Lab 1 basic switch configuration

Examine the current running configuration file.

Switch# show running-config

Examine the startup configuration file in NVRAM.

Switch# show startup-config

startup-config is not present

Examine the characteristics of the SVI for VLAN 1.

Switch# show interface vlan1

What is the MAC address of this SVI? Answers will vary. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
0CD9:96E2:3D40 in this case.

Examine the IP properties of the SVI VLAN 1.

Switch# show ip interface vlan1

What output do you see?  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Vlan1 is up, line protocol is down

Internet protocol processing disabled

 If you are using Netlab, enable interface F0/6 on S1.

Switch# show ip interface vlan1

What output do you see?  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Vlan1 is up, line protocol is up

Internet protocol processing disabled

Examine the Cisco IOS version information of the switch.

Switch# show version

 Examine the default properties of the FastEthernet interface used by PC-A.

Switch# show interface f0/6

 Examine the default VLAN settings of the switch.

Switch# show vlan

Issue one of the following commands to examine the contents of the flash directory.

Switch# show flash

Switch# dir flash:

First, create the new VLAN 99 on the switch. Then set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99.

S1# configure terminal

S1(config)# vlan 99

S1(config-vlan)# exit

S1(config)# interface vlan99

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down

S1(config-if)# ip address 192.168.1.2 255.255.255.0

S1(config-if)# no shutdown

S1(config-if)# exit

S1(config)#

c. Assign all user ports to VLAN 99.

S1(config)# interface range f0/1 – 24,g0/1 - 2

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

S1(config-if-range)# exit

S1(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

 Issue the show vlan brief command to verify that all ports are in VLAN 99.

S1# show vlan brief

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active

99 VLAN0099 active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Gi0/1, Gi0/2

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

 Configure the default gateway for S1. If no default gateway is set, the switch cannot be managed from a remote network that is more than one router away. Although this activity does not include an external IP gateway, assume that you will eventually connect the LAN to a router for external access. Assuming that the LAN interface on the router is 192.168.1.1, set the default gateway for the switch.

S1(config)# ip default-gateway 192.168.1.1

S1(config)#

Console port access should also be restricted. The default configuration is to allow all console connections with no password needed. To prevent console messages from interrupting commands, use the logging synchronous option.

S1(config)# line con 0

S1(config-line)# password cisco

S1(config-line)# login

S1(config-line)# logging synchronous

S1(config-line)# exit

S1(config)#

Configure the virtual terminal (vty) lines for the switch to allow Telnet access. If you do not configure a vty password, you will not be able to Telnet to the switch.

S1(config)# line vty 0 15

S1(config-line)# password cisco

S1(config-line)# login

S1(config-line)# end

S1#

\*Mar 1 00:06:11.590: %SYS-5-CONFIG\_I: Configured from console by console

#### **Step 2: Configure an IP address on PC-A.**

Assign the IP address and subnet mask to the PC as shown in the Addressing Table. An abbreviated version of the procedure is described here. A default gateway is not required for this topology; however, you can enter 192.168.1.1 to simulate a router attached to S1.

1) Click the Windows Start icon > Control Panel.

2) Click View By: and choose Small icons.

3) Choose Network and Sharing Center > Change adapter settings.

4) Select Local Area Network Connection, right click and choose Properties.

5) Choose Internet Protocol Version 4 (TCP/IPv4) > Properties.

6) Click the Use the following IP address radio button and enter the IP address and subnet mask.

S1# show mac address-table

Set up a static MAC address on F0/6 using the address that was recorded for PC-A in Part 4, Step 1. The MAC address 0050.56BE.6C89 is used as an example only. You must use the MAC address of PC-A, which is different than the one given here as an example.

S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface

fastethernet 0/6

Lab2 configure basic router settings

#### **Part 1: Set Up the Topology and Initialize Devices**

• Cable equipment to match the network topology.  
• Initialize and restart the router and switch.

#### **Part 2: Configure Devices and Verify Connectivity**

• Assign static IPv4 and IPv6 information to the PC interfaces.  
• Configure basic router settings.  
• Configure the router for SSH.  
• Verify network connectivity.

