# UNIVERSITY OF BARISAL


## Lab Report

Course Title : Computer Networks Lab

Course Code : CSE-3206

Submitted to

Md. Rashid Al Asif

Lecturer,

Dept. of Computer science and Engineering,

University of Barisal.

Submitted by

Name : Protap Mistry

Class Roll : 17CSE029

Exam Roll : CSE014/6

Session : 2016-2017

Semester: Second

Year : Third

Department: Computer Science and Engineering

Date of Submission: 27-06-2022

# Index

# Experiment – 1: Making Straight, Rollover and Cross-over Cables

**Straight-through Cable:**

A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. A straight-through network cable acts as an extension enabling a device with a network interface card to be attached to a network. A common form of network media is the UTP Cat5 (Unshielded Twisted Pair Category 5) cable. This cable type has identical wiring on both ends (pin 1 on one end of the cable is connected to pin 1 at the other end of the cable, pin 2 is connected to pin 2 etc.)

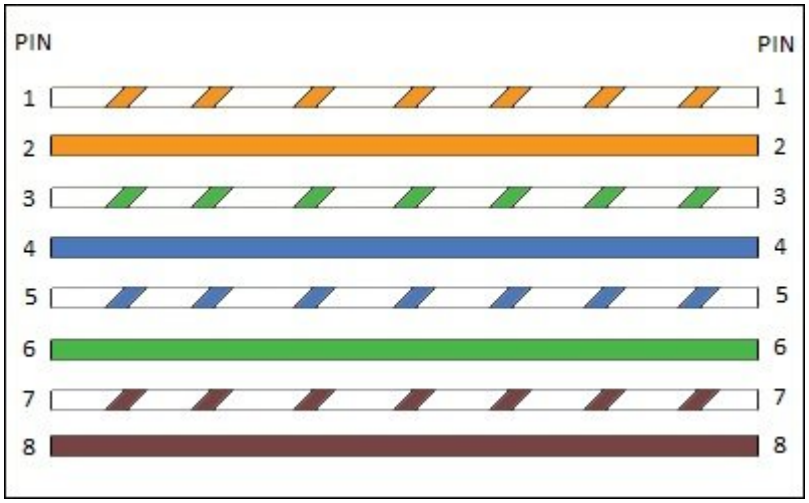



Fig. Straight-through cable

This type of cable is used to connect the following devices:

1) Computer to the hub
2) Computer to switch
3) Router to the hub
4) Router to switch

Computers and routers use wires 1 and 2 to transmit data and wires 3 and 6 to receive data. Hubs and switches use wires 1 and 2 to receive data and wires 3 and 6 to send data. That is why, if you want to connect two computers together, you will need a crossover cable.

The cables should have their sleeving trimmed back at each end by approximately 13mm in order to expose the wires for sorting. The wires should then be flattened out and sorted into the following order from left to right; White/Orange, Orange, White/Green, Blue, White/Blue, Green, White/Brown, Brown. At this point, it is best to make sure that the wires are the same length and trim them as necessary. It's a good idea to check the order of the

wires before moving on to the next stage to make sure that orange and brown have not been mixed up as some white wires don't have their markings colored clearly. Once the wires are confirmed to be in the correct order then it is time to attach the RJ-45 connectors. This is a simple case of pushing the wires in as far as they will go and then using a crimping tool to secure them into place. Once one end is done simply repeat the process for the second end, after being sure to test the cable with an appropriate device before using it in your network.

**Roll-over Cable:**

A rollover cable is a network cable that connects a computer terminal to a network router's console port. It is also referred to as a Cisco console cable and is normally flat and light blue so as to distinguish it from other network cable types. The pin-outs on one end of the cable are reversed from the opposite end, which is how the cable derived its name. Rollover cables are also known as Yost cables or Yost Serial Device Wiring Standard connectors.

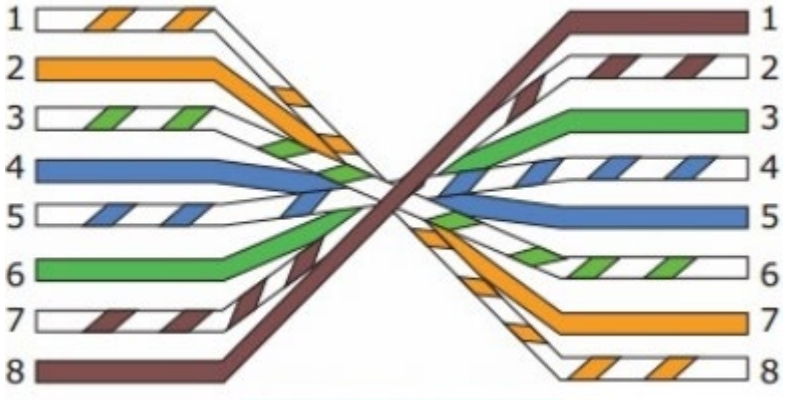


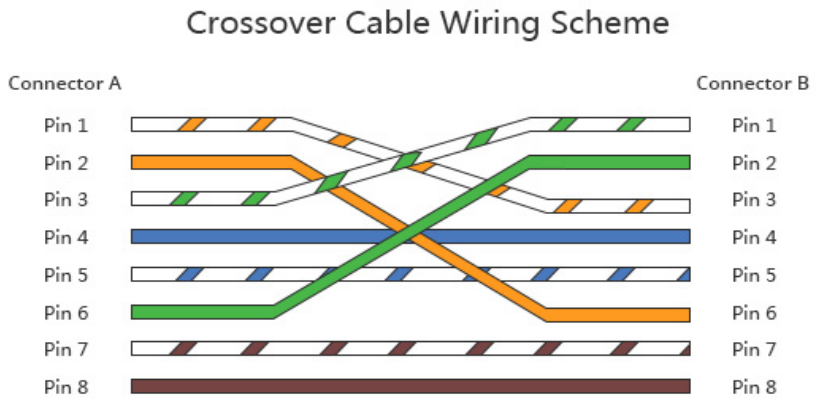

Fig. Roll-over cable

A rollover cable is identified by comparing each end of the cable while they are beside each other. The wire that connects the pin on the outside of the plug on the left-hand side is the same color as the wire connecting the pin on the outside of the plug on the right-hand side. If Cisco Systems produced the rollover cable, the first pin will be white on one of the two connectors and pin number 8 will be white on the other.

Rollover cables primarily connect a device to a switch or router's console port. This permits an engineer or programmer to connect to the network device and manipulate the programming as required. Although many network programming tasks can now be centrally completed, there remains the need for technicians to use rollover cables for network hardware upgrades, maintenance, and troubleshooting.

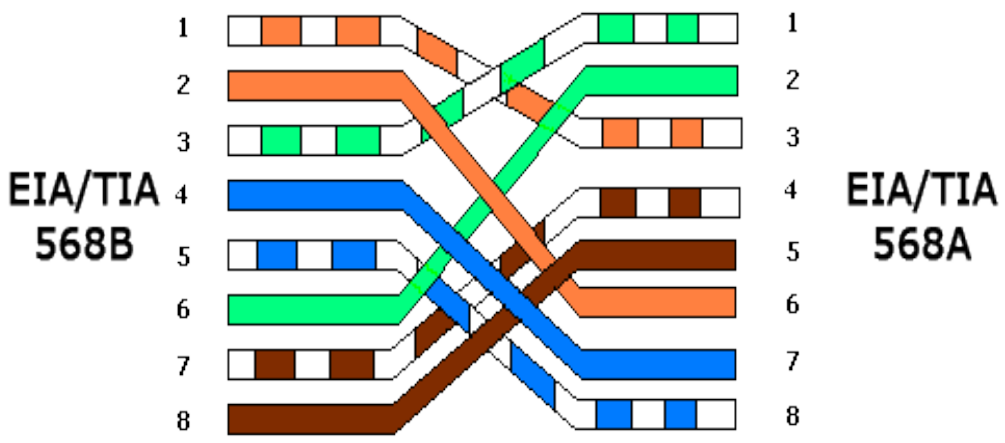
**Cross-over Cable:**

With the crossover cable, the wire pairs are swapped, which means that different pins are connected together – pin 1 on one end of the cable is connected to pin 3 on the other end, pin 2 on one end is connected to pin 6 on the other end.




This type of cable is used when you need to connect two devices or hosts directly (connecting a switch directly to another switch, or connecting a router to a router) and that the use same wires to send and receive data. For example, consider connecting two computers together. If you use straight-through cable, with identical wiring in both ends, both computers will use wires 1 and 2 to send data. If computer A sends some packets to computer B, computer A will send that data using wires 1 and 2. That will cause a problem because computers expect packets to be received on wires 3 and 6, and your network will not work properly. This is why you need to use a crossover cable for such connections.

Using the 568-B standard as an example below you will see that Pin 1 on connector A goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B etc.



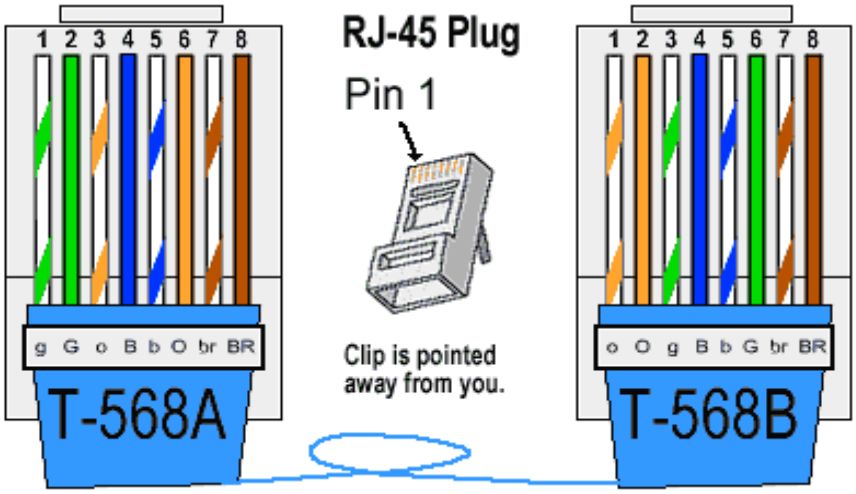
# Experiment – 2: Cable and RJ-45 Jack Outlet Installation

**Cable:**

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

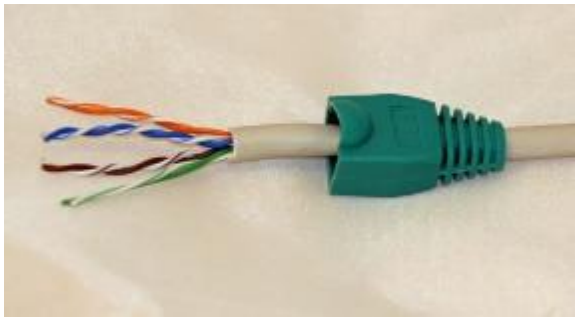
**RJ-45:**

RJ-45 connectors are the most common form of connectors used on UTP Cat5 cables. The RJ simply means Registered Jack and the 45 designations specify the pin numbering scheme. The cable itself contains 4 twisted pairs of wires making a total of 8 wires.

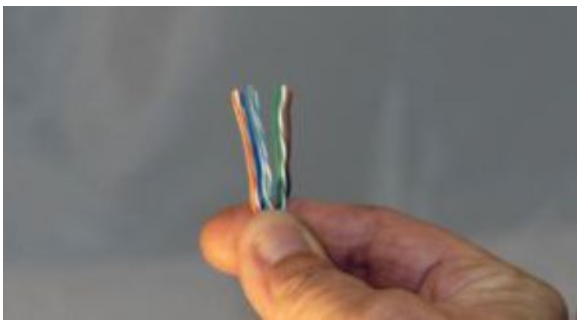



Do not strip the insulation off of the individual paired wires. Just remove about 40mm of the jacket as shown below in photo - 1. The way the stripper tool works is the cable is inserted into the stripper and then the stripper is rotated a couple of times allowing the tools cutting blade to score the cable‘s outer jacket only. Be careful not to cut through any colored wires. Untwist the twisted paired wires. Then arrange them in the correct order. Use the guide below to arrange the wire colors in the proper order. Getting the eight wires arranged in the proper order and pressing the eight wires flat between your thumb and index fingers is an important step to get the wires set up to slide into the RJ-45 connector. Once the wires are flat and in the right order cut them so they are 13mm long as shown in photo – 4. Insert the flattened wire into the RJ-45 connector as shown in photo - 5. Put your RJ45 crimping tool to work. Read the directions for your tool. Drawing B below shows what the crimp tool is doing. The crimp tool presses the gold-plated electrical contact down such that they pierce through the insulation of all eight wires and make contact with the copper conductor.

This is called insulation displacement hence no need to strip the insulation off of the individual wires. The crimp tool presses down on a hinged tab that grips onto the cable's outer jacket to provide a strain relief action and helps to keep the cable and the connector intact.

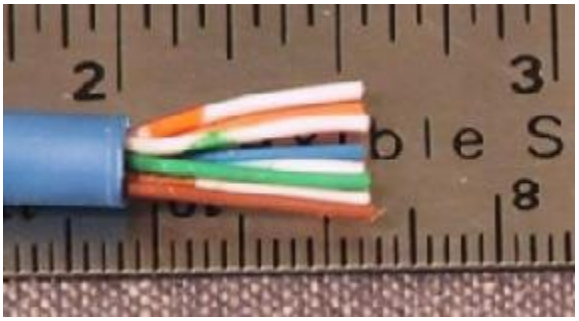


1. Fit Boot - Expose 40mm Wires



2. Straighten Wires Put in Order

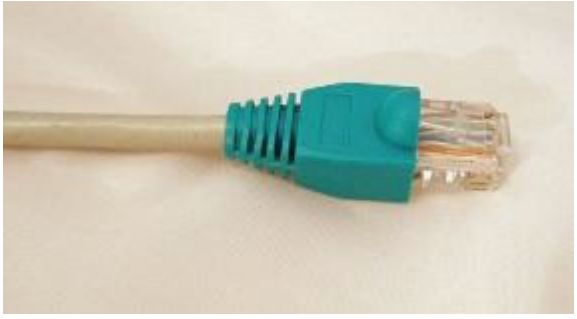
3. Use Crimper to Trim Wires



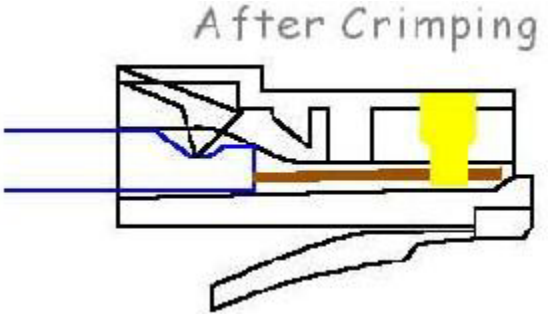

4. Trim to 13mm

5. Insert into RJ-45 Connector

6. Crimp Cable to RJ45 Connector



7. Completed Connection



# Experiment – 3: IP Addressing and Sub-netting Concepts

## Introduction to IP Addressing:

Each Network Interface Card (NIC or Network card) present in a PC is assigned one Network address called an IP address [or Logical address or Network address]. This IP address is assigned by the administrator of the network. No two PCs can have the same IP address. There is a burned-in address on the NIC called Physical Address [or MAC address or Hardware address]. The MAC address of a network card indicates the vendor of that card and a unique serial number. Two types of IP addresses are:

1) IPv4 and 2) IPv6

## IPv4 Addressing:

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device to the internet. The address space of IPv4 is $2^{32}$ or 4,294,967,296. IPv4 addresses use the base-256 numbering system. IPv4 is made up of four parts, in the pattern as w.x.y.z. Each part has 8 binary bits and the values in decimal can range from 0 to 255. In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

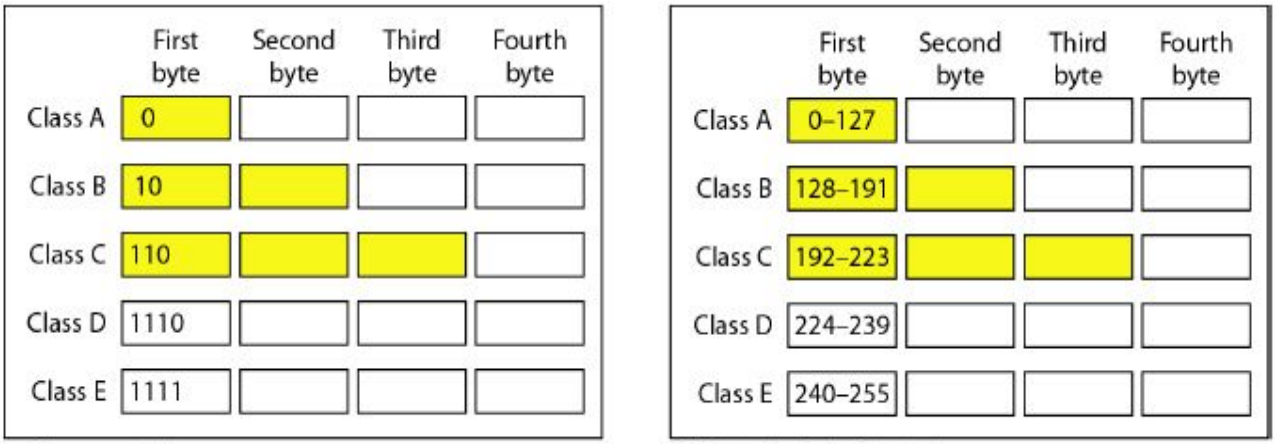



Fig. Finding the classes in binary and dotted-decimal notation

| Class | HOB | NET ID Bits | Host ID Bits | No of Networks | Host Per Network | Start Address | End Address |
|---|---|---|---|---|---|---|---|
| Class A | 0 | 8 | 24 | $2^7$=128 | $2^{24}$=16,777,216 | 0.0.0.0 | 127.255.255.255 |
| Class B | 10 | 16 | 16 | $2^{14}$=16,384 | $2^{16}$=65,536 | 128.0.0.0 | 191.255.255.255 |
| Class C | 110 | 24 | 8 | $2^{21}$=2,097,152 | $2^8$=256 | 192.0.0.0 | 223.255.255.255 |
| Class D | 1110 | - | - | - | - | 224.0.0.0 | 239.255.255.255 |
| Class E | 1111 | - | - | - | - | 240.0.0.0 | 255.255.255.255 |

HOB: High order bits

| Class | Number of Blocks | Block Size | Application |
|---|---|---|---|
| A | 128 | 16,777,216 | Unicast |
| B | 16,384 | 65,536 | Unicast |
| C | 2,097,152 | 256 | Unicast |
| D | 1 | 268,435,456 | Multicast |
| E | 1 | 268,435,456 | Reserved |

- Number of Blocks/Networks
- Block Size or host per network

Fig. Number of blocks and block size in classful IPv4 addressing

**Default Subnet mask** is used to identify the network part from the host part. Put binary one for the parts that represent the network part and zero for the part that represents the host part.

| Class | Binary | Dotted-Decimal | CIDR |
|---|---|---|---|
| A | 11111111 00000000 00000000 00000000 | 255.0.0.0 | /8 |
| B | 11111111 11111111 00000000 00000000 | 255.255.0.0 | /16 |
| C | 11111111 11111111 11111111 00000000 | 255.255.255.0 | /24 |

Hints: /n slash notation or Classless Interdomain Routing (CIDR). The CIDR notation is Used in classless addressing

Fig. Default masks for classful addressing

**IPv6 or IP new generation (IPng) Addressing:**

An IPv6 address is a 128-bit address that uniquely and universally defines the connection of a device to the internet. The address space of IPv6 is $2^{128}$. IPv4 is made up of eight parts. Each part has 8 binary bits or 4 hexadecimal bits.

| Block prefix | CIDR | Block assignment | Fraction |
|---|---|---|---|
| 0000 0000 | 0000::/8 | Special addresses | 1/256 |
| **001** | **2000::/3** | **Global unicast** | **1/8** |
| 1111 110 | FC00::/7 | Unique local unicast | 1/128 |
| 1111 1110 10 | FE80::/10 | Link local addresses | 1/1024 |
| 1111 1111 | FF00::/8 | Multicast addresses | 1/256 |

# Experiment – 4: Basic LAN Setup (Between 2 PC's)

**Procedure:**

**On the Host Computer:**

On the host computer, follow these steps to share the Internet connection:

1. Log on to the host computer as Administrator or as Owner.

2. Click **Start,** and then **click Control Panel.**

3. Click **Network** and **Internet Connections.**

4. Click **Network Connections.**

5. Right-click the connection that you use to connect to the Internet. For example, if you connect to the Internet by using a modem, right-click the connection that you want under Dial-up / other networks available.



