CS23532 - COMPUTER NETWORKS

DHANUSH R

211623180130

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

CS23532- COMPUTER NETWORKS LABORATORY

THIRD YEAR

FIFTH SEMESTER

2025- 2026

ODD SEMESTER

CS23532 - COMPUTER NETWORKS

List of Experiments

	List of Experiments	No of Hours
1.	**Study of various Network commands used in Linux and Windows:** Hands-on practice of various network commands.	[4]
2.	**Study of Network cables.** 1. Understand different types of Network cables. **2.** Make a cross-wired cable and straight through cable using clamping/crimping tool.	[4]
3.	**Experiments on CISCO PACKET TRACER (Simulation Tool):** **a)** To understand environment of CISCO PACKET TRACER to design simple network. **b)** Analyse the behaviour of network devices using CISCO PACKET TRACER simulator. Design a simple network with multiple nodes and connect via networking devices available in library. Perform simulation and trace communication behaviour of specified network devices. 1: Use only HUB to design a small network having 4 to 6 hosts 2: Use only a Switch to design a small network with 4 to 6 hosts. 3: Use both the device (HUB and SWITCH) for a network and find out functioning difference between switch and hub. **Find out the network topology implemented in your college and draw and label that topology in your observation book.**	[2] [2]

CS23532 - COMPUTER NETWORKS

4.	**a) Setup and configure a LAN (Local area network) using a Switch and Ethernet cables in your lab.** 1. Connect 3-4 host machines to a switch. 2. Assign ip addresses to each host machine. 3. Check the connectivity between the machines by using ping command. 4. Share and access files and folder across the machines of the LAN.	[2]

CS23532 - COMPUTER NETWORKS

5.	**Experiments on Packet capture tool: Wireshark** To understand the features of wireshark as a packet capture tool and understand **encapsulation of information at various layers of a Protocol stack**.	[4]
6.	**Error Correction at Data Link Layer:** Write a program to implement error detection and correction using HAMMING code concept. Make a test run to input data stream and verify error correction feature.	[4]
7.	**Flow control at Data Link Layer:** Write a program to implement flow control at data link layer using SLIDING WINDOW PROTOCOL. Simulate the flow of frames from one node to another.	[4]
8.	**NMAP to Discover Live Hosts Using Nmap Scans (ARP, ICMP, TCP/UDP) on the TryHackMe Platform**	[4]
9.	**Implementation of SUBNETTING in CISCO PACKET TRACER simulator.** a) Design multiple subnet with suitable number of hosts. b) Assign static IP address across all subnet and connect the subnets via Router. c) Simulate packet transmission across the subnets and observe the results:- a. When subnets are connected via a router. b. When subnets are not connected without a router.	[4]

CS23532 - COMPUTER NETWORKS

10.	**Internetworking with routers in CISCO PACKET TRACER simulator.** **a) Design and configure a simple internetwork using a router.** 1. Design different networks (with 3 to 4 hosts) and connect via Router. 2. Allot static ip address to machines and router interfaces. 3. Perform simulation and trace how routing is done in packet transmission. **b) Design and configure an internetwork using wireless router DHCP server and internet cloud.** **c) Design and configure an inter-network in your lab using switch, router and Ethernet cables.**	[4] [2] [2]
11.	**Routing at Network Layer:** a) Simulate Static Routing Protocol Configuration using CISCO Packet Tracer. b) Simulate RIP using CISCO Packet Tracer.	[4]
12.	**End –End Communication at Transport Layer** a) Implement echo client server using TCP/UDP sockets. b) Implement a chat program using socket programming.	[4]
13.	Implement your own ping program.	[2]
14.	Write a code using RAW sockets to implement packet sniffing.	[4]
15.	Analyse various types of servers using Webalizer tool.	[4]
	Total	**60 hours**

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

	Additional programs for practice	
1.	**Data Link Layer (Frame Generation):** Write a program to read a stream of data from data file (Having Characters) to create BSC frames by implementing character stuffing concept and inserting control characters. The receiving program must execute on other computer and decode received bytes and write to a file.	
2.	Demonstrate Configuration of Network Address Translation (NAT) and Port Address Translation (PAT) using CISCO Packet Tracer simulation.	
3.	Implement a static routing protocol which also displays the routing table details after every update.	
4.	Implement a dynamic routing protocol which also displays the routing table after every updates.	
5.	Implement FTP server using socket programming.	

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

Practical -1

AIM: - Study of various Network commands used in Linux and Windows:

BASIC NETWORKING COMMANDS:

arp –a:- ARP is short form of address resolution protocol, It will show the IP address of your computer along with the IP address and MAC address of your router.
hostname: This is the simplest of all TCP/IP commands. It simply displays the name of your computer.
ipconfig /all: This command displays detailed configuration information about your TCP/IP connection including Router, Gateway, DNS, DHCP, and type of Ethernet adapter in your system
nbtstat –a: This command helps solve problems with NetBIOS name resolution. (Nbt stands for NetBIOS over TCP/IP)
netstat: (network statistics) netstat displays a variety of statistics about a computers active TCP/IP connections. It is a command line tool for monitoring network connections both incoming and outgoing as well as viewing routing tables, interface statistics etc. e.g.:- netstat -r
nslookup: (name server lookup) is a tool used to perform DNS lookups in Linux. It is used to display DNS details, such as the IP address of a particular computer, the MX records for a domain or the NS servers of a domain. nslookup can operate in two modes: interactive and non-interactive. e.g.:- nslookup www.google.com
pathping: Pathping is unique to Window's, and is basically a combination of the Ping and Tracert commands. Pathping traces the route to the destination address then launches a 25 second test of each router along the way, gathering statistics on the rate of data loss along each hop.
ping: (Packet INternet Groper) command is the best way to test connectivity between two nodes. Ping use ICMP (Internet Control Message Protocol) to communicate to other devices. 1. #ping hostname(ping localhost) 2. #ping ip address (ping 4.2.2.2) 3. #ping fully qualified domain name(ping www.facebook.com
Route: route command is used to show/manipulate the IP routing table. It is primarily used to setup static routes to specific host or networks via an interface.

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

Some important Linux networking commands

1. ip

The ip command is one of the basic commands every administrator will need in daily work, from setting up new systems and assigning IPs to troubleshooting existing systems. The ip command can show address information, manipulate routing, plus display network various devices, interfaces, and tunnels.

ip <OPTIONS> <OBJECT> <COMMAND>

Here are some common use cases for the ip command.

a. To show the IP addresses assigned to an interface on your server:
   a. [root@server ~]# *ip address show*

b. To assign an IP to an interface, for example, **enps03**:
   a. [root@server ~]# ip address add 192.168.1.254/24 dev enps03

c. To delete an IP on an interface:
   a. [root@server ~]# ip address del 192.168.1.254/24 dev enps03

d. Alter the status of the interface by bringing the interface **eth0** online:
   [root@server ~]# ip link set eth0 up

e. Alter the status of the interface by bringing the interface **eth0** offline:
   [root@server ~]# ip link set eth0 down

f. Alter the status of the interface by enabling promiscuous mode for **eth0**:
   [root@server ~]# ip link set eth0 promisc on

g. Add a default route (for all addresses) via the local gateway 192.168.1.254 that can be reached on device **eth0**:
   [root@server ~]# ip route add default via 192.168.1.254 dev eth0

h. Add a route to 192.168.1.0/24 via the gateway at 192.168.1.254:
   [root@server ~]# ip route add 192.168.1.0/24 via 192.168.1.254

i. Add a route to 192.168.1.0/24 that can be reached on device **eth0**:
   [root@server ~]# ip route add 192.168.1.0/24 dev eth0

j. Delete the route for 192.168.1.0/24 via the gateway at 192.168.1.254:
   [root@server ~]# ip route delete 192.168.1.0/24 via 192.168.1.254

k. Display the route taken for IP 10.10.1.4:
   [root@server ~]# ip route get 10.10.1.4

CS23532 - COMPUTER NETWORKS

231801030

2. ifconfig

The ifconfig command was/is a staple in many sysadmin's tool belt for configuring and troubleshooting networks. It has since been replaced by the ip command discussed above.

3. mtr

MTR (Matt's traceroute) is a program with a command-line interface that serves as a network diagnostic and troubleshooting tool. This command combines the functionality of the ping and traceroute commands. Just like a traceroute, the mtr command will show the route from a computer to a specified host. mtr provides a lot of statistics about each hop, such as response time and percentage. With the mtr command, you will get more information about the route and be able to see problematic devices along the way. If you see a sudden increase in response time or packet loss, then obviously, there is a bad link somewhere.
The syntax of the command is as follows:

mtr <options> hostname/IP

Let's look at some common use cases.

a. The basic mtr command shows you the statistics, including each hop (hostnames) with time and loss%:

[root@server ~]# *mtr google.com*

b. Show numeric IP addresses (if you use -g, you will get IP addresses (numbers) instead of hostnames):

[root@server ~]# mtr -g google.com

c. Show the numeric IP addresses and hostnames, too:

[root@server ~]# mtr -b google.com

d. Set the number of pings that you want to send:

[root@server ~]# mtr -c 10 google.com

4. tcpdump

The tcpdump command is designed for capturing and displaying packets.

You can install tcpdump with the command below:
[root@server ~]# *dnf install -y tcpdump*

Before starting any capture, you need to know which interfaces tcpdump can use. You will need to use sudo or have root access in this case.
[root@server ~]# *tcpdump -D*

If you want to capture traffic on **eth0**, you can initiate that with tcpdump -i eth0 sample output:
[root@server ~]# *tcpdump -i eth0*

[root@server ~]# *tcpdump -i eth0 -c 10*

Capture traffic to and from one host

You can filter out traffic coming from a specific host. For example, to find traffic coming from and going to 8.8.8.8, use the command:

[root@server ~]# *tcpdump -i eth0 -c 10 host 8.8.8.8*

For traffic coming from 8.8.8.8, use:

[root@server ~]# *tcpdump -i eth0 src host 8.8.8.8*

For outbound traffic going to 8.8.8.8, use:

[root@server ~]# *tcpdump -i eth0 dst host 8.8.8.8*

Capture traffic to and from a network

You can also capture traffic to and from a specific network using the command below:

[root@server ~]# *tcpdump -i eth0 net 10.1.0.0 mask 255.255.255.0*

or:

[root@server ~]# *tcpdump -i eth0 net 10.1.0.0/24*

Capture traffic to and from port numbers

Capture only DNS port 53 traffic:

[root@server ~]# *tcpdump -i eth0 port 53*

For a specific host,

[root@server ~]# *tcpdump -i eth0 host 8.8.8.8 and port 53*

To capture only HTTPS traffic,

[root@server ~]# *tcpdump -i eth0 -c 10 host www.google.com and port 443*

To capture all port except port 80 and 25,

[root@server ~]# *tcpdump -i eth0 port not 53 and not 25*

CS23532 - COMPUTER NETWORKS

231801030

5. ping

Ping is a tool that verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages is displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

```
[root@server ~]# ping google.com
PING google.com (216.58.206.174) 56(84) bytes of data.
64 bytes from sof02s27-in-f14.1e100.net (216.58.206.174): icmp_seq=1 ttl=56 time=10.7 ms
64 bytes from sof02s27-in-f14.1e100.net (216.58.206.174): icmp_seq=2 ttl=56 time=10.2 ms
64 bytes from sof02s27-in-f14.1e100.net (216.58.206.174): icmp_seq=3 ttl=56 time=10.4 ms
^C
```

You need to stop the ping command by pressing **CTRL+C**. Otherwise, it will ping until you stop it.

If you want to ping a host ten times, use the following command:

```
[root@server ~]# ping -c 10 google.com
```

While pinging a host, you'll find different output from the ping results, including the following three examples.

Destination Host Unreachable

The possible best reason is there is no route from the local host system and to the destination desired destination host, or a remote router reports that it has no route to the destination host.

Request timed out

This result means that no Echo Reply messages were received within the default time of one second or the time that you set while you are pinging that host. This can be due to many different causes; the most common include network congestion, failure of the ARP request, packet filtering/firewall, etc.

Unknown host/Ping Request Could Not Find Host

Maybe you misspelled the hostname or the host does not exist at all in the network.

You must have 0% packet loss for every ping result with a good latency or lower response time. Depending on which transmission medium (UTP, fibre optics cable, Wi-Fi) you're using, your latency will differ.

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

Configuring an Ethernet connection by using nmcli

If you connect a host to the network over Ethernet, you can manage the connection's settings on the command line by using the **nmcli** utility.

Procedure

1. List the NetworkManager connection profiles:

   # **nmcli connection show**

   ```
   NAME                UUID                                  TYPE      DEVICE
   Wired connection 1  a5eb6490-cc20-3668-81f8-0314a27f3f75  ethernet  enp1s0
   ```

2. # **nmcli connection add con-name <*connection-name*> ifname <*device-name*> type ethernet**
   Skip this step to modify an existing profile.

3. Optional: Rename the connection profile:

   # **nmcli connection modify "Wired connection 1"**
   Here, "Wired connection 1" is the name of the connection

4. Display the current settings of the connection profile:
   # **nmcli connection show**

   ```
   connection.interface-name:    enp1s0
   connection.autoconnect:       yes
   ipv4.method:                  auto
   ipv6.method:                  auto
   ...
   ```

5. Configure the IPv4 settings:
   - To use DHCP, enter:

     # **nmcli connection modify "Wired connection 1" ipv4.method auto**
     Skip this step if ipv4.method is already set to auto (default).

   - To set a static IPv4 address, network mask, default gateway, DNS servers, and search domain, enter:

     # **nmcli connection modify "Wired connection 1" ipv4.method manual ipv4.addresses 192.0.2.1/24 ipv4.gateway 192.0.2.254 ipv4.dns 192.0.2.200 ipv4.dns-search example.com**

6. Configure the IPv6 settings:
   - To use stateless address autoconfiguration (SLAAC), enter:

     # **nmcli connection modify "Wired connection 1" ipv6.method auto**
     Skip this step if ipv6.method is already set to auto (default).

CS23532 - COMPUTER NETWORKS

231801030

- To set a static IPv6 address, network mask, default gateway, DNS servers, and search domain, enter:

  # **nmcli connection modify "Wired connection 1" ipv6.method manual ipv6.addresses 2001:db8:1::fffe/64 ipv6.gateway 2001:db8:1::fffe ipv6.dns 2001:db8:1::ffbb ipv6.dns-search example.com**

7. Activate the profile:

   # **nmcli connection up Internal-LAN**

   Verification

1. Display the IP settings of the NIC:

   # **ip address show enp1s0**
   enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 52:54:00:17:b8:b6 brd ff:ff:ff:ff:ff:ff
   inet 192.0.2.1/24 brd 192.0.2.255 scope global noprefixroute enp1s0
   valid_lft forever preferred_lft forever
   inet6 2001:db8:1::fffe/64 scope global noprefixroute
   valid_lft forever preferred_lft forever

2. Display the IPv4 default gateway:

   # **ip route show default**

   default via 192.0.2.254 dev enp1s0 proto static metric 102

3. Display the IPv6 default gateway:

   # **ip -6 route show default**
   default via 2001:db8:1::ffee dev enp1s0 proto static metric 102 pref medium

4. Display the DNS settings:

   # **cat /etc/resolv.conf**
   search example.com
   nameserver 192.0.2.200
   nameserver 2001:db8:1::ffbb
   If multiple connection profiles are active at the same time, the order of nameserver entries depend on the DNS priority values in these profile and the connection types.

CS23532 - COMPUTER NETWORKS

231801030

5. Use the ping utility to verify that this host can send packets to other hosts:

   # **ping <*host-name-or-IP-address*>**

Troubleshooting

- Verify that the network cable is plugged-in to the host and a switch.
- Check whether the link failure exists only on this host or also on other hosts connected to the same switch.
- Verify that the network cable and the network interface are working as expected. Perform hardware diagnosis steps and replace defect cables and network interface cards.
- If the configuration on the disk does not match the configuration on the device, starting or restarting NetworkManager creates an in-memory connection that reflects the configuration of the device.

Student Observation:

1. **Which command is used to find the reachability of a host machine from your device?**
2. **Which command will be give the details of hops taken by a packet to reach its destination?**
3. **Which commands displays the ip configuration of your machine.**
4. **Which command displays the TCP port status in your machine?**
5. **Write the modify the ip configuration in a Linux machine.**

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

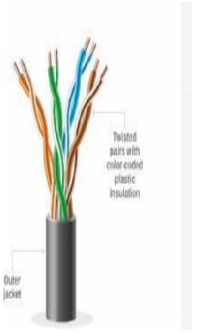
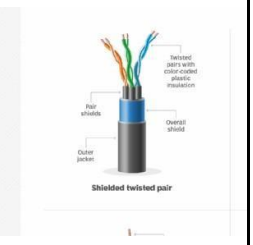
Practical-2

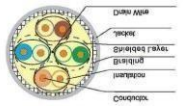
Aim: Study of different types of Network cables.

a) Understand different types of network cable.

Different type of cables used in networking are:

1. Unshielded Twisted Pair (UTP) Cable
2. Shielded Twisted Pair (STP) Cable
3. Coaxial Cable
4. Fibre Optic Cable

Cable type	Category	Maximum Data Transmission	Advantages/ Disadvantages	Application/Use	Image
UTP	Category 3	10 bps	**Advantages** • Cheaper in cost • Easy to install as they have a smaller overall diameter. **Disadvantages** • More prone to (EMI) Electromagnetic interference and noise	10Base-T Ethernet	
	Category 5	Up to 100 Mbps		Fast Ethernet, Gigabit Ethernet	
	Category 5e	1Gbps		Fast Ethernet, Gigabit Ethernet	
STP	Category6,6a	10Gbps	**Advantages** • Shielded. • Faster than UTP. • Less susceptible to noise and interference **Disadvantages**	Gigabit Ethernet, 10G Ethernet (55m) Widely used in data centres	

SSTP	Category 7	10Gbps	• Expensive • Greater installation effort	Gigabit Ethernet, 10G Ethernet (100m)	 

CS23532 - COMPUTER NETWORKS

Coaxial cable	RG-6 RG-59 RG-11	10-100Mbps	• High bandwidth • Immune to interference • Low loss bandwidth • Versatile • **Disadvantages** • Limited distance • Cost • Size is bulky	Speed of signal is 500m Television network High speed internet connections	
fibre optics cable	Single mode Multi mode	100Gbps	**Advantages** • High speed • High bandwidth • High security • Long distance **Disadvantages** • Expensive • Requires skilled installers	• Maximum distance of fibre optics cable is around 100meters	

CS23532 - COMPUTER NETWORKS

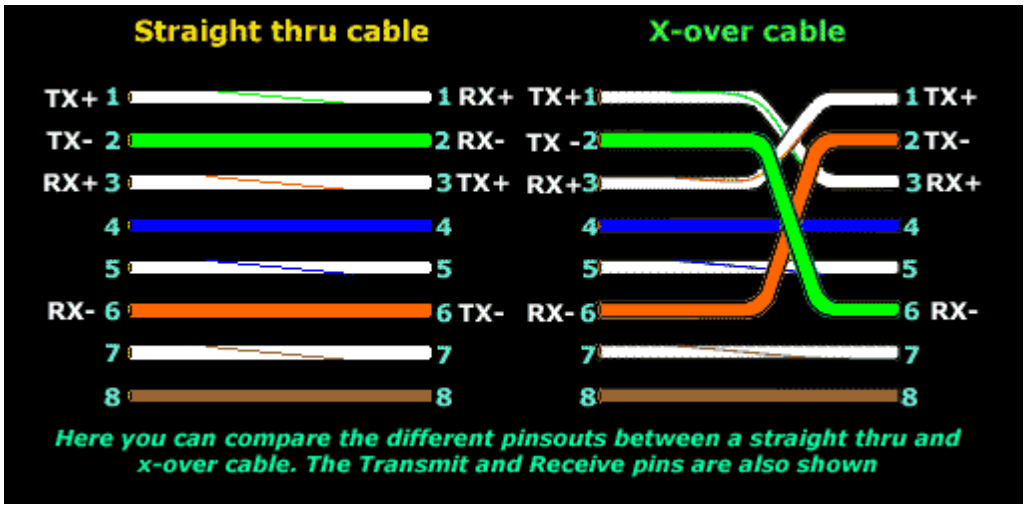
231801030

CS23532 - COMPUTER NETWORKS

b) Make Your Own Ethernet Cross-Over Cable/ Straight cable

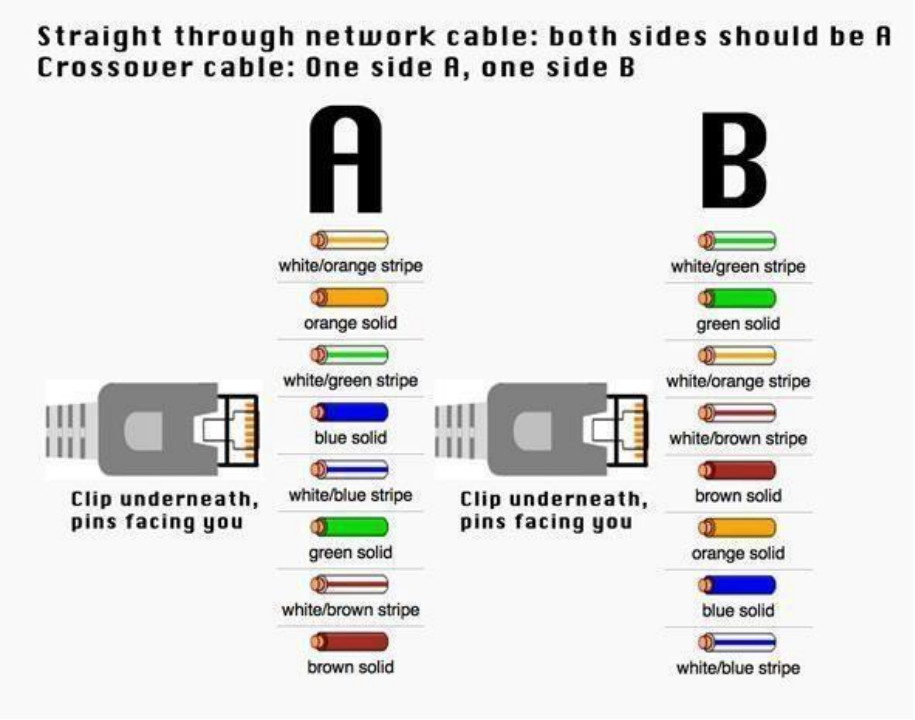
Tools and parts needed:

- Ethernet cabling. CAT5e is certified for gigabit support, but CAT5 cabling works as well, just over shorter distances.
- A crimping tool. This is an all-in-one networking tool shaped to push down the pins in the plug and strip and cut the shielding off the cables.
- Two RJ45 plugs.
- Optional two plug shields.



Difference between crossover cable and straight cable

Take a print out the diagram below or have it handy as a reference



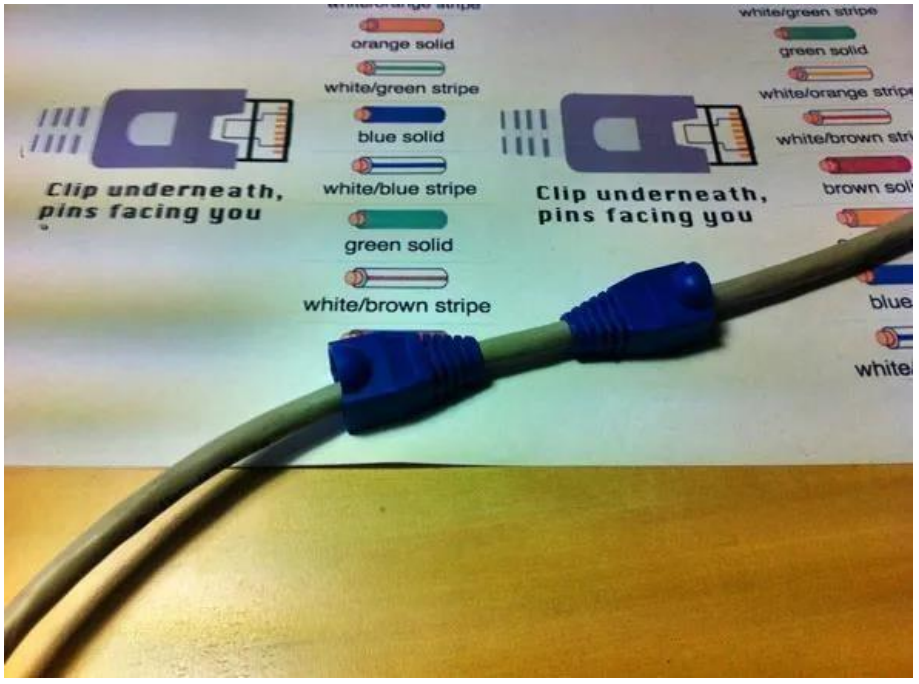
231801030

CS23532 - COMPUTER NETWORKS

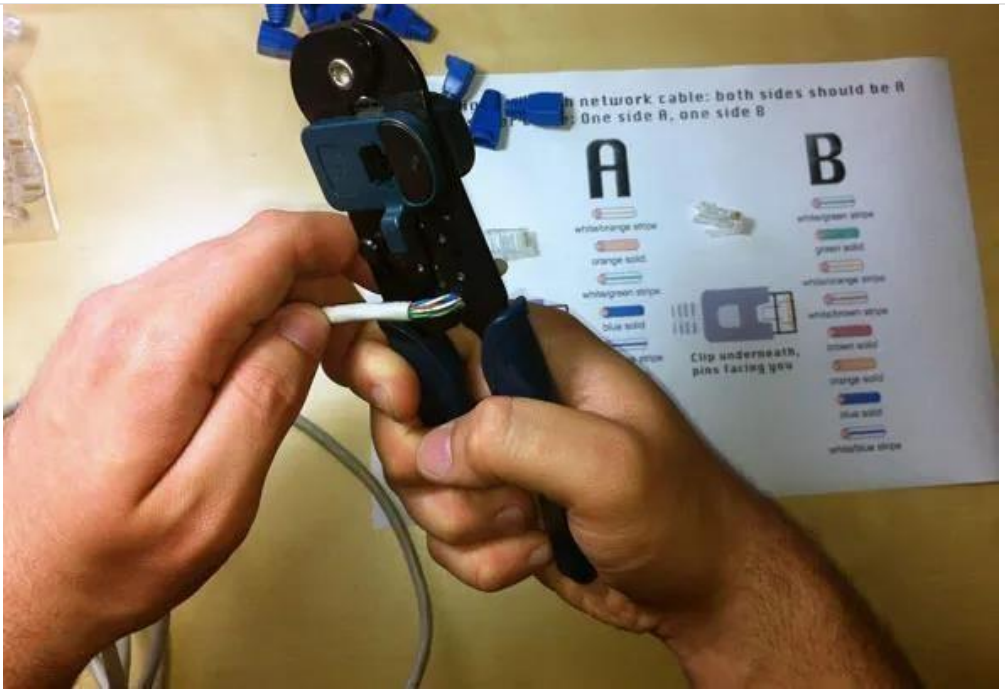
231801030

CS23532 - COMPUTER NETWORKS

Step 1: To start construction of the device, begin by threading shields onto the cable.



Step 2: Next, strip approximately 1.5 cm of cable shielding from both ends. The crimping tool has a round area to complete this task.



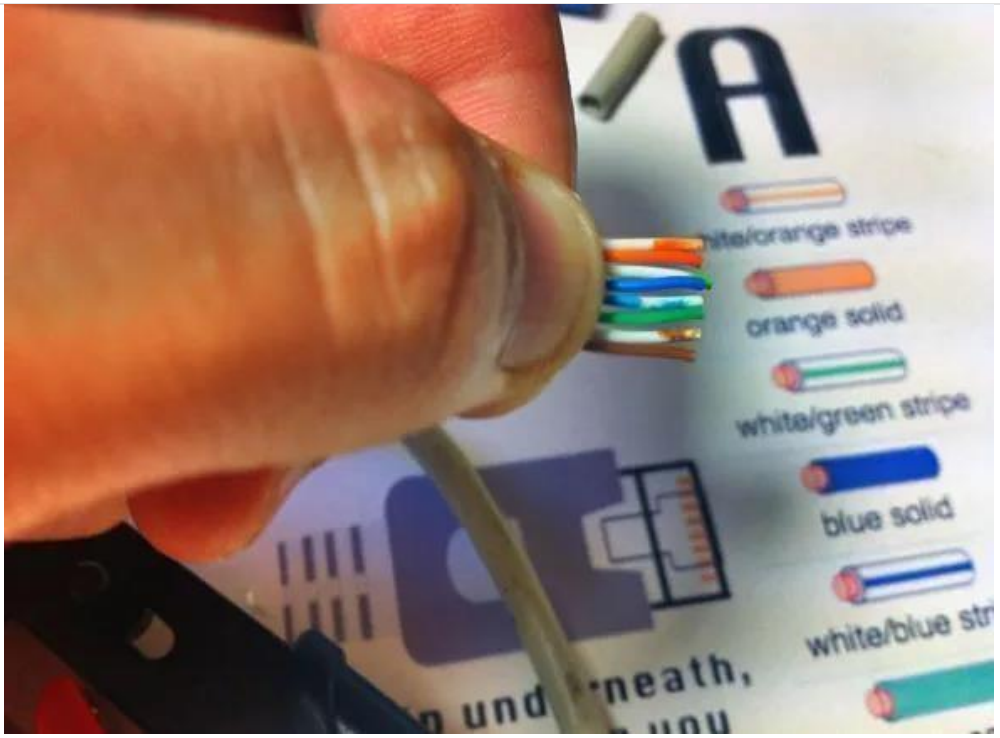
231801030

CS23532 - COMPUTER NETWORKS

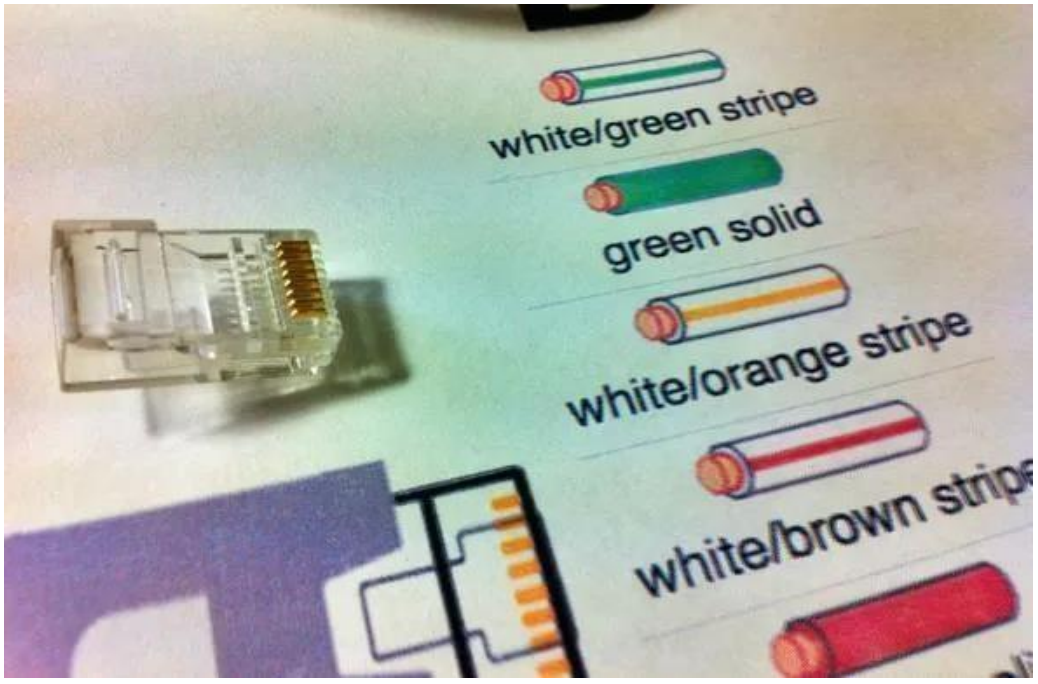
231801030

CS23532 - COMPUTER NETWORKS

Step 3: After, you will need to untangle the wires; there should be four "twisted pairs." Referencing back to the sheet, arrange them from top to bottom. One end should be in arrangement A and the other in B.



Step 4: Once the order is correct, bunch them together in a line, and if there are any that stick out farther than others, snip them back to create an even level. The difficult aspect is placing these into the RJ45 plug without messing up the order. To do so, hold the plug with the clip side facing away from you and have the gold pins facing toward you, as shown.

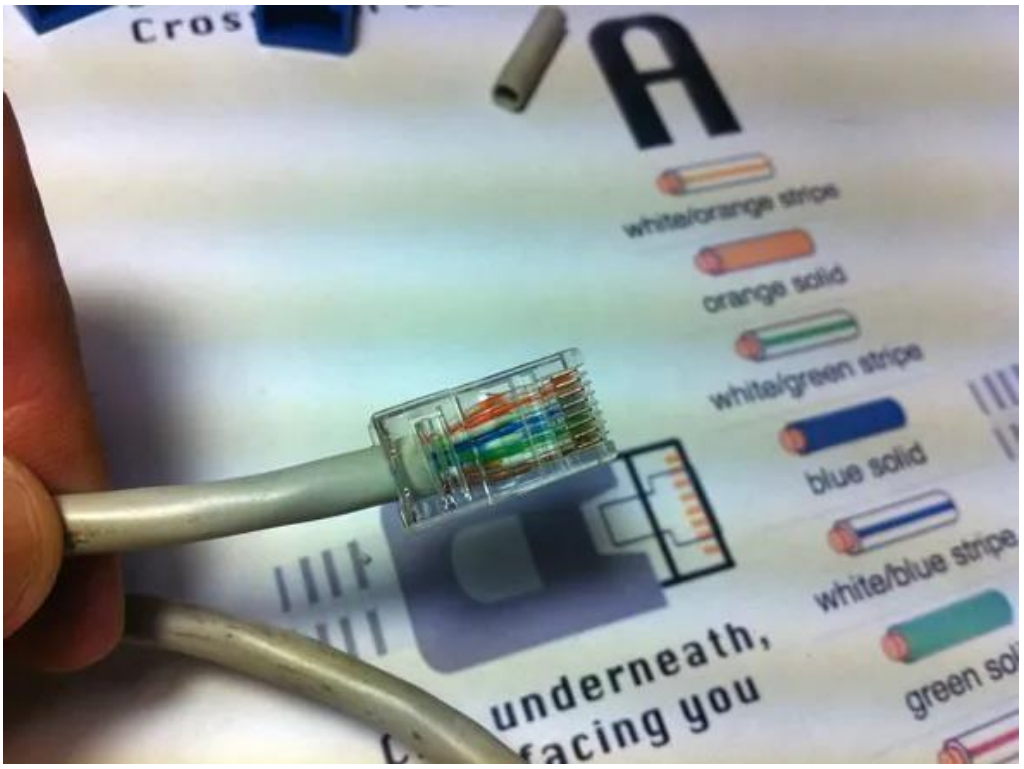


CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

Step 5: Next, push the cable right in. The notch at the end of the plug needs to be just over the cable shielding, and if it isn't, that means that you stripped off too much shielding. Simply snip the cables back a little more.



Step 6: After the wires are securely sitting inside the plug, insert it into the crimping tool and push down.
It should be shaped correctly, but pushing too hard can crack the fragile plastic plug.

Step 7: Lastly, repeat for the other end using diagram B (to make a crossover cables)/ using diagram A (to make a straight through cable)

To test it, plug it in and attempt to connect two devices directly.

Student observation:-

1. **What is the difference between cross cable and straight cable?**
2. **Which type of cable is used to connect two PC?(straight/Cross cable)**
3. **Which type cable is used to connect a router/switch to your PC? (straight/Cross cable)**
4. **Find out the category of twisted pair cable used in your la to connect the PC to the network socket.**
5. **Write down your understanding, challenges faced and output received while making a twisted pair cross/straight cable.**

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

Practical -3

AIM: To study the Packet tracer tool Installation and User Interface Overview

c) To understand environment of CISCO PACKET TRACER to design simple network.

INTRODUCTION:

A simulator, as the name suggests, simulates network devices and its environment. Packet Tracer is an exciting network design, simulation and modelling tool.

