Birzeit University
Faculty of Engineering and Technology
Electrical and Computer Engineering Department
ENCS413 – Computer Networks Laboratory

EXP. No. 2. Introduction to Cisco Packet Tracer - Static Routing Protocol

1. Objectives

- Learn how to configure a Cisco IOS router using the IOS command-line interface (CLI).
- Learn how to use a router simulator.
- Learn how to use the sniffer to capture packets in Packet Tracer.

2. Lab Requirements

- Two Cisco routers.
- Two PCs.
- One Sniffer.
- Two Cisco switches.
- Two CAT5 straight-wired cables.
- One Serial cable (male and female).

3. Pre-lab

- Install at home a simulator from CISCO called Packet Tracer (Latest version preferred).
- Review the subnetting and solve some examples about it.

4. Introduction

In the previous experiment, you built simple (single) networks in which you used TCP/IP to enable the devices in these networks to communicate with each other. To connect more than such networks, we need an entity in this network that is capable of delivering data packets from one network to the correct destination network. This device is called a router, its main role is to route packets to the correct destination. Traditionally, the router is called a layer-3 device. Therefore, it uses the IP address (layer-3 address) to build its path toward the destination. Each network is called a segment (subnet). The main reason for having subnets is to control the traffic. Each node in any segment can hear all packets transmitted by other nodes in the segment. Based on routing information (routing table), a router can determine the next node toward the destination. The router uses the destination IP address of the packet to find the correct path. There are two main types of routing protocols, static and dynamic. In static routing, it is the role of the administrator to update the router with new routing information (add a segment or remove a segment). In Dynamic routing, the routing information will be updated automatically.

4.1. Routing

The term *routing* is used for taking a packet from one device and sending it through the network to another device on a different network. Routers do not care about hosts—they are only used to get packets to a network through a routed network. Then, the hardware address of the host is used to deliver the packet from a router to the correct destination host. If your network has no routers, then it should be apparent that you are not routing. Routers route traffic to all the networks in your internetwork. To be able to route packets, a router must know, at a minimum, the following:

- Destination address.
- Neighbor routers from which it can learn about remote networks.
- Possible routes to all remote networks.
- The best route to each remote network.
- How to maintain and verify routing information.

4.2. Static Routing & Dynamic Routing

The router learns about remote networks from neighbor routers or an administrator. The router then builds a routing table that describes how to find the remote networks. If a network is directly connected, then the router already knows how to get to it. If a network is not connected, the router must learn how to get to the remote network in two ways: by using static routing, meaning that someone must hand-type all network locations into the routing table, or through something called dynamic routing.

4.2.1. Dynamic Routing

A protocol on one router communicates with the same protocol running on neighbor routers. The routers then update each other about all the networks they know about and place this information into the routing table. If a change occurs in the network, the dynamic routing protocols automatically inform all routers about the event. If static routing is used, the administrator is responsible for updating all changes by hand into all routers. Typically, in a large network, a combination of both dynamic and static routing is used.

4.2.2. Static Routing

Static routing occurs when you manually add routes in each router's routing table.

- Static routing has the following benefits:
  - There is no overhead on the router CPU, which means you could buy a cheaper router than if you were using dynamic routing.
  - There is no bandwidth usage between routers, which means you could save money on WAN links.
  - It adds security because the administrator can choose to allow routing access to certain networks only.

- Static routing has the following disadvantages:
  - The administrator must understand the internetwork and how each router is connected to configure routes correctly.
  - If a network is added to the internetwork, the administrator has to add a route to it on all routers—by hand.
  - It is not feasible for large networks because maintaining it would be a full-time job in itself.

The command syntax you use to add a static route to a routing table:

```
ip route <destination_network> <mask> <next-hop_address>
```

This list describes each command in the string:

- **`ip route`:** The command used to create the static route.
- **`destination_network`**: The network you are placing in the routing table.
- **`Mask`:** The subnet mask being used on the network.
- **`next-hop_address`:** The address of the next-hop router that will receive the packet and forward it to the remote network. This router interfaces on a directly connected network. You must be able to ping the router interface before you add the route. If you type in the wrong next-hop address, or the interface to that router is down, the static route will show up in the router's configuration, but not in the routing table.

4.2.3. Packet Sniffing

Packet sniffing is a technique used to monitor and analyze network traffic. It involves capturing data packets as they travel across a network. These packets contain information like source and destination IP addresses, protocols used, and actual data being transmitted.

Packet sniffers, like Wireshark or Packet Tracer's Simulation Mode, capture network packets and allow users to inspect their contents. Here's how it works:

- Capturing Packets – The sniffer listens to network traffic by placing a network interface in promiscuous mode (on wired networks) or monitoring Wi-Fi signals (on wireless networks).
- Decoding Data – Once captured, the tool breaks down packets into readable details, such as headers, payloads, and protocols used.
- Analyzing Network Activity – Users can filter packets to focus on specific traffic, detect errors, and analyze communication between devices.

Why is Packet Sniffing Useful?

