Activity 8.2 - Designing Subnetted IPv4 Addressing Scheme

ON-CAMPUS

Objectives

Part 1: Design Network Subnetting Schemes

Part 2: Configure Devices

Part 3: Test configuration

Background / Scenario

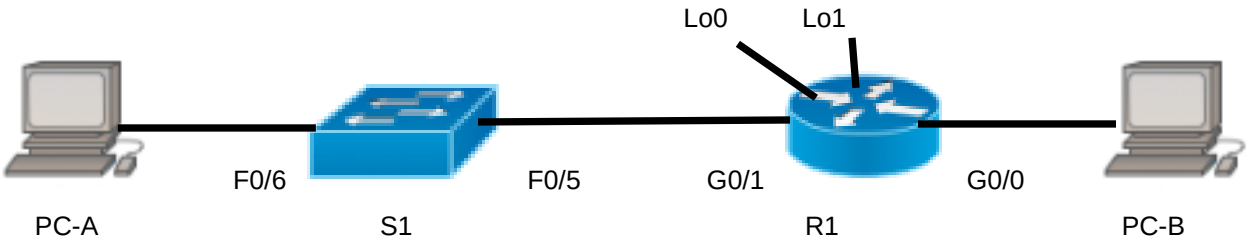
In this lab, starting from a single network address and network mask, you will subnet the network into multiple subnets. The subnet scheme should be based on the number of host computers required in each subnet, as well as other network considerations, like future network host expansion.

Part 1: Create a subnetting scheme that meets the required number of subnets and required number of host addresses.

In this scenario, you are a network administrator for a small subdivision within a larger company. You must create multiple subnets out of the 172.6.0.0/16 network address space to meet the following requirements:

- The first subnet is the employee network. You need a minimum of 612 host IP addresses.
- The second subnet is the administration network. You need a minimum of 491 IP addresses.
- The 3rd, and 4th subnets are reserved as virtual networks on virtual router interfaces, loopback 0 through loopback 1. These virtual router interfaces simulate LANs attached to R1.
- You also need 2 additional unused subnets for future network expansion.

Note: Variable length subnet masks will NOT be used. All of the device subnet masks will be the same length.



Calculating subnet information:

How many host addresses are needed in the largest required subnet? _____

What is the minimum number of subnets required? _____

How many subnetwork bits do you need to satisfy the number of networks required? _____

How many host bits do you need to satisfy the largest network? _____

Which subnet mask supports both the required number of subnets and hosts using the minimum number of host bits? _____

What is the binary value for that subnet mask? _____

What is the magic number? _____

When you have determined which subnet mask meets all of the stated network requirements, you will derive each of the subnets starting from the original network address. List the subnets from first to last below. Remember that the first subnet is 172.6.0.0 with the newly acquired subnet mask.

Subnet Address	/	Prefix	Subnet Mask (dotted decimal)
_____	/	____	_____
_____	/	____	_____
_____	/	____	_____
_____	/	____	_____
_____	/	____	_____
_____	/	____	_____
_____	/	____	_____
_____	/	____	_____
_____	/	____	_____
_____	/	____	_____

On the router:

G0/1 is the first network. Its IP address is the first available address on this network.

G0/0 is the second network. Its IP address is the first available address on this network.

Lo1 is the third network. Its IP address is the first available address on this network.

Lo0 is the fourth network. Its IP address is the first available address on this network.

On the Switch:

The Switch is attached to the G0/1 interface and is part of that network. Its VLAN 1 IP address will be the last available address on that network. Its default gateway will be the G0/1 interface.

On PC-A:

PC-A is attached to the network connected to the G0/1 interface and is part of that network. Its IP address will be the second available address on that network. Its default gateway will be the G0/1 interface.

On PC-B:

PC-B is attached to the network connected to the G0/0 interface and is part of that network. Its IP address will be the second available address on that network. Its default gateway will be the G0/0 interface.

Fill in the table with appropriate IP addresses and subnets masks in slash prefix notation.

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0			N/A
	G0/1			N/A
	Lo0			N/A
	Lo1			N/A
S1	VLAN 1			
PC-A	NIC			
PC-B	NIC			

Part 2: Configure the Devices

In Part 2, set up the network topology and configure settings on the PCs, Switch and router, such as the router Gigabit Ethernet interface IP addresses, and the PC's IP addresses, subnet masks, and default gateways. Refer to the Addressing Table for device names and address information:

a. Fully configure the switch as per the standard configuration steps discussed in previous labs. Please do not save the configuration:

1) Correct device names as per the topology
2) DNS lookup turned off
3) IP address as listed in Addressing Table
4) Configure the default gateway for the Switch
5) Clear text passwords encrypted.
6) **cisco** as the console and vty passwords with login and logging synchronous enabled
7) **class** as the privileged EXEC password
8) Banner that warns anyone accessing the device that unauthorized access is prohibited. With the following text:

Unauthorised access is prohibited and will be prosecuted.

b. Configure the router:

Configure the routers as per the standard configuration in previous labs:

1) Assign a device name to the router.
2) Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
3) Assign **class** as the privileged EXEC encrypted password.
4) Assign **cisco** as the console password and enable login.
5) Assign **cisco** as the VTY password and enable login and logging synchronous. Verify the number of vty lines on the router.
6) Encrypt the clear text passwords.
7) Create a banner that warns anyone accessing the device:

Unauthorised access is prohibited and you will be prosecuted.

8) Assign *IPv4* addresses to all interfaces on Router as per the addressing table and enable them.

Step 2: Configure the PC interfaces.

a. Configure the IP address, subnet mask, and default gateway settings on PC-A.

b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Part 3: Test and Troubleshoot the Network:

Use appropriate commands to verify the configuration