1. It allows you to model complex systems without the need for dedicated equipment.
2. It helps you to practice your network configuration and troubleshooting skills via computer or an Android or iOS based mobile device.
3. It is available for both the Linux and Windows desktop environments.
4. Protocols in Packet Tracer are coded to work and behave in the same way as they would on real hardware.

INSTALLING PACKET TRACER:

To download Packet Tracer, go to **https://www.netacad.com** and log in with your Cisco Networking Academy credentials; then, click on the Packet Tracer graphic and download the package appropriate for your operating system. (Can be used to download in your laptop).

Windows

Installation in Windows is pretty simple and straightforward; the setup comes in a single file named Packettracer_Setup6.0.1.exe. Open this file to begin the setup wizard, accept the license agreement, choose a location, and start the installation.

Linux

Linux users with an Ubuntu/Debian distribution should download the file for Ubuntu, and those using Fedora/Redhat/CentOS must download the file for Fedora. Grant executable permission to this file by using chmod, and execute it to begin the installation.

```
chmod +x PacketTracer601_i386_installer-rpm.bin
        ./PacketTracer601_i386_installer-rpm.bin
```

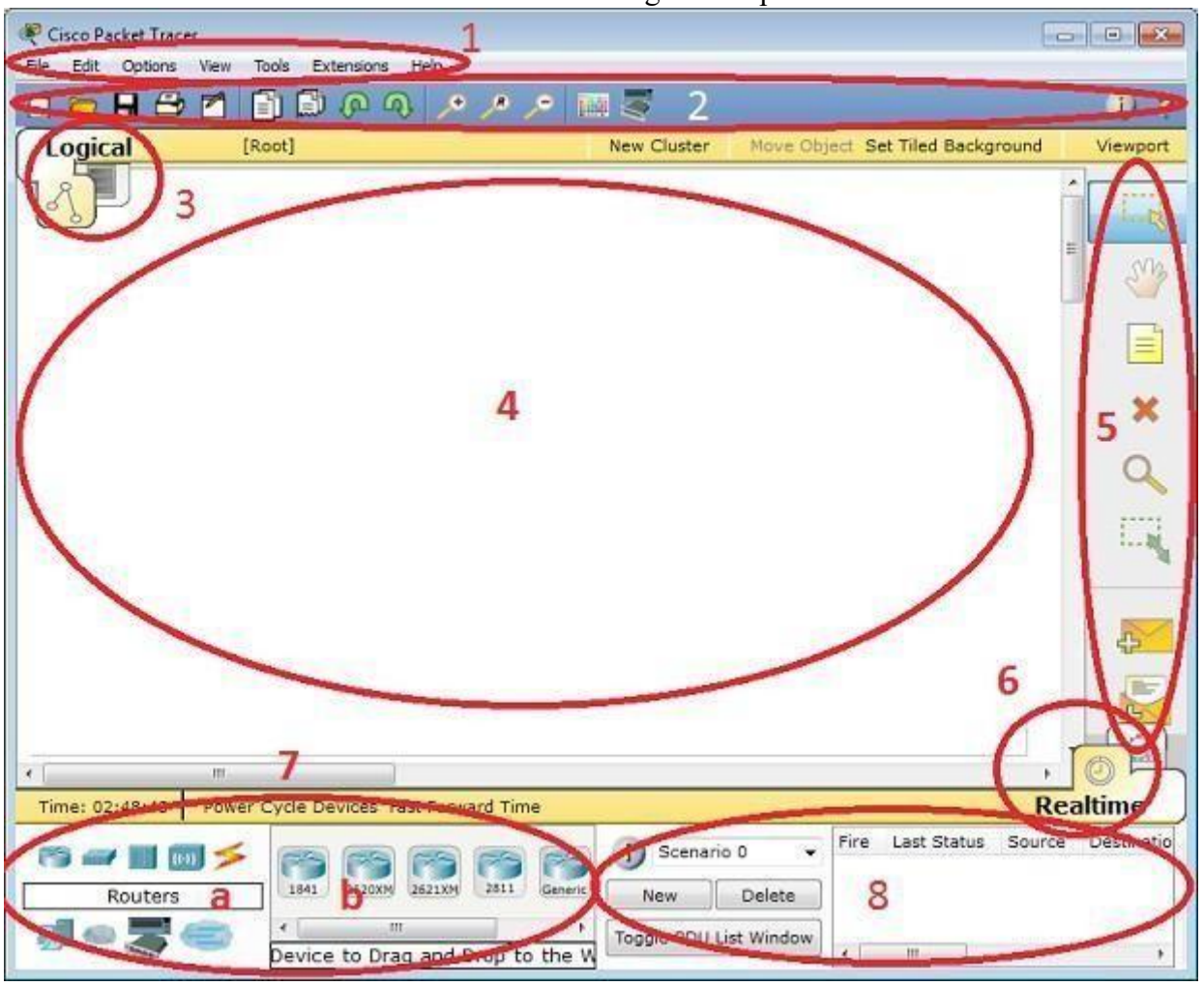
CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

USER INTERFACE OVERVIEW:

The layout of Packet Tracer is divided into several components. The components of the Packet Tracer interface are as follows: match the numbering with explanations.



1. Menu bar – This is a common menu found in all software applications; it is used to open, save, print, change preferences, and so on.
2. Main toolbar – This bar provides shortcut icons to menu options that are commonly accessed, such as open, save, zoom, undo, and redo, and on the right-hand side is an icon for entering network information for the current network.
3. Logical/Physical workspace tabs – These tabs allow you to toggle between the Logical and Physical work areas.
4. Workspace – This is the area where topologies are created and simulations are displayed.
5. Common tools bar – This toolbar provides controls for manipulating topologies, such as select, move layout, place note, delete, inspect, resize shape, and add simple/complex PDU.
6. Real-time/Simulation tabs – These tabs are used to toggle between the real and simulation modes. Buttons are also provided to control the time, and to capture the packets.
7. Network component box – This component contains all of the network and end devices available with Packet Tracer, and is further divided into two areas: Area 7a: Device-type selection box – This area contains device categories Area 7b: Device-specific selection box – When a device category is selected, this selection box displays the different device models within that category

CS23532 - COMPUTER NETWORKS

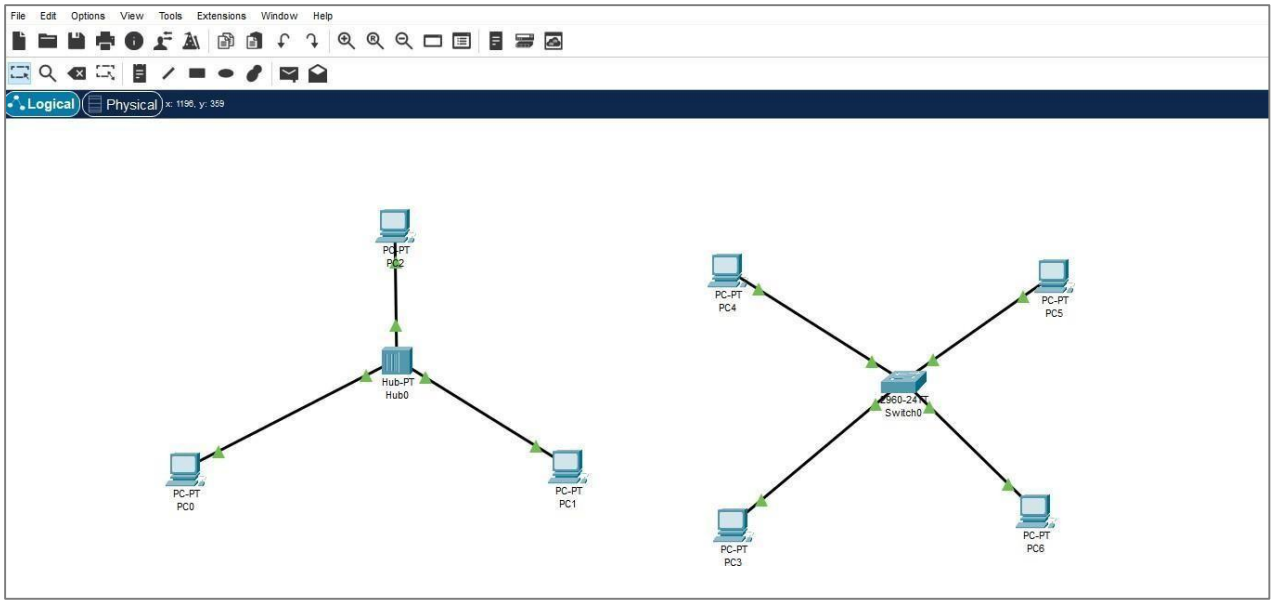
231801030

8. User-created packet box – Users can create highly-customized packets to test their topology from this area, and the results are displayed as a list.

d) Analyse the behaviour of network devices using CISCO PACKET TRACER simulator.

1. From the network component box, click and drag-and-drop the below components:
    a. 4 Generic PCs and One HUB
    b. 4 Generic PCs and One switch

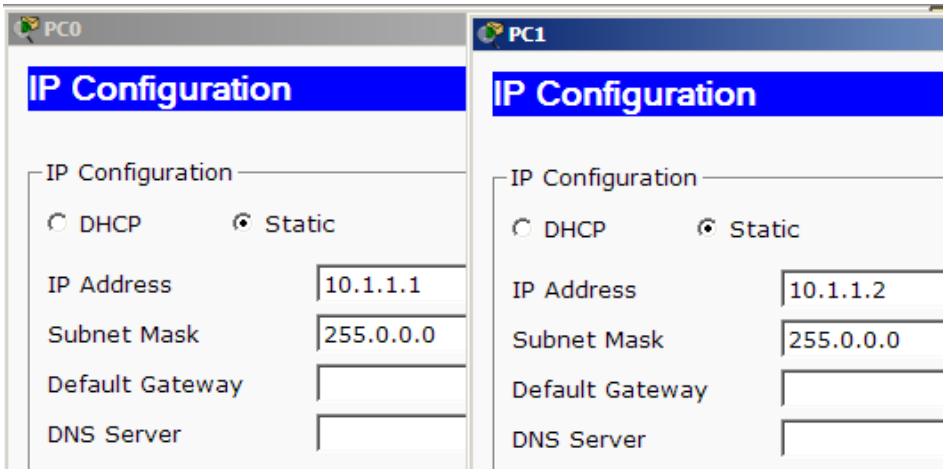
2. Click on Connections:
    a. Click on Copper Straight-Through cable,
    b. Select one of the PC and connect it to HUB using the cable. The link LED should glow in green, indicating that the link is up. Similarly connect remaining 3 PCs to the HUB.
    c. Similarly connect 4 PCs to the switch using copper straight-through cable.



CS23532 - COMPUTER NETWORKS

231801030

3. Click on the PCs connected to hub, go to the Desktop tab, click on IP Configuration, and enter an IP address and subnet mask. Here, the default gateway and DNS server information is not needed as there are only two end devices in the network.



Click on the PDU (message icon) from the common tool bar,

a. Drag and drop it on one of PC (source machine) and then drop it on another PC (destination machine) connected to the HUB.

4. Observe the flow of PDU from source PC to destination PC by selecting the Realtime mode of simulation.

5. Repeat step #3 to step #5 for the PCs connected to the switch.

6. Observe how HUB and switch are forwarding the PDU and write your observation and conclusion about the behaviors of Switch and HUB.

Student observation:

a. From your observation write down the behavior of Switch and HUB in terms of forwarding the packets received by them.

b. Find out the network topology implemented in your college and draw and label that topology in your observation book.

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

Practical -4

AIM: Setup and configure a LAN (Local area network) using a Switch and Ethernet cables in your lab.

What is a LAN?

A Local Area Network (LAN) refers to a network that connects devices within a limited area, such as an office building, school, or home. It enables users to share resources, including data, printers, and internet access. LAN connects devices to promote collaboration and transfer information between users, such as computers, printers, servers, and switches. A local area network (LAN) switch serves as the primary connecting device, managing and directing communications within the local network. Each connected device on a LAN switch can communicate directly with each other, allowing for fast and secure data transfer.

How to set up a LAN

Step 1. Plan and Design an appropriate network topology taking into account network requirements and equipment location.

Step 2. You can take 4 Computers, a Switch with 8, 16, or 24 ports which is sufficient for networks of these sizes, and 4 Ethernet cables.

Step3: Connect your computers to network switch via an Ethernet cable, which is as simple as plugging one end of the Ethernet cable into your computer and the other end into your network switch.

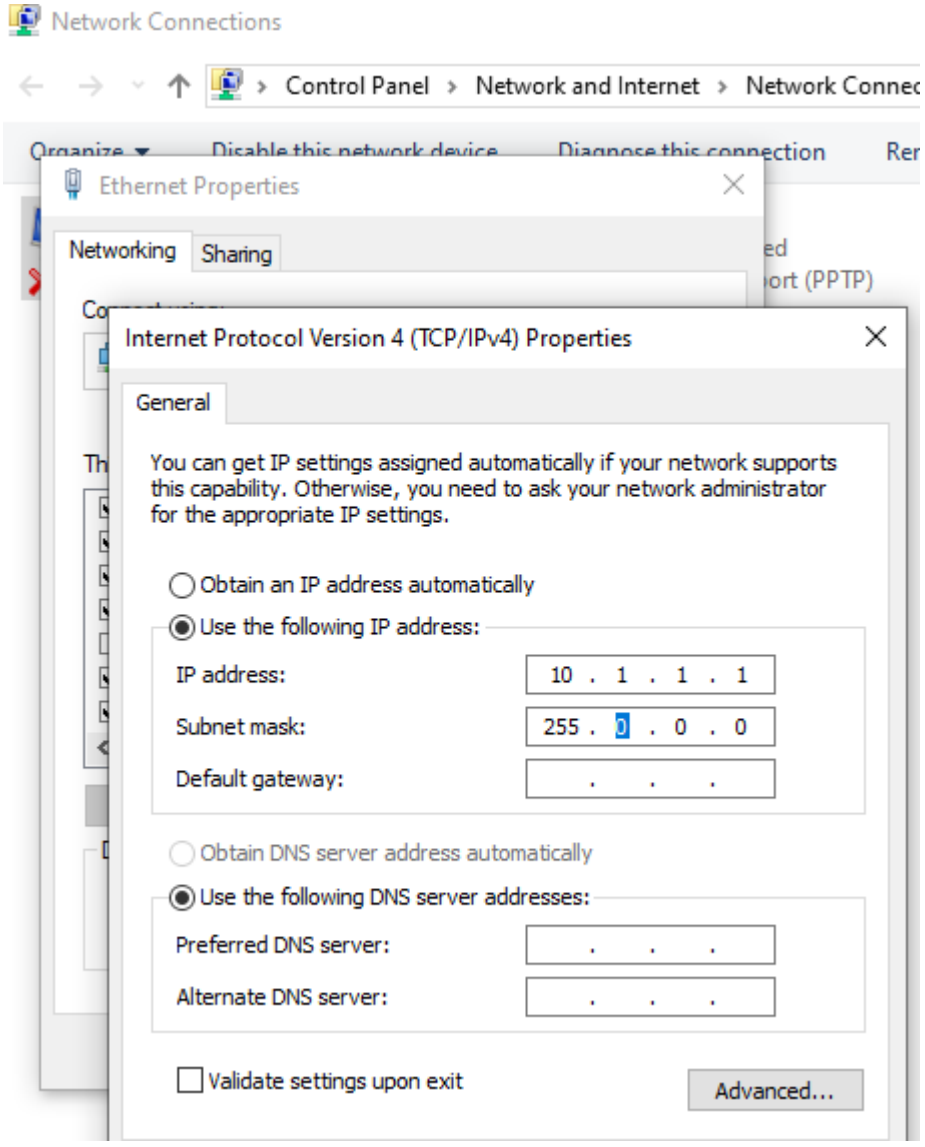
Step4: Assign IP address to your PCs

1. Log on to the client computer as Administrator or as Owner.
2. Click Network and Internet Connections.
3. Right Click Local Area Connection/Ethernet->Go to Properties->Select Internet Protocol (TCP/IPv4)->Click on Properties->Select use the following ip address option and assign ipaddress.

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS



Similarly assign IP address to all the PCS connected to switch.
PC1-IP address: 10.1.1.1, subnet mask 255.0.0.0
PC2-IP address-10.1.1.2, subnet mask 255.0.0.0
PC3-IP address 10.1.1.3, subnet mask 255.0.0.0.
PC4-IP address 10.1.1.4, subnet mask 255.0.0.0.

Step 5:- Configure a network switch:

1. Connect your computer to the switch: To access the switch's web interface, you will need to connect your computer to the switch using an Ethernet cable.
2. Log in to the web interface: Open a web browser and enter the IP address of the switch in the address bar. This should bring up the login page for the switch's web interface. Enter the username and password to log in.
3. Configure basic settings: Once you're logged in, you will be able to configure basic settings for the switch,
4. Assign IP address as: 10.1.1.5, subnet mask 255.0.0.0.

Step 6:- Check the connectivity between switch and other machine by using ping command in the command prompt of the device.

CS23532 - COMPUTER NETWORKS

231801030

Step 7: Select a folder, ->go to properties-> click Sharing tab->share it with everyone on the same LAN.

Step 8. Try to access the shared folder from others Computers of the network.

Student observation:

Draw a neat diagram of the LAN in the configuration observation book. that you have implemented in your lab. Write the ip configuration of each and every device. Write the outcome and challenges faced while configuring the LAN.

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

Practical-5

AIM Experiments on Packet capture tool: Wireshark

Packet Sniffer

- Sniffs messages being sent/received from/by your computer
- Store and display the contents of the various protocol fields in the messages
- Passive program
  - never sends packets itself
  - no packets addressed to it
  - receives a copy of all packets (sent/received)

Packet Sniffer Structure Diagnostic Tools

- Tcpdump
  - E.g. tcpdump -enx host 10.129.41.2 -w exe3.out
- Wireshark
  - wireshark -r exe3.out

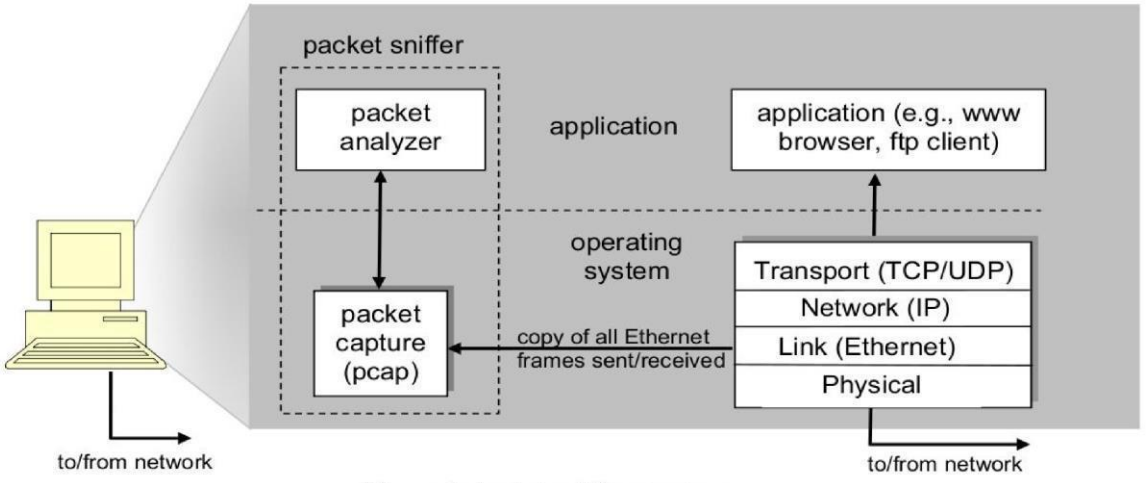


Figure 1: Packet sniffer structure

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

DESCRIPTION:

WIRESHARK

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets. You can use Wireshark to inspect a suspicious program's network traffic, analyze the traffic flow on your network, or troubleshoot network problems.

What we can do with Wireshark:

- Capture network traffic
- Decode packet protocols using dissectors
- Define filters – capture and display
- Watch smart statistics
- Analyze problems
- Interactively browse that traffic

Wireshark used for:

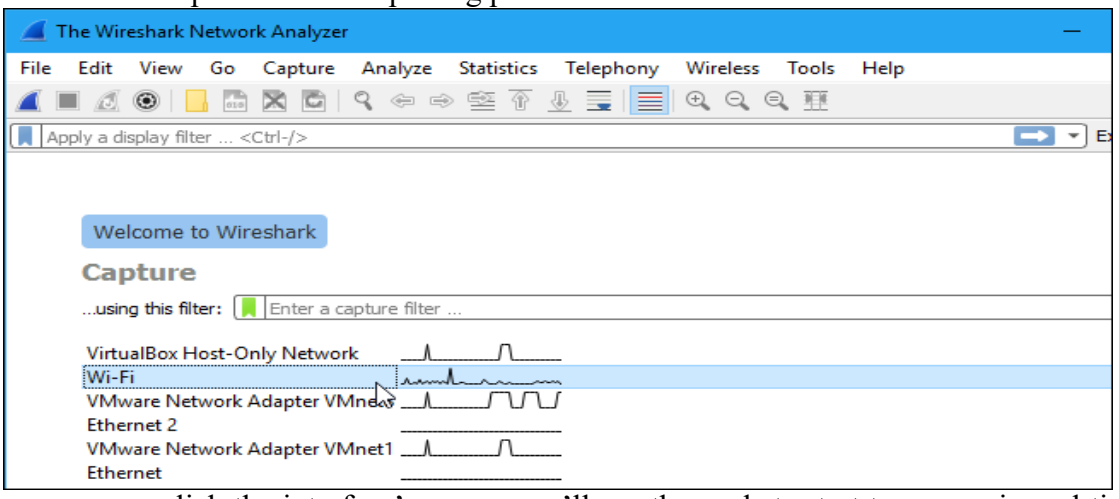
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

Getting Wireshark

Wireshark can be downloaded for Windows or macOS from its official website. For Linux or another UNIX-like system, Wireshark will be found in its package repositories. For Ubuntu, Wireshark will be found in the Ubuntu Software Center.

Capturing Packets

After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface



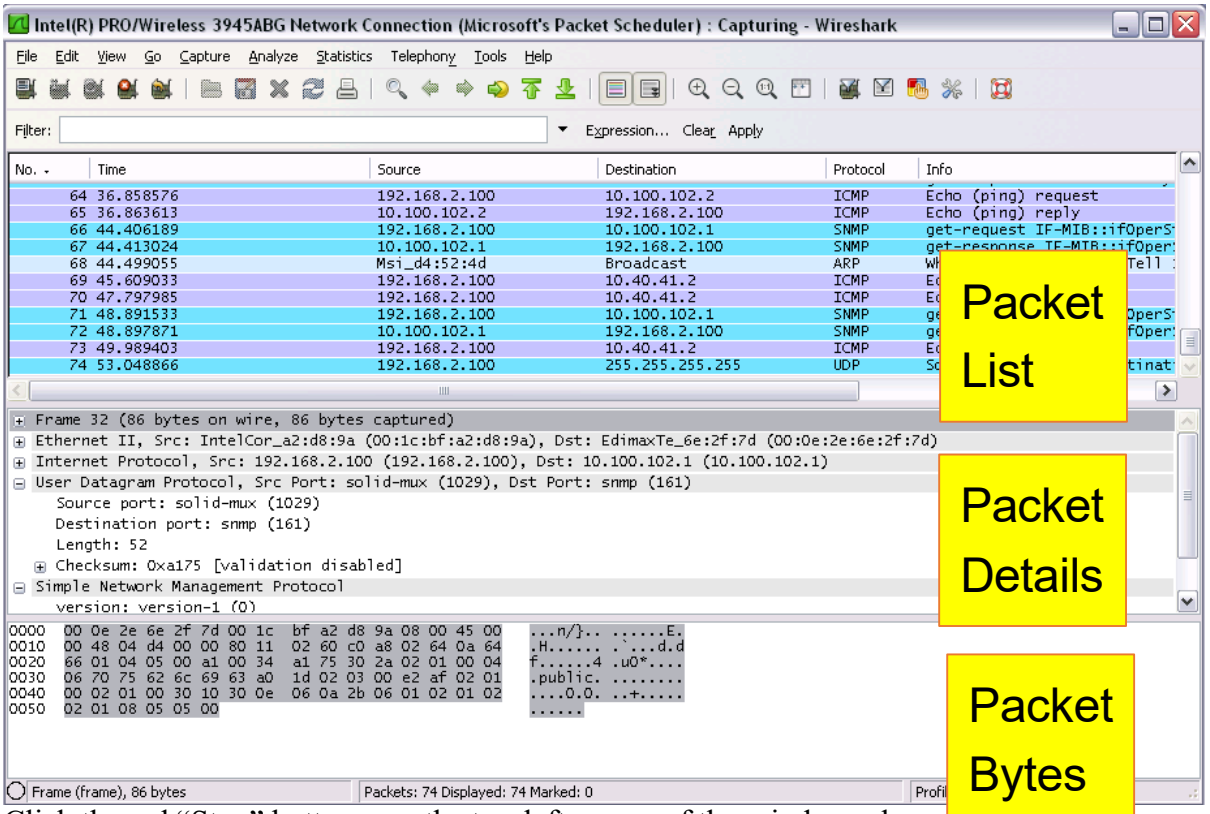
As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS



Click the red "Stop" button near the top left corner of the window wh e o stop capturing traffic.

The "Packet List" Pane

The packet list pane displays all the packets in the current capture file. The "Packet List" pane Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the "Packet Details" and "Packet Bytes" panes.

The "Packet Details" Pane

The packet details pane shows the current packet (selected in the "Packet List" pane) in a more detailed form. This pane shows the protocols and protocol fields of the packet selected in the "Packet List" pane. The protocols and fields of the packet shown in a tree which can be expanded and collapsed.

The "Packet Bytes" Pane

The packet bytes pane shows the data of the current packet (selected in the "Packet List" pane) in a hexdump style.

Color Coding

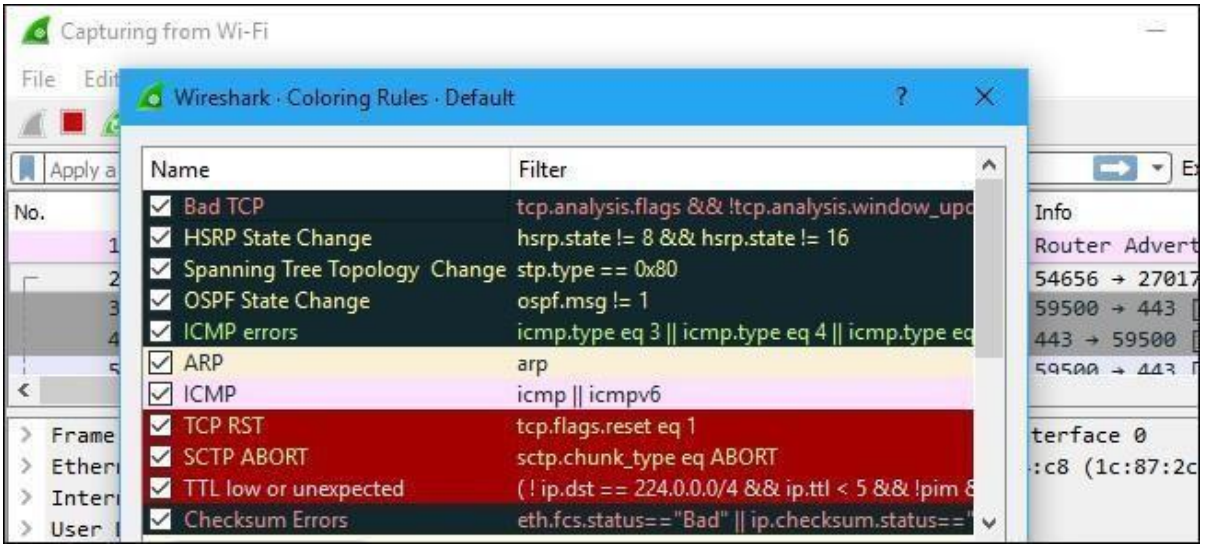
You'll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.

CS23532 - COMPUTER NETWORKS

231801030

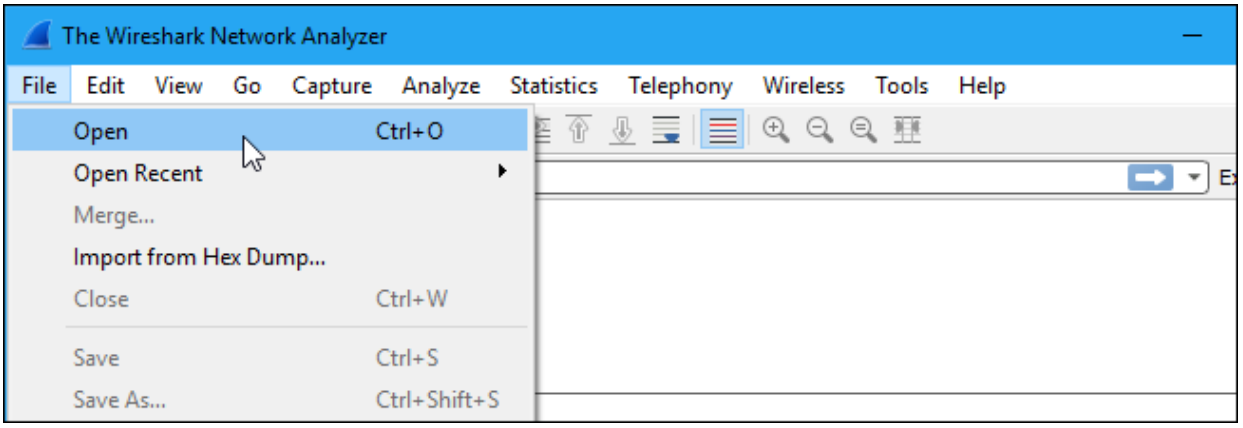
CS23532 - COMPUTER NETWORKS



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



Filtering Packets

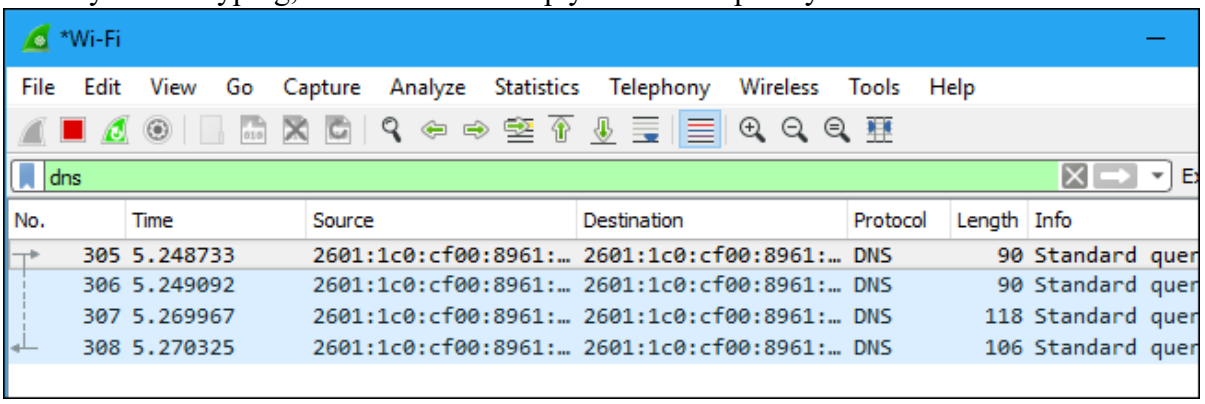
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

CS23532 - COMPUTER NETWORKS

231801030

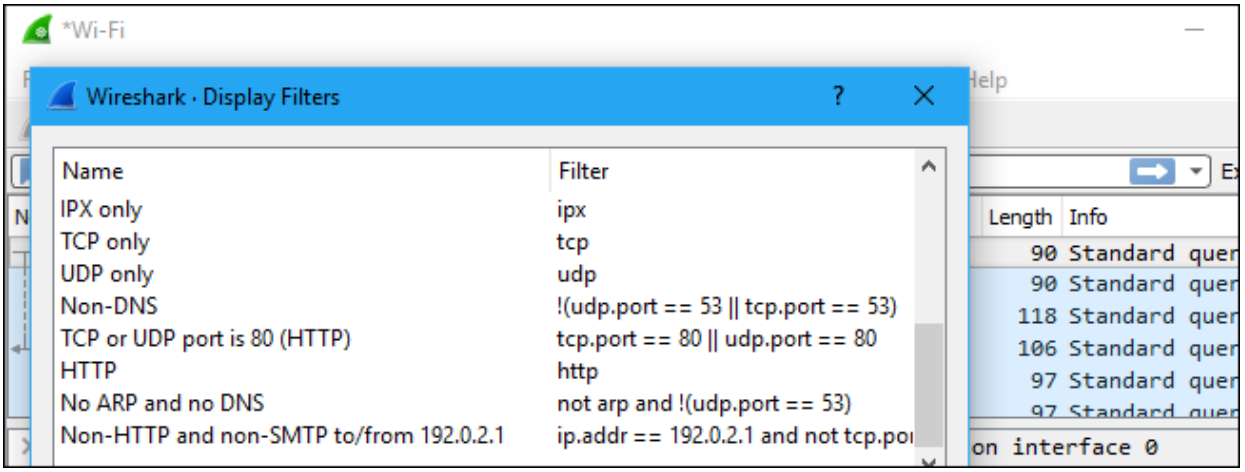
CS23532 - COMPUTER NETWORKS

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type “dns” and you’ll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

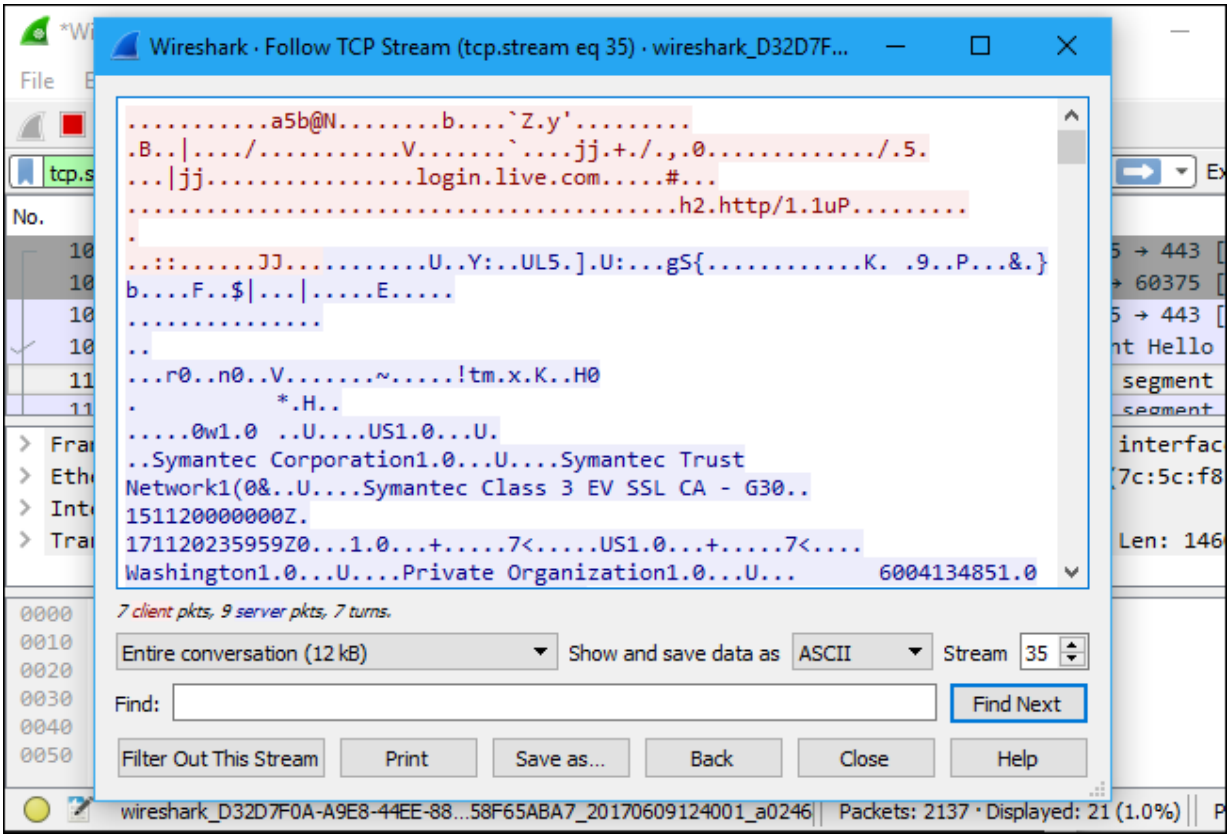
For more information on Wireshark’s display filtering language, read the Building display filter expressions page in the official Wireshark documentation.