6. Click **Properties.**

7. Click the **Advanced tab.**

8. Under **Internet Connection Sharing**, select the **Allow other network users to connect through this computer's Internet connection** check box.

9. If you are sharing a dial-up Internet connection, select the **Establish a dial-up connection whenever a computer on my network attempts to access the Internet** check box if you want to permit your computer to automatically connect to the Internet.

10. Click **OK.** You receive the following message: When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0.1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable **Internet Connection Sharing?**

11. Click **Yes.** The connection to the Internet is shared to other computers on the local area network (LAN). The network adapter that is connected to the LAN is configured with a static IP address of 192.168.0.1 and a subnet mask of 255.255.255.0

**On the Client Computer:**

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP configuration, and then configure the client computer. To confirm the LAN adapter IP configuration, follow these steps:

1. Log on to the client computer as Administrator or as Owner.

2. Click **Start,** and then click Control Panel.

3. Click **Network** and **Internet Connections.**

4. Click **Network Connections.**

5. Right-click **Local Area Connection** and then **click Properties.**

6. Click the **General** tab, **click Internet Protocol (TCP/IP)** in the **connection uses the list of the following items**, and then click **Properties.** 7. In **the Internet Protocol (TCP/IP) Properties** dialog box, **click Obtain an IP address automatically** (if it is not already selected), and then click **OK.**

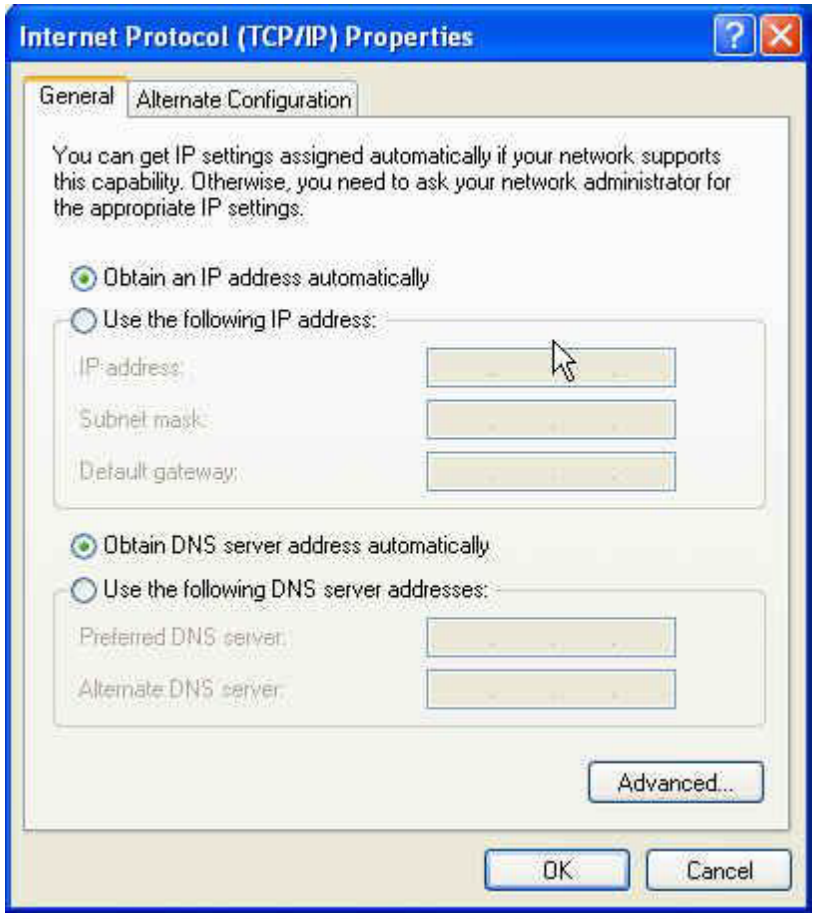
**Note:** You can also assign a unique static IP address in the range of 192.168.0.2 to 192.168.0.254. For example, you can assign the following static IP address, subnet mask, and default gateway:

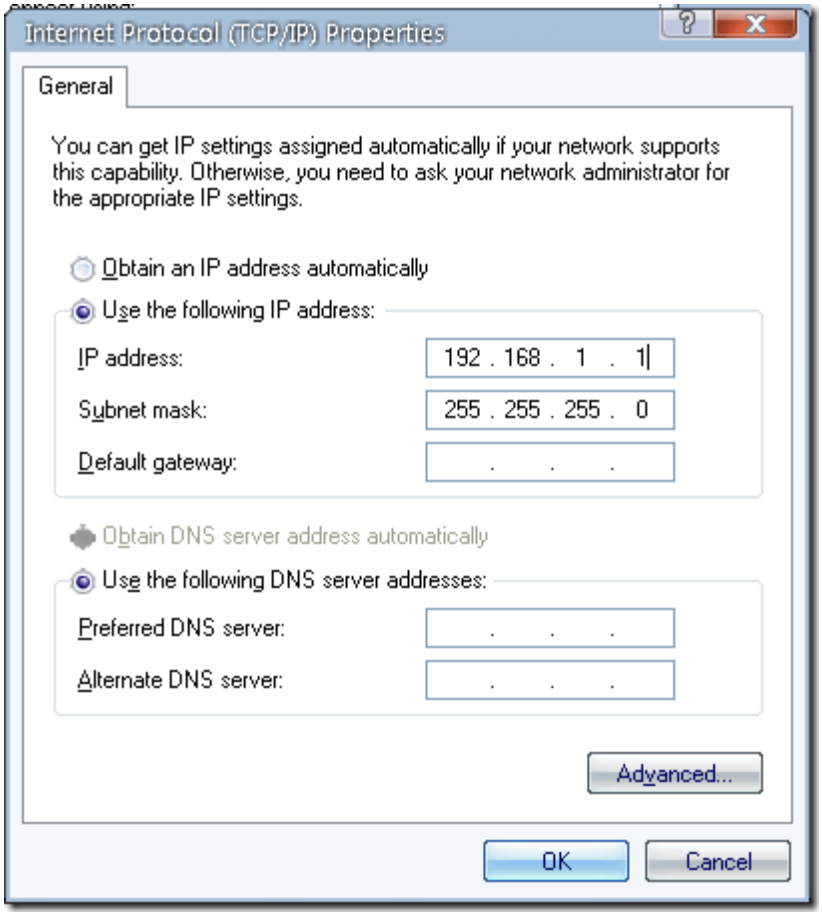
8. IP Address 192.168.1.1

9. Subnet mask 255.255.255.0

10. Default gateway 192.168.31.1

11. In the **Local Area Connection Properties dialog** box, click **OK.**


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

# Experiment – 5: Overview and Basic Configuration of Router

**Router:**

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets.

Basic configuration of the router includes **configuration of the IP address, default routing, static and dynamic routing, static and dynamic NATing, hostname, banner, secret password, user accounts, and other options**.

**Configure Commands:**

| Step | Command | Purpose |
|---|---|---|
| 1 | enable<br>Example: Router>enable | Enables privileged EXEC mode.<br>=> Enter your password if prompted. |
| 2 | configure terminal<br>Example: Router# configure terminal | Enters global configuration mode. |

**Configuring Global Commands:**

To configure selected global parameters for your router, perform these steps (summary):
1. **configure** terminal
2. **hostname** name
3. **enable secret** password

| Step | Command | Purpose |
|---|---|---|
| 1 | configure terminal<br>Example:<br>Router# configure terminal | Enters global configuration mode when using the console port. If you are connecting to the router using a remote terminal, use the following:<br>telnet router name or address<br>Login: login id<br>Password: *********<br>Router> enable |
| 2 | hostname name<br>Example:<br>Router(config)# hostname Router | Specifies the name of the router. |
| 3 | enable secret password<br>Example:<br>Router(config)# enable secret cr1ny5ho | Specifies an encrypted password to prevent unauthorized access to the router. |

**Example:**

Router#**config t (**Enter configuration commands, one per line. End with CNTL/Z.)

Router(config)#**service password-encryption**

Router(config)#**enable password nit**

Router(config)#**line vty 0 197**

Router(config-line)#**login**

Router(config-line)#**password nit2**

Router(config-line)#**line con 0**

Router(config-line)#**login**

Router(config-line)#**password nit1**

Router(config-line)#**line aux 0**

Router(config-line)#**login**

Router(config-line)#**password nit**

Router(config-line)#**exit**

Router(config)#**no service password-encryption**

Router(config)#**^Z**

**Configure Fast Ethernet:**

To configure the Fast Ethernet interface on a Cisco 861 or 881 ISR, perform these steps, beginning in global configuration mode (summary):

1**. interface** type number
2. **ip address** ip-address mask
3. **no shutdown**
4. **exit**

| Step | Command | Purpose |
|---|---|---|
| 1 | **interface** type number<br>**Example:**<br>Router(config)# interface fastethernet 0/0 | Enters the configuration mode for a Fast Ethernet WAN interface on the router. |
| 2 | **ip address** ip-address mask<br>**Example:**<br>Router(config-if)# ip address 192.168.12.2 255.255.255.0 | Sets the IP address and subnet mask for the specified Fast Ethernet interface. |

| | | |
|---|---|---|
| 3 | **no shutdown**<br>**Example:**<br>Router(config-if)# no shutdown | Enables the Ethernet interface, changing its state from administratively down to administratively up. |
| 4 | **exit**<br>**Example:**<br>Router(config-if)# exit<br>Router(config)# | Exits configuration mode for the Fast Ethernet interface and returns to global configuration mode. |

**Configure Static Routes:**

Static routes provide fixed routing paths through the network. They are manually configured on the router. If the network topology changes, the static route must be updated with a new route. Static routes are private routes unless they are redistributed by a routing protocol.
Follow these steps to configure static routes, beginning in global configuration mode (summary):

1. **ip route** prefix mask {ip-address | interface-type interface-number [ip-address]}
2. **end**

| Step | Command | Purpose |
|---|---|---|
| 1 | **ip route** prefix mask {ip-address \|interface-type interface-number [ip-address]}<br>**Example:**<br>Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2 | Specifies the static route for the IP packets. |
| 2 | **end**<br>**Example:**<br>Router(config)# end<br>Router# | Exits router configuration mode, and enters privileged EXEC mode. |

**Basic Configuration Commands:**

| Requirement | Cisco Command |
|---|---|
| Set a console password | Router(config)#line con 0<br>Router(config-line)#login<br>Router(config-line)#password cisco |
| Set a telnet password | Router(config)#line vty 0 4<br>Router(config-line)#login<br>Router(config-line)#password cisco |
| Set the enable password to cisco | Router(config)#enable password cisco |
| Set the enable secret password to peter. This password overrides the enable password and is encrypted within the config file | Router(config)#enable secret peter |
| Enable an interface | |
| To disable an interface | Router(config-if)#no shutdown |
| Set the clock rate for a router with a DCE cable to 64K | Router(config-if)#shutdown |
| To add an IP address to an interface | Router(config-if)clock rate 64000 |
| To enable RIP on all 172.16.x.y interfaces | Router(config-if)#ip addr 10.1.1.1 255.255.255.0 |
| Disable RIP | Router(config)#router rip<br>Router(config-router)#network 172.16.0.0 |
| Static route the remote network is 172.16.1.0, with a mask of 255.255.255.0, the next hop is 172.16.2.1, at a cost of 5 hops | Router(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1 5 |

# Experiment – 6: Router Show Command

1. **sh ip route:** The command **sh ip route** shows the IP routing table, the metric used, and the interface used to find a remote network.

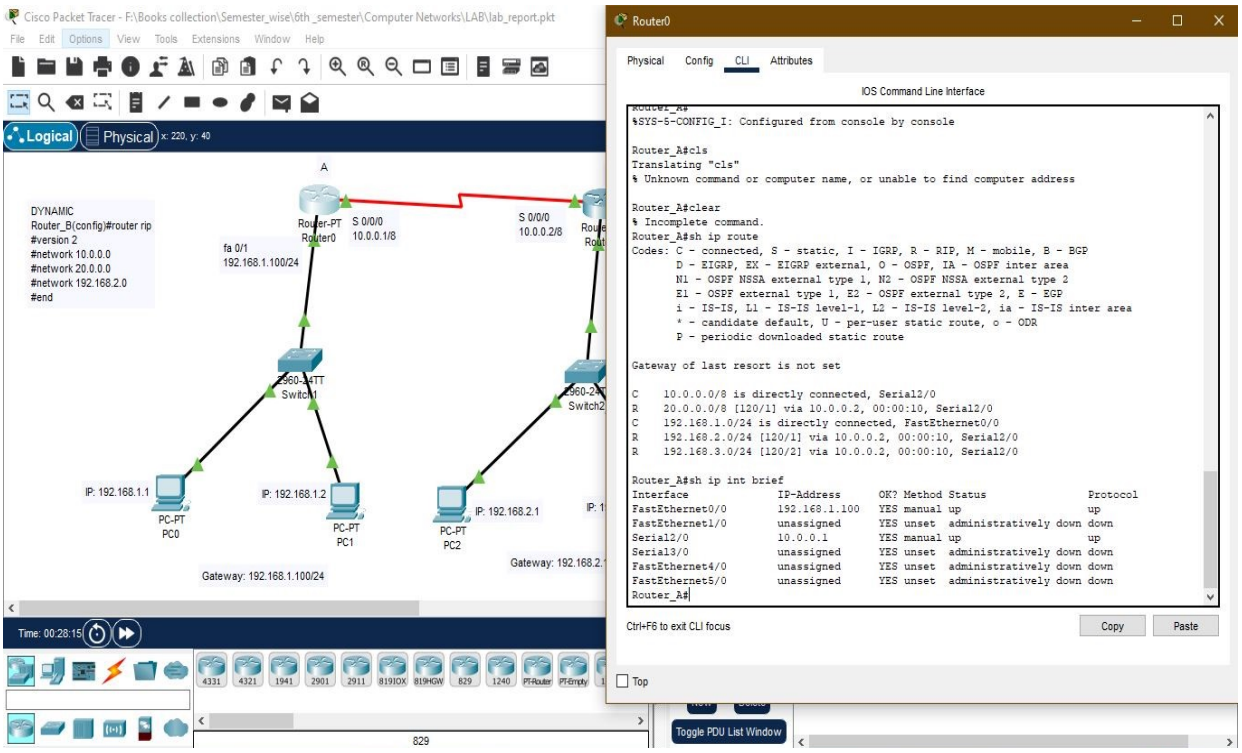



Fig. Command 1 and 2

2. **sh ip int brief:** This command displays a brief summary of the interfaces on a device. It's useful for quickly checking the status of the device.

3. **sh ip rip database:** To display summary address entries in the Routing Information Protocol (RIP) routing database entries if relevant are routes being summarized based upon a summary address, use the show ip rip database command in privileged EXEC mode.

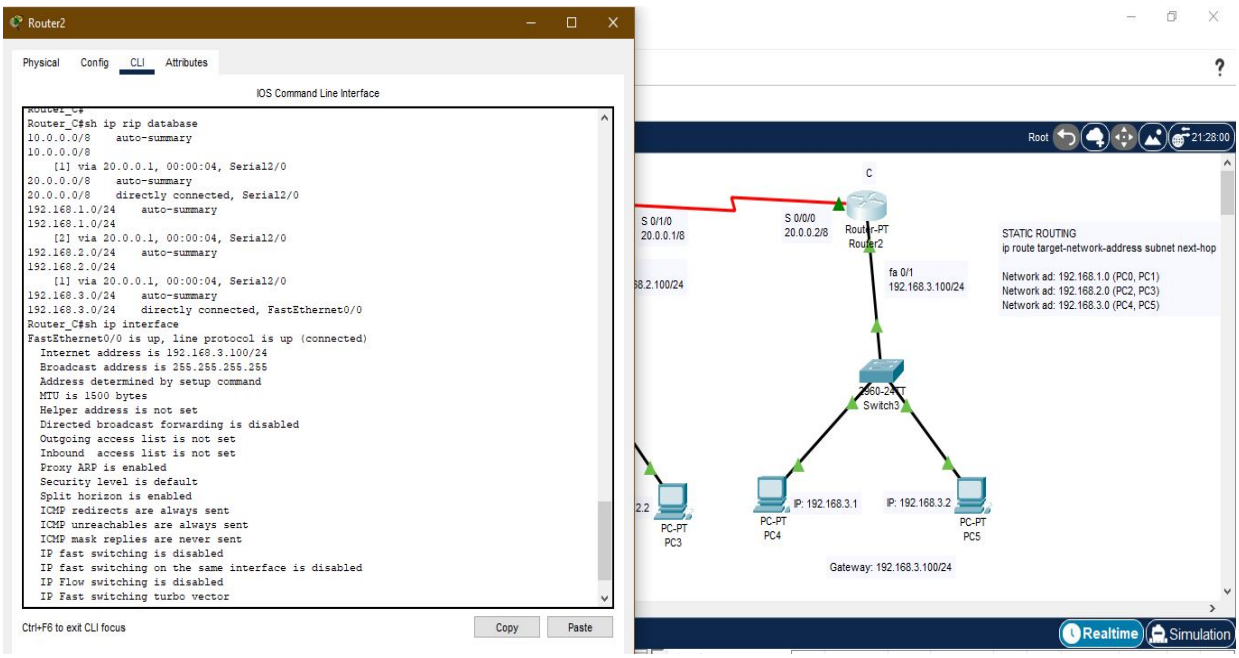



Fig. Command 3 and 4

4. **sh ip interface:** The show ip interface command can be used to tell if an inbound or an outbound access list has been applied to an interface. Rows 9 and 10 of the following output contain the information. The rest of the lines don't pertain to ACLs, so they've been omitted. You should recall that the show ip interface command displays all interfaces.

