**INDEX**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.NO** | **DATE** | **TITLE OF THE EXPERIMENT** | **MARKS** | **SIGNATURE** |
| **1.** | 21/07/2017 | Study of network cables and procedure to crimp and clamp cross over cable and straight through cable |  |  |
| **2.** | 1/08/2017 | Study and installation of packet tracer and its features |  |  |
| **3.** | 11/08/2017 | Implementation of network topology using packet tracer |  |  |
| **4.** | 18/08/2017 | Configuration of static routing using packet tracer |  |  |
| **5.** | 22/08/2017 | Configuration of dynamic routing(RIP)using packet tracer |  |  |
| **6.** | 01/09/2017 | Configuration of link state routing(OSPF)using packet tracer |  |  |
| **7.** | 5/09/2017 | Transport layer protocol header analysis using wireshark- TCP |  |  |
| **8.** | 08/09/2017 | Network layer protocol header analysis using wireshark- IP |  |  |
| **9.** | 08/09/2017 | Network layer protocol header analysis using wireshark- ICMP |  |  |

**EX.NO. :1**

**DATE : 21/07/2017**

**STUDY OF NETWORK CABLES AND PROCEDURE TO CRIMP AND CLAMP CROSS OVER CABLE AND STRAIGHT THORUGH CABLE**

**AIM:**

To study different types of network cables and to identify and write the procedure for crimping and camping of a straight through cable and crossover cable with specific relevance to colour coding of wire

**Solution:**

1)**Different types of cable:**

\*Ethernet cable

\*twisted pair cable

\*co-axial cable

\*optical fibre cable

\*FDDI

**2)characteristics:**

**\*Ethernet :**

Data rate - 10mbps

Signalling method - baseband

Max segment length -500

Media – 50-ohm thick

Topology -bus

Ethernet is a family of computer networking technologies used in LAN,MAN,&WAN.

There are 3elements that comprise Ethernet

1)physical media sequent which are used to interconnect systems

2)the media access control that implement access to Ethernet channels

3) A frame that organises data to be transmitted in a standard way

**Different cable types of Ethernet**

i)10 base 2

ii)10 base T

iii)10 base F

iv)100 base T

v)1000 base T

**Different devices**

i) x box 360

ii)play station 3

iii)printers

iv)hard disks

**Advantages:**

1)Conceptually simple 2)Relatively inexpensive

3)Noise immunity 4)it can be used in bus & mean topology

5)it is easy to install compared to another network

**Disadvantages:**

1)Difficult to change . 2)fault intolerant.

3)difficult trouble shooting. 4)voice signals are enemy of Ethernet, If delay in time.

**\*Twisted pair:**

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purpose of cancelling out electro magnetic interface from external sources.

Data rate – 4mbps

Band width -3MHZ

Repeater spacing -2 to 10km

**Types:**

1)shielded twisted pair.

2)unshielded twisted pair.

**Advantages:**

1)easy to handle and install 2)cheapest form of cable available for networking purpose

3)cross talk is maintained 4)electrical noise going into or coming from the cable can

be prevented

**Disadvantages:**

1)Deformation

2)Delay skew

3)Imbalance

**\*Co-axial cable:**

This type of cable is consisted of a solid wire core surrounds by one or more wire shields each separated by same insulating material. The inner core carries the signal & shielded provides the ground.it is very cheap & has better transmission characteristics than twisted pair cable.

**Advantages:**

1)broadband system 2) greater channel capacity

3)greater bandwidth 4)lower error rates

5)greater spacing between amplifiers

**Disadvantages:**

1)problems with the deployment architecture 2)bi-directional upgrade require

3)great noise 4)high installation costs

5)susceptible to damage from lighting strikes

**\*Optical fibre cable:**

An optical fibre cable also known as fibre optic cable, is an assembly similar to an electrical cable but containing one or more optical fibres that are used to carry light.

**Characteristics:**

1)cost is relatively inexpensive.

2)installation relatively simple.

3)typical band width of 10mbps

4)node capacity is 30 for thinnest 100 for thick net

5)plenum-grade must be used in ceilings and walk

**Advantages:**

1)bandwidth, size, weight.

2)flexibility, interference

3)low power loss 4)security

**Disadvantages:**

1)cost 2)transmission 3)fragile 4)protection

**\*FDDI:**

Fibre distributed data interface (FDDI) is a standard for data transmission in a local area network it was optical fibre as its standard under lying physical medium, although it was also later specified to use copper cable, in which case it may be called CDDI

Characteristics:

1)FDDI is frequently used as high speed

**Procedure for crimping cross over & straight through cables:**

1)To connect pc to pc (cross cable)

2)To connect pc to hub /switch/ router to hub/switch/router(straight cable)

3)CAT 5 cable as 4 pairs of copper wire inside it

4)standard cable has brown, brown white , green, green white, blue, blue white,

Orange, orange white.

5)let us first give a number scheme for cabling which we will follow throughout this tuto, brown (8),brown white(7), green(6), green white(3), blue(4), blue white(5), orange(2),orange white(1).

**Crimp and clamp of straight through cable:**

1)remove the covering CAT cable.

2)straight the eight wires of the cable.

3)using crimping tools cutter cut the end of wire that they are of same length.

4)arrange the wires in order 1,2,3,4,5,6,7,8 respectively

5)insert the arranged cable in RJ45 connected with climp and crimp it handle

6)follow same steps with same colour order for other end of the cable too

7)the wire is then straight through cable

**Crimp and clamp of cross over cable:**

1)only the difference is in the colour coding of other side of wire

2)wire that is on 1st number of A-side(one end) should be on 3rd number on B-side(other end)

3)wire that is on 2nd number on A-side(one end) should be on 6th number on B-side(other side)& vice versa

4)now crimp RJ45 connector

5)your cross wire is completed

**Result:**

The study of network cables and the procedure to crimp and clamp straight through cables and crossover cables are successfully completed.

**EX.NO : 2**

**DATE : 1-08-17**

**STUDY AND INSTALLATION OF PACKET TRACER**

**AND ITS FEATURES**

**AIM :**

To study and install packet tracer and its features

**Solution:**

**1)what is packet tracer?**

Packet tracer is a protocol simulator developed by dennis frezo and his team at cisco systems. Packet tracer is a powerful and dynamic tool that displays the various protocols in networking, in either real time or simulation mode. This includes layer2 protocol such as Ethernet and ppp, layer3 protocols such as IP,ICMP, ARP ,and layer4 protocols such as TCP and VDP. Routing protocols can also be traced.

2) **Devices and connections in packet tracer**:

We will begin our network topology by selecting devices and the media in which to connect them. For this lab we will keep it simple by using end devices, switches, hubs, &connections.

**Router:** Router is a device that switches data packets between two different networks.

By default two different IP network cannot communicate with each other. They need a media to device that exchanges their packets. Routers do this job successfully by taking packet from one network and delivering it to another network. This process is called routing.

**Function:** Router perform the traffic directing functions on the internet. A data packet is

Typically forwarded from one router to another router through the network that constitute the interwork until it reaches its destination mode.

**Switches:** A network switch is a multiport network bridge that uses hardware addresses

To process and forward data at the data link layer of OSI model. The switches that connect devices together on a computer network by using packet switches to receive process and forwards data to the destination devices.

A network switch forwards data only to the devices that need to receive it, rather than the broadcasting the same data out of each of its port.

**Functions of Switches**: Switches may operate at one or more layers of the OSI model , including the Data link and network layer. A device that operates simultaneously at more than one of these layers is known as multilayer switch. Where there is a need for a graph deal of analysis of network performance and security, switches may be connected between WAN routes as places for analytic modules.

Switch is used to create a mirror image of data that can to go to an external device. Since most switches port mirroring provides only one mirrored stream.

**Hubs:** When referring to a network, a hub is the most basic networking devices that

Connects multiple computer or another network devices together. Unlike a network switch or router, a network hub has no routing tables or intelligence on where to send information and broadcasts all network data access each connection. Most hubs can detect basic networker or such as collisions, but having all information broadcast to multiple ports can be security risk and cause bottle nodes.

In general, a hub refers to a hardware device that enables multiple devices or connections to be connected to a computer Ex: USB, HUB.

**Functions:** Hubs and switches function as a common connection point for the

Work stations, pointers, file servers and other devices that make up a network. The main difference between hubs & switches is the way in which they communicate with the network a hub functions as the central connections point of a network.

**RESULT :**

Thus the study and installation of packet tracer is successfully completed.