#### **Part 3: Display Router Information**

• Retrieve hardware and software information from the router.  
• Interpret the output from the startup configuration.  
• Interpret the output from the routing table.  
• Verify the status of the interfaces.

Open configuration window  
a. Console into the router and enable privileged EXEC mode.  
b. Enter configuration mode.

Router>enable

Router#config terminal

##### **Step 2: Configure the router.**

Open configuration window  
a. Console into the router and enable privileged EXEC mode.  
b. Enter configuration mode.

Router>enable

Router#config terminal

c. Assign a device name to the router.  
d. Set the router’s domain name as ccna-lab.com.

R1(config)#ip domain-name ccna-lab.com

e. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

R1(config)#no ip domain-lookup

f. Encrypt the plaintext passwords.

R1(config)#service password-encryption

g. Configure the system to require a minimum 12-character password.

R1(config)#security passwords min-length 12

h. Configure the username **SSHadmin** with an encrypted password of **55Hadm!n2020**.  
i. Generate a set of crypto keys with a 1024 bit modulus

R1(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

R1(config)#username SSHadmin secret 55Hadm!n2020

j. Assign the privileged EXEC password to **$cisco!PRIV\***

R1(config)#enable secret $cisco!PRIV\*

k. Assign **$cisco!!CON\*** as the console password, configure sessions to disconnect after four minutes of inactivity, and enable login.

R1(config)#line console 0

R1(config-line)#password $cisco!!CON\*

R1(config-line)#exec-tim

R1(config-line)#exec-timeout 4

R1(config-line)#login

l. Assign **$cisco!!VTY\*** as the vty password, configure the vty lines to accept SSH connections only, configure sessions to disconnect after four minutes of inactivity, and enable login using the local database.

R1(config)#line vty 0 4

R1(config-line)#transport input ssh

R1(config-line)#exec-timeout 4

R1(config-line)#login local

m. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

R1(config)#banner motd #Unauthorized access to this device is prohibited!#

n. Enable IPv6 Routing

R1(config)#ipv6 unicast-routing

o. Configure all three interfaces on the router with the IPv4 and IPv6 addressing information from the addressing table above. Configure all three interfaces with descriptions. Activate all three interfaces.

R1(config)#interface g0/0/0

R1(config-if)#ip address 192.168.0.1 255.255.255.0

R1(config-if)#ipv6 add 2001:db8:acad::1/64

R1(config-if)#description Link to PC-B

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface g0/0/1

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#ipv6 address 2001:db8:acad:1::1/64

R1(config-if)#description Link to PC-A

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface loopback 0

R1(config-if)#ip address 10.0.0.1 255.255.255.0

R1(config-if)#ipv6 address 2001:db8:acad:2::1/64

R1(config-if)#description Connect to loopback 0

R1(config-if)#exit

p. The router should not allow vty logins for two minutes if three failed login attempts occur within 60 seconds.

R1(config)#login block-for 120 attempts 3 within 60

q. Set the clock on the router.

R1#clock set 15:37:00 5 JUL 2020

r. Save the running configuration to the startup configuration file.

R1#copy running-config startup-config

R1#show version | include register

Configuration register is 0x2142

# Lab – Implement Etherchannel

* ****Part 1: Build the Network and Configure Basic Device Settings****
* ****Part 2: Create VLANs and Assign Switch Ports****
* ****Part 3: Configure 802.1Q Trunks between the Switches****
* ****Part 4: Implement and Verify an EtherChannel between the 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: Configure basic settings for each switch.**

a. Assign a device name to the switch.

switch(config)# hostname S1

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

S1(config)# no ip domain-lookup

c. Assign ****class**** as the privileged EXEC encrypted password.

S1(config)# enable secret class

d. Assign ****cisco**** as the console password and enable login.

S1(config)# line console 0

S1(config-line)# password cisco

S1(config-line)# login

e. Assign ****cisco**** as the VTY password and enable login.

S1(config)# line vty 0 15

S1(config-line)# password cisco

S1(config-line)# login

f. Encrypt the plaintext passwords.

