EXPERIMENT NO. 3

Title: Capturing Packet in Live Traffic

Objective: To Capture the packets in live traffic using tools like Wireshark

AIM: Observe and note the details of the live type of traffic (ARP, Frame analysis, ethernet) from interface using packet capture and analysis tool

THEORY:

Requirements:

Wireshark: Wireshark software tool to capture and examine a packet trace.

arp: "arp" command-line utility to inspect and clear the cache used by the ARP protocol on your computer.

ifconfig / ipconfig: "ipconfig" (Windows) command-line utility to inspect the state of your computer's network interface.

route / netstat: "route" or "netstat" command-line utility to inspect the routes used by your computer.

Network Setup

ARP protocol in action is to be observed. ARP is used to find the Ethernet address that corresponds to a local IP address to which a computer wants to send a packet. A typical example of a local IP address is that of the local router or default gateway that connects a computer to the rest of the Internet. The defined computer caches these translations in an ARP cache so that the ARP protocol need only be used occasionally to do the translation. The setup from the viewpoint of your computer is as shown in the example below.

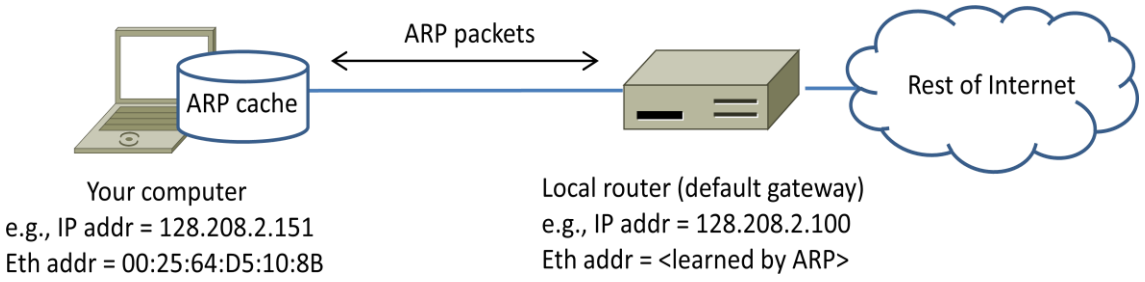


Figure 1: Network setup under which we will study ARP in second part

How ARP Works

When an incoming packet destined for a host machine on a particular local area network arrives ata gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.

A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied. There is a Reverse ARP (RARP) for host machines that don't know their IP address. RARP enables them to request their IP address from the gateway's ARP cache.

Step 1: Finding your IP address and Gateway address

1. Open a command prompt as an administrator as follows:

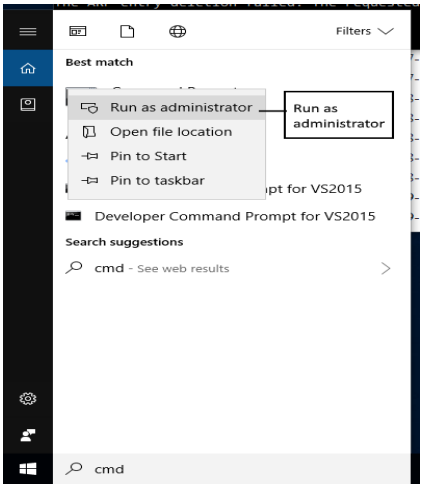


Figure 2: Finding the computer's Ethernet address with ipconfig (Windows)

2. Find the **Ethernet** address of the main network interface OR

the **wireless** address withthe ipconfig command. On Windows, bring up a command-line shell and type “ipconfig /all”. Common names for the interface are “eth0” or “Ethernet adapter”. An ex ample is shown below in figure 2, with added highlighting.

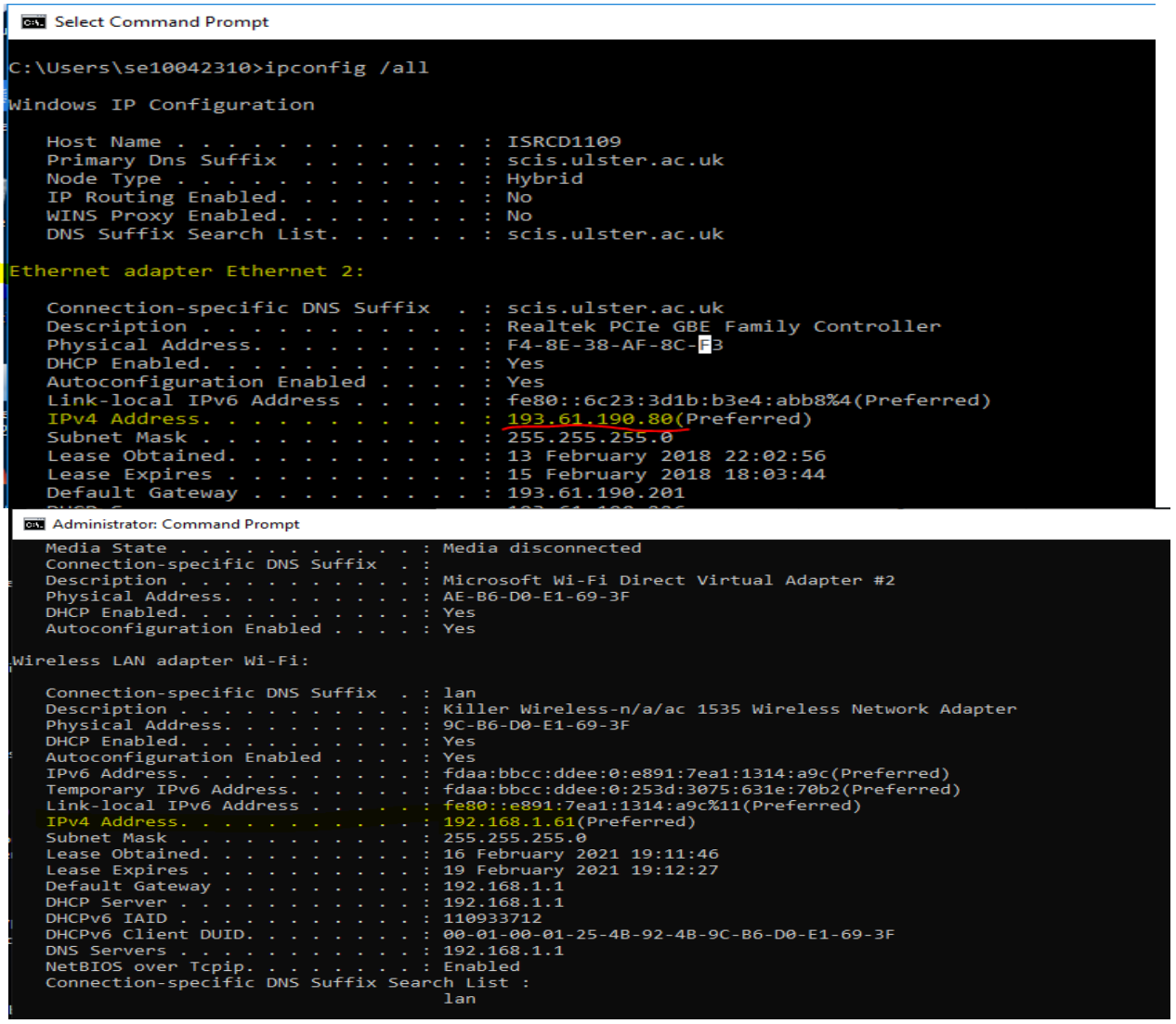


Figure 3: Finding the computer's WiFi IP address with ipconfig (Windows)

3. Find the IP address of the local router or default gateway that your computer uses to reach the rest of the Internet using the netstat / route command. You should be able touse the netstat-r command on Windows.

   Alternatively, you can use the route command ("route print" on Windows). In either case you are looking for the gateway IP address that corresponds to the destination of default or 0.0.0.0. An example is shown in figure 3 for netstat, with added highlighting.

```
C:\Users\se10042310>netstat -r
===========================================================================
Interface List
  4...f4 8e 38 af 8c f3 ......Realtek PCIe GBE Family Controller
  3...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  6...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   193.61.190.201    193.61.190.80     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.139.0    255.255.255.0         On-link     192.168.139.1    291
    192.168.139.1  255.255.255.255         On-link     192.168.139.1    291
  192.168.139.255  255.255.255.255         On-link     192.168.139.1    291
    192.168.159.0    255.255.255.0         On-link     192.168.159.1    291
    192.168.159.1  255.255.255.255         On-link     192.168.159.1    291
  192.168.159.255  255.255.255.255         On-link     192.168.159.1    291
```

Figure 4: Finding the default gateway IP address with netstat(Windows)

4. Now **run Wireshark** by typing "*wireshark*" in the bottom left search box inWindows

5. You should see the main Wireshark interface. **Click on the Ethernet OR Wireless interface** to start traffic analysis on that interface.

