A
Practical File In
The Subject Of

Data Communication (2171008)

BACHELOR OF ENGINEERING
in
ELECTRONICS AND COMMUNICATION ENGINEERING

By

Chaitanya Tejaswi 140080111013

Under The Guidance of
Prof. Anish Vahora
Professor, EC Department.

ELECTRONICS & COMMUNICATION ENGINEERING
DEPARTMENT
BVM ENGINEERING COLLEGE
GUJARAT TECHNOLOGICAL UNIVERSITY
VALLABH VIDYANAGAR-388120
Academic Year- 2016-17

CERTIFICATE

This is to certify that the practical file, submitted by ***Chaitanya Tejaswi (140080111013)*** in the subject of ***Data Communication (2171008)*** for the Bachelor of Engineering in Electronics and Communication of BVM Engineering College, Vallabh Vidyanagar, Gujarat Technological University, is the record of work carried out by them under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination.

Under The Guidance Of
Prof. Anish Vahora
Professor, EC Department.

ELECTRONICS & COMMUNICATION ENGINEERING
DEPARTMENT
BVM ENGINEERING COLLEGE
GUJARAT TECHNOLOGICAL UNIVERSITY
VALLABH VIDYANAGAR-388120
Academic Year- 2016-17

INDEX

PRACTICAL: 1

AIM: Introduction to RS232 Communication & BIOSCOM function.

SOFTWARE: Borland Turbo C/C++

THEORY:

RS232

1. The RS232 serial interface is an interface for communicating data by way of transmission.
2. When dealing with data, there are two types of communication that exist: differential and single-ended. RS232 deals with single-ended data communication and it defines a communication between two gadgets or equipments: DTE (Data Terminal Equipment) and DCE (Data Circuit-Termination Equipment).
3. The difference between the two equipments lies in their pin out assignments. An example of a DTE is a PC while that of a DCE is a dial up modem. The two are connected using a RS 232 link cable known as a straight-through - which transfers pin maps to transfer pins and to receive pin maps, it receives pins - , or uses a null modem (a type of a crossover) to connect between two DTE equipments like personal computers.

RS485

1. The RS232 serial port uses independent cannels that are fully duplex, whereas RS485 is half duplex. This means that the RS232 device can send and receive data at the same time. This usually involves three wires; one of the wires sends RS232 data, the other wire receives RS232 data and the other one is the earth-grounding wire which expedites transmission of RS232 data.

   By using 9 pins, this type of RS232 and RS232 to RS485 communication is possible.
2. Even with all those capabilities, there are some limitations, however. RS232 and RS485 ports transmits data in single bit format using asynchronous mode of transmission. This makes communication very slow, and hence many people prefer using other computer interface peripherals like USB. The latter, USB, is faster than RS232 serial port and has supplanted it in many machines. One of the reasons why RS232 and RS485 serial ports are still in use today is sometimes because the cost of replacing them, in expensive machines like those in the factories, but also because RS232 and RS485 actually is compatible with many devices and can easily be integrated with existing software solutions.

RS-232 logic and voltage levels		
Data circuits	**Control circuits**	**Voltage**
0 (space)	Asserted	+3 to +15 V
1 (mark)	Deasserted	−15 to −3 V

Connectors

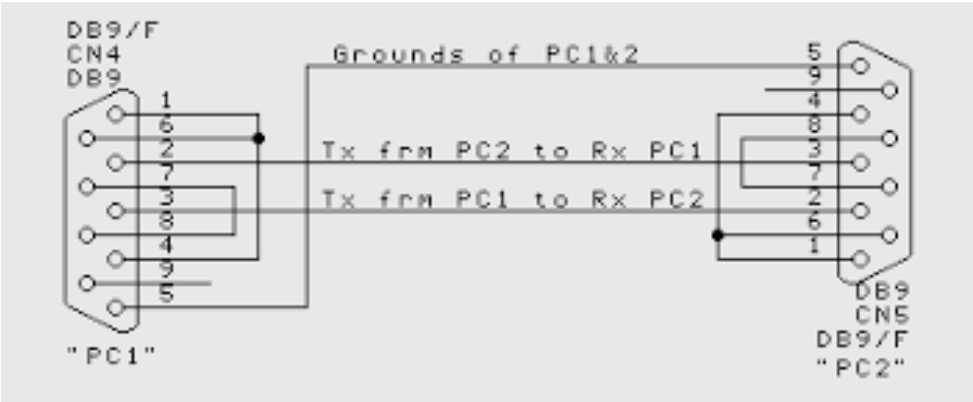
RS-232 devices may be classified as Data Terminal Equipment (DTE) or Data Circuit-terminating Equipment (DCE); this defines at each device which wires will be sending and receiving each signal. According to the standard, male connectors have DTE pin functions, and female connectors have DCE pin functions.

Cables

The standard does not define a maximum cable length, but instead defines the maximum capacitance that a compliant drive circuit must tolerate. A widely used rule of thumb indicates that cables more than 15 m (50 ft) long will have too much capacitance, unless special cables are used. By using low-capacitance cables, full speed communication can be maintained over larger distances up to about 300 m (1,000 ft). For longer distances, other signal standards are better suited to maintain high speed.

3-wire and 5-wire RS-232

A minimal "3-wire" RS-232 connection consisting only of transmit data, receive data, and ground, is commonly used when the full facilities of RS-232 are not required. Even a two-wire connection (data and ground) can be used if the data flow is one way (for example, a digital postal scale that periodically sends a weight reading, or a GPS receiver that periodically sends position, if no configuration via RS-232 is necessary). When only hardware flow control is required in addition to two-way data, the RTS and CTS lines are added in a 5-wire version.



Data and control signals

Circuit		
Name	**Typical purpose**	**Abbreviation**
Data Terminal Ready	DTE is ready to receive, initiate, or continue a call.	DTR
Data Carrier Detect	DCE is receiving a carrier from a remote DCE.	DCD
Data Set Ready	DCE is ready to receive commands or data.	DSR
Ring Indicator	DCE has detected an incoming ring signal on the telephone line.	RI
Request To Send	DTE requests the DCE prepare to transmit data.	RTS
Ready To Receive	DTE is ready to receive data from DCE. If in use, RTS is assumed to be always asserted.	RTR
Clear To Send	DCE is ready to accept data from the DTE.	CTS
Transmitted Data	Carries data from DTE to DCE.	TxD
Received Data	Carries data from DCE to DTE.	RxD
Common Ground	Zero voltage reference for all of the above.	GND
Protective Ground	Connected to chassis ground.	PG

BIOSCOM

The macro bioscom () and function _bios_serialcom() are used in this method in the serial communication using RS-232 connecter. First we have to set the port with the settings depending on our need and availability. In this method, same function is used to make the settings using control word, to send data to the port and check the status of the port. These actions are distinguished using the first parameter of the function. Along with that we are sending data and the port to be used to communicate.

Here are the deatails of the Turbo C Functions for communication ports.

Declaration:

```
bioscom(int cmd,char abyte,int port);
_bios_serialcom(int cmd,int port,char abyte);
```

`bioscom()` and `_bios_serialcom()` uses the BIOS interrupt 0x14 to perform various serial communication preocedures over the I/O ports given in port.

Arguments:

cmd – the I/O operation to be performed.

bioscom	_bios_serialcom	Action
0	_COM_INIT	Initialise the parameters to the port
1	_COM_SEND	Send the character to the port
2	_COM_RECEIVE	Receive character from the port
3	_COM_STATUS	Returns rhe current status of the communication port

portid – port to which data is to be sent or from which data is to be read.

0:COM1
1:COM2
2:COM3

abyte –

- When cmd =2 or 3 (_COM_SEND or _COM_RECEIVE) parameter abyte is ignored.
- When cmd = 0 (_COM_INIT), abyte is an OR combination of the following bits (One from each group):

Value of abyte		Meaning
bioscom	_bios_serialcom	
0x02	_COM_CHR7	7 data bits
0x03	_COM_CHR8	8 data bits
0x00	_COM_STOP1	1 stop bit
0x04	_COM_STOP2	2 stop bits
0x00	_COM_NOPARITY	No parity
0x08	_COM_ODDPARITY	Odd parity
0X10	_COM_EVENPARITY	Even parity
0x00	_COM_110	110 baud
0x20	_COM_150	150 baud
0x40	_COM_300	300 baud
0x60	_COM_600	600 baud
0x80	_COM_1200	1200 baud
0xA0	_COM_2400	2400 baud
0xC0	_COM_4800	4800 baud
0xE0	_COM_9600	9600 baud

CONCLUSION:

Thus we got to learn about RS232 Serial Communication & use of BIOSCOM utility in C to implement serial communication using COM ports.

PRACTICAL: 2

AIM: Implementation of full-duplex communication in C.

SOFTWARE: Borland Turbo C/C++

THEORY:

Full Duplex System

1. Full duplex refers to the transmission of data in two directions simultaneously. For example, a telephone is a full-duplex device because both parties can talk at once. Full-duplex data transmission means that data can be transmitted in both directions on a signal carrier at the same time. For example, on a local area network with a technology that has full-duplex transmission, one workstation can be sending data on the line while another workstation is receiving data. Full-duplex transmission necessarily implies a bidirectional line (one that can move data in both directions).
2. Most modems have a switch that lets you choose between full-duplex and half-duplex modes. The choice depends on which communications program you are running.
3. In full-duplex mode, data you transmit does not appear on your screen until it has been received and sent back by the other party. This enables you to validate that the data has been accurately transmitted. If your display screen shows two of each character, it probably means that your modem is set to half-duplex mode when it should be in full-duplex mode.

PROGRAM:

```
#include <bios.h>
#include <conio.h>

#define COM1        0
#define DATA_READY 0x100
#define TRUE        1
#define FALSE       0

#define SETTINGS ( 0x80 | 0x02 | 0x00 | 0x00)

int main(void){
   int in, out, status, DONE = FALSE;
   /* Initialize bioscom */
   bioscom(0, SETTINGS, COM1);
   /*  Transmitter bioscom initialization */
   cprintf("... BIOSCOM [ESC] to exit ...\n");
   while (!DONE){
      /* Condition initialization for data transmission */
      status = bioscom(3, 0, COM1);
      if (status & DATA_READY)
        if ((out = bioscom(2, 0, COM1) & 0x7F) != 0)
          putch(out);
      if (kbhit()){
        if ((in = getch()) == '\x1B')/* Check the input sequence */
          DONE = TRUE;
        bioscom(1, in, COM1);        /* Call bioscom */
       }

   }
   return 0;
}
```

CONCLUSION:

Thus, we made use of BIOSCOM utility in C to implement full-duplex serial communication using COM ports.

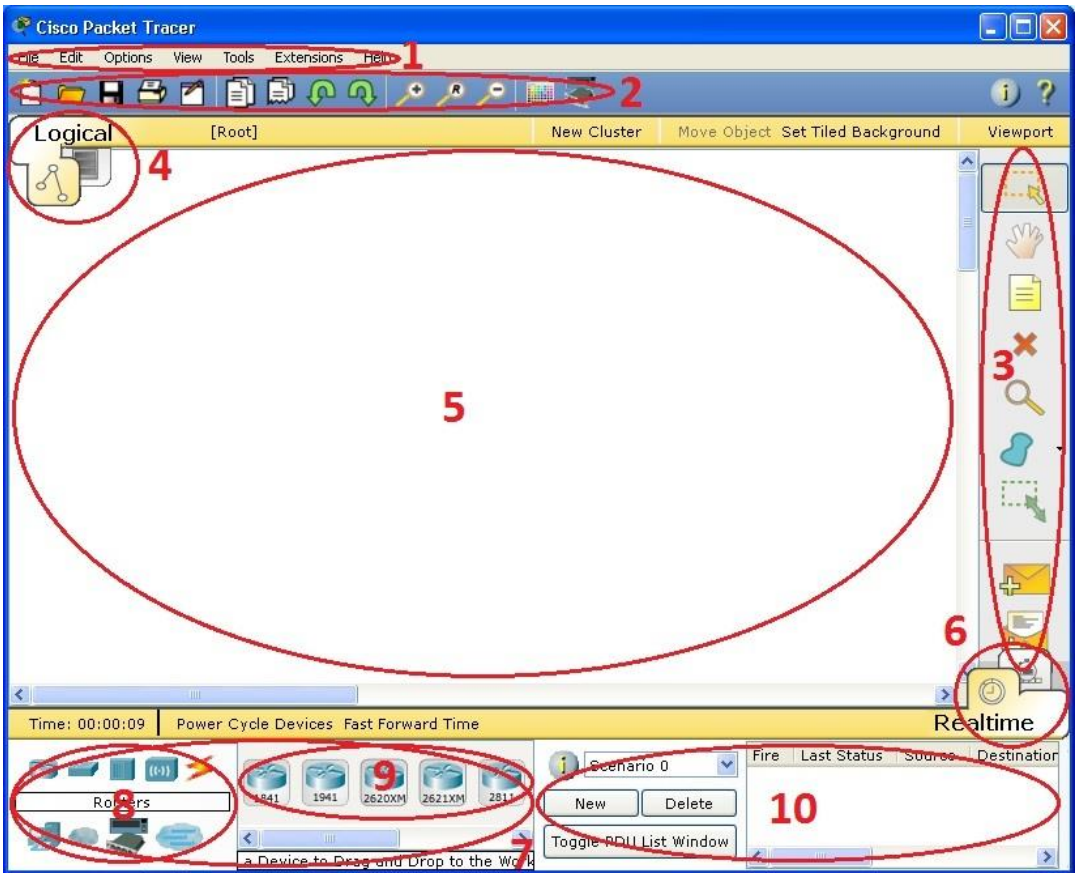
PRACTICAL: 3

AIM: Introduction to CISCO PacketTracer.

SOFTWARE: CISCO PacketTracer 7.0

THEORY:

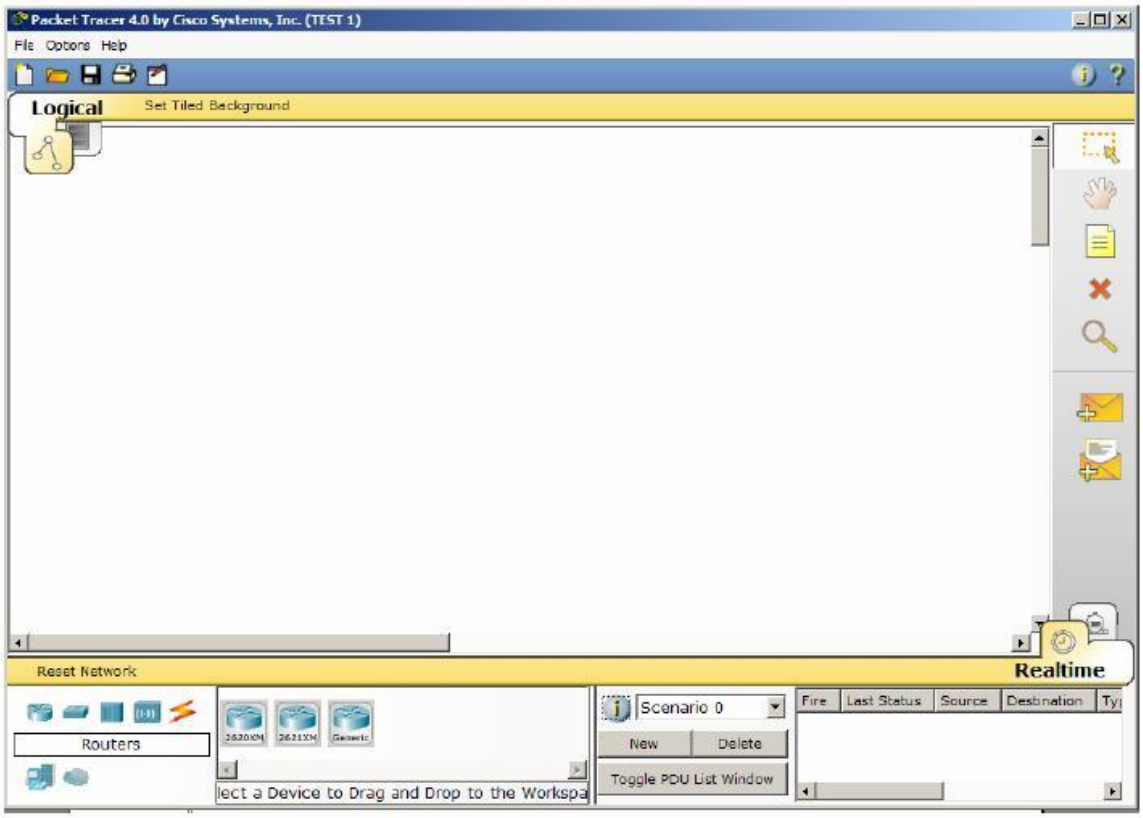
Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts.



1	**Menu Bar**	This bar provides the **File**, **Edit**, **Options**, **View**, **Tools**, **Extensions**, and **Help** menus. You will find basic commands such as **Open**, **Save**, **Save as Pkz**, **Print**, and **Preferences** in these menus. You will also be able to access the **Activity Wizard** from the **Extensions** menu.
2	**Main Tool Bar**	This bar provides shortcut icons to the **File** and **Edit** menu commands. This bar also provides buttons for **Copy**, **Paste**, **Undo**, **Redo**, **Zoom**, the **Drawing Palette**, and the **Custom Devices Dialog**. On the right, you will also find the **Network Information** button, which you can use to enter a description for the current network (or any text you wish to include).
3	**Common Tools Bar**	This bar provides access to these commonly used workspace tools: **Select**, **Move Layout**, **Place Note**, **Delete**, **Inspect**, **Resize Shape**, **Add Simple PDU**, and **Add Complex PDU**. See "Workspace Basics" for more information.
4	**Logical/Physical Workspace and Navigation Bar**	You can toggle between the Physical Workspace and the Logical Workspace with the tabs on this bar. In Logical Workspace, this bar also allows you to go back to a previous level in a cluster, create a **New Cluster**, **Move Object**, **Set Tiled Background**, and **Viewport**. In Physical Workspace, this bar allows you to navigate through physical locations, create a **New City**, create a **New Building**, create a **New Closet**, **Move Object**, apply a **Grid** to the background, **Set Background**, and go to the **Working Closet**.
5	**Workspace**	This area is where you will create your network, watch simulations, and view many kinds of information and statistics.
6	**Realtime/Simulation Bar**	You can toggle between Realtime Mode and Simulation Mode with the tabs on this bar. This bar also provides buttons to **Power Cycle Devices** and **Fast Forward Time** as well as the **Play Control** buttons and the **Event List** toggle button in Simulation Mode. Also, it contains a clock that displays the relative **Time** in Realtime Mode and Simulation Mode.
7	**Network Component Box**	This box is where you choose devices and connections to put into the workspace. It contains the **Device-Type Selection** Box and the **Device-Specific Selection** Box.
8	**Device-Type Selection Box**	This box contains the type of devices and connections available in Packet Tracer. The **Device-Specific Selection** Box will change depending on which type of device you choose.
9	**Device-Specific Selection Box**	This box is where you choose specifically which devices you want to put in your network and which connections to make.
10	**User Created Packet Window***	This window manages the packets you put in the network during simulation scenarios. See the "Simulation Mode" section for more details.

Introduction to the Packet Tracer Interface using a Hub Topology

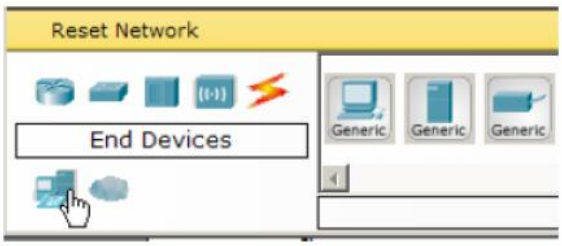
Step 1: Start Packet Tracer and Entering Simulation Mode



Step 2: Choosing Devices and Connections

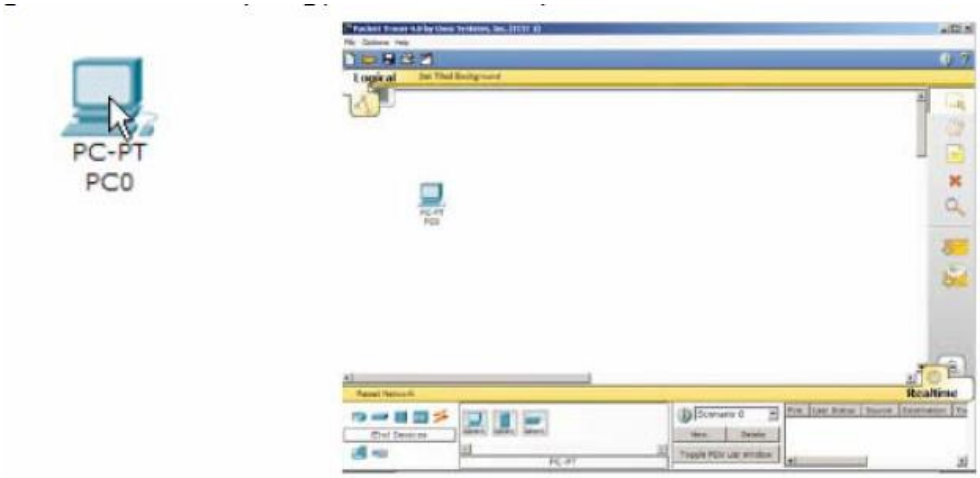
- We will begin building our network topology by selecting devices and the media in which to connect them.
- Several types of devices and network connections can be used. For this lab we will keep it simple by using End Devices, Switches, Hubs, and Connections.
- Single-click on each group of devices and connections to display the various choices.

Step 3: Building the Topology – Adding Hosts Single click on the End Devices



Single click on the **Generic** host.

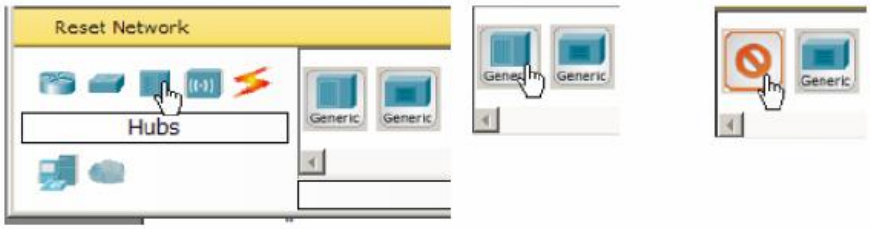
- Move the cursor into topology area. You will notice it turns into a plus "+" sign.
- Single click in the topology area and it copies the device.



- Add three more hosts.

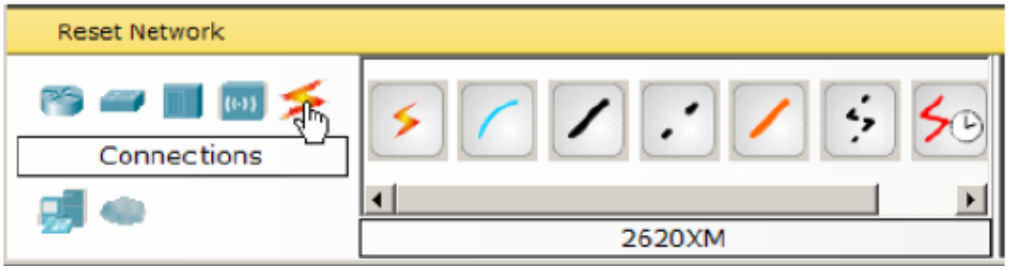
Step 4: Building the Topology – Connecting the Hosts to Hubs and Switches

- Adding a Hub
  Select a hub, by clicking once on Hubs and once on a Generic hub.



  Add the hub, by moving the + sign below PC0 & PC1 and click once.

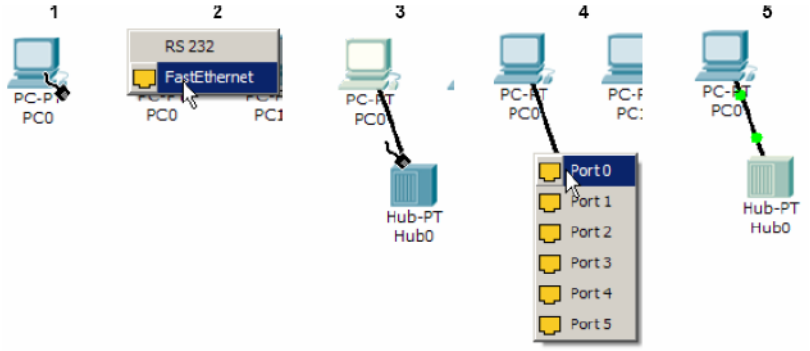
  Connect PC0 to Hub0 by first choosing Connections.



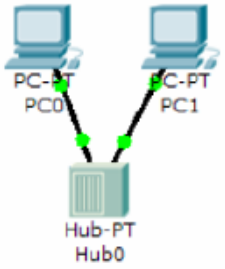
  Click once on the **Copper straight-through** cable.

  Perform the following steps to connect PC0 to Hub0:
  1. Click once on PC0
  2. Choose FastEthernet
  3. Drag the cursor to Hub0
  4. Click once on Hub0 and choose Port 0

5. Notice the green link lights on both the PC0 Ethernet-NIC and the Hub0 Port0 showing that the link is active.

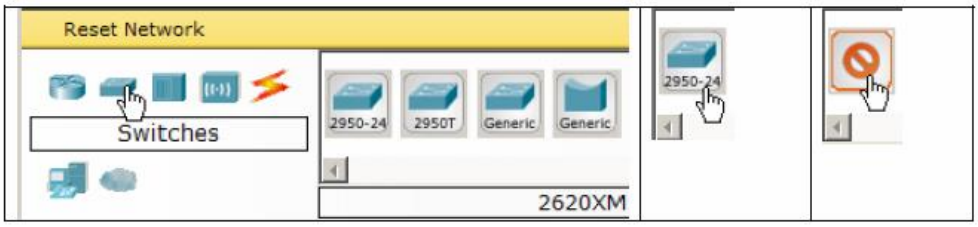


Repeat the above steps for PC1, connecting it to Port1 on Hub0.

