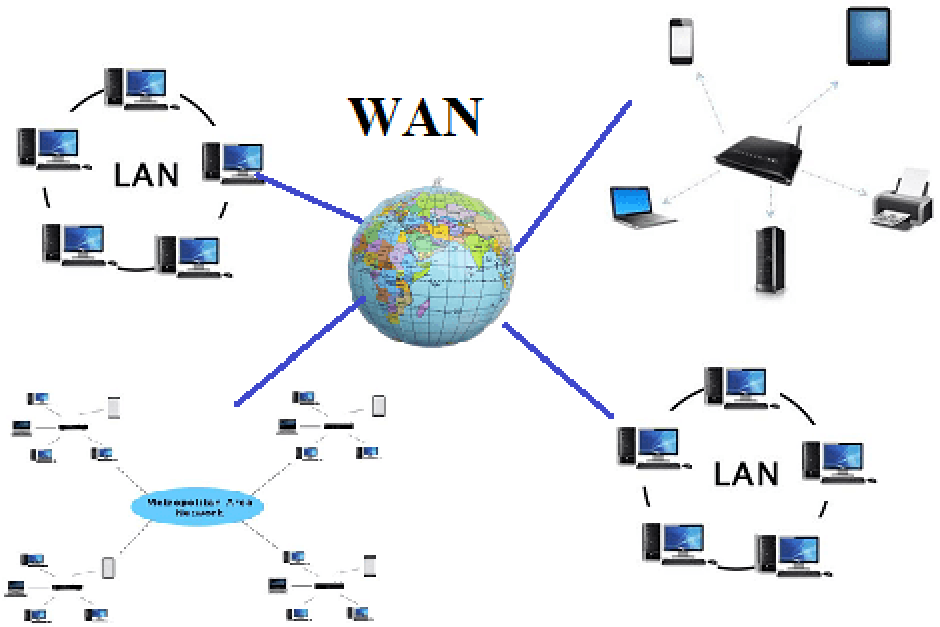
Module-4

WAN Technology

4.1 Wide Area Network (WAN)

A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.



Wide area network (WAN)

Characteristics of WAN

- It generally covers large distances(states, countries, continents).
- Communication medium used are satellite, public telephone networks which are connected by routers.

Advantages of WAN

- Covers a large geographical area so long distance business can connect on the one network.
- Shares software and resources with connecting workstations.

- Messages can be sent very quickly to anyone else on the network. These messages can have picture, sounds or data included with them (called attachments).
- Expensive things (such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.
- Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

Disadvantages of WAN

- Need a good firewall to restrict outsiders from entering and disrupting the network.
- Setting up a network can be an expensive, slow and complicated. The bigger the network the more expensive it is.
- Once set up, maintaining a network is a full-time job which requires network supervisors and technicians to be employed.
- Security is a real issue when many different people have the ability to use information from other computers. Protection against hackers and viruses adds more complexity and expense.

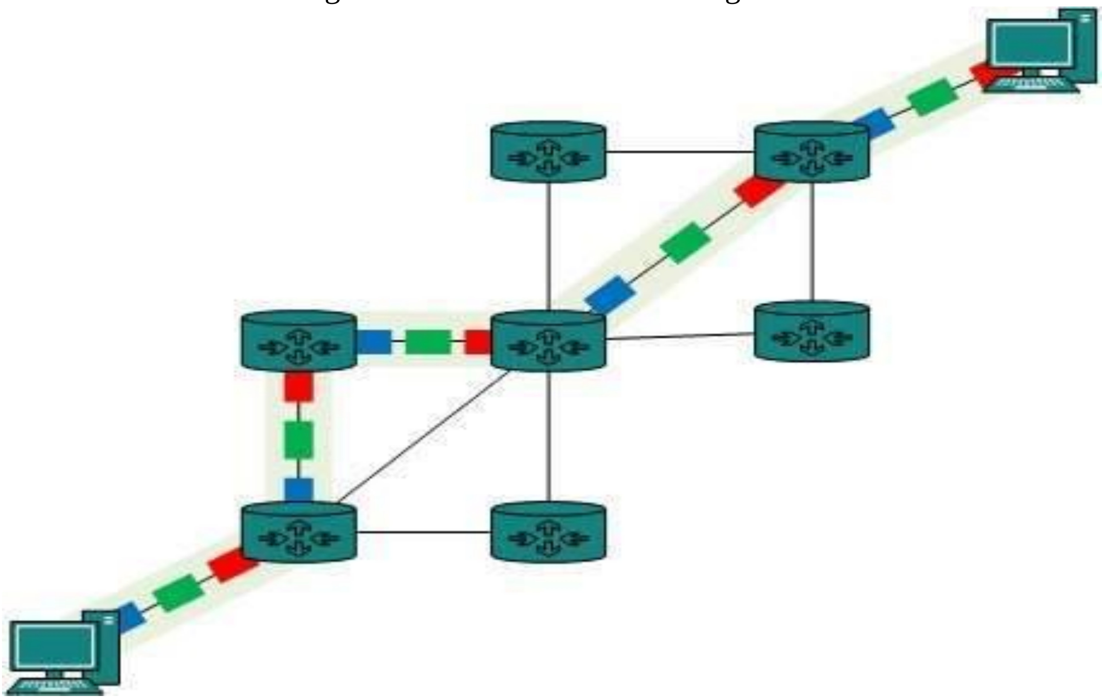
3.2 SWITCHING

The mechanism for exchange of information between different computer networks and network segments is called switching.

