./

Learning Report – **Computer Networks**



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel. No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be approved By** | **Remarks/Revision Details** |
| 1 |  | Name/PS No | Name/PS No | Module Owner Name | Comments |
| 2 | 15/02/21 |  |  |  |  |
| 3 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Document History**

Table of Contents

[Table of Figures 3](#_Toc53129062)

[Table of Tables 4](#_Toc53129063)

[ACTIVITY 1: SYSTEM/ SOFTWARE DEVELOPMENT 4](#_Toc53129064)

[**INTRODUCTION** 4](#_Toc53129065)

[**MY PRODUCT: “Name ”** 6](#_Toc53129066)

[**SWOT ANALYSIS** 7](#_Toc53129067)

[**REQUIREMENTS** 7](#_Toc53129068)

[**DESIGN** 8](#_Toc53129069)

[HIGH LEVEL DESIGN 8](#_Toc53129070)

[LOW LEVEL DESIGN 11](#_Toc53129071)

[**TEST PLANS** 13](#_Toc53129072)

[**REFERENCES** 15](#_Toc53129073)

[ACTIVITY 2: AGILE METHODOLOGY 15](#_Toc53129074)

[**THEME** 15](#_Toc53129075)

[**EPIC** 15](#_Toc53129076)

[**USER STORY** 16](#_Toc53129077)

[**REFERENCES** 17](#_Toc53129078)

[APPENDIX: 17](#_Toc53129079)

## Table of Figures

[Figure 1 CLASS DIAGRAM(HIGH LEVEL) 10](#_Toc52177314)

[Figure 2 USE CASE DIAGRAM (HIGH LEVEL) 11](#_Toc52177315)

[Figure 3 ACTIVITY DIAGRAM (HIGH LEVEL) 12](#_Toc52177316)

[Figure 4 USE CASE DIAGRAM (LOW LEVEL) 12](#_Toc52177317)

[Figure 5 ACTVITY DIAGRAM (LOW LEVEL) 13](#_Toc52177318)

[Figure 6 BLOCK DIAGRAM 13](#_Toc52177319)

[Figure 7 COMPONENT DIAGRAM (HIGH LEVEL) 22](#_Toc52177320)

[Figure 8 ACTIVITY DIAGRAM (high level) 23](#_Toc52177321)

[Figure 9 ACTIVITY DIAGRAM (LOW LEVEL) 24](https://lnttsgroup.sharepoint.com/sites/GEA/Global%20Engineering%20Academy/GEA%20Insights/Genesis/Shared%20Documents/Submission/MYSORE/2009MYSEMB/Foundation/Applied%20SDLC%20with%20Software%20Testing/99002439/FINAL.docx#_Toc52177322)

[Figure 10- ACTIVITY DIAGRAM (LOW LEVEL) 24](#_Toc52177323)

[Figure 11 TEST PLAN 25](#_Toc52177324)

[Figure 12 GIT 27](#_Toc52177325)

[Figure 13 GIT ISSUES 28](#_Toc52177326)

[Figure 14 GIT COMMITS 1 28](#_Toc52177327)

[Figure 15 GIT COMMIT 2 29](#_Toc52177328)

[Figure 16 GIT 30](#_Toc52177329)

[Figure 17 GIT MAKE 31](#_Toc52177330)

[Figure 18 GIT MAKE 2 31](#_Toc52177331)

[Figure 19 GIT BUILD 32](#_Toc52177332)

[Figure 20 GIT CODE QUALITY 32](#_Toc52177333)

## Table of Tables

[Table 1 AGING 6](#_Toc52177304)

[Table 2 GRADING COST 6](#_Toc52177305)

[Table 3 REQUIREMENTS 8](#_Toc52177306)

[Table 4 HIGH LEVEL TEST PLAN 15](#_Toc52177307)

[Table 5 LOW LEVEL TEST PLAN 16](#_Toc52177308)

[Table 6 USER STORIES 17](#_Toc52177309)

[Table 7 AGING 19](#_Toc52177310)

[Table 8 GRADING COST 19](#_Toc52177311)

[Table 9 REQUIREMENTS 21](#_Toc52177312)

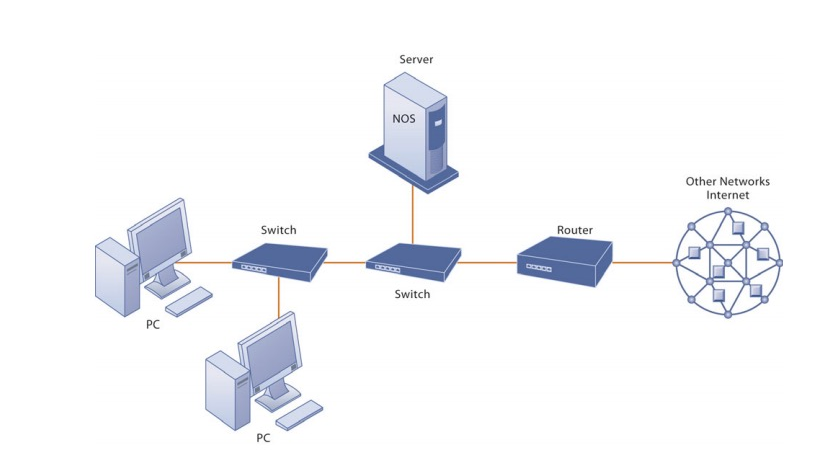
[Table 10 USER STORIES 27](#_Toc52177313)

**OVERVIEW OF NETWORKS**

A computer network is a group of devices linked to each other that enables the device will communicate with another device and share their data, applications and resources. Group of devices connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network.

Computer Networks support many applications and services, such as access to the World Wide Web, Digital video, Digital audio, shared use of application and storage servers, printers, fax machines, and use of email and instant messaging applications.