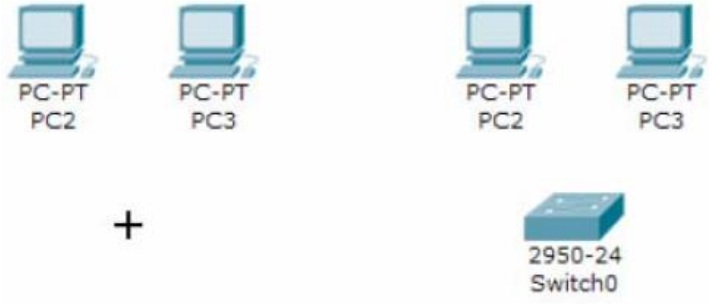


- Adding a Switch

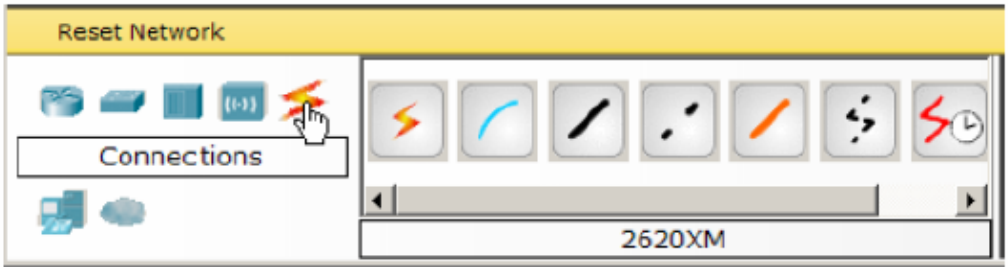
Select a switch, by clicking once on Switches and once on a 2950-24 switch.



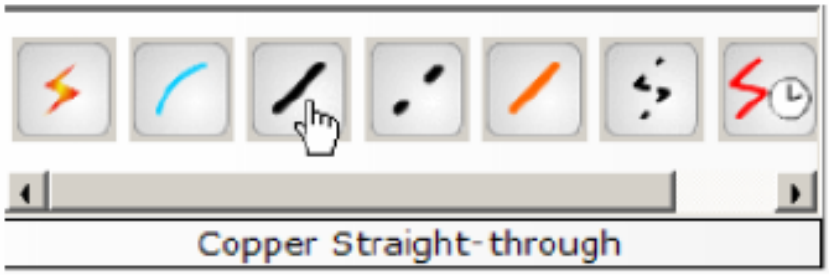
Add the switch by moving the plus sign "+" below PC2 & PC3, click once.



Connect PC0 to Hub0 by first choosing Connections.

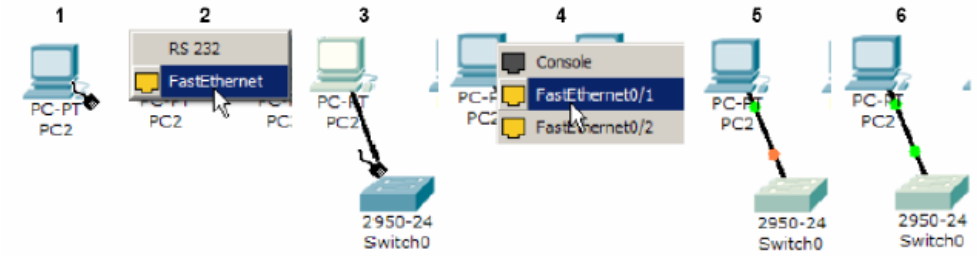


Click once on the **Copper straight-through** cable.

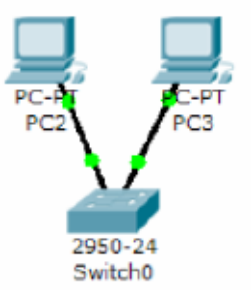


Perform the following steps to connect PC0 to Hub0:

1. Click once on PC2
2. Choose FastEthernet
3. Drag the cursor to Switch0
4. Click once on Switch0 and choose FastEthernet0/1
5. Notice the green link lights on PC2 Ethernet NIC and amber light Switch0 FastEthernet0/1 port. The switch port is temporarily not forwarding frames, while it goes through the stages for the Spanning Tree Protocol (STP) process.
6. After a about 30 seconds the amber light will change to green indicating that the port has entered the forwarding stage. Frames can now forwarded out the switch port.



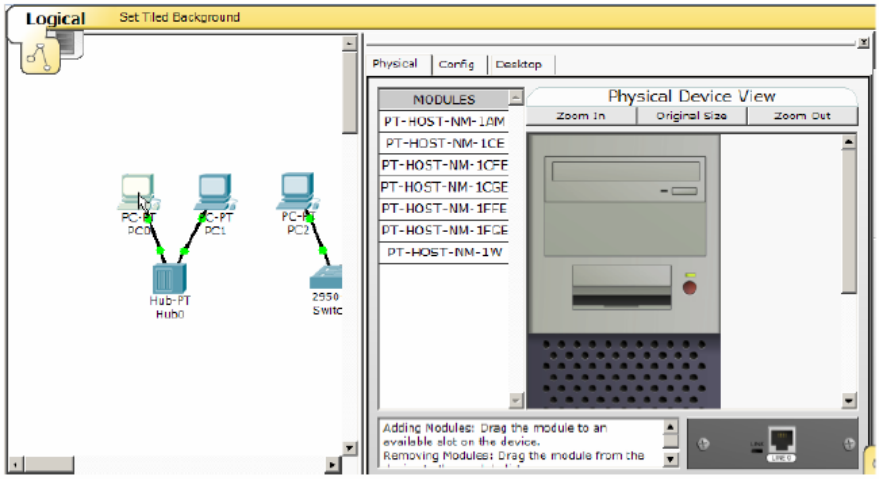
Repeat the above steps for PC3, connecting it to Port3 on Switch0 on port FastEthernet0/2.



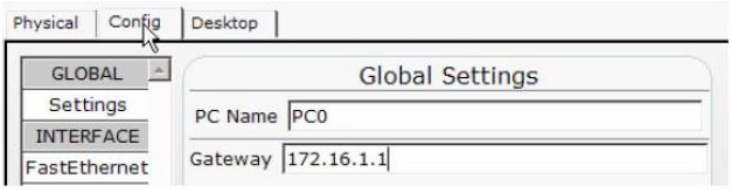
Move the cursor over the link light to view the port number. Fa means Fast Ethernet, 100 Mbps Ethernet.

Step 5: Configuring IP Addresses and Subnet Masks on the Hosts

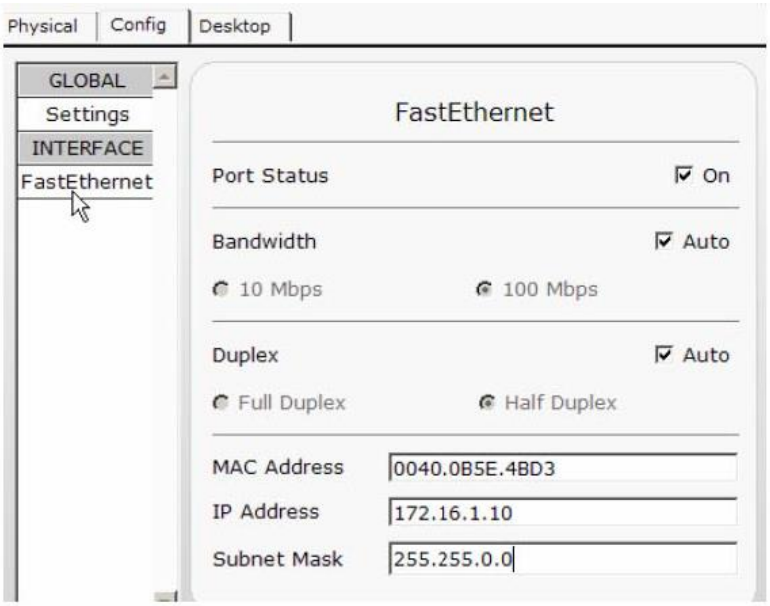
- Before we can communicate between the hosts we need to configure IP Addresses and Subnet Masks on the devices.
- Click once on PC0.



- **Choose the Config tab.**
  It is here that you can change the name of PC0. It is also here where you would enter a Gateway IP Address, also known as the default gateway. We will discuss this later, but this would be the IP address of the local router. If you want, you can enter the IP Address 172.16.1.1, although it will not be used in this lab.



- **Click on FastEthernet.**
  Although we have not yet discussed IP Addresses, add the IP Address to 172.16.1.10. Click once in the Subnet Mask field to enter the default Subnet Mask. You can leave this at 255.255.0.0. We will discuss this later.



  Also, notice this is where you can change the Bandwidth (speed) and Duplex of the Ethernet NIC (Network Interface Card). The default is Auto (autonegotiation), which means the NIC will negotiate with the hub or switch. The bandwidth and/or duplex can be manually set by removing the check from the Auto box and choosing the specific option.

- **Bandwidth - Auto**
  If the host is connected to a hub or switch port which can do 100 Mbps, then the Ethernet NIC on the host will choose 100 Mbps (Fast Ethernet). Otherwise, if the hub or switch port can only do 10 Mbps, then the Ethernet NIC on the host will choose 10 Mbps (Ethernet).

- **Duplex - Auto**
  Hub: If the host is connected to a hub, then the Ethernet NIC on the host will choose Half Duplex.
  Switch: If the host is connected to a switch, and the switch port is configured as Full Duplex (or Autonegotiation), then the Ethernet NIC on the host will choose Full Duplex. If the switch port is configured as Half

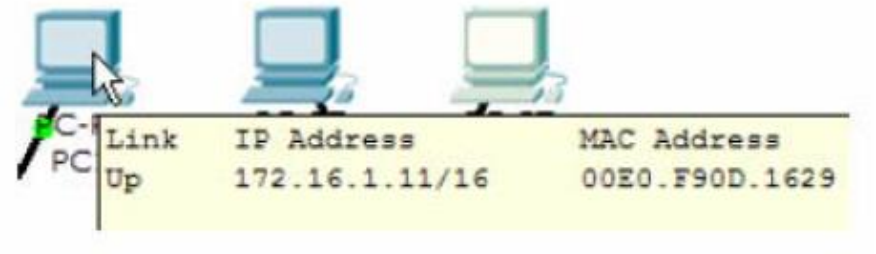
Duplex, then the Ethernet NIC on the host will choose Half Duplex. (Full Duplex is a much more efficient option.)
The information is automatically saved when entered.

- Repeat these steps for the other hosts. Use the information below for IP Addresses and Subnet Masks.

Host	IP Address	Subnet Mask
PC0	172.16.1.10	255.255.0.0
PC1	172.16.1.11	255.255.0.0
PC2	172.16.1.12	255.255.0.0
PC3	172.16.1.13	255.255.0.0

- Verify the information

To verify the information that you entered, move the Select tool (arrow) over each host.

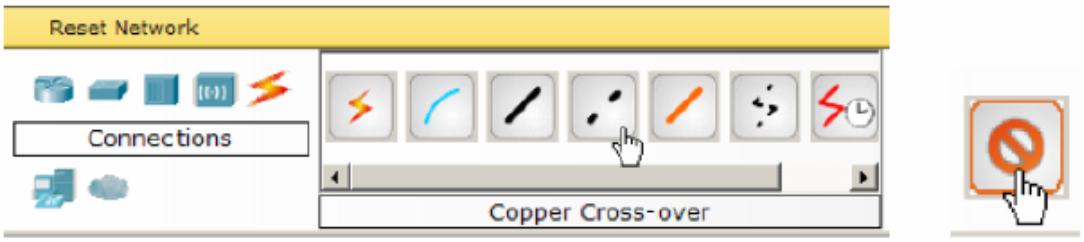


- Deleting a Device or Link

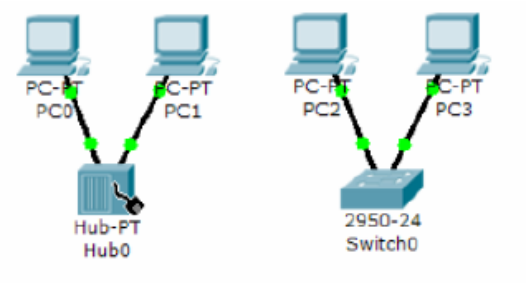
To delete a device or link, choose the Delete tool and click on the item you wish to delete.

Step 6: Connecting Hub0 to Switch0

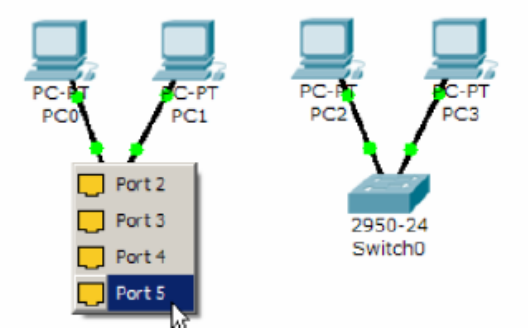
- To connect like-devices, like a Hub and a Switch, we will use a Cross-over cable. Click once the Cross-over Cable from the Connections options.



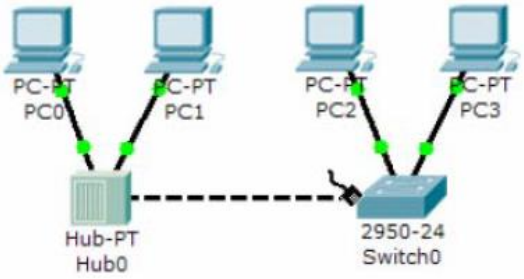
- Move the Connections cursor to Switch0.



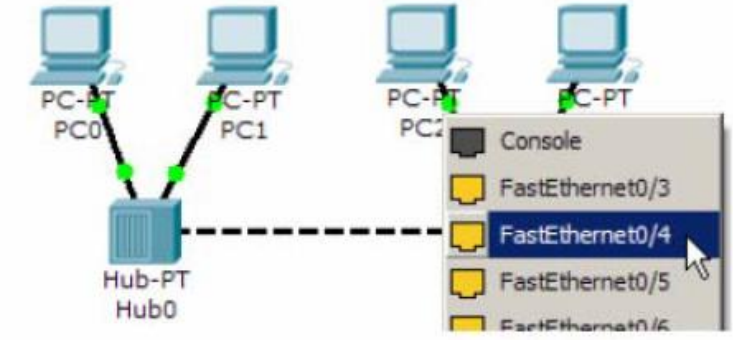
- Select Port5.



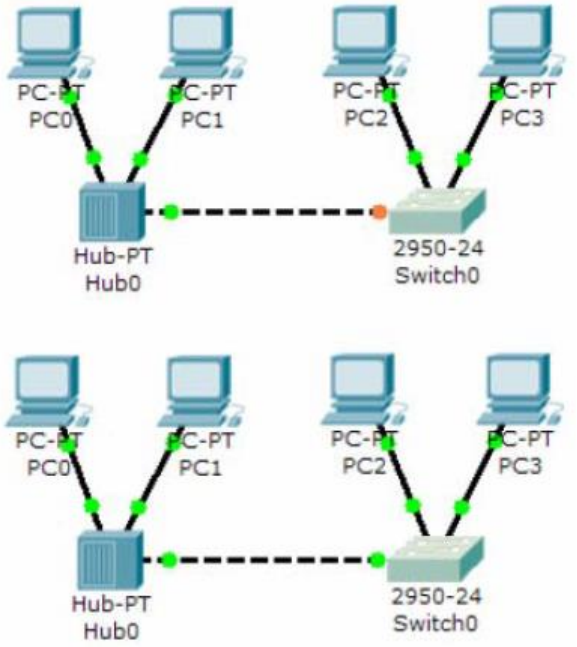
- Move the Connections cursor to Switch0.



- Click once on Switch0 and choose FastEthernet0/4.



- The link light for switch port FastEthernet0/4 will begin as amber and eventually change to green as the Spanning Tree Protocol transitions the port to forwarding.



CONCLUSION: Thus, we got to learn CISCO's PacketTracer software.

PRACTICAL: 4

AIM: To study different network commands.

SOFTWARE: Windows Command Prompt.

THEORY:

Windows Network Diagnostic Commands

`ipconfig`
It's a Console Command which can be issued to the Command Line Interpreter (or command prompt) to display the network settings currently assigned to any or all network adapters in the machine. This command can be utilized to verify a network connection as well as to verify your network settings.

`netstat`
Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, `netstat` displays active TCP connections.

`tracert`
The `tracert` command is used to visually see a network packet being sent and received and the amount of hops required for that packet to get to its destination.

`ping`
Helps in determining TCP/IP Networks IP address as well as determine issues with the network and assists in resolving them.

`pathping`
Provides information about network latency and network loss at intermediate hops between a source and destination. `pathping` sends multiple Echo Request messages to each router between a source and destination over a period of time and then computes results based on the packets returned from each router.

`telnet`
Telnet is software that allows users to remotely access another computer such as a server, network device, or other computer. With `telnet` users can connect to a device or computer, manage a network device, setup a device, transfer files, etc.

`ftp`
FTP is short for File Transfer Protocol, this page contains additional information about the FTP command and help using that command in Unix and MS-DOS (Windows).

`route`
The function and syntax of the Windows `ROUTE` command is similar to the UNIX or Linux `route` command. Use the command to manually configure the routes in the routing table.

`arp`
Displays, adds, and removes `arp` information from network devices.

`nslookup`
Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The Nslookup command-line tool is available only if you have installed the TCP/IP protocol.

`nbtstat`
Displays protocol statistics and current TCP/IP connections using NBT.

`netsh`
One common way of using netsh is to reset the TCP/IP in Windows 2k/XP

```
netsh int ip reset
```

In Windows XP you can run a graphical diagnostics by typing

```
netsh diag gui
```

into the run dialog box. (This may take a little time to startup)

`getmac`

DOS command used to show both local and remote MAC addresses. When run with no parameters (ie. `getmac`) it displays MAC addresses for the local system. When run with the `/s` parameter (eg. `getmac /s \\foo`) it displays MAC addresses for the remote computer. When the `/v` parameter is used, it also displays the associated connection name and network adapter name.

Find All Active/Used IP Addresses on Your Network

There is a really neat way that you can quite easily find all active/used IP Addresses on your network without the need for any third party applications or worse, pinging each IP Address individually.

Open the Command Prompt and type in the following:

```
FOR /L %i IN (1,1,254) DO ping -n 1 192.168.10.%i |
FIND /i "Reply">>c:\ipaddresses.txt
```

Change `192.168.10` to match you own network.

IMPLEMENTATION:
(In the corresponding order as listed in '**THEORY**')

```
C:\Users\Satellite>ipconfig /?

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.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                      ... Show information
    > ipconfig /all                 ... Show detailed information
    > ipconfig /renew               ... renew all adapters
    > ipconfig /renew EL*           ... renew any connection that has its
                                        name starting with EL
    > ipconfig /release *Con*       ... release all matching connections,
                                        eg. "Wired Ethernet Connection 1" or
                                            "Wired Ethernet Connection 2"
    > ipconfig /allcompartments     ... Show information about all
                                        compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                                        compartments
```

```
C:\Users\Satellite>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

```
C:\Users\Satellite>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                  Do not resolve addresses to hostnames.
    -h maximum_hops     Maximum number of hops to search for target.
    -j host-list        Loose source route along host-list (IPv4-only).
    -w timeout          Wait timeout milliseconds for each reply.
    -R                  Trace round-trip path (IPv6-only).
    -S srcaddr          Source address to use (IPv6-only).
    -4                  Force using IPv4.
    -6                  Force using IPv6.
```

```
C:\Users\Satellite>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

```
C:\Users\Satellite>pathping /?

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.
```

```
C:\Users\Satellite>telnet /?

telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]
 -a      Attempt automatic logon. Same as -l option except uses
         the currently logged on user's name.
 -e      Escape character to enter telnet client prompt.
 -f      File name for client side logging
 -l      Specifies the user name to log in with on the remote system.
         Requires that the remote system support the TELNET ENVIRON option.
 -t      Specifies terminal type.
         Supported term types are vt100, vt52, ansi and vtnt only.
 host    Specifies the hostname or IP address of the remote computer
         to connect to.
 port    Specifies a port number or service name.
```

```
C:\Users\Satellite>ftp /?

Transfers files to and from a computer running an FTP server service
(sometimes called a daemon). Ftp can be used interactively.

FTP [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-A] [-x:sendbuffer] [-r:recvbuffer] [-b:a
syncbuffers] [-w:windowsize] [host]

  -v              Suppresses display of remote server responses.
  -n              Suppresses auto-login upon initial connection.
  -i              Turns off interactive prompting during multiple file
                  transfers.
  -d              Enables debugging.
  -g              Disables filename globbing (see GLOB command).
  -s:filename     Specifies a text file containing FTP commands; the
                  commands will automatically run after FTP starts.
  -a              Use any local interface when binding data connection.
  -A              login as anonymous.
  -x:send sockbuf Overrides the default SO_SNDBUF size of 8192.
  -r:recv sockbuf Overrides the default SO_RCVBUF size of 8192.
  -b:async count  Overrides the default async count of 3
  -w:windowsize   Overrides the default transfer buffer size of 65535.
  host            Specifies the host name or IP address of the remote
                  host to connect to.

Notes:
  - mget and mput commands take y/n/q for yes/no/quit.
  - Use Control-C to abort commands.
```

```
C:\Users\Satellite>arp /?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

```
C:\Users\Satellite>nbtstat /?

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses

  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

```
C:\Users\Satellite>route /?

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]

  -f           Clears the routing tables of all gateway entries.  If this is
               used in conjunction with one of the commands, the tables are
               cleared prior to running the command.

  -p           When used with the ADD command, makes a route persistent across
               boots of the system. By default, routes are not preserved
               when the system is restarted. Ignored for all other commands,
               which always affect the appropriate persistent routes.

  -4           Force using IPv4.

  -6           Force using IPv6.

  command      One of these:
                 PRINT     Prints  a route
                 ADD       Adds    a route
                 DELETE    Deletes a route
                 CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid. (Destinat
ion & Mask) != Destination.
 Examples:

    > route PRINT
    > route PRINT -4
    > route PRINT -6
    > route PRINT 157*          .... Only prints those matching 157*

    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              destination^      ^mask      ^gateway     metric^    ^
                                                        Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route ADD 3ffe::/32 3ffe::1

    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.

    > route DELETE 157.0.0.0
    > route DELETE 3ffe::/32
```

```
C:\Users\Satellite>nslookup /?
Usage:
   nslookup [-opt ...]             # interactive mode using default server
   nslookup [-opt ...] - server    # interactive mode using 'server'
   nslookup [-opt ...] host        # just look up 'host' using default server
   nslookup [-opt ...] host server # just look up 'host' using 'server'
```

```
C:\Users\Satellite>netsh /?

Usage: netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName\]UserName] [-p
 Password | *]
            [Command | -f ScriptFile]

The following commands are available:

Commands in this context:
?               - Displays a list of commands.
add             - Adds a configuration entry to a list of entries.
advfirewall     - Changes to the `netsh advfirewall' context.
branchcache     - Changes to the `netsh branchcache' context.
bridge          - Changes to the `netsh bridge' context.
delete          - Deletes a configuration entry from a list of entries.
dhcpclient      - Changes to the `netsh dhcpclient' context.
dnsclient       - Changes to the `netsh dnsclient' context.
dump            - Displays a configuration script.
exec            - Runs a script file.
firewall        - Changes to the `netsh firewall' context.
help            - Displays a list of commands.
http            - Changes to the `netsh http' context.
interface       - Changes to the `netsh interface' context.
ipsec           - Changes to the `netsh ipsec' context.
lan             - Changes to the `netsh lan' context.
mbn             - Changes to the `netsh mbn' context.
namespace       - Changes to the `netsh namespace' context.
nap             - Changes to the `netsh nap' context.
netio           - Changes to the `netsh netio' context.
p2p             - Changes to the `netsh p2p' context.
ras             - Changes to the `netsh ras' context.
rpc             - Changes to the `netsh rpc' context.
set             - Updates configuration settings.
show            - Displays information.
trace           - Changes to the `netsh trace' context.
wcn             - Changes to the `netsh wcn' context.
wfp             - Changes to the `netsh wfp' context.
winhttp         - Changes to the `netsh winhttp' context.
winsock         - Changes to the `netsh winsock' context.
wlan            - Changes to the `netsh wlan' context.

The following sub-contexts are available:
 advfirewall branchcache bridge dhcpclient dnsclient firewall http interface ipsec lan mbn
 namespace nap netio p2p ras rpc trace wcn wfp winhttp winsock wlan

To view help for a command, type the command, followed by a space, and then
 type ?.
```

CONCLUSION:

Thus, we made use of *Command Prompt* utility in *Windows* to implement various network diagnostic tools.

