

Module 2 - Computer Networking

After going through this module, students will be able to

- Understand basic computer network technology
- Understand and configure server environment and backup services
- Configure different protocol services
- Install and configure linux server environment
- Install & configure the different types of network devices in a network
- Configure and manage network security
- Configure and perform remote accessing and routing
- Familiarize with Internet and E-Commerce sites

Understand basic computer network technology

In this section, we will discuss:

- Introduction to networks
- Type of area networks - LAN, VLAN, CAN, MAN, WAN
- Internet and Intranet etc.
- Uses and benefits of Network
- Server-client based network,
- peer to peer networks
- Network Interface Card
- Transmission Media and Topologies Media Type
- Crimping tools and Color standards for Straight crimping and Crosscirmpling

Introduction to Networks

What is a Computer Network?

- A computer network is a set of computers connected together for the purpose of sharing resources.
- The term network originated during the mid of the 1960s in the Department of Defense in the United States.
- A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data.



Introduction to Networks

Characteristics of a Computer Network

- Share resources from one computer to another.
- Create files and store them in one computer, access those files from the other computer(s) connected over the network.



Introduction to Networks

Characteristics of a Computer Network(continued)

- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over the network.

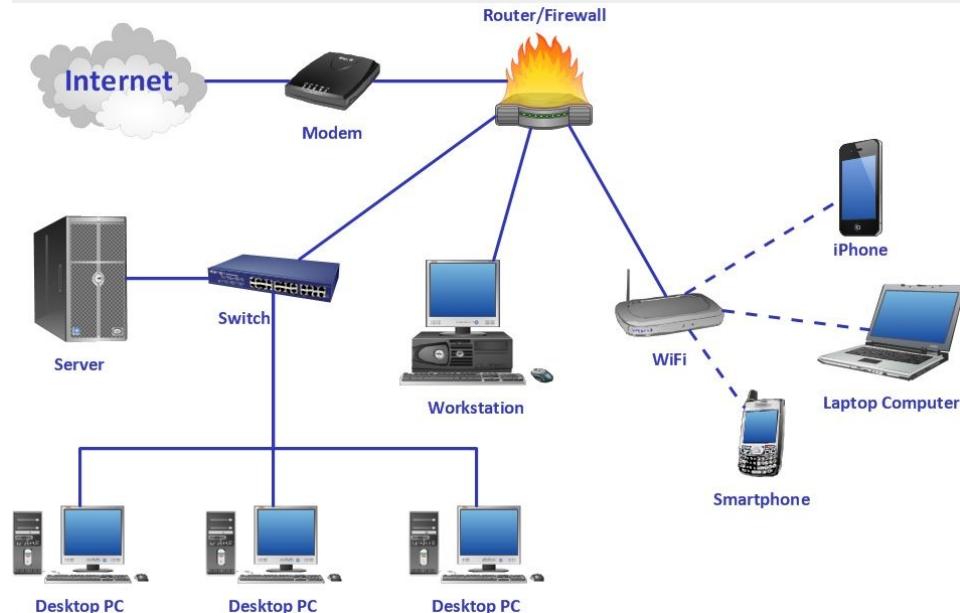


Introduction to Networks

Characteristics of a Computer Network(continued)

Devices required for computer Networking:

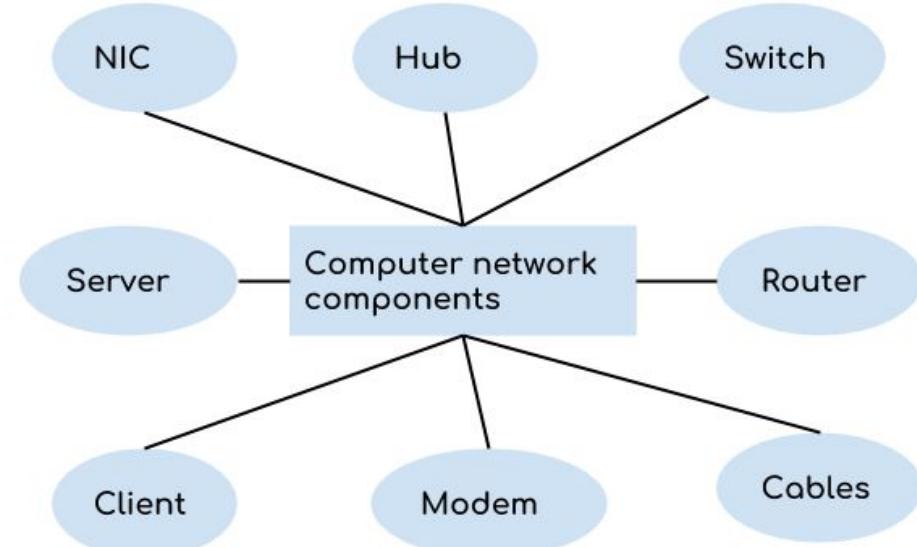
- Network Cables
- Distributors
- Routers
- Internal Network Cards
- External Network Cards



Introduction to Networks

Basics Components Of Computer Network

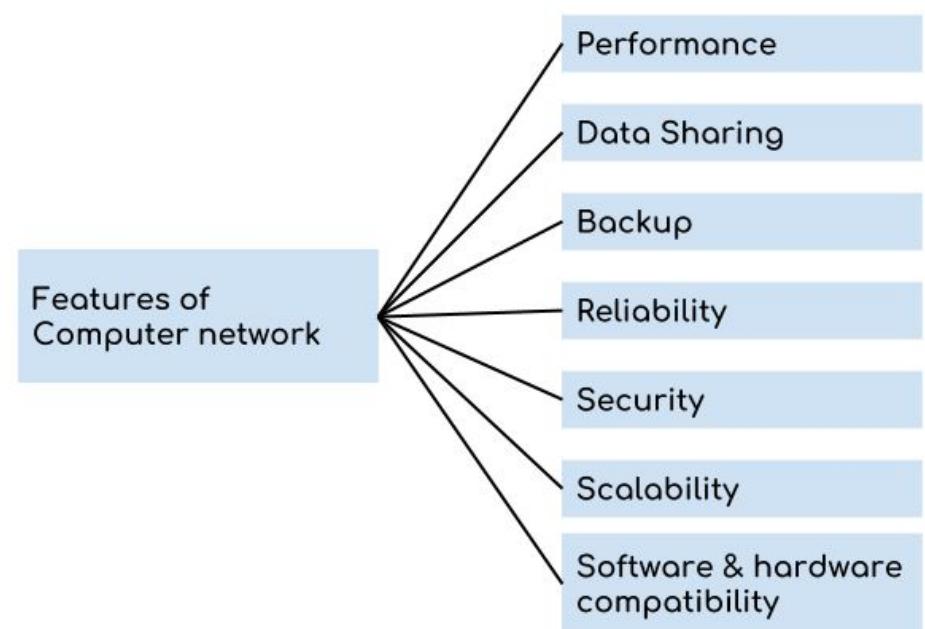
- Servers
- Clients
- Transmission Media
- Network Interface card
- Modem
- Hub
- Switch
- Cables and connectors
- Router
- LAN cable



Introduction to Networks

Features of a Computer Network

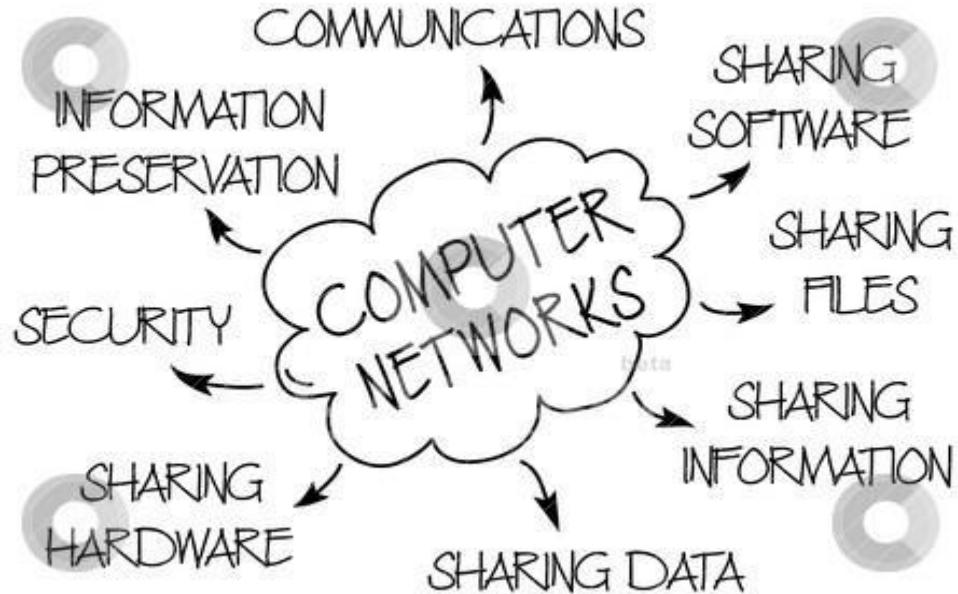
- Performance
- Data Sharing
- Backup
- Software and hardware compatibility
- Reliability
- Security
- Scalability



Introduction to Networks

Advantages of Computer Networks

- Workgroups
- Shared databases
- Distributed Systems
- Communications
- Device Sharing
- Software sharing
- Security



Introduction to Networks

Disadvantages of Computer Networks

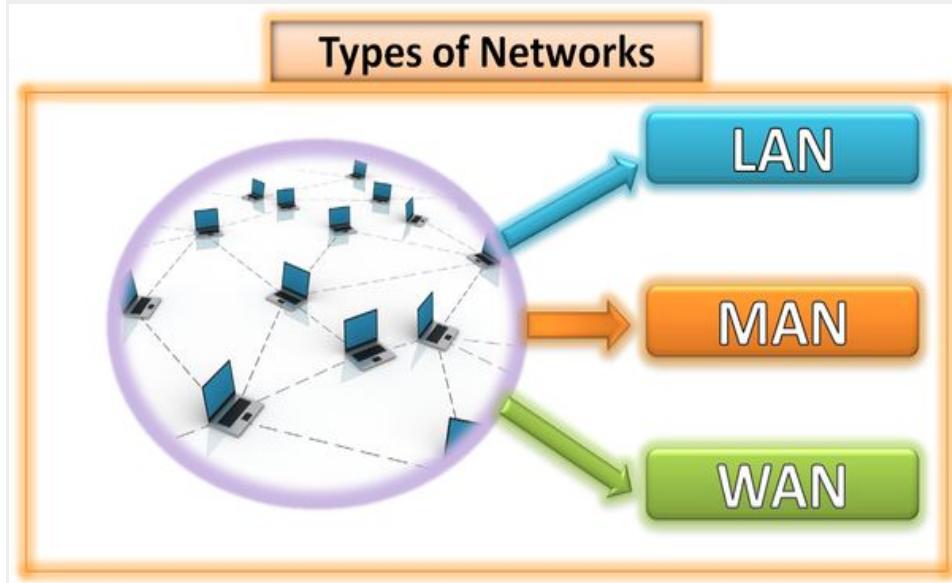
- Buying the computer cable and servers can be very expensive.
- Viruses can spread to other computers throughout a computer network.
- People can hack your computer.
- It encourages people to become dependent on computers.
- It comes with the risk of security issues.



Area Networks

Type of Area Networks

- LAN
- MAN
- WAN
- VLAN
- WLAN
- VPN
- CAN
- SAN
- SHAN
- PAN



Type of Area Networks

LAN(Local Area Network)

- Group of interconnected computers within a small area. (room, building, campus)
- Two or more pc's can from a LAN to share files, folders, printers, applications and other devices
- Coaxial or CAT 5 cables are normally used for connections.

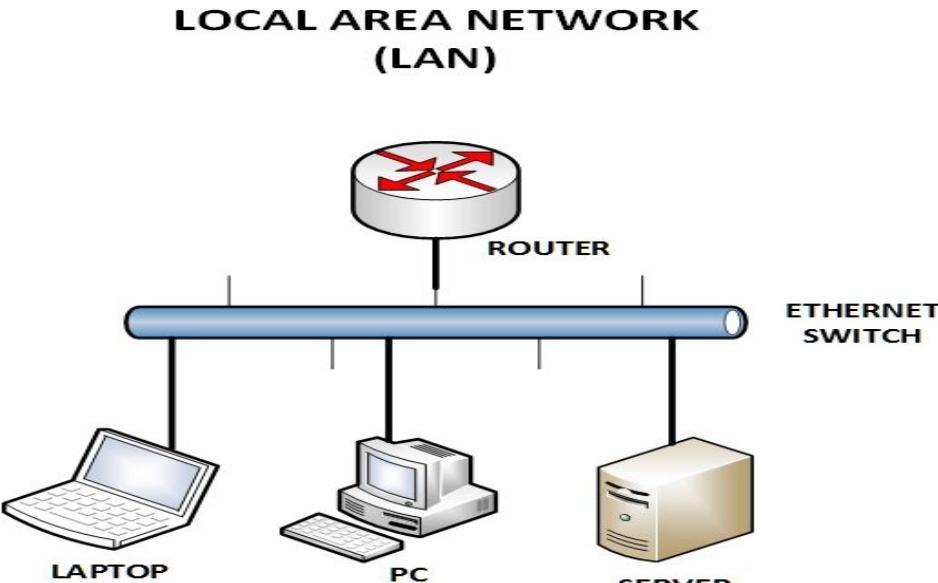


Type of Area Networks

LAN(Local Area Network)(continued)

- Due to short distances, errors and noise are minimum.
- Local Area Network provides higher security.
- Data transfer rate is 10 to 100 mbps.

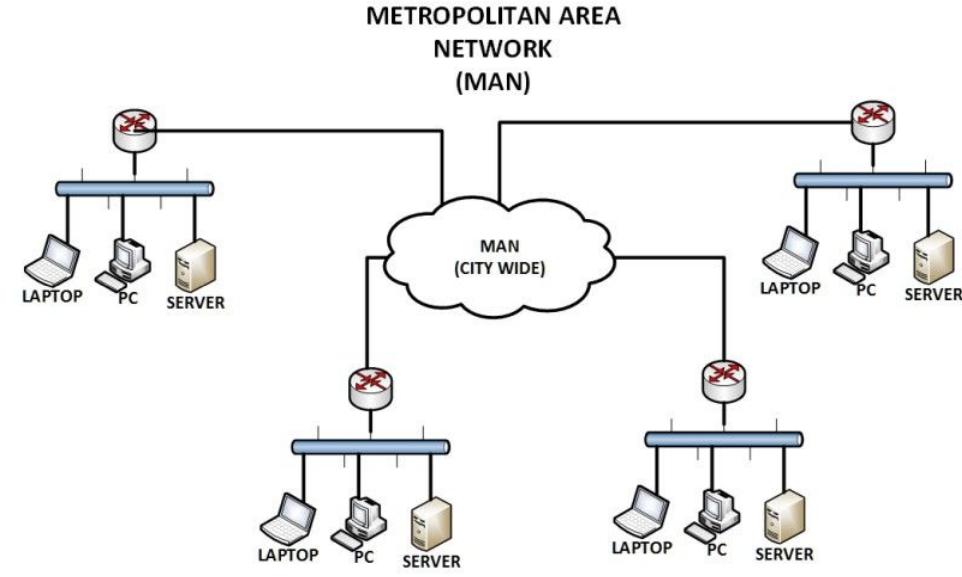
Example: A computer lab in a school



Type of Area Networks

MAN(Metropolitan Area Network)

- Design to extend over a large area.
- Connecting number of LAN's to form larger network, so that resources can be shared.
- Government agencies use MAN to connect to the citizens and private industries

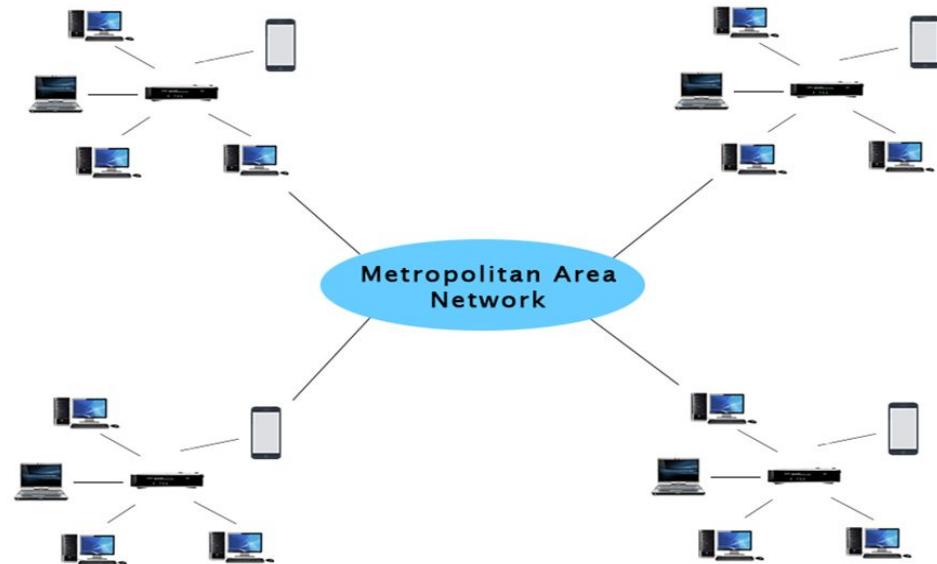


Type of Area Networks

MAN(Metropolitan Area Network)(continued)

- In MAN, various LANs are connected to each other through a telephone exchange line.
- Networks can be up to 5 to 50 km.
- Data transfer rate is low compared to LAN.

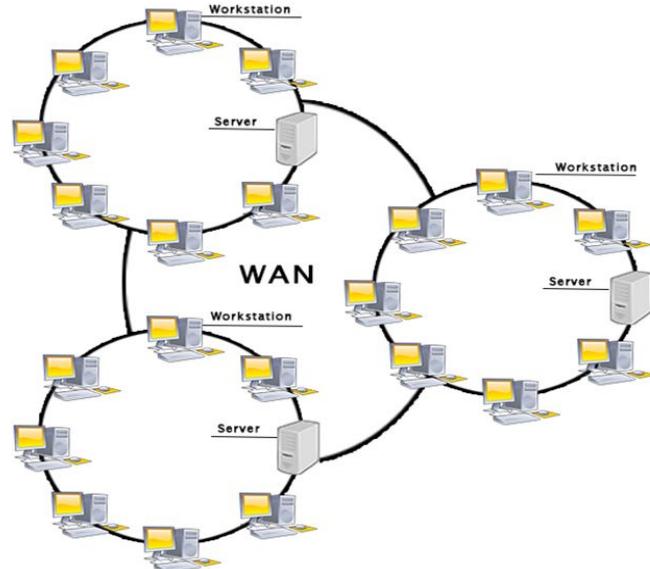
Example: Organization with different branches located in the city.



Type of Area Networks

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- Contains multiple LAN's and MAN's.
- A Wide Area Network is quite bigger network than the LAN.

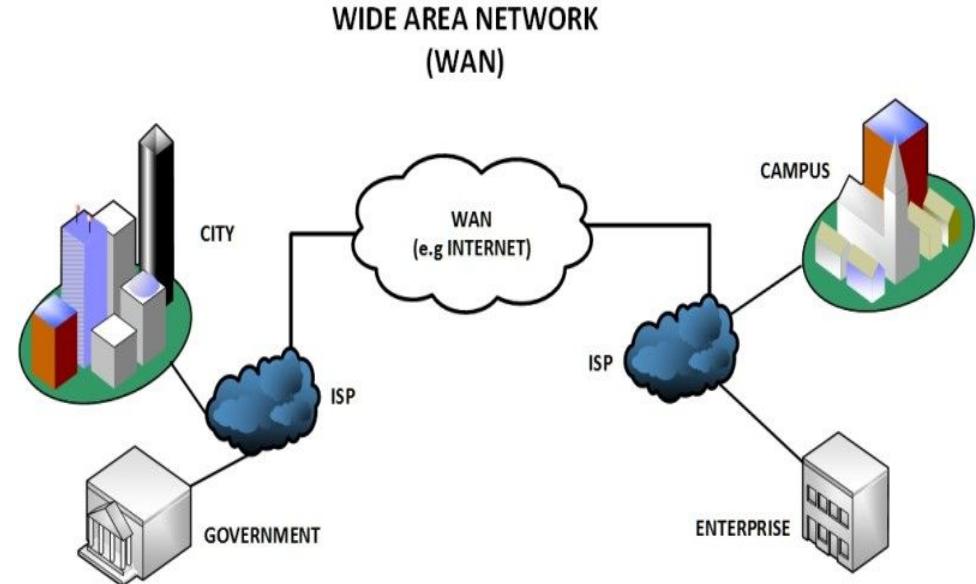


Type of Area Networks

WAN(Wide Area Network)(continued)

- Distinguished in terms of geographical range.
- Data transfer rate depends upon the ISP provider and varies over the location.

Example:Internet



Type of Area Networks

WLAN(Wireless Local Area Network)

- A WLAN makes use of a Wireless Access Point (WAP) device, which serves as the point of connectivity for wireless clients on the network.
- A LAN that uses high frequency radio waves for communication.
- Provides short range connectivity with high speed data transmission

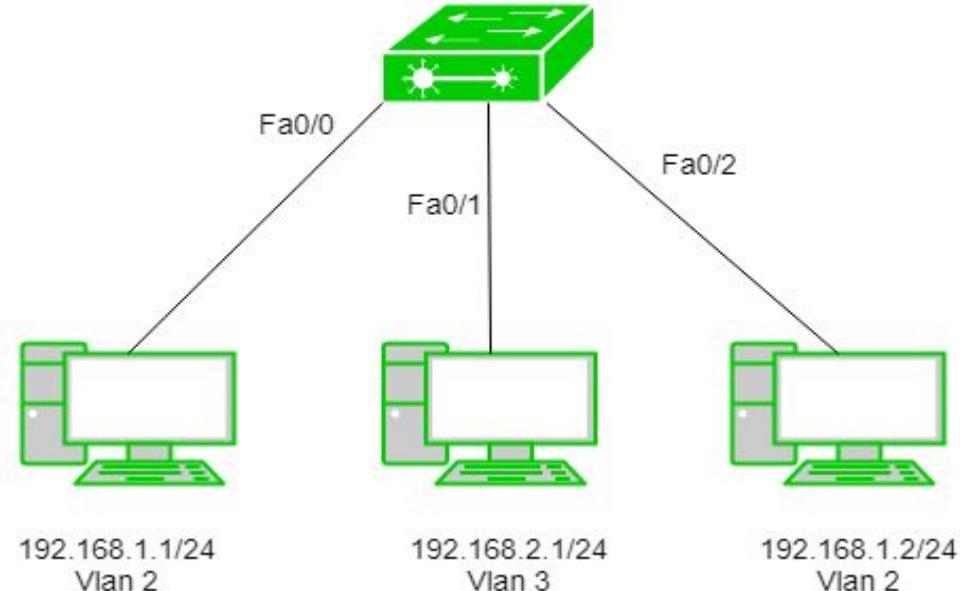
WIRELESS LOCAL AREA NETWORK (W-LAN)



Type of Area Networks

VLAN(Virtual Local Area Network)

- Virtual Local Area Networks (VLANs) divide a single existing physical network into multiple logical networks.
- Thereby, each VLAN forms its own broadcast domain.



Type of Area Networks

VLAN(Virtual Local Area Network)(continued)

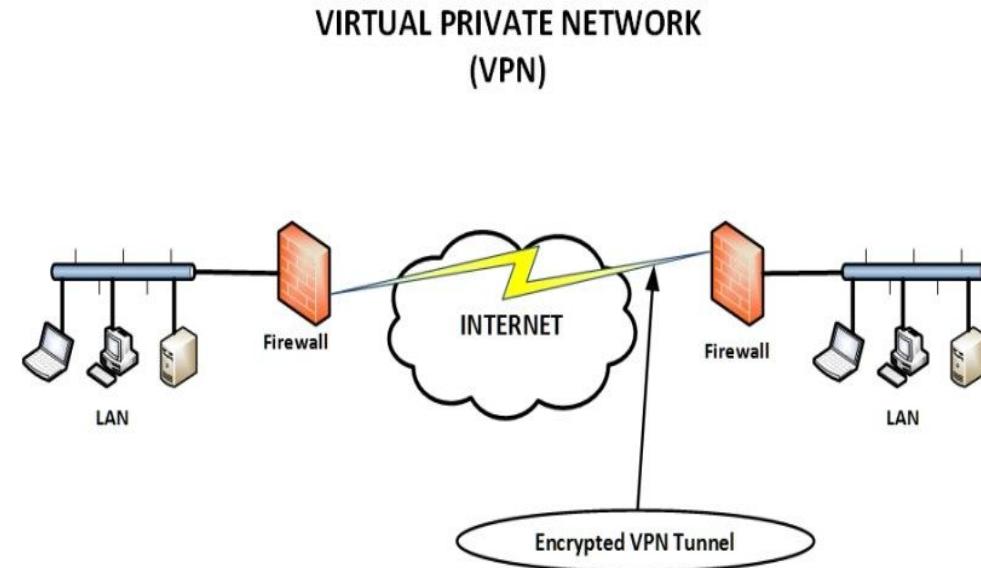
- Communication between two different VLANs is only possible through a router that has been connected to both VLANs.
- VLANs behave as if they had been constructed using switches that are independent of each other.



Type of Area Networks

VPN(Virtual Private Network)

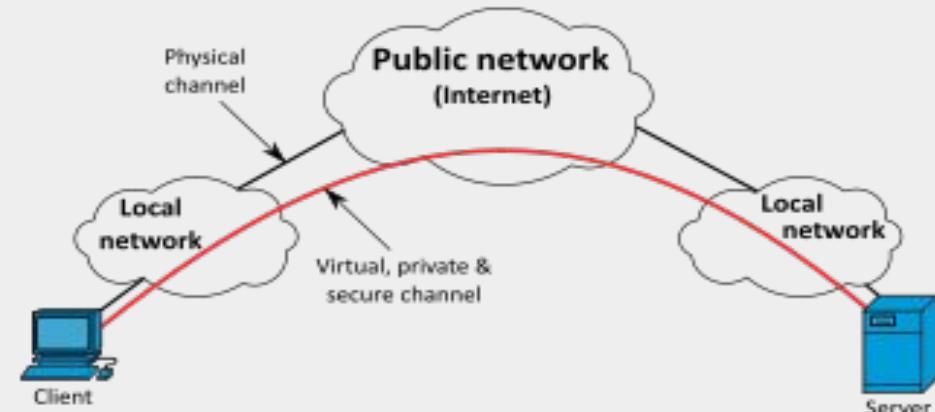
- A Virtual Private Network is a type of network that makes use of existing private or public network infrastructure (e.g the Internet) to provide a secure network connection.
- This is often achieved by creating an encrypted tunnel for secured end-to-end connectivity.



Type of Area Networks

VPN(Virtual Private Network)(continued)

- A Virtual Private Network uses data encryption techniques to provide security for files that are sent or received over the network.
- This is often used by organizations that have highly sensitive data to transfer.

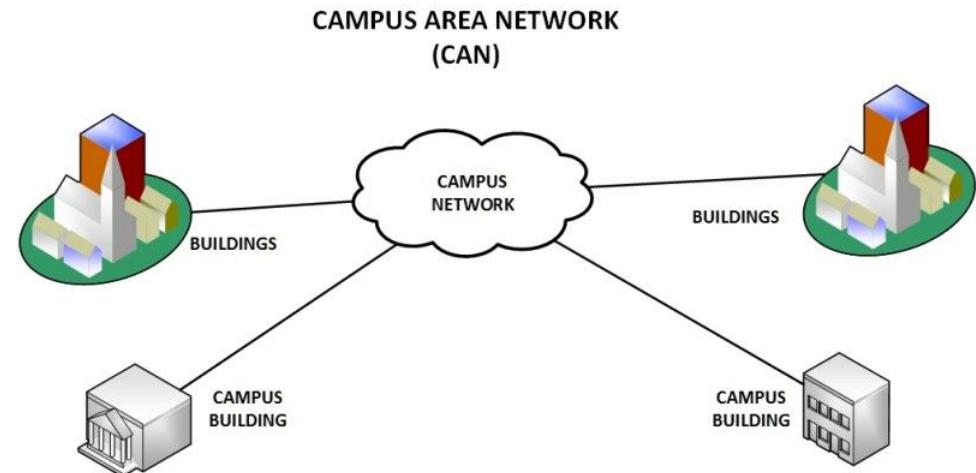


Type of Area Networks

CAN(Campus Area Network)

- A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area.
- CAN is smaller than WAN (Wide Area Network)
- CAN is also known as a controller area network.

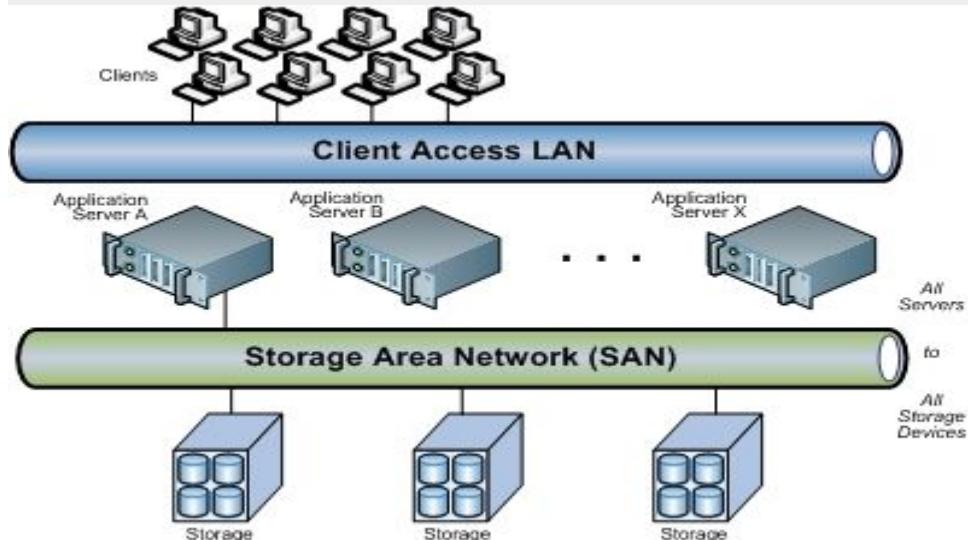
Example:Network in university



Type of Area Networks

SAN(Storage Area Network)

A Storage Area Network (SAN) is a specialized, high-speed network that provides block-level network access to storage. Connects servers to data storage devices via fiber-optic cables.

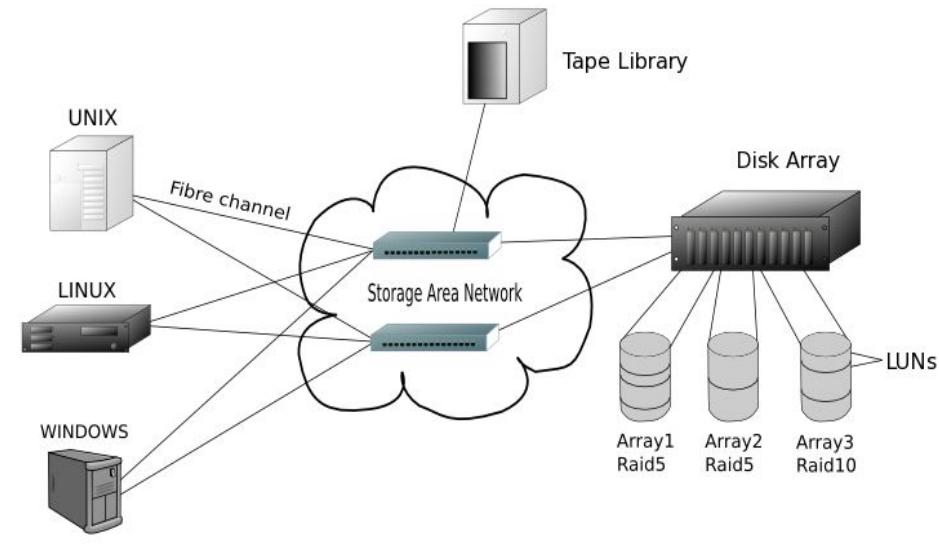


Type of Area Networks

SAN(Storage Area Network)(continued)

- SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols.

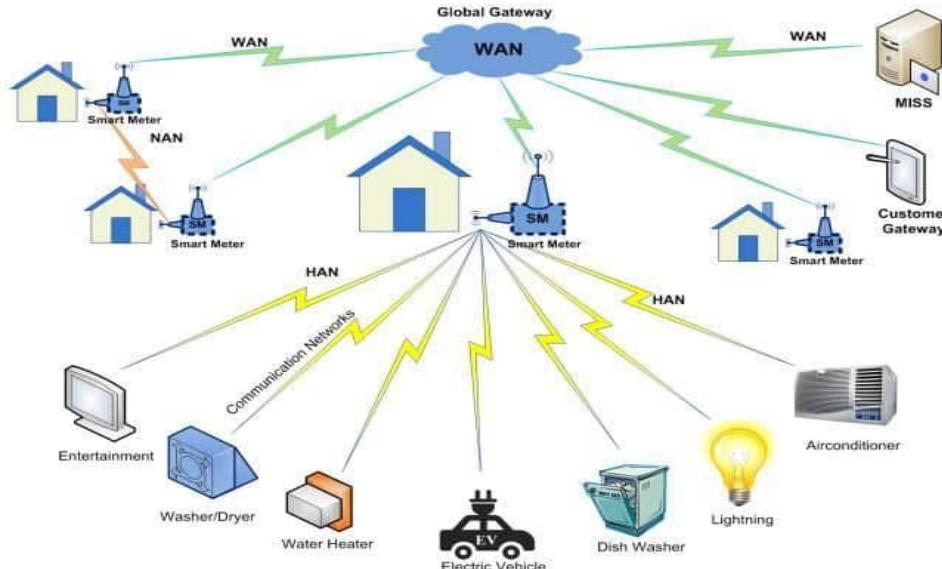
Example: Used for daily backup of organization or a mirror copy



Type of Area Networks

SHAN(Smart Home Area Network)

- A home area network (HAN) is a network contained within a user's home that connects a person's digital devices, from multiple computers and their peripheral devices to telephones, VCRs, televisions, video games, home security systems, smart appliances, fax machines and other digital devices that are wired into the network.
- The SHAN network generally used in homes and office space.

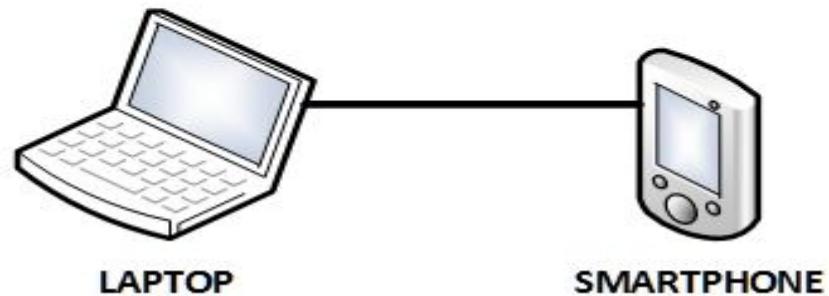


Type of Area Networks

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.

PERSONAL AREA NETWORK (PAN)



Type of Area Networks

PAN(Personal Area Network)(continued)

- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.
- Personal Area Network covers an area of 30 feet.



Internet and Intranet etc

Internet

- The Internet consists of a network of computers that anyone can access.
- Many intranets together make up the internet.
- It is a public network therefore anyone can access the internet.
- There is no limit to the number of users who can use the internet at any given time



ImageSource:

<https://spectrum.ieee.org/tech-talk/aerospace/satellites/facebook-may-have-secret-plans-to-launch-a-internet-satellite>

Internet and Intranet etc

Internet(continued)

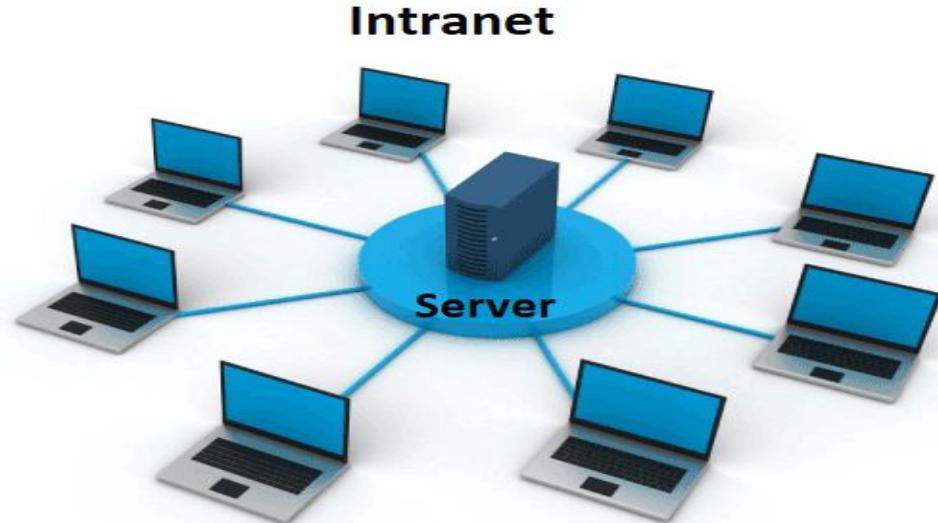
- There is no limit to the number of users who can use the internet at any given time



Internet and Intranet etc

Intranet(continued)

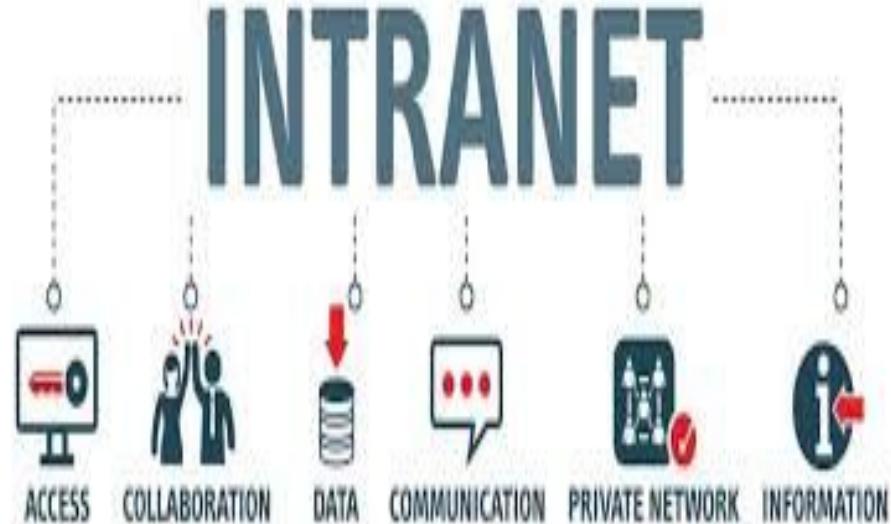
- An intranet is a smaller network of computers that allows access to a particular group of users.
- One can access the intranet from the internet. However, there are restrictions on the number of users.
- Only a specific few users can access the intranet.



Internet and Intranet etc

Intranet(continued)

- There are limitations on the volume of traffic at any given time.
- It is a private network therefore anyone can't access intranet.
- Intranet contains a specific kind of information only.

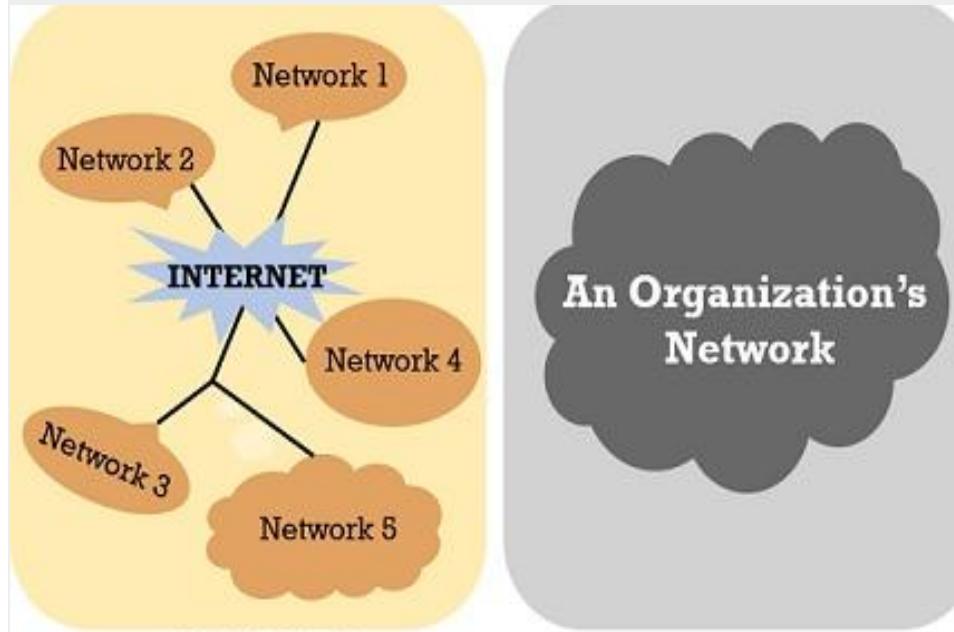


shutterstock.com • 1400185928

Internet and Intranet etc

Difference between Internet and Intranet

- The Internet is a wide network of computers that is available to all whereas Intranet is a network of computers designed for a certain group of users.
- Internet is a public network and Intranet is a private network.
- Number of internet users are very high but the number of users of Intranet is limited.



Internet and Intranet etc

Difference between Internet and Intranet(continued)

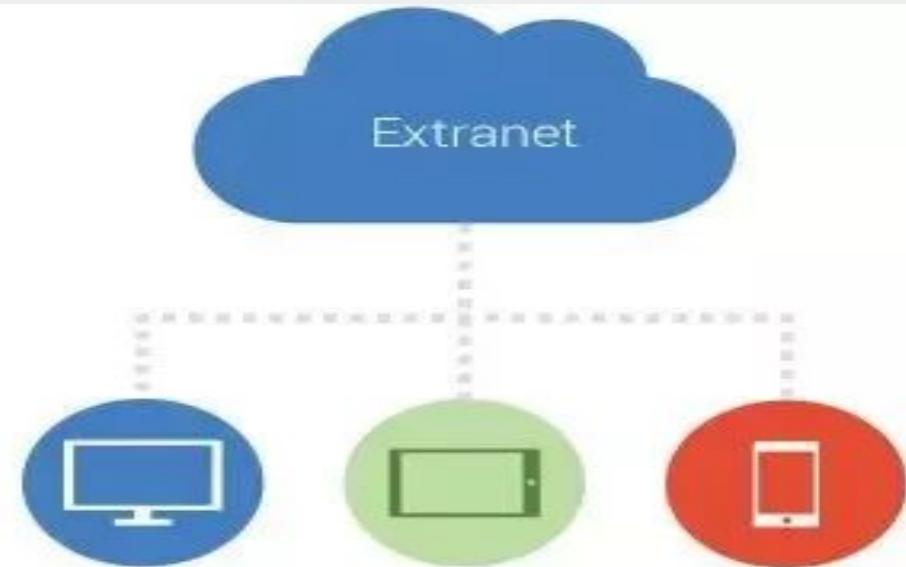
- Internet contains various source of information while Intranet only contains group-specific information.
- Anyone can access the internet while Intranet is accessible only by the organization employees or admin who have login details.

Internet	Intranet
The term ' Internet ' comes from the phrase International Network .	The term ' Intranet ' comes from the phrase Internal Restricted Access Network .
The internet is used to share data globally .	Intranets are used to share data locally and privately .
The internet is used to provide information that is relevant to a wide range of people.	Intranets are used to provide information which is relevant to a single company or organisation .
The internet can be accessed from anywhere as long as you have an internet connection.	Intranets can only be accessed from within the company or organisation that owns it.

Internet and Intranet etc

Extranet

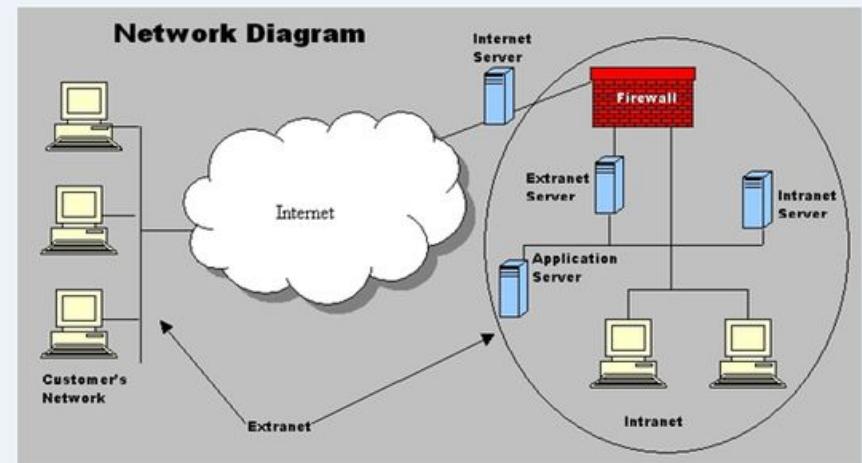
- An extranet is a communication network based on the internet protocol such as Transmission Control protocol and internet protocol.
- It is used for information sharing.
- The access to the extranet is restricted to only those users who have login credentials.



Internet and Intranet etc

Extranet(continued)

- An extranet is the lowest level of internetworking.
- An extranet cannot have a single LAN, atleast it must have one connection to the external network.



ImageSource:

<https://www.quora.com/What-is-the-difference-between-the-internet-intranet-and-extranet>

Uses and benefits of Network

- Increased speed and reduced cost
- File Sharing from one system to another.
- Remote access
- Hardware sharing like a printer, scanner, storage



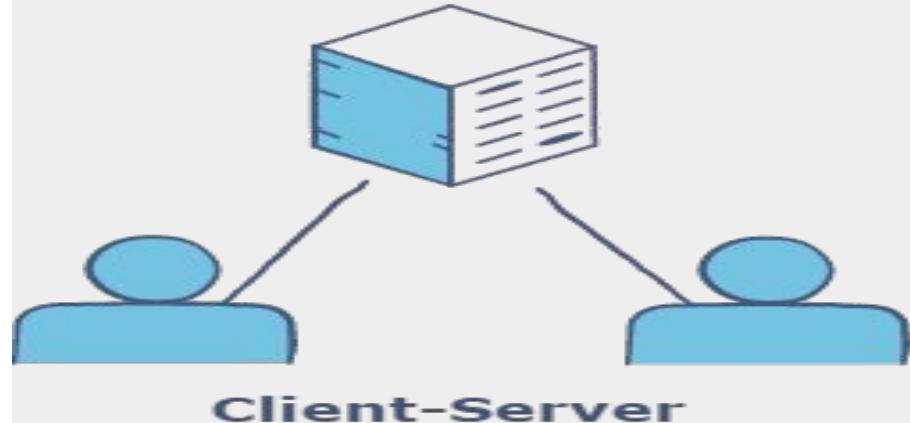
Uses and benefits of Network

- Communication i.e. instant messaging, video calls, mail communication etc.
- Online business
- Ease of administration
- Information security



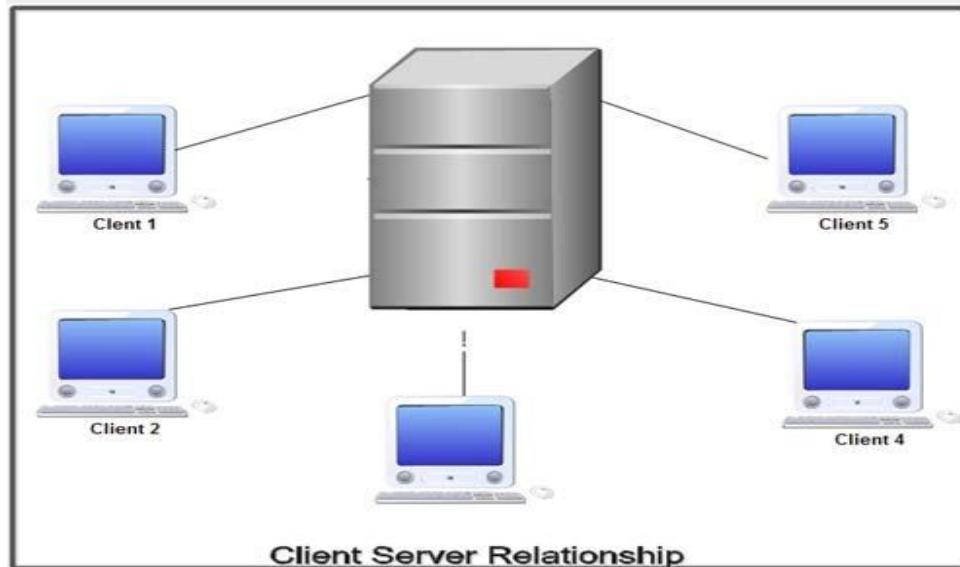
Server-client based Network

- A Computer networking model where one or more powerful computers (servers) provide the different computer network services and all other user of computer network (clients) access those services to perform user's tasks is known as client/server computer networking model.



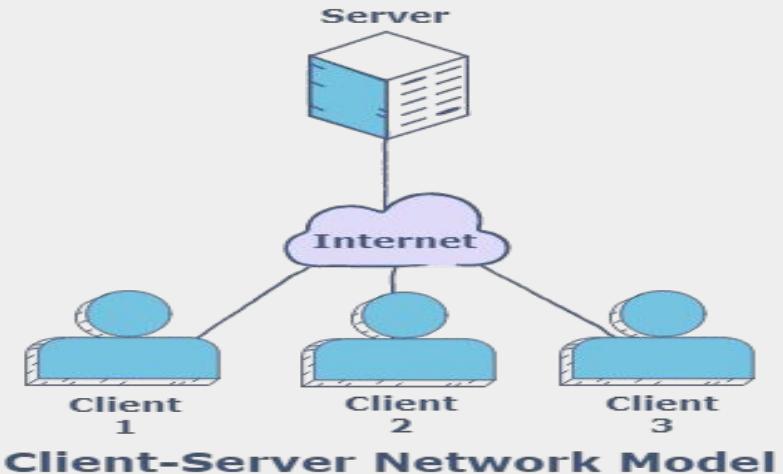
Server-client based Network

- In such networks, there exists a central controller called server. A server is a specialized computer that controls the network resources and provides services to other computers in the network.
- All other computers in the network are called clients.
- A client computer receives the requested services from a server.



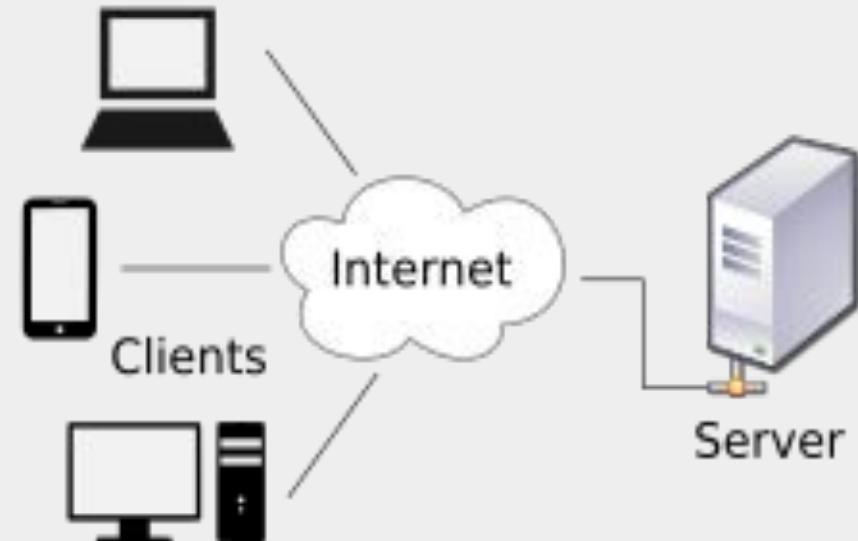
Server-client based Network

- A server performs all the major operations like security and network management.
- All the clients communicate with each other via centralized server
- If client 1 wants to send data to client 2, it first sends request to server to seek permission for it. The server then sends a signal to client 1 allowing it to initiate the communication.



Server-client based Network

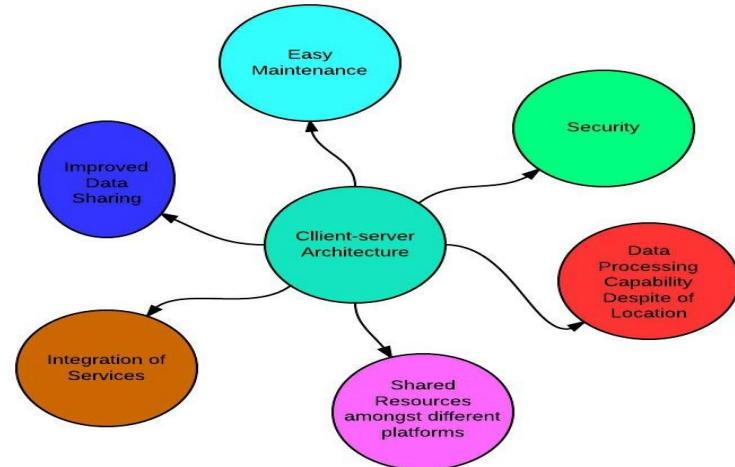
- A server is also responsible for managing all the network resources such as files, directories, applications & shared devices like printer etc.
- If any of the clients wants to access these services, it first seeks permission from the server by sending a request.



Server-client based Network

Advantages of Client Server Networks

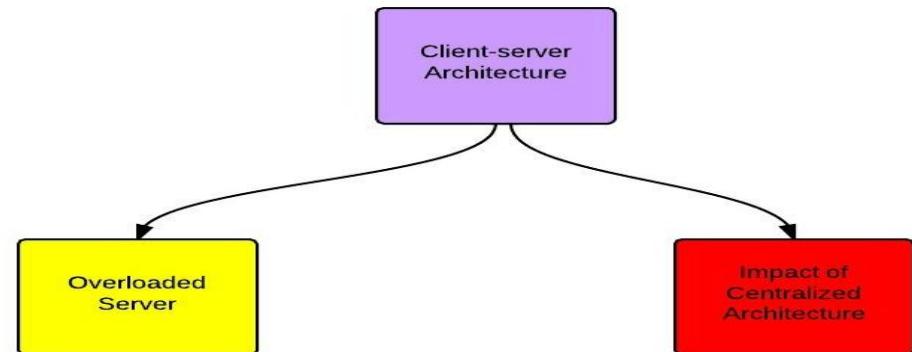
- Centralized backup is possible.
- Use of dedicated server improves the performance of whole system.
- Security is better in these networks as all the shared resources are centrally administered.
- Use of dedicated servers also increases the speed of sharing resources.



Server-client based Network

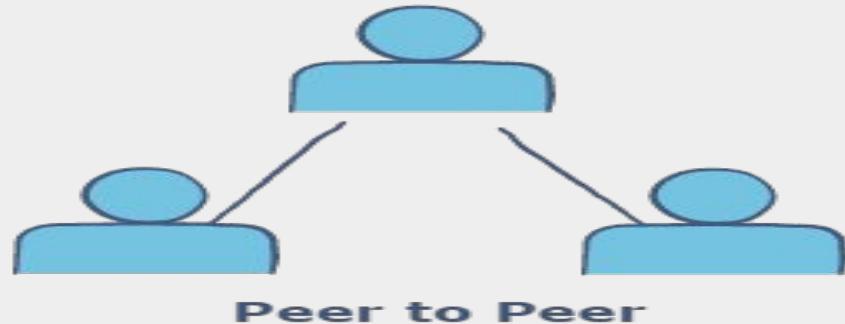
Disadvantages of Client Server Networks

- It requires specialized servers with large memory and secondary storage. This leads to increase in the cost.
- The cost of network operating system that manages the various clients is also high.
- It requires dedicated network administrator.