5. **show run:** One way to see your access lists and how they're applied is to use the show run command to see the active configuration.

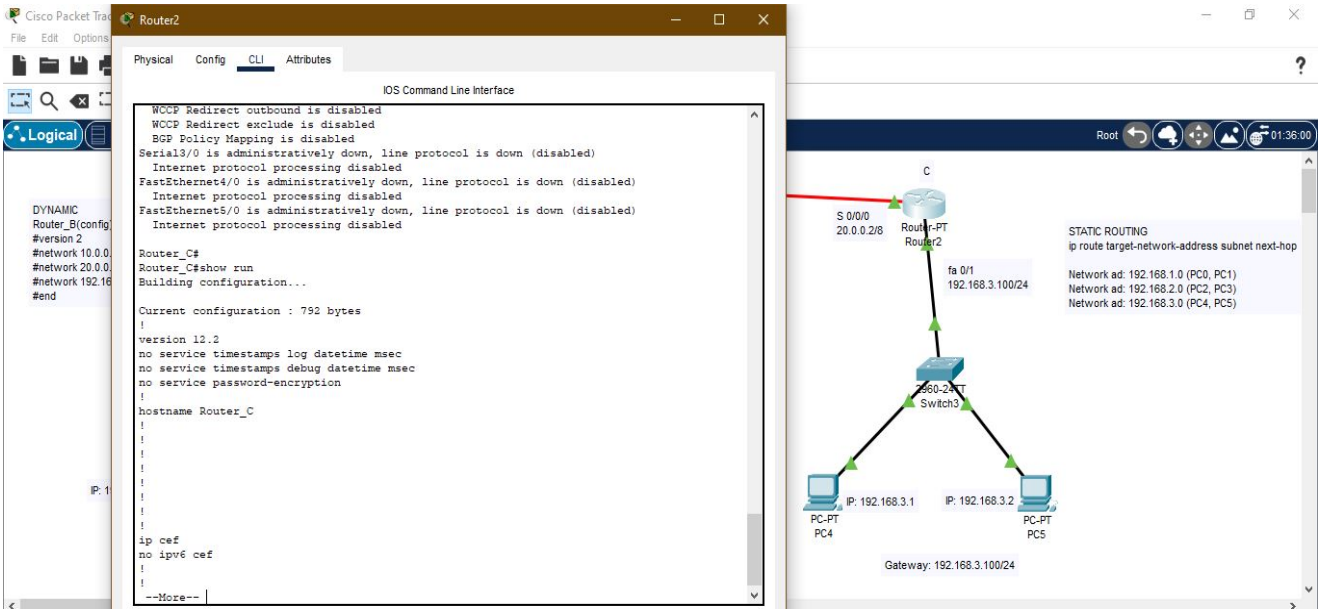



Fig. Command 5

# Experiment – 7: Simulation and Study of Networks Using Router

**Routing** is used for taking a packet from one device and sending it through the network to another device on a different network. If your network has no routers, then you are not routing. Routers route traffic to all the networks on your internetwork. To be able to route packets, a router must know, at a minimum, the following:

1) Destination address
2) Neighbor routers from which it can learn about remote networks
3) Possible routes to all remote networks
4) The best route to each remote network
5) How to maintain and verify routing information

**Global configuration:**

To configure any feature of the router, you must enter configuration mode. This is the first sub-mode of the parent mode. In the parent mode, issue the command **config terminal.**

Router>**enable**

Router#**config terminal**

Router(config)#**hostname Router_A**

**Configuring interfaces:**

To display the configuration of the interface use the following commands:

Router_A(config)#**interface fa0/1**

Router_A(config)#**interface fa0/0**

Router_A(config-if)#**ip address 192.168.1.100 255.255.255.0**

Router_A(config-if)#**no shutdown**

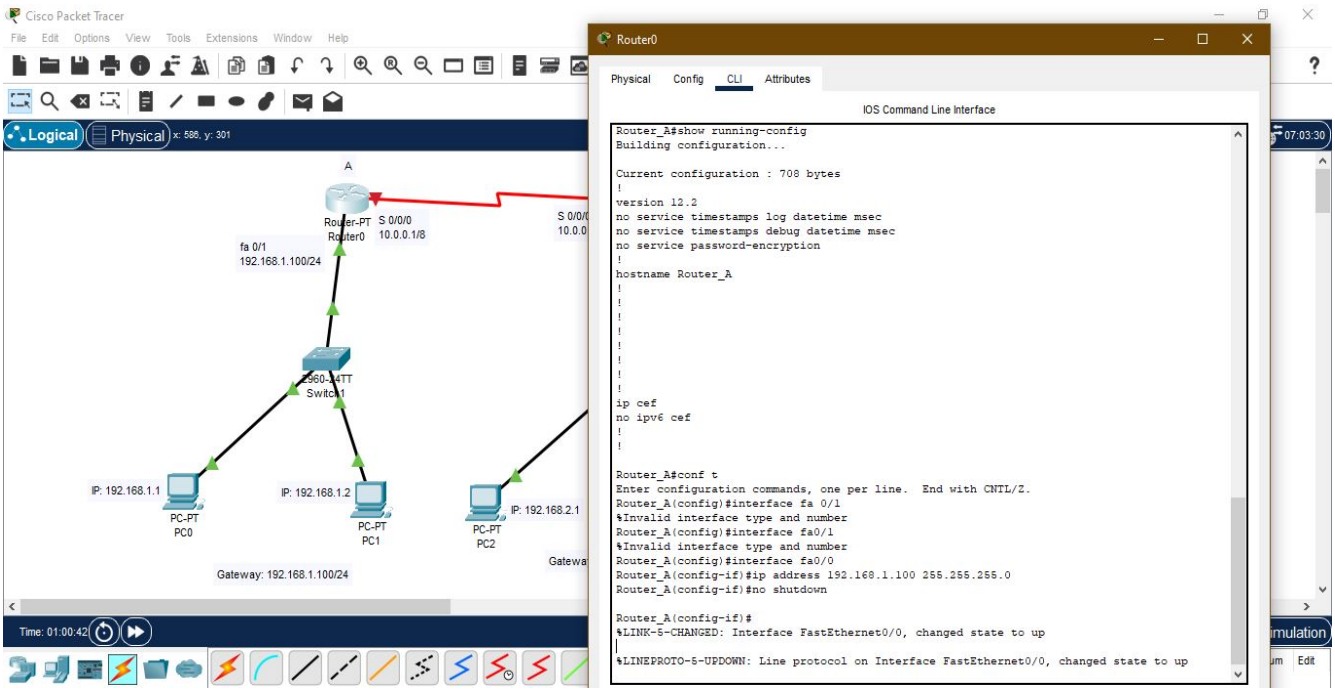
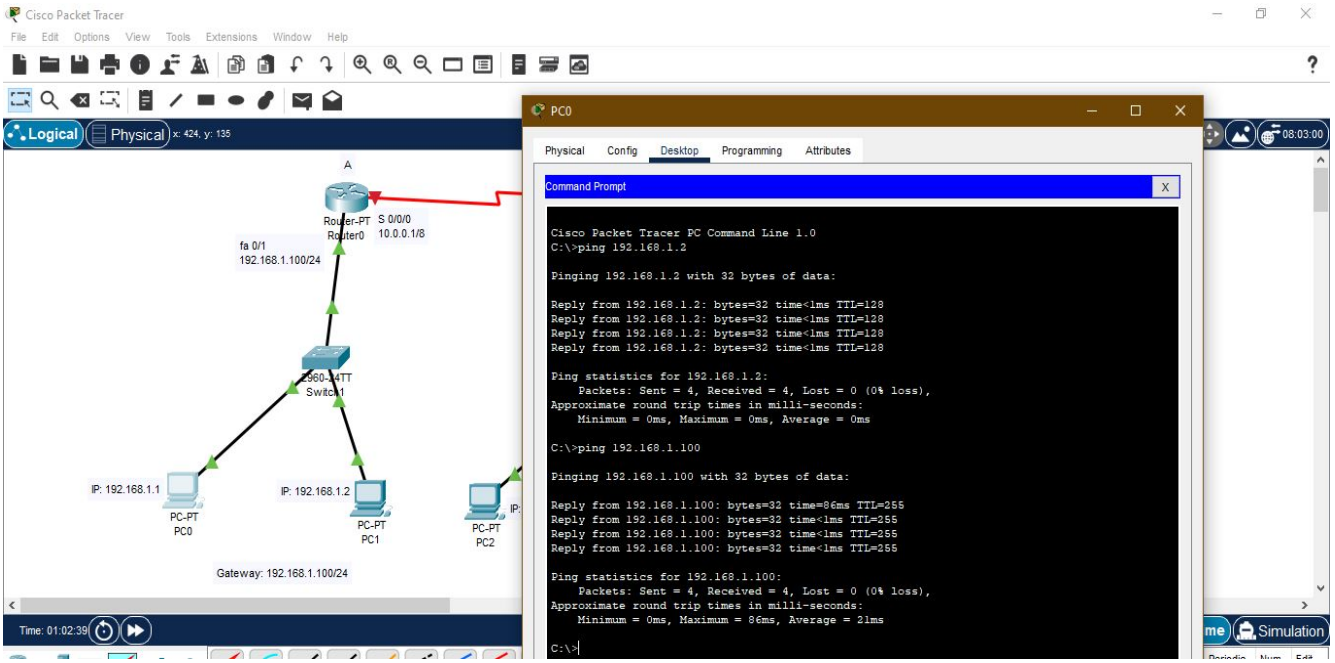



Fig. Global and interfaces configuration

## Check connection (ping test) between PC0 to PC1 and PC0 to Router_A:



# Experiment – 8: Simulation and Study of Dynamic Routing Using RIP Protocol

## Dynamic Routing:

Dynamic routing is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes.

## RIP:

Routing Information Protocol (RIP) is **a distance-vector routing protocol**. Routers running the distance-vector protocol send all or a portion of their routing tables in routing-update messages to their neighbors. You can use RIP to configure the hosts as part of a RIP network.

## Operations of Dynamic Protocol:

1) The router sends and receives routing messages on its interfaces.
2) The router shares routing messages and routing information with other routers that are using the same routing protocol.
3) Routers exchange routing information to learn about remote networks.
4) When a router detects a topology change, the routing protocol can advertise this change to other routers.

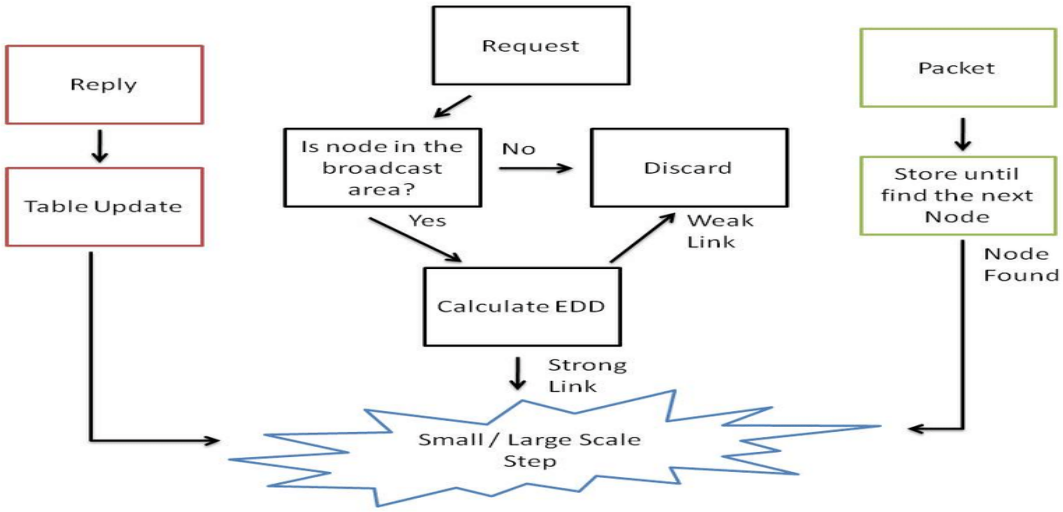



Fig. The dynamic routing step

**Role of Dynamic Routing Protocol:**

Routing protocols are used to facilitate the exchange of routing information between routers. Routing protocols allow routers to dynamically learn information about remote networks and automatically add this information to their own routing tables. Routing protocols determine the best path to each network, which is then added to the routing table. One of the primary benefits of using a dynamic routing protocol is that routers exchange routing information whenever there is a topology change. This exchange allows routers to automatically learn about new networks and also to find alternate paths if there is a link failure to a current network.

Compared to static routing, dynamic routing protocols require less administrative overhead. However, the expense of using dynamic routing protocols is dedicating part of a router‘s resources to protocol operation, including CPU time and network link bandwidth.

**Advantages and Disadvantages:**

Dynamic routing advantages are as follows:

- Administrator has less work in maintaining the configuration when adding or deleting networks.
- Protocols automatically react to the topology changes.
- Configuration is less error-prone.
- More scalable; growing the network usually does not present a problem.

Dynamic routing disadvantages are as follows:

- Router resources are used (CPU cycles, memory, and link bandwidth).
- More administrator knowledge is required for configuration, verification, and troubleshooting.

