Chapter 3 — VLANs

3.0.1.2 Class Activity – Vacation Station

Objective
Explain the purpose of VLANs in a switched network.

Scenario
You have purchased a three floor vacation home at the beach for rental purposes. The floor plan is identical on each floor. Each floor offers one digital television for renters to use.

According to the local Internet service provider, only three stations may be offered within a television package. It is your job to decide which television packages you offer your guests.

- Divide the class into groups of three students per group.
- Choose three different stations to make one subscription package for each floor of your rental home.
- Complete the PDF for this activity.

Share your completed group-reflection answers with the class.

<table>
<thead>
<tr>
<th>Television Station Subscription Package – Floor 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local News</td>
</tr>
<tr>
<td>☐</td>
</tr>
<tr>
<td>Home Improvement</td>
</tr>
<tr>
<td>☐</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Television Station Subscription Package – Floor 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local News</td>
</tr>
<tr>
<td>☐</td>
</tr>
<tr>
<td>Home Improvement</td>
</tr>
<tr>
<td>☐</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Television Station Subscription Package – Floor 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local News</td>
</tr>
<tr>
<td>☐</td>
</tr>
<tr>
<td>Home Improvement</td>
</tr>
<tr>
<td>☐</td>
</tr>
</tbody>
</table>
Reflection

1. What were some of the criteria you used to select the final three stations?

2. Why do you think this Internet service provider offers different television station options to subscribers? Why not offer all stations to all subscribers?

3. Compare this scenario to data communications and networks for small- to medium-sized businesses. Why would it be a good idea to divide your small- to medium-sized business networks into logical and physical groups?
3.2.2.5 Lab - Configuring VLANs and Trunking

Topology

![Topology Diagram]

Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>VLAN 1</td>
<td>192.168.1.11</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>S2</td>
<td>VLAN 1</td>
<td>192.168.1.12</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>PC-A</td>
<td>NIC</td>
<td>192.168.10.3</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>PC-B</td>
<td>NIC</td>
<td>192.168.10.4</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>PC-C</td>
<td>NIC</td>
<td>192.168.20.3</td>
<td>255.255.255.0</td>
<td>192.168.20.1</td>
</tr>
</tbody>
</table>

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.

**Note:** The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

**Note:** Ensure that the switches have been erased and have no startup configurations. If you are unsure contact your instructor.

**Required Resources**

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

**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.**

  a. Disable DNS lookup.
  b. Configure device name as shown in the topology.
  c. Assign **class** as the privileged EXEC password.
  d. Assign **cisco** as the console and vty passwords and enable login for console and vty lines.
  e. Configure **logging synchronous** for the console line.
  f. Configure a MOTD banner to warn users that unauthorized access is prohibited.
  g. Configure the IP address listed in the Addressing Table for VLAN 1 on both switches.
  h. Administratively deactivate all unused ports on the switch.
  i. 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? 
Can PC-A ping PC-C? 
Can PC-A ping S1? 
Can PC-B ping PC-C? 
Can PC-B ping S2? 
Can PC-C ping S2? 
Can S1 ping S2? 

If you answered no to any of the above questions, why were the pings unsuccessful?

Part 2: Create VLANs and Assign Switch Ports

In Part 2, you will create student, faculty, 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.

a. 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
   S1(config-vlan)# name Management
   S1(config-vlan)# end

b. Create the same VLANs on S2.

c. Issue the show vlan command to view the list of VLANs on S1.
   S1# show vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fa0/5, Fa0/6, Fa0/7, Fa0/8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fa0/9, Fa0/10, Fa0/11, Fa0/12</td>
</tr>
</tbody>
</table>
Step 2: Assign VLANs to the correct switch interfaces.

a. Assign VLANs to the interfaces on S1.

1) Assign PC-A to the Student VLAN.

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

2) Move the switch IP address VLAN 99.

   S1(config)# interface vlan 1
   S1(config-if)# no ip address
   S1(config-if)# interface vlan 99
b. Issue the `show vlan brief` command and verify that the VLANs are assigned to the correct interfaces.

````
S1# show vlan brief

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

c. Issue the `show ip interface brief` command.

What is the status of VLAN 99? Why?

d. Use the Topology to assign VLANs to the appropriate ports on S2.

e. Remove the IP address for VLAN 1 on S2.

f. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.

g. Use the `show vlan brief` command to verify that the VLANs are assigned to the correct interfaces.

````
S2# show vlan brief

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

Is PC-A able to ping PC-B? Why?

Is S1 able to ping S2? Why?