**COMPONENTS OF COMPUTER NETWORK**



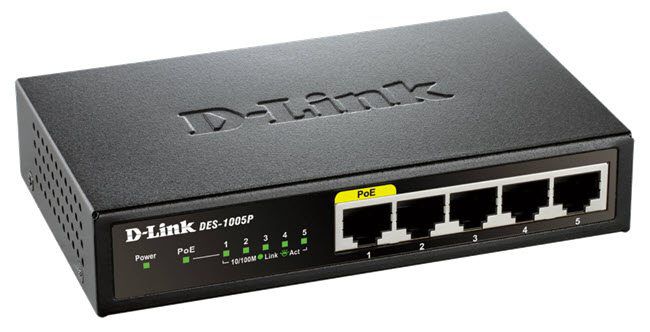
**COMPONENTS OF A SIMPLE COMPUTER NETWORK**

In an Ethernet network, there are some networking devices that play their roles at various levels such as hubs, switches and routers. The functions of the three devices are all quite different from one another, even if sometimes they are all integrated into a single device. due to that, many people feel confused about the differences between the hub, switch, and router. The following part will focus on the topic

hub vs switch vs router, aiming to clarify differences among them.

**HUB**

Hub is a central device that splits the network connection into multiple devices. When computer requests for information from a computer, it sends the request to the Hub. Hub distributes this request to all the interconnected computers.



**TYPES OF HUB**

* **Active Hub:** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. These are used to extend the maximum distances between the modes.
* **Passive Hub:** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals on to the network without cleaning and boosting then and can’t be used to extend the distance between nodes.
* **Intelligent Hub:** It work like active hubs and include remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub

**SWITCHES**

Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network, i.e., it sends the message to the device for which it belongs to. Therefore, we can say that switch sends the message directly from source to the destination.

**Routers**

A router is s device like a switch that routes data packets based on their IP address. Router is mainly a Network layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.

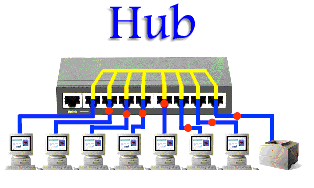
**Bridge**

A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses

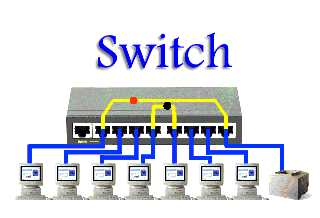
Of source and destination and it also used for the interconnecting two local area networks on the same protocol. It has a single input and output port.

**Hub vs Switch vs Router**

In network equipment and devices, data is usually transmitted in the form of a frame. When a frame is received, it is amplified and then transmitted to the port of the destination PC (Personal Computer). The big difference between hub and switch is in the method in which frames are being delivered.



In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Additionally, a 10/100Mbps hub must share its bandwidth with each and every one of its ports.



Unlike an Ethernet hub or switch that is concerned with transmitting frames, a router is to route packets to other networks until that packet ultimately reaches its destination. One of the key features of a packet is that it not only contains data but the destination addresses of where it's going. What's more, router is the only one of these three devices that will allow you to share a single IP (Internet Protocol) address among multiple network clients.

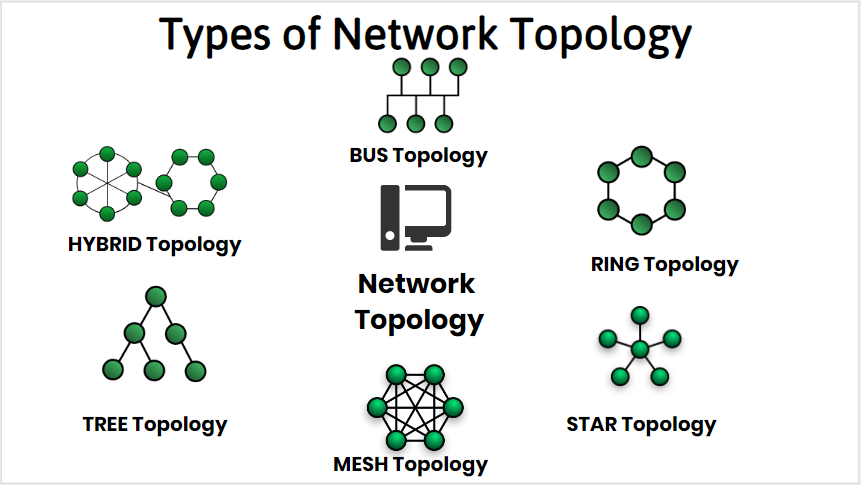
**Conclusion**

The differences between hub, switch and router is a confusing term for users. Understanding these distinctions among them can be helpful to find the most appropriate device for your network.

|  |  |  |  |
| --- | --- | --- | --- |
| **Template** | **HUB** | **SWITCH** | **ROUTER** |
| Layer | Physical Layer | Data Link Layer | Network layer |
| Function | To connect a network of personal computers together, they can be joined through a central hub | Allow connections to multiple devices, manage ports, manage VLAN security settings | Direct data in a network |
| Port | 4/12 ports | multi-port, usually between 4 and 48 | 2/4/5/8 ports |
| Device type | Non-intelligent device | Intelligent device | Intelligent device |
| Used in (LAN, MAN, WAN) | LAN | LAN | LAN, MAN, WAN |
| Transmission mode | Half duplex | Half/Full duplex | Full duplex |
| Speed | 10Mbps | 10/100Mbps, 1Gbps | 1-100Mbps(wireless); 100Mbps- |
| Address used for data transmission | MAC address | MAC address | IP address |
| Data Transmission form | electrical signal or bits | frame & packet | packet |

**Topology**

The physical arrangement of the computer system/node which is connected to each other via communication medium is called Topology