S1(config)# service password-encryption

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

S1(config)# banner motd $ Authorized Users Only! $

h. Save the running configuration to the startup configuration file.

S1# copy running-config startup-config

i. Set the clock on the switch to today’s time and date.

S1# clock set 15:30:00 27 Aug 2019

#### **Part 2: Create VLANs and Assign Switch Ports**

In Part 2, you will create VLANs as specified in the table above on both switches. You will then assign the VLANs to the appropriate interface and verify your configuration settings. Complete the following tasks on each switch.

##### **Step 1: Create VLANs on the switches.**

a. On both switches create and name the required VLANs from the VLAN Table above.

S1(config)# vlan 10

S1(config-vlan)# name Management

S1(config-vlan)# vlan 20

S1(config-vlan)# name Clients

S1(config-vlan)# vlan 999

S1(config-vlan)# name Parking\_Lot

S1(config-vlan)# vlan 1000

S1(config-vlan)# name Native

S1(config-vlan)# exit

S2(config)# vlan 10

S2(config-vlan)# name Management

S2(config-vlan)# vlan 20

S2(config-vlan)# name Clients

S2(config-vlan)# vlan 999

S2(config-vlan)# name Parking\_Lot

S2(config-vlan)# vlan 1000

S2(config-vlan)# name Native

S2(config-vlan)# exit

b. Configure and activate the management interface on each switch using the IP address information in the Addressing Table.

S1(config)# interface vlan 10

S1(config-if)# ip address 192.168.10.11 255.255.255.0

S1(config-if)# no shutdown

S1(config-if)# exit

S2(config)# interface vlan 10

S2(config-if)# ip address 192.168.10.12 255.255.255.0

S2(config-if)# no shutdown

S2(config-if)# exit

c. Assign all unused ports on the switch to the Parking\_Lot VLAN, configure them for static access mode, and administratively deactivate them.

S1(config)# interface range f0/3 - 4, f0/7 - 24, g0/1 - 2

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

S1(config-if-range)# switchport access vlan 999

S1(config-if-range)# shutdown

S2(config)# interface range f0/3 - 17, f0/19 - 24, g0/1 - 2

S2(config-if-range)# switchport mode access

S2(config-if-range)# switchport access vlan 999

S2(config-if-range)# shutdown

##### **Step 2: Assign VLANs to the correct switch interfaces.**

a. Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode.

S1(config)# interface f0/6

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 20

S2(config)# interface f0/18

S2(config-if)# switchport mode access

S2(config-if)# switchport access vlan 20

#### **Part 3: Configure 802.1Q trunks between the switches.**

In Part 3, you will manually configure interfaces F0/1 and F0/2 as 802.1Q trunks.

a. Change the switchport mode on the interfaces to force trunking. Use the interface range command to reduce the number of commands required. Make sure to do this on both switches.

S1(config)# interface range f0/1-2

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

S2(config)# interface range f0/1-2

S2(config-if-range)# switchport mode trunk

b. As a part of the trunk configuration, set the native VLAN to 1000 on both switches. You may see error messages temporarily while the two interfaces are configured for different native VLANs.

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

S2(config-if-range)# switchport trunk native vlan 1000

c. As another part of trunk configuration, specify that VLANs 10, 20, and 1000 are allowed to cross the trunk.

S1(config-if-range)# switchport trunk allowed vlan 10,20,1000

S2(config-if-range)# switchport trunk allowed vlan 10,20,1000

#### **Part 4: Implement and Verify an EtherChannel between the switches.**

a. Create a LACP-based EtherChannel using F0/1 and F0/2 using group number 1, with both switches actively negotiating the EtherChannel protocol. Use the interface range command to reduce the number of commands required.

