CSE 4512 [Computer Networks Lab]

Lab # 02

1. Objectives:

- Understand the working principle of a network simulator (Cisco Packet Tracer)
- Download and install Cisco Packet Tracer
- Understand the packet tracer environment Learn how to set up routers and switches
- Connect multiple networks using static routing
- Get to know Secure Shell (SSH) and Telnet basics

2. Introduction:

In this lab (meaning the whole semester), you'll be working on simulating different real-life networks and understand the networking concepts introduced in the theory course. Over the course of completing each lab, you will get to know how various protocols and mechanisms work and also you'll have an idea on how to operate an industry-standard network simulator. A network simulator is basically a software that allows users to create and analyze computer networks. One can create different network topologies and understand how various components of a network interact with each other. These are used in both academia and industry to understand system behavior without requiring any physical network component.

In all of the labs, you'll be working with a specific network simulator called **Cisco Packet Tracer**. There are also other network simulators like GNS3, NS2 etc. But we've selected Cisco Packet tracer for its large adoption across the industry and widely available documentation. We believe, by being acquainted and well-versed with this network simulator, students will acquire fundamental knowledge of modern network components and as a bonus, will have easier time acing the different Network Professional (CCNA, CCNP etc.) certifications that require working with Cisco Packet Tracer.

Some quick points about the labs:

- Skim the whole pdf before starting the tasks.
- Concepts and tasks introduced in each lab will be needed for completing next labs. So make sure you fully understand each lab and don’t skip any lab.
- Do not copy and paste from your fellow classmates. You may discuss with them but the tasks must be done by yourself and the corresponding lab report must be your own production. You might take help from online resources but Do Not Copy and Paste. In case of online resource, please give a reference. It doesn't cost any to acknowledge someone's work.
- In case of any problem or query, feel free to ask/contact the instructors.

3. Theory:

In this lab, you'll be implementing basic switch and router configuration in cisco packet tracer. So, before anything, lets first understand what a router and a switch is.

Switch:

A switch operates in the data-link layer and is responsible for connecting different devices in a *single network*. As with any data-link layer device, a switch sends and receives data in *frames*. In general, switches use *MAC addresses* for forwarding data and these are restricted to wired connections only.

Router:

Router operates in the network layer and connects *different networks* together to form inter-networks. Routers unit of data is a *packet* and *IP addresses* are used to forward data packets. Unlike switches, routers can work with both wired and wireless connections.

Figure 1: Router and switch in real-life (leftmost two) and inside Cisco Packet Tracer (rightmost two)

Now that you've got an idea about switch and router, let's get your hands dirty.

Telnet and SSH:

Telnet is an application protocol for communication between two end devices which enables virtual access to a remote device. It's a bi-directional client-server protocol i.e., both sides can communicate interactively with one another. The standard TCP port for Telnet is 23. A user can log in to a remote server and interact with it using this protocol. Major drawback of this protocol is that all the communication happens in plain text which enables an attacker to see through any telnet communication by intercepting the packets and makes it possible to capture the password and get access to the remote device.

Secure Shell Protocol (SSH) have now become the application protocol of choice for communicating with remote resources as it provides an encrypted channel between the two ends. It also provides remote authentication and allows for remote administration. The standard TCP port for SSH is 22. In order for SSH to work, both the parties must agree on a common encryption technique. Further communication happens based on the agreed encryption technique.

4. Downloading and installing Cisco Packet Tracer:

I. For downloading the software, you need to create an account on Cisco Networking Academy or Cisco Netacad for short. Goto https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer and sign-up.

II. Then head over to https://www.netacad.com/portal/resources/packet-tracer to download the most recent version (which is 8.0 at the time of writing) of packet tracer. Make sure you select the *right OS version* for the software.

III. Now, open the downloaded exe file and follow the prompts to complete the installation. In case of any problem while installing, consult with the instructor or just google.

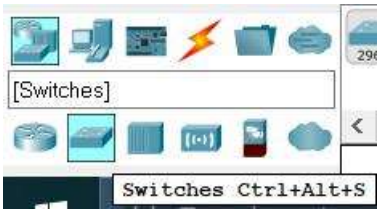
IV. After installation, you should login as normal user with the credentials used to sign-up in step I. Its recommended not to use the guest user as you can only save 3 files with it.