**Bus Topology**

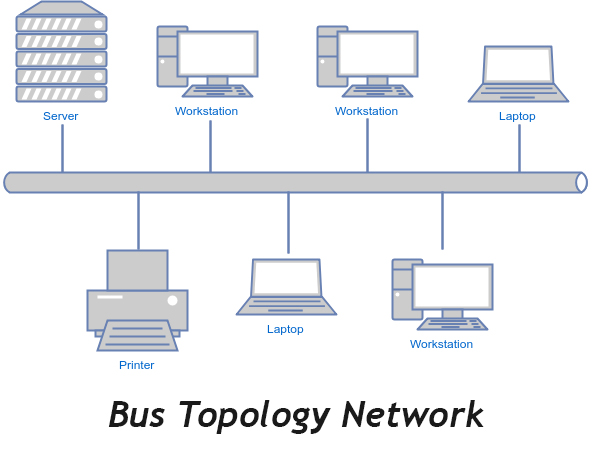
In BUS Topology, one long cable acts as a Single Communication Channel & all the devices are connected to this cable

**Advantage**

* Easy to add / remove nodes in a network
* Required only cable
* It is less expensive
* It broadcast the messages to each device which are connected through the cable.
* It is easy to maintain.
* In case of any computer failure, there will be no effect on other devices.

**Dis-Advantage**

* If cable is fail then the entire network will be failed.
* The messages are broadcast So, we can’t send private messages.
* It takes more time to pass the messages from one place to another place.
* The length cable is limited.
* In this topology data is transmitted only one direction.

****

**Ring Topology**

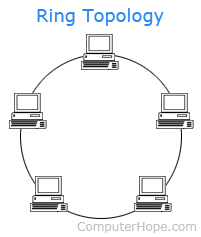
It is called ring topology because it forms a ring. In this Topology each node is strongly connected with is adjacent node.

**Advantage**

* It forms a strong network.
* Each an every node can share data with another node connected through a ring topology.
* Transmission rate of data is very speed.
* The data send through ring topology will be broadcast.

**Dis-Advantage**

* It is very difficult task to add some new computer.
* If we want to send data from a source to destination machine then data will un-necessary passed to all nodes.
* Single point of failure, that means if a node goes down entire network goes down.
* It is very difficult to recover the ring topology if any particular machine is not working properly.
* We can’t send private messages

****

**Star Topology**

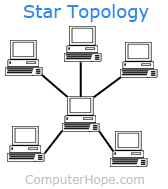
In star topology all the nodes are connected with a central device called Hub. And the sharing of data is only possible through HUB

**Advantage**

* It broadcast the messages.
* It is less expensive due to less cable.
* Easy to connect new nodes without affecting rest of the network.
* If one node is failed, then it would not be failure entire network.

**Dis-Advantage**

* In star topology we must required a network device like HUB, SWITCH etc.
* If two nodes want to share the data sharing is only possibly through HUB.
* If HUB is failed the entire network will be failed.
* We can’t send private data.

****

**Mesh Topology**

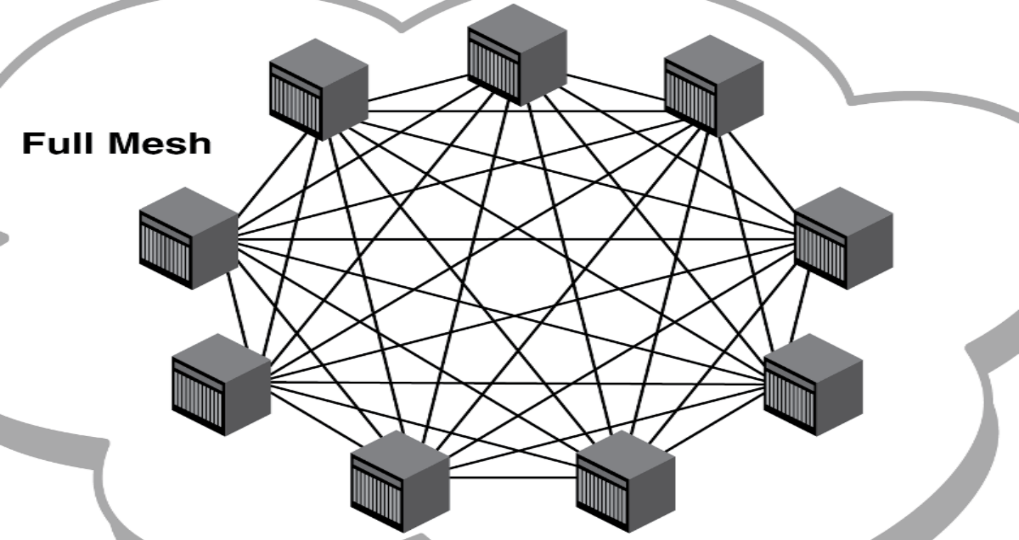
In this topology each an every computer is directly connected with each-other, So we can directly send the data to the destination machine without going to intermediate machine.

**Advantage**

* It is very good topology to send the private messages.
* All nodes are directly associated with another node so it provide point to point connection
* Un-like ring topology, if a particular machine is failed then entire network will not fail.
* Multiple devices can send or receive data Simultaneously.

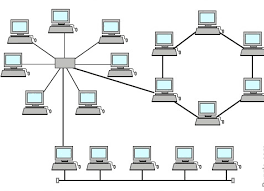
**Dis-Advantage**

* It is very difficult to add some new node because each an every computer directly connected with another one.
* If a particular machine not working then, we can’t send or receive data from the failure machine.