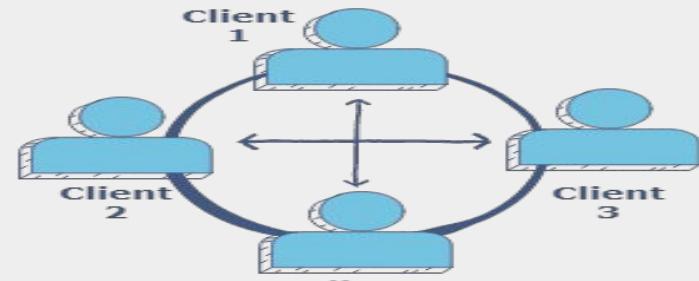
Peer to peer Networks

- In the peer to peer computer network model we simply use the same Workgroup for all the computers and a unique name for each computer in a computer network.
- There is no master or controller or central server in this computer network and computers join hands to share files, printers and Internet access.
- Peer to peer relationship is suitable for small networks having less than 10 computers on a single LAN.



Peer to peer Networks

- It is practical for workgroups of a dozen or less computers making it common environments, where each PC acts as an independent workstation and maintaining its own security that stores data on its own disk but which can share it with all other PCs on the network.
- Software for peer-to-peer network is included with most modern desktop operating systems such as Windows and Mac OS.

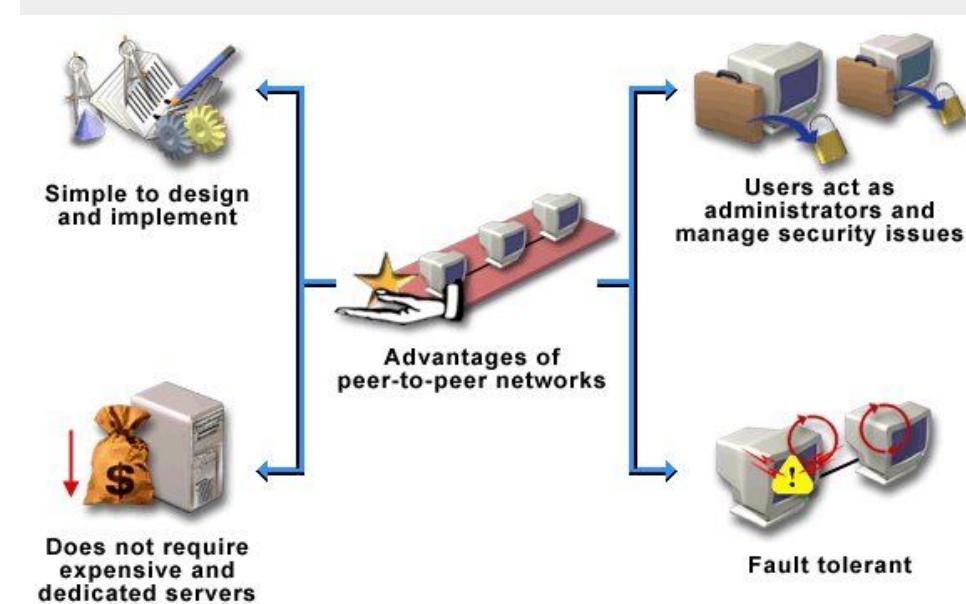


Peer-to-Peer Network Model

Peer to peer Networks

Advantages of Peer to Peer Networks

- Such networks are easy to set up and maintain as each computer manages itself.
- It eliminates extra cost required in setting up the server.
- Since each device is master of its own, they are not dependent on other computers for their operations.



Peer to peer Networks

Disadvantages of Peer to Peer Networks

- In peer-to-peer network, the absence of centralized server make it difficult to backup data as data is located on different workstations.
- Security is weak as each system manages itself only.
- There is no central point of data storage for file archiving.



Peer to peer Networks

Difference between Client-server and Peer to Peer Networks

- Both peer-to-peer and client-server networks connect computers so that they can share resources from one computer to others such as files, videos, and pictures.

Client/Server	Peer-To-Peer
Server has the control ability while clients don't	All computers have equal ability
Higher cabling cost	Cheaper cabling cost
It is used in small and large networks	Normally used in small networks with less than 10 computers
Easy to manage	Hard to manage
Install software only in the server while the clients share the software	Install software to every computer
One powerful computer acting as server	No server is needed

Network Interface Card

What is a Network Interface Card?

- A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network.
- It is also called Ethernet Card, interface controller, Lan Adapter or Network Adapter.



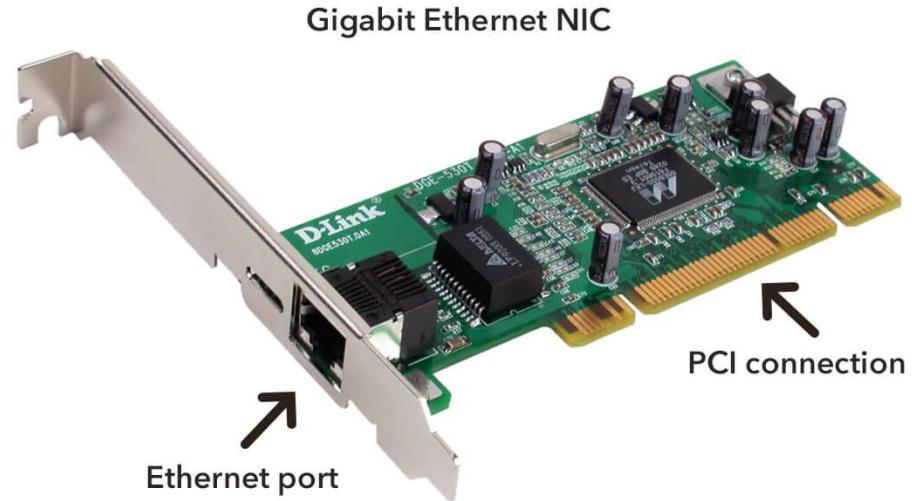
ImageSource:

<https://www.tttech.com/products/aerospace-space/development-test-vv/development-end-systems/tte-network-interface-cards/>

Network Interface Card

What is a Network Interface Card?(continued)

- It is a circuit board installed in a computer that provides a dedicated network connection to the computer.
- Every NIC has a 48-bit unique serial number called a MAC address which is stored in ROM carried on the card.
- NIC allows both wired and wireless communications

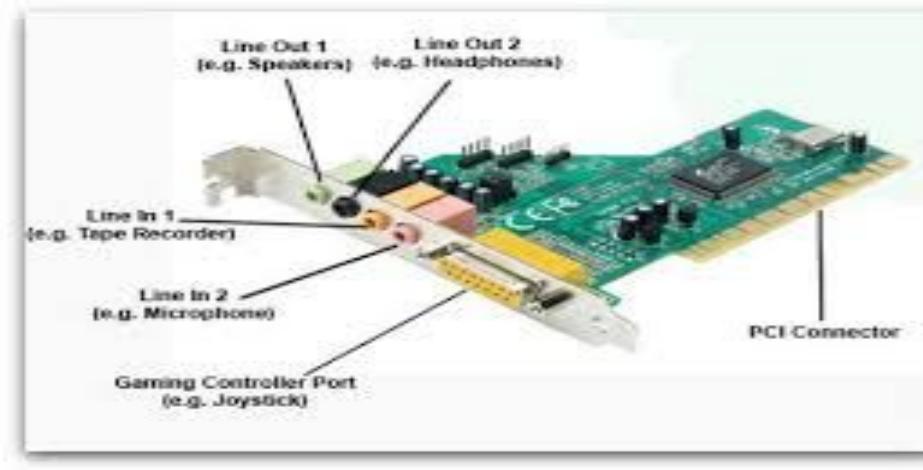


TechTerms.com

Network Interface Card

Components of NIC

- An external Memory is used to store the data temporarily and uses the stored data whenever required while processing the communication.
- Connectors are used to make the physical link between cables and plugin with the board, this type of connection is especially seen in Ethernet type of NIC cables.



Network Interface Card

Components of NIC(continued)

- A Processor converts the data message into a signal format for communication to take place easily.
- Different types of standard Buses are plugged into Buses Connector slots, based on the compatibility of the operation process buses are chosen.



Network Interface Card

Components of NIC(continued)

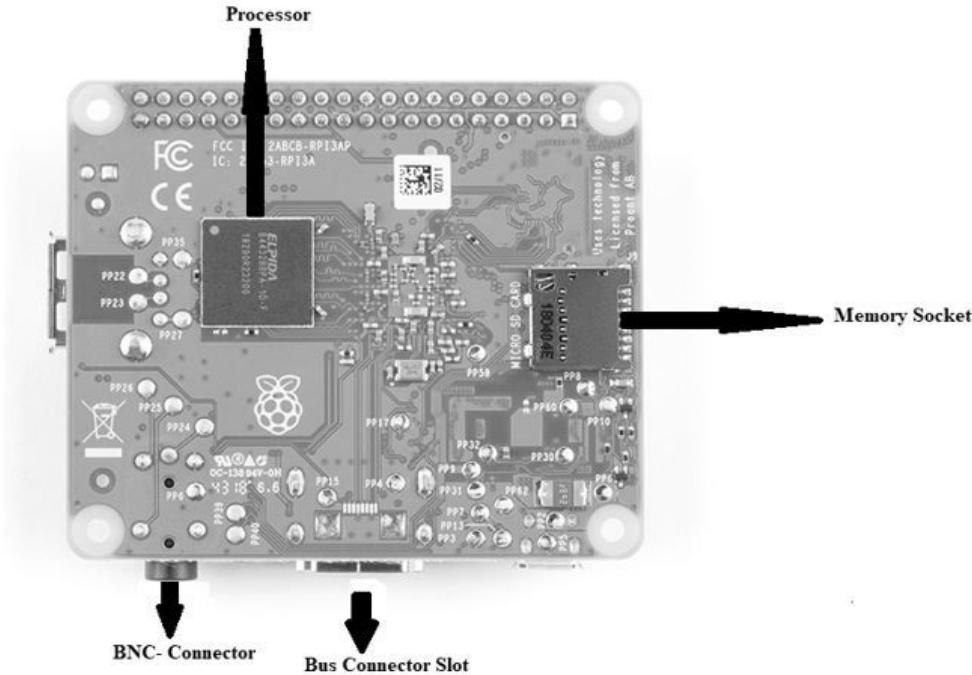
- Jumpers or Dual in package switches are used to control the communication operation, which is either by turning on or turning off the switch.
- A router is an NIC device that is used to connect wirelessly to the internet.



Network Interface Card

Components of NIC(continued)

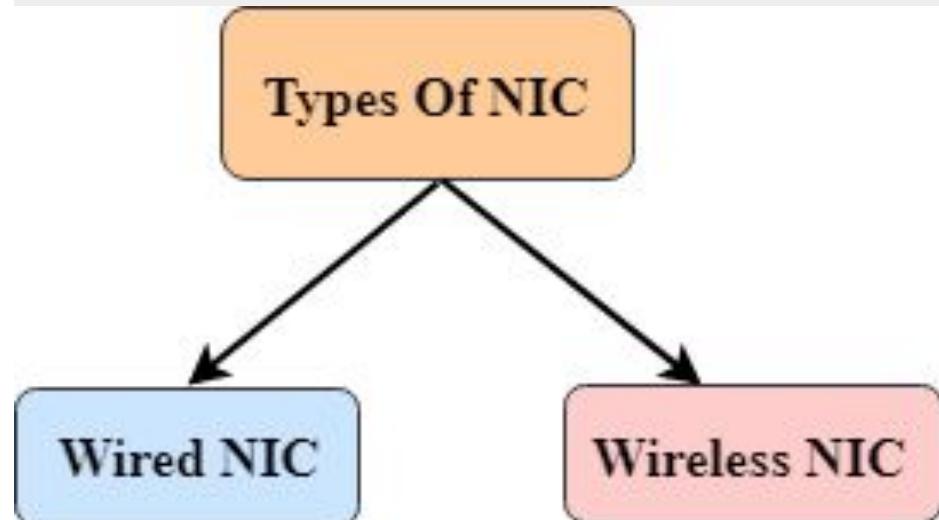
- MAC address which is a unique identity address is given to network interface card where ethernet packets are communicated with the computer.
- MAC address is also known as a physical network address.



Network Interface Card

Types of NIC Cards

- Wired
- Wireless
- USB



Network Interface Card

Types of NIC Cards(continued)

Wired

- These NIC have input jacks made of cables(Ethernet Cable).
- The motherboard has a slot for the network cards where they are inserted.
- The most widely used LAN technology is Ethernet.

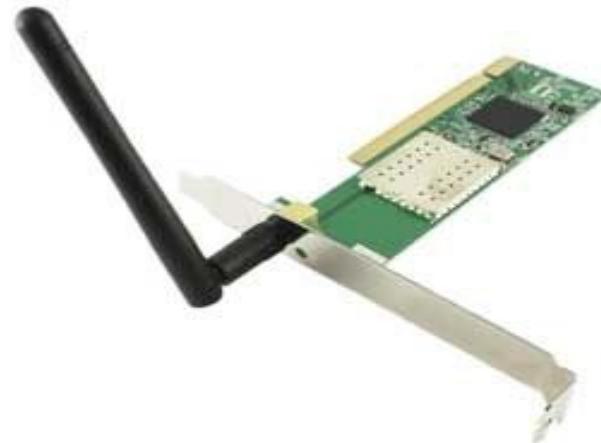


Network Interface Card

Types of NIC Cards(continued)

Wired

- Ethernet-based NIC is available in hardware shops.
- The speed of Ethernet-based NIC can be 10/100/1000 Mbps.



Network Interface Card

Types of NIC Cards(continued)

Wireless

- Wireless network cards are inserted into the motherboard but no network cables are required to connect the computer to the internet.
- These NICs are designed for Wi-Fi connections.



Network Interface Card

Types of NIC Cards(continued)

USB

- These are NICs that provide network connection over the device plugged in the USB port.



Network Interface Card

Advantages of NIC

- The communication speed using the Internet is high usually in Gigabytes
- Highly reliable connection
- Many peripheral devices can be connected using many ports of NIC cards.
- Bulk data can be shared among many users.



Network Interface Card

Disadvantages of NIC

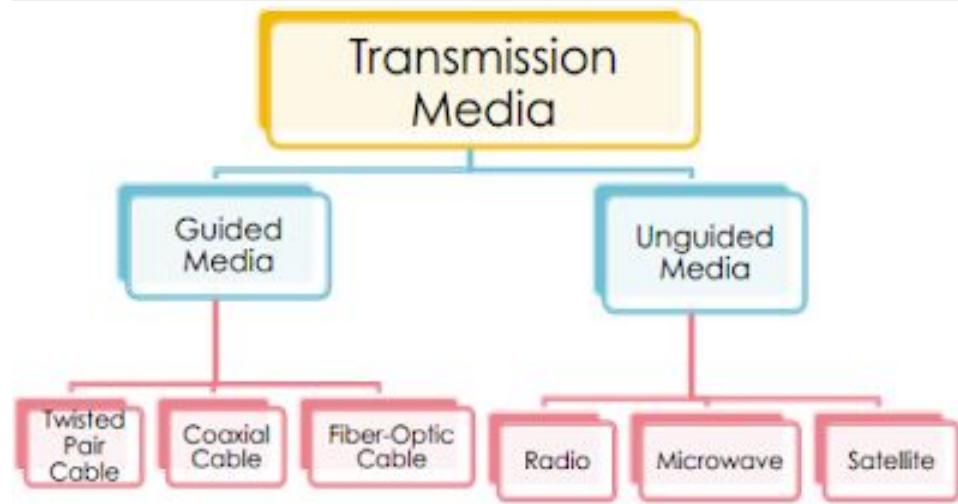
- Inconvenient in case of wired cable NIC, as it is not portable like a wireless router
- The configuration should be proper for better communication.
- Data is unsecured.



Transmission Media and Topologies Media Type

What is Transmission Media?

- A communication channel that is used to carry the data from the transmitter to the receiver through the electromagnetic signals.
- The main function of this is to carry the data in the bits form through the Local Area Network (LAN). In data communication, it works like a physical path between the sender & the receiver.



Transmission Media and Topologies Media Type

Types of Transmission Media

- Physical transmission media/Guided media/Wired
- Wireless transmission media/Unguided media/Wireless



Crimping tools and Color standards for Straight crimping and Crosscrimping

Crimping Tools

- A crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them in a way that causes them to hold each other. The result of the tool's work is called a crimp.

RJ-11 (6-Pin) and RJ-45 (8-Pin) Crimping Tool



ComputerHope.com

Crimping tools and Color standards for Straight crimping and Crosscrimping

Crimping Tools(continued)

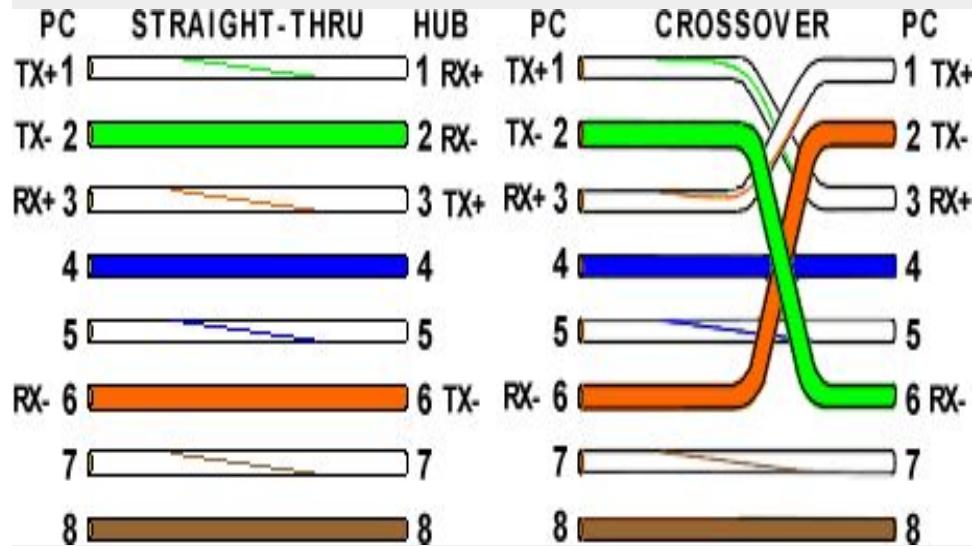
- For instance, network cables and phone cables are created using a crimping tool (shown below) to join the RJ-45 and RJ-11 connectors to both ends of either phone or Cat 5 cable.



Crimping tools and Color standards for Straight crimping and Crosscrimping

Ethernet Cable Color

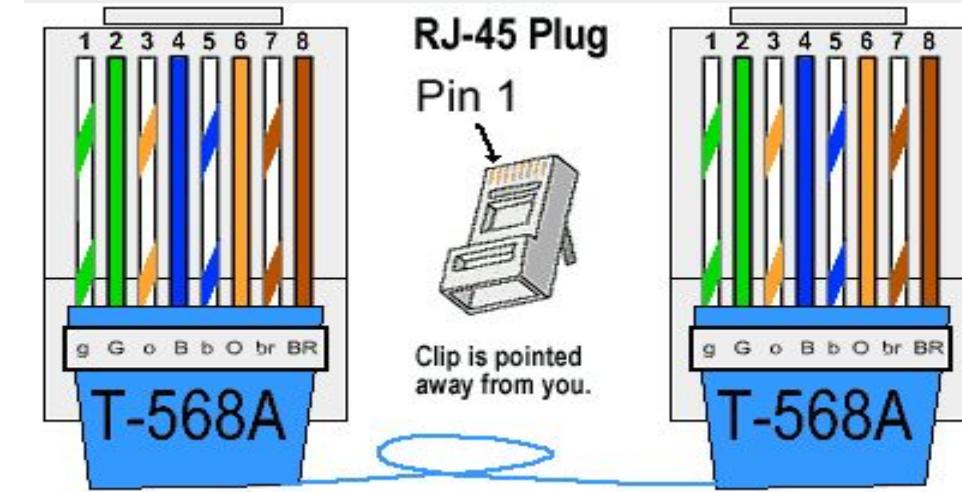
- A straight-thru is used as a patch cord in Ethernet connections.
- A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs.
- A crossover has one end with the Orange set of wires switched with the Green set.



Crimping tools and Color standards for Straight crimping and Crosscrimping

T-568A Straight-Through Ethernet Cable

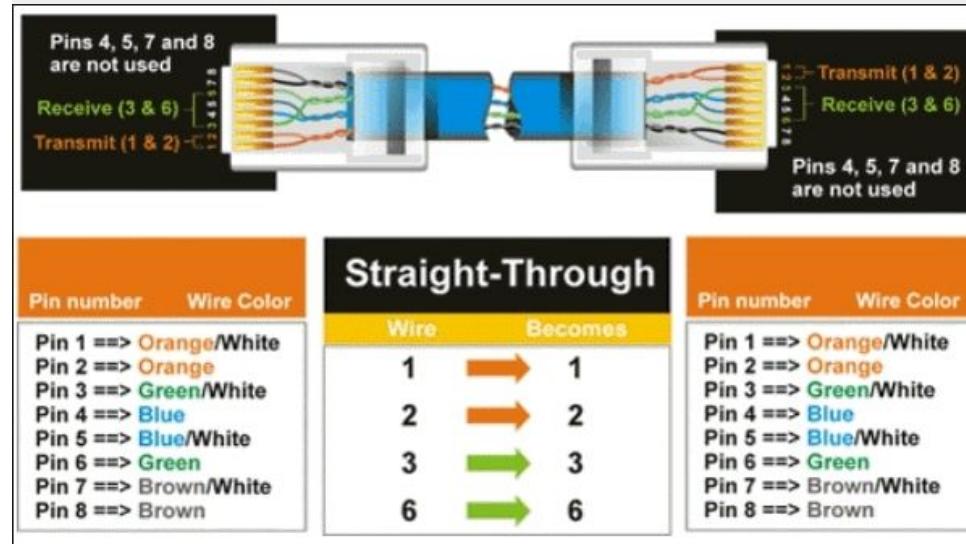
- The TIA/EIA 568-A standard which was ratified in 1995, was replaced by the TIA/EIA 568-B standard in 2002 and has been updated since.
- Both standards define the T-568A and T-568B pin-outs for using Unshielded Twisted Pair cable and RJ-45 connectors for Ethernet connectivity.



Crimping tools and Color standards for Straight crimping and Crosscrimping

T-568A Straight-Through Ethernet Cable(continued)

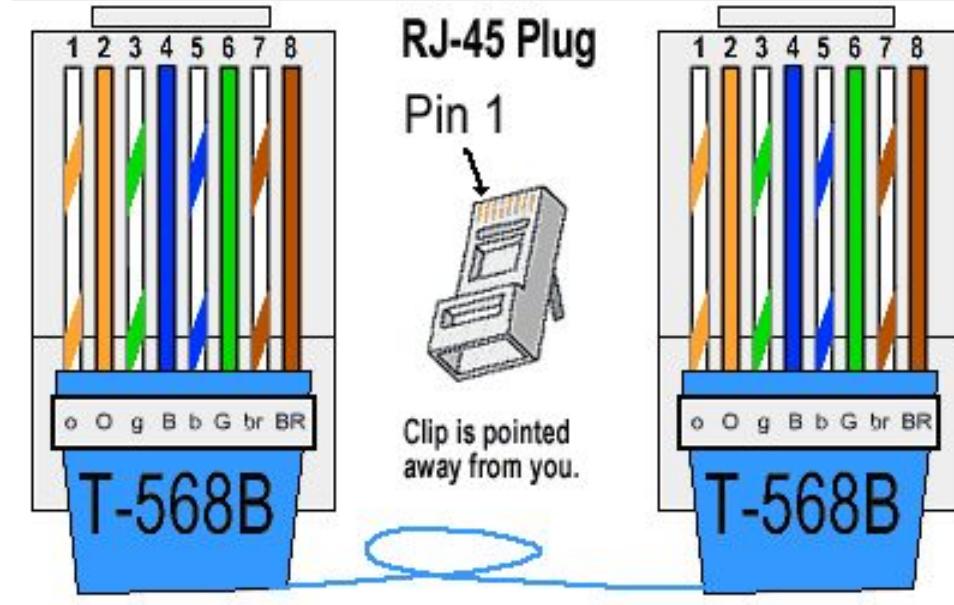
- The standards and pinout specification appear to be related and interchangeable, but are not the same and should not be used interchangeably.



Crimping tools and Color standards for Straight crimping and Crosscrimping

T-568B Straight-Through Ethernet Cable

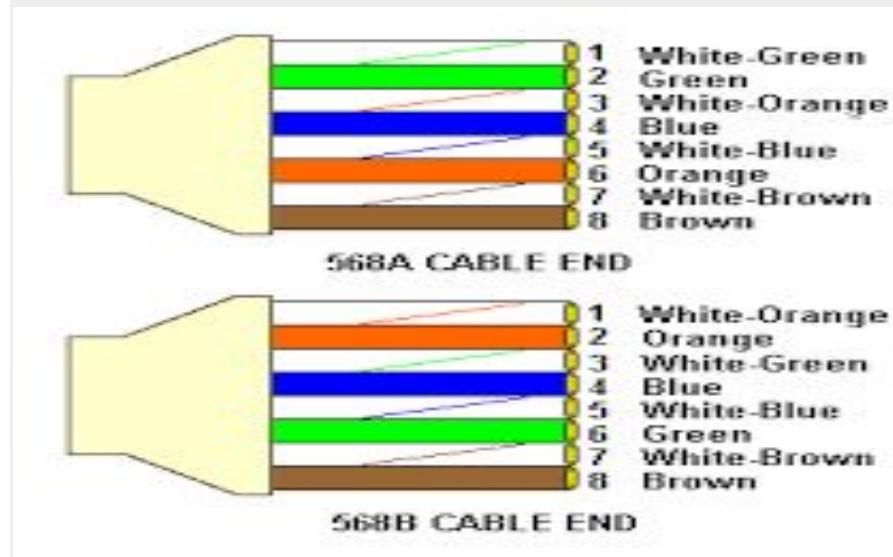
- Both the T-568A and the T-568B standard Straight-Through cables are used most often as patch cords for your Ethernet connections.



Crimping tools and Color standards for Straight crimping and Crosscrimping

T-568B Straight-Through Ethernet Cable(continued)

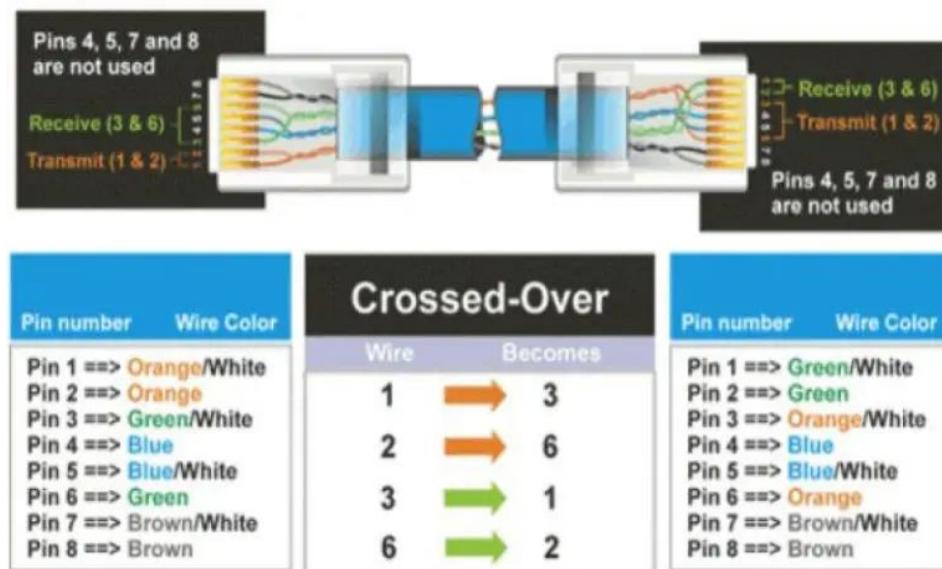
- If user require a cable to connect two Ethernet devices directly together without a hub or when you connect two hubs together, you will need to use a Crossover cable alternative.



Crimping tools and Color standards for Straight crimping and Crosscrimping

RJ-45 Crossover Ethernet Cable

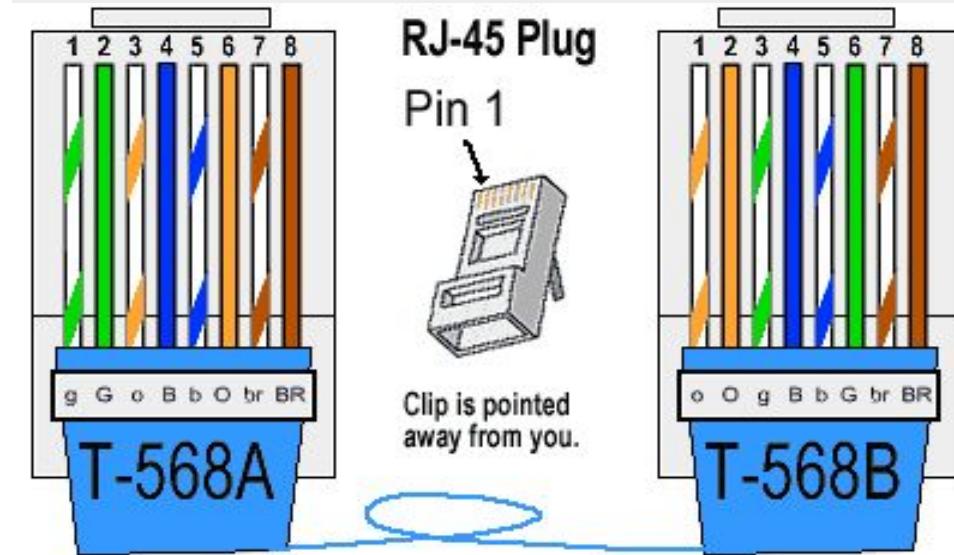
- A good way of remembering how to wire a Crossover Ethernet cable is to wire one end using the T-568A standard and the other end using the T-568B standard.



Crimping tools and Color standards for Straight crimping and Crosscrimping

RJ-45 Crossover Ethernet Cable

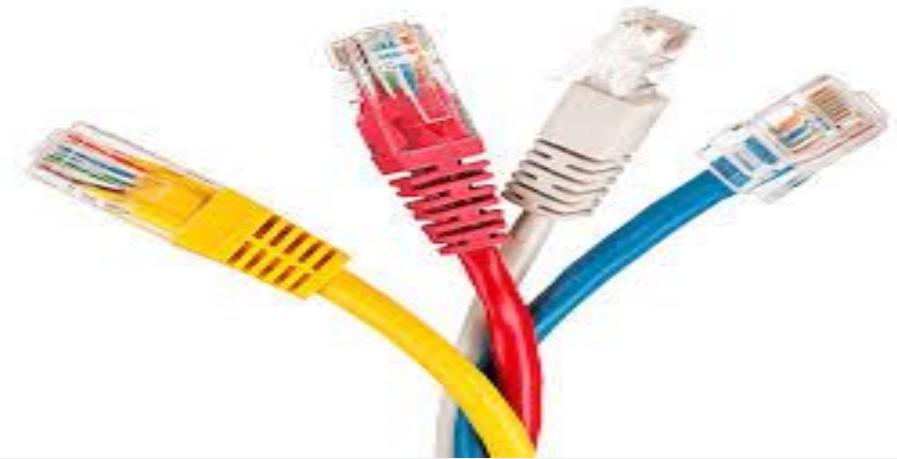
- Another way of remembering the color coding is to simply switch the Green set of wires in place with the Orange set of wires.
- Specifically, switch the solid Green (G) with the solid Orange, and switch the green/white with the orange/white.



Crimping tools and Color standards for Straight crimping and Crosscrimping

Ethernet Cable Instructions

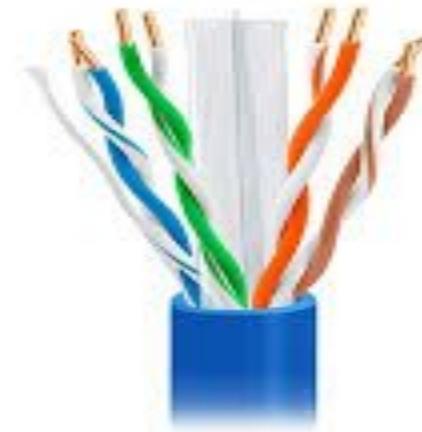
- Pull the cable off the reel to the desired length and cut. If you are pulling cables through holes, its easier to attach the RJ-45 plugs after the cable is pulled.



Crimping tools and Color standards for Straight crimping and Crosscirmpling

Ethernet Cable Instructions(continued)

- The total length of wire segments between a PC and a hub or between two PC's cannot exceed 100 Meters (328 feet) for 100BASE-TX and 300 Meters for 10BASE-T



Crimping tools and Color standards for Straight crimping and Crosscrimping

Ethernet Cable Instructions(continued)

- Start on one end and strip the cable jacket off (about 1") using a stripper or a knife. Be extra careful not to nick the wires, otherwise you will need to start over.



Crimping tools and Color standards for Straight crimping and Crosscrimping

Ethernet Cable Instructions(continued)

- Spread, untwist the pairs, and arrange the wires in the order of the desired cable end. Flatten the end between your thumb and forefinger. Trim the ends of the wires so they are even with one another, leaving only 1/2" in wire length.



Crimping tools and Color standards for Straight crimping and Crosscrimping

Ethernet Cable Instructions(continued)

- If it is longer than 1/2" it will be out-of-spec and susceptible to crosstalk. Flatten and insure there are no spaces between wires.
- Hold the RJ-45 plug with the clip facing down or away from you. Push the wires firmly into the plug.



Crimping tools and Color standards for Straight crimping and Crosscrimping

Ethernet Cable Instructions(continued)

- Inspect each wire is flat even at the front of the plug. Check the order of the wires. Double check again. Check that the jacket is fitted right against the stop of the plug. Carefully hold the wire and firmly crimp the RJ-45 with the crimper.



ImageSource:

<https://medium.com/@julydd/how-to-make-your-own-ethernet-cables-513d56470698>

Crimping tools and Color standards for Straight crimping and Crosscrimping

Ethernet Cable Instructions

- Check the color orientation, check that the crimped connection is not about to come apart, and check to see if the wires are flat against the front of the plug. If even one of these are incorrect, you will have to start over. Test the Ethernet cable.



Understand and configure server environment and backup services

In this section, we will discuss:

- Server
- client
- node
- segment
- backbone
- host
- Analog and Digital transmission
- STP cable
- UTP cable
- Coaxial cable
- Fiber cable

In this section, we will discuss:

- Base band and Broadband transmission
- Cables and Connectors
- Network Cable Crimping and troubleshooting
- Physical and logical topologies
- Bus topology
- Star topology,
- Ring topology
- Mesh topology
- Asynchronous Transmission
- Synchronous Transmission

Server

What is a Server

- A **server** is a type of computer or device on a network that manages network resources.
- **Servers** are often dedicated, meaning that they perform no other tasks besides their **server** tasks.
- On multiprocessing operating systems, however, a single computer can execute several programs at once.



Image Source:

https://sifuweb.com/wp-content/uploads/2020/02/shutterstock_571378933-compressed.jpg

Server

Characteristics and capabilities of the server

- Update hardware and software without a reboot or restart.
- Frequent backup of critical data
- Advanced networking performance
- Instinctive data transfer between devices
- High security for data



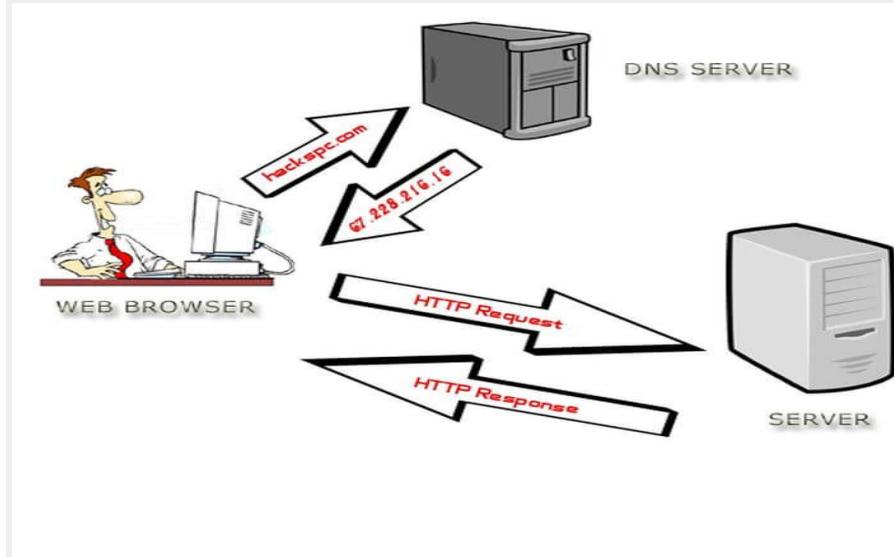
Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcRe4Bi-i0DhXP0YbGRP_Sc-G-TX2Y-C-uhk-12uL-Wf-PCi3-ucm-CAU

Server

How a server works?

- A **network server** is a computer system, which is used as the central repository of data and various programs that are shared by users in a **network**.
- If you have a computer that you're no longer using due to its slow speed, you can turn it into a **network server** for other computers in your household.



Server

Types of Servers

- File servers
- Print servers
- Application servers
- DNS servers
- Mail servers
- Web servers
- Database servers
- Virtual servers
- Proxy servers
- FTP servers

**How Many Types
Of Servers Are
There?**



Image Source:
<https://www.technotification.com/wp-content/uploads/2014/02/Untitled-1-1280x720.jpg>

Types of Server

File Server

- File servers store and distribute files.
- Multiple clients or users may share files stored on a server.
- In addition, centrally storing files offers easier backup or fault tolerance solutions than attempting to provide security and integrity for files on every device in an organization.
- File server hardware can be designed to maximize read and write speeds to improve performance.



Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcSK2P4dbJcgSnvv3lSCUJ2XC16AMtXNKx14d_K_ZJPDMoY4GM5J&usqp=CAU

Types of Server

Print Server

- Print servers allow for the management and distribution of printing functionality.
- Rather than attaching a printer to every workstation, a single print server can respond to printing requests from numerous clients.
- The internal print server also functions by responding to print requests from a client.



Image Source:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcRO6pj8TufL4rSCzwHvyRKazJzfTGHzgqN7ulj6v7pY8S9fmn&usqp=CAU>

Types of Server

Application Server

- Application servers run applications in lieu of client computers running applications locally.
- Application servers often run resource-intensive applications that are shared by a large number of users.
- It also removes the need to install and maintain software on many machines as opposed to only one.



ComputerHope.com

Image Source:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcS6qG6yjQLZrbHAU XKyJk69JdNXn4dMBNIlvCcfGyy3Xscclte0&usqp=CAU>

Types of Server

DNS Server

- A **DNS server** is any computer that is registered to join the **DNS**.
- It has an index of domain names and IP addresses, and when requested, it can tell you the current **IP address** associated with a domain name.
- If it doesn't know, then it will try to find out from other **DNS** servers.



Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcQlhd_gxqtpjXkW WKiGntnC2V8_nw_9nEUSqnpxFKSg0TCIqJh&usqp=CAU

Types of Server

Mail Server

- Mail servers are a very common type of application server.
- Mail servers receive emails sent to a user and store them until requested by a client on behalf of said user.
- Having an email server allows for a single machine to be properly configured and attached to the network at all times.
- It is then ready to send and receive messages rather than requiring every client machine to have its own email subsystem continuously running.



MAIL
SERVER



Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcTy-IL5r0K1kpZJuKmmh9e7ZQ_XcZZR5GM7mlgozFdnoAR_EjS&usqp=CAU

Types of Server

Web Server

- A **web server** is a computer that runs websites.
- The **basic** objective of the **web server** is to store, process and deliver **web** pages to the users.
- This intercommunication is done using Hypertext Transfer Protocol (**HTTP**).



Web Server

Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcQ9f8Oclax2yAR75S3iA9mGws1Y5WeUO4hyv3r-Eu4Ay7M0y_kq&usqp=CAU

Types of Server

Database Server

- A **Database Server** is a computer in a LAN that is dedicated to **database** storage and retrieval.
- The **database server** holds the **Database Management System (DBMS)** and the **databases**.
- Upon requests from the client machines, it searches the **database** for selected records and passes them back over the network.



Image Source:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcQ0vAYlhrcZW2dOo0DwT-t8qrHqEkzmZJi9-i5LrdnPLA4dxxfl&usqp=CAU>

Types of Server

Virtual Server

- the number of virtual servers deployed exceeded the number of physical servers.
- Today, server virtualization has become near ubiquitous in the data center.

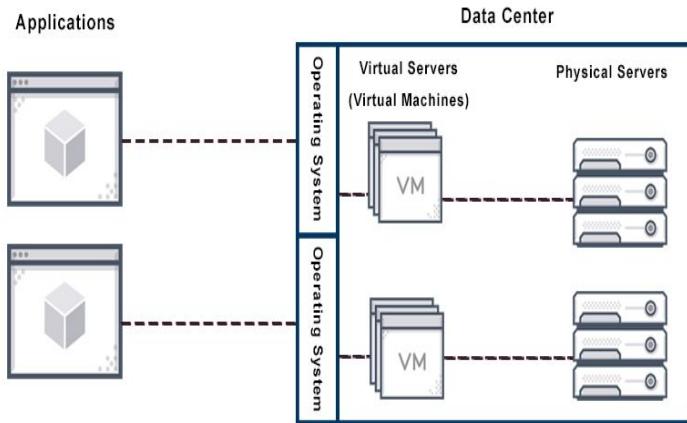


Image Source:

[https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcR48braSt3vm0y5D
KM0CvbVaZhe9WzAcF2LR6LWr5Rp3NVCdcoz&usqp=CAU](https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcR48braSt3vm0y5DKM0CvbVaZhe9WzAcF2LR6LWr5Rp3NVCdcoz&usqp=CAU)

Types of Server

Proxy Server

- It acts as a mediator between a client program and an external server to filter requests, improves performance and share connections..
- **Proxy servers** offers the following basic functionalities:
 - Firewall
 - Network data filtering.



Image Source:

https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.seobility.net%2Fen%2Fwiki%2FProxy_Server&psig=AOvVaw3REvWxxcpw0Znbh2JFC2yv&ust=158957175231000&source=images&cd=fe&ved=0CAIQiRxaEwoTCNiqiMWQtOkC

Types of Server

FTP server

- It works on one of the oldest of the Internet services, the file transfer protocol.
- It provides a secure file transfer between computers while ensuring file security and transfer control.

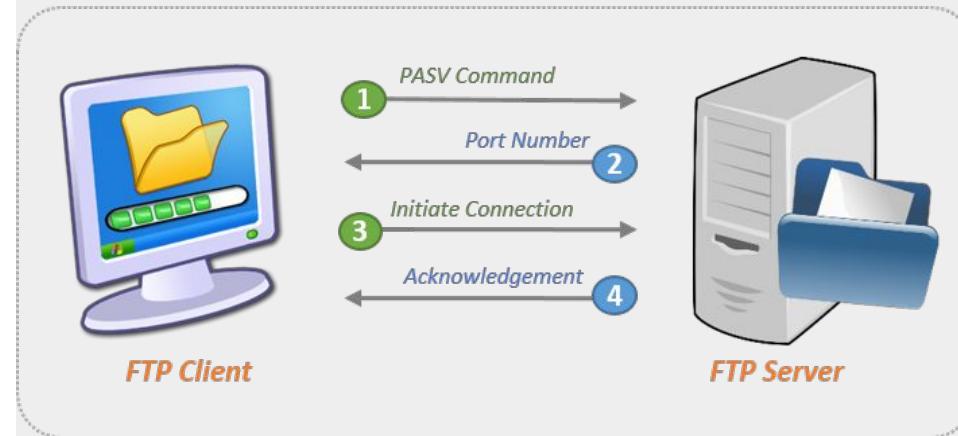


Image Source:

<https://www.serv-u.com/-/media/solarwinds/serv-u/features/windows-setup/ftp-set-up-windows-image-1.ashx?rev=022de70a7ab6435cb0ecd3435edab50d>

Server

Server Structures

The point of a network is to allow one computer to talk to another computer and distribute either work or resources. Computing has evolved since then, resulting in several types of server structures and hardware are follows:-

- Computer hardware server
- Blade Server
- Combining Server



Image Source:
https://centerpeer.org/wp-content/uploads/2018/03/serverack_zoom-825x510.jpg

Server Structure

Computer Hardware Server

- The next major wave of servers included computer-based servers.
- In many respects, these servers were nothing more than larger, more powerful desktop computers.
- Servers like this were often warehoused in air-conditioned rooms called server rooms, and were later bolted into racks for better storage and accessibility.



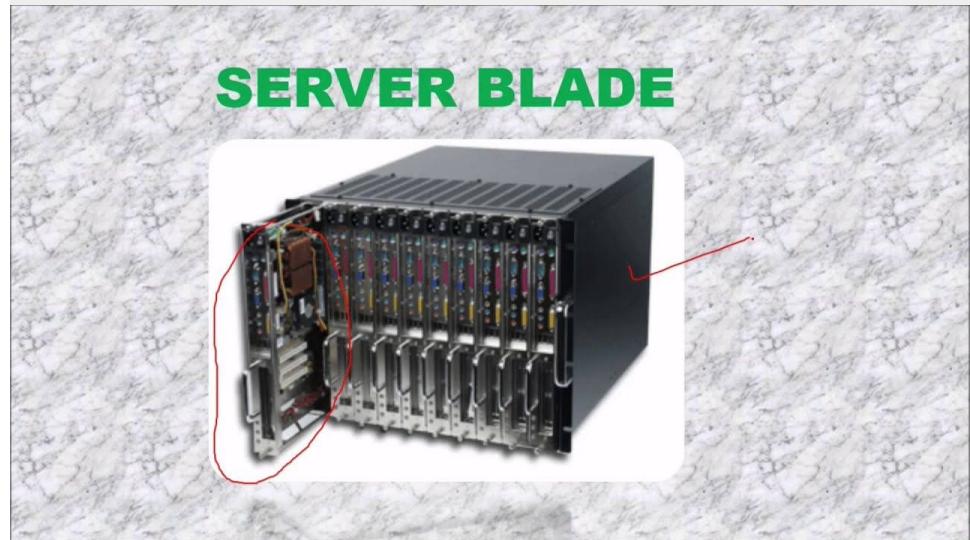
Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcT4pxPUzZFXuj1pK_pbuYS5q96OGNi_5yQXVboeo-PGGDv_MK7M&usqp=CAU

Server Structure

Blade Server

- A **blade server** is a stripped-down **server** computer with a modular design optimized to minimize the use of physical space and energy.
- **Blade servers** have many components removed to save space, minimize power consumption and other considerations, while still having all the functional components to be considered a computer.



Server Structure

Combining Server

- Combining server might consist of several blades, several attached storage devices, and an external power supply.
- Each piece could be swapped out for another while the server was still running.

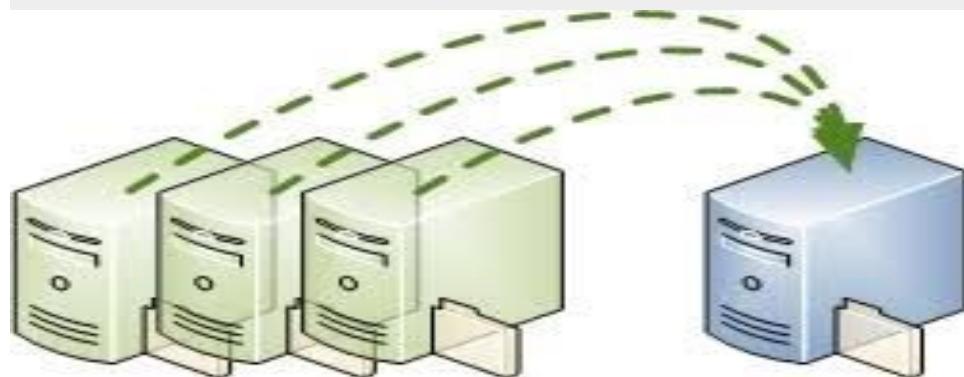


Image Source:

https://www.google.com/imgres?imgurl=http%3A%2F%2Fmicro.net%2Fwp-content%2Fuploads%2F2016%2F12%2Fsrv_srv.jpg&imgrefurl=http%3A%2F%2Fomi

Server

Example of Server Operating System

- Microsoft Windows servers
- Linux / Unix servers
- NetWare
- Cloud servers



Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcRWf0N8_eNhALiv2t_NyBTMvvzhGVsxo6LLP6MOx4T-luehCOd1&usqp=CAU

Example of Server Operating System

Microsoft Windows Servers

- **Windows Server** is a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications.
- Previous versions of **Windows Server** have focused on stability, security, networking, and various improvements to the file system.



Image Source:

https://appsupport.solidrockit.com/images/windows_os/ms_windows_server_os_update.gif

Example of Server Operating System

Linux/Unix Servers

- There are multiple versions and flavors of Linux/Unix including Red Hat Enterprise Linux, Debian, and CentOS.
- As an open-source operating system, Linux is very popular as a web server, often with the Apache web application server installed.



Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcQYkpVpwOSCegV5bpq7uapqA6jau_Qn-1PlcaZxk26Lsmk3eUd8&usqp=CAU

Example of Server Operating System

NetWare

- NetWare was a major player in the server software space as the client-server era was ramping up.
- Eventually, NetWare moved its server operating system to a Linux-based kernel and named it a Novell Open Enterprise Server (OES).

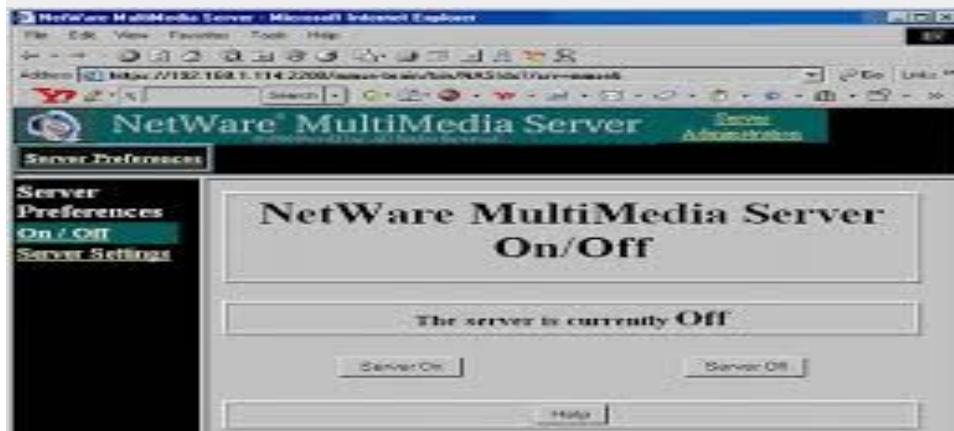


Image Server:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcQW0jaDTjl5loEUx0MBS1d1h9azgvUetDbp1p2aS5W72PtX9JM2&usqp=CAU>

Example of Server Operating System

Cloud Servers

- Virtual servers hosted on a third-party infrastructure on an open network, such as the Internet, are called cloud servers.
- There are numerous cloud server providers these days, including Google's Cloud Platform, Microsoft Azure, and IBM Cloud.



Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcTHuaFqzQPvXkkL0veQ_0BIYaVebQBMfzMxx_eeW7g6TmnN23S&usqp=CAU

Client

What does Client mean?

- A client is the receiving end of a service or the requester of a service in a client/server model type of system.
- The client is most often located on another system or computer, which can be accessed via a network.

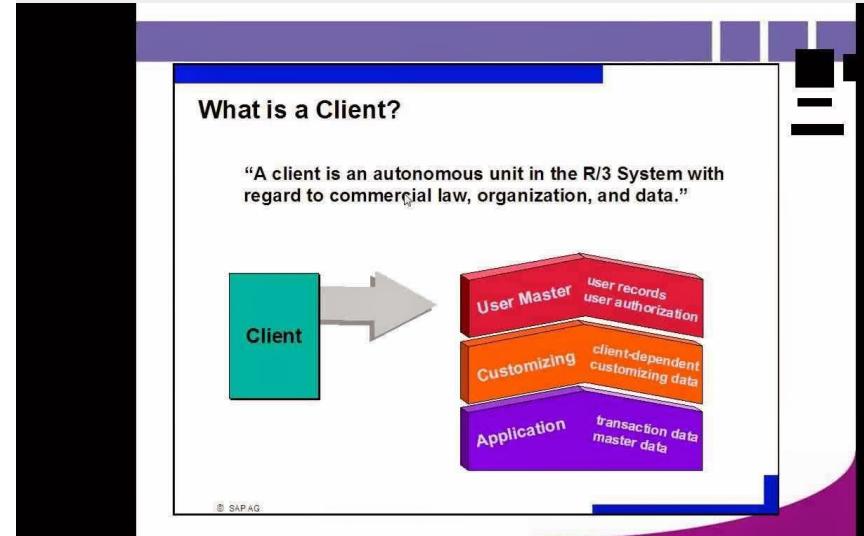


Image Source:

https://2.bp.blogspot.com/-5DVqnk0_55U/VTfSWVnSjyl/AAAAAAAACWc/1f3pW9NLDM0/s1600/maxresdefault.jpg

Client

Types of Client

- Clients are classified into three types:
 - Thin Client
 - Thick/Fat Client
 - Hybrid Client

Types of Client

- **Fat Clients**
- **Thin Clients**
- **Hybrid**

Image Source:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcTNhkaonOxDuUs2LJ1PykUFj-YHvuaEwVUbrH5XuURxNG6FEfGQ&usqp=CAU>

Types of Client

Thin Client

- A client application with minimum functions that uses the resources provided by a host computer
- Its job is usually just to display results processed by a server.
- It simply relies on a server to do most or all of its processing.

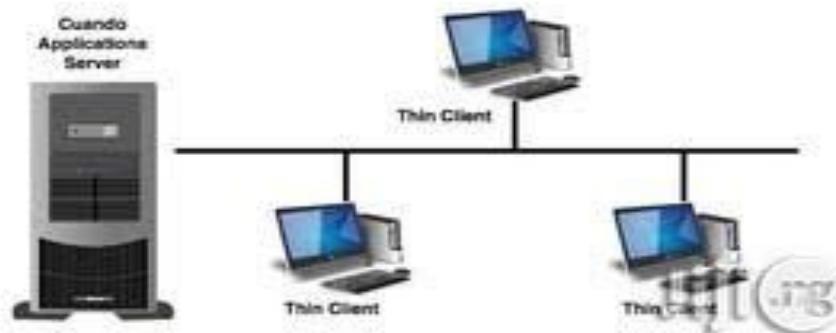


Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcRHgD_LjoMTpkT9Z8PzAGMQu7ZFHT3qF42PIF2hma7cBgpL2xMG&usqp=CAU

Types of Client

Thick/Fat Client

- **Thick clients**, also called **heavy clients**, **are** full-featured computers that **are** connected to a network.
- Unlike **thin clients**, which lack hard drives and other features, **thick clients** **are** functional whether they **are** connected to a network or not.

Thick Client

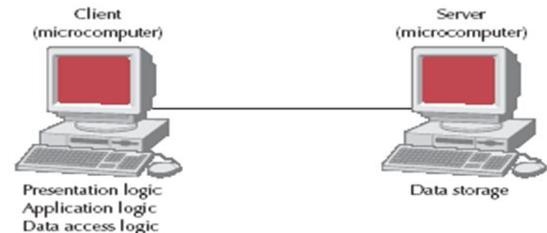


FIGURE 13-2
Client-based
Architectures

Types of Client

Hybrid Client

- Exhibits characteristics from the two above types.
- It can do most processes on its own but may rely on a server for critical data or for storage.