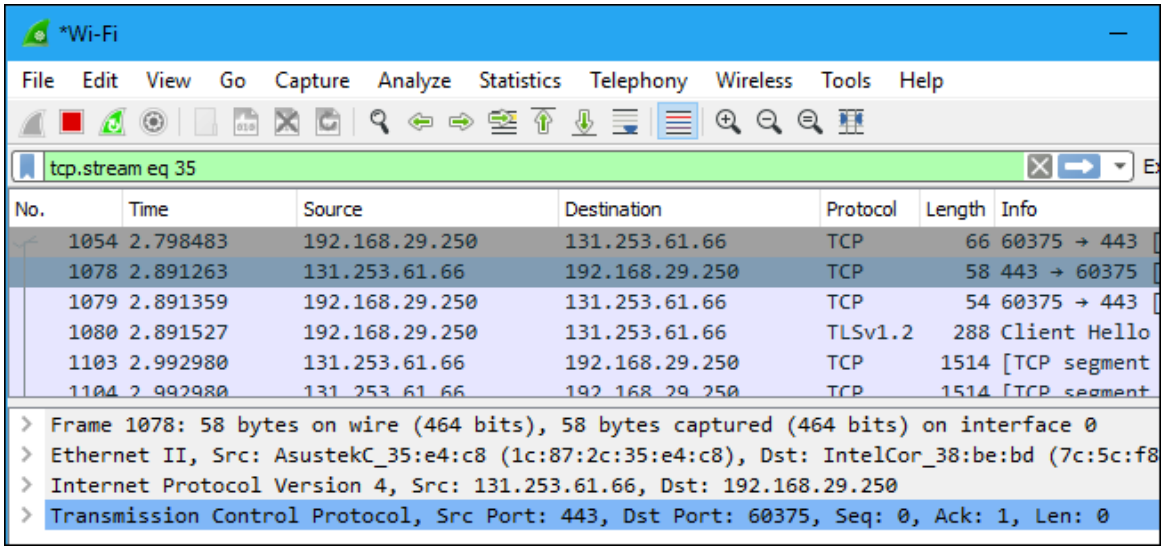
Another interesting thing you can do is right-click a packet and select Follow > TCP Stream. You’ll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.

CS23532 - COMPUTER NETWORKS

231801030



Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.



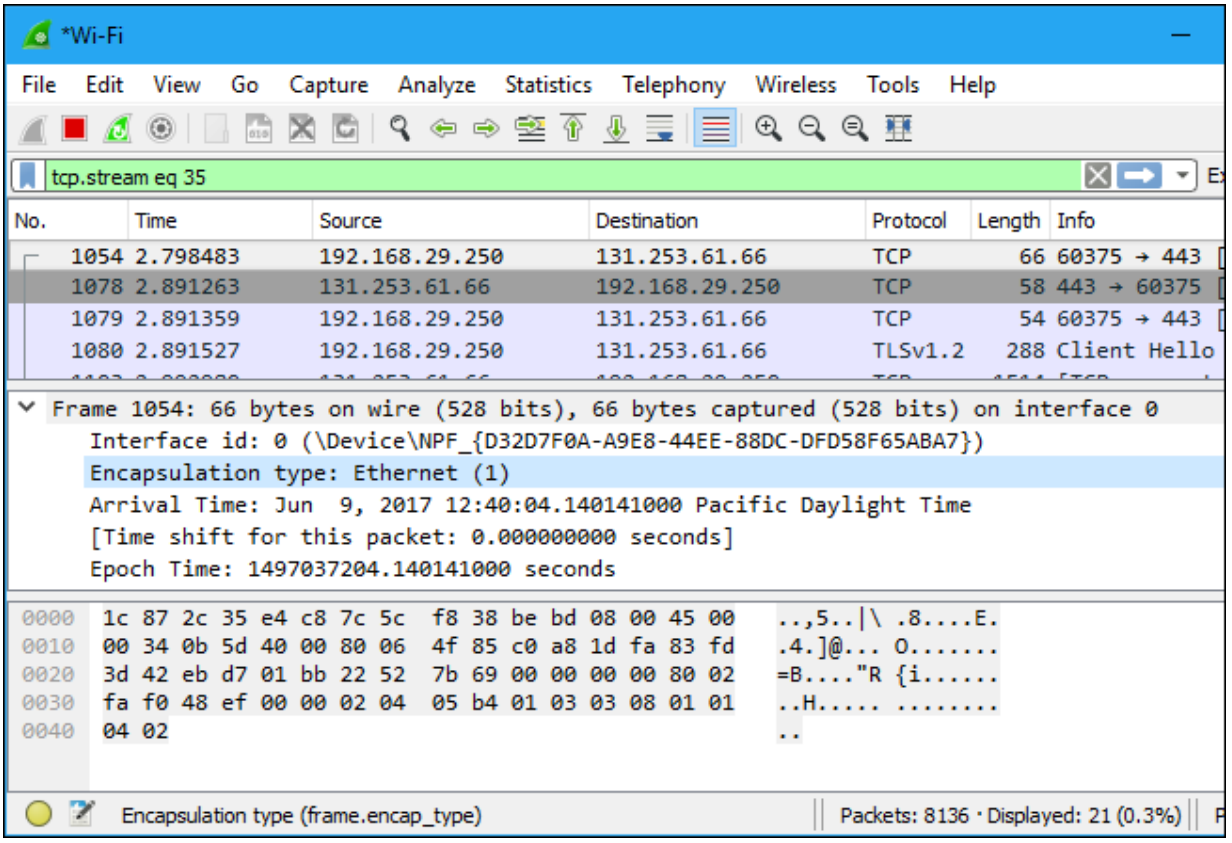
Inspecting Packets

Click a packet to select it and you can dig down to view its details.

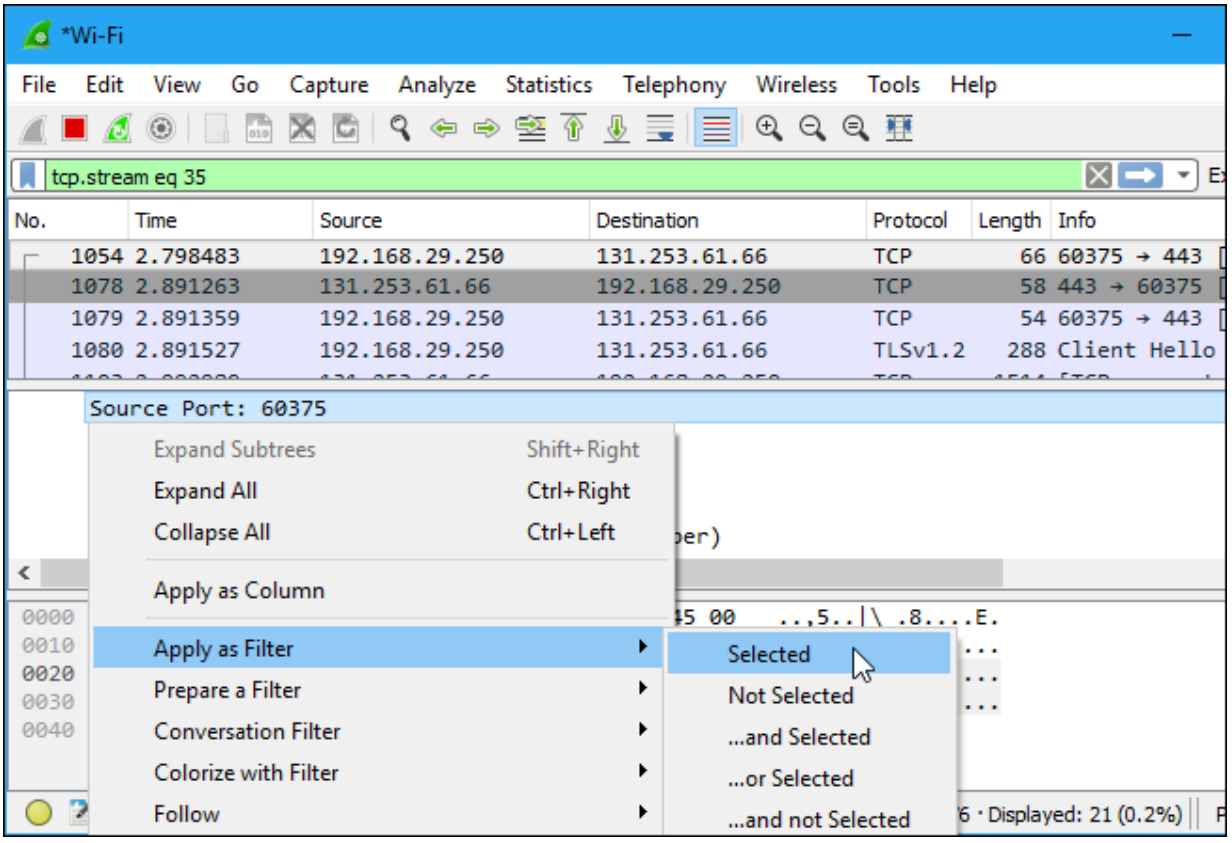
CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS



You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



231801030

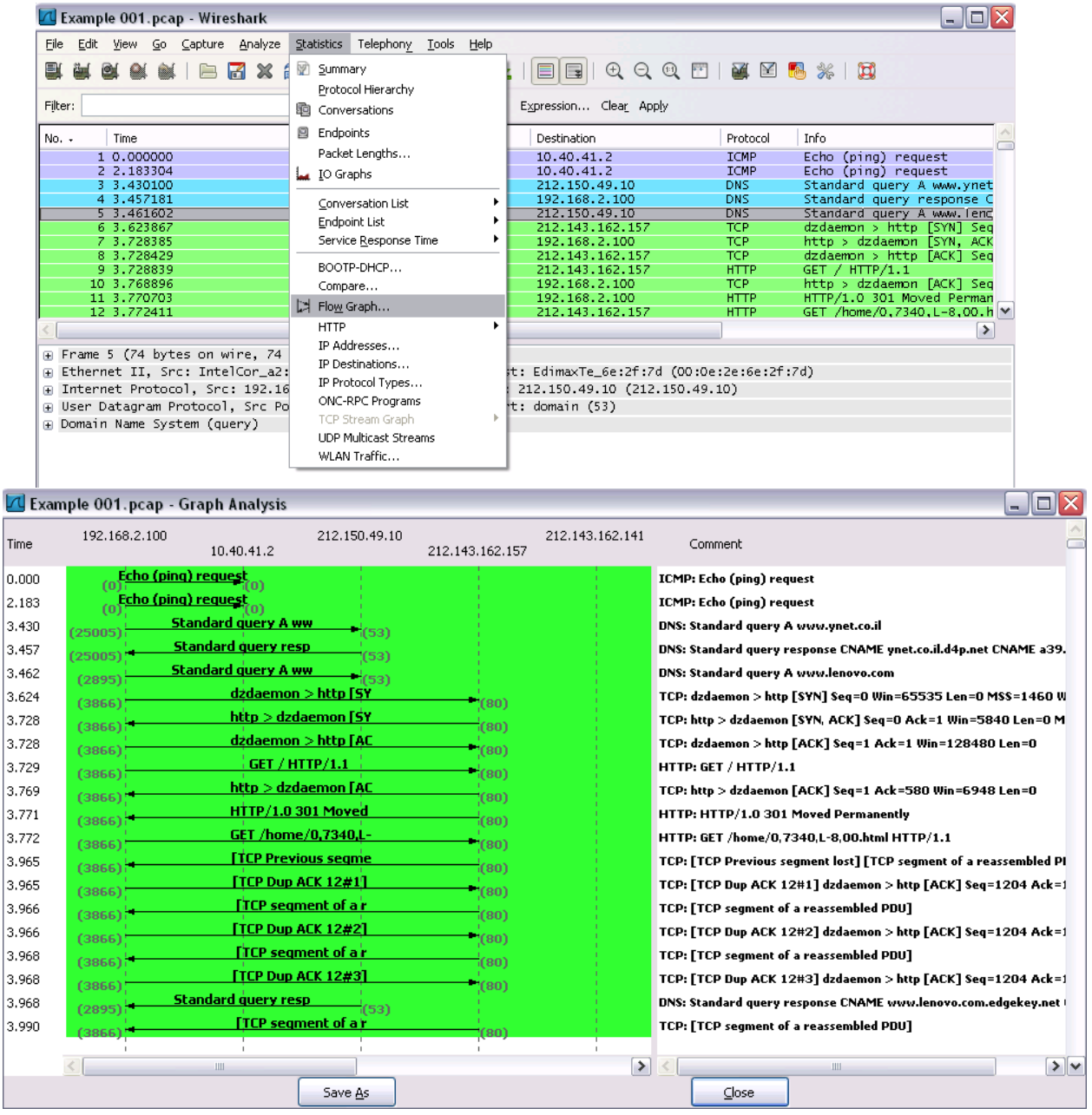
CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

Flow Graph: Gives a better understanding of what we see.



231801030

CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS

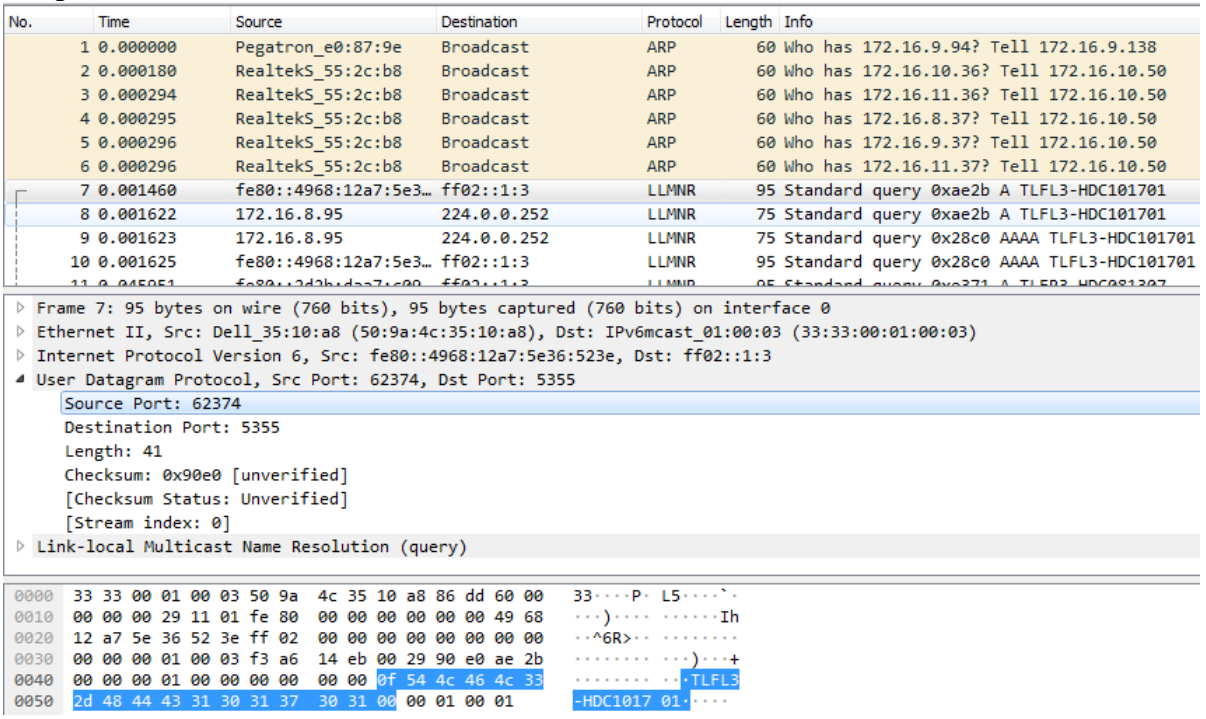
CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL

To filter, capture, view, packets in Wireshark Tool.
Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture → option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Save the packets.

Output



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Pegatron_e0:87:9e	Broadcast	ARP	60	Who has 172.16.9.94? Tell 172.16.9.138
2	0.000180	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.10.36? Tell 172.16.10.50
3	0.000294	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.11.36? Tell 172.16.10.50
4	0.000295	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.8.37? Tell 172.16.10.50
5	0.000296	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.9.37? Tell 172.16.10.50
6	0.000296	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.11.37? Tell 172.16.10.50
7	0.001460	fe80::4968:12a7:5e3…	ff02::1:3	LLMNR	95	Standard query 0xae2b A TLFL3-HDC101701
8	0.001622	172.16.8.95	224.0.0.252	LLMNR	75	Standard query 0xae2b A TLFL3-HDC101701
9	0.001623	172.16.8.95	224.0.0.252	LLMNR	75	Standard query 0x28c0 AAAA TLFL3-HDC101701
10	0.001625	fe80::4968:12a7:5e3…	ff02::1:3	LLMNR	95	Standard query 0x28c0 AAAA TLFL3-HDC101701

```
▷ Frame 7: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
▷ Ethernet II, Src: Dell_35:10:a8 (50:9a:4c:35:10:a8), Dst: IPv6mcast_01:00:03 (33:33:00:01:00:03)
▷ Internet Protocol Version 6, Src: fe80::4968:12a7:5e36:523e, Dst: ff02::1:3
◢ User Datagram Protocol, Src Port: 62374, Dst Port: 5355
    Source Port: 62374
    Destination Port: 5355
    Length: 41
    Checksum: 0x90e0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▷ Link-local Multicast Name Resolution (query)
```

```
0000  33 33 00 01 00 03 50 9a  4c 35 10 a8 86 dd 60 00   33····P· L5····`·
0010  00 00 00 29 11 01 fe 80  00 00 00 00 00 00 49 68   ···)···· ·····Ih
0020  12 a7 5e 36 52 3e ff 02  00 00 00 00 00 00 00 00   ··^6R>·· ········
0030  00 00 00 01 00 03 f3 a6  14 eb 00 29 90 e0 ae 2b   ········ ···)···+
0040  00 00 00 01 00 00 00 00  00 00 0f 54 4c 46 4c 33   ········ ···TLFL3
0050  2d 48 44 43 31 30 31 37  30 31 00 00 01 00 01      -HDC1017 01·····
```

1. **Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph**

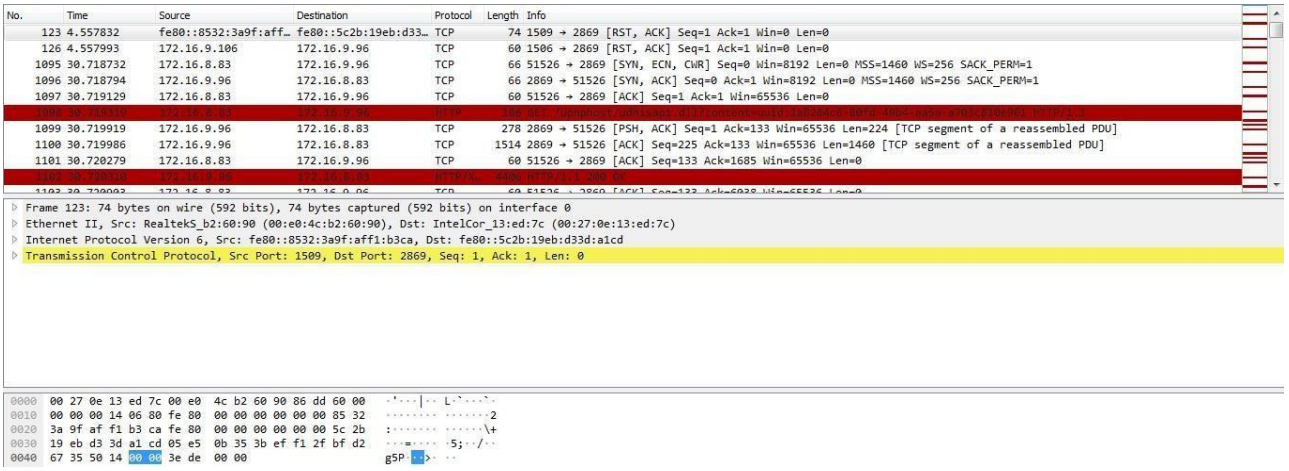
Procedure

- Select Local Area Connection in Wireshark.
- Go to capture → option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics→Flow graph.
- Save the packets.

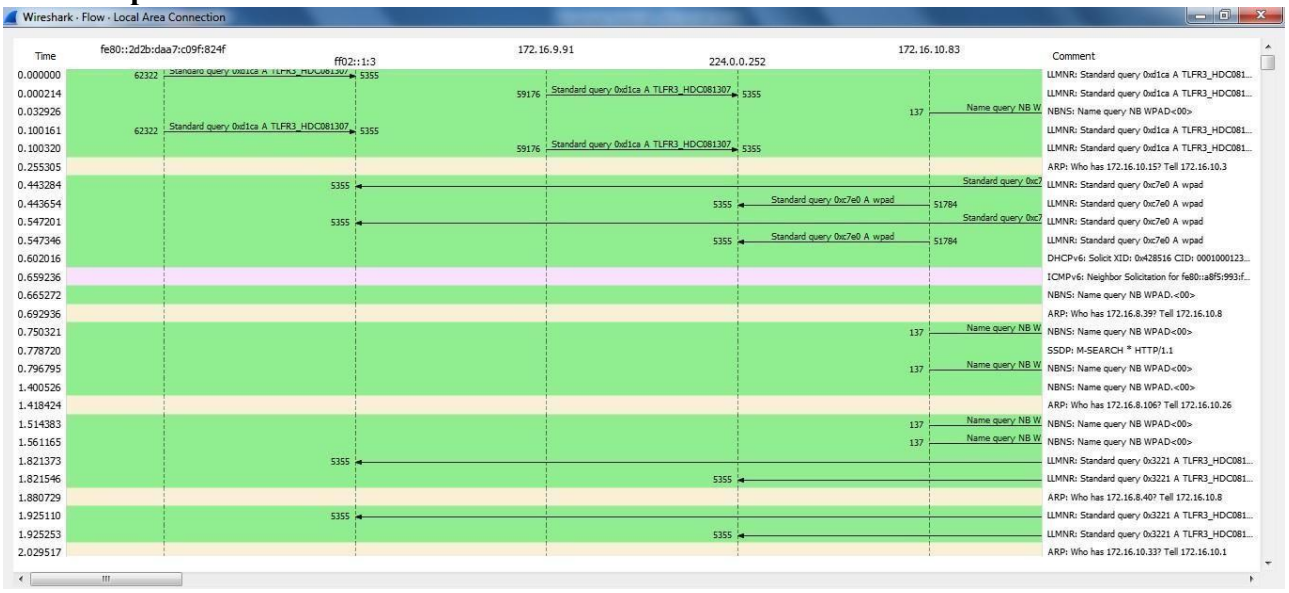
CS23532 - COMPUTER NETWORKS

231801030

CS23532 - COMPUTER NETWORKS



Flow Graph



2. Create a Filter to display only ARP packets and inspect the packets.

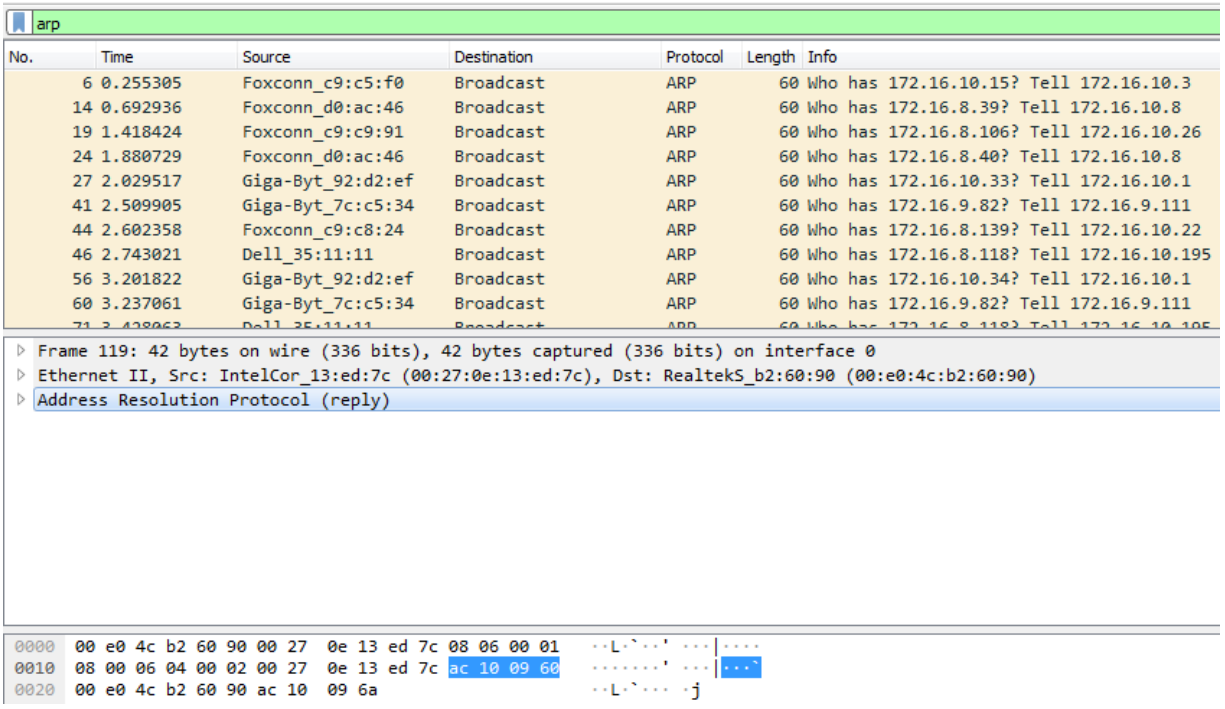
Procedure

- Go to capture → option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ARP packets in search bar.
- Save the packets.

CS23532 - COMPUTER NETWORKS

231801030

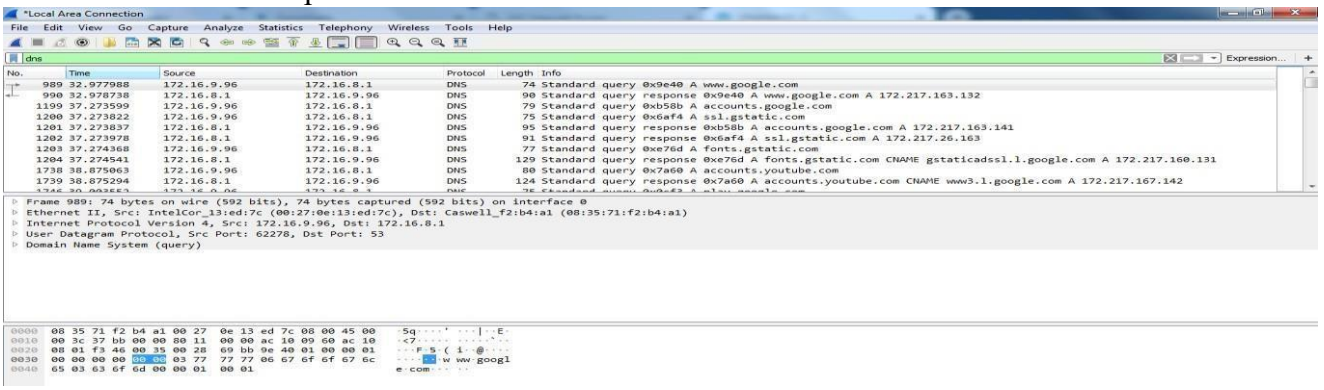
Output



3. Create a Filter to display only DNS packets and provide the flow graph.

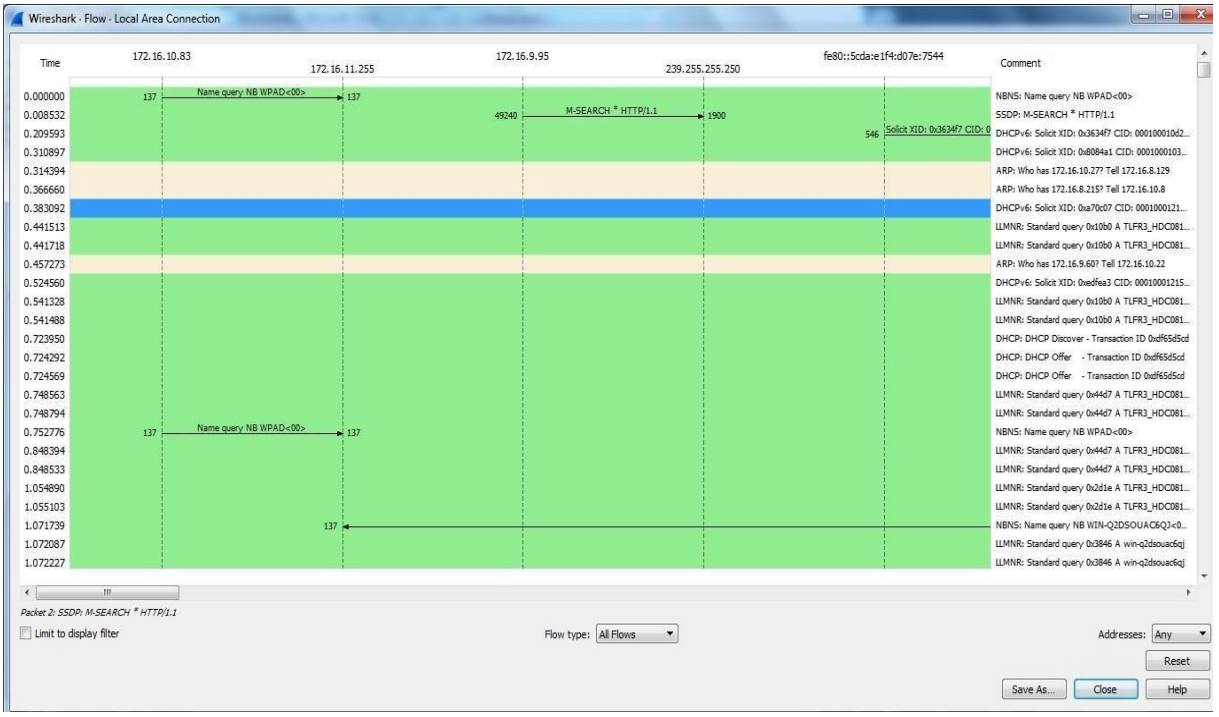
Procedure

- Go to capture → option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics→Flow graph.
- Save the packets.



CS23532 - COMPUTER NETWORKS

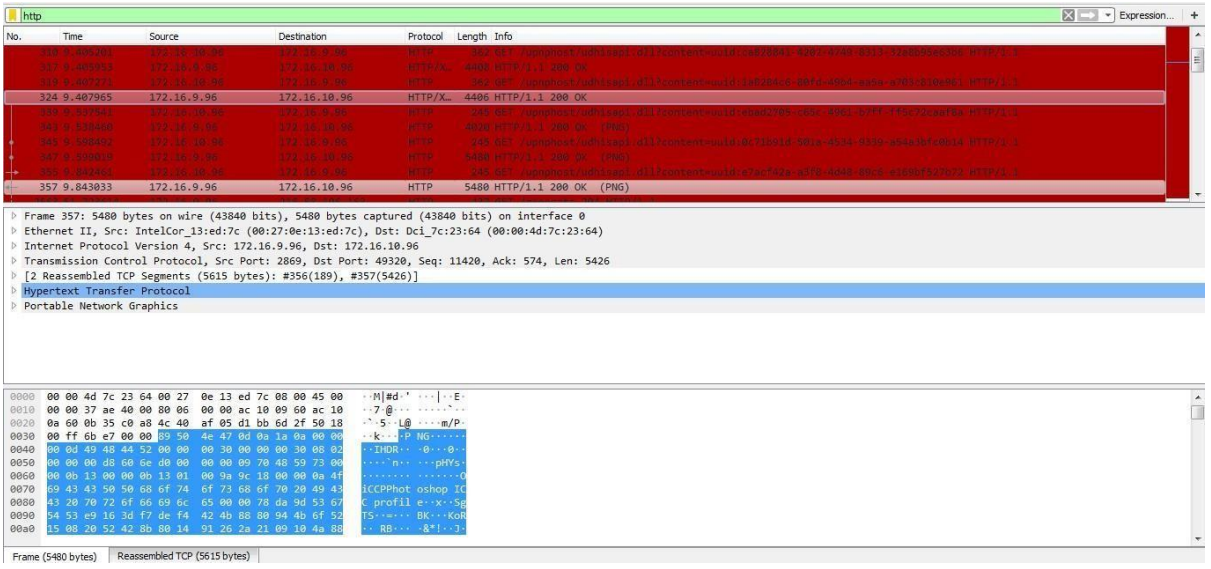
231801030



4. Create a Filter to display only HTTP packets and inspect the packets

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture → option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search HTTP packets in search bar.
- Save the packets.



CS23532 - COMPUTER NETWORKS

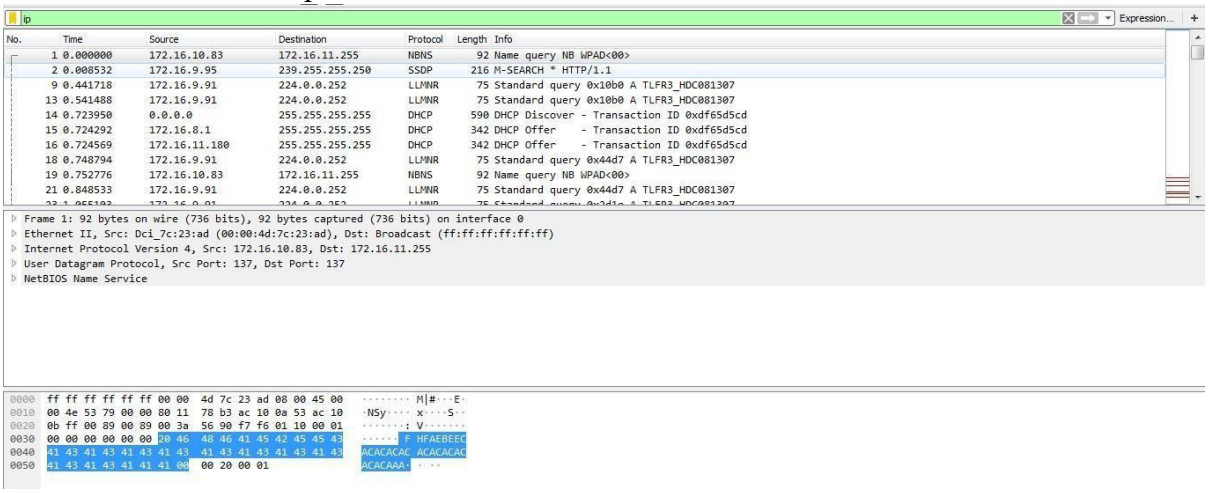
231801030

CS23532 - COMPUTER NETWORKS

5. Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture → option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ICMP/IP packets in search bar.
- Save the packets

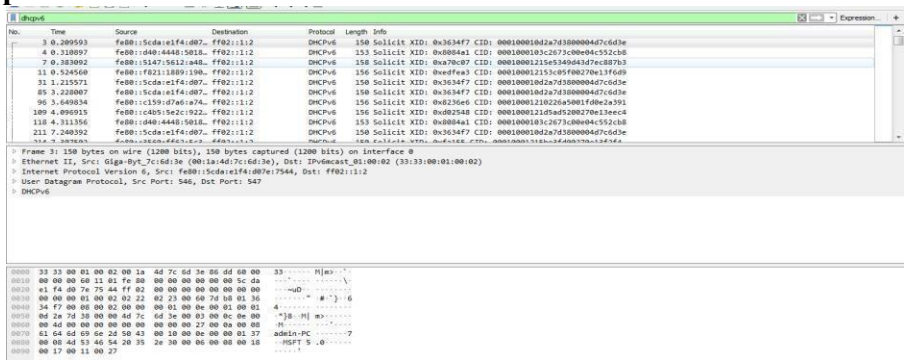


6. Create a Filter to display only DHCP packets and inspect the packets.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture → option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DHCP packets in search bar.
- Save the packets

Output



Student observation:

1. **What is promiscuous mode?**
2. **Does ARP packets has transport layer header? Explain.**
3. **Which transport layer protocol is used by DNS?**
4. **What is the port number used by http protocol?**
5. **What is a broadcast ip address?**

231801030

CS23532 - COMPUTER NETWORKS

231801030

CS19541-COMPUTER NETWORKS-LAB MANUAL

Practical-6

AIM: Write a program to implement error detection and correction using HAMMING code concept. Make a test run to input data stream and verify error correction feature.