PRACTICAL: 5

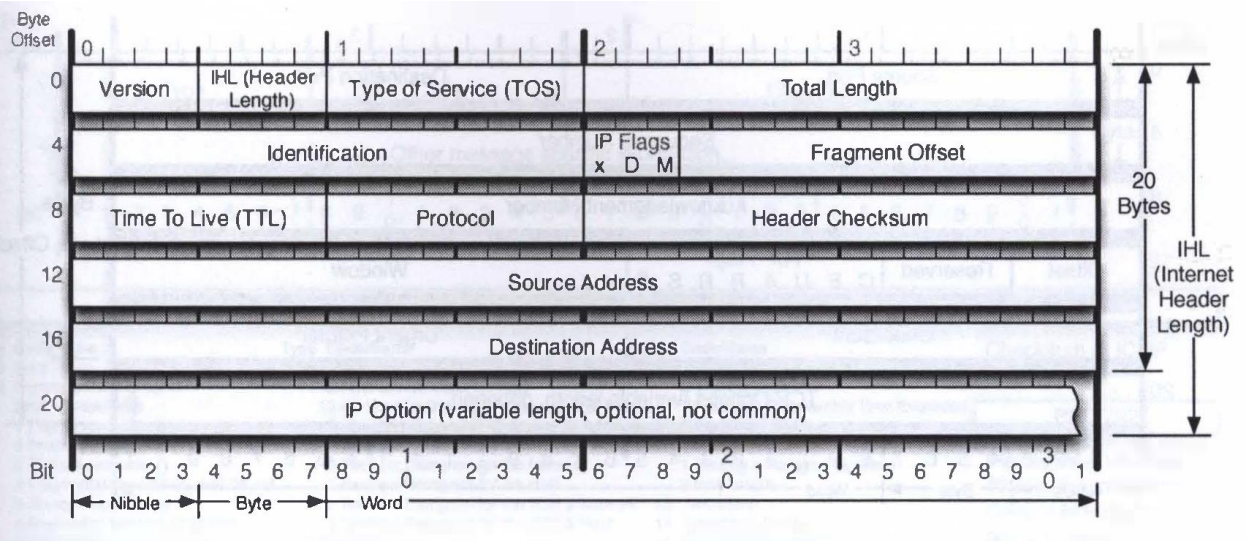
AIM: To study IPv4 Addressing & Subnet Masking.

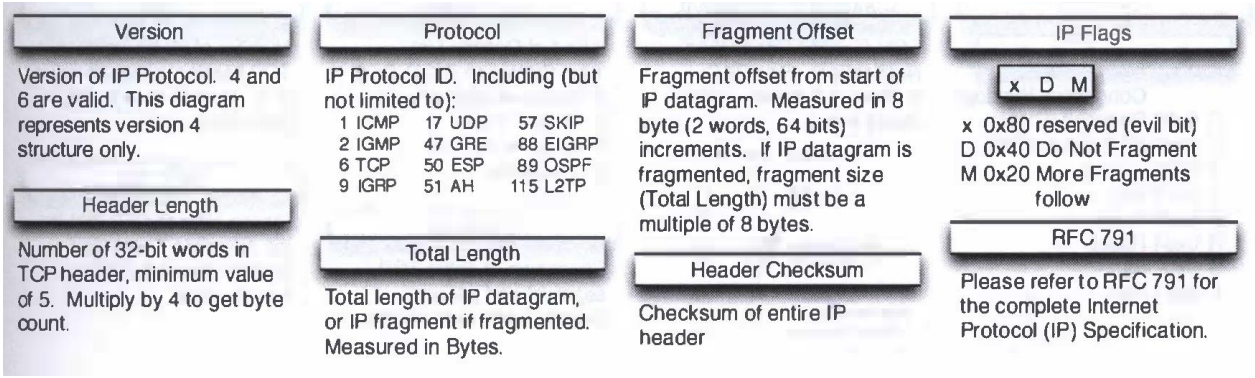
THEORY:

IPv4

1. Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet, and was the first version deployed for production in the ARPANET in 1983. It still routes most Internet traffic today, despite the ongoing deployment of a successor protocol, IPv6. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).
2. IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

IPv4 Header





IPv4 Classes

Class	Theoretical Address Range	Binary Start	Used for
A	0.0.0.0 to 127.255.255.255	0	Very large networks
B	128.0.0.0 to 191.255.255.255	10	Medium networks
C	192.0.0.0 to 223.255.255.255	110	Small networks
D	224.0.0.0 to 239.255.255.255	1110	Multicast
E	240.0.0.0 to 247.255.255.255	1111	Experimental

IPv4 Addressing

IPv4 uses 32-bit addresses which limits the address space to 4294967296 (232) addresses. IPv4 reserves special address blocks for private networks (~18 million addresses) and multicast addresses (~270 million addresses).

Address representations

1. IPv4 addresses may be represented in any notation expressing a 32-bit integer value. They are most often written in the dot-decimal notation, which consists of four octets of the address expressed individually in decimal numbers and separated by periods. The CIDR notation standard combines the address with its routing prefix in a compact format, in which the address is followed by a slash character (/) and the count of consecutive 1 bits in the routing prefix (subnet mask).
2. For example, the quad-dotted IP address 192.0.2.235 represents the 32-bit decimal number 3221226219, which in hexadecimal format is 0xC00002EB. This may also be expressed in dotted hex format as 0xC0.0x00.0x02.0xEB, or with octal byte values as 0300.0000.0002.0353.

Allocation

1. In the original design of IPv4, an IP address was divided into two parts: the network identifier was the most significant (highest order) octet of the address, and the host identifier was the rest of the address. The latter was also called the rest field. This

structure permitted a maximum of 256 network identifiers, which was quickly found to be inadequate.

2. To overcome this limit, the most-significant address octet was redefined in 1981 to create network classes, in a system which later became known as classful networking. The revised system defined five classes. Classes A, B, and C had different bit lengths for network identification. The rest of the address was used as previously to identify a host within a network, which meant that each network class had a different capacity for addressing hosts. Class D was defined for multicast addressing and Class E was reserved for future applications.

Special-use addresses

The Internet Engineering Task Force (IETF) and the Internet Assigned Numbers Authority (IANA) have restricted from general use various reserved IP addresses for special purposes. Some are used for maintenance of routing tables, for multicast traffic, operation under failure modes, or to provide addressing space for public, unrestricted uses on private networks.

Reserved address blocks

Range	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	RFC 6890
10.0.0.0/8	Private network	RFC 1918
100.64.0.0/10	Shared Address Space	RFC 6598
127.0.0.0/8	Loopback	RFC 6890
169.254.0.0/16	Link-local	RFC 3927
172.16.0.0/12	Private network	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 6890
192.0.2.0/24	TEST-NET-1, documentation and examples	RFC 5737
192.88.99.0/24	IPv6 to IPv4 relay (includes 2002::/16)	RFC 3068
192.168.0.0/16	Private network	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
198.51.100.0/24	TEST-NET-2, documentation and examples	RFC 5737
203.0.113.0/24	TEST-NET-3, documentation and examples	RFC 5737
224.0.0.0/4	IP multicast (former Class D network)	RFC 5771
240.0.0.0/4	Reserved (former Class E network)	RFC 1700
255.255.255.255	Broadcast	RFC 919

Private networks

Of the approximately four billion addresses defined in IPv4, three ranges are reserved for use in private networks. Packets addresses in these ranges are not routable in the public Internet, because they are ignored by all public routers. Therefore, private hosts cannot directly communicate with public networks, but require network address translation at a routing gateway for this purpose.

Name	Address range	Number of addresses	*Classful* description	Largest CIDR block
24-bit block	10.0.0.0 – 10.255.255.255	16 777 216	Single Class A	10.0.0.0/8
20-bit block	172.16.0.0 – 172.31.255.255	1 048 576	Contiguous range of 16 Class B blocks	172.16.0.0/12
16-bit block	192.168.0.0 – 192.168.255.255	65 536	Contiguous range of 256 Class C blocks	192.168.0.0/16

Since two private networks, e.g., two branch offices, cannot directly interoperate via the public Internet, the two networks must be bridged across the Internet via a virtual private network (VPN) or an IP tunnel, which encapsulate the packet in a protocol layer during transmission across the public network. Additionally, encapsulated packets may be encrypted for the transmission across public networks to secure the data.

Link-local addressing

1. RFC 3927 defines the special address block 169.254.0.0/16 for link-local addressing. These addresses are only valid on links (such as a local network segment or point-to-point connection) connected to a host. These addresses are not routable. Like private addresses, these addresses cannot be the source or destination of packets traversing the internet. These addresses are primarily used for address autoconfiguration (`Zeroconf`) when a host cannot obtain an IP address from a DHCP server or other internal configuration methods.
2. When the address block was reserved, no standards existed for address autoconfiguration. Microsoft created an implementation called Automatic Private IP Addressing (APIPA), which was deployed on millions of machines and became a de facto standard. Many years later, in May 2005, the IETF defined a formal standard in RFC 3927, entitled Dynamic Configuration of IPv4 Link-Local Addresses.

Loopback

The class A network 127.0.0.0 (classless network 127.0.0.0/8) is reserved for loopback. IP packets whose source addresses belong to this network should never appear outside a host. The modus operandi of this network expands upon that of a loopback interface:

- IP packets whose source and destination addresses belong to the network (or subnetwork) of the same loopback interface are returned to that interface;
- IP packets whose source and destination addresses belong to networks (or subnetworks) of different interfaces of the same host, one of them being a loopback interface, are forwarded regularly.

Addresses ending in 0 or 255

1. Networks with subnet masks of at least 24 bits, i.e. Class C networks in classful networking, and networks with CIDR suffixes /24 to /32 (255.255.255.0–255.255.255.255) may not have an address ending in 0 or 255.
2. ***Classful Addressing*** prescribed only three possible subnet masks: Class A, 255.0.0.0 or /8; Class B, 255.255.0.0 or /16; and Class C, 255.255.255.0 or /24.
   For example, in the subnet 192.168.5.0/255.255.255.0 (192.168.5.0/24) the identifier 192.168.5.0 commonly is used to refer to the entire subnet. To avoid ambiguity in representation, the address ending in the octet 0 is reserved.
3. A ***Broadcast Address*** is an address that allows information to be sent to all interfaces in a given subnet, rather than a specific machine. Generally, the broadcast address is found by obtaining the bit complement of the subnet mask and performing a bitwise OR operation with the network identifier. In other words, the broadcast address is the last address in the address range of the subnet.
   For example, the broadcast address for the network 192.168.5.0 is 192.168.5.255. For networks of size /24 or larger, the broadcast address always ends in 255.
4. However, this does not mean that every address ending in 0 or 255 cannot be used as a host address. For example, in the /16 subnet 192.168.0.0/255.255.0.0, which is equivalent to the address range 192.168.0.0–192.168.255.255, the broadcast address is 192.168.255.255. One can use the following addresses for hosts, even though they end with 255: 192.168.1.255, 192.168.2.255, etc. Also, 192.168.0.0 is the network identifier and must not be assigned to an interface. The addresses 192.168.1.0, 192.168.2.0, etc., may be assigned, despite ending with 0.
5. In the past, conflict between network addresses and broadcast addresses arose because some software used non-standard broadcast addresses with zeros instead of ones.
6. In networks smaller than /24, broadcast addresses do not necessarily end with 255. For example, a CIDR subnet 203.0.113.16/28 has the broadcast address 203.0.113.31.

Address Resolution

1. Hosts on the Internet are usually known by names, e.g., www.example.com, not primarily by their IP address, which is used for routing and network interface identification. The use of domain names requires translating, called resolving, them to addresses and vice versa. This is analogous to looking up a phone number in a phone book using the recipient's name.
2. The translation between addresses and domain names is performed by the Domain Name System (DNS), a hierarchical, distributed naming system which allows for sub delegation of name spaces to other DNS servers.

IPv4 Subnetting

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

Classless Inter Domain Routing (CIDR) provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

Class A Subnets

1. In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

2. For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (2^1=2) with (2^{23}-2) 8388606 Hosts per Subnet.

3. The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

4. In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits providing (2^{14}) 16384 Networks and (2^{16}-2) 65534 Hosts. Class B IP Addresses can be subnetted the

same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

RESULTS:

Checking IPv4 Configuration

```
C:\Users\Satellite>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : TOSHIBA
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Npcap Loopback Adapter
   Physical Address. . . . . . . . . : 02-00-4C-4F-4F-50
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ad16:741d:e2ca:4dc1%25(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.77.193(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 771883084
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-3F-EB-C0-C4-54-44-4C-50-FC
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 1A-EE-65-36-A7-CC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
   Physical Address. . . . . . . . . : B8-EE-65-36-A7-CC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c0e0:ff86:90de:f04%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.31.171(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, October 11, 2017 5:31:24 PM
   Lease Expires . . . . . . . . . . : Thursday, October 12, 2017 5:31:23 AM
   Default Gateway . . . . . . . . . : 192.168.31.1
   DHCP Server . . . . . . . . . . . : 192.168.31.1
   DHCPv6 IAID . . . . . . . . . . . : 96005733
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-3F-EB-C0-C4-54-44-4C-50-FC
   DNS Servers . . . . . . . . . . . : 192.168.31.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : C4-54-44-4C-50-FC
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

```
Tunnel adapter isatap.{067BC1FD-AB1A-47F3-9CE9-9A3FB7499031}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter isatap.{C18EC9D3-612F-4CED-B923-C014305DE212}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #2
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