S1(config)# interface range f0/1-2

S1(config-if-range)# channel-group 1 mode active

S1(config-if-range)# exit

S2(config)# interface range f0/1-2

S2(config-if-range)# channel-group 1 mode active

S2(config-if-range)# exit

# Lab – Configure VLANs and Trunking

* ****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****

a. Console into the switch and enable privileged EXEC mode.

switch> enable

b. Enter configuration mode.

switch# config terminal

c. Assign a device name to the switch.

switch(config)# hostname S1

switch(config)# hostname S2

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

S1(config)# no ip domain-lookup

S2(config)# no ip domain-lookup

e. Assign class as the privileged EXEC encrypted password.

S1(config)# enable secret class

S2(config)# enable secret class

f. Assign cisco as the console password and enable login.

S1(config)# line console 0S1(config-line)# password ciscoS1(config-line)# login

S2(config)# line console 0S2(config-line)# password ciscoS2(config-line)# login

g. Assign cisco as the vty password and enable login.

S1(config)# line vty 0 4S1(config-line)# password ciscoS1(config-line)# login

S2(config)# line vty 0 4S2(config-line)# password ciscoS2(config-line)# login

h. Encrypt the plaintext passwords.

S1(config)# service password-encryption

S2(config)# service password-encryption

i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

S1(config)# banner motd $ Authorized Users Only! $

S2(config)# banner motd $ Authorized Users Only! $

j. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.

S1(config)# interface vlan 1S1(config-if)# ip address 192.168.1.11 255.255.255.0S1(config-if)# no shutdownS1(config-if)# exit

S2(config)# interface vlan 1S2(config-if)# ip address 192.168.1.12 255.255.255.0S2(config-if)# no shutdownS2(config-if)# exit

k. Shut down all interfaces that will not be used.

S1(config)# interface range f0/2-5, f0/7-24, g0/1-2S1(config-if-range)# shutdown

S2(config)# interface range f0/2-17, f0/18-24, g0/1-2S2(config-if-range)# shutdown

l. Set the clock on the switch.

S1# clock set 15:30:00 19 September 2019

S2# clock set 15:30:00 19 September 2019

m. Save the running configuration to the startup configuration file.

S1# copy running-config startup-config

S2# copy running-config startup-config

#### **Part 2: 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.

##### **Step 1: Create VLANs on the switches.**

a. 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

b. Create the same VLANs on S2.

##### **Step 2: Assign VLANs to the correct switch interfaces.**

a. 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

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

S1(config-if)# ip address 192.168.1.11 255.255.255.0

S1(config-if)# end

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

d. Assign PC-B to the Operations VLAN on S2.

S2(config)# interface f0/18

S2(config-if)# switchport mode access

S2(config-if)# switchport access vlan 10

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

S2(config)# interface vlan 1

S2(config-if)# no ip address

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

S2(config-if)# interface vlan 99

S2(config-if)# ip address 192.168.1.12 255.255.255.0

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

#### **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 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

 Reassign F0/11 and F0/21 to VLAN 10.

S1(config)# interface range f0/11, f0/21

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

S1(config-if-range)# end

##### **Step 2: Remove a VLAN assignment from an interface.**

a. 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

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

a. 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.

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

#### **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

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 FastEthe

c. 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

S2(config)# interface f0/1S2(config-if)# switchport trunk native vlan 1000

##### **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.

S1# ****delete vlan.dat****

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

## Lab – Implement DHCPv4

* ****Part 1: Build the Network and Configure Basic Device Settings****
* ****Part 2: Configure and verify two DHCPv4 Servers on R1****
* ****Part 3: Configure and verify a DHCP Relay on R2****

##### **Step 3: Configure basic settings for each router.**

a. Assign a device name to the router.

router(config)# hostname R1

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

R1(config)# no ip domain lookup

c. Assign ****class**** as the privileged EXEC encrypted password.

R1(config)# enable secret class

d. Assign ****cisco**** as the console password and enable login.

R1(config)# line console 0

R1(config-line)# password cisco

R1(config-line)# login

e. Assign ****cisco**** as the VTY password and enable login.

R1(config)# line vty 0 4

R1(config-line)# password cisco

R1(config-line)# login

f. Encrypt the plaintext passwords.

R1(config)# service password-encryption

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

R1(config)# banner motd $ Authorized Users Only! $

h. Save the running configuration to the startup configuration file.