Error Correction at Data Link Layer:
Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is transmitted from the sender to the receiver. It is a technique developed by R.W. Hamming for error correction.

Create sender program with below features.

1. Input to sender file should be a text of any length. Program should convert the text to binary.
2. Apply hamming code concept on the binary data and add redundant bits to it.
3. Save this output in a file called channel.

Create a receiver program with below features

1. Receiver program should read the input from Channel file.
2. Apply hamming code on the binary data to check for errors.
3. If there is an error, display the position of the error.
4. Else remove the redundant bits and convert the binary data to ascii and display the output.

Student observation:-

Write the code here:

Input:-

Output:

CS19541-COMPUTER NETWORKS-LAB MANUAL

Practical-7

AIM: Write a program to implement flow control at data link layer using SLIDING WINDOW PROTOCOL. Simulate the flow of frames from one node to another.

Program should achieve at least below given requirements. You can make it a bidirectional program wherein receiver is sending its data frames with acknowledgement (Piggybacking).

Create a sender program with following features:-

1. Input Window size from the user.
2. Input a Text message from the user.
3. Consider 1 character per frame.
4. Create a frame with following fields [Frame no., DATA].
5. Send the frames. [Print the output on screen and save it in a file called Sender_Buffer.]
6. Wait for the acknowledgement from the Receiver. [Induce delay in the program]
7. Reader a file called Receiver_Buffer.
8. Check ACK field for the Acknowledgement number.
9. If the Acknowledgement number is as expected, send new set of frames accordingly, [overwrite the Sender_Buffer file with new frames] Else if NACK is received, resend the frames accordingly. [Overwrite the Sender_Buffer with old frame].

Create a receiver file with following features

1. Reader a file called Sender_Buffer.
2. Check the Frame no.
3. If the Fame no. are as expected, write the appropriate ACK no. in the Receiver_ Buffer file. Else write NACK no. in the Receiver_Buffer file.

NOTE: Induce error and verify the behaviour of the program. Manually Change the Frame no and Ack no in the files].

Student observation:

Write the code here:

Input:

Output:

Practical-8

AIM: - To Discover Live Hosts Using Nmap Scans (ARP, ICMP, TCP/UDP) on the TryHackMe Platform Room Link :https://tryhackme.com/room/nmap01

Introduction

When targeting a network, we need an efficient tool to handle repetitive tasks. This tool should help us find out which systems are active and what services are running on those systems. The tool that we will rely on is Nmap. The first question about finding live computers is answered in this room. This room is the first in a series of four rooms dedicated to Nmap. The second question about discovering running services is answered in the next Nmap rooms that focus on port-scanning.

This room is the first of four in this Nmap series. These four rooms are also part of the Network Security module.

- Nmap Live Host Discovery
- Nmap Basic Port Scans
- Nmap Advanced Port Scans
- Nmap Post Port Scans

This room explains the steps that Nmap carries out to discover the systems that are online before port-scanning. This stage is crucial because trying to port-scan offline systems will only waste time and create unnecessary noise on the network.

We present the different approaches that Nmap uses to discover live hosts. In particular, we cover:
ARP scan: This scan uses ARP requests to discover live hosts
ICMP scan: This scan uses ICMP requests to identify live hosts
TCP/UDP ping scan: This scan sends packets to TCP ports and UDP ports to determine live hosts.

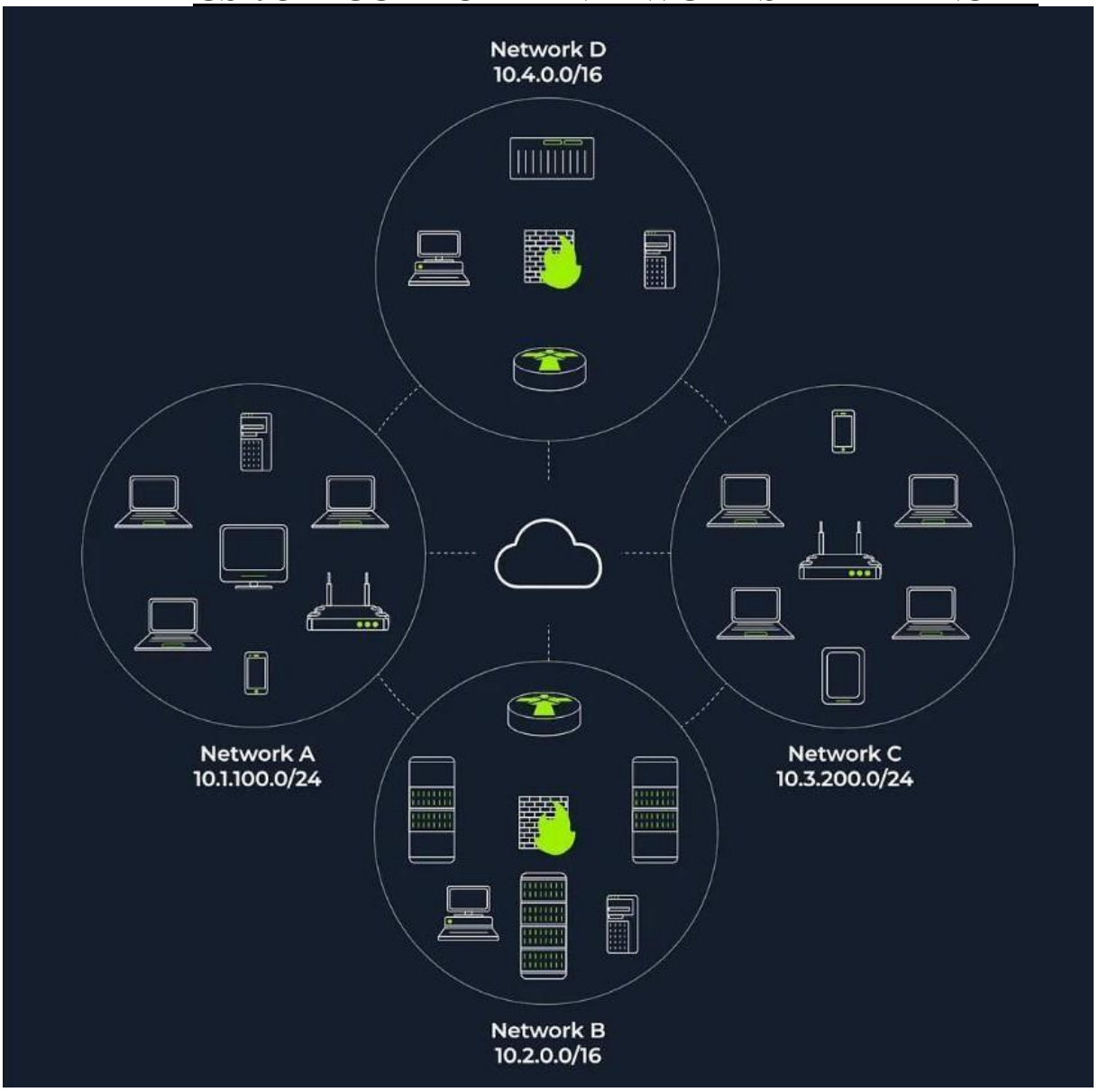
We also introduce two scanners, arp-scan and masscan, and explain how they overlap with part of Nmap's host discovery.

As already mentioned, starting with this room, we will use Nmap to discover systems and services actively. Nmap was created by Gordon Lyon (Fyodor), a network security expert and open source programmer. It was released in 1997. Nmap, short for Network Mapper, is free, open-source software released under GPL license. Nmap is an industry-standard tool for mapping networks, identifying live hosts, and discovering running services. Nmap's scripting engine can further extend its functionality, from fingerprinting services to exploiting vulnerabilities. A Nmap scan usually goes through the steps shown in the figure below, although many are optional and depend on the command-line arguments you provide.

Subnetworks

A network segment is a group of computers linked through a shared medium, like an Ethernet switch or WiFi access point. In IP networks, a subnetwork typically consists of one or more network segments connected together and configured to use the same router. A network segment is a physical connection, while a subnetwork is a logical connection.

In the provided network diagram, there are four network segments or subnetworks. Your system would usually connect to one of these segments/subnetworks. Each subnet has its own IP address range and is connected to a larger network through a router. Depending on the network, there might be a firewall enforcing security policies.

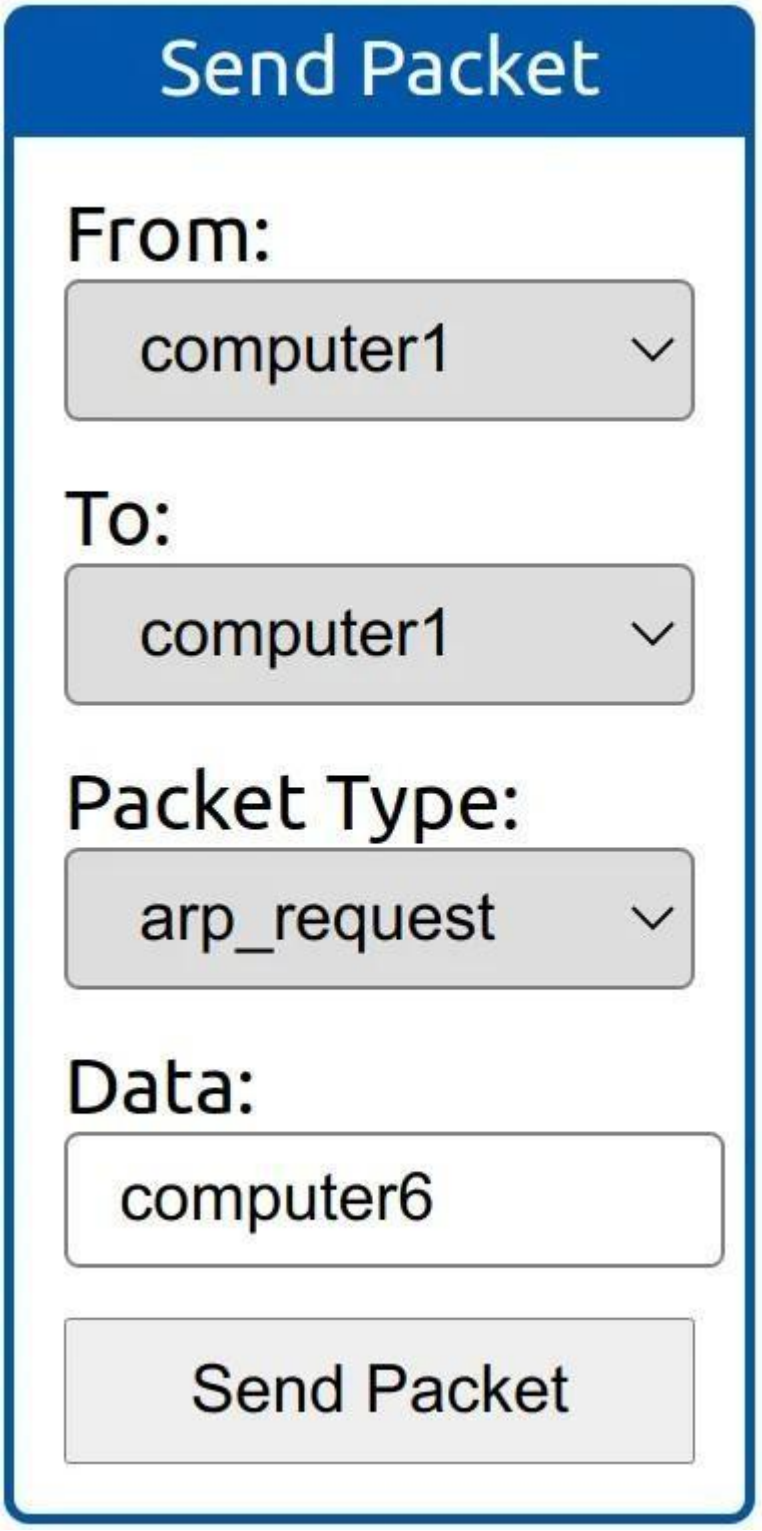


The figure displays two types of subnets:

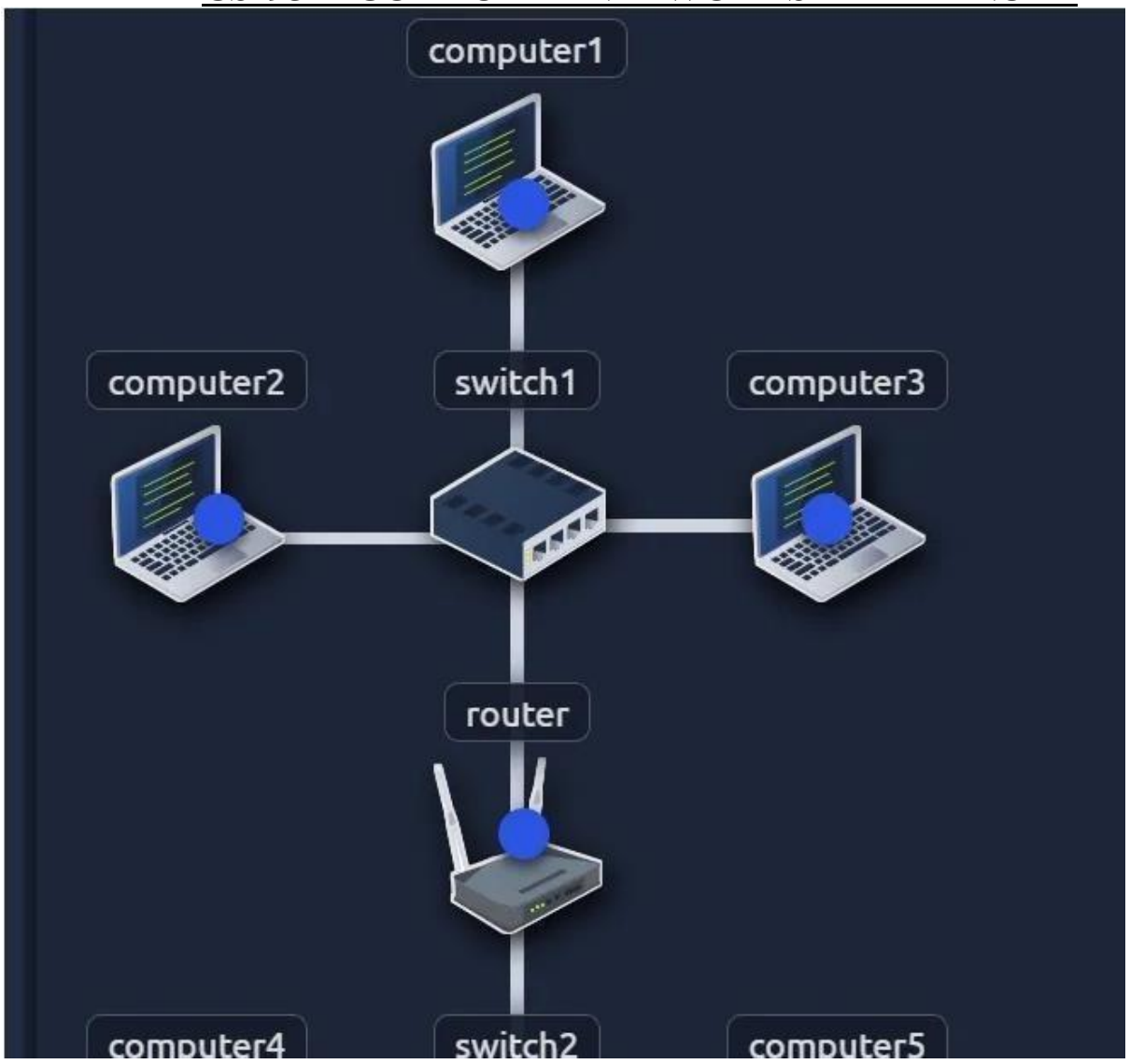
/16 Subnets: These have a subnet mask of 255.255.0.0 and can accommodate approximately 65 thousand hosts.

/24 Subnets: These feature a subnet mask of 255.255.255.0 and can support around 250 hosts.

In active reconnaissance, when attempting to gather information about a group of hosts or a subnet, if you're on the same subnet, your scanner relies on ARP (Address Resolution Protocol) queries to find live hosts. ARP queries seek to obtain the MAC address, enabling link-layer communication, which implies the host is online. However, ARP can only discover devices within the same subnet. If you're on a different subnet from the target, your scanner's packets will be routed through the default gateway, but ARP queries cannot cross subnet routers since ARP packets are tied to their specific subnet due to being a link-layer protocol.



- from computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: “ARP Request”
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

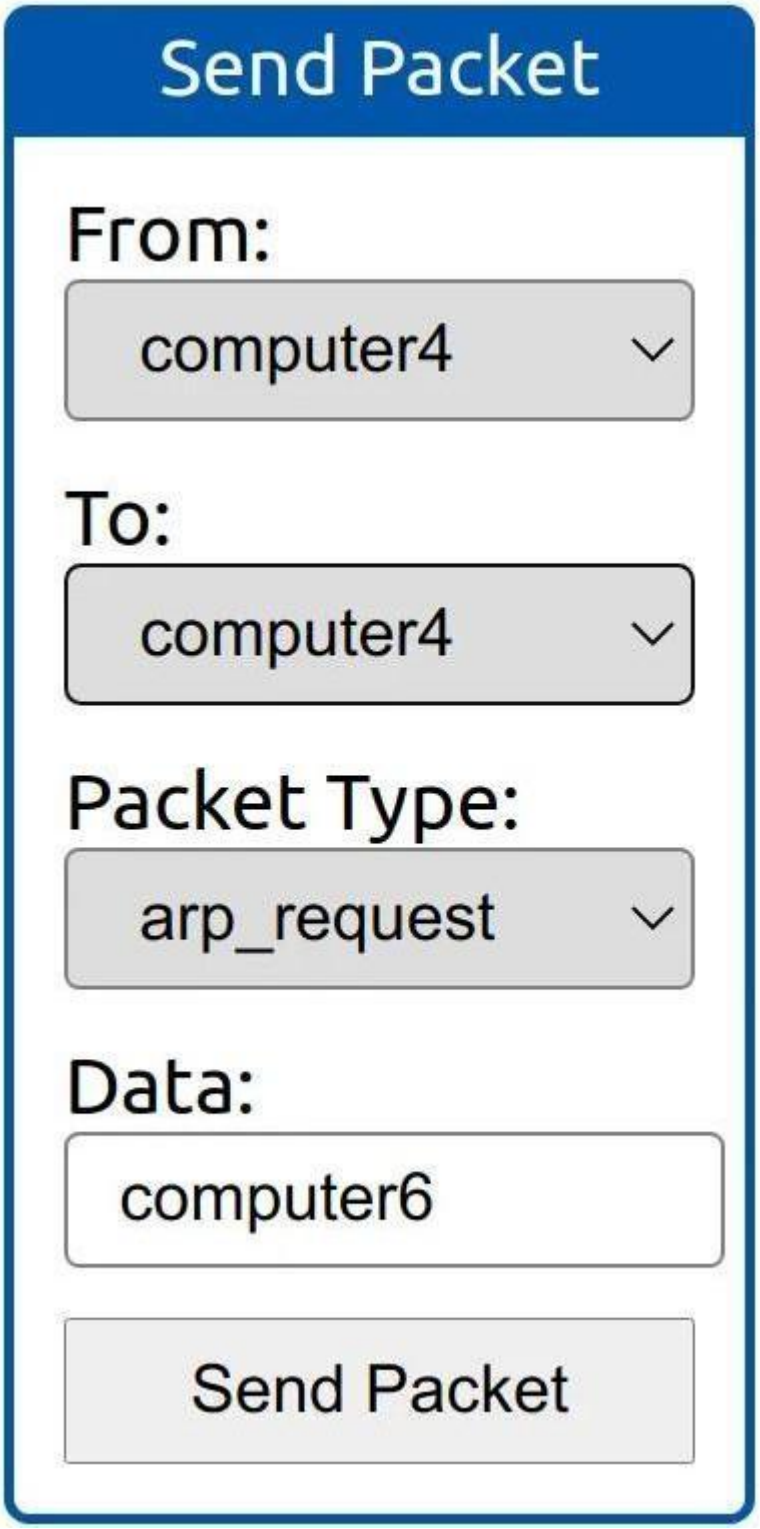


How many devices can see the ARP Request?

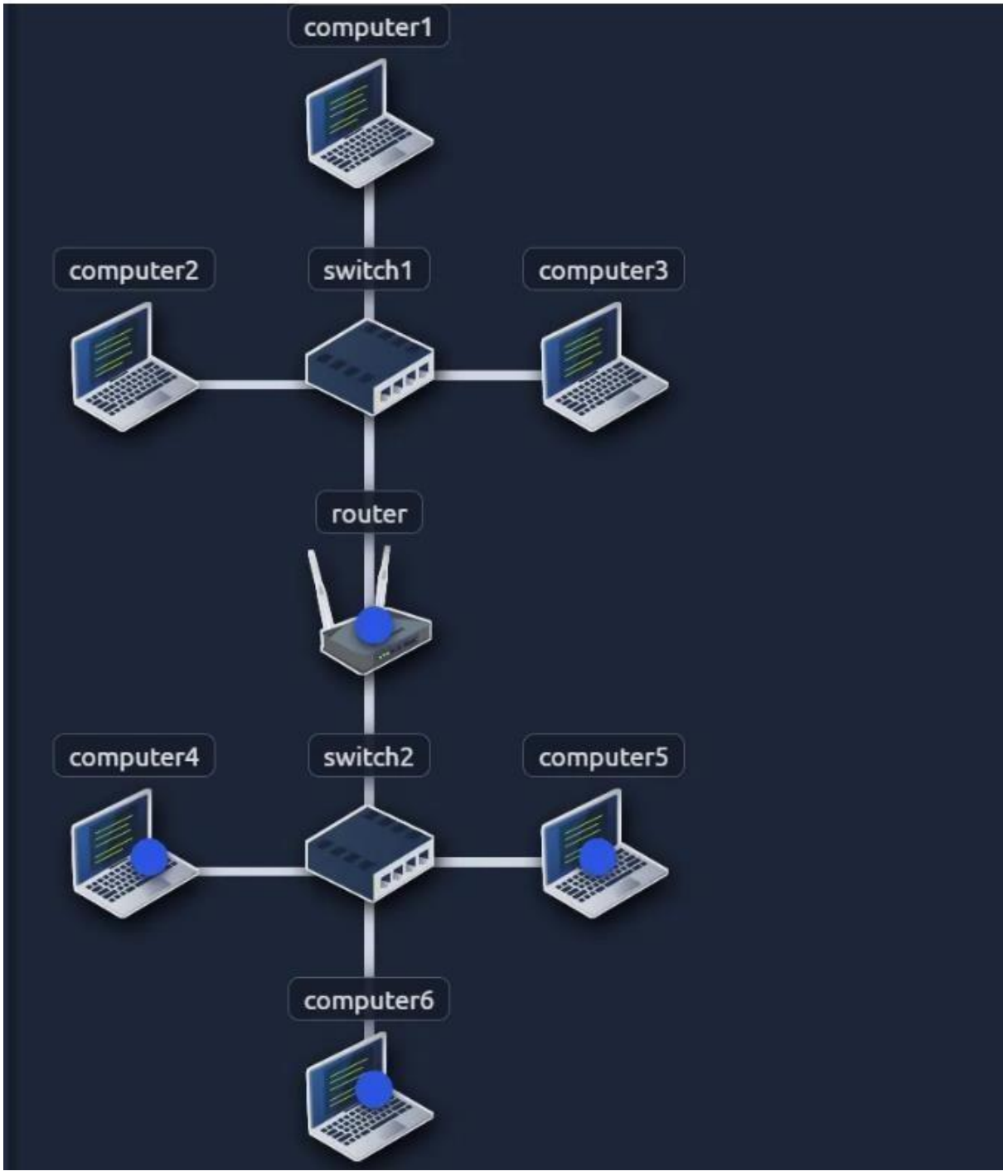
4

Did computer6 receive the ARP Request? (Y/N)

N



- From computer4
- To computer4 (to indicate it is broadcast)
- Packet Type: “ARP Request”
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)



How many devices can see the ARP Request?

4

Did computer6 reply to the ARP Request? (Y/N)

Y

Enumerating Targets

Before delving into the details of scanning techniques, it's essential to define the targets we want to scan. Targets can be specified in three ways:

1. List: You can provide a list of specific IP addresses or hostnames, like "MACHINE_IP," "scanme.nmap.org," and "example.com," which would result in scanning 3 IP addresses.
2. Range: You can specify a range, such as "10.11.12.15–20," which will scan 6 IP addresses: 10.11.12.15, 10.11.12.16, and so on, up to 10.11.12.20.

3. Subnet: You can define a subnet like "MACHINE_IP/30," which will scan 4 IP addresses within that subnet.

Nmap allows you to input a list of targets from a file using "nmap -iL list_of_hosts.txt." You can also preview the list of hosts that Nmap intends to scan by using "nmap -sL TARGETS," which provides a detailed list without actually scanning them. However, Nmap will attempt reverse-DNS resolution to obtain host names, potentially revealing valuable information to the pentester. To prevent DNS resolution, you can add the "-n" flag.

What is the first IP address Nmap would scan if you provided 10.10.12.13/29 as your target?

=>/29= 8 address,

=> 10.10.12.[0–7][8–15]

=>10.10.12.8

How many IP addresses will Nmap scan if you provide the following range 10.10.0-255.101-125?

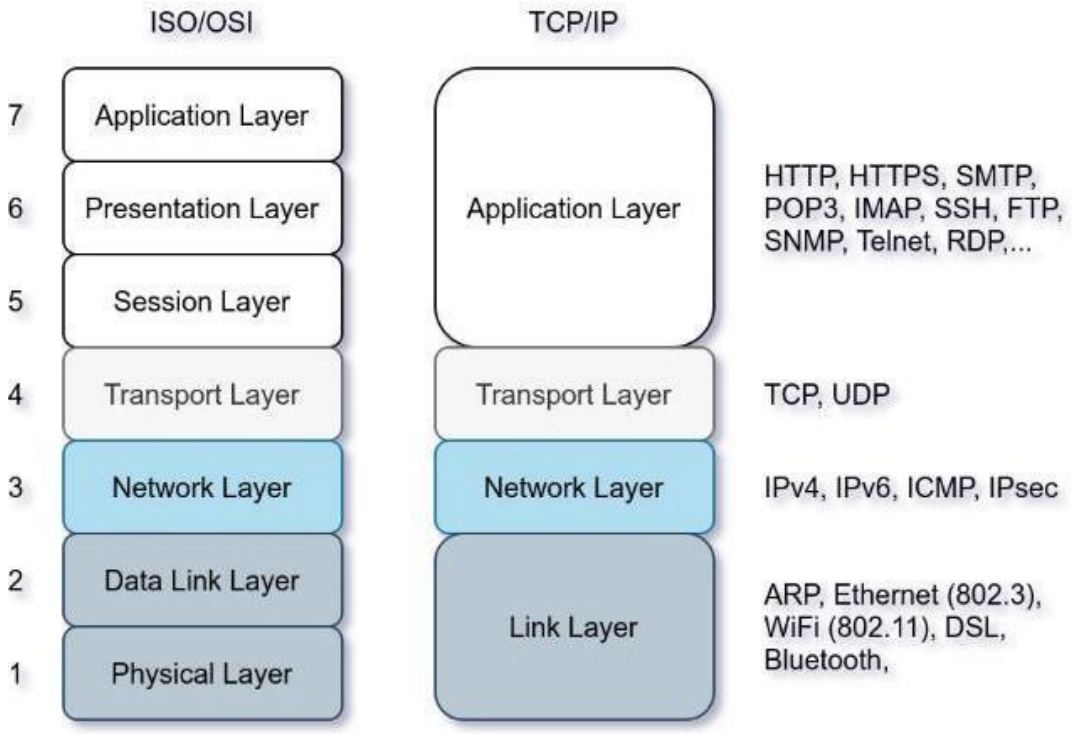
*=> 255*25*

=>6400

Discvoering Live hosts

TCP/IP layers:

- ARP from Link Layer
- ICMP from Network Layer
- TCP from Transport Layer
- UDP from Transport Layer



This passage discusses four network protocols: ARP, ICMP, TCP, and UDP, and their roles in network scanning. ARP is used to request a computer's MAC address with a specific IP address. ICMP has various types, including ping (Type 8 and Type 0). When pinging a system on the same subnet, an ARP query should be sent before ICMP Echo. Additionally, network scanners can use specially-crafted packets to common TCP or UDP ports for efficient target response checking, especially when ICMP Echo is blocked.

Send a packet with the following:

- From computer1
- To computer3
- Packet Type: "Ping Request"

What is the type of packet that computer1 sent before the ping?
ARP Request
What is the type of packet that computer1 received before being able to send the ping?
ARP Response
How many computers responded to the ping request?
1
Send a packet with the following:

- From computer2
- To computer5
- Packet Type: "Ping Request"

What is the name of the first device that responded to the first ARP Request?
router
What is the name of the first device that responded to the second ARP Request?
computer5
Send another Ping Request. Did it require new ARP Requests? (Y/N)
N
NMAP Host Discovery Using ARP

How can we determine which hosts are operational? It's crucial to prevent unnecessary port scanning on hosts that are offline or not in use. There are several methods to identify active hosts. When no specific host discovery options are specified, Nmap employs the following strategies to find live hosts:

When a privileged user tries to scan targets on a local network (Ethernet), Nmap uses ARP requests. A privileged user is root or a user who belongs to sudoers and can run sudo.

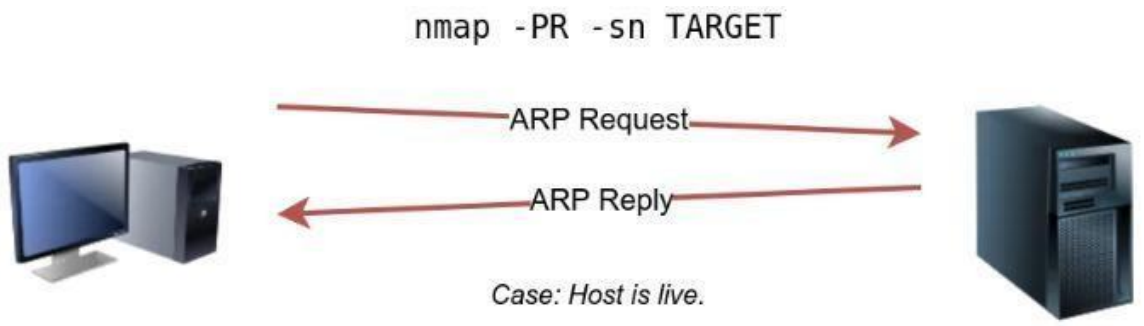
When a privileged user tries to scan targets outside the local network, Nmap uses ICMP echo requests, TCP ACK (Acknowledge) to port 80, TCP SYN (Synchronize) to port 443, and ICMP timestamp request.

When an unprivileged user tries to scan targets outside the local network, Nmap resorts to a TCP 3-way handshake by sending SYN packets to ports 80 and 443.

Nmap typically uses a ping scan to find live hosts and then proceeds to scan those live hosts. However, you can use the "nmap -sn TARGETS" command to discover online hosts without conducting port scans. ARP scan is one such method, but it only works when you are on the same subnet as the target systems because it relies on MAC addresses for communication. ARP queries are sent to obtain MAC addresses, and hosts that respond to these queries are considered up. You may see many ARP queries during a local network scan with Nmap. To perform only an ARP scan without port scanning, you can use "nmap -PR -sn TARGETS," where "-PR" specifies an ARP scan. This allows you to discover live systems on the same subnet as your target machine without conducting any port scans.

```
Pentester Terminal

pentester@TryHackMe$ sudo nmap -PR -sn 10.10.210.6/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-02 07:12 BST
Nmap scan report for ip-10-10-210-75.eu-west-1.compute.internal (10.10.210.75)
Host is up (0.00013s latency).
MAC Address: 02:83:75:3A:F2:89 (Unknown)
Nmap scan report for ip-10-10-210-100.eu-west-1.compute.internal (10.10.210.100)
Host is up (-0.100s latency).
MAC Address: 02:63:D0:1B:2D:CD (Unknown)
Nmap scan report for ip-10-10-210-165.eu-west-1.compute.internal (10.10.210.165)
Host is up (0.00025s latency).
MAC Address: 02:59:79:4F:17:B7 (Unknown)
Nmap scan report for ip-10-10-210-6.eu-west-1.compute.internal (10.10.210.6)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.12 seconds
```

In this scenario, the AttackBox had the IP address 10.10.210.6 and employed ARP requests to identify active hosts within the same subnet. Nmap sends ARP requests to all the target machines, and those that are online will respond with an ARP reply. The ARP scan operates as depicted in the accompanying figure.



- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: “ARP Request”

Data: try all the possible eight devices (other than computer1) in the network: computer2, computer3, computer4, computer5, computer6, switch1, switch2, and router.

How many devices are you able to discover using ARP requests?

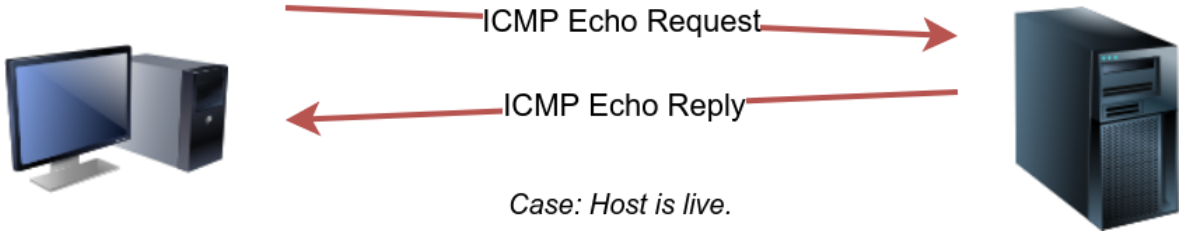
3

NMAP Host Discovery Using ICMP

A simple method to identify live hosts on a target network is by pinging each IP address and checking for responses (ICMP Type 8/Echo requests and Type 0/Echo replies). However, this approach is not always reliable because some firewalls block ICMP echo requests, and newer versions of Windows have default settings that do so as well. If the target is on the same subnet, an ARP query will precede the ICMP request. To perform host discovery using ICMP echo requests, you can use the option “-PE” and include “-sn” if you don’t want to conduct a subsequent port scan.

As shown in the following figure, an ICMP echo scan works by sending an ICMP echo request and expects the target to reply with an ICMP echo reply if it is online.

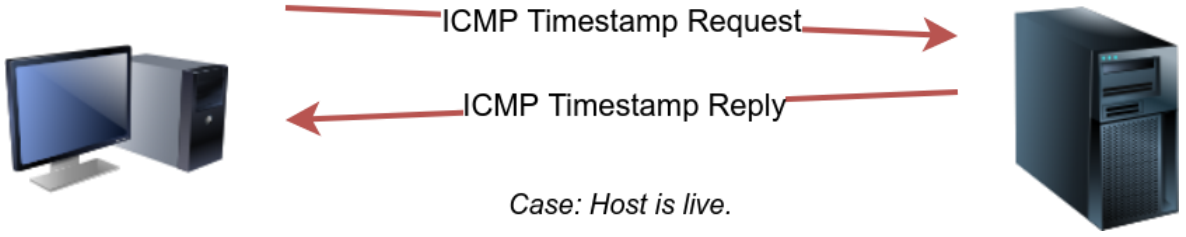
```
nmap -PE -sn TARGET
```



Case: Host is live.