V. Assuming you've followed everything properly, you are now ready to start the actual work.

5. Basic Switch Configuration:

Now you'll configure a switch inside the cisco packet tracer. Note that all the commands used below will only work in case of cisco devices. One important point while working in packet tracer is that it supports *tab completion*, meaning if you press tab key after typing only some initial letters of a command then it will be auto completed. Also if you just type in a portion of a command it will work as long as the portion you typed is not ambiguous. For example, the command *configure terminal* will also work if you just type *conf t*.

I. Select a switch in the left-most pane of the packet tracer window under Network Devices category and drag it into the workspace. Remember that you can see the name of a component by just hovering over it.



II. If you hover over the switch you will see a list of interfaces, their status (up/down), MAC address etc. This info will come in handy while setting up the network.

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	1	--	0050.0F05.5201
FastEthernet0/2	Down	1	--	0050.0F05.5202
FastEthernet0/3	Down	1	--	0050.0F05.5203
FastEthernet0/4	Down	1	--	0050.0F05.5204
FastEthernet0/5	Down	1	--	0050.0F05.5205
FastEthernet0/6	Down	1	--	0050.0F05.5206
FastEthernet0/7	Down	1	--	0050.0F05.5207
FastEthernet0/8	Down	1	--	0050.0F05.5208
FastEthernet0/9	Down	1	--	0050.0F05.5209
FastEthernet0/10	Down	1	--	0050.0F05.520A
FastEthernet0/11	Down	1	--	0050.0F05.520B
FastEthernet0/12	Down	1	--	0050.0F05.520C
FastEthernet0/13	Down	1	--	0050.0F05.520D
FastEthernet0/14	Down	1	--	0050.0F05.520E
FastEthernet0/15	Down	1	--	0050.0F05.520F
FastEthernet0/16	Down	1	--	0050.0F05.5210
FastEthernet0/17	Down	1	--	0050.0F05.5211
FastEthernet0/18	Down	1	--	0050.0F05.5212
FastEthernet0/19	Down	1	--	0050.0F05.5213
FastEthernet0/20	Down	1	--	0050.0F05.5214
FastEthernet0/21	Down	1	--	0050.0F05.5215
FastEthernet0/22	Down	1	--	0050.0F05.5216
FastEthernet0/23	Down	1	--	0050.0F05.5217
FastEthernet0/24	Down	1	--	0050.0F05.5218
GigabitEthernet0/1	Down	1	--	0050.0F05.5219
GigabitEthernet0/2	Down	1	--	0050.0F05.521A
Vlan1	Down	1	<not set>	0001.C9D0.ADE1

Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

III. Now, select the switch in the workspace and you'll see 4 different tabs namely *Physical*, *Config*, *CLI* and *Attributes*. For the most part of our work, you'll be working with the CLI tab. you can write different commands here and those will be executed directly on the switch.

IV. Intially the CLI prompt will be like following:

```
Switch>
```

V. For configuring the switch, you need to enter *privileged mode* by typing the following:

```
Router> enable
```

```
Router#
```
You'll notice that the > symbol after `Router` is changed to # to indicate privileged mode.

VI. All the commands needed to setup a cisco device are stored in configuration files. There are mainly two of these: *startup-config* and *running-config*. running-config is stored in device's RAM and is lost whenever the device is switched off. startup-config is stored in NVRAM or non-volatile ram and all configuration changes are saved even if the device loses power. So, whenever you are done with configuration changes, you need to save it to startup-config so that when the device boots later the changes are retained. To view the configs, type in the following:

```
Switch# show running-config
Switch# show startup-config
```
Note that, at the very first, there won't be any startup-config. Only a basic running-config will be available.

VII. Now, enter into Global Configuration Mode. This mode allows users to modify the running-config.

```
Switch# configure terminal
Switch(config)#
```

VIII. Give the switch a *hostname*.
```
Switch(config)# hostname IUT
IUT(config)#
```
Note that, the commands in cisco are not case-sensitive, meaning you could also use *HOSTNAME* instead of *hostname*.