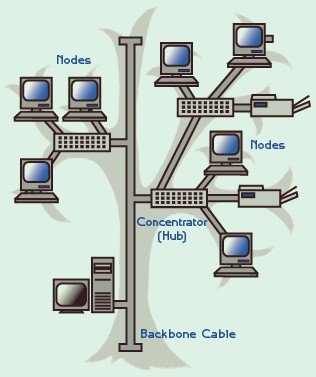
**Hybrid Topology**

Combination of various different topology is called Hybrid topology. A hybrid topology is a type of network topology that uses two or more differing network topologies. These topologies can include a mix of bus topology, mesh topology, ring topology, star topology, and tree topology.



**Tree Topology**

In this topology, all the nodes are connected like a branches of tree the Combination of BUS & STAR topology is called Tree Topology



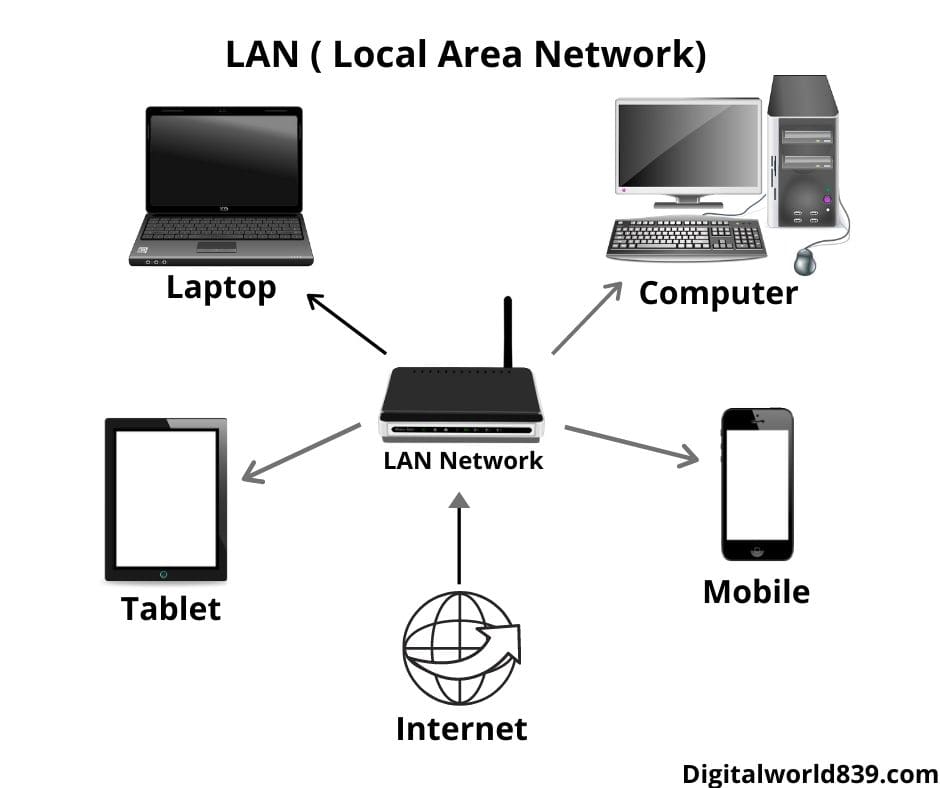
# Types of networks

A network is defined as a group of two or more computer systems linked together.

There are many types of computer networks, the common types of area networks including those five: LAN - Local Area Network, WAN - Wide Area Network, WLAN - Wireless Local Area Network, MAN - Metropolitan Area Network and CAN - Campus Area Network.

**LAN (Local Area Network)**

Can go up to 1 KM radius. A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment.

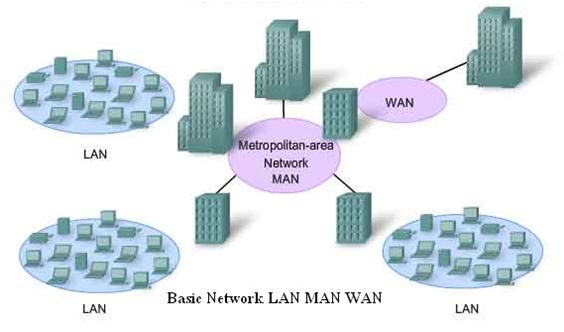


**MAN (Metropolitan Area Network)**

A Metropolitan Area Network is a bigger version of LAN that uses similar technology as LAN. It spans over a larger geographical area such as a town or an entire city.

It can be connected using an optical fiber cable as a communication medium. Two or more LAN's can also be connected using routers to create a MAN. When this type of network is created for a specific campus, then it is termed as CAN(Campus Area Network).

provide network communications over larger geographical regions. The primary difference between the two lies within the size of the regions being served.

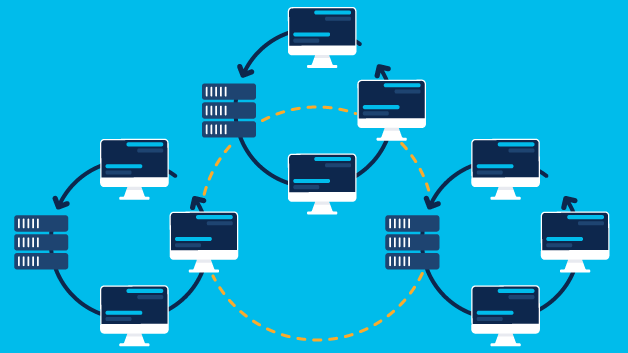


**WAN (Wide Area Network)**

In its simplest form, a wide-area network (WAN) is a collection of local-area networks (LANs) or other networks that communicate with one another.  A WAN is essentially a network of networks, with the Internet the world's largest WAN.

Today, there are several types of WANs, built for a variety of use cases that touch virtually every aspect of modern life.

A WAN router, also known as an edge router or border router is a device that routes data packets between WAN locations, giving an enterprise access to a carrier network.  Several WAN protocols have been developed over time, including Packet over SONET/SDH (PoS), Multiprotocol Label Switching (MPLS), ATM, and Frame Relay.