Packet sniffing is widely used in IT and cybersecurity for:

- Troubleshooting Network Issues – Helps identify slow connections, dropped packets, and misconfigured devices.
- Security Monitoring – Detects suspicious activity, unauthorized data transfers, or potential cyber threats.
- Protocol Analysis – Examines how different network protocols operate and ensures they function correctly.

Cisco Packet Tracer includes a Simulation Mode, which allows users to inspect packets step by step as they move through the network. It helps students and professionals:

- Visualize Data Flow – Users can see how packets travel between devices.
- Inspect Packet Details – Clicking on a captured packet displays information such as source, destination, and protocol used.
- Understand Protocol Operations – By analyzing different protocol layers, users can learn how data is processed.

5. Procedure

In this lab, we will connect two routers and two PCs on different networks. This will require configuring routing protocols between the routers. We will configure static routing which will be used as a routing protocol.

The **IP addresses** must include the least significant two digits of your **Student ID**, as the example: Student ID: 1161378 … IP = 192.78.xx.xx /S.M.

5.1. Building the Topology:

5.1.1. Open Cisco packet tracer and set up the topology shown in Figure .1-2

- For the routers use Router-PT
- For the switches use Switch-PT
- For the PCs use PC-PT
- For the connections between the PCs, switches, and routers, use "Automatically use the connection type".

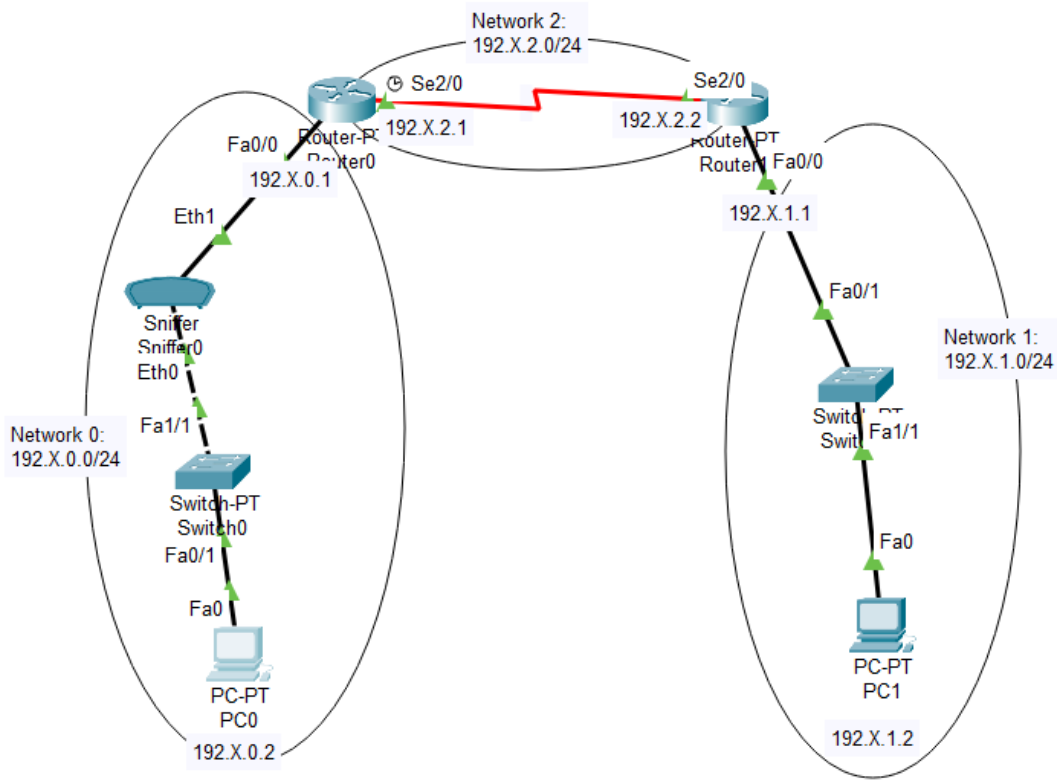

Figure 2-1: Topology

5.1.2. Configuring IPs for the PCs

- Click on the PC0 and go to the **Desktop** tab.
- Choose **IP configuration** to add an IP address for the PC as shown in Figure 2-2.