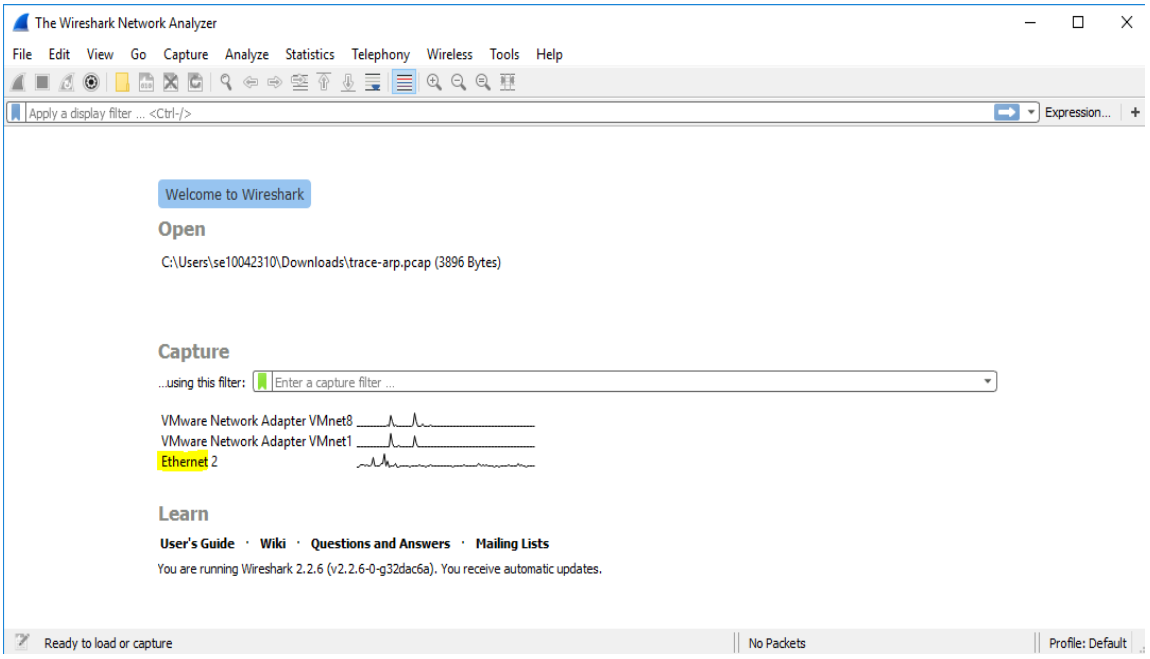


Figure 5: Applying a filter

6. Add a filter of "arp".

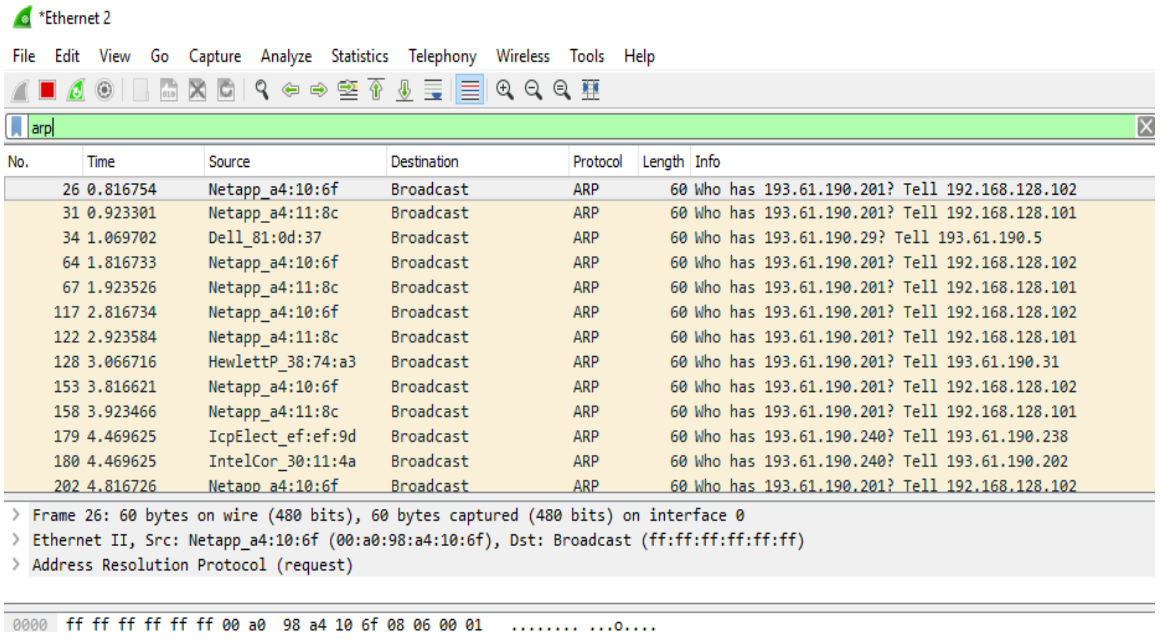
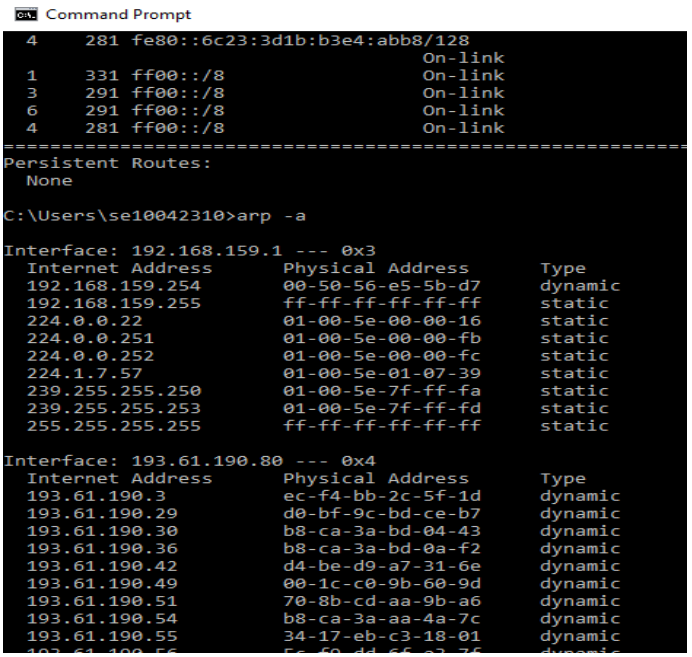
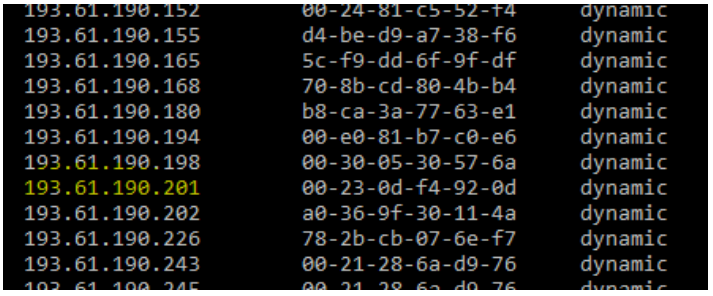


Figure 6: Setting up the capture options

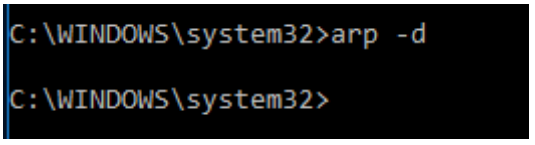
7. When the capture is started, use the "arp" command to clear the default gateway from the ARPcache. Using the command "arp –a" will show you the contents of the ARP cacheasa check that you can run "arp". Go to command prompt and type **arp -a** as shown below.


Command Prompt
4 281 fe80::6c23:3d1b:b3e4:abb8/128
On-link
1 331 ff00::/8 On-link
3 291 ff00::/8 On-link
6 291 ff00::/8 On-link
4 281 ff00::/8 On-link
Persistent Routes:
None
C:\Users\se10042310>arp -a
Interface: 192.168.159.1 --- 0x3
Internet Address Physical Address Type
192.168.159.254 00-50-56-e5-5b-d7 dynamic
192.168.159.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
224.1.7.57 01-00-5e-01-07-39 static
239.255.255.250 01-00-5e-7f-ff-fa static
239.255.255.253 01-00-5e-7f-ff-fd static
255.255.255.255 ff-ff-ff-ff-ff-ff static
Interface: 193.61.190.80 --- 0x4
Internet Address Physical Address Type
193.61.190.3 ec-f4-bb-2c-5f-1d dynamic
193.61.190.29 d0-bf-9c-bd-ce-b7 dynamic
193.61.190.30 b8-ca-3a-bd-04-43 dynamic
193.61.190.36 b8-ca-3a-bd-0a-f2 dynamic
193.61.190.42 d4-be-d9-a7-31-6e dynamic
193.61.190.49 00-1c-c0-9b-60-9d dynamic
193.61.190.51 70-8b-cd-aa-9b-a6 dynamic
193.61.190.54 b8-ca-3a-aa-4a-7c dynamic
193.61.190.55 34-17-eb-c3-18-01 dynamic

You should see an entry for the IP address of the default gateway as shown in image below. In this case it is 193.61.190.201 which is the default gateway on my office PC.