**Main Command Format:**

Router(config)# **router rip**

Router(config-router)# **version 2**

Router(config- router)# **network [connected net address]**

*** If remain more connections

Router(config- router)# **network [connected 2nd net address]**

Router(config- router)# **end**

## Simulation using RIP protocol (Dynamic):

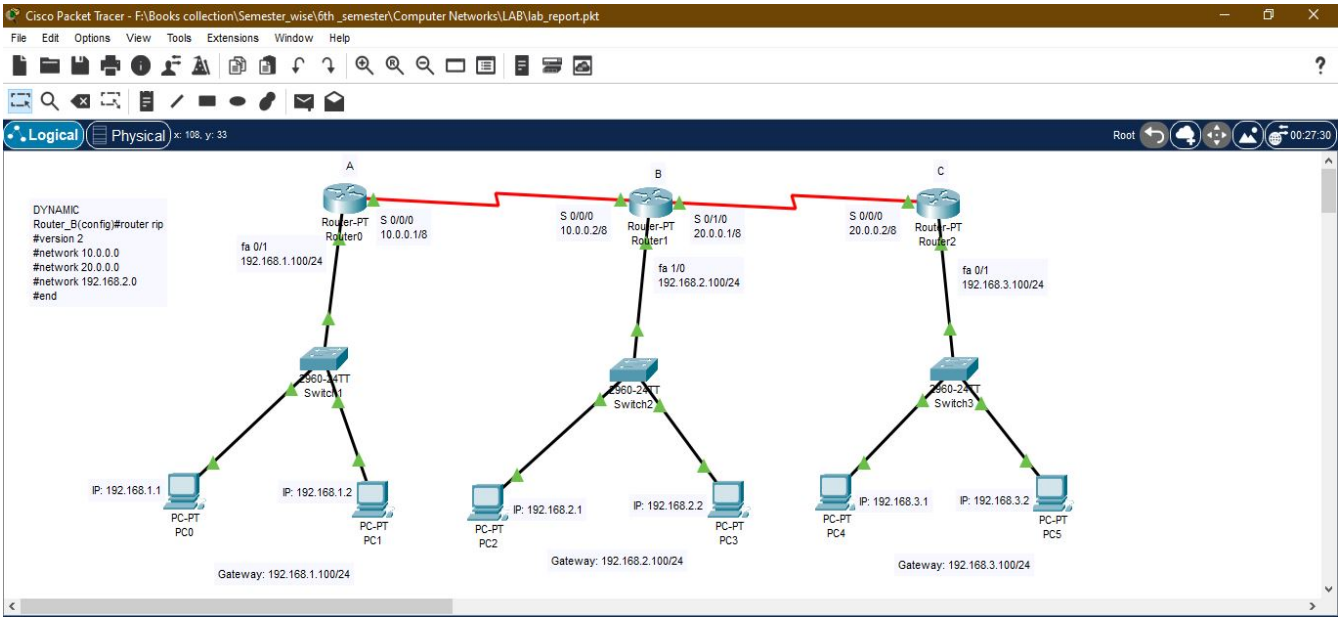



Fig. Complete network diagram

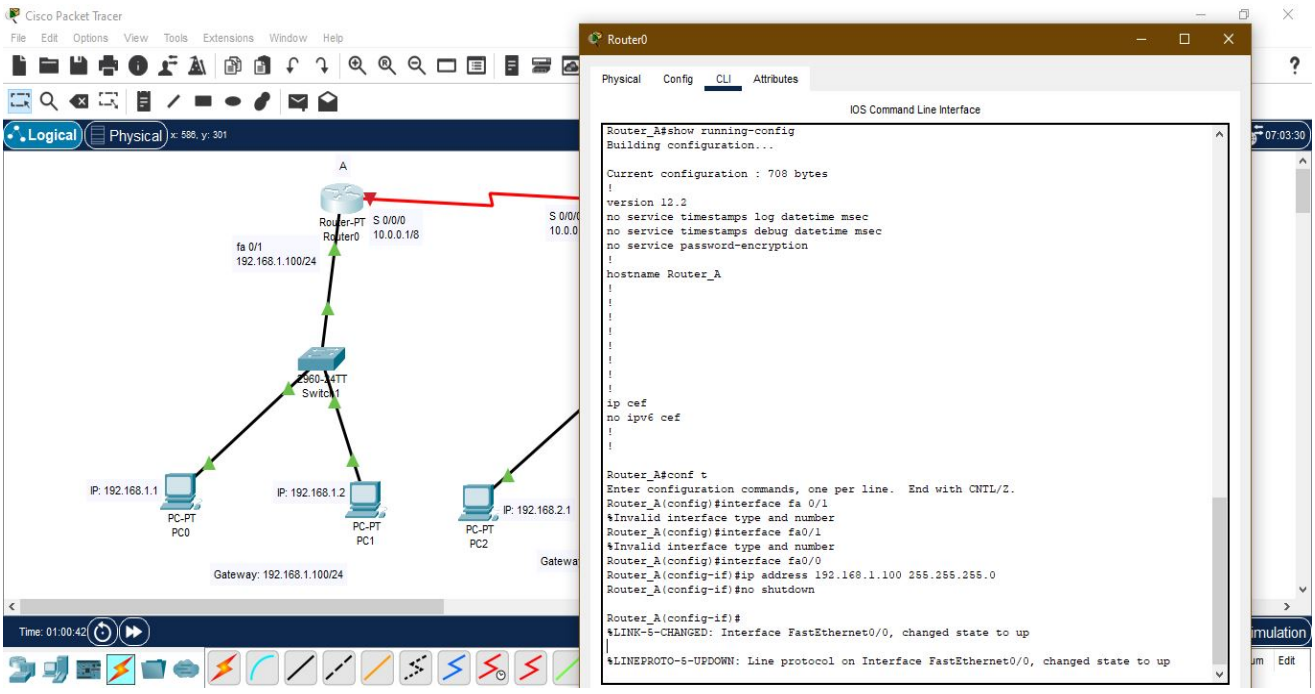



Fig. Router_A configuration

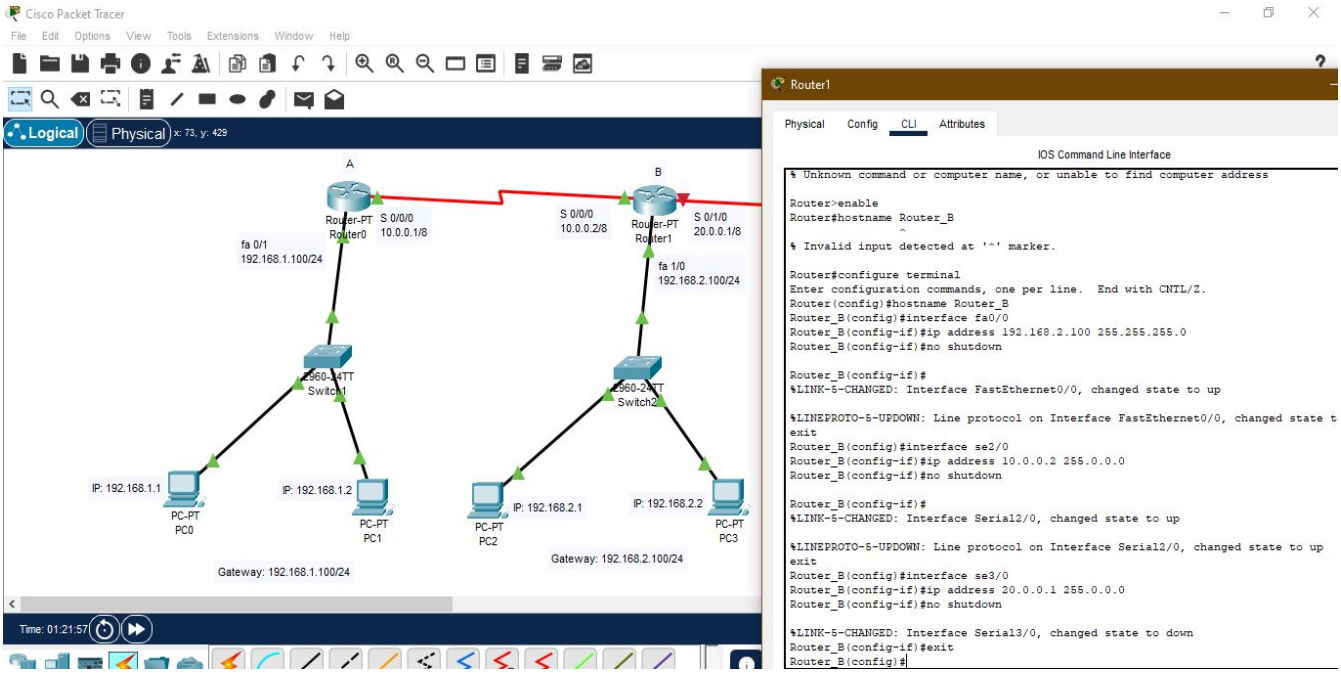



Fig. Router_B configuration

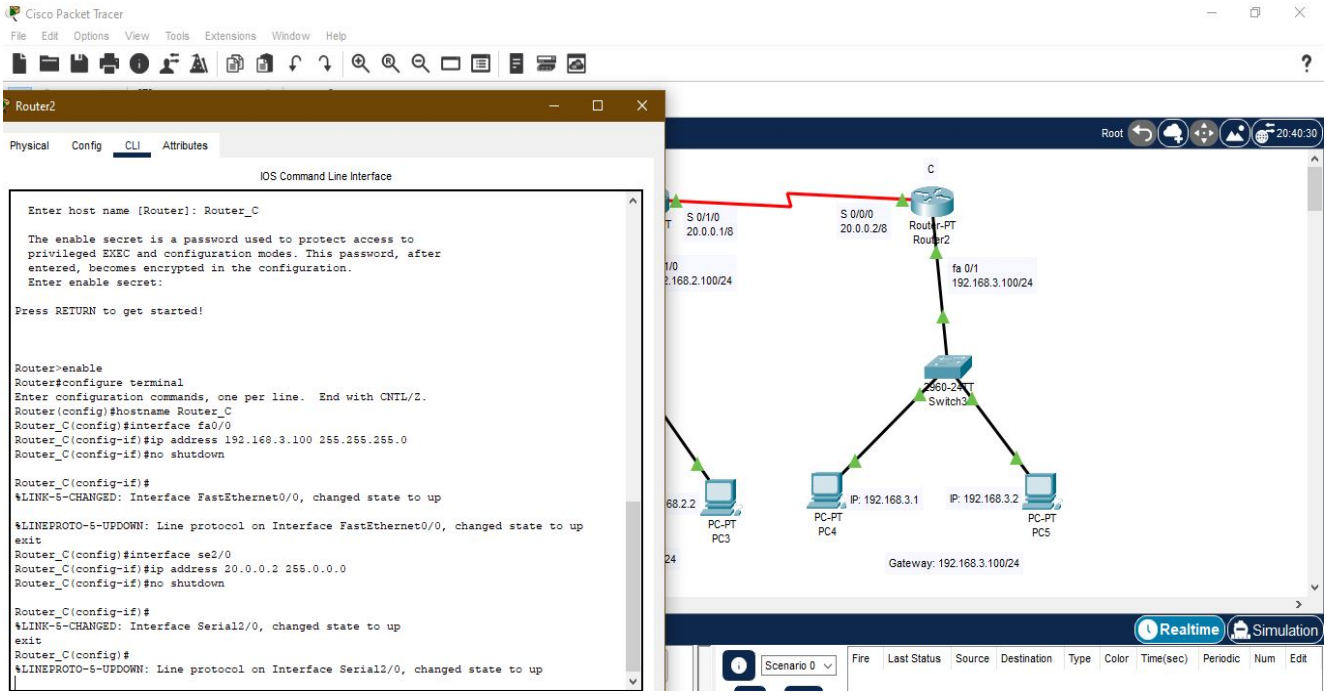



Fig. Router_C configuration

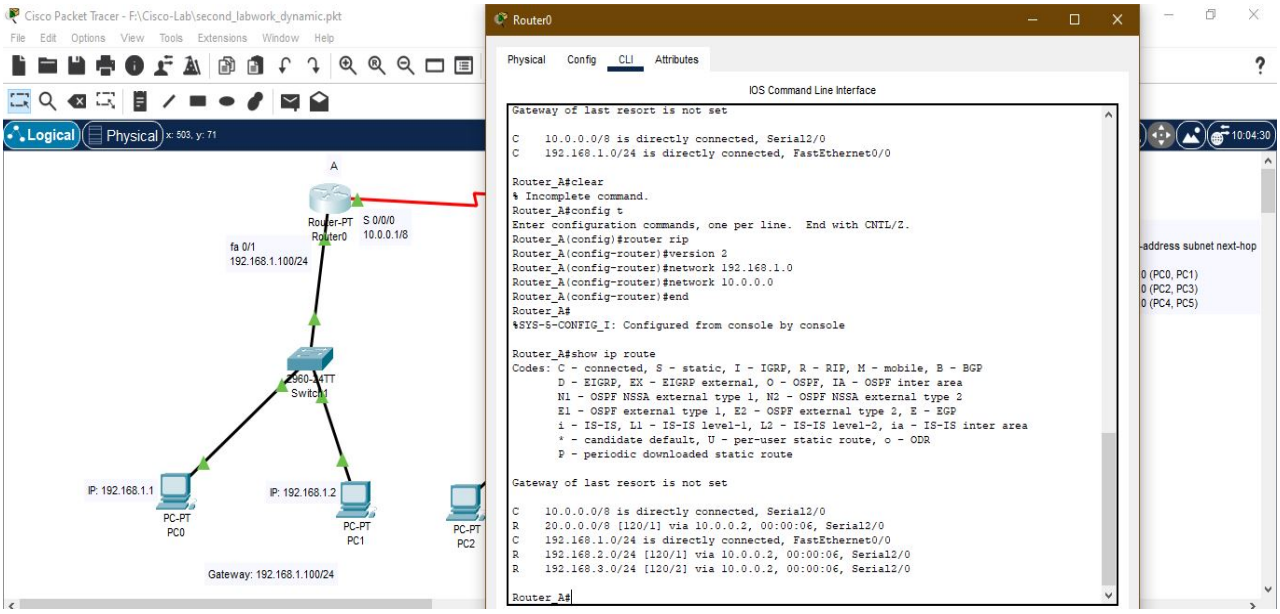



Fig. Connection among Router_A, Router_B and Router_C from Router_A

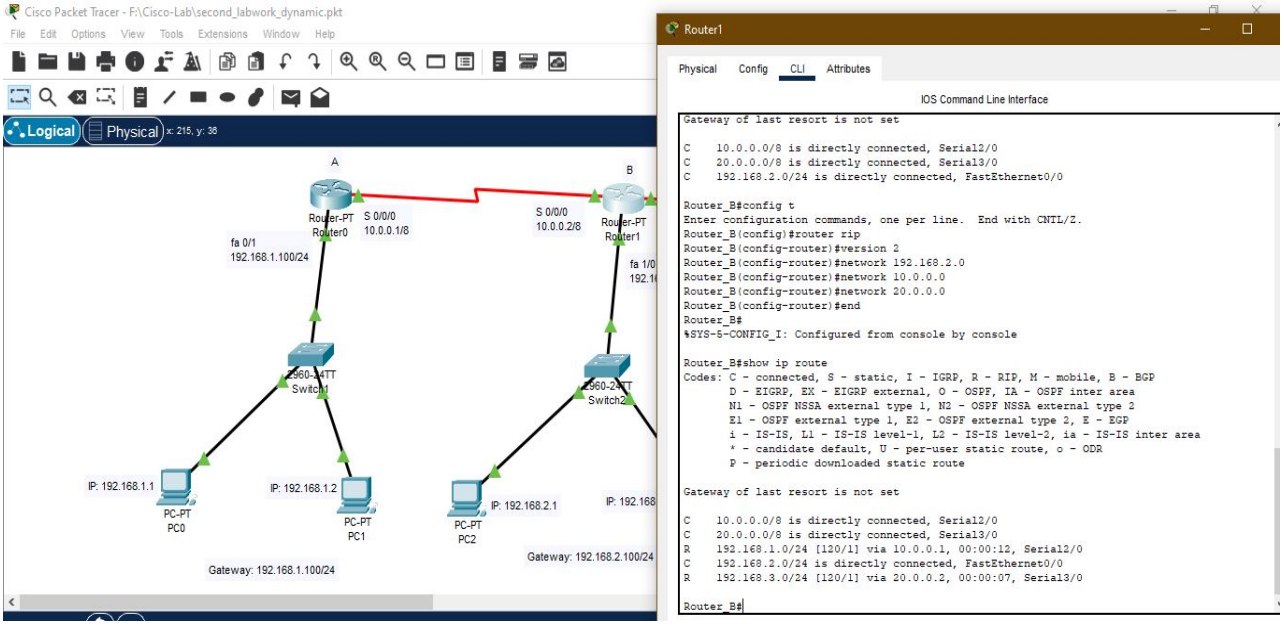



Fig. Connection among Router_A, Router_B and Router_C from Router_B

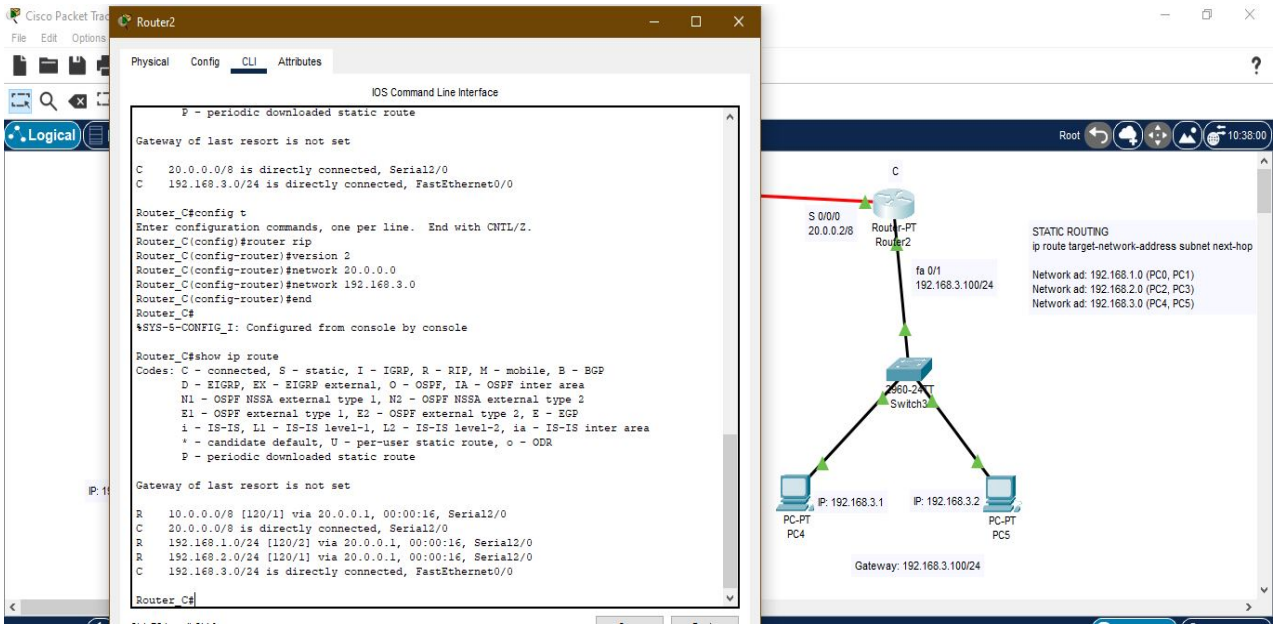



Fig. Connection among Router_A, Router_B and Router_C from Router_C

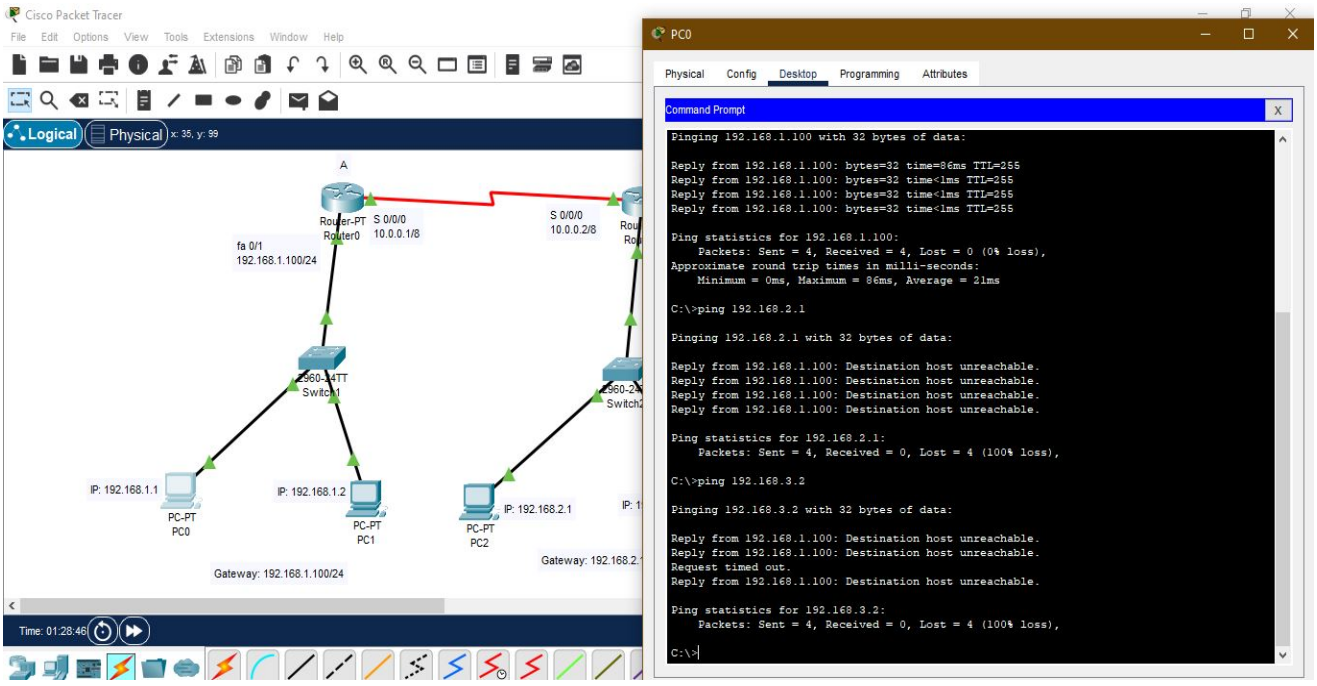



Fig. Ping test between PC0 to PC2 and PC0 to PC5

# Experiment – 9: Simulation and Study of Static Routing in Network

**Static Routing:**

It is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. Static routing occurs when you manually add routes in each router's routing table. Static routing is the term used to refer to a manual method that is used to set up routing between networks. The network administrator configures static routes in a router by entering routes directly into the routing table of a router. Static routing has the advantage of being predictable and simple to set up. It is easy to manage in small networks but does not scale well.