**EX.NO: 3**

**DATE : 11-08-2017**

**IMPLEMENTATION OF NETWORK TOPOLOGY**

**USING PACKET TRACER**

**AIM:** To implement the network topology using packet tracer.

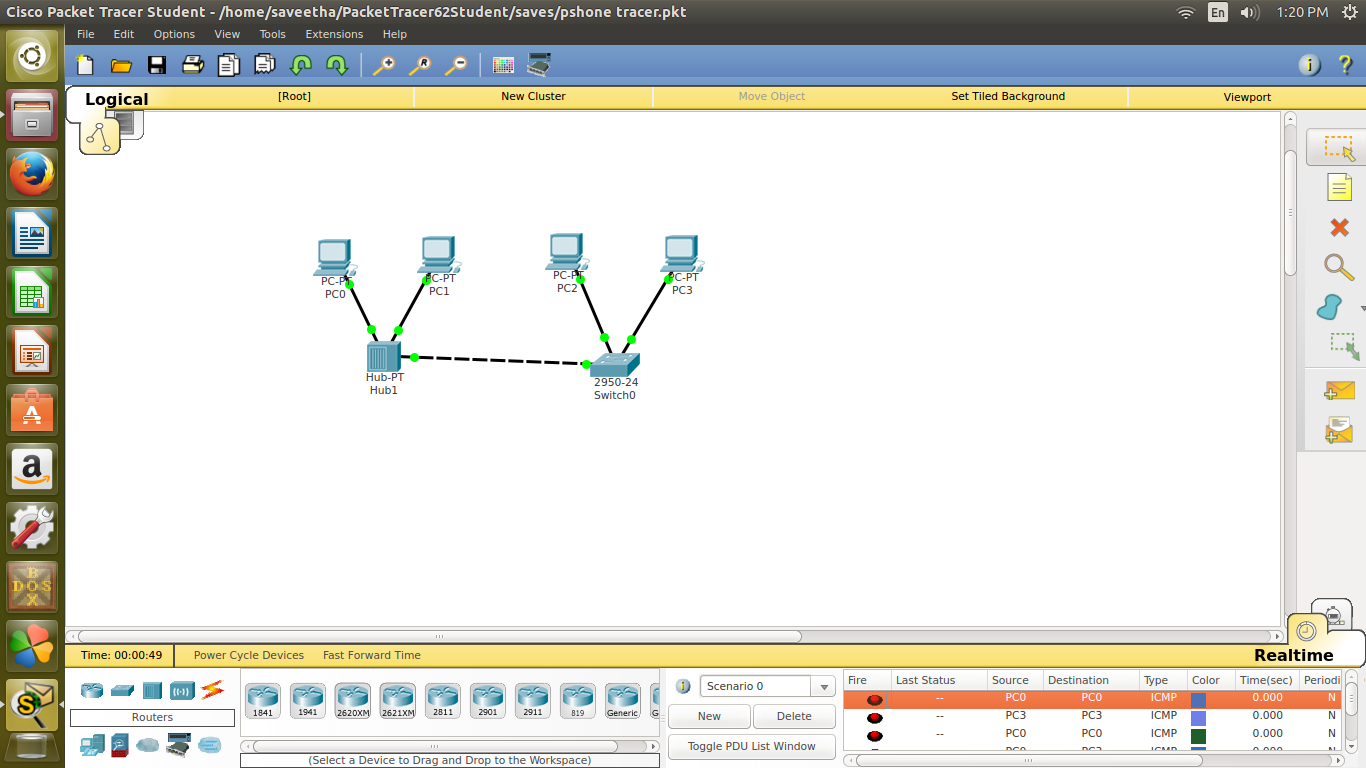
**PROCEDURE :**

1. Start the packet tracer.
2. Choosing devices and connections.

**🡪** Devices like end devices, switches, hubs, connections e.t.c;

1. Build the topology- adding hosts.
2. Build the topology – connecting the hosts to hubs and switches.
3. Configure IP addresses and subnet masks on the hosts.
4. Connect hub0 to switch0 .
5. Verify connectivity in real time mode .
6. Verify connectivity in simulation mode.
7. Save the topology.

**OUTPUT :**



**RESULT:**

The implementation of the network topology using packet tracer is successfully completed and verified.

**EX.NO: 4**

**DATE : 18-08-2017**

**CONFIGURATION OF STATIC ROUTING**

**IN PACKET TRACER**

**AIM :**

To configure a simple static routing in packet tracer using a simple topology with two routers.

**PROCEDURE :**

1. First create a topology using packet tracer.
2. Configure IP address to routers go to global configuration made in R1 and R2 configure connects interface .

**IN ROUTER 1:**

Interface faster Ethernet 0/0 in global configuration mode.

R1(config)# interface Ethernet 0/0

R1(config)# IP address 10.0.0.1 255.0.0.0

R1(config)# no shutdown

R1(config)# exit

**INTERFACE SERIES 2/O:**

R1(config)# interface series 2/0

R1 (config)# IP address 20.0.0.1 255.0.0.0

R1(config)# clock rate 64000

R1(config)# no shut down

**IN ROUTER 2 :**

Interface Ethernet 0/0

R2(config)# interface serial 2/0

R2 (config)# IP address 30.0.0.1 255.0.0.0

R2(config)# encapsulation ppp

R2(config)# no shutdown

R2(config)# exit

**INTERFACE SERIAL 2/0:**

R2(config)# interface serial 2/0

R2(config)# IP address 20.0.0.2 255.0.0.0

R2(config)# no shutdown

R2(config)# exit

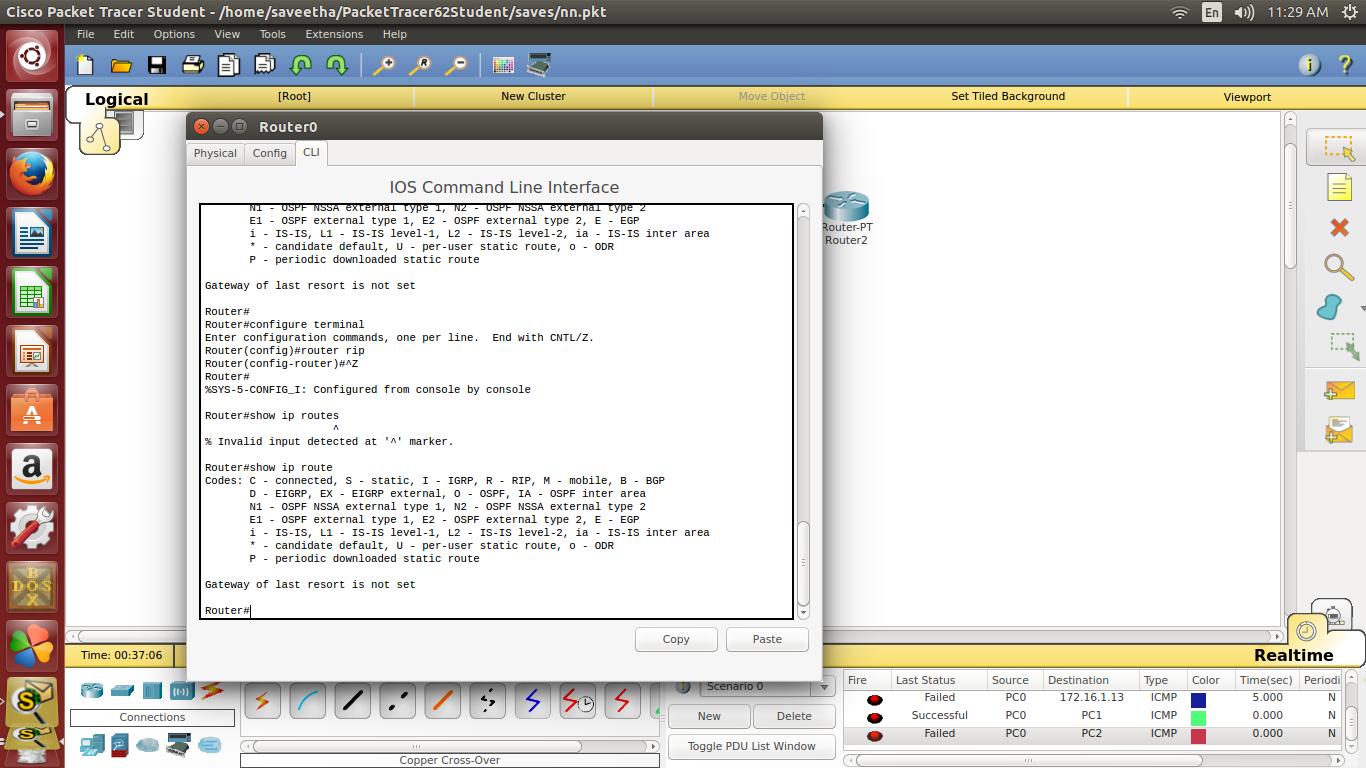
1. Assign IP address for both pc’s with the appropriate IP and subnet mask and default gateways.
2. Now configure both the routers with static routing

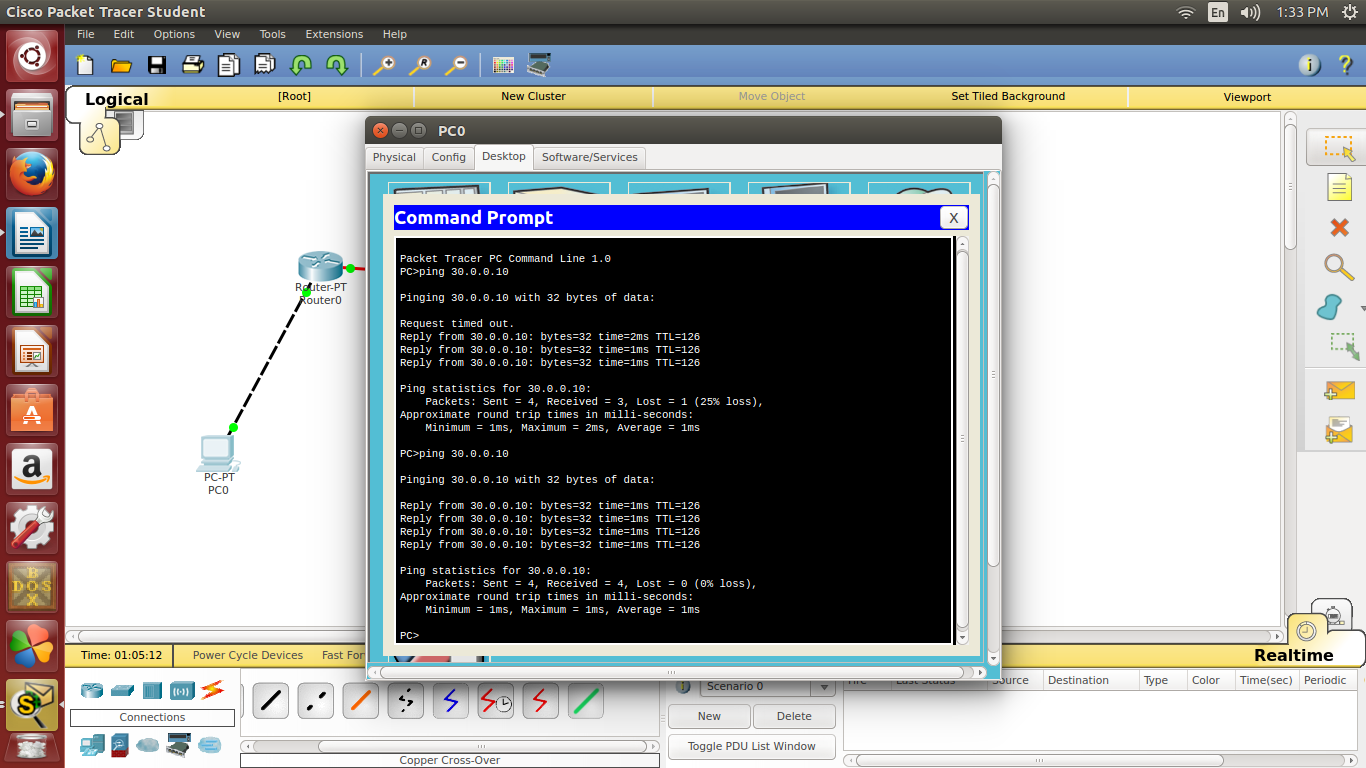
By default, routers know only directly connected network here router 1 know only 10.0.0.1 and 20.0.0.0 it doesn’t know the 30.0.0.0 like this R2 doesn’t know about 10.0.0.0 . So we are going to add static route to this both routers.