Nmap uses timestamp request (ICMP Type 13) and checks whether it will get a Timestamp reply (ICMP Type 14). Adding the -PP option tells Nmap to use ICMP timestamp requests. As shown in the figure below, you expect live hosts to reply.

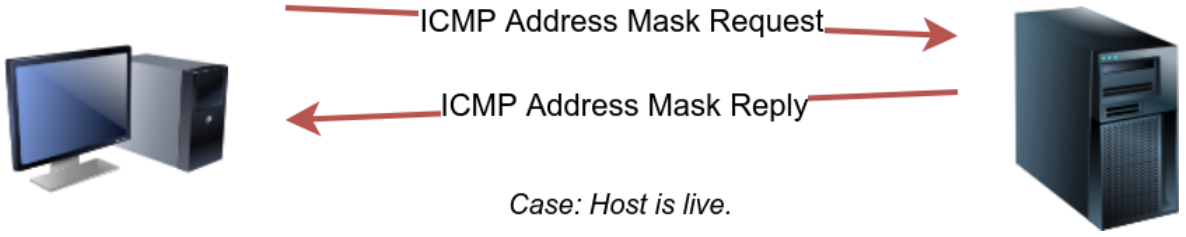
```
nmap -PP -sn TARGET
```



Case: Host is live.

Similarly, Nmap uses address mask queries (ICMP Type 17) and checks whether it gets an address mask reply (ICMP Type 18). This scan can be enabled with the option -PM. As shown in the figure below, live hosts are expected to reply to ICMP address mask requests.

```
nmap -PM -sn TARGET
```



Case: Host is live.

Answer the questions below

What is the option required to tell Nmap to use ICMP Timestamp to discover live hosts?

-PP

What is the option required to tell Nmap to use ICMP Address Mask to discover live hosts?

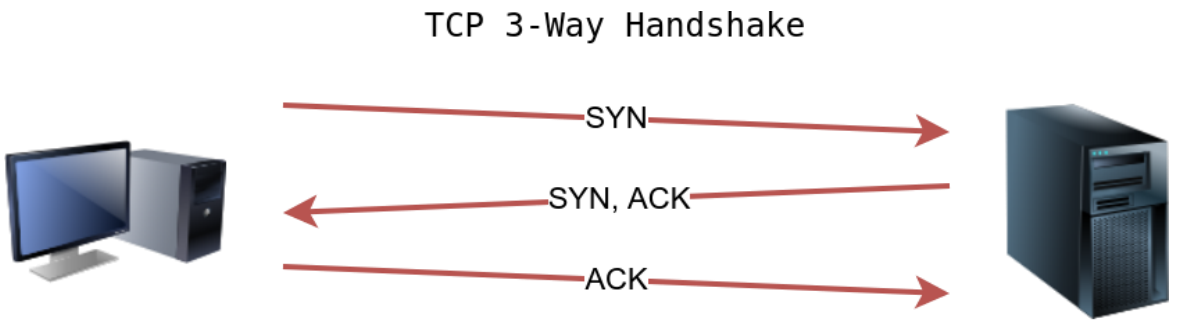
-PM

What is the option required to tell Nmap to use ICMP Echo to discover live hosts?

-PE

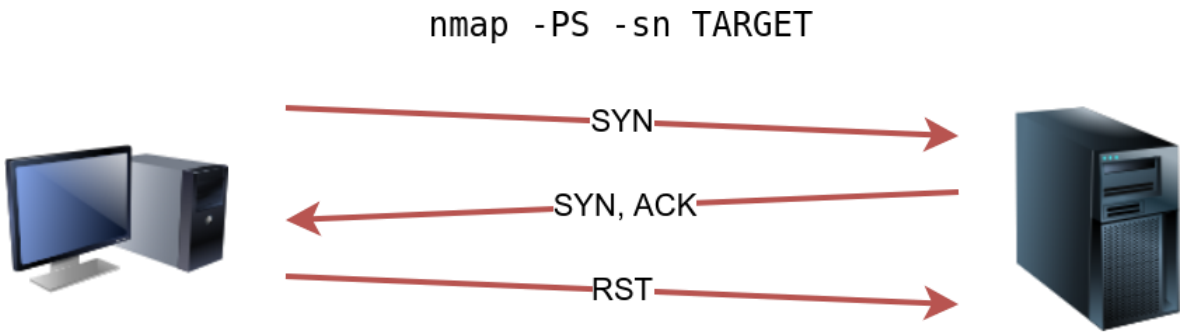
NMAP Host Discovery Using TCP AND UDP

TCP SYN Ping



Case: TCP port is open.

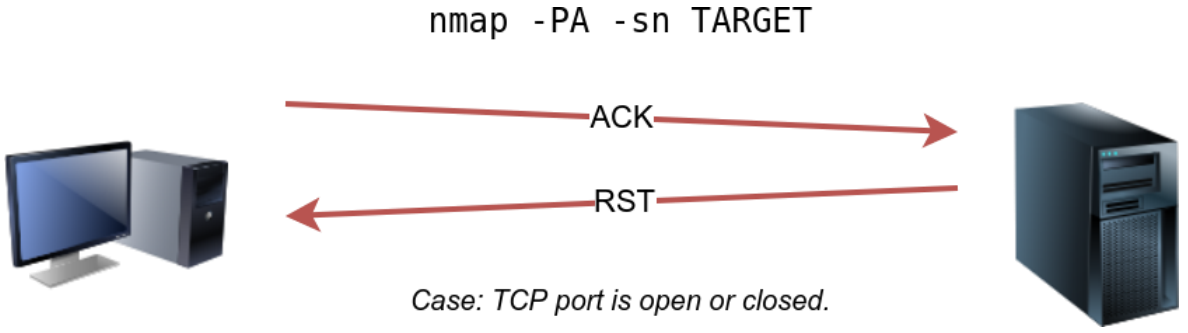
To determine if a host is up, you can send a packet with the SYN (Synchronize) flag set to a default TCP port, usually 80, and wait for a response. An open port will reply with SYN/ACK, while a closed port will result in an RST. In this method, the specific state of the port is not crucial; it's about checking for any response to confirm the host's status. You can enable Nmap to use TCP SYN ping with the option "-PS" followed by the port number, range, or list. For example, "-PS21" targets port 21, while "-PS21–25" targets ports 21 to 25. Privileged users can send TCP SYN packets without completing the 3-way handshake, unlike unprivileged users who must complete it if the port is open.



Case: TCP port is open.

TCP ACK Ping

To utilize ACK ping in Nmap, which sends a packet with the ACK flag set, you need to run Nmap as a privileged user. If you attempt this as an unprivileged user, Nmap will perform a 3-way handshake by default.



Case: TCP port is open or closed.

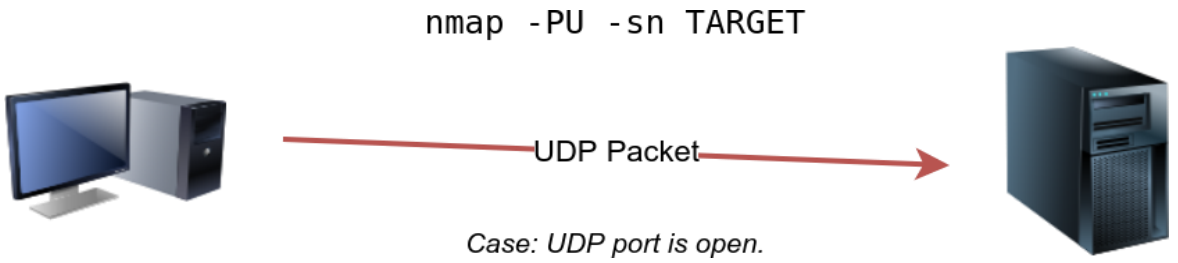
By default, Nmap uses port 80, and you can specify the port(s) using the "-PA" option, followed by a port number, range, list, or a combination thereof. For instance, you can use "- PA21," "-PA21–25," or "-PA80,443,8080." If no port is specified, Nmap will use port 80.

The expected response for an ACK ping is a TCP packet with the RST flag set because the ACK packet is not part of an established connection. This response helps determine if the target host is up.

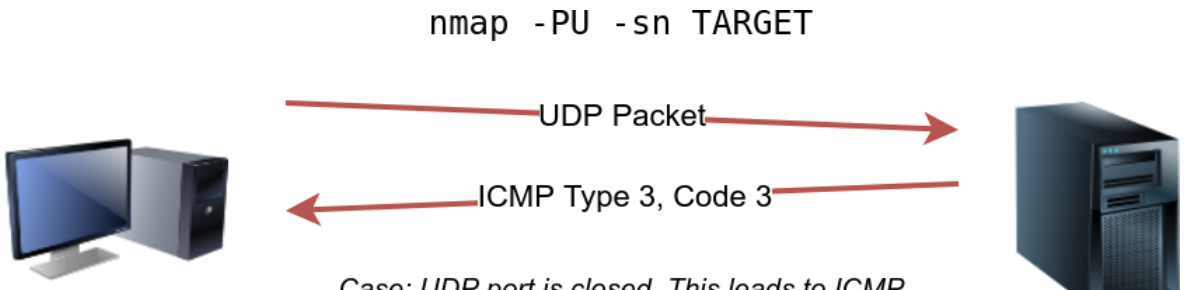
UDP Ping

You can also employ UDP to check if the host is online. Unlike TCP SYN ping, sending a UDP packet to an open port typically doesn't elicit a response. However, when sending a UDP packet to a closed UDP port, you anticipate receiving an ICMP "port unreachable" packet, which indicates the target system is active and reachable.

In summary, while sending UDP packets to open UDP ports may not trigger a response, sending them to closed UDP ports can indirectly indicate that the target is online, as it may generate a "port unreachable" ICMP message.



Case: UDP port is open.



Case: UDP port is closed. This leads to ICMP Destination Unreachable (Port Unreachable)

Answer the questions below

Which TCP ping scan does not require a privileged account?

TCP SYN Ping

Which TCP ping scan requires a privileged account?

TCP ACK Ping

What option do you need to add to Nmap to run a TCP SYN ping scan on the telnet port?

-PS23

Using Reverse-DNS Lookup

Nmap's standard operation is to perform reverse-DNS lookups for online hosts, which can provide valuable information through hostnames. If you prefer not to conduct these DNS queries, you can use the "-n" option to bypass this process.

By default, Nmap performs DNS queries for online hosts, but you can use the "-R" option to query the DNS server even for hosts that are offline. Additionally, if you wish to specify a particular DNS server, you can include the " — dns-servers DNS_SERVER" option.

We want Nmap to issue a reverse DNS lookup for all the possibles hosts on a subnet, hoping to get some insights from the names. What option should we add?

-R

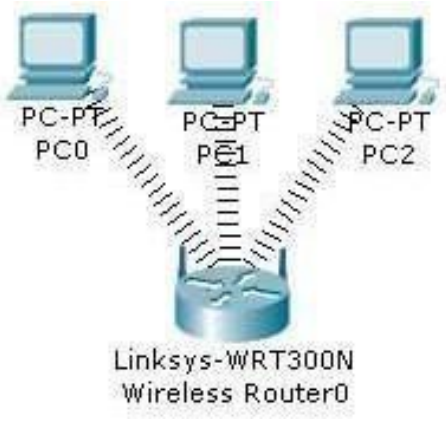
Summary

We have learned how ARP, ICMP, TCP, and UDP can detect live hosts by completing this room.

Practical-8

AIM:-b) Configuration of Wireless LAN using CISCO Packet Tracer.

Design a topology with three PCs connected from Linksys Wireless routers.



Perform following configuration:-

- Configure Static IP on PC and Wireless Router
- Set SSID to MotherNetwork
- Set IP address of router to 192.168.0.1, PC0 to 192.168.0.2, PC1 to 192.168.0.3 and PC2 to 192.168.0.4.
- Secure your network by configuring WAP key on Router
- Connect PC by using WAP key

To complete these tasks follow these step by step instructions:-

Step1:- Click on wireless router,

- Select Administration tab from top Menu, set username and password to admin and click on Save Setting.

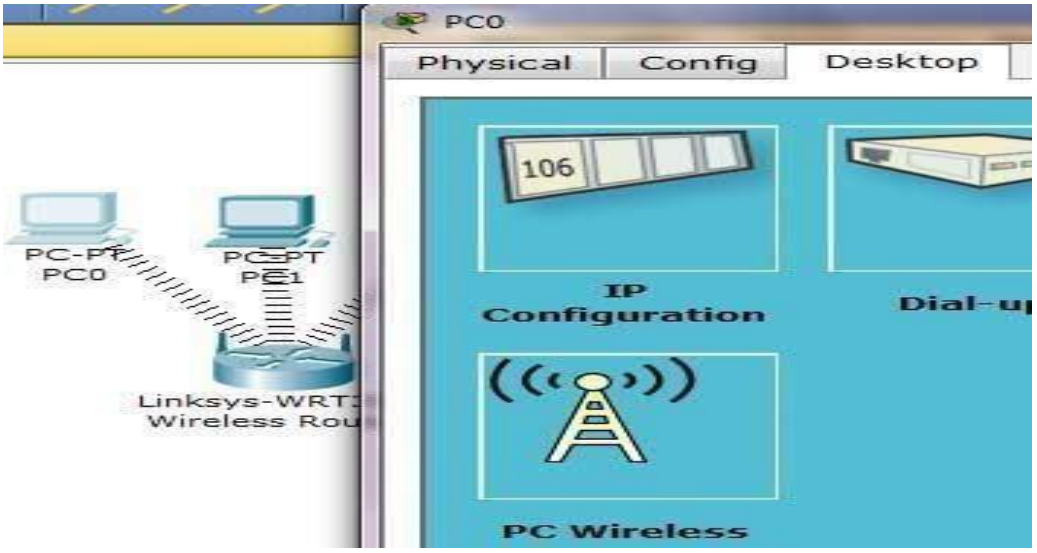
- Next click on wireless tab and set default SSID to MotherNetwork.
- Now Select wireless security and change Security Mode to WEP

- Set Key1 to 0123456789

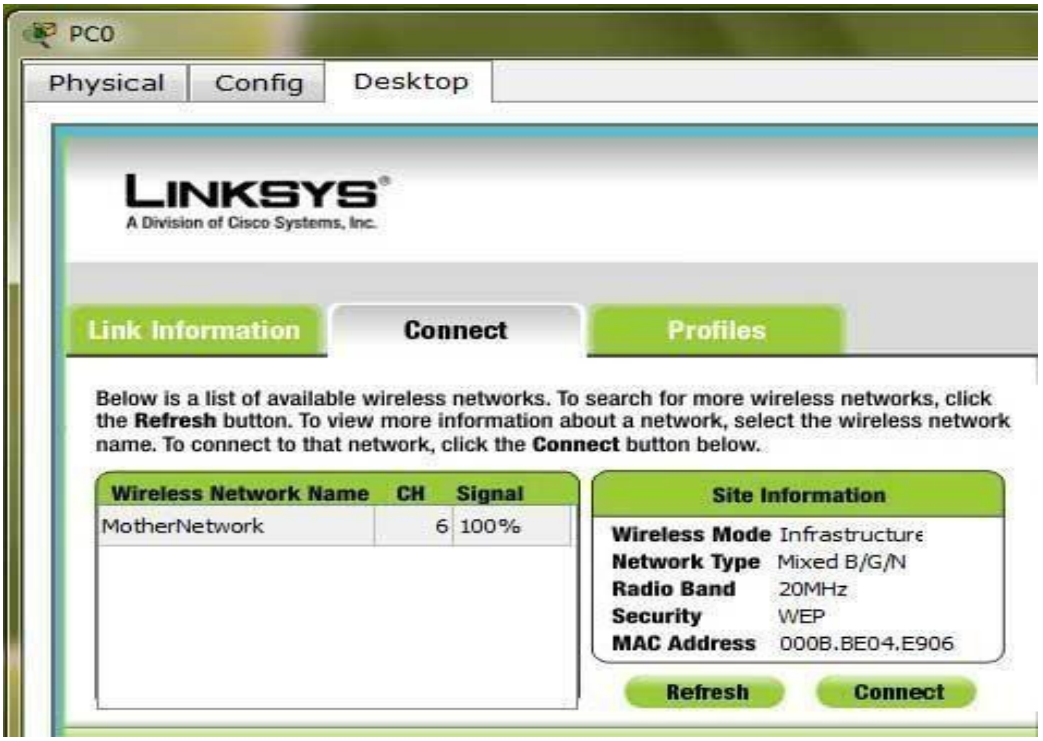
- Again go in the end of page and Click on Save Setting
- Now we have completed all given task on Wireless router. Now configure the static IP on all three PC's
- Double click on pc select Desktop tab click on IP configuration select Static IP and set IP as given below

PC	IP	Subnet Mask	Default Gateway
PC0	192.168.0.2	255.255.255.0	192.168.0.1
PC1	192.168.0.3	255.255.255.0	192.168.0.1
PC2	192.168.0.4	255.255.255.0	192.168.0.1

- Now it's time to connect PC's from Wireless router. To do so click PC select Desktop click on PC Wireless

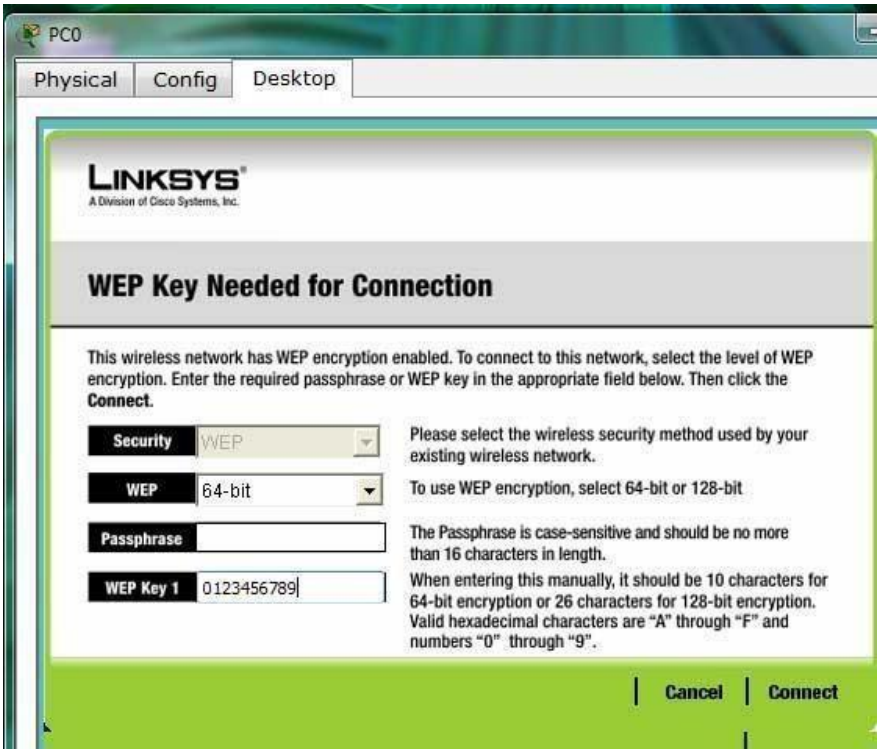


- Click on connect tab and click on Refresh button



As you can see in image that Wireless device is accessing MotherNetwork on CH 6 and signal strength is 100%. In left side you can see that WEP security is configured in network. Click on connect button to connect MotherNetwork

- It will ask for WAP key insert 0123456789 and click connect



It will connect you with wireless router.

As you can see in image below that system is connected. And PCI card is active.

- Repeat same process on PC1 and PC2.

Student observation:

c) **What is SSID of a wireless router?**
d) **What is a security key in wireless router?**
e) **Configure a simple Wireless LAN in your lab using a real access point and write down the configurations in your notebook.**

Practical-9

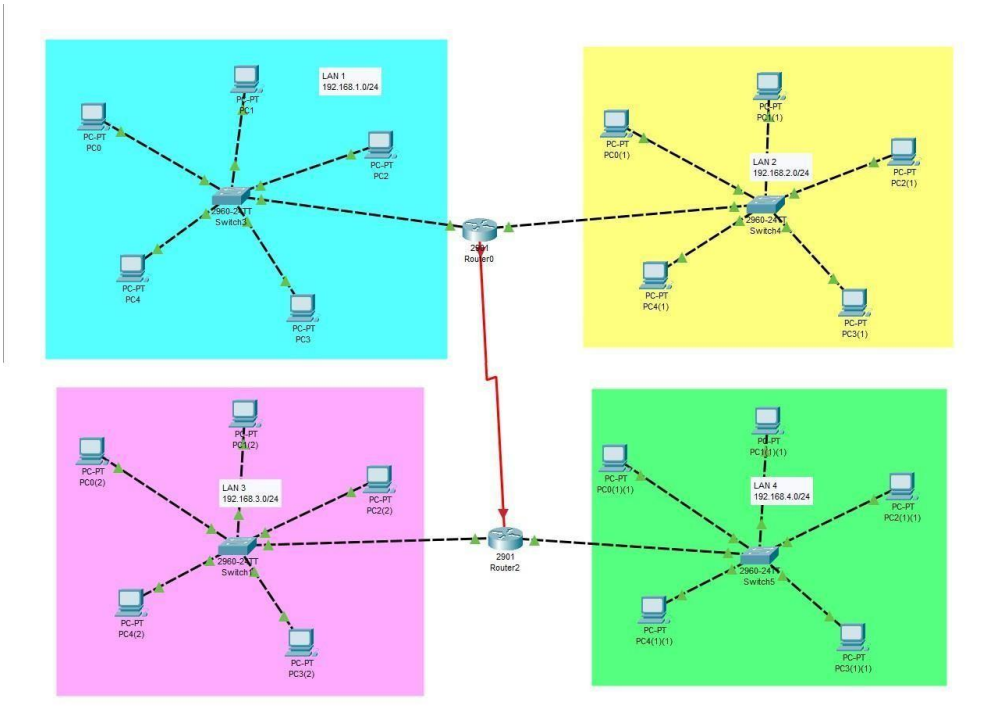
AIM:-Implementation of SUBNETTING in CISCO PACKET TRACER simulator.

Classless IP subnetting is a technique that allows for more efficient use of IP addresses by allowing for subnet masks that are not just the default masks for each IP class. This means that we can divide our IP address space into smaller subnets, which can be useful when we have a limited number of IP addresses but need to create multiple networks.

CREATING A NETWORK TOPOLOGY:
The first step in implementing classless IP subnetting is to create a network topology in Packet Tracer. To create a network topology in Packet Tracer, select the "New" button in the top left corner, then select "Network" and "Generic". This will create a blank network topology that we can use to add devices.

ADDING THE DEVICES:
Once we have created our network topology, we can add devices to it. Here, we will be adding routers, witches, and PCs. To add a device, select the device from the bottom left corner and drag it onto the network topology. Then, connect the devices by dragging a cable from one device's port to another device's port.

SUBNETTING:
To subnet the network address of 192.168.1.0/24 to provide enough space for at least 5 addresses for end devices, the switch, and the router, we can use a /27 subnet mask. This will give us 8 subnets with 30 host addresses each.



The IP addressing for the network shown in the topology can be as follows:

- Router R1:
- GigabitEthernet0/0: 192.168.1.1
- GigabitEthernet0/1: 192.168.2.1
- Switch S1:
- FastEthernet0/1: 192.168.1.0/27
- PC1: 192.168.1.11
- PC2: 192.168.1.12
- PC3: 192.168.1.13
- PC4: 192.168.1.14
- PC5: 192.168.1.15
- FastEthernet0/2: 192.168.2.0/27
- PC1: 192.168.2.11
- PC2: 192.168.2.12
- PC3: 192.168.2.13
- PC4: 192.168.2.14
- PC5: 192.168.2.15
- Router R2:
- FastEthernet0/0: 192.168.3.1
- FastEthernet0/1: 192.168.4.1
- Switch S2:
- FastEthernet0/1: 192.168.3.0/27
- PC1: 192.168.3.11
- PC2: 192.168.3.12
- PC3: 192.168.3.13
- PC4: 192.168.3.14
- PC5: 192.168.3.15
- FastEthernet0/2: 192.168.4.0/27
- PC1: 192.168.4.11
- PC2: 192.168.4.12
- PC3: 192.168.4.13
- PC4: 192.168.4.14
- PC5: 192.168.4.15

CONFIGURING THE DEVICES:

Now that we have added our devices and connected them, we can start configuring them. We will start by configuring the router. Right-click on the router and select "CLI". This will open the command-line interface (CLI) for the router. In the CLI, enter the following commands:

```
#enable
#configure terminal
#interface FastEthernet0/0
#ip address {IP address} {subnet mask}
#no shutdown
#exit

interface FastEthernet0/1
ip address {IP address} {subnet mask}

no shutdown
exit
```

Replace "{IP address}" and "{subnet mask}" with your desired IP address and subnet mask. The first interface, FastEthernet0/0, will be connected to the switch, while the second interface, FastEthernet0/1, will be connected to one of the PCs. These commands configure the router's interfaces with IP addresses and subnet masks.
Next, we will configure the switch. Right-click on the switch and select "CLI". In the CLI, enter the following commands:

```
enable
configure terminal
interface FastEthernet0/1
switchport mode access
exit

interface FastEthernet0/2
switchport mode access
exit
```

These commands configure the switch to operate in access mode on its two ports, which are connected to the two PCs.
Finally, we will configure the PCs. Right-click on each PC and select "Config". In the configuration window, enter the IP address, subnet mask, default gateway, and DNS server information. The IP address and subnet mask should be within the same subnet as the router's FastEthernet0/1 interface.

To configure the GigabitEthernet interface on the router, you can follow these steps:

1. Right-click on the router and select "CLI".
2. Enter the following commands:

```
enable
configure terminal
interface GigabitEthernet0/0
ip address {IP address} {subnet mask}
no shutdown
exit
```

Replace "{IP address}" and "{subnet mask}" with your desired IP address and subnet mask. These commands configure the GigabitEthernet interface with an IP address and subnet mask, and enable the interface.

TESTING THE NETWORK:

Now that our network topology is configured, we can test the network. Open a command prompt on each PC and try to ping the other PC. If the ping is successful, then the network is functioning properly. We can also use the "ping" command to test connectivity between the router and the PCs.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC4(2)	Router2	ICMP		0.000	N	12
	Successful	PC4(2)	PC2(1)(1)	ICMP		0.000	N	13
	Successful	PC0	Router0	ICMP		0.000	N	14

Student observation:

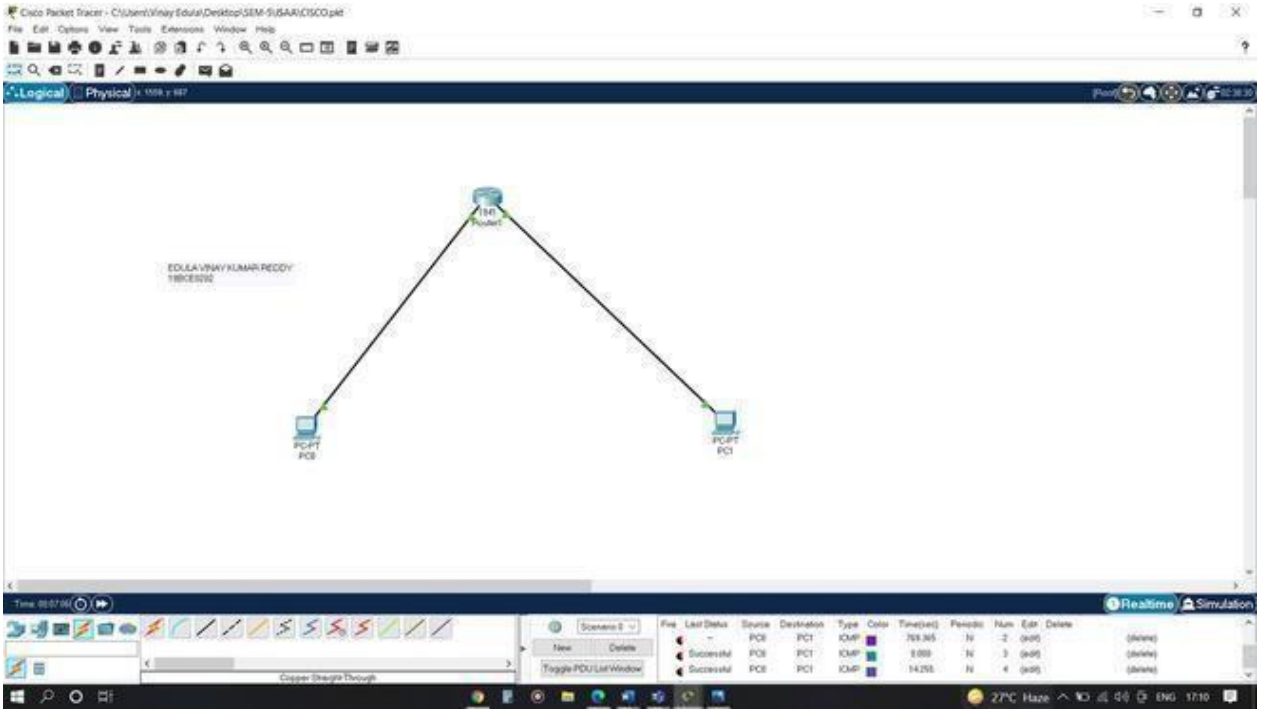
a) Write down your understanding of subnetting.
b) What is the advantage of implementing subnetting within a Network?
c) Find out whether subnetting is implemented in your college. If yes, draw and list down the subnets used with ip addresses.

Practical-10

AIM:-a) Internetworking with routers in CISCO PACKET TRACER simulator.

d) Design and configure a simple internetwork using a router.

In this network, a router and 2 PCs are used. Computers are connected with routers using a copper straight-through cable. After forming the network, to check network connectivity a simple PDU is transferred from PC0 to PC1.



Procedure:

Step-1(Configuring Router1):

1. Select the router and Open CLI.
2. Press ENTER to start configuring Router1.
3. Type enable to activate the privileged mode.

Router1 Command Line Interface:

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 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
Router(config-if)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.20.1 255.255.255.0
Router(config-if)#no shutdown

Step-2(Configuring PCs):

1. Assign IP Addresses to every PC in the network.
2. Select the PC, Go to the desktop and select IP Configuration and assign an IP address, Default gateway, Subnet Mask
3. Assign the default gateway of PC0 as 192.168.10.1.
4. Assign the default gateway of PC1 as 192.168.20.1.

Step-3(Connecting PCs with Router):

1. Connect FastEthernet0 port of PC0 with FastEthernet0/0 port of Router1 using a copper straight-through cable.
2. Connect FastEthernet0 port of PC1 with FastEthernet0/1 port of Router1 using a copper straight-through cable.