R1# copy running-config startup-config

i. Set the clock on the router to today’s time and date.

R1# clock set 15:30:00 27 Aug 2019

****Note:**** Use the question mark (?) to help with the correct sequence of parameters needed to execute this command.

##### **Step 4: Configure Inter-VLAN Routing on R1**

a. Activate interface G0/0/1 on the router.

R1(config)# interface g0/0/1

R1(config-if)# no shutdown

R1(config-if)# exit

b. Configure sub-interfaces for each VLAN as required by the IP addressing table. All sub-interfaces use 802.1Q encapsulation and are assigned the first usable address from the IP address pool you have calculated. Ensure the sub-interface for the native VLAN does not have an IP address assigned. Include a description for each sub-interface.

R1(config)# interface g0/0/1.100

R1(config-subif)# description Client Network

R1(config-subif)# encapsulation dot1q 100

R1(config-subif)# ip address 192.168.1.1 255.255.255.192

R1(config-subif)# interface g0/0/1.200

R1(config-subif)# encapsulation dot1q 200

R1(config-subif)# description Management Network

R1(config-subif)# ip address 192.168.1.65 255.255.255.224

R1(config-subif)# interface g0/0/1.1000

R1(config-subif)# encapsulation dot1q 1000 native

R1(config-subif)# description Native VLAN

c. Verify the sub-interfaces are operational.

R1# show ip interface brief

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 unassigned YES unset administratively down down

GigabitEthernet0/0/1 unassigned YES unset up up

Gi0/0/1.100 192.168.1.1 YES manual up up

Gi0/0/1.200 192.168.1.65 YES manual up up

Gi0/0/1.1000 unassigned YES unset up up

Step 5: Configure G0/0/1 on R2, then G0/0/0 and static routing for both routers

a. Configure G0/0/1 on R2 with the first IP address of Subnet C you calculated earlier.

R2(config)# interface g0/0/1

R2(config-if)# ip address 192.168.1.97 255.255.255.240

R2(config-if)# no shutdown

R2(config-if)# exit

b. Configure interface G0/0/0 for each router based on the IP Addressing table above.

R1(config)# interface g0/0/0

R1(config-if)# ip address 10.0.0.1 255.255.255.252

R1(config-if)# no shutdown

R2(config)# interface g0/0/0

R2(config-if)# ip address 10.0.0.2 255.255.255.252

R2(config-if)# no shutdown

c. Configure a default route on each router pointed to the IP address of G0/0/0 on the other router.

R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2

R2(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1

d. Verify static routing is working by pinging R2’s G0/0/1 address from R1.

R1# ping 192.168.1.97

e. Save the running configuration to the startup configuration file.

R1# copy running-config startup-config

##### **Step 6: Configure basic settings for each switch.**

a. Assign a device name to the switch.

switch(config)# hostname S1

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

S1(config)# no ip domain-lookup

c. Assign ****class**** as the privileged EXEC encrypted password.

S1(config)# enable secret class

d. Assign ****cisco**** as the console password and enable login.

S1(config)# line console 0

S1(config-line)# password cisco

S1(config-line)# login

e. Assign ****cisco**** as the VTY password and enable login.

S1(config)# line vty 0 4

S1(config-line)# password cisco

S1(config-line)# login

f. Encrypt the plaintext passwords.

S1(config)# service password-encryption

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

S1(config)# banner motd $ Authorized Users Only! $

h. Save the running configuration to the startup configuration file.

S1(config)# exit

S1# copy running-config startup-config

i. Set the clock on the switch to today’s time and date.

S1# clock set 15:30:00 27 Aug 2019

##### **Step 7: Create VLANs on S1.**

****Note:**** S2 is only configured with basic settings.

a. Create and name the required VLANs on switch 1 from the table above.

S1(config)# vlan 100

S1(config-vlan)# name Clients

S1(config-vlan)# vlan 200

S1(config-vlan)# name Management

S1(config-vlan)# vlan 999

S1(config-vlan)# name Parking\_Lot

S1(config-vlan)# vlan 1000

S1(config-vlan)# name Native

S1(config-vlan)# exit

b. Configure and activate the management interface on S1 (VLAN 200) using the second IP address from the subnet calculated earlier. Additionally, set the default gateway on S1.