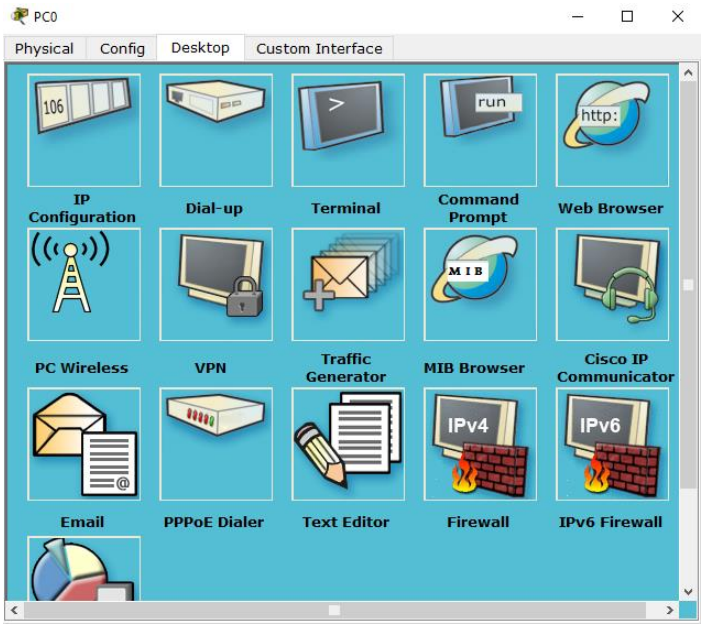

Figure 2-2*:* PC Desktop

- Add the following IP address (192. X.0.2/24) as shown in Figure 2-3.

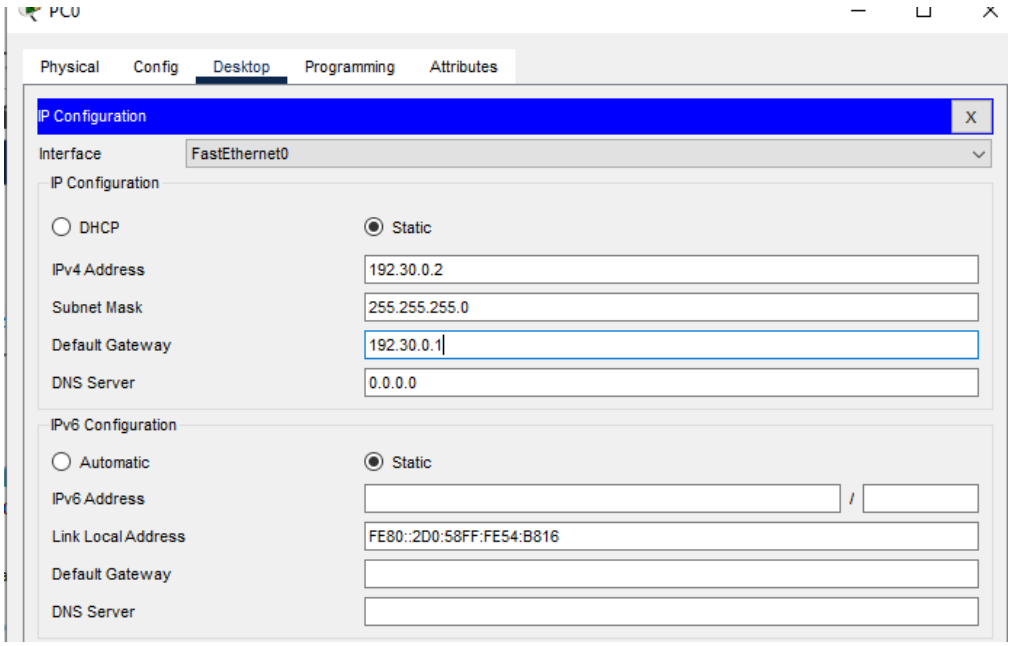

Figure 2-3: PC0 IP address

- **Repeat the previous steps for PC1 with the IP address 192. X.1.2/24**
  - **Note that subnet mask /24 is equivalent to 255.255.255.0**

5.1.3. Configuring IPs for the Routers

The router IPs and subnet masks for each interface are shown in Table 2-1.

Table 2-1: Routers IPs

Router	Interface	IP address	Subnet mask
Router 0	Fa0/0	192.X.0.1	255.255.255.0
	Se2/0	192.X.2.2	255.255.255.0
Router 1	Fa0/0	192.X.1.1	255.255.255.0
	Se2/0	192.X.2.1	255.255.255.0

- **Click on router 0 to configure the router.**
- **Go to the CLI tab as shown in Figure 2-4**.