Router Configuration Table:

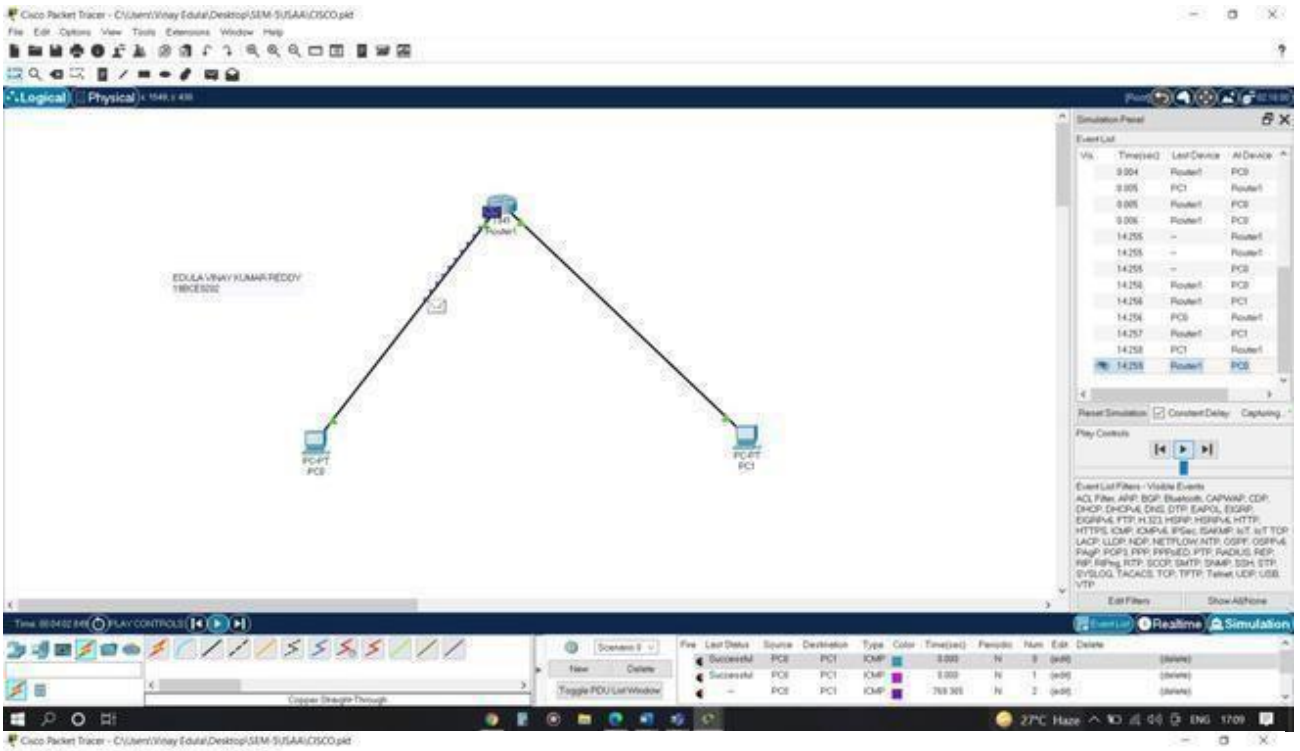
Device Name	IP address FastEthernet0 /0	Subnet Mask	IP Address FastEthernet0/1	Subnet Mask
Router1	192.168.10.1	255.255.255.0	192.168.20.1	255.255.255.0

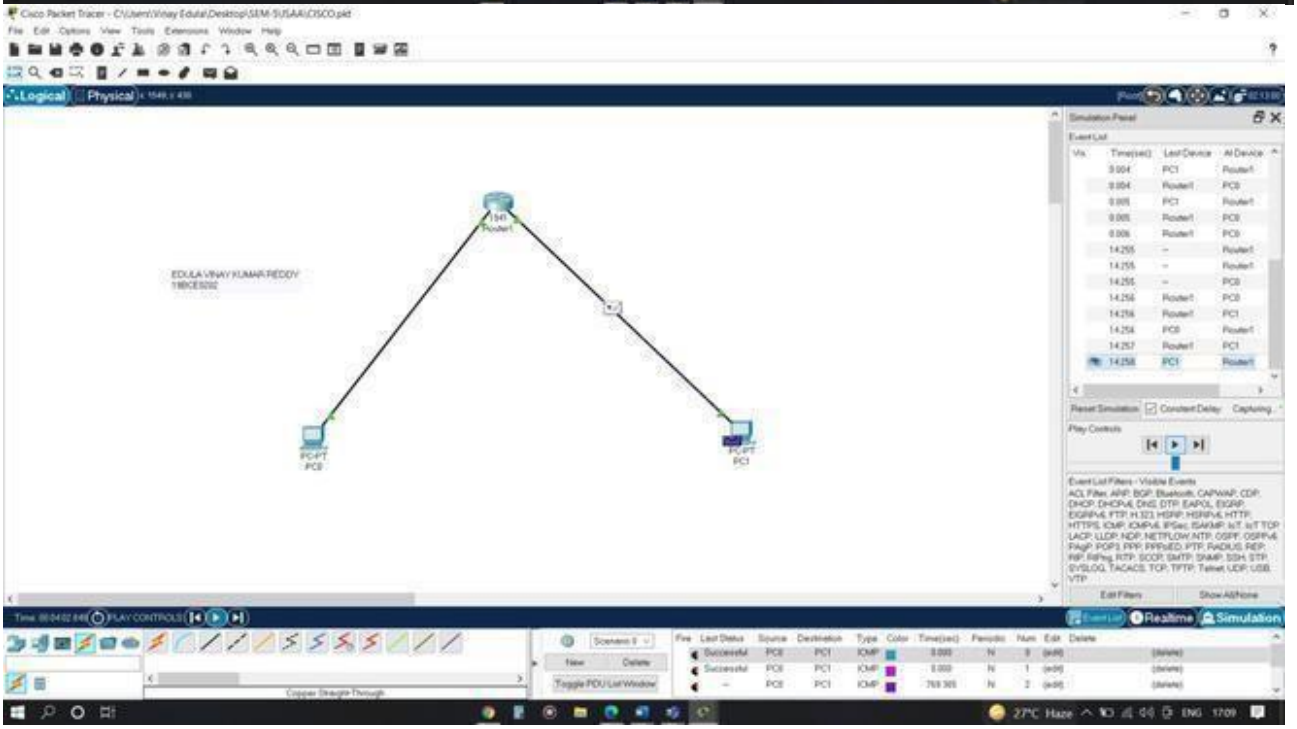
PC Configuration Table:

Device Name	IP address	Subnet Mask	Gateway
PC 0	192.168.10.2	255.255.255.0	192.168.10.1
PC 1	192.168.20.2	255.255.255.0	192.168.20.1

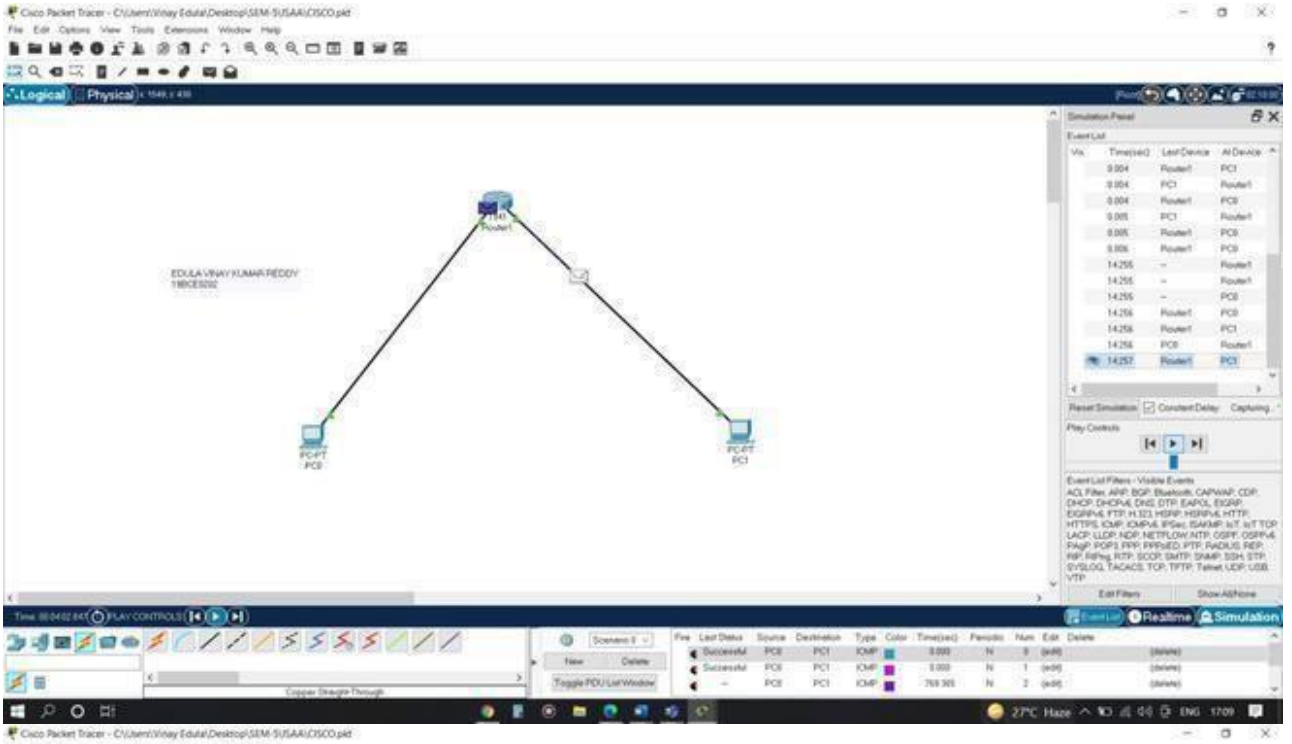
Designed Network topology:
Simulation of Designed Network Topology:

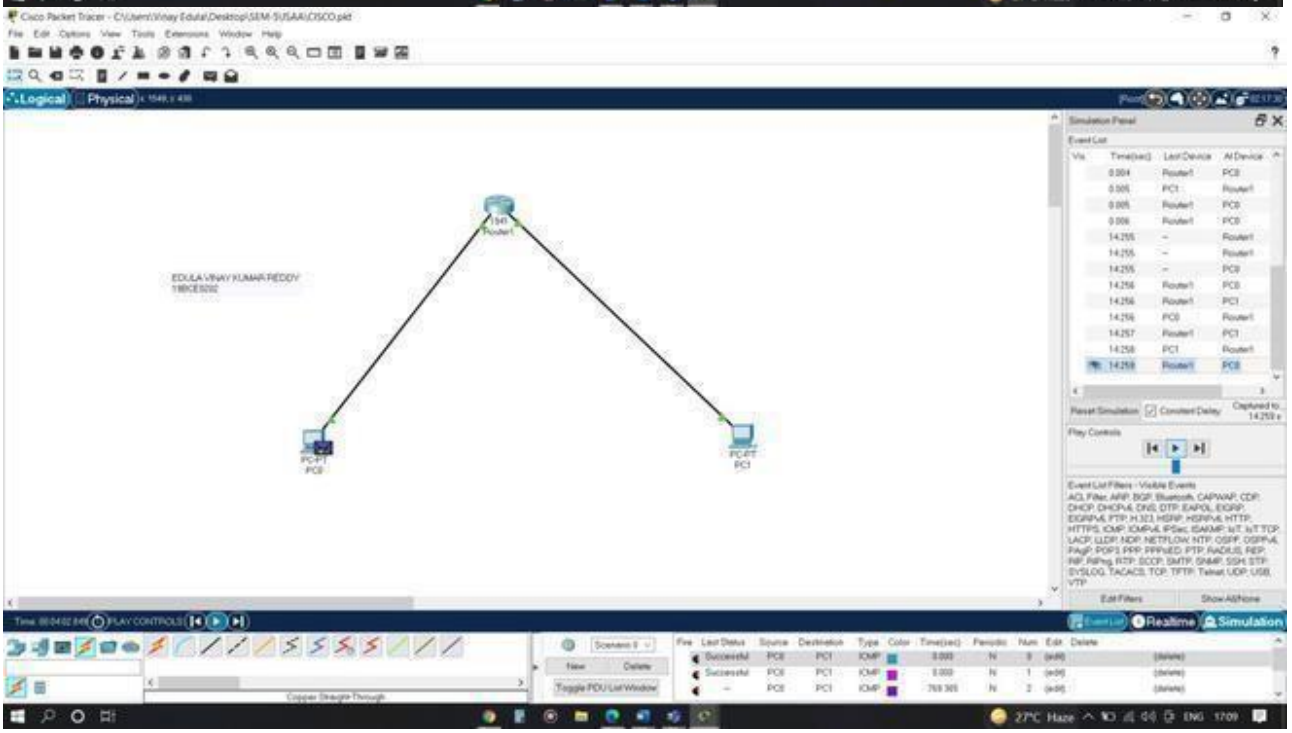
Sending a PDU From PC0 to PC1:





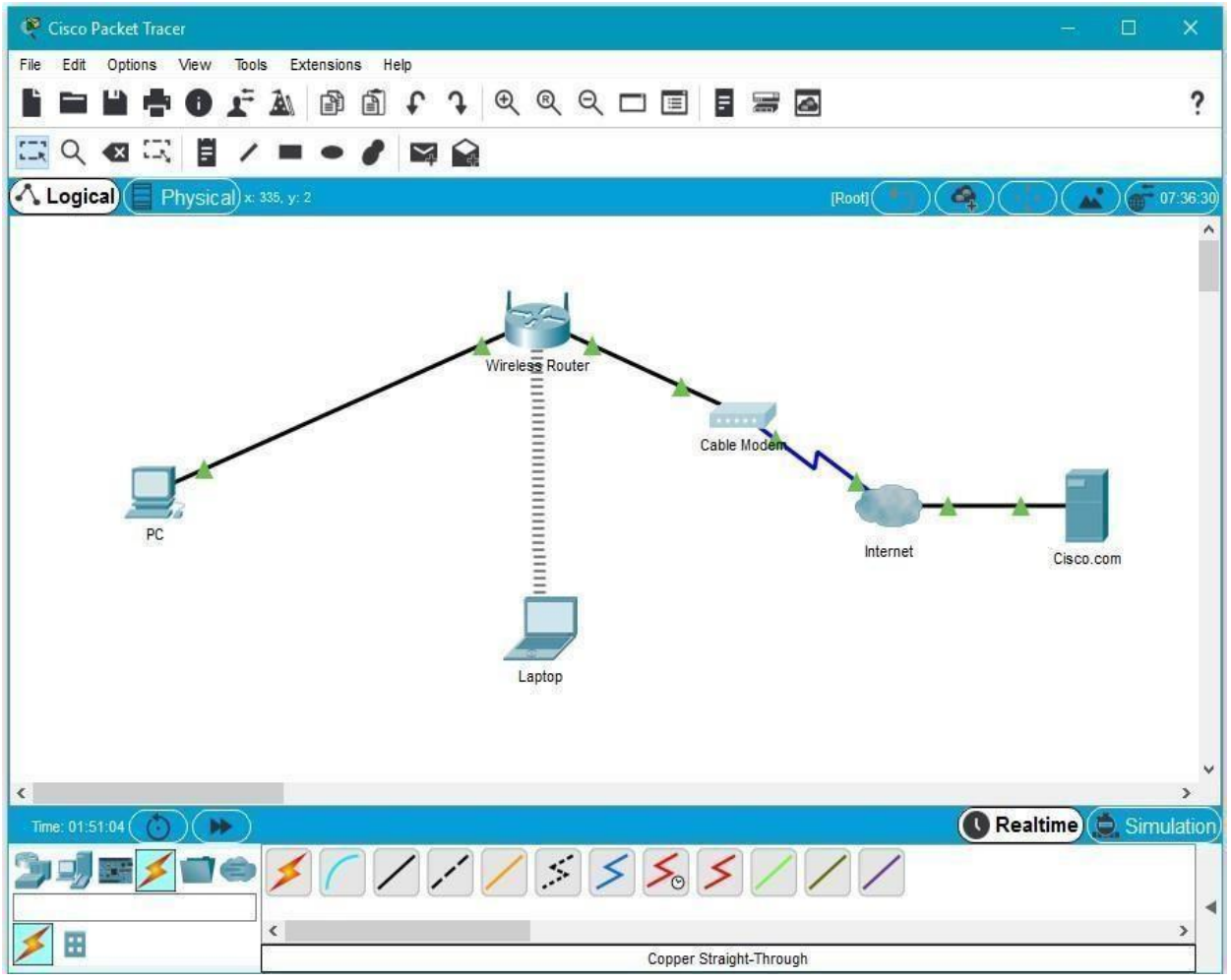
Acknowledgment From PC1 to PC0:





Practical 10

AIM:- b) Design and configure an internetwork using wireless router, DHCP server and internet cloud.



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC	Ethernet0	DHCP		192.168.0.1
Wireless Router	LAN	192.168.0.1	255.255.255.0	
Wireless Router	Internet	DHCP		
Cisco.com Server	Ethernet0	208.67.220.220	255.255.255.0	
Laptop	Wireless0	DHCP		

Objectives

Part 1: Build a Simple Network in the Logical Topology Workspace

Part 2: Configure the Network Devices
Part 3: Test Connectivity between Network Devices Part 4: Save the File and Close Packet Tracer

Part 1: Build a Simple Network in the Logical Topology Workspace

Step 1: Launch Packet Tracer.

Step 2: Build the topology

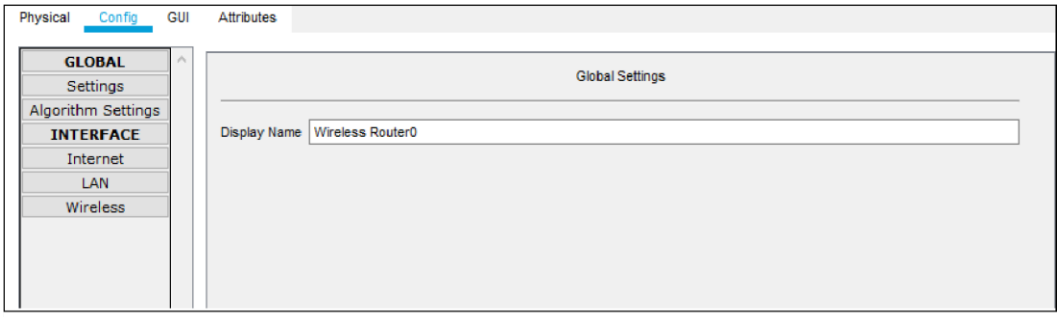
a. Add network devices to the workspace.

Using the device selection box, add the network devices to the workspace as shown in the topology diagram.

To place a device onto the workspace, first choose a device type from the **Device-Type Selection** box. Then, click on the desired device model from the **Device-Specific Selection** box. Finally, click on a location in the workspace to put your device in that location. If you want to cancel your selection, click the **Cancel** icon for that device. Alternatively, you can click and drag a device from the **Device-Specific Selection** box onto the workspace.

b. Change display names of the network devices.

To change the display names of the network devices click on the device icon on the Packet Tracer **Logical** workspace, then click on the **Config** tab in the device configuration window. Type the new name of the device into the **Display Name** box as show in the figure below.



c. Add the physical cabling between devices on the workspace

Using the device selection box, add the physical cabling between devices on the workspace as shown in the topology diagram.

The PC will need a copper straight-through cable to connect to the wireless router. Select the copper straight-through cable in the device selection box and attach it to the FastEthernet0 interface of the PC and the Ethernet 1 interface of the wireless router.

The wireless router will need a copper straight-through cable to connect to the cable modem. Select the copper straight-through cable in the device-selection box and attach it to the Internet interface of the wireless router and the Port 1 interface of the cable modem.

The cable modem will need a coaxial cable to connect to the Internet cloud. Select the coaxial cable in the device-selection box and attach it to the Port 0 interface of the cable modem and the coaxial interface of the Internet cloud.

The Interne cloud will need copper straight-through cable to connect to the Cisco.com server. Select the copper straight-through cable in the device-selection box and attach it to the Ethernet interface of the Internet cloud and the FastEthernet0 interface of the Cisco.com server.

Part 2: Configure the Network Devices

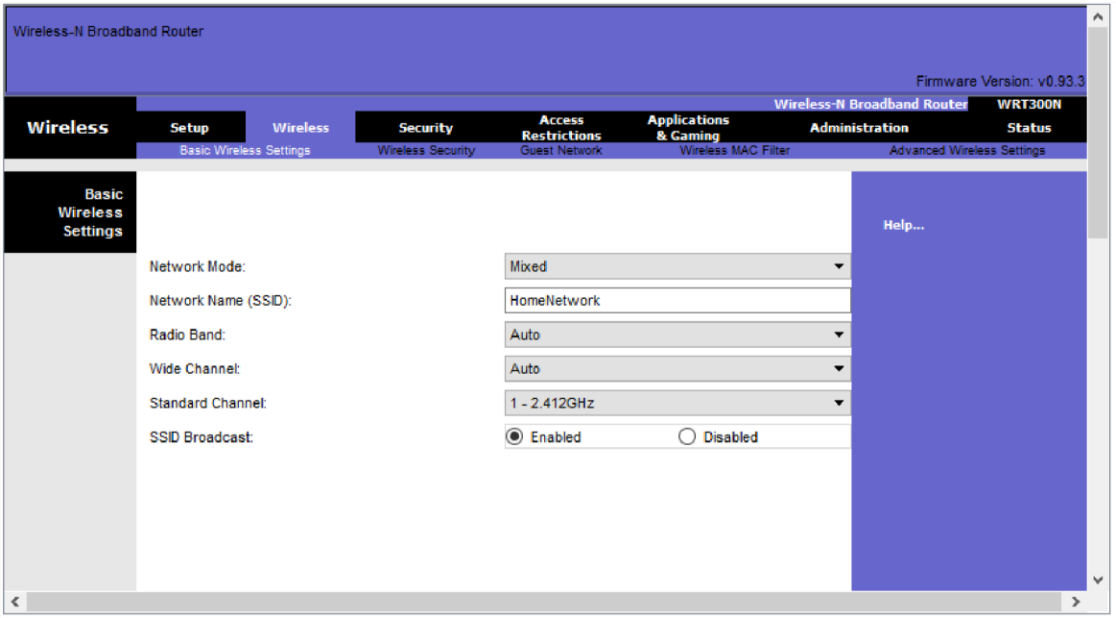
Step 1: Configure the wireless router

a. Create the wireless network on the wireless router

Click on the **Wireless Router** icon on the Packet Tracer **Logical** workspace to open the device configuration window.

In the wireless router configuration window, click on the **GUI** tab to view configuration options for the wireless router.

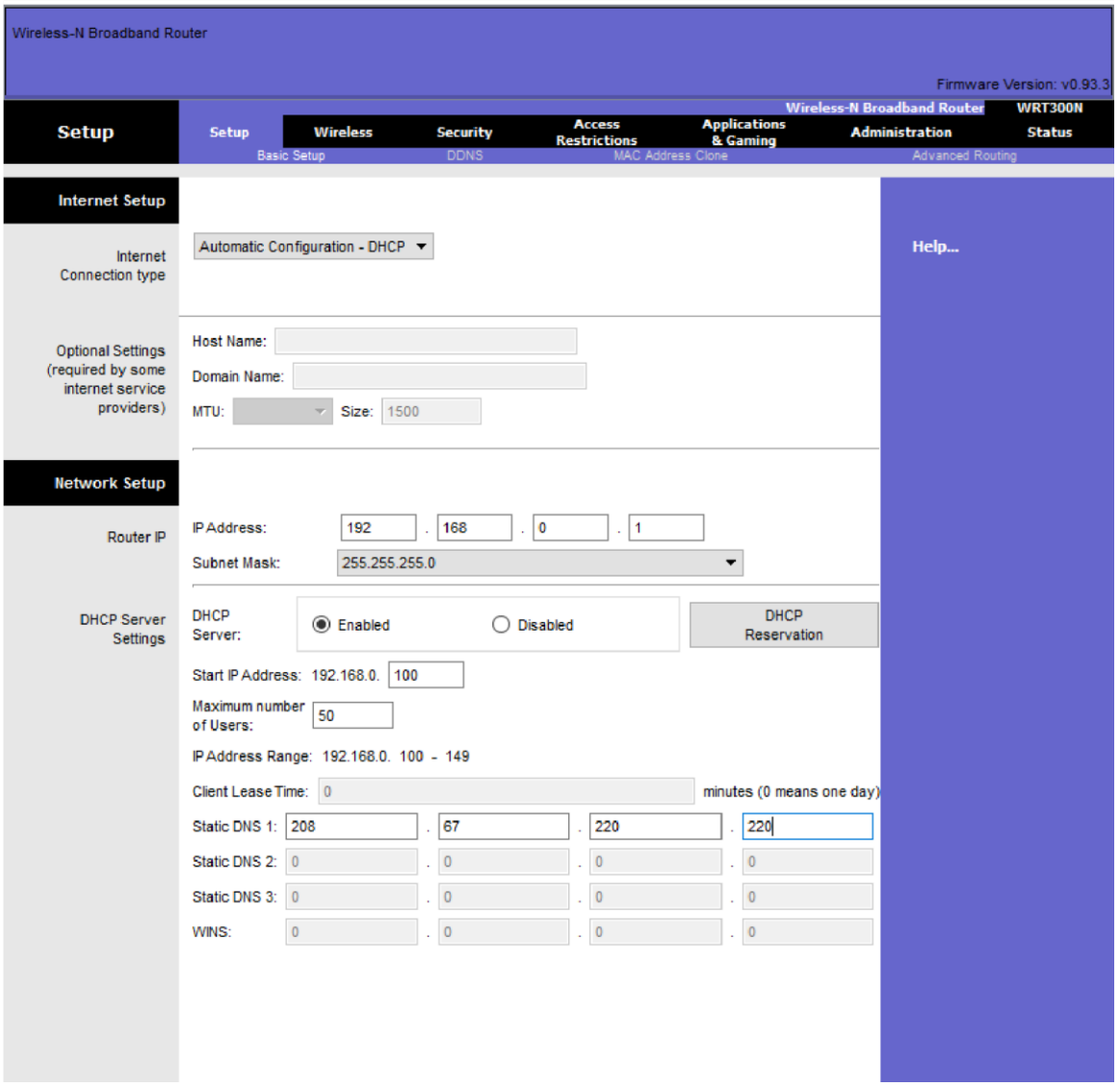
Next, click on the **Wireless** tab in the GUI to view the wireless settings. The only setting that needs to be changed from the defaults is the **Network Name (SSID)**. Here, type the name "HomeNetwork" as shown in the figure.



Configure the Internet connection on the wireless router
Click on the **Setup** tab in the wireless router GUI.

In the **DHCP Server** settings verify that the **Enabled** button is selected and configure the static IP address of the DNS server as 208.67.220.220 as shown in the figure.

b. Click on the **Save Settings** tab.



Step 2: Configure the laptop

a. Configure the Laptop to access the wireless network

Click on the Laptop icon on the Packet Tracer **Logical** workspace and in the laptop configuration windows select the **Physical** tab.

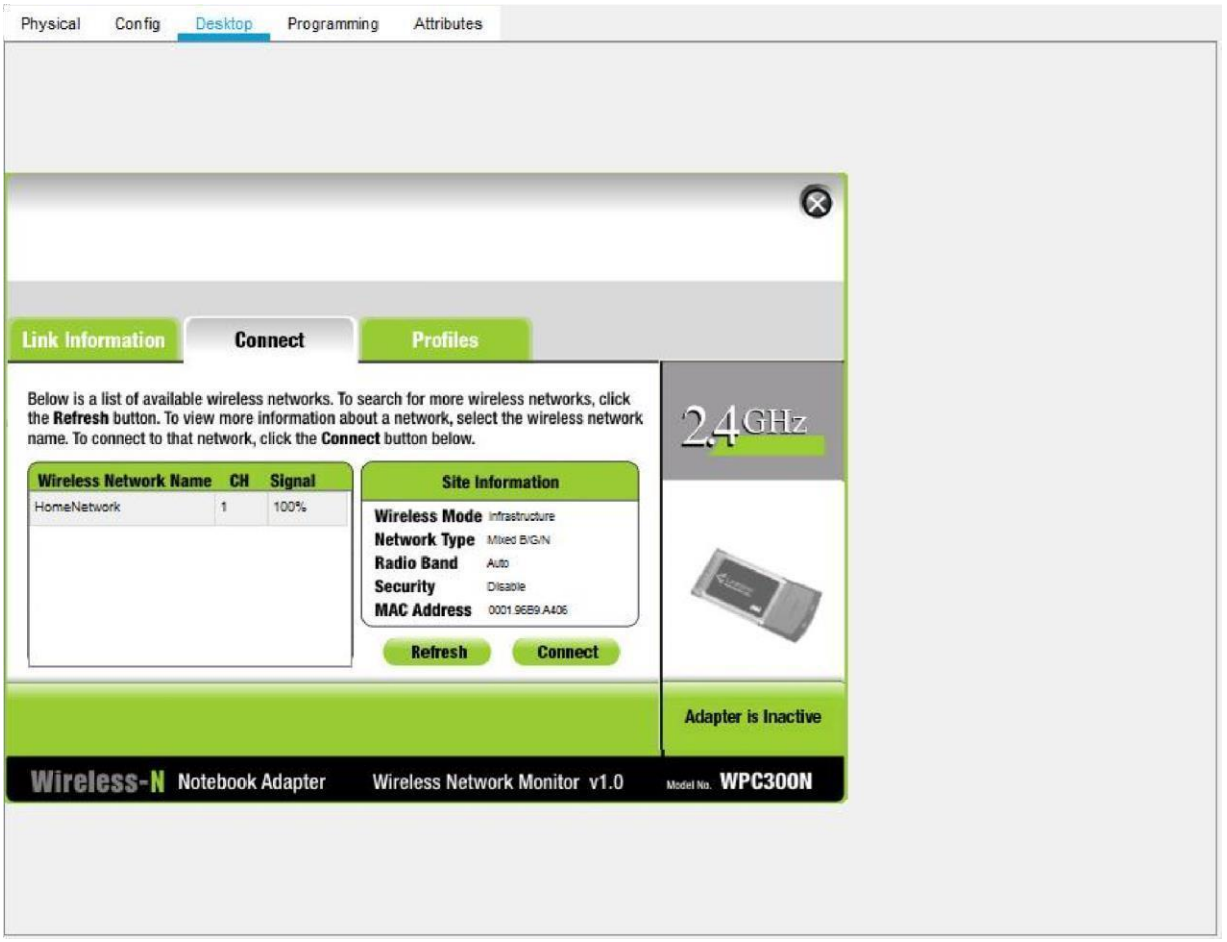
In the **Physical** tab you will need to remove the Ethernet copper module and replace it with the Wireless WPC300N module.

To do this, you first power the Laptop off by clicking the power button on the side of the laptop. Then remove the currently installed Ethernet copper module by clicking on the module on the side of the laptop and dragging it to the **MODULES** pane on the left of the laptop window. Then install the Wireless WPC300N module by clicking on it in the **MODULES** pane and dragging it to the empty module port on the side of the laptop. Power the laptop back on by clicking on the Laptop power button again.

With the wireless module installed, the next task is to connect the laptop to the wireless network.

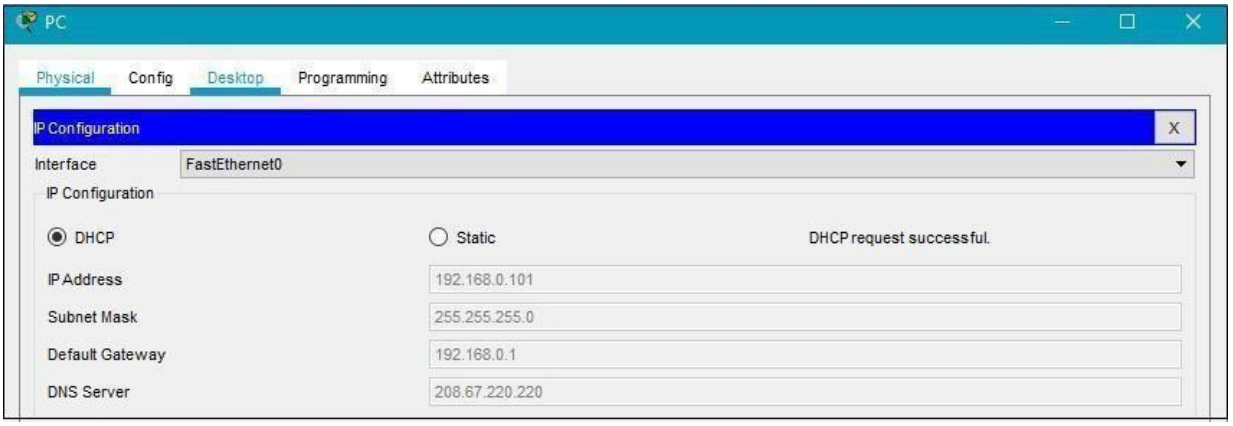
Click on the **Desktop** tab at the top of the Laptop configuration window and select the **PC Wireless** icon.

Once the Wireless-N Notebook Adapter settings are visible, select the **Connect** tab. The wireless network "HomeNetwork" should be visible in the list of wireless networks as shown in the figure.
Select the network, and click on the **Connect** tab found below the **Site Information pane.**

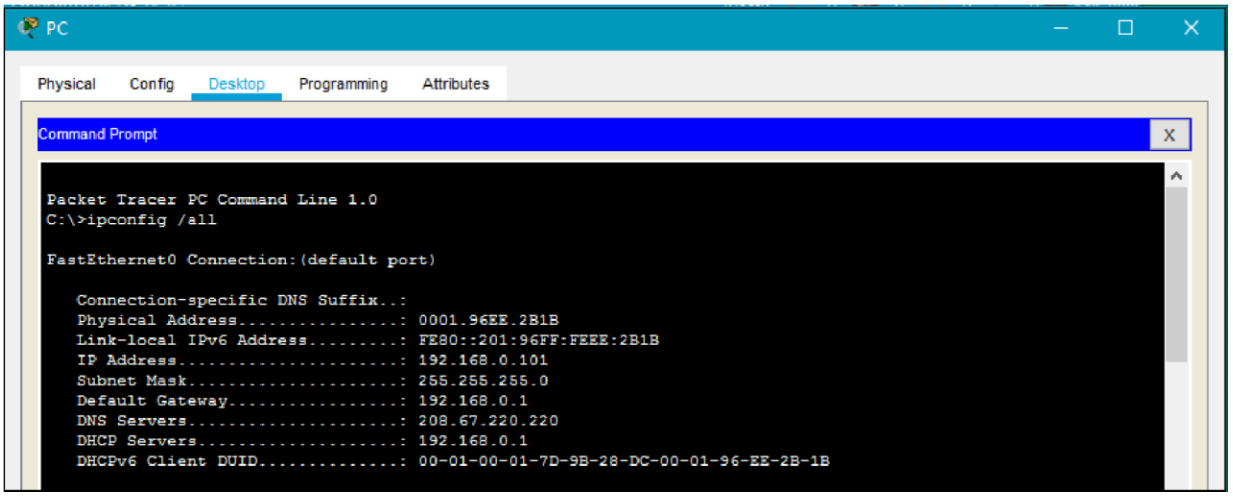


Step 3: Configure the PC

a. Configure the PC for the wired network
Click on the **PC** icon on the Packet Tracer **Logical** workspace and select the **Desktop** tab and then the **IP Configuration** icon.
In the IP Configuration window, select the **DCHP** radio button as shown in the figure so that the PC will use DCHP to receive an IPv4 address from the wireless router. Close the IP Configuration window.



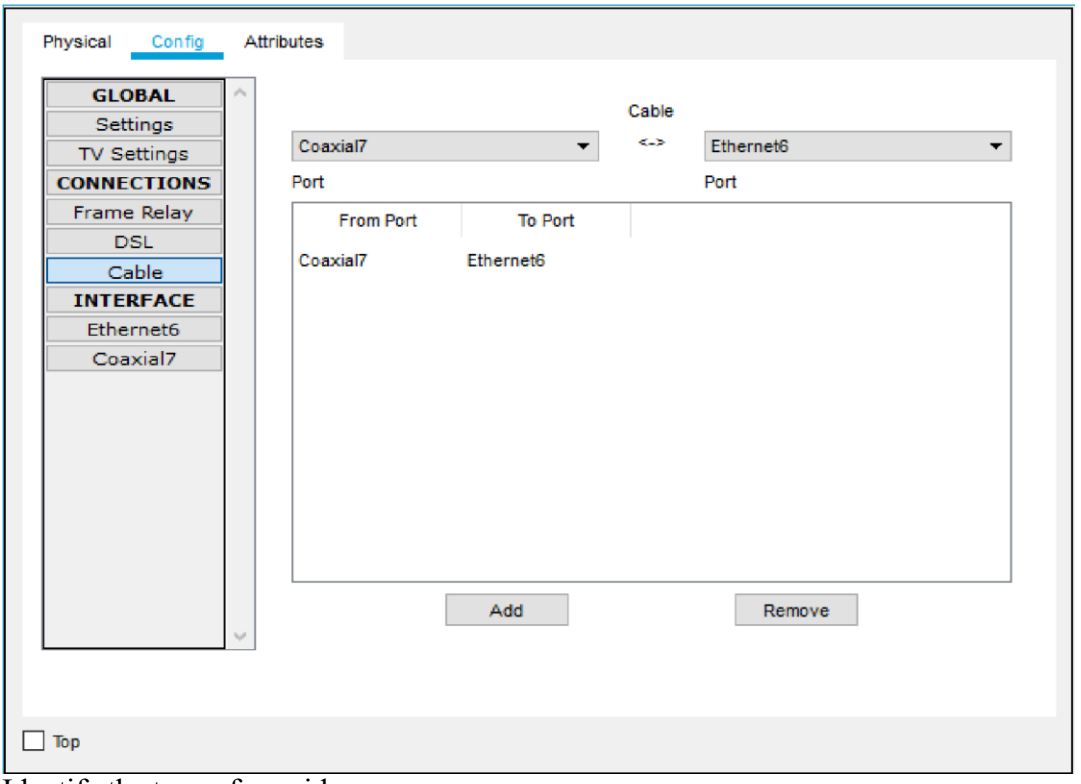
Click on the Command Prompt icon. Verify that the PC has received an IPv4 address by issuing the **ipconfig /all** command from the command prompt as shown in the figure. The PC should receive an IPv4 address in the 192.168.0.x range.



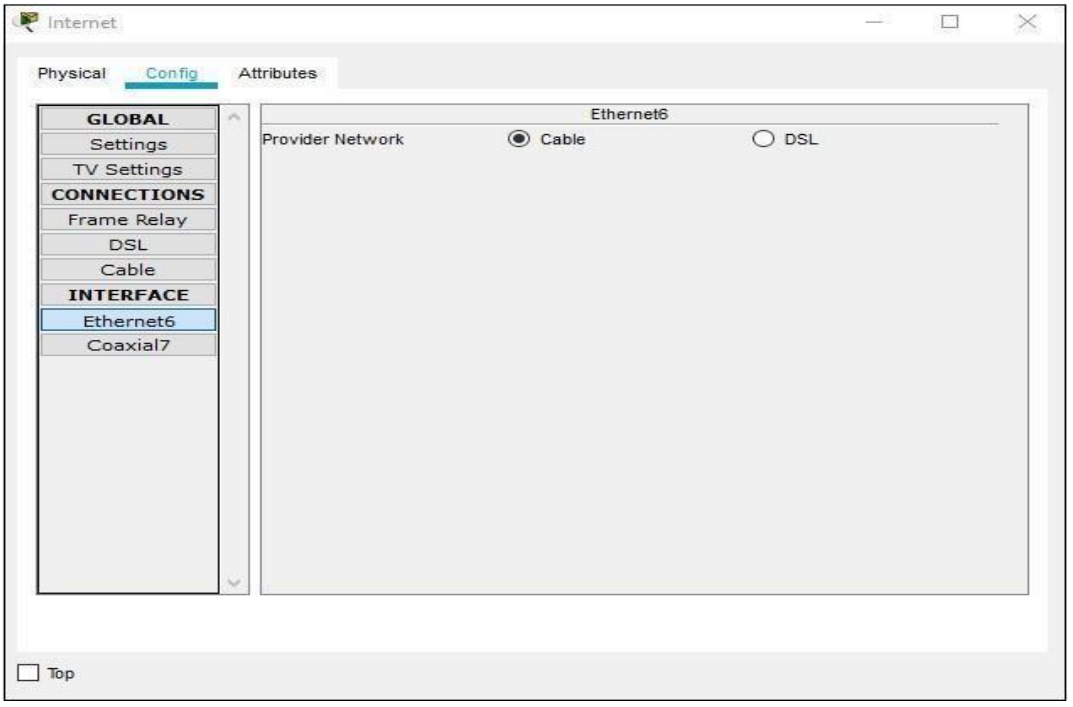
Step 4: Configure the Internet cloud

a. Install network modules if necessary
Click on the **Internet Cloud** icon on the Packet Tracer **Logical** workspace and then click on the **Physical** tab. The cloud device will need two modules if they are not already installed. The PT-CLOUD-NM-1CX which is for the cable modem service connection and the PT-CLOUD-NM-1CFE which is for a copper Ethernet cable connection. If these modules are missing, power off the physical cloud devices by clicking on the power button and drag each module to an empty module port on the device and then power the device back on.

b. Identify the From and To Ports
Click on the **Config** tab in the Cloud device window. In the left pane click on **Cable** under **CONNECTIONS**. In the first drop down box choose Coaxial and in the second drop down box choose
Ethernet then click the **Add** button to add these as the **From Port** and **To Port** as shown in the figure.



c. Identify the type of provider
While still in the **Config** tab click Ethernet under **INTERFACE** in the left pane. In the Ethernet configuration window select **Cable** as the Provider Network as shown in the figure.



