAN 20, and the port connected to PC1 (S2 Fa0/11) is assigned to VLAN 10. Reassign the S2 Fa0/11 port to VLAN 20. You do not need to first remove a port from a VLAN to change its VLAN membership. After you reassign a port to a new VLAN, that port is automatically removed from its previous VLAN.

```
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface fastethernet 0/11
S2(config-if)#switchport access vlan 20
S2(config-if)#end
```

Ping from host PC2 to host PC1. Is the ping attempt successful? _____ no

Even though the ports used by PC1 and PC2 are in the same VLAN, they are still in different subnetworks, so they cannot communicate directly.

Step 11: Change the IP address and network on PC1.

Change the IP address on PC1 to 172.17.20.22. The subnet mask and default gateway can remain the same. Once again, ping from host PC2 to host PC1, using the newly assigned IP address.

Is the ping attempt successful? _____ yes

Why was this attempt successful?

Hosts must be in the same VLAN and in the same subnet to communicate directly through the switches.

Task 5: Document the Switch Configurations

On each switch, capture the running configuration to a text file and save it for future reference.

Task 6: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Final Switch Configurations

S1

```
hostname S1
!
enable secret class
no ip domain-lookup
!
interface FastEthernet0/1
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/2
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/5
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/6
  shutdown
!
<all remaining FastEthernet and GigabitEthernet interface are shutdown>
!
interface Vlan1
  no ip address
  no ip route-cache
!
interface Vlan99
  ip address 172.17.99.11 255.255.255.0
  no ip route-cache
```

```
!  
line con 0  
  exec-timeout 0 0  
  password cisco  
  logging synchronous  
  login  
line vty 0 4  
  exec-timeout 0 0  
  password cisco  
  logging synchronous  
  login  
line vty 5 15  
  exec-timeout 0 0  
  password cisco  
  logging synchronous  
  login  
!  
end
```

S2

```
hostname S2  
!  
enable secret class  
no ip domain-lookup  
!  
interface FastEthernet0/1  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/2  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/3  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/4  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/5  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/6  
  switchport access vlan 30  
  switchport mode access  
!  
interface FastEthernet0/7  
  switchport access vlan 30  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/8
```



```
    switchport access vlan 30
    switchport mode access
    shutdown
!
interface FastEthernet0/9
    switchport access vlan 30
    switchport mode access
    shutdown
!
interface FastEthernet0/10
    switchport access vlan 30
    switchport mode access
    shutdown
!
interface FastEthernet0/11
    switchport access vlan 20
    switchport mode access
!
interface FastEthernet0/12
    switchport access vlan 10
    switchport mode access
    shutdown
!
interface FastEthernet0/13
    switchport access vlan 10
    switchport mode access
    shutdown
!
interface FastEthernet0/14
    switchport access vlan 10
    switchport mode access
    shutdown
!
interface FastEthernet0/15
    switchport access vlan 10
    switchport mode access
    shutdown
!
interface FastEthernet0/16
    switchport access vlan 10
    switchport mode access
    shutdown
!
interface FastEthernet0/17
    switchport access vlan 10
    switchport mode access
    shutdown
!
interface FastEthernet0/18
    switchport access vlan 20
    switchport mode access
!
interface FastEthernet0/19
    switchport access vlan 20
    switchport mode access
    shutdown
```

```
!  
interface FastEthernet0/20  
  switchport access vlan 20  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/21  
  switchport access vlan 20  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/22  
  switchport access vlan 20  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/23  
  switchport access vlan 20  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/24  
  switchport access vlan 20  
  switchport mode access  
  shutdown  
!  
interface GigabitEthernet0/1  
  shutdown  
!  
interface GigabitEthernet0/2  
  shutdown  
!  
interface Vlan1  
  no ip address  
  no ip route-cache  
  shutdown  
!  
interface Vlan99  
  ip address 172.17.99.12 255.255.255.0  
  no ip route-cache  
!  
ip http server  
!  
control-plane  
!  
!  
line con 0  
  exec-timeout 0 0  
  password cisco  
  logging synchronous  
  login  
line vty 0 4  
  exec-timeout 0 0  
  password cisco  
  logging synchronous  
  login
```

```
line vty 5 15
  exec-timeout 0 0
  password cisco
  logging synchronous
  login
!
!
end
```

S3

```
hostname S3
no ip domain-lookup
enable secret class
!
interface FastEthernet0/1
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/2
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/5
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/6
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/7
  switchport access vlan 30
!
interface FastEthernet0/8
  switchport access vlan 30
!
interface FastEthernet0/9
  switchport access vlan 30
!
interface FastEthernet0/10
  switchport access vlan 30
!
interface FastEthernet0/11
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/12
```

```
    switchport access vlan 10
!
interface FastEthernet0/13
    switchport access vlan 10
!
interface FastEthernet0/14
    switchport access vlan 10
!
interface FastEthernet0/15
    switchport access vlan 10
!
interface FastEthernet0/16
    switchport access vlan 10
!
interface FastEthernet0/17
    switchport access vlan 10
!
interface FastEthernet0/18
    switchport access vlan 20
    switchport mode access
!
interface FastEthernet0/19
    switchport access vlan 20
!
interface FastEthernet0/20
    switchport access vlan 20
!
interface FastEthernet0/21
    switchport access vlan 20
!
interface FastEthernet0/22
    switchport access vlan 20
!
interface FastEthernet0/23
    switchport access vlan 20
!
interface FastEthernet0/24
    switchport access vlan 20
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
    no ip address
    no ip route-cache
    shutdown
!
interface Vlan99
    ip address 172.17.99.13 255.255.255.0
    no ip route-cache
!
line con 0
    password cisco
    login
line vty 0 4
```

```
password cisco
login
line vty 5 15
password cisco
login
!
end
```