Checking IPv4 Subnetting

```
C:\Users\Satellite>route PRINT
===========================================================================
Interface List
 25...02 00 4c 4f 4f 50 ......Npcap Loopback Adapter
  5...1a ee 65 36 a7 cc ......Microsoft Wi-Fi Direct Virtual Adapter
  4...b8 ee 65 36 a7 cc ......Qualcomm Atheros AR956x Wireless Network Adapter
  3...c4 54 44 4c 50 fc ......Realtek PCIe GBE Family Controller
  1...........................Software Loopback Interface 1
 23...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 24...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.31.1   192.168.31.171     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      169.254.0.0      255.255.0.0         On-link    169.254.77.193    266
   169.254.77.193  255.255.255.255         On-link    169.254.77.193    266
  169.254.255.255  255.255.255.255         On-link    169.254.77.193    266
     192.168.31.0    255.255.255.0         On-link    192.168.31.171    281
   192.168.31.171  255.255.255.255         On-link    192.168.31.171    281
   192.168.31.255  255.255.255.255         On-link    192.168.31.171    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    169.254.77.193    266
        224.0.0.0        240.0.0.0         On-link    192.168.31.171    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    169.254.77.193    266
  255.255.255.255  255.255.255.255         On-link    192.168.31.171    281
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 25    266 fe80::/64                On-link
  4    281 fe80::/64                On-link
 25    266 fe80::ad16:741d:e2ca:4dc1/128
                                    On-link
  4    281 fe80::c0e0:ff86:90de:f04/128
                                    On-link
  1    306 ff00::/8                 On-link
 25    266 ff00::/8                 On-link
  4    281 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

CONCLUSION:

Thus, we've studied the concepts of *IPv4 Addressing* including subnetting for various classes.

PRACTICAL: 6

AIM: To study & simulate Ping/ARP packets using CISCO PacketTracer.

SOFTWARE: CISCO PacketTracer 7.0

THEORY:

Ping

1. **`ping`** is a network utility used to test the reachability of a host on an Internet Protocol (IP) network.
2. It measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source. The name comes from active sonar terminology that sends a pulse of sound and listens for the echo to detect objects under water, although it is sometimes interpreted as a backronym to packet Internet groper.
3. Ping operates by sending *Internet Control Message Protocol (ICMP/ICMP6) Echo Request* packets to the target host and waiting for an *ICMP Echo Reply*. The program reports errors, packet loss, and a statistical summary of the results, typically including the minimum, maximum, the mean round-trip times, and standard deviation of the mean.
4. The command-line options of the ping utility and its output vary between the numerous implementations. Options may include the size of the payload, count of tests, limits for the *number of network hops (TTL)* that probes traverse, and interval between the requests. Many systems provide a companion utility ping6, for testing on *Internet Protocol version 6 (IPv6*) networks.

ARP

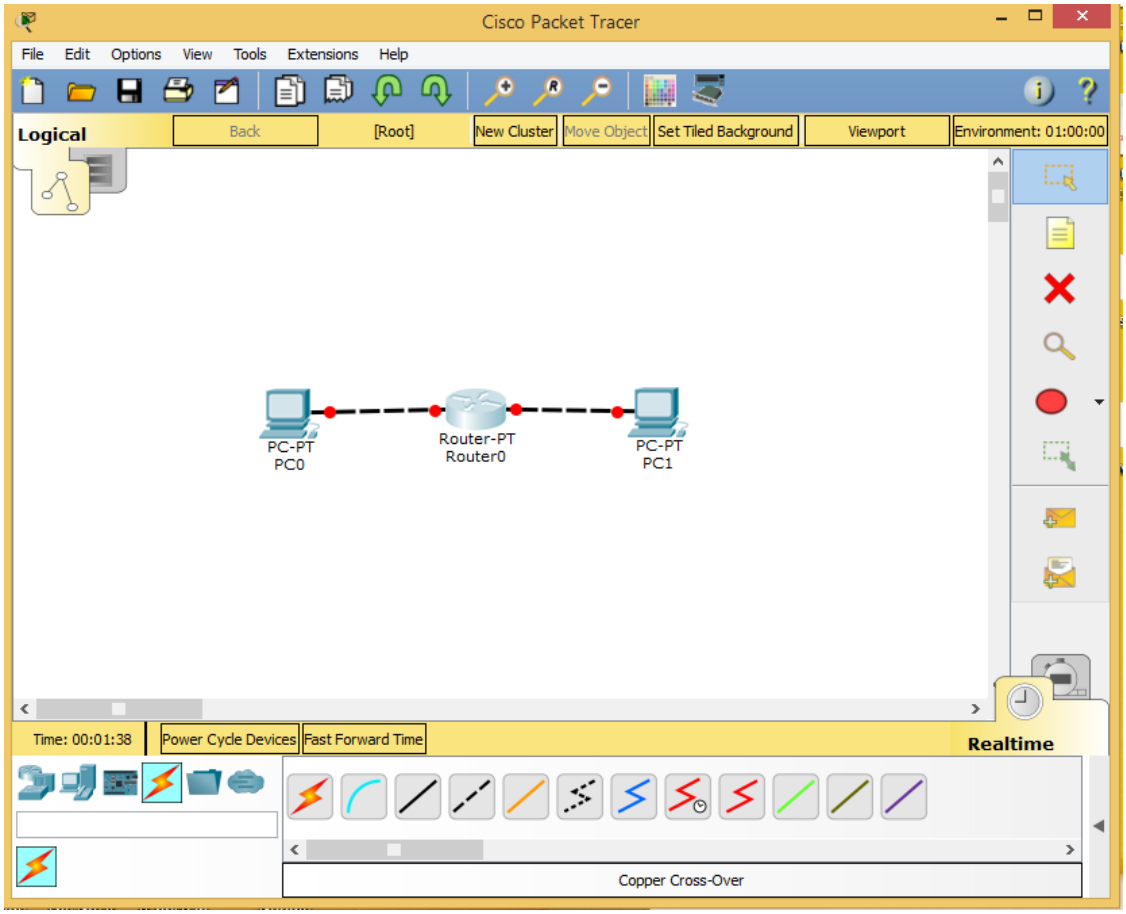
1. The *Address Resolution Protocol (ARP)* is a communications protocol used for discovering the *link layer address* associated with a given *Internet layer address*, a critical function in the Internet protocol suite. ARP was defined by RFC 826 in 1982, and is Internet Standard STD 37.
2. ARP is used for mapping a network address (e.g. an IPv4 address) to a physical address like an MAC address. ARP has been implemented with many combinations of network and data link layer technologies, like IPv4, Chaosnet, DECnet and Xerox PARC Universal Packet (PUP) using IEEE 802 standards, FDDI, X.25, Frame Relay and Asynchronous Transfer Mode (ATM). IPv4 over IEEE 802.3 and IEEE 802.11 is the most common usage.
3. In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery Protocol (NDP).

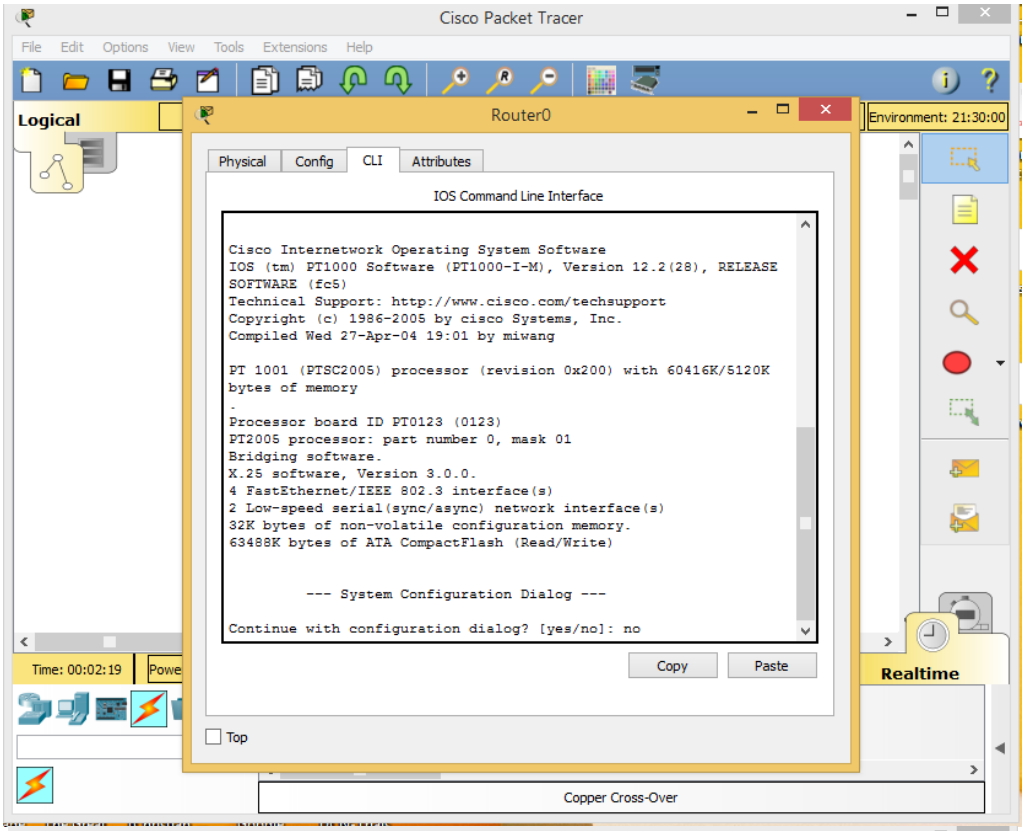
PROCEDURE:

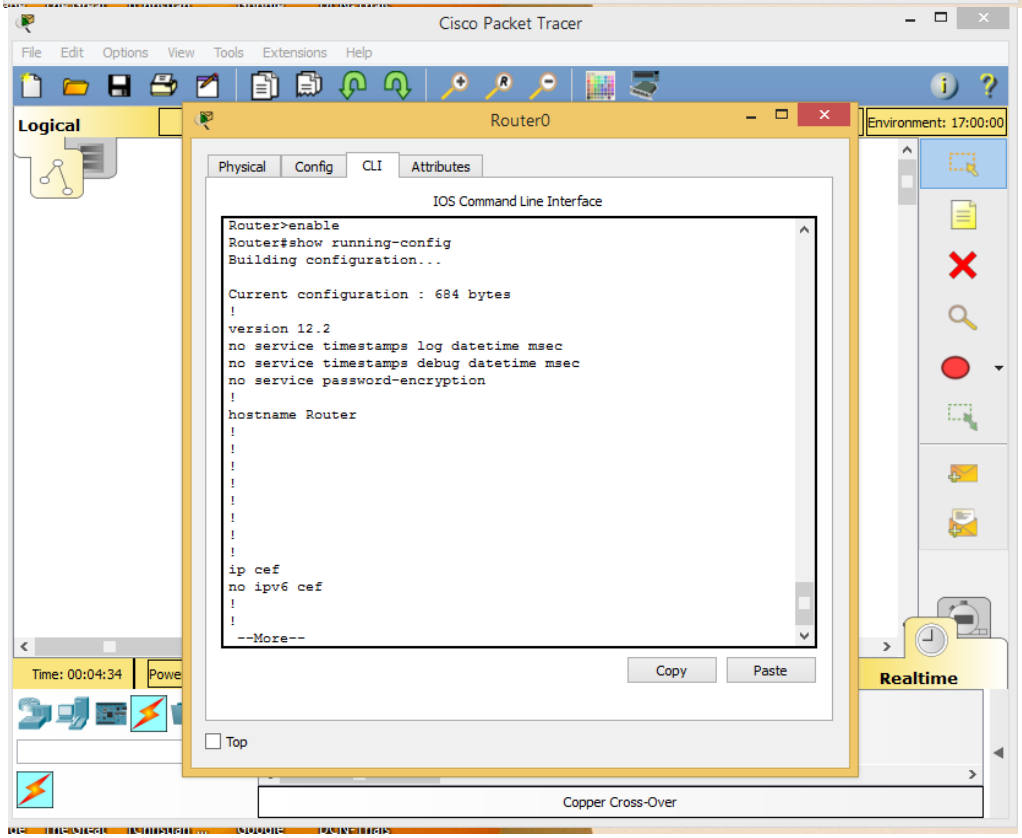
[1] Place the various physical blocks (one router & two PCs) using the Logical View of PT.
[2] Make necessary connections using Copper-Crossover wires.
[3] Configure CLI options of the router.
[4] Configure IPv4 Addressing scheme for the two PCs.
[5] Ping PC1 from PC0, using CLI of PC0.
[6] To visualize the pinging process of [5], use *PDU* in *Simulation Mode*, check only *ICMP* packets, and click *AutoCapture/Ping* to begin the simulation.

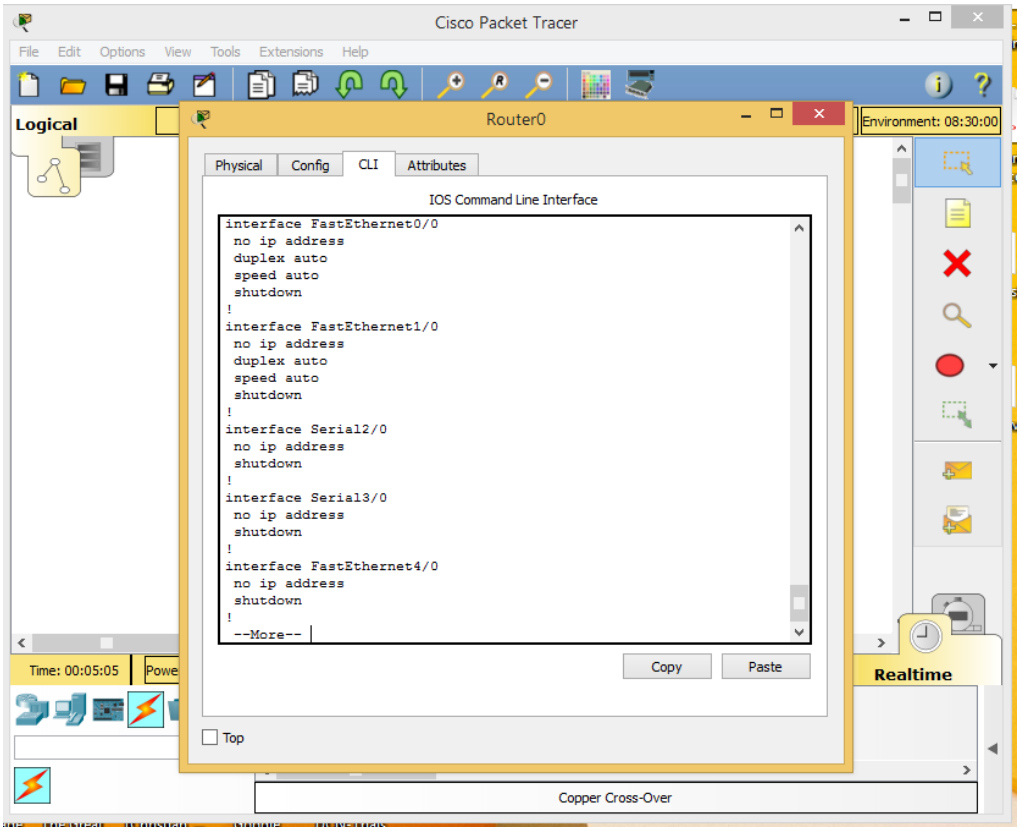
IMPLEMENTATION:

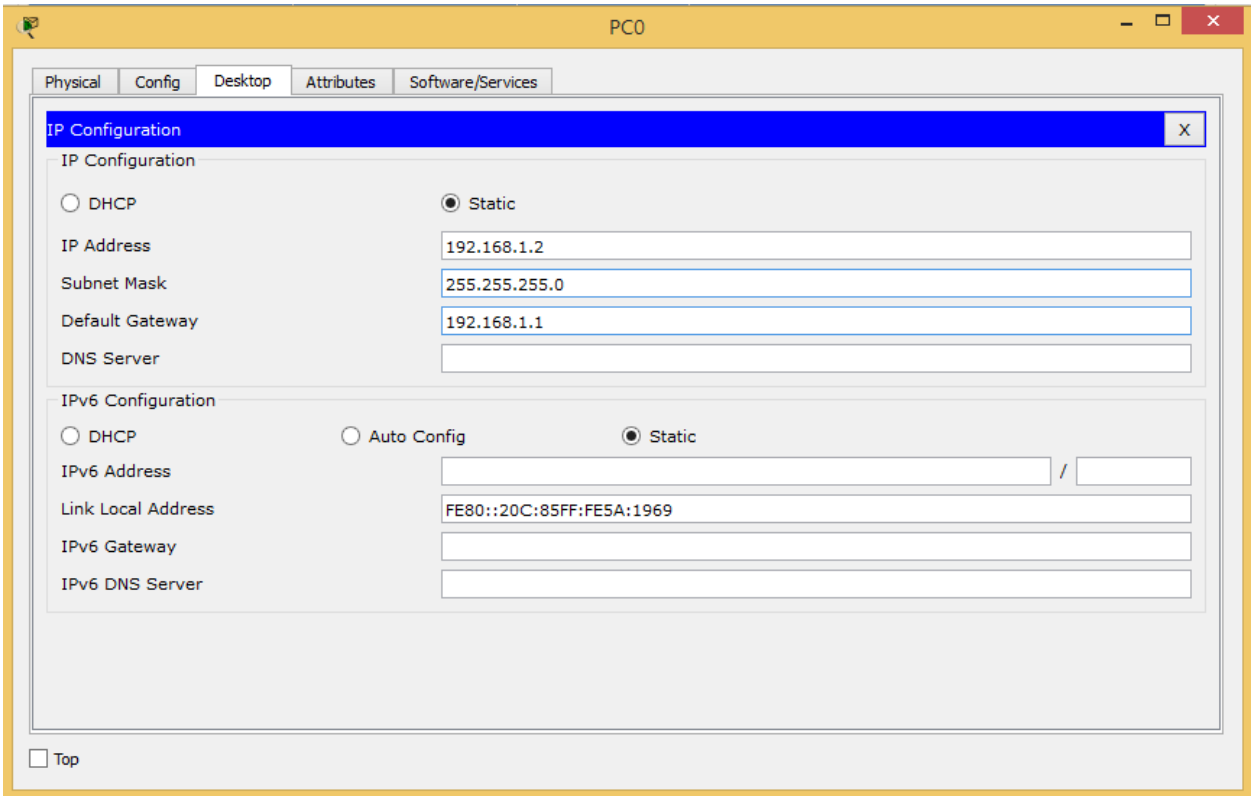
(In the corresponding order as listed in '**PROCEDURE**')

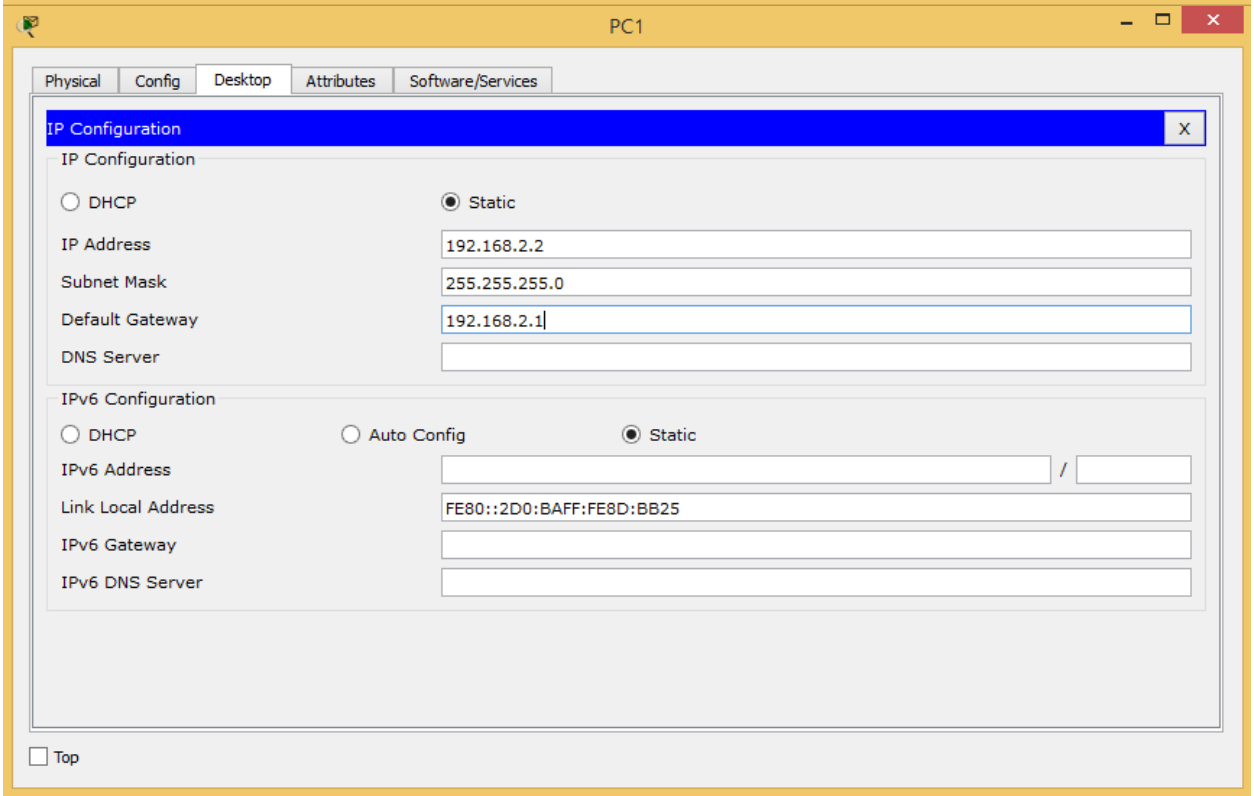


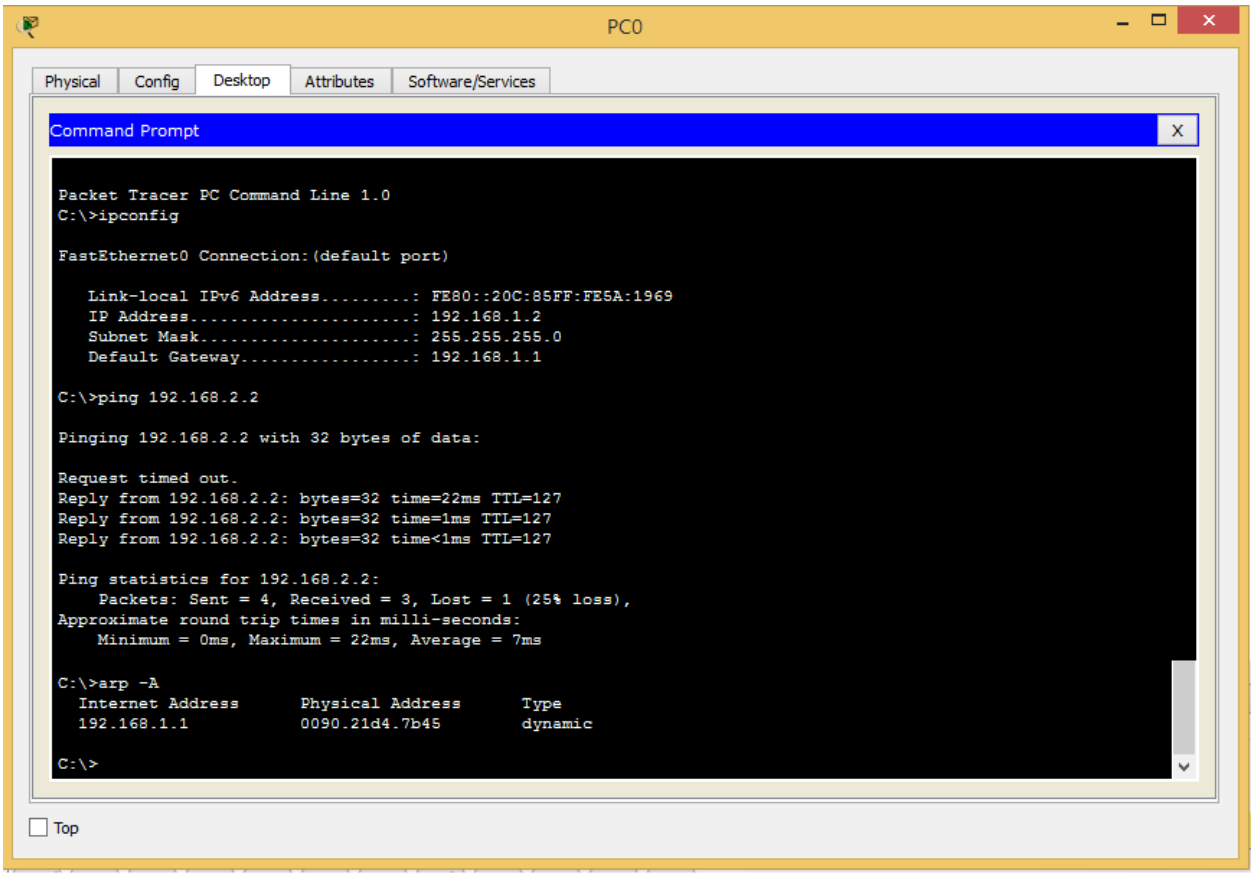

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no
Copy
Paste
Top
Environment: 21:30:00
Time: 00:02:19
Realtime
Copper Cross-Over

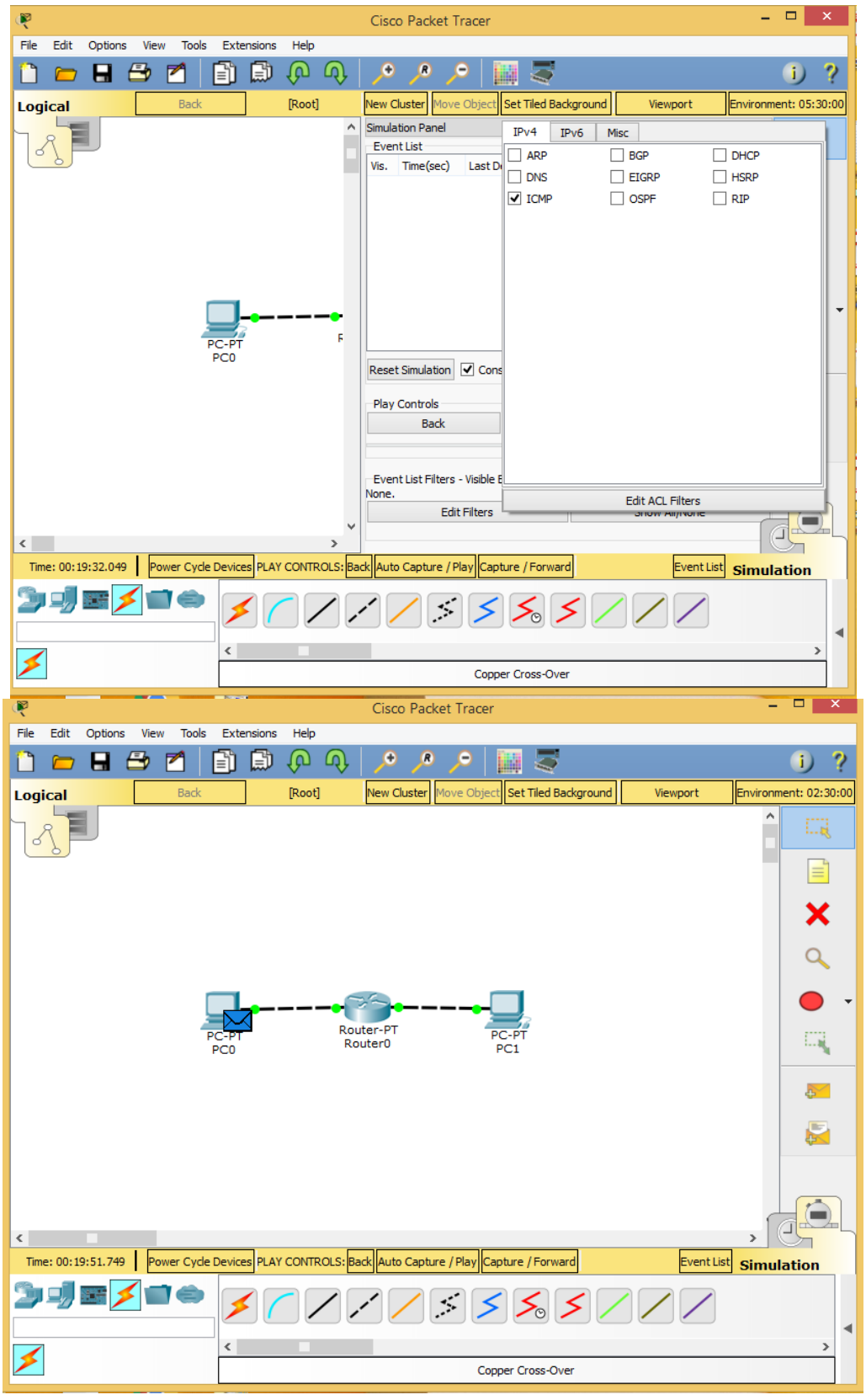

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
Router#show running-config
Building configuration...
Current configuration : 684 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
--More--
Copy
Paste
Top
Environment: 17:00:00
Time: 00:04:34
Realtime
Copper Cross-Over

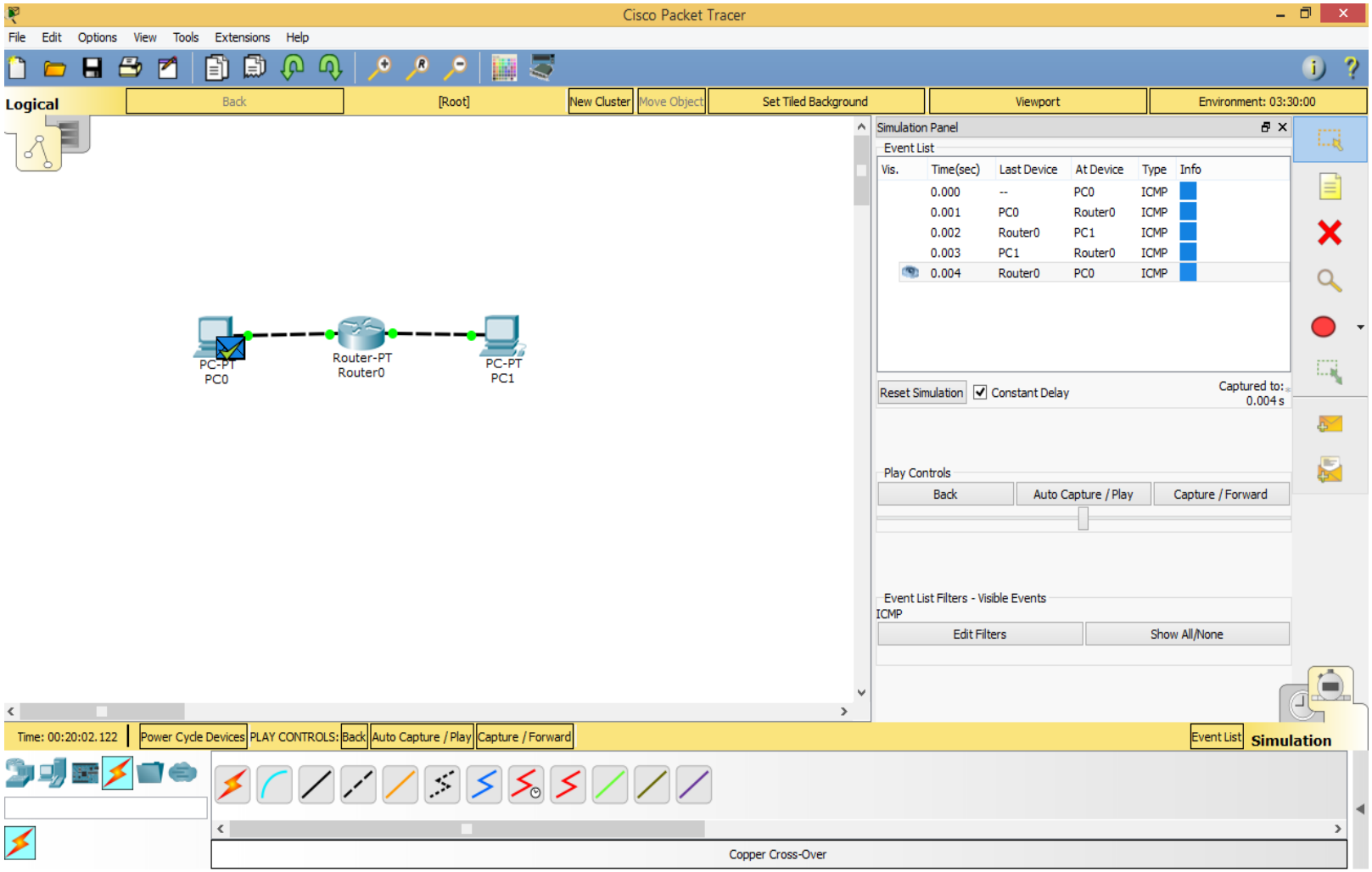

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Router0
Physical Config CLI Attributes
IOS Command Line Interface
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial2/0
no ip address
shutdown
!
interface Serial3/0
no ip address
shutdown
!
interface FastEthernet4/0
no ip address
shutdown
!
--More--
Copy
Paste
Top
Environment: 08:30:00
Time: 00:05:05
Realtime
Copper Cross-Over


PC0
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::20C:85FF:FE5A:1969
IPv6 Gateway
IPv6 DNS Server
Top


PC1
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FE8D:BB25
IPv6 Gateway
IPv6 DNS Server
Top


PC0
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::20C:85FF:FE5A:1969
IP Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.2: bytes=32 time=22ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 22ms, Average = 7ms
C:\>arp -A
Internet Address
Physical Address
Type
192.168.1.1
0090.21d4.7b45
dynamic
C:\>
Top


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Environment: 05:30:00
Simulation Panel
Event List
Vis.
Time(sec)
IPv4
IPv6
Misc
ARP
BGP
DHCP
DNS
EIGRP
HSRP
ICMP
OSPF
RIP
PC-PT
PC0
Reset Simulation
Play Controls
Back
Edit ACL Filters
Edit Filters
None.
Time: 00:19:32.049
Power Cycle Devices
PLAY CONTROLS:
Back
Auto Capture / Play
Capture / Forward
Event List
Simulation
Copper Cross-Over
Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Environment: 02:30:00
PC-PT
PC0
Router-PT
Router0
PC-PT
PC1
Time: 00:19:51.749
Power Cycle Devices
PLAY CONTROLS:
Back
Auto Capture / Play
Capture / Forward
Event List
Simulation
Copper Cross-Over


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Environment: 03:30:00
PC-PT
PC0
Router-PT
Router0
PC-PT
PC1
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Router0 ICMP
0.002 Router0 PC1 ICMP
0.003 PC1 Router0 ICMP
0.004 Router0 PC0 ICMP
Reset Simulation
Constant Delay
Captured to:
0.004 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ICMP
Edit Filters
Show All/None
Time: 00:20:02.122
Power Cycle Devices
PLAY CONTROLS:
Back
Auto Capture / Play
Capture / Forward
Event List
Simulation
Copper Cross-Over

CLI-INPUT:

(Entered for configuring the router with the two PCs)

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#description Router0 FastEthernet0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#description Router0 FastEthernet1/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0,
changed state to up

Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show running-config
Building configuration...

Current configuration : 784 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
```

```
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
description Router0 FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
description Router0 FastEthernet1/0
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
interface Serial2/0
no ip address
shutdown
!
interface Serial3/0
no ip address
shutdown
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
```

```
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end


Router#
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

CONCLUSION:

Thus, we made use of *CLI* & *PDU* utilities in *PacketTracer* to implement a *two node network*, and simulated a real-time ping and also visualized it.

PRACTICAL: 7

AIM: To study & simulate VLAN using CISCO PacketTracer.

SOFTWARE: CISCO PacketTracer 7.0

THEORY:

VLAN

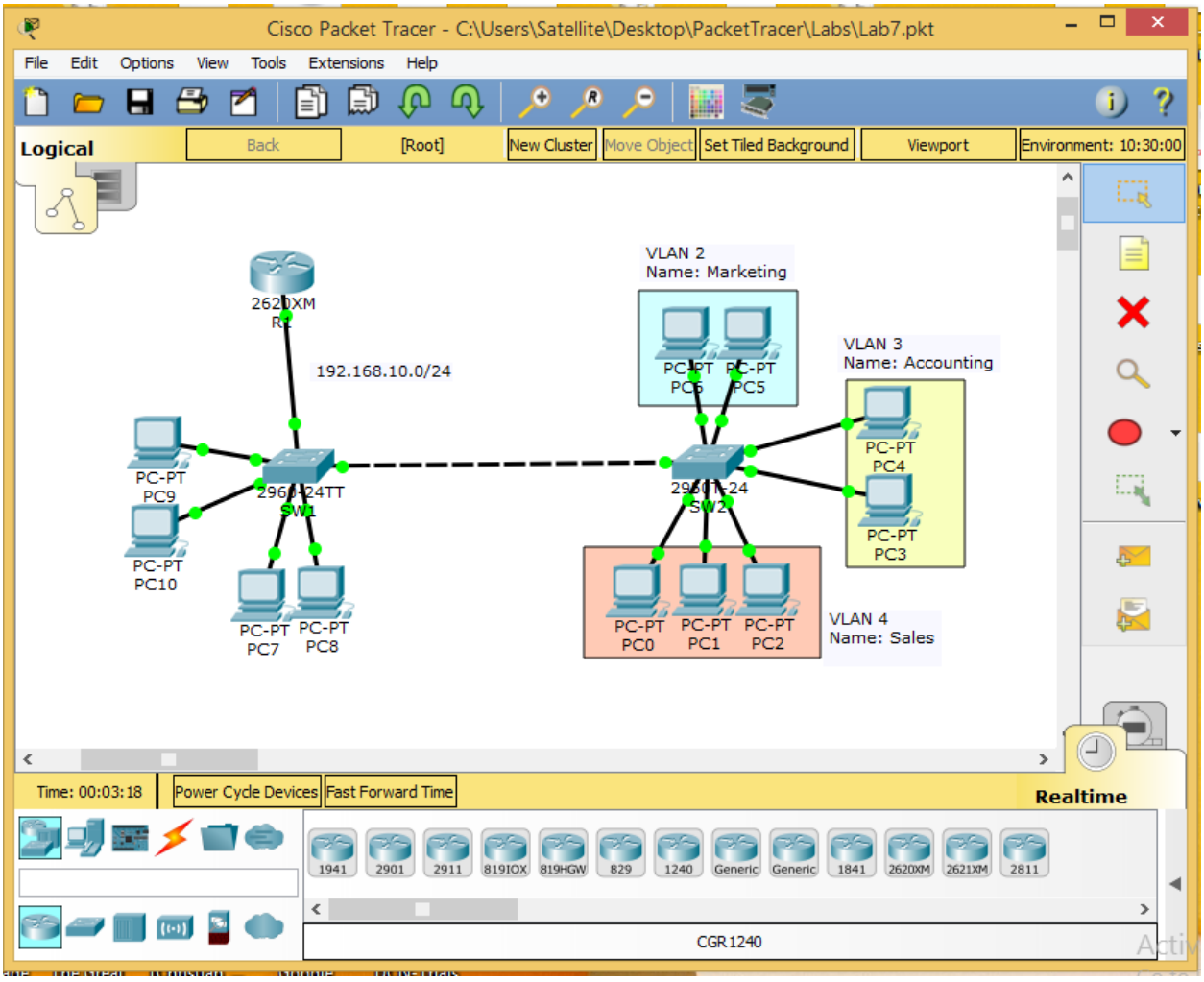
1. A *Virtual LAN (VLAN)* is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).
2. VLANs work by applying tags to network packets and handling these tags in networking systems - creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.
3. VLANs allow network administrators to group hosts together even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource needs necessitates the labor of relocating nodes or rewiring data links.
4. It also has benefits in allowing networks and devices that must be kept separate to share the same physical cabling without interacting, for reasons of simplicity, security, traffic management, or economy.
   For example, a VLAN could be used to separate traffic within a business due to users, and due to network administrators, or between types of traffic, so that users or low priority traffic cannot directly affect the rest of the network's functioning. Many Internet hosting services use VLANs to separate their customers' private zones from each other, allowing each customer's servers to be grouped together in a single network segment while being located anywhere in their datacenter. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.
5. To subdivide a network into virtual LANs, one configures network equipment. Simpler equipment can partition only per physical port (if at all), in which case each VLAN is connected with a dedicated network cable. More sophisticated devices can mark frames through VLAN tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk can use link aggregation, quality-of-service prioritization, or both to route data efficiently.

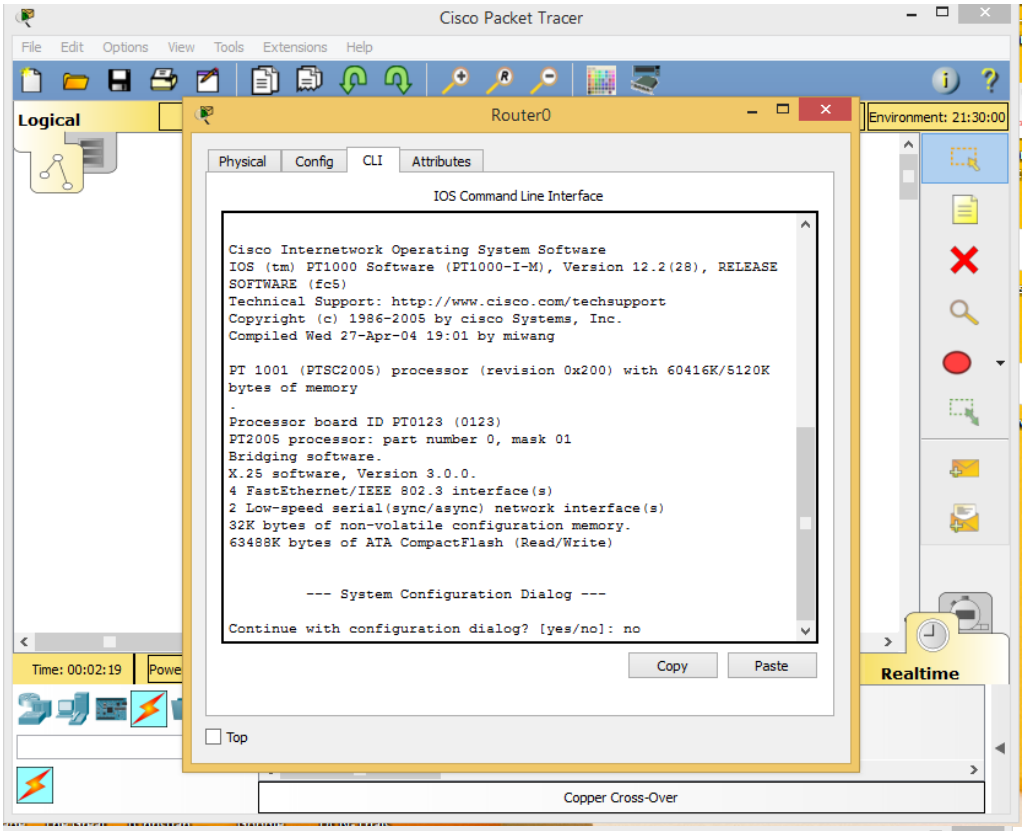
PROCEDURE:

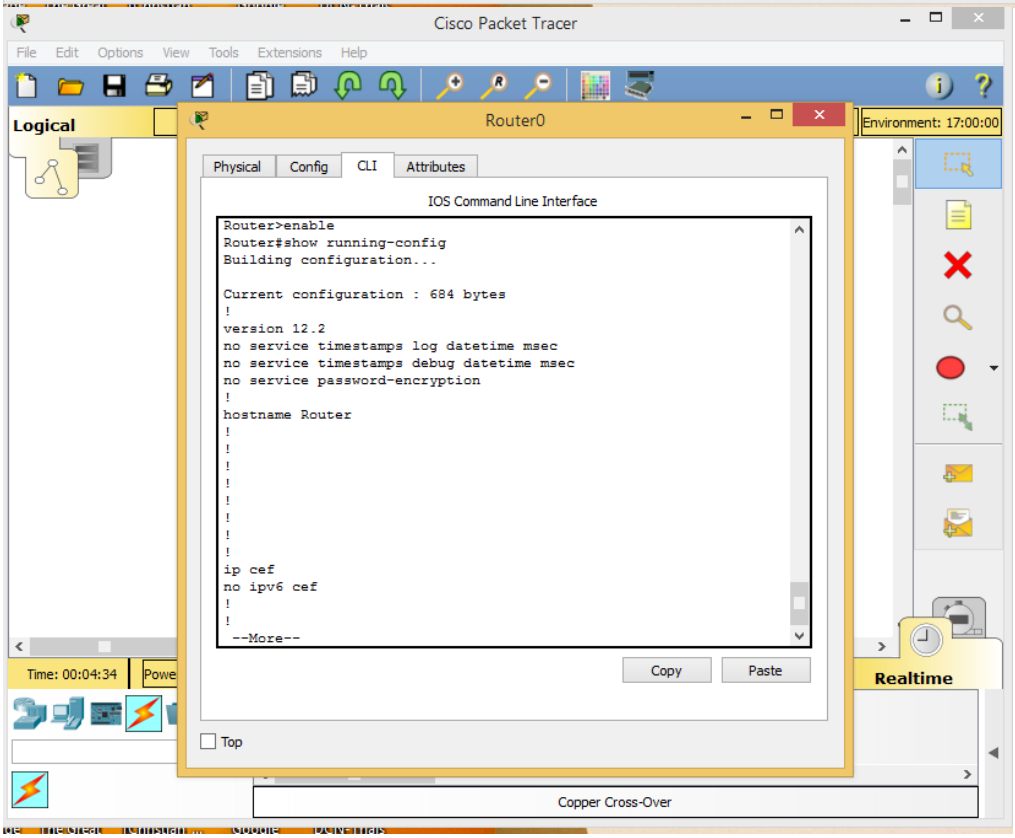
[1] Place the various physical blocks (one router & two switches) using the Logical View of PT.
[2] Make necessary connections using Copper-Crossover & Straight-Through wires.
[3] Configure CLI options of the router.
[4] Configure IPv4 Addressing scheme for the two PCs.
[5] Create 3 VLANs at Switch SW2 – Marketing, Accounting, Sales.
[6] Add interfaces to the newly created VLANs using CLI.

IMPLEMENTATION:

(In the corresponding order as listed in '**PROCEDURE**')




Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no
Copy
Paste
Top
Environment: 21:30:00
Time: 00:02:19
Realtime
Copper Cross-Over


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
Router#show running-config
Building configuration...
Current configuration : 684 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
--More--
Copy
Paste
Top
Environment: 17:00:00
Time: 00:04:34
Realtime
Copper Cross-Over

CLI-INPUT:

(Entered for configuring the router with the two PCs)

Configure VLAN-2,3,4

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW2
SW2(config)#vlan 2
SW2(config-vlan)#name Marketing
SW2(config-vlan)#vlan 3
SW2(config-vlan)#name Accounting
SW2(config-vlan)#vlan 4
SW2(config-vlan)#name Sales
SW2(config-vlan)#do sh vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------
---------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
2 Marketing active
3 Accounting active
4 Sales active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- -----
- ------
1 enet 100001 1500 - - - - - 0 0
2 enet 100002 1500 - - - - - 0 0
3 enet 100003 1500 - - - - - 0 0
4 enet 100004 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs
------------------------------------------------------------------------
--------
```

```
Primary Secondary Type Ports
------- --------- ----------------- ---------------------------------
--------
SW2(config-vlan)#
```