Step 5: Configure the Cisco.com server

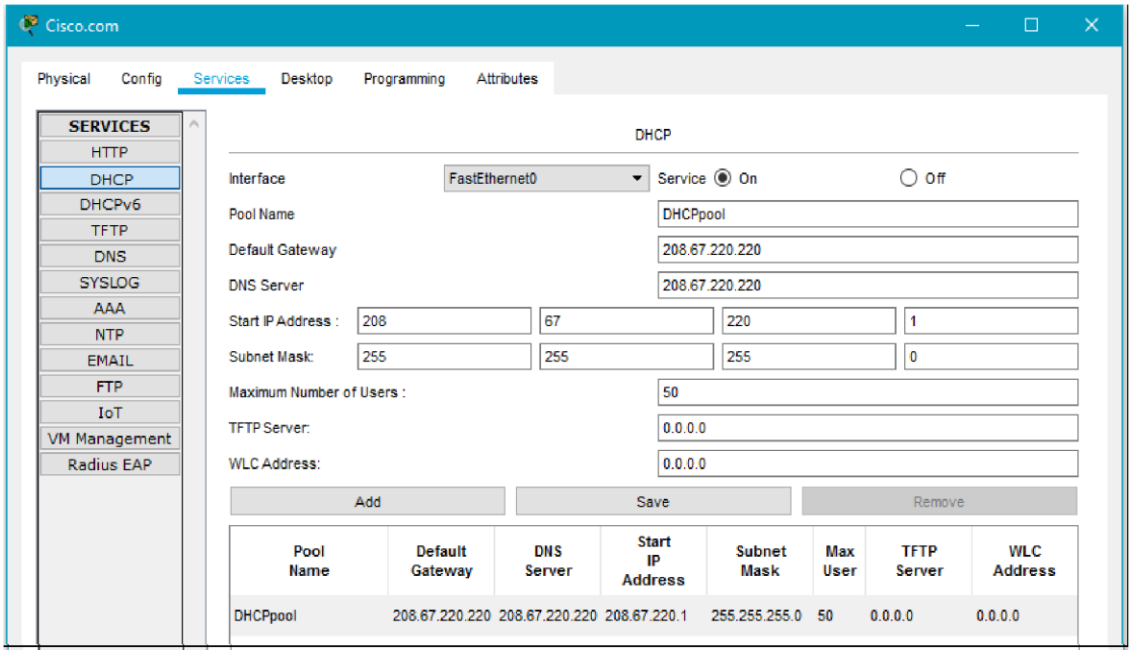
a. Configure the Cisco.com server as a DHCP server

Click on the Cisco.com server icon on the Packet Tracer **Logical** workspace and select the **Services** tab. Select **DHCP** from the **SERVICES** list in the left pane.

In the DHCP configuration window, configure a DHCP as shown in the figure with the following settings.

- ☐ Click **On** to turn the DCHP service on
- ☐ Pool name: DHCPpool
- ☐ Default Gateway: 208.67.220.220
- ☐ DNS Server: 208.67.220.220
- ☐ Starting IP Address: 208.67.220.1
- ☐ Subnet Mask 255.255.255.0
- ☐ Maximum number of Users: 50

Click **Add** to add the pool



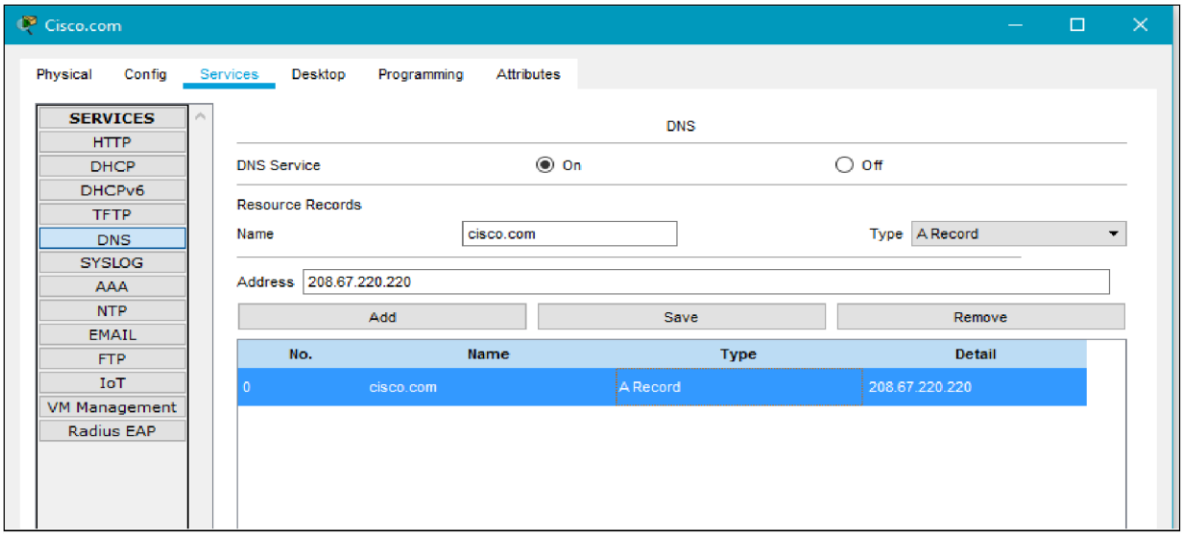
b. Configure the Cisco.com server as a DNS server to provide domain name to IPv4 address resolution.

While still in the **Services** tab, select **DNS** from the **SERVICES** listed in the left pane.

Configure the DNS service using the following settings as shown in the figure.

- Click **On** to turn the DNS service on
- Name: Cisco.com
- Type: A Record
- Address: 208.67.220.220

Click **Add** to add the DNS service settings



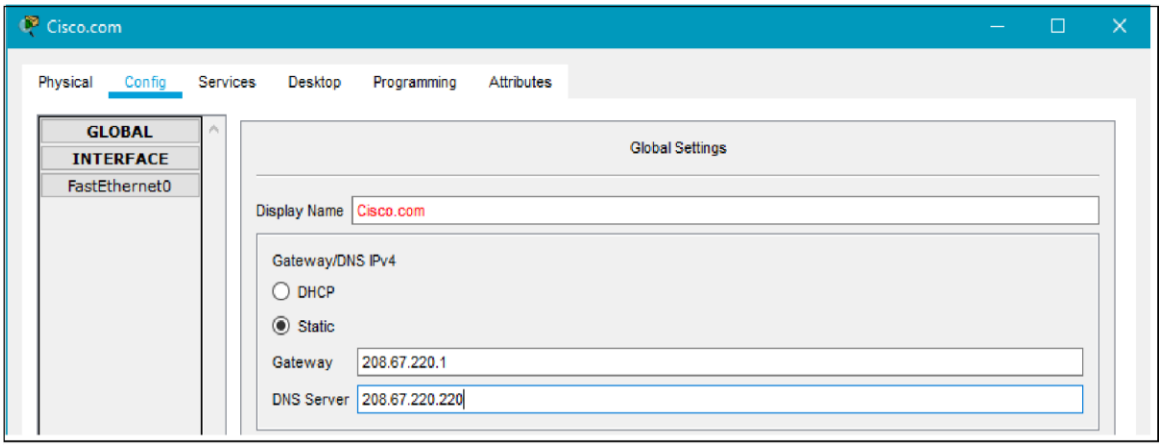
c. Configure the Cisco.com server Global settings.

Select the **Config** tab.

Click on **Settings** in left pane.

Configure the Global settings of the server as follows:

- Select **Static**
- Gateway: 208.67.220.1
- DNS Server: 208.67.220.220

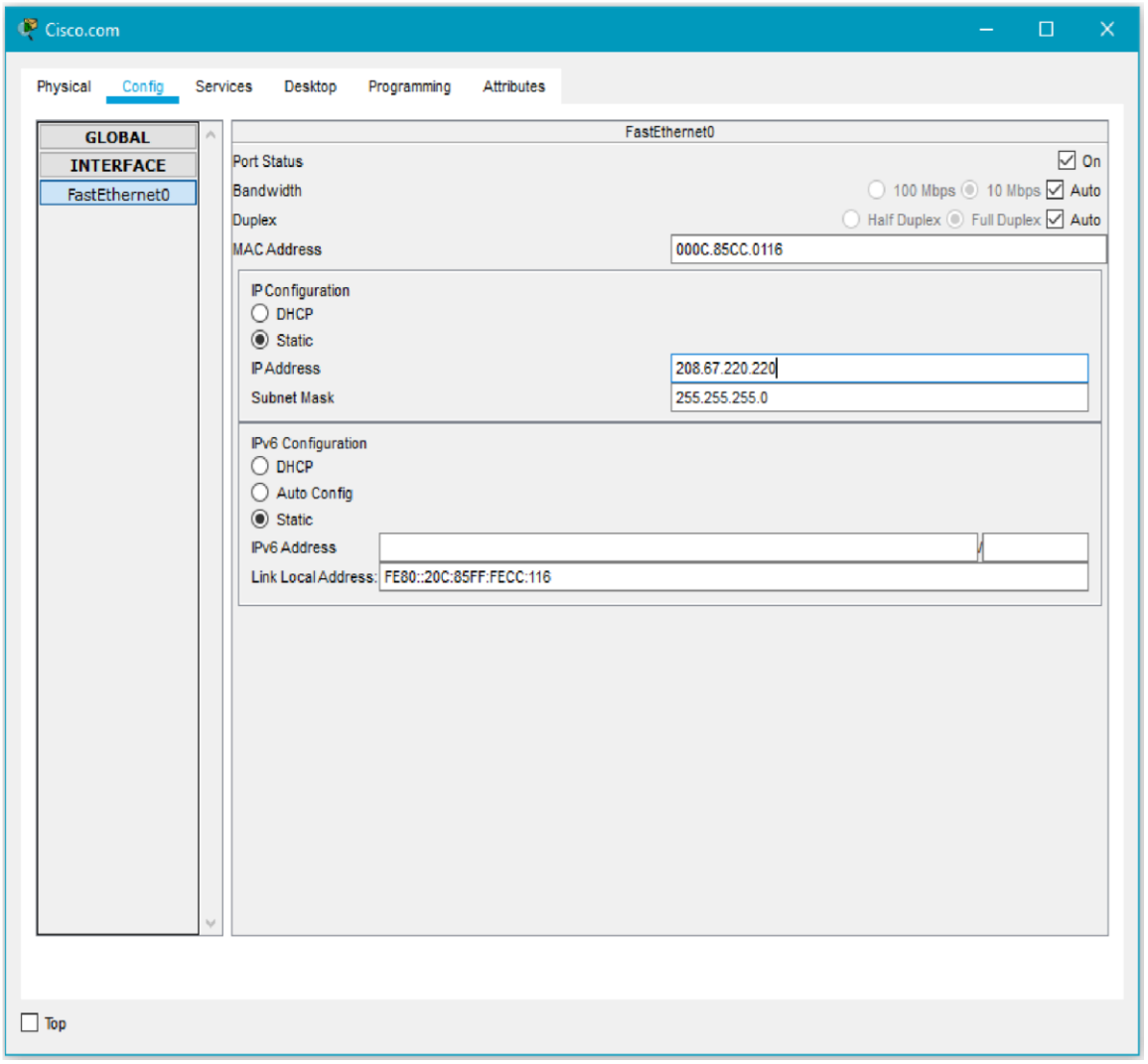


d. Configure the Cisco.com server FastEthernet0 Interface settings.

Click on **Fast Ethernet** in left pane of the **Config** tab

Configure the Fast Ethernet Interface settings of the server as follows:

- Select **Static** under IP Configuration
- IP Address: 208.67.220.220
- Subnet Mask: 255.255.255.0



Part 3: Verify Connectivity

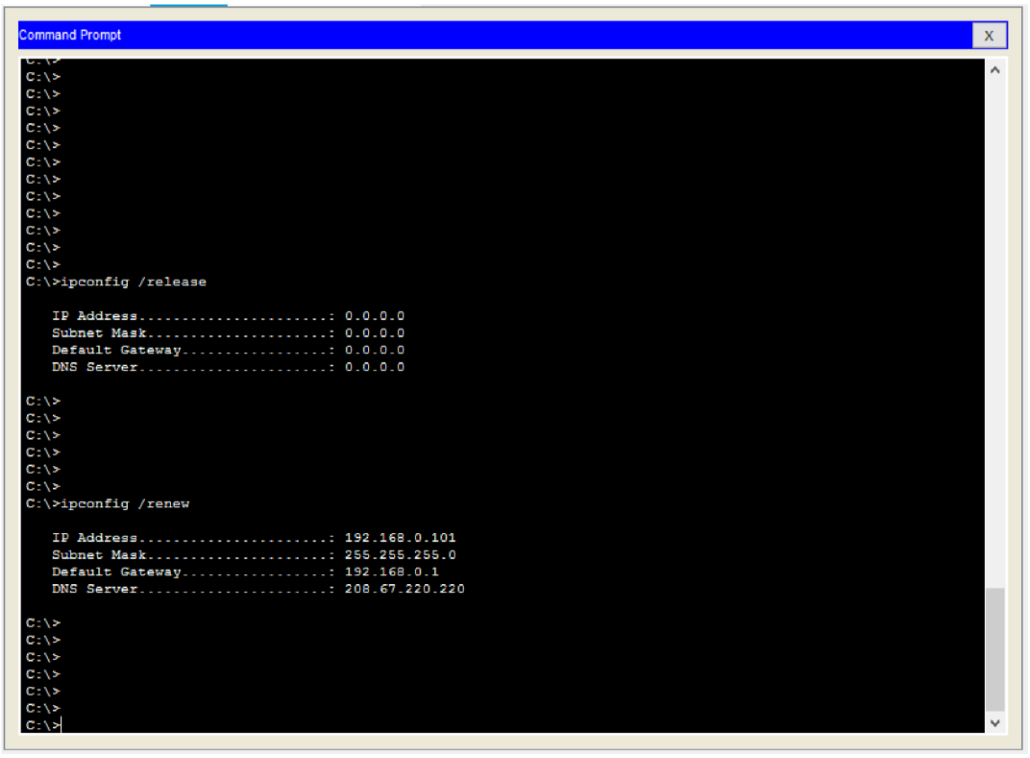
Step 1: Refresh the IPv4 settings on the PC

a) Verify that the PC is receiving IPv4 configuration information from DHCP.

Click on the **PC** on the Packet Tracer **Logical** workspace and then the select the **Desktop** tab of the PC configuration window.

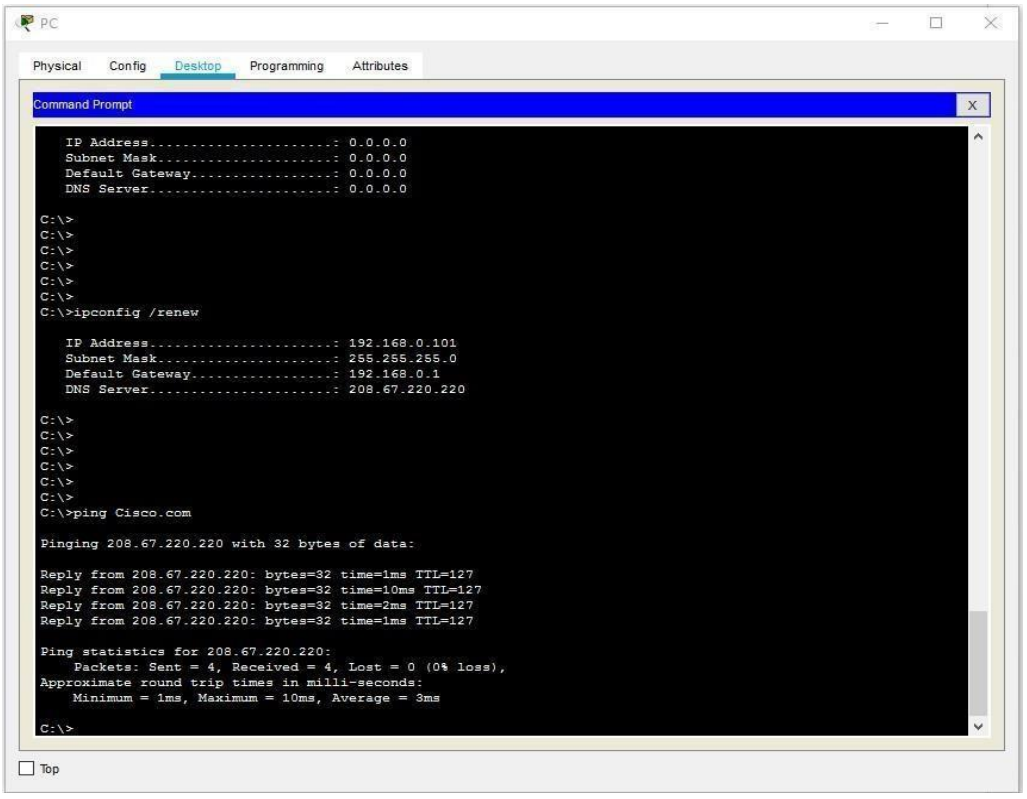
Click on the **Command Prompt** icon

In the command prompt refresh the IP settings by issuing the commands **ipconfig /release** and then **ipconfig /renew.** The output should show that the PC has an IP address in the 192.168.0.x range, a subnet mask, a default gateway, and DNS server address as shown in the figure.



b) Test connectivity to the Cisco.com server from the PC

From the command prompt, issue the command **ping Cisco.com.** It may take a few seconds for the ping to return. Four replies should be received as shown in the figure.



Student observation:

1. **Write down the key features of configuring Wireless router and DHCP server.**
2. **What is the significance of DHCP sever in internetworking.**
3. **Design and configure an inter-network in your lab using switch, router and Ethernet cables. Draw and label the design in your notebook. Also, show the ip address configuration of each and every device.**

Practical 11

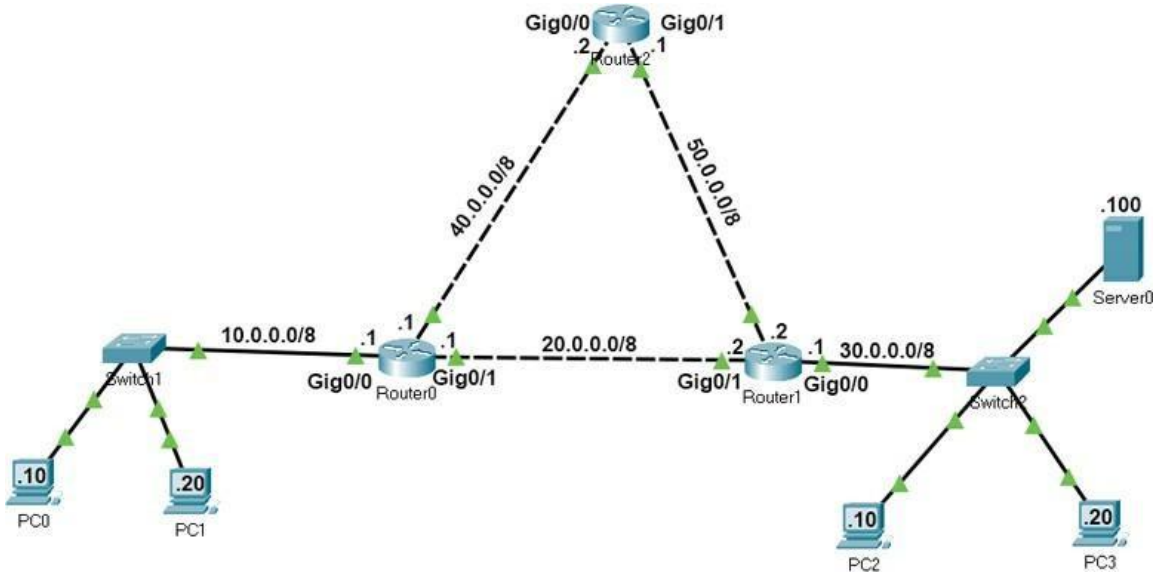
AIM:- a)Simulate Static Routing Configuration using CISCO Packet Tracer

Static routes are the routes you manually add to the router's routing table. The process of adding static routes to the routing table is known as static routing. Let's take a packet tracer example to understand how to use static routing to create and add a static route to the routing table.

Setting up a practice lab

Create a packet tracer lab as shown in the following image or download the following pre-created lab and load it on Packet Tracer.

Packet Tracer Lab with Initial IP Configuration



In this lab, each network has two routes to reach. We will configure one route as the main route and another route as the backup route. If the link bandwidth of all routes is the same, we use the route that has the least number of routers as the main route. If the link bandwidth and the number of routers are the same, we can use any route as the main route and another route as the backup route.

If we specify two routes for the same destination, the router automatically selects the best route for the destination and adds the route to the routing table. If you manually want to select a route that the router should add to the routing table, you have to set the AD value of the route lower than other routes. For example, if you use the following commands to create two static routes for network 30.0.0/8, the route will place the first route to the routing table.

```
#ip route 30.0.0.0 255.0.0.0 20.0.0.2 10
#ip route 30.0.0.0 255.0.0.0 40.0.0.2 20
```

If the first route fails, the router automatically adds the second route to the routing table.

Creating, adding, verifying static routes

Routers automatically learn their connected networks. We only need to add routes for the networks that are not available on the router's interfaces. For example, network 10.0.0.0/8, 20.0.0.0/8 and 40.0.0.0/8 are directly connected to Router0. Thus, we don't need to configure routes for these

networks. Network 30.0.0.0/8 and network 50.0.0.0/8 are not available on Router0. We have to create and add routes only for these networks.

The following table lists the connected networks of each router.

Router	Available networks on local interfaces	Networks available on other routers' interfaces
Router0	10.0.0.0/8, 20.0.0.0/8, 40.0.0.0/8	30.0.0.0/8, 50.0.0.0/8
Router1	20.0.0.0/8, 30.0.0.0/8, 50.0.0.0/8	10.0.0.0/8, 40.0.0.0/8
Router2	40.0.0.0/8, 50.0.0.0/8	10.0.0.0/8, 20.0.0.0/8, 30.0.0.0/8

Let's create static routes on each router for networks that are not available on the router.

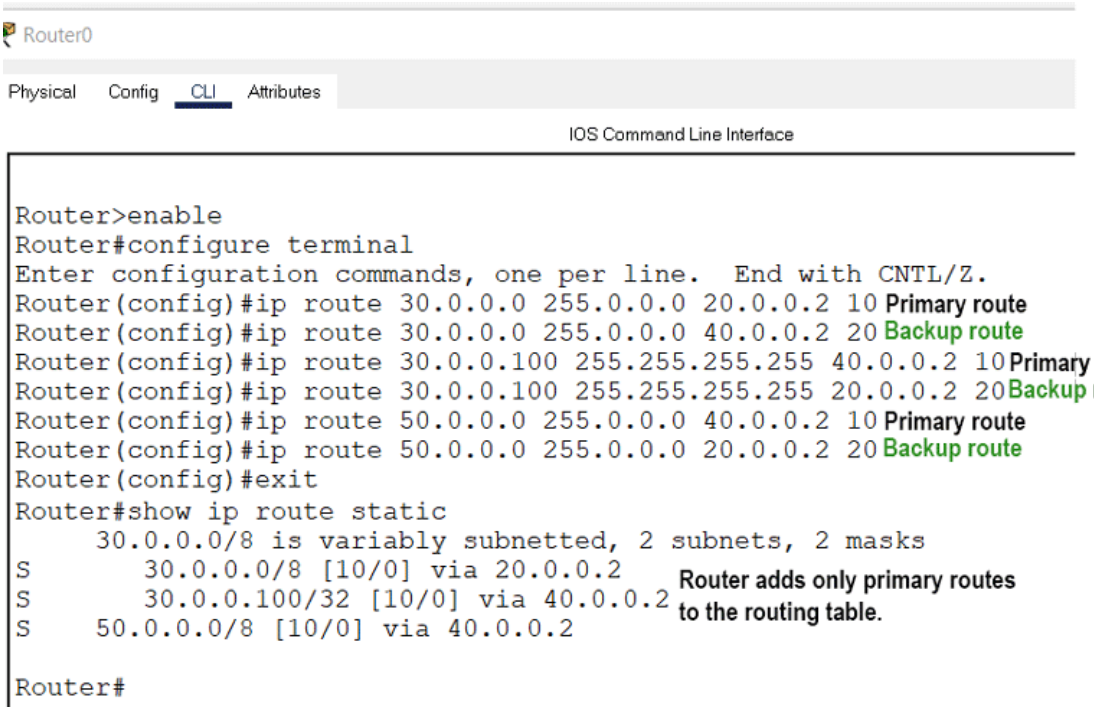
Router0 requirements

- Create two routes for network 30.0.0.0/8 and configure the first route (via -Router1) as the main route and the second route (via-Router2) as a backup route.
- Create two routes for the host 30.0.0.100/8 and configure the first route (via -Router2) as the main route and the second route (via-Router1) as a backup route.
- Create two routes for network 50.0.0.0/8 and configure the first route (via -Router2) as the main route and the second route (via-Router1) as a backup route.
- Verify the router adds only main routes to the routing table.

Router0 configuration

Access the CLI prompt of Router0 and run the following commands.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2 10
Router(config)#ip route 30.0.0.0 255.0.0.0 40.0.0.2 20
Router(config)#ip route 30.0.0.100 255.255.255.255 40.0.0.2 10
Router(config)#ip route 30.0.0.100 255.255.255.255 20.0.0.2 20
Router(config)#ip route 50.0.0.0 255.0.0.0 40.0.0.2 10
Router(config)#ip route 50.0.0.0 255.0.0.0 20.0.0.2 20
Router(config)#exit
Router#show ip route static
30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S 30.0.0.0/8 [10/0] via 20.0.0.2
S 30.0.0.100/32 [10/0] via 40.0.0.2
S 50.0.0.0/8 [10/0] via 40.0.0.2
Router#
```

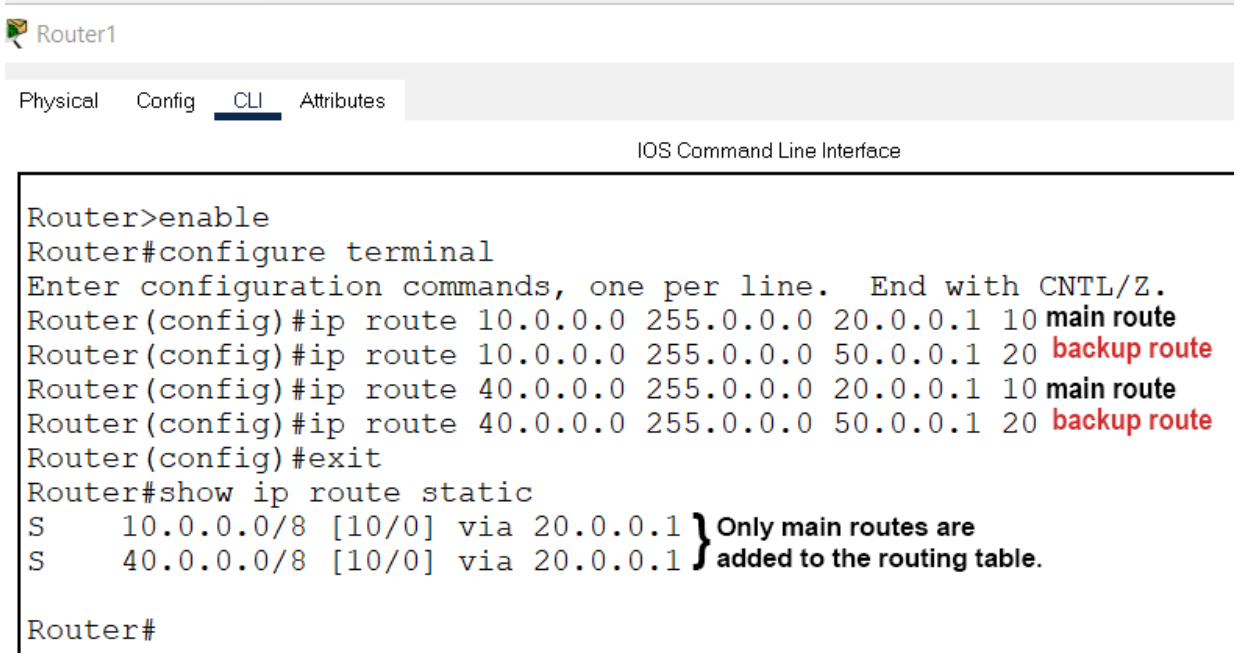


Router1 requirements

- Create two routes for network 10.0.0.0/8 and configure the first route (via -Router0) as the main route and the second route (via-Router1) as a backup route.
- Create two routes for network 40.0.0.0/8 and configure the first route (via -Router0) as the main route and the second route (via-Router2) as a backup route.
- Verify the router adds only main routes to the routing table.

Router1 configuration

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1 10
Router(config)#ip route 10.0.0.0 255.0.0.0 50.0.0.1 20
Router(config)#ip route 40.0.0.0 255.0.0.0 20.0.0.1 10
Router(config)#ip route 40.0.0.0 255.0.0.0 50.0.0.1 20
Router(config)#exit
Router#show ip route static
S 10.0.0.0/8 [10/0] via 20.0.0.1
S 40.0.0.0/8 [10/0] via 20.0.0.1
Router#
```

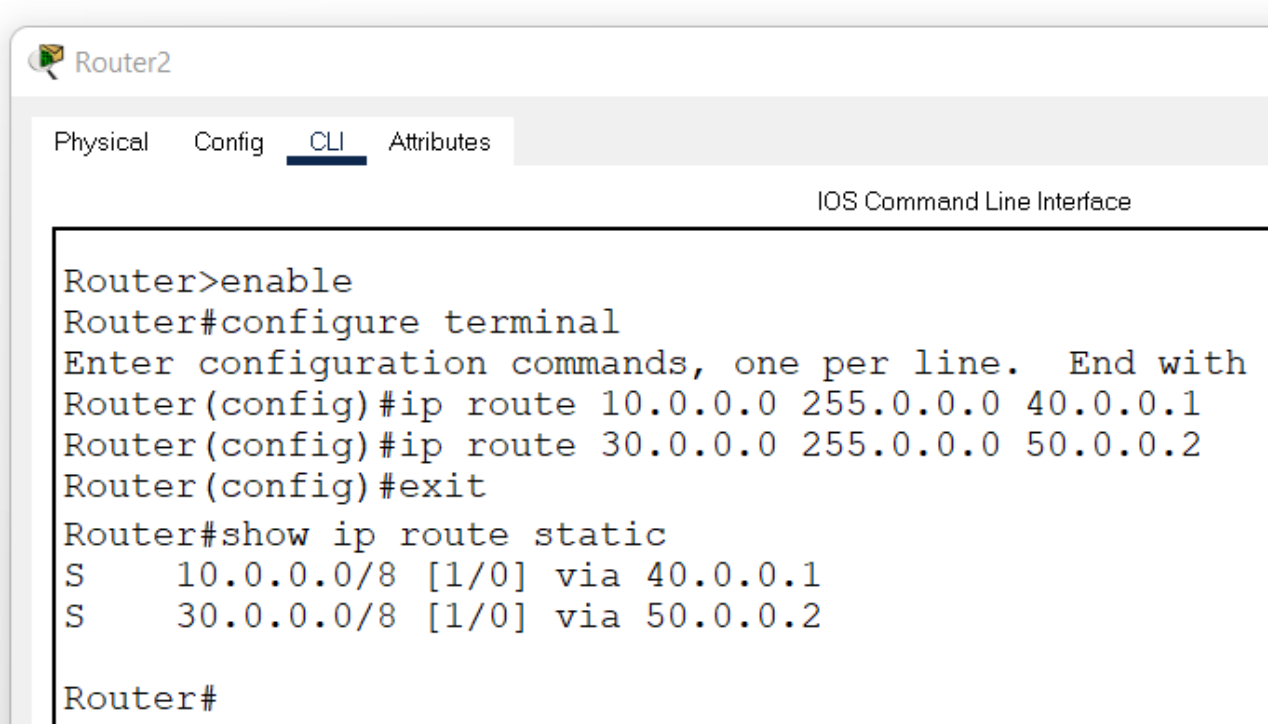


Router2 requirements

Create static routes for network 10.0.0.0/8 and network 30.0.0.0/8 and verify the router adds both routes to the routing table.

Router2 configuration

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 10.0.0.0 255.0.0.0 40.0.0.1
Router(config)#ip route 30.0.0.0 255.0.0.0 50.0.0.2
Router(config)#exit
Router#show ip route static
S 10.0.0.0/8 [1/0] via 40.0.0.1
S 30.0.0.0/8 [1/0] via 50.0.0.2
Router#
```



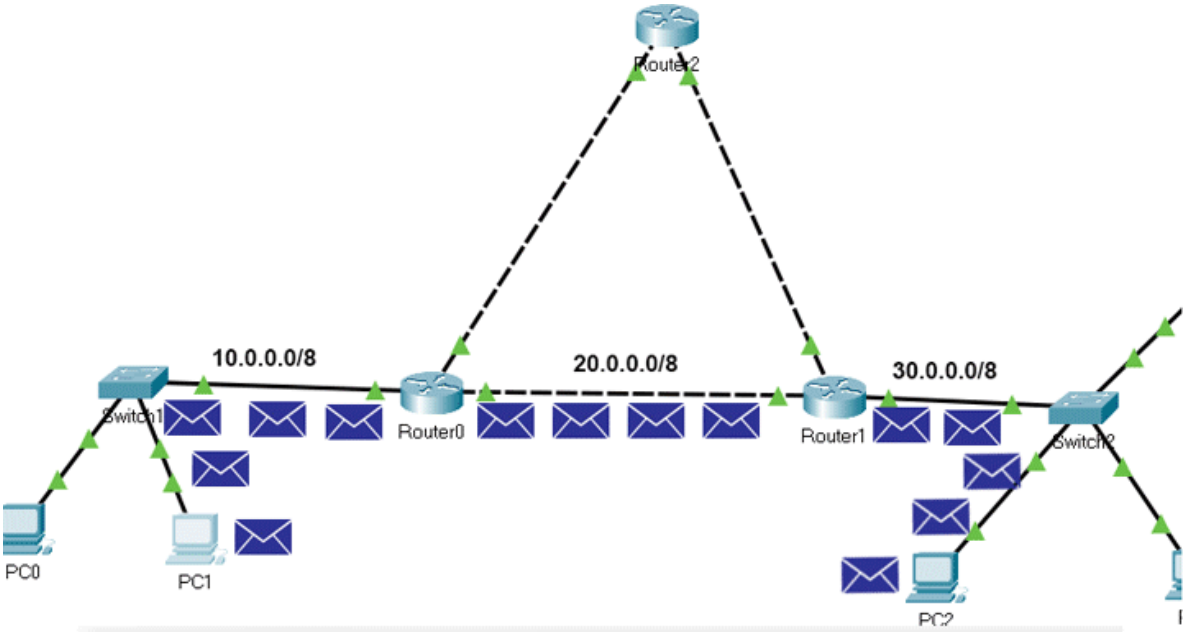
Verifying static routing

On Router0, we configured two routes for network 30.0.0.0/8. These routes are via Router1 and via Router2. We set the first route (via-Router1) as the main route and the second route as the backup route. We can verify this configuration in two ways.

By sending ping requests to a PC of network 30.0.0.0/8 and tracing the path they take to reach the network 30.0.0.0/8. For this, you can use **'tracert'** command on a PC of network 10.0.0.0/8. The **'tracert'** command sends ping requests to the destination host and tracks the path they take to reach the destination.

By listing the routing table entries on Router0. Since a router uses the routing table to forward data packets, you can check the routing table to figure out the route the router uses to forward data packets for each destination.

The following image shows the above testing.



Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>enable
Router#show ip route static
     30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       30.0.0.0/8 [10/0] via 20.0.0.2
S       30.0.0.100/32 [10/0] via 40.0.0.2
S    50.0.0.0/8 [10/0] via 40.0.0.2

Router#
```

PC1

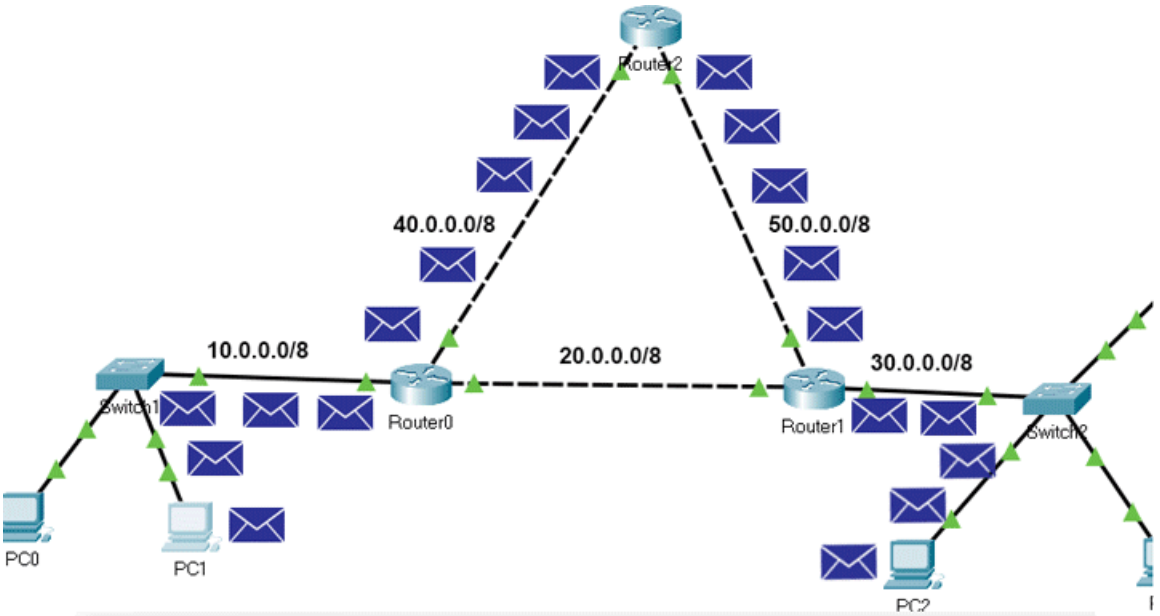
Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>tracert 30.0.0.20

Tracing route to 30.0.0.20 over a maximum of 30
hops:

  1    0 ms      0 ms      0 ms      10.0.0.1
  2    0 ms      0 ms      0 ms      20.0.0.2
  3    *         0 ms      0 ms      30.0.0.20

Trace complete.