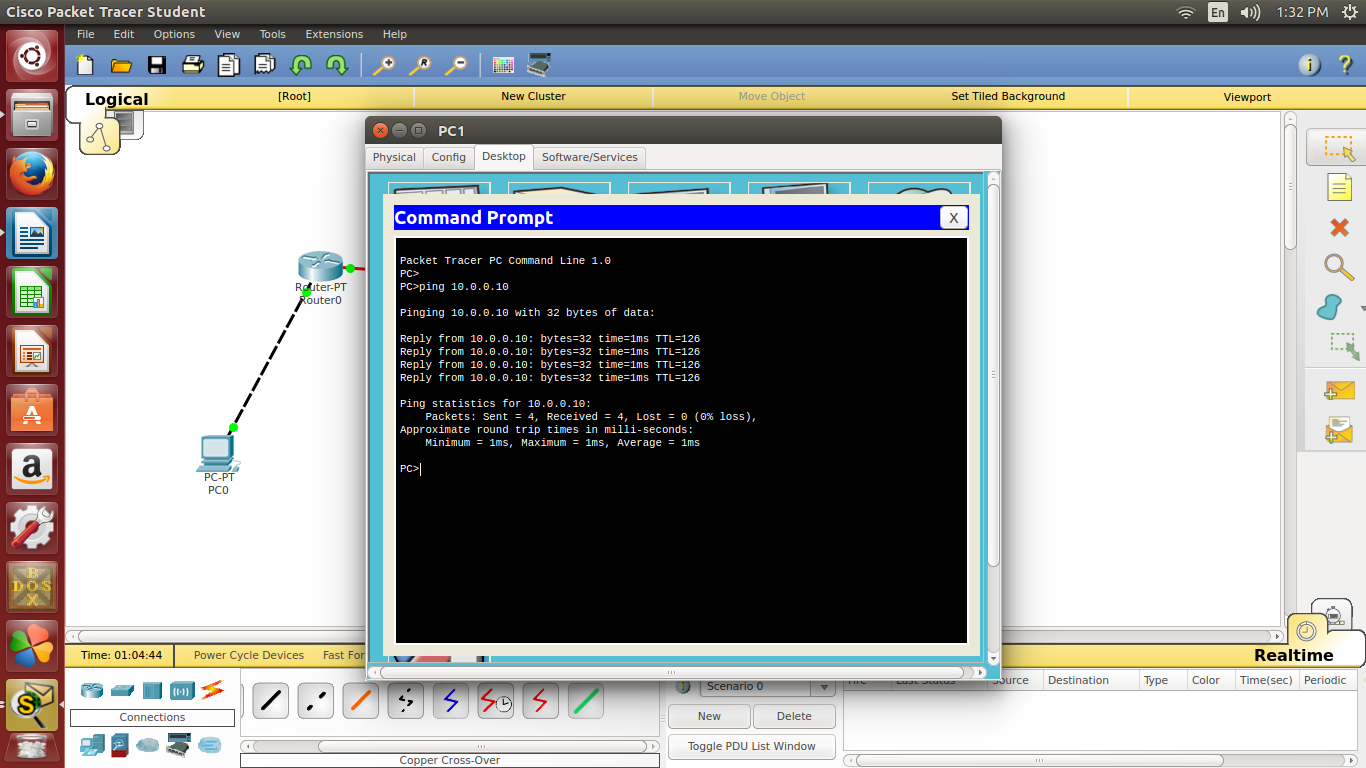
1. Double click on Pc move to desktop then command prompt give the command ping 30.0.0.10 in PC0 you will get reply from 30.0.0.10 and from other systems also.

**OUTPUT :**

****







**RESULT :**

Configuring a simple static routing in packet tracer with 2 routers is successfully completed.

**EX.NO : 5**

**DATE : 22/08/2017**

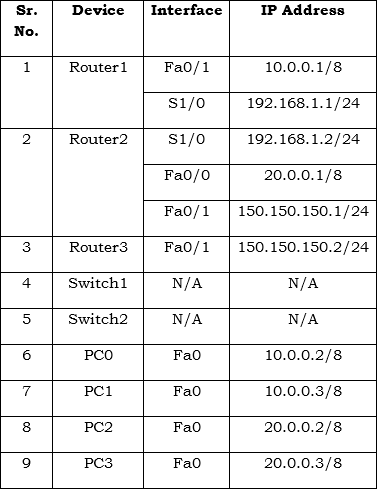
**CONFIGURATION OF DYNAMIC ROUTING(RIP)**

**USING PACKET TRACER**

**AIM :** To configure dynamic routing in a network using packet tracer

**PROCEDURE :**

**Create a topology with the following configurations.**



Once you have configured the appropriate IP addresses on each device, perform the following steps to configure RIP routing. The default version of RIP is RIPv1. In the later section, we will also configure RIPv2 routing.

1. On **Router1**, execute the following commands to configure **RIP** routing.

Router1(config)#router rip

Router1(config-router)#network 10.0.0.0

Router1(config-router)#network 192.168.1.0

Router1(config-router)#exit

1. On **Router2**, execute the following commands to configure **RIP**routing.

Router2(config)#router rip

Router2(config-router)#network 20.0.0.0

Router2(config-router)#network 192.168.1.0

Router2(config-router)#network 150.150.150.0

Router2(config-router)#exit

Router2(config)#

1. On **Router3**, execute the following commands to configure **RIP** routing.
2. Router3(config)#router rip
3. Router3(config-router)#network 150.150.150.0

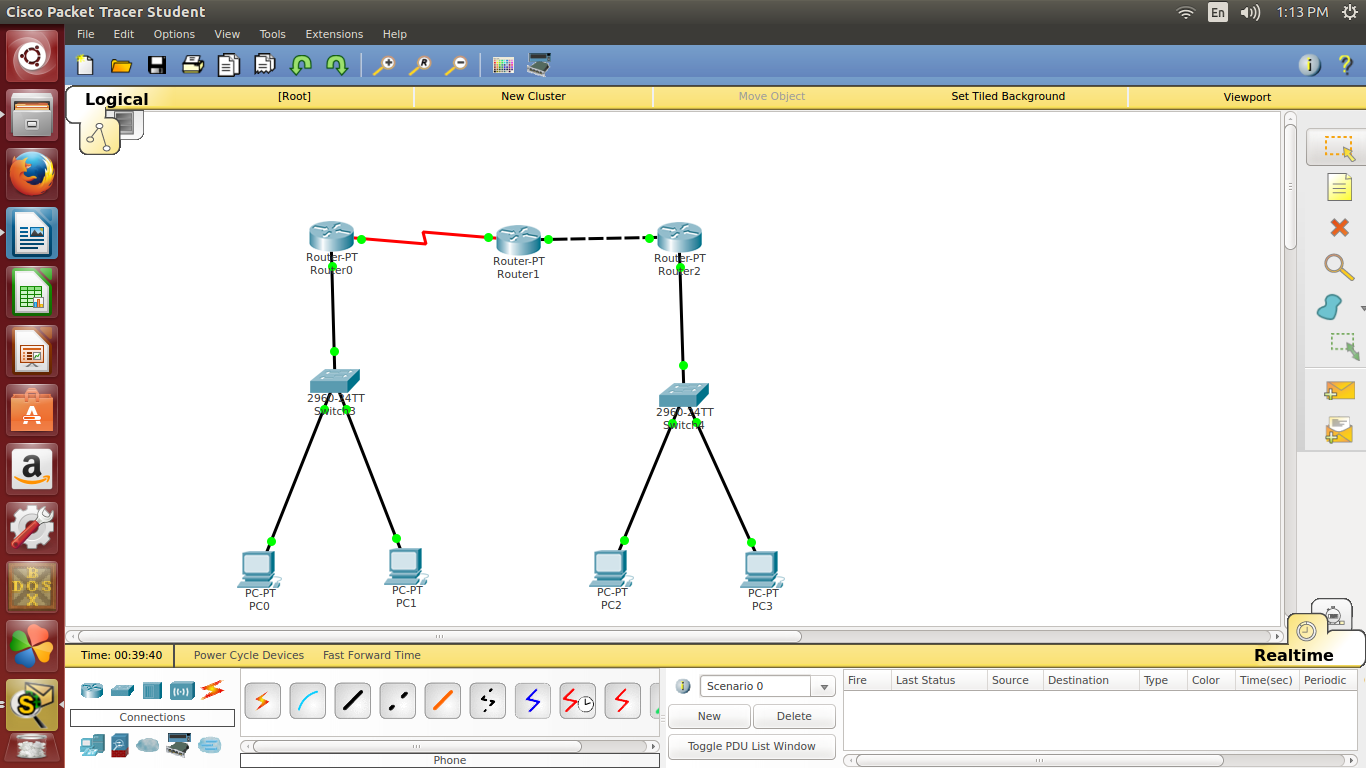
Router3(config-if)#exit

1. Once you have configured RIP routing protocol on each router, wait for a few seconds (let complete the convergence process), and then execute the **show IP route** command on any router to show the routing information.