Add Interfaces to VLAN-2,3,4

```
SW2(config)#interface range FastEthernet 0/5-6
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 2
SW2(config-if-range)#exit

SW2(config)#interface range FastEthernet 0/7-8
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 3
SW2(config-if-range)#exit

SW2(config)#interface range FastEthernet 0/2-4
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 4
SW2(config-if-range)#exit
```

Check for Interfaces on VLAN-2,3,4

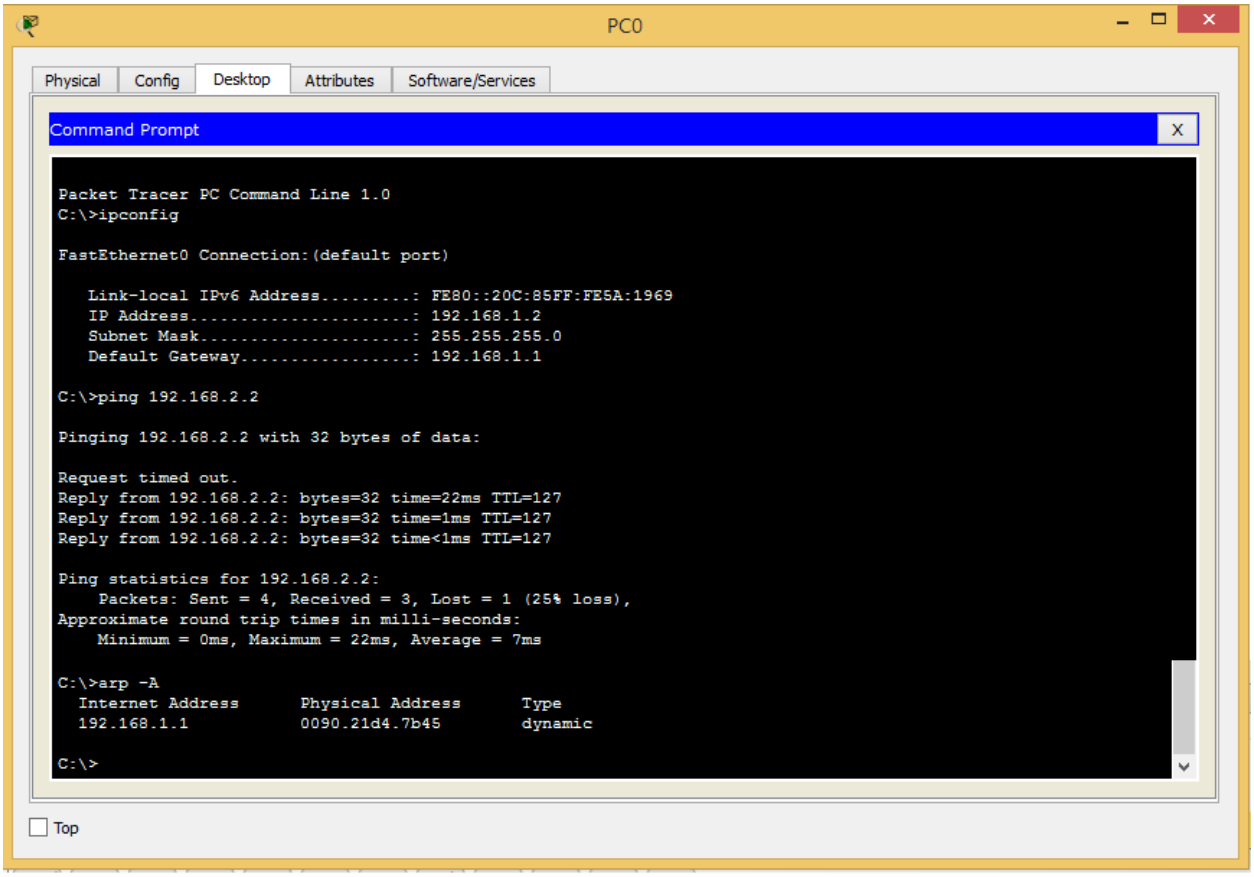
```
SW2(config)#do sh vlan

VLAN Name Status Ports
---- -------------------------------- --------- ----------------------
1 default active Fa0/1, Fa0/9, Fa0/10, Fa0/11
Fa0/12, Fa0/13, Fa0/14, Fa0/15
Fa0/16, Fa0/17, Fa0/18, Fa0/19
Fa0/20, Fa0/21, Fa0/22, Fa0/23
Fa0/24, Gig0/1, Gig0/2
2 Marketing active Fa0/5, Fa0/6
3 Accounting active Fa0/7, Fa0/8
4 Sales active Fa0/2, Fa0/3, Fa0/4
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- -----
1 enet 100001 1500 - - - - - 0 0
2 enet 100002 1500 - - - - - 0 0
3 enet 100003 1500 - - - - - 0 0
4 enet 100004 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
```

```
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs
Primary Secondary Type Ports
```



CONCLUSION:

Thus, we made use of *CLI* & *PDU* utilities in *PacketTracer* to implement a *VLAN network*, and simulated a real-time ping and also visualized it.

PRACTICAL: 8

AIM: To study & simulate static routing using CISCO PacketTracer.

SOFTWARE: CISCO PacketTracer 7.0

THEORY:

Static Routing

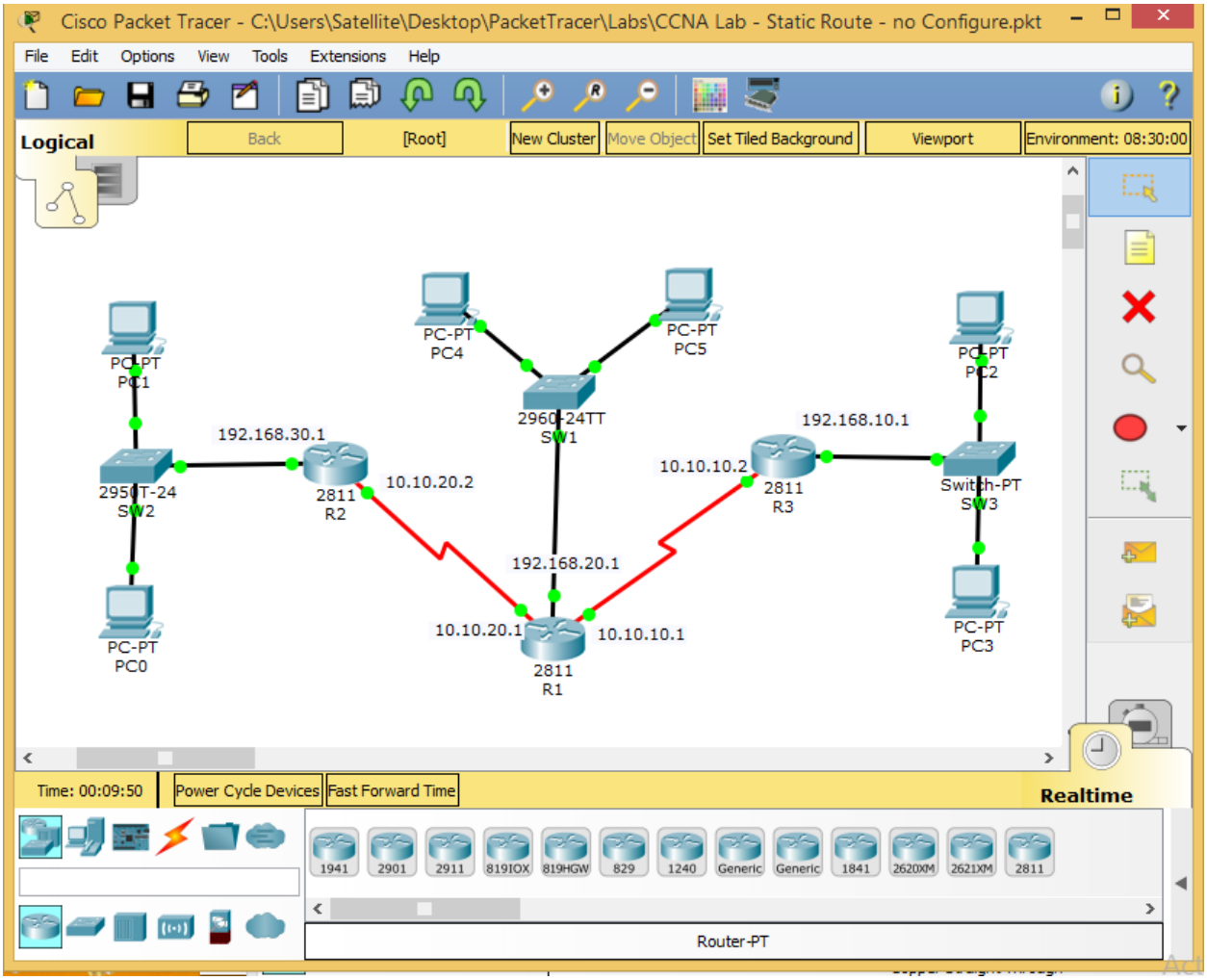
1. Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic.
2. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case.
3. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing can also be used in stub networks, or to provide a gateway of last resort.
4. **Uses:**
    - It can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.
    - It can be used for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
    - It is often used as a complement to dynamic routing to provide a failsafe backup in the event that a dynamic route is unavailable.
    - It is often used to help transfer routing information from one routing protocol to another (routing redistribution).

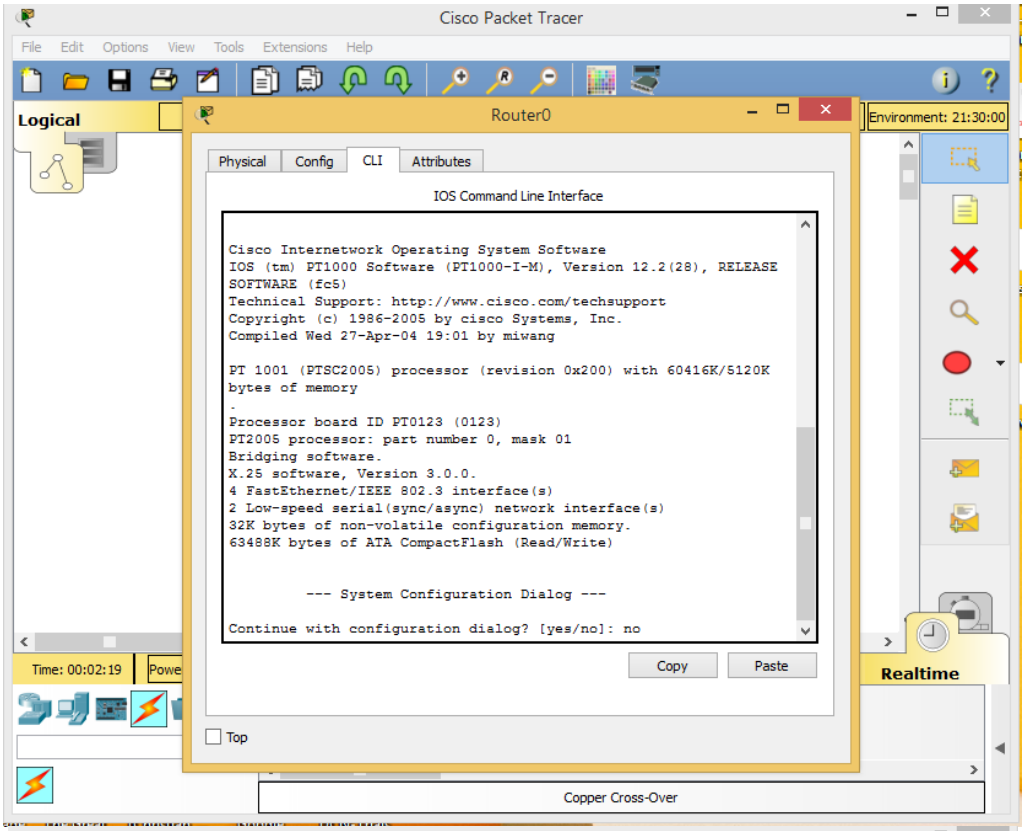
PROCEDURE:

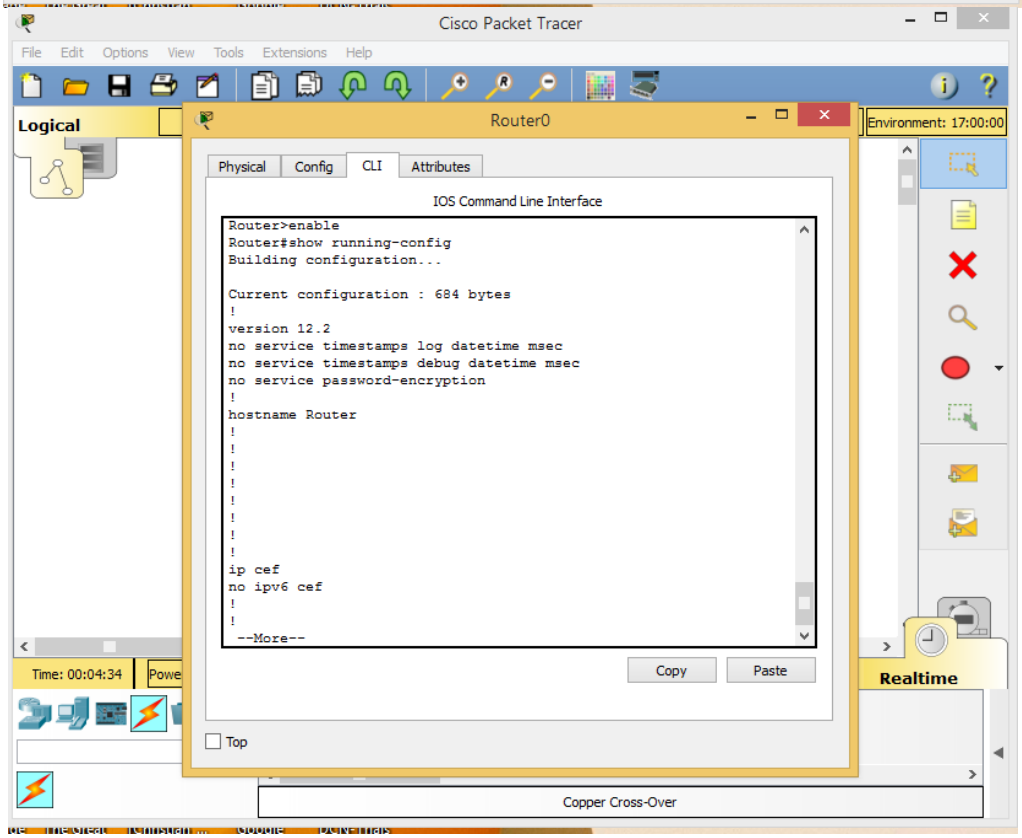
[1] Place the various physical blocks (3 routers, 3 switches & 3 PCs) using the Logical View of PT.
[2] Make necessary connections using Copper Straight-Through wires (Serial DTE wires for router-router connections).
[3] Configure CLI options of the routers.
[4] Configure IPv4 Addressing scheme for the two PCs.
[5] Ping PC1 from PC0, using CLI of PC0.
[6] To visualize the pinging process of [5], use *PDU* in *Simulation Mode*, check only *ICMP* packets, and click *AutoCapture/Ping* to begin the simulation.