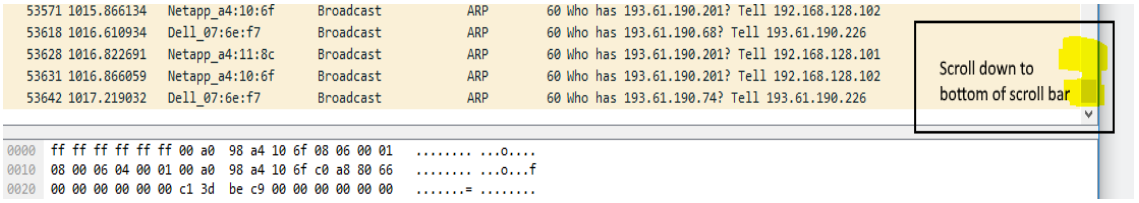
8. To clear this entry, use the arp command with different arguments ("arp –d" on Windows) as follows. Type **arp -d** in the command prompt.



Note: This usage of arp will need administrator privileges to run, so you have to run as a privi- leged user on Windows which is what you should have done in step 1. The command should run without error, but the ARP entry may not appear to be cleared if you check with "arp –a". This is because your computer will send ARP packets to repopulate this entry as soon as you need to send a packet to a remote IP address, and that can happen very quickly due to background activity on the computer.

Now that you have cleared your ARP cache, **fetch a remote page with your Web browser**. This will cause ARP to find the Ethernet address of the default gateway so that the packets can be sent.

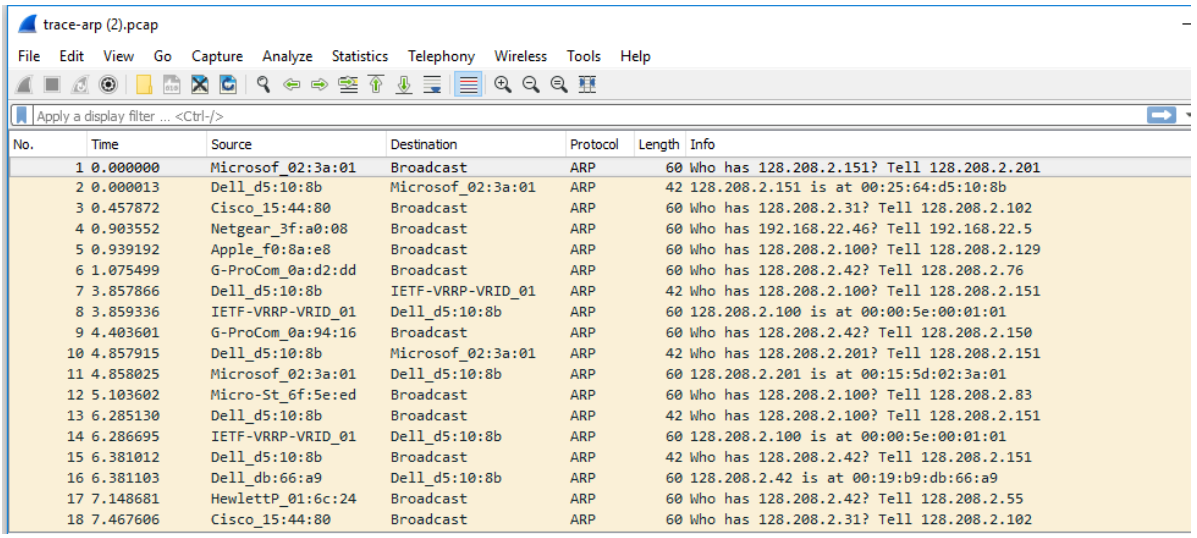
9. You will see these packets flowing through your computer by scrolling down in the Wireshark window to the bottom as shown below.



10. These ARP packets will be captured by Wireshark. You might clear the ARP cache and fetch a document a couple of times. Hopefully there will also be other ARP packets sent by other computers on the local network that will be captured. These packets are likely to be present if there are other computers on your local network. In fact, if you have a busy computer and extensive local network then you may capture many ARP packets. The ARP traffic of other computers will be captured when the ARP packets are sent to the broadcast address, since in this case they are destined for all computers including the one on which you are running Wireshark. Because ARP activity happens slowly, you may need to wait up to 30 seconds to observe some of this back- ground ARP traffic.
11. Once you have captured some ARP traffic, stop the capture. You will need the trace, plus the Ethernet address of your computer and the IP address of the default gateway for the next steps.

Step 2: Inspect the supplied ARP Trace

1. **Close** Wireshark.
2. Once Wireshark is closed, **open** the ARP trace here:
3. You should see a screen as shown below.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Microsof_02:3a:01	Broadcast	ARP	60	Who has 128.208.2.151? Tell 128.208.2.201
2	0.000013	Dell_d5:10:8b	Microsof_02:3a:01	ARP	42	128.208.2.151 is at 00:25:64:d5:10:8b
3	0.457872	Cisco_15:44:80	Broadcast	ARP	60	Who has 128.208.2.31? Tell 128.208.2.102
4	0.903552	Netgear_3f:a0:08	Broadcast	ARP	60	Who has 192.168.22.46? Tell 192.168.22.5
5	0.939192	Apple_f0:8a:e8	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.129
6	1.075499	G-ProCom_0a:d2:dd	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.76
7	3.857866	Dell_d5:10:8b	IETF-VRRP-VRID_01	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
8	3.859336	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
9	4.403601	G-ProCom_0a:94:16	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.150
10	4.857915	Dell_d5:10:8b	Microsof_02:3a:01	ARP	42	Who has 128.208.2.201? Tell 128.208.2.151
11	4.858025	Microsof_02:3a:01	Dell_d5:10:8b	ARP	60	128.208.2.201 is at 00:15:5d:02:3a:01
12	5.103602	Micro-St_6f:5e:ed	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.83
13	6.285130	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
14	6.286695	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
15	6.381012	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.42? Tell 128.208.2.151
16	6.381103	Dell_db:66:a9	Dell_d5:10:8b	ARP	60	128.208.2.42 is at 00:19:b9:db:66:a9
17	7.148681	HewlettP_01:6c:24	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.55
18	7.467606	Cisco_15:44:80	Broadcast	ARP	60	Who has 128.208.2.31? Tell 128.208.2.102

The setup from the viewpoint of your computer from this trace is shown in the example below.

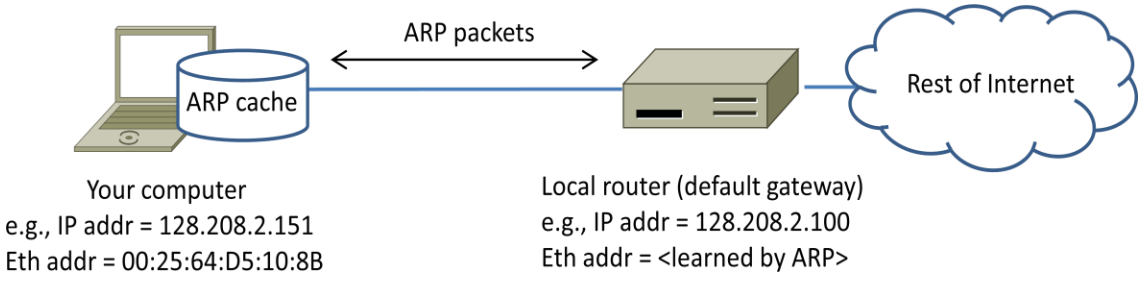


Figure 7: Network setup under which we will study ARP in thispart Note: **Ethernet address** of computer: 00:25:64:d5:10:8b and IP address of **gateway**:128.208.2.100

4. Now we can look at an ARP exchange. Since there may be many ARP packets in your trace, we'll first narrow our view to only the ARP packets that are sent directly from or to your computer.

Set a display filter for packets with the Ethernet address of your computer which is this case is

00:25:64:d5:10:8b.

You can do this by entering an expression in the blank "Filter:" box near the top of the Wireshark window and clicking "Apply" or Enter. After applying this filter your capture should look something like the figure below, in which we have expanded the ARP protocol details.