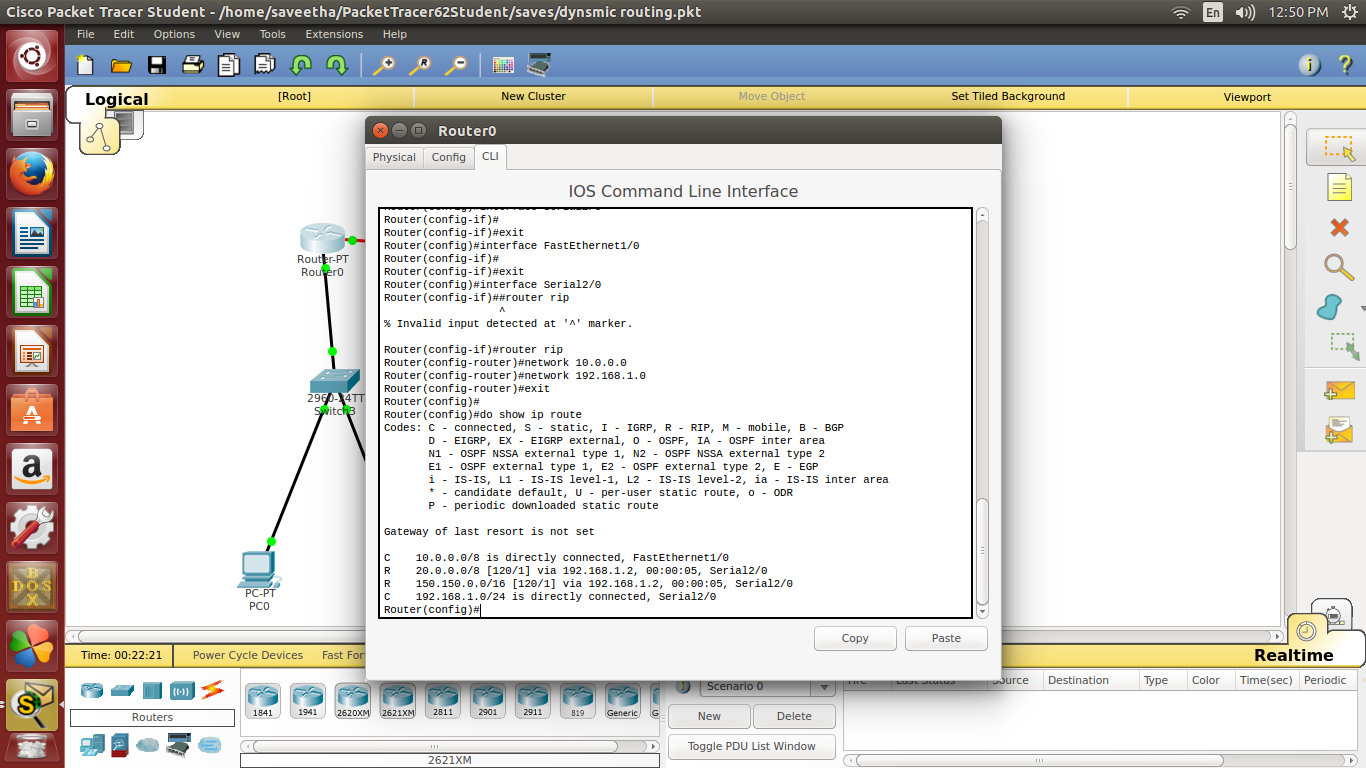
Router(config)#do show IP route

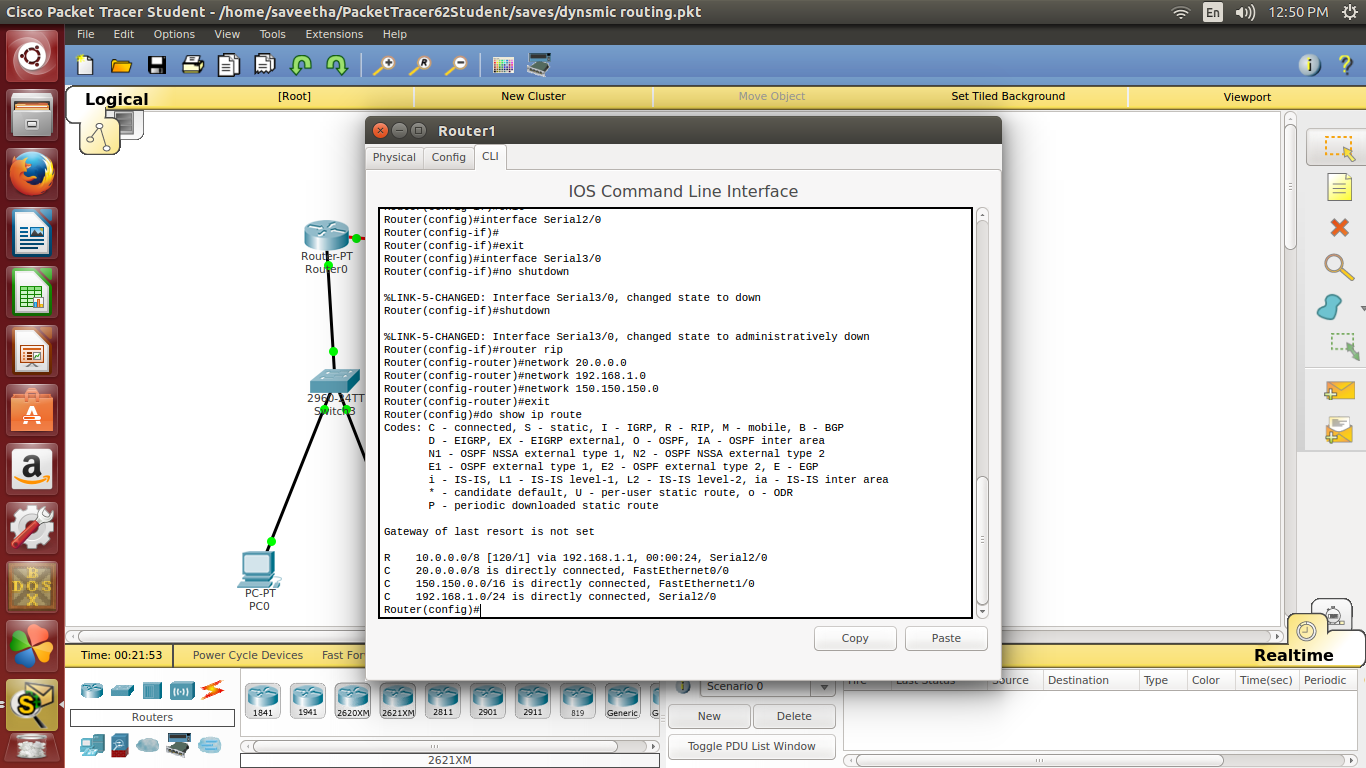
Finally PING one system with other system across two different networks.

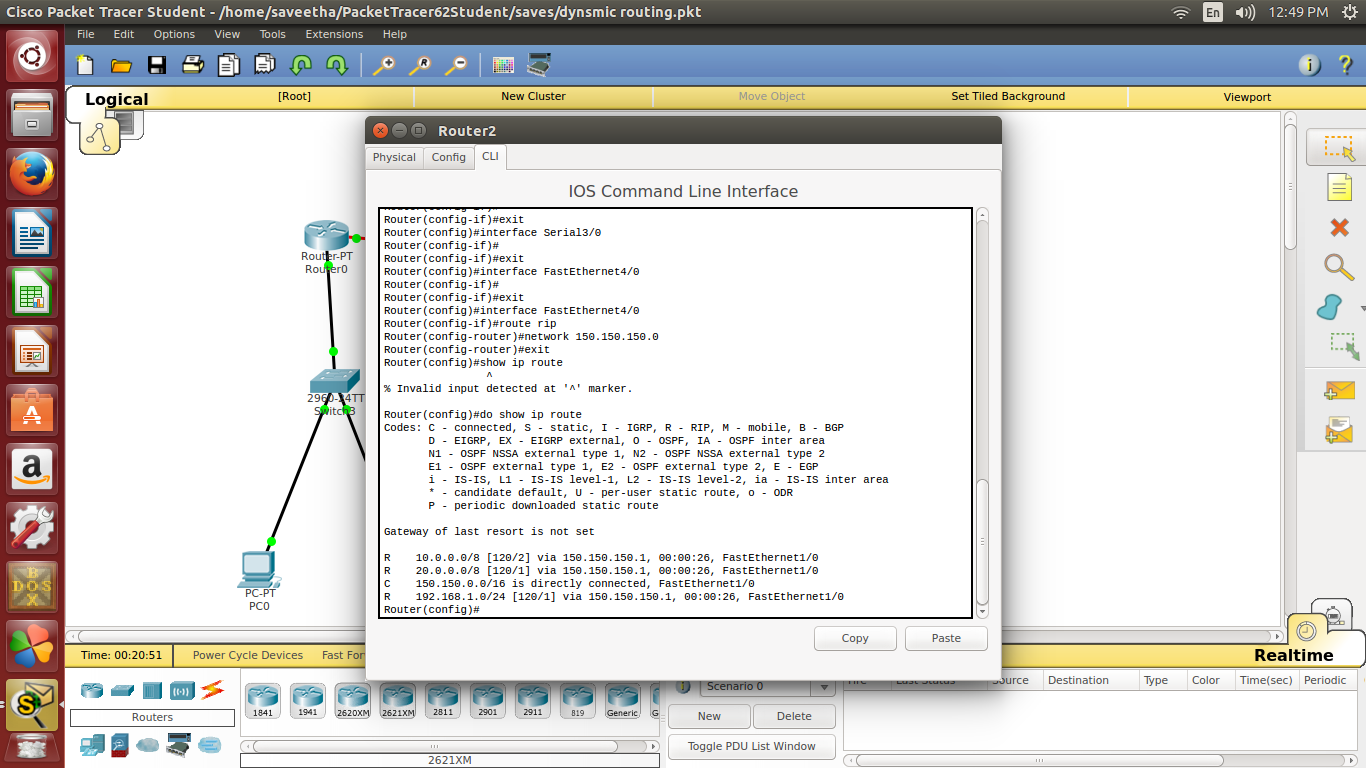
Example routes learned by RIP in router 3 is given below for your reference:

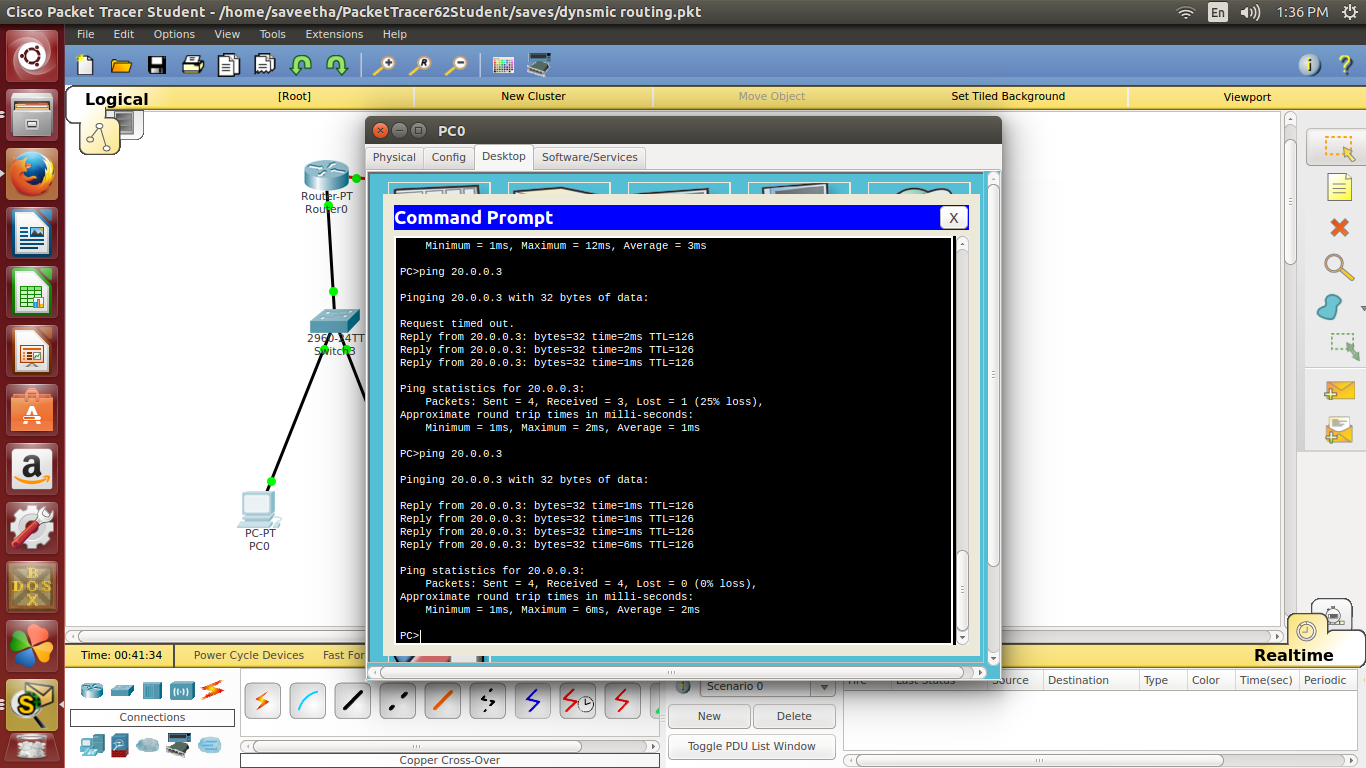


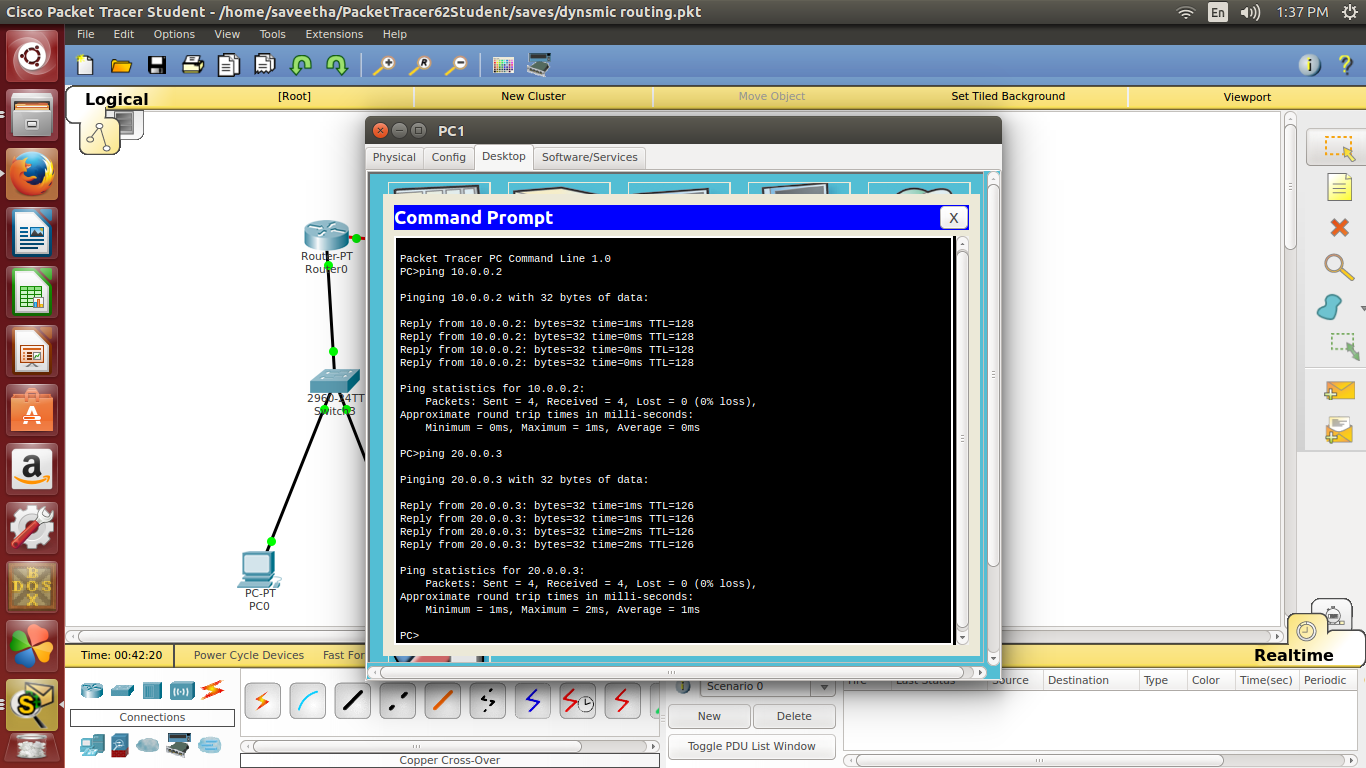
**OUTPUT:**

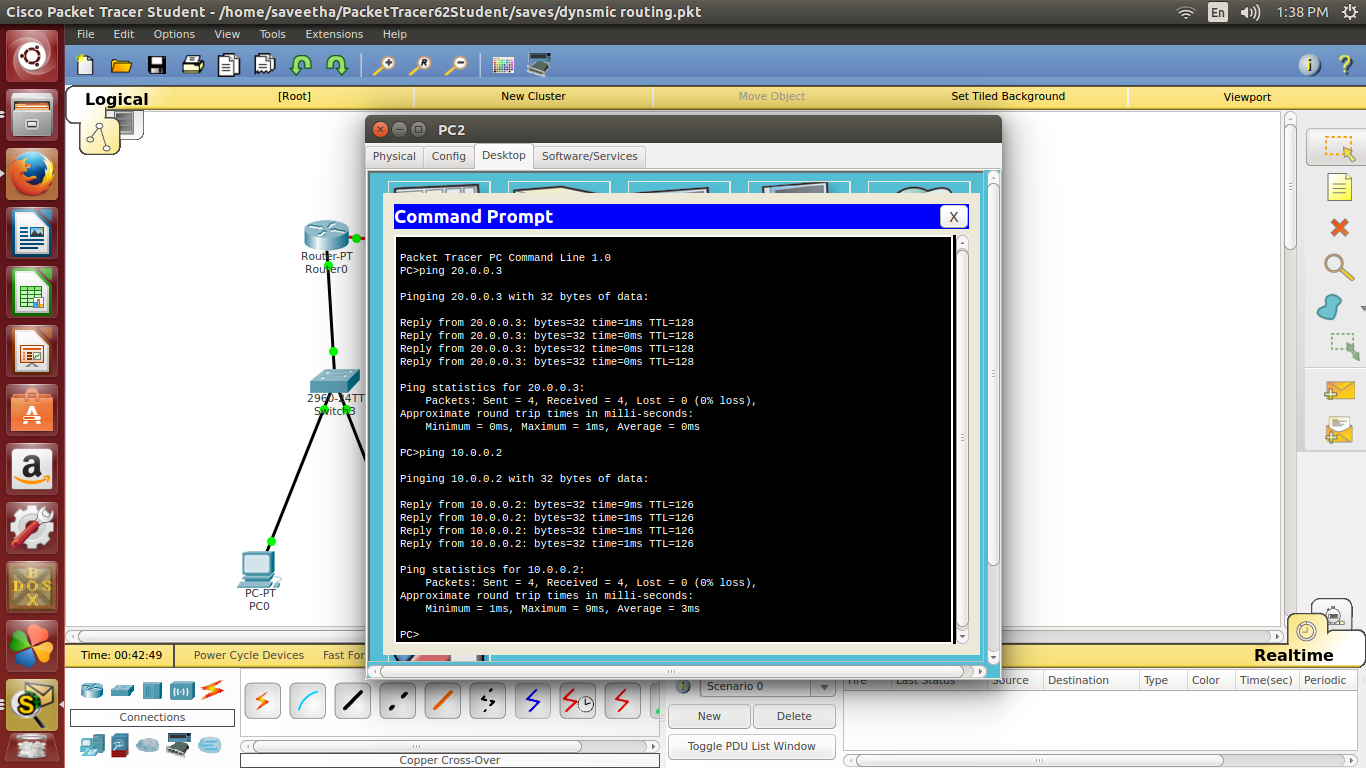


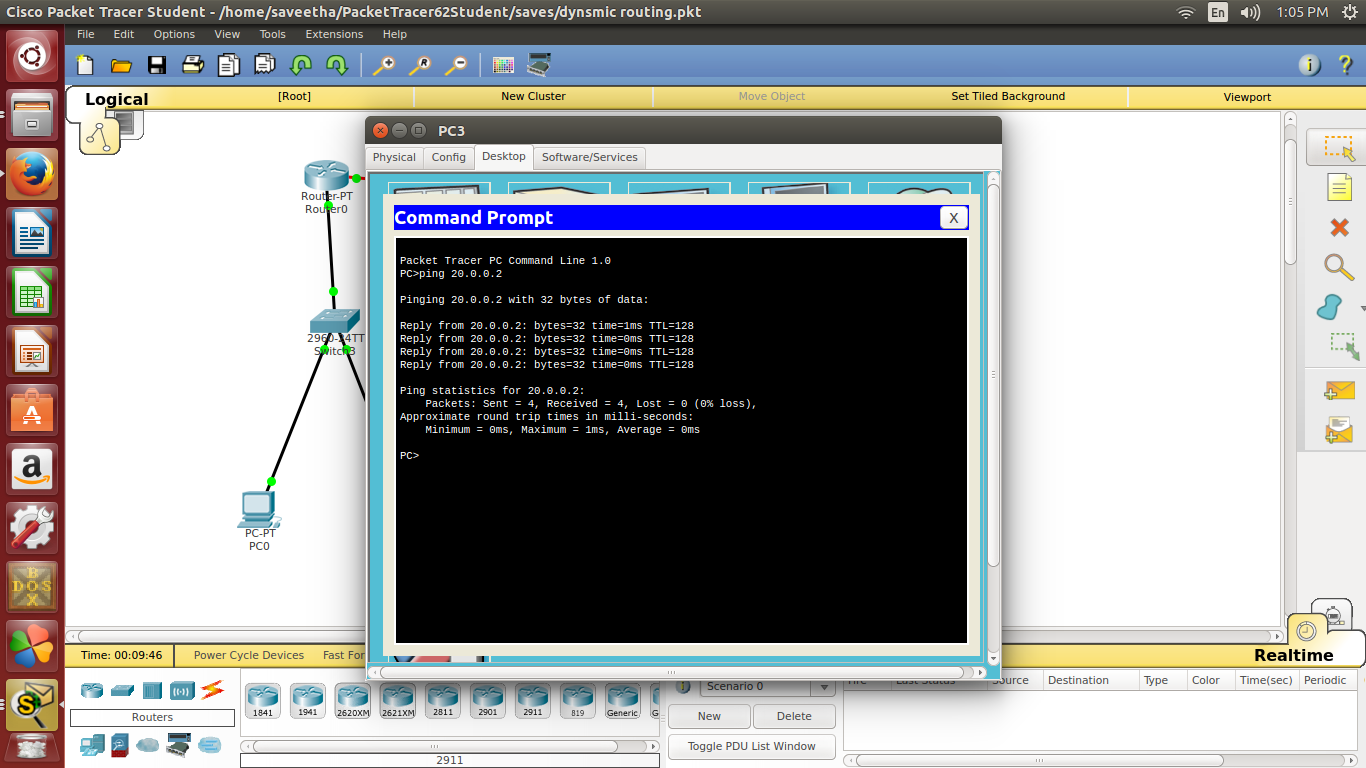












**RESULT :**

The implementation of dynamic routing using packet tracer is successfully completed.