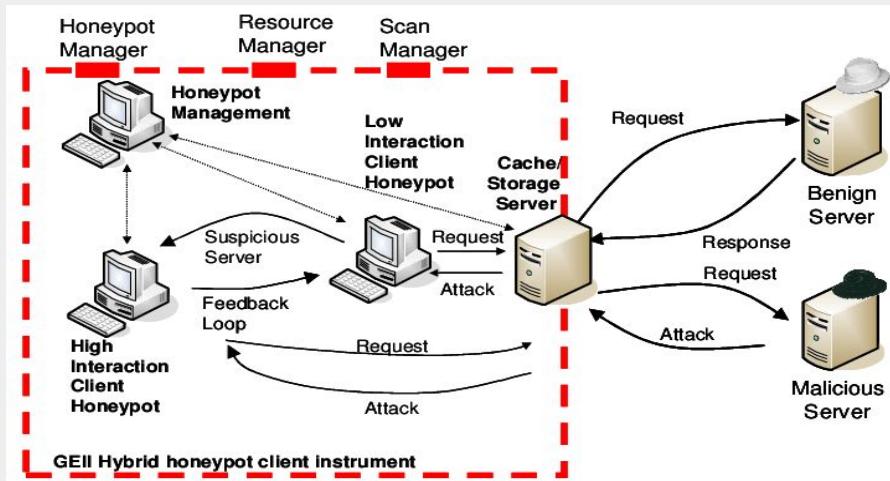


Image Source:

https://www.researchgate.net/profile/Peter_Komisarczuk/publication/202141505/figure/fig2/AS:667681795624961@1536199153132/Hybrid-client-honeypot-architec

Node

What is Node?

- A node is a point of connection within the range of the network.
- It is a major hub through which internet traffic is generally routed.
- The nodes are also known as internet hubs.
- The concept of a node is familiarized with the notion of a distributed network and packet switching theory.

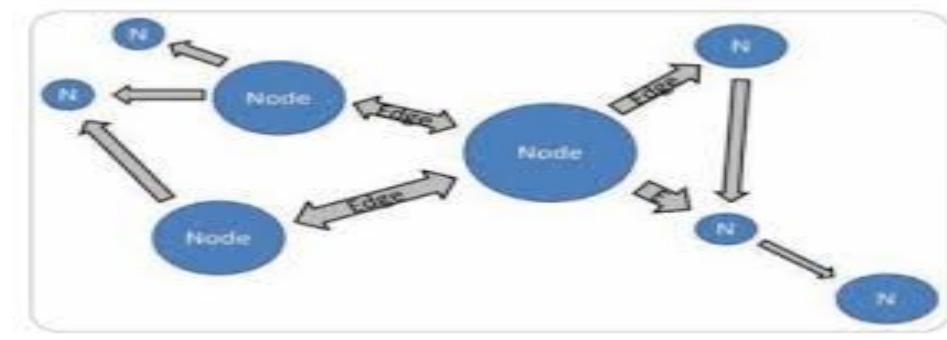


Image Source:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcQmrRNSBtCDS04s0-05OXS40ucSA4s2IGrlkb9kzB1Ve7B4eENm&usqp=CAU>

Node

What is Node?

- A node is a point of connection within the range of the network.
- It is a major hub through which internet traffic is generally routed.
- The nodes are also known as internet hubs.
- The concept of a node is familiarized with the notion :-
 - distributed network
 - packet switching method

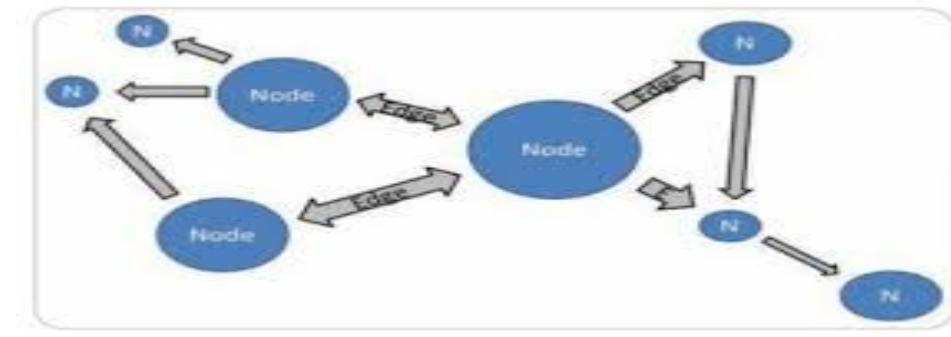


Image Source:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcQmrRNSBtCDSo4s0-o5OXs40ucSA4s2lGrIkb9kzb1Ve7B4eENm&usqp=CAU>

Node

Distributed Network

- A **distributed network** is a type of computer **network** that is spread over different networks.
- This provides a single data communication **network**, which can be managed jointly or separately by each **network**.
- Besides shared communication within the **network**, a **distributed network** often also distributes processing.



Image Source:

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcT8cBUgLabB_dMlb3hlrZuF3tFBtS6HxTzGCZx_xC4JeS0lx30T&usqp=CAU

Node

Packet Switching Method

- **Packet switching** is a method of transferring the data to a network in form of **packets**.
- In order to transfer the file fast and efficient manner over the network
- And minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**.

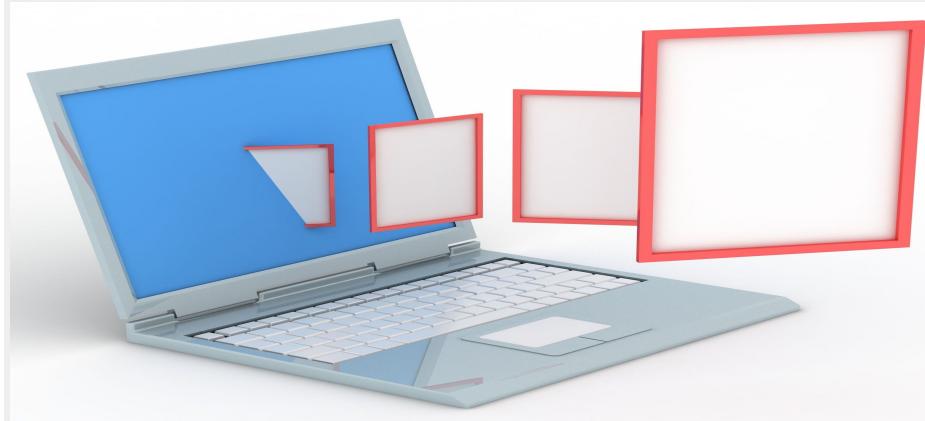


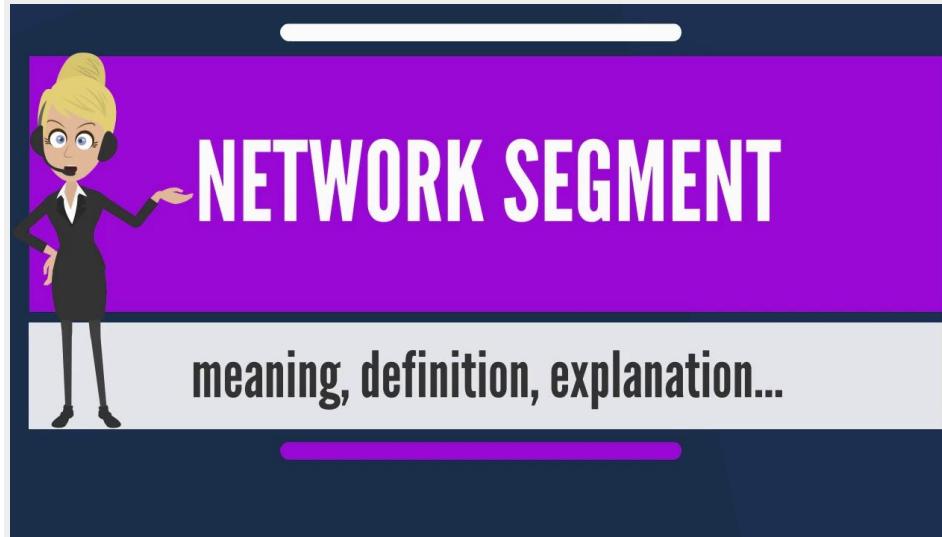
Image Source:

[https://www.lifewire.com/thmb/ltsfAazqk1IkSAfMt79rVmwL1Vg=/3555x2666/smart/filters:no_upscale\(\)/file-concept-123354656-593c5b613df78c537b39e531-696316c434764fec80d6b79cae8cb882.jpg](https://www.lifewire.com/thmb/ltsfAazqk1IkSAfMt79rVmwL1Vg=/3555x2666/smart/filters:no_upscale()/file-concept-123354656-593c5b613df78c537b39e531-696316c434764fec80d6b79cae8cb882.jpg)

Segment

What is Segment?

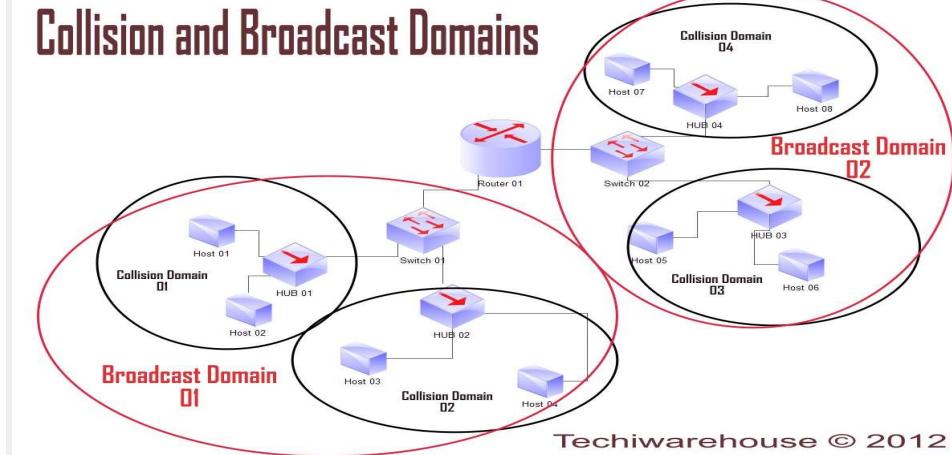
- A network segment is a portion of a computer network.
- It is parted from the rest of the whole network by a device such as a hub, switch, repeater, bridge or router.
- Each segment can comprise one or many computers and hosts.



Segment

Types of Segmentation

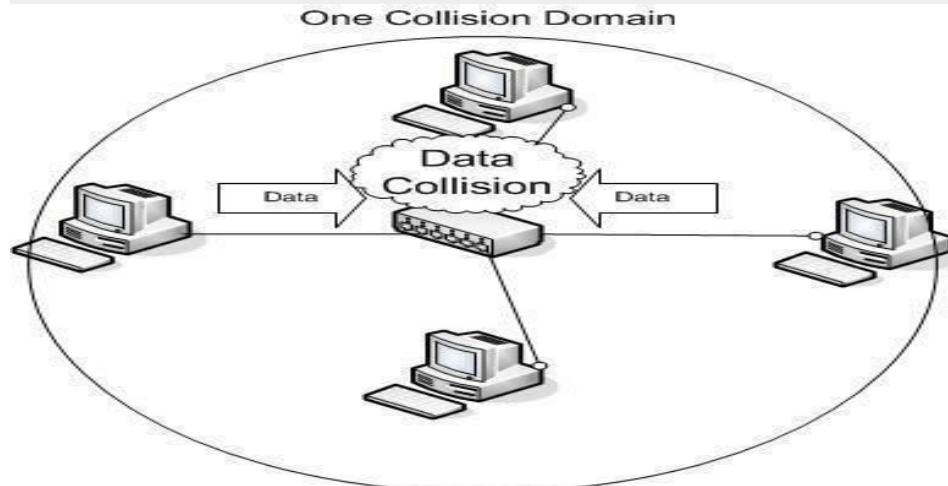
- The type of segmentation differs according to the type of device used.
- For example,
 - a bridge separates **collision domains**,
 - while a router separates both **collision domains and broadcast domains**.



Types of Segmentation

Collision Domains

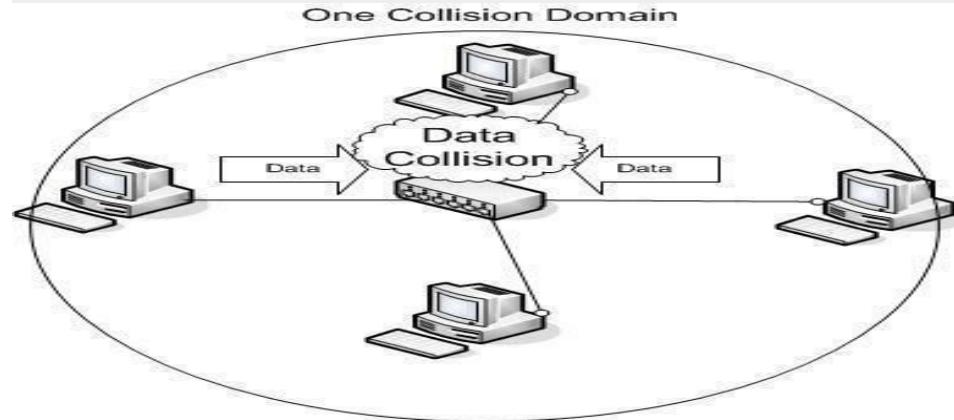
- A collision domain is a logical area in a computer network where data packets can collide with one another.
- A collision occurs when two or more devices attempt to send a signal along the same transmission channel at the same time.
- It can result in garbled, and thus useless, messages.



Types of Segmentation

Collision Domains (Contd..)

- Collision domains can range in size from a single segment of cable to an entire network, at least a small one.
- The optimal size of a collision domain depends on a number of factors.
- Among them is the number of collisions, as a higher number of them results in a lower efficiency of the network.



Types of Segmentation

Broadcast Domains

- A broadcast domain is the portion of a network that is reachable by a network broadcast, i.e.,
- A simultaneous transmission of a single message to all hosts on the network, or part, thereof.

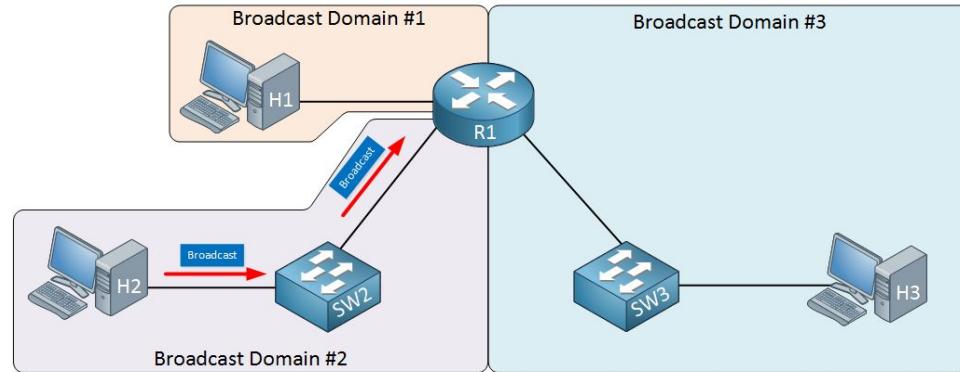


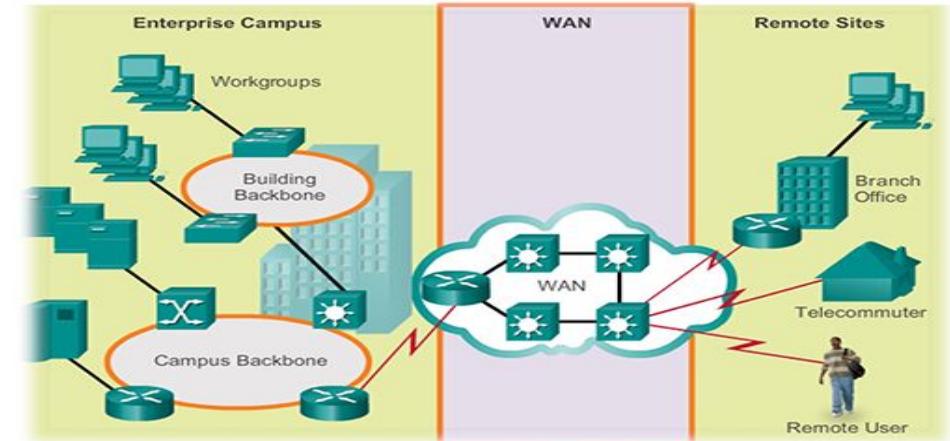
Image Source:

https://cdn.networklessons.com/wp-content/uploads/2016/11/xrouter-breaks-broadcast-domain.png.pagespeed.ic.FzR4ox_5t4.png

Backbone

What is Backbone?

- A backbone is a fragment of a network that connects several bits of the network, providing a route for the sharing of data between different networks.
- A backbone can couple networks in the same building or in different infrastructures or over wide areas.



ImageSource:

https://www.open.edu/openlearncreate/pluginfile.php/259785/mod_oucontent/oucontent/10252424/1741175/H141951/

Host

What is Host?

- A host acts as a replacement for an in-house Web server and is the basic building block behind Web hosting services.
- A host is built, delivered and managed by a hosting service provider that rents out host(s) some portion of its computing power by sharing those resources among several websites/users.

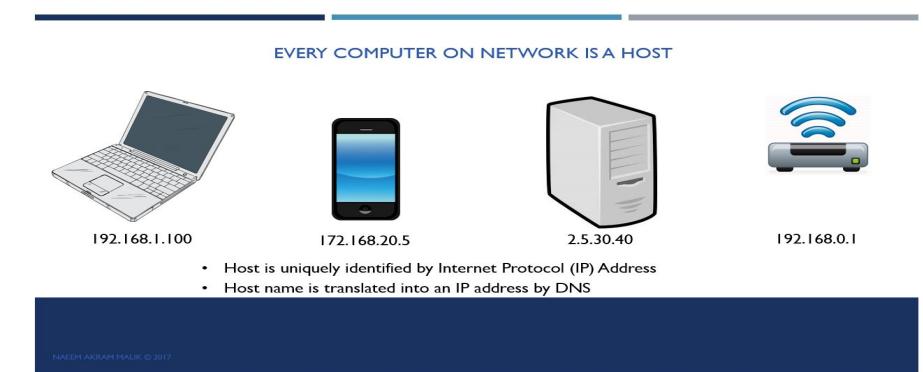


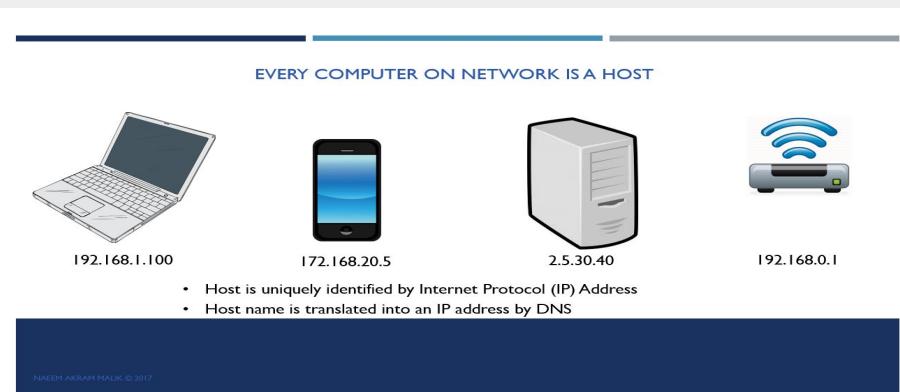
Image Source:

https://2.bp.blogspot.com/-nw1guSvWmGM/XEjORHYceOI/AAAAAAAFA2I/Bw8aM_9tF_E-0_E/EC02NLUHUGWHQCL-PCA-/1000x450.jpg

Host

What is Host? (Contd..)

- A host functions as a typical Web server but is generally shared and has a different delivery/access mode.



NAEEM AKSAM MALIK © 2017

Image Source:

https://2.bp.blogspot.com/-nw1guSvWmGM/XEjORHYceOI/AAAAAAAFA2I/Bw8aM_9tF_E-9tF_UU_EG2GNLUHUGWHQCL_PCA-/1200/

Host

Key Components of Host

- Hardware
- Software
- Network



Image Source:

<https://qph.fs.quoracdn.net/main-qimg-30c45af8fc0a0ecc2717ba469255a8da.web>

Key Components of Host

Hardware

- This includes the computing server, storage and other critical components of a Web server

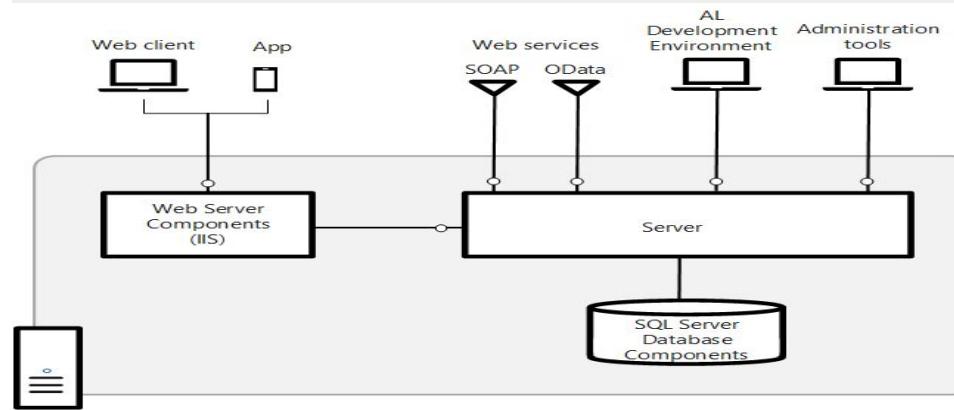


Image Source:

<https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/media/architecture-diagram>

Key Components of Host

Software

- A basic operating system with specialized Web hosting and management software

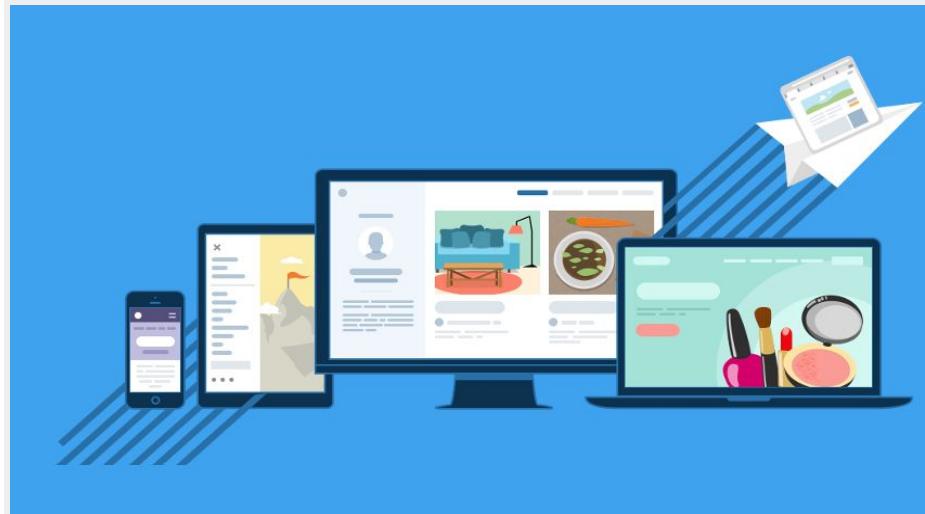


Image Source:

<https://www.hostpapa.eu/blog/wp-content/uploads/2018/06/blog1.png>

Key Components of Host

Network

- Interconnectivity, data routing and other types of networking.

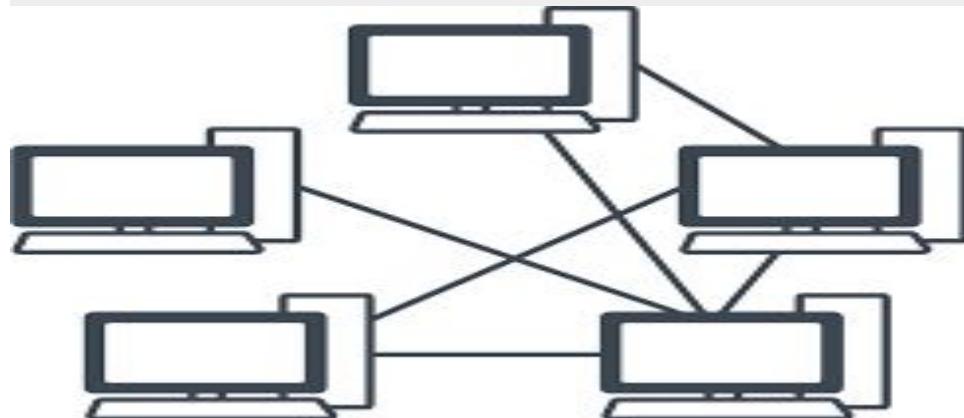


Image Source:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcQrVG3mSRcVJcmqTMYino4MeFtFHpZC0mGKMGwyBH3qaQujFYQ&usqp=CAU>

Analog and Digital Transmission

Define analog and digital transmission

- There are a number of differences between analog and digital transmission.
- It is important to understand how conversions between analog and digital occur.
- Let's look first at the older form of transmission, analog.

Analog and Digital Signals

Analog



Digital



www.electricalfundablog.com

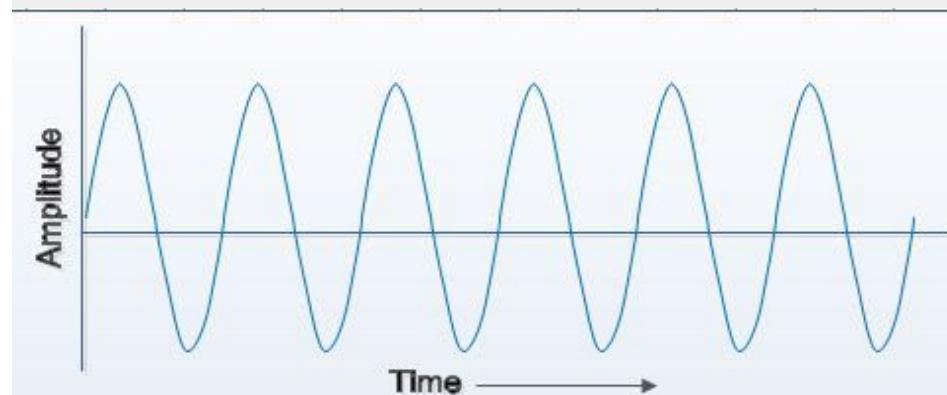
ImageSource:

https://electricalfundablog.com/wp-content/uploads/2018/02/Analog-and-Digital-Signals_thumb.png

Analog and Digital Transmission

Analog Transmission

- Analog Transmission is the transmission of signals that vary smoothly with time, as shown in the diagram.
- An analog signal can take on any value in a specified range of values.
- A simple example is alternating current (AC), which continually varies between about +110 volts and -110 volts in a sine wave fashion 60 times per second.



Analog signal Waveform

Analog and Digital Transmission

Digital Transmission

- Data or information can be stored in two ways, analog and digital.
- For a computer to use that data is must be in discrete digital form.
- Like data, signals can also be in analog and digital form.
- To transmit data digitally it needs to be first converted to digital form.

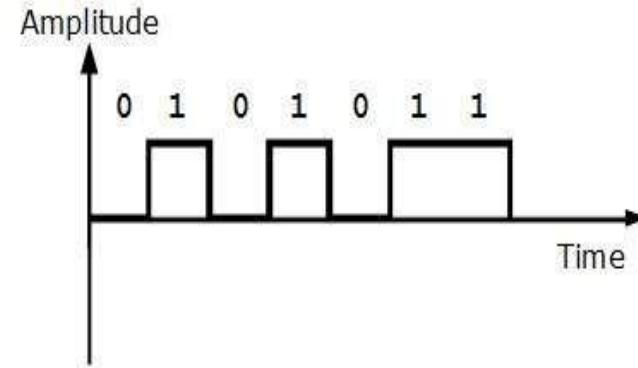


Image Source:

https://www.tutorialspoint.com/data_communication_computer_network/images/Unipolar_NRZ.jpg

Analog and Digital Transmission

Difference between Analog and Digital Transmission (Contd..)

- The **difference between analog and digital** technologies is that in **analog** technology, information is translated into electric pulses of varying amplitude.
- In **digital** technology, translation of information is into binary format (zero or one) where each bit is representative of two distinct amplitudes.

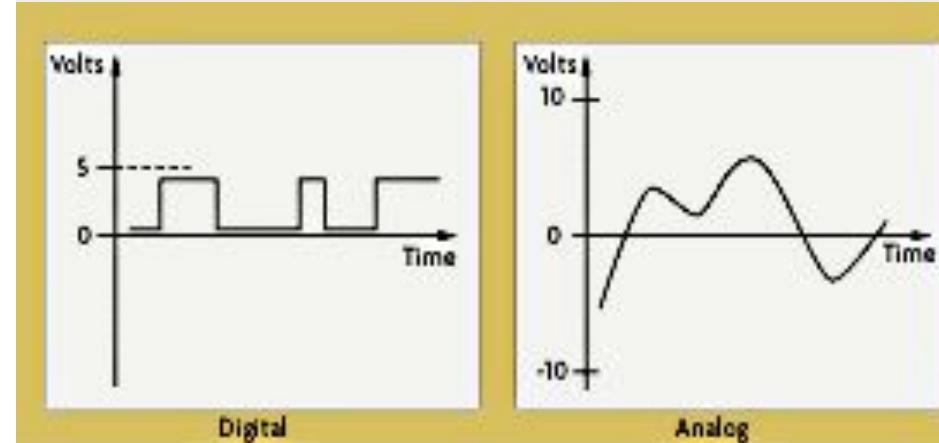


Image Source:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcR4FwBZITnY7wqearWz4OUgIgyvqi8YgL7tJSos67WNKcHKGH-&usqp=CAU>

Analog and Digital Transmission

Difference between Analog and Digital Transmission

- The **difference between analog and digital** technologies is that in **analog** technology, information is translated into electric pulses of varying amplitude.
- In **digital** technology, translation of information is into binary format (zero or one) where each bit is representative of two distinct amplitudes.

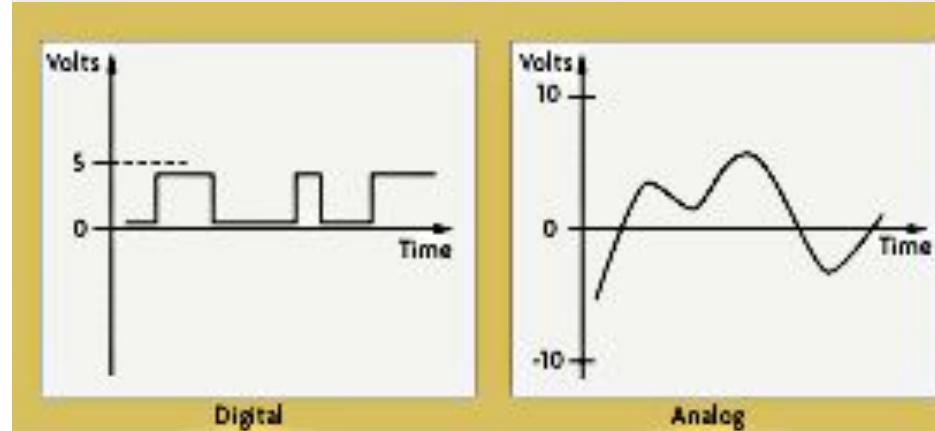


Image Source:

<https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcR4FwBZITnY7wqearWz4OUgIgyvqi8YgL7tJSos67WNKcHKGH-&usqp=CAU>

Analog and Digital Transmission

What are the advantages of digital transmission over analog transmission (Contd...)

Analog is far superior than digital but digital has two distinct advantage over analog because of which whole world has gone digital.

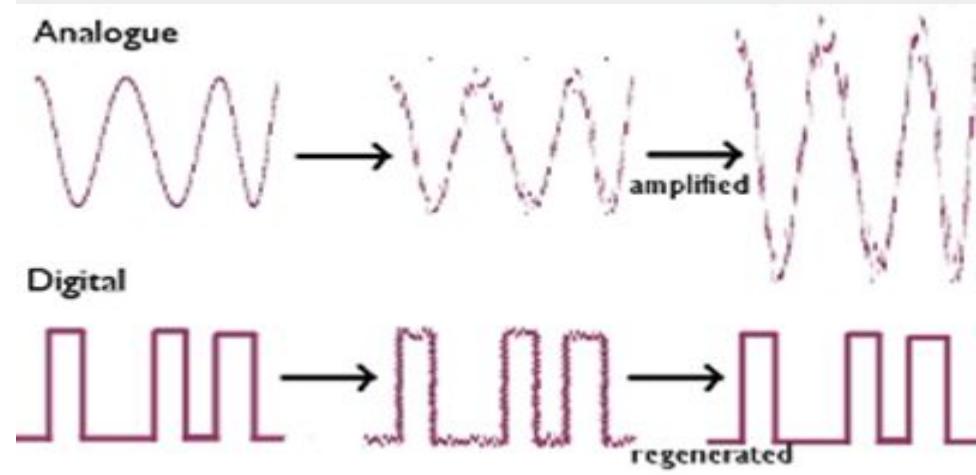


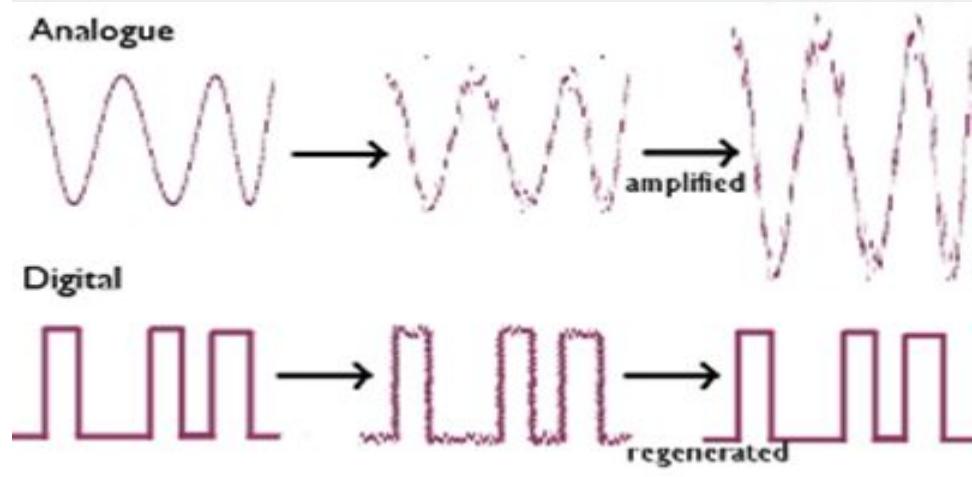
Image Source:

https://2.bp.blogspot.com/-VdvEo1bKvps/Vt1RnTArZ_I/AAAAAAAAC0/f0J643LKlw0/s1600/Regenerationofsi%253Dgnals..png

Analog and Digital Transmission

What are the advantages of digital transmission over analog transmission

- **Transmission:** Digital signal can be transmitted over long distance without worry of noise and distortion and degradation.
- **Storage:** Digital signal/data can be stored for long time without worry of degradation. Duplicating data will produce exact one to one copy.



Image

Source: https://2.bp.blogspot.com/-VdvEo1bKvps/Vt1RnTArZ_I/AAAAAAAAC0/f0J643Lklw0/s1600/Regenerationofsi%253Dgnals..png

Analog and Digital Transmission

Why digital signal better than analog

- **Digital signals** are more secure, and they do not get damaged by noise.
- They allow the **signals** transmitted over a lengthy distance.

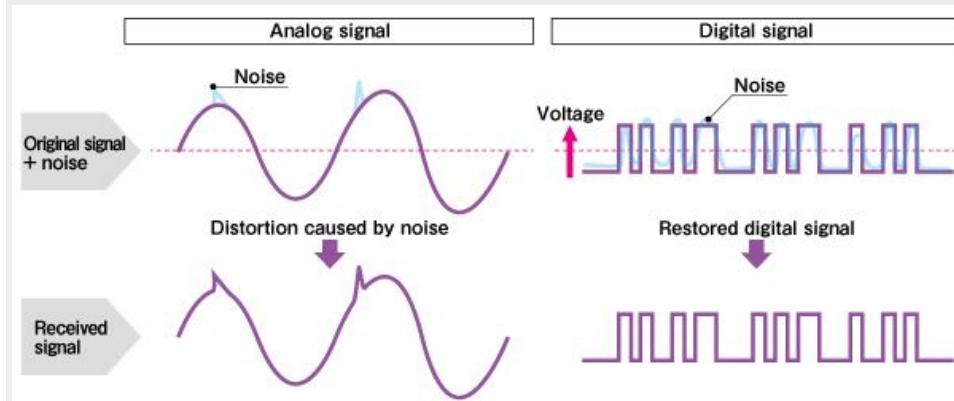


Image Source:

https://2.bp.blogspot.com/-J3YUIQrcYLI/Vt1RcJ8r5HI/AAAAAAAACw/oEx_z0NpB3o/s1600/NoisImmunity.png

Analog and Digital Transmission

What are the advantages of digital transmission

- Noise Immunity
- Multiplexing
- Easy to Store
- Resistant to additive Noise
- Used for Long Distance
- Transmission errors can be detected easily

Advantages & disadvantages of Digital Transmission

Advantages

- Noise immunity
- (Time domain) Multiplexing
- Regeneration
- Simple to evaluate and measure

Disadvantages

- More bandwidth
- Additional encoding (A/D) and decoding (D/A) circuitry

Image

Source: <https://slideplayer.com/slide/5927221/20/images/2/Advantages+of+digital+transmission.jpg>

Analog and Digital Transmission

What are the disadvantages of digital transmission

- More Bandwidth Requirement
- Extra Circuitry for encoding and Decoding
- Require Synchronization

Advantages & disadvantages of Digital Transmission

Advantages

- Noise immunity
- (Time domain) Multiplexing
- Regeneration
- Simple to evaluate and measure

Disadvantages

- More bandwidth
- Additional encoding (A/D) and decoding (D/A) circuitry

Image

Source: <https://slideplayer.com/slide/5927221/20/images/2/Advantages+&+disadvantages+of.jpg>

Analog and Digital Transmission

What are the advantages of Analog Transmission

- No quantization errors, requires less bandwidth, low cost and can be easily constructed because of less pre-processing requirements.
- A method of storing, processing and **transmitting** information through the use of distinct electronic or optical pulses that represent the binary digits 0 and 1.

Analog Advantages

- **Low cost and simplicity in some applications**
 - Attenuators/amplifiers
 - Simple filters
- **Wide bandwidth (GHz)**
- **Low signal levels**
- **Infinite effective sampling rate**
 - Infinite resolution in frequency
 - No aliasing/reconstruction issues
- **Infinite resolution in amplitude**
 - No quantitation noise

Analog and Digital Transmission

What are the disadvantages of Analog Transmission

- **Analog** tends to have a lower quality signal than digital.
- The cables are sensitive to external influences. The cost of the **Analog** wire is high and not easily portable.
- Low availability of models with digital interfaces.

Disadvantages of Analog Transmission

- Use amplifier to strengthen a weak signal but the amplifier itself introduces noise into the transmission medium
- When you amplify (boost) the signal, you are also amplifying the distortion.
- Cumulative effect, more amplifications result in more distortion.

Image

Source: <https://slideplayer.com/slide/16853987/97/images/1/Disadvantages+of+Analog+Transmission.jpg>

Analog and Digital Transmission

What are the disadvantages of Analog Transmission

- **Analog** tends to have a lower quality signal than digital.
- The cables are sensitive to external influences. The cost of the **Analog** wire is high and not easily portable.
- Low availability of models with digital interfaces.

Disadvantages of Analog Transmission

- Use amplifier to strengthen a weak signal but the amplifier itself introduces noise into the transmission medium
- When you amplify (boost) the signal, you are also amplifying the distortion.
- Cumulative effect, more amplifications result in more distortion.

Image

Source: <https://slideplayer.com/slide/16853987/97/images/1/Disadvantages+of+Analog+Transmission.jpg>

STP Cable

What is STP Cable

- **Shielded twisted pair (STP) cable** was originally designed by IBM for token ring networks that include two individual wires covered with a foil shielding, which prevents electromagnetic interference, thereby transporting data faster.
- STP is similar to unshielded twisted pair (UTP); however, it contains an extra foil wrapping or copper braid jacket to help shield the cable signals from interference.



STP Cable

Where is STP Cable used?

- The extra covering in shielded twisted pair wiring protects the transmission line from electromagnetic interference leaking into or out of the **cable**.
- **STP cabling** often is **used** in Ethernet networks, especially fast data rate Ethernets.



Image

Source: <https://www.cmple.com/Content/Images/uploaded/UTP%20Cable.jpeg>

STP Cable

Which connector is used in STP
Cable?

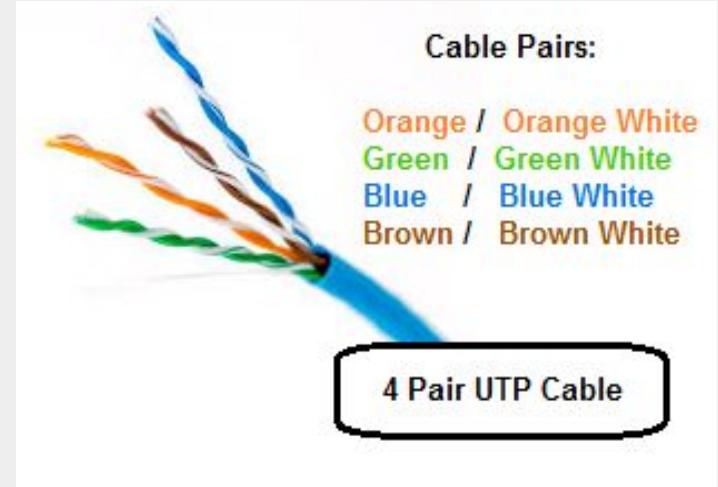
- Most commonly your connector are in two flavors:
 - **BNC** (Bayonet Naur Connector) used in thicknets
 - **RJ-45** used in smaller networks using UTP/STP.



UTP cable

Introduction

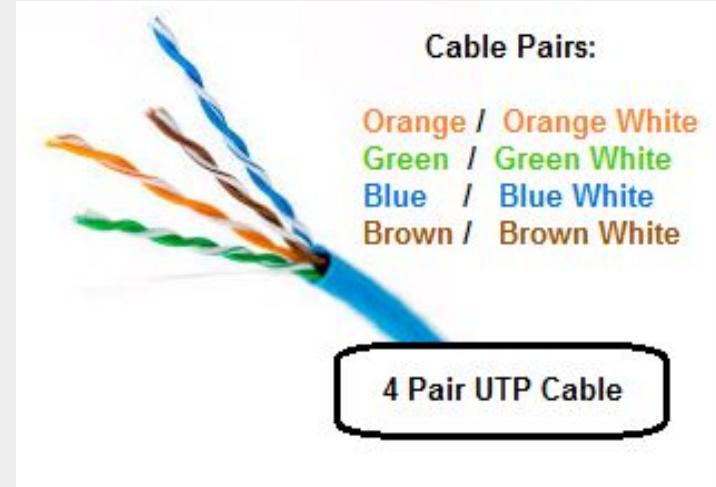
- (UTP) cable, digital signal protection comes from the twists in the wire.
- 4 twisted pairs with four different colours wires.



UTP cable

3 types of UTP cables

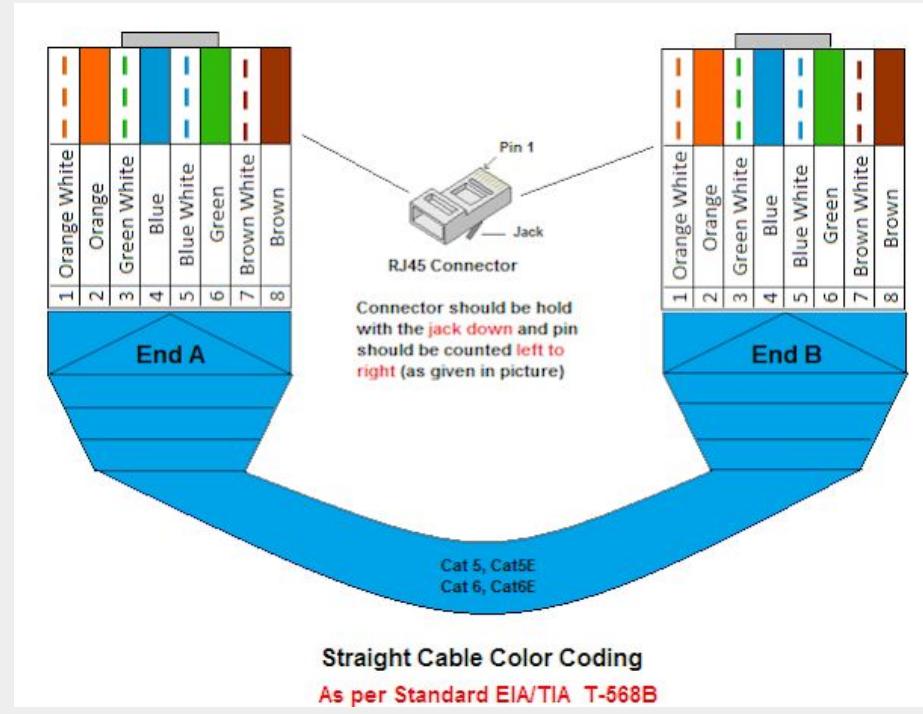
- Straight
- Cross
- Rollover or Console



3 types of UTP cables

Straight Cable

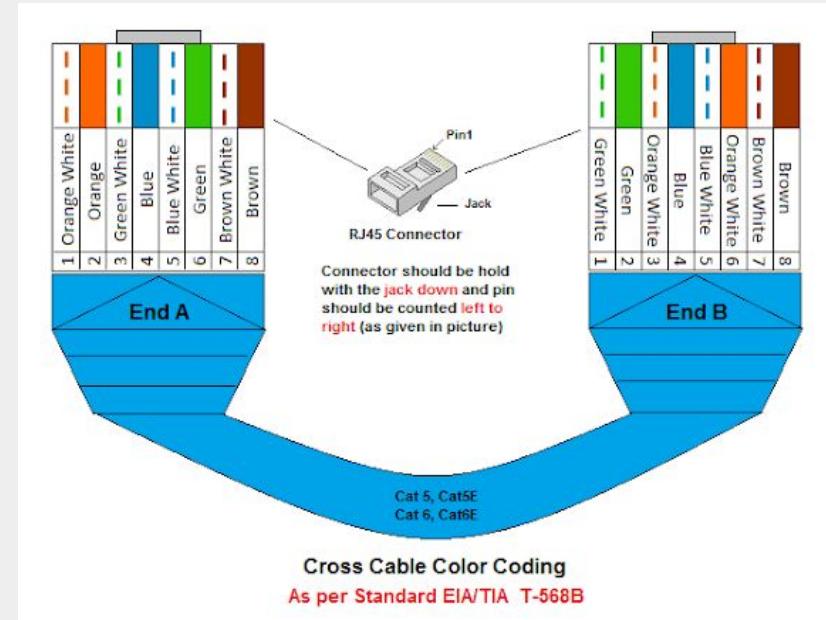
- It is used to connect devices having different function.



UTP cable

Cross Cable

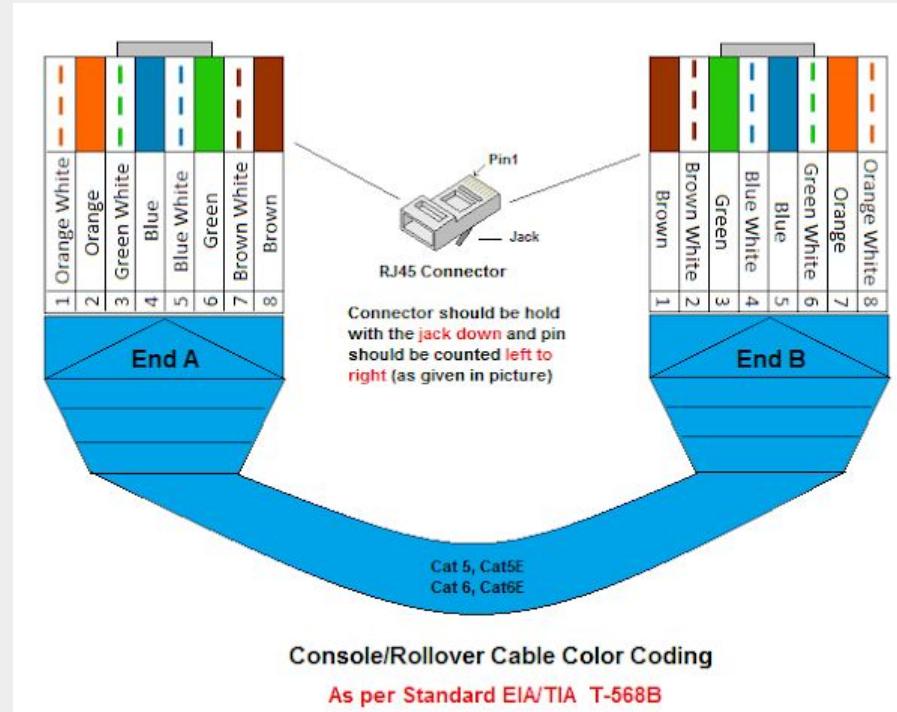
- It is used to connect devices having same functions or roles.



UTP cables

Console or Rollover cable

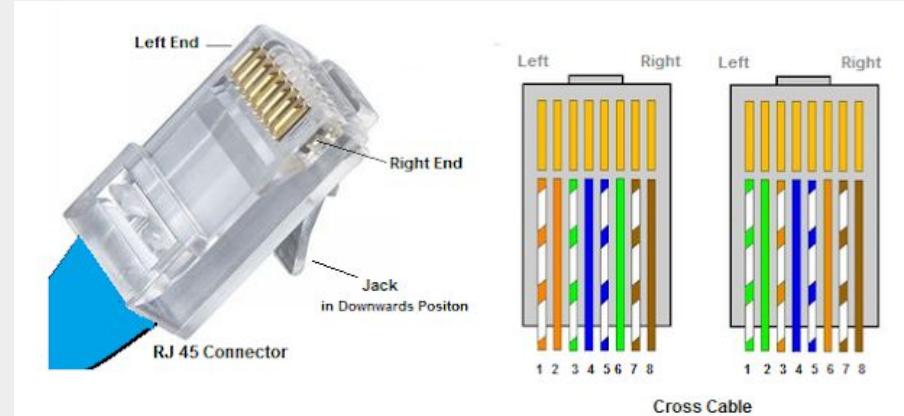
- It is used for device configuration



UTP cable

Identifying the Cable type

- Hold both ends/RJ-45connectors of cable with their Jack in downward position.
- Now start matching the colour coding from left pin of connector towards right.



UTP cables

Categories

UTP Categories - Copper Cable				
UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Ring & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

- Image source :
<http://www.firewall.cx/networking-topics/cabling-utp-fibre/112-network-cabling-utp.html>

UTP cables

Similarities and differences between
STP and UTP cables

- Both cables use the same RJ-45 (registered jack) modular connectors.
- Both cables can accommodate a maximum of 1024 nodes in each segment.

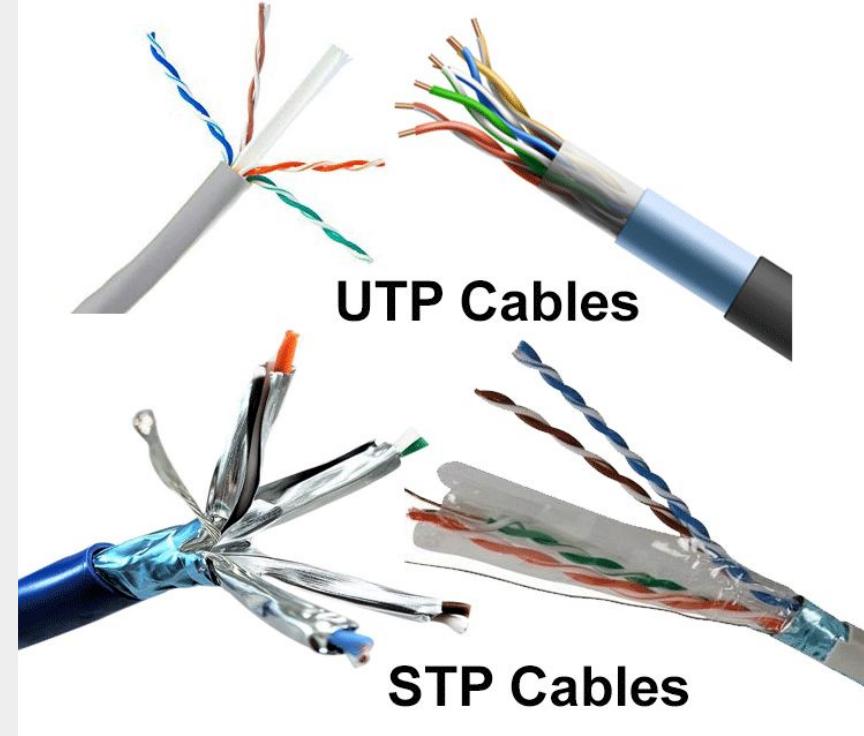


Image Source :
computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html

Coaxial cable

Components

- This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, braiding covers the insulation, and the insulation covers the conductor.
- The following image shows these components.

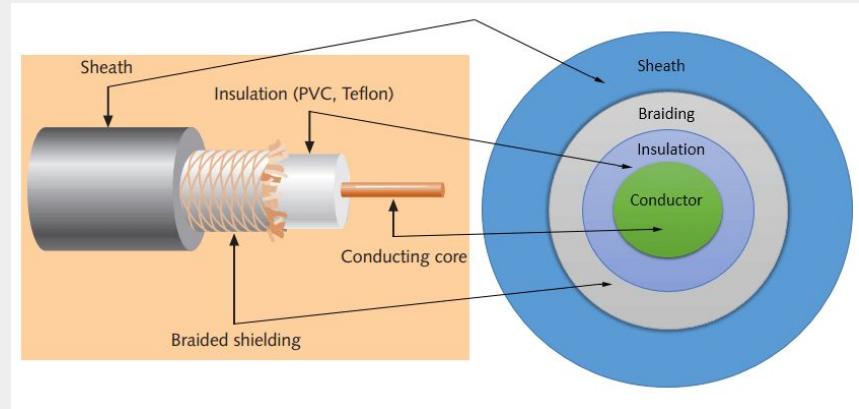


Image Source :
computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html

Coaxial cable

Coaxial Type

- **Single-core** coaxial cable uses a single central metal (usually copper) conductor.
- **Multi-core** coaxial cable uses multiple thin strands of metal wires.



Single core coaxial cable



Multi-core coaxial cable

Specifications

Type	Ohms	AWG	Conductor	Description
RG-6	75	18	Solid copper	Used in cable network to provide cable Internet service and cable TV over long distances.
RG-8	50	10	Solid copper	Used in the earliest computer networks. This cable was used as the backbone-cable in the bus topology. In Ethernet standards, this cable is documented as the 10base5 Thicknet cable.
RG-58	50	24	Several thin strands of copper	This cable is thinner, easier to handle and install than the RG-8 cable. This cable was used to connect a system with the backbone-cable. In Ethernet standards, this cable is documented as the 10base2 Thinnet cable.
RG-59	75	20 - 22	Solid copper	Used in cable networks to provide short-distance service.

- Refer Notes Section

Image Source :

computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html

Fibber cable

Fibber



- Because of the low loss, high bandwidth properties of fibre cables they can be used over greater distances than copper cables.