**Static routing has the following advantages**:

- There is no overhead on the router CPU.
- There is no bandwidth usage between routers.
- 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 really understand the internetwork and how each router is connected in order to configure routes correctly.
- If a network is added to the internetwork, the administrator has to add a route to it on all routers—manually.
- It's not possible in large networks because maintaining it would be a full-time job in itself.

**Command syntax for the static route:**

**ip route [destination_network_address] [mask] [next-hop_address or exit_interface] [administrative_distance] [permanent]**

**ip route:** The command used to create the static route.

**destination_network:** The network you're 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.

**exit_interface:** Used in place of the next-hop address if you want, and shows up as a directly connected route.

**administrative_distance:** By default, static routes have an administrative distance of 1 (or even 0 if you use an exit interface instead of a next-hop address).

**permanent (Optional):** Without the permanent keyword in a static route statement, a static route will be removed if an interface goes down. Adding the permanent keyword to a static route statement will keep the static routes in the routing table even if the interface goes down and the directly connected networks are removed.

**Simulation (Static):**

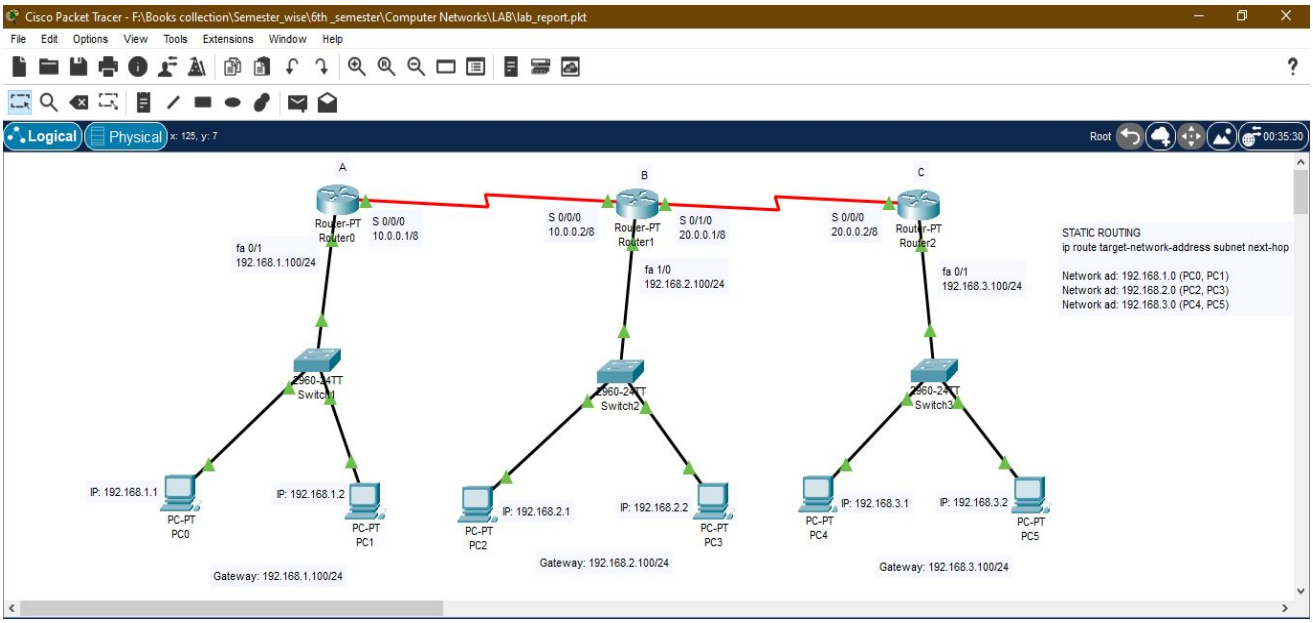



Fig. Complete network diagram

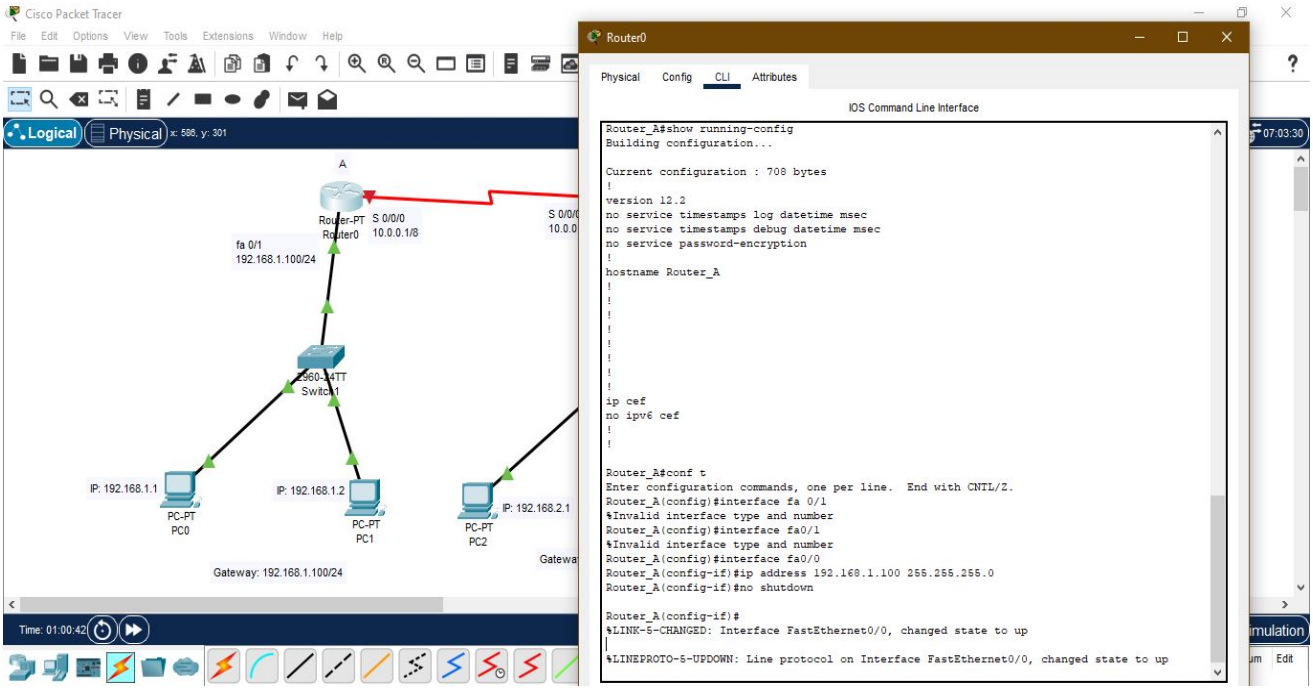



Fig. Router_A configuration

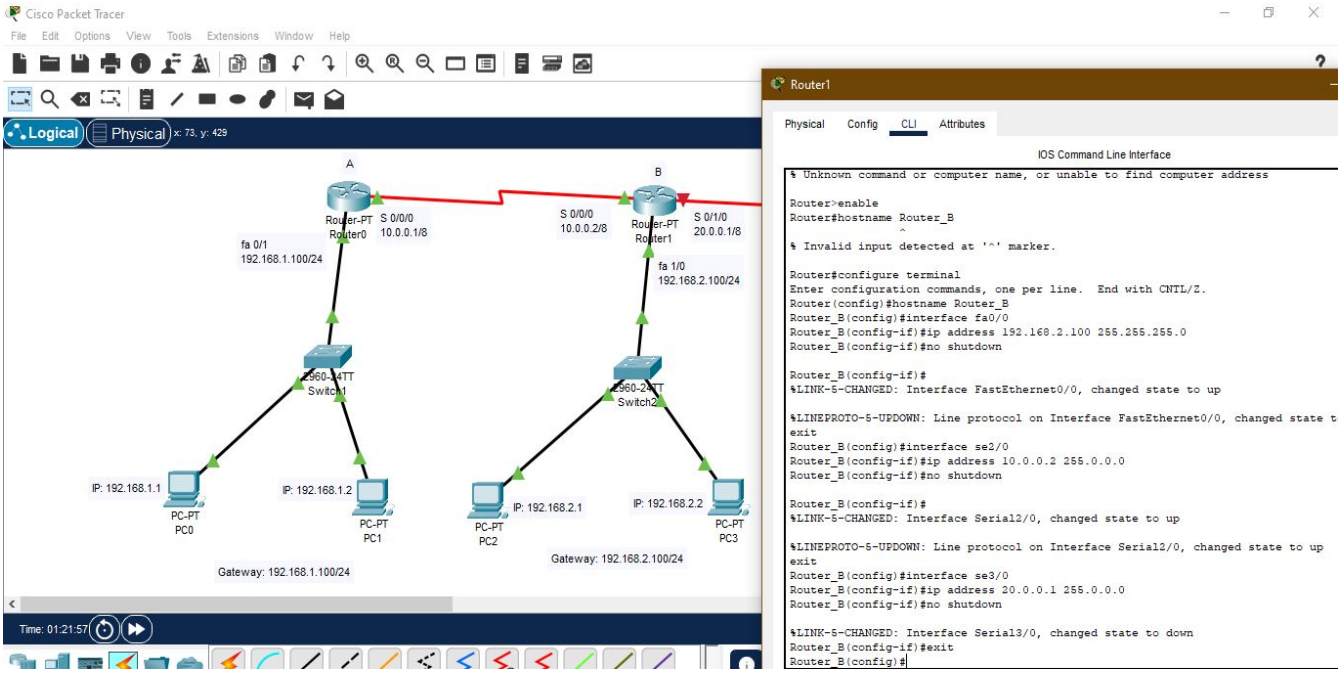



Fig. Router_B configuration

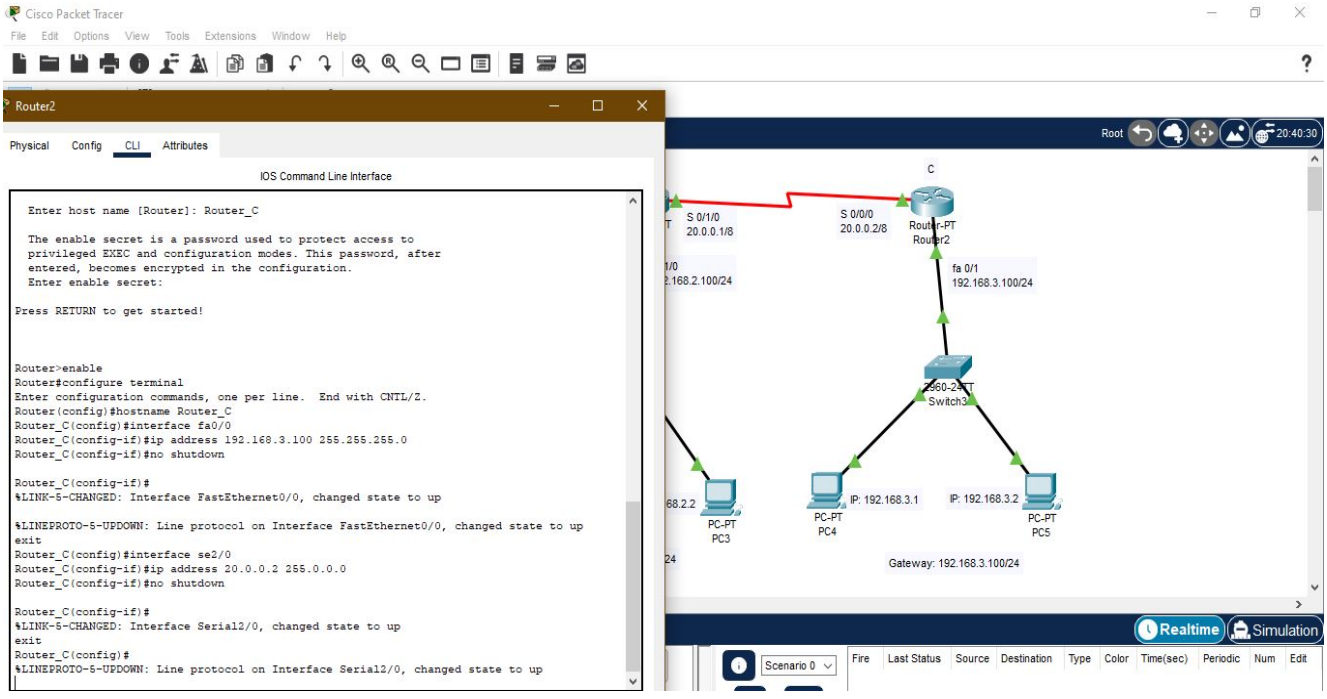



Fig. Router_C configuration

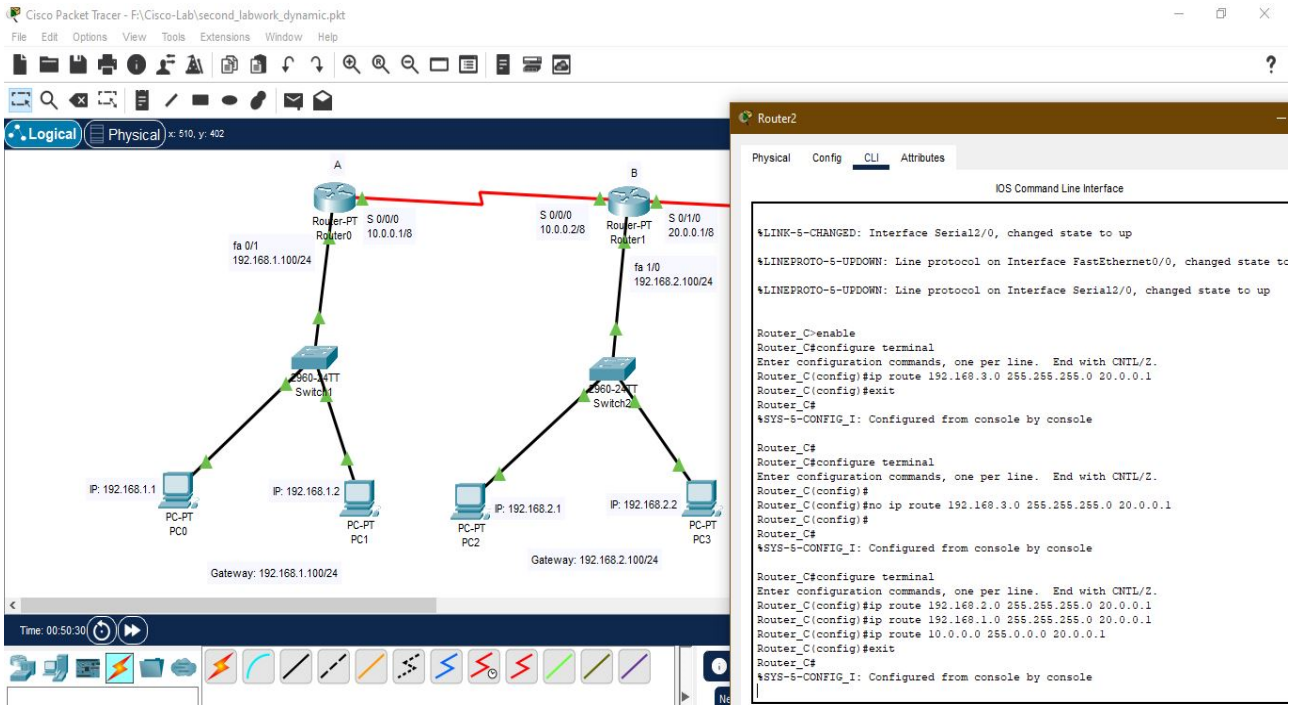



Fig. Connection among Router_A, Router_B and Router_C from Router_C

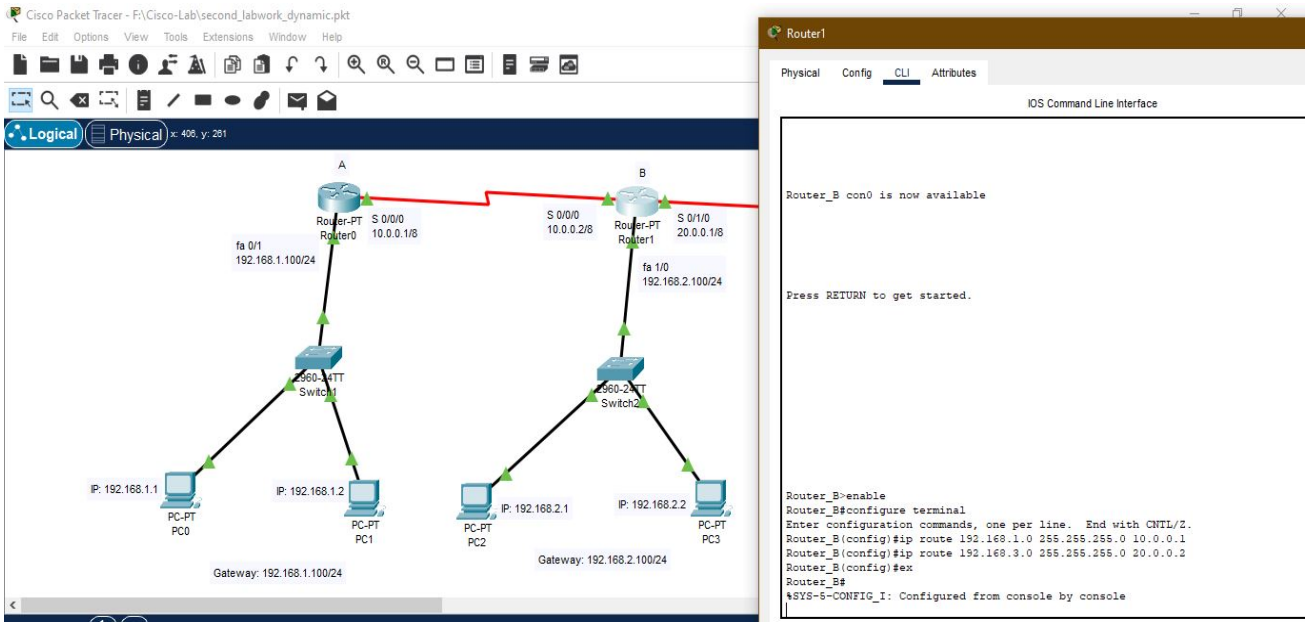



Fig. Connection among Router_A, Router_B and Router_C from Router_B

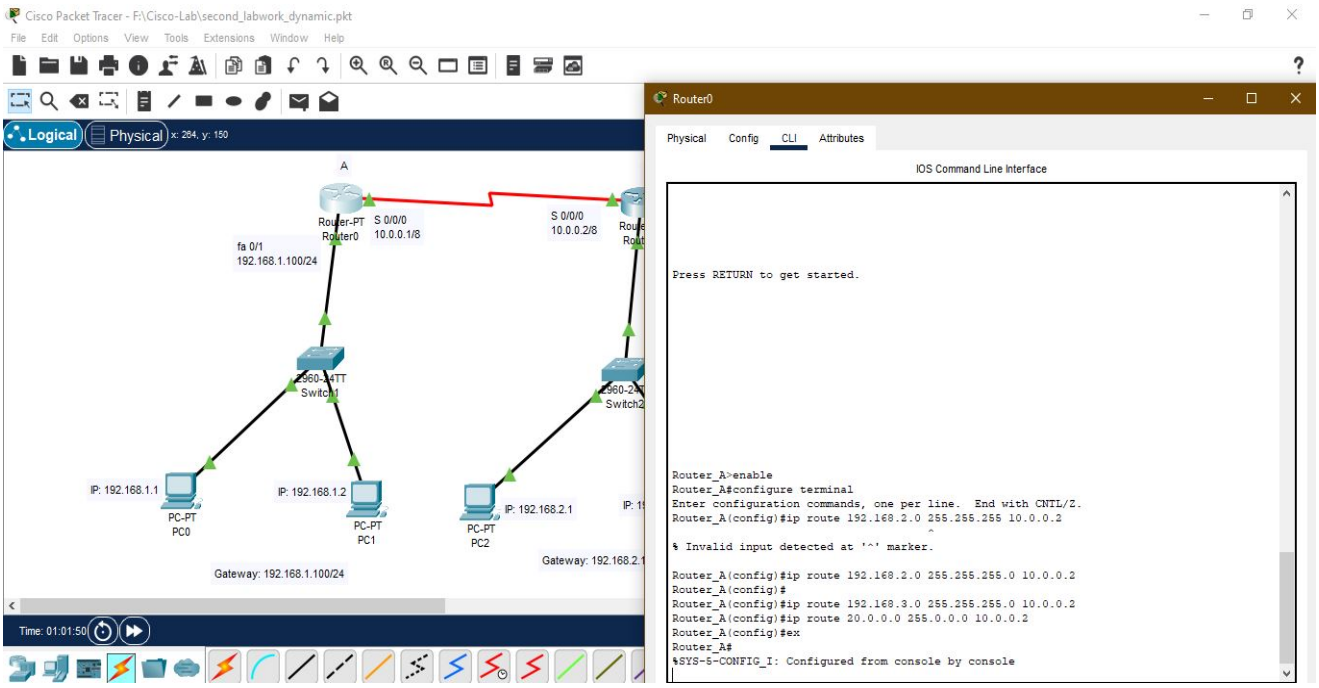



Fig. Connection among Router_A, Router_B and Router_C from Router_A

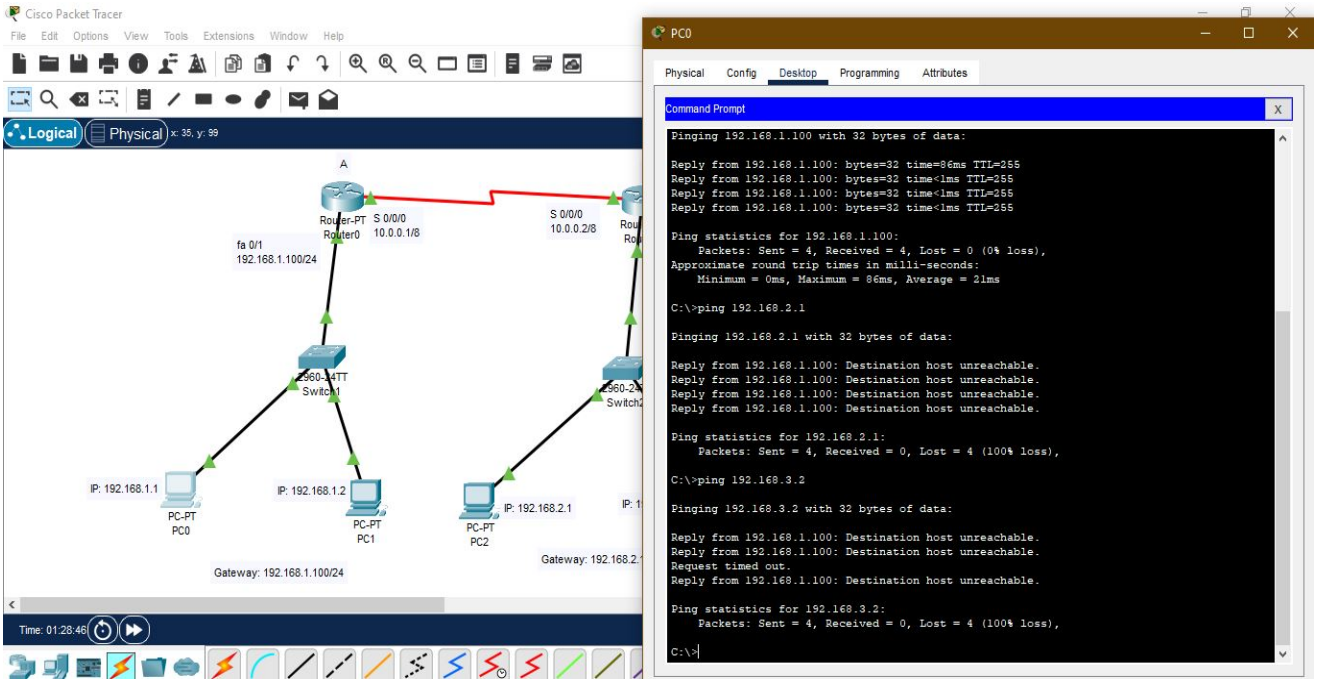
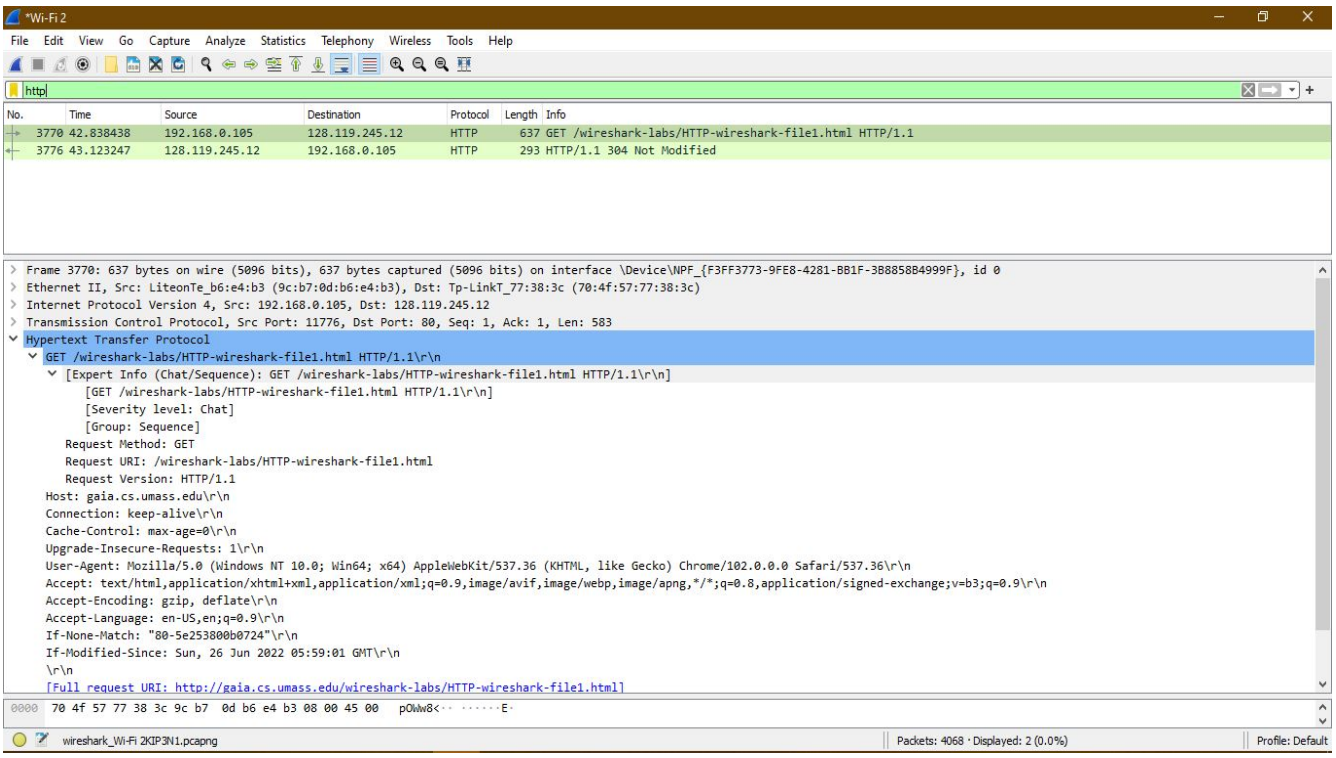


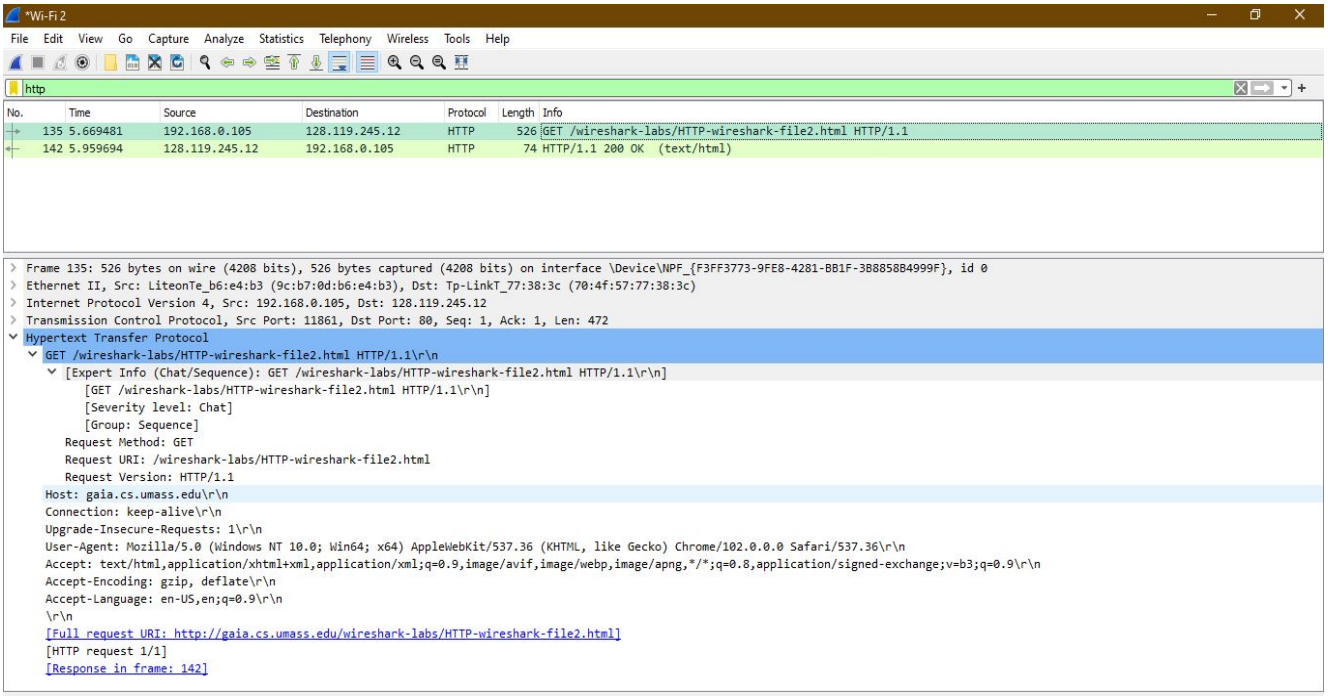

Fig. Ping test between PC0 to PC2 and PC0 to PC5

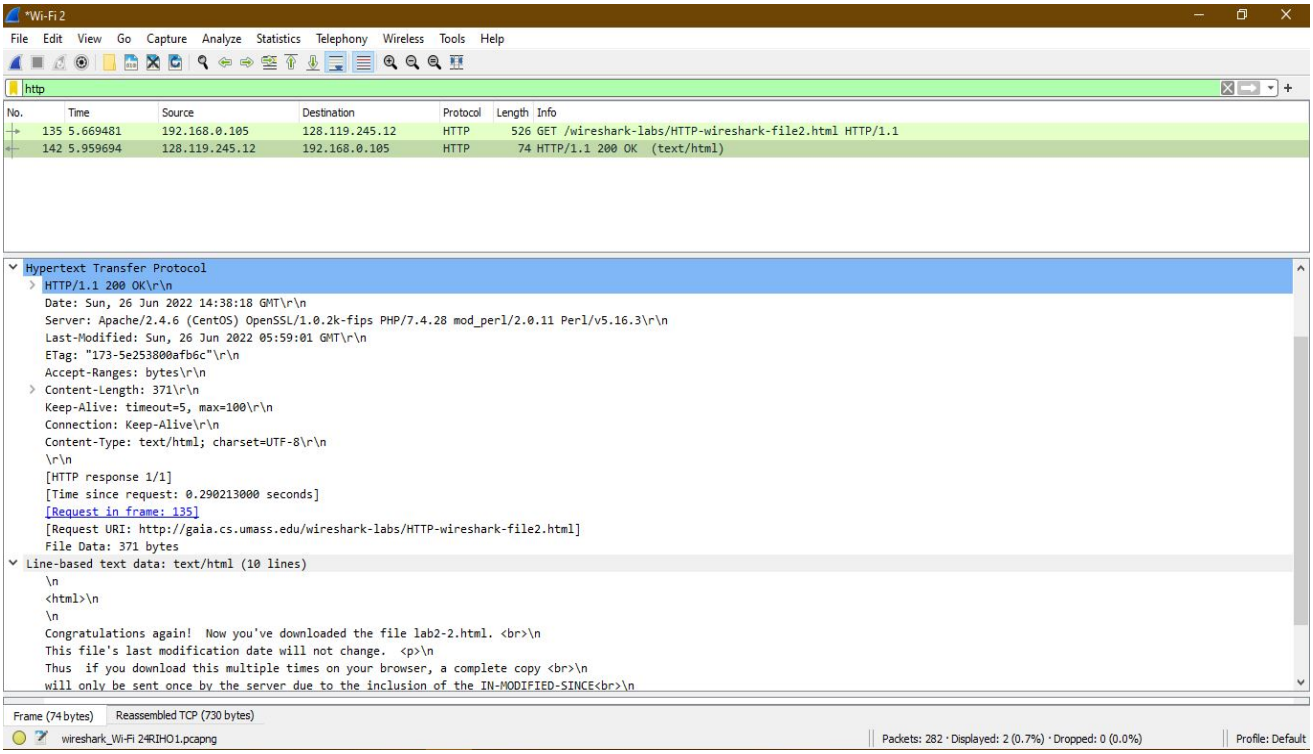
# Experiment – 10: Wireshark - HTTP

1.

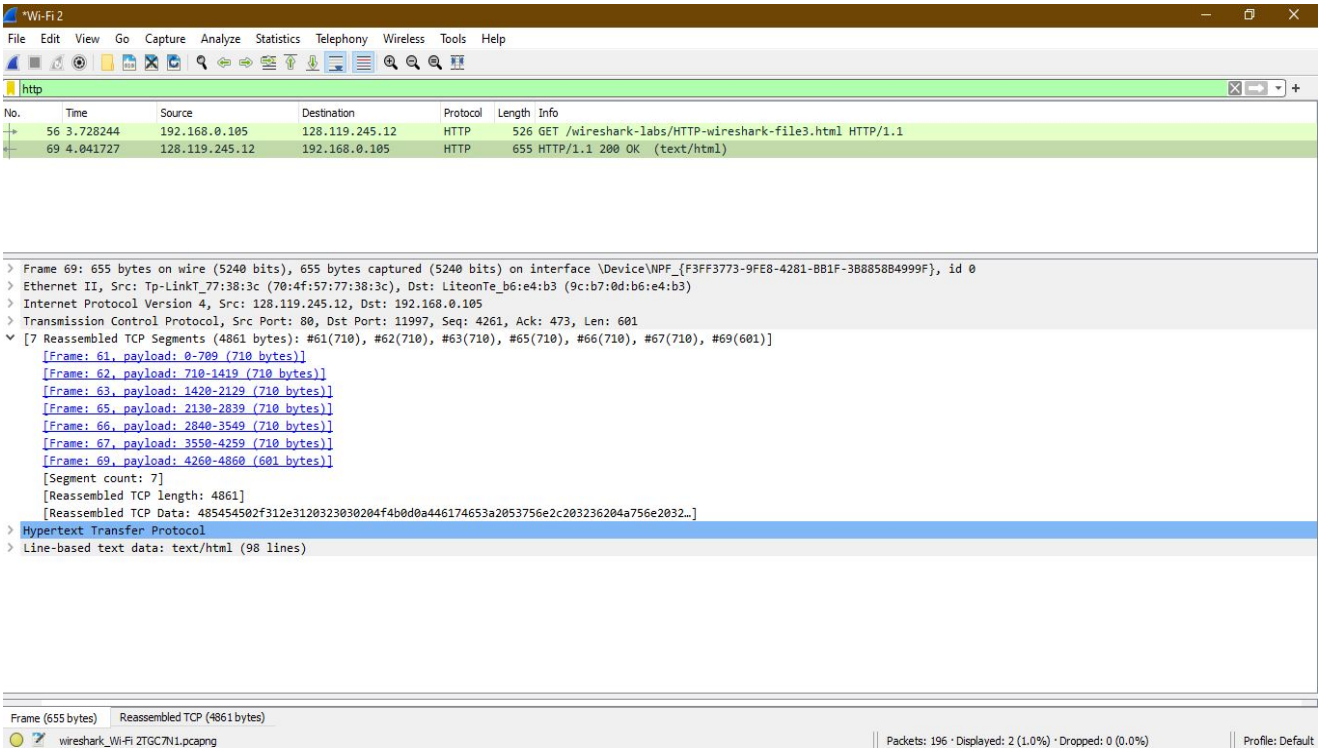



2.