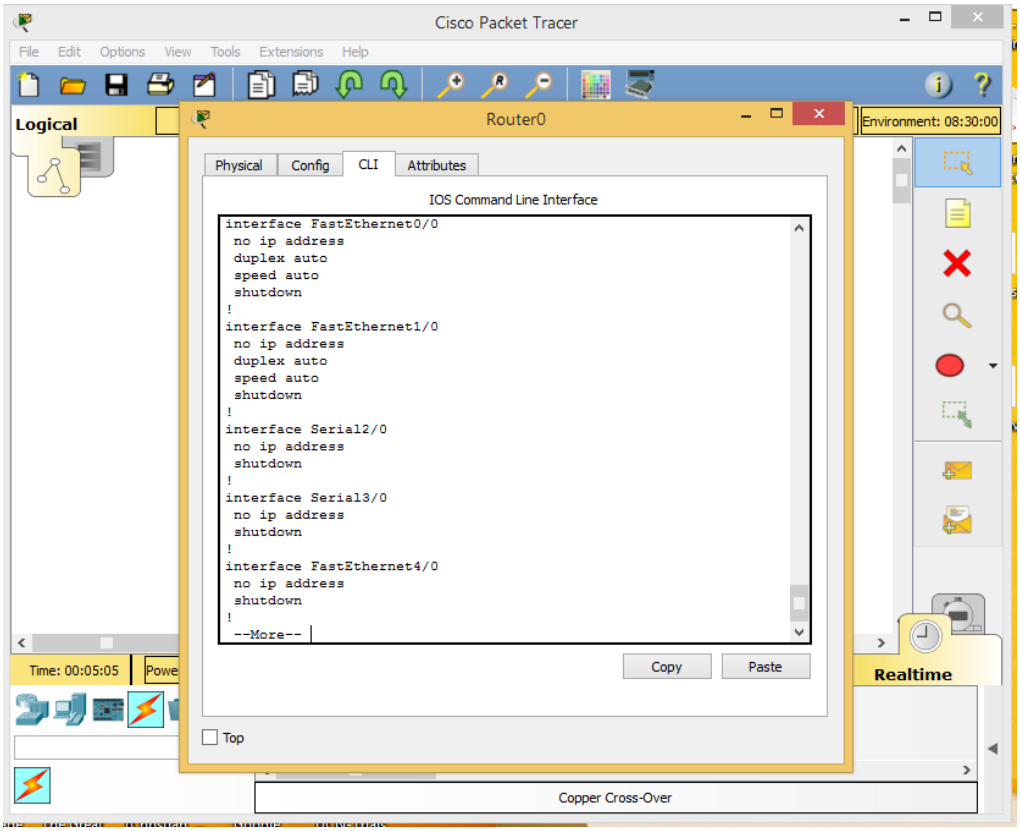
IMPLEMENTATION:

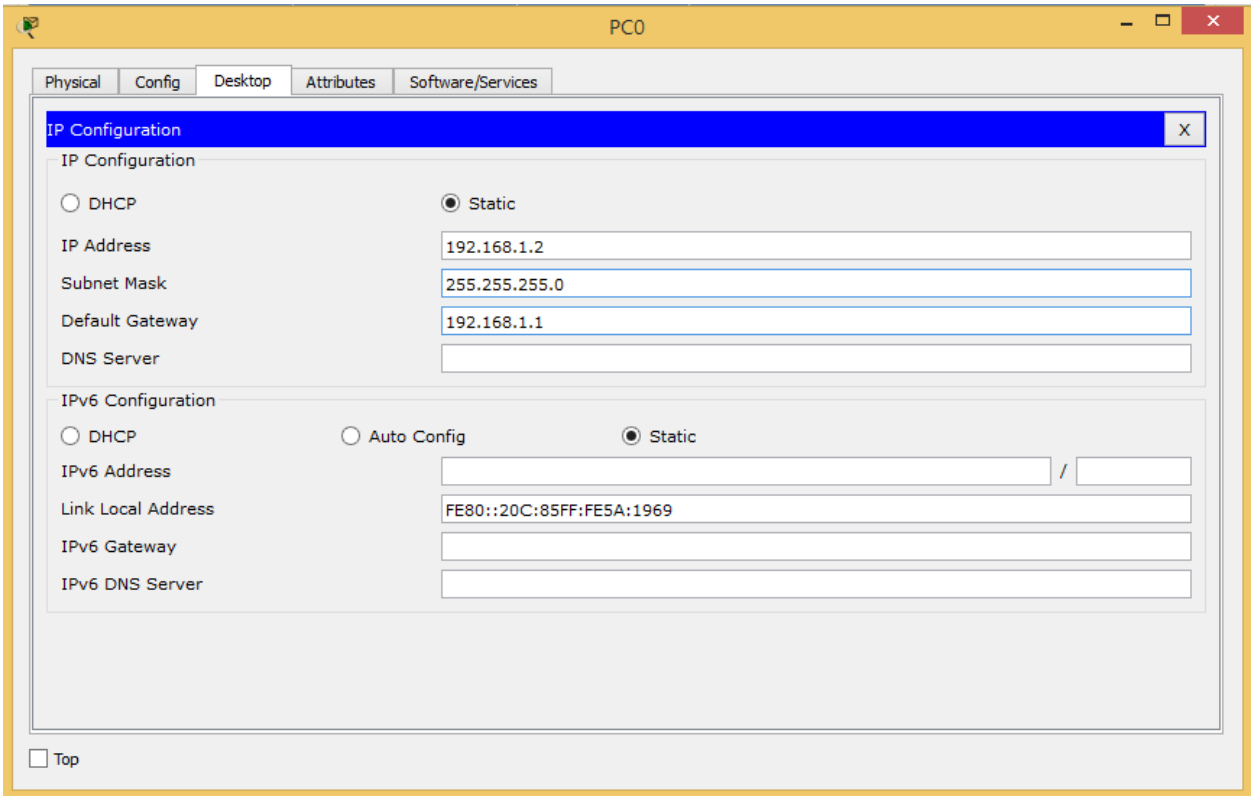
(In the corresponding order as listed in '**PROCEDURE**')

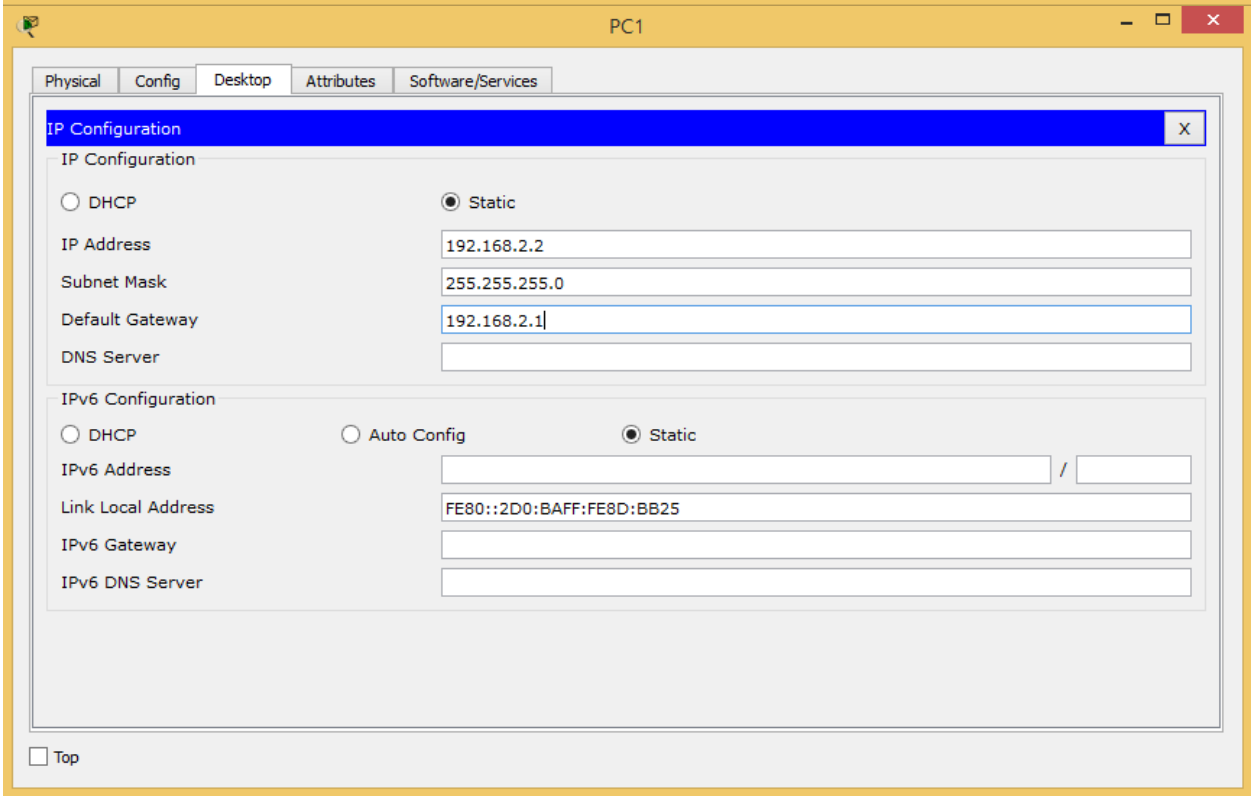


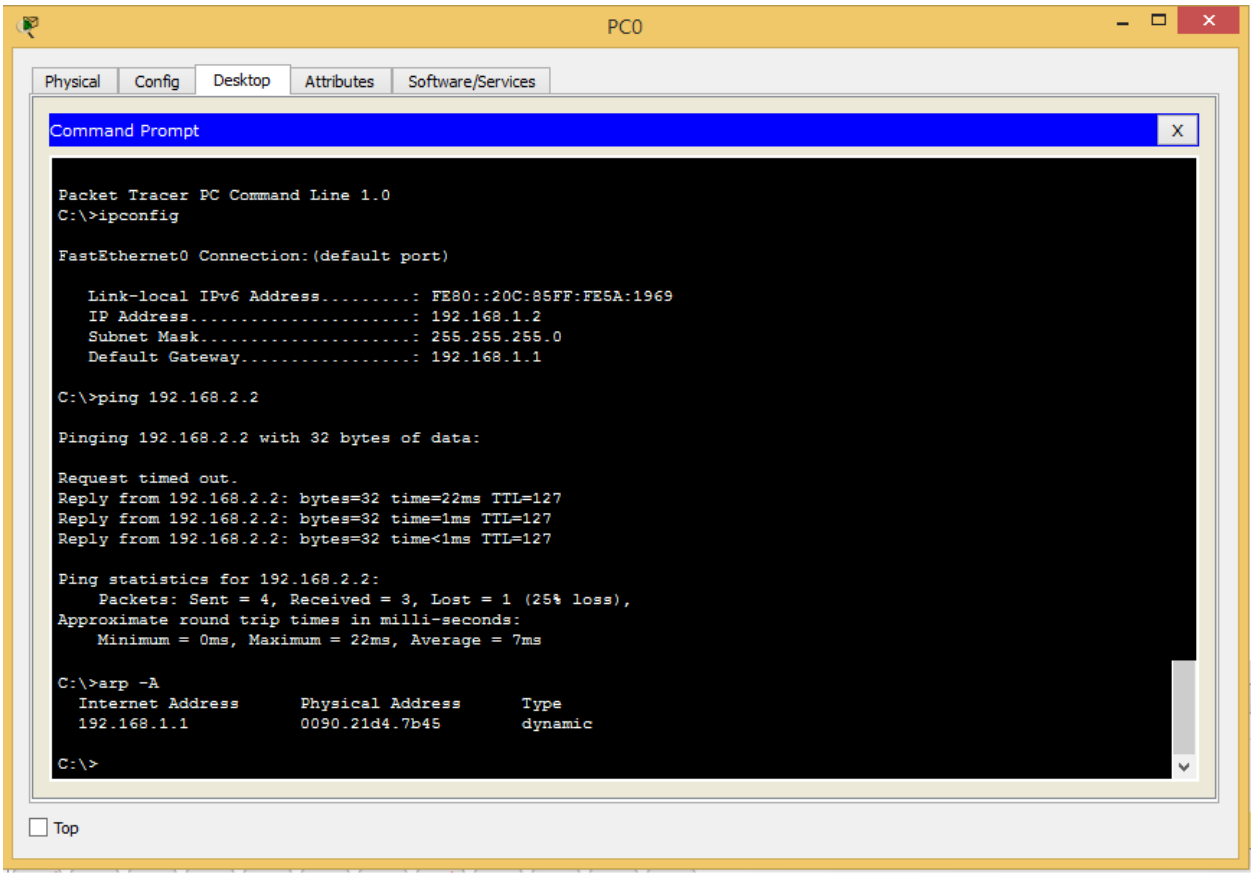

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no
Copy
Paste
Top
Environment: 21:30:00
Time: 00:02:19
Realtime
Copper Cross-Over

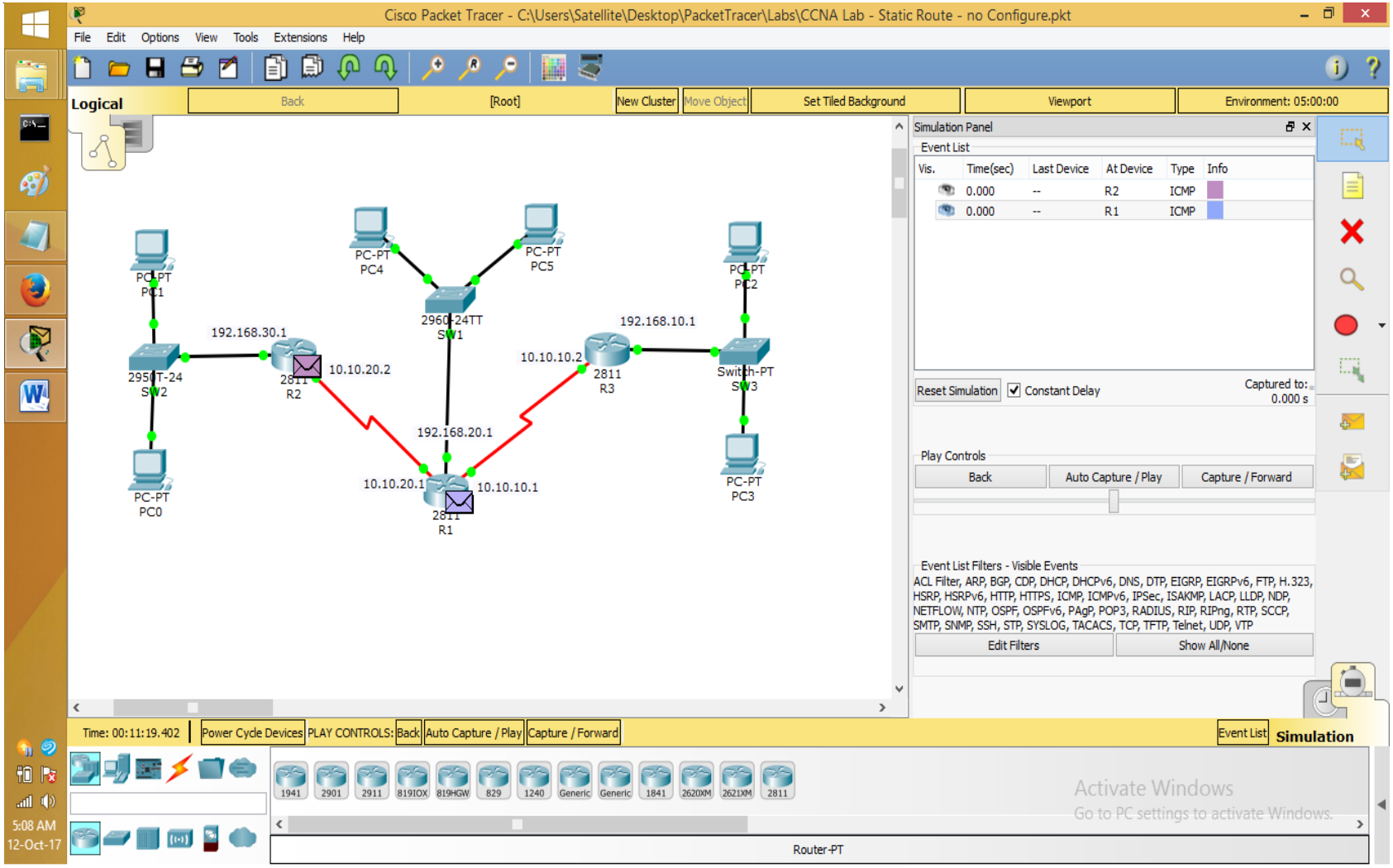

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
Router#show running-config
Building configuration...
Current configuration : 684 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
--More--
Copy
Paste
Top
Environment: 17:00:00
Time: 00:04:34
Realtime
Copper Cross-Over

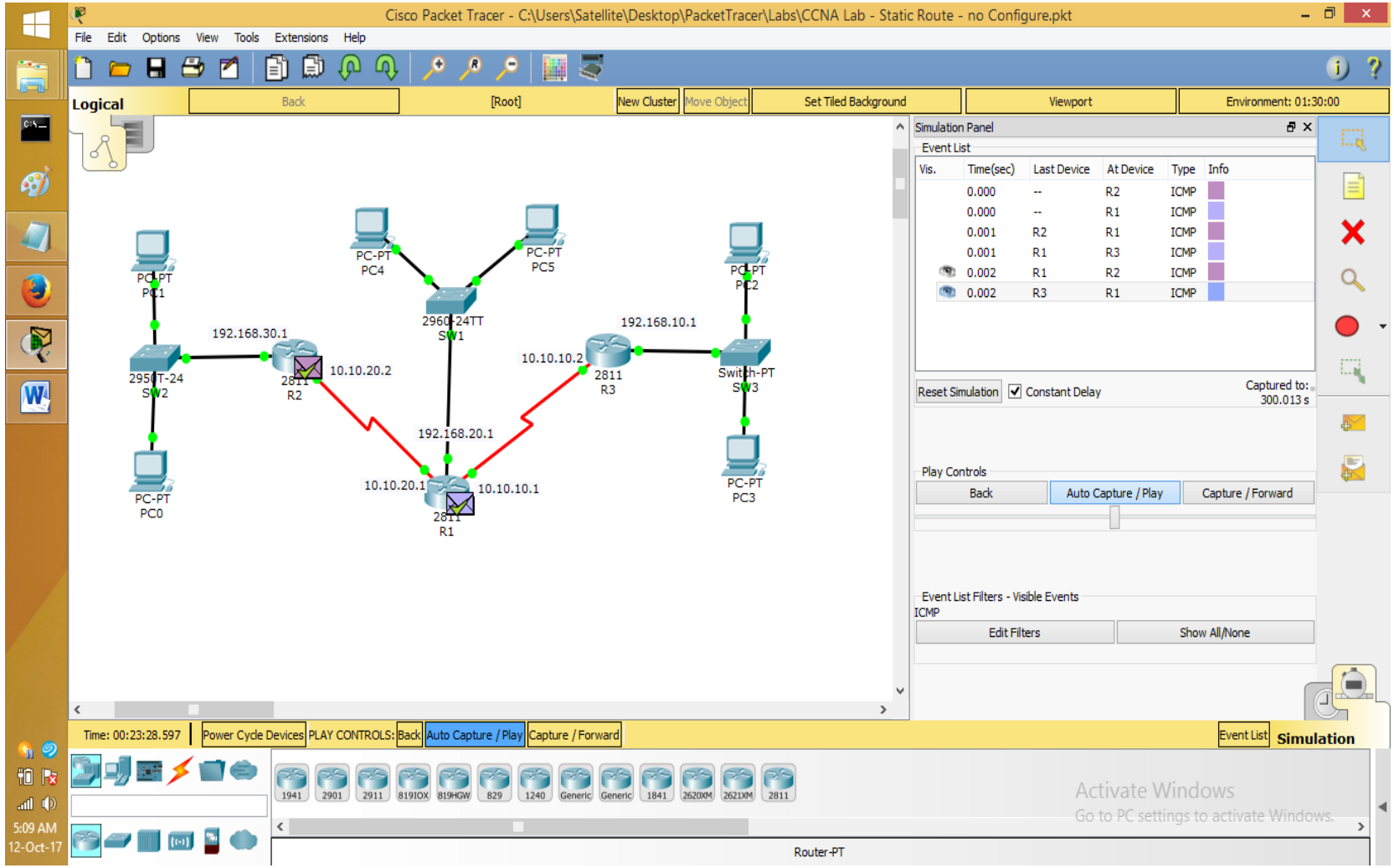

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
Router0
Physical Config CLI Attributes
IOS Command Line Interface
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial2/0
no ip address
shutdown
!
interface Serial3/0
no ip address
shutdown
!
interface FastEthernet4/0
no ip address
shutdown
!
--More--
Copy
Paste
Top
Environment: 08:30:00
Realtime
Time: 00:05:05
Copper Cross-Over


PC0
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20C:85FF:FE5A:1969
IPv6 Gateway
IPv6 DNS Server
Top


PC1
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2D0:BAFF:FE8D:BB25
IPv6 Gateway
IPv6 DNS Server
Top


PC0
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::20C:85FF:FE5A:1969
IP Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.2: bytes=32 time=22ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 22ms, Average = 7ms
C:\>arp -A
Internet Address
Physical Address
Type
192.168.1.1
0090.21d4.7b45
dynamic
C:\>
Top


Cisco Packet Tracer - C:\Users\Satellite\Desktop\PacketTracer\Labs\CCNA Lab - Static Route - no Configure.pkt
File Edit Options View Tools Extensions Help
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Environment: 05:00:00
PC-PT PC1
PC-PT PC4
PC-PT PC5
PC-PT PC2
2960-24TT SW1
192.168.30.1
192.168.10.1
2950T-24 SW2
2811 R2
10.10.20.2
10.10.10.2
2811 R3
Switch-PT SW3
192.168.20.1
10.10.20.1
10.10.10.1
PC-PT PC0
2811 R1
PC-PT PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- R2 ICMP
0.000 -- R1 ICMP
Reset Simulation
Constant Delay
Captured to: 0.000 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:11:19.402
Power Cycle Devices
PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation
1941 2901 2911 819IOX 819HGW 829 1240 Generic Generic 1841 2620XM 2621XM 2811
Router-PT
Activate Windows
Go to PC settings to activate Windows.
5:08 AM
12-Oct-17


Cisco Packet Tracer - C:\Users\Satellite\Desktop\PacketTracer\Labs\CCNA Lab - Static Route - no Configure.pkt
File Edit Options View Tools Extensions Help
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Environment: 01:30:00
PC-PT PC1
PC-PT PC4
PC-PT PC5
PC-PT PC2
2960-24TT SW1
192.168.30.1
192.168.10.1
2950T-24 SW2
2811 R2
10.10.20.2
10.10.10.2
2811 R3
Switch-PT SW3
192.168.20.1
PC-PT PC0
10.10.20.1
10.10.10.1
2811 R1
PC-PT PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- R2 ICMP
0.000 -- R1 ICMP
0.001 R2 R1 ICMP
0.001 R1 R3 ICMP
0.002 R1 R2 ICMP
0.002 R3 R1 ICMP
Reset Simulation
Constant Delay
Captured to: 300.013 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ICMP
Edit Filters
Show All/None
Time: 00:23:28.597
Power Cycle Devices
PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation
1941 2901 2911 819IOX 819HGW 829 1240 Generic Generic 1841 2620XM 2621XM 2811
Router-PT
Activate Windows
Go to PC settings to activate Windows.
5:09 AM
12-Oct-17

CLI-INPUT:

(Entered for configuring the routers with the two PCs)

Router R1

```
R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 192.168.30.0 255.255.255.0 10.10.20.2 150
R1(config)#ip route 192.168.10.0 255.255.255.0 10.10.10.2 150
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
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

10.0.0.0/24 is subnetted, 2 subnets
C 10.10.10.0 is directly connected, Serial0/0/1
C 10.10.20.0 is directly connected, Serial0/0/0
S 192.168.10.0/24 [150/0] via 10.10.10.2
C 192.168.20.0/24 is directly connected, FastEthernet0/1
S 192.168.30.0/24 [150/0] via 10.10.20.2
```

Router R2

```
R2>enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 192.168.10.0 255.255.255.0 10.10.10.1 150
R2(config)#ip route 10.10.10.0 255.255.255.0 10.10.20.1 150
R2(config)#ip route 192.168.20.0 255.255.255.0 10.10.20.1 150
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
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

10.0.0.0/24 is subnetted, 2 subnets
S 10.10.10.0 [150/0] via 10.10.20.1
C 10.10.20.0 is directly connected, Serial0/0/0
S 192.168.10.0/24 [150/0] via 10.10.10.1
S 192.168.20.0/24 [150/0] via 10.10.20.1
C 192.168.30.0/24 is directly connected, FastEthernet0/0
```

Router R3

```
R3>enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip route 192.168.30.0 255.255.255.0 10.10.20.1 150
R3(config)#ip route 10.10.20.0 255.255.255.0 10.10.10.1 150
R3(config)#ip route 192.168.20.0 255.255.255.0 10.10.10.1 150
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
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 192.168.3.0/24 is directly connected, FastEthernet0/0
```

CONCLUSION: Thus, we made use of *CLI* & *PDU* utilities in *PacketTracer* to implement a *static-routing network*, and simulated real-time pings and also visualized them.

PRACTICAL: 9

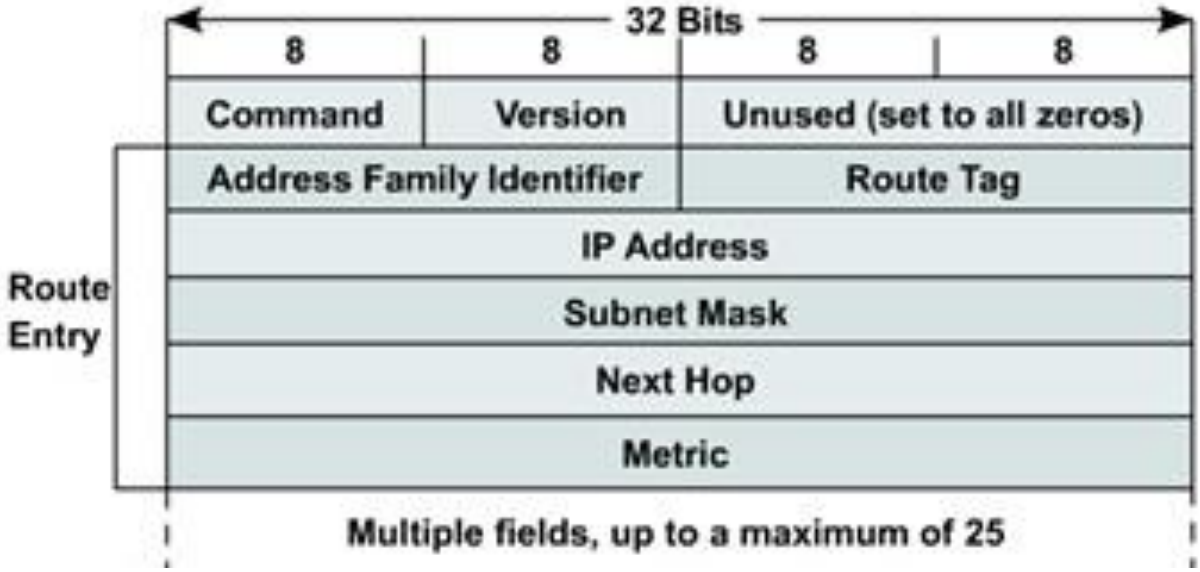
AIM: To study & simulate RIP using CISCO PacketTracer.

SOFTWARE: CISCO PacketTracer 7.0

THEORY:

Routing Information Protocol

1. The Routing Information Protocol (RIP) is a *distance-vector routing protocol* which employs the *hop count* as a *routing metric*.
2. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.
3. The maximum number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and the route is considered unreachable. RIP implements the split horizon, route poisoning and holddown mechanisms to prevent incorrect routing information from being propagated.
4. RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved Port-520.