Image Source :
<http://www.firewall.cx/networking-topics/cabling-utp-fibre/117-network-cabling-fiberoptic.html>

Fibber cable

Types

- **Multimode** cable has a larger diameter; however, both cables provide high bandwidth at high speeds.
- **Single mode** can provide more distance, but it is more expensive

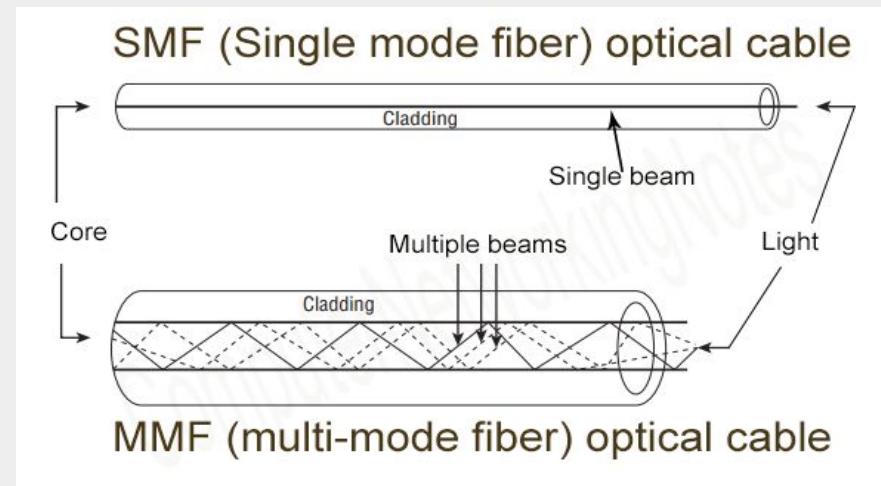


Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html>

Fibber cable

Fibber Construction

- Most common types -- **62.5/125 micron** loose tube.
- More details refer notes section

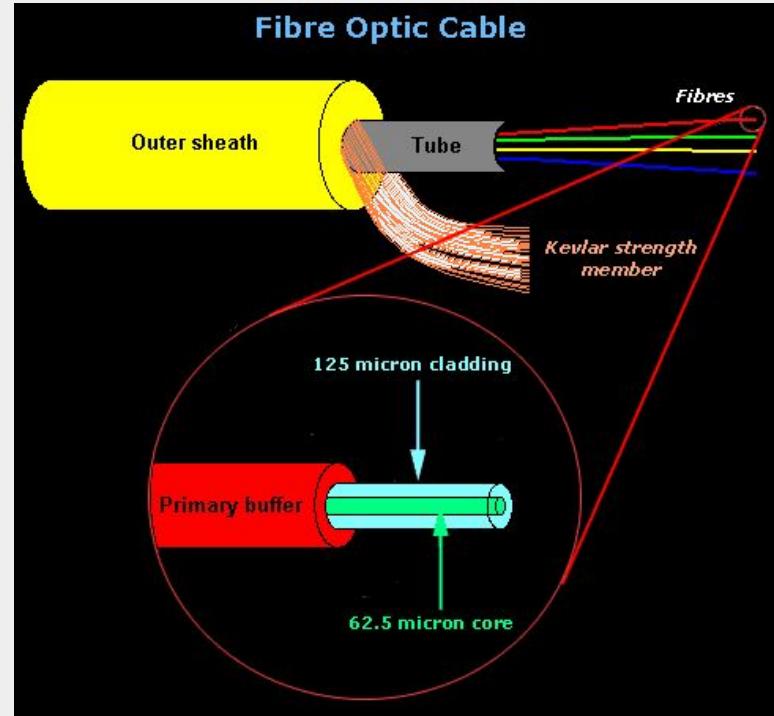


Image Source :

<http://www.firewall.cx/networking-topics/cabling-utp-fibre/117-network-cabling-fiberoptic.html>

Fibber cable

Fibber Construction – patch lead

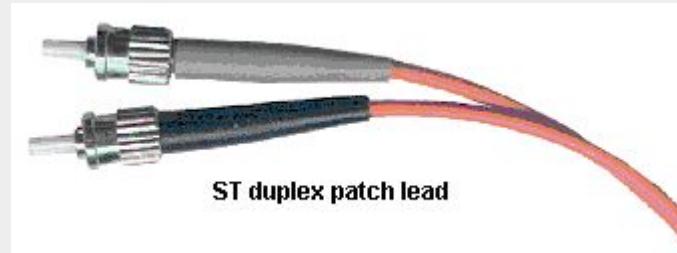


Image Source :

<http://www.firewall.cx/networking-topics/cabling-utp-fibre/117-network-cabling-fiberoptic.html>

Baseband and Broadband

Introduction

- Baseband technology transmits a single data signal/stream/channel at a time.
- While broadband technology transmits multiple data signalsstreams/channels simultaneously at the same time.

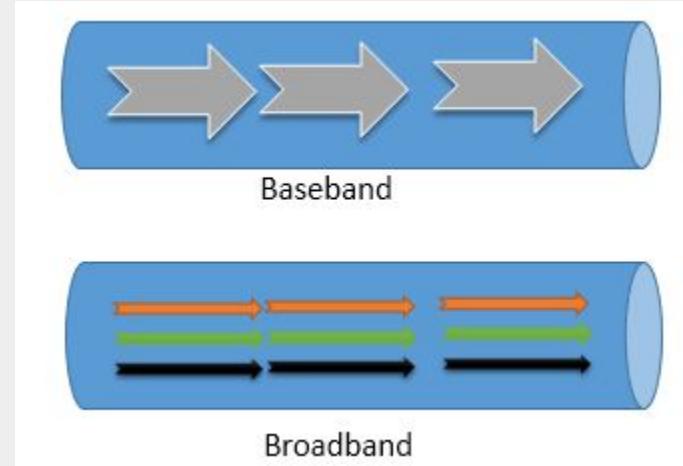


Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

Baseband and Broadband

Baseband

- Baseband technology is mainly used in Ethernet networks to exchange data between nodes.
- This technology can be used on all three popular cable media types of Ethernet; coaxial, twisted-pair, fiber-optic.

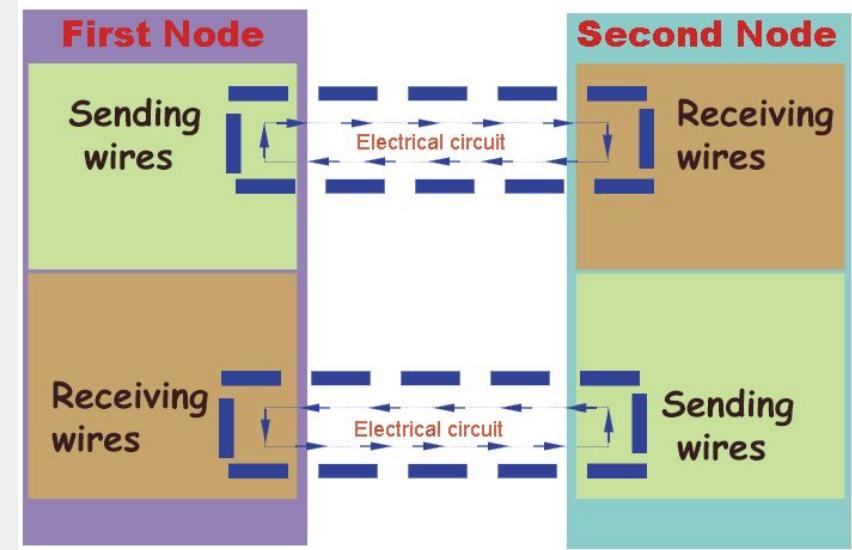


Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

Baseband and Broadband

Broadband

- Broadband technology uses analog signals in data transmission.
- This technology uses a special analog wave known as the **carrier wave**.
- A carrier wave does not contain any data but contains all properties of the analogue signal.

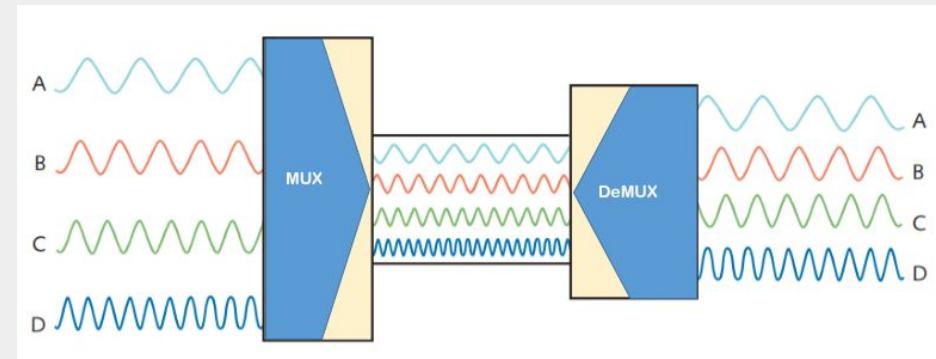


Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

Baseband and Broadband

Differences

- Broadband
 - Transmit digital signals
 - To boost signal strength, use repeaters
 - Can transmit only a single data stream at a time
 - Support bidirectional communication simultaneously
 - Support TDM based multiplexing
 - Use coaxial, twisted-pair, and fiber-optic cables
 - Mainly used in Ethernet LAN networks

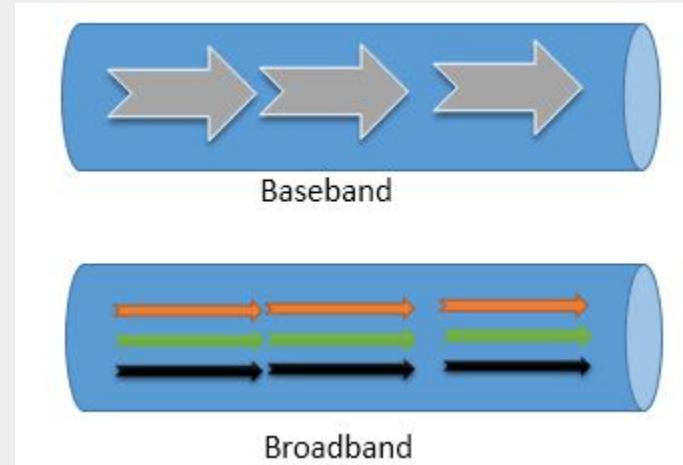


Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

Baseband and Broadband

Differences

- Baseband
 - Transmit analog signals
 - To boost signal strength, use amplifiers
 - Can transmit multiple signal waves at a time
 - Support unidirectional communication only
 - Support FDM based multiplexing
 - Use radio waves, coaxial cables, and fiber optic cables
 - Mainly used in cable and telephone networks

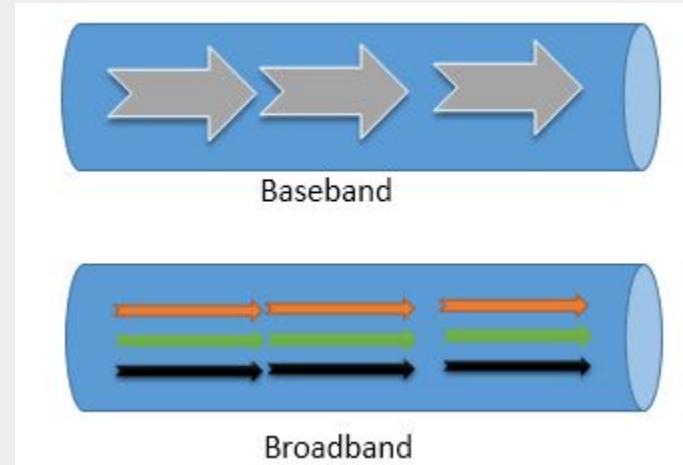


Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

Network cable Crimping Tools

Wire Cutter

- To cut the network cable of the required length from the bundle, you can use any standard wire cutter tool or can use a wire cutter tool that is specially designed for the twisted-pair cable. A twisted-pair wire cutter usually includes additional blades for stripping the wire.



Image source:

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Network cable Crimping Tools

Wire Stripper

- This tool is used to remove the outer and inner jackets of the network cable.
- Typically, you do not need to purchase this tool separately as all standard twisted-pair wire cutters are equipped with wire-stripppers



Image source:

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Network cables

Crimping Tool

Crimp tool

- This tool is used to attach the connectors to the cable. Typically, this tool also includes a wire-cutter and wire-stripper.
- So if you buy a crimp tool, you don't have to buy a wire-cutter and wire-striper separately.
- The following image shows a crimping device equipped with a wire-stripper and wire-cutter.



Image source:

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Network cable Troubleshooting tools

Cable certifier

- This device thoroughly tests a network cable and certifies that the cable installation meets a special wiring standard such as Cat 5e, Cat 6, Cat 6a, and so forth.
- This device can check and test total segment length, crosstalk, noise, wire map, resistance, impedance, and the capability to transfer data at the maximum frequency rated for the cable.

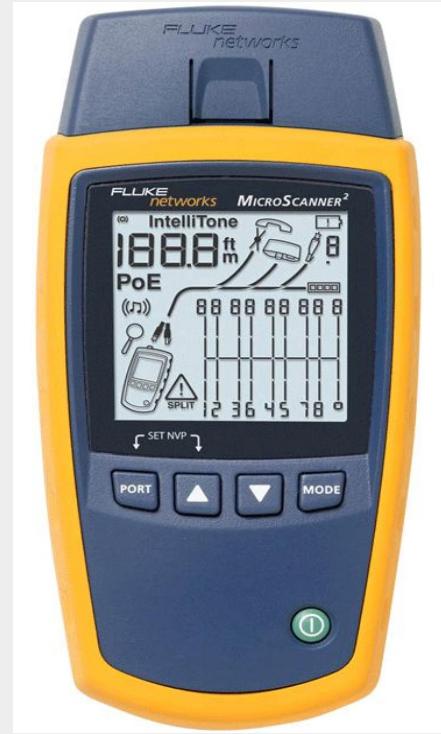


Image source:

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Network cable Troubleshooting tools

Cable tester

- Besides certifying the cable installation, this device provides all remaining functionalities of a network cable certifier.
- It can test cable length, cross talk, and breaks in the cable. It can also check whether the connectors on both ends of a network cable are properly attached or not..



Image source:

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Network cable Troubleshooting tools

Tone generator and the probe

- This device is used to trace the unlabeled network cables. This device comes in two pieces: the tone generator and the probe. The tone generator generates tones or signals and places them on the network cable. The probe detects these signals on the other end of the cable.



Image source:

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Network cable Troubleshooting tools

Time domain reflectometer

- This device is used to measure the length of a network cable as well as the breaks in the cable. This device transmits a signal on one end and measures the time the signal takes to reach the end of the cable.

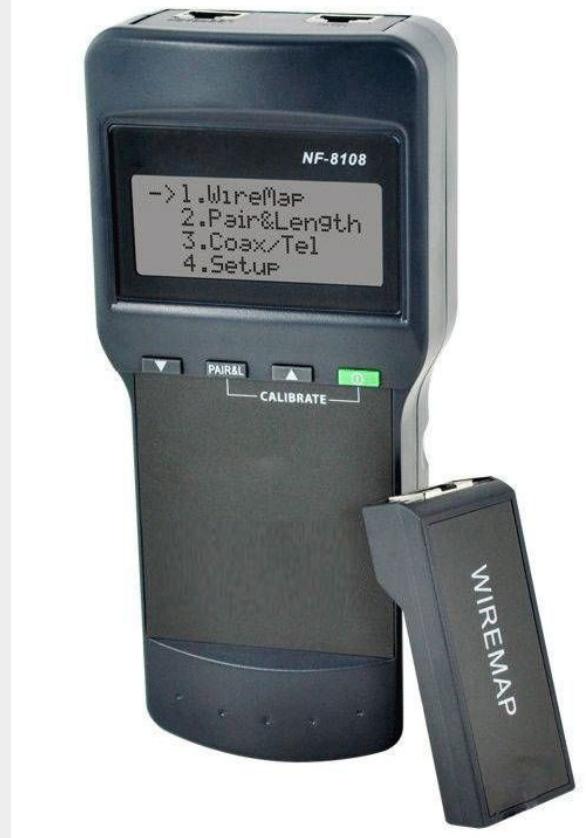


Image source:

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Cables and Connectors

Universal Serial Bus



- USB 1.0
- USB 2.0
- USB 3.0

Image Source:
<https://static.makeuseof.com/wp-content/uploads/2016/08/usb-3-micro-cable.jpg>

Cables and Connectors

USB Differences

- Advantages
- Disadvantages
- Limitations
- Refer Notes Section

Data Size	Time Taken		
	USB 1.0	USB 2.0	USB 3.0
Image/MP3 (4MB)	5.3 Sec	0.1 Sec	0.01 Sec
Flash Drive (1 GB)	22 Min	33 Sec	3.3 Sec
HD-Movie (16 GB)	9.3 Hr	13.9 Min	70 Sec

Image Source:

<https://static.makeuseof.com/wp-content/uploads/2016/08/usb-3-micro-cable.jpg>

Cables and Connectors

Registered Jack(RJ11)

- Standard telephone cable connectors,
- **RJ-11** has 4 wires (and RJ-12 has 6 wires). **RJ-11** is the acronym for Registered Jack-11, a four- or six-wire connector primarily used to connect telephone equipment.

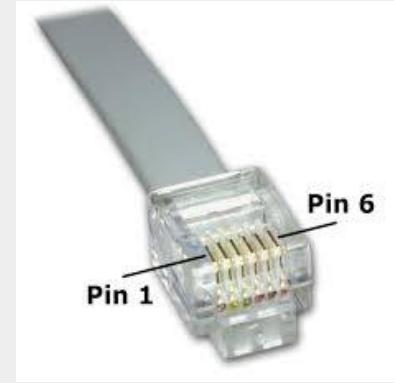


Image Source: <https://microchipdeveloper.com/jlink:mchp-adapter>

Cables and Connectors

RJ-45 (Registered Jack)

- RJ45 is commonly used to connect computers to a local area network (LAN).

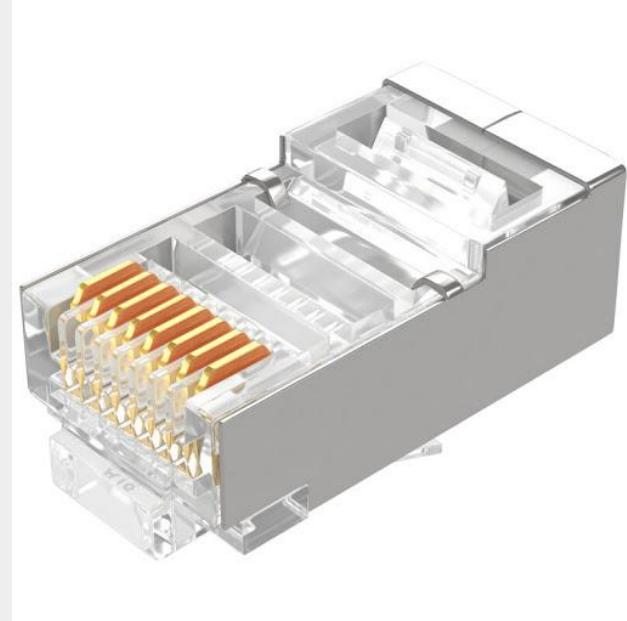


Image Source : <http://www.cns.lk/product/rj45-connector/>

Cables and Connectors

F-Type



- **F connector** is a type of RF connector commonly used for cable and universally for satellite television.

Image Source :

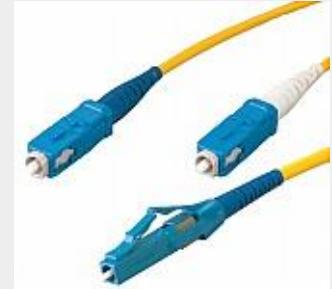
<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-connectors-types-and-specifications.html>

Cables and Connectors

ST (Straight Tip) and
SC (Subscriber Connector or
Standard Connector)



ST connector



SC connector

- Fiber network segments always require two fiber cables: one for transmitting data, and one for receiving.

Image Source :
<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-connectors-types-and-specifications.html>

Cables and Connectors

Fiber LC (Local Connector)

- These connectors are used for single-mode and multimode fiber-optic cables.



Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-connectors-types-and-specifications.html>

Cables and Connectors

MT-RJ (Mechanical Transfer Registered Jack)



- **MT-RJ** interfaces, use multimode fiber-optic cables.

Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/network-cable-connectors-types-and-specifications.html>

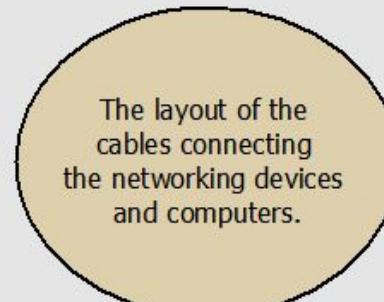
Physical and logical topologies

Topology

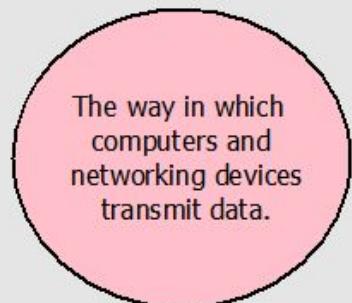
- Network topology is the layout of a network.
- It consists of two parts; **physical and logical**.
- The physical part describes the physical layout of a network while the logical part describes how the data flows in that network.
- Both, physical and logical parts are also known as the physical topology and the logical topology.
- **Physical part (topology) + Logical part (topology) = Network topology**

Network topology

The structure or map of the network.



Physical Topology



Logical topology

Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/network-topologies-explained-with-examples.html>

Physical and logical topologies

Types of Topology

- Physical network topology
- Logical network topology

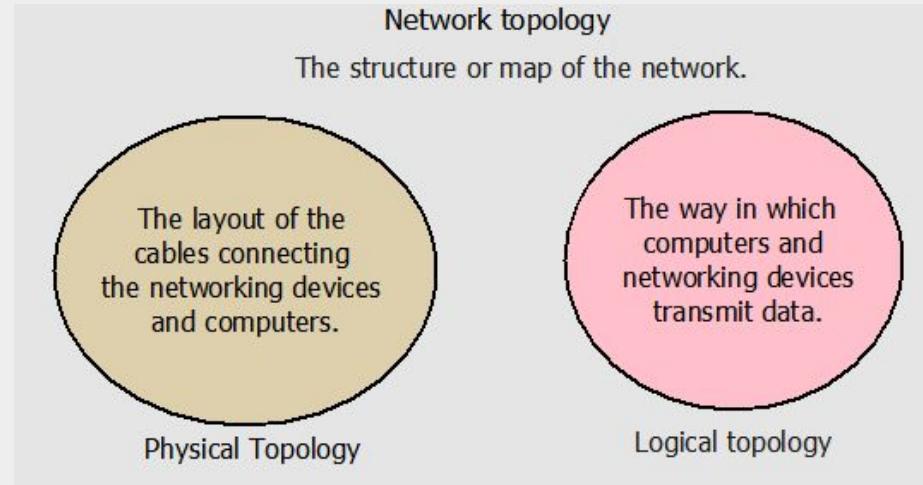


Image Source :

<https://www.computernetworkingnotes.com/networking-tutorials/network-topologies-explained-with-examples.html>

Physical and logical topologies

Hierarchical internetworking model

- Hierarchical Internetworking model divides enterprise networks into three layers.
- Core
- Distribution or Aggregation
- Access

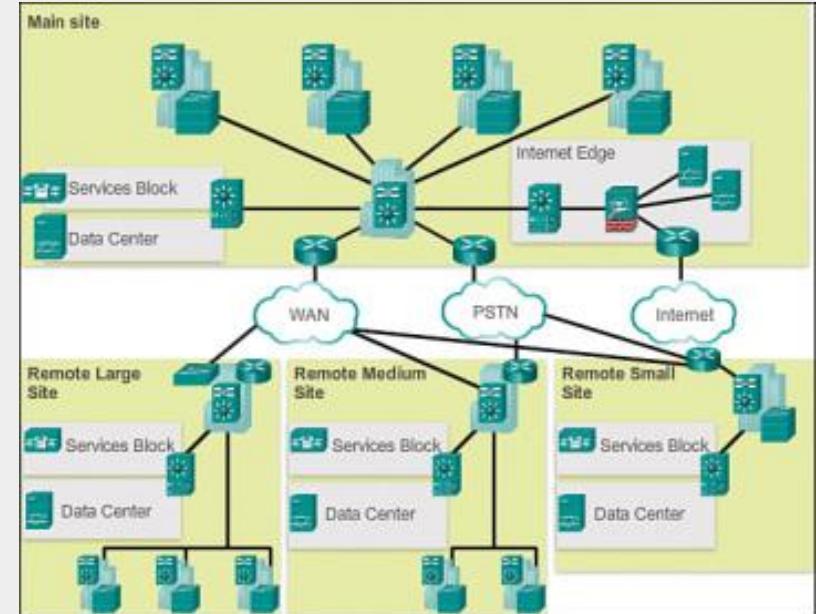


Image Source: <https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>

Physical and logical topologies

Leaf-Spine Network Topology

- The leaf-spine topology is a special case of a two-layer model, designed to build fast, predictable, scalable and efficient data centre network infrastructure

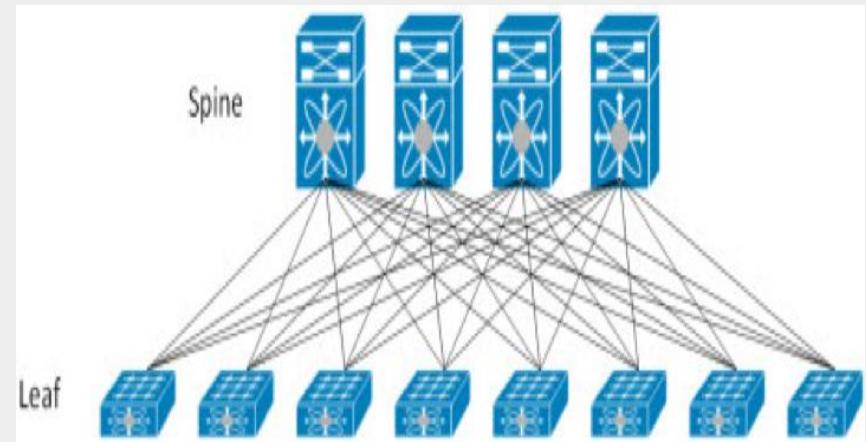


Image Source :
<https://blogs.arubanetworks.com/solutions/network-topologies-logical-vs-physical/>

Bus topology

What is bus topology

- Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.

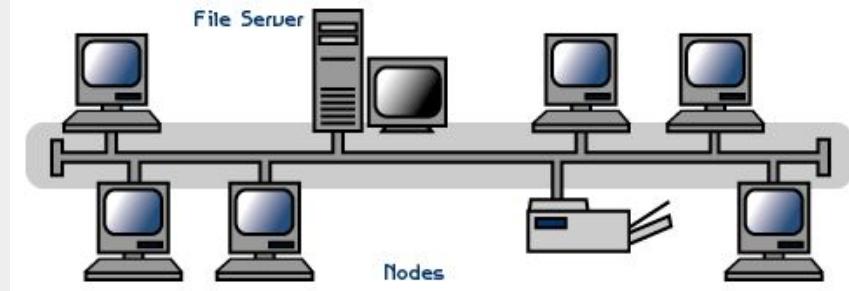


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

Bus topology

Features

- It transmits data only in one direction.
- Every device is connected to a single cable

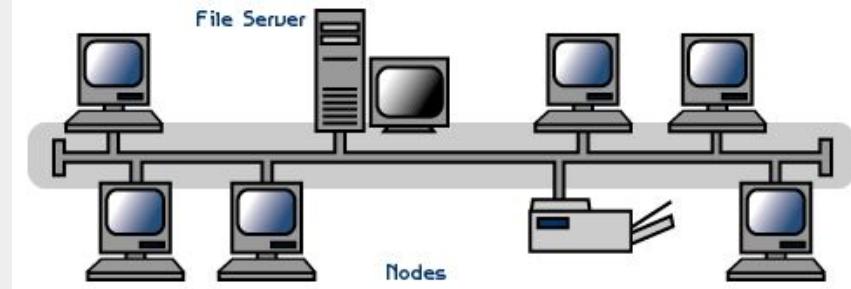


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

Bus topology

Advantage & Disadvantages

- **Advantages of a Linear Bus Topology**
 - It is cost effective.
 - Cable required is least compared to other network topology.
 - Used in small networks.
 - It is easy to understand.
 - Easy to expand joining two cables together.

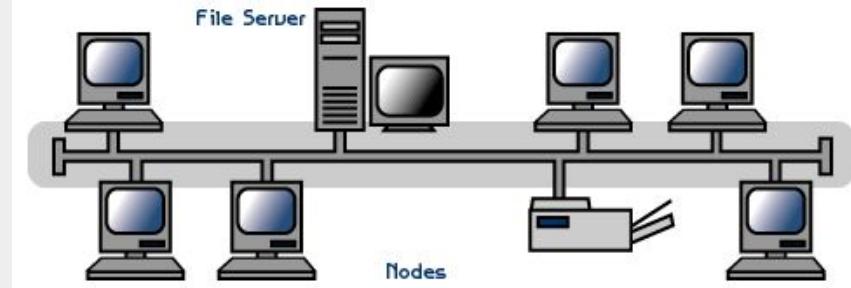


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

Bus topology

Advantage & Disadvantages

- **Disdvantages of a Linear Bus Topology**
 - Cables fails then whole network fails.
 - If network traffic is heavy or nodes are more the performance of the network decreases.
 - Cable has a limited length.
 - It is slower than the ring topology.

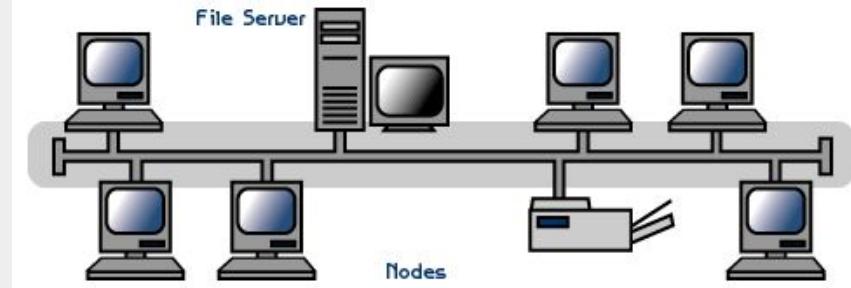


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

Star Topology

- In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

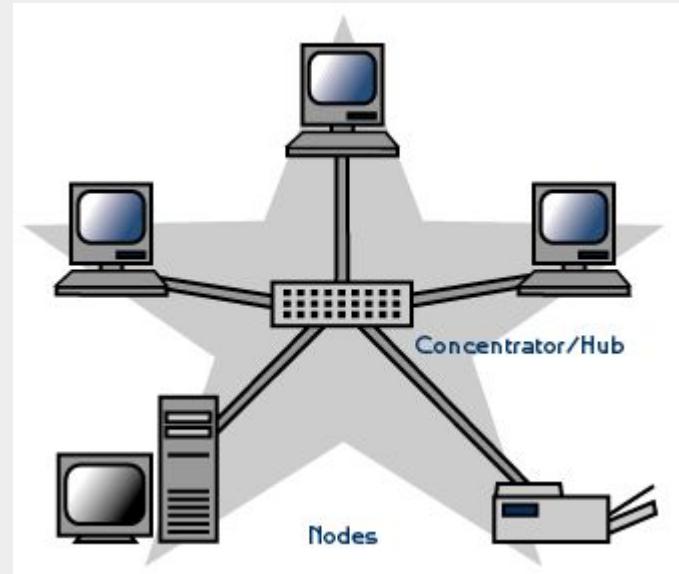


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

Star Topology

Features

- Every node has its own dedicated connection to the hub.
- Hub acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fibre or coaxial cable.

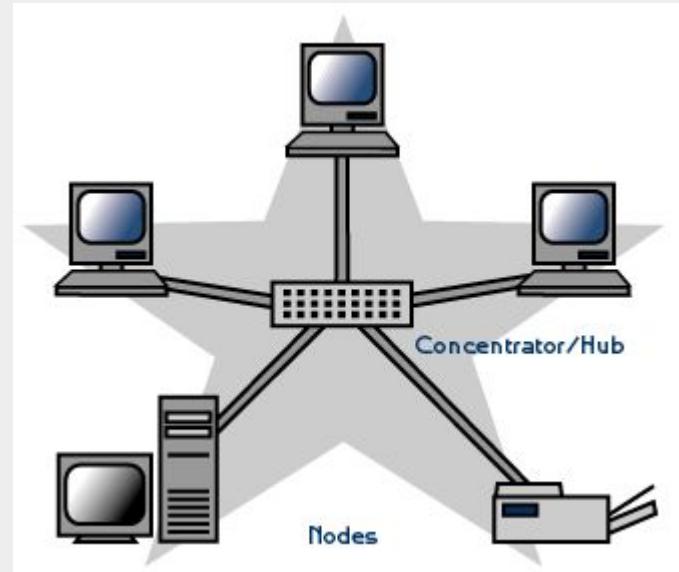


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

Star Topology

Advantage & Disadvantage

- **Advantages of Star Topology**
 - Fast performance with few nodes and low network traffic.
 - Hub can be upgraded easily.
 - Easy to troubleshoot.
 - Easy to setup and modify.
 - Only that node is affected which has failed, rest of the nodes can work smoothly

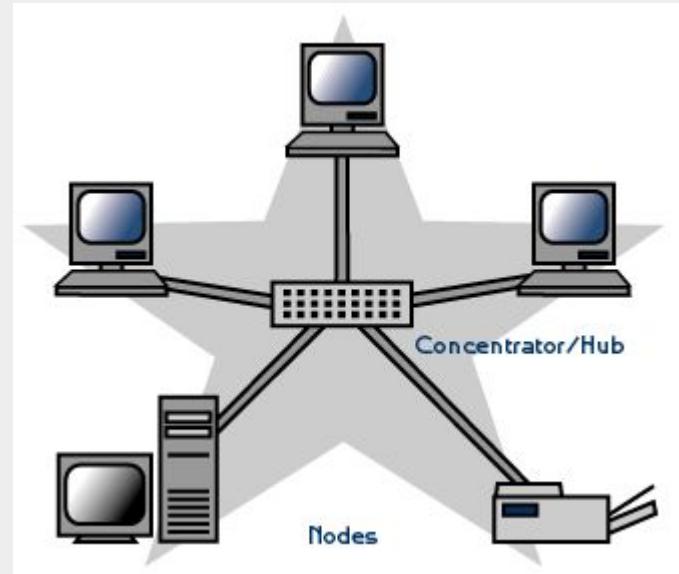


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

Star Topology

Advantage & Disadvantage

- **Disadvantages of Star Topology**
 - Cost of installation is high.
 - Expensive to use.
 - If the hub fails then the whole network is stopped because all the nodes depend on the hub.
 - Performance is based on the hub that is it depends on its capacity

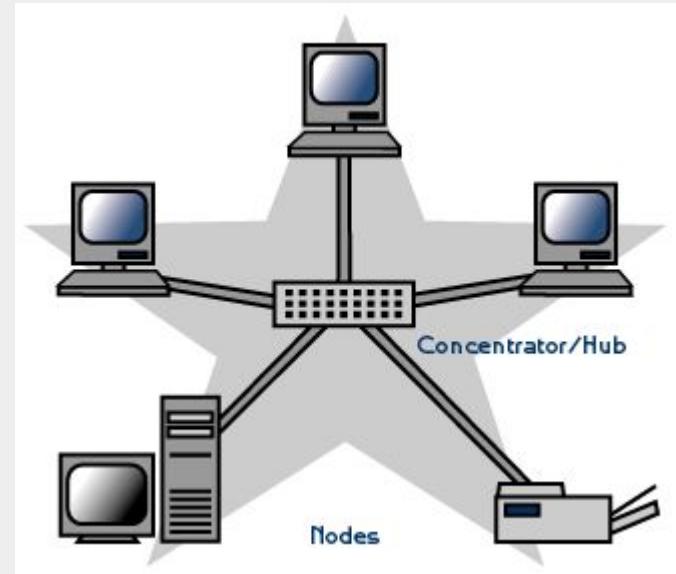


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

Star Topology

Tree or Expanded Star

- A tree topology combines characteristics of linear bus and star topologies.
- It consists of groups of star-configured workstations connected to a linear bus backbone cable .
- Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

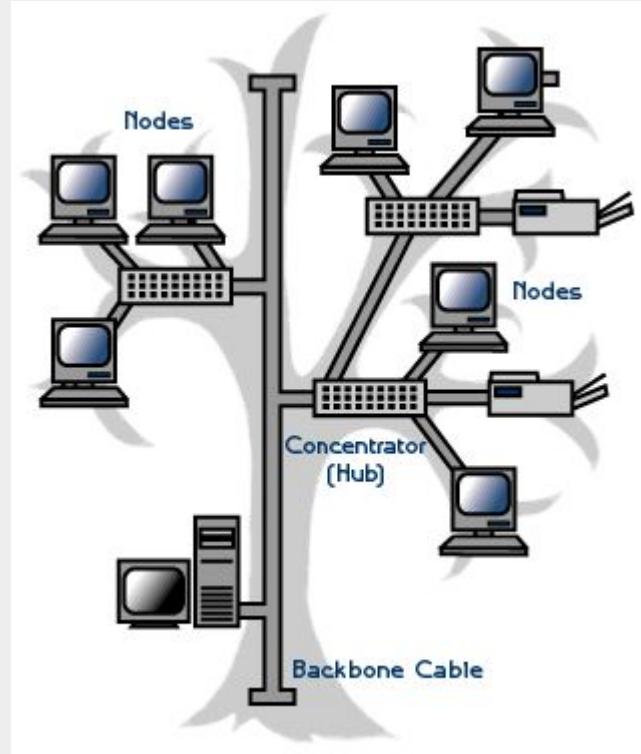
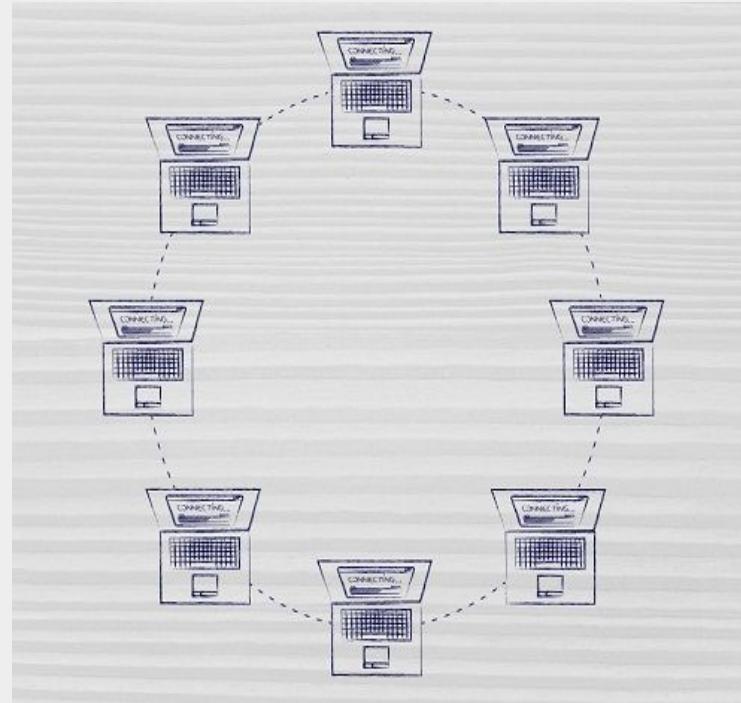


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

Ring Topology

What is Ring Topology?

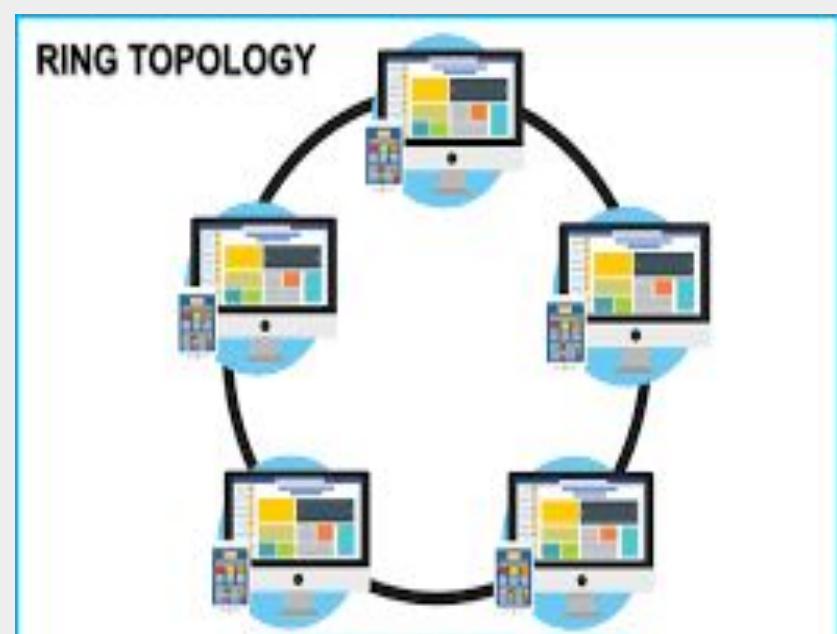
- Each device/node is connected with its neighboring node forming the shape of ring hence it is known as Ring Topology.
- In ring topology the data circulate from one computer to another.
- In case of any failure in a computer or cable breaks the entire network can be shutdown.
- When a terminal has to send data, it transmits it to the neighboring node which transmits it to the next one.



Ring Topology

Advantages of Ring Topology

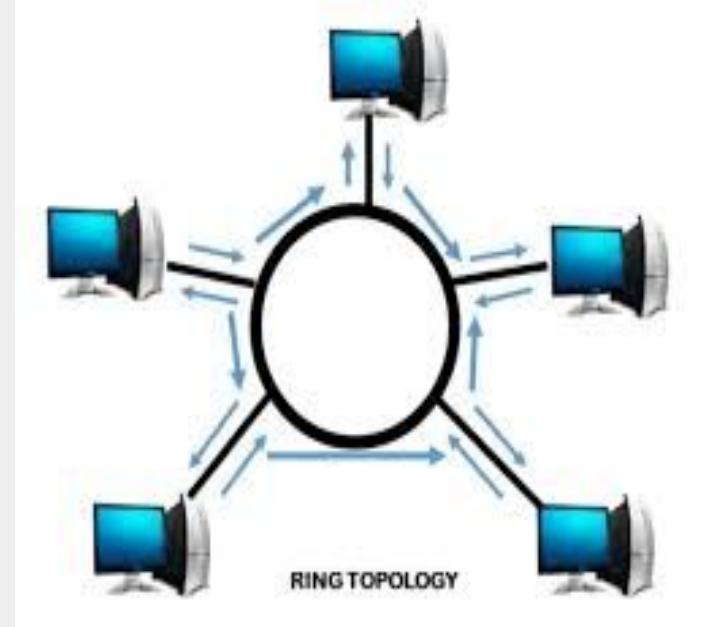
- Small cable segments are needed to connect two nodes
- Ideal for optical fibres as data travels in only one direction
- Very high transmission speeds possible



Ring Topology

Disadvantages of Ring Topology

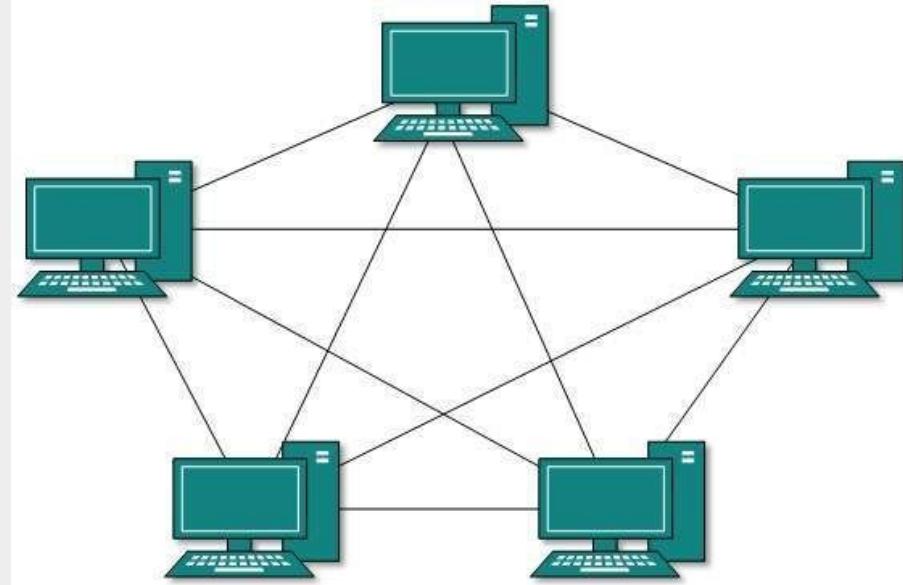
- Failure of single node brings down the whole network
- Troubleshooting is difficult as many nodes may have to be inspected before faulty one is identified
- Difficult to remove one or more nodes while keeping the rest of the network intact



Mesh Topology

What is Mesh Topology?

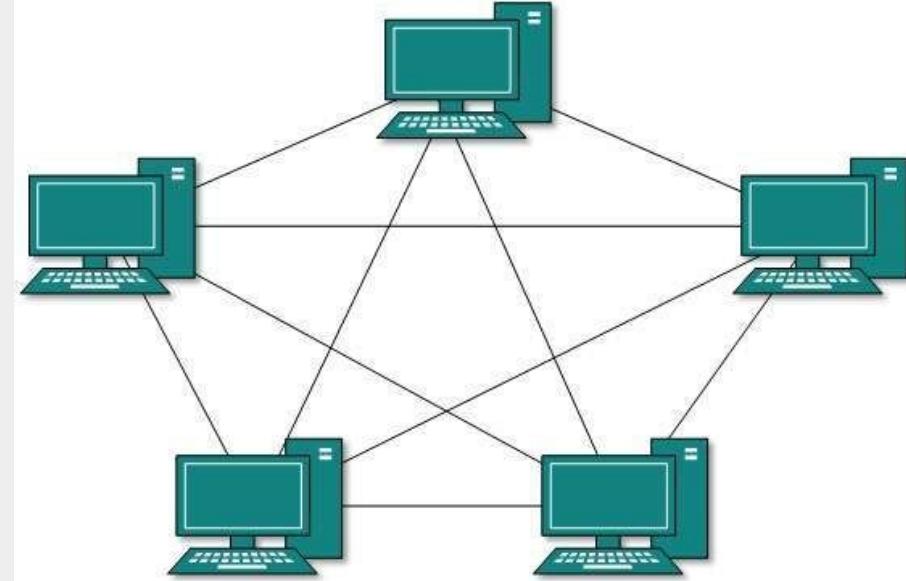
- In this type of topology, a host is connected to one or multiple hosts.
- This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.
- It is a topology commonly used for wireless networks.



Mesh Topology

Advantages of Mesh Topology

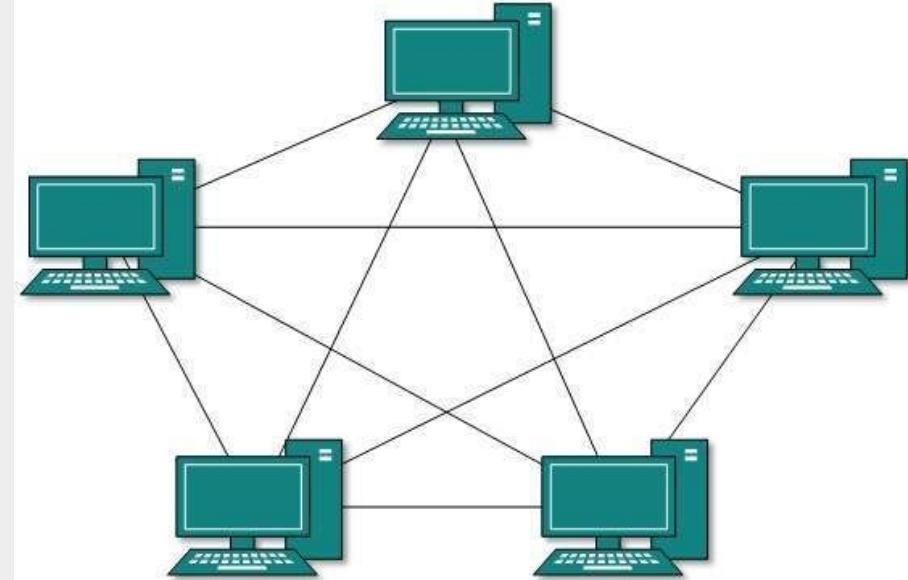
- Manages high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.



Mesh Topology

Disadvantages of Mesh Topology

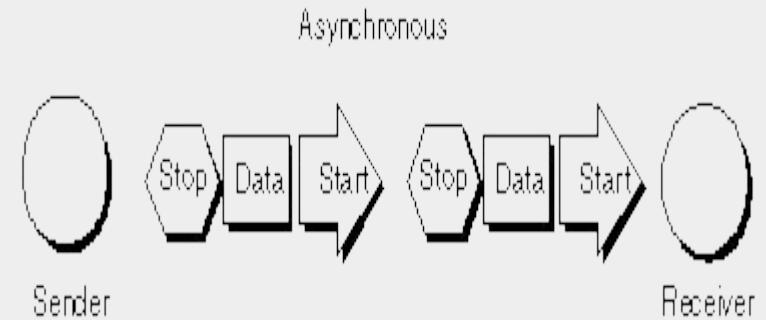
- The cost to implement is higher than other network topologies, making it a less desirable option.
- Building and maintaining the topology is difficult and time consuming.
- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.



Asynchronous Transmission

What is Asynchronous Transmission?

- In asynchronous transmission, data moves in a half-paired approach, 1 byte or 1 character at a time.
- The size of a character transmitted is 8 bits, with a parity bit added both at the beginning and at the end, making it a total of 10 bits.
- It is straightforward, quick, cost-effective, and doesn't need 2-way communication to function.

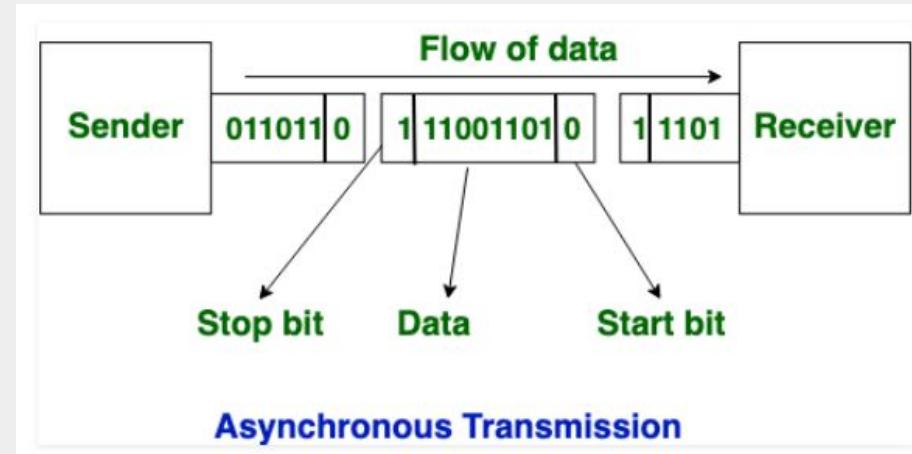


ImageSource:<https://www.webopedia.com/FIG/ASYNC.gif>

Asynchronous Transmission

Characteristics of Asynchronous Transmission

- Each character is headed by a beginning bit and concluded with one or more end bits.
- There may be gaps or spaces in between characters.



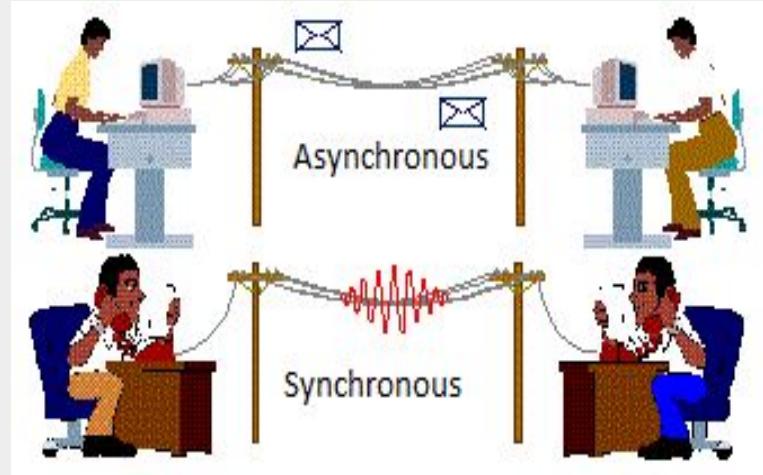
Asynchronous Transmission

Asynchronous Transmission

Examples of Asynchronous Transmission

Examples of Asynchronous Transmission

- Emails
- Forums
- Letters
- Radios
- Televisions

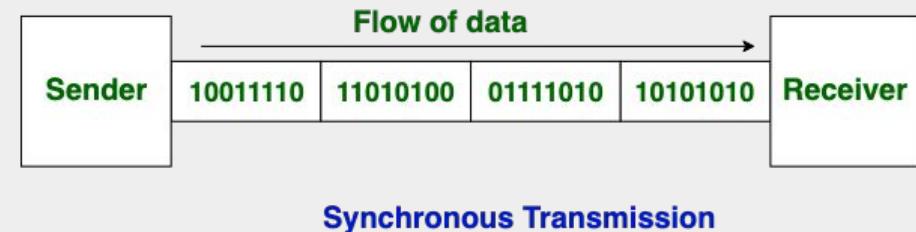


ImageSource:<https://2.bp.blogspot.com/-hs01gQedFFI/WB9MW4o7X3I/AAAAAAAAPq8/TbpnJuAwBGs6cT6V14FtFC9CR8UQstqoACLcB/w1200-h630-p-k-no-nu/difference-between-synchronous-and-asynchronous-messages.gif>

Synchronous Transmission

What is Synchronous Transmission?

- In Synchronous Transmission, data is sent in form of blocks or frames. This transmission is the full duplex type.
- Between sender and receiver the synchronization is compulsory. In Synchronous transmission, There is no gap present between data.
- It is more efficient and more reliable than asynchronous transmission to transfer the large amount of data.

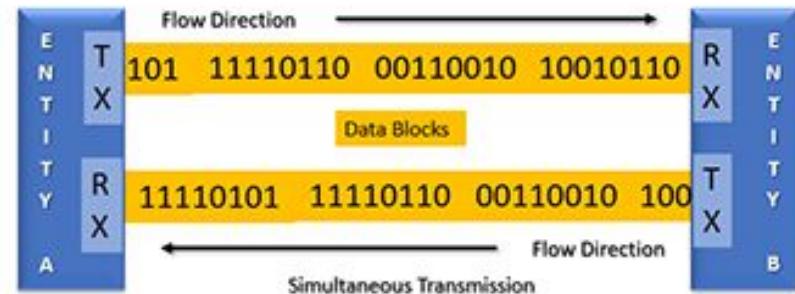


Asynchronous Transmission

Characteristics of Synchronous Transmission

- There are no spaces in between characters being sent.
- Timing is provided by modems or other devices at the end of the transmission.
- Special 'syn' characters goes before the data being sent.
- The syn characters are included between chunks of data for timing functions.

