**CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY**

FACULTY OF TECHNOLOGY AND ENGINEERING

**Devang Patel Institute of Advance Technology & Research**

Semester: III

Academic year: 2019-20

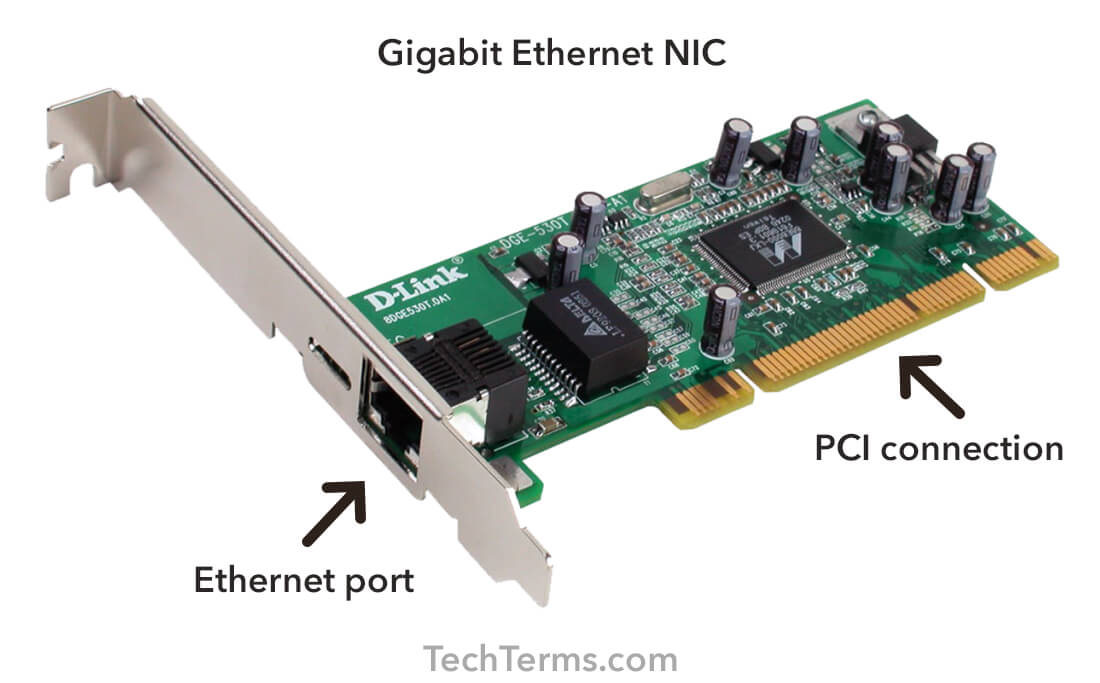
**PRACTICAL-1**

**AIM: Configuration, Management and Administration of various networking and Internetworking Devices.**

1. **NIC**
2. **Gateway**
3. **Hub**
4. **Repeater**
5. **Switch**
6. **Bridge**
7. **Router**
8. **Cables**

**THEORY/PRACTICAL:**

1. **NIC**



A network interface controller ( NIC, also known as a network interface card ) is a computer hardware component that connects a computer to a computer network.

The network controller implements the electronic circuitry required to communicate using a specific [physical layer](https://en.wikipedia.org/wiki/Physical_layer) and [data link layer](https://en.wikipedia.org/wiki/Data_link_layer) standard such as [Ethernet](https://en.wikipedia.org/wiki/Ethernet) or [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi). This provides a base for a full network [protocol stack](https://en.wikipedia.org/wiki/Protocol_stack), allowing communication among computers on the same [local area network](https://en.wikipedia.org/wiki/Local_area_network) (LAN) and large-scale network communications through routable protocols, such as [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP).

The NIC allows computers to communicate over a computer network, either by using cables or wirelessly. The NIC is both a **Physical Layer** and **Data Link Layer** device, as it provides physical access to a networking medium and similar networks, provides a low-level addressing system through the use of [MAC addresses](https://en.wikipedia.org/wiki/MAC_address) that are uniquely assigned to network interfaces.

1. **GATEWAY**



The gateway operates at the **Network Layer** of the OSI Model. The gateway is used when transmitting packets. When packets are sent over a network, the destination IP address is examined. If the destination IP is outside of the network, then the packet goes to the gateway for transmission outside of the network. The gateway is on the same network as end devices. The gateway address must have the same subnet mask as host devices. Each host on the network uses the same gateway.

The gateway should have a static address, as changing the address would cause packets not to be delivered. The gateway is typically assigned either the highest or lowest network address. This is not a requirement, but many organizations use a consistent addressing scheme to facilitate network planning.

1. **HUB**



A hub, in the context of networking, is a hardware device that relays communication data. A hub works at the **Physical Layer** of the OSI model. A hub sends data packets to all devices on a network, regardless of any MAC addresses contained in the data packet.

**Types of Hub**

* **ACTIVE HUB**: As its name suggests, Active Hub is a hub which can amplify or regenerate the information signal. This type of bus has an advantage as it also amplifies the incoming signal as well as forward it to multiple devices. This Bus is also known as Multiport Repeater. It can upgrade the properties if incoming signal before sending them to destination.
* **PASSIVE HUB**: Passive Hub works like a simple Bridge. It is used for just creating a connection between various devices. It does not have the ability to amplify or regenerate any incoming signal. It receives signal and then forward it to multiple devices.

1. **REPEATER**



In telecommunications, a repeater is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction.

In computer networking, because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the **Physical Layer**, the first layer of the OSI model.

1. **SWITCH**

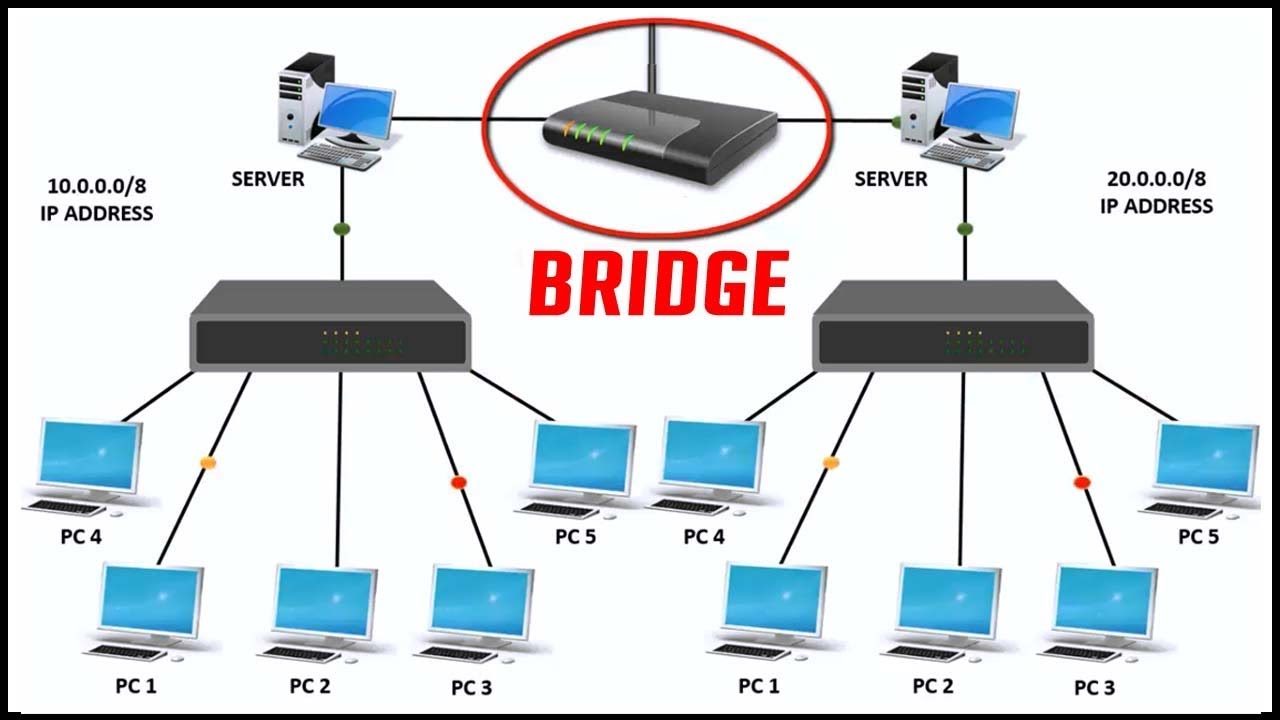


A network switch is a computer networking device that connects devices on a computer network by using packet switching to receive, process, and forward data to the destination device. A network switch forwards data only to the devices that need to receive it.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the **Data Link Layer** of the OSI model. Some switches can also process data at the **Network Layer** by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

**There are two main categories of Ethernet Switches:**

1. **Modular Configuration.**
2. **Fixed Configuration.**
3. **BRIDGE**



A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol.

Bridge devices work at the **Data Link Layer** of the Open System Interconnect (OSI) model, connecting two different networks together and providing communication between them. Bridges are similar to repeaters and hubs in that they broadcast data to every node. However, bridges maintain the media access control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.

Bridges are also known as Layer 2 switches.

**Types of Bridges**

**Transparent Bridges :-**These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of the stations is unnecessary. These bridges makes use of two processes i.e. bridge forwarding and bridge learning.

**Source Routing Bridges :-**In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

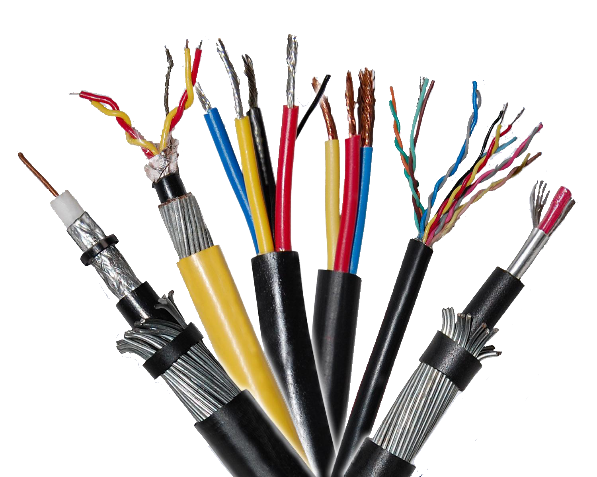
1. **ROUTER**



A router is a specialized networking device connected to two or more networks running software that allows the router to move data from one network to another. Router functions in an Internet protocol based network operate at the **Network** **Layer** of OSI Model.

The primary function of a router is to connect networks together and keep certain kinds of broadcast traffic under control. There are several companies that make routers: Cisco, Linksys, Juniper, Netgear, Nortel , Redback, Lucent, HP, Dlink, etc.

1. **CABLES**



Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc. Different types of network cables, such as coaxial cable, optical fibre cable, and twisted pair cables, are used depending on the network's physical layer, topology, and size. It works at **Physical Layer** of OSI Model.

**REFERENCES:**

https://www.techopedia.com/definition/3160/bridge

https://en.m.wikipedia.org/wiki/Networking\_cables

https://en.wikipedia.org/wiki/Gateway\_address

https://en.wikipedia.org/wiki/Ethernet\_hub

http://www.wikiforu.com/2013/04/hub-types-applications-in-network.html

https://en.wikipedia.org/wiki/Repeater

https://www.inetdaemon.com/tutorials/internet/ip/routing/define\_router.shtml

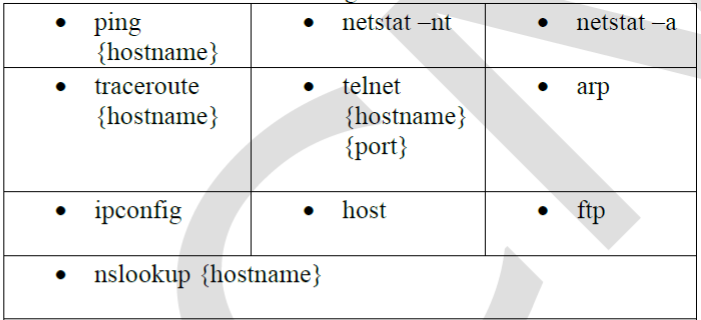
https://en.wikipedia.org/wiki/Network\_switch

**CONCLUSION:**

In this practical I learnt about Configuration, Management and Administration of various networking and Internet working Devices.

**PRACTICAL-2**

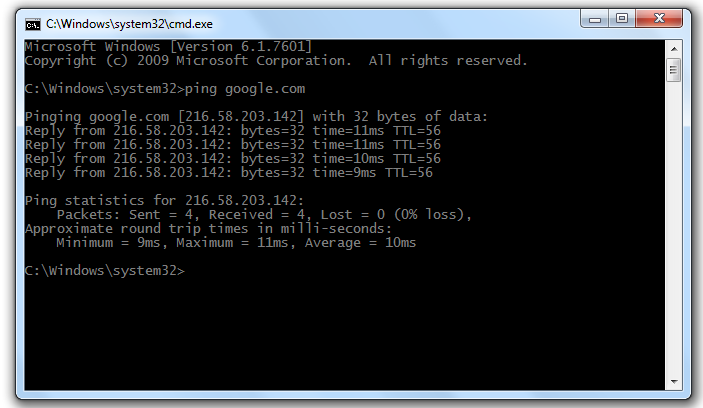
**AIM: Illustration of various networking commands:**



**THEORY/PRACTICAL:**

* **ping { hostname }**

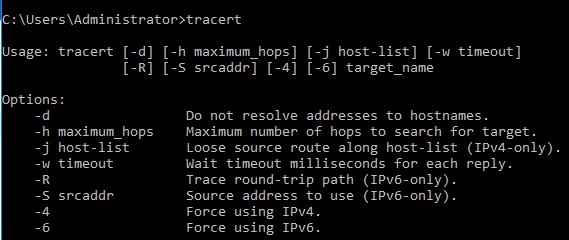
Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) echo Request messages. The receipt of corresponding echo Reply messages are displayed, along with round-trip times. ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, ping displays help.