Types of Switching Techniques

3.1.1 Circuit Switching

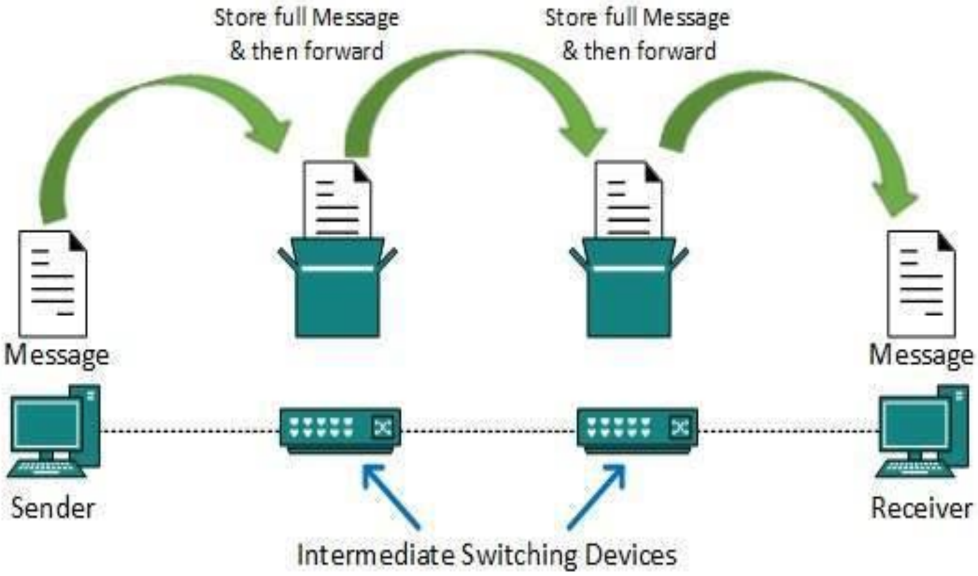
- When two nodes communicate with each other over a dedicated communication path, it is called circuit switching.
- There is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.
- Circuits can be permanent or temporary.
- Applications which use circuit switching may have to go through three phases:
    - ✓ Establish a circuit
    - ✓ Transfer the data
    - ✓ Disconnect the circuit



- Circuit switching was designed for voice applications.
- Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

3.1.2 Message Switching

- In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.
- A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.
- Message switching is advantageous as it enables efficient usage of network resources. Also, because of the store-and-forward capability of intermediary nodes, traffic can be efficiently regulated and controlled. Message delivery as one unit, rather than in pieces, is another benefit.


Store full Message & then forward
Store full Message & then forward
Message
Message
Sender
Receiver
Intermediate Switching Devices

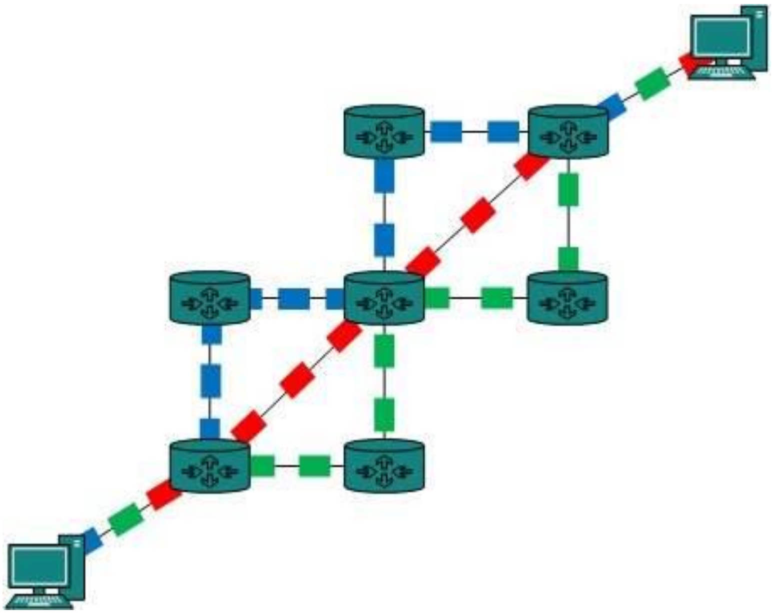
- This technique was considered substitute to circuit switching.
- As in circuit switching the whole path is blocked for two entities only.

Message switching has the following drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

3.1.3 Packet Switching

- Drawbacks of message switching gave birth to an idea of packet switching.
- The entire message is broken down into smaller chunks called packets.
- The switching information is added in the header of each packet and transmitted independently.
- It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.



- Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier.
- The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities.
- Packets are stored and forwarded according to their priority to provide quality of service.

CIRCUIT SWITCHING	PACKET SWITCHING
In circuit switching there are 3 phases i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place.
In circuit switching, each data unit know the entire path address which is provided by the source	In Packet switching, each data unit just knows the final destination address intermediate path is decided by the routers.
Delay between data units in circuit switching is uniform.	Delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources are more in Circuit Switching	Less wastage of resources as compared to Circuit Switching

3.2 CONNECTING TO THE INTERNET

A router is a hardware device that allows user to connect several computers and other devices to a single Internet connection, which is known as a home network.

3.2.1 Through Internet Service Provider (ISP)

ISP is a business or organization that provides access to Internet and related services to consumers. An ISP is our gateway to the Internet and everything else we can do online. The second our connection is activated and set up, we will be able to send emails, go shopping, do research and more. The ISP is the link or conduit between our computer and all the other "servers" on the Internet. we may feel like we are talking to our mom directly through email, but in reality it's more "indirectly." our email goes from our computer, to the ISP computers/servers, where it's sent along to its destination through other servers on the network.

They offer various Services:

- Internet Access
- Domain name registration
- Dial-up access
- Leased line access

Connections types

Many equipment and technologies are used to connect WANs to the Internet.

- PSTN
- ISDN
- DSL
- Cable Connection
- Satellite Based Services

3.2.2 PSTN-Public switched telephone network

- A public switched telephone network is a combination of telephone networks used worldwide, including telephone lines, fiber optic cables, switching centers, cellular networks, satellites and cable systems. A PSTN lets users make landline telephone calls to one another.
- A PSTN is made up of switches at centralized points on a network that function as nodes to enable communication between two points on the network. A call is placed after being routed through multiple switches. Voice signals can then travel over the connected phone lines.
- The PSTN phone line is used with traditional dial-up network modems to connect a computer to the Internet. Dial-up Internet connections support up to 56 Kbps. In the early days of the Internet, this was the main method for home Internet access but it became obsolete with the introduction of broadband Internet services.
- Dial-up connection uses telephone line to connect PC to the internet. It requires a modem to setup dial-up connection.

- This modem works as an interface between PC and the telephone line.
- Connection rates for dial-up modems tend to fall between 24 kbps to 56 kbps.