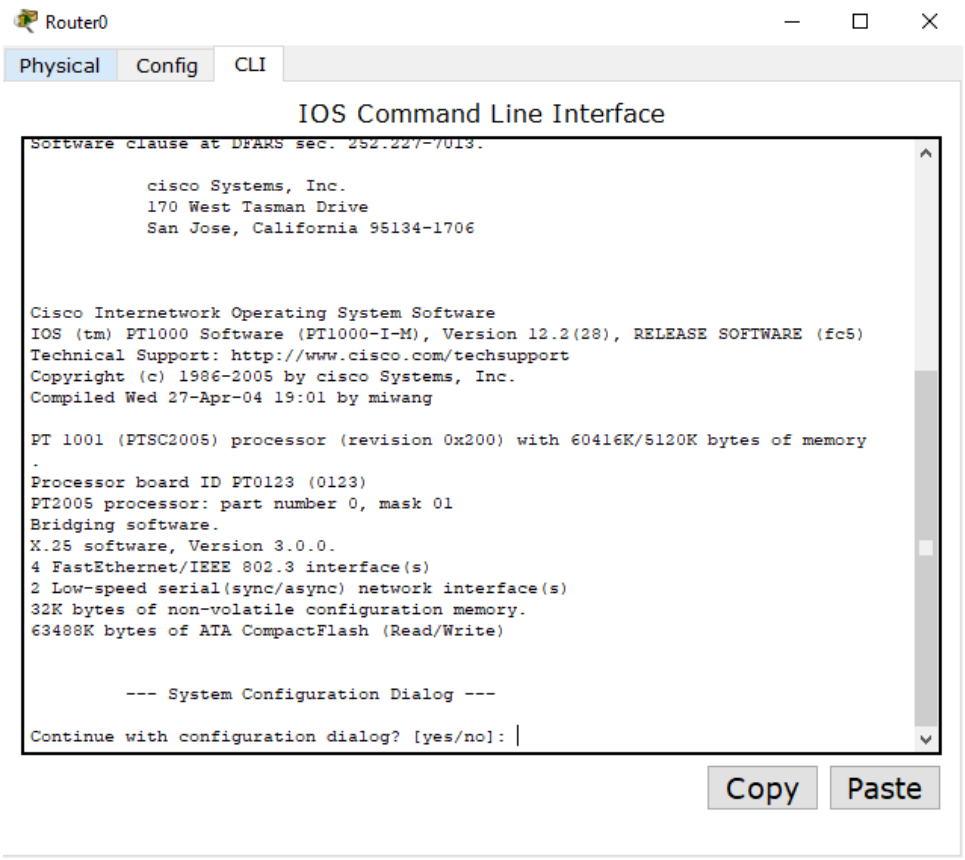

Figure 2-4: Router 0 CLI

- **Setup Mode and Command Line interface mode (CLI)**

A router initializes by loading the bootstrap, the operating system, and a configuration file. If the router cannot find a configuration file, then it enters setup mode. The router stores, in NVRAM, a backup copy of the new configuration from setup mode.

- The goal of the startup routines for Cisco IOS software is to start the router operations. The router must deliver reliable performance in its job of connecting the user networks it was configured to serve.
- To exit setup mode press **ctrl+Z**

Because it is so much more flexible, the command-line interface (CLI) truly is the best way to configure a router. Using CLI you can create advanced configurations on Cisco routers and switches. To use the CLI, just say "**No"** to enter the initial configuration dialog. After you do that, the router will respond with messages that tell you all about the status of each one of the router's interfaces. The router will show you the following.

```
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>
```

- **Logging into the Router**

After the interface status messages appear and you press Enter, the **Router>** prompt will appear. This is called user exec mode (user mode) and is mostly used to view statistics, but it is also a stepping-stone to logging into privileged mode. You can only view and change the configuration of a Cisco router in privileged exec mode (privileged mode), which you get into with the enable command. Here is how you would do that:

```
Router>
Router> enable
Router#
```

You now end up with a **Router#** prompt, which indicates you are in *privileged mode*, where you can both view and change the router's configuration. You can go back from privileged mode into user mode by using the **disable** command, as seen here:

```
Router# disable
Router>
```

At this point, you can type **logout** to exit the console:

```
Router> logout
```

After trying all these commands put the Cisco router in privileged exec mode (privileged mode). Using the enable command.

- **Overview of Router Modes**

To configure from a CLI, you can make global changes to the router by typing configure terminal (or **`config t`** for short), which puts you in global configuration mode and changes what is known as the running-config. A global command (a command run from global config) is set once and affects the entire router.

You can type **`configure`** from the privileged-mode prompt and then just press Enter to take the default of the terminal, as seen here:

```
Router#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

At this point, you make changes that affect the router as a whole, hence the term global configuration mode. To change the running-config—the current configuration running in dynamic RAM (DRAM) you use the configure terminal.

- **Router Interfaces**

To make changes to an interface, you use the interface command from global configuration mode, the configuration would be

```
interface <TYPE> <SLOT>/<PORT>
```

as seen here:

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#
```

Interface configuration is one of the most important router configurations because, without interfaces, a router is useless. In addition, interface configurations must be exact to enable communication with other devices. Some of the configurations used to configure an interface are

Network layer addresses, media type, bandwidth, and other administrator commands. Different routers use different methods to choose the interfaces used on them.

To exit the interface you can type the command:

```
Router(config-if)#exit
Router(config)#
```

Now it is time to choose the interface you want to configure. Once you do that, you will be in interface configuration for that specific interface. (choose the interface Fa0/0).

- **Bringing Up an Interface**

You can turn an interface off with the interface command **shutdown** and turn it on with the **no shutdown** command.

```
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN:    Line    protocol    on    Interface
FastEthernet0/0, changed state to up
```

Now the interface is up, we can add an IP address to that interface.

- **Configuring the first IP Address on an interface**

Even though you do not have to use IP on your routers, it is most often what people use. To configure IP addresses on an interface, use the command

```
ip address <IP-ADDRESS> <SUBNET-MASK>
```

from interface configuration mode for example to add the IP address 192.X.0.1/24 to the interface Fa0/0 use the command:

```
Router(config-if)#ip address 192.X.0.1 255.255.255.0
```

Make sure that you are in the correct interface before adding the IP address.