S1(config)# interface vlan 200

S1(config-if)# ip address 192.168.1.66 255.255.255.224

S1(config-if)# no shutdown

S1(config-if)# exit

S1(config)# ip default-gateway 192.168.1.65

c. Configure and activate the management interface on S2 (VLAN 1) using the second IP address from the subnet calculated earlier. Additionally, set the default gateway on S2

S2(config)# interface vlan 1

S2(config-if)# ip address 192.168.1.98 255.255.255.240

S2(config-if)# no shutdown

S2(config-if)# exit

S2(config)# ip default-gateway 192.168.1.97

d. Assign all unused ports on S1 to the Parking\_Lot VLAN, configure them for static access mode, and administratively deactivate them. On S2, administratively deactivate all the unused ports.

****Note:**** The interface range command is helpful to accomplish this task with as few commands as necessary.

S1(config)# interface range f0/1 - 4, f0/7 - 24, g0/1 - 2

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

S1(config-if-range)# switchport access vlan 999

S1(config-if-range)# shutdown

S1(config-if-range)# exit

S2(config)# interface range f0/1 - 4, f0/6 - 17, f0/19 - 24, g0/1 - 2

S2(config-if-range)# switchport mode access

S2(config-if-range)# shutdown

S2(config-if-range)# exit

Step 8: Assign VLANs to the correct switch interfaces.

a. Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode.

S1(config)# interface f0/6

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 100

##### **Step 9: Manually configure S1’s interface F0/5 as an 802.1Q trunk.**

a. Change the switchport mode on the interface to force trunking.

S1(config)# interface f0/5

S1(config-if)# switchport mode trunk

b. As a part of the trunk configuration, set the native VLAN to 1000.

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

c. As another part of trunk configuration, specify that VLANs 100, 200, and 1000 are allowed to cross the trunk.

S1(config-if-range)# switchport trunk allowed vlan 100,200,1000

d. Save the running configuration to the startup configuration file.

S1(config)# exit

S1# copy running-config startup-config

#### **Part 2: Configure and verify two DHCPv4 Servers on R1**

In Part 2, you will configure and verify a DHCPv4 Server on R1. The DHCPv4 server will service two subnets, Subnet A and Subnet C.

##### **Step 1: Configure R1 with DHCPv4 pools for the two supported subnets. Only the DHCP Pool for subnet A is given below**

a. Exclude the first five useable addresses from each address pool.

R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.5

b. Create the DHCP pool (Use a unique name for each pool).

R1(config)# ip dhcp pool R1\_Client\_LAN

c. Specify the network that this DHCP server is supporting.

R1(dhcp-config)# network 192.168.1.0 255.255.255.192

d. Configure the domain name as ccna-lab.com

R1(dhcp-config)# domain-name ccna-lab.com

e. Configure the appropriate default gateway for each DHCP pool.

R1(dhcp-config)# default-router 192.168.1.1

f. Configure the lease time for 2 days 12 hours and 30 minutes.

R1(dhcp-config)# lease 2 12 30

g. Next, configure the second DHCPv4 Pool using the pool name R2\_Client\_LAN and the calculated network, default-router and use the same domain name and lease time from the previous DHCP pool.

R1(config)# ip dhcp excluded-address 192.168.1.97 192.168.1.101

R1(config)# ip dhcp pool R2\_Client\_LAN

R1(dhcp-config)# network 192.168.1.96 255.255.255.240

R1(dhcp-config)# default-router 192.168.1.97

R1(dhcp-config)# domain-name ccna-lab.com

R1(dhcp-config)# lease 2 12 30

##### **Step 2: Save your configuration**

Save the running configuration to the startup configuration file.

R1# copy running-config startup-config

#### **Part 3: Configure and verify a DHCP Relay on R2**

In Part 3, you will configure R2 to relay DHCP requests from the local area network on interface G0/0/1 to the DHCP server (R1).