**EX. NO : 6**

**DATE :1/09/2017**

**CONFIGURATION OF LINK STATE ROUTING(OSPF)**

**USING PACKET TRACER**

**AIM :** To configure the link state routing(OSPF) of a network using packet tracer

**PROCEDURE :**

Configure IP address to all interaces:

**In Router R1,**  
R1(config)#interface fastethernet 2/0  
R1(config-if)#ip address 10.0.0.1 255.0.0.0  
R1(config-if)#no shutdown  
R1(config-if)#exit  
  
  
R1(config)#interface serial 1/0  
R1(config-if)#ip address 20.0.0.1 255.0.0.0  
R1(config-if)#encapsulation ppp  
R1(config-if)#clock rate 64000  
R1(config-if)#no shutdown  
R1(config-if)#exit  
  
 **In Router R2,**  
R2(config)#interface serial 1/0  
R2(config-if)#ip address 20.0.0.2 255.0.0.0  
R2(config-if)#encapsulation ppp  
R2(config-if)#no shutdown  
R2(config-if)#exit  
  
  
R2(config)#interface serial 1/1  
R2(config-if)#ip address 30.0.0.1 255.0.0.0  
R2(config-if)#encapsulation ppp  
R2(config-if)#clock rate 64000  
R2(config-if)#no shutdown  
R2(config-if)#exit  
 **In Router R3,**  
R3(config)#  
R3(config)#interface serial 1/0  
R3(config-if)#ip address 30.0.0.2 255.0.0.0  
R3(config-if)#encapsulation ppp  
R3(config-if)#no shutdown  
R3(config-if)#exit  
  
  
R3(config)#  
R3(config)#interface fastethernet 2/0  
R3(config-if)#ip address 40.0.0.1 255.0.0.0  
R3(config-if)#no shutdown  
R3(config-if)#exit

Enable ip routing by configuring OSPF routing protocol in all routers

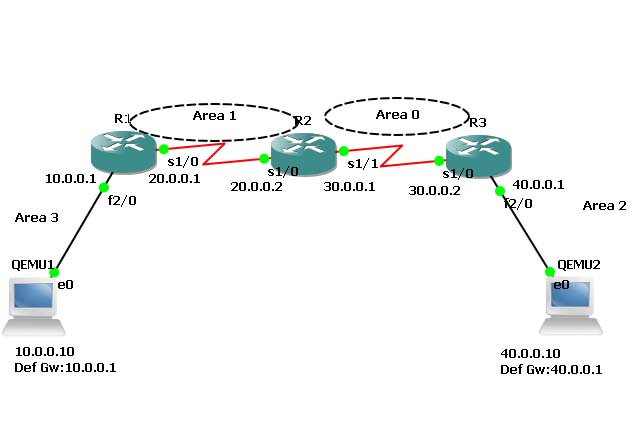
**In Router R1**  
 R1(config)#router ospf 1  
 R1(config-router)#router-id 1.1.1.1  
 R1(config-router)#network 10.0.0.0 0.255.255.255 area 3  
 R1(config-router)#network 20.0.0.0 0.255.255.255 area 1  
 R1(config-router)#exit

**In Router R2,**  
R2(config)#router ospf 1  
R2(config-router)#router-id 2.2.2.2  
R2(config-router)#network 20.0.0.0 0.255.255.255 area 1  
R2(config-router)#network 30.0.0.0 0.255.255.255 area 0  
R2(config-router)#exit  
  
**In Router R3,**  
R3(config)#router ospf 1  
R3(config-router)#router-id 3.3.3.3  
R3(config-router)#network 30.0.0.0 0.255.255.255 area 0  
R3(config-router)#network 40.0.0.0 0.255.255.255 area 2  
R3(config-router)#exit

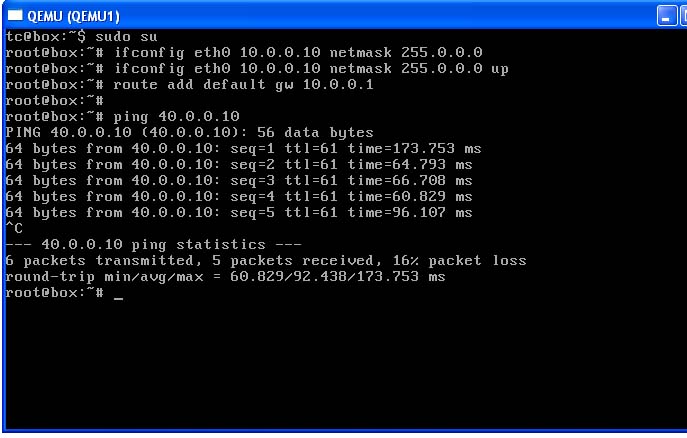
You have to configure router id when we configure ospf.It is used to identify the router  
  
  
  
**Step 4** : Now check routing table of R1,  
  
  
Router#show ip route  
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP  
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
       E1 - OSPF external type 1, E2 - OSPF external type 2  
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
       \* - candidate default, U - per-user static route, o - ODR  
       P - periodic downloaded static route  
  
Gateway of last resort is not set  
  
C    10.0.0.0/8 is directly connected, FastEthernet2/0  
C     20.0.0.0/8 is directly connected, Serial1/0  
O IA 40.0.0.0/8 [110/129] via 20.0.0.2, 00:04:23, Serial1/0  
O IA 30.0.0.0/8 [110/128] via 20.0.0.2, 00:07:29, Serial1/0  
  
  
  
  
Here,R2 knows Area 0.Network 20.0.0.0 connected to R2 from R1,So R1 learns networks through this network.  
  
R3(config)#router ospf 1, Here, 1 is Process ID, it can be 1-65535.It initializes ospf process.  
            
  
There must be one interface up to keep ospf process up.So its better to configure loopback address to routers.It is a virtual interface never goes down once we configured.  
  
  
R1(config-if)#interface loopback 0  
R1(config-if)#ip add 172.16.1.252 255.255.0.0  
R1(config-if)#no shutdown  
  
  
R2(config-if)#interface loopback 0  
R2(config-if)#ip add 172.16.1.253 255.255.0.0  
R2(config-if)#no shutdown  
  
  
R3(config-if)#interface loopback 0  
R3(config-if)#ip add 172.16.1.254 255.255.0.0  
R3(config-if)#no shutdown  
  
  
**Step 5** : Now ,Check Routing table of R3,  
  
  
R3#show ip route  
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP  
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
       E1 - OSPF external type 1, E2 - OSPF external type 2  
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
       \* - candidate default, U - per-user static route, o - ODR  
       P - periodic downloaded static route  
  
Gateway of last resort is not set  
  
O IA 20.0.0.0/8 [110/128] via 30.0.0.1, 00:18:58, Serial1/0  
C    40.0.0.0/8 is directly connected, FastEthernet2/0  
C    30.0.0.0/8 is directly connected, Serial1/0  
  
  
Here,R3 doesn't know about the area 3 so we have to create virtual link between R1 and R2  
  
  
  
**Step 6** : Create virtual link between R1,R2,by this we create a virtual link to connect area 3 to area 0.  
  
  
**In Router R1,**  
  
R1(config)#router ospf 1  
R1(config-router)#area 1 virtual-link 2.2.2.2  
R1(config-router)#  
\*Feb 10 10:29:23.767: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on OSPF\_VL0 from LOADING to FULL, Loadi  
ng Done  
  
 **In Router R2**  
  
\*Feb 10 10:28:59.543: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 20.0.0.1, Serial1/0a  
\*Feb 10 10:29:09.535: %OSPF-4-ERRRCV: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from 20.0.0.1, Serial1/0.1.1  
  
  
R2(config-router)#  
R2(config-router)#area 1 virtual-link 1.1.1.1  
R2(config-router)#exit  
R2(config)#  
  
  
\*Feb 10 10:29:19.667: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on OSPF\_VL0 from LOADING to FULL, Loadi  
ng Done  
  
  
  
  
  
  
**Step 7** : R2 and R3 get updates about Area 3 .Now,Check routing table of R3,  
  
  
  
  
R3#show ip route  
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP  
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
       E1 - OSPF external type 1, E2 - OSPF external type 2  
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
       \* - candidate default, U - per-user static route, o - ODR  
       P - periodic downloaded static route  
  
Gateway of last resort is not set  
  
O IA 20.0.0.0/8 [110/128] via 30.0.0.1, 00:01:56, Serial1/0  
C    40.0.0.0/8 is directly connected, FastEthernet2/0  
O IA 10.0.0.0/8 [110/129] via 30.0.0.1, 00:01:56, Serial1/0  
C     30.0.0.0/8 is directly connected, Serial1/0  
  
  
**Step 8** : Check connectivity between host 10.0.0.10 to 40.0.0.10

**RESULT :**

The implementation of link state routing(ospf) using packet tracer is successfully completed.



**OUTPUT:**



**RESULT :**

The implementation of link state routing(ospf) using packet tracer is successfully completed.