- **Now repeat Steps F – H for Router 0 and the second interface (Se2/0) with IP shown in Table 2-1.**
- **Now repeat Steps A – I for Router 1 using the correct IP addresses shown in Table 2-1.**

5.1.4. Configuring Static Routing

The command syntax you use to add a static route to a routing table:

```
ip route <destination_network> <mask> <next-hop_address>
```

To configure Router 0 to network 192.X.1.0/24 the following command is used:

destination_network: the network Router 0 is not connected to (192.X.1.0).

mask: the subnet mask being used on the destination network /24 (255.255.255.0**)**

next-hop_address: is the address of Se2/0 on Router 1 (192.X.2.1)

```
Router(config)#ip route 192.X.1.0 255.255.255.0 192.X.2.1
```

- **Now repeat this step 5.1.4 for router 1 with the correct addresses.**

5.1.5. Showing all router configurations to make sure everything is good

Go to the router setup and write the command

```
Router#show running-config
```

This will show you all the configurations for the router you have made.

5.1.6. Showing the routing table

To show the routing table for each router type

```
Router#show ip route
```

This will show you all the routing paths for the router

5.2. Verifying Your Configuration

Once all the routers' routing tables are configured, they need to be verified. The best way to do this, besides using the **`show ip route`** command, is with the **`ping`** program. By pinging from routers PC0 and PC1, the whole internetwork will be tested end-to-end.

Open PC0, go to desktop, command_prompt, and type

```
Ping <IP-ADDRESS>

 Ex: Ping 192.X.1.2
```

If the ping is working correctly then everything is configured well.

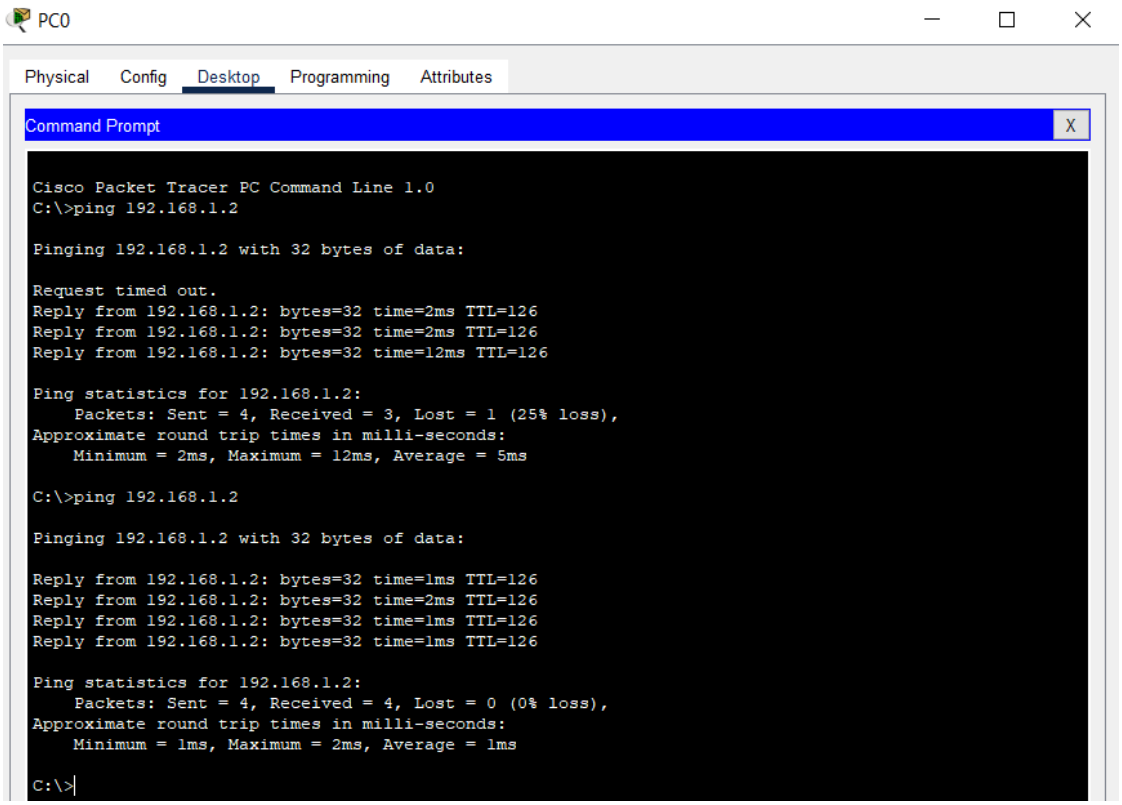

Figure 14: Pinging to test the connectivity

5.3. Packet Sniffing

Packet sniffing allows us to monitor and analyze network traffic by capturing packets as they travel between devices. In Cisco Packet Tracer, we used the **Sniffer** tool to visualize packet movement and understand how data flows through the network.