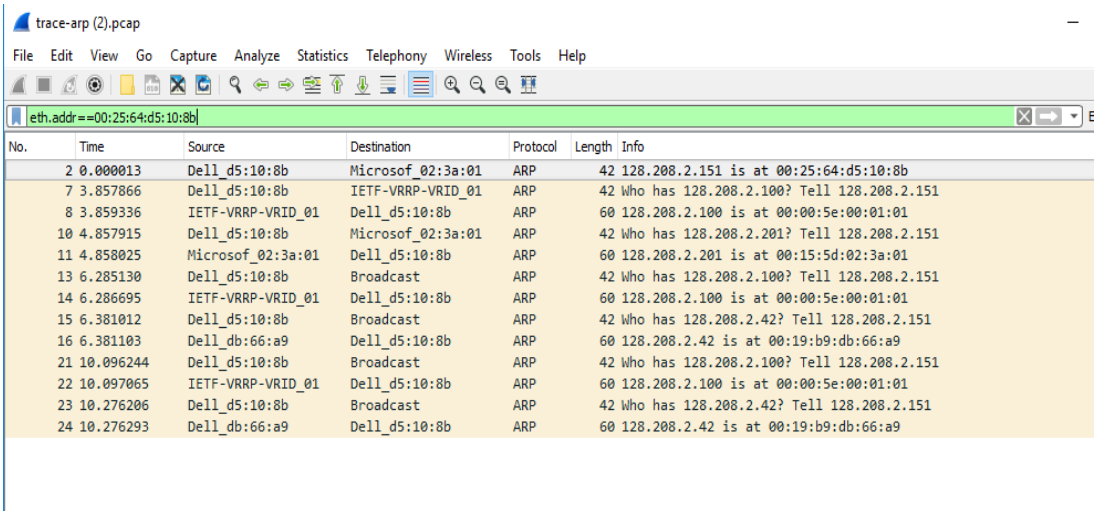


Figure 8: Capture of ARP packets, showing details of a request

Find and select an ARP request for the default gateway and examine its fields. There are two kinds of ARP packets, a request and a reply, Next come the four key fields, the sender MAC (Ethernet) and IP and the target MAC (Ethernet) and IP. These fields are filled in as much as possible. For a request, the sender knows their MAC and IP address and fills them in. The sender also knows the target IP address – it is the IP address for which an Ethernet address is wanted. But the sender does not know the target MAC

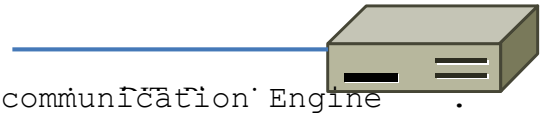
Step 3: Details of ARP over Ethernet

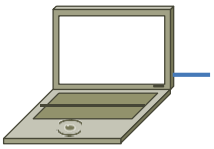
ARP packets are carried in Ethernet frames, and the values of the Ethernet header fields are chosen to support ARP. For instance, you may wonder how an ARP request packet is delivered to the target computer so that it can reply and tell the requestor its MAC address. The answer is that the ARP request is (normally) broadcast at the Ethernet layer so that it is received by all computers on the local network including the target. Look specifically at the destination Ethernet address of a request: it is set to ff:ff:ff:ff:ff:ff, the broadcast address. So, the target receives the request and recognizes that it is the in- tended recipient of the message; other computers that receive the request know that it is not meant for them. Only the target responds with a reply. However, anyone who receives an ARP packet can learn a mapping from it: the sender MAC and sender IP pair. The ARPheader for a request and a reply is 28 bytes for both the request and reply for IPv4.

Answers to Step 3: ARP request and reply

Your computer Sender MAC=00:25:64:D5:10:8BSender IP=128.208.2.151

Target MAC=00:00:00:00:00:00 Target IP=128.208.2.1





Default gateway

Reply

Sender MAC=00:00:5E:00:00:01

Sender
IP=128.208.
2.10 0
Target
MAC=00:25:64:D5
:1 0:
8B Target

IP=128.208.2.151

Figure 9: Details of the ARP request and reply to resolve the default gateway

There are several features to note:

- On the request, the target MAC is not known so it is usually filled in as 00:00:00:00:00:00.
- On the reply, the request target becomes the reply sender and vice versa.
- On the reply, the sender MAC returns the answer that is sought; it ishighlighted.
- All of the fields that are shown are ARP header fields

CONCLUSION:

EXPERIMENT NO.4

TITLE: Using a Network Simulator (e.g., packet tracer) Configure router using RIP

OBJECTIVE: To Configure and analyze the performance of the Routing Information Protocol (RIP) .

AIM: Installation and configuration of RIP using Cisco packet tracer.

SOFTWARE USED: Cisco packet Tracer

HARDWARE USED:

- Operating System: Windows XP/Vista/7/8,10
- Memory (RAM): 512MB of RAM required.
- Hard Disk Space: 300MB of free space required.
- Processor: Intel Pentium 4 or later.

THEORY:

A router in the network needs to be able to look at the destination address in the packet and then determine which one of the output ports is the best choice to get the packet to that address. The router makes this decision by consulting a forwarding table. The fundamental problem of routing is: How do routers acquire the information in their forwarding tables? Routing algorithms are required to build the routing tables and, hence, forwarding tables. The basic problem of routing is to find the lowest-cost path between any two nodes, where the cost

of a path equals the sum of the costs of all the edges that make up the path. Routing is achieved in most practical networks by running routing protocols among the nodes. The protocols provide a distributed, dynamic way to solve the problem of finding the lowest-cost path in the presence of link and node failures and changing edge costs. One of the main classes of routing algorithms is the distance-vector algorithm. Each node constructs a vector containing the distances (costs) to all other nodes and distributes that vector to its immediate neighbors. RIP is the canonical example of a routing protocol built on the distance-vector algorithm. Routers running RIP send their advertisements regularly (e.g., every 30 s). A router also sends an update message whenever a triggered update from another router causes it to change its routing table. The Internet Control Message Protocol (ICMP) can be utilized to analyze the performance of the created routes. It can be used to model traffic between routers without the need for running applications in an end node. In this lab, you will set up a network that utilizes RIP as its routing protocol. You will analyze the routing tables generated in the routers, and you will observe how RIP is affected by link failures.

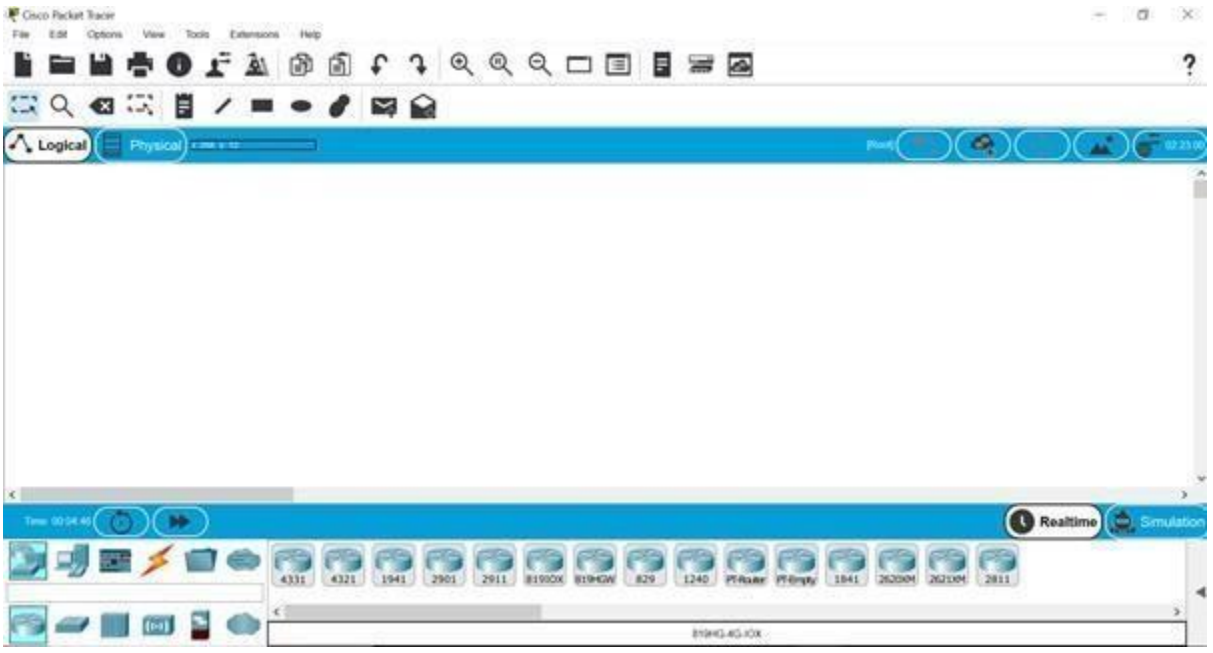
RIP (Routing Information Protocol) RIP is a standardized Distance Vector protocol, designed for use on smaller networks. RIP was one of the first true Distance Vector routing protocols, and is supported on a wide variety of systems.