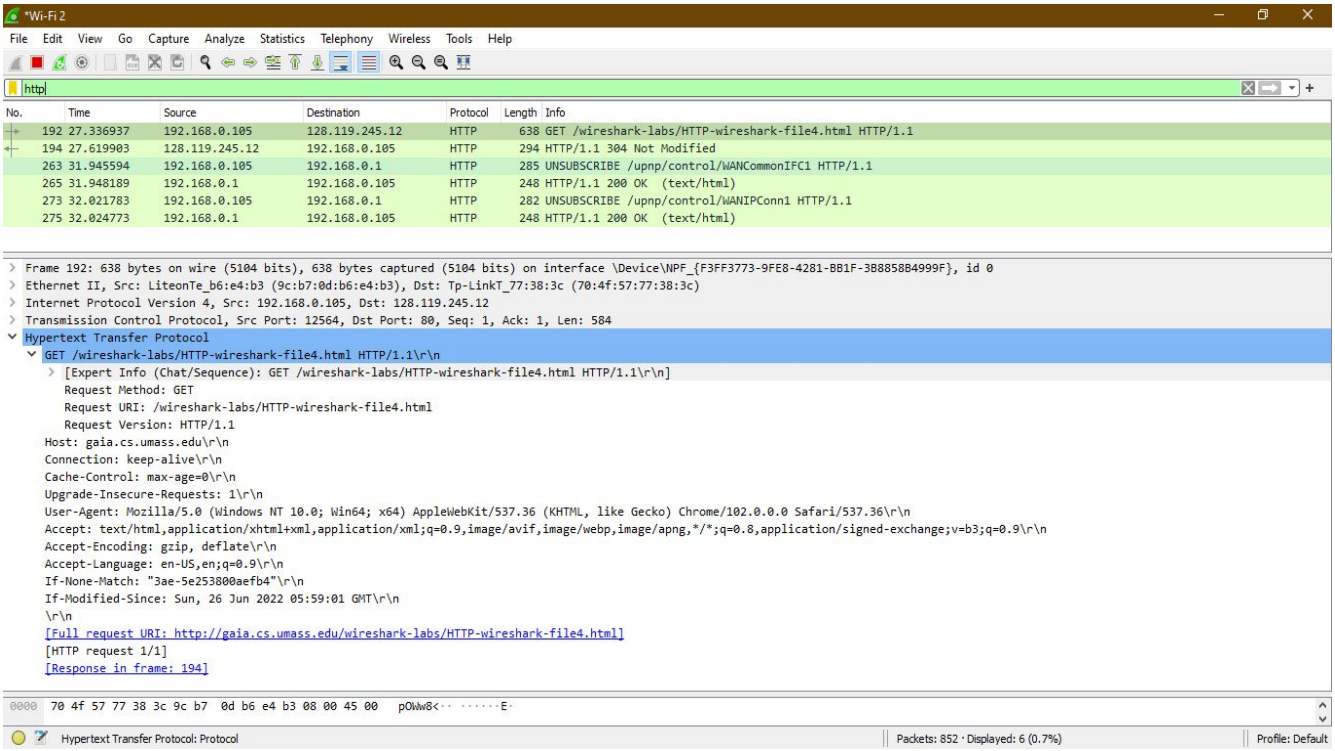



*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
135 5.669481 192.168.0.105 128.119.245.12 HTTP 526 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
142 5.959694 128.119.245.12 192.168.0.105 HTTP 74 HTTP/1.1 200 OK (text/html)
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 26 Jun 2022 14:38:18 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sun, 26 Jun 2022 05:59:01 GMT\r\n
ETag: "173-5e253800afb6c"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.290213000 seconds]
[Request in frame: 135]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
Frame (74 bytes)
Reassembled TCP (730 bytes)
wireshark_Wi-Fi 24RIHO1.pcapng
Packets: 282 · Displayed: 2 (0.7%) · Dropped: 0 (0.0%)
Profile: Default

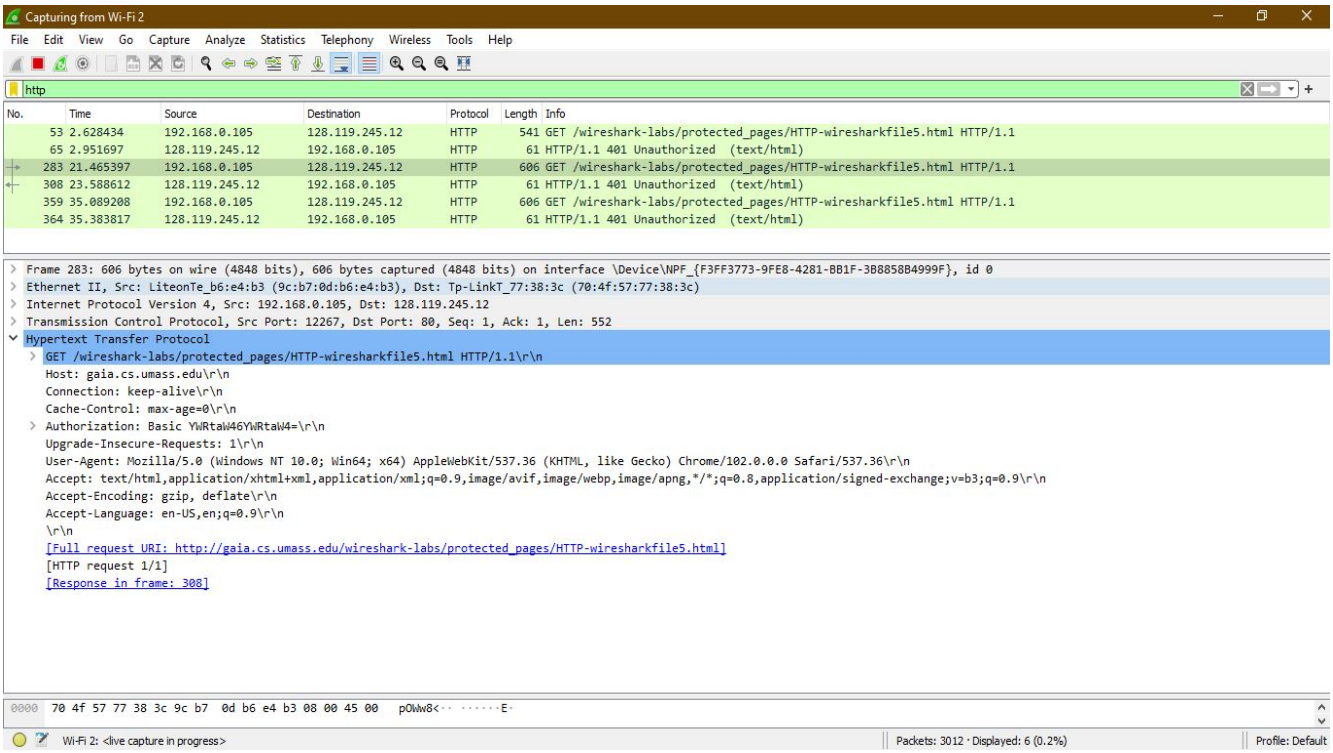
3.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
56 3.728244 192.168.0.105 128.119.245.12 HTTP 526 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
69 4.041727 128.119.245.12 192.168.0.105 HTTP 655 HTTP/1.1 200 OK (text/html)
Frame 69: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) on interface \Device\NPF_{F3FF3773-9FE8-4281-BB1F-3B8858B4999F}, id 0
Ethernet II, Src: Tp-LinkT_77:38:3c (70:4f:57:77:38:3c), Dst: LiteonTe_b6:e4:b3 (9c:b7:0d:b6:e4:b3)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.105
Transmission Control Protocol, Src Port: 80, Dst Port: 11997, Seq: 4261, Ack: 473, Len: 601
[7 Reassembled TCP Segments (4861 bytes): #61(710), #62(710), #63(710), #65(710), #66(710), #67(710), #69(601)]
[Frame: 61, payload: 0-709 (710 bytes)]
[Frame: 62, payload: 710-1419 (710 bytes)]
[Frame: 63, payload: 1420-2129 (710 bytes)]
[Frame: 65, payload: 2130-2839 (710 bytes)]
[Frame: 66, payload: 2840-3549 (710 bytes)]
[Frame: 67, payload: 3550-4259 (710 bytes)]
[Frame: 69, payload: 4260-4860 (601 bytes)]
[Segment count: 7]
[Reassembled TCP length: 4861]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203236204a756e2032…]
Hypertext Transfer Protocol
Line-based text data: text/html (98 lines)
Frame (655 bytes)
Reassembled TCP (4861 bytes)
wireshark_Wi-Fi 2TGC7N1.pcapng
Packets: 196 · Displayed: 2 (1.0%) · Dropped: 0 (0.0%)
Profile: Default

4.

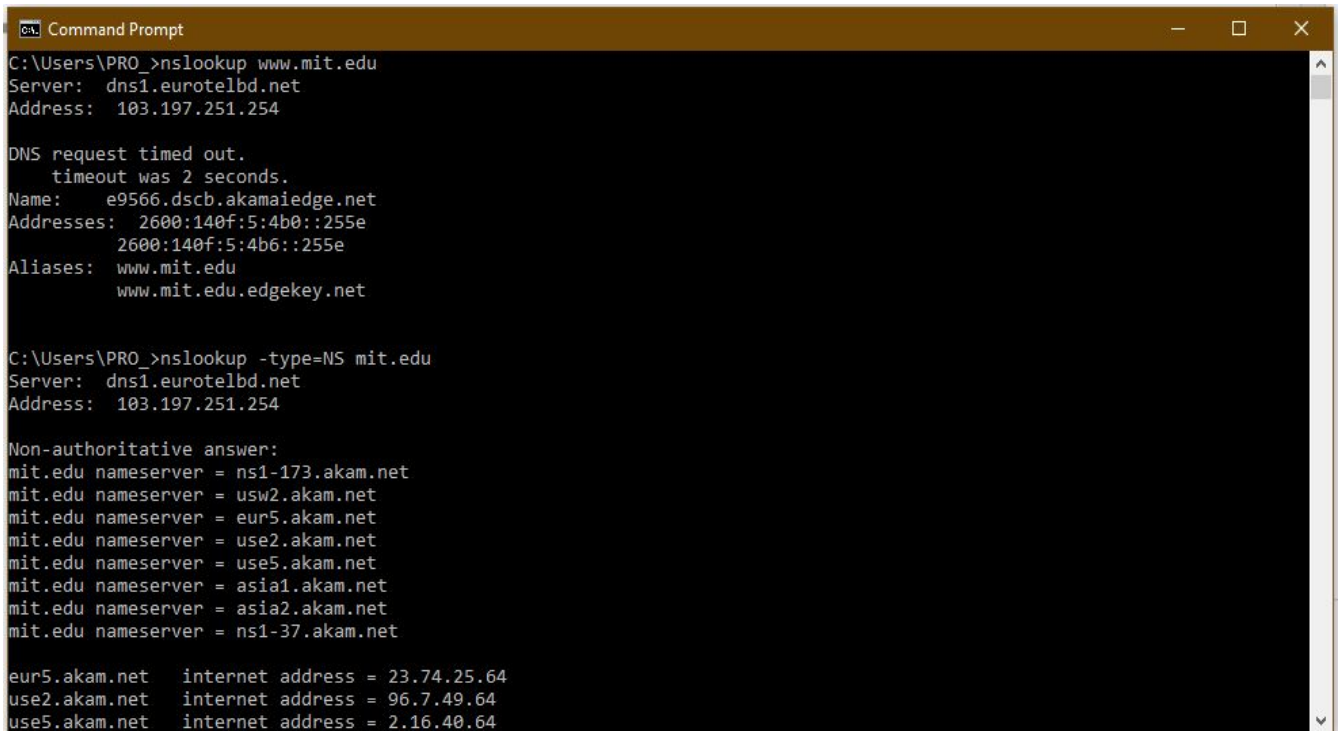

*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
192 27.336937 192.168.0.105 128.119.245.12 HTTP 638 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
194 27.619903 128.119.245.12 192.168.0.105 HTTP 294 HTTP/1.1 304 Not Modified
263 31.945594 192.168.0.105 192.168.0.1 HTTP 285 UNSUBSCRIBE /upnp/control/WANCommonIFC1 HTTP/1.1
265 31.948189 192.168.0.1 192.168.0.105 HTTP 248 HTTP/1.1 200 OK (text/html)
273 32.021783 192.168.0.105 192.168.0.1 HTTP 282 UNSUBSCRIBE /upnp/control/WANIPConn1 HTTP/1.1
275 32.024773 192.168.0.1 192.168.0.105 HTTP 248 HTTP/1.1 200 OK (text/html)
Frame 192: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF_{F3FF3773-9FE8-4281-BB1F-3B8858B4999F}, id 0
Ethernet II, Src: LiteonTe_b6:e4:b3 (9c:b7:0d:b6:e4:b3), Dst: Tp-LinkT_77:38:3c (70:4f:57:77:38:3c)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 12564, Dst Port: 80, Seq: 1, Ack: 1, Len: 584
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file4.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "3ae-5e253800aefb4"\r\n
If-Modified-Since: Sun, 26 Jun 2022 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
[HTTP request 1/1]
[Response in frame: 194]
0000 70 4f 57 77 38 3c 9c b7 0d b6 e4 b3 08 00 45 00 pOWw8<
Hypertext Transfer Protocol: Protocol
Packets: 852 · Displayed: 6 (0.7%)
Profile: Default

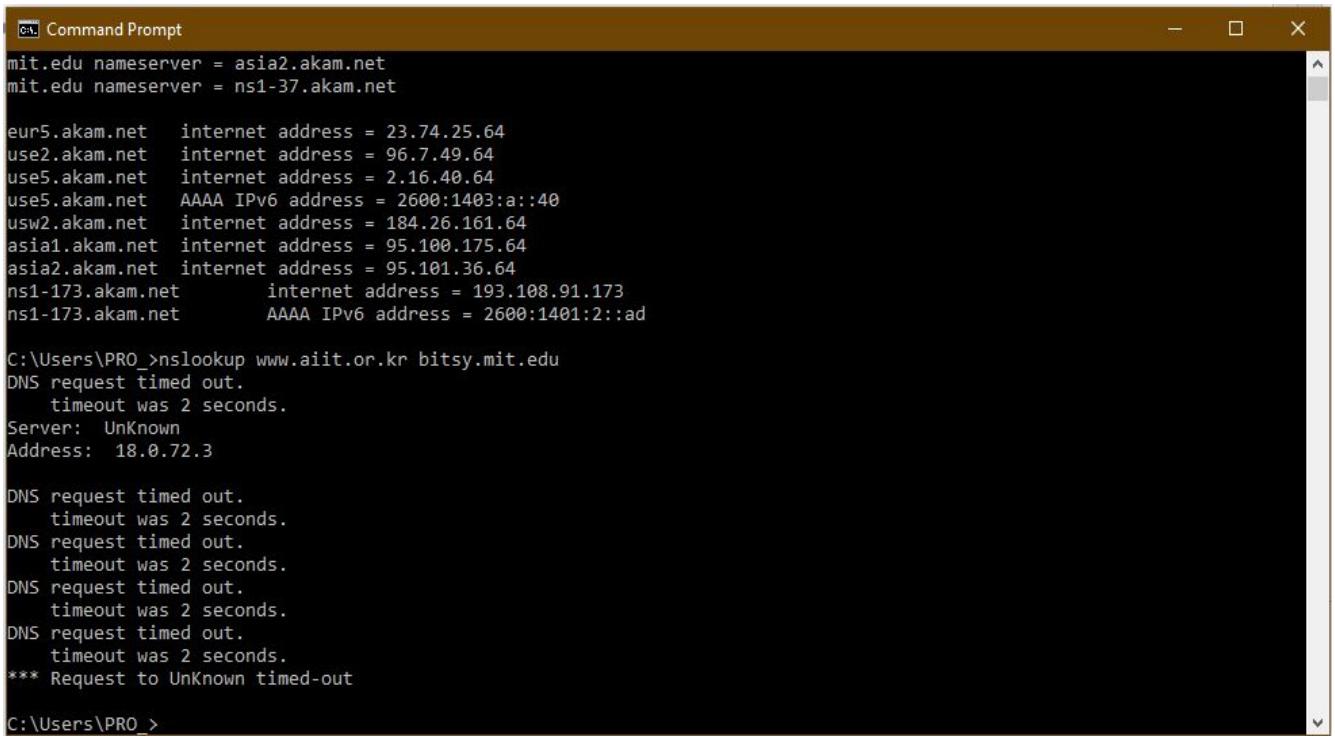
5.