PSTN structure: The traditional PSTN has a hierarchical architecture and a star structure. The individual subscriber lines are connected to a local exchange, which communicates with trunk exchanges as well as main and central exchanges. The lines within a local exchange typically have the same area code. A user who wants to call a number outside the local exchange has to add an area code. To make an international call, a user has to dial the country code.

-

3.2.3 ISDN-Integrated Services Digital Network

These are a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. Before Integrated Services Digital Network (ISDN), the telephone system was seen as a way to transmit voice, with some special services available for data. The main feature of ISDN is that it can integrate speech and data on the same lines, which were not available in the classic telephone system.
ISDN is a circuit-switched telephone network system, but it also provides access to packet switched networks that allows digital transmission of voice and data. This results in potentially better voice or data quality than an analog phone can provide. It provides a packet-switched connection for data in increments of 64 kilobit/s. It provided a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. A greater data rate was achieved through channel bonding. Generally ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

In the context of the OSI model, ISDN is employed as the network in data-link and physical layers but commonly ISDN is often limited to usage to Q.931 and related protocols. These protocols introduced in 1986 are a set of signaling protocols establishing and breaking circuit-switched connections, and for advanced calling features for the user. ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group videoconferencing systems.

ISDN Interfaces:

The following are the interfaces of ISDN:

1. **Basic Rate Interface (BRI)**
   There are two data-bearing channels (‘B’ channels) and one signaling channel (‘D’ channel) in BRI to initiate connections. The B channels operate at a maximum of 64 Kbps while the D channel operates at a maximum of 16 Kbps. The two channels are independent of each other. For example, one channel is used as a TCP/IP connection to a location while the other channel is used to send a fax to a remote location. In iSeries ISDN supports basic rate interface (BRl).
   The basic rate interface (BRl) specifies a digital pipe consisting two B channels of 64 Kbps each and one D channel of 16 Kbps. This equals a speed of 144 Kbps. In addition, the BRl

service itself requires an operating overhead of 48 Kbps. Therefore a digital pipe of 192 Kbps is required.

2. **Primary Rate Interface (PRI)**
   Primary Rate Interface service consists of a D channel and either 23 or 30 B channels depending on the country we are in. PRI is not supported on the iSeries. A digital pipe with 23 B channels and one 64 Kbps D channel is present in the usual Primary Rate Interface (PRI). Twenty-three B channels of 64 Kbps each and one D channel of 64 Kbps equals 1.536 Mbps. The PRI service uses 8 Kbps of overhead also. Therefore PRI requires a digital pipe of 1.544 Mbps.

3. **Broadband-ISDN (B-ISDN)**
   Narrowband ISDN has been designed to operate over the current communications infrastructure, which is heavily dependent on the copper cable however B-ISDN relies mainly on the evolution of fiber optics. According to CCITT B-ISDN is best described as 'a service requiring transmission channels capable of supporting rates greater than the primary rate.

ISDN Services:

ISDN provides a fully integrated digital service to users. These services fall into 3 categories-bearer services, teleservices and supplementary services.

1. **Bearer Services**
   Transfer of information (voice, data and video) between users without the network manipulating the content of that information is provided by the bearer network. There is no need for the network to process the information and therefore does not change the content. Bearer services belong to the first three layers of the OSI model. They are well defined in the ISDN standard. They can be provided using circuit-switched, packet-switched, frame-switched, or cell-switched networks.

2. **Teleservices**
   In this the network may change or process the contents of the data. These services corresponds to layers 4-7 of the OSI model. Teleservices relay on the facilities of the bearer services and are designed to accommodate complex user needs. The user need not to be aware of the details of the process. Teleservices include telephony, teletex, telefax, videotex, telex and teleconferencing. Though the ISDN defines these services by name yet they have not yet become standards.
3. **Supplementary Service**
   Additional functionality to the bearer services and teleservices are provided by supplementary services. Reverse charging, call waiting, and message handling are examples of supplementary services which are all familiar with today's telephone company services.

Principle of ISDN:

The ISDN works based on the standards defined by ITU-T (formerly CCITT). The Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU) and is based in Geneva, Switzerland. The various principles of ISDN as per ITU-T recommendation are:

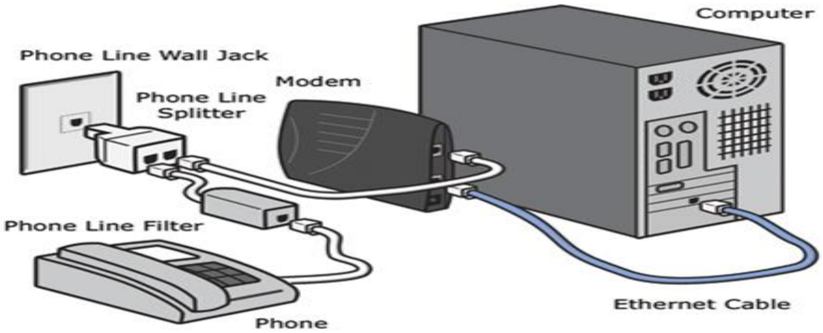
- To support switched and non-switched applications
- To support voice and non-voice applications
- Reliance on 64-kbps connections
- Intelligence in the network
- Layered protocol architecture
- Variety of configurations

PSTN verses ISDN

ISDN (Integrated Services Digital Network) was developed for the digital transmission of data and voice over ordinary phone lines. ISDN provides better voice quality than PSTN. The ISDN provides 128 Kbps. One of the key features of the ISDN is that it integrates both speech and data in the same line, which is not available with ordinary telephone wires. Users can make faster calls with ISDN than with PSTN.

3.2.4 DSL- Digital Subscriber Line

- Stands for "Digital Subscriber Line." DSL is a communications medium used to transfer digital signals over standard telephone lines. Along with cable Internet, DSL is one of the most popular ways ISPs provide broadband Internet access.
- DSL is acronym of Digital Subscriber Line. It is a form of broadband connection as it provides connection over ordinary telephone lines.
- Digital Subscriber Line or DSL connections are becoming widely available and can provide user with an excellent Internet connection.
- DSL services let the user the current copper phone lines in his/her home for both data and voice communication and (s)he can even use them simultaneously over the same copper pair.
- This means that the user can surf the Internet and talk on the phone at the same time.



