Lab 5
Network Device Configuration and Switch Forwarding

Prof. Kredo

Due: Start of lab Friday, February 27

Name:	
Name:	

Introduction

In this lab you will accomplish several goals:

- Learn to configure and connect network switches
- Begin to study how switches forward traffic
- Experiment with forwarding tables in switches

Work in pairs for this lab using the equipment at your desk. Distribute the work evenly to make sure both group members know the material, as you will be required to know the material for evaluation.

1 Prelab [10 Points]

Executing the `ping` utility causes the host to send a *unicast* packet, called the request, to the destination specified on the command line. If the ping request arrives at the destination, a ping reply is sent as a *unicast* packet back to the host that sent the ping request. Assume three hosts, `A`, `B`, and `C`, are connected to the same switch and the switch's forwarding table is empty.

1. If `A` pings `B`, what packets, if any, does `C` receive?

2 Switch Connection and Management [40 Points]

This section details how you can configure the switches for your desk. Connect your hosts to the same switch and that switch to the INT network.

2.1 Switch Login and Command Line

The network switches used in this class are not simply passive devices. You can connect to them to perform configuration, read status information, and perform network diagnostics through the switch's console port. Switches with this functionality are called managed switches. A console port is a special interface used solely for configuration and management. You can connect to a switch's console port by opening a terminal and using the `telnet` command. (Technically, you are connecting to a special router configured as a terminal server and the terminal server is forwarding commands and responses between you and the switch.) `telnet` takes two arguments for our uses today, the first is the device address you wish to connect to and the second is a port number. The login password for the switches is `chico`. Below is an example login sequence that desk N would use; replace the address and port numbers with those for your desk from the sheet posted in lab. You may have to hit return to get the Password prompt. Only one telnet connection can be made to a switch at any time, but a single host can telnet to multiple switches simultaneously.

```
student@N1host>telnet 10.12.100.17 2002
Trying 10.12.100.17, 2002 ... Open

User Access Verification

Password: chico  ### <- this won't appear as you type it
NS2>
```

You are now in the command line for the switch. Here you can enter commands to configure your switch and find the current status. A helpful tool in the command line is the command line helper, which is accessed by typing `?` (a question mark). Do that now.

1. How many commands are available to you?

The command line helper can also give you hints on what to type next in a command sequence. Explore this by typing `show ?` on the command line. `show` is the command to display information from the switch. Using the command line helper, find and enter the command to display the system hardware and software status.

2. What version of the Cisco IOS software does your switch run? What is the uptime for your switch?

2.2 Privileged Mode

While the current command line is helpful, it does not allow you to perform some operations. To be able to enter all possible commands into the switch, you must be in privileged mode. Enter privileged mode by typing `enable` on the command line. The password to enter the privileged mode is the same as the login password, `chico`.

1. How many commands are available to you now?

Explore with the command line helper and find the command that will show you the MAC address table for the switch and enter it on the command line.

2. What command did you enter?

3. From looking at the table, what are the MAC addresses for your hosts (PCs)? By looking at the table, which physical ports are your hosts connected to?

Verify you are correct by checking with `ip` on your hosts and by examining your switch ports.

2.3 Switch Reset

The switches at your desk do not reset or reboot by default, so you need to manually configure them each time you use them in experiments to ensure they are configured as you desire. The directions required to reset the devices are available in three places:

1. When connected to the INT network, open `http://10.12.0.2` in a web browser.
2. Posted on the lab bulletin board.
3. On Learn under the Lab heading.

Follow the reset instructions to reset your devices to the default state. If you fail to do this, your switches may have an old configuration and corrupt your results.

You must reset your devices **at the start of each lab session** by following these steps.

1. Connect your hosts to the INT network and configure their network interfaces.
   - You can ping 10.12.0.2 to verify your network is setup correctly.
   - If you are unable to ping any device and your configuration looks good, try using different switch ports; the switch may be configured to prevent the setup you're using.
2. Follow the directions posted to reset your switch, and in general all the devices you use.