Capturing from Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
53 2.628434 192.168.0.105 128.119.245.12 HTTP 541 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
65 2.951697 128.119.245.12 192.168.0.105 HTTP 61 HTTP/1.1 401 Unauthorized (text/html)
283 21.465397 192.168.0.105 128.119.245.12 HTTP 606 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
308 23.588612 128.119.245.12 192.168.0.105 HTTP 61 HTTP/1.1 401 Unauthorized (text/html)
359 35.089208 192.168.0.105 128.119.245.12 HTTP 606 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
364 35.383817 128.119.245.12 192.168.0.105 HTTP 61 HTTP/1.1 401 Unauthorized (text/html)
Frame 283: 606 bytes on wire (4848 bits), 606 bytes captured (4848 bits) on interface \Device\NPF_{F3FF3773-9FE8-4281-BB1F-3B8858B4999F}, id 0
Ethernet II, Src: LiteonTe_b6:e4:b3 (9c:b7:0d:b6:e4:b3), Dst: Tp-LinkT_77:38:3c (70:4f:57:77:38:3c)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 12267, Dst Port: 80, Seq: 1, Ack: 1, Len: 552
Hypertext Transfer Protocol
GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic YWRtaW46YWRtaW4=\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
[HTTP request 1/1]
[Response in frame: 308]
0000 70 4f 57 77 38 3c 9c b7 0d b6 e4 b3 08 00 45 00 pOWw8<
Wi-Fi 2: <live capture in progress>
Packets: 3012 · Displayed: 6 (0.2%)
Profile: Default

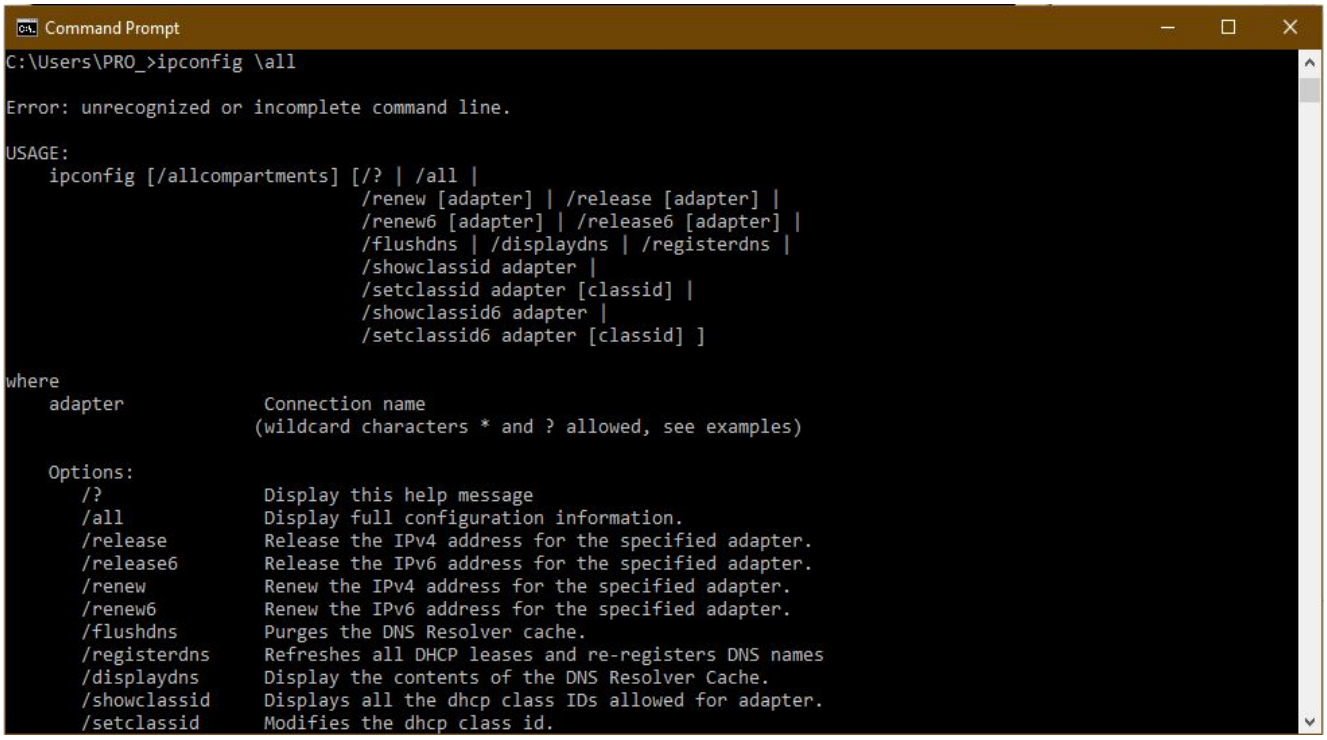
# Experiment – 11: Wireshark - DNS

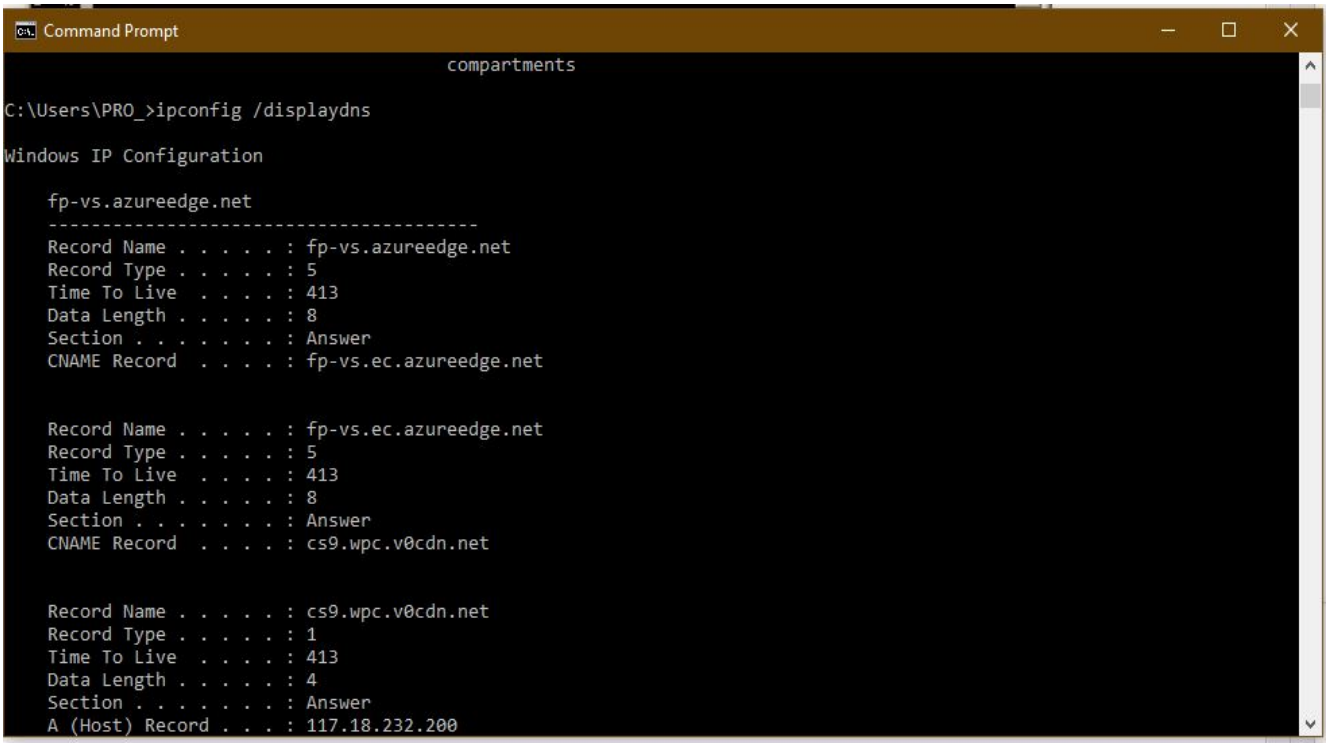
1.

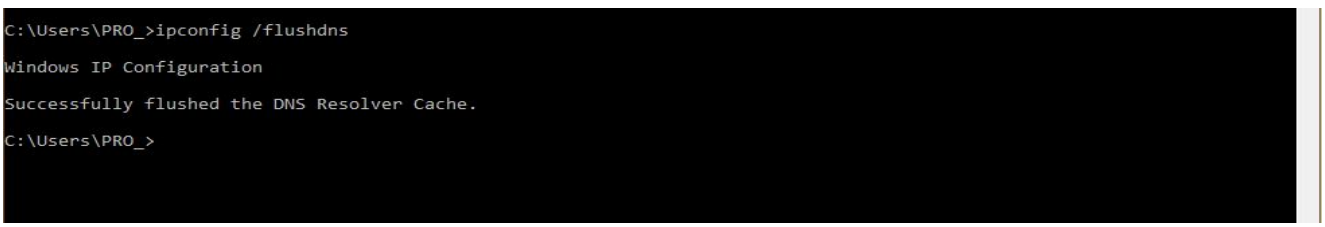


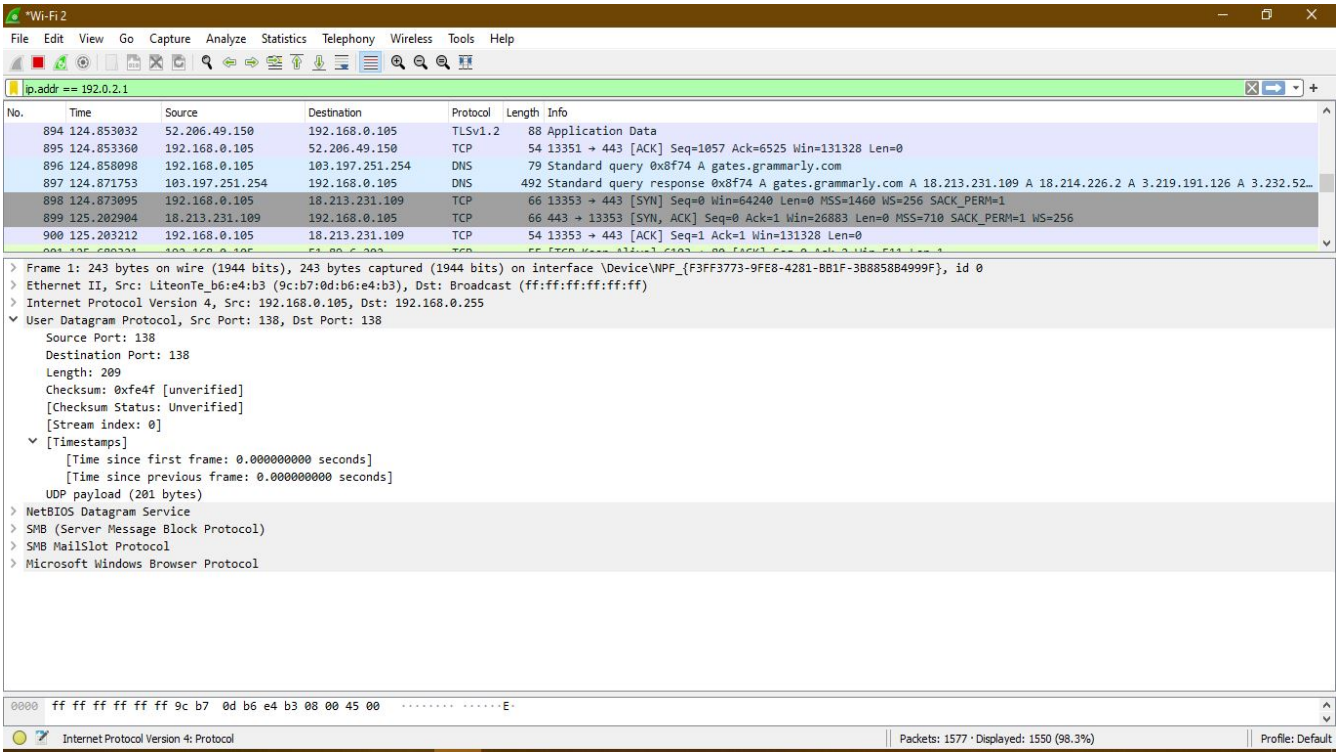
2.

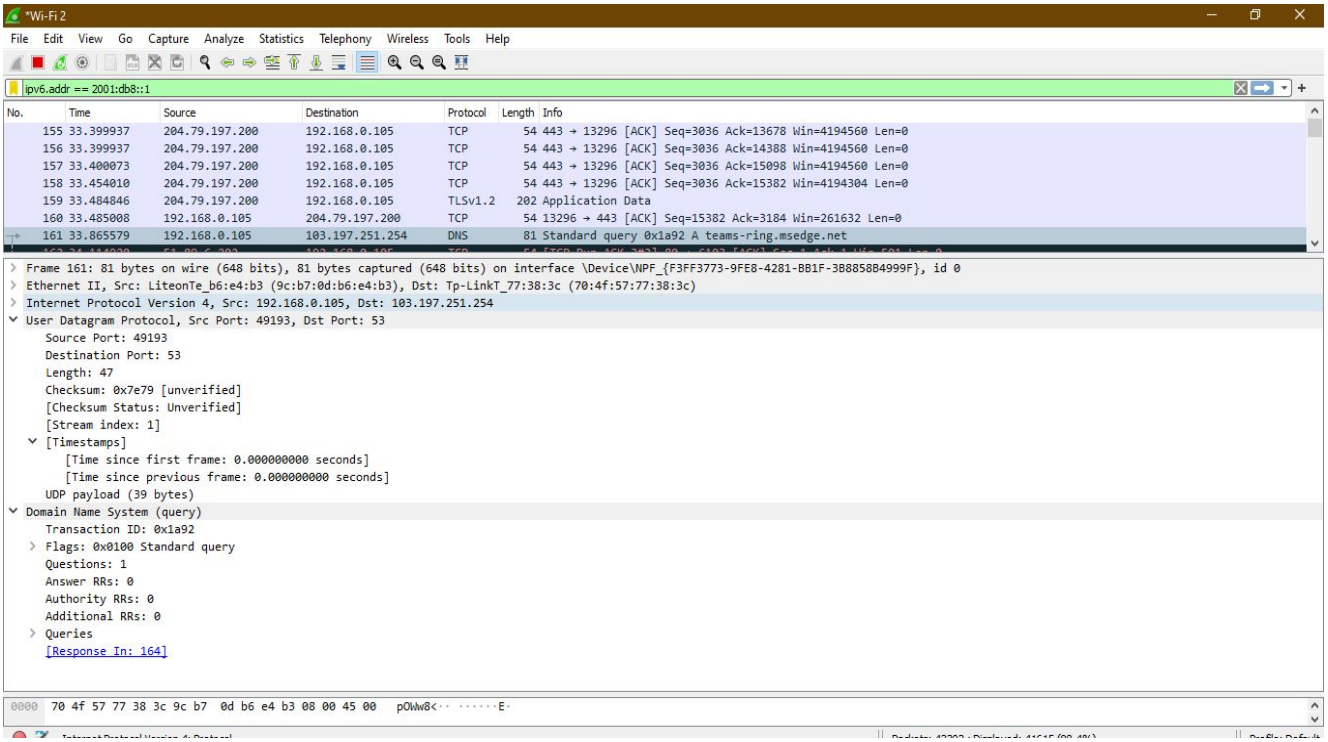

Command Prompt
C:\Users\PRO_>ipconfig \all
Error: unrecognized or incomplete command line.
USAGE:
ipconfig [/allcompartments] [/? | /all |
/renew [adapter] | /release [adapter] |
/renew6 [adapter] | /release6 [adapter] |
/flushdns | /displaydns | /registerdns |
/showclassid adapter |
/setclassid adapter [classid] |
/showclassid6 adapter |
/setclassid6 adapter [classid] ]
where
adapter Connection name
(wildcard characters * and ? allowed, see examples)
Options:
/? Display this help message
/all Display full configuration information.
/release Release the IPv4 address for the specified adapter.
/release6 Release the IPv6 address for the specified adapter.
/renew Renew the IPv4 address for the specified adapter.
/renew6 Renew the IPv6 address for the specified adapter.
/flushdns Purges the DNS Resolver cache.
/registerdns Refreshes all DHCP leases and re-registers DNS names
/displaydns Display the contents of the DNS Resolver Cache.
/showclassid Displays all the dhcp class IDs allowed for adapter.
/setclassid Modifies the dhcp class id.


Command Prompt
compartments
C:\Users\PRO_>ipconfig /displaydns
Windows IP Configuration
fp-vs.azureedge.net
Record Name . . . . . : fp-vs.azureedge.net
Record Type . . . . . : 5
Time To Live . . . . : 413
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : fp-vs.ec.azureedge.net
Record Name . . . . . : fp-vs.ec.azureedge.net
Record Type . . . . . : 5
Time To Live . . . . : 413
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : cs9.wpc.v0cdn.net
Record Name . . . . . : cs9.wpc.v0cdn.net
Record Type . . . . . : 1
Time To Live . . . . : 413
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 117.18.232.200


C:\Users\PRO_>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\PRO_>

3.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.0.2.1
No. Time Source Destination Protocol Length Info
894 124.853032 52.206.49.150 192.168.0.105 TLSv1.2 88 Application Data
895 124.853360 192.168.0.105 52.206.49.150 TCP 54 13351 → 443 [ACK] Seq=1057 Ack=6525 Win=131328 Len=0
896 124.858098 192.168.0.105 103.197.251.254 DNS 79 Standard query 0x8f74 A gates.grammarly.com
897 124.871753 103.197.251.254 192.168.0.105 DNS 492 Standard query response 0x8f74 A gates.grammarly.com A 18.213.231.109 A 18.214.226.2 A 3.219.191.126 A 3.232.52…
898 124.873095 192.168.0.105 18.213.231.109 TCP 66 13353 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
899 125.202904 18.213.231.109 192.168.0.105 TCP 66 443 → 13353 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=710 SACK_PERM=1 WS=256
900 125.203212 192.168.0.105 18.213.231.109 TCP 54 13353 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{F3FF3773-9FE8-4281-BB1F-3B8858B4999F}, id 0
Ethernet II, Src: LiteonTe_b6:e4:b3 (9c:b7:0d:b6:e4:b3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
Source Port: 138
Destination Port: 138
Length: 209
Checksum: 0xfe4f [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]
UDP payload (201 bytes)
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 9c b7 0d b6 e4 b3 08 00 45 00
Internet Protocol Version 4: Protocol
Packets: 1577 · Displayed: 1550 (98.3%)
Profile: Default


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ipv6.addr == 2001:db8::1
No. Time Source Destination Protocol Length Info
155 33.399937 204.79.197.200 192.168.0.105 TCP 54 443 → 13296 [ACK] Seq=3036 Ack=13678 Win=4194560 Len=0
156 33.399937 204.79.197.200 192.168.0.105 TCP 54 443 → 13296 [ACK] Seq=3036 Ack=14388 Win=4194560 Len=0
157 33.400073 204.79.197.200 192.168.0.105 TCP 54 443 → 13296 [ACK] Seq=3036 Ack=15098 Win=4194560 Len=0
158 33.454010 204.79.197.200 192.168.0.105 TCP 54 443 → 13296 [ACK] Seq=3036 Ack=15382 Win=4194304 Len=0
159 33.484846 204.79.197.200 192.168.0.105 TLSv1.2 202 Application Data
160 33.485008 192.168.0.105 204.79.197.200 TCP 54 13296 → 443 [ACK] Seq=15382 Ack=3184 Win=261632 Len=0
161 33.865579 192.168.0.105 103.197.251.254 DNS 81 Standard query 0x1a92 A teams-ring.msedge.net
Frame 161: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{F3FF3773-9FE8-4281-BB1F-3B8858B4999F}, id 0
Ethernet II, Src: LiteonTe_b6:e4:b3 (9c:b7:0d:b6:e4:b3), Dst: Tp-LinkT_77:38:3c (70:4f:57:77:38:3c)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 103.197.251.254
User Datagram Protocol, Src Port: 49193, Dst Port: 53
Source Port: 49193
Destination Port: 53
Length: 47
Checksum: 0x7e79 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]
UDP payload (39 bytes)
Domain Name System (query)
Transaction ID: 0x1a92
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 164]
0000 70 4f 57 77 38 3c 9c b7 0d b6 e4 b3 08 00 45 00