WAN NETWORK

**Personal Area Network (PAN)**

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

**Campus Area Network (CAN)**

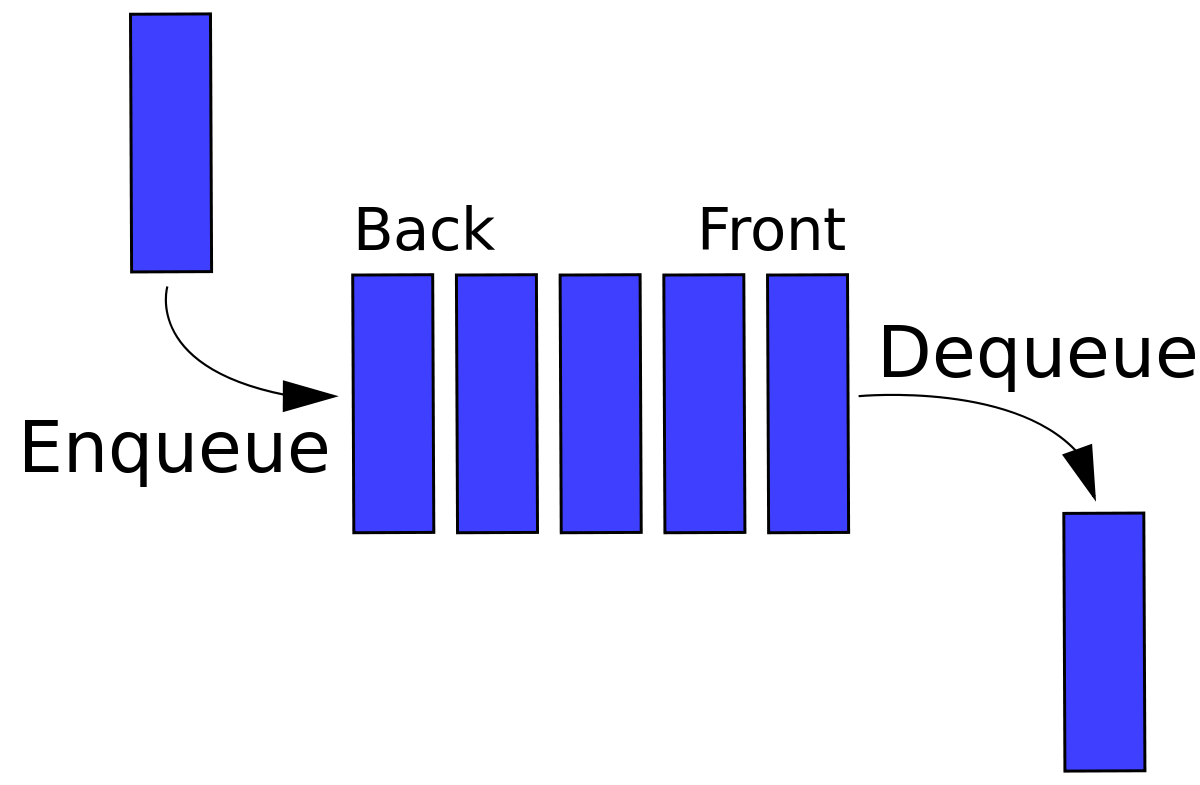
Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

**Queuing**

Regardless of how simple or how sophisticated the rest of the resource allocation mechanism is, each router must implement some queuing discipline that governs how packets are buffered while waiting to be transmitted. The queuing algorithm can be thought of as allocating both bandwidth (which packets get transmitted) and buffer space (which packets get discarded). It also directly affects the latency experienced by a packet by determining how long a packet waits to be transmitted. This section introduces two common queuing algorithms—first-in, first-out (FIFO) and fair queuing (FQ)—and identifies several variations that have been proposed.

**scheduling**

In computing, **s**cheduling is the method by which work is assigned to resources that complete the work. The work may be virtual computation elements such as threads, processes or data flows, which are in turn scheduled onto hardware resources such as processors, network links or expansion cards.



**Wired Networks:**

Wired communication refers to the transmission of the data over wire-based technology, it may include connection of two or more computers, printers, scanners, keypad and devices linked by Ethernet cables.

Some of the Ethernet standards are:

802.3 – It is a 10BASE5 thick coax, which has data rate of 10Mbps and operates on CSMA/CD (Carrier Sense Multiple Access with Collision Detection) process

802.3a – It is a 10BASE2 thin coax, which has data rate of 10Mbps.

802.3i – It is a 10BASET twisted pair cable, which has data rate of 10Mbps.

802.3j - 10Base-F (fiber optic)

802.3u – It is a 100BASET twisted pair cable, which has data rate of 100Mbps.

802.3x - Full duplex

802.3ae - 10-Gigabit Ethernet

802.3ba - 40Gbps & 100Gbps Ethernet

**Wireless Networks:**

Wireless Networking is a network that uses electromagnetic waves traveling through free space to connect stations or devices. It enables data to be shared between two devices without any physical connection between them.

Some wireless networking standards are:

802.11a - 802.11a applies to wireless local area networks and supports a maximum a maximum connect rate of 54 Mbps throughput in the 5GHz band.

802.11b - 802.11b applies to wireless local area networks and supports a maximum connect rate of 11 Mbps with fallback to 5.5, 2, and 1 Mbps in the 2.4GHz ISM band

802.11n- This standard works on both the 2.4 GHZ and 5 GHZ bands, its net data ranges from 54Mbits/s to 600Mbits/s.

**NETWORK SECURITY**

How do we keep them from impersonating us, or from listening in to our conversations or downloading our data? Computer security problems are in the news on almost a daily basis. In this chapter and the next we take a look at just a few of the issues involved in building secure networks.

