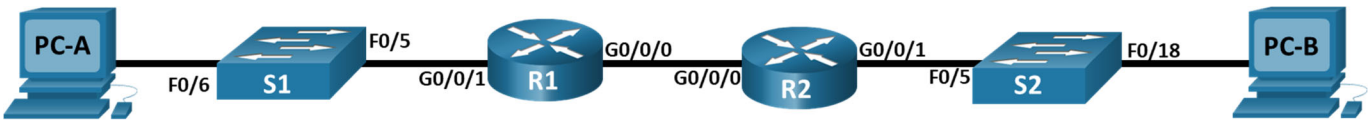
Lab - Implement DHCPv4

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/0	10.0.0.1	255.255.255.252	N/A
	G0/0/1	N/A	N/A	
	G0/0/1.100			
	G0/0/1.200			
	G0/0/1.1000	N/A	N/A	
R2	G0/0/0	10.0.0.2	255.255.255.252	N/A
	G0/0/1			
S1	VLAN 200			
S2	VLAN 1			
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

VLAN Table

VLAN	Name	Interface Assigned
1	N/A	S2: F0/18
100	Clients	S1: F0/6
200	Management	S1: VLAN 200
999	Parking_Lot	S1: F0/1-4, F0/7-24, G0/1-2
1000	Native	N/A

Objectives

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

© 2017 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Background / Scenario

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that lets network administrators manage and automate the assignment of IP addresses. Without DHCP for IPv4, the administrator must manually assign and configure IP addresses, preferred DNS servers, and default gateways. As the network grows in size, this becomes an administrative problem when devices are moved from one internal network to another.

In this scenario, the company has grown in size, and the network administrators can no longer assign IP addresses to devices manually. Your job is to configure the R1 router to assign IPv4 addresses on two different subnets.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the 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 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 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

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: Establish an addressing scheme

Subnet the network 192.168.1.0/24 to meet the following requirements:

a. One subnet, “Subnet A”, supporting 58 hosts (the client VLAN at R1).

Subnet A:

Record the first IP address in the Addressing Table for R1 G0/0/1.100. Record the second IP address in the Address Table for S1 VLAN 200 and enter the associated default gateway.

b. One subnet, “Subnet B”, supporting 28 hosts (the management VLAN at R1).

Subnet B:

Record the first IP address in the Addressing Table for R1 G0/0/1.200. Record the second IP address in the Address Table for S1 VLAN 1 and enter the associated default gateway.

c. One subnet, “Subnet C”, supporting 12 hosts (the client network at R2).

Subnet C:

© 2017 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Record the first IP address in the Addressing Table for R2 G0/0/1.

Step 2: Cable the network as shown in the topology.

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

Step 3: Configure basic settings for each router.

a. Assign a device name to the router.

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

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

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

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

f. Encrypt the plaintext passwords.

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

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

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

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.

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.

c. Verify the sub-interfaces are operational.

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.

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

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

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

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

Step 6: Configure basic settings for each switch.

a. Assign a device name to the switch.

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

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

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

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

© 2017 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

f. Encrypt the plaintext passwords.

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

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

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

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

j. Copy the running configuration to the startup configuration.

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.

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.

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

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.

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.

b. Verify that the VLANs are assigned to the correct interfaces.

Why is interface F0/5 listed under VLAN 1?

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.

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

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

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

e. Verify trunking status.

At this point, what IP address would the PC's have if they were connected to the network using DHCP?

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.

© 2017 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

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

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

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

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

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

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.

Step 2: Save your configuration

Save the running configuration to the startup configuration file.

Step 3: Verify the DHCPv4 Server configuration

a. Issue the command **show ip dhcp pool** to examine the pool details.

b. Issue the command **show ip dhcp bindings** to examine established DHCP address assignments.

c. Issue the command **show ip dhcp server statistics** to examine DHCP messages.

Step 4: Attempt to acquire an IP address from DHCP on PC-A

a. Open a command prompt on PC-A and issue the command **ipconfig /renew**.

b. Once the renewal process is complete, issue the command **ipconfig** to view the new IP information.

c. Test connectivity by pinging R1's G0/0/1 interface IP address.

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.

b. Save your configuration.

Step 2: Attempt to acquire an IP address from DHCP on PC-B

a. Open a command prompt on PC-B and issue the command **ipconfig /renew**.

b. Once the renewal process is complete, issue the command **ipconfig** to view the new IP information.

c. Test connectivity by pinging R1's G0/0/1 interface IP address.

d. Issue the **show ip dhcp binding** on R1 to verify DHCP bindings.

e. Issue the **show ip dhcp server statistics** on R1 and R2 to verify DHCP messages.

© 2017 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

www.netacad.com