R&S

Module-1

Network Architecture

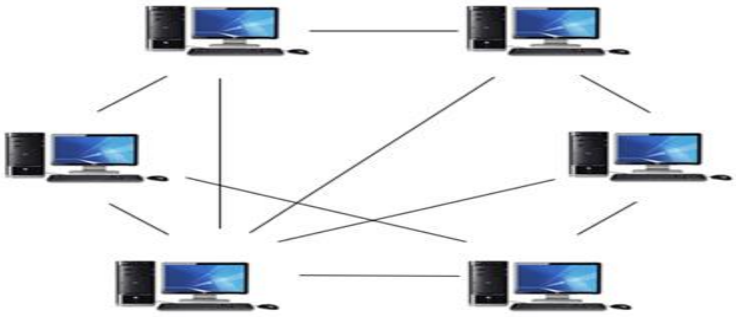
Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

The two types of network architectures are used:

- Peer-To-Peer network
- Client/Server network

Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages Of Peer-To-Peer Network:

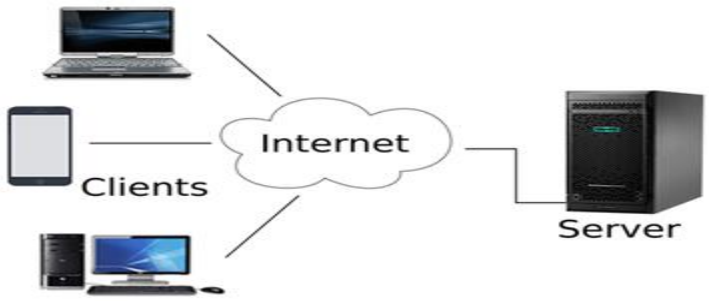
- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages Of Client/Server network:

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Enterprise Networking

Enterprise networking refers to the physical, virtual and logical design of a network, and how the various software, hardware and protocols work together to transmit data. When it comes to enterprise networking, every organization has different needs, and in the era of digital transformation, modern enterprises are relying more on software-driven solutions to power intelligent network architecture, automation and design.

What is an Enterprise Network Made Of?

Routers

Routers are devices on the network that connect multiple networks together. They forward data from one device to another, which is sent in packets. They also connect devices on networks to the internet. It is possible to add other features to routers to increase ease of use or security.

Switches

Switches can be thought of as network controllers. They connect devices such as computers, printers, and servers on the network, and enable data to be transferred within it. Switches make it possible for devices on the network to talk to each other and other networks, resulting in a single network of shared resources.

Wireless Access Points

Wireless access points perform the precise function they're named for: enabling wireless connections. WAPs work like a router, sending data from one device to another.

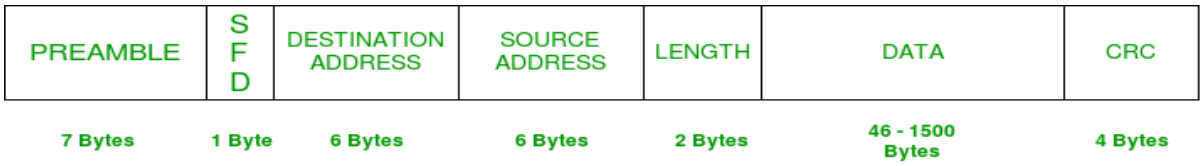
Why Is Enterprise Networking Important?

In our hyper-connected world, a stable, reliable network is regarded as a given, and the consequences of an unreliable network are only getting more severe. In fact, according to Gartner, the approximate cost of network downtime is $5,600 per minute, and can be much higher for technology-dependent organizations. As enterprise network architectures grow more complex, many organizations are finding it difficult to keep up. Thankfully, a number of networking solutions are available to simplify the process, like unified wired/wireless infrastructures, automated campus and agile data center networking solutions.

Ethernet Frame Format

Basic frame format which is required for all MAC implementation is defined in **IEEE 802.3 standard**. Though several optional formats are being used to extend the protocol's basic capability. Ethernet frame starts with Preamble and SFD, both works at the physical layer. Ethernet header contains both Source and Destination MAC address, after which the payload of the frame is present. The last field is CRC which is used to detect the error. Now, let's study each field of basic frame format.

Ethernet (IEEE 802.3) Frame Format –



IEEE 802.3 ETHERNET Frame Format

- **PREAMBLE –** Ethernet frame starts with 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization. Initially, PRE (Preamble) was introduced to allow for the loss of a few bits due to signal delays. But today's high-speed Ethernet don't need Preamble to protect the frame bits. PRE (Preamble) indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.
- **Start of frame delimiter (SFD) –** This is a 1-Byte field which is always set to 10101011. SFD indicates that upcoming bits are starting of the frame, which is the destination address. Sometimes SFD is considered the part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.
- **Destination Address –** This is 6-Byte field which contains the MAC address of machine for which data is destined.
- **Source Address –** This is a 6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.
- **Length –** Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 Bytes because of some own limitations of Ethernet.
- **Data –** This is the place where actual data is inserted, also known as **Payload**. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.

- **Cyclic Redundancy Check (CRC) –** CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

Note – Size of frame of Ethernet IEEE 802.3 varies 64 bytes to 1518 bytes including data length (46 to 1500 bytes).

IP Address

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.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

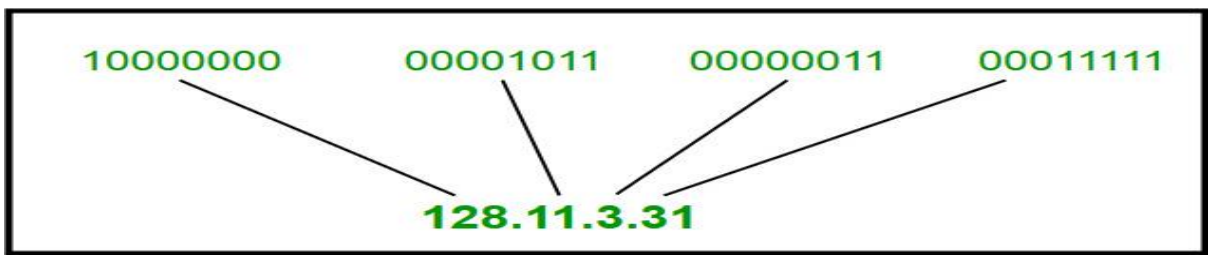
What is an IP Address?

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

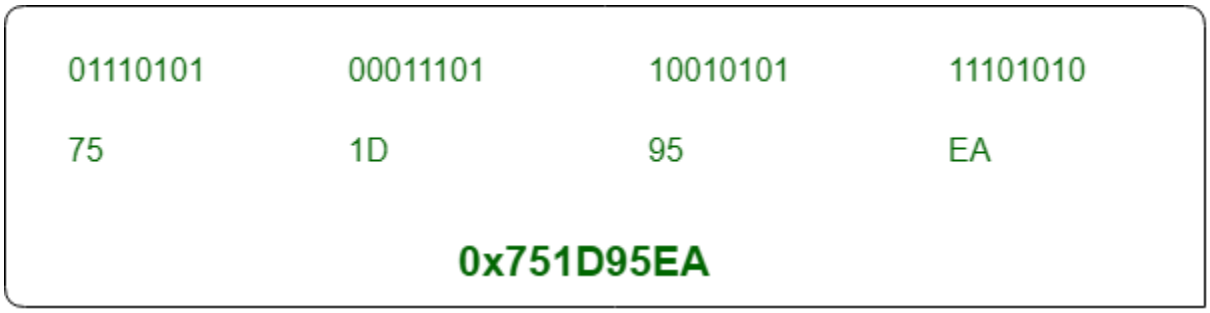
IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit organization that was established in the United States in 1998 to help maintain the security of the internet and allow it to be usable by all. Each time anyone registers a domain on the internet, they go through a domain name registrar, who pays a small fee to ICANN to register the domain.

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32}. Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation:



Hexadecimal Notation:



Some points to be noted about dotted decimal notation:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).

Classful Addressing

The 32 bit IP address is divided into five sub-classes. These are:

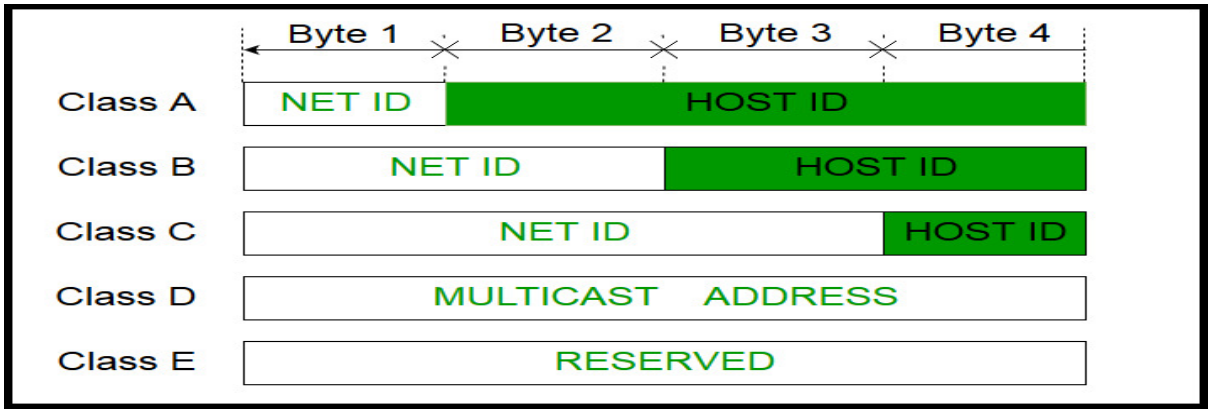
- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.

IPv4 address is divided into two parts:

- **Network ID**
- **Host ID**

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

ICMP Protocol

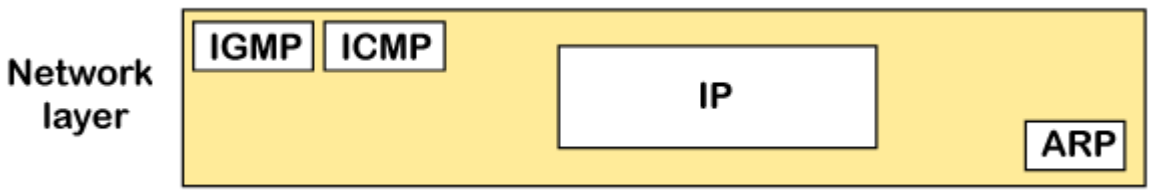
The ICMP stands for Internet Control Message Protocol. It is a network layer protocol. It is used for error handling in the network layer, and it is primarily used on network devices such as routers. As different types of errors can exist in the network layer, so ICMP can be used to report these errors and to debug those errors.

For example, some sender wants to send the message to some destination, but the router couldn't send the message to the destination. In this case, the router sends the message to the sender that I could not send the message to that destination.

The IP protocol does not have any error-reporting or error-correcting mechanism, so it uses a message to convey the information. For example, if someone sends the message to the destination, the message is somehow stolen between the sender and the destination. If no one reports the error, then the sender might think that the message has reached the destination. If someone in-between reports the error, then the sender will resend the message very quickly.

Position of ICMP in the network layer

The ICMP resides in the IP layer, as shown in the below diagram.



Messages

The ICMP messages are usually divided into two categories:

ICMP messages

Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

- **Error-reporting messages**

The error-reporting message means that the router encounters a problem when it processes an IP packet then it reports a message.

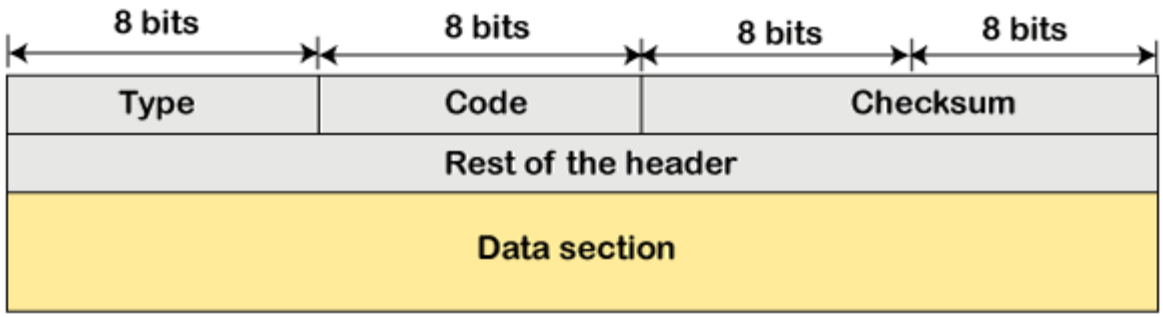
- **Query messages**

The query messages are those messages that help the host to get the specific information of another host. For example, suppose there are a client and a server, and the client wants to know whether the server is live or not, then it sends the ICMP message to the server.

ICMP Message Format

The message format has two things; one is a category that tells us which type of message it is. If the message is of error type, the error message contains the type and the code. The type defines the type of message while the code defines the subtype of the message.

The ICMP message contains the following fields:

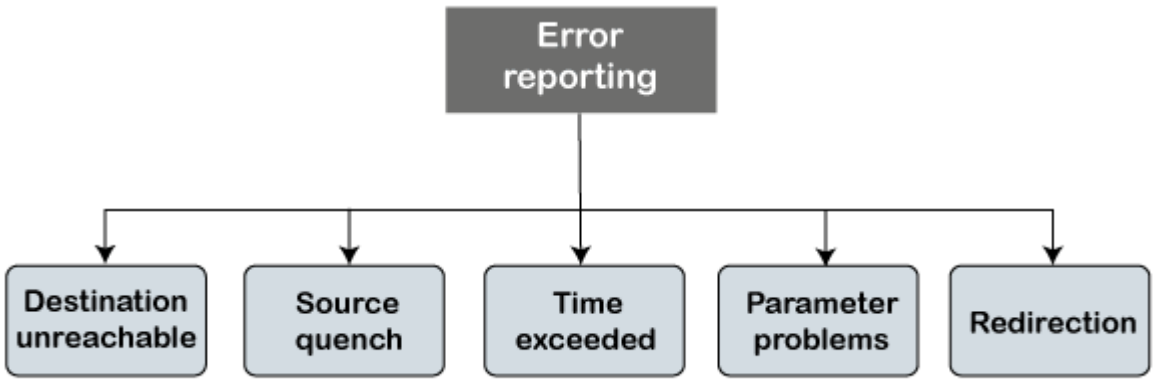


- **Type:** It is an 8-bit field. It defines the ICMP message type. The values range from 0 to 127 are defined for ICMPv6, and the values from 128 to 255 are the informational messages.
- **Code:** It is an 8-bit field that defines the subtype of the ICMP message
- **Checksum:** It is a 16-bit field to detect whether the error exists in the message or not.

Note: The ICMP protocol always reports the error messages to the original source. For example, when the sender sends the message, if any error occurs in the message then the router reports to the sender rather than the receiver as the sender is sending the message.

Types of Error Reporting messages

The error reporting messages are broadly classified into the following categories:



ICMP Query Messages

The ICMP Query message is used for error handling or debugging the internet. This message is commonly used to ping a message.

Debugging tools

There are several tools used for debugging. In this topic, we will learn two tools that use ICMP for debugging. The two tools are **ping** and **traceroute**. We have learned about ping in echo-request and echo-reply messages that check whether the host or a router is alive or running.

Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.

Types of ARP

Proxy ARP - Proxy ARP is a method through which a Layer 3 devices may respond to ARP requests for a target that is in a different network from the sender. The Proxy ARP configured router responds to the ARP and map the MAC address of the router with the target IP address and fool the sender that it is reached at its destination.

At the backend, the proxy router sends its packets to the appropriate destination because the packets contain the necessary information.

Example - If Host A wants to transmit data to Host B, which is on the different network, then Host A sends an ARP request message to receive a MAC address for Host B. The router

responds to Host A with its own MAC address pretend itself as a destination. When the data is transmitted to the destination by Host A, it will send to the gateway so that it sends to Host B. This is known as proxy ARP.

Gratuitous ARP - Gratuitous ARP is an ARP request of the host that helps to identify the duplicate IP address. It is a broadcast request for the IP address of the router. If an ARP request is sent by a switch or router to get its IP address and no ARP responses are received, so all other nodes cannot use the IP address allocated to that switch or router. Yet if a router or switch sends an ARP request for its IP address and receives an ARP response, another node uses the IP address allocated to the switch or router.

There are some primary use cases of gratuitous ARP that are given below:

- The gratuitous ARP is used to update the ARP table of other devices.
- It also checks whether the host is using the original IP address or a duplicate one.

Reverse ARP (RARP) - It is a networking protocol used by the client system in a local area network (LAN) to request its IPv4 address from the ARP gateway router table. A table is created by the network administrator in the gateway-router that is used to find out the MAC address to the corresponding IP address.

When a new system is set up or any machine that has no memory to store the IP address, then the user has to find the IP address of the device. The device sends a RARP broadcast packet, including its own MAC address in the address field of both the sender and the receiver hardware. A host installed inside of the local network called the RARP-server is prepared to respond to such type of broadcast packet. The RARP server is then trying to locate a mapping table entry in the IP to MAC address. If any entry matches the item in the table, then the RARP server sends the response packet along with the IP address to the requesting computer.

Inverse ARP (InARP) - Inverse ARP is inverse of the ARP, and it is used to find the IP addresses of the nodes from the data link layer addresses. These are mainly used for the frame relays, and ATM networks, where Layer 2 virtual circuit addressing are often acquired from Layer 2 signaling. When using these virtual circuits, the relevant Layer 3 addresses are available.

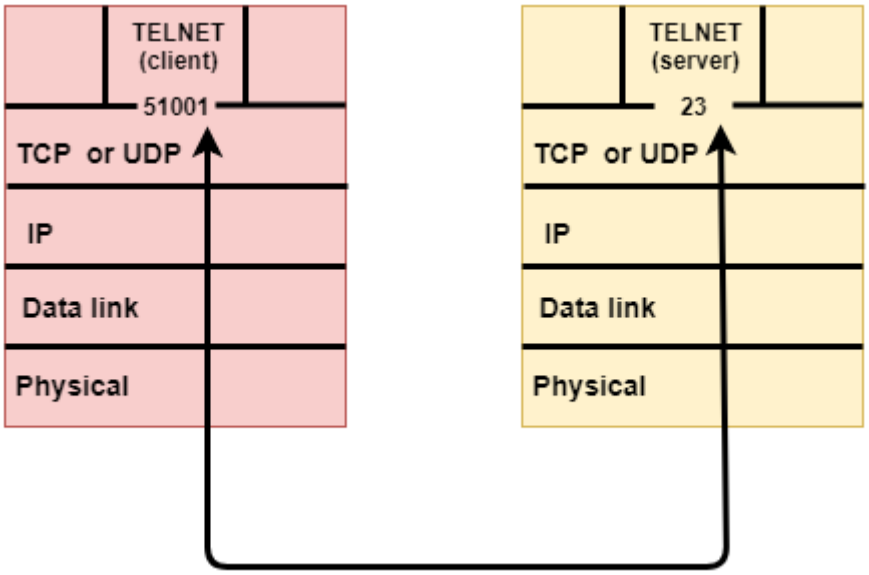
ARP conversions Layer 3 addresses to Layer 2 addresses. However, its opposite address can be defined by InARP. The InARP has a similar packet format as ARP, but operational codes are different.

Transport Layer protocols

- The transport layer is represented by two protocols: TCP and UDP.
- The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message

to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.

- An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
- Each port is defined by a positive integer address, and it is of 16 bits.

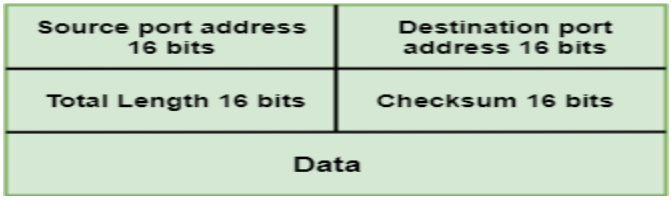


UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:



Where,

- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

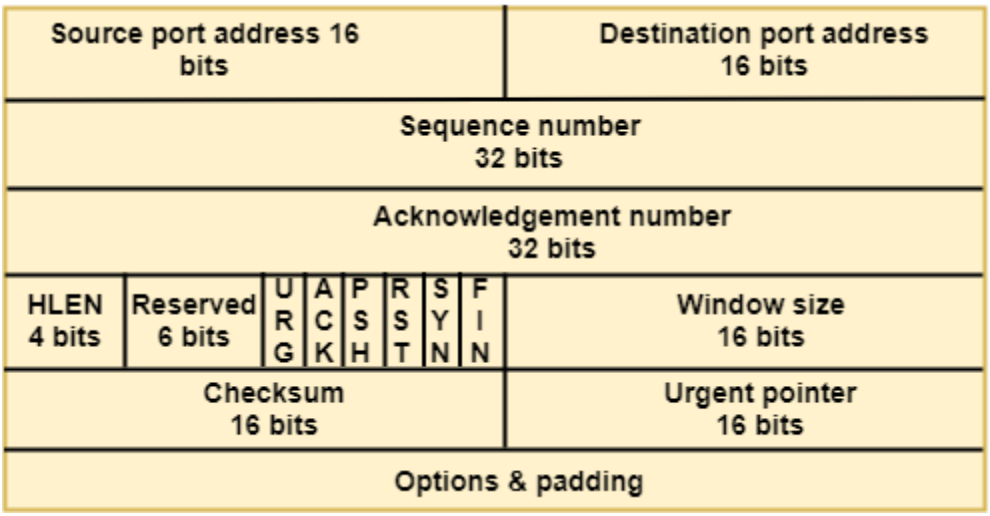
TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features Of TCP protocol

- **Stream data transfer:**
- **Reliability:**
- **Flow Control:**
- **Multiplexing:**
- **Logical Connections:**
- **Full Duplex:**

TCP Segment Format



Where,

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

- **URG:** The URG field indicates that the data in a segment is urgent.
- **ACK:** When ACK field is set, then it validates the acknowledgement number.
- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.

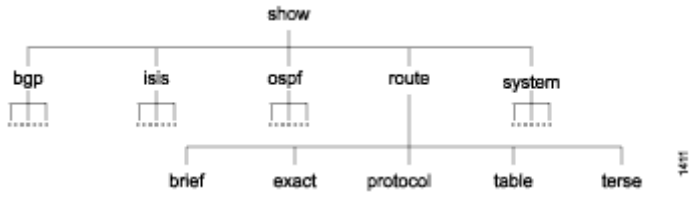
- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement.
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.
    - **Window Size:** The window is a 16-bit field that defines the size of the window.
    - **Checksum:** The checksum is a 16-bit field used in error detection.
    - **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
    - **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

Navigating the CLI

CLI Command Hierarchy

CLI commands are organized in a hierarchy. Commands that perform a similar function are grouped together under the same level of the hierarchy. For example, all commands that display information about the system and the system software are grouped under the show system command, and all commands that display information about the routing table are grouped under the show route command. Figure 1 illustrates a portion of the show command hierarchy.

Figure 1: CLI Command Hierarchy



To execute a command, you enter the full command name, starting at the top level of the hierarchy. For example, to display a brief view of your Ethernet switching options for your interfaces, use the command show ethernet-switching-options interfaces.

CLI Configuration Statements

The configuration statement hierarchy has two types of statements: *container statements*, which are statements that contain other statements, and *leaf statements*, which do not

contain other statements. All of the container and leaf statements together form the *configuration hierarchy*.

The protocols statement is a top-level statement at the trunk of the configuration tree. The ospf, area, and interface statements are all subordinate container statements of a higher statement (they are branches of the hierarchy tree), and the hello-interval statement is a leaf on the tree.

Moving Among Hierarchy Levels

You can use the CLI commands to navigate the levels of the configuration statement hierarchy:

- edit— Moves to an existing configuration statement hierarchy or creates a hierarchy and moves to that level.
- exit—Moves up the hierarchy to the previous level where you were working. This command is, in effect, the opposite of the edit command. Alternatively, you can use the quit command. The exit and quit commands are interchangeable.
- up—Moves up the hierarchy one level at a time.
- top—Moves directly to the top level of the hierarchy.

File System Management

Files are used to provide a uniform view of data storage by the operating system. All the files are mapped onto physical devices that are usually non volatile so data is safe in the case of system failure.

File Attributes

The attributes of a file may vary a little on different operating systems. However, the common file attributes are −

Name

This denotes the symbolic name of the file. The file name is the only attribute that is readable by humans easily.

Identifier

This denotes the file name for the system. It is usually a number and uniquely identifies a file in the file system.

Type

If there are different types of files in the system, then the type attribute denotes the type of file.

Location

This points to the device that a particular file is stored on and also the location of the file on the device.

Size

This attribute defines the size of the file in bytes,words or blocks. It may also specify the maximum allowed file size.

Protection

The protection attribute contains protection information for the file such as who can read or write on the file.

Operations on Files

The operations that can performed on a file are −

Creating a file

To create a file, there should be space in the file system. Then the entry for the new file must be made in the directory. This entry should contain information about the file such as its name, its location etc.

Reading a file

To read from a file, the system call should specify the name and location of the file. There should be a read pointer at the location where the read should take place. After the read process is done, the read pointer should be updated.

Writing a file

To write into a file, the system call should specify the name of the file and the contents that need to be written. There should be a write pointer at the location where the write should take place. After the write process is done, the write pointer should be updated.

Deleting a file

The file should be found in the directory to delete it. After that all the file space is deleted so it can be reused by other files.

Repositioning in a file

This is also known as file seek. To reposition a file, the current file value is set to the appropriate entry. This does not require any actual I/O operations.

Truncating a file

This deletes the data from the file without destroying all its attributes. Only the file length is reset to zero and the file contents are erased. The rest of the attributes remain the same.

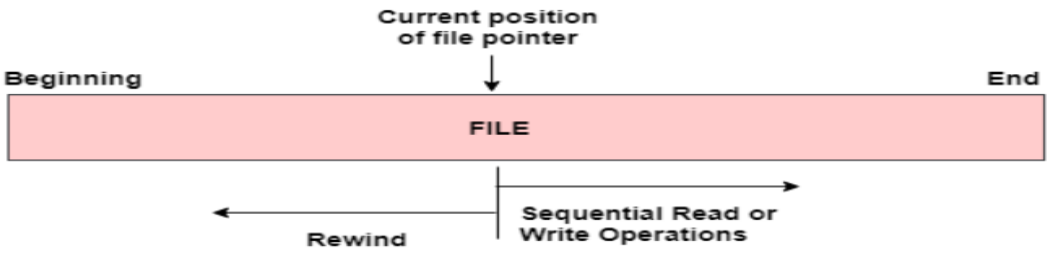
File Access Methods

The information in a file can be accessed in various ways. The most common among them are using sequential access or direct access. More details about these are −

Sequential Access

The information in a file is processed in order using sequential access. The files records are accessed on after another. Most of the file systems such as editors, compilers etc. use sequential access. It is based on the tape model of a file and so can be used with sequential access devices as well as random access devices.

A diagram to illustrate sequential access is as follows −



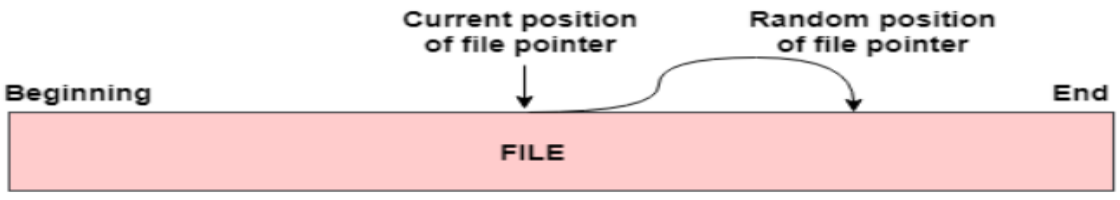
SEQUENTIAL ACCESS IN FILES

As seen in the image, the read and write operations in the file can only be done in a sequential manner. However, the file can be reset to the beginning or rewinded as required.

Direct Access

In direct access or relative access files can be accessed in random for read and write operations. The direct access model is based on the disk model of a file, since it allows random accesses. In this method, the file is divided into numbered blocks. Any of these arbitrary blocks can be read or written. For example, we may read block 8, then write into block 10 and then read block 15. Direct access system is quite useful and mostly databases are of this type.

A diagram to illustrate direct access is as follows −



DIRECT ACCESS IN FILES

As seen in the above image, the file pointer can be positioned randomly as required for read and write operations. This can be done without any particular order in positioning.

Introduction to VRP(Versatile Routing Platform)

VRP is a general network operating system of which Huawei Technologies Co., Ltd. has completely independent intellectual property rights. It can run on a full range of communication products from low-end to high-end, such as routers and switches. It is similar to Microsoft's Windows operating system and Apple's iOS operating system. At present, Huawei devices are almost ubiquitous in network devices around the world, so it is especially important for network communication technicians to learn about the knowledge of VRP.

VRP can run on a variety of hardware platforms, including routers, LAN switches, ATM switches, dial-up access servers, IP telephony gateways, carrier-grade integrated service access platforms, intelligent service selection gateways and dedicated hardware firewalls. VRP has a consistent network interface, user interface and management interface, providing users with flexible and rich application solutions, as shown in Fig. 3.1.

VRP application solutions

With TCP/IP protocol stack as the core, VRP implements various data link layer, network layer and application layer protocols, integrates data communication functions such as routing and switching technology, QoS technology, security technology and IP voice technology in the operating system, and provides excellent data forwarding function for network devices based on IP forwarding engine technology.