Go to **Sniffer → GUI → Service**, and toggle **Check On or Off** to enable or disable packet capturing. Then, select **Port 0 or 1** to determine which interface will be used to capture incoming packets. This setting allows you to control the direction and source of the captured traffic.

By default, the sniffer captures **all protocols**, but you can apply filters by;

- Clearing all incoming packets by clicking on ‘Clear’
- Clicking on ‘Edit Filters’ to focus on specific types of network traffic for more precise analysis.

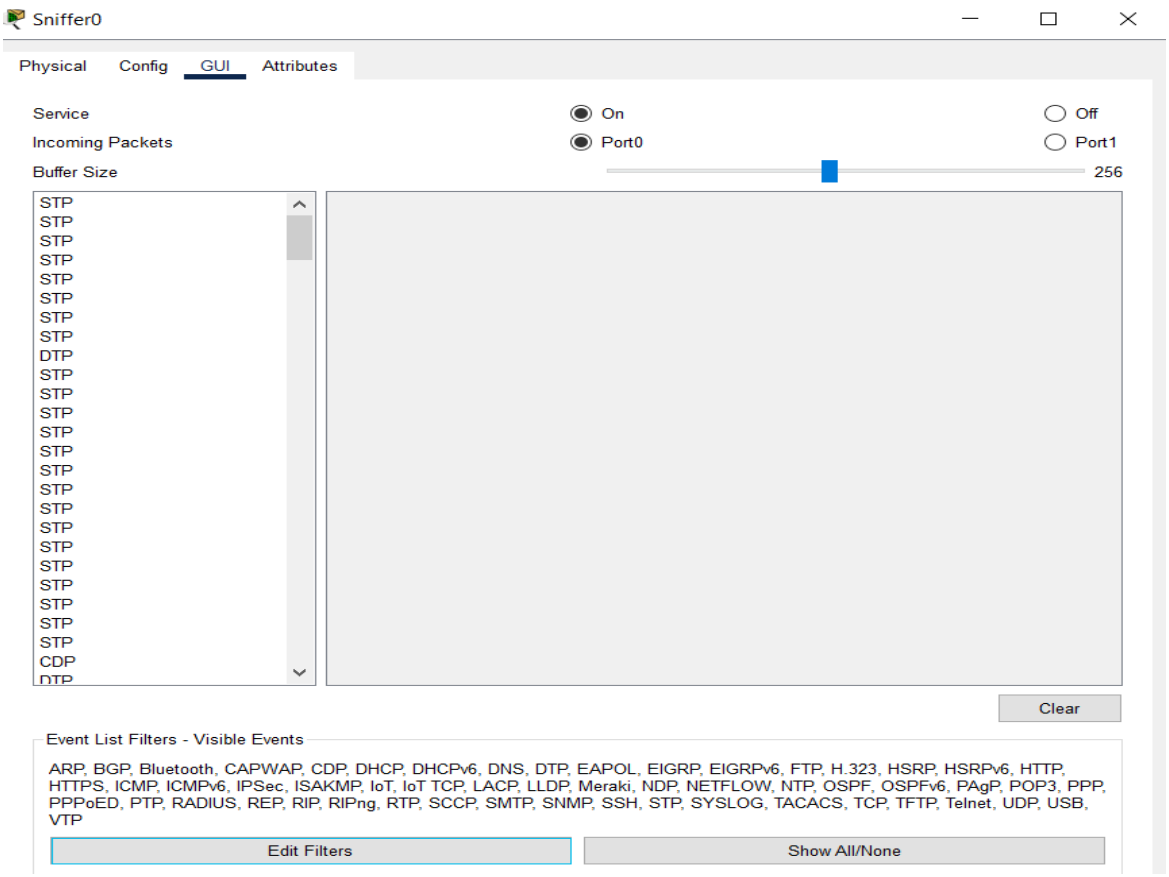

Figure 15: Capturing all Packets

We need to check **ICMP** because it is used for **ping** to test connections between devices. So, I filtered the packets to show only **ICMP**, making it easier to see if the ping works without other unnecessary data.