Practice resetting your switches now. You will do this operation many times this semester, so become adept at it.

3 Switch Forwarding [40 Points]

As discussed in class, switches have several advantages over hubs, which you will now examine.

Start Wireshark on one host and begin a new packet capture trace. On the other host, begin to ping 10.12.0.2 and let it run in the background (don't use the `-c` argument). Be sure to start Wireshark before you `ping`. You may want to try the experiment a few times to ensure you get the correct results; between each experiment disconnect the host that `ping`s from the switch, wait one minute, reconnect the host that `ping`s, and try again.

1. Describe the pings you see. Do you see all the pings, some of the pings, none of the pings?

2. Does this match your expectations from the prelab? If not, what was different?

Stop your pings to 10.12.0.2 by entering `^C` (hold control and press 'c').

Use PC2 to telnet into your switch and enter privileged mode. You need to configure the forwarding table timeout values for your switch so that entries are removed quickly. Find the default forwarding table timeout values for your switch. (HINT: The command is very similar to the command that displays the forwarding table.)

3. What is the default timeout period?

The default value is too large for this lab. Enter configuration mode with the command `configure terminal` and change the timeout value to 30 s. The command is very similar to the command that displays the timeout value.

4. What command did you use while in configuration mode?

Exit configuration mode and examine the forwarding table for your switch.

5. How many addresses has your switch learned (ignoring addresses with the port `CPU`)?

`ping` PC1 from PC2 and then examine the forwarding table for your switch. Verify the switch learns the address for PC1 by using `ip` on PC1. Let PC1 remain idle so its forwarding table entry times out. Verify the forwarding table entry for PC1 is gone by using PC2.

4 Switch Port Monitoring [10 Points]

While switches improve network performance by selectively forwarding packets, sometimes you may want to temporarily fall back to the eavesdropping behavior of hubs. This functionality is called port monitoring or port mirroring.

You will now enable monitoring to see how it works with your switches. Select one host to be monitored (the source) and use the other host to perform the monitoring (the destination). The destination eavesdrops on the source. Fill in the table below with your selection.

	Source/Destination	**Switch Port Number**
PC 1		
PC 2		

Have the **source** host login to the switch and enter privileged mode. Enable monitoring by entering the following commands after replacing the unknown entries with the appropriate values. The source port should be the port leading to the monitoring source and the destination port is the port leading to the monitoring destination.

```
NS2#configure terminal
NS2(config)#monitor session 1 source interface <port> both
NS2(config)#monitor session 1 destination interface <port>
NS2(config)#exit
```

On the monitoring destination, start a new packet capture trace. From the monitoring source, ping 10.12.0.2. If you do not see the packets between the monitoring source and 10.12.0.2 at the monitoring destination, ask for assistance.

1. What do you think the switch is doing when port monitoring is enabled?

Turn off port monitoring by entering:

```
NS2#configure terminal
NS2(config)#no monitor session 1
NS2(config)#exit
```

If you desire, repeat the procedure by reversing the host roles.

5 Lab 5 Addresses

	Host Addresses	
Desk	**PC 1**	**PC 2**
A	10.12.50.101	10.12.50.201
B	10.12.50.102	10.12.50.202
C	10.12.50.103	10.12.50.203
D	10.12.50.104	10.12.50.204
E	10.12.50.105	10.12.50.205
F	10.12.50.106	10.12.50.206
G	10.12.50.107	10.12.50.207
H	10.12.50.108	10.12.50.208

	Host Addresses	
Desk	**PC 1**	**PC 2**
I	10.12.50.109	10.12.50.209
J	10.12.50.110	10.12.50.210
K	10.12.50.111	10.12.50.211
L	10.12.50.112	10.12.50.212
M	10.12.50.113	10.12.50.213
N	10.12.50.114	10.12.50.214
O	10.12.50.115	10.12.50.215