3.2.5 Cable Connection

Cable TV Internet connection is provided through Cable TV lines.
It uses coaxial cable which is capable of transferring data at much higher speed than common telephone line.

Key Points:

- A cable modem is used to access this service, provided by the cable operator.
- The Cable modem comprises of two connections: one for internet service and other for Cable TV signals.
- Since Cable TV internet connections share a set amount of bandwidth with a group of customers, therefore, data transfer rate also depends on number of customers using the internet at the same time.

3.3 SATELLITE BASED SERVICES

- Satellite Internet connection offers high speed connection to the internet.
- There are two types of satellite internet connection: one way connection or two way connection.
- In one way connection, we can only download data but if we want to upload, we need a dialup access through ISP over telephone line.
- In two way connection, we can download and upload the data by the satellite. It does not require any dialup connection.
- This technology is a method by which Internet content is downloaded to a satellite dish and then transmitted directly from the dish to the user's PC.

3.3.1 LAST MILE FIBER

- Last mile technology is any information-transfer technology that conveys signals through the expansive telecom backbone along the generally short separation to and from the home or business.
- Last mile technology is the last and final connectivity between the individual customer and telecommunication service provider.
- It is important to understand that distance between them can be more than a mile, specifically in the rural areas.
- Last mile fibres are very expensive and demand high level of maintenance since they provide high-tech, high bandwidth.

3.4 CELLULAR TECHNOLOGY

Cellular technology is what mobile phone networks are based on, and it's the technology that gave mobile phones the name cell phones. Cellular technology basically refers to having many small interconnected transmitters as opposed to one big one.
The other main concept of cellular technology was that they were multiple access, meaning that they placed multiple voice or data connections into a single radio channel.

3.4.1 1G TECHNOLOGY

- 1G refers to the first generation of wireless telephone technology, mobile telecommunications which was first introduced in 1980s and completed in early 1990s.
- It's Speed was upto 2.4kbps.
- It allows the voice calls in 1 country.
- 1G network use Analog Signal.

DRAWBACKS OF 1G

- Poor Voice Quality
- Poor Battery Life
- Large Phone Size
- No Security
- Limited Capacity
- Poor Handoff Reliability

3.4.2 2G TECHNOLOGY

- 2G technology refers to the 2nd generation which is based on GSM.
- It was launched in Finland in the year 1991.
- 2G network use digital signals.
- It's data speed was upto 64kbps.

Features Includes:

- It enables services such as text messages, picture messages and MMS (multi media message).
- It provides better quality and capacity.

DRAWBACKS OF 2G

- 2G requires strong digital signals to help mobile phones work. If there is no network coverage in any specific area , digital signals would weak.
- These systems are unable to handle complex data such as Videos.

3.4.3 3G TECHNOLOGY

- 3G technology refer to third generation which was introduced in year 2000s.
- Data Transmission speed increased from 144kbps- 2Mbps.
- Typically called Smart Phones and features increased its bandwidth and data transfer rates to accommodate web-based applications and audio and video files.

FEATURES OF 3G TECHNOLOGY

- Providing Faster Communication
- Send/Receive Large Email Messages
- High Speed Web / More Security/ Video Conferencing / 3D Gaming
- TV Streaming/ Mobile TV/ Phone Calls
- Large Capacities and Broadband Capabilities
- 11 sec – 1.5 min. time to download a 3 min Mp3 song.

DRAWBACKS OF 3G TECHNOLOGY

- Expensive fees for 3G Licenses Services
- High Bandwidth Requirement

- Expensive 3G Phones.
- Large Cell Phones

3.4.4 4G TECHNOLOGY (Anytime, Anywhere)

- 4G technology refer to or short name of fourth Generation which was started from late 2000s.
- Capable of providing 100Mbps – 1Gbps speed.
- One of the basic term used to describe 4G is MAGIC.
- MAGIC:
  - Mobile Multimedia
  - Anytime Anywhere
  - Global Mobility Support
  - Integrated Wireless Solution
  - Customized Personal Services
- Also known as Mobile Broadband Everywhere.
- The next generations of wireless technology that promises higher data rates and expanded multimedia services.
- Capable to provide speed 100Mbps-1Gbps.
- High QOS and High Security
- Provide any kind of service at any time as per user requirements, anywhere.

Features Include:

- More Security
- High Speed
- High Capacity
- Low Cost Per-bit etc.

DRAWBACKS OF 4G

- Battery uses is more
- Hard to implement
- Need complicated hardware
- Expensive equipment required to implement next generation network.

COMPARISON BETWEEN 3G Vs 4G

Technology	**3G**	**4G**
Data Transfer Rate	3.1 MB/sec	100 MB/sec
Internet Services	Broadband	Ultra Broadband
Mobile - TV Resolution	Low	High
Bandwidth	5-20 MHz	100MHz

Frequency	1.6-2 GHz	2-8 GHz
Download and upload	5.8 Mbps	14 Mbps

3.5 CONNECTING TO LANS

This type of backbone network is useful when a company has several offices with LANs and needs to connect them. The connection can be done through bridges, sometimes called remote bridges. The bridges act as connecting devices connecting LANs and point-to-point networks, such as leased telephone lines.

3.5.1 Leased Line:

- A dedicated leased line is a point-to-point, high speed communication line that directly connects their computer to their ISP's network.
- The speed of their internet access depends on the type of leased line we have.
- Dedicated Leased Line is much more expensive than the DSL and Cable Connection.
- A leased line is a telephone line that is rented directly from the telephone company, and sometimes is referred to as direct connections to the Internet.

3.5.2 SONET/SDH(Synchronous Optical Network/ Synchronous Digital Hierarchy)

It is used for the transmission of various kinds of information such as text, audio, voice etc. over fiber optic cables.

Three Important concerns in designing SONET/ SDH.

1. **It is a Synchronous network.**

A single clock is used to handle the timing of transmission and equipment across the entire network.

Network wise synchronization adds a level of predictability to the system.

This predictability, coupled with powerful frame design, enables individual channels to be multiplexed, thereby improving speed and reducing cost.

2. **Standardization.**

SDH/SONET contains recommendations for the standardization of fiber optic transmission system equipment sold by different manufacturers.