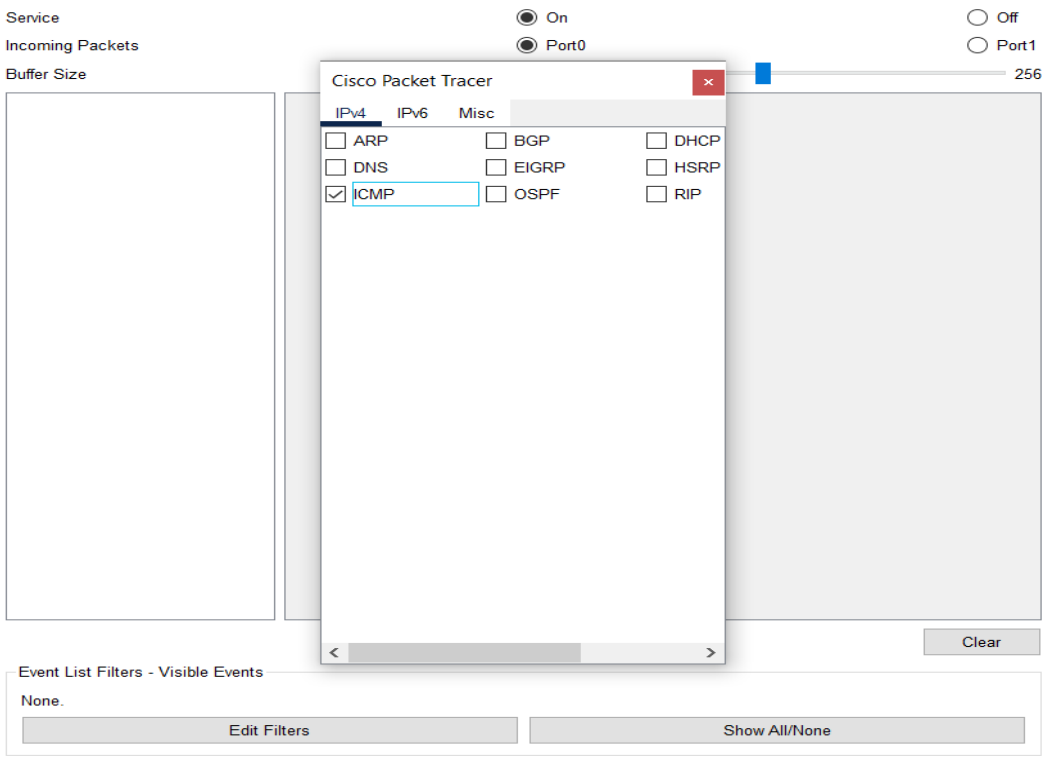

Figure 16 Applying Filter to Capture a Specific Protocol

Now, after specifying only ICMP to show and sending a packet from PC0 to PC1, we can click on the packet in the sniffer tool to examine its details. The packet details include the following information:

- **Source MAC Address**: This is the unique hardware address of the device that initiated the packet transmission, in this case, PC0. The MAC address is used at the Data Link Layer to ensure the packet reaches the correct device on the same local network.
- **Destination MAC Address**: This is the MAC address of the device that the packet is being sent to, in this case, PC1. The destination MAC address ensures the packet reaches the correct target device on the local network.
- **Source IP Address**: This is the IP address of the sender, which is PC0. The IP address operates at the Network Layer and is used for routing the packet across different networks. In this case, the IP address of PC0 is included to help identify the source device.

- **Destination IP Address**: This is the IP address of the recipient, which is PC1. The destination IP address is used by routers and other network devices to determine the final destination of the packet across different network segments.

Figure 17 Packet Details

To verify the source MAC address, we can click on PC0, go to the **Config** tab, select **FastEthernet**, and view the **MAC Address** field. The MAC address displayed here should match the source MAC address in the captured packet, confirming that the packet originated from PC0.

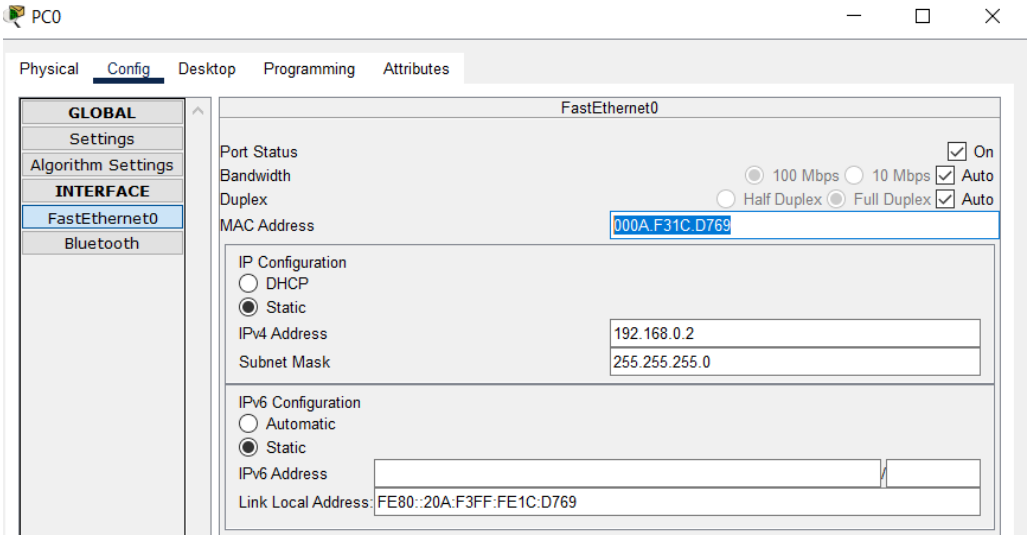

Figure 18 Source Mac Address for PC0

5.4. Other Important Configurations:

5.4.1. Editing and Help Features

You can use the Cisco advanced editing features to help you configure your router. If you type in a question mark (**?**) at any prompt. Here is a shortcut: To find commands that start with a certain letter, use the letter and the question mark with no space between them:

```
Router#c?
Clear clock configures connect copy
```