C:\>
```

We also configured a separate static host route for the host 30.0.0.100/8. The router must use this route to forward data packets to the host 30.0.0.100/8. To verify this, you can do the same testing for the host 30.0.0.100/8.

The following image shows this testing.



Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>enable
Router#show ip route static
     30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       30.0.0.0/8 [10/0] via 20.0.0.2
S       30.0.0.100/32 [10/0] via 40.0.0.2
S    50.0.0.0/8 [10/0] via 40.0.0.2

Router#
```

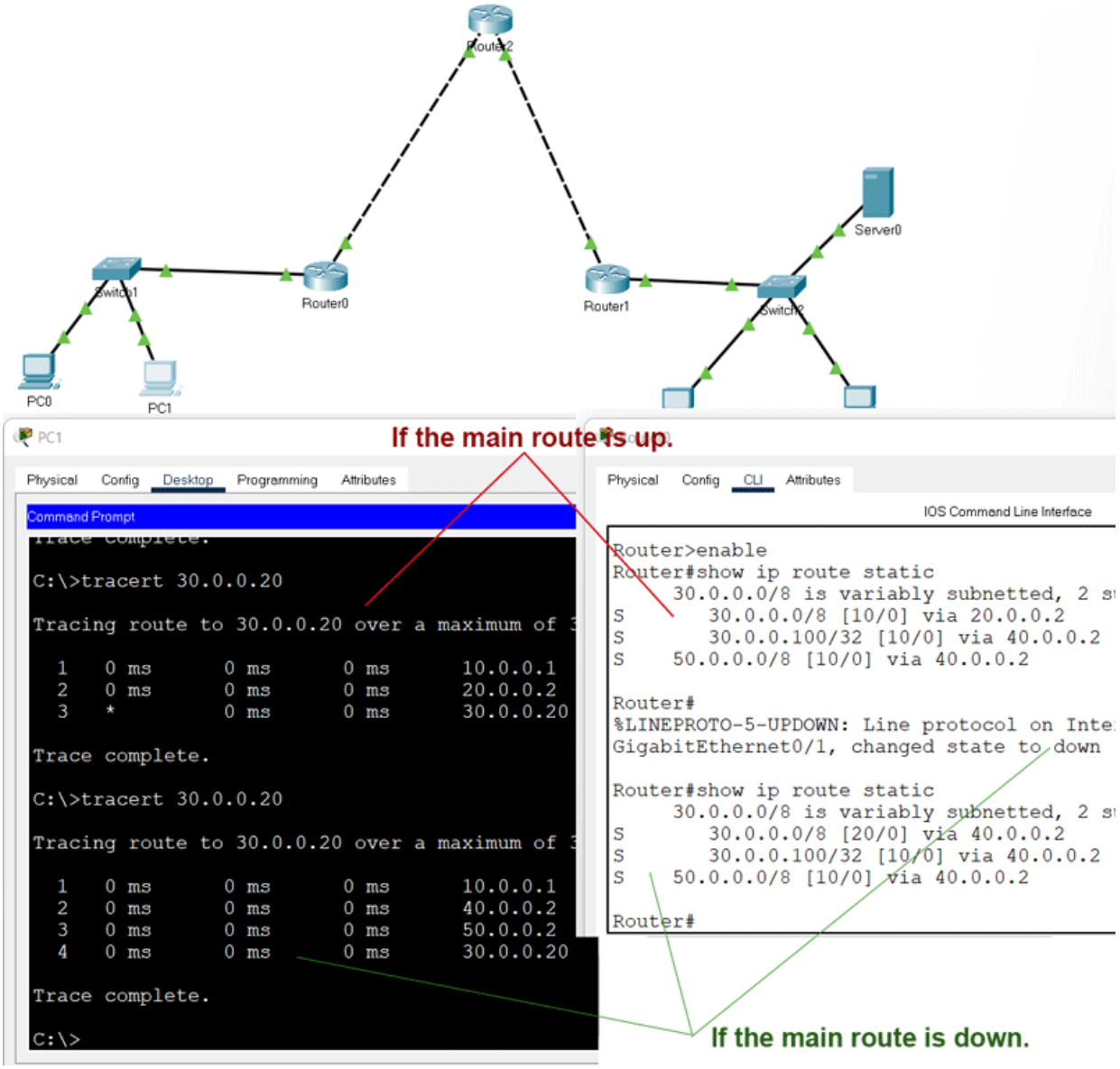
PC1

Physical Config Desktop Programming Attributes

```
Packet Tracer PC Command Line 1.0
C:\>tracert 30.0.0.100

Tracing route to 30.0.0.100 over a maximum of 30
hops:

  1    1 ms       0 ms       0 ms       10.0.0.1
  2    *          0 ms       0 ms       40.0.0.2
  3    *          *          0 ms       20.0.0.2
  4    *          0 ms       0 ms       30.0.0.100

Trace complete.

C:\>
```

We also configured a backup route for network 30.0.0.0/8. The router must put the backup route to the routing table and use it to forward data packets to network 30.0.0.0/8 when the main route fails. To verify this, we have to simulate the failure of the main route.

To simulate the failure of the main route, you can delete the link between Router0 and Router1. After deleting the link, do the same testing again for the network 30.0.0.0/8.



The following link provides the configured packet tracer lab of the above example.
Packet Tracer Lab with Static Routing Configuration

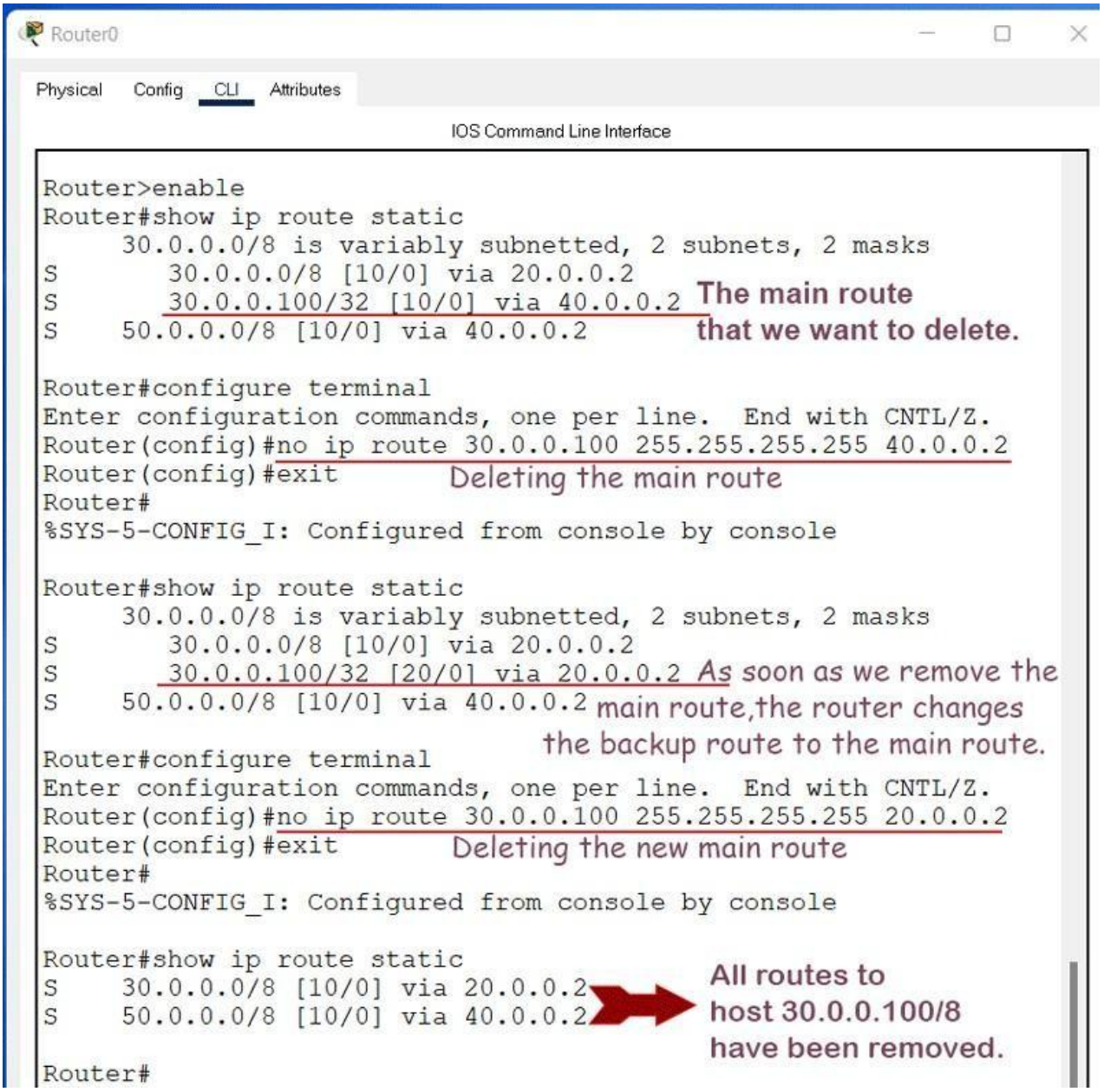
Deleting a static route

To delete a static route, use the following steps.

- Use the **'show ip route static'** command to print all static routes.
- Note down the route you want to delete.
- Use the **'no ip route'** command to delete the route.

If you have a backup route, the backup route becomes the main route when you delete the main route.

In our example, we have a backup route and a main route for the host 30.0.0.100/8. The following image shows how to delete both routes.


Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>enable
Router#show ip route static
30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S 30.0.0.0/8 [10/0] via 20.0.0.2
S 30.0.0.100/32 [10/0] via 40.0.0.2
S 50.0.0.0/8 [10/0] via 40.0.0.2
The main route that we want to delete.
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip route 30.0.0.100 255.255.255.255 40.0.0.2
Router(config)#exit
Deleting the main route
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip route static
30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S 30.0.0.0/8 [10/0] via 20.0.0.2
S 30.0.0.100/32 [20/0] via 20.0.0.2
S 50.0.0.0/8 [10/0] via 40.0.0.2
As soon as we remove the main route,the router changes the backup route to the main route.
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip route 30.0.0.100 255.255.255.255 20.0.0.2
Router(config)#exit
Deleting the new main route
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip route static
S 30.0.0.0/8 [10/0] via 20.0.0.2
S 50.0.0.0/8 [10/0] via 40.0.0.2
All routes to host 30.0.0.100/8 have been removed.
Router#

Practical 11

AIM:- b)Simulate RIP using CISCO Packet Tracer

Initial IP configuration

Device	Interface	IP Configuration	Connected with
PC0	Fast Ethernet	10.0.0.2/8	Router0's Fa0/1
Router0	Fa0/1	10.0.0.1/8	PC0's Fast Ethernet
Router0	S0/0/1	192.168.1.254/30	Router2's S0/0/1
Router0	S0/0/0	192.168.1.249/30	Router1's S0/0/0
Router1	S0/0/0	192.168.1.250/30	Router0's S0/0/0
Router1	S0/0/1	192.168.1.246/30	Router2's S0/0/0
Router2	S0/0/0	192.168.1.245/30	Router1's S0/0/1
Router2	S0/0/1	192.168.1.253/30	Router0's S0/0/1
Router2	Fa0/1	20.0.0.1/30	PC1's Fast Ethernet
PC1	Fast Ethernet	20.0.0.2/30	Router2's Fa0/1

Assign IP address to PCs

Double click **PCs** and click **Desktop** menu item and click **IP Configuration**. Assign IP address referring the above table.

Assign IP address to interfaces of routers

Double click **Router0** and click **CLI** and press **Enter key** to access the command prompt of **Router0**.

We need to configure IP address and other parameters on interfaces before we could actually use them for routing. Interface mode is used to assign IP address and other parameters. Interface mode can be accessed from global configuration mode. Following commands are used to access the global configuration mode.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

From global configuration mode we can enter in interface mode. From there we can configure the interface. Following commands will assign IP address on FastEthernet0/0.

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

interface *fastEthernet 0/0* command is used to enter in interface mode.
ip address *10.0.0.1 255.0.0.0* command will assign IP address to interface.

no shutdown command will bring the interface up.
exit command is used to return in global configuration mode.
Serial interface needs two additional parameters **clock rate** and **bandwidth**. Every serial cable has two ends DTE and DCE. These parameters are always configured at DCE end.
We can use **show controllers interface** command from privilege mode to check the cable's end.

```
Router#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 2000000
[Output omitted]
```

Fourth line of output confirms that DCE end of serial cable is attached. If you see DTE here instead of DCE skip these parameters.
Now we have necessary information let's assign IP address to serial interface.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.249 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.1.254 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Router#configure terminal Command is used to enter in global configuration mode.
Router(config)#interface *serial 0/0/0* Command is used to enter in interface mode.
Router(config-if)#ip address *192.168.1.249 255.255.255.252* Command assigns IP address to interface. For serial link we usually use IP address from /30 subnet.
Router(config-if)#clock rate *64000* And **Router(config-if)#bandwidth *64*** In real life environment these parameters control the data flow between serial links and need to be set at service providers end. In lab environment we need not to worry about these values. We can use these values.
Router(config-if)#no shutdown Command brings interface up.
Router(config-if)#exit Command is used to return in global configuration mode.
We will use same commands to assign IP addresses on interfaces of remaining routers. We need to provided clock rate and bandwidth only on DCE side of serial interface. Following command will assign IP addresses on interface of Router1.

Router1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.250 255.255.255.252
```

```
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.1.246 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth  64
Router(config-if)#no shutdown
Router(config-if)#exit
```

Use same commands to assign IP addresses on interfaces of Router2.

Router2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.245 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.1.253 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

Now routers have information about the networks that they have on their own interfaces. Routers will not exchange this information between them on their own. We need to implement RIP routing protocol that will insist them to share this information.

Configure RIP routing protocol

Configuration of RIP protocol is much easier than you think. It requires only two steps to configure the RIP routing.

- Enable RIP routing protocol from global configuration mode.
- Tell RIP routing protocol which networks you want to advertise.

Let's configure it in Router0

Router0

```
Router0(config)#router rip
Router0(config-router)# network 10.0.0.0
Router0(config-router)# network 192.168.1.252
Router0(config-router)# network 192.168.1.248
```

router rip command tell router to enable the RIP routing protocol.

network command allows us to specify the networks which we want to advertise. We only need to specify the networks which are directly connected with the router.

That's all we need to configure the RIP. Follow same steps on remaining routers.

Router1

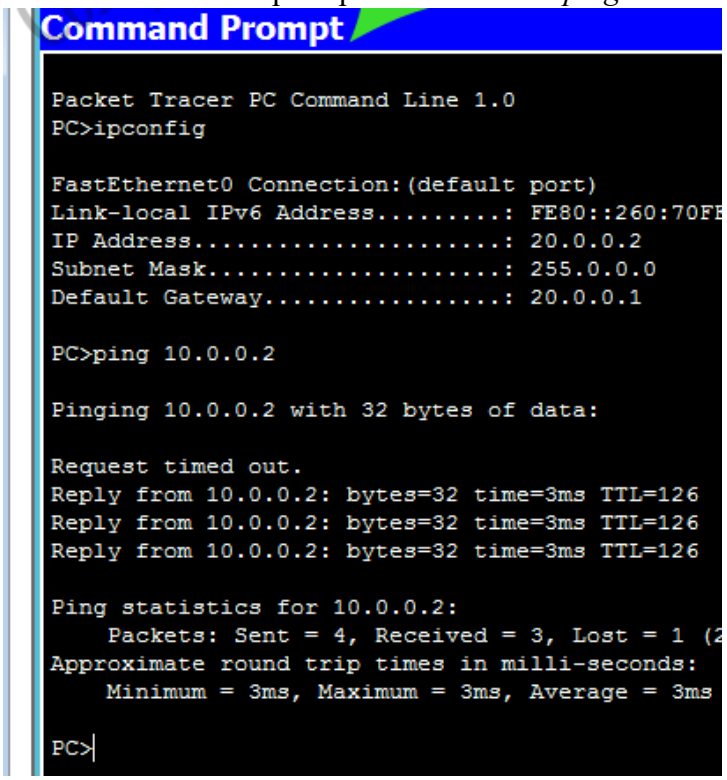
```
Router1(config)#router rip
Router1(config-router)# network 192.168.1.244
Router1(config-router)# network 192.168.1.248
```

Router2

```
Router2(config)#router rip
```

```
Router2(config-router)# network 20.0.0.0
Router2(config-router)# network 192.168.1.252
Router2(config-router)# network 192.168.1.244
```

That's it. Our network is ready to take the advantage of RIP routing. To verify the setup we will use ping command. ping command is used to test the connectivity between two devices. Access the command prompt of **PC1** and use *ping* command to test the connectivity from **PC0**.



RIP protocol automatically manage all routes for us. If one route goes down, it automatically switches to another available. To explain this process more clearly we have added one more route in our network.

Currently there are two routes between PC0 and PC1.

Route 1

PC0 [Source / destination – 10.0.0.2] <==> Router0 [FastEthernet0/1 – 10.0.0.1] <==> Router0 [Serial0/0/1 – 192.168.1.254] <==> Router2 [Serial 0/0/1 – 192.168.1.253] <==> Router2 [FastEthernet0/0 – 20.0.0.1] <==> PC1 [Destination /source – 20.0.0.2]

Route 2

PC0 [Source / destination – 10.0.0.2] <==> Router0 [FastEthernet0/1 – 10.0.0.1] <==> Router0 [Serial0/0/0 – 192.168.1.249] <==> Router1 [Serial 0/0/0 – 192.168.1.250] <==> Router1 [Serial 0/0/1 – 192.168.1.246] <==> Router2 [Serial 0/0/0 – 192.168.1.245] <==> Router2 [FastEthernet0/0 – 20.0.0.1] <==> PC1 [Destination /source – 20.0.0.2]

By default RIP will use the route that has low hops counts between source and destination. In our network route1 has low hops counts, so it will be selected. We can use *tracert* command to verify it.

Now suppose route1 is down. We can simulate this situation by removing the cable attached between **Router0 [s0/0/1]** and **Router2 [s0/0/1]**.

What will happen now? There is no need to worry. RIP will automatically reroute the traffic. Use ***tracert*** command again to see the magic of dynamic routing.

Practical 12

AIM: - a) Implement echo client server using TCP/UDP sockets.

Algorithm:-

Input:-

Output:-

Practical 12

AIM: - b) Implement chat client server using TCP/UDP sockets.

Algorithm:-

Input:-

Output:-

Practical 13

AIM: - Implement your own ping program

Algorithm:

Input:-

Output:-

Practical 14

AIM: - Write a code using RAW sockets to implement packet sniffing.

Algorithm:

Input:-

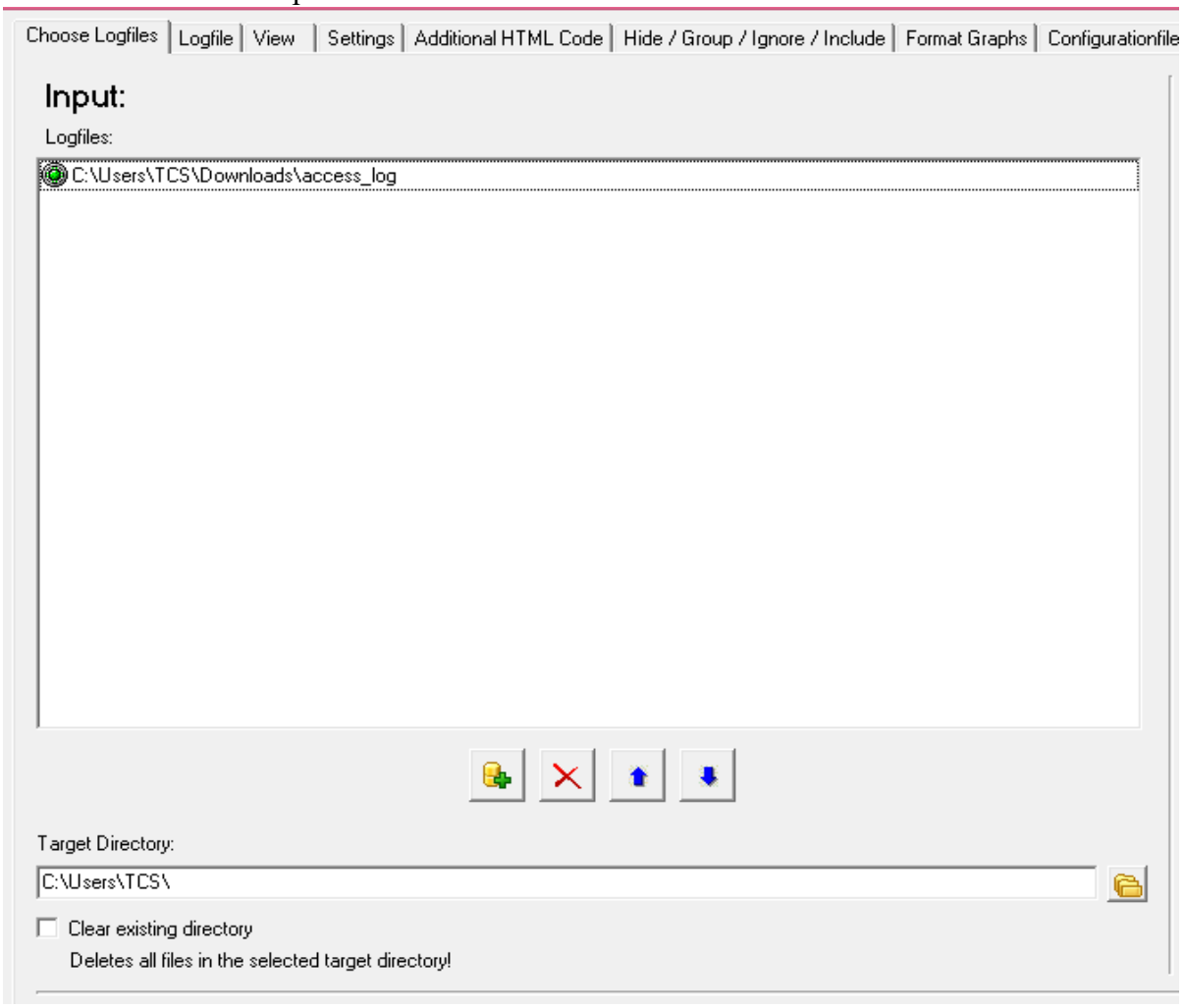
Output:-

Practical 15

AIM:- To analyze the different types of web logs using Webalizer tool.

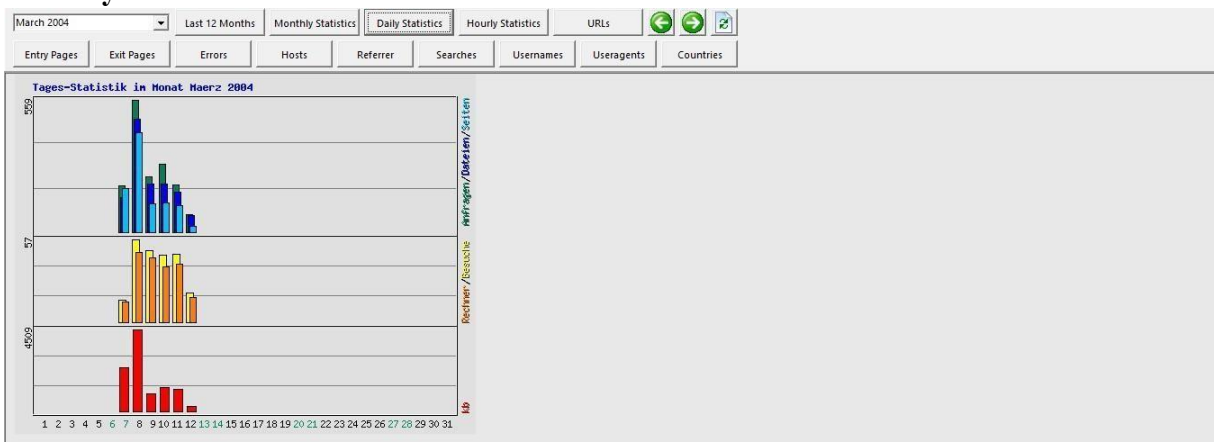
Procedure

Step1: Run webalizer windows version
Step2. Input web log file (down load from web)
Step3: Press Run webalizer



Output:

Monthly statistics

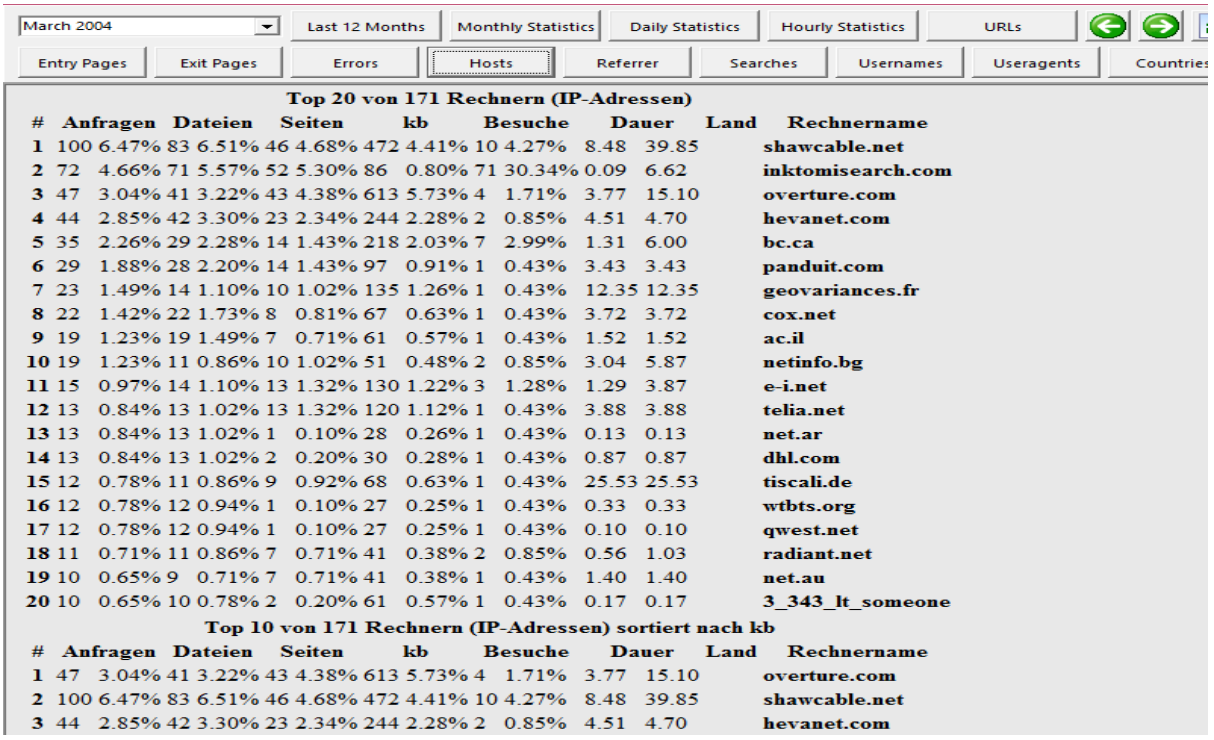


Seiten - Dokument-Abfragen (z.B. html, asp, txt); Dateien - erfolgreiche Anfragen für alle Typen (z.B. html, gif, css); Treffer - alle Anfragen, inklusive Fehler;

Tages-Statistik im Monat Maerz 2004

Tag	Anfragen			Dateien			Seiten			Besuche			Rechner			kb		
	Summe	Schnitt	Maximum	Summe	Schnitt	Maximum	Summe	Schnitt	Maximum	Summe	Schnitt	Maximum	Summe	Schnitt	Maximum	Summe	Schnitt	Maximum
7	197 12.74%	25	29	147 11.54%	18	21	186 18.94%	23	27	15 6.41%	2	3	14 8.19%	2	3	2383 22.27%	298	542
8	559 36.16%	24	63	478 37.52%	21	56	419 42.67%	18	40	57 24.36%	2	7	48 28.07%	2	7	4509 42.14%	196	386
9	232 15.01%	11	29	205 16.09%	10	29	118 12.02%	6	16	49 20.94%	2	5	44 25.73%	2	5	955 8.93%	45	138
10	286 18.50%	14	102	205 16.09%	10	34	124 12.63%	6	28	46 19.66%	2	5	38 22.22%	2	4	1336 12.49%	67	379

Hosts



Top 20 von 171 Rechnern (IP-Adressen)

#	Anfragen	Dateien	Seiten	kb	Besuche	Dauer	Land	Rechnername
1	100 6.47%	83 6.51%	46 4.68%	472 4.41%	10 4.27%	8.48	39.85	shawcable.net
2	72 4.66%	71 5.57%	52 5.30%	86 0.80%	71 30.34%	0.09	6.62	inktomisearch.com
3	47 3.04%	41 3.22%	43 4.38%	613 5.73%	4 1.71%	3.77	15.10	overture.com
4	44 2.85%	42 3.30%	23 2.34%	244 2.28%	2 0.85%	4.51	4.70	hevanet.com
5	35 2.26%	29 2.28%	14 1.43%	218 2.03%	7 2.99%	1.31	6.00	bc.ca
6	29 1.88%	28 2.20%	14 1.43%	97 0.91%	1 0.43%	3.43	3.43	panduit.com
7	23 1.49%	14 1.10%	10 1.02%	135 1.26%	1 0.43%	12.35	12.35	geovariances.fr
8	22 1.42%	22 1.73%	8 0.81%	67 0.63%	1 0.43%	3.72	3.72	cox.net
9	19 1.23%	19 1.49%	7 0.71%	61 0.57%	1 0.43%	1.52	1.52	ac.il
10	19 1.23%	11 0.86%	10 1.02%	51 0.48%	2 0.85%	3.04	5.87	netinfo.bg
11	15 0.97%	14 1.10%	13 1.32%	130 1.22%	3 1.28%	1.29	3.87	e-i.net
12	13 0.84%	13 1.02%	13 1.32%	120 1.12%	1 0.43%	3.88	3.88	telia.net
13	13 0.84%	13 1.02%	1 0.10%	28 0.26%	1 0.43%	0.13	0.13	net.ar
14	13 0.84%	13 1.02%	2 0.20%	30 0.28%	1 0.43%	0.87	0.87	dhl.com
15	12 0.78%	11 0.86%	9 0.92%	68 0.63%	1 0.43%	25.53	25.53	tiscali.de
16	12 0.78%	12 0.94%	1 0.10%	27 0.25%	1 0.43%	0.33	0.33	wtbts.org
17	12 0.78%	12 0.94%	1 0.10%	27 0.25%	1 0.43%	0.10	0.10	qwest.net
18	11 0.71%	11 0.86%	7 0.71%	41 0.38%	2 0.85%	0.56	1.03	radiant.net
19	10 0.65%	9 0.71%	7 0.71%	41 0.38%	1 0.43%	1.40	1.40	net.au
20	10 0.65%	10 0.78%	2 0.20%	61 0.57%	1 0.43%	0.17	0.17	3_343_lt_someone

Top 10 von 171 Rechnern (IP-Adressen) sortiert nach kb

#	Anfragen	Dateien	Seiten	kb	Besuche	Dauer	Land	Rechnername
1	47 3.04%	41 3.22%	43 4.38%	613 5.73%	4 1.71%	3.77	15.10	overture.com
2	100 6.47%	83 6.51%	46 4.68%	472 4.41%	10 4.27%	8.48	39.85	shawcable.net
3	44 2.85%	42 3.30%	23 2.34%	244 2.28%	2 0.85%	4.51	4.70	hevanet.com

User-agents

March 2004 | Last 12 Months | Monthly Statistics | Daily Statistics | Hourly Statistics | URLs

Entry Pages | Exit Pages | Errors | Hosts | Referrer | Searches | Usernames | Useragents | Countries

9	72	4.66%	71	5.57%	52	5.30%	86	0.80%	71	30.34%	0.09	6.62	inktomisearch.com
10	4	0.26%	4	0.31%	4	0.41%	74	0.69%	4	1.71%	0.00	0.00	rhyolite.com

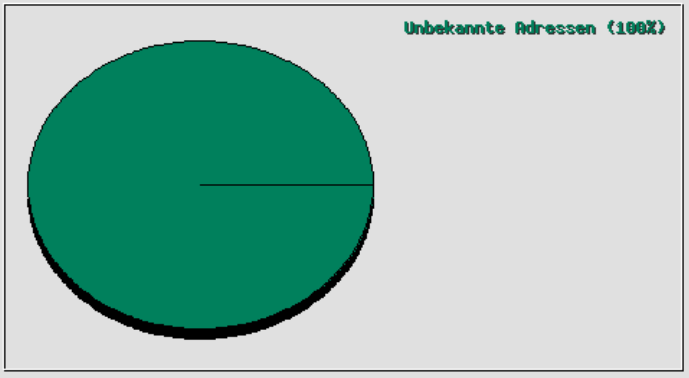
Top 1 von 1 Verweise

#	Anfragen		Besuche		Verweise
1	1546	100.00%	234	100.00%	- (Direkte Anfrage)

Top 1 von 1 Anwenderprogramme

#	Anfragen		kb		Besuche		Anwenderprogramm
1	1546	100.00%	10699	100.00%	234	100.00%	-

Anfragen aus Laendern in Monat Maerz 2004



Top 1 von 1 Ländern

#	Anfragen		Dateien		kb		Besuche		Land
1	1543	99.81%	1271	99.76%	10684	99.85%	231	100.00%	Unbekannte Adressen

100% MicroSoft free!

Stone Steps Webalizer (v3.10.2.5)