3. **Universal Connectivity.**

SDH/SONET physical specification and frame design include mechanism that allow it to carry signals from incompatible tributary systems. This flexibility gives SONET/ SDH a reputation for universal connectivity.

3.6 REMOTE ACCESS

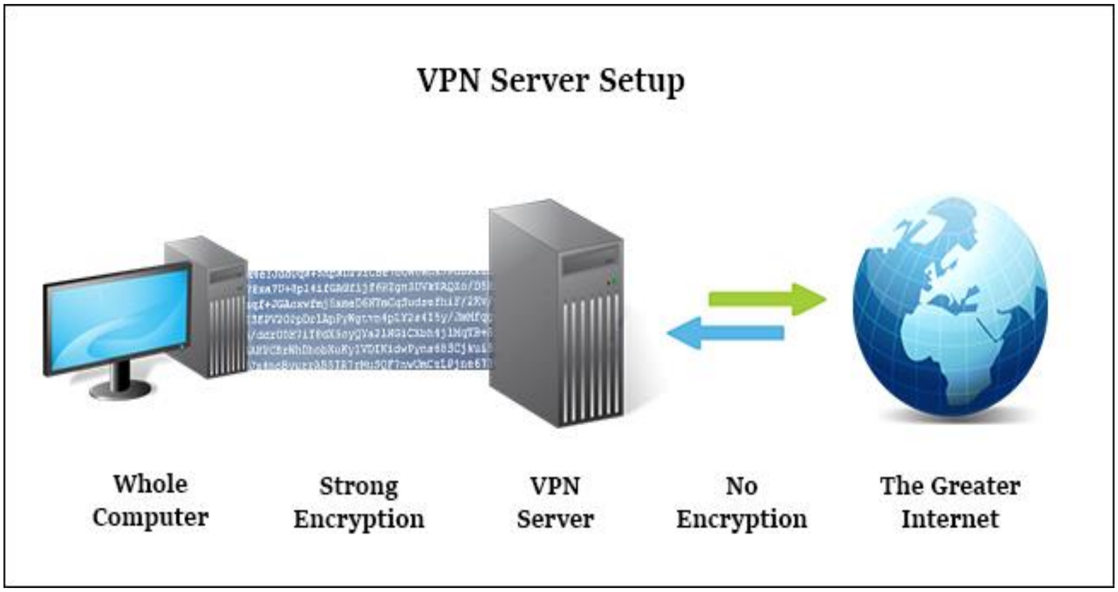
Remote access is the ability for an authorized person to access a computer or a network from a geographical distance through a network connection. Remote access enables users to connect to the systems they need when they are physically far away.

3.6.1 Remote and Dial-up Connections

- It is a form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a dialed connection to an Internet service provider (ISP) via telephone lines.
- The user's computer or router uses an attached modem to encode and decode Internet Protocol packets and control information into and from analogue audio frequency signals, respectively.
- Remote Access connection can be using Dial-up PPP.
- A dial-up connection is the least expensive way to access the Internet, but it also slowest connection.

3.6.2 VPN(Virtual Private Network)

- A Virtual Private Network is a connection method used to add security and privacy to private and public networks, like WiFi Hotspots and the Internet.
- Virtual Private Networks are most often used by corporations to protect sensitive data.
- The remote computer and the network server establish a secured connection across the Internet.
- This technique is called tunneling, because the connection runs across the Internet inside a secure medium.
- This connection makes used of the PPTP (Point-to-Point Tunneling Protocol)



VPN also uses **IPSec(Internet Protocol Security)**

- Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services.
- IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

VPN has the following advantages:

- Helps us to avoid censorship blocks
- Masks our IP address
- Hides our physical location
- Encrypts data between our computer and the VPN server
- Does not log our browsing activity
- Allows us to access popular streaming services like Netflix and YouTube from other countries.

3.6.3 SSL VPN

- An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser.
- In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer.
- The primary reason to use an SSL VPN product is to prevent unauthorized parties from eavesdropping on network communications and extracting or modifying sensitive data.
- SSL VPN systems offer secure and flexible options for enterprise employees, telecommuters and contractors to remotely connect to private enterprise networks.
- SSL VPNs rely on the TLS protocol, which has replaced the older SSL protocol, to secure remote access.

Advantages of SSL VPNs

- One of the primary advantages of an SSL VPN is that it uses the TLS technology implemented in modern web browsers, so there is no need to install specific client software. That makes it easy to deploy.
- Another benefit is that SSL VPNs require less administrative overhead and technical support than traditional VPN.
- SSL VPNs enable users to choose any web browser, regardless of the operating systems (OSes) their devices are running.

3.6.4 Remote Terminal Emulation

- A terminal emulator allows a host computer to access another computer, including remote ones, through either a command-line interface or a graphical one.
- The communication is made possible using protocols such as Telnet and SSH(Secure Shell).

- The terminal emulator allows the host computer to use or run applications on the remote computer, as well as transfer files between the two.
- The two systems need not be running the same operating system.

3.7 NETWORK SECURITY

Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.
Network security consists of following steps:

1. Protection: we should configure our systems and networks as correctly as possible

2. Detection: we must be able to identify when the configuration has changed or when some network traffic indicates a problem

3. Reaction: After identifying problems quickly, we must respond to them and return to a safe state as rapidly as possible

3.7.1 Authentication

Authentication is about validating our credentials like User Name/User ID and password to verify our identity. The system determines whether we are what we say we are using our credentials. In public and private networks, the system authenticates the user identity via login passwords. Authentication is usually done by a username and password, and sometimes in conjunction with factors of authentication, which refers to the various ways to be authenticated.

Authentication factors determine the various elements the system use to verify one’s identity prior to granting him access to anything from accessing a file to requesting a bank transaction. A user’s identity can be determined by what he knows, what he has, or what he is. When it comes to security, at least two or all the three authentication factors must be verified in order to grant someone access to the system.

Based on the security level, authentication factor can vary from one of the following:

- **Single-Factor Authentication**
  It’s the simplest authentication method which commonly relies on a simple password to grant user access to a particular system such as a website or a network. The person can request access to the system using only one of the credentials to verify his identity. The most common example of a single-factor authentication would be login credentials which only require a password against a username.