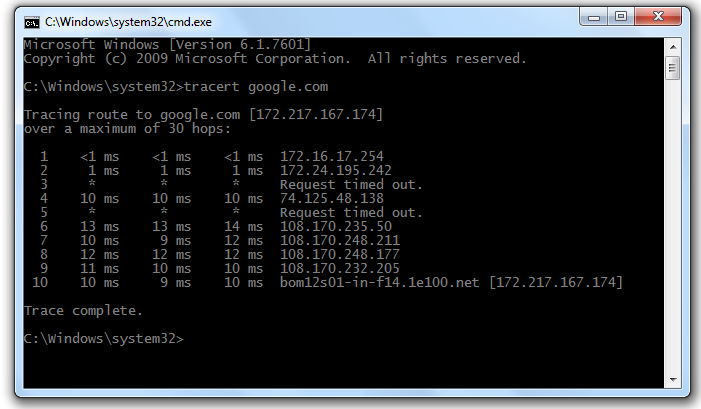


* **traceroute { hostname }**

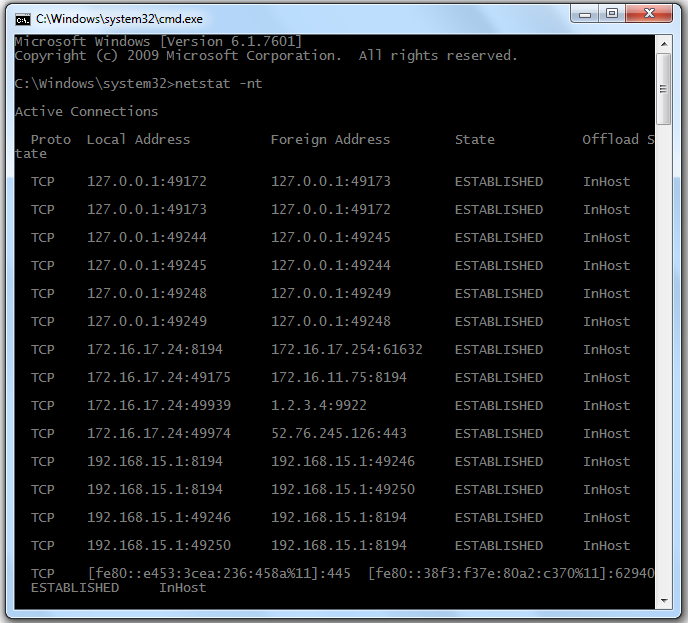
Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) echo Request or ICMPv6 messages to the destination with incrementally increasing time to Live (TTL) field values. The path displayed is the list of near/side router interfaces of the routers in the path between a source host and a destination. The near/side interface is the interface of the router that is closest to the sending host in the path. Used without parameters, tracert displays help.

[-*options*]

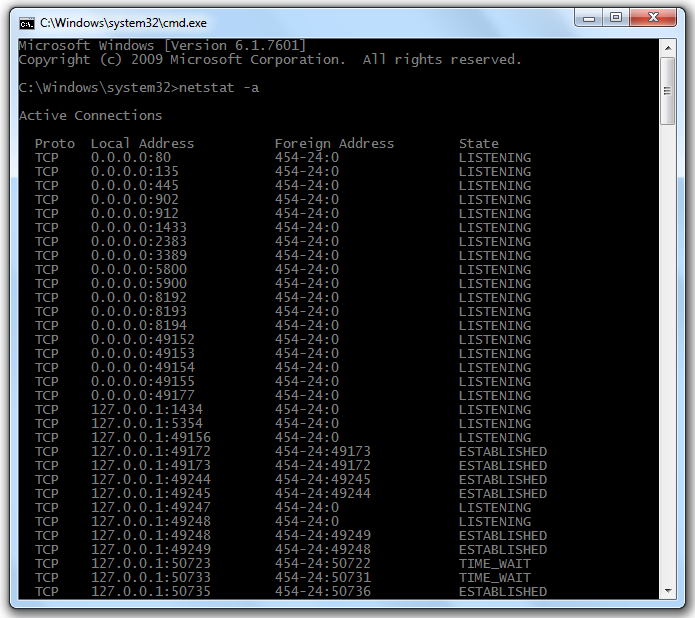




* **netstat –nt**

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols),and IPv6 statistics (for theIPv6, ICMPv6,TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

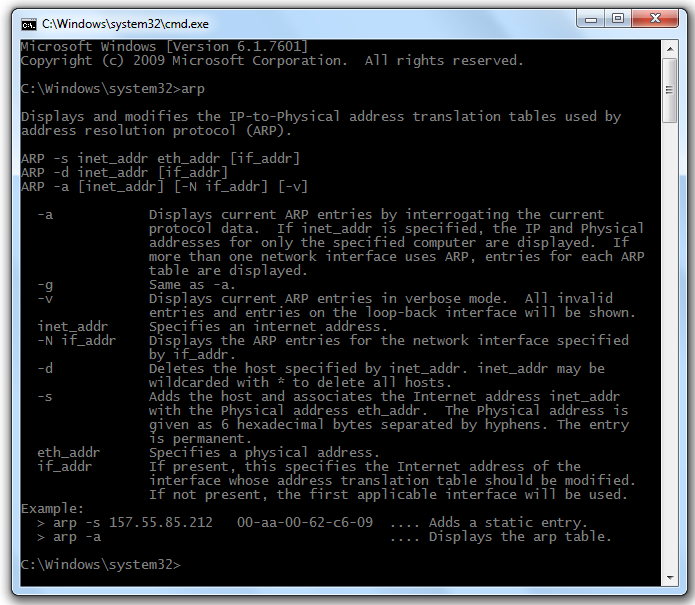
* **netstat –a**

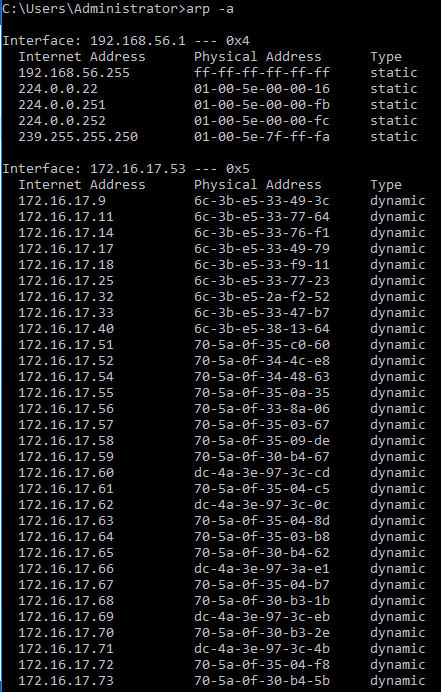
Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

* **arp**

Using the Arp command allows you to display and modify the Address Resolution Protocol (ARP) cache. An ARP cache Isa simple mapping of IP addresses to MAC addresses.

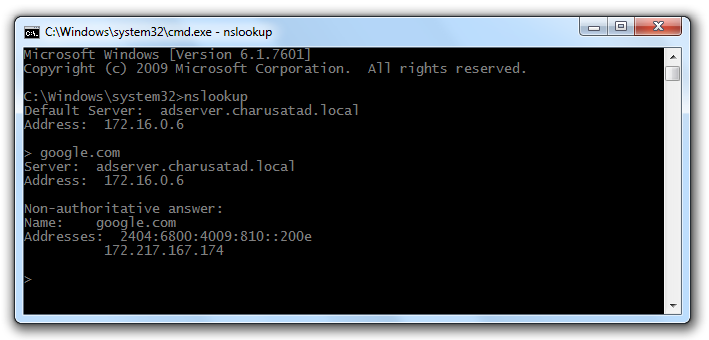
[-*options*] -a -g -n -s -d -v





* **nslookup { hostname }**

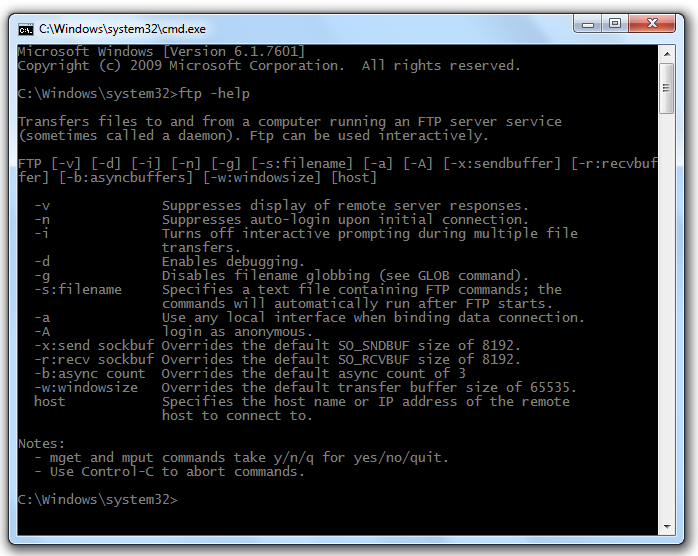
Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The nslookup command-line tool is available only if you have installed the TCP/IP protocol.



* **ftp**

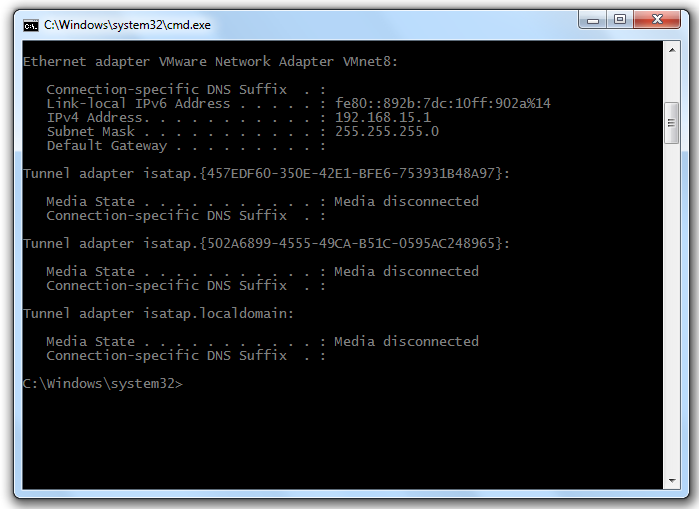
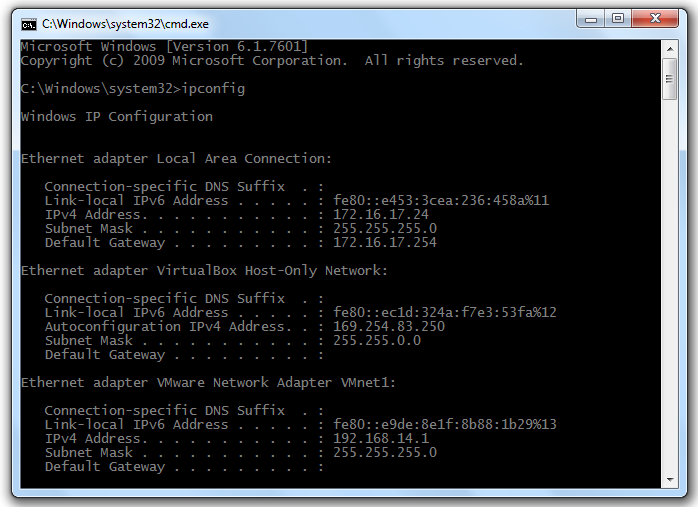
FTP is the simplest file transfer protocol to exchange files to and from a remote computer or network. Similar to Windows, Linux and UNIX operating systems also have built-in command-line prompts that can be used as FTP clients to make an FTP connection.

[-*options*] -s -g -n -i -v -w -d -a -r -b



* **ipconfig**

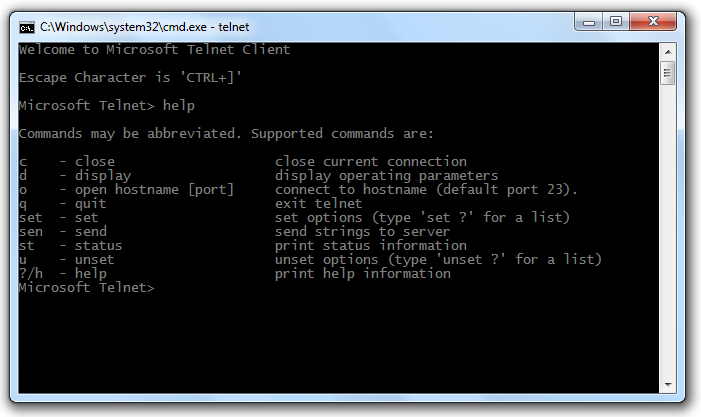
Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.



* **telnet**

Telnet is a user command and an underlying [TCP/IP](https://searchnetworking.techtarget.com/definition/TCP-IP) protocol for accessing remote computers. Through Telnet, an administrator or another user can [access](https://whatis.techtarget.com/definition/access) someone else's computer remotely

[-*options*] -a -e -f -l -t



* **host**

Host is a simple utility for performing DNS lookups. It is normally used to convert names to IP addresses and vice versa. When no arguments or options are given, host prints a short summary of its command line arguments and options.

**REFERENCES:**

<https://www.tp-link.com/us/support/faq/840/>

<https://www.tutorialspoint.com/unix_commands/host.htm>

<https://kb.intermedia.net/Article/819>

<https://kencenerelli.wordpress.com/2017/07/16/enabling-telnet-client-in-windows-10/>

<https://www.comentum.com/netstat.html>

<https://www.cellstream.com/219-what-is-the-arp-command-and-how-can-i-use-it>

<https://kb.globalscape.com/KnowledgebaseArticle10407.aspx>

<https://stevessmarthomeguide.com/ping-command-home-network-testing/>

<https://kb.intermedia.net/article/682>

**CONCLUSION:**

In this Practical I learnt various networking commands in CMD. I also learnt how they are implemented and options provided by each and every command.