By typing **c?**, we received a response listing all the commands that start with *c*. To find the next command in a string, type the first command and then a question mark:

```
Router#clock ?
Set the time and date

Router#clock set ?
hh:mm:ss Current Time

Router#clock set 10:30:10 ?
<1-31> Day of the month
MONTH Month of the year

Router#clock set 10:30:10 28 ?
MONTH Month of the year

Router#clock set 10:30:10 28 january ?
<1993-2035> Year

Router#clock set 10:30:10 28 january 2020 ?
<cr>
```

By typing the **clock ?** command, you will get a list of the next possible parameters and what they do. Notice that you should just keep typing a command, a space, and then a question mark until <**cr**> (carriage return) is your only option.

Table 2-2: Enhanced Editing Command

Command	**Meaning**
Ctrl+P or up arrow	Shows last command entered
Ctrl+N or down arrow	Shows previous commands entered
show history	Shows last 10 commands entered by default
Ctrl+A	Moves your cursor to the beginning of the line
Ctrl+E	Moves your cursor to the end of the line

Esc+B	Moves back one word
Ctrl+F	Moves forward one character
Esc+F	Moves forward one word
Ctrl+B	Moves back one character
Ctrl+D	Deletes a single character
Backspace	Deletes a single character
Ctrl+R	Redisplays a line
Ctrl+U	Erases a line
Ctrl+W	Erases a word
Ctrl+Z	Ends configuration mode and returns to EXEC
Tab	Tab Finishes typing a command for you

5.4.2. Gathering Basic Routing Information

The show version command will provide basic configuration for the system hardware as well as the software version, the names and sources of configuration files, and the boot images. Here is an example:

```
Router#sh version
```

5.4.3. Serial Interface Commands

There are a couple of things you need to know. First, the interface will usually be attached to a CSU/DSU type of device that provides clocking for the line to the router. But if you have a back-to-back configuration (for example, one that is used in a lab environment), one end—the data communication equipment (DCE) end of the cable—must provide clocking. By default, Cisco routers are all data terminal equipment (DTE) devices, so you must tell an interface to provide clocking if you need it to act like a DCE device. You configure a DCE serial interface with the clock rate command:

```
Router#config t
Router(config)#int s1
Router(config-if)#clock rate ?
Router(config-if)#clock rate 64000
```

Here is an example of using the bandwidth command:

```
Router(config-if)#bandwidth <BANDWIDTH-IN-KILOBITS>
Router(config-if)#bandwidth 64
```

5.4.4. Hostnames

You can set the identity of the router with the **hostname** command. This is only locally significant, which means it has no bearing on how the router performs name lookups or how the router works on the internetwork. Here is an example:

```
Router#config t
Router(config)#hostname RouterA
RouterA(config)#hostname RouterB
RouterB(config)#
```

Even though it is pretty tempting to configure the hostname after your name, it is a better idea to name the router something pertinent to the location.

5.4.5. Passwords

You can secure your system by using passwords to restrict access. Passwords can be established both on individual lines and in the privileged EXEC mode.

- **line console 0** -- establishes a password on the console terminal
- **line vty 0 4** -- establishes password protection on incoming Telnet sessions
- **enable password** -- restricts access to privileged EXEC mode
- **enable secret** password (from the system configuration dialog to set up global parameters uses a Cisco proprietary encryption process to alter the password character string

A. Set your enable secret password by typing enable secret Cisco (the third word Cisco should be your personalized password) and pressing Enter.

B. Now let us see what happens when you log out of the router and then log in. Log out by pressing **Ctrl+Z**, then type exit and press Enter. Go to privileged mode. Before you are allowed to enter privileged mode, you will be asked for a password. If you successfully enter the secret password, you can proceed.

C. Remove the secret password. Go to privileged mode, type **config t**, and press Enter. Type no enable secret and press Enter. Log out and then log back in again, and now you should not be asked for a password.

D. To set the Telnet or VTY password, type line **`vty 0 4`** and then press Enter. The **`0 4`** is the range of the five available virtual lines used to connect with Telnet. If you have an enterprise IOS, the number of lines may vary. Use the question mark to determine the last line number available on your router.

E. One more command you need to set for your VTY password is password. Type password cisco to set the password. (cisco is your password.)

F. Here is an example of how to set the VTY passwords:

```
Router#config t
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
```

G. Set your console password by first typing **`line console 0`** or **`line con 0`**.

5.4.6. Viewing and Saving Configurations

If you run through setup mode, you will be asked if you want to use the configuration you just created. If you say Yes, then it will copy the configuration running in DRAM, (known as the running-config), into NVRAM, and name the file startup-config. You can manually save the file from DRAM to NVRAM by using the copy running-config startup-config command (you can use the shortcut copy run start also):

```
Router# copy run start
```

Also, you can type the command:

```
Router# write
```

This will save your configuration even when shutting down your router.

6. Todo

This part will be given to you by the instructor