- **Two-Factor Authentication**
  As the name suggests, it's a two-step verification process which not only requires a username and password, but also something only the user knows, to ensure an additional level of security, such as an ATM pin, which only the user knows. Using a username and password along with an additional piece of confidential information makes it virtually impossible for fraudsters to steal valuable data.
- **Multi-Factor Authentication**
  It's the most advanced method of authentication which uses two or more levels of security from independent categories of authentication to grant user access to the system. All the factors should be independent of each other to eliminate any vulnerability in the system. Financial organizations, banks, and law enforcement agencies use multiple-factor authentication to safeguard their data and applications from potential threats.
  For example, when we enter our ATM card into the ATM machine, the machine asks us to enter our pin. After we enter the pin correctly, the bank then confirms our identity that the card really belongs to us and we are the rightful owner of the card. By validating our ATM card pin, the bank actually verifies our identity, which is called authentication. It merely identifies who we are, nothing else.

3.7.2 Authorization

Authorization, on the other hand, occurs after our identity is successfully authenticated by the system, which ultimately gives us full permission to access the resources such as information, files, databases, funds, locations, almost anything. In simple terms, authorization determines our ability to access the system and up to what extent. Once our identity is verified by the system after successful authentication, we are then authorized to access the resources of the system.

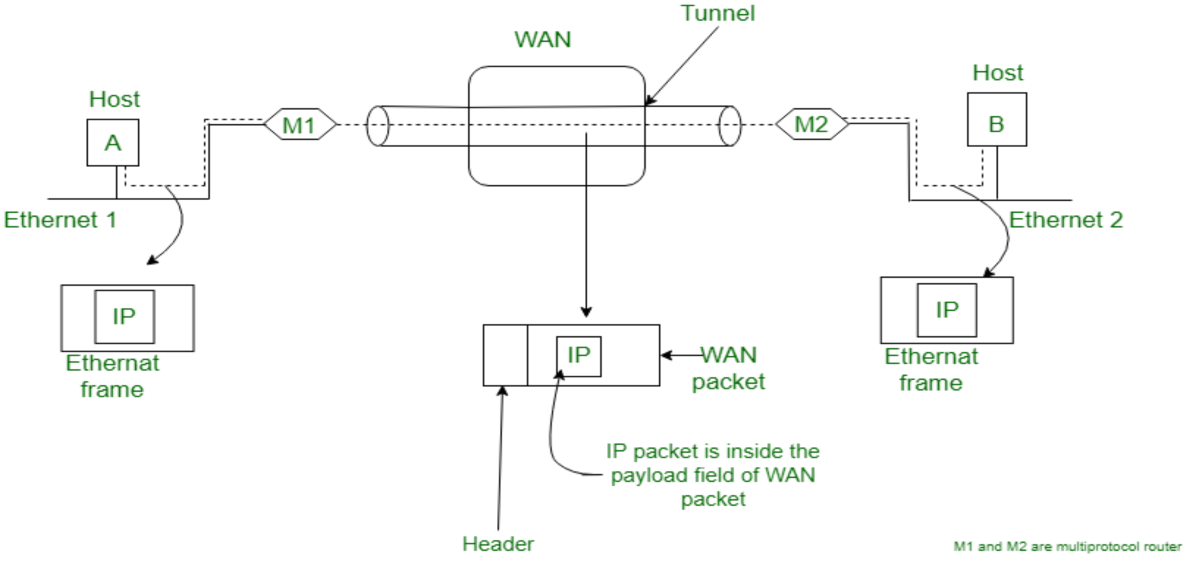
Authorization is the process to determine whether the authenticated user has access to the particular resources. It verifies our rights to grant us access to resources such as information, databases, files, etc. Authorization usually comes after authentication which confirms our privileges to perform. In simple terms, it's like giving someone official permission to do something or anything.

For example, the process of verifying and confirming employees ID and passwords in an organization is called authentication, but determining which employee has access to which floor is called authorization. Let's say we are traveling and we're about to board a flight. When we show our ticket and some identification before checking in, we receive a boarding pass which confirms that the airport authority has authenticated our identity. But that's not it. A flight attendant must authorize we to board the flight we're supposed to be flying on, allowing we access to the inside of the plane and its resources.

Access to a system is protected by both authentication and authorization. Any attempt to access the system might be authenticated by entering valid credentials, but it can only be accepted after successful authorization. If the attempt is authenticated but not authorized, the system will deny access to the system.

3.7.3Tunneling

A tunneling protocol is a communications protocol that allows for the movement of data from one network to another. It involves allowing private network communications to be sent across a public network through a process called encapsulation. For example, let us consider an Ethernet to be connected to another Ethernet through a WAN as:



Tunneling

The task is sent on an IP packet from host A of Ethernet-1 to the host B of ethernet-2 via a WAN.

Sequence of events:

1. Host A construct a packet which contains the IP address of Host B.
2. It then inserts this IP packet into an Ethernet frame and this frame is addressed to the multiprotocol router M1
3. Host A then puts this frame on Ethernet.
4. When M1 receives this frame, it removes the IP packet, inserts it in the payload packet of the WAN network layer packet and addresses the WAN packet to M2. The multiprotocol router M2 removes the IP packet and send it to host B in an Ethernet frame.

Encryption Protocols

Encryption is a method of “scrambling” data before transmitting it onto the Internet.

3.7.4 Symmetric encryption

To encrypt something, we need to use a key. Then, to decrypt it, we need the same key. For example user and their roommate having separate, but identical keys for theri place that unlock the same door. This is what symmetric encryption is a algorithms that use the same key to both encrypt and decrypt data.

3.7.5 Asymmetric encryption

There is another branch of cryptography that relies on different keys for the different processes. It is called asymmetric, *or* **public key cryptography** and in it, we have a pair of keys: a public one for encryption, and a private one for decryption.
This could be more confusing, but think of the one key as the lock rather than as a key everyone can put something in someone's mailbox (because it's public), but only they can unlock it (because only they have the private key).

SYMMETRIC KEY ENCRYPTION	ASYMMETRIC KEY ENCRYPTION
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity and non-repudiation.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

3.7.6 Digital Signatures

A Digital Signature (DS) is an authentication technique based on public key cryptography used in e-commerce applications. It associates a unique mark to an individual within the body of his message. This helps others to authenticate valid senders of messages.
Typically, a user's digital signature varies from message to message in order to provide security against counterfeiting. The method is as follows:

- The sender takes a message, calculates the message digest of the message and signs it digest with a private key.