**PRACTICAL-3**

**AIM: To implement straight through and cross over cable using cat 5 cable and RJ-45 connector.**

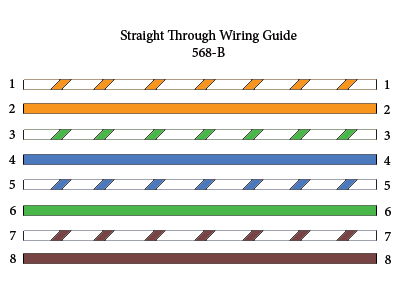
**THEORY/PRACTICAL:**

**STRAIGHT THROUGH CABLE**

You usually use straight cable to connect different type of devices. This type of cable will be used most of the time and can be used to:

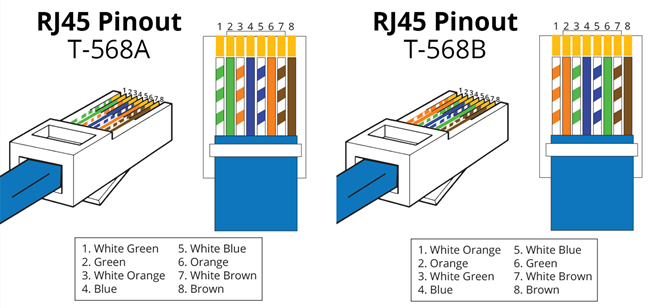
1) Connect a computer to a switch/hub's normal port.   
2) Connect a computer to a cable/DSL modem's LAN port.   
3) Connect a router's WAN port to a cable/DSL modem's LAN port.   
4) Connect a router's LAN port to a switch/hub's uplink port. (normally used for expanding network)   
5) Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.

Straight-Through refers to cables that have the pin assignments on each end of the cable. In other words Pin 1 connector A goes to Pin 1 on connector B, Pin 2 to Pin 2 etc. Straight-Through wired cables are most commonly used to connect a host to client. When we talk about cat5e patch cables, the Straight-Through wired cat5e patch cable is used to connect computers, printers and other network client devices to the router switch or hub.

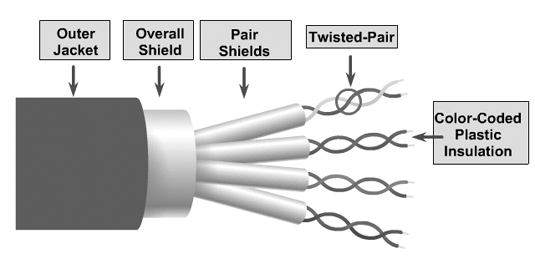


Standards of Straight Through Cables are:

* T-568A
* T-568B

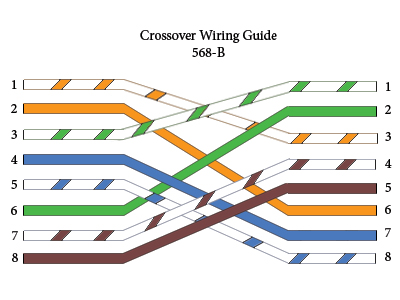


**CROSSOVER CABLE**

Sometimes you will use crossover cable, it's usually used to connect same type of devices. A crossover cable can be used to:

1) Connect 2 computers directly.   
2) Connect a router's LAN port to a switch/hub's normal port. (normally used for expanding network)   
3) Connect 2 switches/hubs by using normal port in both switches/hubs.

Crossover wired cables (commonly called crossover cables) are very much like Straight-Through cables with the exception that TX and RX lines are crossed (they are at opposite positions on either end of the cable. Using the 568-B standard as an example below you will see that Pin 1 on connector A goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B etc. Crossover cables are most commonly used to connect two hosts directly. Examples would be connecting a computer directly to another computer, connecting a switch directly to another switch, or connecting a router to a router.



Types Of Cross Over Cables:

* CAT3
* CAT4
* CAT5
* CAT5e
* CAT6
* CAT6a
* CAT7
* CAT8

**DIFFERENCE BETWEEN STRAIGHT THROUGH & CROSSOVER CABLES**

|  |  |
| --- | --- |
| **STRAIGHT THROUGH CABLES** | **CROSSOVER CABLES** |
| A straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. On a straight through cable, the wired pins match. | An Ethernet crossover cable is a type of Ethernet cable used to connect computing devices together directly. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: e.g. two computers or two switches to each other. |
| Straight Through vs Crossover Cable | Straight Through vs Crossover Cable |

**RJ-45 CONNECTOR**

A registered jack (RJ) is a standardized physical network interface for connecting telecommunications or data equipment. The physical connectors that registered jacks use are mainly of the modular connector and 50-pin miniature ribbon connector types. The most common twisted-pair connector is an 8-position, 8-contact (8P8C) modular plug and jack commonly referred to as an [RJ45 connector](https://www.anixter.com/en_au/search-results.html?searchTerms=RJ45+connector).

* An 8-pin/8-position plug or jack is commonly used to connect computers onto Ethernet-based local area networks (LAN).
* Two wiring schemes–T568A and T568B–are used to terminate the twisted-pair cable onto the connector interface

|  |
| --- |
| **TYPES OF RJ45 Jacks** |
| Cat 5e RJ45 Jack, WHITE |
| Cat 6 RJ45 Jack, BLUE |
| Cat 6A RJ45 Jack, BLUE |

**REFERENCES:**

<https://www.quora.com/What-is-the-difference-between-a-straight-through-and-a-crossover-cable>

<https://www.computercablestore.com/straight-through-crossover-and-rollover-wiring>

<https://www.techopedia.com/definition/13358/straight-through-cable>

<http://www.cables-solutions.com/difference-between-straight-through-and-crossover-cable.html>

<https://www.anixter.com/en_au/resources/literature/techbriefs/what-is-an-rj45-connector.html>

**CONCLUSION:**

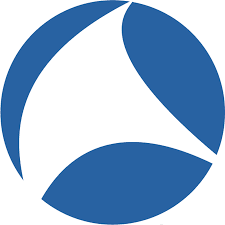
In this Practical I learnt about Cables, Types Of Cables and RJ-45 Connector. Also got to know about how to implement straight through and cross over cable using cat 5 cable and RJ-45 connector.

**PRACTICAL-4**

**AIM: Understand basic networking concept using Wireshark.**

**THEORY/PRACTICAL:**

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



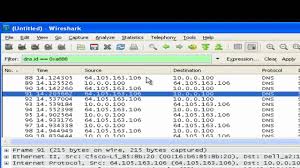
Wireshark is a network or protocol analyzer (also known as a network sniffer) available for free at the Wireshark website. It is used to analyze the structure of different network protocols and has the ability to demonstrate encapsulation. The analyzer operates on Unix, Linux and Microsoft Windows operating systems, and employs the GTK+ widget toolkit and pcap for packet capturing.

Features of Wireshark include:

* Data is analyzed either from the wire over the network connection or from data files that have already captured data packets.
* Supports live data reading and analysis for a wide range of networks (including Ethernet, IEEE 802.11, point-to-point Protocol (PPP) and loopback).
* With the help of GUI or other versions, users can browse captured data networks.
* For programmatically editing and converting the captured files to the editcap application, users can use command line switches.
* Display filters are used to filter and organize the data display.
* New protocols can be scrutinized by creating plug-ins.

When using Linux, it is also possible to capture raw USB traffic.

**PROGRAM/OUTPUT:**

****

****

**ADVANTAGES/DISADVANTAGES:**

**Advantages:**

* Free software
* Available for multiple platforms - Windows & UNIX
* Can see detailed information about packets within a network
* Not proprietary can be used on multiple vendors unlike Cisco Prime

**Disadvantages:**

* Wireshark is not an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn’t allowed to do.
* Wireshark will not manipulate things on the network, it will only measure things from it. Wireshark doesn’t send packets on the network or do other active things.

**REFERENCES:**

<https://www.wireshark.org/>

<https://www.techopedia.com/definition/25325/wireshark>

<https://en.wikipedia.org/wiki/Wireshark>

**CONCLUSION:**

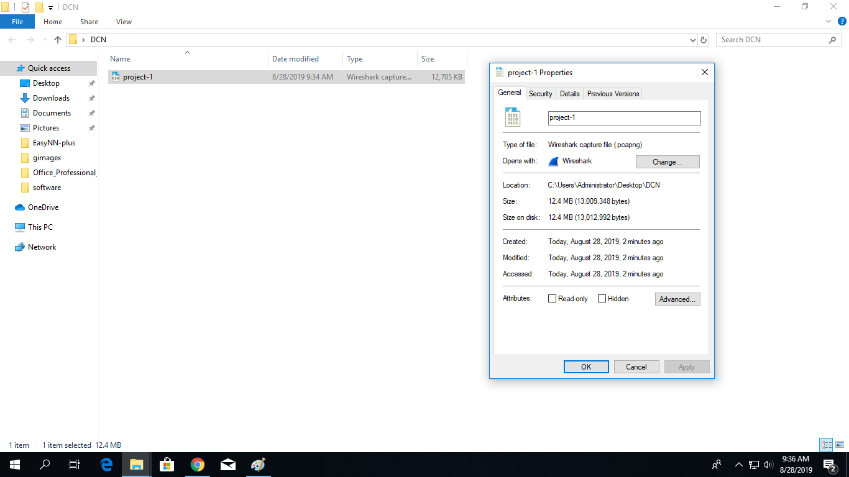
In this practical we have learnt the basic concepts of Wireshark and we have also learnt how to create .pcap file in it.

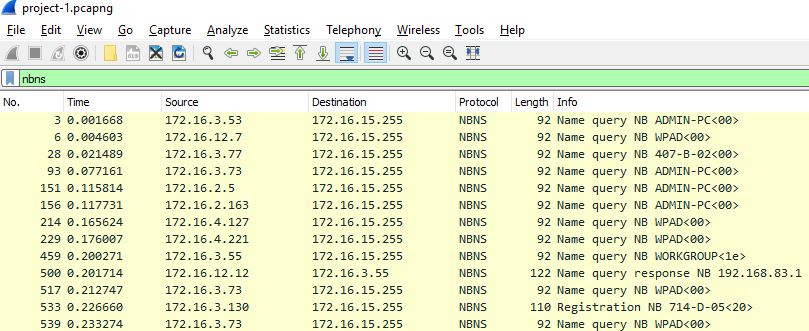
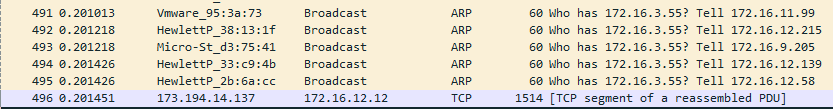
**PRACTICAL-5**

**AIM: Analyzing packet captured using CHARUSAT intranet using Wireshark. Use of different Wireshark Display Filters.**

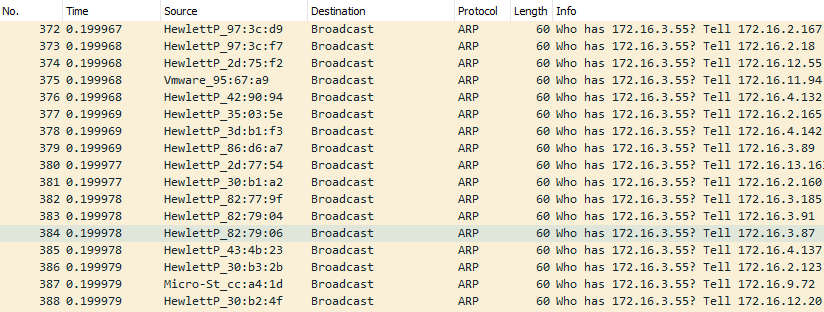
**PRACTICAL:**

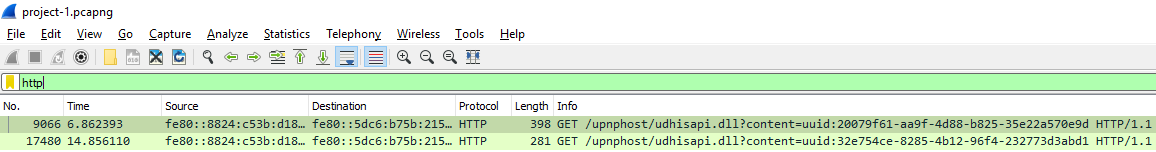
* Create a .pcap file in Wireshark.