**EX.NO : 7**

**DATE : 5/09/2017**

**TRANSPORT LAYER PROTOCOL HEADER ANALYSIS**

**USING WIRESHARK - TCP**

**AIM:**

To analyse the transport layer protocol header using wireshark-tcp

**PROCEDURE :**

1. Start Wireshark

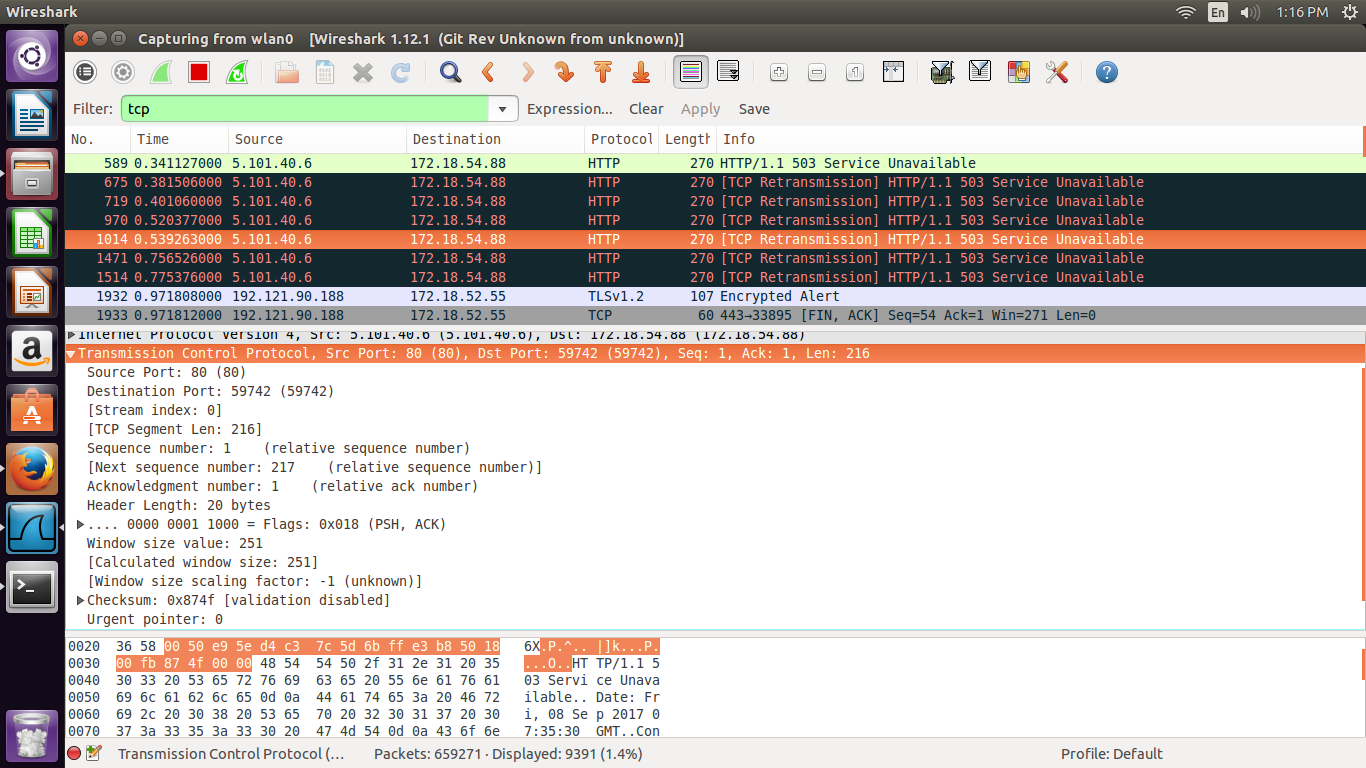
Select the appropriate interface in which the wireshark , should look for packets and capture them. (Mostly it should be, Ethernet interface or LAN interface)

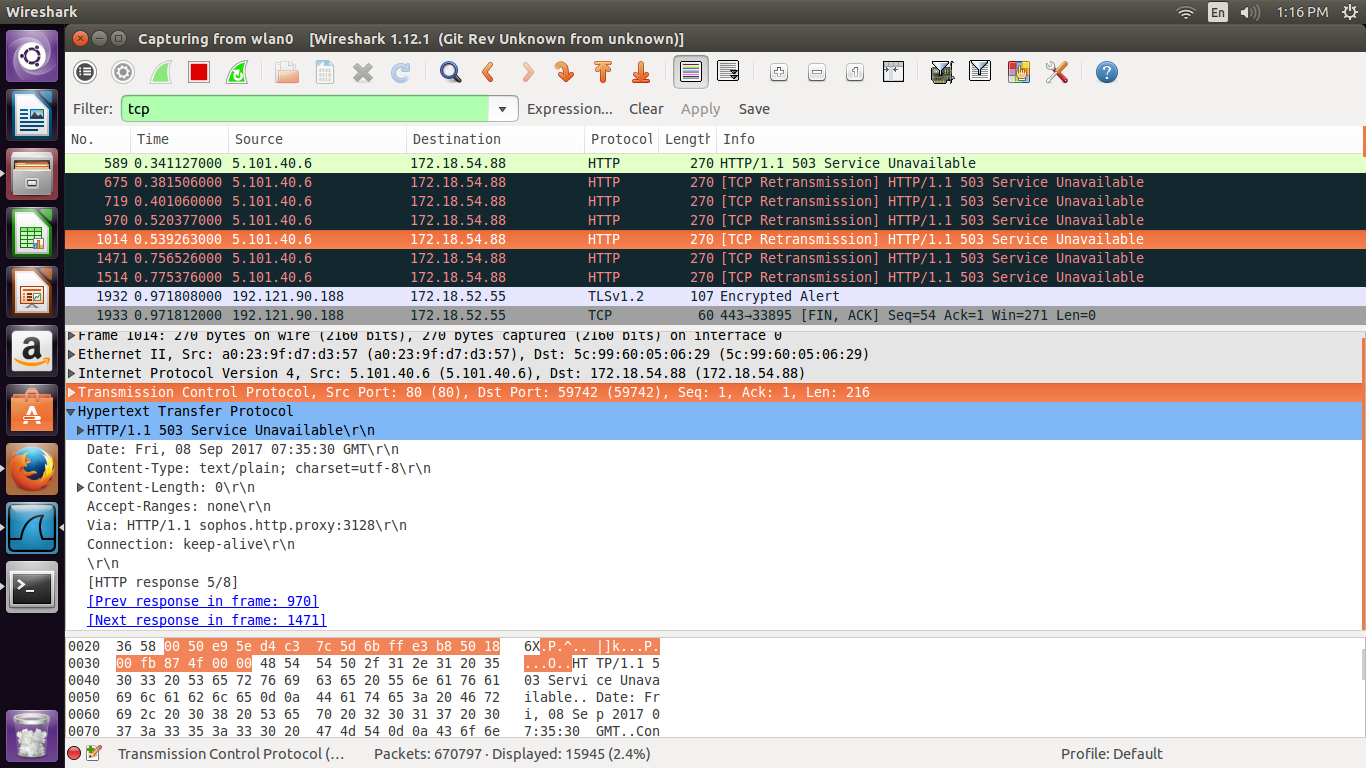
1. Wireshark interface has five major components:
2. Command menus
3. Packet listing window
4. Packet header details window
5. Packet contents window
6. Packet display filter field- Towards the top of the wireshark graphical user interface, - type a protocol name or other information based on which packets displayed will be filtered and hence packet header details and packet contents are also filtered.
7. Go to terminal mode of operation (in Linux systems) or Command prompt (in Windows systems) and execute the following command after starting the packet capture in Wireshark:

Ping << ip address of your neighbouring system>>

1. After sometime, stop the packet capturing, in wireshark and in the filter window, type TCP , to display the TCP echo request and echo reply packets and examine the ip address of the source and destination of those packets.
2. Expand the protocol header in the packet header window and write the contents of every field in the header of the packet for TCP.

**OUTPUT :**

****

****

**RESULT :**

The analysis of transport layer protocol using wireshark-TCP is successfully executed.

**EX.NO : 8**

**DATE :08/09/2017**

**NETWORK LAYER PROTOCOL HEADER ANALYSIS**

**USING WIRESHARK - IP**

**AIM :** To analyse the network layer protocol header using wireshark-IP

**PROCEDURE :**

1. Start Wireshark

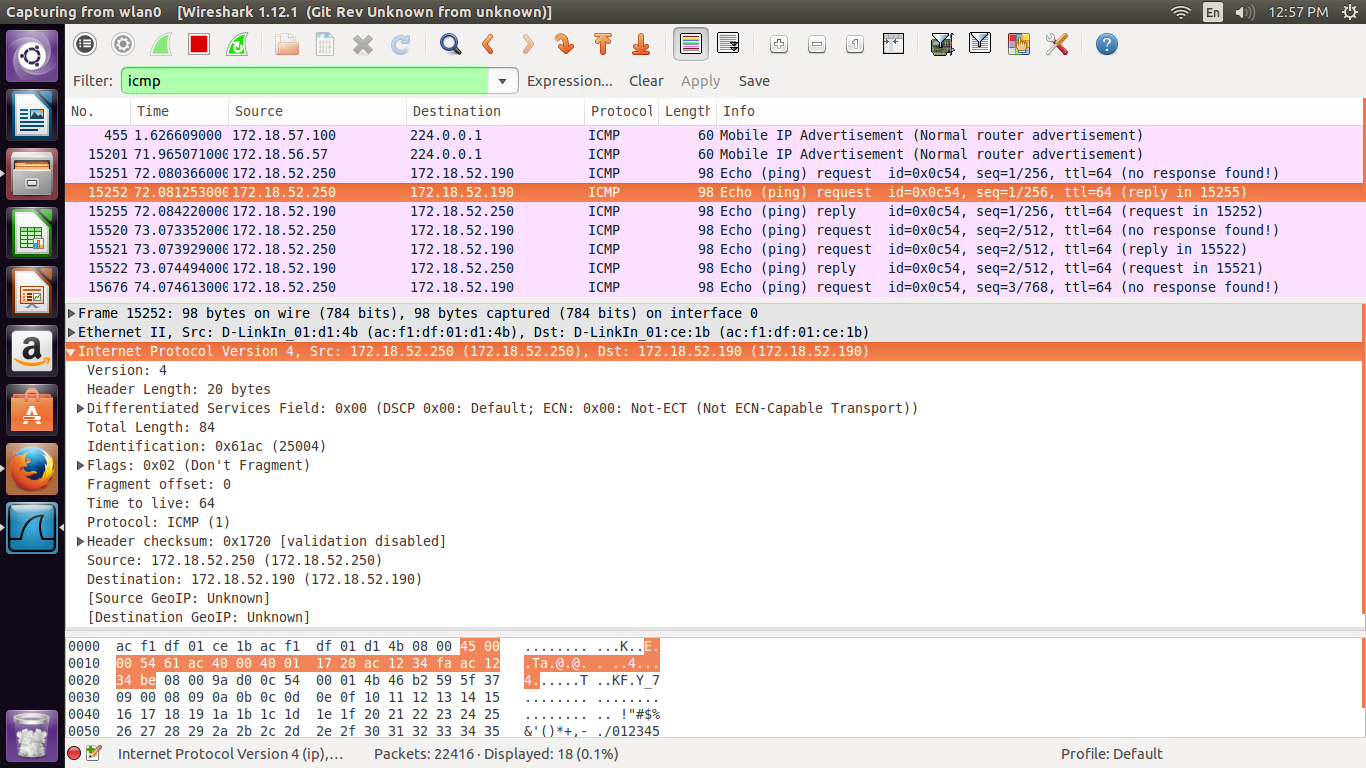
Select the appropriate interface in which the wireshark , should look for packets and capture them. (Mostly it should be, Ethernet interface or LAN interface)

1. Wireshark interface has five major components:
2. Command menus
3. Packet listing window
4. Packet header details window
5. Packet contents window
6. Packet display filter field- Towards the top of the wireshark graphical user interface, - type a protocol name or other information based on which packets displayed will be filtered and hence packet header details and packet contents are also filtered.
7. Go to terminal mode of operation (in Linux systems) or Command prompt (in Windows systems) and execute the following command after starting the packet capture in Wireshark:

Ping << ip address of your neighbouring system>>

1. After sometime, stop the packet capturing, in wireshark and in the filter window, type IP , to display the IP echo request and echo reply packets and examine the ip address of the source and destination of those packets.
2. Expand the protocol header in the packet header window and write the contents of every field in the header of the packet for IP.