- The sender then appends the signed digest along with the plaintext message.
- The message is sent over communication channel.
- The receiver removes the appended signed digest and verifies the digest using the corresponding public key.
- The receiver then takes the plaintext message and runs it through the same message digest algorithm.
- If the results of step 4 and step 5 match, then the receiver knows that the message has integrity and authentic.

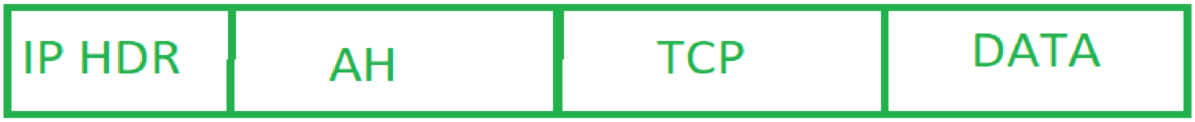
3.7.6 IP security (IPSec)

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

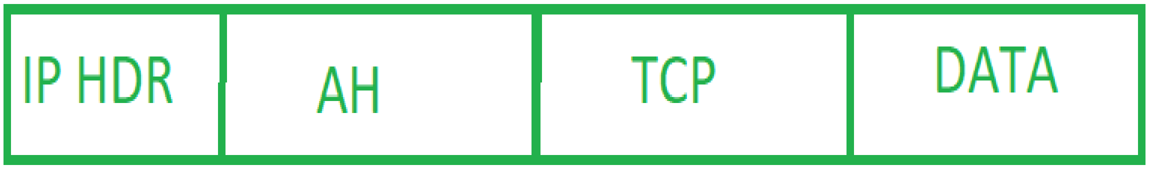
Uses of IP Security includes:
IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security:
It has the following components:

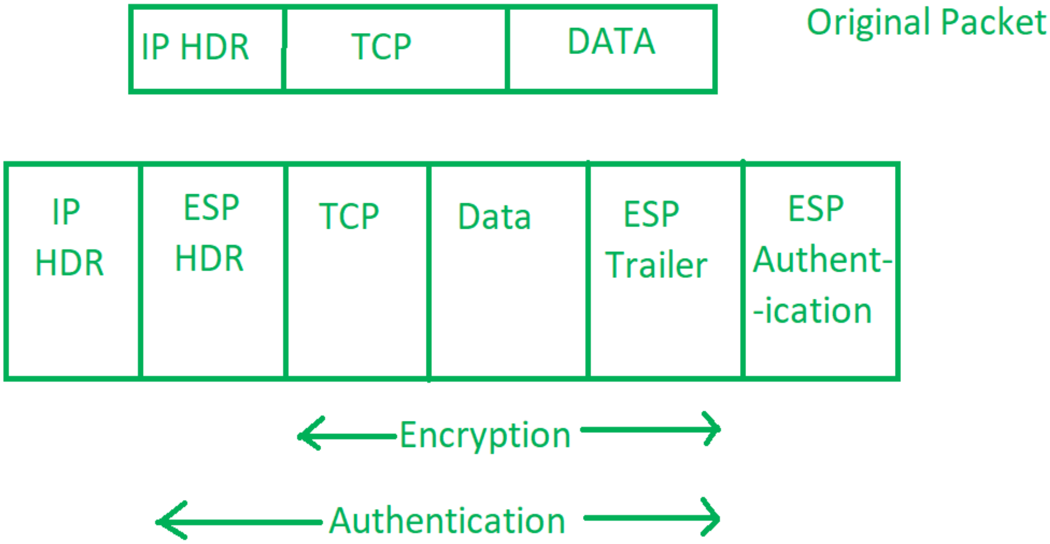


1. Encapsulating Security Payload (ESP)
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. Authentication Header (AH)
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data’s confidentiality.



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. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.
   Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



Working of IP Security

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.

2. Then the IKE Phase 1 starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode which provides the greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data accross the IP circuit.
4. Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

3.7.7 SSL and TLS

- SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. The two systems can be a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personal identifiable information or with payroll information).

- It does this by making sure that any data transferred between users and sites, or between two systems remain impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which can include credit card numbers and other financial information, names and addresses.

- TLS (Transport Layer Security) is just an updated, more secure, version of SSL.
- The two systems can be a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personal identifiable information or with payroll information).
- It does this by making sure that any data transferred between users and sites, or between two systems remain impossible to read.
- It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection.
- This information could be anything sensitive or personal which can include credit card numbers and other financial information, names and addresses.
- TLS (Transport Layer Security) is just an updated, more secure, version of SSL. We still refer to our security certificates as SSL because it is a more commonly used term.

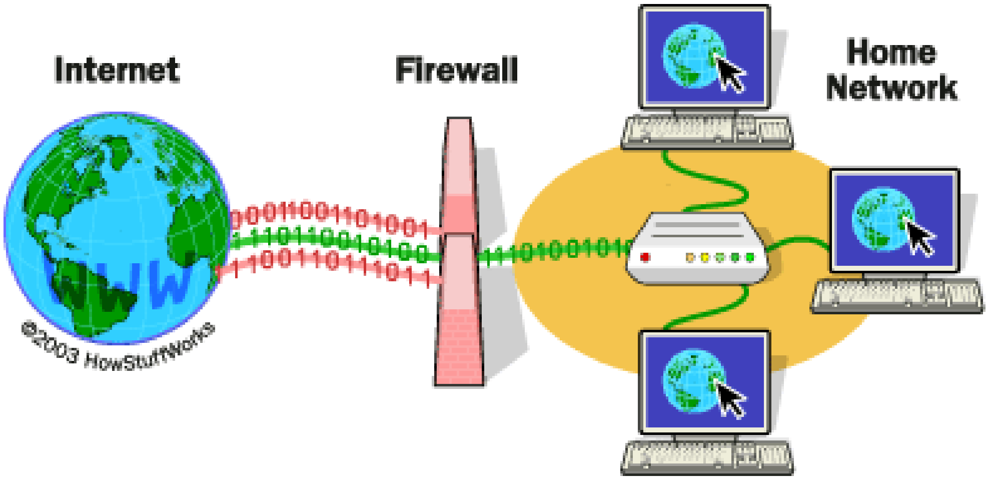
SSL handshake process

The handshake process is quite complex, and there are a number of variations allowed by the protocol. The following steps provide a broad outline that should give us a sense of how it works.