IX. Define a password for the switch. This will prevent any unauthorized access.
```
IUT(config)# enable password cisco
IUT(config)# enable secret cisco
```
cisco is the password here. Notice that there are two commands. The first one is unsafe to use because it stores the password in plain text. The second one with secret is the recommended way to enable password as it stores the md5 hash of the given password. You can view the password in running-config. Note that, if run both of the above commands, the second one will get priority.

X. Each cisco device has a single console port. Configure the *console* port to restrict unauthorized access. Console port is used to access the switch locally.
```
IUT(config)# line console 0
```
As there's only a single console port, the port number is 0 (numbering starts from 0).

```
IUT(config-line)# password
class
```
class is the password.

```
IUT(config-line)# login
```
This command enables password check at login time and verifies that the password is working.

XI. Configure the *vty* line. Vty stands for virtual teletype. It's a virtual port and used for remotely accessing the device through telnet and ssh.

```
IUT(config)# line VTY 0 4
```
0 4 means allow 4 simultaneous connections to vty in ports 0 through 4.

```
IUT(config-line)# password class
IUT(config-line)# login
```
The following commands define which protocol to allow through vty line connection.

```
IUT(config-line)# transport input telnet
```
It allows only telnet.

```
IUT(config-line)# transport input ssh
```
It allows only ssh.

```
IUT(config-line)# transport input all
```
It allows all supported protocols.

XII. Though switches operate using MAC addresses, switches need IP address for switch management or to use protocols like SNMP. For this, you need to configure a *VLAN*.
```
IUT(config)# interface vlan 1
```
1 specifies the vlan id which uniquely represents the vlan.

```
IUT(config-if)# ip address 192.168.10.1 255.255.255.0
```
Specify the ip address and subnet mask for the vlan.

```
IUT(config-if)# no shutdown
```
This command will activate the vlan.

```
IUT(config-if)# description LAN-IUT
```
Add a description for the vlan.

XIII. As a security best-practice, enable encryption on all passwords on this switch.
```
IUT(config)# service password-encryption
```

XIV. Define a *banner* message. Banner is basically a message that a cisco device shows when a user connects to it.
```
IUT(config)# banner motd #Authoized Access Only!!#
```
motd represents *message of the day* banner. This particular banner is shown to everyone connecting to the switch. Remember to enclose the banner string inside # symbol.

XV. You're at the end of basic switch configuration. As mentioned in step VI, to make all the changes you did till now persistent, the running-config has to be saved in startup-config. This is done by the following command:
```
IUT# copy running-config startup-config
```

XVI. Now you can view the running-config as well as startup-config by entering commands in step VI.

XVII. Some interface related commands:

```
IUT# show interface
IUT# show ip interface brief
IUT# show interface <interface name>
IUT# show interface status
```

6. Basic Router Configuration:

I. Select a router from the left-most pane as before the switch.

II. Hover over the router to view information about various interfaces and their status.

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Down	--	<not set>	<not set>	0090.0CB0.DD01
GigabitEthernet0/1	Down	--	<not set>	<not set>	0090.0CB0.DD02
GigabitEthernet0/2	Down	--	<not set>	<not set>	0090.0CB0.DD03
Vlan1	Down	1	<not set>	<not set>	0002.4AAB.987E

Hostname: Router

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

III – X. Same as steps III-X of switch.

XI. Configure the interfaces. Remember that a router can have multiple interfaces and you'll need to configure each one separately. While doing the tasks, follow given network specification carefully to properly assign the ip addresses to the router interfaces. This is where most students get stuck. And remember to use the tab completion feature because you'll need it a lot at this step.

```
IUT(config)# interface fastEthernet 0/0 IUT(config-
if)# ip address 192.168.11.1 255.255.255.0
IUT(config-if)# no shutdown IUT(config-if)#
description LAN-NORTH-HALL
```

```
IUT(config)# interface gigabitEthernet 0/0
IUT(config-if)# ip address 192.168.12.1 255.255.255.0
IUT(config-if)# no shutdown IUT(config-if)#
description LAN-SOUTH-HALL
```

```
IUT(config)# interface serial 0/0/0
```

```
IUT(config-if)# ip address 192.168.13.1 255.255.255.0
IUT(config-if)# no shutdown

IUT(config)# interface VLAN 1 IUT(config-if)# ip
address 192.168.10.5 255.255.255.0 IUT(config-if)# no
shutdown IUT(config-if)# description VLAN-Management
```