##### **Step 1: Configure R2 as a DHCP relay agent for the LAN on G0/0/1**

a. Configure the ip helper-address command on G0/0/1 specifying R1’s G0/0/0 IP address.

R2(config)# interface g0/0/1

R2(config-if)# ip helper-address 10.0.0.1

b. Save your configuration.

R2(config-if)# exit

R2# copy running-configuration startup-configuration

* ****Part 1: Build the Network and Configure Basic Device Settings****
* ****Part 2: Create VLANs and Assign Switch Ports****
* ****Part 3: Configure an 802.1Q Trunk between the Switches****
* ****Part 4: Configure Inter-VLAN Routing on the Router****
* ****Part 5: Verify Inter-VLAN Routing is working****

##### **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: Configure basic settings for the router.**

a. Console into the router and enable privileged EXEC mode.

router> enable

b. Enter configuration mode.

router# config terminal

c. Assign a device name to the router.

ADVERTISING

router(config)# hostname R1

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

R1(config)# no ip domain-lookup

e. Assign ****class**** as the privileged EXEC encrypted password.

R1(config)# enable secret class

f. Assign ****cisco**** as the console password and enable login.

R1(config)# line console 0

R1(config-line)# password cisco

R1(config-line)# login

g. Assign ****cisco**** as the VTY password and enable login.

ADVERTISING

R1(config)# line vty 0 4

R1(config-line)# password cisco

R1(config-line)# login

h. Encrypt the plaintext passwords.

R1(config)# service password-encryption

i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

R1(config)# banner motd $ Authorized Users Only! $

j. Save the running configuration to the startup configuration file.

R1(config)# exit

R1# copy running-config startup-config

k. Set the clock on the router.

R1# clock set 15:30:00 19 September 2019

##### **Step 3: Configure basic settings for each switch.**

a. Console into the switch and enable privileged EXEC mode.

switch> enable

b. Enter configuration mode.

switch# config terminal

c. Assign a device name to the switch.

switch(config)# hostname S1

switch(config)# hostname S2

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

S1(config)# no ip domain-lookup

S2(config)# no ip domain-lookup

e. Assign ****class**** as the privileged EXEC encrypted password.

S1(config)# enable secret class

S2(config)# enable secret class

f. Assign ****cisco**** as the console password and enable login.

S1(config)# line console 0

S1(config-line)# password cisco

S1(config-line)# login

S2(config)# line console 0

S2(config-line)# password cisco

S2(config-line)# login

g. Assign ****cisco**** as the vty password and enable login.

S1(config)# line vty 0 15

S1(config-line)# password cisco

S1(config-line)# login

S2(config)# line vty 0 15

S2(config-line)# password cisco

S2(config-line)# login

h. Encrypt the plaintext passwords.

S1(config)# service password-encryption

S2(config)# service password-encryption

i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

S1(config)# banner motd $ Authorized Users Only! $

S2(config)# banner motd $ Authorized Users Only! $

j. Set the clock on the switch.

S1# clock set 15:30:00 19 September 2019

S2# clock set 15:30:00 19 September 2019

****Note:**** Use the question mark (?) to help with the correct sequence of parameters needed to execute this command.

k. Copy the running configuration to the startup configuration.

S1# copy running-config startup-config

S2# copy running-config startup-config

##### **Step 4: Configure PC hosts.**

Refer to the Addressing Table for PC host address information.

#### **Part 2: Create VLANs and Assign Switch Ports**

In Part 2, you will create VLANs, as specified in the table above, on both switches. You will then assign the VLANs to the appropriate interface. The show vlan command is used to verify your configuration settings. Complete the following tasks on each switch.

##### **Step 1: Create VLANs on both switches.**

a. Create and name the required VLANs on each switch from the table above.