RIP adheres to the following Distance Vector characteristics:

- RIP sends out periodic routing updates (every 30 seconds)
- RIP sends out the full routing table every periodic update
- RIP uses a form of distance as its metric (in this case, hop count)
- RIP uses the Bellman-Ford Distance Vector algorithm to determine the best “path” to a particular destination.

PROCEDURE:

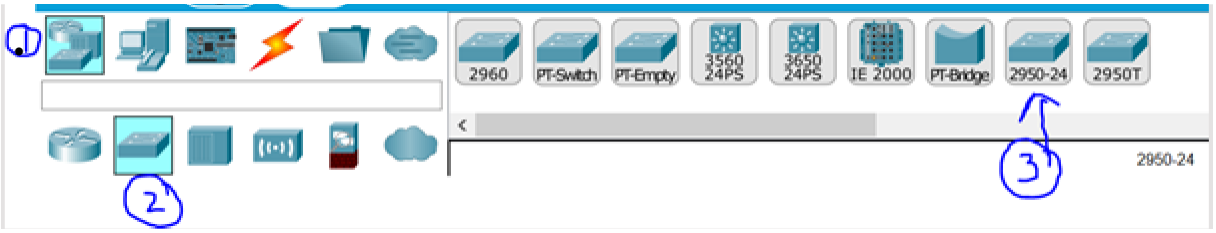
STEP 1: OPEN CISCO PACKET TRACER



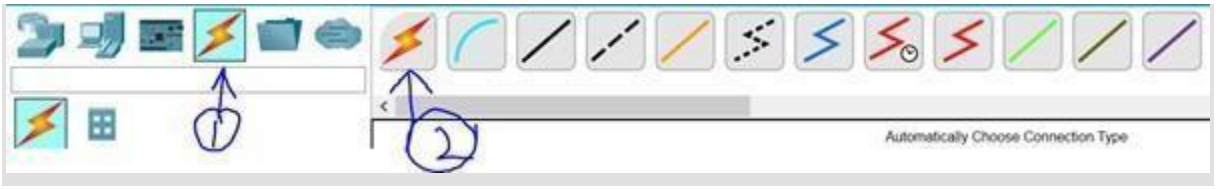
Blank Cisco Packet Tracer

STEP 2: MAKE CONNECTIONS: As shown in the figure below, go to (1) End Devices and select (2) PC and then finally drag and drop PC on Screen.

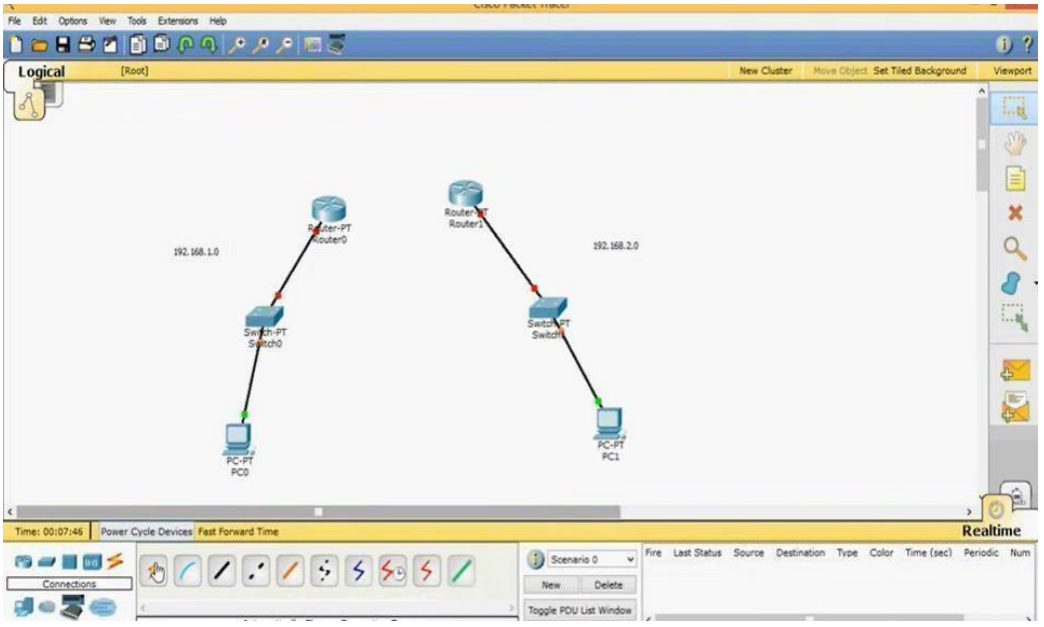
Then select a switch [I have taken Switch named as 2950-24]. Go to (1)Network device ->(2) switches ->(3) 2950-24 as shown in the

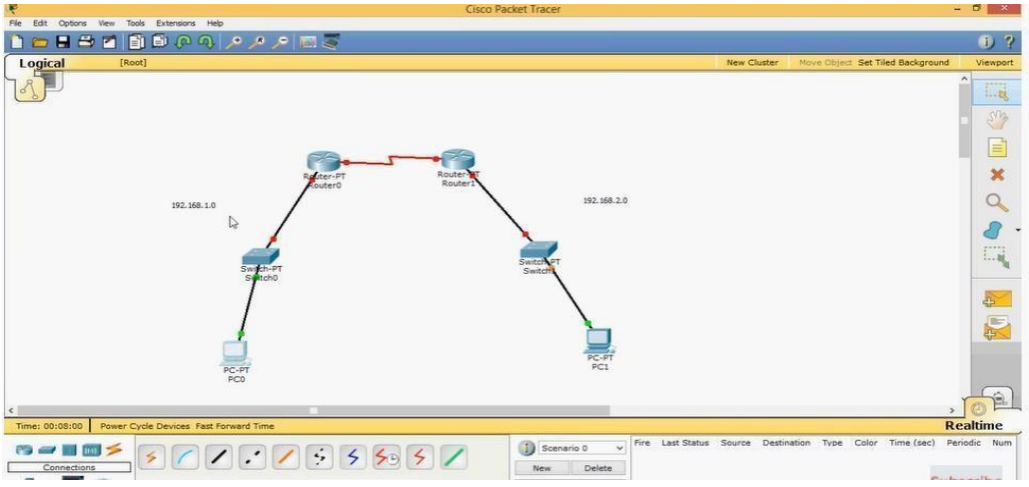


Then finally take a wire and connect PC to switch or you can click first option in connection as automatically choose connection type as shown below no .2 (use copper straight through