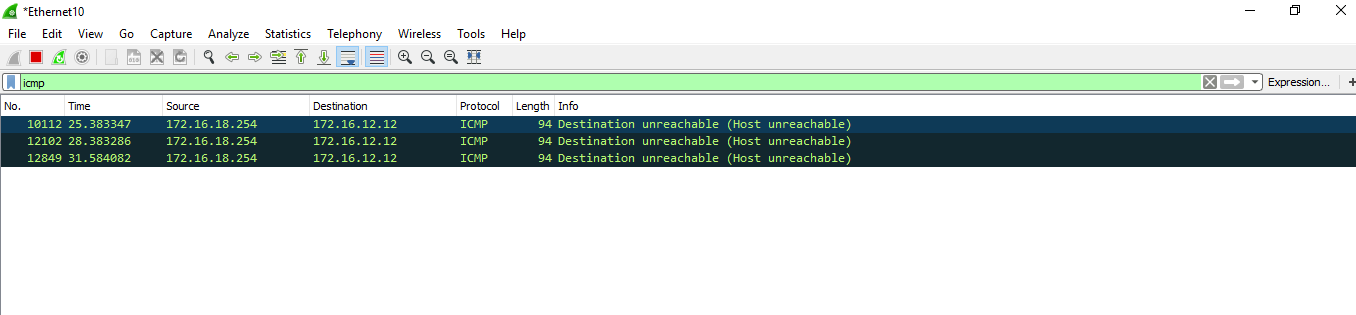


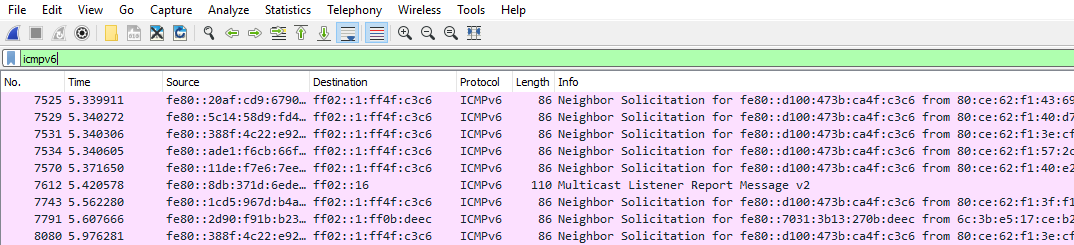
* Traffic filtering is also possible using the Wireshark. Different filters can be applied to filter out different required information.
* Different IP addresses of the devices connected to a network can be obtained using the Wireshark. Wireshark gives the list of all the devices to which your device has communicated till date.
* Identifying of distinct protocols is also possible using Wireshark as follows,

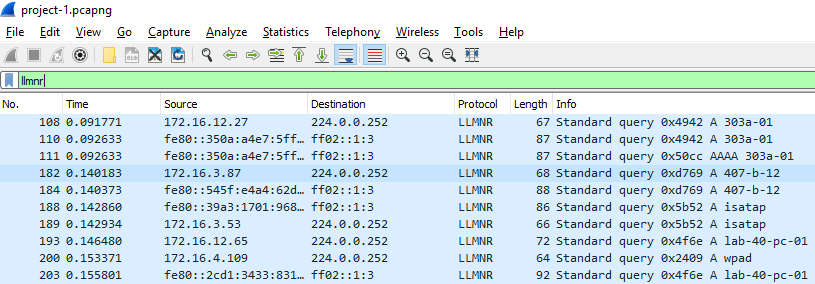
(I) ARP

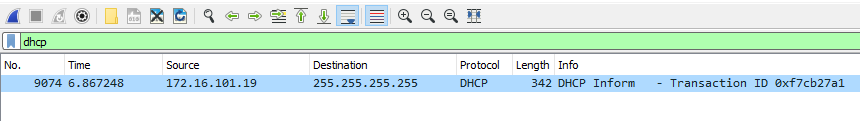


(II) HTTP

(III) ICMP

 (IV) ICMPv6

 (V) LLMNR

* The application layer protocol is DHCP protocol.

**CONCLUSION:**

In this practical we have used the filter options of Wireshark to filter out different protocols in it.

**PRACTICAL-6**

**AIM: Capture ARP and ICMP Protocol Traffic using Wireshark.**

**THEORY:**

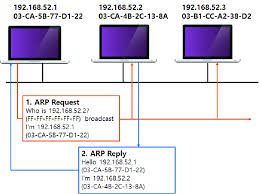
The Address Resolution Protocol (**ARP**) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.

***Example:-***

Two computers in an office (Computer 1 and Computer 2) are connected to each other. Computer 1 has a packet to send to Computer 2. Through [DNS](https://en.wikipedia.org/wiki/DNS), it determines that Computer 2 has the IP address 192.168.0.55.

To send the message, it also requires Computer 2's [MAC address](https://en.wikipedia.org/wiki/MAC_address). First, Computer 1 uses a cached ARP table to look up 192.168.0.55 for any existing records of Computer 2's MAC address (00:eb:24:b2:05:ac). If the MAC address is found, it sends an Ethernet [frame](https://en.wikipedia.org/wiki/Frame_(networking)) with destination address 00:eb:24:b2:05:ac, containing the IP packet onto the link. If the cache did not produce a result for 192.168.0.55, Computer 1 has to send a broadcast ARP request message (destination FF:FF:FF:FF:FF:FF MAC address), which is accepted by all computers on the local network, requesting an answer for 192.168.0.55.

Computer 2 responds with an ARP response message containing its MAC and IP addresses. As part of fielding the request, Computer 2 may insert an entry for Computer 1 into its ARP table for future use.



Computer 1 receives and caches the response information in its ARP table and can now send the packet.

**RARP (Reverse Address Resolution Protocol)**

The Reverse Address Resolution Protocol (RARP) is an obsolete computer networking protocol used by a client computer to request its Internet Protocol ([IPv4](https://en.wikipedia.org/wiki/IPv4)) address from a computer network, when all it has available is its [link layer](https://en.wikipedia.org/wiki/Link_layer) or hardware address, such as a [MAC address](https://en.wikipedia.org/wiki/MAC_address). The client broadcasts the request and does not need prior knowledge of the network topology or the identities of servers capable of fulfilling its request.

**Uses of RARP**

Although the original uses for RARP have been overcome by different protocols, some modern day protocols use RARP. Examples are:

Cisco's Overlay Transport Virtualization (OTV). RARP is used to update the layer 2 forwarding tables when a MAC address moves between data centers.

**ICMP (INTERNET CONTROL MESSAGE PROTOCOL)**

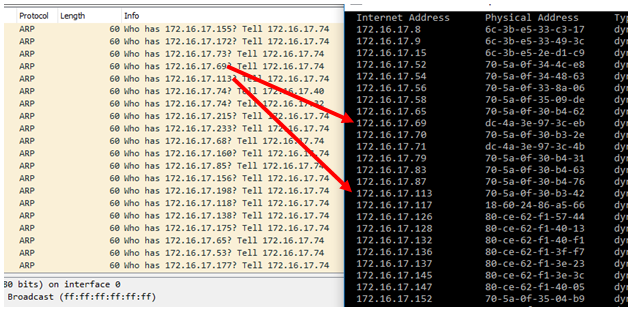
The Internet Control Message Protocol (ICMP) is a supporting [protocol](https://en.wikipedia.org/wiki/Communications_protocol) in the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite). It is used by [network devices](https://en.wikipedia.org/wiki/Network_device), including [routers](https://en.wikipedia.org/wiki/Router_(computing)), to send error messages and operational information indicating, for example, that a requested service is not available or that a [host](https://en.wikipedia.org/wiki/Host_(network)) or router could not be reached.

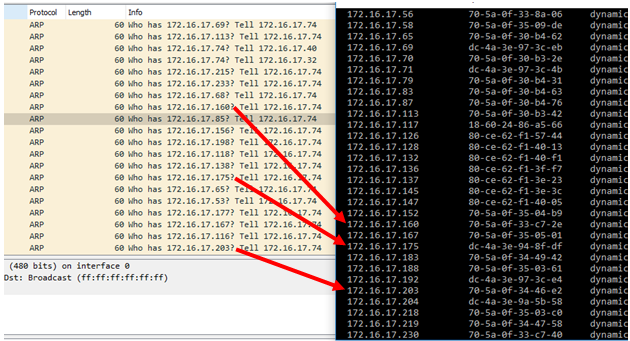
Some of the error messages are:

* Source quench message
* Parameter problem
* Time exceeded message
* Destination unreachable message
* Redirection message

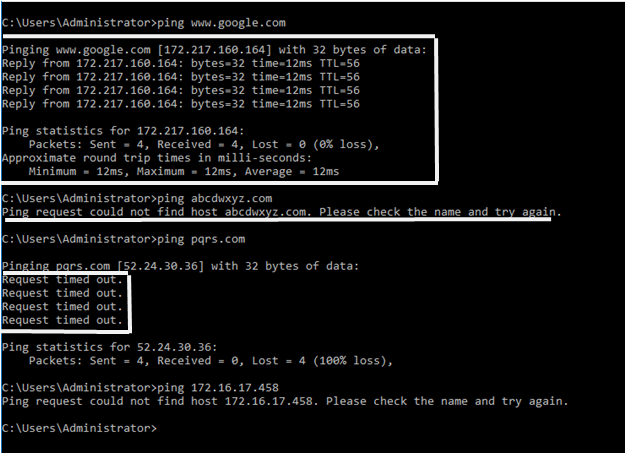
**OUTPUT:**

ARP





**ICMP**

 Some of the error messages on cmd.

**CONCLUSION:**

In this practical we have learnt how to monitor and filter the ICMP and ARP protocol traffic.

**PRACTICAL-7**

**AIM: Understand basic networking concept using Wireshark.**

**THEORY:**

A **Network Simulator** is [software](https://en.wikipedia.org/wiki/Software) that predicts the behavior of a [computer network](https://en.wikipedia.org/wiki/Computer_network). Since communication networks have become too complex for traditional analytical methods to provide an accurate understanding of system behavior, network simulators are used. In simulators, the computer network is modeled with devices, links, applications etc. and the network performance is reported. Simulators come with support for the most popular technologies and networks in use today such as [5G](https://en.wikipedia.org/wiki/5G), [Internet of Things](https://en.wikipedia.org/wiki/Internet_of_things) (IoT), [Wireless LANs](https://en.wikipedia.org/wiki/Wireless_LAN), [mobile ad hoc networks](https://en.wikipedia.org/wiki/Mobile_ad_hoc_network), [wireless sensor networks](https://en.wikipedia.org/wiki/Wireless_sensor_network), [vehicular ad hoc networks](https://en.wikipedia.org/wiki/Vehicular_ad_hoc_network), [cognitive radio networks](https://en.wikipedia.org/wiki/Cognitive_Radio_Networks), [LTE](https://en.wikipedia.org/wiki/LTE_(telecommunication)) etc.

Following are some of the Network Simulators:

* GNS3- Design and Configure
* Cisco Packet Tracer
* Putty Configure
* Secure CRT- Configure
* Microsoft Visio- Design Only
* PRTG: Monitoring

**Network Emulator:**

A network emulator, also referred to as a WAN emulator, is used to test the performance of a real network. These devices can also be used for such purposes as quality assurance, proof of concept, or troubleshooting. Available as hardware or software solutions, a network emulator allows network architects, engineers, and developers to accurately gauge an application’s responsiveness, throughput, and quality of end-user experience prior to applying making changes or additions to a system.

Following are some of the Network Emulators:

* MiniNet
* EMANE
* NS3

**Features of Cisco Packet Tracer:**

Cisco Packet Tracer has two workspaces—logical and physical. The logical workspace allows users to build logical network topologies by placing, connecting, and clustering virtual network devices. The physical workspace provides a graphical physical dimension of the logical network, giving a sense of scale and placement in how network devices such as routers, switches, and hosts would look in a real environment. The physical view also provides geographic representations of networks, including multiple cities, buildings, and wiring closets.

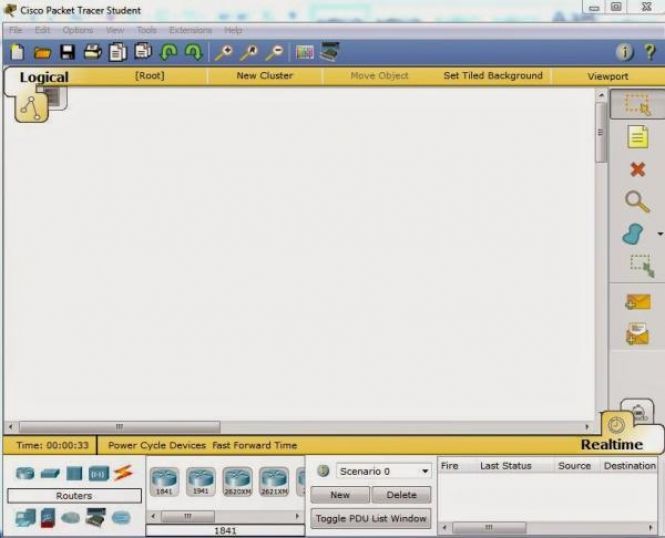
* Lab grading function
* International language support
* Compatible with the following platforms: Windows, Windows XP;Vista Basic, Vista Premium); Windows 7; and Linux (Ubuntu, Fedora)
* Available to registered Networking Academy instructors, students, and alumni

**Comparison of Network Simulator with Network Emulator**

* Network emulation provides a suitable alternative to both simplistic simulators and expensive simulators and test beds. It can provide real-time performance measurements of production-ready prototype technologies in a laboratory abstraction of real-world networks.
* Network simulation and emulation both provide a cost effective alternative to hardware emulators that have high costs, complicated configuration requirements and limited scale. Both can be scaled to hundreds of nodes.
* The primary advantage of emulation is the time savings in prototype testing. Further, the ability to port emulators into general purpose clusters offers a scalable solution.

Among network emulators, there are two different approaches: hardware emulation and software solutions with the latter being significantly less expensive than the former. We believe that high-fidelity software emulation is an attractive solution to obtain the performance of an actual system and complements network simulation analysis.

**OUTPUT:**



**REFERENCES:**

<https://getpcsoft.wikisend.com/cisco-packet-tracer-free-download.html>

<https://en.wikipedia.org/wiki/Packet_Tracer>

<https://www.coursera.org/lecture/internet-connection-how-to-get-online/packet-tracer-building-a-small-network-dv7Pn>

<https://www.cisco.com/c/dam/en_us/training-events/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pd>

<https://www.robocomtech.com/network-emulation-vs-simulation/>

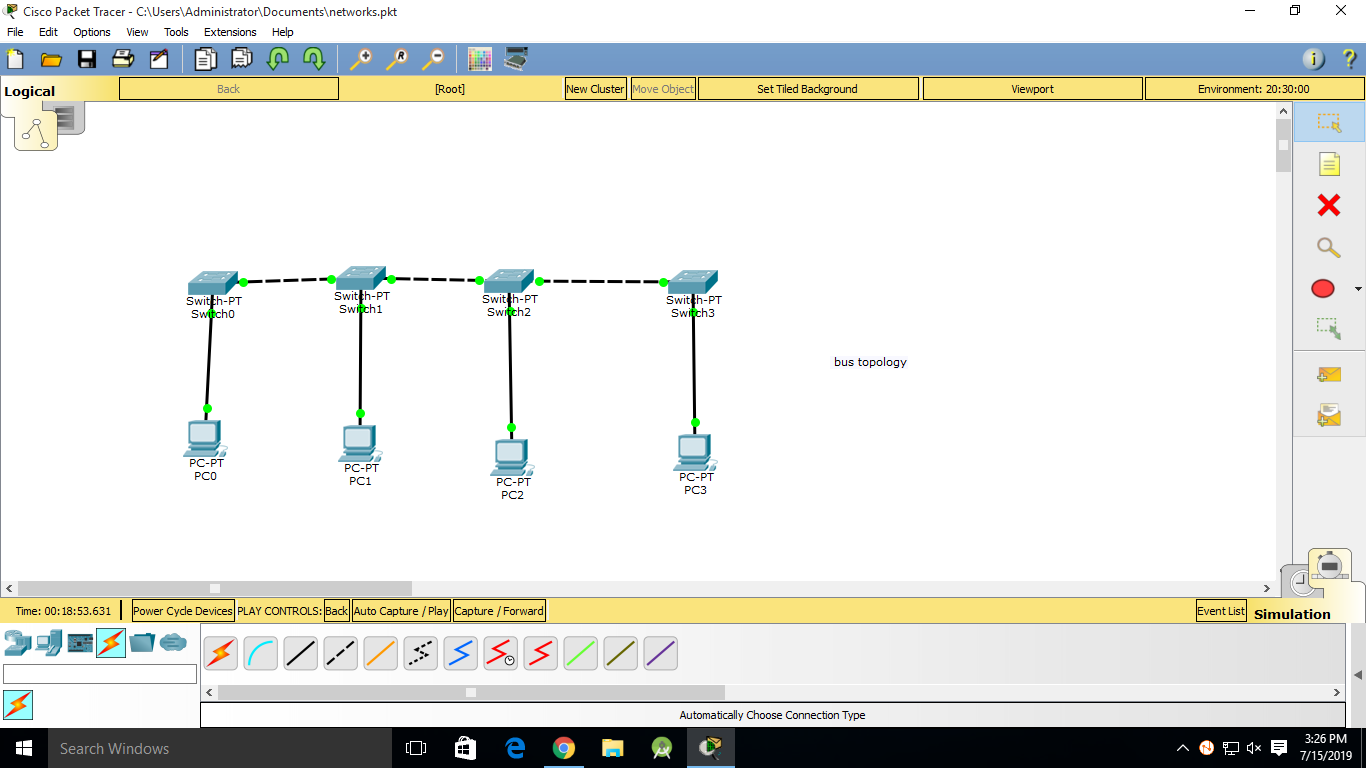
**CONCLUSION:**

In this practical we have learnt about Cisco packet tracer and also about its features and different functionalities.

**PRACTICAL-8**

**AIM: Configuration of different topologies in Cisco Packet Tracer to understand decision taken at each 4 layers of TCP/IP protocol stack.**

**PRACTICAL/OUTPUT:**

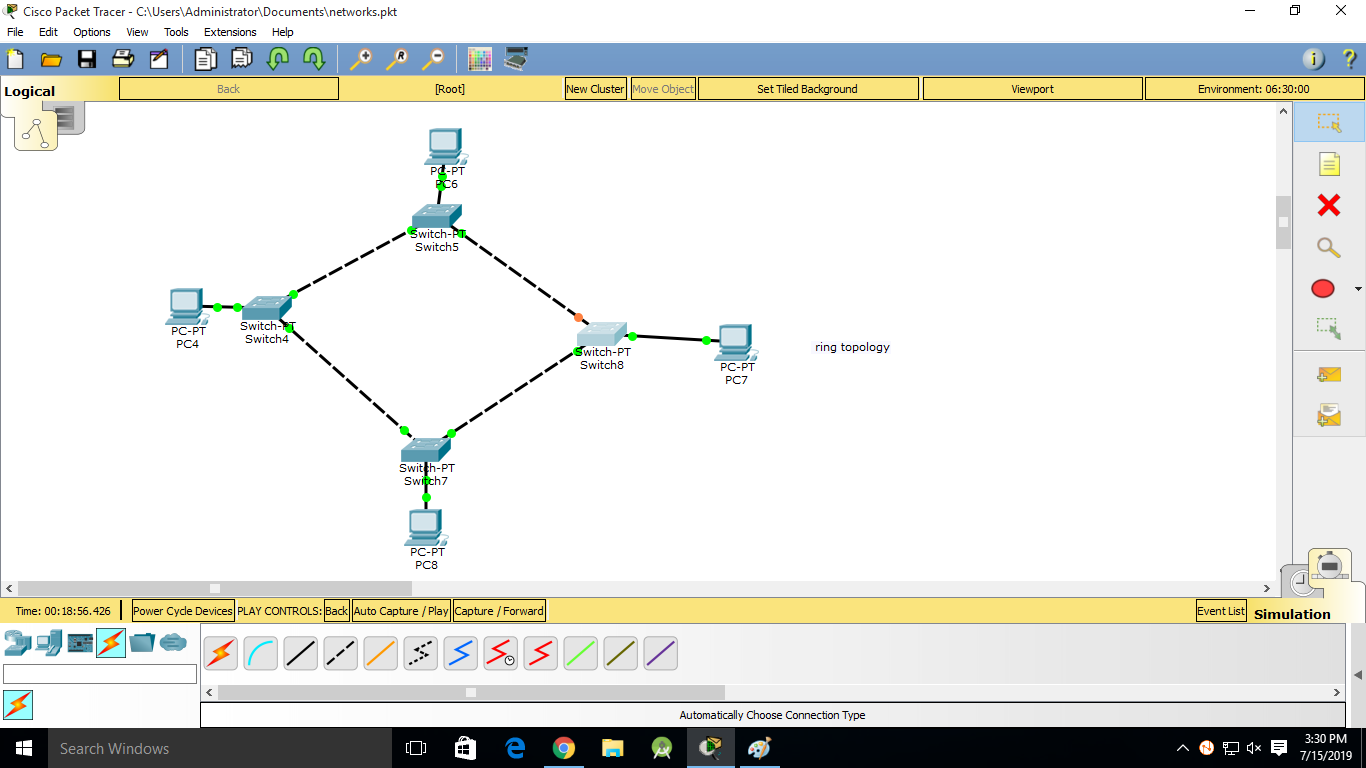
**Bus Topology:-**  Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology.

|  |
| --- |
|  |

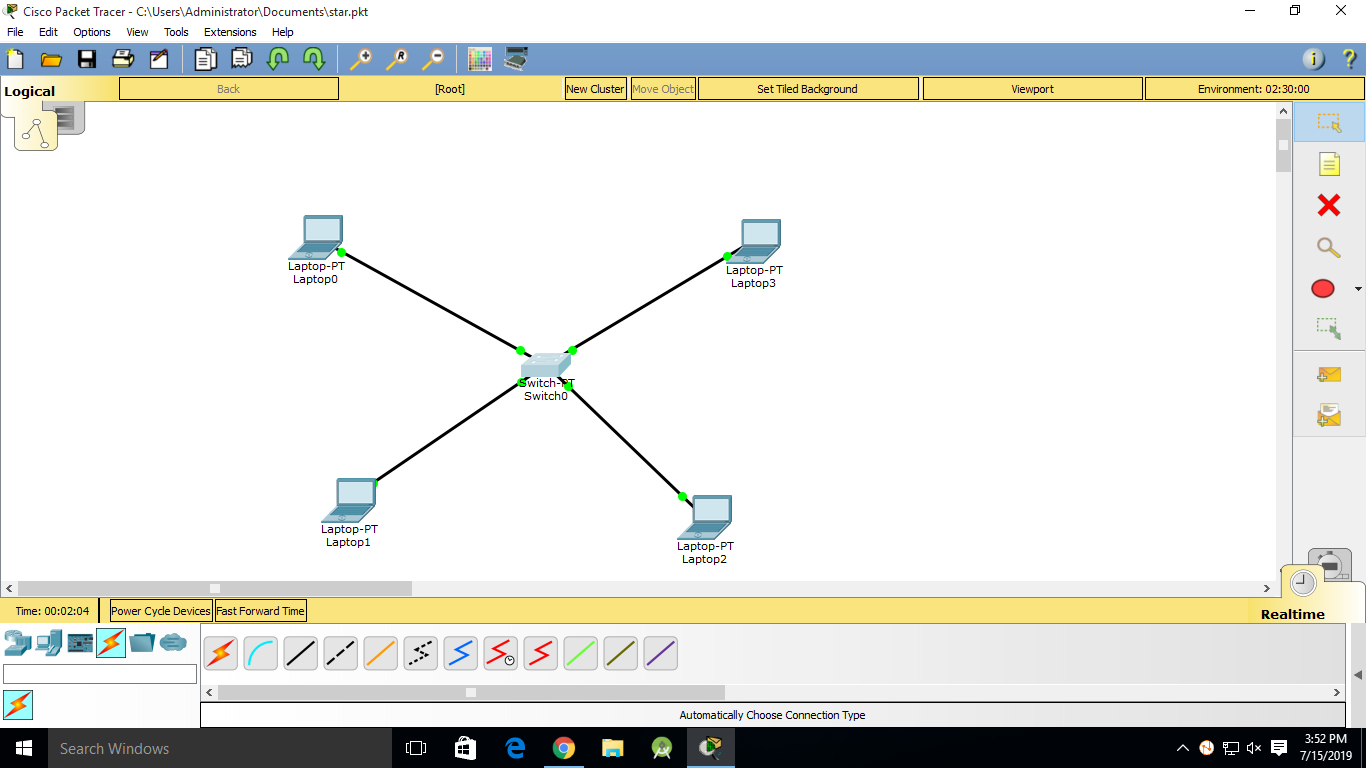
**Mesh Topology:-**In mesh topology , every device is connected with another via dedicated channels. These channels are known as links. But this topology is very much complex and costly to form for the network having larger number of connected devices.



**Ring topology:-** ​ In the ring topology, it forms a ring connecting a devices with its exactly two neighboring devices. In this topology each device is only able to communicate with two of its neighboring devices. And also in this topology if any of the link gets distorted or damaged then communication stops in the whole circuit.



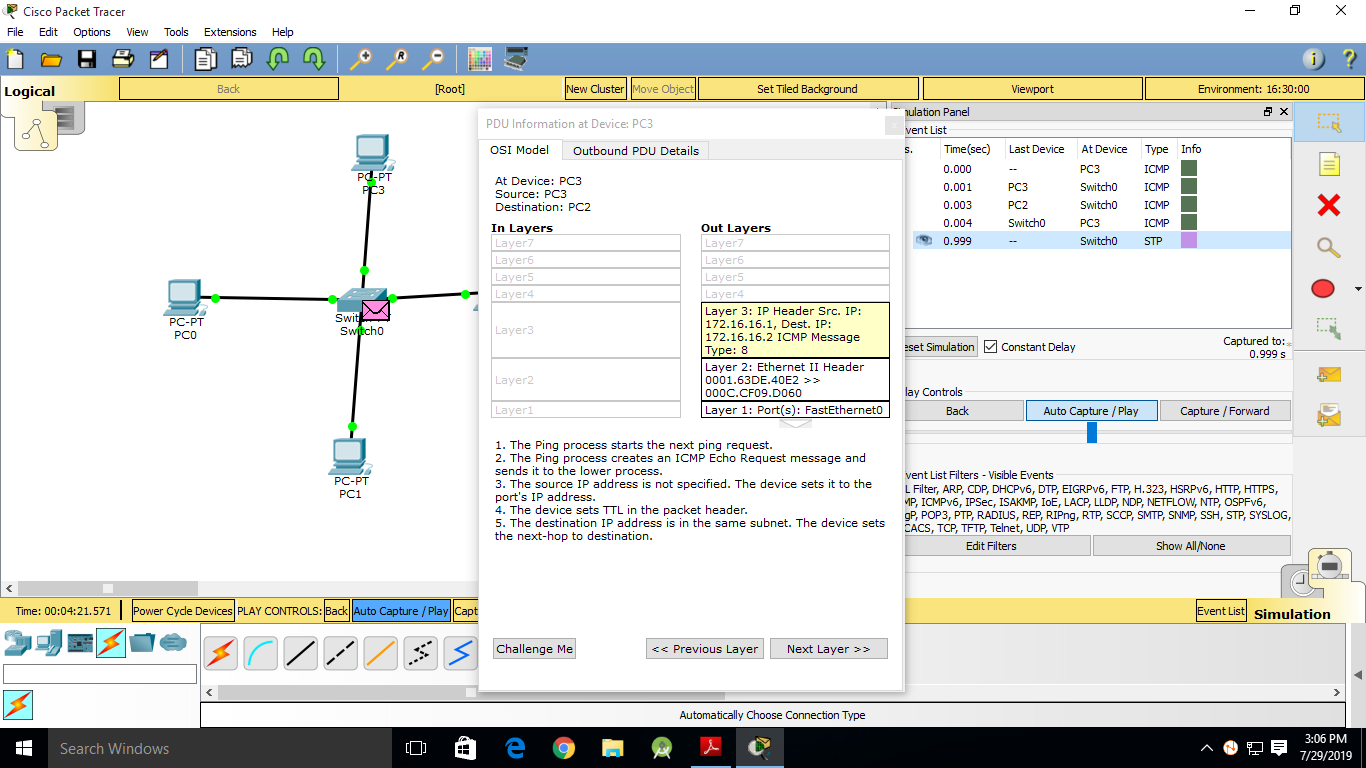
**Star topology:-** ​ In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. Active hubs have repeaters in them.



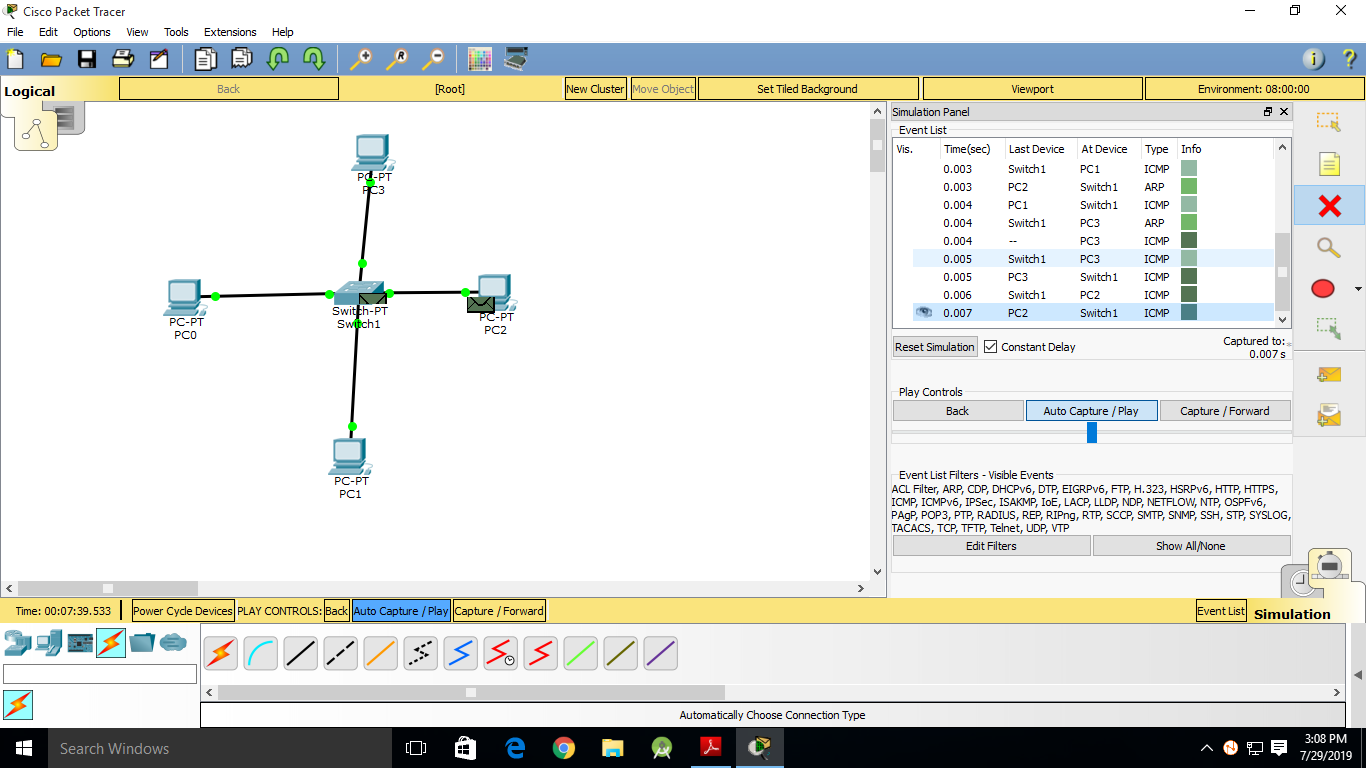
**Hybrid Topology:-**Hybrid topology is basically the combination of two or more network topologies to improve the network configuration and to make the network more efiicient using less costing. The hybrid network topology shown here is the combination of bus and star topologies.



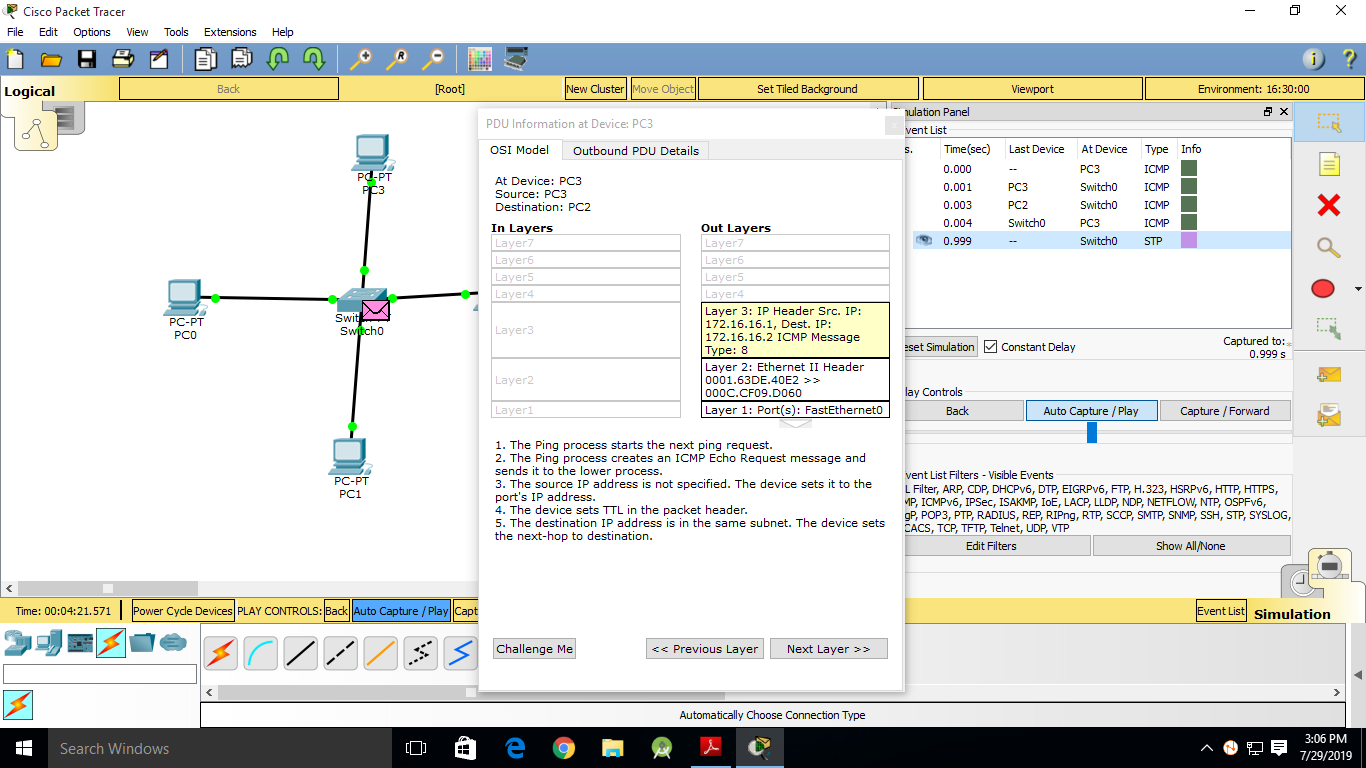
**Run the cisco packet tracer in simulated mode:-**

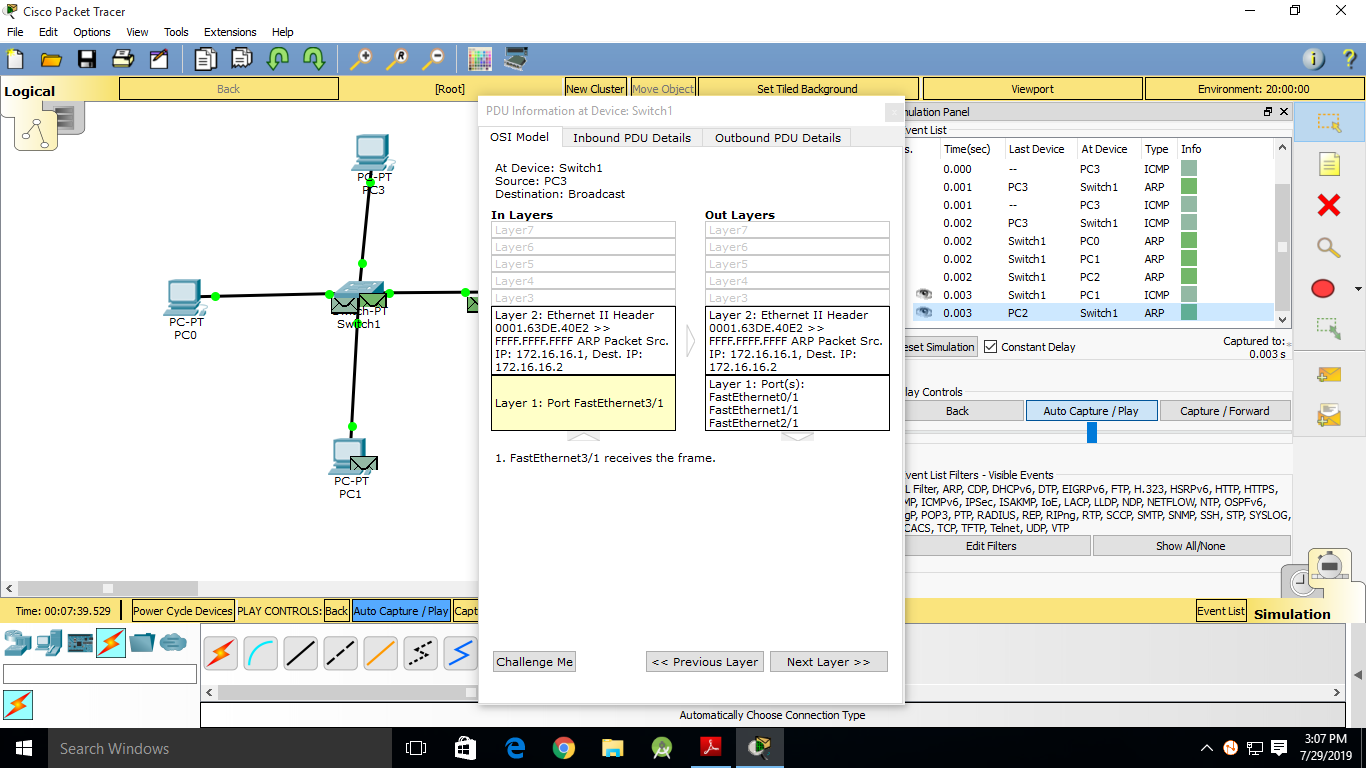


**Filter the traffic related to ARP and ICMP protocol:-**



**Check the content at network layer in simulated mode:-**

(I) ICMP protocol in the network layer

(II) ARP protocol in the data link layer

**REFERENCES:**

<http://www.telecomabc.com/s/star.html>

<https://www.techopedia.com/definition/13335/star-topology>

<https://www.studytonight.com/computer-networks/network-topology-types>

**CONCLUSION:**

In this practical we have learnt the concepts of cisco packet tracer and also we have learnt the process of message transfer in a network using different topologies by cisco packet tracer.

**PRACTICAL-9**

**AIM: To demonstrate CHARUSAT campus network setup.**

**THEORY/PRACTICAL:**

*STAR TOPOLOGY:*

In Star type of topology all the computers are connected to a single hub/switch through a cable. This hub/switch is the central node and all others nodes are connected to the central node. *Visit to WinCell Department:*

* The pictorial representation of the CHARUSAT campus network setup is shown in the following picture.
* All the different buildings of the CHARUSAT campus are connected to the WinCell department through the manageable switches and fiber optic cable.



**CHARUSAT NETWORK SETUP**

* WinCell is the main or the central server of the CHARUSAT campus.
* Due to the manageable switches each and every node/building/component/end user can be controlled by seating in the WinCell department.
* And due to the fiber optic cable there’s no physical effect on the cable which gives the proof of continuous working network.
* Each and every building follows the Star topology internally due to which if in case any of the network/device/component goes down it doesn’t affect the other network.
* The total bandwidth available is 300Mbps.
* The ISP(Internet Service Provider) is BSNL(Bharat Sanchar Nigam Limited) from two stations one being the Nadiad station and the other being the Anand station.
* WinCell is the gateway provider for the CHARUSAT network.
* Talking about the security, we are equipped with super-speciality SOPHOS lab which provides the best security to our network.
* The firewall blocks all the malicious activities to enter our CHARUSAT network.
* Due to security reasons our WinCell department has blocked some countries like Pakistan, Afghanistan, and some others from accessing our network.
* In each and every lab all the computers are connected to a switch and all such switches are connected to the main switch of the building.

**CONCLUSION:**

From this practical we came to know about the CHARUSAT network setup and also visited the WinCell department.

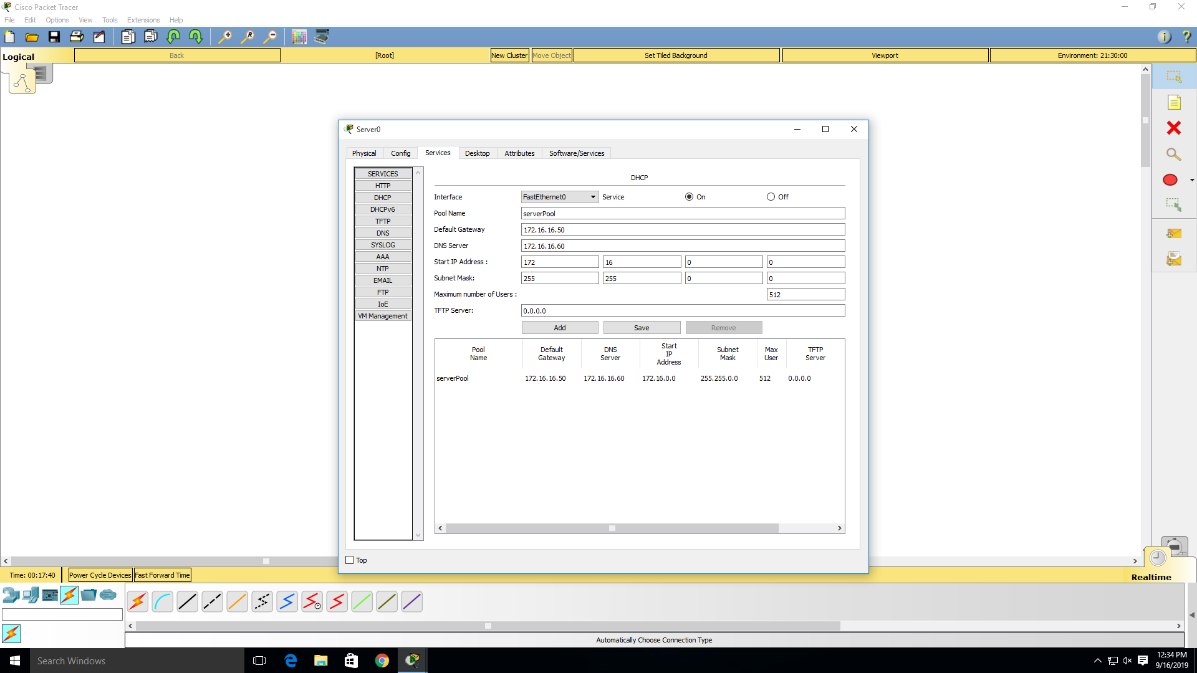
**PRACTICAL-10**

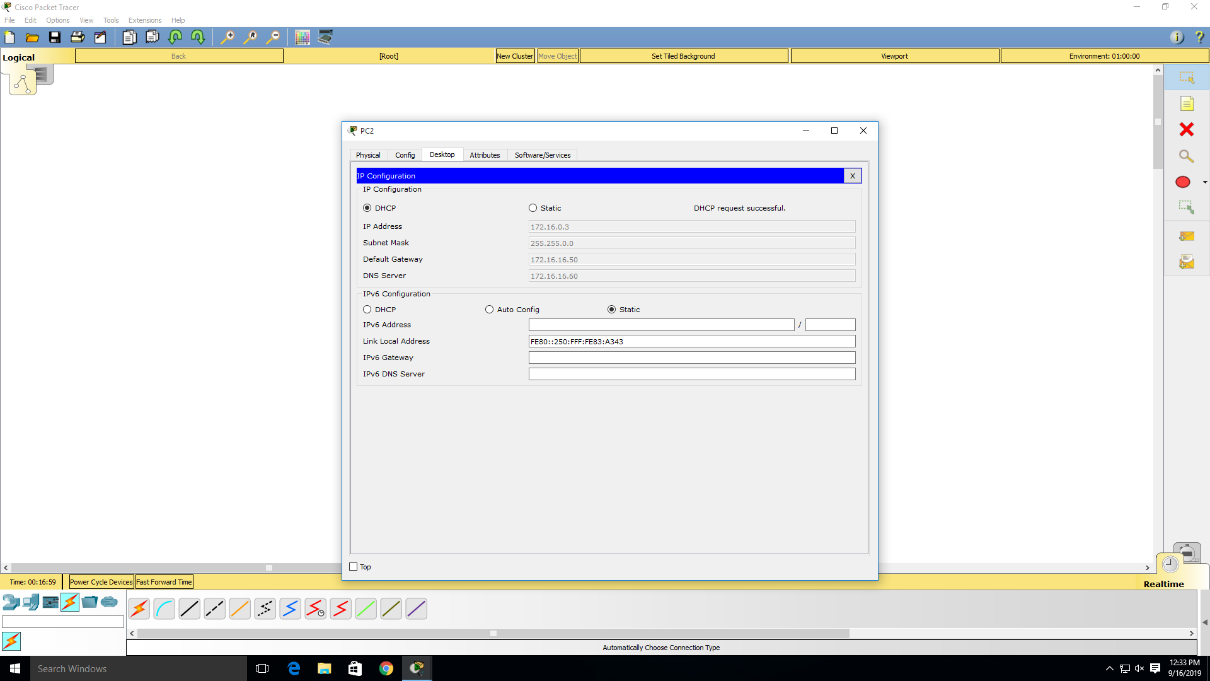
**AIM: Configure DHCP, DNS and HTTP servers using cisco packet tracer.**

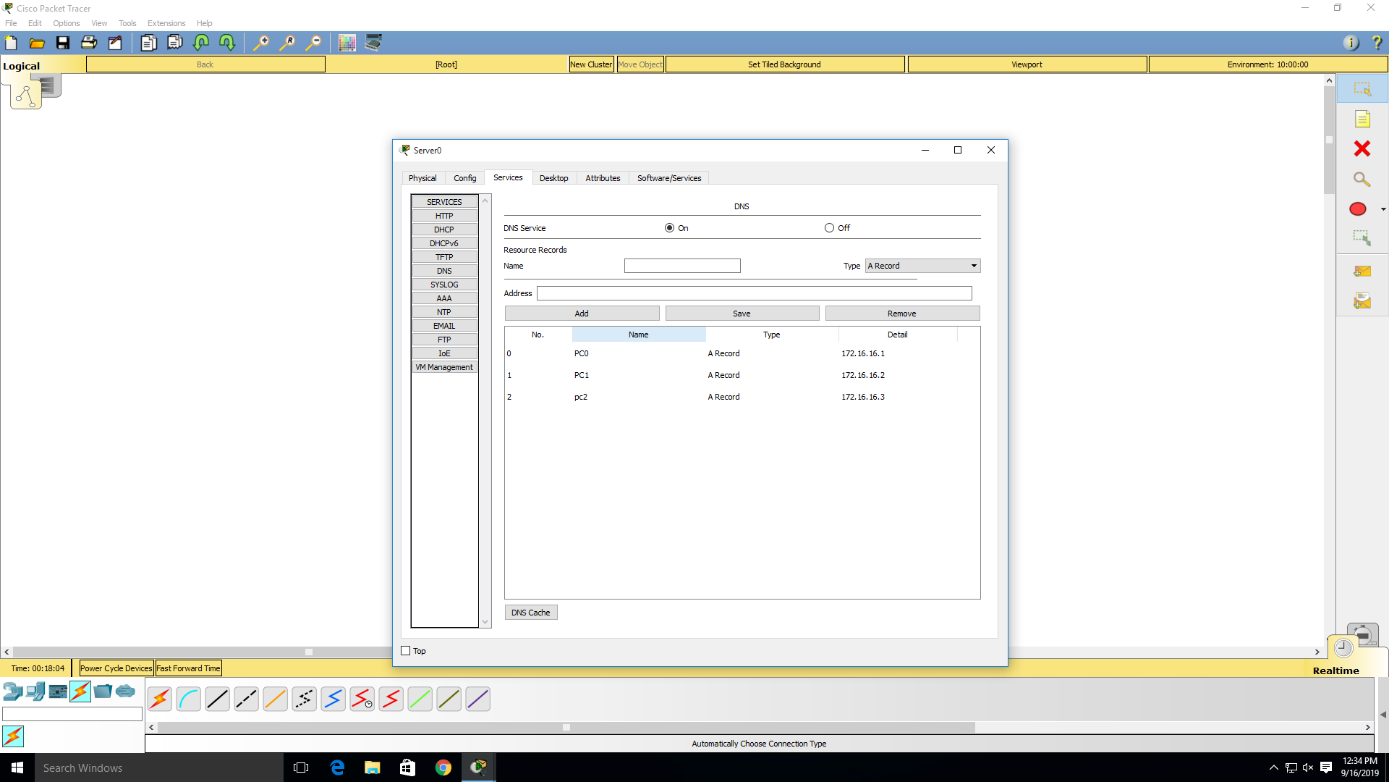
**THEORY/PRACTICAL:**

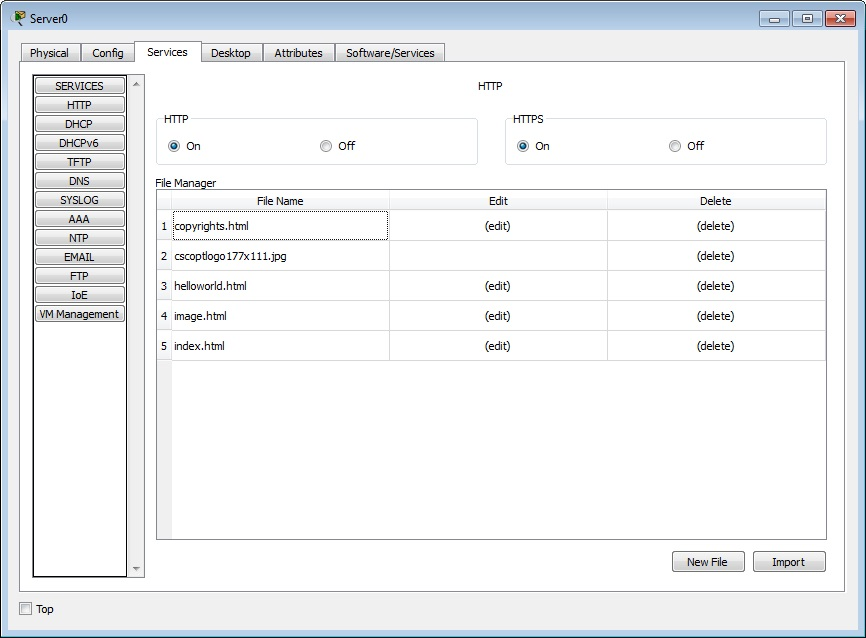
DHCP,DNS and HTTP are different types of protocols which are most commonly used in the different types of networks.

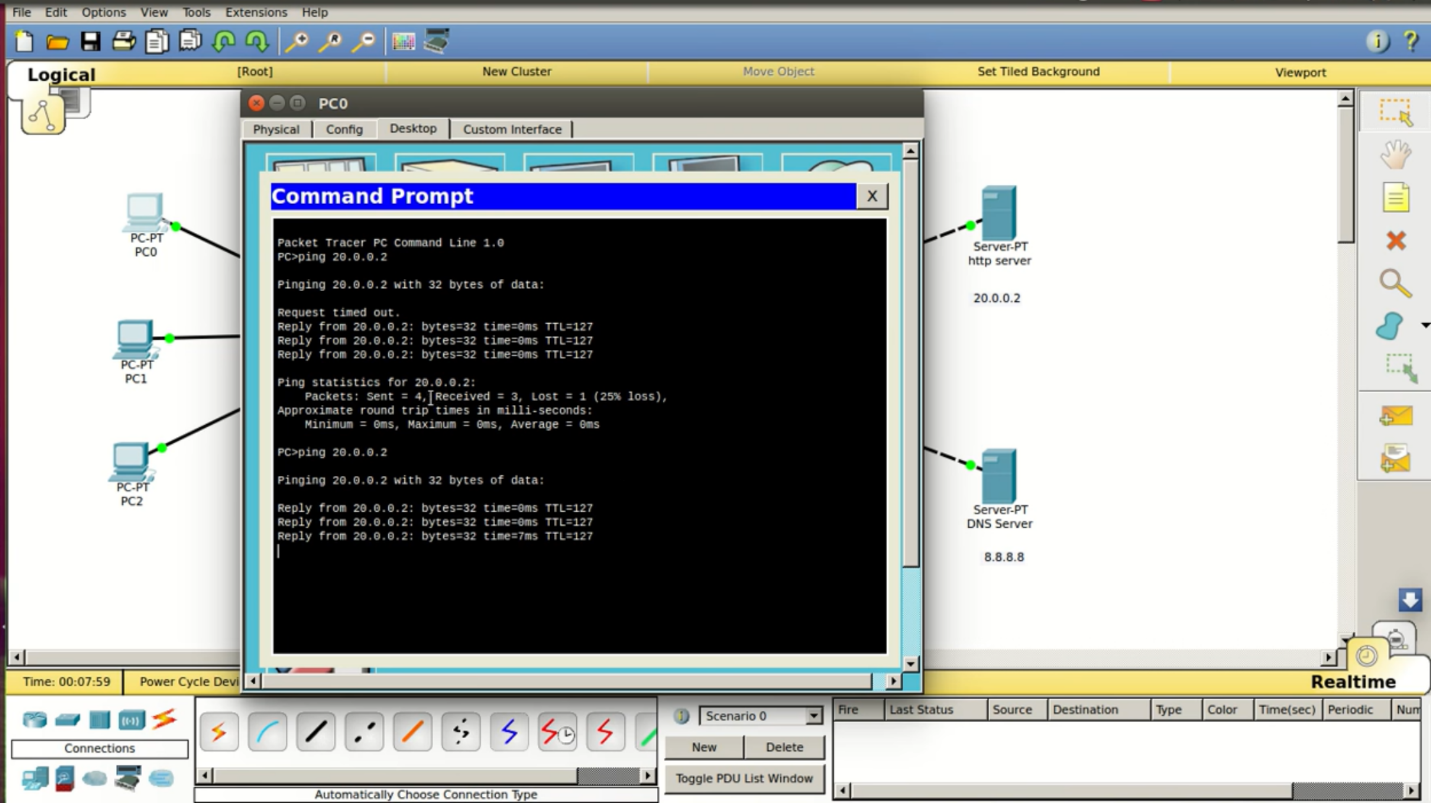
* **DHCP**:- The Dynamic Host Configuration **Protocol** (**DHCP**) is a network management **protocol** used on UDP/IP networks whereby a **DHCP** server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.





* **DNS**:- DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.
* **HTTP**:- HTTP means Hyper Text Transfer Protocol. HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.





**REFERENCES:**

<https://www.geeksforgeeks.org/domain-name-server-dns-in-application-layer/>

<https://www.webopedia.com/TERM/H/HTTP.html>

<https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>

**CONCLUSION:**

In this practical we have learnt the concepts of DHCP , DNS, and HTTP protocols and using this protocols with cisco packet tracer.

**PRACTICAL-11**

**AIM: Write a program to find Checksum and Cyclic Redundancy check of two binary strings.**

**THEORY/PRACTICAL:**

*CHECKSUM:-*

#include<stdio.h>

#include<string.h>

int main()

{

char a[20],b[20];

char sum[20],complement[20];

int i,length;

printf("Enter first binary string\n");

scanf("%s",&a);

printf("Enter second binary string\n");

scanf("%s",&b);

if(strlen(a)==strlen(b)){

length = strlen(a);

char carry='0';

for(i=length-1;i>=0;i--)

{

if(a[i]=='0' && b[i]=='0' && carry=='0')

{

sum[i]='0';

carry='0';

}

else if(a[i]=='0' && b[i]=='0' && carry=='1')

{

sum[i]='1';

carry='0';

}

else if(a[i]=='0' && b[i]=='1' && carry=='0')

{

sum[i]='1';

carry='0';

}

else if(a[i]=='0' && b[i]=='1' && carry=='1')

{

sum[i]='0';

carry='1';

}

else if(a[i]=='1' && b[i]=='0' && carry=='0')

{

sum[i]='1';

carry='0';

}

else if(a[i]=='1' && b[i]=='0' && carry=='1')

{

sum[i]='0';

carry='1';

}

else if(a[i]=='1' && b[i]=='1' && carry=='0')

{

sum[i]='0';

carry='1';

}

else if(a[i]=='1' && b[i]=='1' && carry=='1')

{

sum[i]='1';

carry='1';

}

else

break;

}

printf("\nSum=%c%s",carry,sum);

for(i=0;i<length;i++)

{

if(sum[i]=='0')

complement[i]='1';

else

complement[i]='0';

}

if(carry=='1')

carry='0';

else

carry='1';

printf("\nChecksum=%c%s",carry,complement);

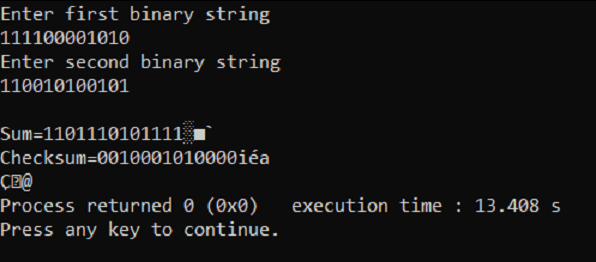
}

else {

printf("\nWrong input strings");

}}

**OUTPUT:-**



*CRC(Cyclic Redundancy Check):-*

#include<iostream>

#include<fstream>

using namespace std;

void withoutfile()

{

int i,j,k;

int fs;

cout<<"Enter Frame size:";

cin>>fs;

int f[20];

cout<<endl<<"Enter Frame:"<<endl;

for(i=0;i<fs;i++)

{

cin>>f[i];

}

int gs;

cout<<endl<<"Enter Generator size:";

cin>>gs;

int g[20];

cout<<endl<<"Enter Generator:"<<endl;

for(i=0;i<gs;i++)

{

cin>>g[i];

}

cout<<endl<<"Sender Side:";

cout<<endl<<"Frame: ";

for(i=0;i<fs;i++)

{

cout<<f[i];

}

cout<<endl<<"Generator :";

for(i=0;i<gs;i++)

{

cout<<g[i];

}

int rs=gs-1;

cout<<endl<<"Number of 0's to be appended: "<<rs;

for (i=fs;i<fs+rs;i++)

{

f[i]=0;

}

int temp[20];

for(i=0;i<20;i++)

{

temp[i]=f[i];

}

cout<<endl<<"Message after appending 0's :";

for(i=0; i<fs+rs;i++)

{

cout<<temp[i];

}

for(i=0;i<fs;i++)

{

j=0;

k=i;

if (temp[k]>=g[j])

{

for(j=0,k=i;j<gs;j++,k++)

{

if((temp[k]==1 && g[j]==1) || (temp[k]==0 && g[j]==0))

{

temp[k]=0;

}

else

{

temp[k]=1;

}

}

}

}

int crc[15];

for(i=0,j=fs;i<rs;i++,j++)

{

crc[i]=temp[j];

}

cout<<endl<<"CRC bits: ";

for(i=0;i<rs;i++)

{

cout<<crc[i];

}

cout<<endl<<"Transmitted Frame: ";

int tf[15];

for(i=0;i<fs;i++)

{

tf[i]=f[i];

}

for(i=fs,j=0;i<fs+rs;i++,j++)

{

tf[i]=crc[j];

}

for(i=0;i<fs+rs;i++)

{

cout<<tf[i];

}

}

void withfilecheck()

{

int i=0,j=0,k;

int fs=6;

int f[20];

int gs=4;

int g[20];

fstream f1,f2;

f1.open("FrameFile.txt",ios::in|ios::out);

while(f1)

{

f1>>f[i];

i++;

}

f2.open("GeneratorFile.txt",ios::in|ios::out);

while(f2)

{

f2>>g[j];

j++;

}

cout<<endl<<"Sender Side:";

cout<<endl<<"Frame: ";

for(i=0;i<fs;i++)

{

cout<<f[i];

}

cout<<endl<<"Generator :";

for(i=0;i<gs;i++)

{

cout<<g[i];

}

int rs=gs-1;

cout<<endl<<"Number of 0's to be appended: "<<rs;

for (i=fs;i<fs+rs;i++)

{

f[i]=0;

}

int temp[20];

for(i=0;i<20;i++)

{

temp[i]=f[i];

}

cout<<endl<<"Message after appending 0's :";

for(i=0; i<fs+rs;i++)

{

cout<<temp[i];

}

for(i=0;i<fs;i++)

{

j=0;

k=i;

if (temp[k]>=g[j])

{

for(j=0,k=i;j<gs;j++,k++)

{

if((temp[k]==1 && g[j]==1) || (temp[k]==0 && g[j]==0))

{

temp[k]=0;

}

else

{

temp[k]=1;

}

}

}

}

int crc[15];

for(i=0,j=fs;i<rs;i++,j++)

{

crc[i]=temp[j];

}

cout<<endl<<"CRC bits: ";

for(i=0;i<rs;i++)

{

cout<<crc[i];

}

cout<<endl<<"Transmitted Frame: ";

int tf[15];

for(i=0;i<fs;i++)

{

tf[i]=f[i];

}

for(i=fs,j=0;i<fs+rs;i++,j++)

{

tf[i]=crc[j];

}

for(i=0;i<fs+rs;i++)

{

cout<<tf[i];

}

}

int main()

{

int x;

char ans;

do

{

cout<<endl<<"1.Without filecheck";

cout<<endl<<"2.Filecheck";

cout<<endl<<"Enter the your choice:";

cin>>x;

switch(x)

{

case 1:

cout<<endl<<"CRC without file"<<endl;

withoutfile();

break;

case 2:

cout<<endl<<"CRC with file";

withfilecheck();

}

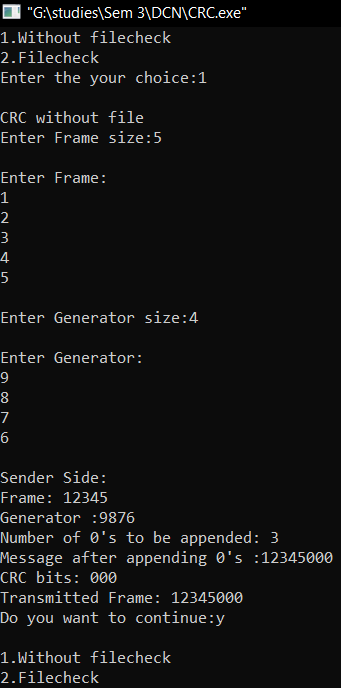
cout<<endl<<"Do you want to continue:";

cin>>ans;

}while(ans=='y'||ans=='Y');

}

**OUTPUT:-**



**REFERENCES:-**

<https://www.geeksforgeeks.org/modulo-2-binary-division/>

<http://scanftree.com/programs/c/c-program-to-implement-crc-cyclic-redundancy-code/>

**CONCLUSION:-**In this practical we have learnt the concepts of checksum and CRC (Cyclic Redundancy Check).we have also written C and C++ codes for performing the CRC and Checksum practicals.

**PRACTICAL-12**

**AIM :- Demonstrate NS2 network simulator.**

**PRACTICAL/THEORY:-**

**NS2 Simulator**

NS (from network simulator) is a name for a series of discrete events,network simulators specifically ns-1, ns-2, and ns-3. All are discrete-event computer network simulators, primarily used in research and teaching. Ns-2 began as a revision of ns-1. We are able to crete our own topologies using the NS2 simulator .The Ns simulator versions are basically written in C++ and python where the core language is C++. This task can be performed by two ways . The topologies can be created using the drag and drop facility and also by the codes.

**Our Topology in NS2 simulator:-**

We have created our Topology which is Combination of Ring Topology and Star Topology. Outer Nodes that are N0 – N1 – N3 – N4 – N2 are connected in Ring topology and Node N5 acts as Hub for Star Topology.

**RING TOPOLOGY**

Ring topology, also known as Ring network, is a type of network topology where each node is exactly connected to two other nodes, forward and backward, thus forming a single continuous path for signal transmission.

### Advantages of Ring topology:

* Reduced chances of data collision as each node release a data packet after receiving the token.
* No need of server to control connectivity among the nodes
* Equal access to the resources

### Disadvantages of Ring topology:

* In Unidirectional Ring, a data packet must pass through all the nodes.

**STAR TOPOLOGY**

In Star topology, all the components of network are connected to the central device called “hub” which may be a hub, a router or a switch. Unlike [Bus topology](http://www.ianswer4u.com/2011/05/bus-topology-advantages-and.html), where nodes were connected to central cable, here all the workstations are connected to central device with a point-to-point connection.

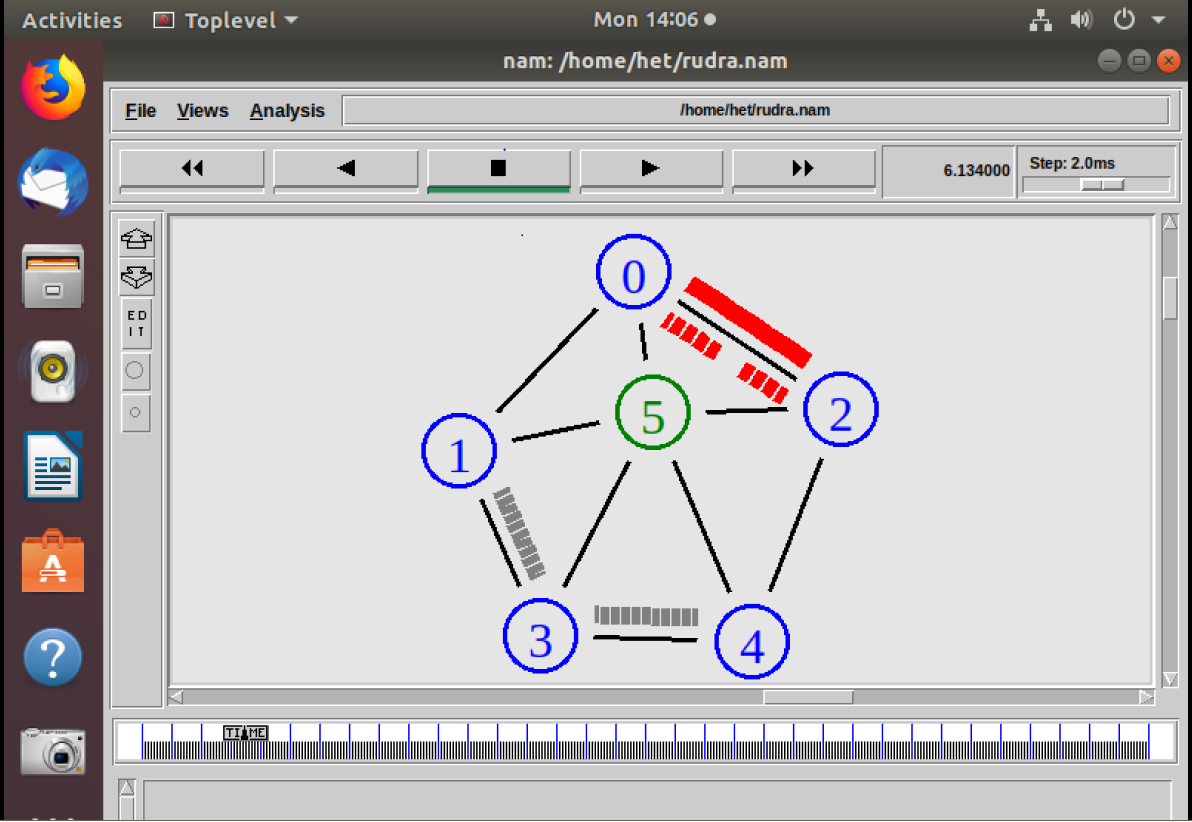
### Advantages of Star Topology

**1)**  As compared to Bus topology it gives far much better performance, signals don’t necessarily get transmitted to all the workstations. Performance of the network is dependent on the capacity of central hub.  
**2)** Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network.   
**3)**  Centralized management. It helps in monitoring the network.  
**4)**  Failure of one node or link doesn’t affect the rest of network. At the same time its easy to detect the failure and troubleshoot it.

### Disadvantages of Star Topology

**1)**  Too much dependency on central device has its own drawbacks. If it fails whole network goes down.  
**2)**  The use of hub, a router or a switch as central device increases the overall cost of the network.

**3)**  Performance and as well number of nodes which can be added in such topology is depended on capacity of central device



**HOW OUR TOPOLOGY IS CONNECTED ?**

In our Topology Node N5 acts as Hub for Star Topology and it is connected to Nodes N1, N2, N4, N3, N1 directly. We have Given TCP ( Transfer Control Protocol ) / FTP ( File Transfer Protocol ) to N0 which Sends Signal and at the Receiving Node which is N2 we have given TCPSink.

We have Given UDP (User Datagram Protocol) to Node N1 and along with it at receiving node i.e. N4 we’ve given Null and CBR ( Constant Bitrate ) Protocol with UDP as it is Supporting Protocol to UDP Protocol.

**REFERENCES:-**

<https://www.linuxjournal.com/article/5929>

<https://www.youtube.com/watch?v=7x2ltAWy3-c>

<http://www.jgyan.com/ns2/mesh%20topology%20simulation.php>

<https://www.cs.virginia.edu/~cs757/slidespdf/cs757-ns2-tutorial-exercise.pdf>

**CONCLUSION:-**In this practical we have learnt the process of making a hybrid topology using the NS2 network simulators.