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.
   a. 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
      ```
   b. Issue the `show vlan brief` command to verify VLAN assignments.
   c. Reassign F0/11 and F0/21 to VLAN 20.
   d. Verify that VLAN assignments are correct.

Step 2: Remove a VLAN assignment from an interface.
   a. 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
      ```
   b. Verify that the VLAN change was made.
      Which VLAN is F0/24 now associated with?

Step 3: Remove a VLAN ID from the VLAN database.
   a. 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.
   b. Verify that the new VLAN is displayed in the VLAN table.
      ```
      S1# show vlan brief
      ```
<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Gi0/1, Gi0/2</td>
</tr>
<tr>
<td>10</td>
<td>active</td>
<td>Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/22, Fa0/23</td>
</tr>
<tr>
<td>20</td>
<td>active</td>
<td>Fa0/11, Fa0/21</td>
</tr>
<tr>
<td>99</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>

What is the default name of VLAN 30?

c. Use the `no vlan 30` command to remove VLAN 30 from the VLAN database.

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

d. 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
```

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Gi0/1, Gi0/2</td>
</tr>
<tr>
<td>10</td>
<td>active</td>
<td>Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/22, Fa0/23</td>
</tr>
<tr>
<td>20</td>
<td>active</td>
<td>Fa0/11, Fa0/21</td>
</tr>
<tr>
<td>99</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>
e. Issue the `no switchport access vlan` command on interface F0/24.

f. Issue the `show vlan brief` command to determine the VLAN assignment for F0/24. To which VLAN is F0/24 assigned?

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 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.

a. 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
```

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

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

c. 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 to auto.

S1# show interfaces trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>desirable</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>auto</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

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 allows all VLANs to traverse F0/1.
d. Verify that VLAN traffic is traveling over trunk interface F0/1.
   Can S1 ping S2?  
   Can PC-A ping PC-B?  
   Can PC-A ping PC-C?  
   Can PC-B ping PC-C?  
   Can PC-A ping S1?  
   Can PC-B ping S2?  
   Can PC-C ping S2?  
   If you answered no to any of the above questions, explain below.

---

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.

a. 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

b. Issue the show interfaces trunk command to view the trunk mode. Notice that the mode changed from desirable to on.
   S2# show interfaces trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>99</td>
</tr>
</tbody>
</table>

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.

```
Sl# 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.

a. 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.

```
Sl# delete vlan.dat
Delete filename [vlan.dat]? [confirm]
Sl#
```

b. Issue the `show flash` command to verify that the vlan.dat file has been deleted.

```
Sl# 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
```

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?
3.2.4.9 Lab - Troubleshooting VLAN Configurations

Topology

Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>VLAN 1</td>
<td>192.168.1.2</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>S2</td>
<td>VLAN 1</td>
<td>192.168.1.3</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>PC-A</td>
<td>NIC</td>
<td>192.168.10.2</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>PC-B</td>
<td>NIC</td>
<td>192.168.10.3</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>PC-C</td>
<td>NIC</td>
<td>192.168.20.3</td>
<td>255.255.255.0</td>
<td>192.168.20.1</td>
</tr>
</tbody>
</table>

Switch Port Assignment Specifications

<table>
<thead>
<tr>
<th>Ports</th>
<th>Assignment</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>F0/1</td>
<td>802.1Q Trunk</td>
<td>N/A</td>
</tr>
<tr>
<td>F0/6-12</td>
<td>VLAN 10 – Students</td>
<td>192.168.10.0/24</td>
</tr>
<tr>
<td>F0/13-18</td>
<td>VLAN 20 – Faculty</td>
<td>192.168.20.0/24</td>
</tr>
<tr>
<td>F0/19-24</td>
<td>VLAN 30 – Guest</td>
<td>192.168.30.0/24</td>
</tr>
</tbody>
</table>

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot VLAN 10

Part 3: Troubleshoot VLAN 20
Background / Scenario

VLANs provide logical segmentation within an internetwork and improve network performance by separating large broadcast domains into smaller ones. By separating hosts into different networks, VLANs can be used to control which hosts can communicate. In this lab, a school has decided to implement VLANs in order to separate traffic from different end users. The school is using 802.1Q trunking to facilitate VLAN communication between switches.

The S1 and S2 switches have been configured with VLAN and trunking information. Several errors in the configuration have resulted in connectivity issues. You have been asked to troubleshoot and correct the configuration errors and document your work.

Note: The switches used with this lab are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the switches with some basic settings, such as passwords and IP addresses. Preset VLAN-related configurations, which contain errors, are provided for you for the initial switch configurations. You will also configure the IP settings for the PCs in the topology.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the switches as necessary.

Step 4: Configure basic settings for each switch.
   a. Disable DNS lookup.
   b. Configure the IP address according to the Addressing Table.
   c. Assign cisco as the console and vty passwords and enable login for console and vty lines.
   d. Assign class as the privileged EXEC password.
   e. Configure logging synchronous to prevent console messages from interrupting command entry.

Step 5: Load switch configurations.

The configurations for the switches S1 and S2 are provided for you. There are errors within these configurations, and it is your job to determine the incorrect configurations and correct them.

Switch S1 Configuration:

```
hostname S1
vlan 10
name Students
```
vlan 2
  name Faculty
vlan 30
  name Guest
interface range f0/1-24
  switchport mode access
  shutdown

interface range f0/7-12
  switchport access vlan 10
interface range f0/13-18
  switchport access vlan 2

interface range f0/19-24
  switchport access vlan 30
end

Switch S2 Configuration:
  hostname S2
  vlan 10
    name Students
  vlan 20
    name Faculty
  vlan 30
    name Guest
  interface f0/1
    switchport mode trunk
    switchport trunk allowed vlan 1,10,2,30

interface range f0/2-24
  switchport mode access
  shutdown

interface range f0/13-18
  switchport access vlan 20
interface range f0/19-24
  switchport access vlan 30
  shutdown
end

Step 6: Copy the running configuration to the startup configuration.
Part 2: Troubleshoot VLAN 10

In Part 2, you must examine VLAN 10 on S1 and S2 to determine if it is configured correctly. You will troubleshoot the scenario until connectivity is established.

Step 1: Troubleshoot VLAN 10 on S1.

a. Can PC-A ping PC-B? ______________

b. After verifying that PC-A was configured correctly, examine the S1 switch to find possible configuration errors by viewing a summary of the VLAN information. Enter the show vlan brief command.

c. Are there any problems with the VLAN configuration?

d. Examine the switch for trunk configurations using the show interfaces trunk and the show interfaces f0/1 switchport commands.

e. Are there any problems with the trunking configuration?

f. Examine the running configuration of the switch to find possible configuration errors.

Are there any problems with the current configuration?

g. Correct the errors found regarding F0/1 and VLAN 10 on S1. Record the commands used in the space below.

h. Verify the commands had the desired effects by issuing the appropriate show commands.

i. Can PC-A ping PC-B? ______________

Step 2: Troubleshoot VLAN 10 on S2.

a. Using the previous commands, examine the S2 switch to find possible configuration errors.

Are there any problems with the current configuration?

b. Correct the errors found regarding interfaces and VLAN 10 on S2. Record the commands below.

Can PC-A ping PC-B? ______________
Part 3: Troubleshoot VLAN 20

In Part 3, you must examine VLAN 20 on S1 and S2 to determine if it is configured correctly. To verify functionality, you will reassign PC-A into VLAN 20, and then troubleshoot the scenario until connectivity is established.

Step 1: Assign PC-A to VLAN 20.

a. On PC-A, change the IP address to 192.168.20.2/24 with a default gateway of 192.168.20.1.

b. On S1, assign the port for PC-A to VLAN 20. Write the commands needed to complete the configuration.


c. Verify that the port for PC-A has been assigned to VLAN 20.

d. Can PC-A ping PC-C? __________

Step 2: Troubleshoot VLAN 20 on S1.

a. Using the previous commands, examine the S1 switch to find possible configuration errors.

Are there any problems with the current configuration?

b. Correct the errors found regarding VLAN 20.

c. Can PC-A ping PC-C? __________

Step 3: Troubleshoot VLAN 20 on S2.

a. Using the previous commands, examine the S2 switch to find possible configuration errors.

Are there any problems with the current configuration?

b. Correct the errors found regarding VLAN 20. Record the commands used below.


c. Can PC-A ping PC-C? __________

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

1. Why is a correctly configured trunk port critical in a multi-VLAN environment?

2. Why would a network administrator limit traffic for specific VLANs on a trunk port?
3.3.2.2 Lab – Implementing VLAN Security

Topology

![Topology Diagram]

Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>F0/1</td>
<td>172.17.99.11</td>
<td>255.255.255.0</td>
<td>172.17.99.1</td>
</tr>
<tr>
<td>S2</td>
<td>F0/11</td>
<td>172.17.99.12</td>
<td>255.255.255.0</td>
<td>172.17.99.1</td>
</tr>
<tr>
<td>PC-A</td>
<td>F0/6</td>
<td>172.17.99.3</td>
<td>255.255.255.0</td>
<td>172.17.99.1</td>
</tr>
<tr>
<td>PC-B</td>
<td>F0/18</td>
<td>172.17.99.4</td>
<td>255.255.255.0</td>
<td>172.17.99.1</td>
</tr>
</tbody>
</table>

VLAN Assignments

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Data</td>
</tr>
<tr>
<td>99</td>
<td>Management&amp;Native</td>
</tr>
<tr>
<td>999</td>
<td>BlackHole</td>
</tr>
</tbody>
</table>

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Implement VLAN Security on the Switches

Background / Scenario

Best practice dictates configuring some basic security settings for both access and trunk ports on switches. This will help guard against VLAN attacks and possible sniffing of network traffic within the network.

In this lab, you will configure the network devices in the topology with some basic settings, verify connectivity and then apply more stringent security measures on the switches. You will examine how Cisco switches behave by using various show commands. You will then apply security measures.