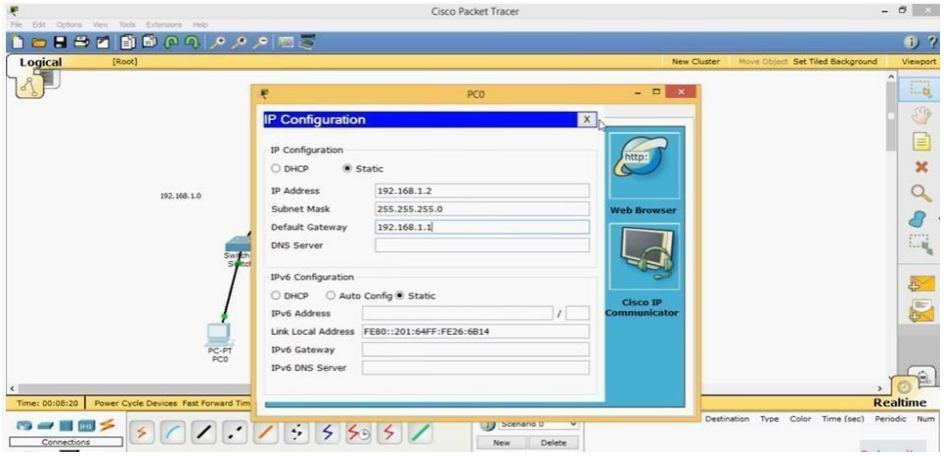


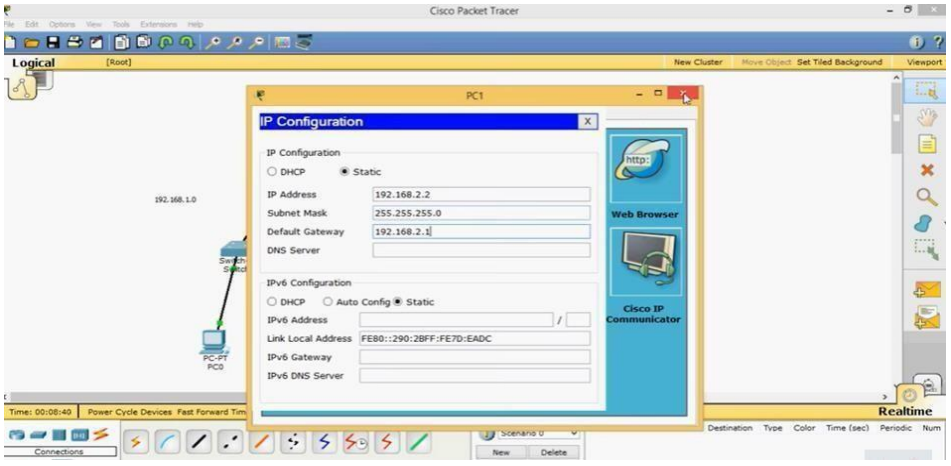
Connect Router0 and Router 1



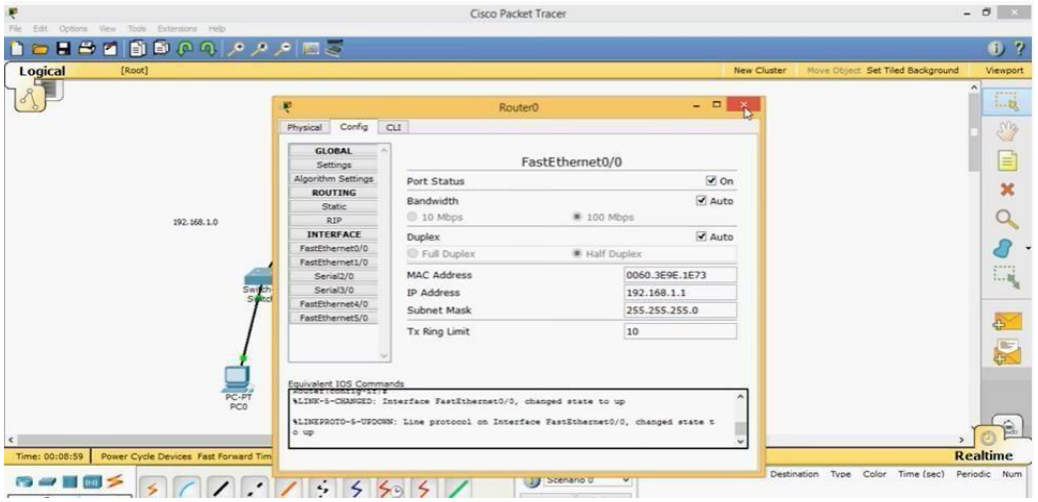


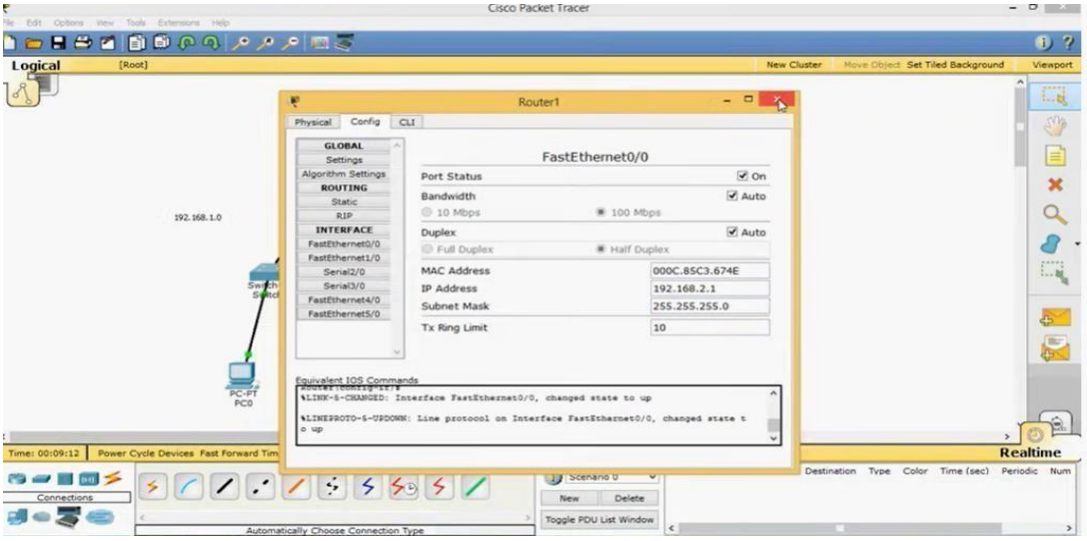
STEP 3: Configuration of IP for PC 0 &PC1



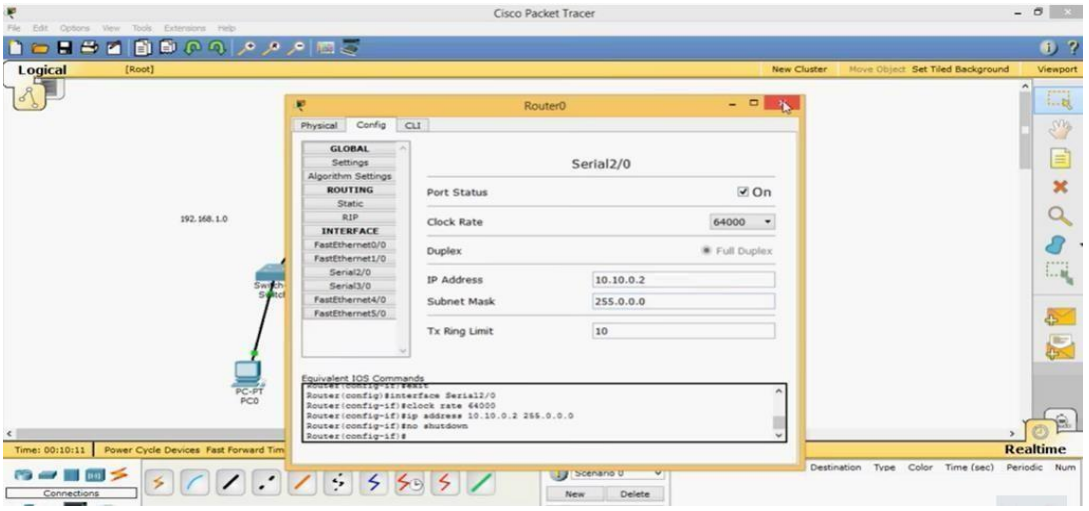


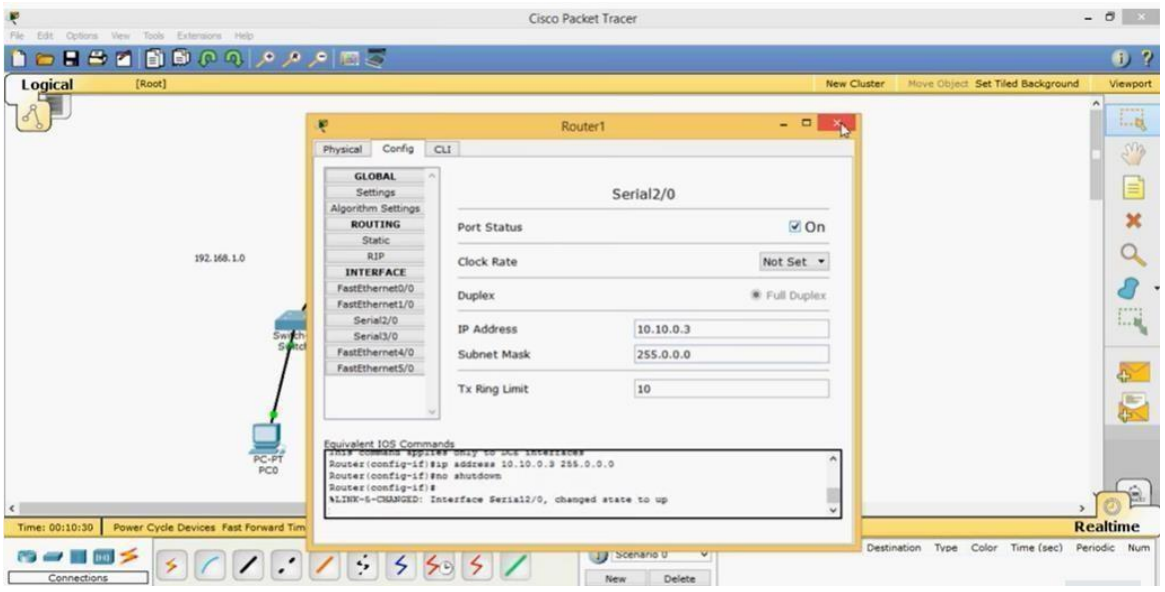
STEP 4: Configuration of Router 0 & Router 1