- The client contacts the server and requests a secure connection. The server replies with the list of cipher suites for algorithmic toolkits of creating encrypted connections that it knows how to use. The client compares this against its own list of supported cipher suites, selects one, and lets the server know that they'll both be using it.
- The server then provides its digital certificate, an electronic document issued by a third-party authority confirming the server's identity. We'll discuss digital certificates in more detail in a moment, but for now the most important thing we need to know about them is that they contain the server's public cryptographic key. Once the client receives the certificate, it confirms the certificate's authenticity.
- Using the server's public key, the client and server establish a session key that both will use for the rest of the session to encrypt communication. There are several techniques for doing this. The client may use the public key to encrypt a random number that's then sent to the server to decrypt, and both parties then use that number to establish the session key. Alternately, the two parties may use what's called a Diffie–Hellman key exchange to establish the session key.

3.7.8 Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between our internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.



Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

Types of firewalls

Firewalls can either be software or hardware, though it's best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between our network and gateway.

Packet-filtering firewalls, the most common type of firewall, examine packets and prohibit them from passing through if they don't match an established security rule set. This type of firewall checks the packet's source and destination IP addresses. If packets match those of an "allowed" rule on the firewall, then it is trusted to enter the network.

Packet-filtering firewalls are divided into two categories: stateful and stateless. Stateless firewalls examine packets independently of one another and lack context, making them easy targets for hackers. In contrast, stateful firewalls remember information about previously passed packets and are considered much more secure.

While packet-filtering firewalls can be effective, they ultimately provide very basic protection and can be very limited—for example, they can't determine if the contents of the request that's being sent will adversely affect the application it's reaching. If a malicious request that was allowed from a trusted source address would result in, say, the deletion of a database, the firewall would have no way of knowing that. Next-generation firewalls and proxy firewalls are more equipped to detect such threats.

- **Next-generation firewalls (NGFW)**

Combine traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more. Most notably, it includes deep packet inspection (DPI). While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious data.

- **Proxy firewalls**

Filter network traffic at the application level. Unlike basic firewalls, the proxy acts an intermediary between two end systems. The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked. Most notably, proxy firewalls monitor traffic for layer 7 protocols such as HTTP and FTP, and use both stateful and deep packet inspection to detect malicious traffic.

- **Network address translation (NAT) firewalls**

Allow multiple devices with independent network addresses to connect to the internet using a single IP address, keeping individual IP addresses hidden. As a result, attackers scanning a network for IP addresses can't capture specific details, providing greater security against attacks. NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.

- **Stateful multilayer inspection (SMLI) firewalls**

Filter packets at the network, transport, and application layers, comparing them against known trusted packets. Like NGFW firewalls, SMLI also examine the entire packet and only allow them to pass if they pass each layer individually. These firewalls examine packets to determine the state of the communication (thus the name) to ensure all initiated communication is only taking place with trusted sources.

Deploying firewall at network boundary is like aggregating the security at a single point. It is analogous to locking an apartment at the entrance and not necessarily at each door.
Firewall is considered as an essential element to achieve network security for the following reasons:

- Internal network and hosts are unlikely to be properly secured.
- Internet is a dangerous place with criminals, users from competing companies, disgruntled ex-employees, spies from unfriendly countries, vandals, etc.
- To prevent an attacker from launching denial of service attacks on network resource.
- To prevent illegal modification/access to internal data by an outsider attacker.

3.8 SECURITY THREATS

Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.
Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behave differently.

Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

1. Infection Methods
2. Malware Actions

Malware on the **basis of Infection** Method are following:

1. **Virus :** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. Ther Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms:** Worms are also self replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will for example consume hard disk space thus slowing down the computer.
3. **Trojan:** The Concept of Trojan is completely different from the viruses and worms. The name Trojan derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.
4. **Bots**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need of human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

Malware on the **basis of Actions:**

1. **Adware:** Adware is not exactly malicious but they do breach privacy of the users. They display ads on computer's desktop or inside individual programs. They come attached with free to use software, thus main source of revenue for such developers. They monitor our interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor our system activities and can even compromise our machine.
2. **Spyware:** It is a program or we can say a software that monitors our activities on computer and reveal collected information to interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they installs themselves and sits silently to avoid detection.

   One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.
3. **Ransomware:** It is type of malware that will either encrypt our files or will lock our computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.

4. **Scareware:** It masquerades as a tool to help fix our system but when the software is executed it will infect our system or completely destroy it. The software will display a message to frighten user and force to take some action like pay them to fix our system.
5. **Rootkits:** They designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
6. **Zombies:** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

- **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.
- **Identity theft** means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.
- **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.
- **Sabotage** means destroying company's website to cause loss of confidence on part of its customer.
- **Information extortion** means theft of company's property or information to receive payment in exchange. For example ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim's files will be unlocked.

These are the old generation attacks that continue these days also with advancement every year. Apart from these there are many other threats. Below is the brief description of these new generation threats.

- **Technology with weak security**
  With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follows Information Security principles. Since the market is very competitive Security factor is compromised to make device more up to date. This leads to theft of data/ information from the devices
- **Social media attacks**
  In this cyber criminals identify and infect a cluster of websites that persons of a particular organisation visit, to steal information.
- **Mobile Malware**
  There is a saying when there is a connectivity to Internet there will be danger to Security. Same goes to Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus in the device.
- **Outdated Security Software**
  With new threats emerging everyday, updation in security software is a pre requisite to have a fully secured environment.
- **Corporate data on personal devices**
  These days every organization follows a rule BYOD. BYOD means Bring their own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.
- **Social Engineering**

It is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick user into giving their private and confidential information or they will gain user trust to get access to their computer to install a malicious software- that will give them control of their computer. For example email or message from user friend, that was probably not sent by user friend. Criminal can access their friends device and then by accessing the contact list he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definately check the link or attachment in the message, thus unintentionally infecting the computer.