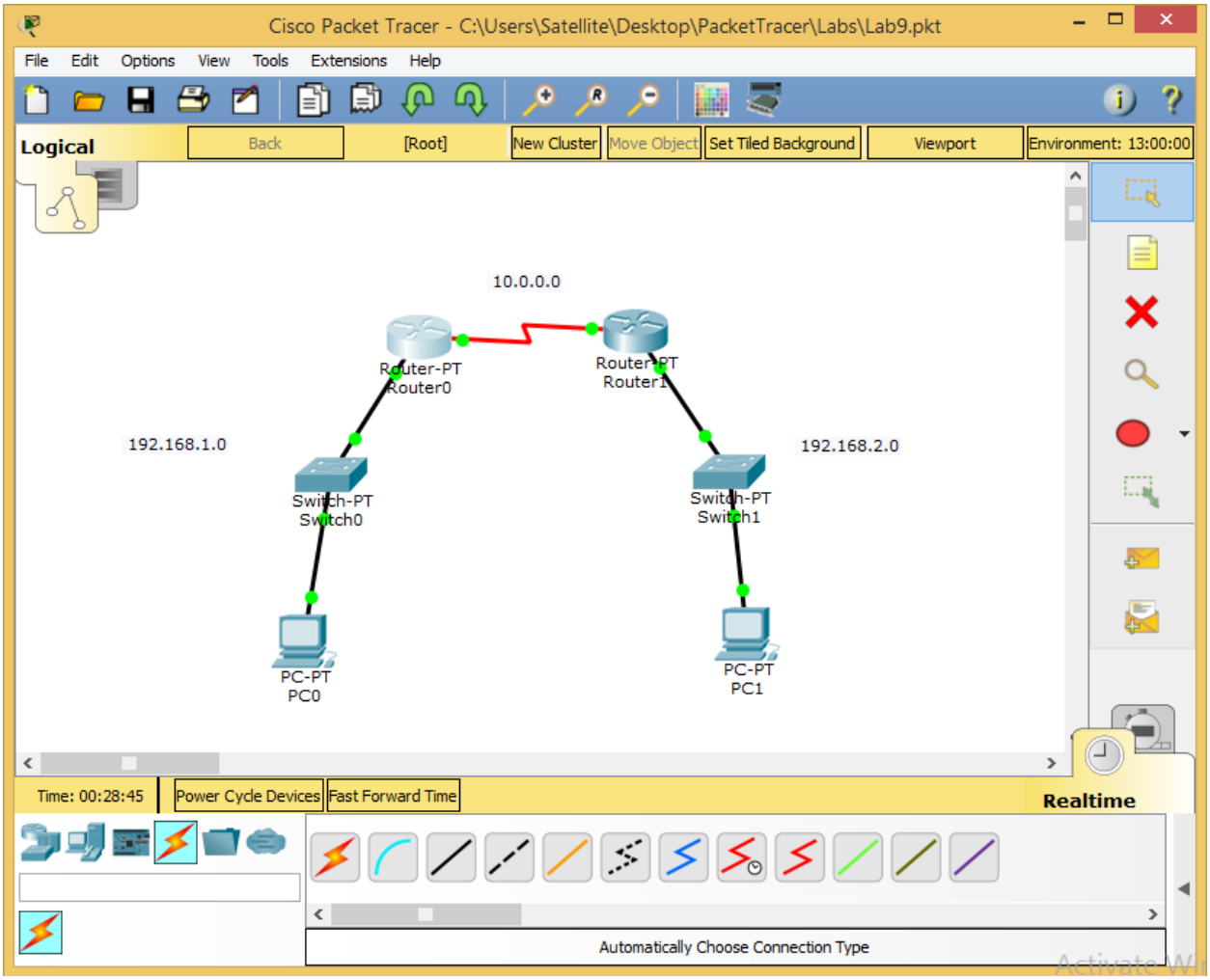


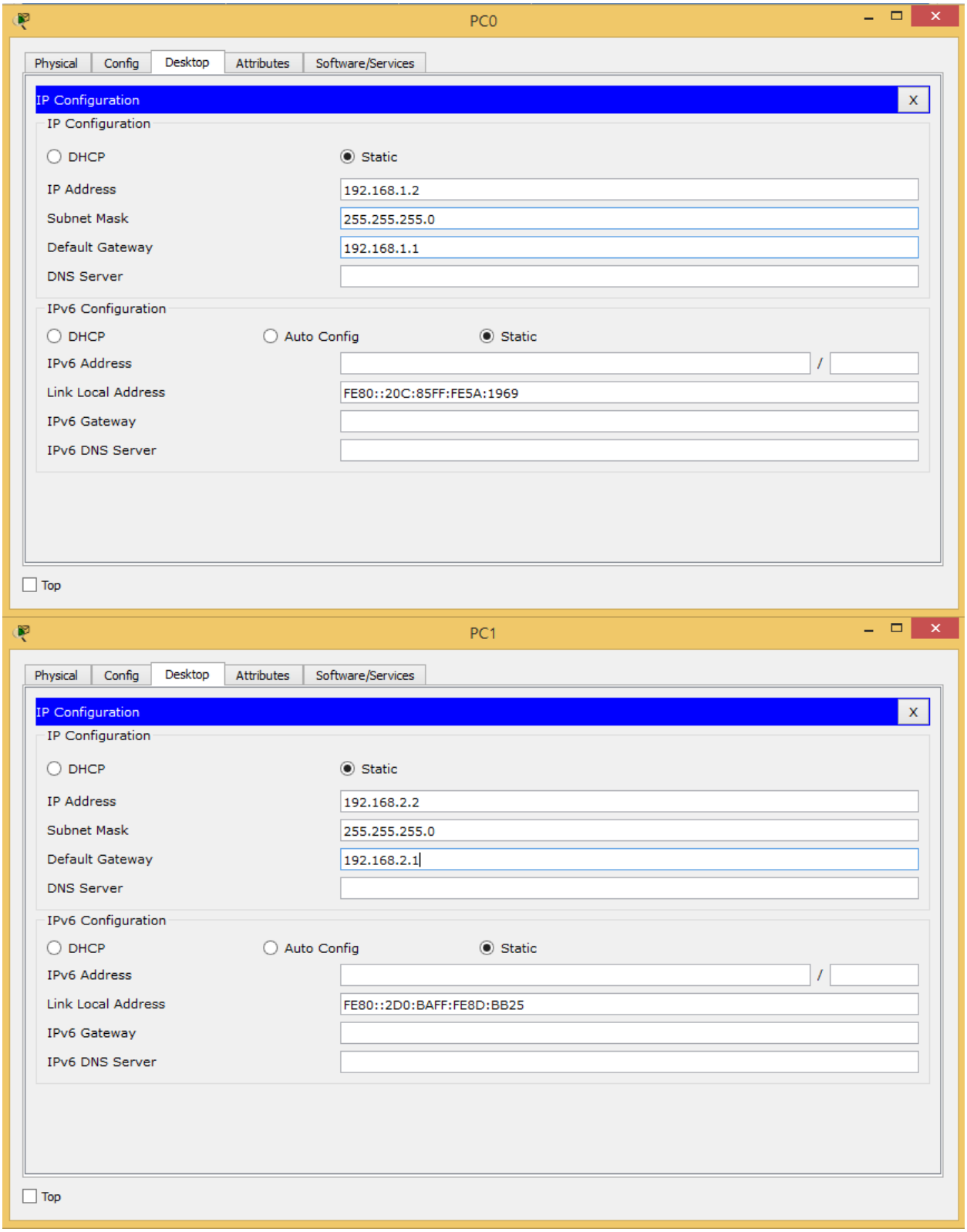
PROCEDURE:

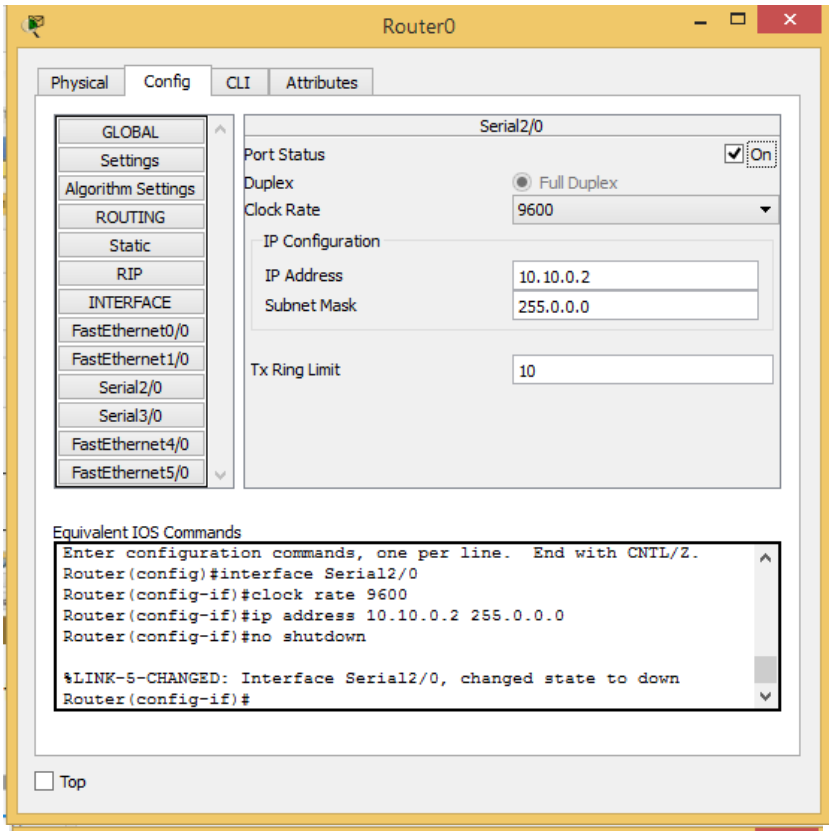
[1] Place the various physical blocks (2 routers, 2 switches & 2 PCs) using the Logical View of PT.
[2] Make necessary connections using Copper Straight-Through wires (Serial DTE wires for router-router connections).
[3] Configure CLI options of the routers.
[4] Configure IPv4 Addressing scheme for the two PCs.
[5] Ping PC1 from PC0, using CLI of PC0. Similarly for PC1.
[6] To visualize the pinging process of [5], use *PDU* in *Simulation Mode*, check only *ICMP* packets, and click *AutoCapture/Ping* to begin the simulation.

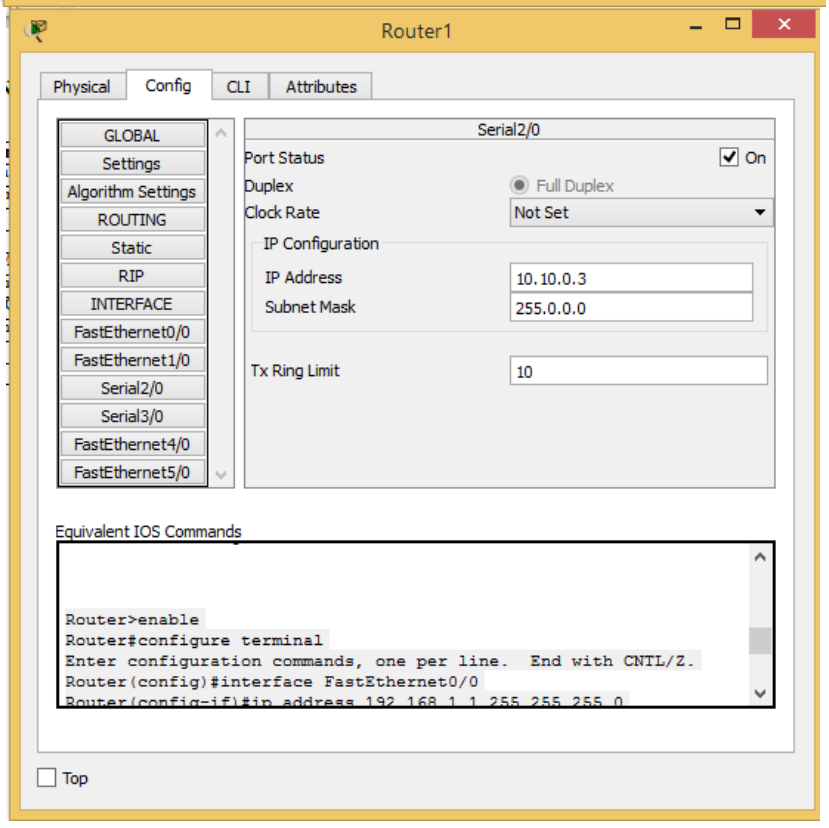
IMPLEMENTATION:

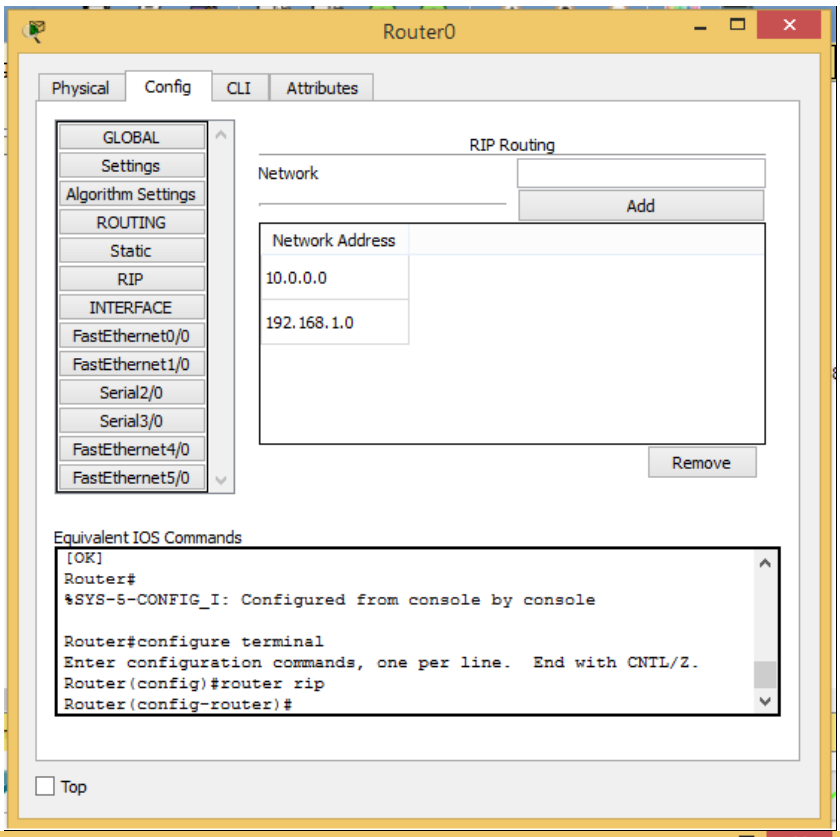
(In the corresponding order as listed in '**PROCEDURE**')

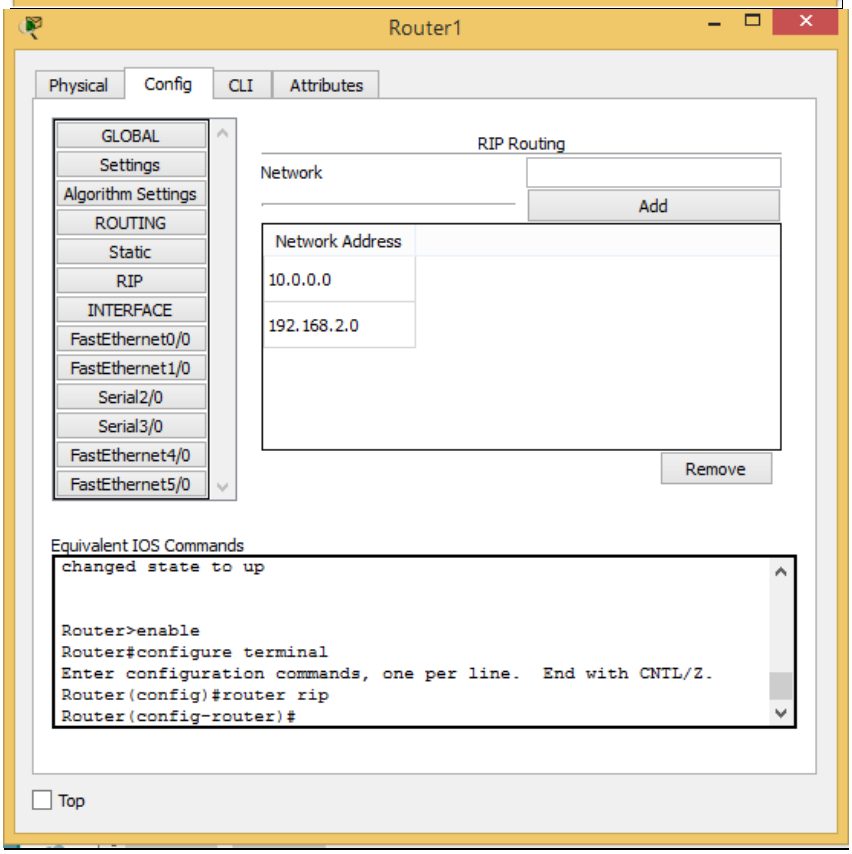


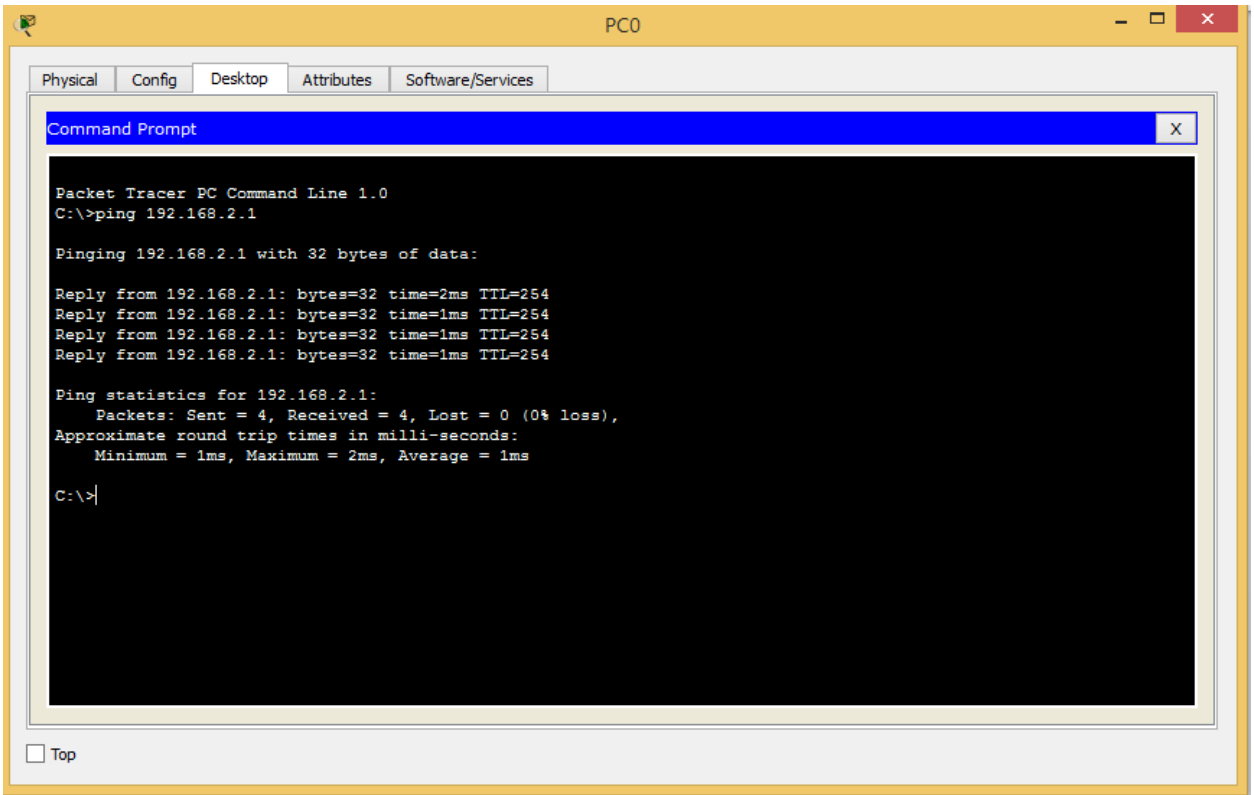

PC0
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::20C:85FF:FE5A:1969
IPv6 Gateway
IPv6 DNS Server
Top
PC1
Physical
Config
Desktop
Attributes
Software/Services
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FE8D:BB25
IPv6 Gateway
IPv6 DNS Server
Top

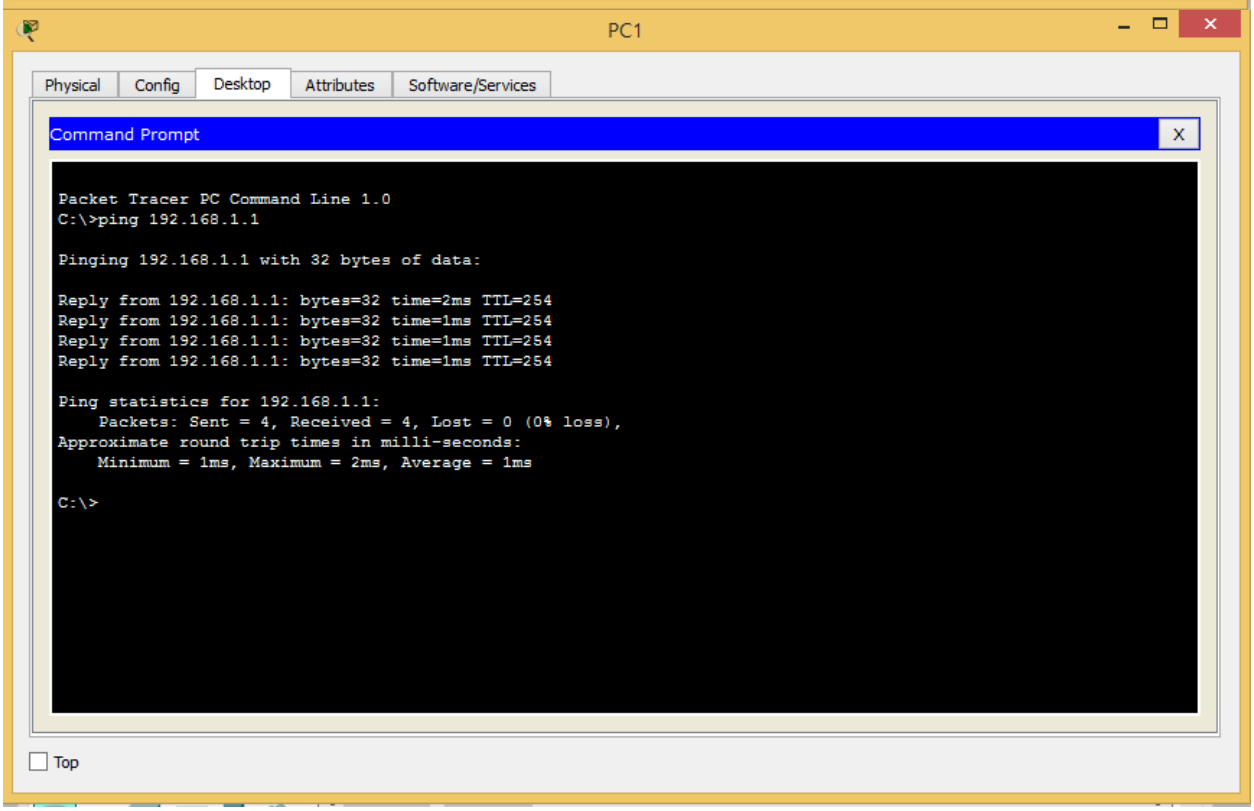

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
9600
IP Configuration
IP Address
10.10.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#clock rate 9600
Router(config-if)#ip address 10.10.0.2 255.0.0.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial2/0, changed state to down
Router(config-if)#
Top

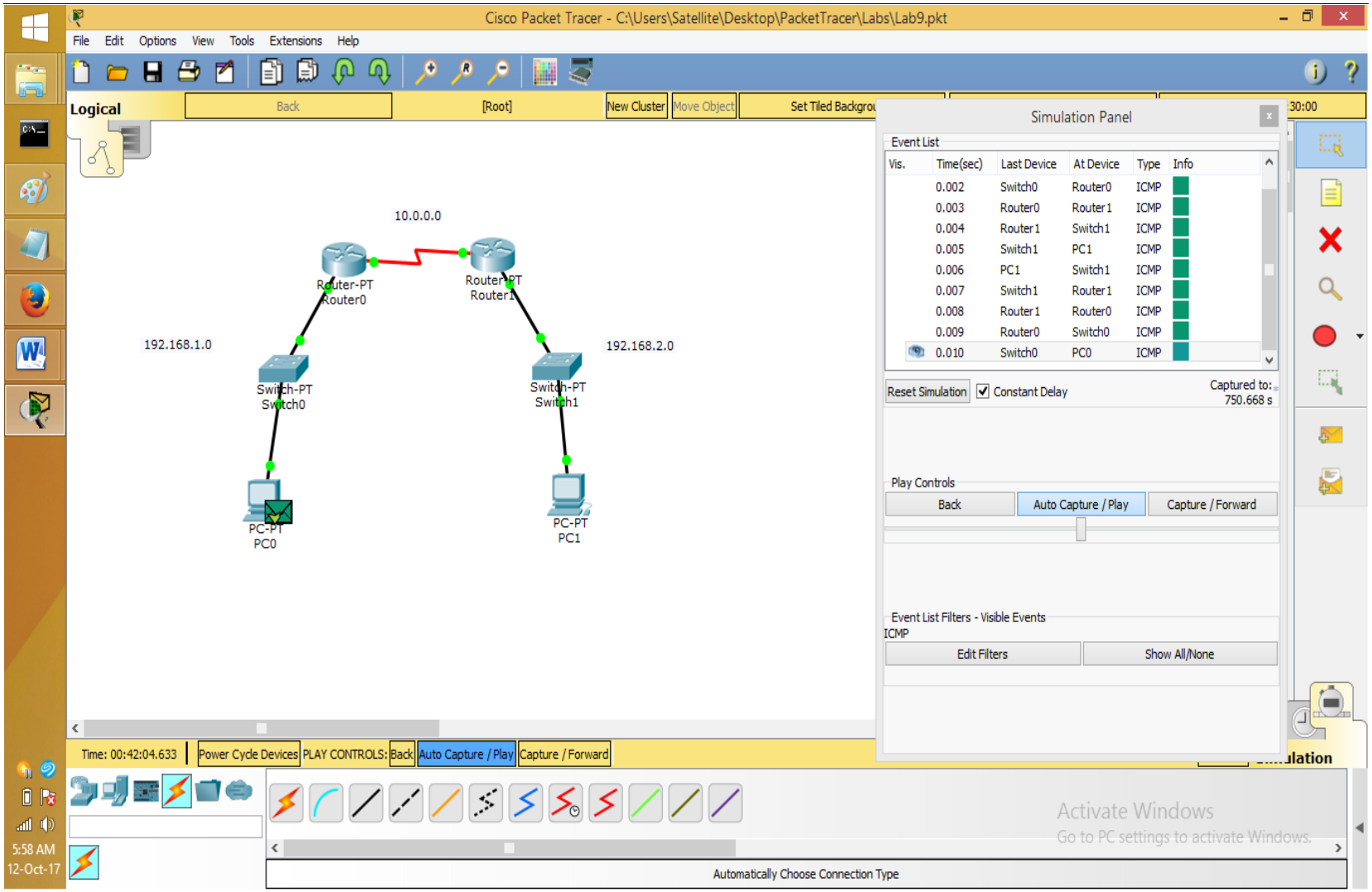

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
Not Set
IP Configuration
IP Address
10.10.0.3
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Top


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
RIP Routing
Network
Add
Network Address
10.0.0.0
192.168.1.0
Remove
Equivalent IOS Commands
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
RIP Routing
Network
Add
Network Address
10.0.0.0
192.168.2.0
Remove
Equivalent IOS Commands
changed state to up
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
Top


PC0
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=2ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>
Top


PC1
Physical
Config
Desktop
Attributes
Software/Services
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>
Top


Cisco Packet Tracer - C:\Users\Satellite\Desktop\PacketTracer\Labs\Lab9.pkt
File Edit Options View Tools Extensions Help
Logical
Back
[Root]
New Cluster
Move Object
Set Tiled Backgrou
30:00
10.0.0.0
Router-PT Router0
Router-PT Router1
192.168.1.0
192.168.2.0
Switch-PT Switch0
Switch-PT Switch1
PC-PT PC0
PC-PT PC1
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.002 Switch0 Router0 ICMP
0.003 Router0 Router1 ICMP
0.004 Router1 Switch1 ICMP
0.005 Switch1 PC1 ICMP
0.006 PC1 Switch1 ICMP
0.007 Switch1 Router1 ICMP
0.008 Router1 Router0 ICMP
0.009 Router0 Switch0 ICMP
0.010 Switch0 PC0 ICMP
Reset Simulation
Constant Delay
Captured to: 750.668 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ICMP
Edit Filters
Show All/None
Time: 00:42:04.633
Power Cycle Devices
PLAY CONTROLS: Back
Auto Capture / Play
Capture / Forward
Activate Windows
Go to PC settings to activate Windows.
Automatically Choose Connection Type
5:58 AM
12-Oct-17

CLI-INPUT:

(Entered for configuring the routers with the two PCs)

Router R0

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial3/0
Router(config-if)#
Router(config-if)#end
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
%SYS-5-CONFIG_I: Configured from console by console
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial2/0
Router(config-if)#clock rate 9600
Router(config-if)#ip address 10.10.0.2 255.0.0.0
Router(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial2/0, changed state to down
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed
state to up

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
Router(config-router)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Router R1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

Router(config-if)#exit
Router(config)#interface Serial3/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
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
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed
state to up

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
Router(config-router)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

CONCLUSION: Thus, we made use of *CLI* & *PDU* utilities in *PacketTracer* to implement a *RIP-routing network*, and simulated real-time pings and also visualized them.