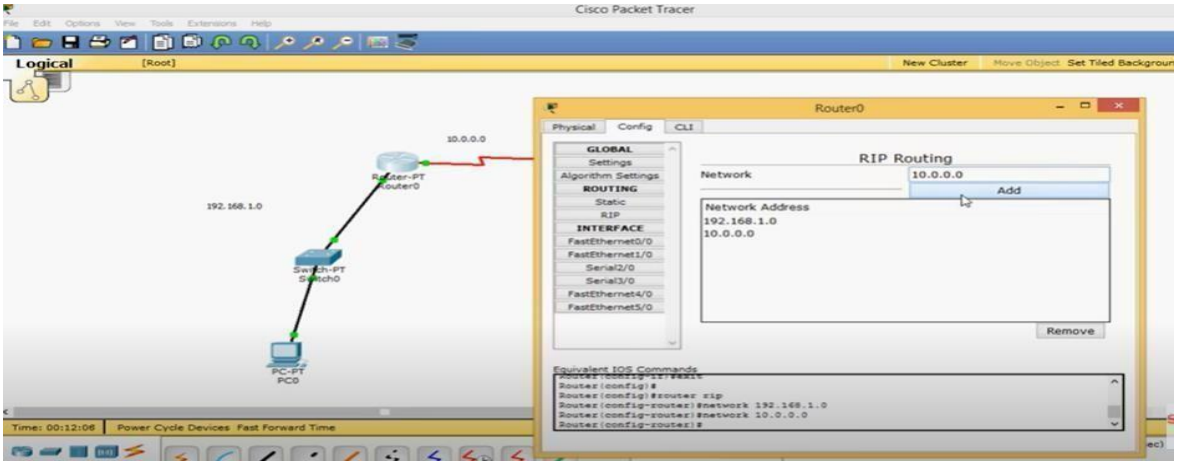
The Network between two router as IP address 10.0.0.0, We have connected a serial cable to the serial interface of the router0 &router 1, determine the interface is DTE or DCE. Since clocking is required to enable the interface, one of the two routers should function as DCE and DTE should provide clocking. Now configure serial2/0 of router 0 and router 1 as shown


Cisco Packet Tracer
Logical
[Root]
Router0
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Clock Rate
64000
Duplex
Full Duplex
IP Address
10.10.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface Serial2/0
Router(config-if)#clock rate 64000
Router(config-if)#ip address 10.10.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
192.168.1.0
PC-PT
PC0
Realtime

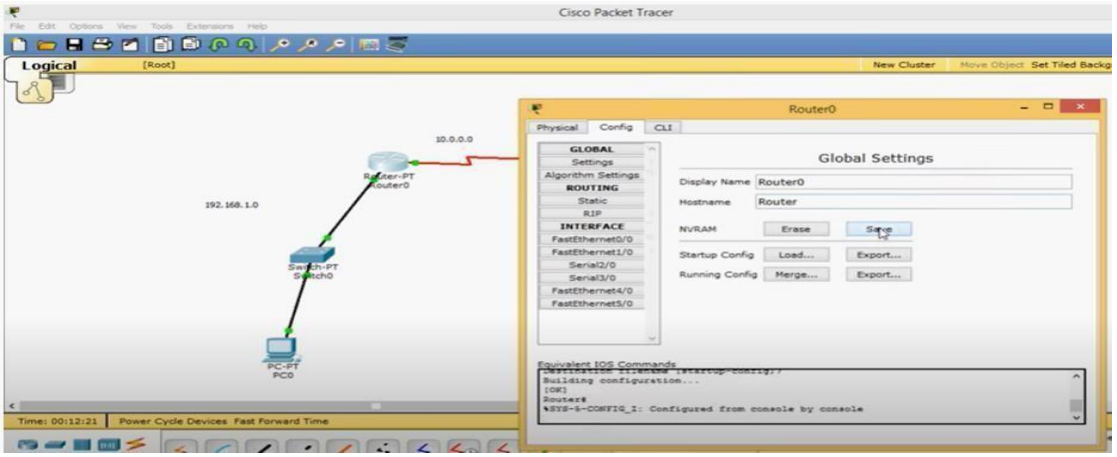

Cisco Packet Tracer
Logical
[Root]
Router1
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Clock Rate
Not Set
Duplex
Full Duplex
IP Address
10.10.0.3
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#ip address 10.10.0.3 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
192.168.1.0
PC-PT
PC0
Realtime

Configure Routing information in to router 0:

add Network IP 192.168.1.0 and 10.0.0.0



Save the global settings router 0



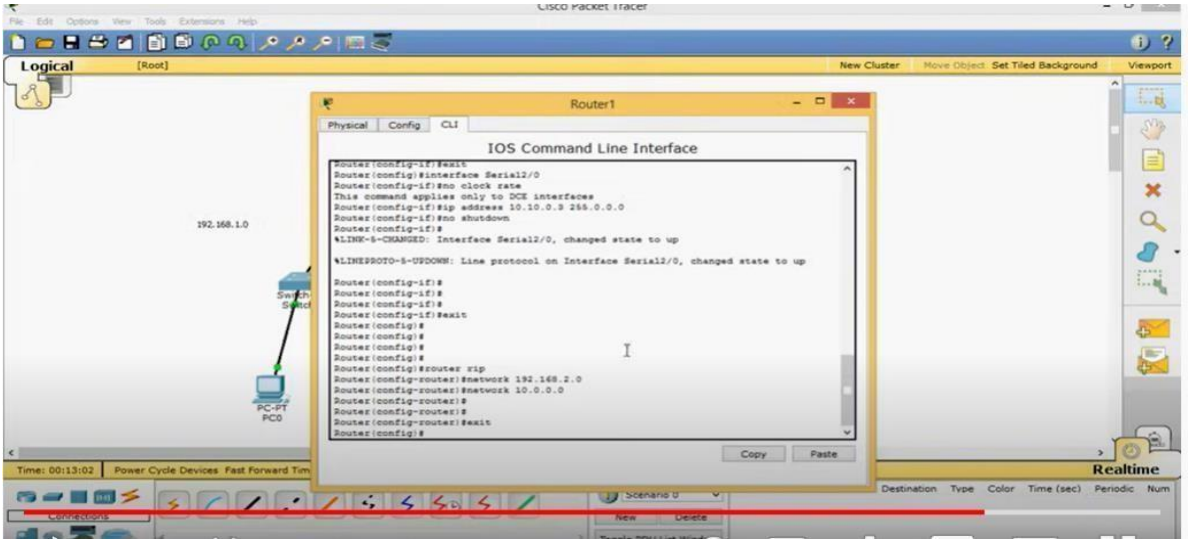
Or configure using CLI of router 1 and save global setting

On Router1, execute the following commands to configure RIP routing. Router1(config)#router rip

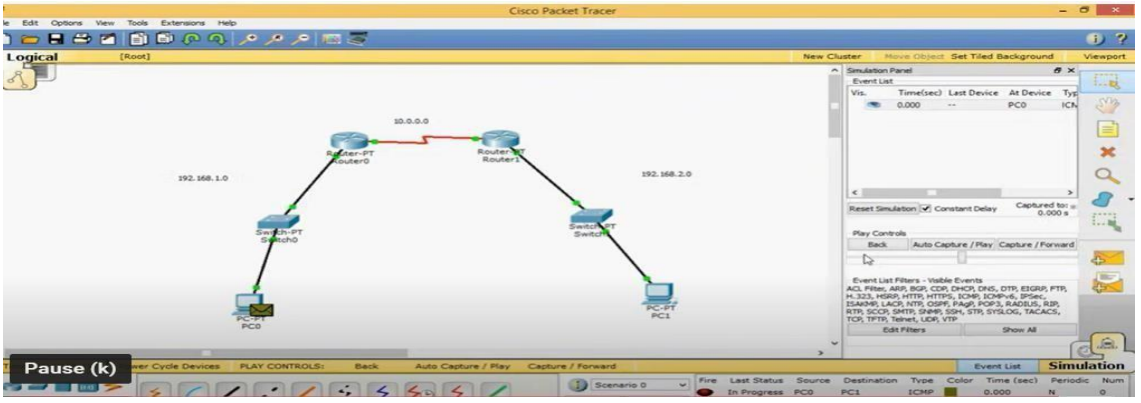
Router1(config-router)#network 192.168.1.0