Note: The switches used with this lab are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will configure basic settings on the switches and PCs. Refer to the Addressing Table for device names and address information.

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

Step 2: Initialize and reload the switches.

Step 3: Configure IP addresses on PC-A, PC-B, and PC-C.

Refer to the Addressing Table for PC address information.

Step 4: Configure basic settings for each switch.

a. Disable DNS lookup.
b. Configure the device names as shown in the topology.
c. Assign class as the privileged EXEC mode password.
d. Assign cisco as the console and VTY password and enable login for console and vty lines.
e. Configure synchronous logging for console and vty lines.

Step 5: Configure VLANs on each switch.

a. Create and name VLANs according to the VLAN Assignments table.
b. Configure the IP address listed in the Addressing Table for VLAN 99 on both switches.
c. Configure F0/6 on S1 as an access port and assign it to VLAN 99.
d. Configure F0/11 on S2 as an access port and assign it to VLAN 10.
e. Configure F0/18 on S2 as an access port and assign it to VLAN 99.
f. Issue show vlan brief command to verify VLAN and port assignments.

To which VLAN would an unassigned port, such as F0/8 on S2, belong?
Step 6: Configure basic switch security.
   a. Configure a MOTD banner to warn users that unauthorized access is prohibited.
   b. Encrypt all passwords.
   c. Shut down all unused physical ports.
   d. Disable the basic web service running.
      
      S1(config) # no ip http server
      S2(config) # no ip http server
   e. Copy the running configuration to startup configuration.

Step 6: Verify connectivity between devices and VLAN information.
   a. From a command prompt on PC-A, ping the management address of S1. Were the pings successful? Why?

   b. From S1, ping the management address of S2. Were the pings successful? Why?

   c. From a command prompt on PC-B, ping the management addresses on S1 and S2 and the IP address of PC-A and PC-C. Were your pings successful? Why?

   d. From a command prompt on PC-C, ping the management addresses on S1 and S2. Were you successful? Why?

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

Part 2: Implement VLAN Security on the Switches

Step 1: Configure trunk ports on S1 and S2.
   a. Configure port F0/1 on S1 as a trunk port.
      
      S1(config) # interface f0/1
      S1(config-if) # switchport mode trunk
b. Configure port F0/1 on S2 as a trunk port.
   S2(config)# interface f0/1
   S2(config-if)# switchport mode trunk

c. Verify trunking on S1 and S2. Issue the show interface trunk command on both switches.
   S1# show interface trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

   Port Vlans allowed on trunk
   Fa0/1 1-4094

   Port Vlans allowed and active in management domain
   Fa0/1 1,10,99,999

   Port Vlans in spanning tree forwarding state and not pruned
   Fa0/1 1,10,99,999

Step 2: Change the native VLAN for the trunk ports on S1 and S2.

Changing the native VLAN for trunk ports from VLAN 1 to another VLAN is a good practice for security.

a. What is the current native VLAN for the S1 and S2 F0/1 interfaces?

b. Configure the native VLAN on the S1 F0/1 trunk interface to Management & Native VLAN 99.
   S1# config t
   S1(config)# interface f0/1
   S1(config-if)# switchport trunk native vlan 99

c. Wait a few seconds. You should start receiving error messages on the console session of S1. What does the %CDP-4-NATIVE_VLAN_MISMATCH: message mean?

d. Configure the native VLAN on the S2 F0/1 trunk interface to VLAN 99.
   S2(config)# interface f0/1
   S2(config-if)# switchport trunk native vlan 99

e. Verify that the native VLAN is now 99 on both switches. S1 output is shown below.
   S1# show interface trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>99</td>
</tr>
</tbody>
</table>

   Port Vlans allowed on trunk
   Fa0/1 1-4094

   Port Vlans allowed and active in management domain
Step 3: Verify that traffic can successfully cross the trunk link.

a. From a command prompt on PC-A, ping the management address of S1. Were the pings successful? Why?

b. From the console session on S1, ping the management address of S2. Were the pings successful? Why?

c. From a command prompt on PC-B, ping the management addresses on S1 and S2 and the IP address of PC-A and PC-C. Were your pings successful? Why?

d. From a command prompt on PC-C, ping the management addresses on S1 and S2 and the IP address of PC-A. Were you successful? Why?

Step 4: Prevent the use of DTP on S1 and S2.

Cisco uses a proprietary protocol known as the Dynamic Trunking Protocol (DTP) on its switches. Some ports automatically negotiate to trunking. A good practice is to turn off negotiation. You can see this default behavior by issuing the following command:

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

a. Turn off negotiation on S1.
```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

b. Turn off negotiation on S2.
```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```
c. Verify that negotiation is off by issuing the `show interface f0/1 switchport` command on S1 and S2.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
```

Step 5: Secure access ports on S1 and S2.

Even though you shut down unused ports on the switches, if a device is connected to one of those ports and the interface is enabled, trunking could occur. In addition, all ports by default are in VLAN 1. A good practice is to put all unused ports in a "black hole" VLAN. In this step, you will disable trunking on all unused ports. You will also assign unused ports to VLAN 999. For the purposes of this lab, only ports 2 through 5 will be configured on both switches.

a. Issue the `show interface f0/2 switchport` command on S1. Notice the administrative mode and state for trunking negotiation.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

b. Disable trunking on S1 access ports.

```
S1(config)# interface range f0/2 - 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

c. Disable trunking on S2 access ports.

d. Verify that port F0/2 is set to access on S1.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

<Output Omitted>
e. Verify that VLAN port assignments on both switches are correct. S1 is shown below as an example.

   S1# show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/7, Fa0/8, Fa0/9, Fa0/10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/11, Fa0/12, Fa0/13, Fa0/14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/15, Fa0/16, Fa0/17, Fa0/18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/19, Fa0/20, Fa0/21, Fa0/22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/23, Fa0/24, Gi0/1, Gi0/2</td>
</tr>
<tr>
<td>10 Data</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>99 Management&amp;Native</td>
<td>active</td>
<td>Fa0/6</td>
</tr>
<tr>
<td>999 BlackHole</td>
<td>active</td>
<td>Fa0/2, Fa0/3, Fa0/4, Fa0/5</td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005 trnet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>

   Restrict VLANs allowed on trunk ports.

   By default, all VLANs are allowed to be carried on trunk ports. For security reasons, it is a good practice to only allow specific desired VLANs to cross trunk links on your network.

f. Restrict the trunk port F0/1 on S1 to only allow VLANs 10 and 99.

   S1(config)# interface f0/1
   S1(config-if)# switchport trunk allowed vlan 10,99

g. Restrict the trunk port F0/1 on S2 to only allow VLANs 10 and 99.

h. Verify the allowed VLANs. Issue a show interface trunk command in privileged EXEC mode on both S1 and S2.

   S1# show interface trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>99</td>
</tr>
</tbody>
</table>

   Port Vlans allowed on trunk
   Fa0/1 10,99

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

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

   What is the result?
Reflection

What, if any, are the security problems with the default configuration of a Cisco switch?
3.4.1.1 Class Activity – VLAN Plan

Objective
Implement VLANs to segment a small- to medium-sized network.

Scenario
You are designing a VLAN switched network for your small- to medium-sized business.

Your business owns space on two floors of a high-rise building. The following elements need VLAN consideration and access for planning purposes:

- Management
- Finance
- Sales
- Human Resources
- Network administrator
- General visitors to your business location

You have two Cisco 3560-24PS switches.

Use a word processing software program to design your VLAN-switched network scheme.

Section 1 of your design should include the regular names of your departments, suggested VLAN names and numbers, and which switch ports would be assigned to each VLAN.

Section 2 of your design should list how security would be planned for this switched network.

Once your VLAN plan is finished, complete the reflection questions from this activity.

Save your work. Be able to explain and discuss your VLAN design with another group or with the class.

Required Resources
Word processing program

Reflection
1. What criteria did you use for assigning ports to the VLANs?

2. How could these users access your network if the switches were not physically available to general users via direct connection?

3. Could you reduce the number of switch ports assigned for general users if you used another device to connect them to the VLAN network switch? What would be affected?