PRACTICAL: 10

AIM: Introduction to WireShark.

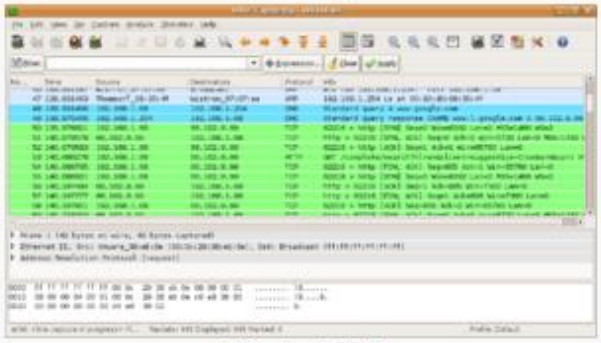
SOFTWARE: WireShark GUI.

THEORY:

WireShark

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

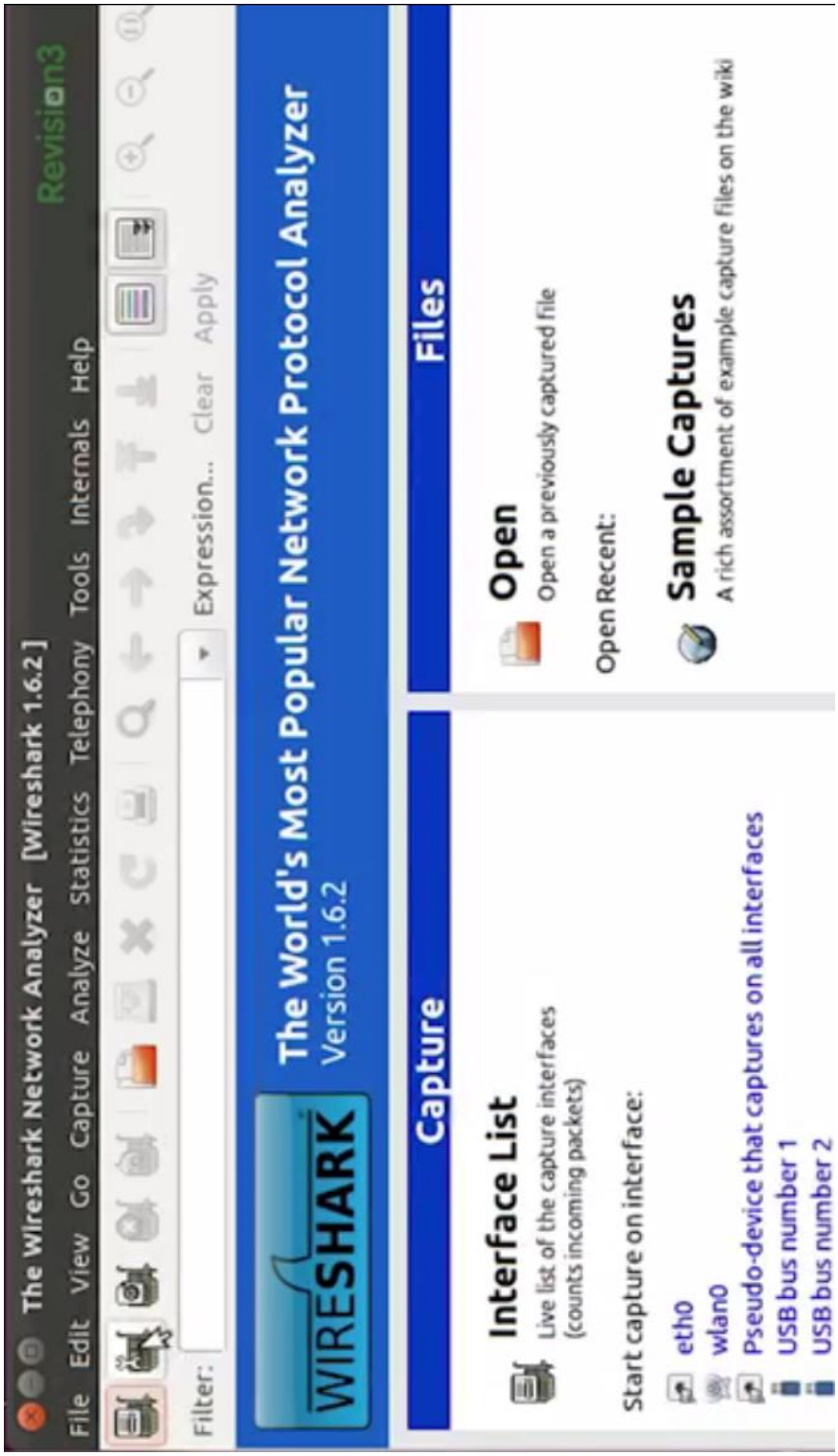
Wireshark



Wireshark GUI

Original author(s)	Gerald Combs[1]
Developer(s)	The Wireshark team
Initial release	Around 1998; 18 years ago
Stable release	2.2.0 / 7 September 2016; 25 days ago[2]
Written in	C, C++
Operating system	Cross-platform
Type	Packet analyzer
License	GNU GPL[3]
Website	www.wireshark.org
Repository	code.wireshark.org/review/gitweb?p=wireshark.git

Interface


The Wireshark Network Analyzer [Wireshark 1.6.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Revision3
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.6.2
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start capture on interface:
eth0
wlan0
Pseudo-device that captures on all interfaces
USB bus number 1
USB bus number 2
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki

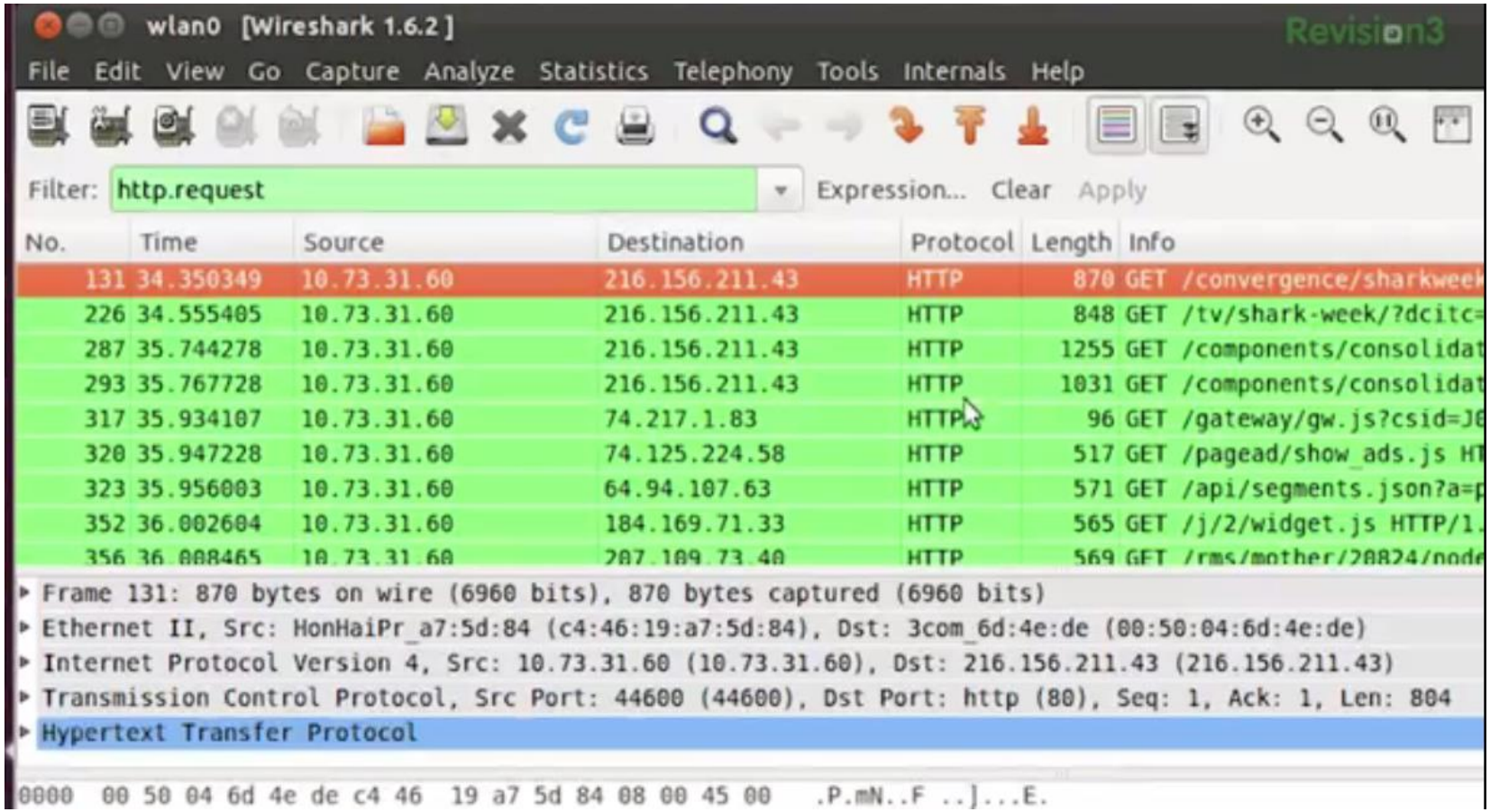
Capture Interface #1

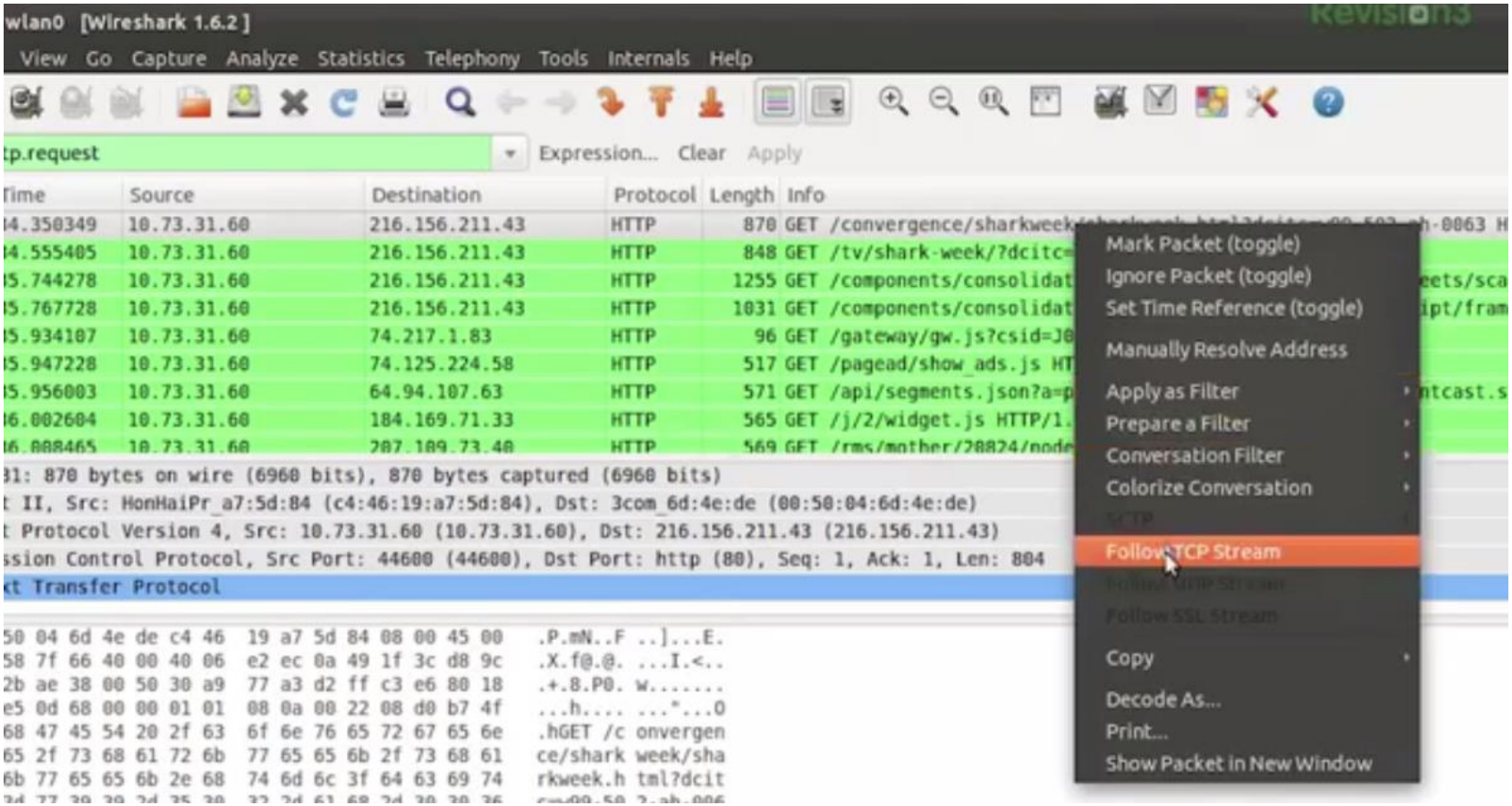
Capture Interface #2

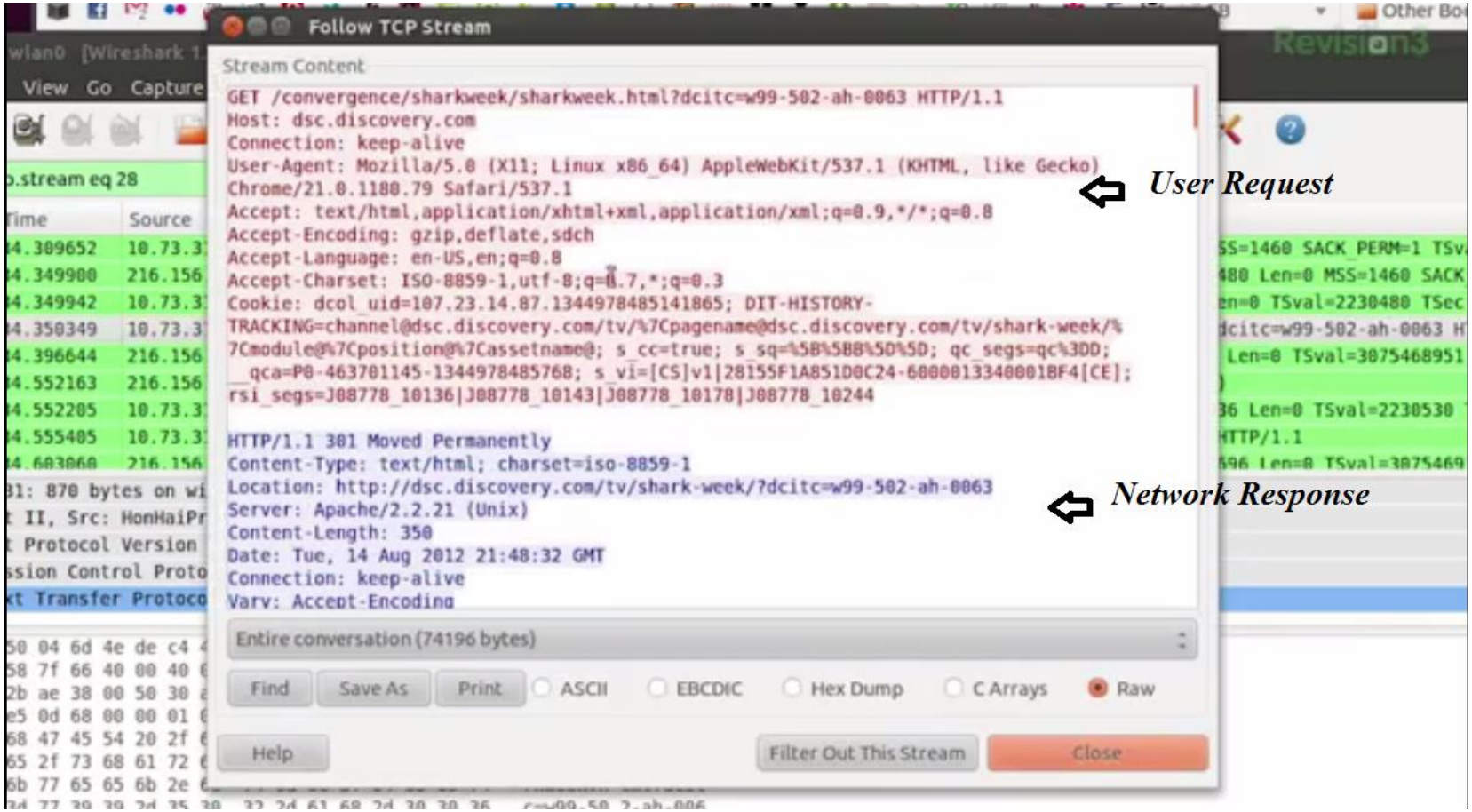
CLI Options

IMPLEMENTATION:

As an example, we will see how to analyze the packets of an ***HTTP Request***.


wlan0 [Wireshark 1.6.2]
Revision3
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.request
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
131 34.350349 10.73.31.60 216.156.211.43 HTTP 870 GET /convergence/sharkweek
226 34.555405 10.73.31.60 216.156.211.43 HTTP 848 GET /tv/shark-week/?dcitc=
287 35.744278 10.73.31.60 216.156.211.43 HTTP 1255 GET /components/consolidat
293 35.767728 10.73.31.60 216.156.211.43 HTTP 1031 GET /components/consolidat
317 35.934107 10.73.31.60 74.217.1.83 HTTP 96 GET /gateway/gw.js?csid=J0
320 35.947228 10.73.31.60 74.125.224.58 HTTP 517 GET /pagead/show_ads.js HT
323 35.956003 10.73.31.60 64.94.107.63 HTTP 571 GET /api/segments.json?a=p
352 36.002604 10.73.31.60 184.169.71.33 HTTP 565 GET /j/2/widget.js HTTP/1.
356 36.008465 10.73.31.60 207.189.73.40 HTTP 569 GET /rms/mother/20824/node
Frame 131: 870 bytes on wire (6960 bits), 870 bytes captured (6960 bits)
Ethernet II, Src: HonHaiPr_a7:5d:84 (c4:46:19:a7:5d:84), Dst: 3com_6d:4e:de (00:50:04:6d:4e:de)
Internet Protocol Version 4, Src: 10.73.31.60 (10.73.31.60), Dst: 216.156.211.43 (216.156.211.43)
Transmission Control Protocol, Src Port: 44600 (44600), Dst Port: http (80), Seq: 1, Ack: 1, Len: 804
Hypertext Transfer Protocol
0000 00 50 04 6d 4e de c4 46 19 a7 5d 84 08 00 45 00 .P.mN..F ..]...E.


wlan0 [Wireshark 1.6.2]
View Go Capture Analyze Statistics Telephony Tools Internals Help
tp.request
Expression... Clear Apply
Time Source Destination Protocol Length Info
4.350349 10.73.31.60 216.156.211.43 HTTP 870 GET /convergence/sharkweek
4.555405 10.73.31.60 216.156.211.43 HTTP 848 GET /tv/shark-week/?dcitc=
5.744278 10.73.31.60 216.156.211.43 HTTP 1255 GET /components/consolidat
5.767728 10.73.31.60 216.156.211.43 HTTP 1031 GET /components/consolidat
5.934107 10.73.31.60 74.217.1.83 HTTP 96 GET /gateway/gw.js?csid=J0
5.947228 10.73.31.60 74.125.224.58 HTTP 517 GET /pagead/show_ads.js HT
5.956003 10.73.31.60 64.94.107.63 HTTP 571 GET /api/segments.json?a=p
6.002604 10.73.31.60 184.169.71.33 HTTP 565 GET /j/2/widget.js HTTP/1.
31: 870 bytes on wire (6960 bits), 870 bytes captured (6960 bits)
t II, Src: HonHaiPr_a7:5d:84 (c4:46:19:a7:5d:84), Dst: 3com_6d:4e:de (00:50:04:6d:4e:de)
t Protocol Version 4, Src: 10.73.31.60 (10.73.31.60), Dst: 216.156.211.43 (216.156.211.43)
ssion Control Protocol, Src Port: 44600 (44600), Dst Port: http (80), Seq: 1, Ack: 1, Len: 804
xt Transfer Protocol
50 04 6d 4e de c4 46 19 a7 5d 84 08 00 45 00 .P.mN..F ..]...E.
58 7f 66 40 00 40 06 e2 ec 0a 49 1f 3c d8 9c .X.f@.@. ...I.<..
2b ae 38 00 50 30 a9 77 a3 d2 ff c3 e6 80 18 .+.8.P0. w.......
e5 0d 68 00 00 01 01 08 0a 00 22 08 d0 b7 4f ...h.... ..."...O
68 47 45 54 20 2f 63 6f 6e 76 65 72 67 65 6e .hGET /c onvergen
65 2f 73 68 61 72 6b 77 65 65 6b 2f 73 68 61 ce/shark week/sha
6b 77 65 65 6b 2e 68 74 6d 6c 3f 64 63 69 74 rkweek.h tml?dcit
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window


Follow TCP Stream
Stream Content
GET /convergence/sharkweek/sharkweek.html?dcitc=w99-502-ah-0063 HTTP/1.1
Host: dsc.discovery.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.1 (KHTML, like Gecko)
Chrome/21.0.1180.79 Safari/537.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: dcol_uid=107.23.14.87.1344978485141865; DIT-HISTORY-
TRACKING=channel@dsc.discovery.com/tv/%7Cpagename@dsc.discovery.com/tv/shark-week/%
7Cmodule@%7Cposition@%7Cassetname@; s_cc=true; s_sq=%5B%5BB%5D%5D; qc_segs=qc%3DD;
__qca=P0-463701145-1344978485768; s_vi=[CS]v1|28155F1A851D0C24-6000013340001BF4[CE];
rsi_segs=J08778_10136|J08778_10143|J08778_10178|J08778_10244
HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=iso-8859-1
Location: http://dsc.discovery.com/tv/shark-week/?dcitc=w99-502-ah-0063
Server: Apache/2.2.21 (Unix)
Content-Length: 350
Date: Tue, 14 Aug 2012 21:48:32 GMT
Connection: keep-alive
Vary: Accept-Encoding
User Request
Network Response
Entire conversation (74196 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

CONCLUSION:

Thus, we made use of *WireShark GUI* utility to analyze network packets, by analyzing the contents of an *HTTP Request*.