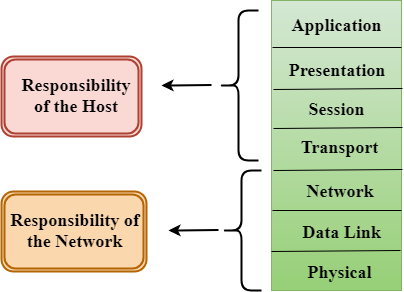
**EXPERIMENT 1A**

**AIM**

To study different layers of OSI Model and define proper functions of protocols involved in OSI Model.

**THEORY**

* OSI stands for Open System Interconnection is a reference model that describes how information from a [software](https://www.javatpoint.com/software) application in one [computer](https://www.javatpoint.com/what-is-computer) moves through a physical medium to the software application in another computer.
* OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
* OSI consists of seven layers, and each layer performs a particular network function.
* Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.



**LAYERS**

The 7 Layers of the OSI Model:

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Datalink Layer
7. Physical Layer

**FUNCTIONS OF LAYERS**

**Application Layer**

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication. An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer. This layer provides the network services to the end-users.

**Presentation Layer**

It acts as a data translator for a network. This layer is a part of the operating system that converts the data from one presentation format to another format. Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network. It at times also called the syntax layer.

**Session Layer**

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and terminates at layer 5. Session layer services also include authentication and reconnections.

**Transport Layer**

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol. It receives the data from the upper layer and converts them into smaller units known as segments.

This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably. When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

**Network Layer**

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

**Datalink Layer**

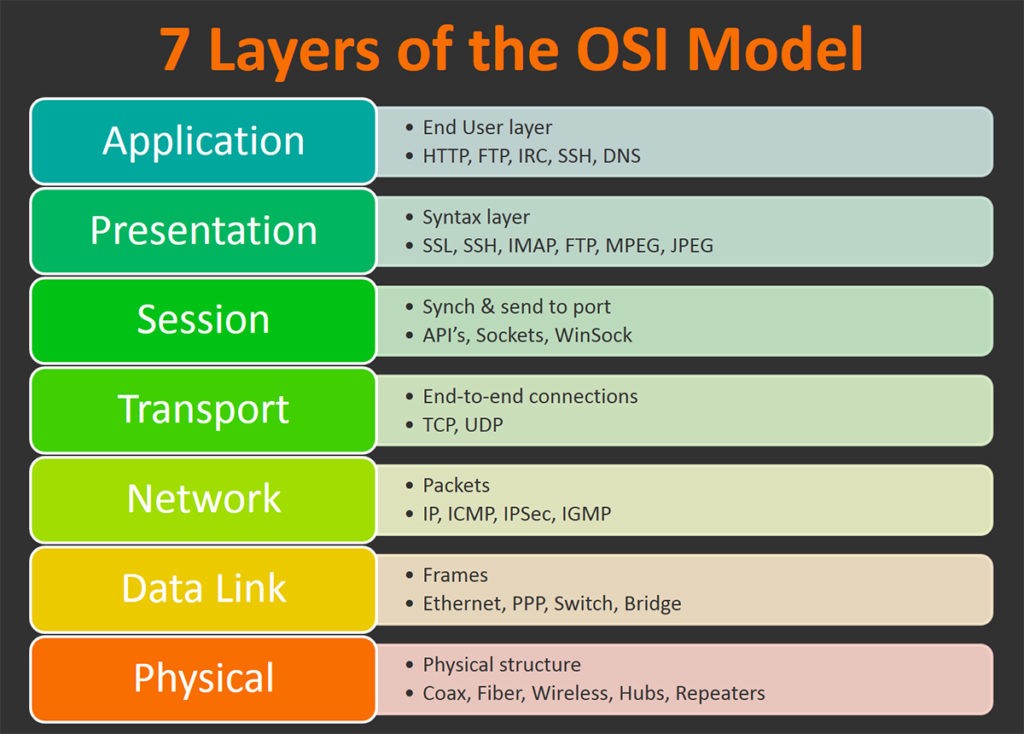
At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

**Physical Layer**

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

**PROTOCOLS**

****

1. HTTP: Hypertext Transfer Protocol (HTTP) is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers.
2. FTP: The File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server.
3. DNS: DNS stands for Domain Name System. The main function of DNS is to translate domain names into IP Addresses, which computers can understand. It also provides a list of mail servers which accept Emails for each domain name.
4. IMAP: In computing, the Internet Message Access Protocol is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection.
5. TCP: TCP stands for Transmission Control Protocol a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.
6. UDP: User datagram protocol (UDP) operates on top of the Internet Protocol (IP) to transmit datagrams over a network.
7. IP: An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.
8. ICMP: Internet Control Message Protocol (ICMP) is used for reporting errors and performing network diagnostics. In the error reporting process, ICMP sends messages from the receiver to the sender when data does not come though as it should.
9. SSH: SSH provides password or public-key based authentication and encrypts connections between two network endpoints. It is a secure alternative to legacy login protocols (such as telnet, login) and insecure file transfer methods (such as FTP).
10. IRC:  It is mainly used for group discussion in chat rooms called “channels” although it supports private messages between two users, data transfer, and various server-side and client-side commands.

**EXPERIMENT 1B**

**AIM**

To study the different layers of TCP-IP Model and define proper definition of protocols involved in TCP-IP Model.

**THEORY**

* The TCP/IP model was developed prior to the OSI model.
* The TCP/IP model is not exactly similar to the OSI model.
* The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
* The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
* TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.



**LAYERS**

The 4 layers of TCP-IP Model is as follows:

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Network Access Layer

**FUNCTIONS OF LAYERS**

Application Layer

An application layer is the topmost layer in the TCP/IP model. It is responsible for handling high-level protocols, issues of representation. This layer allows the user to interact with the application. When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD.

Transport Layer

It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network. The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

Internet Layer

An internet layer is the second layer of the TCP/IP model. An internet layer is also known as the network layer. The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take. This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network.

Network Access Layer

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data. This layer is mainly responsible for the transmission of the data between two devices on the same network. The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

**PROTOCOLS**

1. HTTP and HTTPS – HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
2. SSH – SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. NTP – NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions.
4. Transmission Control Protocol (TCP) – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
5. User Datagram Protocol (UDP) – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.
6. IP – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions

IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.

1. ICMP – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
2. ARP – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.
3. IP – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
4. IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
5. ICMP – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
6. ARP – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.
7. SNMP: SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
8. SMTP: SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
9. DNS: DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

**EXPERIEMENT 1C**

**AIM**

To study the data characteristics of Network and User data with respect to Physical Layer of OSI model. To study what is Modulation and it’s types. To study what is encoding and its type.

**THEORY**

1. **Modulation**

Modulation is the process of encoding information from a message source in a way that is suitable for transmission. This is achieved by altering the characteristics of a wave. By superimposing a message on to a high frequency signal known as a carrier wave (or sinusoidal signal), video, voice and other data can be transmitted. In the modulation process, a parameter of the carrier wave (such as amplitude, frequency or phase) is varied in accordance with the modulating signal. This variation acts as a code for data transmission. This modulated signal is then transmitted by the transmitter. The receiver demodulates the received modulated signal and gets the original information signal back.

1. **Types of Modulation**
2. Analog Modulation

In analog modulation, analog signal (sinusoidal signal) is used as a carrier signal that modulates the message signal or data signal. The general function Sinusoidal wave’s is shown in the figure below, in which, three parameters can be altered to get modulation – they are amplitude, frequency and phase; so, the types of analog modulation are:

* Amplitude Modulation (AM)
* Frequency Modulation (FM)
* Phase Modulation (PM)

Amplitude Modulation

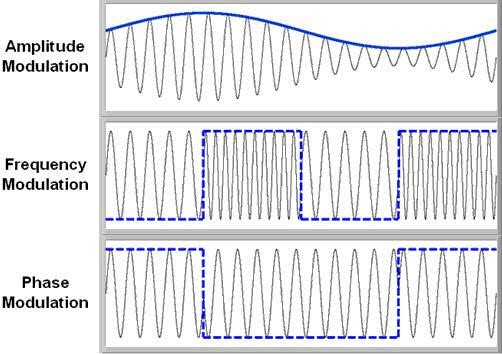
Amplitude modulation was developed in the beginning of the 20th century. It was the earliest modulation technique used to transmit voice by radio. This type of modulation technique is used in electronic communication. In this modulation, the amplitude of the carrier signal varies in accordance with the message signal, and other factors like phase and frequency remain constant.

Frequency Modulation

In this type of modulation, the frequency of the carrier signal varies in accordance with the message signal, and other parameters like amplitude and phase remain constant. Frequency modulation is used in different applications like radar, radio and telemetry, seismic prospecting and monitoring newborns for seizures via EEG, etc.

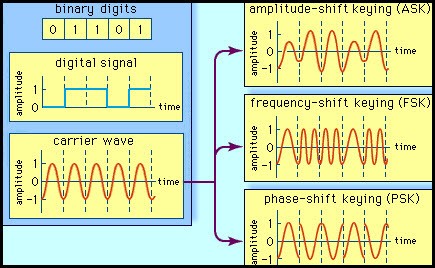
Phase Modulation

In this type of modulation, the phase of the carrier signal varies in accordance with the message signal. When the phase of the signal is changed, then it affects the frequency. So, for this reason, this modulation is also comes under the frequency modulation.



1. Digital Modulation

For a better quality and efficient communication, digital modulation technique is employed. The main advantages of the digital modulation over analog modulation include available bandwidth , high noise immunity and permissible power. In digital modulation, a message signal is converted from analog to digital message, and then modulated by using a carrier wave.



**Digital Modulation**

The carrier wave is switched on and off to create pulses such that the signal is modulated. Similar to the analog, in this system, the type of the digital modulation is decided by the variation of the carrier wave parameters like amplitude, phase and frequency.

1. **Encoding**

Encoding and decoding processes for data communications have interesting origins.

In computers, encoding is the process of putting a sequence of [characters](https://whatis.techtarget.com/definition/character) (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage. Decoding is the opposite process -- the conversion of an encoded format back into the original sequence of characters.

Digital-to-Digital Encoding

• The binary signals created by your computer (DTE) are translated into a

sequence of voltage pulses that can be sent through the transmission

medium.

• Binary signals have two basic parameters: amplitude and duration.

• As the number of bits sent per unit of time increases, the bit duration

decreases.

• The three most common methods of encoding used are: unipolar, polar,

and bipolar.

**NRZ**

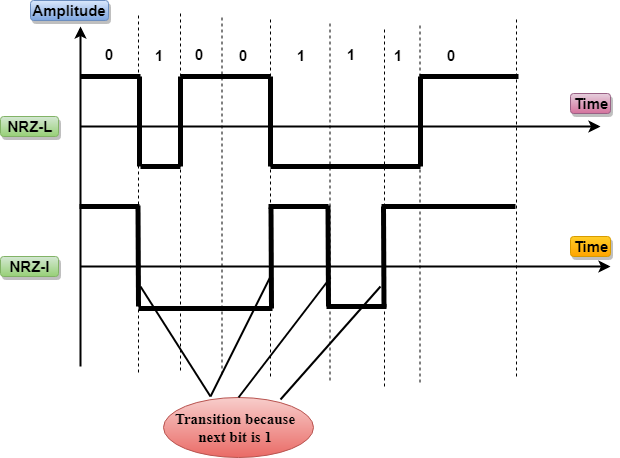
NRZ stands for Non-Return Zero.

In NRZ encoding, the level of the signal can be represented either positive or negative.

**The two most common methods used in NRZ are:**

**NRZ-L:** In NRZ-L encoding, the level of the signal depends on the type of the bit that it represents. If a bit is 0 or 1, then their voltages will be positive and negative respectively. Therefore, we can say that the level of the signal is dependent on the state of the bit.

**NRZ-I:** NRZ-I is an inversion of the voltage level that represents 1 bit. In the NRZ-I encoding scheme, a transition occurs between the positive and negative voltage that represents 1 bit. In this scheme, 0 bit represents no change and 1 bit represents a change in voltage level.

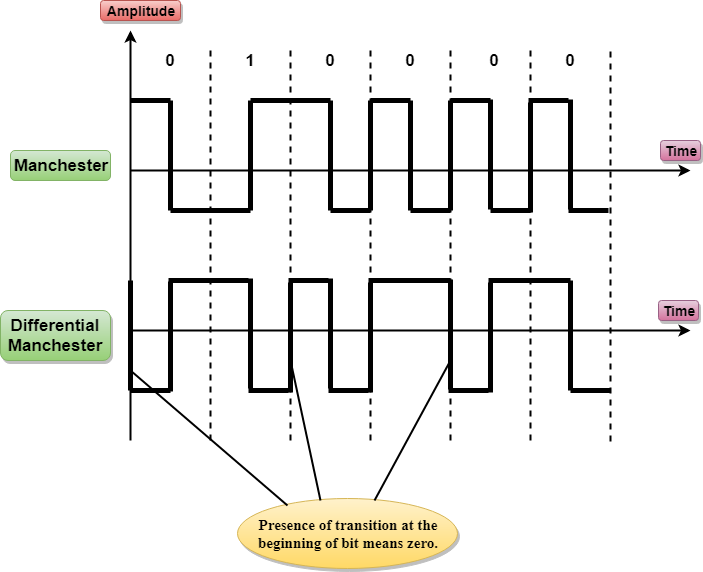


**Manchester Encoding**

* It changes the signal at the middle of the bit interval but does not return to zero for synchronization.
* In Manchester encoding, a negative-to-positive transition represents binary 1, and positive-to-negative transition represents 0.
* Manchester has the same level of synchronization as RZ scheme except that it has two levels of amplitude.

**Differential Manchester**

* It changes the signal at the middle of the bit interval for synchronization, but the presence or absence of the transition at the beginning of the interval determines the bit. A transition means binary 0 and no transition means binary 1.
* In Manchester Encoding scheme, two signal changes represent 0 and one signal change represent 1.



**Analog-to-Digital Encoding**

* When an analog signal is digitalized, this is called an analog-to-digital conversion.
* Suppose human sends a voice in the form of an analog signal, we need to digitalize the analog signal which is less prone to noise. It requires a reduction in the number of values in an analog message so that they can be represented in the digital stream.
* In analog-to-digital conversion, the information contained in a continuous wave form is converted in digital pulses.

**Digital-to-Analog Encoding**

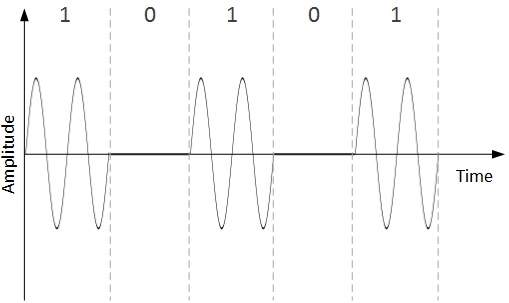
When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data. An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

* **Amplitude Shift Keying**

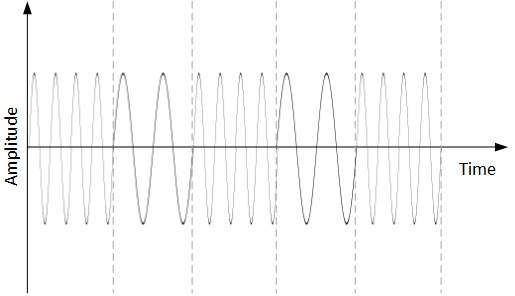
In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

* **Frequency Shift Keying**

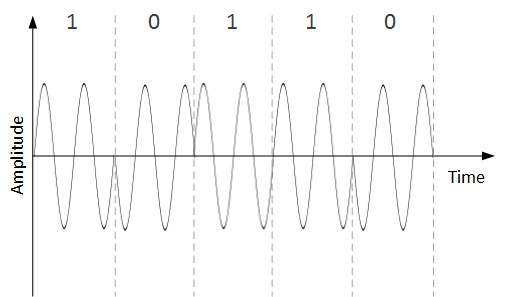
In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

* **Phase Shift Keying**

In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.



When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

**Analog to Analog**

Analog-to-analog conversion, or modulation, is the representation of analog information by an analog signal. It is a process by virtue of which a characteristic of carrier wave is varied according to the instantaneous amplitude of the modulating signal. This modulation is generally needed when a **bandpass channel**is required. Bandpass is a range of frequencies which are transmitted through a bandpass filter which is a filter allowing specific frequencies to pass preventing signals at unwanted frequencies.

**EXPERIMENT 02**

**AIM**

To study about Physical layer of ISO-OSI Model in detail.

**THEORY**

**Define the Following terms: -**

**Channel Impairment**: In communication system, analog signals travel through transmission media, which tends to deteriorate the quality of analog signal, which means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. The imperfection causes signal impairment.

**Signal Attenuation**:  It means loss of energy. The strength of signal decreases with increasing distance which causes loss of energy in overcoming resistance of medium. This is also known as attenuated signal. Amplifiers are used to amplify the attenuated signal which gives the original signal back and compensate for this loss.

**Delay**: Network delay is a design and performance characteristic of a telecommunications network. It specifies the latency for a bit of data to travel across the network from one communication endpoint to another.

**Distortion**: It means changes in the form or shape of the signal. This is generally seen in composite signals made up with different frequencies. Each frequency component has its own propagation speed travelling through a medium. And that’s why it delay in arriving at the final destination Every component arrive at different time which leads to distortion. Therefore, they have different phases at receiver end from what they had at sender’s end.

**Noise**: The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal. Induced noise comes from sources such as motors and appliances. These devices act as sending antenna and transmission medium act as receiving antenna. Thermal noise is movement of electrons in wire which creates an extra signal. Crosstalk noise is when one wire affects the other wire. Impulse noise is a signal with high energy that comes from lightning or power lines

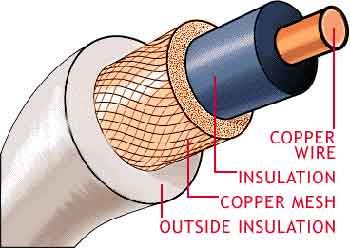
**Multipath**: Multipath is very similar to echo in concept. It is the phenomenon in which a signal arrives at the receiver from reflections and sometime including the direct line of sight (LoS). The resulting signal is a sum of its replicas with different arrival times. The study of multipath is important especially in the wireless communication systems and offers the most significant challenge to the system designers. The uniqueness of this noise type is that it could be used constructively by combining the signal replications in a constructive way

**B) State various types of Transmission Media Techniques.**

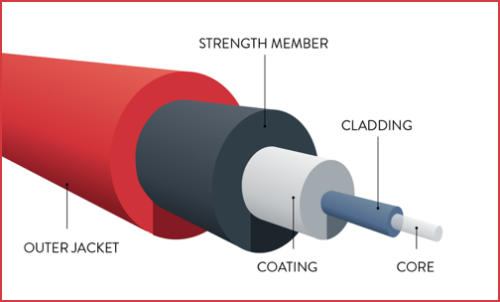
**Twisted Pair Copper Cables:** A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures. All transmissions are prone to noise, interferences, and crosstalk. When the wires are twisted, some part of the noise signals is in the direction of data signals while the other parts are in the opposite directions. Thus the external waves cancel out due to the different twists. The receiver calculates the difference in the voltages of the two wires for retrieving data. Thus a much better immunity against noise is obtained. There are two types of twisted pair cables −

* Unshielded Twisted Pair (UTP): These generally comprise of wires and insulators.
* Shielded Twisted Pair (STP): They have a braided wired mesh that encases each pair of insulated wires.

**Co-axial Cable**: It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.



* **Optical Fiber cable**: It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data. The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode. It basically has Total Internal Reflection mech present in it. When angle of Incidence is greater than critical angle then TIR happens. Increased capacity and bandwidth. It’s features are that is Lightweight, Less signal attenuation, having Immunity to electromagnetic interference and Resistance to corrosive materials.



**C)** **Wireless Transmission Media**

**Radio-waves:** These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio-waves for transmission.

**Micro-waves**: It is a line-of-sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

**Infrared-waves:** Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

**D) Define the below with the help of Physical Layer Protocol Example: EIA-232-F.**

**Mechanical properties:** EIA 232 defines a 25-pin connector referred to as DB-25. Although 22 of the 25 pins have been allocated specific functions, it is rarely the case that all the 22 pins are used during a connection. In fact, some companies have defined their own connectors that vary slightly from one another. Prominent among these has been the IBM PC serial port connector using 9 pins (DB-9 connector). Figure 4-8 gives an account of pin definitions for DB25 and DB-9 on the DTE side. Figure 4-8 is simply a functional diagram and is not drawn according to the true scale or proportions of the actual standard.

**Electrical properties:** The standard specifies the use of digital signaling (bipolar mark and space) with a voltage below -3 volts representing binary 1 and a voltage above +3 volts represents binary 0. The peak voltage levels are restricted within For control signals, the circuit state of logical ‘1’ is used to indicate an inactive condition while a transition to logical ‘0’ indicates an active condition. For data signals, the transition of signal pulse on the signal element timing circuit is used as transition to the next data element on the data circuits. The tolerances of timing vary according to the data rate, from less than 1 ms for very low data rates data rates to less than 5 µsec for data rates up to 8 kbps.

**Functional properties:** The functional characteristics of EIA-232 follow easily from the pin definitions. Each pin has an associated circuit that performs a specific task. Over the years there have been improvements and additions over the original RS-232. There are still some pins that can be used to expand the functions in future. We will discuss various operation modes under the ‘Procedures’ in the next section. Here, we simply categorize the functions into the following: Call Setup and Handshaking, Data Transfer, Timing, Control, Testing.

**Procedural properties:** The standard specifies functions of each pin as well as the sequence of their use for different calling modes and phases. These could be the call setup, data transfer using primary or secondary circuits, full-duplex, halfduplex and simplex transfer, synchronous or asynchronous modes using internal or external timing, and test modes, for local and remote loopback. There is a way of utilizing EIA-232 interface without the intervening modems to connect two DTEs directly. In this section, we will take some examples of the procedural characteristics of the EIA-232 standard. Let’s start with the definitions of some terms. Suppose DTE A and is connected to a network via DCE A through the EIA-232 interface. Then, by ‘direction’ of data transfer, we mean either from the DTE A to DCE A or from DCE A to DTE A. Duplexity of data transfer pertains to the direction of data flow. Full-duplex data transfer takes place in both directions simultaneously. Half-duplex data transfer takes place in both directions with turns. Simplex data transfer takes place in one direction only. Two simplex circuits used to transfer data in opposite directions make up one full-duplex circuit.

**E) PHY or IEEE Wireless Local Area Network.**

The next example is from the IEEE802.11 standard for wireless local area networks (WLAN). In this protocol, the transmission characteristics play a greater role than the EIA-232. The WLANs are LANs without wires. Such networks provide the flexibilities of mobility and topology. Coupled with an ease of installation, WLAN are taking over the local network market rather swiftly. The PHY for a wireless data network does not require many functions of a 122 fixed network PHY. For example, there is no connector. In some cases, such as infrastructure networks, one of the network components, called an access point, may be connected to fixed network. In such cases, the connector is specified by the fixed network PHY. For example, if the access point is connected to an Ethernet, then it will have a socket for the RJ45 connector for UTP, a BNC terminal for this coaxial Ethernet, or an attachment unit interface (AUI) for the thick Ethernet. More than one of such socket types may be provided by many manufacturers of access points.

**F) WLAN TYPES:**

There are two types of WLANs, the infrastructure WLANs and the independent WLANs. In an infrastructure WLAN, the wireless terminals communicate via a central point called the access point. The access point is connected to a wired network. Figure 4-11 shows an example layout for an infrastructure WLAN. The infrastructure WLANs are easy to expand by using either more than one access points, or simply by using extension points. An extension point is just like an access point except that it is not connected to the wired network. A second mechanism of configuring WLANs is by having all wireless terminals with the capability of direct communications with another terminals. This eliminates the need of an access point. Such networks are called independent or ad hoc networks. Peer networking is another term used for such a layout. In addition to the two types of layouts, there are three different mechanisms used as communication media in WLANs. Two PHYs use electromagnetic (EM) radiation and the third uses infrared light. The most popularly used EM spectrum for WLANs is license-free and has been allocated for research in industrial, scientific and medical areas. Because of this reason, it is called the ISM band (ISM = Industrial, Scientific and Medical).

**EXPERIMENT 3A**

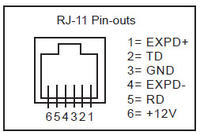
**AIM**

To understand the following connectors.

**THEORY**

**RJ-11 Connector**

A registered jack-11 (RJ-11) is a 6-position 2-conductor telephone connector/jack (6P2C) with 4 positions unused. In the United States, RJ-11 is commonly used to connect the telephone handset to the base unit, and the entire telephone to the wall outlet. A registered Jack-11 can also be used to connect LANs, but RJ-45 connectors are more commonly used for this purpose.RJ11 is used to terminate the conventional PSTN telephone networks. RJ11 is a four pins connector which is used for terminating the telephone wires. The RJ11 technically uses the center 2 contacts of 6 available and is used for wiring a single phone line. It is the common connector for plugging a telephone into the wall and the handset into the telephone. Bandwidth supported by RJ-1 is 24 Mbps.RJ11 is an 6P4C connector.

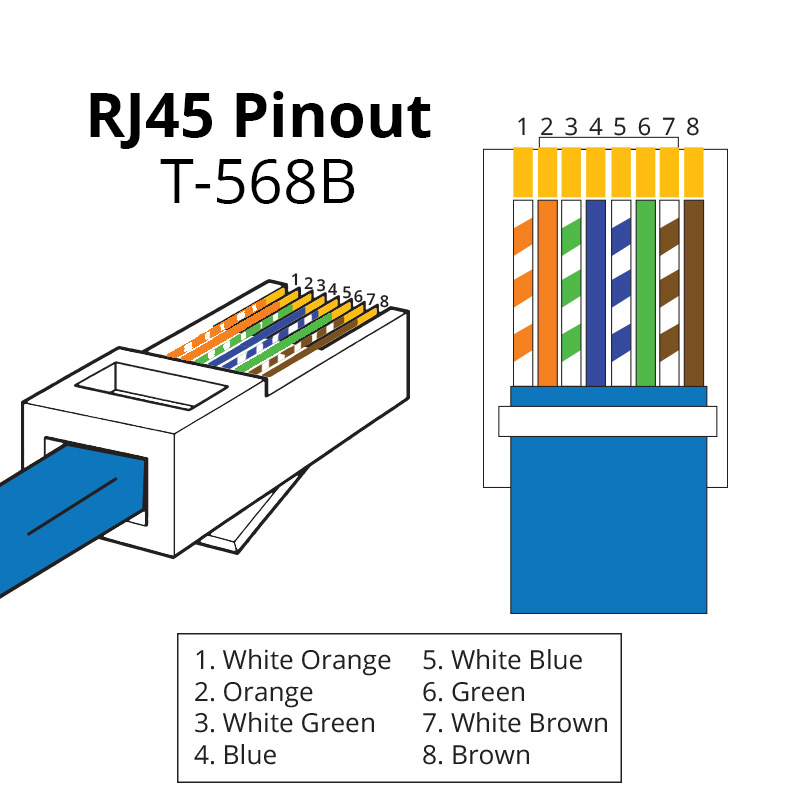


**RJ-45 Connector**

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/content/anixter/apac/en_au/search-results.html?searchTerms=RJ45+connector). RJ45 is newer, modular, self-securing and compact technology used for connecting the ethernet cables to different electronic devices. The RJ45 is an 8 pin connector used to attach the ethernet interfaces. It is known as an 8P8C connector.

Types of cables based on the termination:

1. Straight-over cable
2. Crossover cable

****

**EXPERIMENT 3B**

**AIM**

To study about various networking devices used in Computer network.

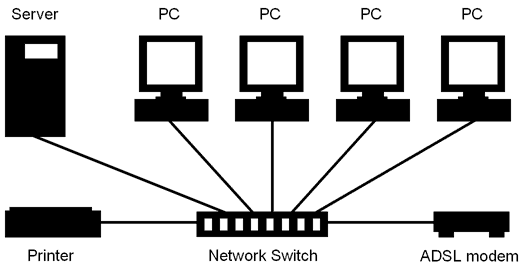
**THEORY**

**1)Switches:** Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network. A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications. A switch operates in the layer 2, i.e. data link layer of the OSI model.

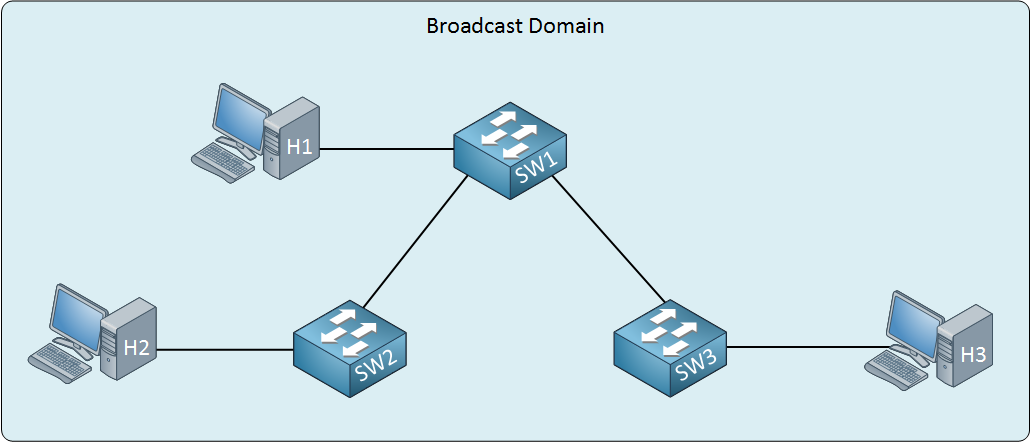
* It is an intelligent network device that can be conceived as a multiport network bridge.
* It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
* It uses packet switching technique to receive and forward data packets from the source to the destination device.
* It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.

**Types of Switches:**

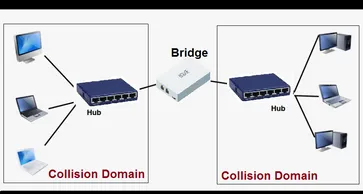
* Unmanaged Switch − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
* Managed Switch − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
* LAN Switch − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
* PoE Switch − Power over Ethernet (PoE) switches are used in PoE Gigabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections.



**2)Broadcast Switches**: A broadcast is sent by computers when they want to **send a message** to all other devices on the same LAN. ... If a switch receives a message that is sent to that destination MAC address then the switch knows it is a broadcast and will forward the message to every other connected port.



* **3)Bridges**: A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches. Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.
* By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
* Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
  + If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.
  + If the frame has a destination MAC address in a connected network, it will forward the frame toward it.
* By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
* In cases where the destination MAC address is not available, bridges can broadcast data frames to each node. To discover new segments, they maintain the MAC address table.

****

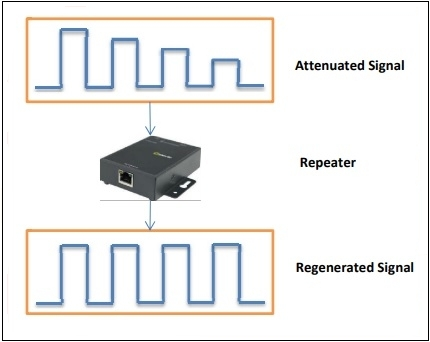
**4)Router:** The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are Cisco, 3Com, HP, Juniper, D-Link, Nortel, etc. Some important points of routers are given below:

* A router is used in LAN (Local Area Network) and WAN (Wide Area Network) environments. For example, it is used in offices for connectivity, and you can also establish the connection between distant networks such as from Bhopal to
* It shares information with other routers in networking.
* It uses the routing protocol to transfer the data across a network.

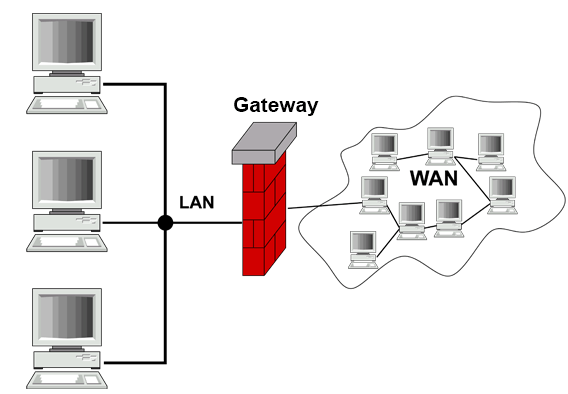


**5)Repeater:** Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters. When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.

Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss. So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

****

**6)Gateway:** A gateway is a data communication framework giving admittance to a host network through a remote network. The computer gives connectivity to a remote network or a computerized framework outside the host network node boundaries. A gateway is a hardware device that goes about as a “gate” between two networks. It very well might be a server, firewall, router, or another device that empowers traffic to stream all through the network. Gateways serve as an exit and entry point for a network as all data should go through or communication gateway before being routed.



**7)Hub:** A hub is a common connection point, also known as a network hub, which is used for connection of devices in a network. It works as a central connection for all the devices that are connected through a hub. The hub has numerous ports. If a packet reaches at one port, it is able to see by all the segments of the network due to a packet is copied to the other ports. A network hub has no routing tables or intelligence (unlike a network switch or router), which is used to send information and broadcast all network data across each and every connection.

**Types of Hub:**

There are three types of the hub that are given below:

1. Passive Hub
2. Active Hub
3. Intelligent Hub

**Passive Hub**: The passive hubs are the connection point for wires that helps to make the physical network. It is capable of determining the bugs and faulty hardware. Simply, it accepts the packet over a port and circulates it to all ports. It includes connectors (10base-2 port and RJ-45) that can be applied as a standard in your network. This connector is connected to all [local area network (LAN)](https://www.javatpoint.com/wireless-lan-introduction) devices. Additionally, the advanced passive hubs have AUI ports, which are connected as the transceiver according to the network design.

**Active Hub**: As compared to a passive hub, it includes some additional features. It is able to monitor the data sent to the connected devices. It plays an important role between the connected devices with the help of store technology, where it checks the data to be sent and decides.

**Intelligent Hub:** It is a little smarter than passive and active hubs. These hubs have some kinds of management software that help to analyze the problem in the network and resolve them. It is beneficial to expend the business in networking; the management can assign users that help to work more quickly and share a common pool efficiently by using intelligent hubs. which packet to send first.



**EXPERIMENT 04**

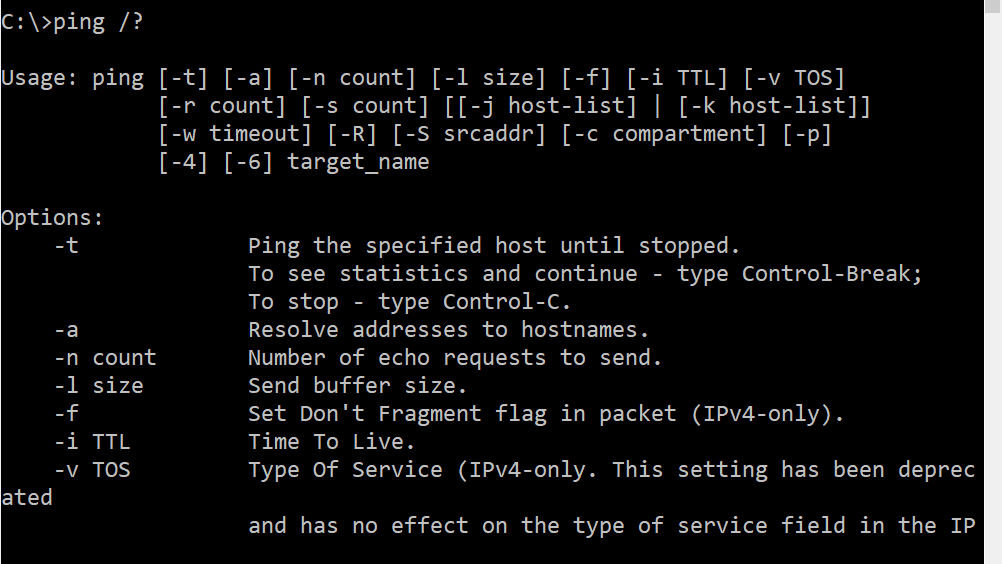
**AIM**

To work and assess various networking commands.

**THEORY**

**1)Ping command:** Ping is used to testing a network host capacity to interact with another host. Just enter the command Ping, followed by the target host’s name or IP address. The ping utilities seem to be the most common network tool. This is performed using ICMP, which allows the echo packet to be sent to the destination host and a listening mechanism. If the destination host reply to the requesting host, that means the host is reachable. This utility usually gives a basic image of where there may be a specific networking issue,

For Example: If an Internet connection is not in the office, for instance, the ping utility is used to determine if the problem exists in the office or the Internet provider’s network. The following shows an image of how ping tools to obtain the locally connected router’s connectivity status.



**2)Netstat command:** Netstat is a Common TCP – IP networking command-line method present in most Windows, Linux, UNIX, and other operating systems. The netstat provides the statistics and information in the use of the current TCP-IP Connection network about the protocol.

There are various options a user can use with the Netstat command.

Options are as follows-

* **-a:** This will display all connection and ports
* **-b:** Shows the executable involved in each connection or hearing port
* **-e:** This protocol will combine with the -sand display the ethernet statistics
* **-n:** This will display the address and the port number in the form of numerical
* **-o:** It will display the ID of each connection for the ownership process.
* **-r:** It will display the routing table

**3)Nslookup command**: The Nslookup, which stands for name server lookup command, is a network utility command used to obtain information about internet servers. It provides name server information for the DNS (Domain Name System), i.e. the default DNS server’s name and IP Address.

**4)Ipconfig command:** The command IP config will display basic details about the device’s IP address configuration. Just type IP config in the Windows prompt and the IP, subnet mask and default gateway that the current device will be presented. If you have to see full information, then type on command prompt config-all and then you will see full information. There are also choices to assist you in resolving DNS and DHCP issues.

**5)Traceroute command:** The tracert command is a cmd command which is used to get the network packet being sent and received and the number of hops required for that packet to reach to target. This command can also be referred to as a traceroute. It provides several details about the path that a packet takes from the source to the specified destination. The tracert command is available for the Command Prompt in all Windows operating systems.

Options for tracert Command are as follows-

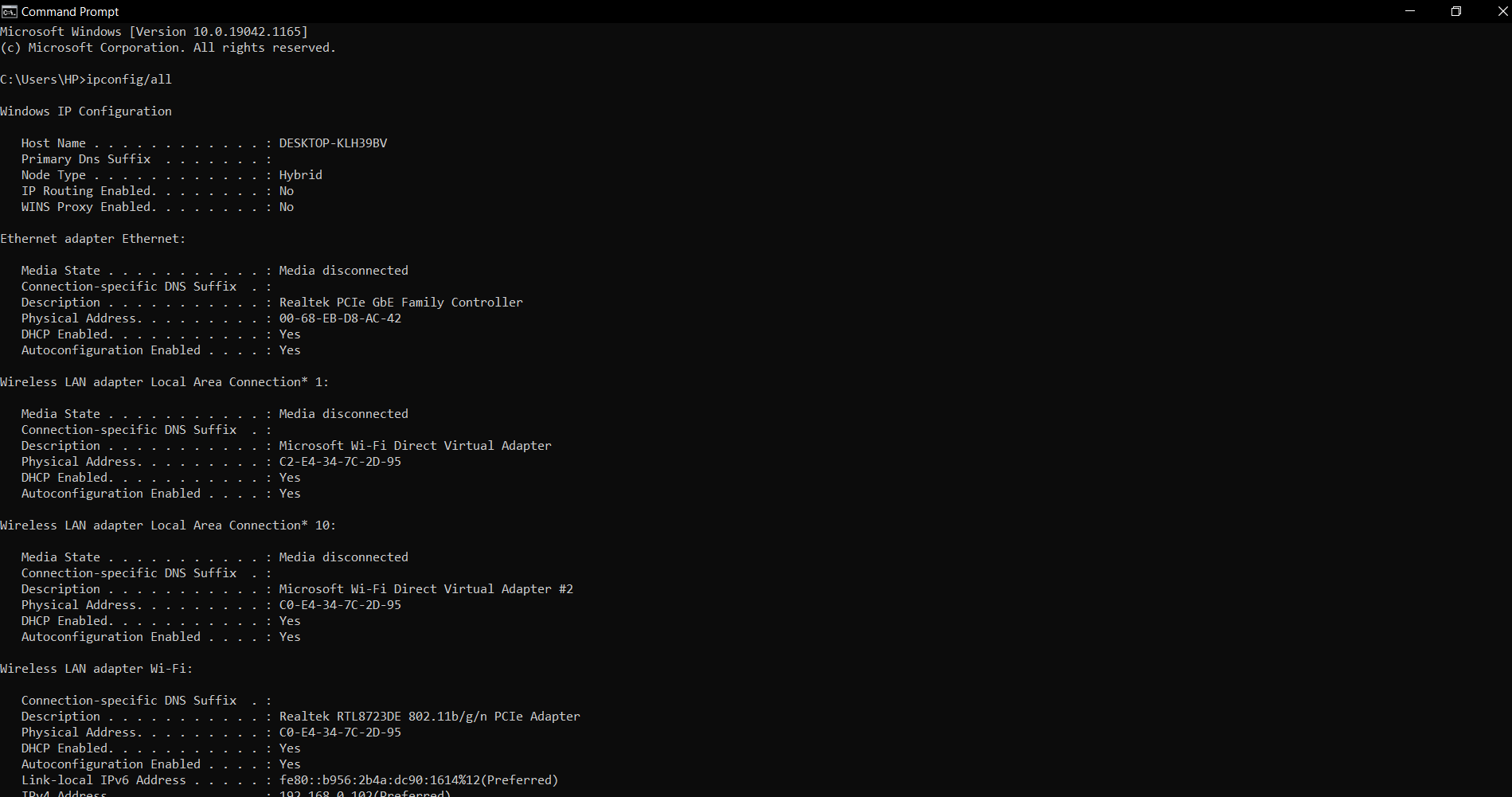
* **target:** This is the destination, either an IP address or hostname.
* –**d:** This option prevents Tracert from resolving IP addresses to hostnames to get faster results.
* **-h MaxHops:** This Tracert option specifies the maximum number of hops in the search for the target. If the MaxHops option is not specified the target has not been found by 30 hops, then the tracert command will stop looking.
* **-w timeout:** A timeout value must be specified while executing this ping command. It adjusts the amount of time in milliseconds.

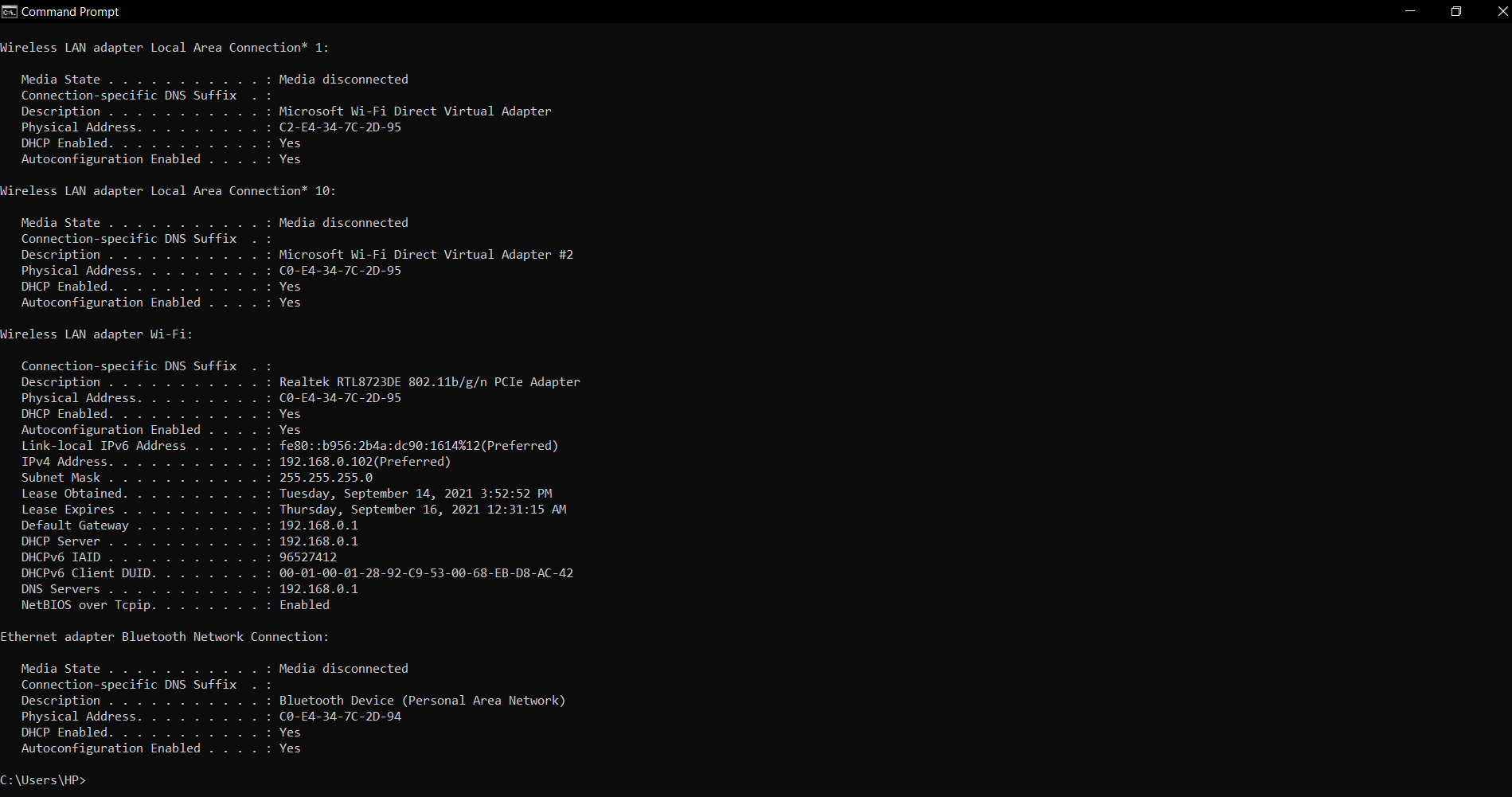
**6)Hostname command:** To communicate with each and other, the computer needs a unique address. A hostname can be alphabetic or alphanumeric and contain specific symbols used specifically to define a specific node or device in the network. For example, a hostname should have a domain name (TLD) of the top-level and a distance between one and 63 characters when used in a domain name system (DNS) or on the Internet.

**7)ARP command:** The ARP command provides information like Address, Flags, Mask, IFace, Hardware Type, Hardware Address, etc.

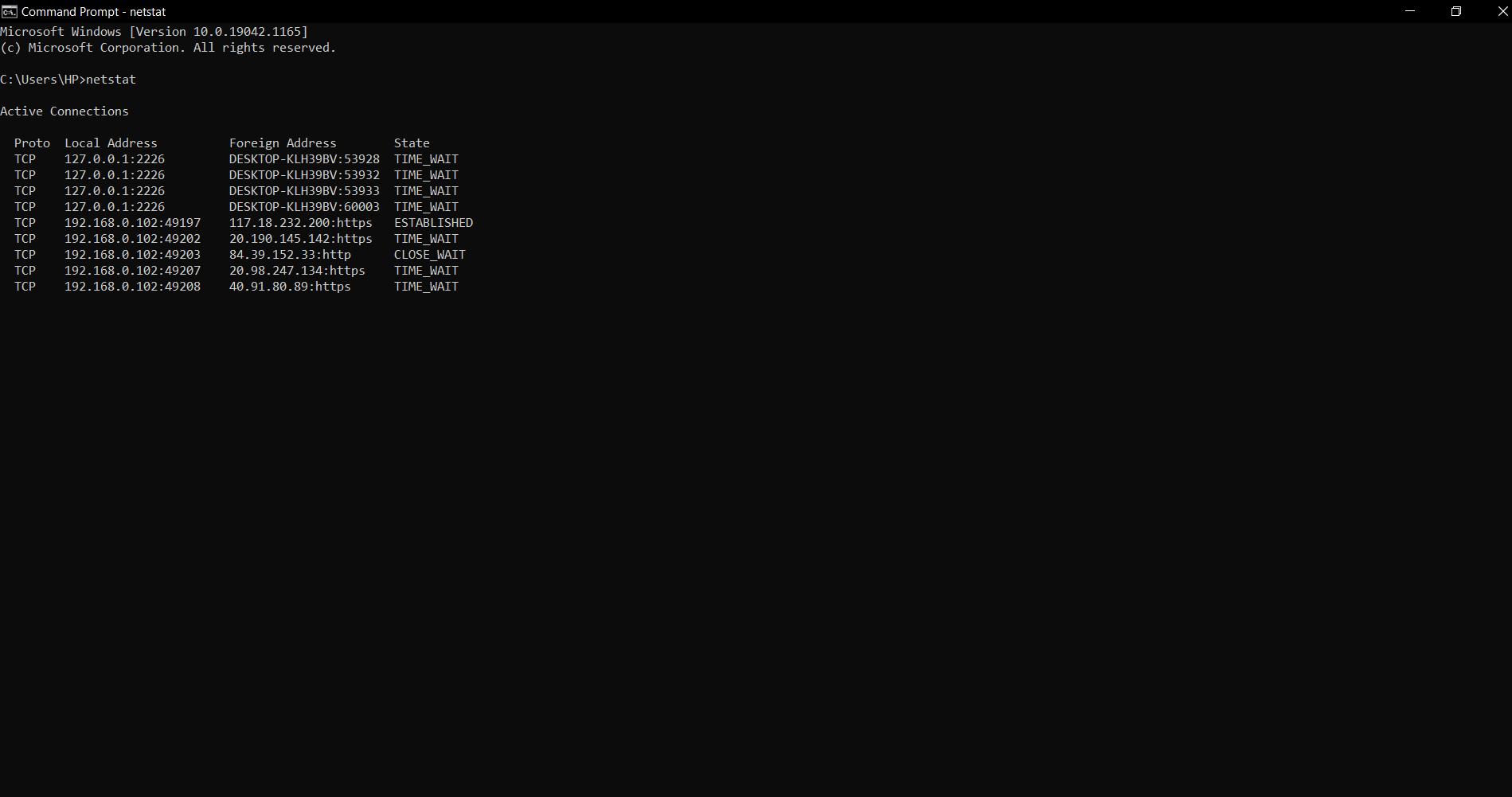
**OUTPUT**

**1)Ipconfig**

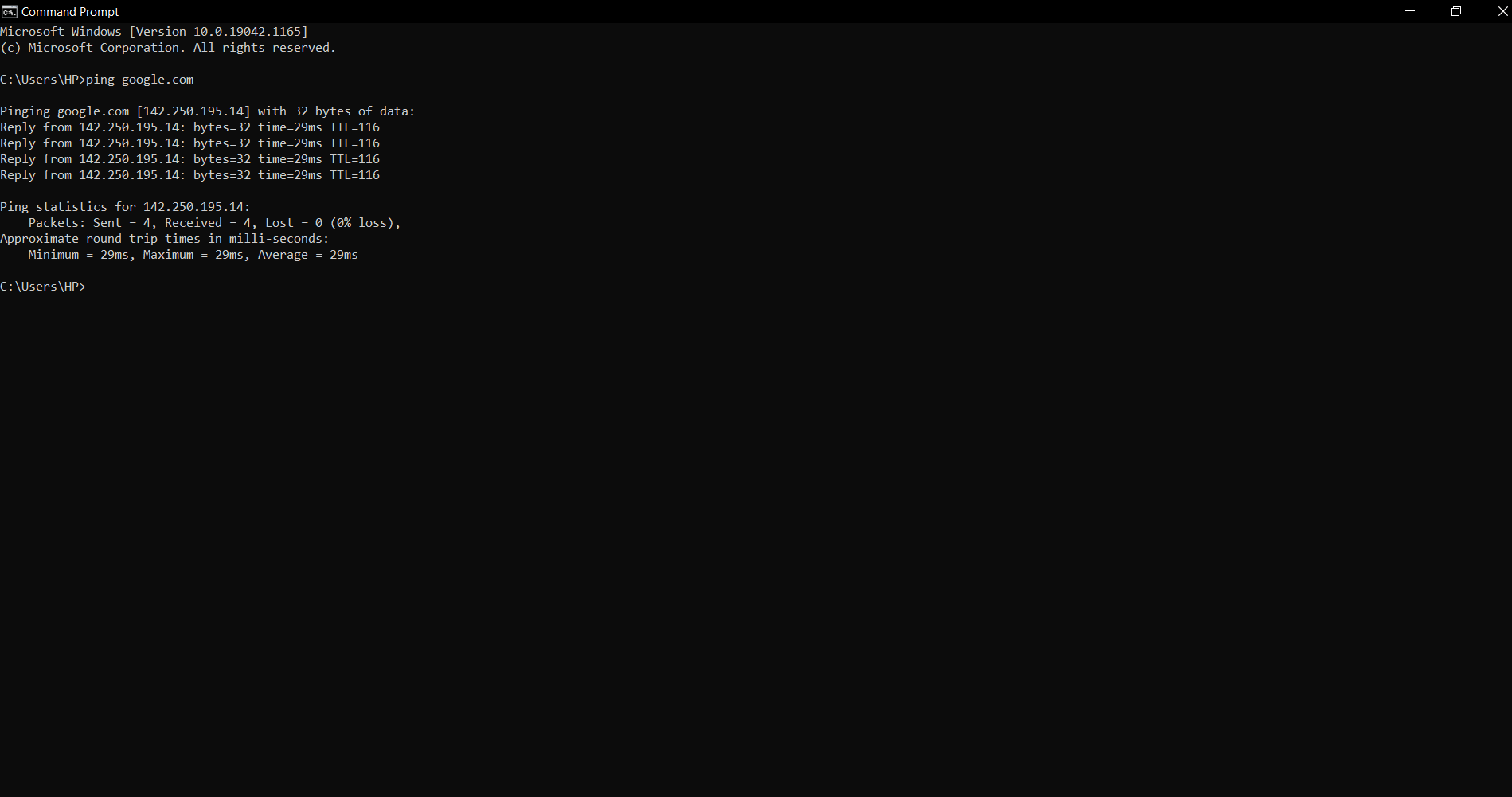
****

****

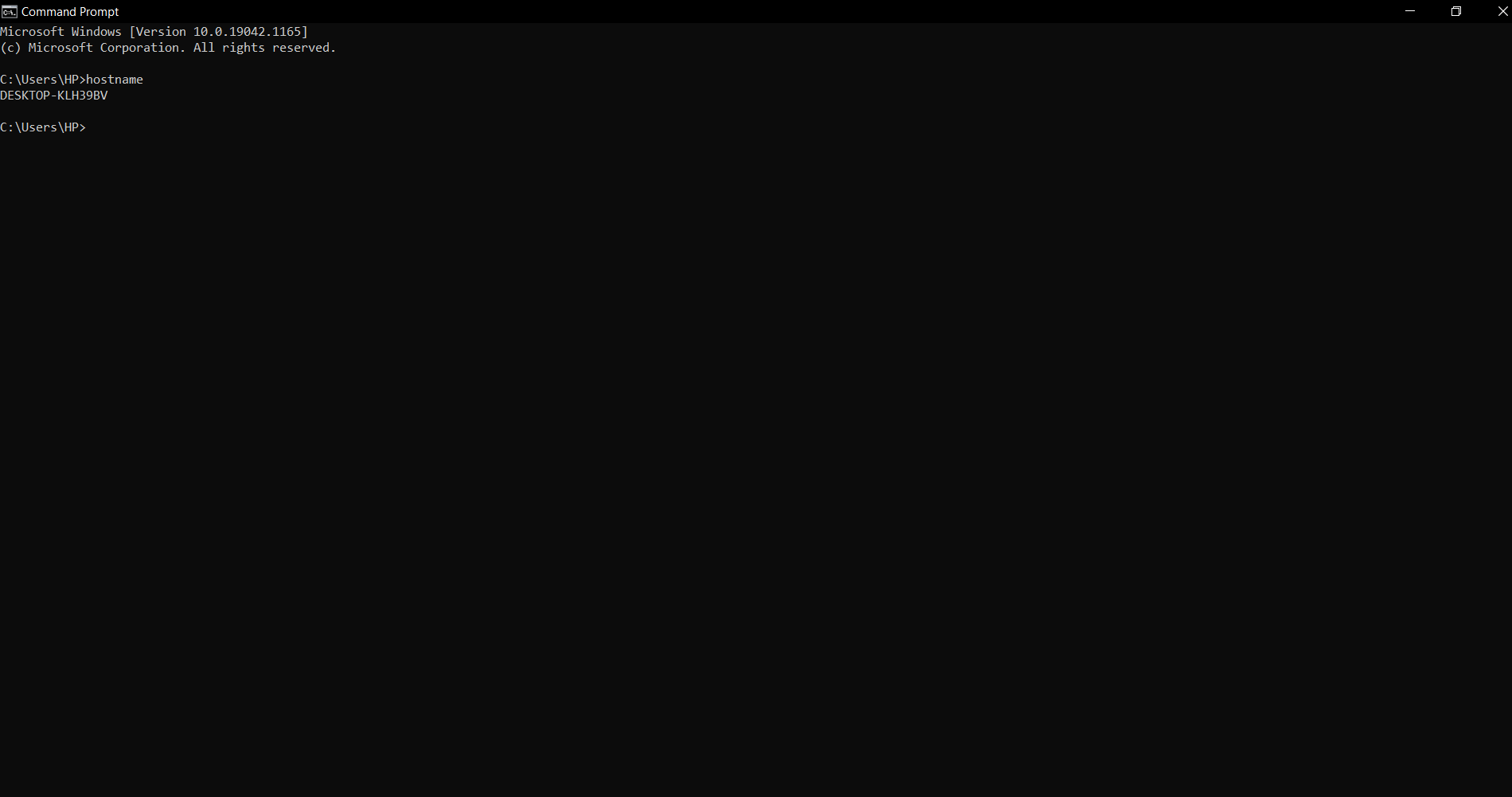
**2)Netstat**

****

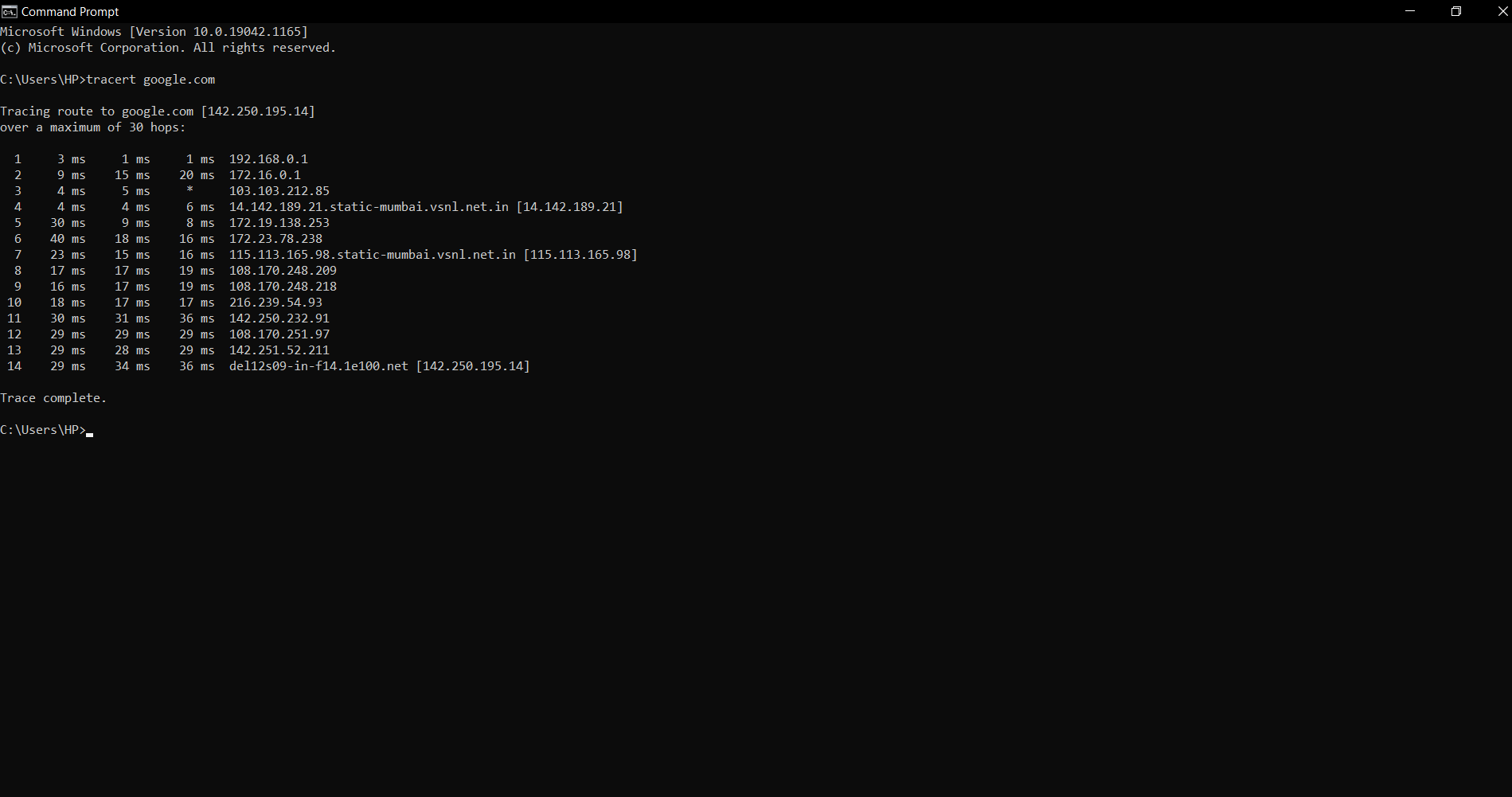
**3)Ping**

****

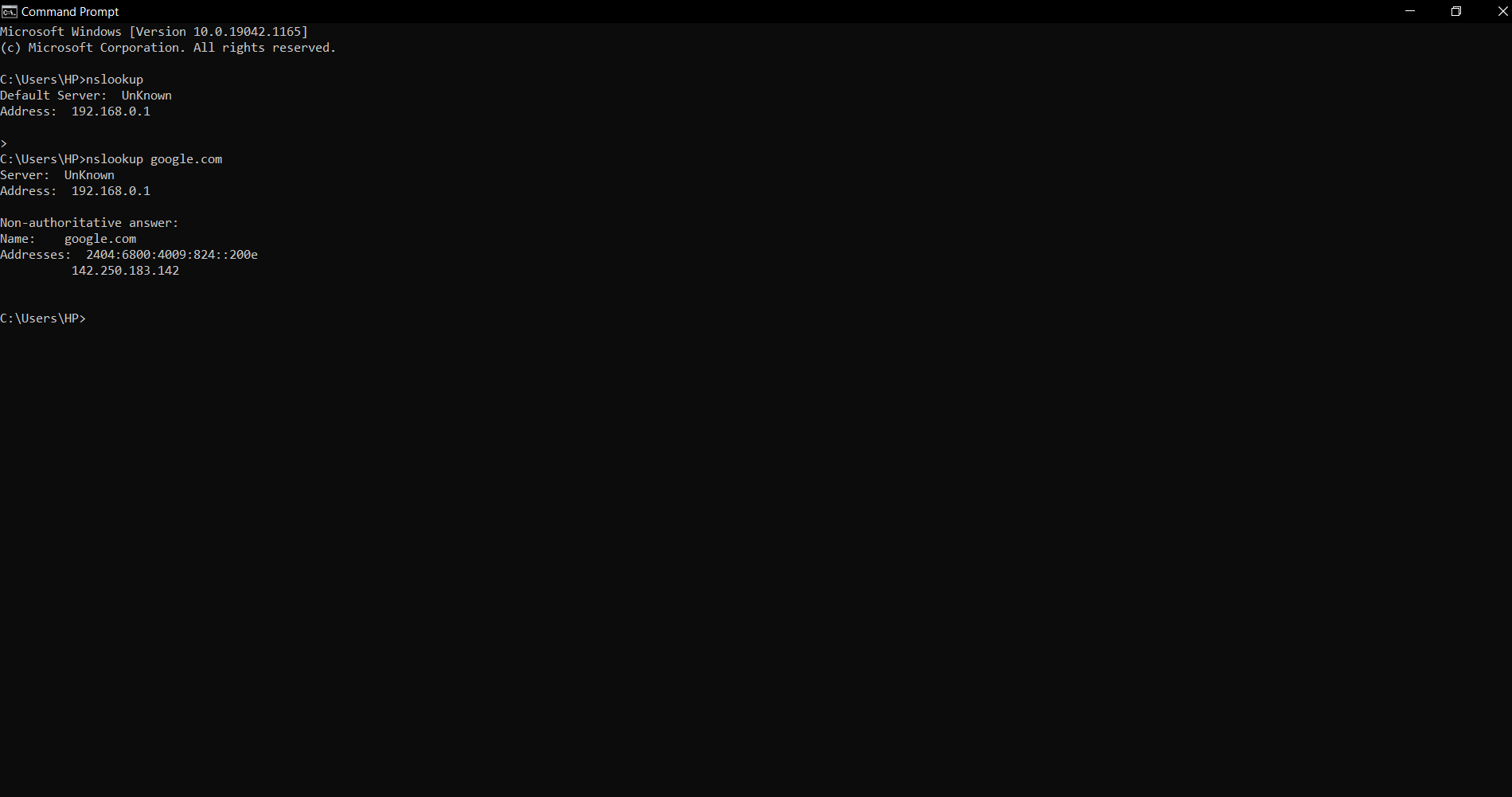
**4)Hostname**

****

**5)Traceroute**

****

**6)Nslookup**

****

**7)ARP**

****