For our limited overview here, we will divide attacks into three categories:

1. Attacks that execute the intruder’s code on the target computer

2. Attacks that extract data from the target, without code injection

3.Eavesdropping on or interfering with computer-to-computer communication.

More technical forms of attack may involve a virus, a buffer overflow Stack Buffer Overflow and Heap Buffer Overflow,some other software flaw The Morris Worm.

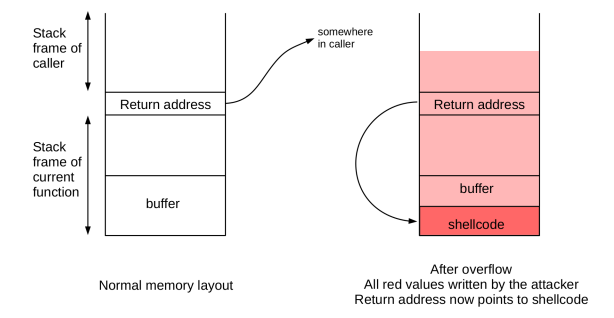
**stack overflow**

The stack buffer overflow is perhaps the classic way for an attacker to execute a short piece of machine code on a remote machine, thus compromising it. Such attacks are always due to an implementation flaw. A server application reads attacker-supplied data into a buffer, buf, of length buflen. Due to the flaw, however, the server reads more than buflen bytes of data, and the additional data is written into memory past the end of buf, corrupting memory. In the C language, there is no bounds checking with native arrays, and so such an overflow is not detected at the time it occurs.

A common goal for the attacker is to supply an overflowing buffer that does two things:

1. It includes a shellcode - a small snippet of machine code that, when executed, does something bad (traditionally but not necessarily by starting a shell with which the attacker can invoke arbitrary commands).

2. It overwrites the stack return address so that, when the current function exits, control is returned not to the caller but to the supplied shellcode.

****

**Heap Overflow**

As with stack overflows, heap overflows all rely on some software flaw that allows data to be written beyond the confines of the designated buffer. A buffer on the heap is subject to the same software-failure overflow prospects as a buffer on the stack. An important difference, however, is that buffers on the heap are not in clear proximity to an obvious return address. Despite that difference, heap overflows can also be used to enable remote-code-execution attacks.

Perhaps the simplest heap overflow is to take advantage of the fact that some heap pages contain executable code,. If the page with the overflowable buffer is pointed to by p, and the following page in memory pointed to by q contains code, then all an attacker has to do is to have the overflow fill the q page and a shellcode. When at some point a call is made to the code pointed to by q, the shellcode is executed instead. A drawback to this attack is that the layout of heap pages.

**Cryptography**

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it

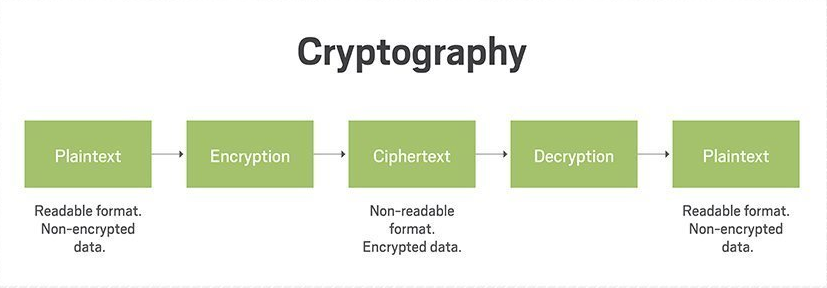
"crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing."

To protect packet contents. Different techniques address different issues; three classic goals are the following:

1. Message confidentiality: eavesdroppers should not be able to read the contents.

2. Message integrity: the recipient should be able to verify that the message was received correctly, even in the face of a determined adversary along the way.

3. Sender authentication: the recipient should be able to verify the identity of the sender

****

**Encryption**

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

The process of encrypting and decrypting messages involves keys. The two main types of keys in cryptographic systems are symmetric-key and public-key (also known as asymmetric-key).

**Types:**

**Symmetric key**

In symmetric-key schemes, the encryption and decryption keys are the same. Communicating parties must have the same key in order to achieve secure communication. The German Enigma Machine utilized a new symmetric-key each day for encoding and decoding messages.

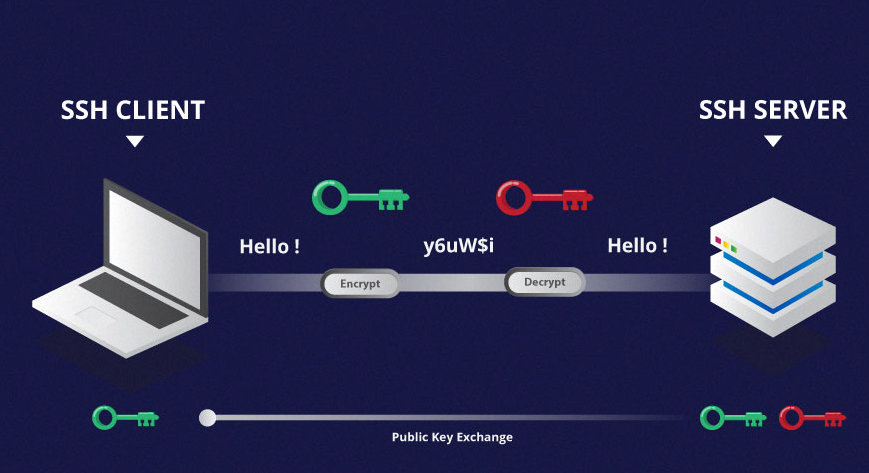
**Public key**

Illustration of how encryption is used within server Public key encryption.

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read. Public-key encryption was first described in a secret document in 1973, beforehand, all encryption schemes were symmetric-key (also called private-key).

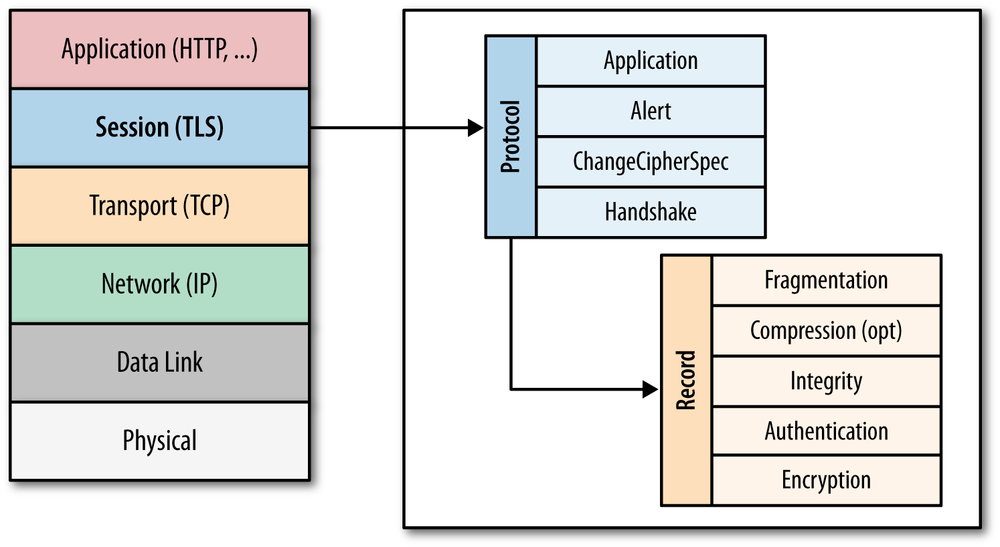
**SSH**

SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.

****

**TLS**

Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in web application security

****

**MTLS**

Mutual authentication is a desired characteristic in verification schemes that transmit sensitive data, in order to ensure data security. Mutual authentication can be accomplished with two types of credentials: usernames and passwords, and public key certificates.

**Protocols**

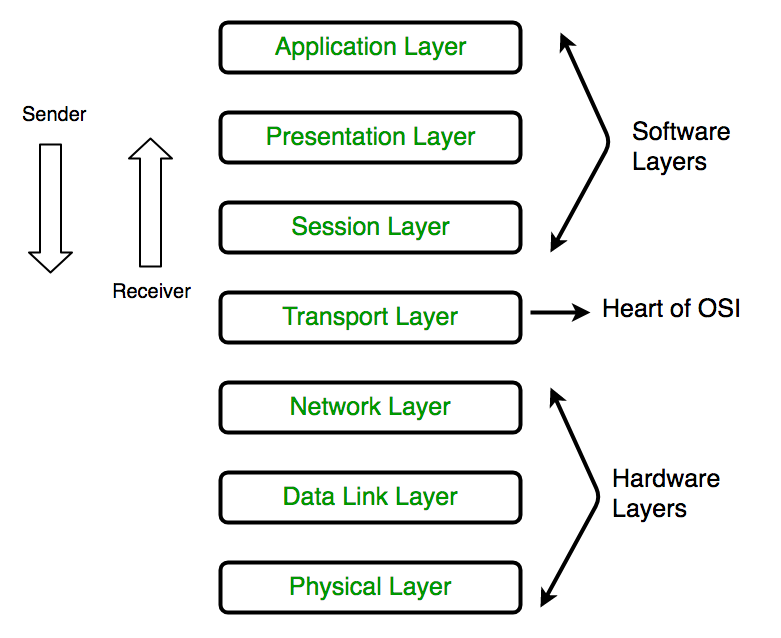
**OSI Layers**

**Open System Interconnection:**

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

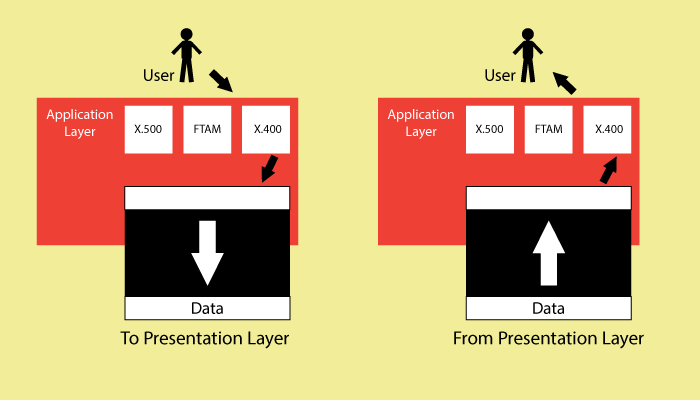
**Introduction:**

OSI (Open Systems Interconnection) is used to understand how data is transfer from one device to another. It has 7 layers. It is a reference model for how applications communicate over a network. This model focuses on providing a visual design of how each communications layer is built on top of the other.

****

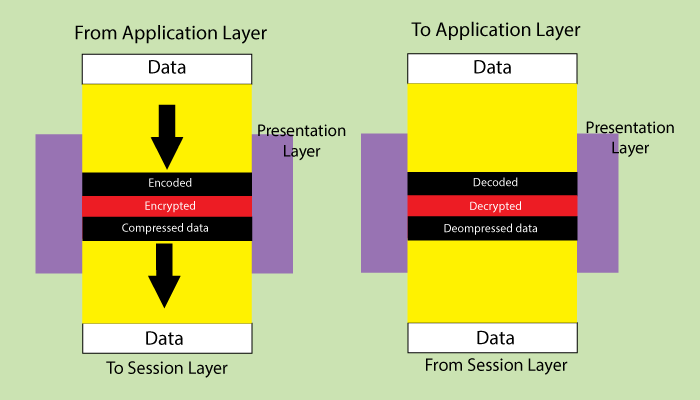
**LAYER 7: APPLICATION LAYER**

The top layer of an OSI model (layer seven) is the application layer that delivers network services or protocols that comply with an end-user’s data to the end-user. It provides protocols that allow software to send and receive information and present meaningful data to users.  
  
Examples of Layer 7 applications include web browsers such as Google Chrome or Firefox, as well as apps such as Office, Outlook, and Skype. The services provided by each of these applications permit the application layer to supply and receive data from the Presentation layer.  
  
A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).



**Layer 6: Presentation layer:**  
  
Presentation layer get the data from the Application layer. The data is in the form of numbers and characters. Presentation layer convert that characters and numbers to machine understandable binary format

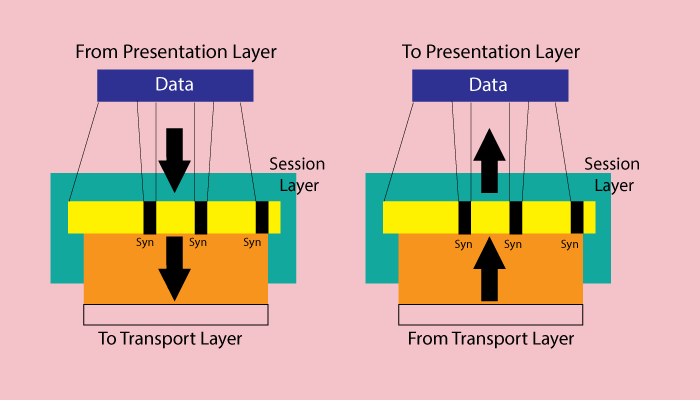
* Example conversion of ASCII to EBCDIC (Extended Binary Coded Decimal Interchange Code)
* This process is known as translation. Before the data is transmitted to the presentation layer reduces the number of bits that are used to represent the original data.
* This bit reduction process is called data compression and it can be Lossy or Lossless.
* To maintain the integrity of data, before transmission data is encrypted at the sender side and data is decrypted at the receiver side.
* Here SSL (Secure Sockets Layer) protocol is used for encrypting and decrypting the data.
* Some of the protocols used in presentation layer are SSH, IMAP, MPEG, JPEG



**Layer 5: Session Layer:**

Session layer helps in setting up and managing connections enabling sending and receiving of data followed by termination of connections or sessions

* Session layer has its helpers called APIs (Application Programming interfaces)
* NETBIOS (Network Basic Input output System) is an example of APIs which allows applications of different computers to communicate with each other. Just before a session or connection is established with the server.
* Server perform a function called authentication. It is a process of verifying who you are.
* For this server uses a username and password. Once the username and password are matched the session or a connection is established between your computer and the server
* After the authentication session layer check for authorization
* This process is determined if you have permission to access a file. If not you will get a message saying you are not authorized to access this page.
* These are the two functions authentication and authorization are performed by the session layer



**Layer 4: Transport Layer:**

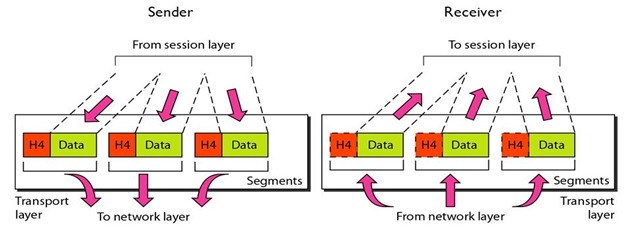
Transport layer controls the reliability of communication through Segmentation, Flow control, Error control.

* + Segmentation:
    - In segmentation, the data received from the session layer is divided into small data units called as segments.
    - Each segment contains a source and destination port number and a sequence number.
    - Port number help to direct each segment to the correct application
    - Sequence number helps to reassemble the segments in correct order to form correct message at the receiver.
  + Flow Control:
    - In flow control the transport layer controls the amount of data being transmitted.
    - For example, a mobile is connected to a server, Here server can transmit data maximum at 100Mbps and our mobile can process data maximum at 10Mbps. Now we are downloading the file from the server. Server start sending the file at 50Mbps which is greater than the rate our mobile can process.
    - So the mobile phone tell the transmission layer to slow down the data transmission rate up to 10Mbps so that no data can get lost. Like this wise versa.
* Error Control:
* Transport layer also help in error control, if some data does not arrive the destination. Transport layer uses automatic repeat request scheme to retransmit the lost or corrupted data.
* A group of bits called checksum is added to each segment by the transport layer to find out the received corrupted segment
* Protocols for transport layer:
* Transmission Control protocol (TCP)

1. TCP is the connection oriented transmission
2. It provided feedback that data delivered or not.
3. Lost data can be recovered in TCP

* User Datagram Protocol (UDP)

1. UDP is the connectionless transmission it is faster than the
2. It doesn’t provide any feedback where it delivered data or not
3. Lost data can’t be recovered



**LAYER 3: Network Layer:**

1. Network layer work for the transmission of the received data segment from one computer to the another located in different networks.
2. Data units in network layer are called packets. It is the layer where routers to decide the function of network layer are logical addressing, routing and path determination.
3. IP addressing (IPv4, IPv6) done in network layer is called logical addressing.
4. Every computer in a network has a unique IP addressing
5. IP address is assigned to each data packet to ensure that data can reach the correct destination.
6. Routing is a method of moving the data packets from source to destination and it is based on the logical address format of IPv4 or IPv6.
7. Based on IP address and Mask routing decisions are made in a computer.

* Path Determination

A computer can be connected to internet server for a computer in a number of ways. Choosing the best delivery path for the data delivery from source to destination.

* Protocols used
* OSPF (Open Shortest path first border)
* BGP (Boarder Gateway protocol)
* IS-IS (Intermediate System To Intermediate)

These are the protocols to determine the best path for data delivery.