Lab - Configure VLANs and Trunking

# Topology



# Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | N/A |
| S2 | VLAN 1 | 192.168.1.12 | 255.255.255.0 | N/A |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-B | NIC | 192.168.10.4 | 255.255.255.0 | 192.168.10.1 |

# 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.

**Note**: The switches used with CCNA hands-on labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

**Note**: Ensure that the routers and 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 15.2(2) lanbasek9 image or comparable)
* 2 PCs (Windows with a 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

# Instructions

## 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.

### Cable the network as shown in the topology.

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

### Configure basic settings for each switch.

* + - 1. Console into the switch and enable privileged EXEC mode.

Open configuration window

* + - 1. Enter configuration mode.
      2. Assign a device name to the switch.
      3. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
      4. Assign **class** as the privileged EXEC encrypted password.
      5. Assign **cisco** as the console password and enable login.
      6. Assign **cisco** as the vty password and enable login.
      7. Encrypt the plaintext passwords.
      8. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
      9. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.
      10. Shut down all interfaces that will not be used.
      11. Set the clock on the switch.
      12. Save the running configuration to the startup configuration file.

Close configuration window

### Configure PC hosts.

Refer to the Addressing Table for PC host address information.

### 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.

#### Questions:

Can PC-A ping PC-B?

Answer: Yes

Can PC-A ping S1?

Answer: No

Can PC-B ping S2?

Answer: No

Open configuration window

Can S1 ping S2?

Answer: No

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

Answer: Because they are on different subnets. A router needs to exist to allow this behaviour.

Close configuration window

## Create VLANs and Assign Switch Ports

In Part 2, you will create Management, Operations, Parking\_Lot, and Native 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.

### Create VLANs on the switches.

Open configuration window

* + - 1. Create the VLANs on S1.

S1(config)# **vlan 10**

S1(config-vlan)# **name Operations**

S1(config-vlan)# **vlan 20**

S1(config-vlan)# **name Parking\_Lot**

S1(config-vlan)# **vlan 99**

S1(config-vlan)# **name Management**

S1(config-vlan)# **vlan 1000**

S1(config-vlan)# **name Native**

S1(config-vlan)# **end**

* + - 1. Create the same VLANs on S2.
      2. Issue the **show vlan brief** command to view the list of VLANs on S1.

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, 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 Operations active

20 Parking\_Lot active

99 Management active

1000 Native active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

#### Questions:

What is the default VLAN?

Answer: 1

What ports are assigned to the default VLAN?

Answer: All

### Assign VLANs to the correct switch interfaces.

* + - 1. Assign VLANs to the interfaces on S1.
         1. Assign PC-A to the Operation VLAN.

S1(config)# **interface f0/6**

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

S1(config-if)# **switchport access vlan 10**

* + - * 1. Move the switch IP address 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**

* + - 1. Issue the **show vlan** **brief** command and verify that the VLANs are assigned to the correct interfaces.
      2. Issue the **show ip interface brief** command.

#### Question:

What is the status of VLAN 99? Explain.

Answer: Up/Down. Up because the vlan exists, down because the vlan yet has not been assigned to an active port.

* + - 1. Assign PC-B to the Operations VLAN on S2.
      2. Remove the IP address for VLAN 1 on S2.
      3. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.
      4. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

#### Questions:

Is S1 able to ping S2? Explain.

Answer: No, because the interface f0/1 has not been assigned a vlan yet

Close configuration window

Is PC-A able to ping PC-B? Explain.

Answer: No, because the switches can’t communicate yet

## 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.

### Assign a VLAN to multiple interfaces.

Open configuration window

* + - 1. On S1, assign interfaces F0/11 – 24 to VLAN99.

S1(config)# **interface range f0/11-24**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 99**

S1(config-if-range)# **end**

* + - 1. Issue the **show vlan brief** command to verify VLAN assignments.
      2. Reassign F0/11 and F0/21 to VLAN 10.
      3. Verify that VLAN assignments are correct.

### Remove a VLAN assignment from an interface.

* + - 1. Use the **no** **switchport access vlan** command to remove the VLAN 99 assignment to F0/24.

S1(config)# **interface f0/24**

S1(config-if)# **no switchport access vlan**

S1(config-if)# **end**

* + - 1. Verify that the VLAN change was made.

#### Question:

Which VLAN is F0/24 now associated with?

Answer: Default. Vlan 1

### Remove a VLAN ID from the VLAN database.

* + - 1. Add VLAN 30 to interface F0/24 without issuing the global 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 will be created and added to the VLAN database.

* + - 1. Verify that the new VLAN is displayed in the VLAN table.

#### Question:

What is the default name of VLAN 30?

Answer: Vlan0030

* + - 1. Use the **no vlan 30** command to remove VLAN 30 from the VLAN database.

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

S1(config)# **end**

* + - 1. Issue the **show vlan brief** command. F0/24 was assigned to VLAN 30.

#### Question:

After deleting VLAN 30 from the VLAN database, what VLAN is port F0/24 assigned to? What happens to the traffic destined to the host attached to F0/24?

Answer: Port f0/24 is still assigned to vlan 30. The Port will not transfer any traffic.

* + - 1. Issue the **no switchport access vlan** command on interface F0/24.
      2. Issue the **show vlan brief** command to determine the VLAN assignment for F0/24.

#### Questions:

To which VLAN is F0/24 assigned?

Answer: Vlan1, Default

**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?

Answer: Because the vlan becomes active again after deallocating the interface to the vlan. Because it is harder to diagnose. The interface might be a part of a trunked interface or who knooows.

Close configuration window

## 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.

### 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.

Open configuration window

* + - 1. Set F0/1 on S1 to negotiate trunk mode.

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

S1(config-if)# **switchport mode dynamic desirable**

Sep 19 02:51:47.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Sep 19 02:51:47.291: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

You should also receive link status messages on S2.

S2#

Sep 19 02:42:19.424: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

Sep 19 02:42:21.454: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

Sep 19 02:42:22.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

* + - 1. 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.
      2. 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**

S2# **show interfaces trunk**

**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.

Close configuration window

* + - 1. Verify that VLAN traffic is traveling over trunk interface F0/1.

#### Questions:

Can S1 ping S2?

Answer: Yes

Can PC-A ping PC-B?

Answer: Yes

Can PC-A ping S1?

Answer: No

Can PC-B ping S2?

Answer: No

If you answered no to any of the above questions, explain below.

Answer: The switches are on vlan 99 while the PC’s are on vlan 1

### 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.

Open configuration window

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

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

* + - 1. Issue the **show interfaces trunk** command to view the trunk mode. Notice that the mode changed from **desirable** to **on**.

S2# **show interfaces trunk**

* + - 1. Modify the trunk configuration on both switches by changing the native VLAN from VLAN 1 to VLAN 1000.

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

S1(config-if)# **switchport trunk native vlan 1000**

* + - 1. Issue the show interfaces trunk command to view the trunk. Notice the Native VLAN information is updated.

S2# **show interfaces trunk**

#### Questions:

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

Answer: To ensure that the port actually becomes a trunk

Why might you want to change the native VLAN on a trunk?

Answer: Because using the default vlan 1 is a security risk

Close configuration window

## 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.

### Determine if the VLAN database exists.

Open configuration window

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

S1# **show flash:**

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

### 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]

* + - 1. Issue the **show flash** command to verify that the vlan.dat file has been deleted.

S1# **show flash:**

#### Question:

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

Answer: erase startup-config

Close configuration window

# Reflection Questions

* 1. What is needed to allow hosts on VLAN 10 to communicate to hosts on VLAN 99?

# Answer: allow Inter-VLAN routing requires a Layer 3 device is needed to route traffic between VLANs.

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

# Answer: VLAN benefits include: better security, cost savings (efficient use of bandwidth and uplinks), higher performance (smaller broadcast domains), broadcast storm mitigation, improved IT staff efficiency, simpler project and application management.

End of Document