XII. Enable encryption on all passwords as like the switch.

XIII. Provide a banner message same as before with the switch.

XIV. You can specify a username and password for extra layer of security.

```
IUT(config)#  username cse password iut
```

XV. Finally, its time to save the running-config to startup-config as like before.

```
IUT# copy running-config startup-config
```

XVI. Interface related commands for a router are same as switch.

7. Basic Telnet and SSH configuration:

I. Configure the vty line. Vty stands for virtual teletype. It's a virtual port and used for remotely accessing the device through telnet and ssh.

```
IUT(config)# line VTY 0 4
```

0 4 means allow 4 simultaneous connections to vty in ports 0 through 4.

(Switch(config)# line VTY 0 15)

```
IUT(config-line)# password class
```

class is the password

```
IUT(config-line)# login
```

This command enables password check at login time and verifies that the password is working.

The following commands define which protocol to allow through vty line connection.

```
IUT(config-line)# transport input telnet
```

It allows only telnet.

```
Or
IUT(config-line)# transport input ssh
```

It allows only ssh.

```
Or
IUT(config-line)# transport input all
```

It allows all supported protocols.

II. Configure the Interfaces (FastEthernet or GigabitEthernet or VLAN):

```
IUT(config)# interface fastEthernet 0/0
IUT(config-if)# ip address 192.168.10.1 255.255.255.0
IUT(config-if)# no shutdown
IUT(config-if)# description LAN-NORTH-HALL

IUT(config)# interface gigabitEthernet 0/0
IUT(config-if)# ip address 192.168.11.1 255.255.255.0
IUT(config-if)# no shutdown
IUT(config-if)# description LAN-SOUTH-HALL

IUT(config)# interface serial 0/0/0
IUT(config-if)# ip address 192.168.10.1 255.255.255.0
IUT(config-if)# no shutdown

IUT(config)# interface VLAN 1
IUT(config-if)# ip address 192.168.10.5 255.255.255.0
IUT(config-if)# no shutdown
IUT(config-if)# description VLAN-Student
```

III. Create Username and Password:

```
IUT(config)#  username admin password IUT
```

IV. Configuring SSH:

The following command will set the domain name for the Cisco router/switch. The SSH keys will be generated based on this domain name and also the host name.

```
IUT(config)# ip domain-name iut.com
```

The following command will generate RSA (a public-key cryptographic algorithm) key pairs for the device in use. Please make sure the domain name and hostname for the device is configured before issuing the command.

```
IUT(config)# crypto key generate rsa

How many bits in modulas [512]: 1024
```

Note that, the longer the modulus the stronger is the key. But longer modulus will take more time to generate the key.

```
IUT(config)# line VTY 0 4
                      (Switch(config)# line VTY 0 15)
IUT(config-line)# login local
```

This command tells the Router to authenticate all incoming virtual terminal sessions via the local username database i.e., users created using the *username* XXX *password* YYY command in global configuration mode. Whereas, the login command that we used in step 1 is used to authenticate against the password set inside line console or vty configuration mode.

```
IUT(config-line)# transport input ssh
```

Now, you can use telnet and ssh from a desktop connected with this cisco device.

For login using telnet from Command Prompt:

```
>telnet 192.168.11.1
```

For login using SSH from Command Prompt:

```
>ssh -l admin 192.168.11.1
```

Some final points to consider before moving on to the tasks:

- Make proper use of the tab completion feature.
- Look carefully at the prompt to understand what state you're in now. Not all states accept every command. For example, *(config-if)* tells that you're in interface setup mode. *(config-line)* means you're in line setup mode. Make sure the state you're in matches the command you're typing.
- Type *exit* at any state to move back to the previous state. Remember to run all commands in privileged mode.
- Type *end* to return to initial state in privileged mode.
- Follow the given network specification in the task very carefully.