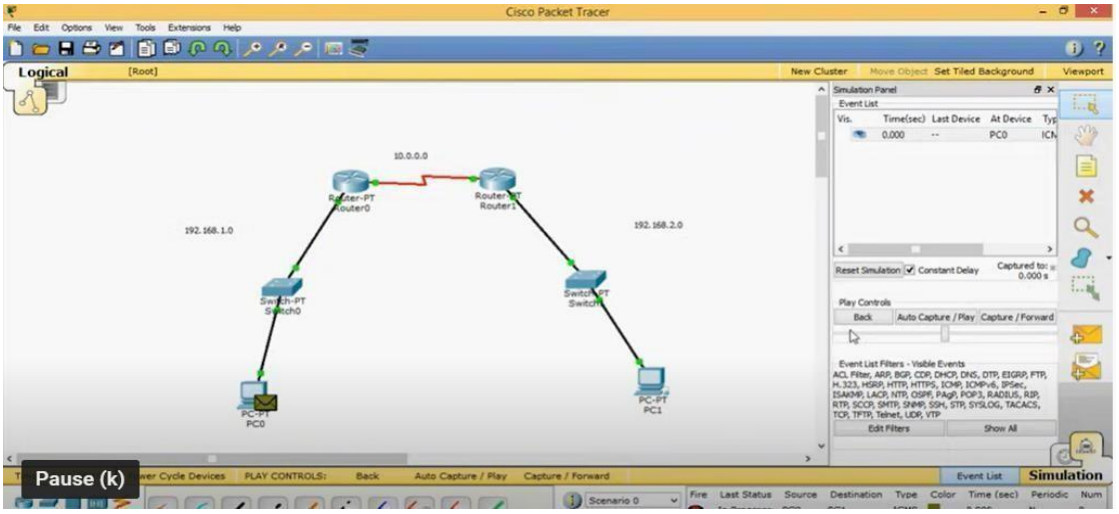
Router1(config-router)#network 10.0.0.0

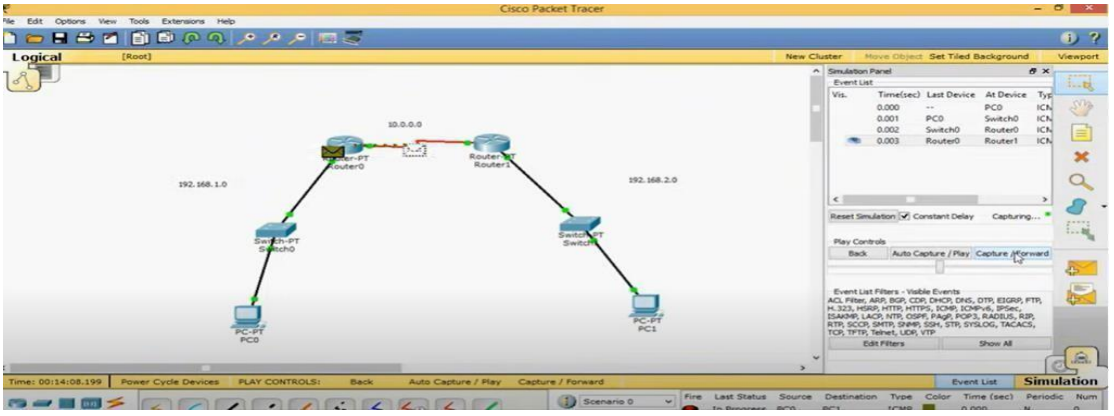
Router1(config-router)#exit

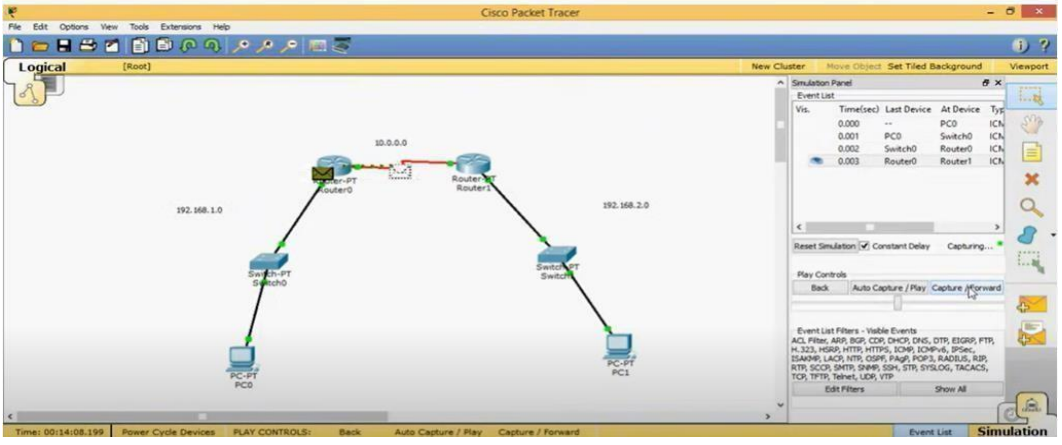


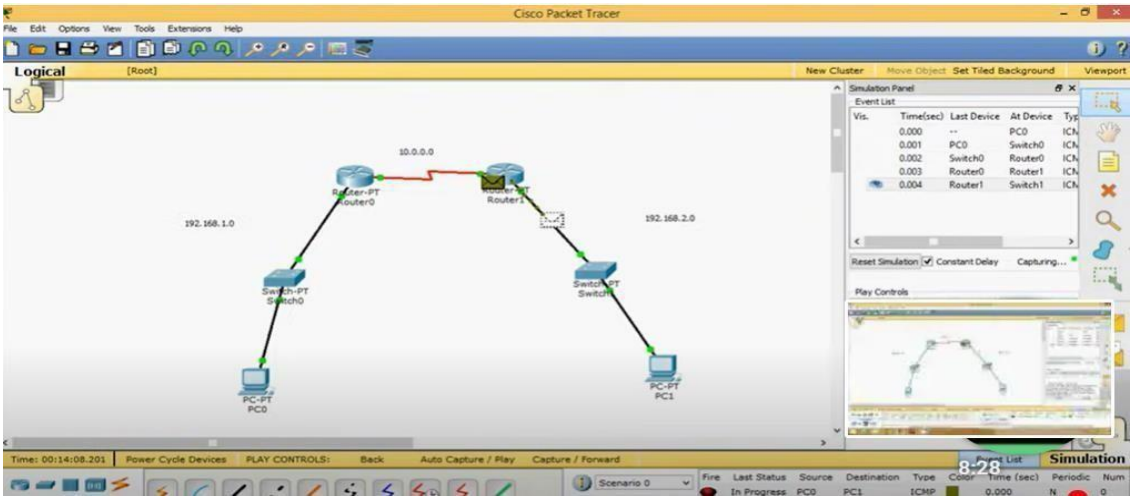
Observe the simulation by adding packet PC0& PC 1

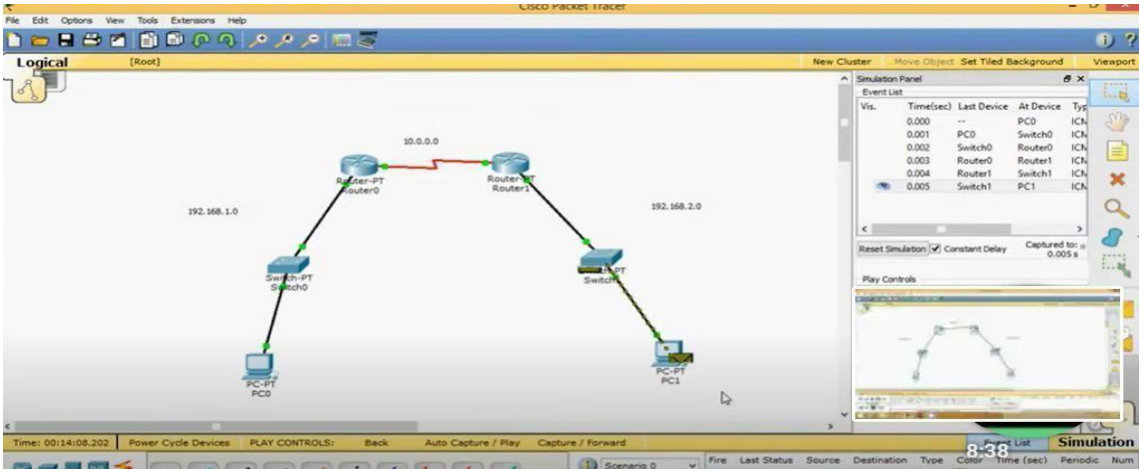



Cisco Packet Tracer
Logical
[Root]
10.0.0.0
192.168.1.0
192.168.2.0
Router0
Router1
Switch0
Switch1
PC0
PC1
Pause (k)
Simulation


Cisco Packet Tracer
Logical
[Root]
10.0.0.0
192.168.1.0
192.168.2.0
Router0
Router1
Switch0
Switch1
PC0
PC1
Simulation


Cisco Packet Tracer
Logical
[Root]
10.0.0.0
192.168.1.0
192.168.2.0
Router0
Router1
Switch0
Switch1
PC0
PC1
Simulation





OUTPUT:

CONCLUSION: