Networking

Computer Network Architecture

Computer Network Architecture

This document contains a detailed explanation of how every network layer works, along with several important network protocols that govern digital communication today. Before we jump into the layered functions, let's recall what a computer network, and network models are.

What is a computer network?

A network of computers is a group of computers, that can communicate with each other and share resources and data. The concept of networking amongst computers relies on well set rules and modular design. The rules are called network protocols, and the design patterns are known as network models.

In this document, we focus on the Open System Interconnection (OSI) model, as it serves as a base model for all other modern models like TCP/IP. The process of a packet, getting from one computer to another, is relatively the same across most models, with nuanced differences in their parameters, such as addressing modes.

Getting Data on the Wire

This section will give a detailed overview on how a packet gets onto the wire and handles complexities like different networks following different protocols. The process of getting data on to the wire is complex. To understand how data gets onto the wire it's essential to understand the working of your ***Network Interface Card*** or NIC.

The NIC

The network must provide a mechanism to uniquely identify each system on a network, something analogous to a telephone number, so data is delivered to the correct system. At some level, this is provided by the MAC address or media access control address. Inside every NIC, the MAC address is burned on to the ROM chip.

All MAC addresses are unique. Any company that manufactures NICs must consult with the Institute of Electrical and Electronics Engineering (IEEE) and get a block of MAC address. Let's suppose the MAC address is **AA-06-84-6C-76-9A.**

Here the first three segments denote the manufactures identity often referred to as the Organisationally Unique Identifier (OUI). Once the IEEE issues the six-hex-digit to the manufacturer, no other manufacturer will use them. The last six digits, in this example, 6C769A, are the manufacturer's unique serial number for that particular NIC. This portion of the MAC is called the device ID.

If you want to check the MAC address of your system, type ipconfig/all in a terminal window.

So how are these unique MAC addresses used? Computer data is binary, which means it is made of a stream of ones and zeroes. NICs send and receive this binary data as pulses of electricity, light, or radio-waves. Now that you know that data moves along the wire as electrical signals that symbolize 1s and 0s, how does the network get the right data to the right system? All networks transmit data by breaking whatever is moving across the Physical Layer, the intro discrete chunks called frames. A frame is a container for a segment of data moving across a network. The NIC creates, sends, receives, and reads these frames. Here, the MAC address becomes essential.

Even though a frame, practically speaking, is a string of ones and zeroes, we often represent frames as a series of rectangles.

Note, that the frame begins with the MAC address of the receiver, followed by the MAC of the sender. This step is followed by the actual data of the frame. The FCS is used to determine whether the frame is intact when it is received. It uses math called *cyclic redundancy check*.

The NIC is ignorant of the data that is being transmitted by the frame. It could be print material, a photograph, or a simple web page. NICs aren't concerned with content. The NIC takes whatever data is to be passed via its device driver and addresses it for the correct system. This is known as the utility of frames. A single frame may hold 1500 bytes of data. When the data exceeds this limit, it is further broken down into frame sized chunks before transmission.

Using MAC addresses is a great way to move data around, but this process raises a few questions. How does a sending NIC know the MAC of the destination? It could be, that the NIC had earlier communicated with the destination and has the MAC address saved. If it already doesn't know the MAC, the NIC sends a broadcast onto the network and asks for it. This step forms the basis of Address Resolution Protocol discussed in the presentation of module 4.

Frame Movement – Physical and Data Link Layer

Now that you are familiar with all pieces used to send and receive frames let's study how a frame gets from one system to another.

1. First the sending system's Network Operating System (NOS), example, Windows 8, hands some data to its NIC. The NIC builds a frame to transport that data to the receiving NIC.
2. After the frame is created, the NIC adds the FCS and dumps the data into the frame.
3. Next, the NIC updates the destination MAC, and it puts down its own MAC in the sender field. It then waits until no other NIC is using the cable and send the frame through the cable to the network.
4. The frame moves down the wire into the hub. Here multiple copies of the frame are created and sent to every other system on the network.
5. Receiving NICs check the frame and try to match the MAC address. If a NIC finds that the frame is addressed to it, it processes the frame; else the NIC discards the frame.
6. When the frame reaches the correct NIC, the receiving NIC verifies the validity of the data. If the data is valid, it strips all the frame-information and sends the data to its NOS for processing.

Any device that deals with a MAC address is part of the OSI data link layer.

Most networking books that describe the OSI model put the NIC into the data link layer. It is at the MAC sublayer, that data gets encapsulated into a frame, destination and source MAC addresses are added to the frame and error checking commences. The confusing aspect for most students is that while placing the NIC solely in the data link layer. Network cards technically work at both layer 1 and 2, but if somebody were to pinch you and ask you to choose one, choose the second layer.

This covers how data moves in the first two layers. Now let's look at the working of layers 3 to 7.

One problem with simple computer networks is that there is a broadcast message involved to get the MAC address. It works well for small networks, but what about when the network is as huge as the internet? Imagine millions of computers broadcasting at the same time for MAC addresses. It would be an utterly chaotic situation. Another point to note would be that data flows over the internet using a multitude of technologies such as SONET, ATM, and many more. These technologies don't know what to do with Ethernet-based MAC addresses. Hence, when networks get large, you can't simply depend on the MAC address solely, anymore.

Large networks need logical addressing that ignores hardware and lets you break a network into a host of smaller subdivisions. This requirement is essentially a subnet. To move past the MAC address and start using a logical addressing scheme requires the usage of special software called network protocols. Network protocols exist in every operating system, and this is where the merits of TCP/IP as a protocol shine. Let's understand more.

Network Layer

At the network layer, packets get created and addressed so they can go from one network to another. The *Internet Protocol* is the primary logical addressing protocol for TCP/IP. IP ensures that a piece of data gets to its destination. It does so by giving each device on a network a unique identifier called an IP address, which is a logical address.

IP addresses must be unique, or data will not get to the correct place. Two devices having the same IP address would wreak havoc over the network. Logical addressing is empowered by the router, that connects each of these subnets. Routers use the IP address instead of the MAC address for forwarding packets to their correct destination.

In a TCP/IP based network, a system therefore has two identifiers: The MAC address (physical) and the IP address (logical).

For a TCP/IP network to transmit a piece of data correctly, it must be wrapped in two containers – A frame of some sort, that enables the data to move from one device to another. Inside the frame, is an IP specific container, that helps the router transmit the data; and the data container itself, which is the packet. Each IP packet is handed to the NIC, which then encapsulates the IP packet in a regular frame. When data is transmitted from a computer to another using a TCP/IP network, the data can go through many routers before it reaches its destination. Each router strips off the incoming frame to determine where it should send the packet according to the IP address in the packet. It then creates a new frame and sends the packet within a new frame on its way. The new frame type will be appropriate for the technology that is being used at the next router. This process is repeated until the packet reaches its destination.

Once the packet has reached the destination, the receiving NIC strips the packet off the frame and passes on the data to the network software.

Transport Layer

Most data must be fragmented into frame/packet sized parts before they are sent off onto the wire. When a serving computer receives a request for some data, it must be able to chop the requested data into chunks that will fit into a packet, and eventually into the NIC's frame. It must also be able to organize the data for

the receiver. The receiving system must be able to recognize a series of packets as one data transmission. Reassemble the packets correctly based on information included in the packets by the serving system.

The transport layer handles this part. It is analogous to how Amazon would send you a large shipping in parts. To make sure you get all the parts correctly, Amazon uses a numbering system and labels each box with a specific number. A computer sending data on a network does the same thing using sequencing numbers. This process helps the receiving system realize the number of packets for a certain stream and how to put them back together in correct order.

Session Layer

Now that it is clear, that a system uses software to put data into chunks and then reassemble these chunks, let's see what happens next. In a network, a system may be communicating to many other systems at any given point in time. For example, if a computer wants to send a print job to a printer on the network, it must ensure it is free. The session layer handles this. The session layer of the OSI model handles all the session for any particular system. It is responsible for initiating the session for communication, accept any incoming session, and terminate any existing session. The session layer also keeps a log of naming conventions, for example, calling your computer DEVICE01, or any other convention that makes more sense than using IP and MAC address.

Presentation Layer

The presentation layer is where all formats get standardized. A stronghold of a network lies in the fact that it works with almost any operating system. Modern-day networks connect to separate operating system easily, even though these two operating systems use different types of formats for different kinds of data. It was a huge problem back in the day before applications like Microsoft Word could import/export thousands of other word processor formats.

This obstacle encourages people to create a standardized format that anyone, with the right application, could read from any device. Special file formats like Portable Document Format (PDF), provide formats that any system can read, regardless of the operating system that they are running.

The presentation layer handles this conversion of data into formats that are readable by the system in concern.

Application Layer

The most distinct part of any network model is the applications that use it. If you want to copy/move a file residing on another system in your network, you need an application like Network in Windows 7 that enables you to access files on a remote system. If you want to surf the web, you need a web browser, like Chrome or Mozilla. A user who knows nothing about the other parts of a network may still know how to open an email application to retrieve their emails.

The application layer is the last layer of the OSI model, and in the TCP/IP model, it combines the session-presentation-application layers. The application layer doesn't refer to the applications themselves. It refers to the code, that is built into all operating systems that enable network-based applications. Every operating system has Application Programing Interfaces (APIs) that developers can use to make their programs network enabled. An API, in general, provides a standard way for programmers to enhance or extend an application's capabilities.

This concludes the functions of the seven layers of the OSI model and how a packet travels through them.

Network Protocols

What is Network Protocol?

The word protocol means a set of rules. Network protocols are a set of rules that govern how they function. Today, there are numerous network protocols that work in synergy to output the network that we are so affluent with. It is nigh impossible to list out all these protocols. What follows is a brief discussion on the working on the more prominent protocols, that have paved the way to modern computer networks.

Ethernet

Ethernet is the most widely used LAN technology today The scope of Ethernet's operability covers both the data link layer and the physical layer. It is a set of networking technologies that are defined in the IEEE 802.2 and 802.3 standards. Ethernet can support a data bandwidth in the following range:

- 10 Mb/s
- 100 Mb/s
- 1000 Mb/s (1 Gb/s)
- 10,000 Mb/s (10 Gb/s)
- 40,000 Mb/s (40 Gb/s)
- 100,000 Mb/s (100 Gb/s)

Ethernet standards define the protocols of layer 2 and the technologies of layer 1. Ethernet relies on the two separate sublayers of the data link layer to function, the Logical Link Control (LLC) and the MAC sublayers.

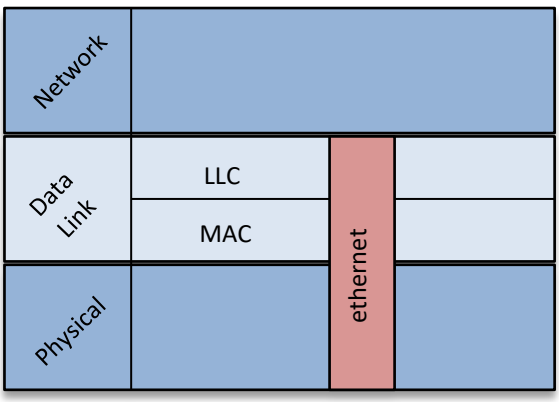
Logical Link Control Sublayer

The Ethernet LLC sublayer orchestrates the communication between the networking software and the device hardware. The LLC sublayer takes the data, typically an IPv4 packet and adds control information to help transmit the packet to the destination node. The LLC is used to communicate with the upper layers of the application and transit the packet to the lower layers for delivery.

LLC is a software implementation completely independent from the hardware. In a computer, the LLC can be considered the driver software for the NIC. The NIC driver is a program that interacts directly with the hardware on the NIC to pass the data between the MAC sublayer and the physical media.

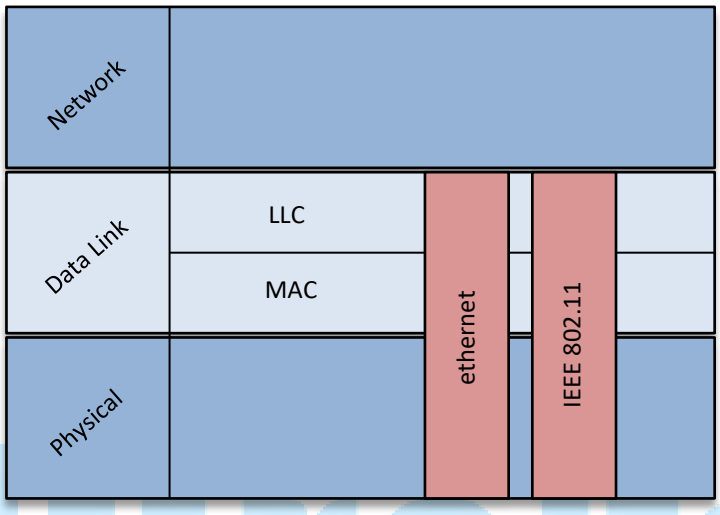
MAC Sublayer

MAC constitutes the lower sublayer of the data link layer. MAC is implemented by hardware, typically in the computer NIC. The specifics are set down in the IEEE 802.3 standards.



IEEE 802.11 (Wi-Fi)

Wireless Fidelity (Wi-Fi) is a technology for orchestrating wireless local area networking with devices based on IEEE 802.11 standards. Wi-Fi enabled systems can connect to the internet via a WLAN network and a wireless access point commonly known as AP. The access point is responsible for receiving and transmitting data from/to users. IEEE has defined precise specifications for wireless LAN, called **IEEE 802.11**, which covers physical and data link layers.

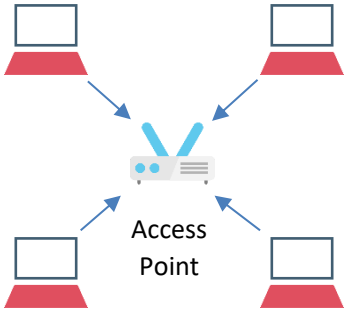


Access Point is a wireless LAN base station that can connect one or many wireless devices simultaneously to the internet.

The architecture of this standard has two kinds of services:
1. Basic Service Set (BSS)
2. Extended Service Set (ESS)

BSS is the fundamental pillar of WLAN. It constitutes of a *wireless mobile station* and *an optional central station* called *Access Point*. Stations can form a network with or without an AP and can form a Basic Service Set. A BSS with an AP is called an **infrastructure network.**

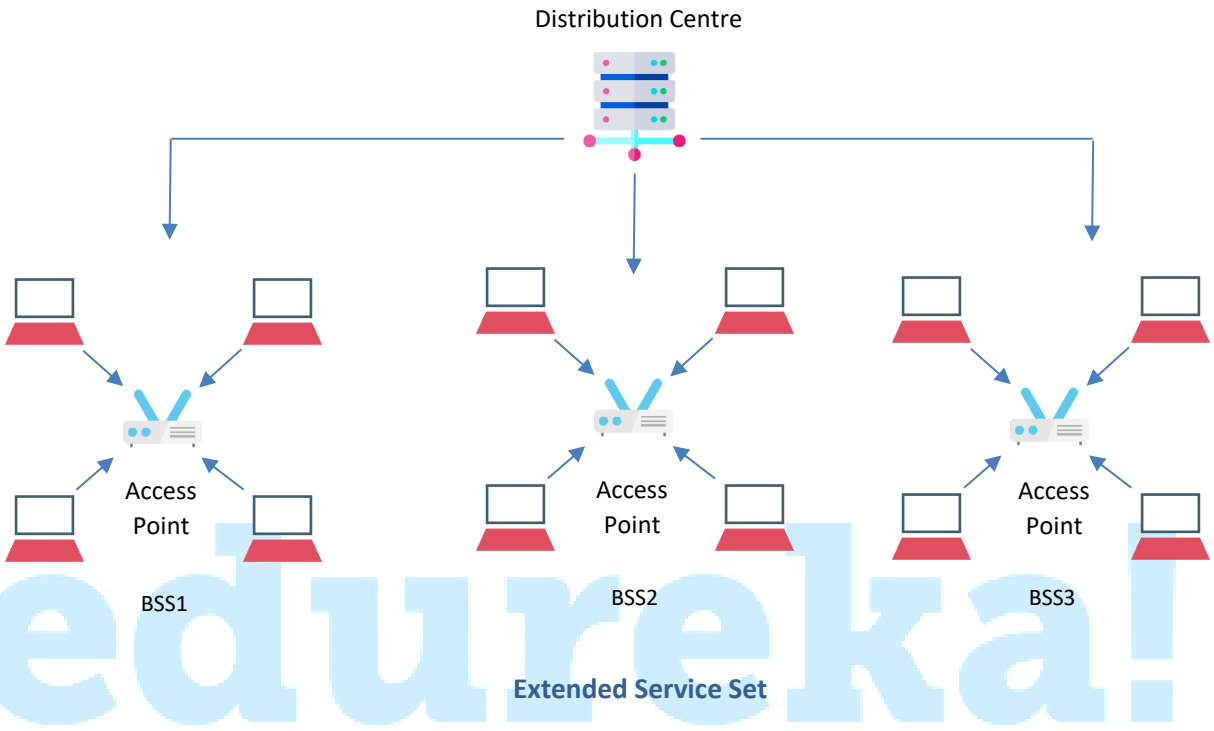
A BSS without an AP cannot send data to other BSSs. It defines a standalone network and is known as an **ad hoc network** or **Independent BSS (IBSS).**



Basic Service Set

An ***Extended Service Set*** is consisting of 2 or more BSSs with APs. BSSs are connected to the *distribution system* via their access points. The distribution system can be any IEEE LAN such as Ethernet.

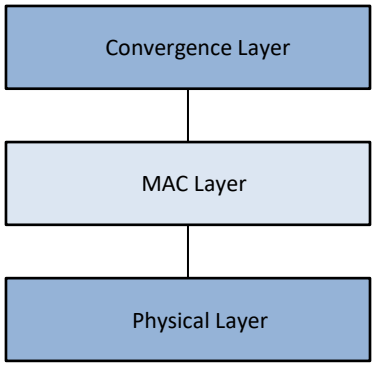
ESS has two kinds of stations:
1. Mobile – stations inside the BSS
2. Stationary – AP stations that are part of wired LAN.



Here the laptops connected to the access point are mobile stations, while the access points themselves are stationary stations. **IEEE 802.16 (WiMAX)**

Wireless Interoperability for Microwave Access (WiMAX),a technology based on IEEE 802.16, is used to serve higher data rates with a boarder scope of coverage. It is often adopted in MAN (Metropolitan Area Network) technology since it has a range of over 50 Km. Additionally, WiMAX provides speeds reaching 70 Mbps, and it can also operate in a Non-Line-of-Sight situation.

WiMAX has found widespread use due to its robust, convenient, and cost-effective nature. Below is the general architecture of WiMAX.



The WiMAX protocol architecture has three distinct layers

Physical Layer:

- It is responsible for encoding and decoding signals.
- The physical layer also manages bit transmission and reception.
- It converts MAC layer frames into signals to be transmitted.

MAC Layer:

- It serves as an interface between the convergence layer and physical layer of the WiMAX protocol stack.
- It provides point to multipoint communication and is based on *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA)

Convergence Layer:

- This layer communicates the information from the external network.
- It accepts a higher layer protocol data unit (PDU) and converts it to lower layer PDU.
- It provides functions depending upon the service being used.

IPsec

IP security or IPsec is an Internet Engineering Task Force (IETF) standard suite of protocols. It provides data authentication, integrity and confidentiality between 2 communication points across the IP network. It also deals with the encryption, decryption and authentication of packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –

- Encryption of application layer data.
- Provides security to the router
- Authentication of data without encryption
- Protection of network data using IPsec tunneling

Components of IP Security –
IPsec has the following major components.

1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication, and anti-replay for payload. The anti-replay protection safeguards against unauthorized transmission of packets. It does not protect the data's confidentiality.

2. **Authentication Header (AH) –**
   Provides data integrity, authentication, and anti-replay but it doesn't offer encryption.

3. **Internet Key Exchange (IKE) –**
   It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. IKE provides message content protection and an open frame for implementing standard algorithms, e.g. SHA

Working of IP Security –

1. The host checks if the packet should be transmitted using IPsec or not. This packet traffic triggers the security policy for themselves. It is done when the system sending the packet applies an appropriate encryption. The host also checks if the incoming packets are correctly encrypted or not.

2. If the packet is to be transmitted using IPsec, then the first phase of information key exchange is initiated. In this, both the hosts authenticate themselves to each other so a channel can be created.

3. Through this channel, IPsec communicates how the data will be encrypted.

4. After this, phase 2 of the information key exchange begins. In this phase, the secret key is decided, and the type of cryptographic algorithm is discussed. This cryptographic algorithm will be used to protect the session.

5. The data is now exchanged through this IPsec encrypted tunnel.

6. Post communication, the session automatically times out.

SMTP

Simple Mail Transfer Protocol (SMTP) is an application layer protocol. As the name suggests, the protocol dictates how emails are transmitted over the internet.

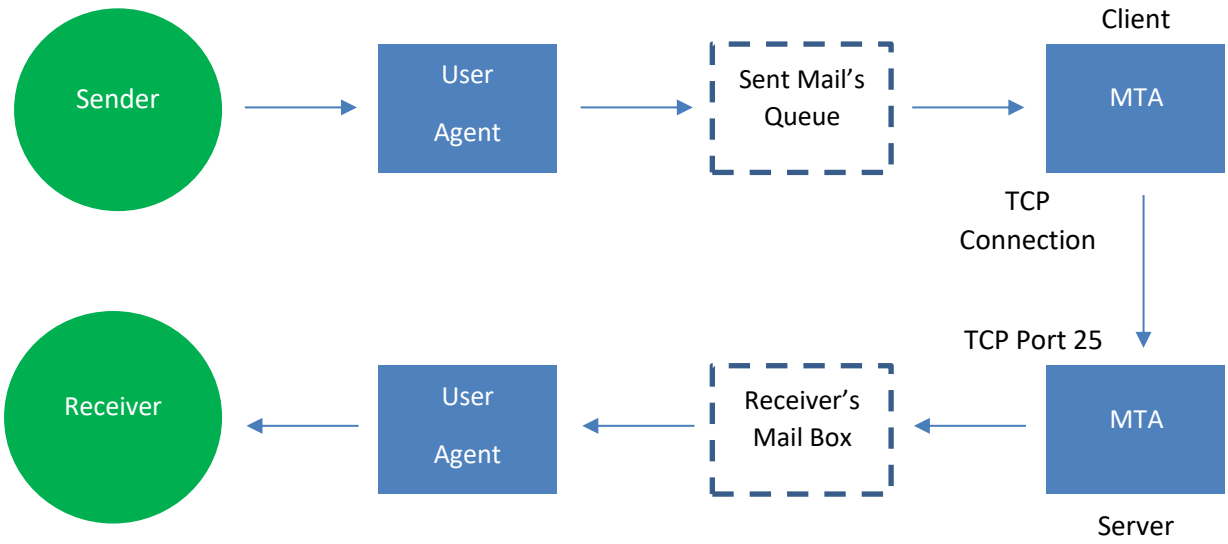
SMTP has two major models which follow their distinct methods:

1. End-to-end method
2. Store-and-forward method

The end-to-end model is used for inter-organizational communication, whereas the store-and-forward method is used for intra-organizational communication. An SMTP client who wants to send the mail will contact the destination's host SMTP directly to send the mail to the destination. The SMTP server will retain the mail on the sender system until it is successfully copied to the receiver's SMTP.

Model of SMTP system

In the SMTP model, the sending party engages with the user agent (UA), for example Microsoft Outlook, Google Chrome, etc. to exchange the mail using TCP and a Message Transfer Agent (MTA). The party sending the mail does not have to deal with the MTA. The system admin sets up the local MTA. The MTA maintains a small queue of emails so that they can be queued into repeat delivery of mail in case the receiver is not available. The mail is delivered to the mailboxes by the MTA, and the user agents can later download the information.



SENDING EMAIL:

An email is sent by a series of request and response messages between the client and a server. The message consists of a header and a body. A null line is used to show the ending of the mail header. Everything which is after the null line is considered as the body of the message, which is a sequence of ASCII characters. The message body contains the actual information that is to be sent using email.

RECEIVING EMAIL:

The user agent at the receiving side checks the mailboxes at regular intervals. If any information is received, it informs the user about the mail. The UA prepares a list of mails on the receiving side for the user to read. The user can read any mail by selecting it and then viewing its contents on the receiving UA.

S/MIME

Multipurpose Internet Mail Extension (MIME) is a standard, proposed by Bell Communications. Its purpose is to expand the limited capabilities of email. MIME is an add-on protocol which permits the transmission of non-ASCII data through SMTP. This transmission, in return, allows users to exchange different kinds of data files over email, e.g. audio, video, images, etc. MIME changes non-ASCII data, at transmitting side to NVT 7-bit data and delivers it to the client over SMTP. The message at receiver's side is transferred back to the original data format.

Features of MIME –

1. Send multiple attachments in a single email.
2. Unlimited message length.
3. Binary attachments can be fragmented if needed.

Working of MIME –
When a person wants to send an email in a non-ASCII format, the MIME protocol converts it into 7-bit NVT ASCII format. The message is transferred through an email system to the other side in 7-bit format. At the receivers' end, the MIME protocol converts the message back into non-ASCII code. The MIME header is basically inserted at the beginning of any email transfer.

Routing Information Protocol

Routing Information Protocol (RIP) is a dynamic routing protocol which implements hop count as a metric for calculating the most optimum path between a source and destination for a packet. Hop count is the number of routers a packet must go through before it finally reaches the destination. In RIP, any hop count over 15, is considered as an unreachable network. RIP works on the application layer of the OSI model on port number 520.

Features of RIP:

- Network Information is exchanged periodically
- Information is exchanged in broadcast mode
- Network updates consist of entire routing tables
- Routers always trust the routing information received from neighbor routers. This phenomenon is called routing on rumors.

RIP Versions

Rip has three versions, namely: RIPv1, RIPv2, and RIPng

RIPv1	RIPv2	RIPng
Updates are transmitted as broadcast	Updates are sent as multicast	Updates are sent as multicast
Broadcast address: 255.255.255.255	Multicast address: 224.0.0.9	Only works with IPv6. Multicast address: FF02::9
No authentication of update messages	Update messages are authenticated	
Classful routing protocol	Classless routing protocol, but supports classful	Updates sent are classless

RIP timers:

- **Update timer:** Update timer refers to the time interval in which a router exchanges network information. RIP has an update timer of 30 seconds by default.

- **Invalid timer:** This is the time when a router waits for a response from a destination before considering it unreachable. RIP has an invalid timer of 180 seconds. After 180 seconds, the destination router will be given a hop count of 16, thus deeming it unreachable.

  It is also analogous to ***Hold-down timer.***

- **Flush time:** It is the time after which the entry of the route will be flushed if it doesn't respond within the flush time. It is 60 seconds by default. This timer starts after the route has been declared invalid and after 60 seconds, i.e. time will be 180 + 60 = 240 seconds.

All these timers can be adjusted using the command-line.

```
timers basic 20 60 60 90
```