**OUTPUT :**

****

**RESULT :**

The analysis of network layer protocol header using wireshark-IP is successfully completed.

**EX.NO : 9**

**NETWORK LAYER PROTOCOL HEADER ANALYSIS USING**

**WIRESHARK – ICMP**

**Aim :** To analyse the network layer protocol header using wireshark-ICMP

**PROCEDURE :**

1. Start Wireshark

Select the appropriate interface in which the wireshark , should look for packets and capture them. (Mostly it should be, Ethernet interface or LAN interface)

1. Wireshark interface has five major components:
2. Command menus

b. Packet listing window

c. Packet header details window

d. Packet contents window

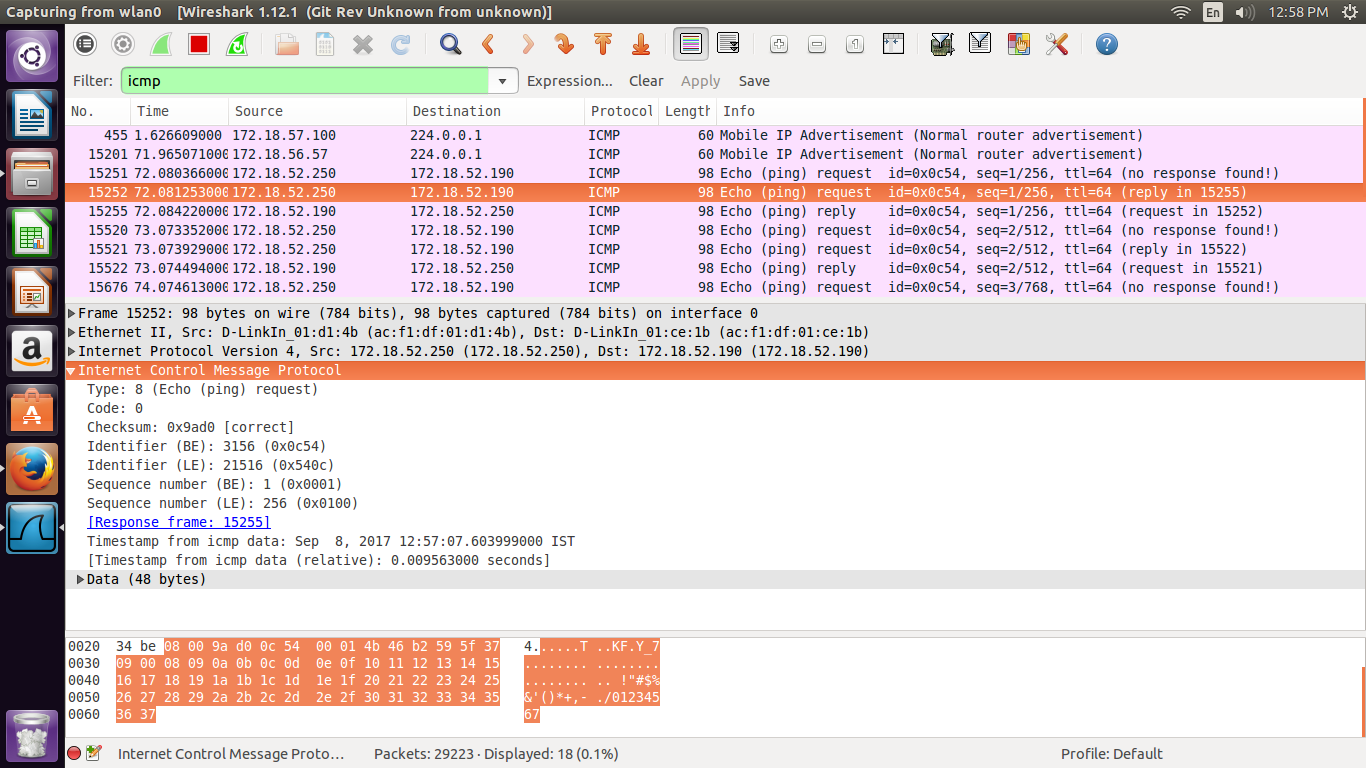
e. Packet display filter field- Towards the top of the wireshark graphical user interface, - type a protocol name or other information based on which packets displayed will be filtered and hence packet header details and packet contents are also filtered.

1. Go to terminal mode of operation (in Linux systems) or Command prompt (in Windows systems) and execute the following command after starting the packet capture in Wireshark:

Ping << ip address of your neighbouring system>>

1. After sometime, stop the packet capturing, in wireshark and in the filter window, type ICMP , to display the ICMP echo request and echo reply packets and examine the ip address of the source and destination of those packets.
2. Expand the protocol header in the packet header window and write the contents of every field in the header of the packet for ICMP.

**OUTPUT :**



**RESULT :** The analysis of network layer protocol header using wireshark ICMP is successfully completed.

**EX.NO : 10 A**

**PROGRAM USING TCP SOCKETS**

EX NO: 1.i DATE AND TIME SERVER

**AIM:**

TO implement date and time display from local host to server using TCP

**ALGORITHM: CLIENT**

1.start the program

2. Include necessary package in java

3. To create a socket in client to server.

4. the client connection accept to the server and replay to read the system date and time.

5. Stop the program.

**ALGORITHM: SERVER**

1.start the program

2. Include necessary package in java

3. To create a socket in server to client.

4. To display the current date and time to client

5. Stop the program.

**Program :**

**DATECLIENT:**

import java.net.\*;

import java.io.\*;

class dateclient

{

public static void main (String args[])

{

Socket soc;

DataInputStream dis;

String sdate;

PrintStream ps;

try

{

InetAddress ia=InetAddress.getLocalHost();

soc=new Socket(ia,8020);

dis=new DataInputStream(soc.getInputStream());

sdate=dis.readLine();

System.out.println("THE date in the server is:"+sdate);

ps=new PrintStream(soc.getOutputStream());

ps.println(ia);

}

catch(IOException e)

{

System.out.println("THE EXCEPTION is :"+e);

}

}

}

**DATESERVER:**

import java.net.\*;

import java.io.\*;

import java.util.\*;

class dateserver

{

public static void main(String args[])

{

ServerSocket ss;

Socket s;

PrintStream ps;

DataInputStream dis;

String inet;

try

{

ss=new ServerSocket(8020);

while(true)

{

s=ss.accept();

ps=new PrintStream(s.getOutputStream());

Date d=new Date();

ps.println(d);

dis=new DataInputStream(s.getInputStream());

inet=dis.readLine();

System.out.println("THE CLIENT SYSTEM ADDRESS IS :"+inet);

ps.close();

}

}

catch(IOException e)

{

System.out.println("The exception is :"+e);

}

}

}

**OUTPUT:**

**CLIENTSIDE:**

C:\Program Files\Java\jdk1.5.0\bin>javac dateclient.java

Note: dateclient.java uses or overrides a deprecated API.

Note: Recompile with -deprecation for details.

C:\Program Files\Java\jdk1.5.0\bin>java dateclient

THE date in the server is:Sat Jul 19 13:01:16 GMT+05:30 2008

C:\Program Files\Java\jdk1.5.0\bin>

**SERVERSIDE:**

C:\Program Files\Java\jdk1.5.0\bin>javac dateserver.java

Note: dateserver.java uses or overrides a deprecated API.

Note: Recompile with -deprecation for details.

C:\Program Files\Java\jdk1.5.0\bin>java dateserver

THE CLIENT SYSTEM ADDRESS IS :com17/192.168.21.17

**RESULT:**

Thus the program for date time sever client is executed and output is verified.

EX.No : 10.B

**CLIENT-SERVER APPLICATION FOR CHAT**

**AIM:**

To write a client-server application for chat using TCP

**ALGORITHM: CLIENT**

1.start the program

2. Include necessary package in java

3. To create a socket in client to server.

4. The client establishes a connection to the server.

5. The client accept the connection and to send the data from client to server and vice versa

6. The client communicate the server to send the end of the message

7. Stop the program.

**ALGORITHM: SERVER**

1.start the program

2. Include necessary package in java

3. To create a socket in server to client

4. The server establishes a connection to the client.

5. The server accept the connection and to send the data from server to client and vice versa

6. The server communicate the client to send the end of the message

7. Stop the program.

**TCPserver1.java**

import java.net.\*;

import java.io.\*;

public class TCPserver1

{

public static void main(String arg[])

{

ServerSocket s=null;

String line;

DataInputStream is=null,is1=null;

PrintStream os=null;

Socket c=null;

try

{

s=new ServerSocket(9999);

}

catch(IOException e)

{

System.out.println(e);

}

try

{

c=s.accept();

is=new DataInputStream(c.getInputStream());

is1=new DataInputStream(System.in);

os=new PrintStream(c.getOutputStream());

do

{

line=is.readLine();

System.out.println("Client:"+line);

System.out.println("Server:");

line=is1.readLine();

os.println(line);

}while(line.equalsIgnoreCase("quit")==false);

is.close();

os.close();

}

catch(IOException e)

{

System.out.println(e);

}

}

}

**TCPclient1.java**

import java.net.\*;

import java.io.\*;

public class TCPclient1

{

public static void main(String arg[])

{

Socket c=null;

String line;

DataInputStream is,is1;

PrintStream os;

try

{

c=new Socket("10.0.200.36",9999);

}

catch(IOException e)

{

System.out.println(e);

}

try

{

os=new PrintStream(c.getOutputStream());

is=new DataInputStream(System.in);

is1=new DataInputStream(c.getInputStream());

do

{

System.out.println("Client:");

line=is.readLine();

os.println(line);

System.out.println("Server:" + is1.readLine());

}while(line.equalsIgnoreCase("quit")==false);

is1.close();

os.close();

}

catch(IOException e)

{

System.out.println("Socket Closed!Message Passing is over");

}

}

**OUT PUT :**

Server

C:\Program Files\Java\jdk1.5.0\bin>javac TCPserver1.java

Note: TCPserver1.java uses or overrides a deprecated API.

Note: Recompile with -deprecation for details.

C:\Program Files\Java\jdk1.5.0\bin>java TCPserver1

Client: Hai Server

Server:

Hai Client

Client: How are you

Server:

Fine

Client: quit

Server:

quit

**Client**

C:\Program Files\Java\jdk1.5.0\bin>javac TCPclient1.java

Note: TCPclient1.java uses or overrides a deprecated API.

Note: Recompile with -deprecation for details.

C:\Program Files\Java\jdk1.5.0\bin>java TCPclient1

Client:

Hai Server

Server: Hai Client

Client:

How are you

Server: Fine

Client:

quit

Server: quit

**RESULT:**

Thus the above program a client-server application for chat using TCP / IP was executed and successfully.