S1(config)# vlan 3

S1(config-vlan)# name Management

S1(config-vlan)# vlan 4

S1(config-vlan)# name Operations

S1(config-vlan)# vlan 7

S1(config-vlan)# name ParkingLot

S1(config-vlan)# vlan 8

S1(config-vlan)# name Native

S2(config)# vlan 3

S2(config-vlan)# name Management

S2(config-vlan)# vlan 4

S2(config-vlan)# name Operations

S2(config-vlan)# vlan 7

S2(config-vlan)# name ParkingLot

S1(config-vlan)# vlan 8

S1(config-vlan)# name Native

b. Configure the management interface and default gateway on each switch using the IP address information in the Addressing Table.

S1(config)# interface vlan 3

S1(config-if)# ip address 192.168.3.11 255.255.255.0

S1(config-if)# no shutdown

S1(config-if)# exit

S1(config)# ip default-gateway 192.168.3.1

S2(config)# interface vlan 3

S2(config-if)# ip address 192.168.3.12 255.255.255.0

S2(config-if)# no shutdown

S2(config-if)# exit

S2(config)# ip default-gateway 192.168.3.1

c. Assign all unused ports on both switches to the ParkingLot VLAN, configure them for static access mode, and administratively deactivate them.

****Note:**** The interface range command is helpful to accomplish this task with as few commands as necessary.

S1(config)# interface range f0/2 - 4 , f0/7 - 24 , g0/1 - 2

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

S1(config-if-range)# switchport access vlan 7

S1(config-if-range)# shutdown

S2(config)# interface range f0/2 - 17, f0/19 - 24 , g0/1 - 2

S2(config-if-range)# switchport mode access

S2(config-if-range)# switchport access vlan 7

S2(config-if-range)# shutdown

##### **Step 2: Assign VLANs to the correct switch interfaces.**

a. Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode. Be sure to do this on both switches

S1(config)# interface f0/6

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 3

S2(config)# interface f0/18

S2(config-if)# switchport mode access

S2(config-if)# switchport access vlan 4

#### **Part 3: Configure an 802.1Q Trunk Between the Switches**

In Part 3, you will manually configure interface F0/1 as a trunk.

##### **Step 1: Manually configure trunk interface F0/1.**

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

S2(config)# interface f0/1

S2(config-if)# switchport mode trunk

b. As a part of the trunk configuration, set the native VLAN to 8 on both switches. You may see error messages temporarily while the two interfaces are configured for different native VLANs.

S1(config-if)# switchport trunk native vlan 8

S2(config-if)# switchport trunk native vlan 8

c. As another part of trunk configuration, specify that VLANs 3, 4, and 8 are only allowed to cross the trunk.

S1(config-if)# switchport trunk allowed vlan 3,4,8

S2(config-if)# switchport trunk allowed vlan 3,4,8

##### **Step 2: Manually configure S1’s trunk interface F0/5**

a. Configure the F0/5 on S1 with the same trunk parameters as F0/1. This is the trunk to the router.

S1(config)# interface f0/5

S1(config-if)# switchport mode trunk

S1(config-if)# switchport trunk native vlan 8

S1(config-if)# switchport trunk allowed vlan 3,4,8

b. Save the running configuration to the startup configuration file on S1 and S2.

S1# copy running-config startup-config

S2# copy running-config startup-config

#### **Part 4: Configure Inter-VLAN Routing on the Router**

a. Activate interface G0/0/1 on the router.

R1(config)# interface g0/0/1

R1(config-if)# no shutdown

R1(config-if)# exit

b. Configure sub-interfaces for each VLAN as specified in the IP addressing table. All sub-interfaces use 802.1Q encapsulation. Ensure the sub-interface for the native VLAN does not have an IP address assigned. Include a description for each sub-interface.

R1(config)# interface g0/0/1.3

R1(config-subif)# description Management Network

R1(config-subif)# encapsulation dot1q 3

R1(config-subif)# ip address 192.168.3.1 255.255.255.0

R1(config-subif)# interface g0/0/1.4

R1(config-subif)# description Operations Network

R1(config-subif)# encapsulation dot1q 4

R1(config-subif)# ip address 192.168.4.1 255.255.255.0

R1(config-subif)# interface g0/0/1.8

R1(config-subif)# description Native VLAN

R1(config-subif)# encapsulation dot1q 8 native