Synchronous Transmission

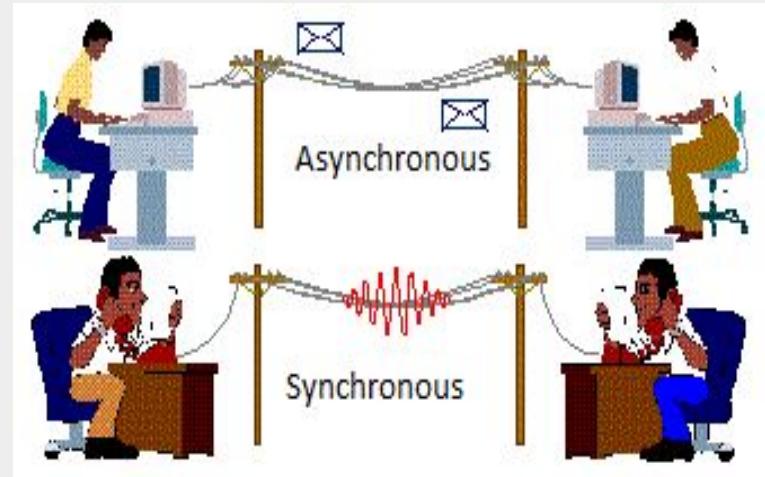


Asynchronous Transmission

Examples of Synchronous Transmission

Examples of Synchronous Transmission

- Chat rooms
- Video conferencing
- Telephonic conversations
- Face-to-face interactions



ImageSource:<https://2.bp.blogspot.com/-hs01gQedFFI/WB9MW4o7X3I/AAAAAAAAPq8/TbpnJuAwBGs6cT6V14FtFC9CR8UQstqoACLcB/w1200-h630-p-k-no-nu/difference-between-synchronous-and-asynchronous-messages.gif>

Asynchronous Transmission

Difference Between Synchronous and Asynchronous Transmission

- Both synchronous and asynchronous transmission have their benefits and limitations.
- Asynchronous transmission is used for sending a small amount of data
- while synchronous transmission is used for sending bulk amounts of data.

Synchronous and Asynchronous Transmission

Point of Comparison	Synchronous Transmission	Asynchronous Transmission
Definition	Transmits data in the form of chunks or frames	Transmits 1 byte or character at a time
Speed of Transmission	Quick	Slow
Cost	Expensive	Cost-effective
Time Interval	Constant	Random
Gaps between the data?	Yes	No
Examples	Chat Rooms, Telephonic Conversations, Video Conferencing	Email, Forums, Letters

Configure different protocol services

In this section, we will discuss:

- User Authentication Strategy
- OU Structure
- User Environment
- Group Policies
- AGDLP Process
- Different types of protocols - TCP/IP,HTTP, FTP,SMTP
- OSI Model
- Media Access Method
- DNS services

In this section, we will discuss:

- DHCP services
- WINS services
- RAS services
- Web services
- Proxy Services

User Authentication Strategy

Define User Authentication Strategy

- User authentication or verification is a process that lets a device to authenticate the recognize somebody who links to a network resource.
- In simple terms, user authentication is the process of human to machine transfer of credentials necessary for confirmation of a user's authenticity.
- The user authentication happens on both wired and wireless networks.

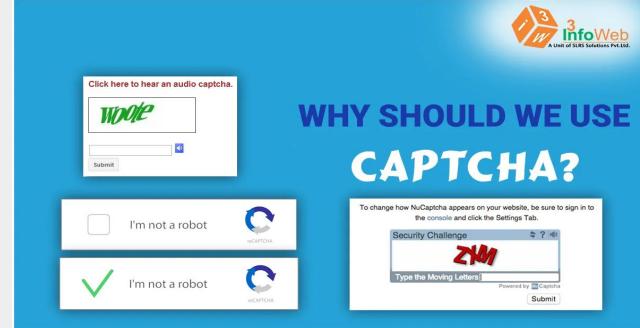


ImageSource: https://cdn.ttgtmedia.com/rms/onlineImages/security-twofactor_authentication.jpg

User Authentication Strategy

Define User Authentication Strategy (Continued)

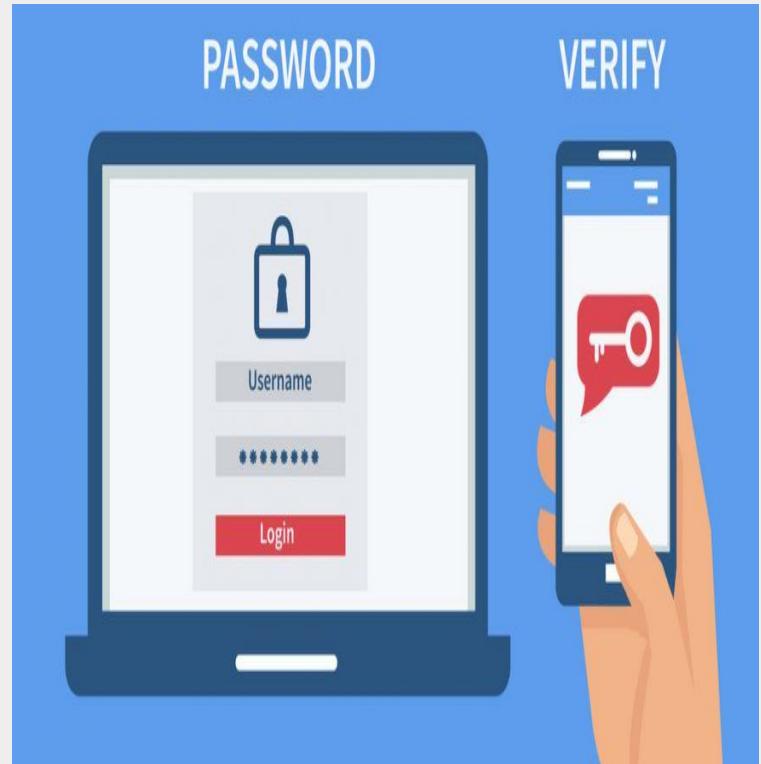
- Today we have multiple means of user authentication such as one-time password, text captcha, image captcha, number captcha, logical questions, face recognition, thumb impression, retina scan, and many other methods.



User Authentication Strategy

Purpose of Authentication strategy

- Authentication is used to verify that you are who you say you are.
- After a user's identity is confirmed, for instance with a username and password, that identity may be used in an authorization policy to determine the appropriate access privileges.
- Organizations today must ensure that the right users are given access to the right resources, whether it is physical or--increasingly--digital.



ImageSource:<https://www.channelfutures.com/files/2019/10/Two-Factor-Authentication-877x432.jpg/>

User Authentication Strategy

Types of Authentications

- Two-factor authentication (2FA) -It combines a username and password, or PIN, with a physical or mobile token for extra security.
- Three-factor authentication (3FA)-along with 2FA it uses biometrics such as fingerprints to verify a user's identity.
- Four-factor authentication (4FA)-along with 3FA it involves knowledge, possession, inherence, and location.

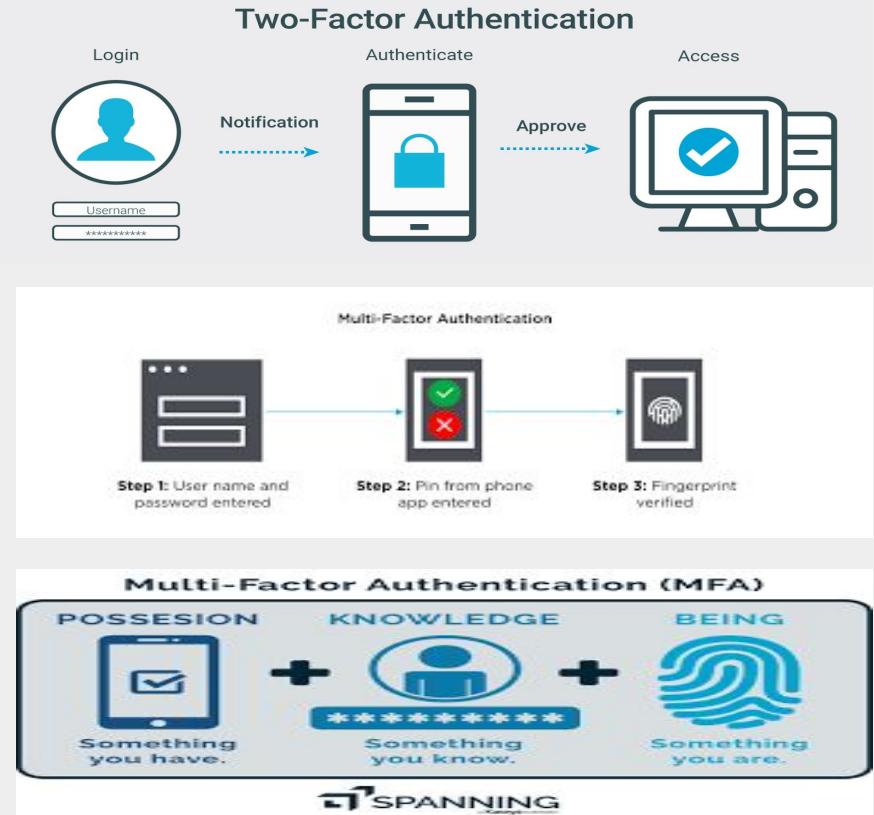


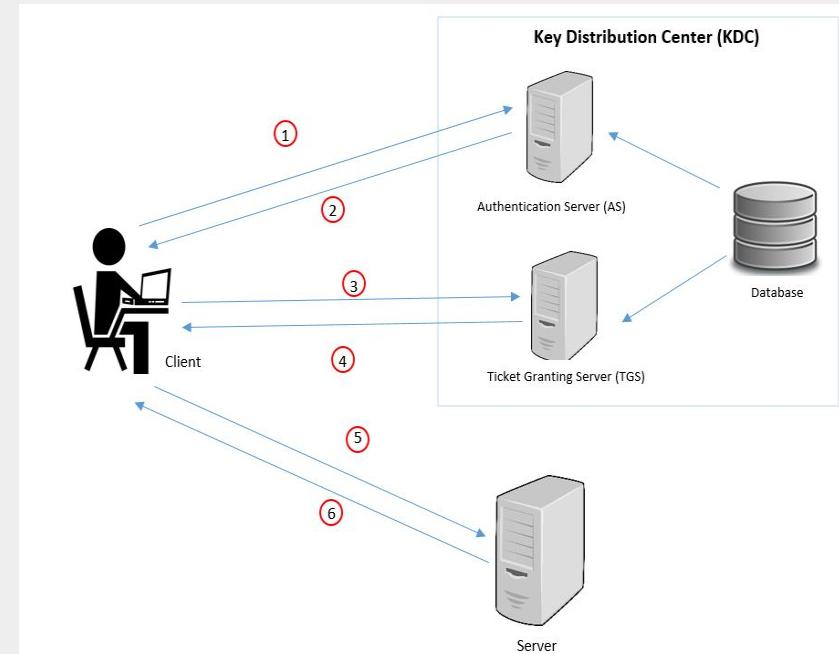
Image Source: <https://www.avatier.com/blog/defining-multi-factor-authentication-need-now/>

User Authentication Strategy

Types of Authentication Protocols

There are several different authentication protocols for network access control, including:

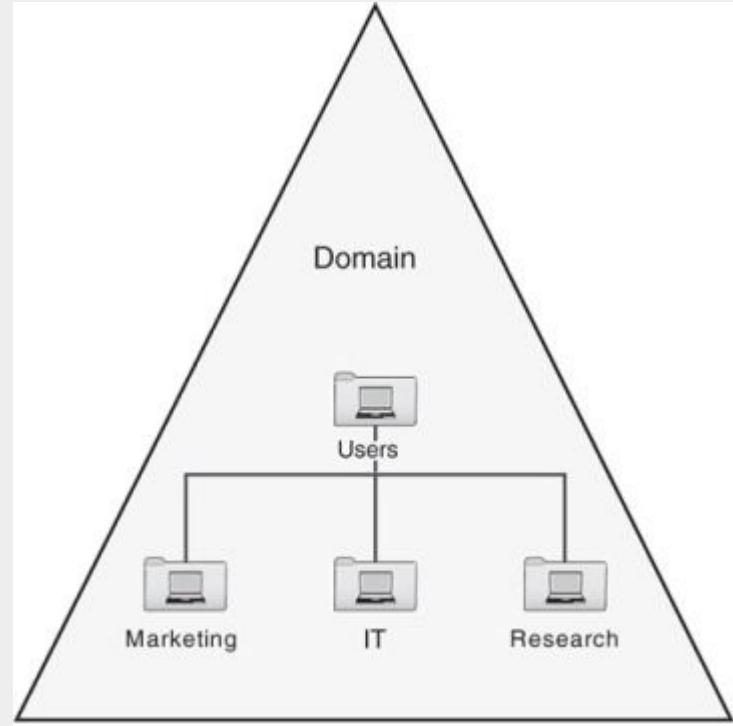
- Kerberos
- Extensible Authentication Protocol (EAP)
- IEEE 802.1X
- Remote Authentication Dial-In User Service (RADIUS)
- Terminal Access Controller Access-Control System (TACACS)



OU Structure

Define Organization Unit

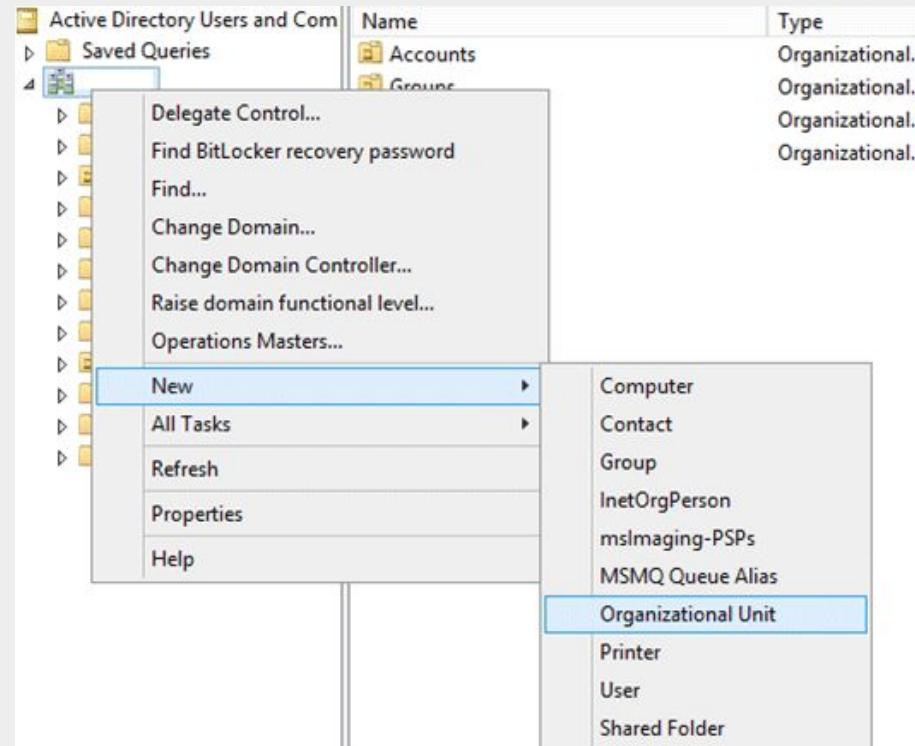
- The Organizational Unit (OU) is a sub-division in an Active directory into which, we can place users, groups, computers and other organizational units.
- Using organizational units, we can create containers within a domain that represent the hierarchical, logical structures within organization.
- We can manage the configuration and use of accounts and resources based on your organizational model.



OU Structure

Tasks of Organization Unit

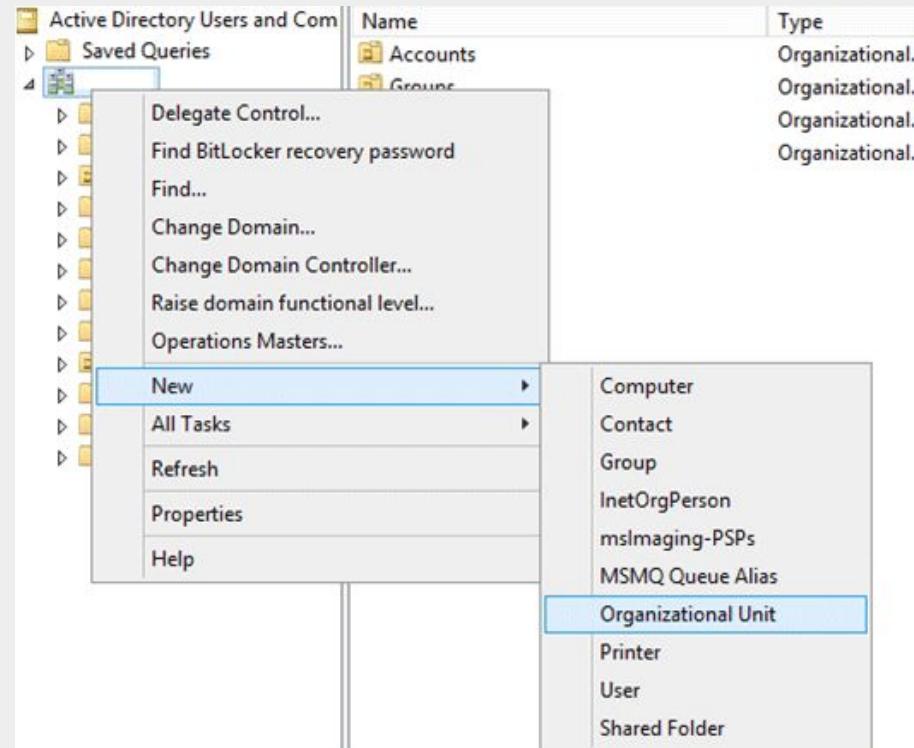
- Managing users (create, delete, etc.)
- Managing groups
- Modifying group membership
- Managing group policy links
- Resetting passwords on user accounts



OU Structure

Benefits of Organization Structure

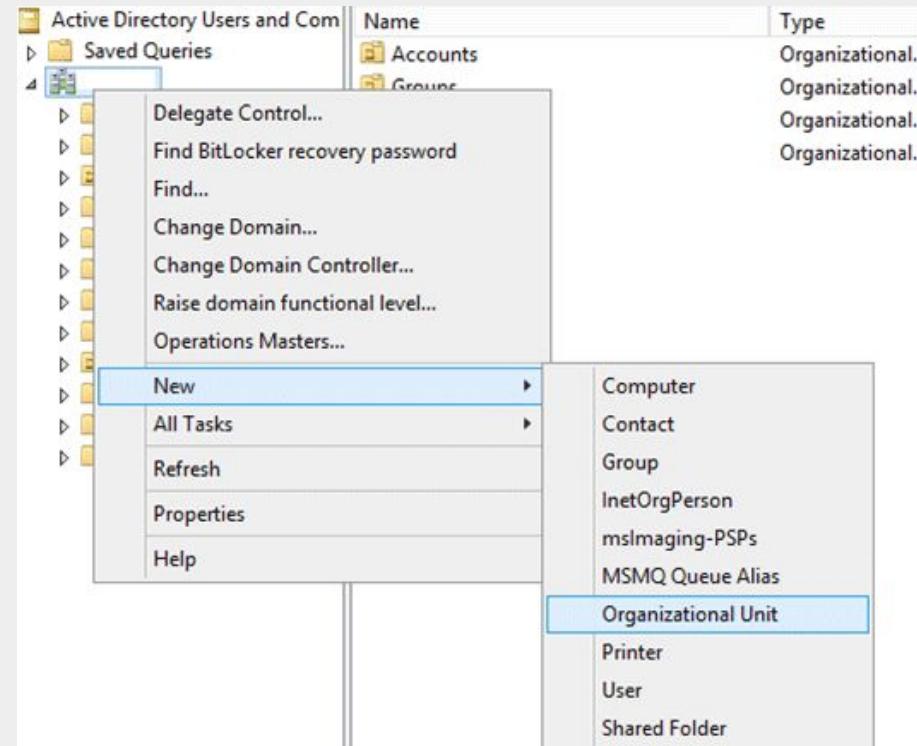
- OUs can be nested to support different hierarchy levels. Each domain in the Active Directory environment can have its own OU structure.
- One domain's OU structure is independent of another domain's OU structure.
- It is fairly simple to change an OU structure.
- OU structures are much more flexible than domain structures.



OU Structure

Benefits of Organization Structure (Continued)

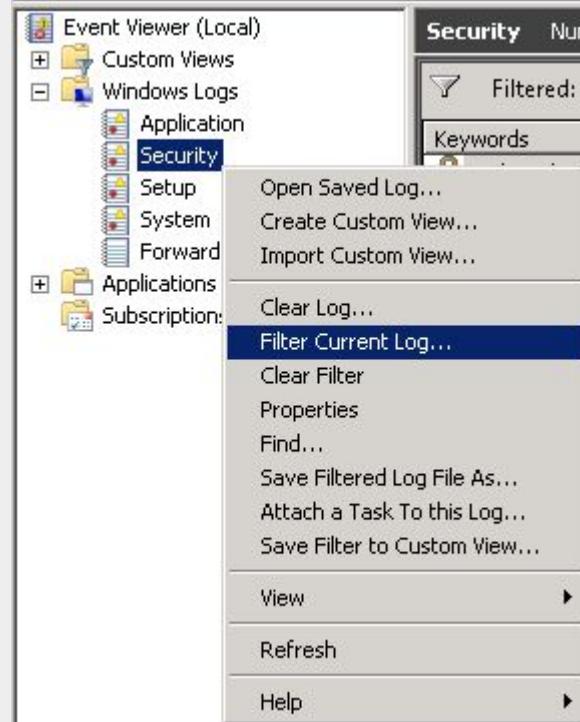
- Objects in child OUs can inherit OU configuration settings.
- Group Policy settings can also be applied to OUs
- Users can delegate administrative control of Active Directory objects through OUs



User Environment

What is User Environment?

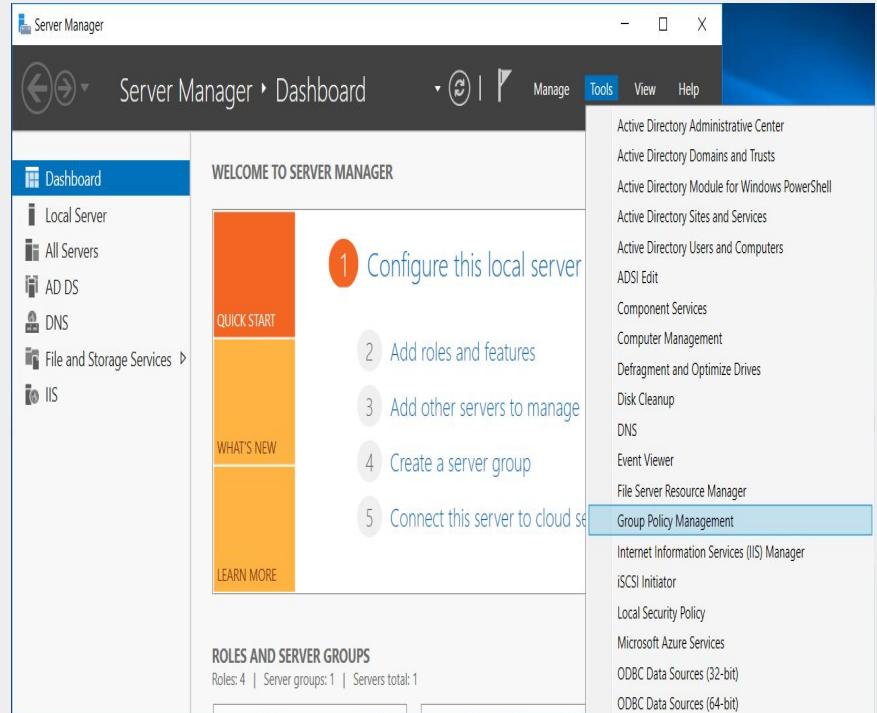
- A user environment is a set of distributed objects that collectively, completely characterize the activity of a user in a universal system.
- A user environment is then an abstraction that captures the essence of a user in a universal system and consists of:
 - environment identification
 - user profile
 - user location
 - user activity



Group Policy

Group policy Object

- Group Policies are computer or user settings that can be defined to control or secure the Windows server and client infrastructure.
- Two main components of Group Policy are,
 1. GPO Object and
 2. GPO Policy Settings.



Group Policy

Group Policy Settings?

- GPO policy settings are the real settings within GPO object that defines particular action.
- GPO policy settings comes from GPO templates which are stored in **SYSVOL** folder of each domain controller.
- After creating a group policy, it can be linked to Sites, Domains and OUs. Group policy is process in the order of **LSDOU**: –
 1. Local Group Policy
 2. Sites
 3. Domains
 4. Organizational OUs

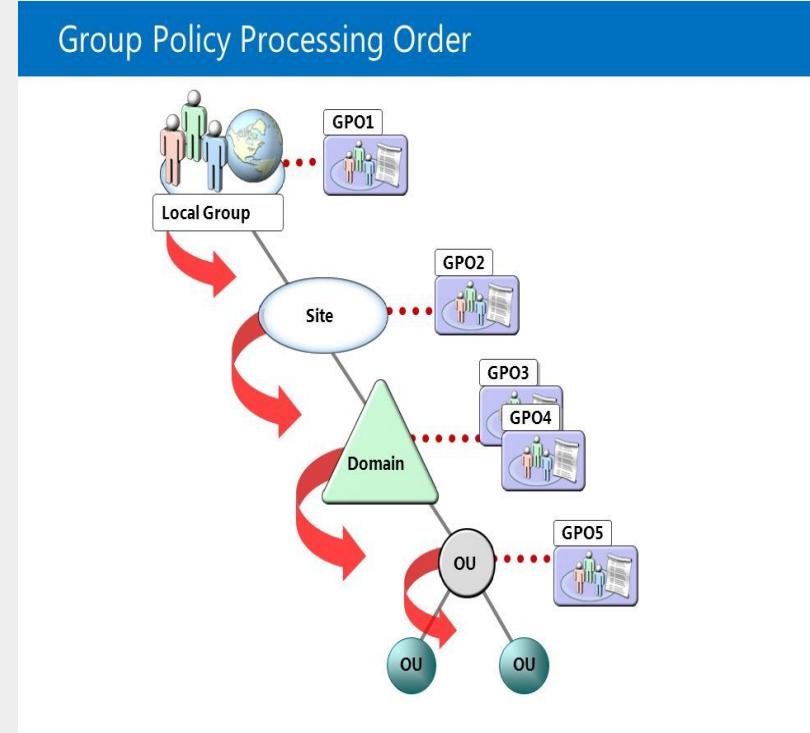
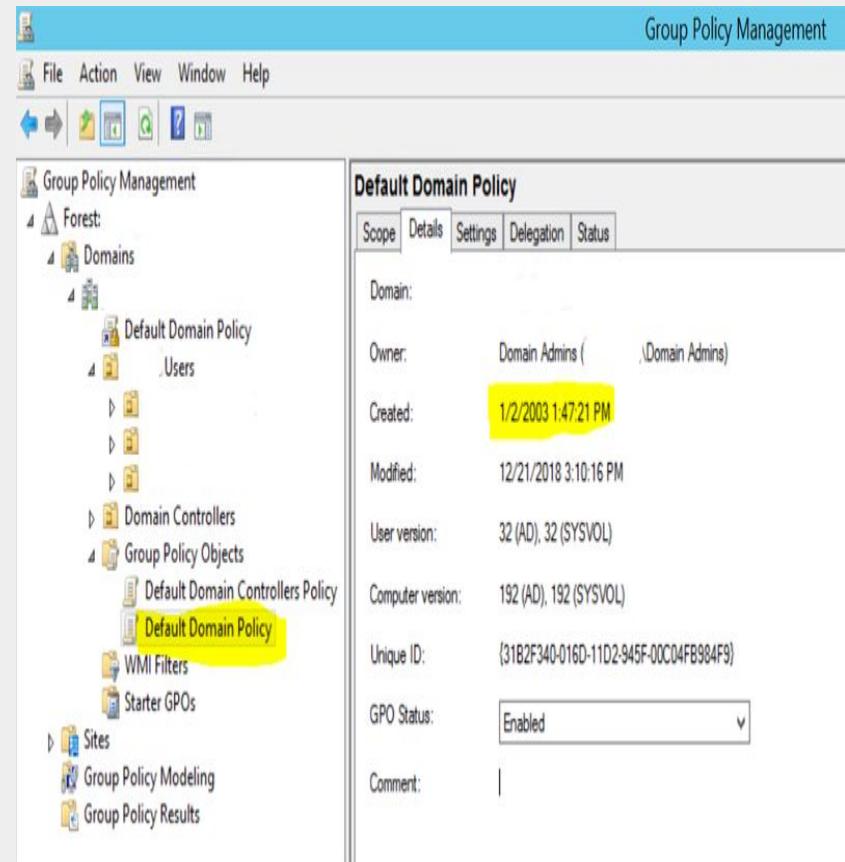


Image Source: <https://slideplayer.com/slide/9141558/27/images/24/Group+Policy+Processing+Order.jpg>

Group Policy

Types of Group Policy Settings

- In fresh domain controller there are two default group policy settings configured. They are: –
- Default Domain Policy
- Default Domain Controller Policy

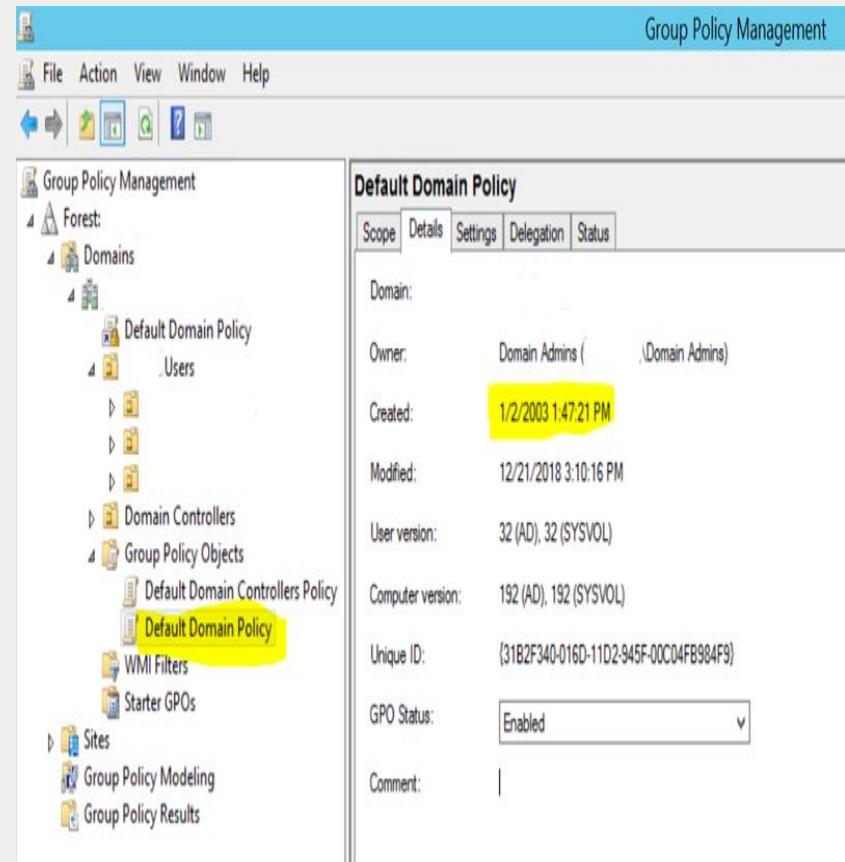


ImageSource: <https://i.stack.imgur.com/gACXZ.png>

Group Policy

Default Domain Policy

- This policy is linked to the entire domain and has policies like password policies, account lockout policies and kerberos protocol policies.
- It is recommended that not to edit this policy.
- If you want to link new group policy then create new GPO and link to the domain.

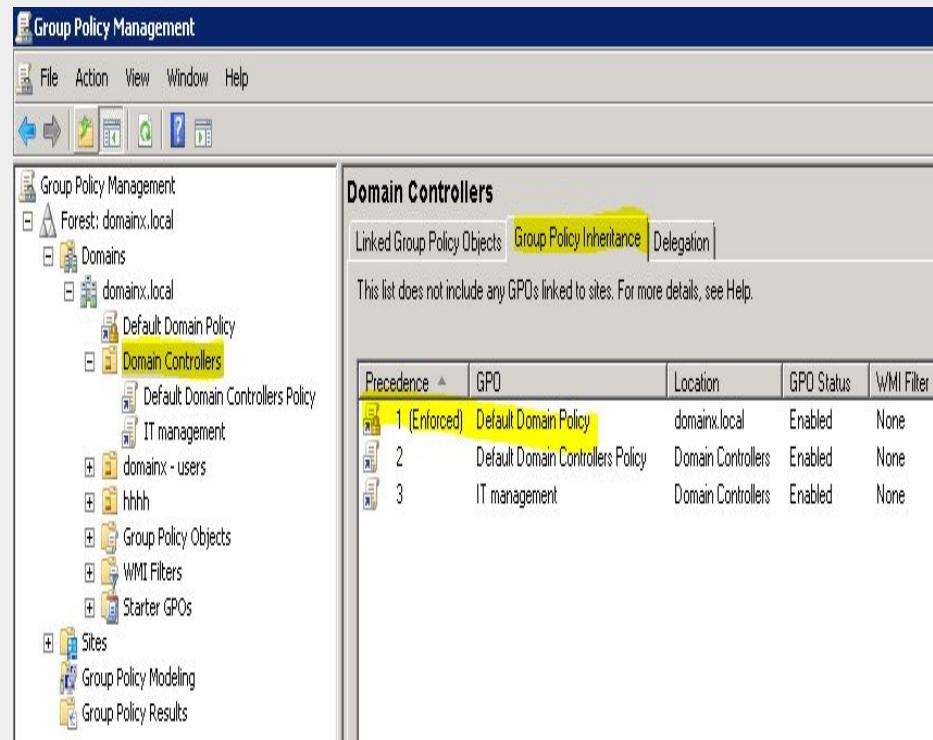


ImageSource: <https://i.stack.imgur.com/gACXZ.png>

Group Policy

Default Domain Controller Policy

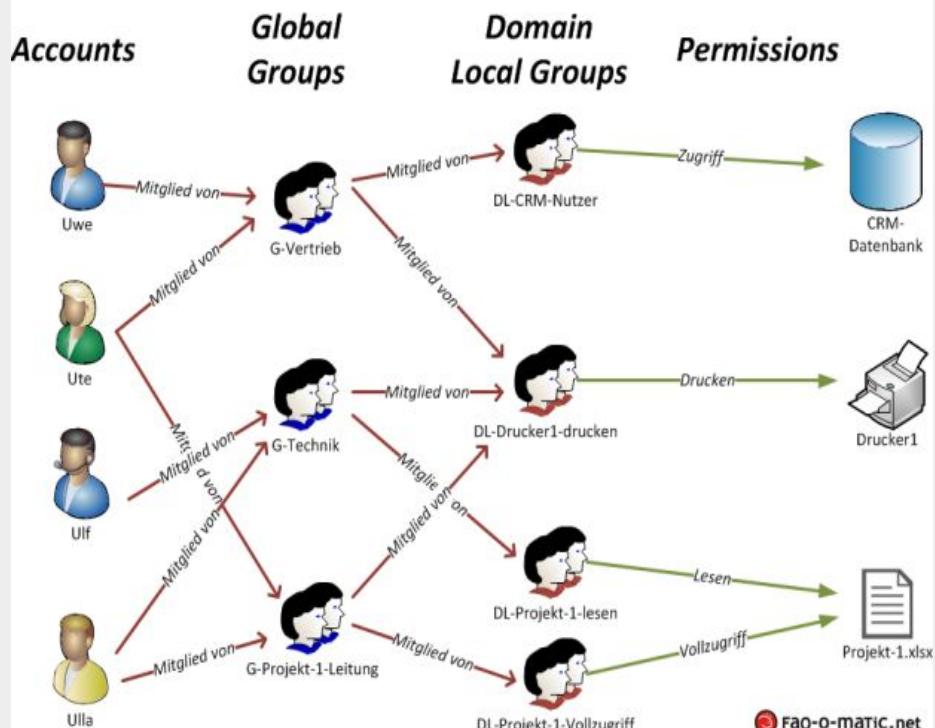
- This policy setting is applied to domain controllers and is linked to domain controllers OU. This policy affects domain controllers only.



AGDLP Process

Introduction

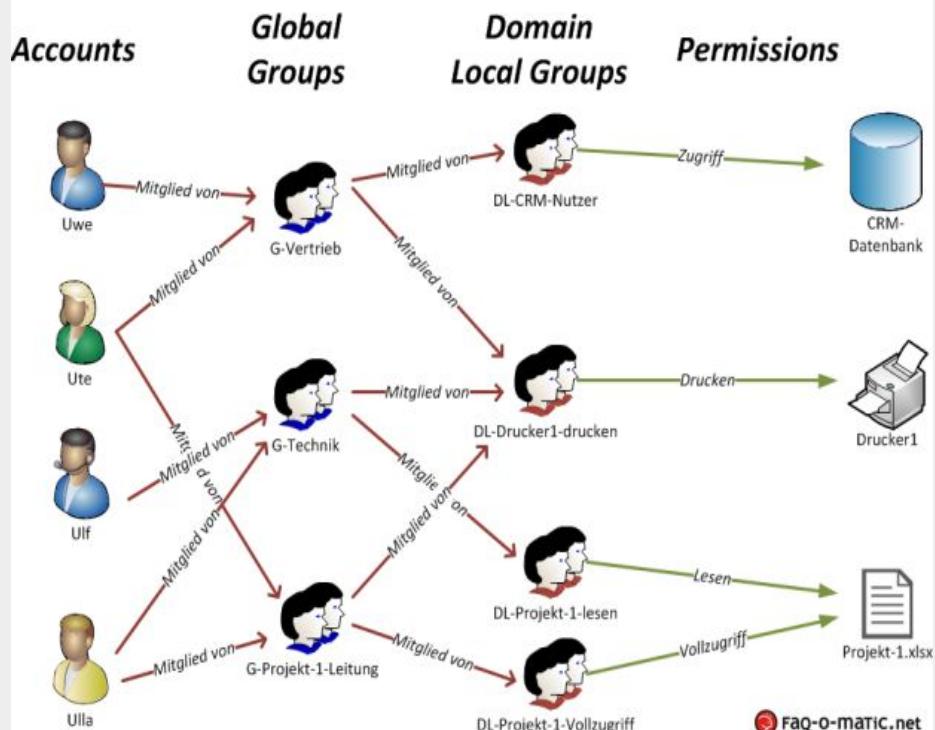
- AGDLP is a role based strategy that is designed to provide flexible resource management using groups.
- Managing those permissions and group memberships are simplified and configured to allow for multiple domains.



AGDLP Process

Introduction

- AGDLP - ADDLP stands for the following.
- A for Accounts.
- G for Global Group.
- DL for Domain Local Group.
- P for Permissions.



AGDLP Process

Advantages of AGDLP

- AGDLP is a role base strategy for applying permissions, as a user changes their role in an organization.
- Looking at the users in the groups, you can quickly determine who has access to which resources in your domain.

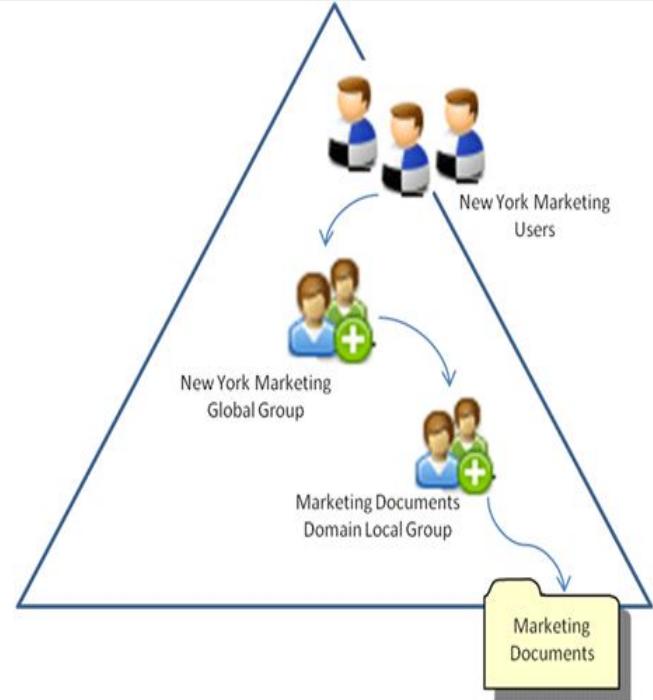


Image Source:

<https://mk0resourcesinfm536w.kinstacdn.com/wp-content/uploads/AGDLP11132011-15>

AGDLP Process

Advantages of AGDLP

- Domain Local Groups can only be used in the domain that the group was created in.
- Helps for auditing.

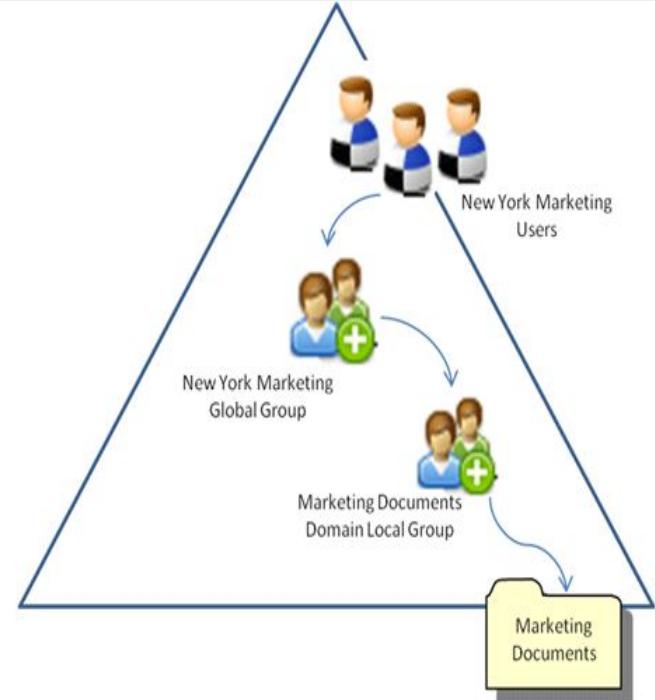
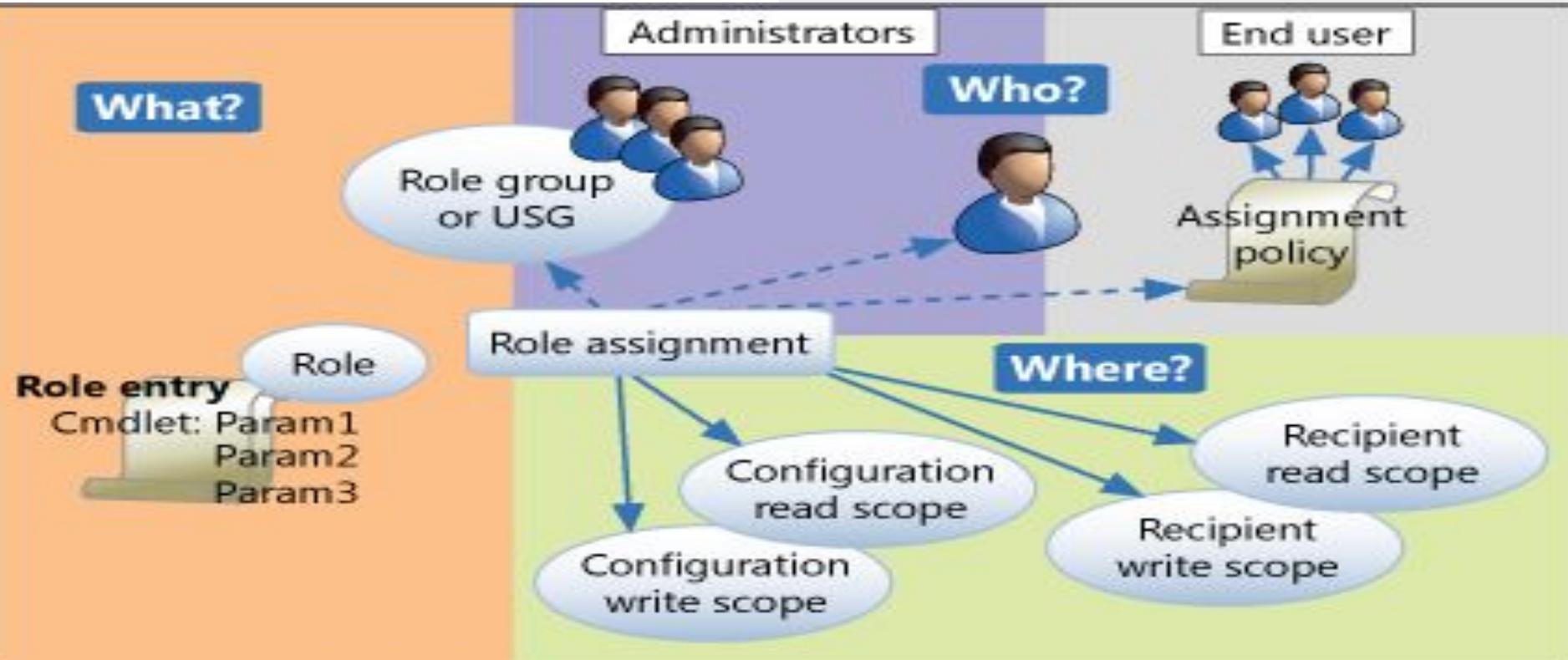


Image Source:

<https://mk0resourcesinfm536w.kinstacdn.com/wp-content/uploads/AGDLP11132011-15>

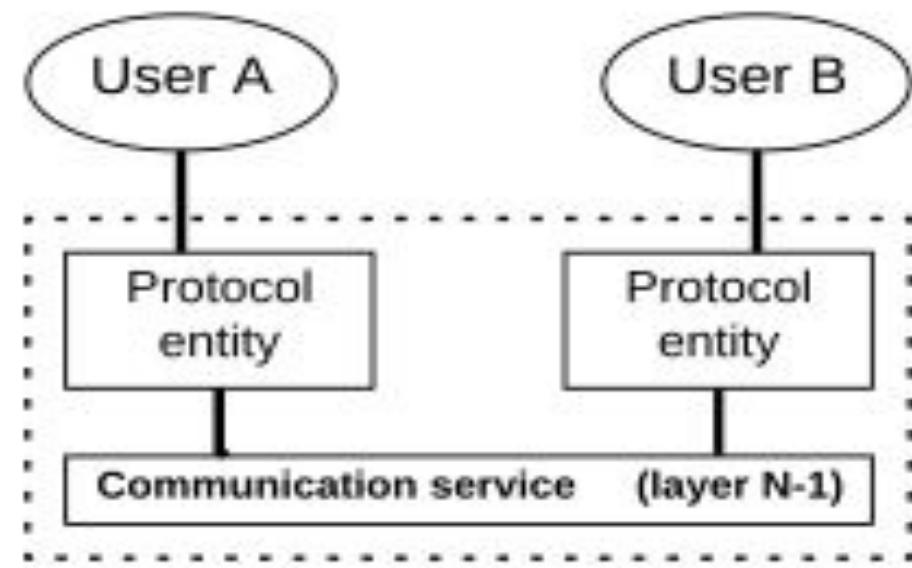
ADGLP Process



Different types of protocols

Definitions

- Definition 1: A protocol is a standard set of rules that allow electronic devices to communicate with each other.
- Definition 2: A protocol is a set of guidelines to govern the data transfer between the devices.



Transmission Control Protocol

Introduction

- It provides a full transport layer services to applications.
- TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames.

TCP header format

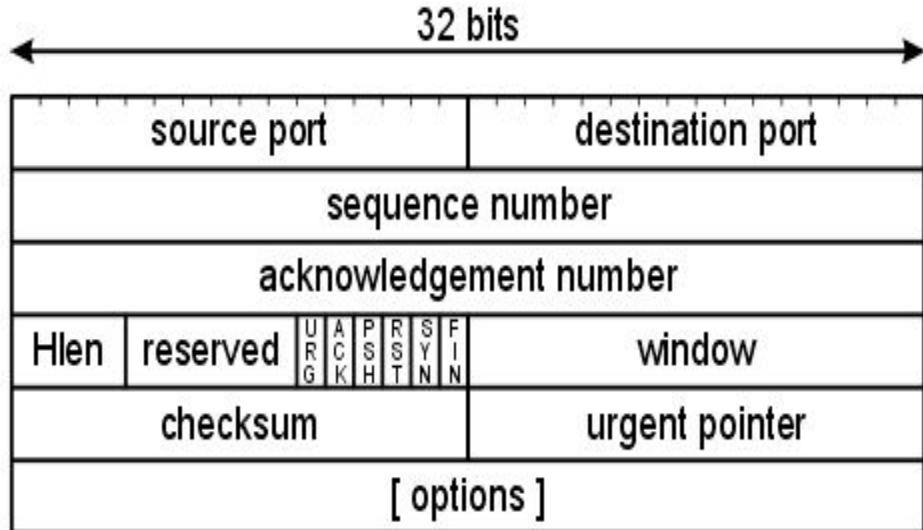


Image Source:

<https://lh3.googleusercontent.com/proxy/MmQAc8LIPH97fO51WtYBRv6hMEL4GN1G-Cg-NQWYI-C-4i-XDwHL71JGGLoYEY15EK-4i-2JUKWJLBPUIC>

Transmission Control Protocol

Transmission Control Protocol Offers

- Stream Data Transfer.
- Reliability.
- Efficient Flow Control
- Full-duplex operation.
- Multiplexing.
- TCP offers connection oriented end-to-end packet delivery.

TCP header format

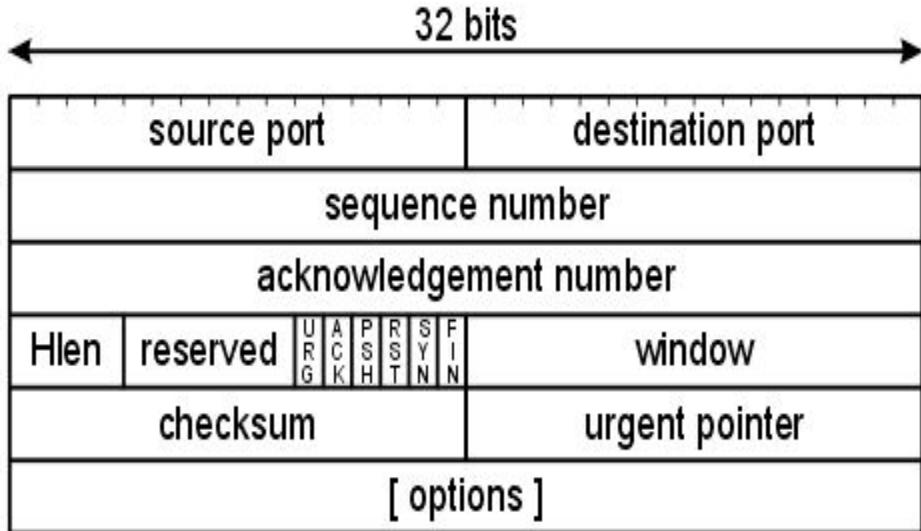


Image Source:

<https://lh3.googleusercontent.com/proxy/MmQAc8LIPH97fO51WtYBRv6hMEL4GN1G-Cg-N8WYI-C-4i-XDWH-L71JCGI-iYEY15EK-4i-2UICWUJ-BDUIG>

Transmission Control Protocol

Services

- Stream Delivery Service
- Sending and Receiving Buffers
- Bytes and Segments
- Full Duplex Service
- Connection Oriented Service
- Reliable Service

TCP header format

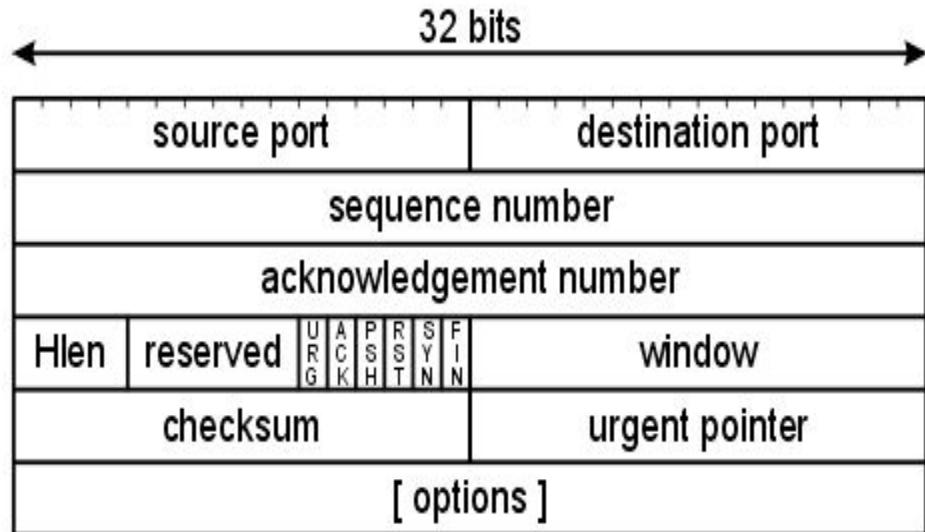
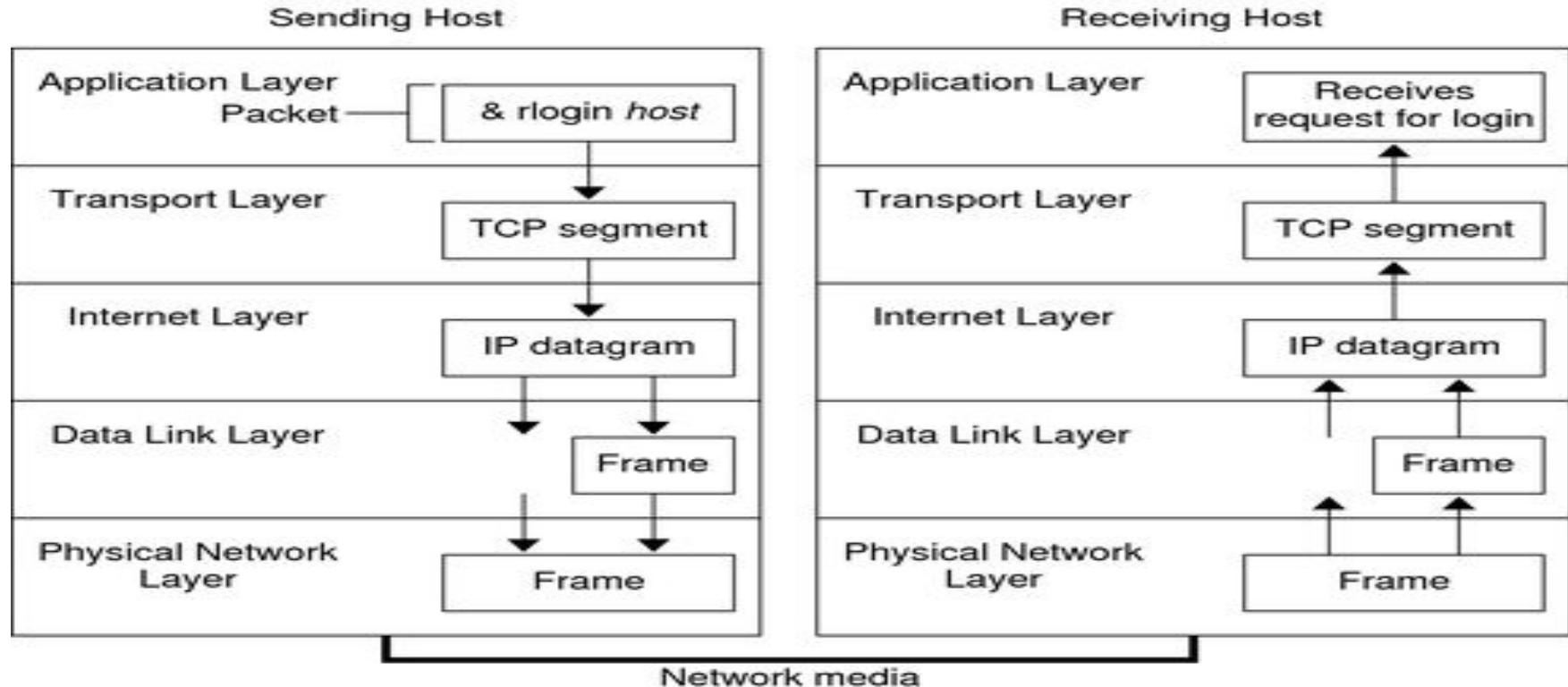


Image Source:

<https://lh3.googleusercontent.com/proxy/MmQAc8LIPH97fO51WtYBRv6hMEL4GN1G-Cg-N8WYI-C-4i-XDWHL-71JCGI-+YEY15EK-4i-2JUKWJLBPUIC>

Transmission Control Protocol



Transmission Control Protocol

Benefits

- It is an Open standard and is independent of hardware and software manufacturer.
- It can send data between different computer systems running completely through Operating system.
- It is separated from the underlying hardware and it will run over Ethernet, tokens ring and even over dial-up telephones lines.

TCP header format

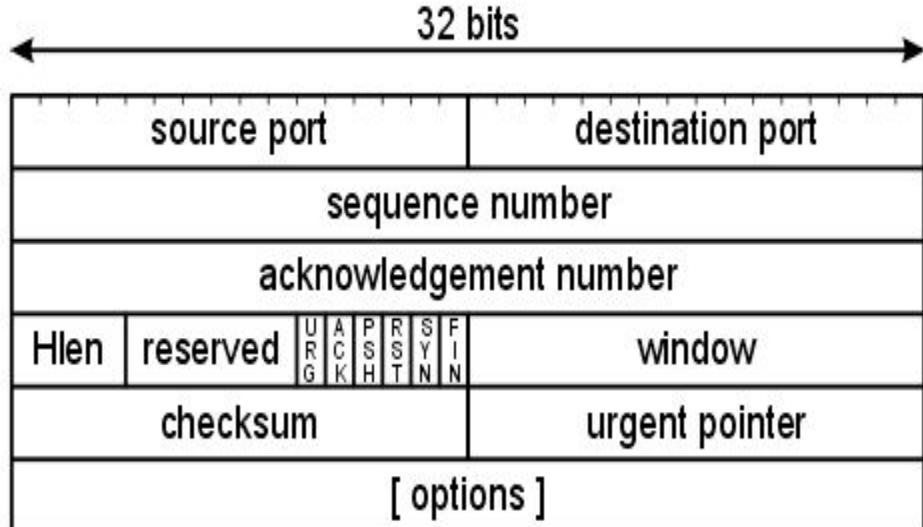


Image Source:

<https://lh3.googleusercontent.com/proxy/MmQAc8LIPH97fO51WtYBRv6hMEL4GN1G-Cg-NQWYI-C-4i-XDWH-L71JCGI-1YEY15EK-1ci-2UJKWJLBBUIC>

Transmission Control Protocol

Benefits

- It is a routable protocol.
- It has a reliable and efficient data-delivery mechanism.
- It uses a common addressing scheme, so any system can address any other system.

TCP header format

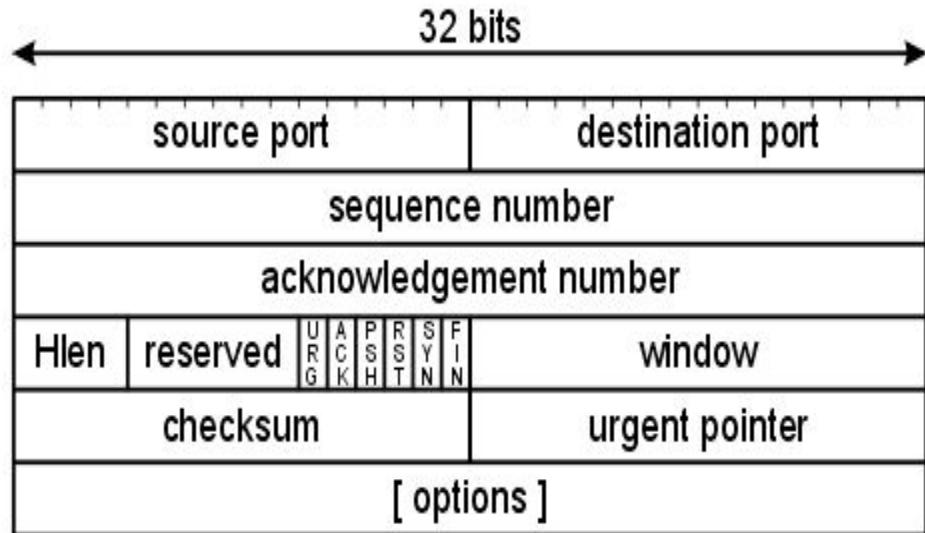


Image Source:

<https://lh3.googleusercontent.com/proxy/MmQAc8LIPH97fO51WtYBRv6hMEL4GN1G-Cg-NQWYI-C-4i-XDwHL71JGGLoYEY15EK-4i-2UICWILBPUIC>

Internet Protocol

Introduction

- Internet Protocol is connectionless and unreliable protocol. It ensures no guarantee of successfully transmission of data.
- In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

Position of IP in TCP/IP protocol suite

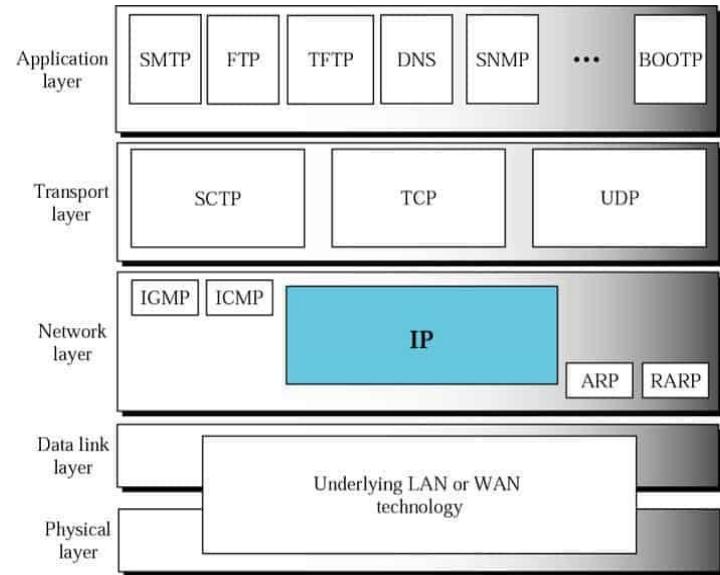
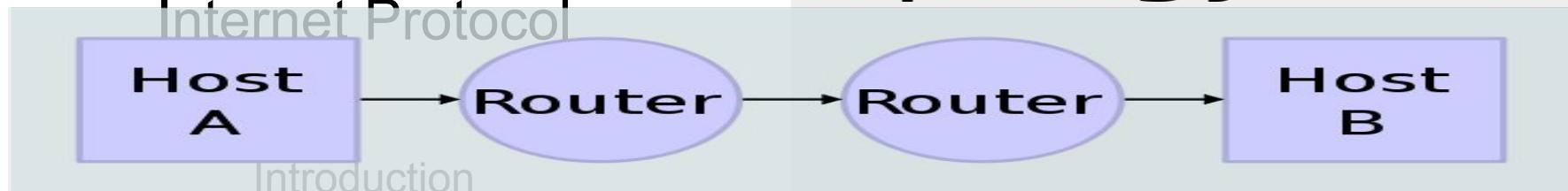


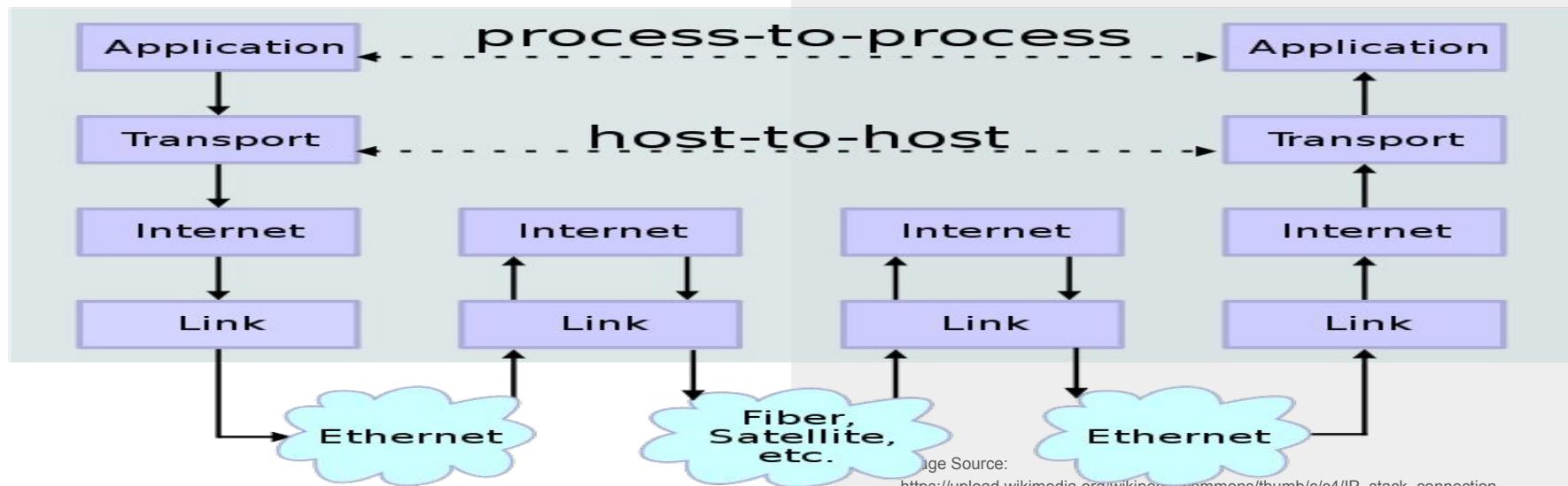
Image Source

<https://networkencyclopedia.com/wp-content/uploads/2019/09/internet-protocol-in-tcp-ip-stack-diagram.jpg>

Network Topology



Data Flow



Internet Protocol

Introduction

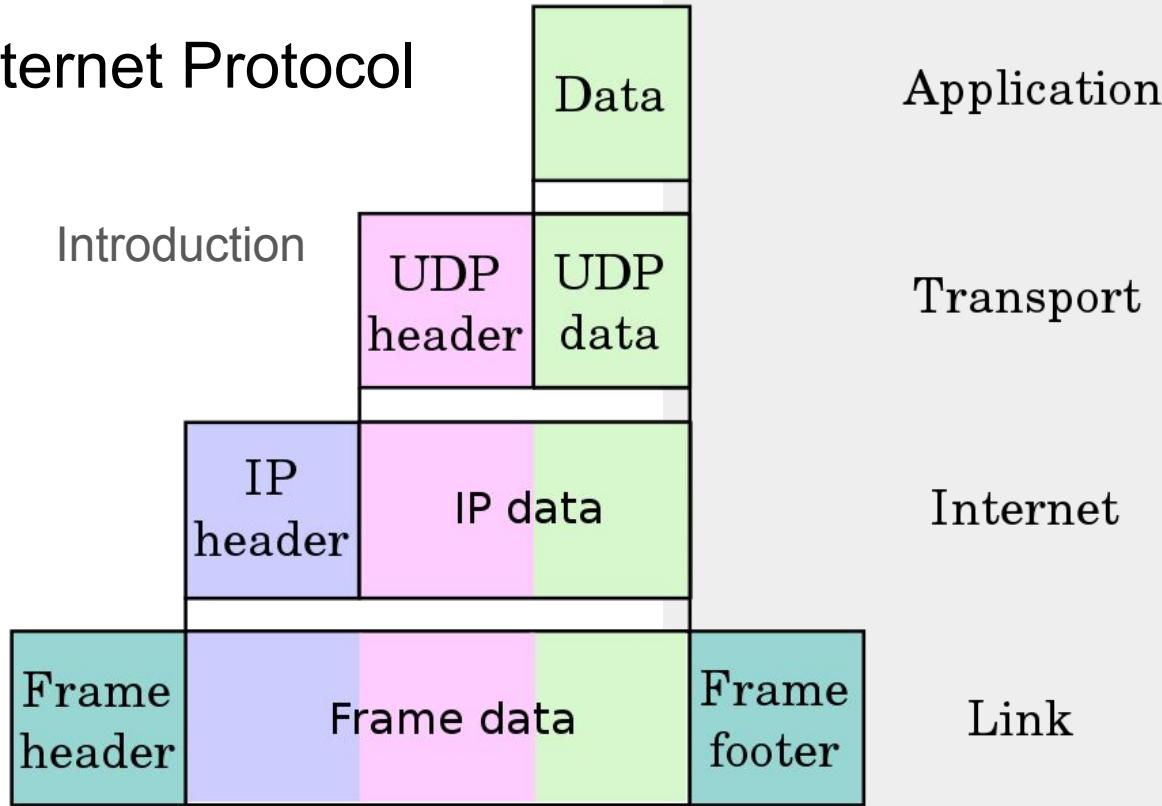
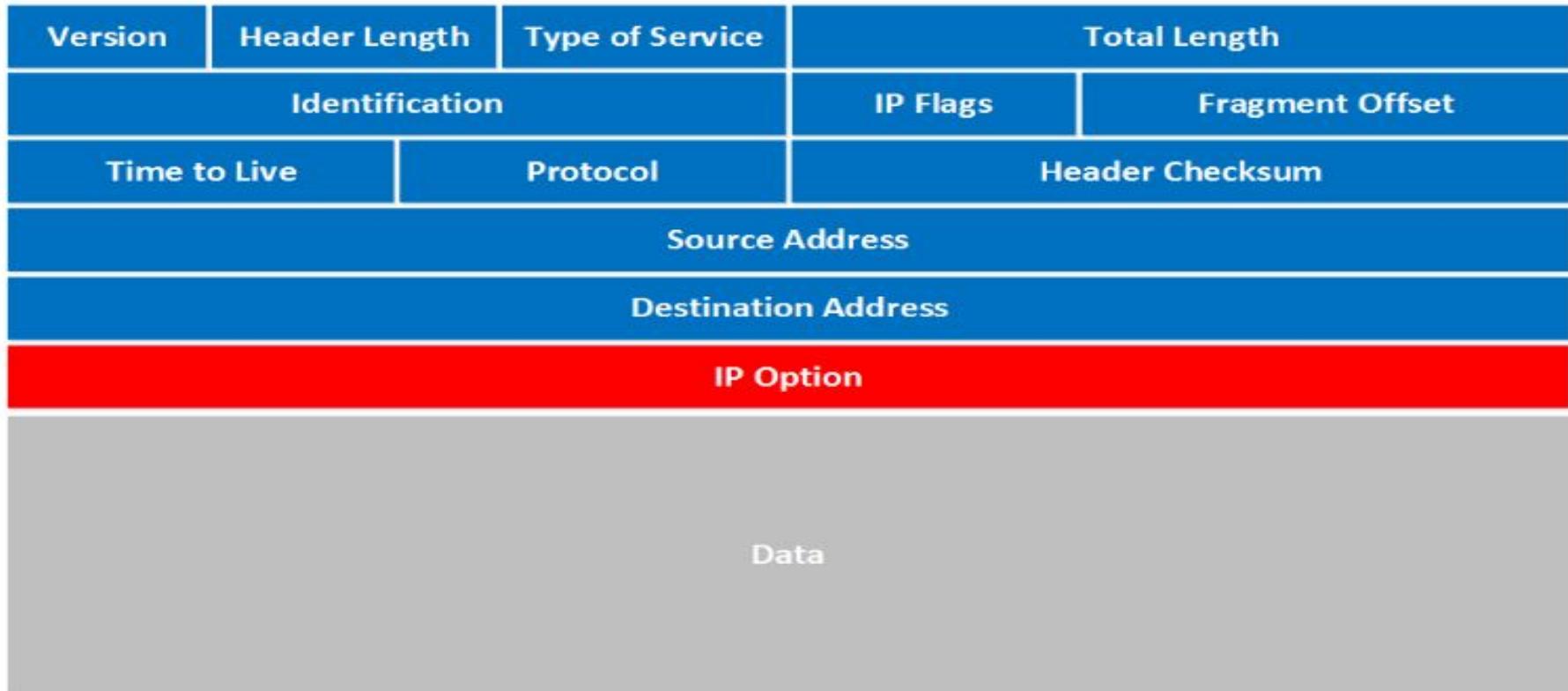


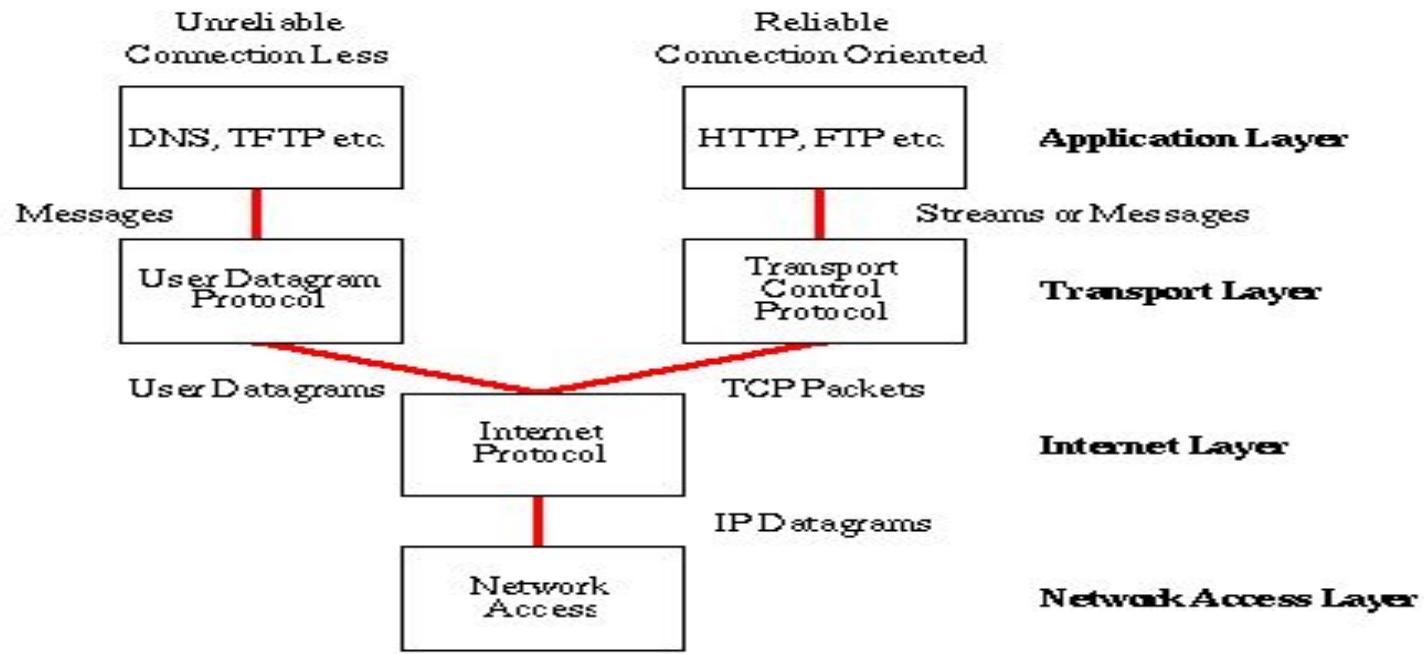
Image Source:

https://upload.wikimedia.org/wikipedia/commons/thumb/3/3b/UDP_encapsulation.svg/1000px-UDP_encapsulation.svg.png

Internet Protocol



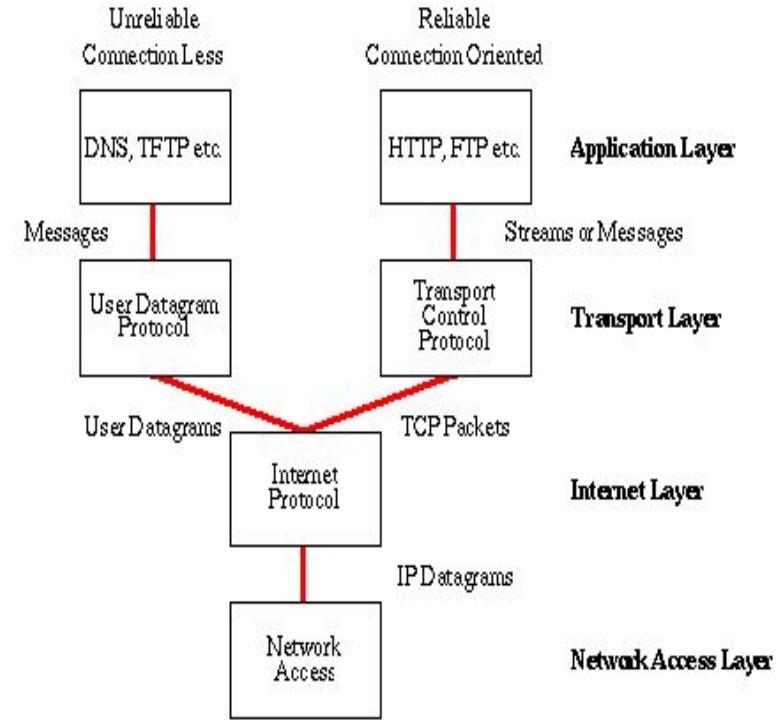
Internet Protocol



Internet Protocol

Points to remember

- The length of datagram is variable.
- The Datagram is divided into two parts: header and data.
- The length of header is 20 to 60 bytes.
- The header contains information for routing and delivery of the packet.



Hypertext Transfer Protocol

Introduction

- HTTP is a communication protocol. It defines mechanism for communication between browser and the web server.
- HTTP request comprises of lines which contains:
 - I. Request line
 - II. Header Fields
 - III. Message body

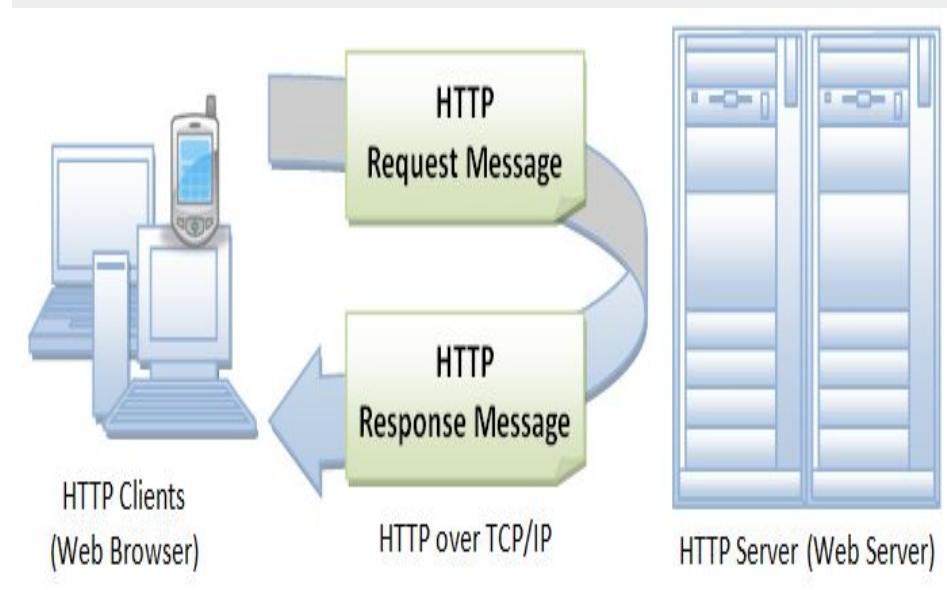


Image Source:

<https://www.ntu.edu.sg/home/ehchua/programming/webprogramming/images/HTT>

TP

Hypertext Transfer Protocol

- Key Points
 1. The first line i.e. the Request line specifies the request method i.e. Get or Post.
 2. The second line specifies the header which indicates the domain name of the server from where index.htm is retrieved.

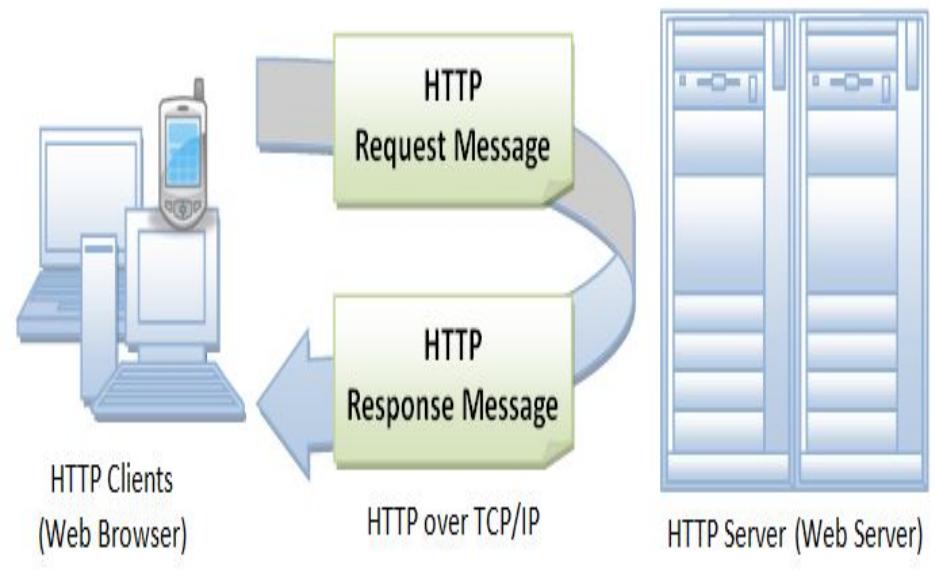


Image Source:

<https://www.ntu.edu.sg/home/ehchua/programming/webprogramming/images/HTTP.png>

Image Source:

Hypertext Transfer Protocol

- HTTP Response
 - I. Like HTTP request, HTTP response also has certain structure. HTTP response contains:
 - II. Status line
 - III. Headers
 - Message body

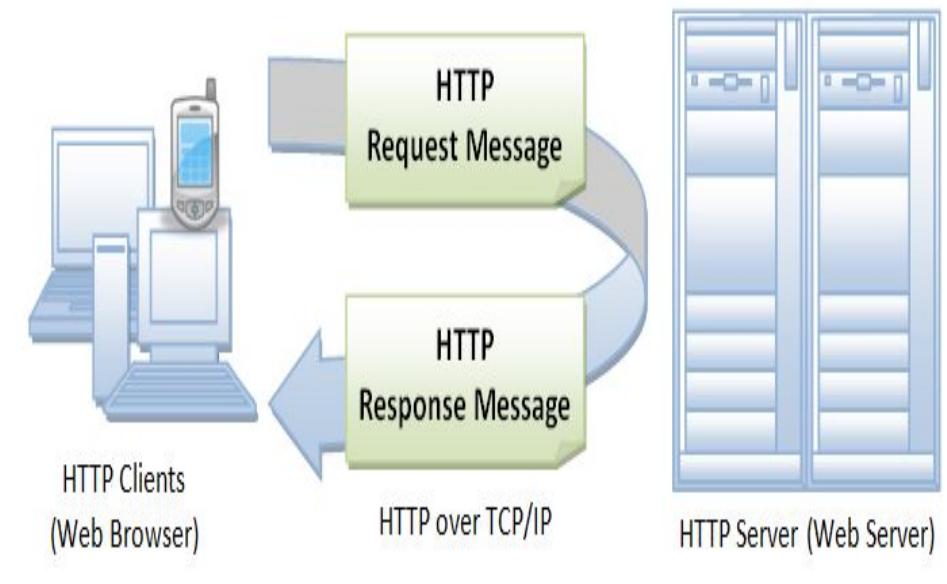


Image Source:

<https://www.ntu.edu.sg/home/ehchua/programming/webprogramming/images/HTP.png>

Image Source:

Hypertext Transfer Protocol Secure

Introduction

- Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.
- In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL).

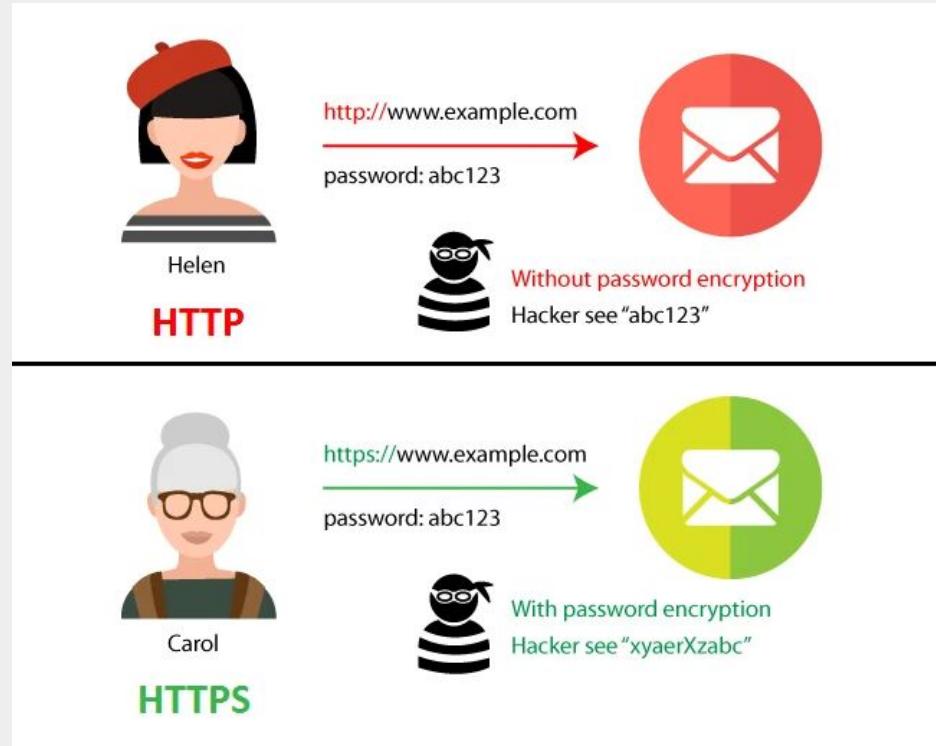


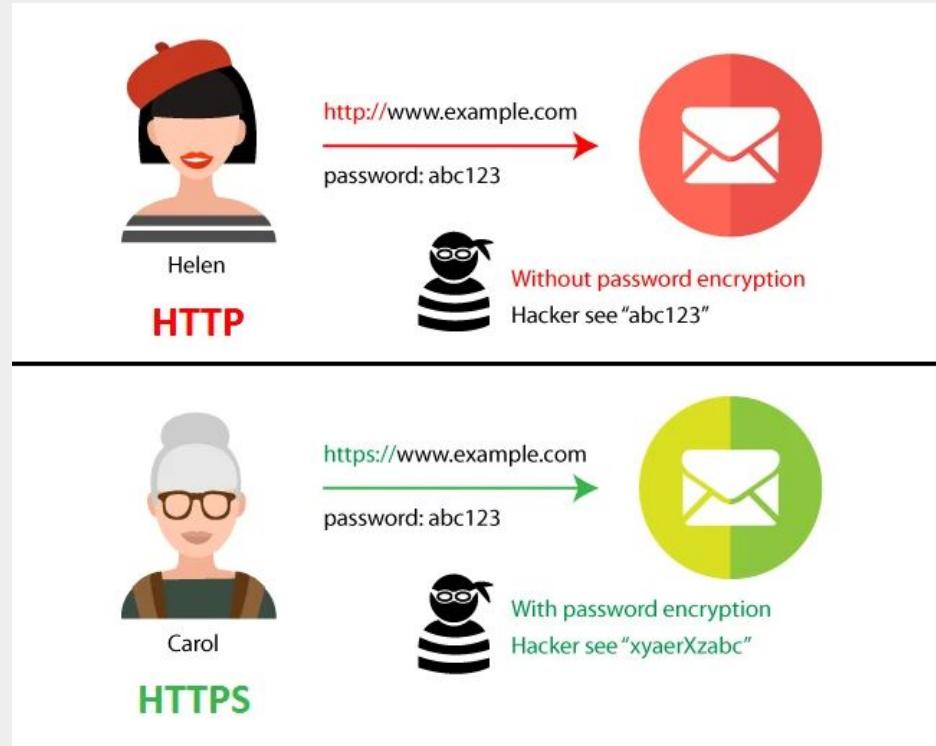
Image Source:

<https://www.edhotels.com/wp-content/uploads/2020/04/Difference-Between-HTTP-and-HTTPS-.png>

Hypertext Transfer Protocol Secure

Introduction

- The protocol is therefore also referred to as HTTP over TLS,[3] or HTTP over SSL.



Hypertext Transfer Protocol Secure

Advantages

- User Data is Encrypted
- You'll Enjoy Better SEO
- Protects your website from Phishing

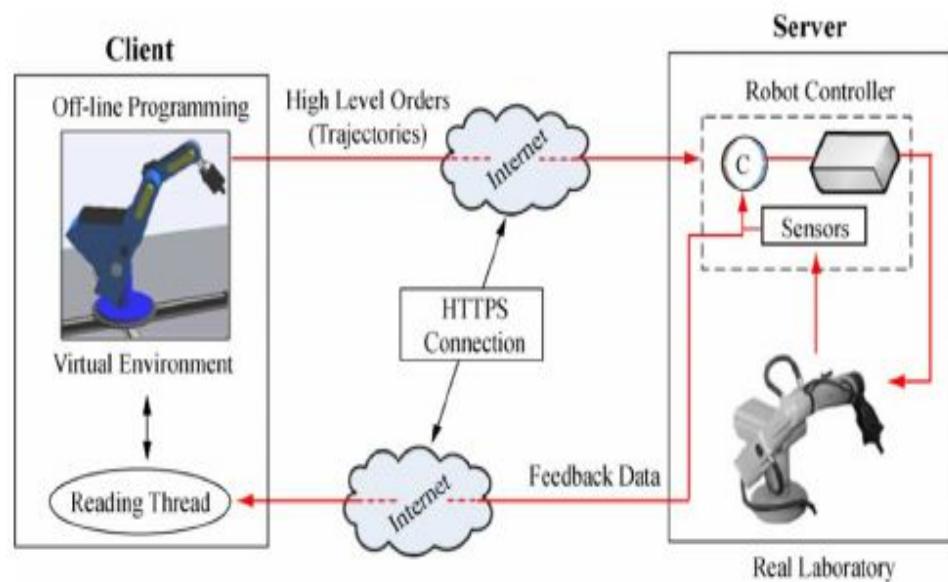


Image Source:

https://www.researchgate.net/profile/S_Dormido/publication/232652131/figure/fig5/AS:8000104000000000C1110001050001/Secured-control-architecture-diagram.jpg

Hypertext Transfer Protocol Secure

Advantages

- Authentication of the accessed website, and protection of the privacy and integrity of the exchanged data while in transit.
- It protects against man-in-the-middle attacks, and the bidirectional encryption of communications between a client and server protects the communications against eavesdropping and tampering.

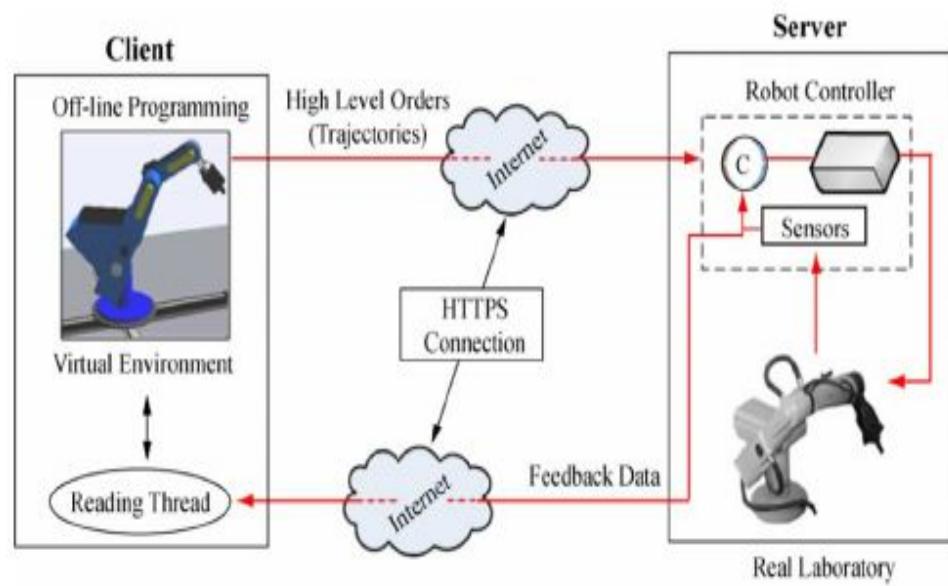


Image Source:

https://www.researchgate.net/profile/S_Dormido/publication/232652131/figure/fig5/AS:8000104000000000C1110001050001/Robotics-control-and-architecture-diagram.jpg

Hypertext Transfer Protocol Secure(SSL)

Limitations

- SSL/TLS does not prevent the indexing of the site by a web crawler
 - SSL (Secure Sockets Layer) and TLS (Transport Layer Security) encryption can be configured in two modes: simple and mutual.

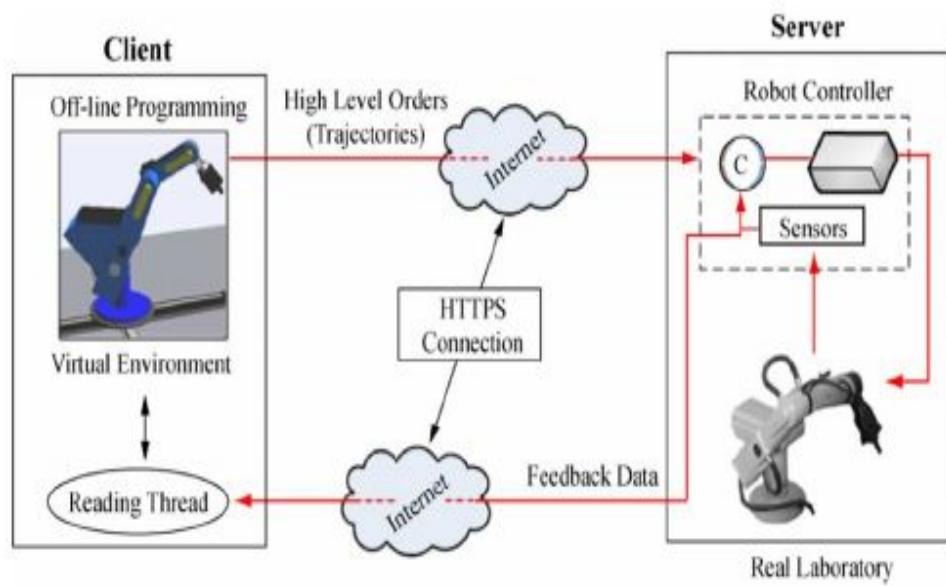


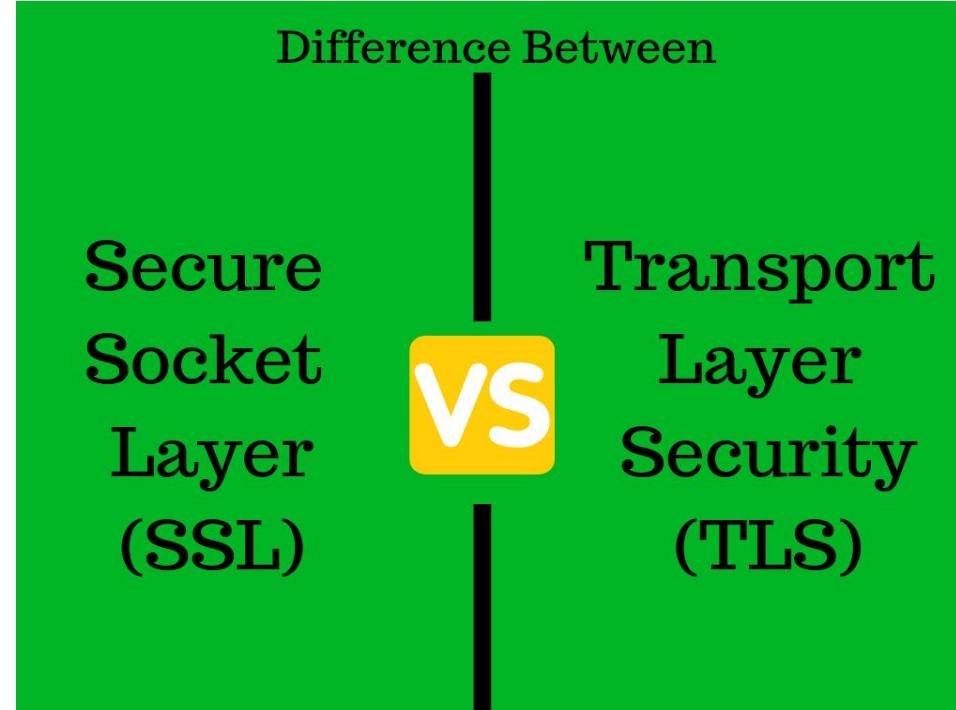
Image Source:

https://www.researchgate.net/profile/S_Dormido/publication/232652131/figure/fig5

History of SSL and TLS releases

Limitations

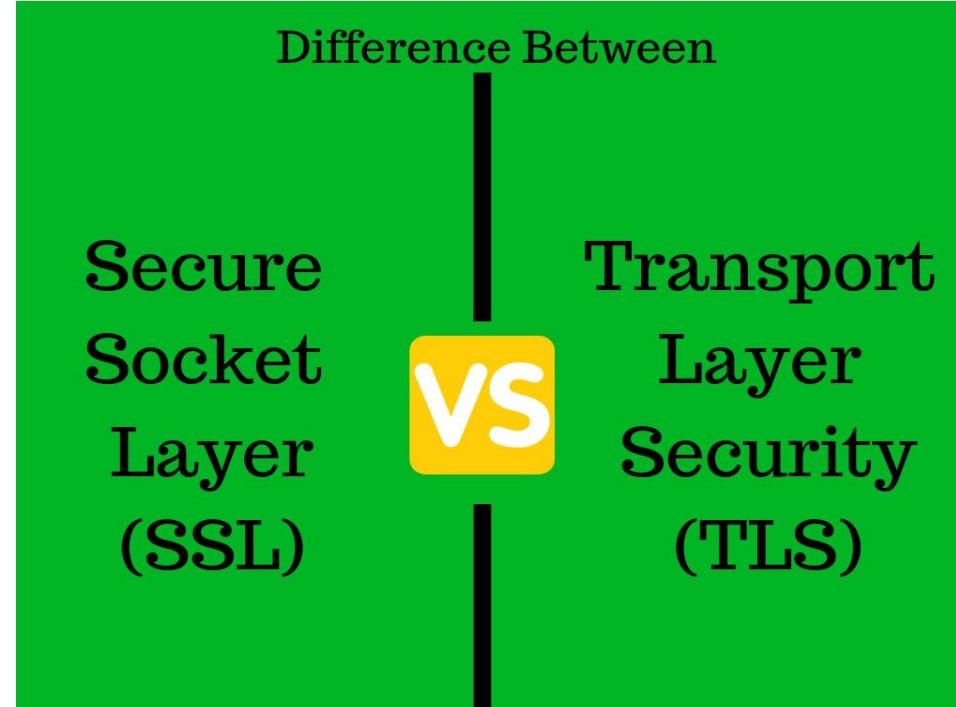
- SSL 1.0 – never publicly released due to security issues.
- SSL 2.0 – released in 1995. Deprecated in 2011. Has known security issues.
- SSL 3.0 – released in 1996. Deprecated in 2015. Has known security issues.



History of SSL and TLS releases

Limitations

- TLS 1.0 – released in 1999 as an upgrade to SSL 3.0. Planned depreciation in 2020.
- TLS 1.1 – released in 2006. Planned depreciation in 2020.
- TLS 1.2 – released in 2008.
- TLS 1.3 – released in 2018.



File Transfer Protocol

Introduction

- FTP is used to copy files from one host to another browser and the web server.
- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
- FTP establishes two different connections: one is for data transfer and other is for control information.

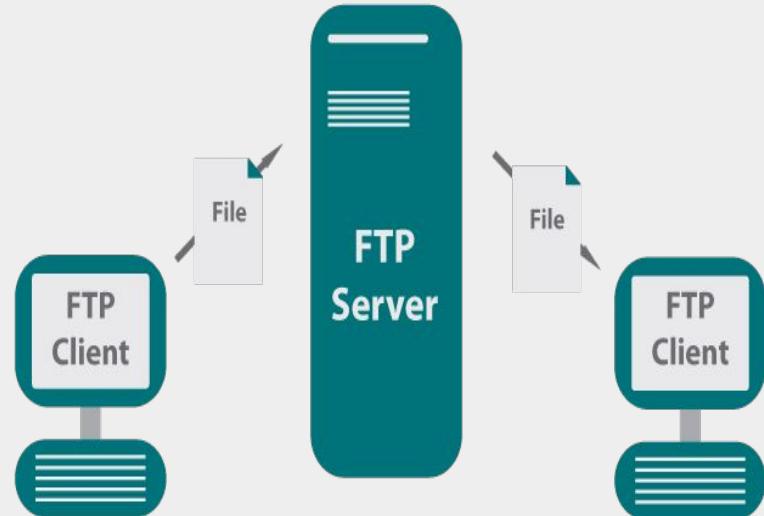


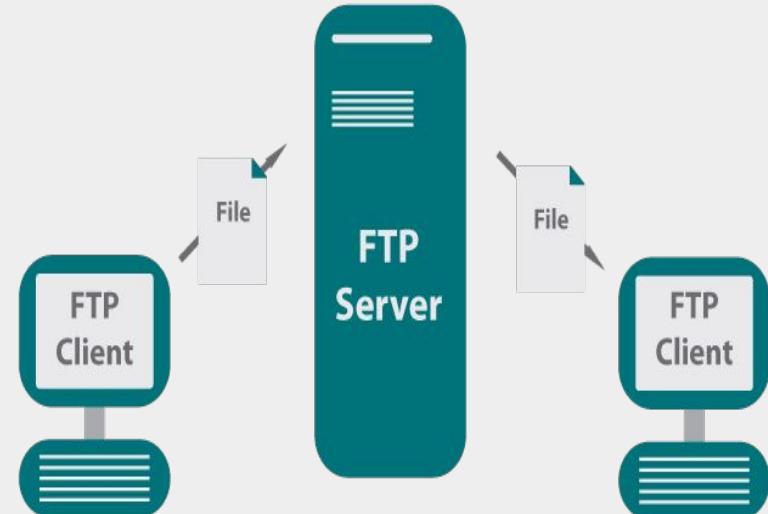
Image Source:

<https://blog.ipswitch.com/hs-fs/hubfs/ftp-diagram.png?width=750&height=378&name=ftp-diagram.png>

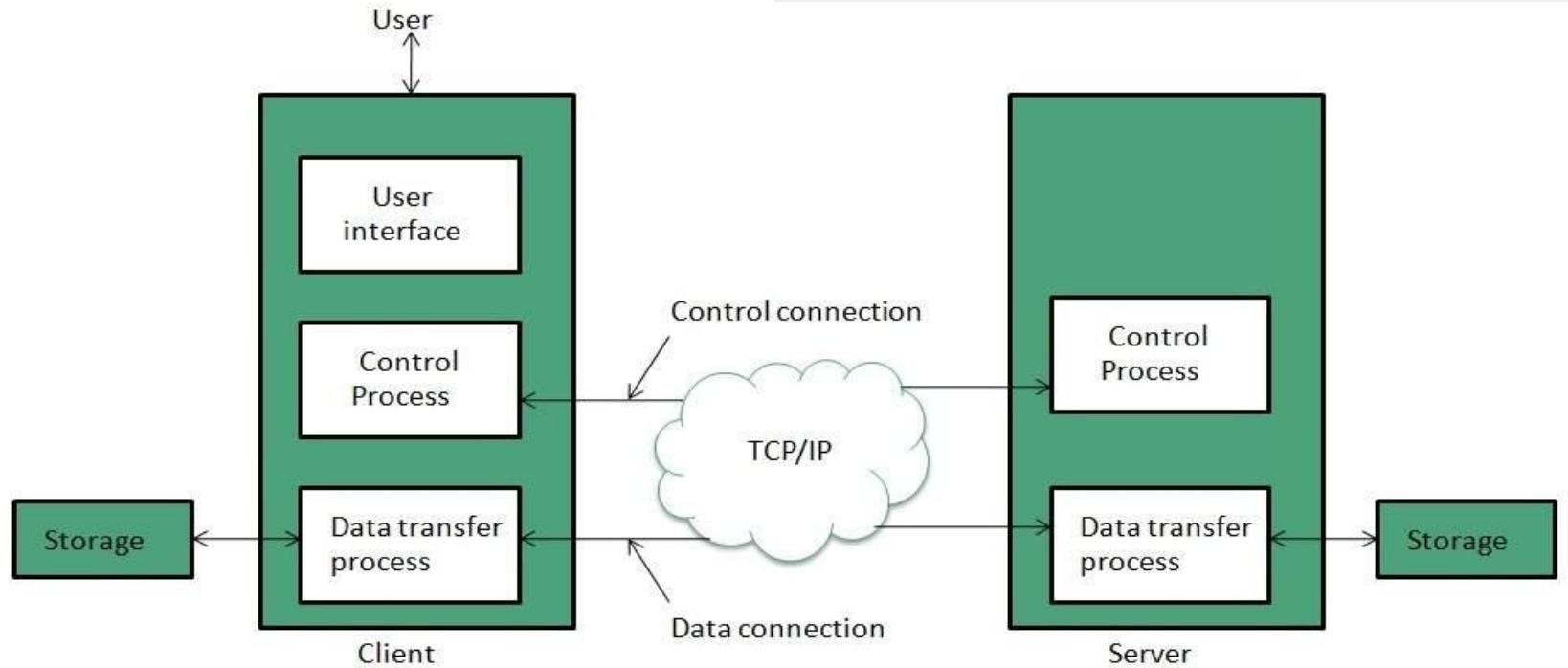
File Transfer Protocol

Introduction

- Control connection is made between control processes while Data Connection is made between
- FTP uses port 21 for the control connection and Port 20 for the data connection.



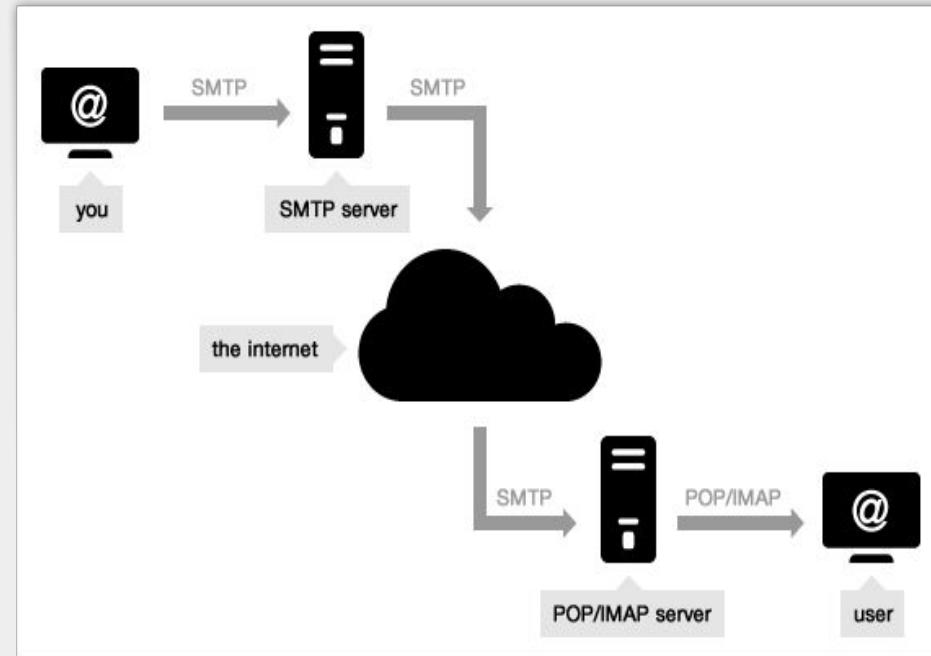
File Transfer Protocol



Simple Mail Transfer Protocol

Introduction

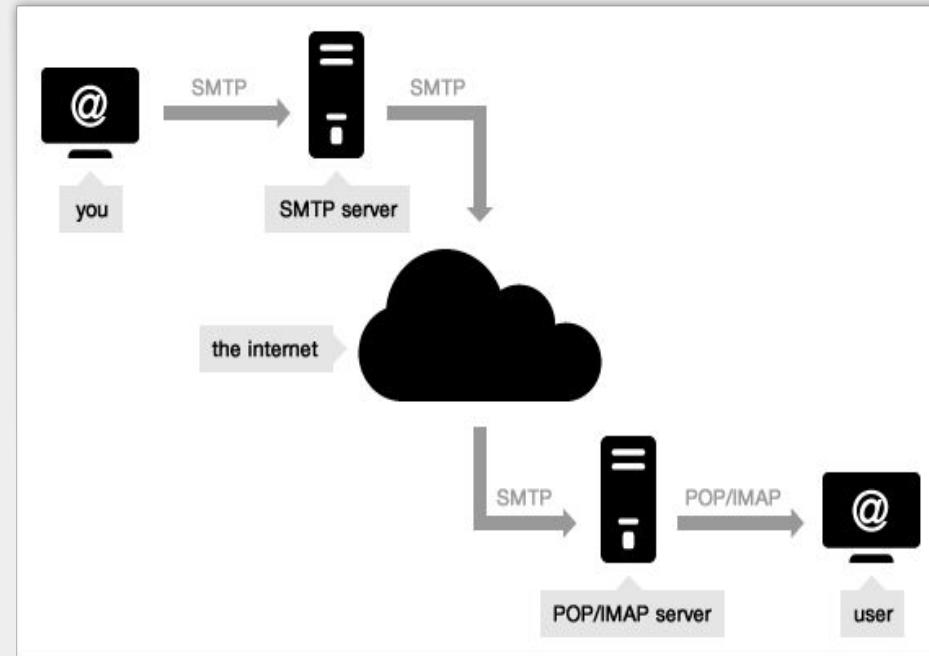
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.
- It is a program used for sending messages to other computer users based on e-mail addresses.



Simple Mail Transfer Protocol

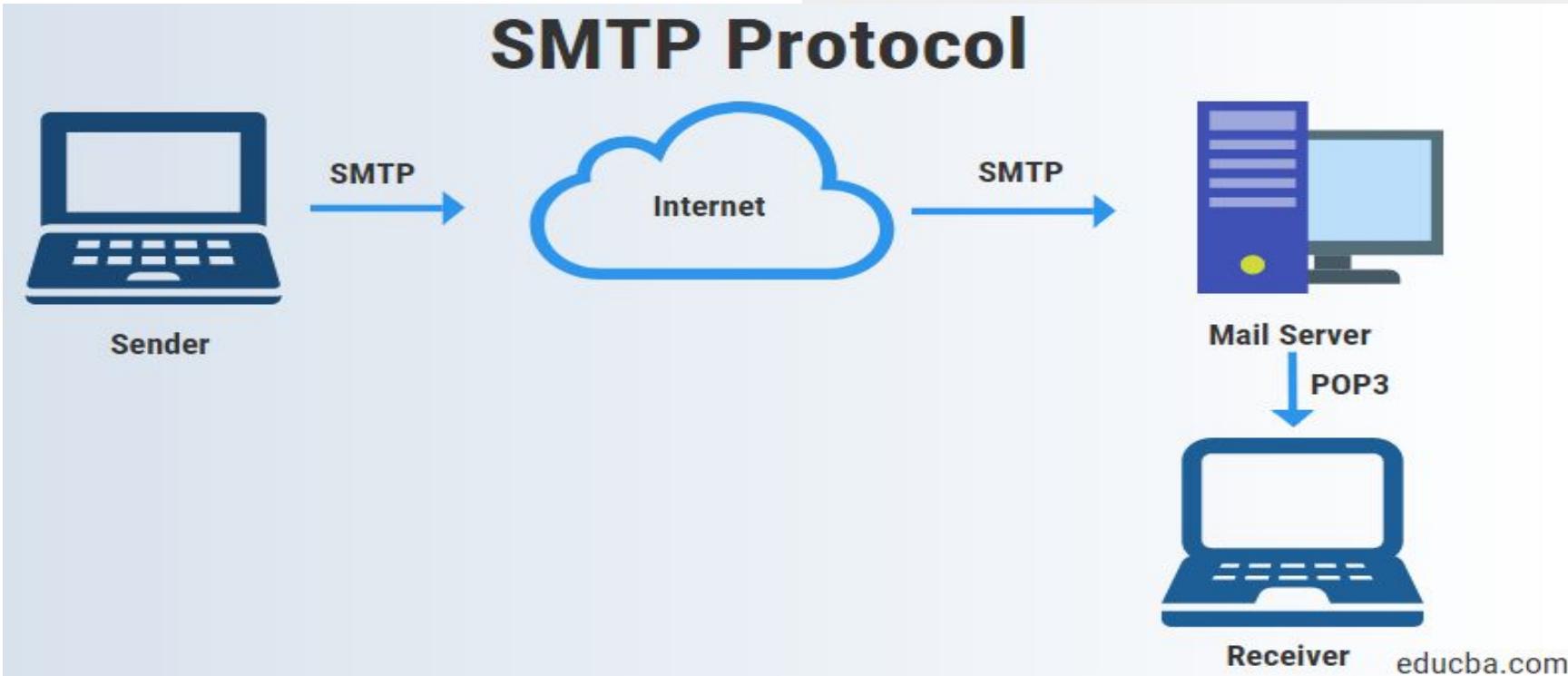
Introduction

- It provides a mail exchange between users on the same or different computers, and it also supports:
1. It can send a single message to one or more recipients.
 2. Sending message can include text, voice, video or graphics.
 3. It can also send the messages on networks outside the internet.

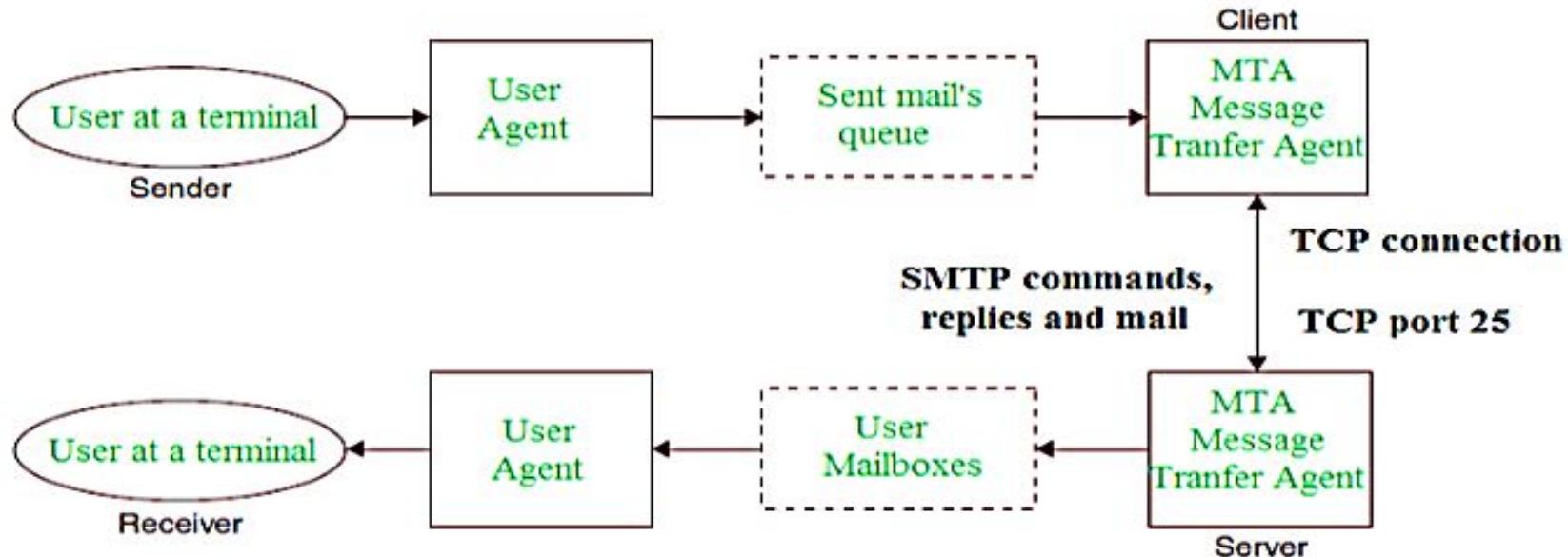


Simple Mail Transfer Protocol

SMTP Protocol



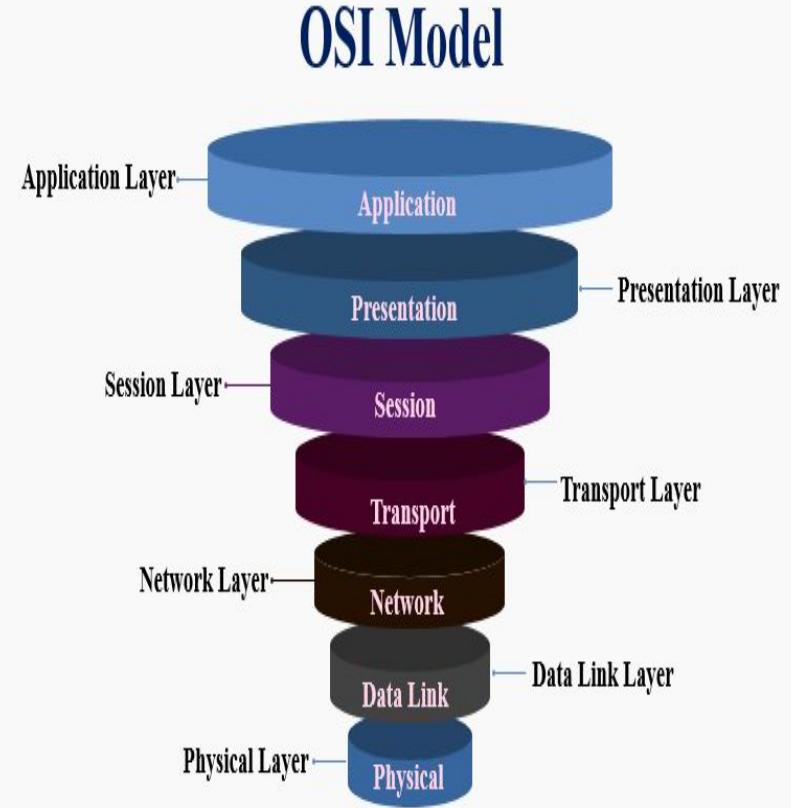
Simple Mail Transfer Protocol



Open System Interconnection Model(OSI)

Introduction

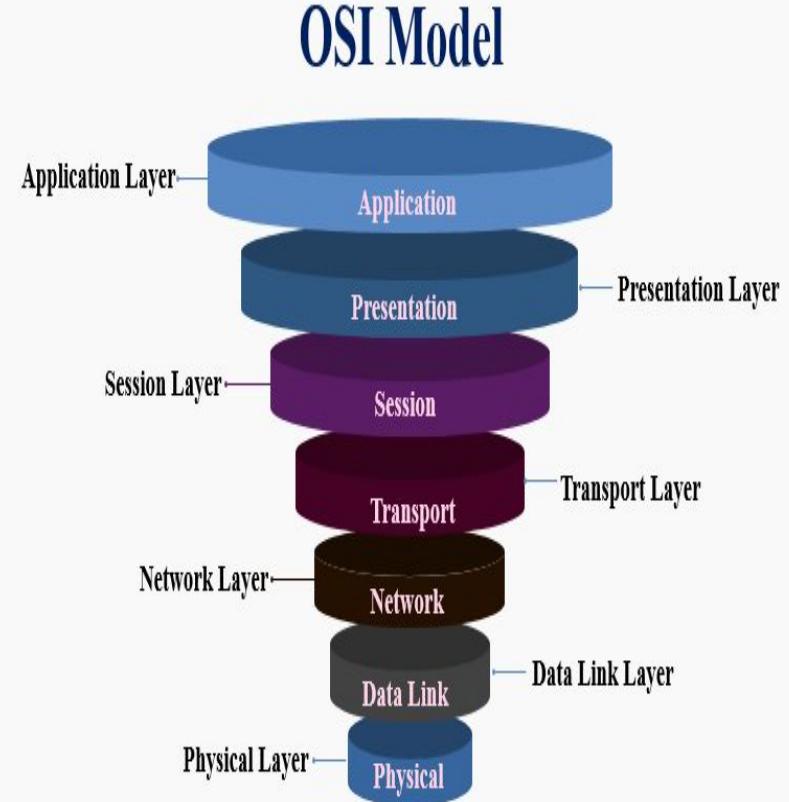
- OSI stands for Open Systems Interconnection. It has been developed by ISO – ‘International Organization of Standardization’, in the year 1984.
- Designed to show the flow of moving data from one software application of one computer to another software application of another computer.

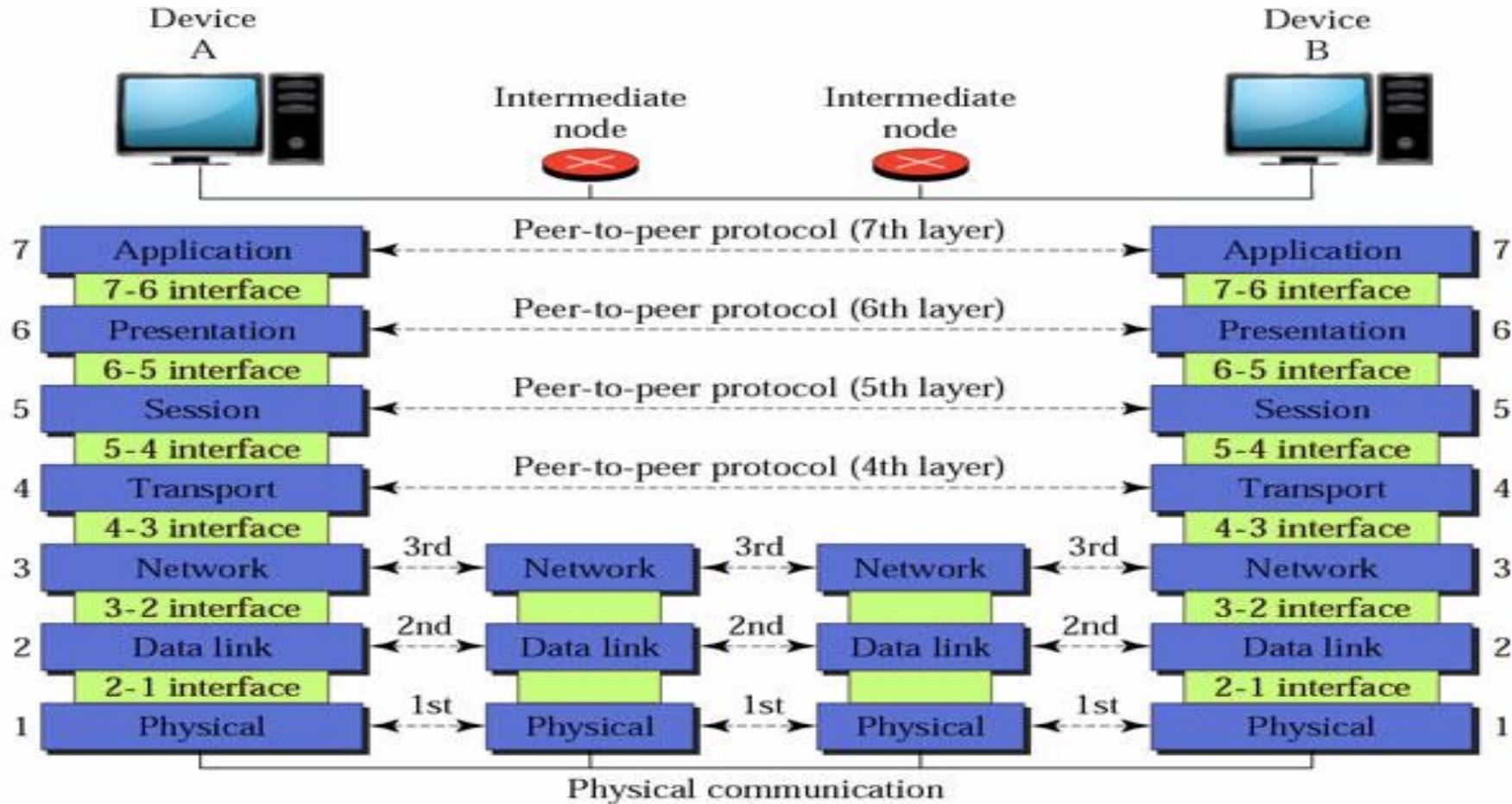


Open System Interconnection Model(OSI)

Introduction

- Open Systems Interconnection (OSI) model is the virtual model which describes the Concept of a computer system with the concern of internal structure and technology.

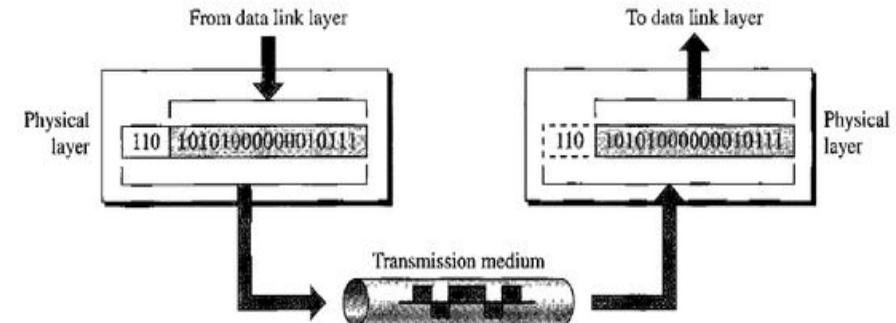




Open System Interconnection Model(OSI)

Physical Layer Functions

- The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices.
- Bit synchronization
- Bit rate control
- Physical topologies and Transmission mode

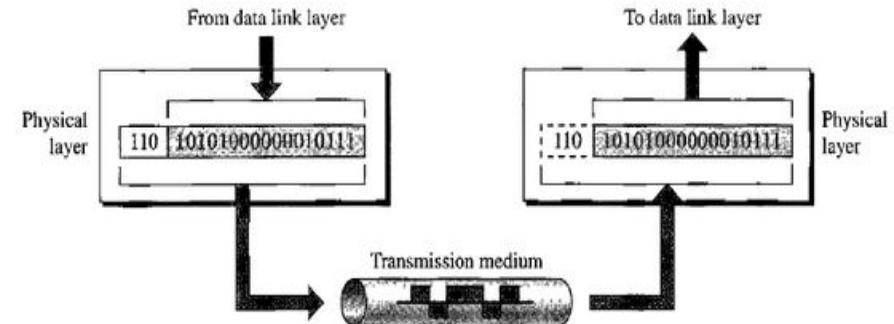


The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Open System Interconnection Model(OSI)

Physical Layer Functions

- Hub, Repeater, Modem, Cables are Physical Layer devices.
- Network Layer, Data Link Layer and Physical Layer are also known as Lower Layers or Hardware Layers.

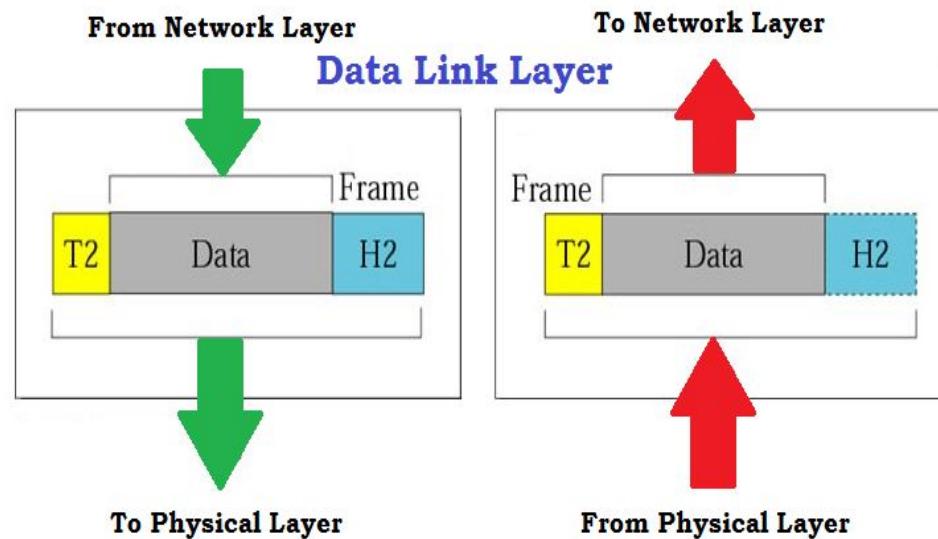


The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Open System Interconnection Model(OSI)

Data Link Layer (DLL) Functions

- The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.
- Packet in Data Link layer is referred as Frame.

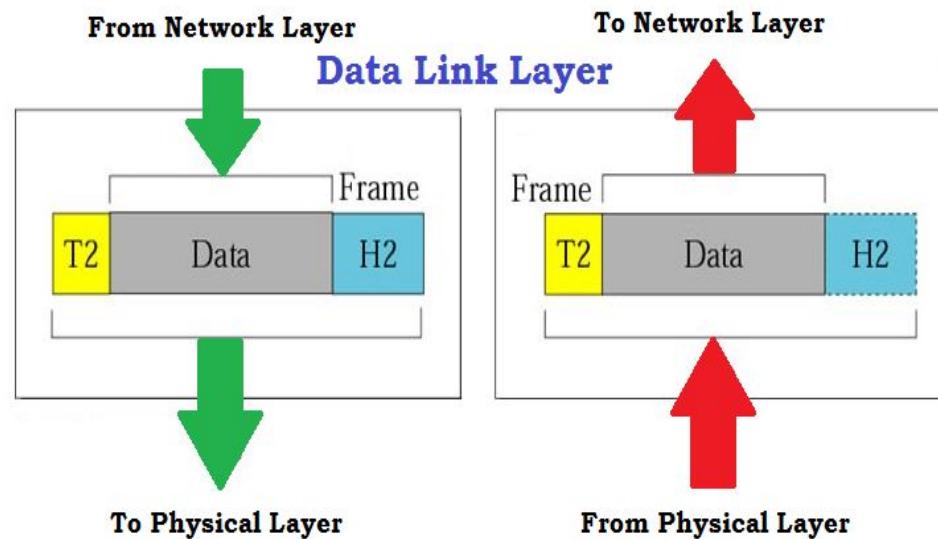


Open System Interconnection Model(OSI)

Data Link Layer (DLL) Functions

- Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
- Switch & Bridge are Data Link Layer devices.

Logical Link Control (LLC)
Media Access Control (MAC)



Open System Interconnection Model(OSI)

Data Link Layer (DLL) Functions

- Framing
- Physical addressing
- Error control
- Flow Control
- Access control

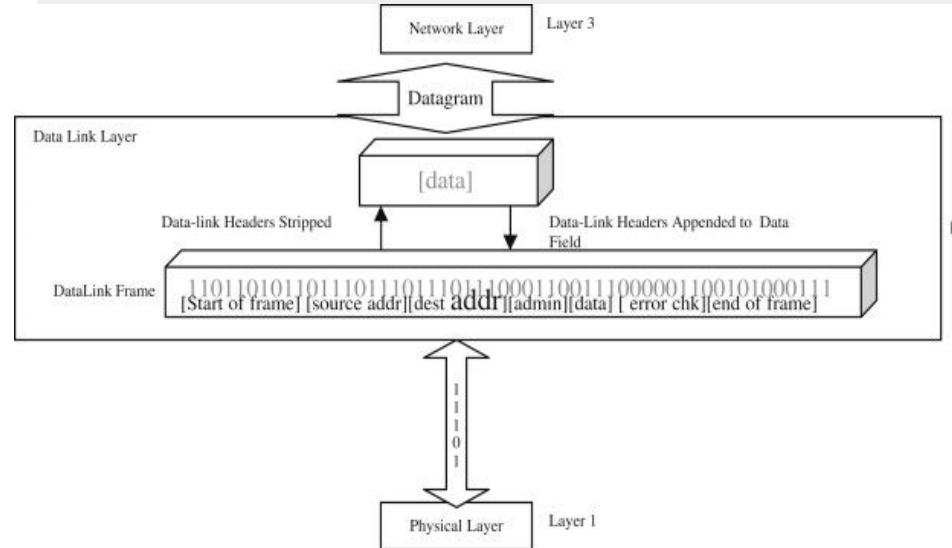


Image Source:

<https://ars.els-cdn.com/content/image/3-s2.0-B9780123821966000029-f02-31-97-001200010001.htm>

Open System Interconnection Model(OSI)

Data Link Layer (DLL) Functions

- Packet in Data Link layer is referred as Frame.
 - Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
 - Switch & Bridge are Data Link Layer devices.

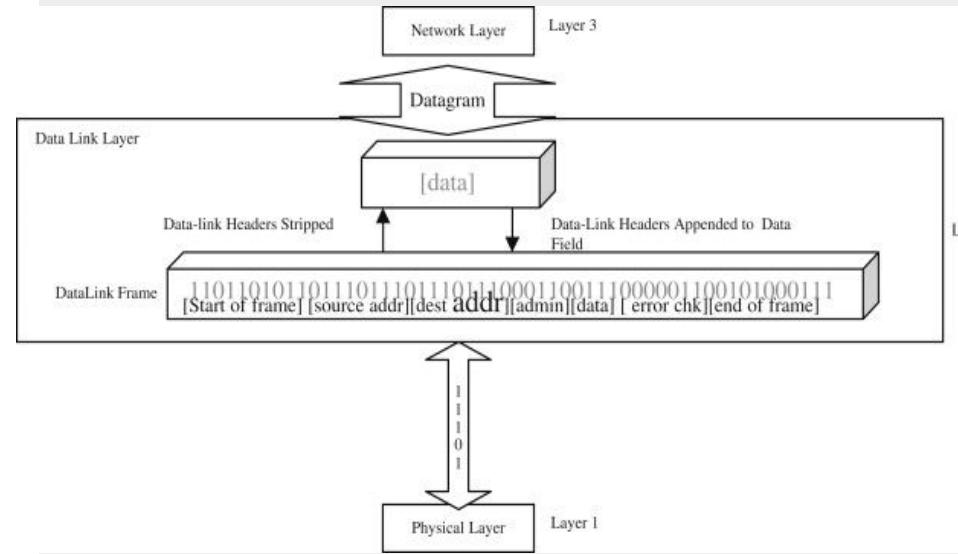


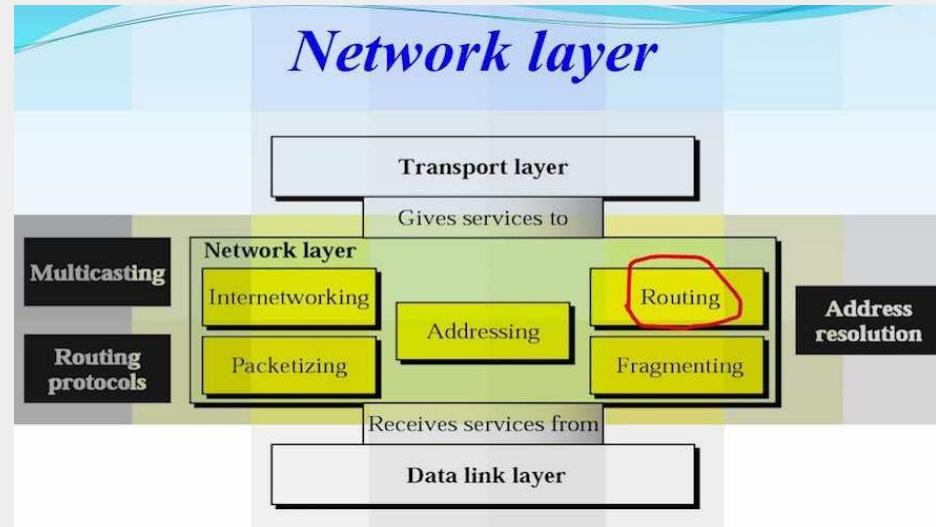
Image Source:

<https://ars.els-cdn.com/content/image/3-s2.0-B9780123821966000029-f02-31-97>

Open System Interconnection Model(OSI)

Network Layer Functions

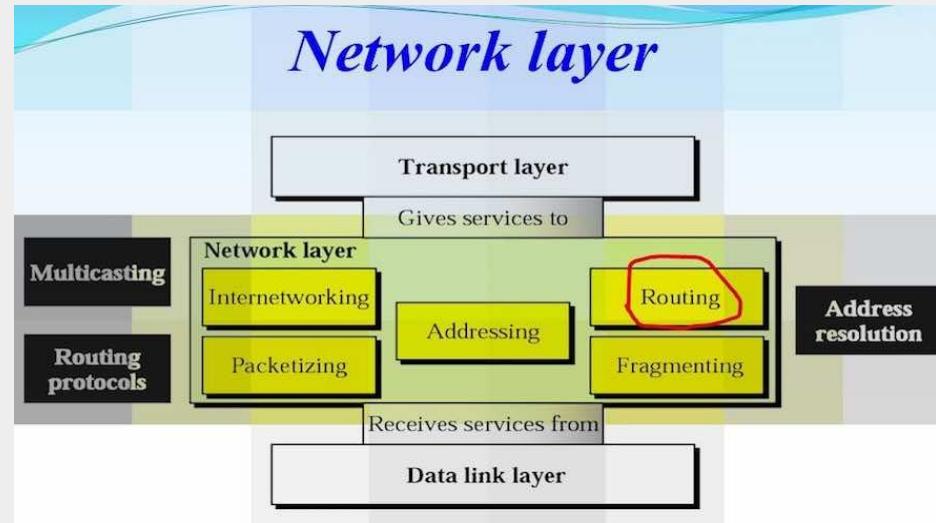
- Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing.
- Routing: The network layer protocols determine which route is suitable from source to destination.
- Logical Addressing



Open System Interconnection Model(OSI)

Network Layer Functions

- Segment in Network layer is referred as Packet.
- Network layer is implemented by networking devices such as routers.



Open System Interconnection Model(OSI)

Transport Layer Functions

- Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message.
- Segmentation and Reassembly
- Service Point Addressing

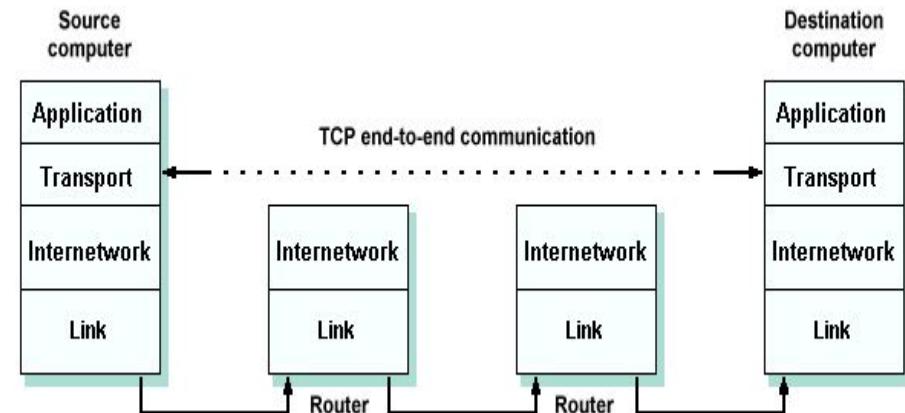


Image Source:

https://www.technologyuk.net/computing/computer-networks/internet/images/tcp_end_to_end_comunication.gif

Open System Interconnection Model(OSI)

Transport Layer Functions

- Service provided by transport layer
 - Connection Oriented Service: It is a three-phase process which include
 - Connection Establishment
 - Data Transfer
 - Termination / disconnection
- Connection less service: It is a one-phase process and includes Data Transfer.

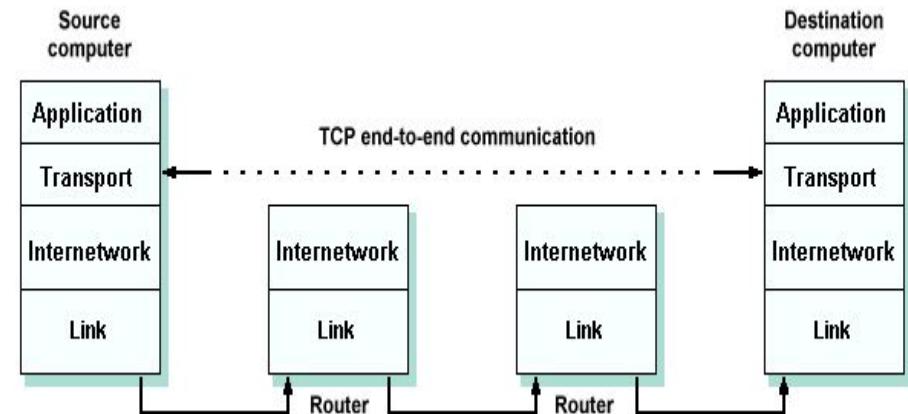


Image Source:

https://www.technologyuk.net/computing/computer-networks/internet/images/tcp_end_to_end_communication.gif

Open System Interconnection Model(OSI)

Transport Layer Functions

- Data in the Transport Layer is called as Segments.
- Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
- Transport Layer is called as Heart of OSI model.

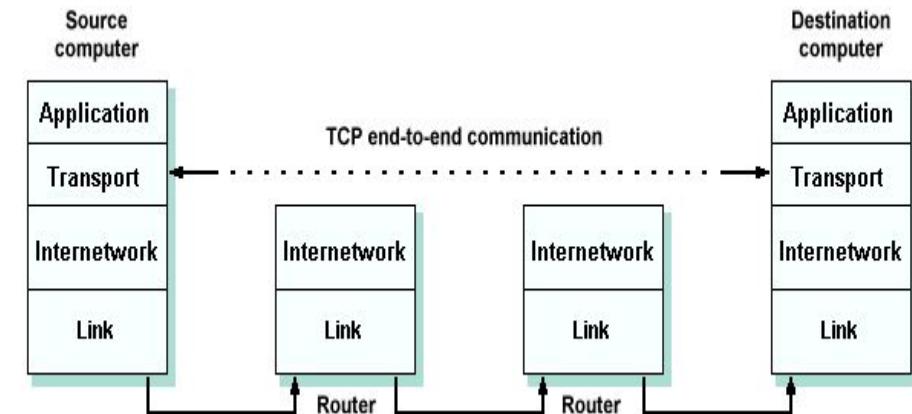


Image Source:

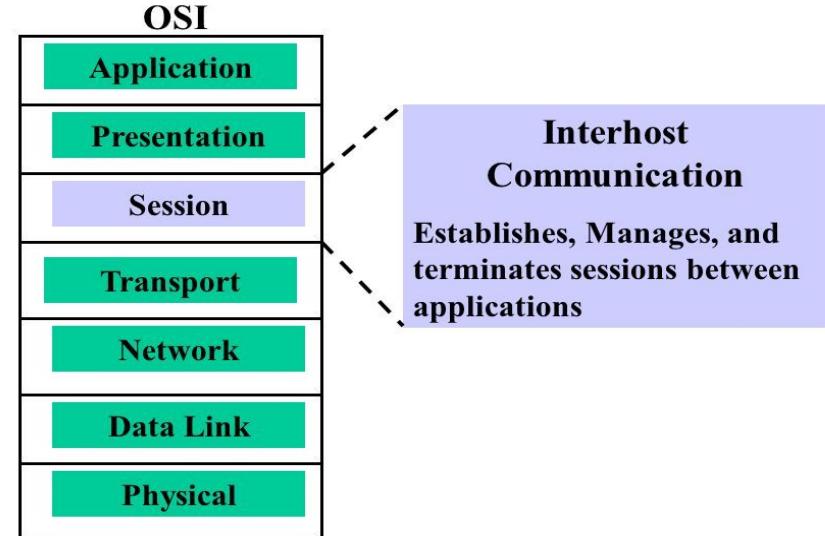
https://www.technologyuk.net/computing/computer-networks/internet/images/tcp_end-to-end_communication.gif

Open System Interconnection Model(OSI)

Session Layer Functions

- This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
- Session establishment, maintenance and termination
- Synchronization
- Dialog Controller

Functions of Session Layer

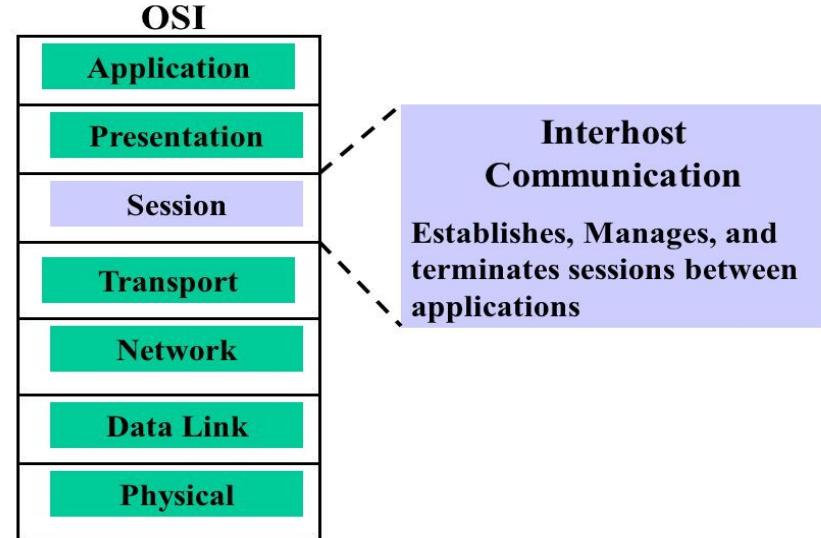


Open System Interconnection Model(OSI)

Session Layer Functions

- All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as “Application Layer”.
- Implementation of these 3 layers is done by the network application itself. These are also known as Upper Layers or Software Layers.

Functions of Session Layer



Open System Interconnection Model(OSI)

Presentation Layer Functions

- Presentation layer is also called the Translation layer.
- The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
- Translation

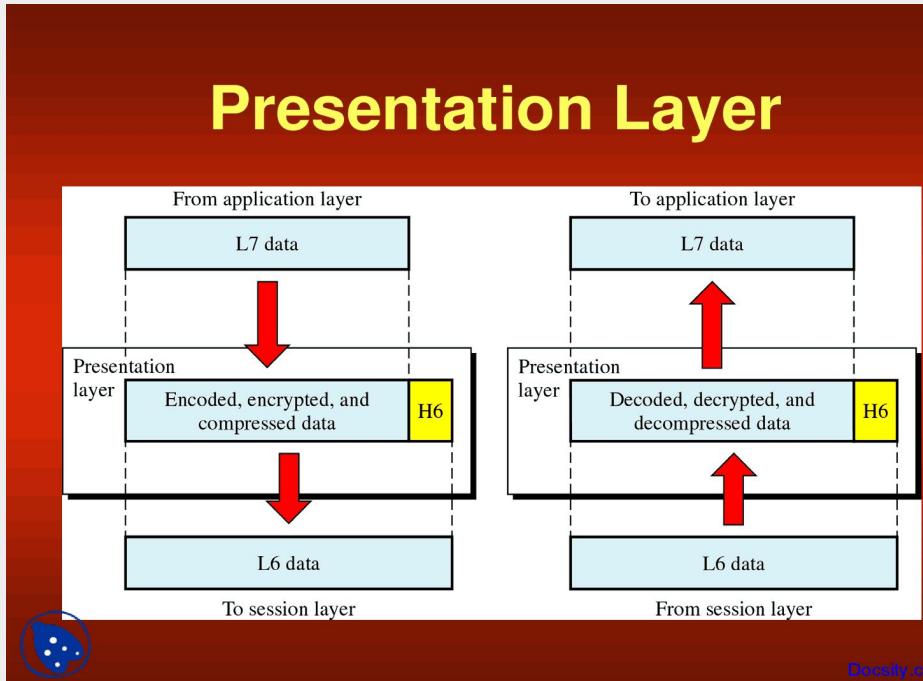


Image Source:

https://static.docsity.com/documents_pages/2012/11/03/73287fb7f97f04abcee7dd

[Page 24 of 42]

Open System Interconnection Model(OSI)

Presentation Layer Functions

- Encryption/ Decryption
- Compression: Reduces the number of bits that need to be transmitted on the network.

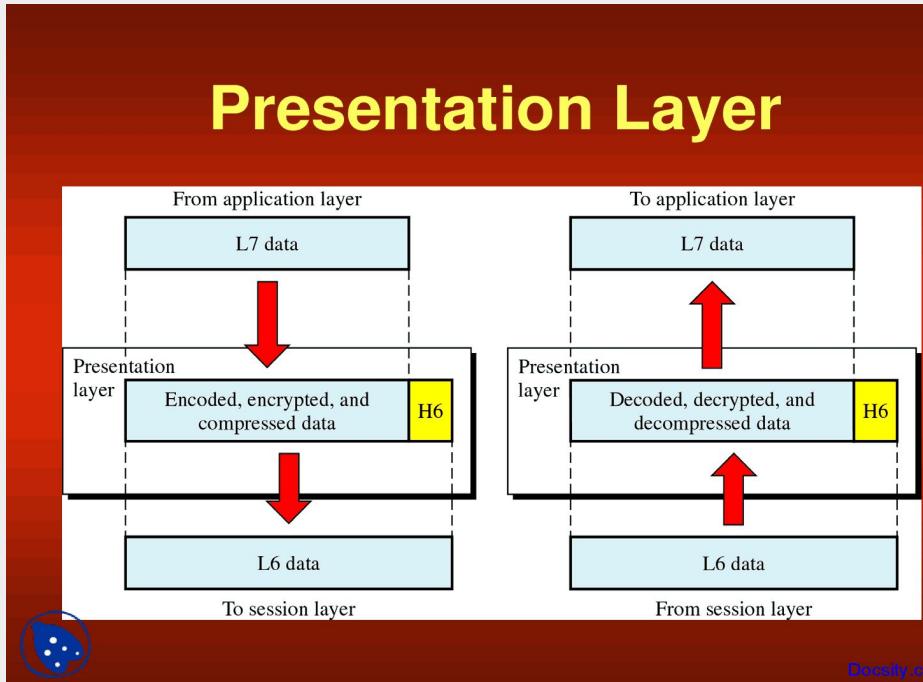


Image Source:

https://static.docsity.com/documents_pages/2012/11/03/73287fb7f97f04abcee7dd

[CC-BY-SA]

Open System Interconnection Model(OSI)

Application Layer Functions

- The functions of the Application layer are :
- Network Virtual Terminal
- FTAM-File transfer access and management
- Mail Services
- Directory Services

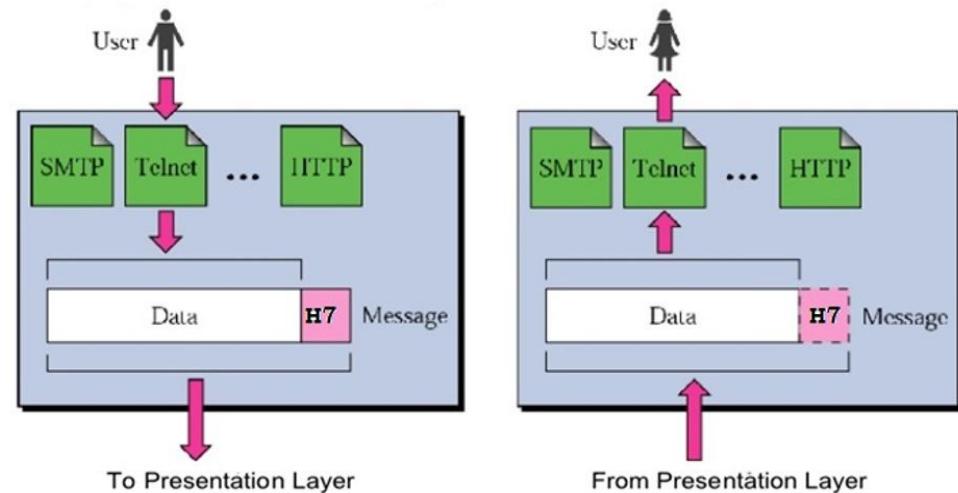


Fig: Application Layer

Media Access Methods

Introduction

- A media access method refers to the manner in which a computer terminal on a network gains and controls access to the network's physical medium such as a cable.
- The prime objective of media access is to prevent data packets from colliding when two or more computer terminals on a network try to transmit data simultaneously over a network.

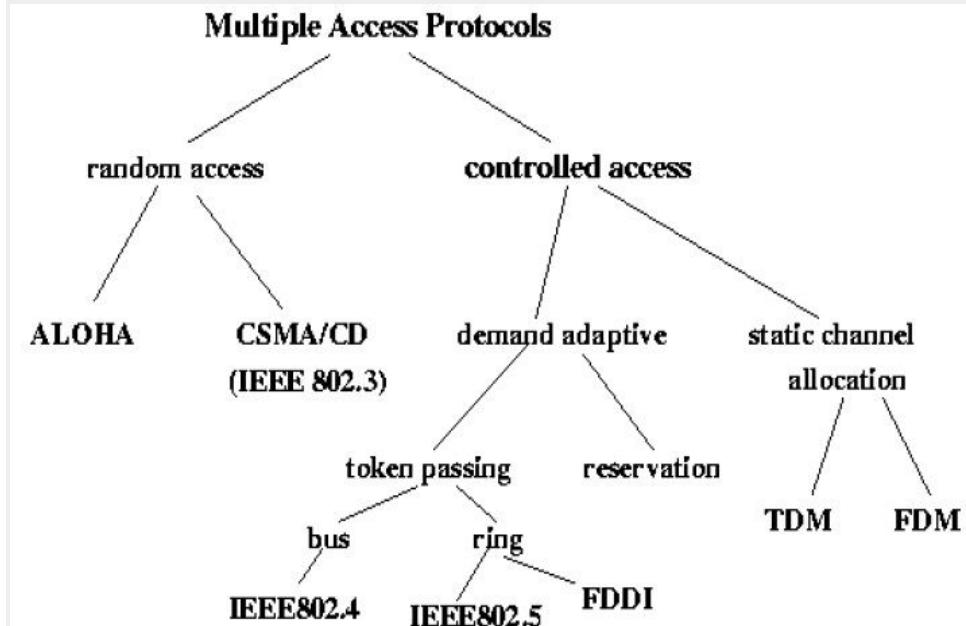


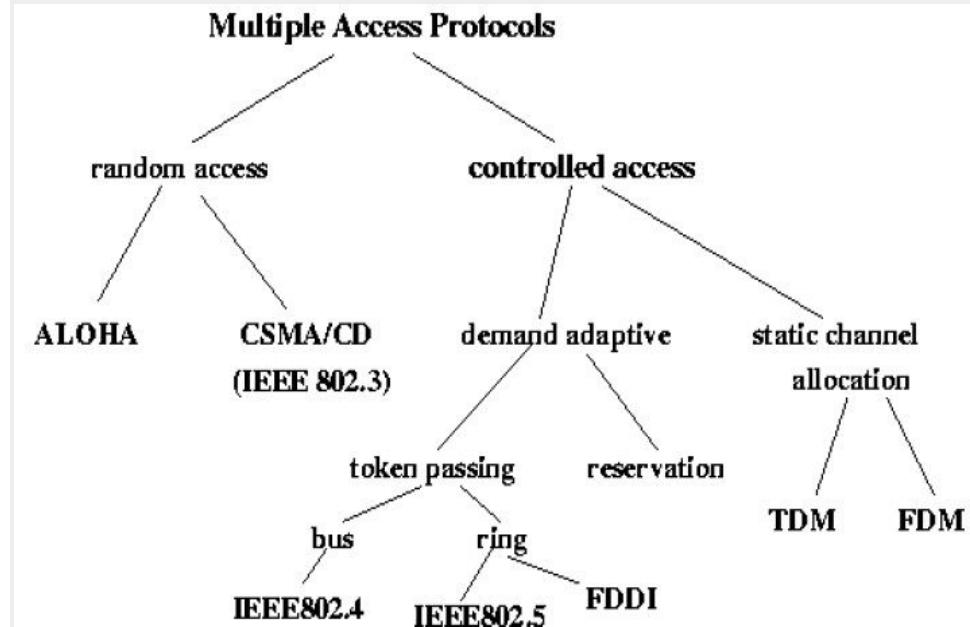
Image Source:

https://lh6.googleusercontent.com/-v1XCMM7aMys/TXQjf_saj7I/AAAAAAAACF0/EN_K_Co_UK1299Tc-image-of-MAC-Protocols-in-Networking.pptx

Media Access Methods

Introduction

- Given below are some of the common media access methods:
 - CSMA/CD
 - CSMA/CA
 - Token Passing
 - Demand Priority



Media Access Methods

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- This is a media access method which defines how the network places data on the cable and how it takes it off.
 - CSMA/CD specifies how bus topologies such as Ethernet handle transmission collisions.
 - It usually operates in two modes of Carrier Sense, Multiple Access and Collision Detection.

CSMA/CD : CSMA with Collision Detection

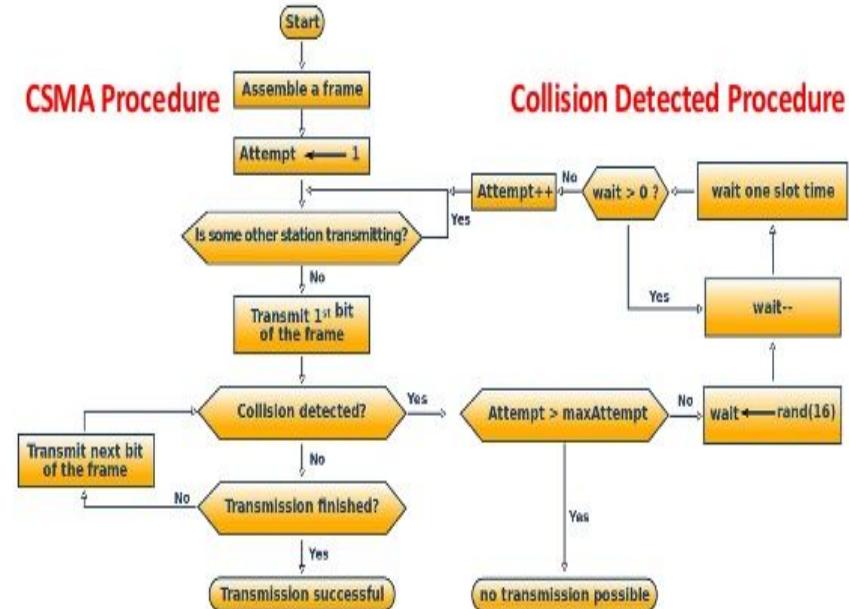


Image Source

<https://image.slidesharecdn.com/csmamohammedabuibaid-160701034304/95/car>

Media Access Methods

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- **Carrier Sense** means that each station on the LAN continually listens to (tests) the cable for the presence of a signal prior to transmitting.
- **Multiple Access** means that there are many computers attempting to transmit and compete for the opportunity to send data (i.e., they are in contention).

CSMA/CD : CSMA with Collision Detection

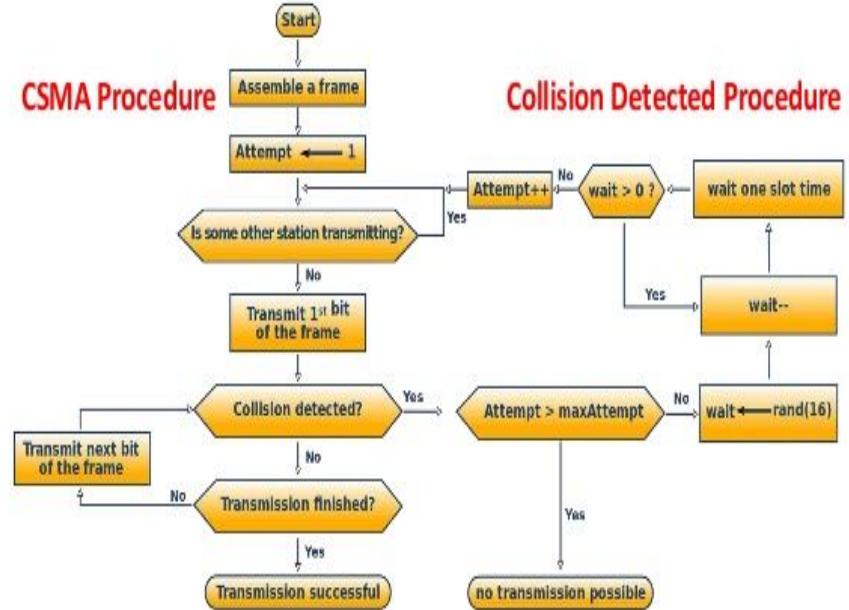


Image Source:

<https://image.slidesharecdn.com/csmamohammedabuibaid-160701034304/95/carrier-sense-multiple-access-with-collision-detection-11-638.jpg?cb=1467615200>

Media Access Methods

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- **Collision Detection** means that when a collision is detected, the stations will stop transmitting and wait a random length of time before retransmitting the data.

CSMA/CD : CSMA with Collision Detection

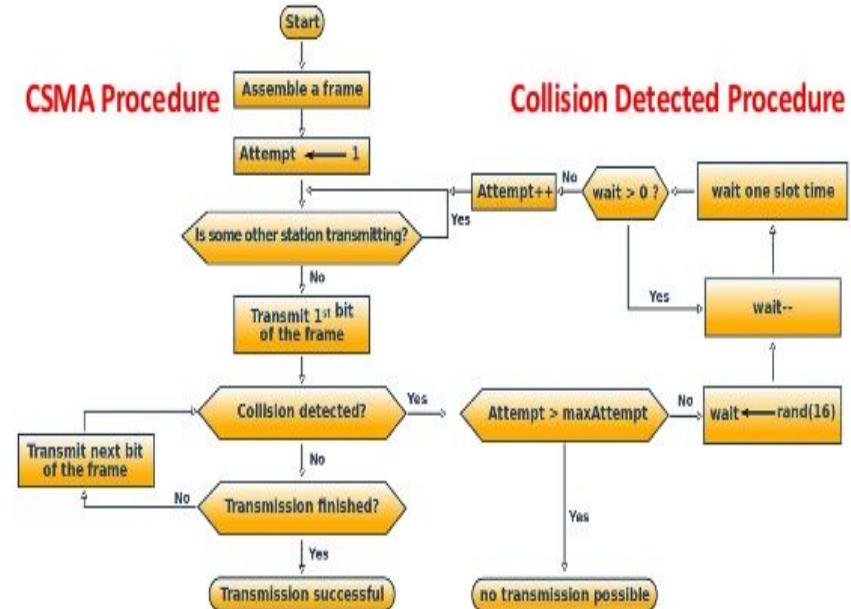


Image Source:

<https://image.slidesharecdn.com/csmamohammedabuibaid-160701034304/95/carrier-sense-multiple-access-with-collision-detection-11-638.jpg?cb=1467615200>

Media Access Methods

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- CSMA/CA stands for Carrier-Sense Multiple Access with Collision Avoidance and is a media access method very similar to CSMA/CD.
- The difference is that the CD (collision detection) is changed to CA (collision avoidance).

CSMA with Collision Avoidance

Collisions are avoided by three strategies:

- Inter-frame space
- The contention window
- Acknowledgments

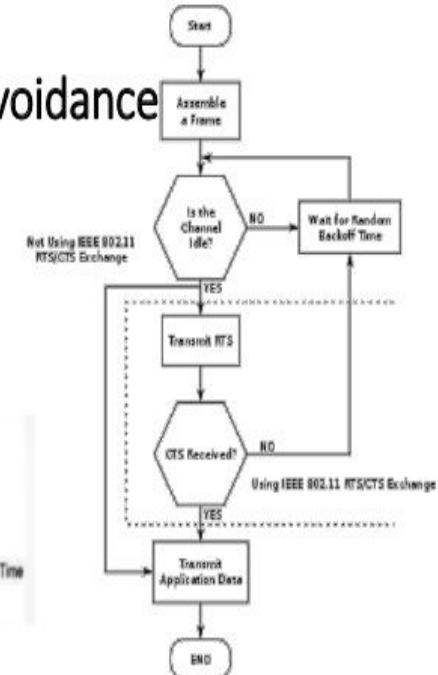
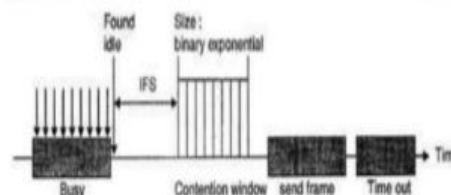


Image Source:

<https://image.slidesharecdn.com/csmamohammedabuibaid-160701034304/95/carrier-sense-multiple-access-with-collision-avoidance-14-638.jpg?cb=1467915900>

Media Access Methods

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- Instead of detecting and reacting to collisions, CSMA/CA tries to avoid them by having each computer signal its intention to transmit before actually transmitting.
- In effect, the transmitting computer gives a “Request” prior to transmitting.

CSMA with Collision Avoidance

Collisions are avoided by three strategies:

- Inter-frame space
- The contention window
- Acknowledgments

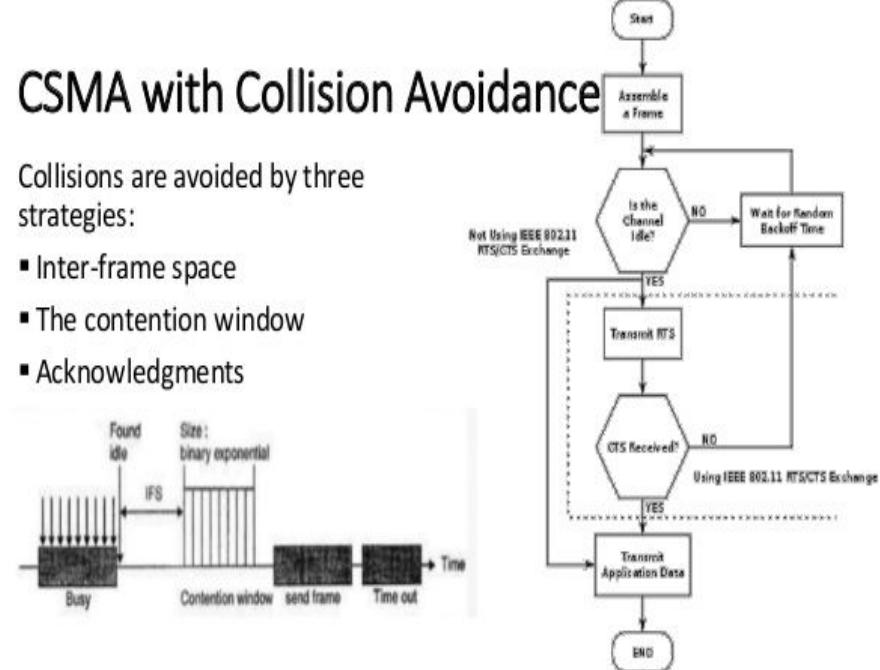
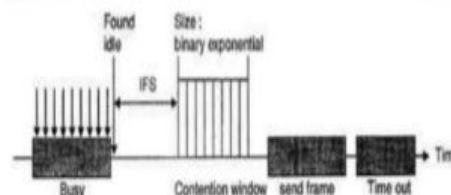


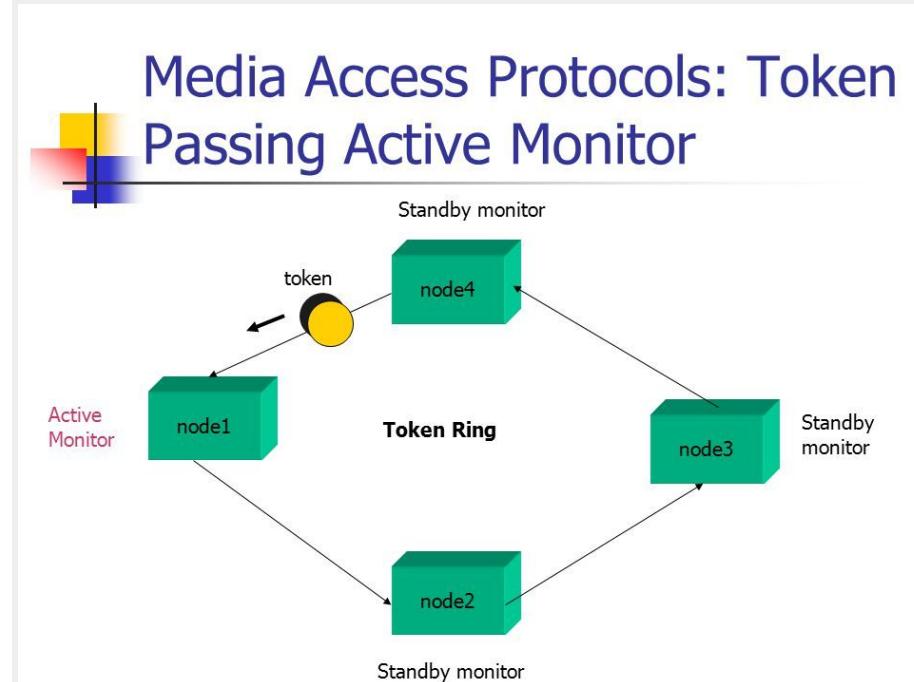
Image Source:

<https://image.slidesharecdn.com/csmamohammedabuibaid-160701034304/95/carrier-sense-multiple-access-with-collision-avoidance-14-638.jpg?cb=1467615000>

Media Access Methods

Token Passing

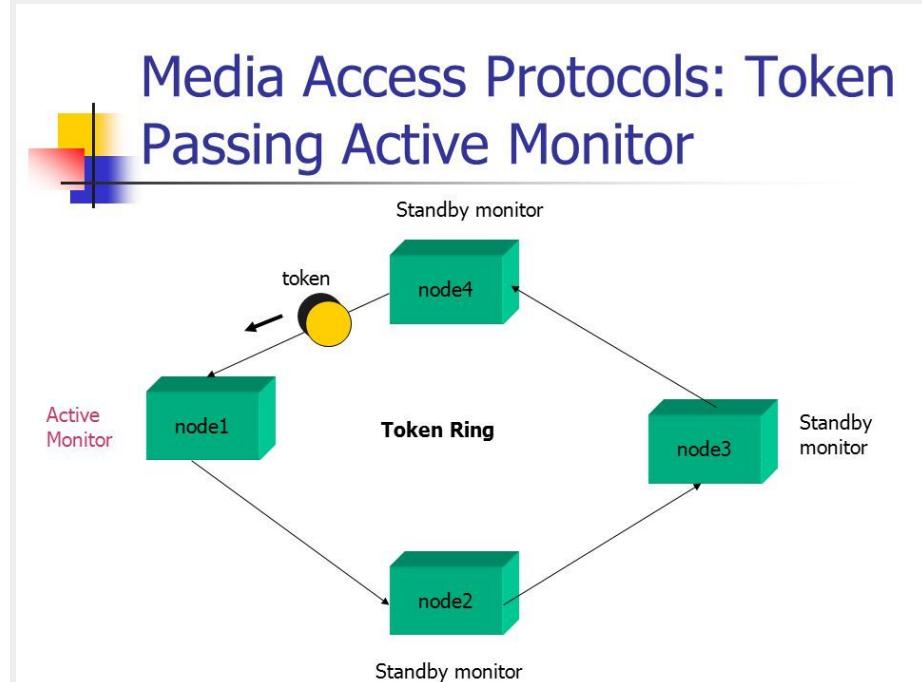
- Token passing is a media access method by which collisions are prevented.
- Collisions are eliminated under token passing because only a computer that possesses a free token (a small data frame) is allowed to transmit.
- The token passing method also allows different priorities to be assigned to different stations on the ring.



Media Access Methods

Token Passing

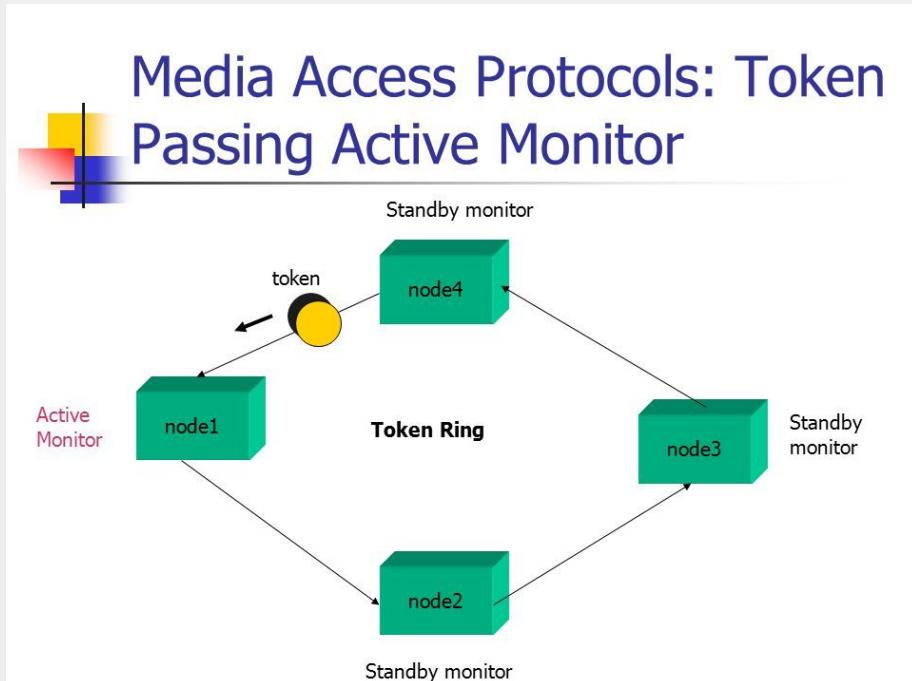
- Transmissions from stations with higher priority take precedence over stations with lower priority.
- Token passing works best in an environment where a relatively large number of shorter data frames are being transmitted



Media Access Methods

Token Passing

- There are two common error conditions that can occur on a token passing LAN:
 - Constant Frame Error
 - A token cannot be acknowledged and continues to be passed around the ring.
- A token is accidentally “hung up” or removed from the ring.



Media Access Methods

Demand Priority

- Demand priority is the new Ethernet media access method that will probably replace the popular but older CSMA/CD method.
- In demand priority, an active hub is an essential requirement that can control the access to the network.

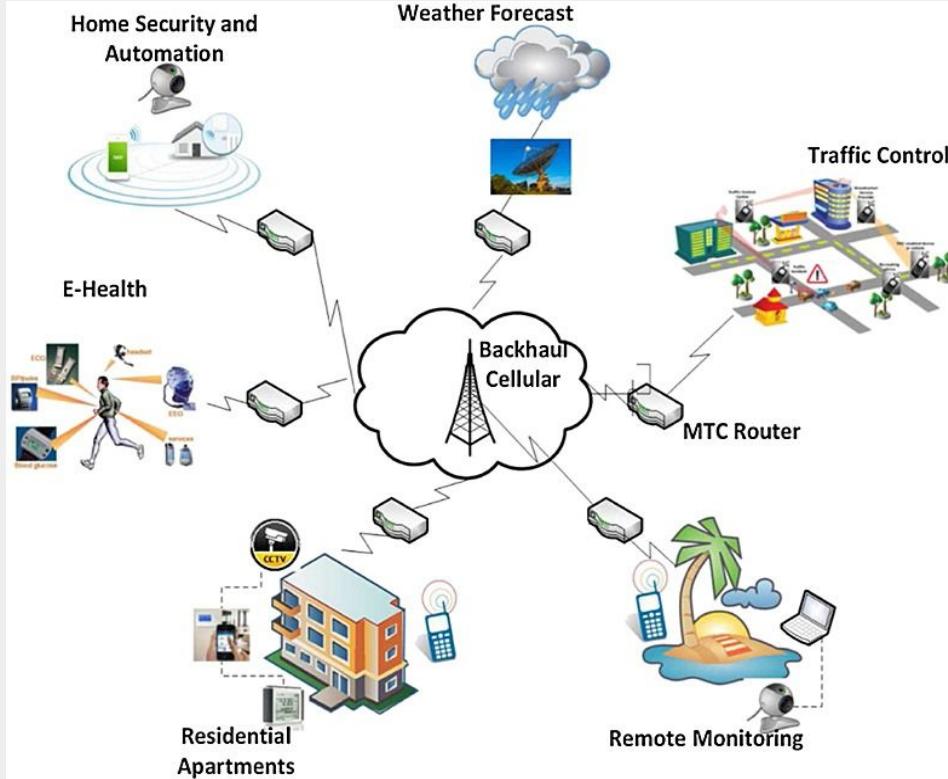


Image Source:

[https://onlinelibrary.wiley.com/cms/asset/70bc301f-349e-41bd-a976-bfcacf792ffcc/
IJCN2020_Lec_0001.pdf](https://onlinelibrary.wiley.com/cms/asset/70bc301f-349e-41bd-a976-bfcacf792ffcc/IJCN2020_Lec_0001.pdf)

Media Access Methods

Demand Priority

- The terminals on a network are required to obtain permission from the hub before they start transmitting the bytes over a network.

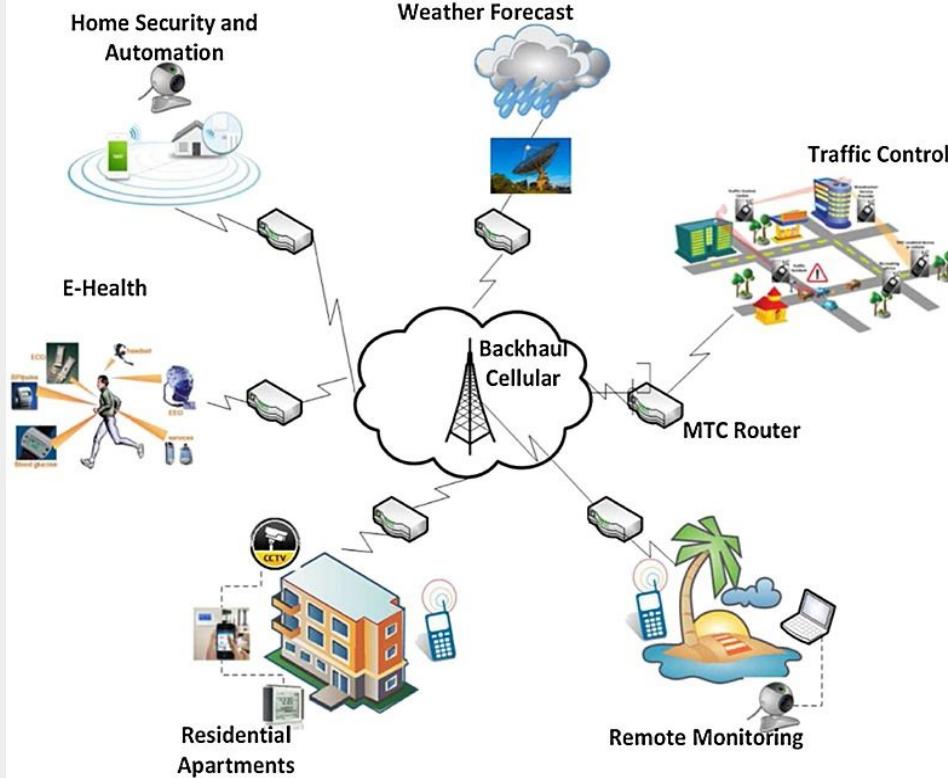


Image Source:

[https://onlinelibrary.wiley.com/cms/asset/70bc301f-349e-41bd-a976-bfcacf792ffcc/
IJCN2020_Lec_0001.pdf](https://onlinelibrary.wiley.com/cms/asset/70bc301f-349e-41bd-a976-bfcacf792ffcc/IJCN2020_Lec_0001.pdf)

Media Access Methods

Demand Priority

- In this the terminals involved in communication can send and receive at the same time.
- The transmission can be prioritized based on the requirements; for example, time sensitive data such as video can be given priority.

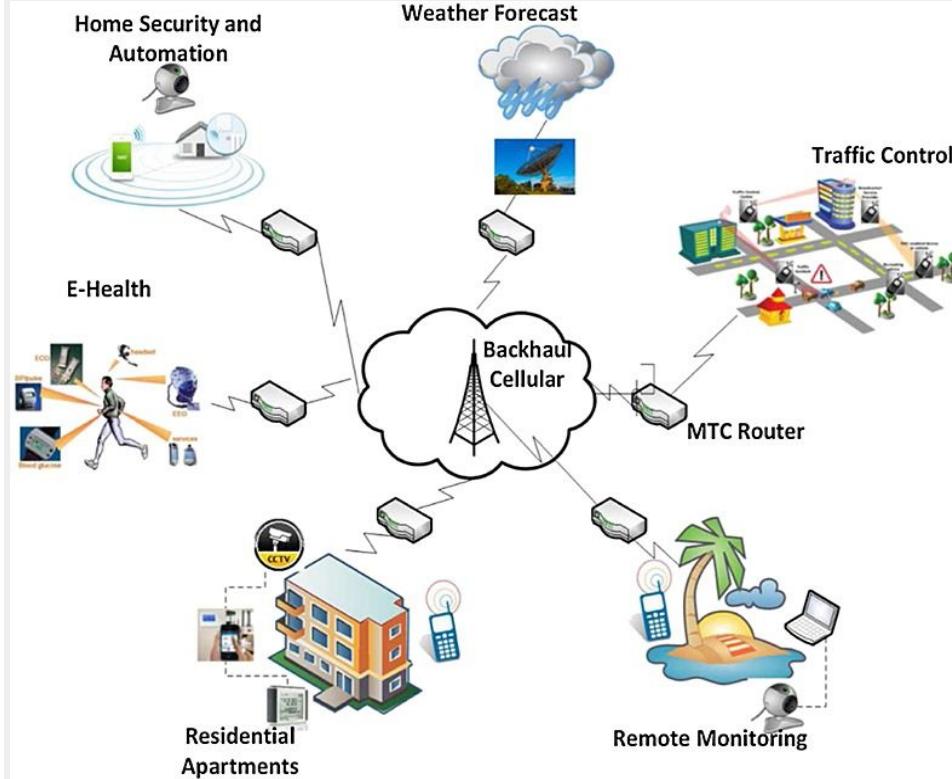


Image Source:

[https://onlinelibrary.wiley.com/cms/asset/70bc301f-349e-41bd-a976-bfcacf792ffcc/
IJCCS2020-1-1-2.pdf](https://onlinelibrary.wiley.com/cms/asset/70bc301f-349e-41bd-a976-bfcacf792ffcc/IJCCS2020-1-1-2.pdf)

Media Access Methods

Difference

CSMA/CD

Used primarily by Ethernet LANs.

Works best in larger networks with relatively fewer, longer data frames.

Does not allow different priorities to be assigned to stations.

Normally less expensive than token passing.

Token Passing

Used primarily by Token Ring LANs.

Works best in small to medium size networks with many short data frames

Allows different priorities to be assigned to stations.

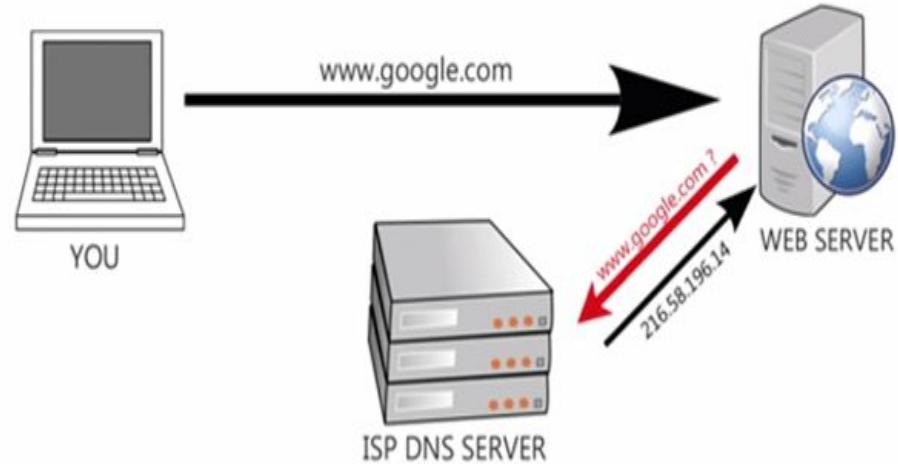
Normally more expensive than **CSMA/CD**.

DNS Service

Introduction

- Domain Name System (DNS) is an Internet service that translates the domain names into IP addresses, which computer can understand.
- Every device connected to the internet has a unique IP address which other machines use to find the device.

HOW DNS WORKS



DNS Records

Records	Description	Function
A	Address Record	It returns a 32bit IP addresses. This is where the actual Website is redirected towards most commonly.
CNAME	Canonical Name Record	This is an Alias. The DNS Server will continue to lookup with this new name.
DNAME	Delegation Name	This again is an alias for a name and also its subname, unlike CNAME, which is only an alias for itself. But similar to CNAME, the DNS Server tries to lookup with this new name as well.
DNSKEY	DNS KEY Record	There is another record known as KEY record which I haven't mentioned here. The format of DNSKEY is same as the KEY, and is used in DNSSEC (more in description).

DNS Service

DNS Records

LOC	Location Record	This provides the geographical location depending upon the domain name.
MX	Mail Exchange Record	This is related to the email routing which I mentioned previously. This maps the domain name with the email ID.
NS	Name Server Record	Provides a DNS ZONE to authorized name servers.
TKEY	Secret Key Record	This is the Key used with TSIG which is encrypted under Public Key.
TSIG	Transaction Signature	This is used to authenticate updates coming from an approved source or name server. It is used along with TKEY.

DNS Service

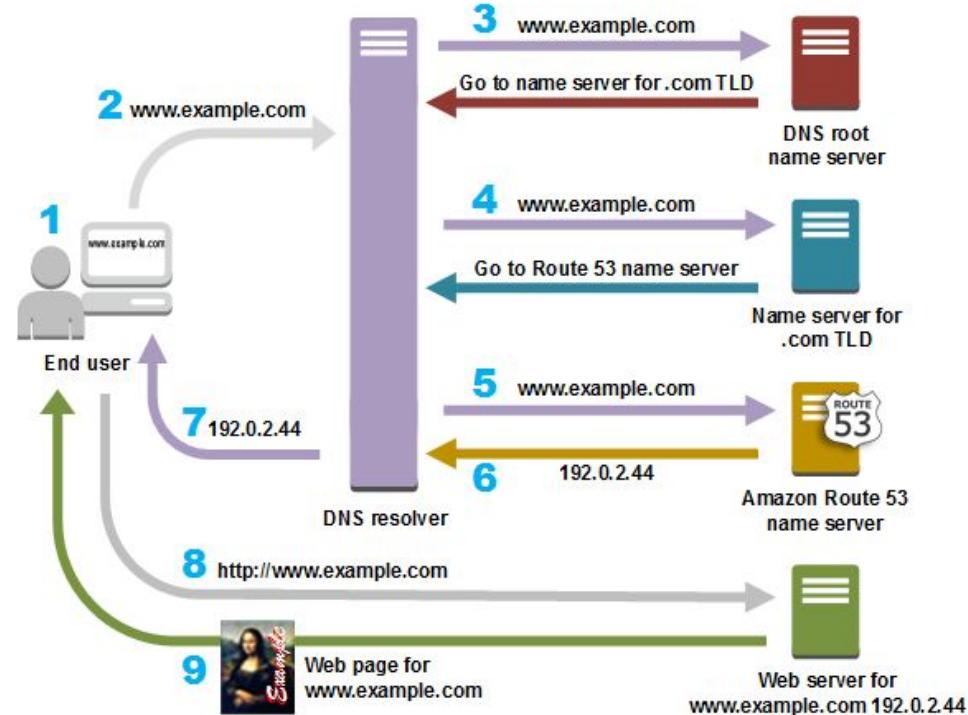
DNS Records

TXT	Text Record	This file provides machine data related to frameworks and encryption.
-----	-------------	---

DNS Service

There are 4 DNS servers involved in loading a webpage:

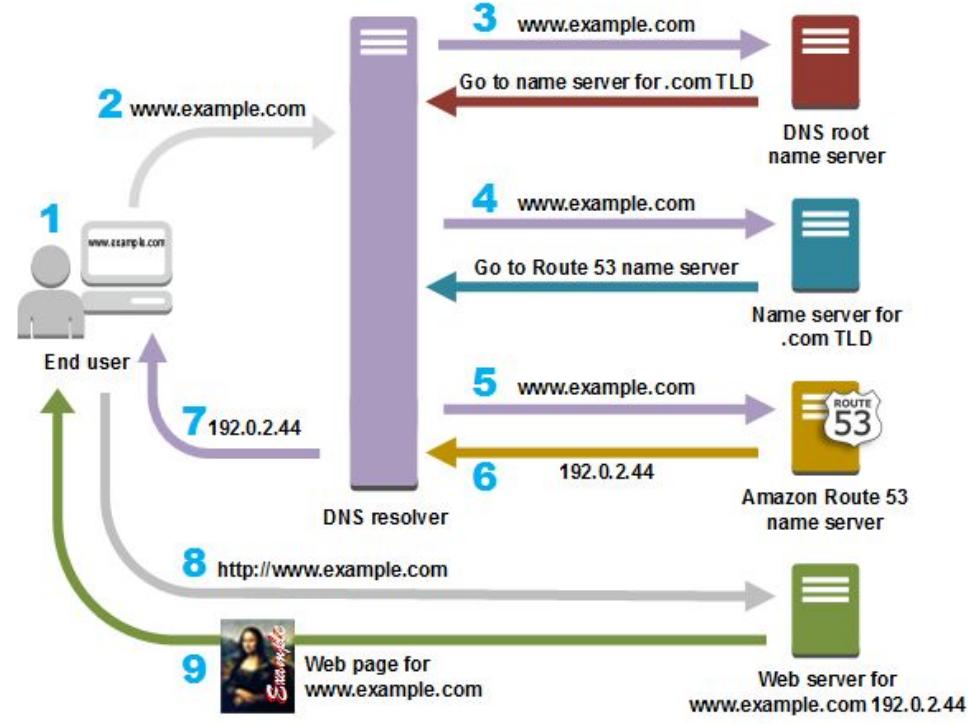
- DNS recursor - The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers.
- Root nameserver - The root server is the first step in translating (resolving) human readable host names into IP addresses



DNS Service

There are 4 DNS servers involved in loading a webpage:

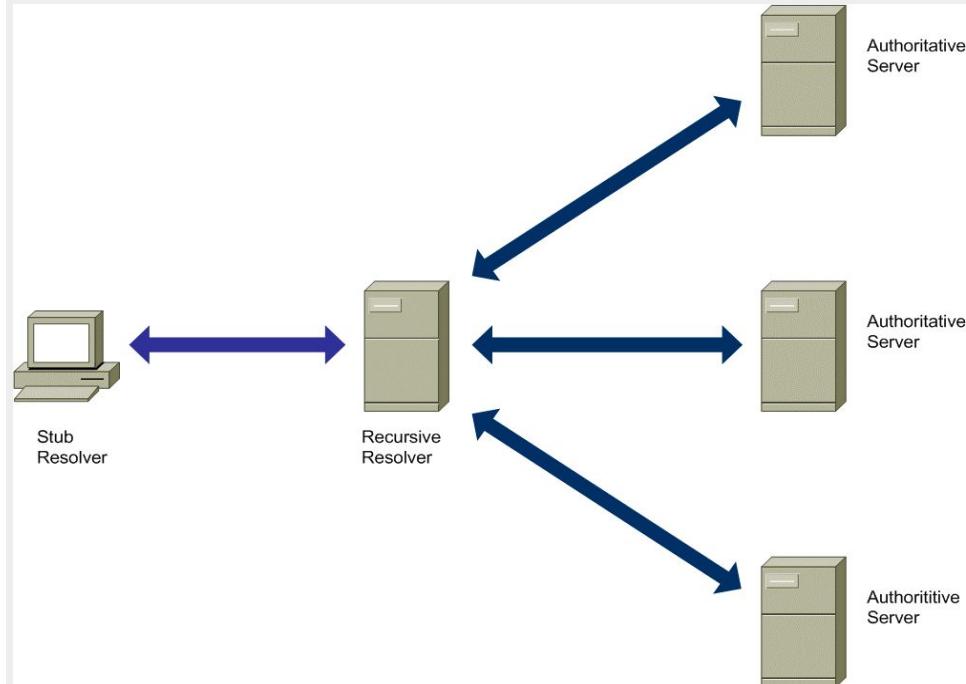
- TLD nameserver - The top level domain server (TLD) ,This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is “com”).



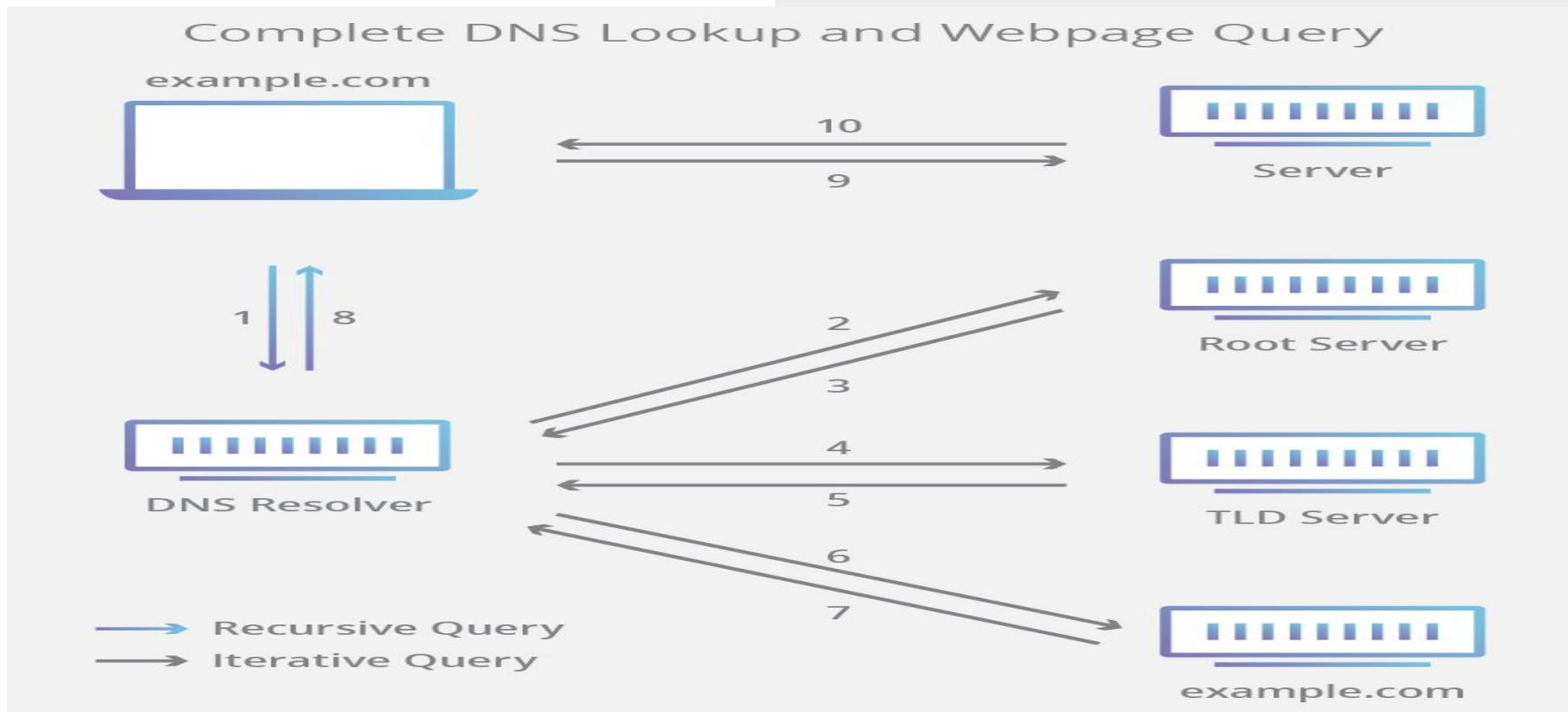
DNS Service

There are 4 DNS servers involved in loading a webpage:

- Authoritative nameserver - If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.



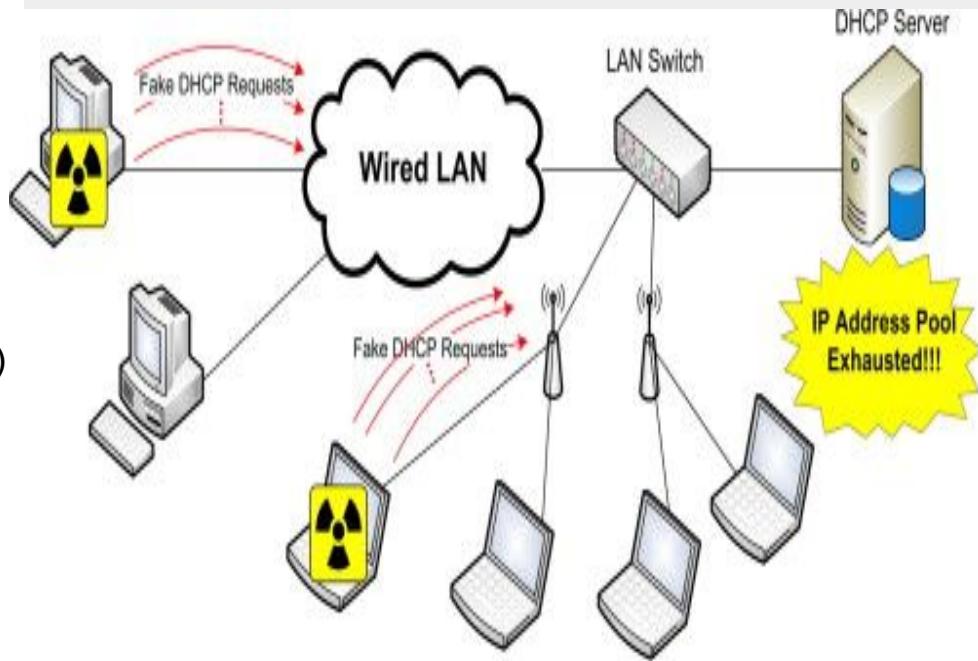
DNS Lookup Process



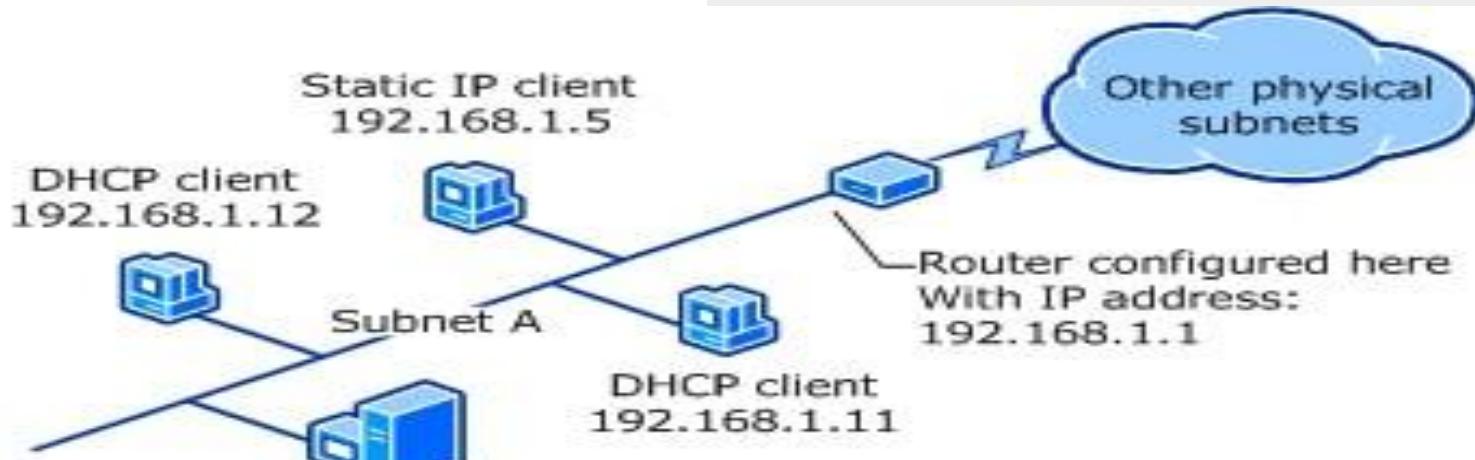
DHCP Service

Introduction

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP.
- The DHCP client will demand an IP address by broadcasting a DHCP Discover message to the local subnet.



DHCP Service



Single scope here configured as follows:

Scope1: 192.168.1.1 – 192.168.1.254

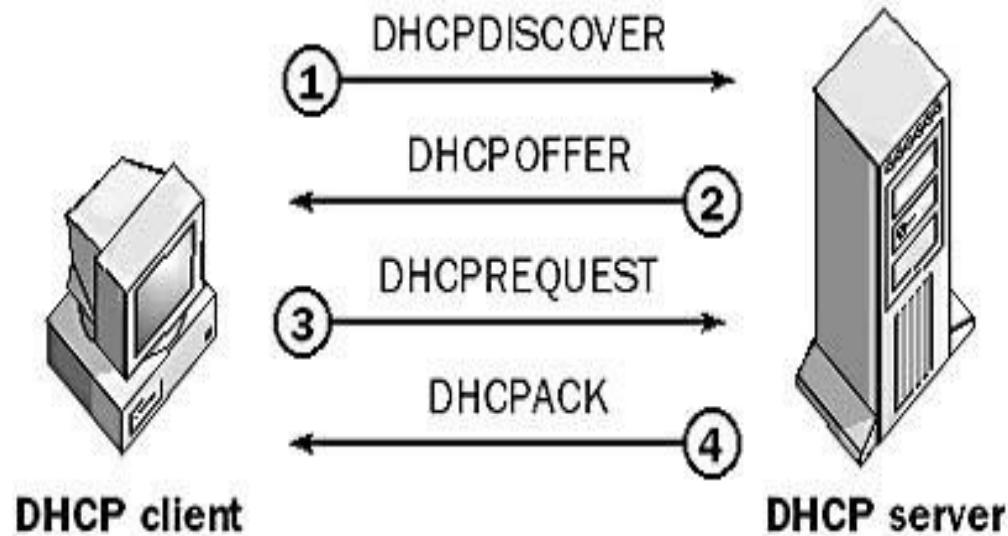
Subnet mask: 255.255.255.0

Excluded addresses: 192.168.1.1 – 192.168.1.10

DHCP Service

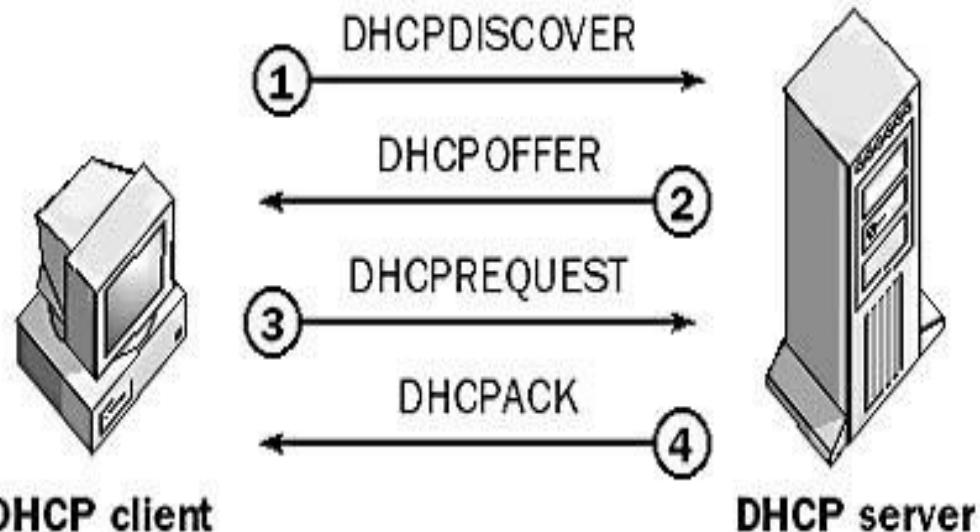
DHCP Process

1. **DHCPDISCOVER:** The client broadcasts a request for a DHCP server.
2. **DHCPOFFER:** DHCP servers on the network offer an address to the client.
3. **DHCPREQUEST:** The client broadcasts a request to lease an address from one of the offering DHCP servers.



DHCP Service

4. **DHCPACK:** The DHCP server that the client responds to acknowledges the client, assigns it any configured DHCP options, and updates its DHCP database. The client then initializes and binds its TCP/IP protocol stack **DHCP client** and can begin network communication.



Windows Internet Name Service

Introduction

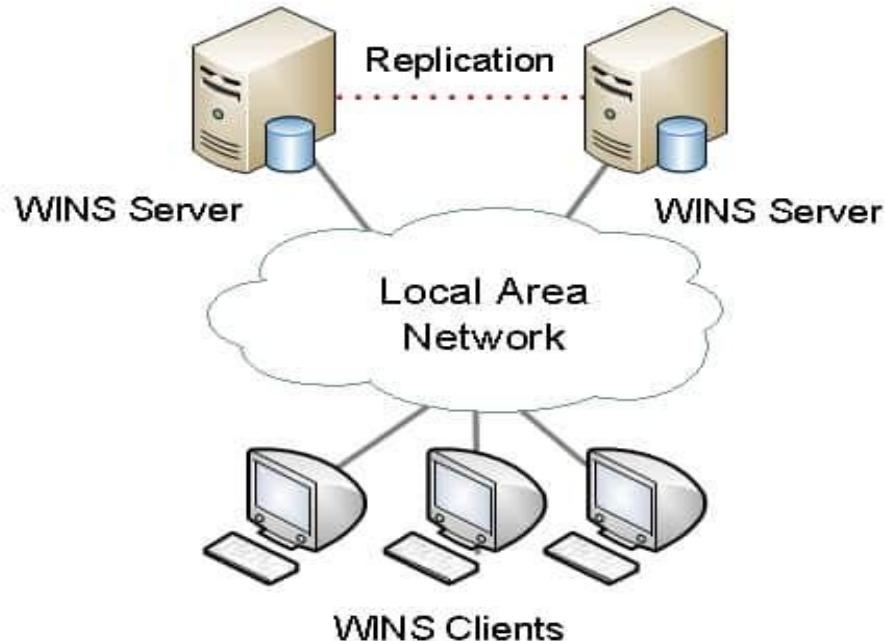
- Windows Internet Name Service, or WINS, is a Microsoft Windows service that dynamically registers NetBIOS names of computers on the network.
- The Windows Internet Naming Service (WINS) converts the NetBIOS host names into IP addresses.



Windows Internet Name Service

Introduction

- It allows the Windows machines on a given LAN segment to recognize Windows machines on other LAN segments.
- It was designed specifically to support NetBIOS over TCP/IP (NetBT)



Windows Internet Name Service

Advantages

- In order for NetBIOS hosts (servers and clients running pre-Windows 2000 versions of Microsoft Windows) to communicate on a network, their NetBIOS names must first be resolved into IP addresses. WINS servers perform this task.



Windows Internet Name Service

Advantages

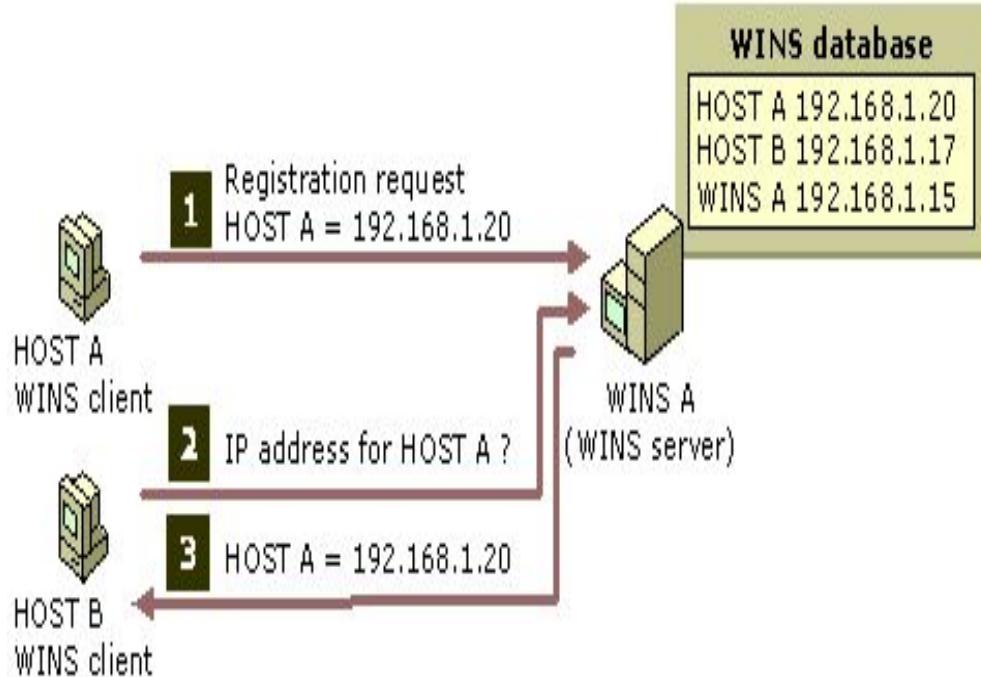
- Directed traffic to WINS servers generates less network traffic than broadcasts.
- WINS provides a mechanism for browsing network resources across multiple domains and subnets.
- The WINS database of NetBIOS name to IP address mappings is dynamically maintained, eliminating the need for lmhosts files on clients.



Windows Internet Name Service

Example

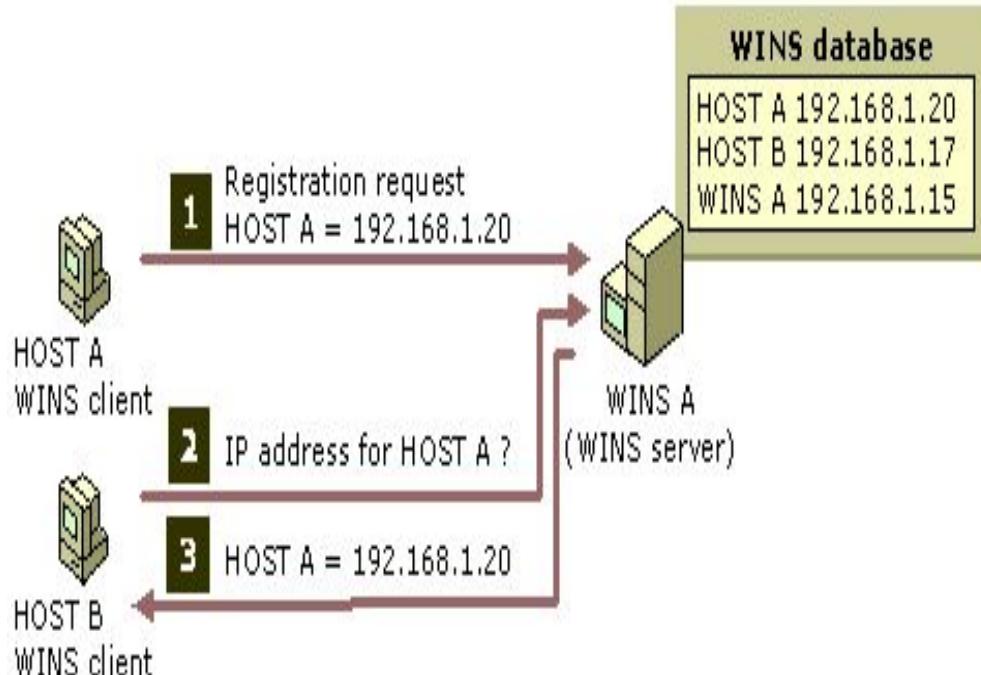
- In this example, the following occurs:
1. A WINS client, HOST-A, registers any of its local NetBIOS names with WINS-A, its configured WINS server.
 2. Another WINS client, HOST-B, queries WINS-A to locate the IP address for HOST-A on the network.



Windows Internet Name Service

Example

- In this example, the following occurs:
 3. WINS-A replies with the IP address for HOST-A, 192.168.1.20.

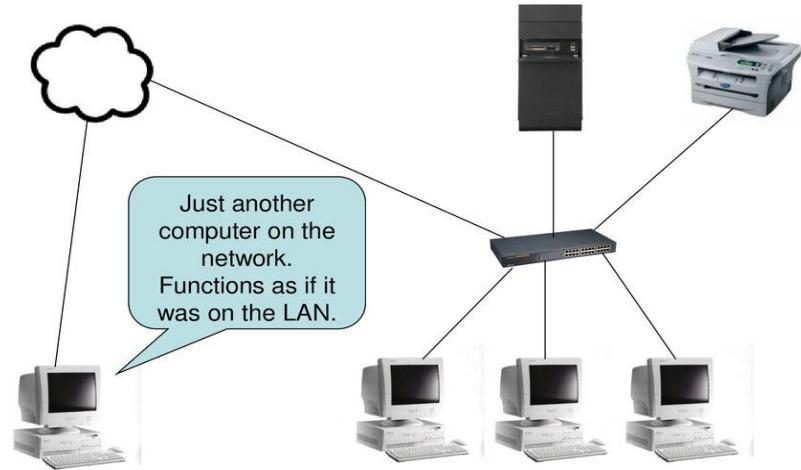


Remote Access Service

Introduction

- A remote access service (RAS) is any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
- A remote access service connects a client to a host computer, known as a remote access server.

Remote Access



Image

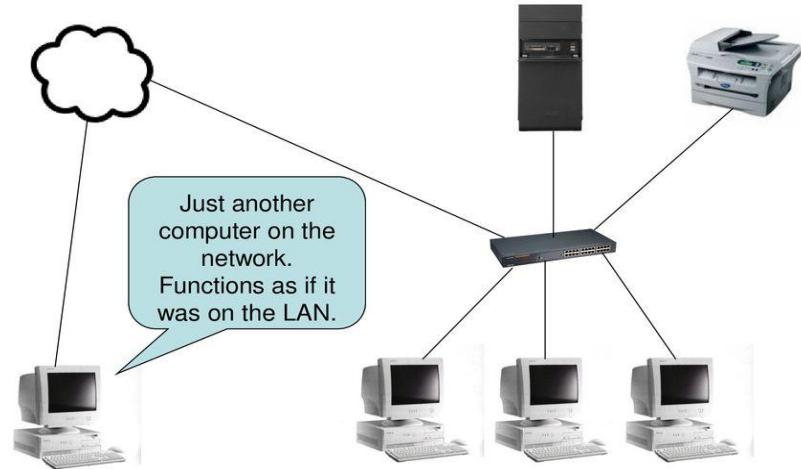
Source: <https://slideplayer.com/slide/14892336/91/images/2/Remote+Access+Just+another+computer+on+the+network+Functions+as+if+it+was+on+the+LAN.jpg>

Remote Access Service

Introduction

- RAS is arranged within an organization and directly connected with the organization's internal network and systems.

Remote Access



Image

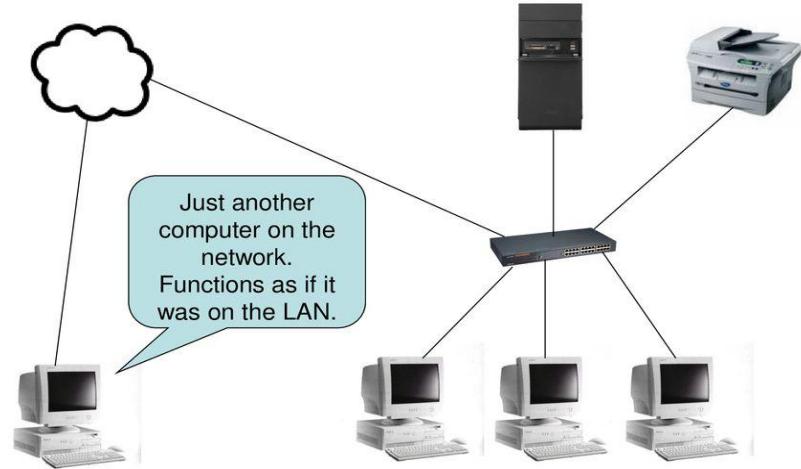
Source: <https://slideplayer.com/slide/14892336/91/images/2/Remote+Access+Just+another+computer+on+the+network+Functions+as+if+it+was+on+the+LAN.jpg>

Remote Access Service

Remote Access Server

- A remote access server (RAS) is a type of server that provides a suite of services to remotely connected users over a network or the Internet.
- It operates as a remote gateway or central server that connects remote users with an organization's internal local area network (LAN).

Remote Access



Image

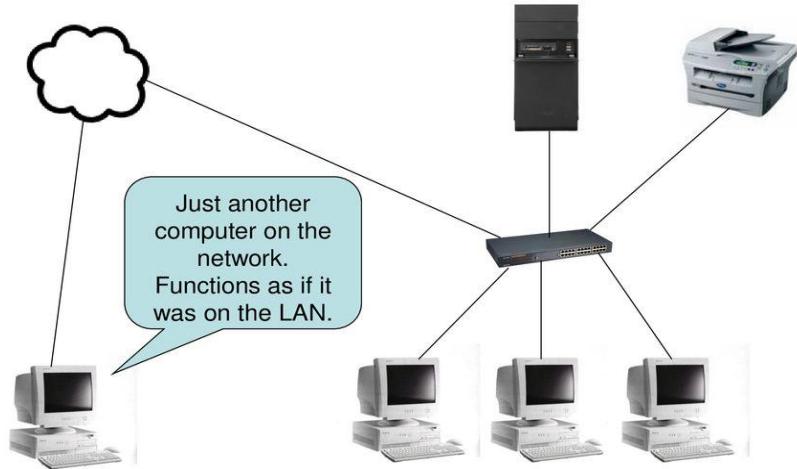
Source: <https://slideplayer.com/slide/14892336/91/images/2/Remote+Access+Just+another+computer+on+the+network+Functions+as+if+it+was+on+the+LAN.jpg>

Remote Access Service

Remote Access Server

- RAS is a service that allows remote clients to connect to the server over a modem using a RAS-based protocol such as the Serial Line Internet Protocol (SLIP) or the newer Point-to-Point Protocol (PPP).

Remote Access



Image

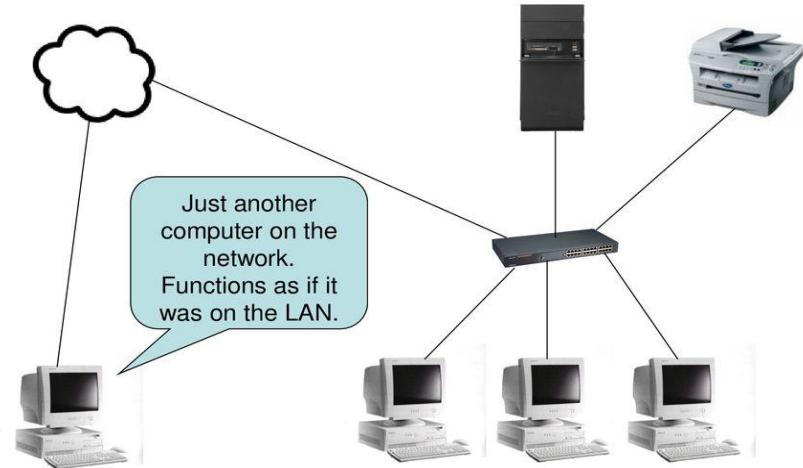
Source: <https://slideplayer.com/slide/14892336/91/images/2/Remote+Access+Just+another+computer+on+the+network+Functions+as+if+it+was+on+the+LAN.jpg>

Remote Access Service

Remote Access Server

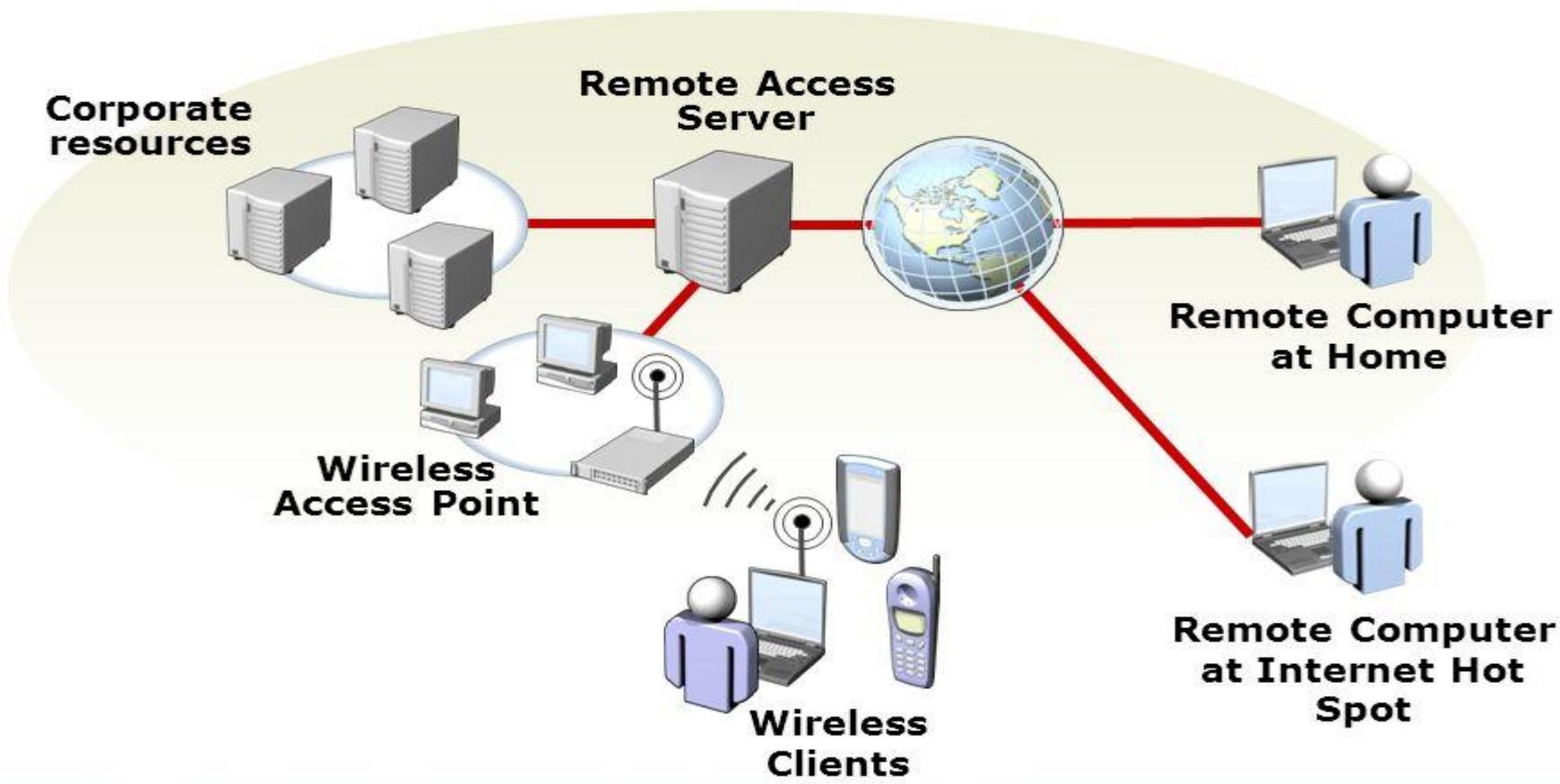
- PPP can run with network protocols such as TCP/IP, IPX/SPX, and NetBEUI; SLIP only supports TCP/IP.
- Examples : Team Viewer, Ammyy software

Remote Access



Image

Source: <https://slideplayer.com/slide/14892336/91/images/2/Remote+Access+Just+another+computer+on+the+network+Functions+as+if+it+was+on+the+LAN.jpg>

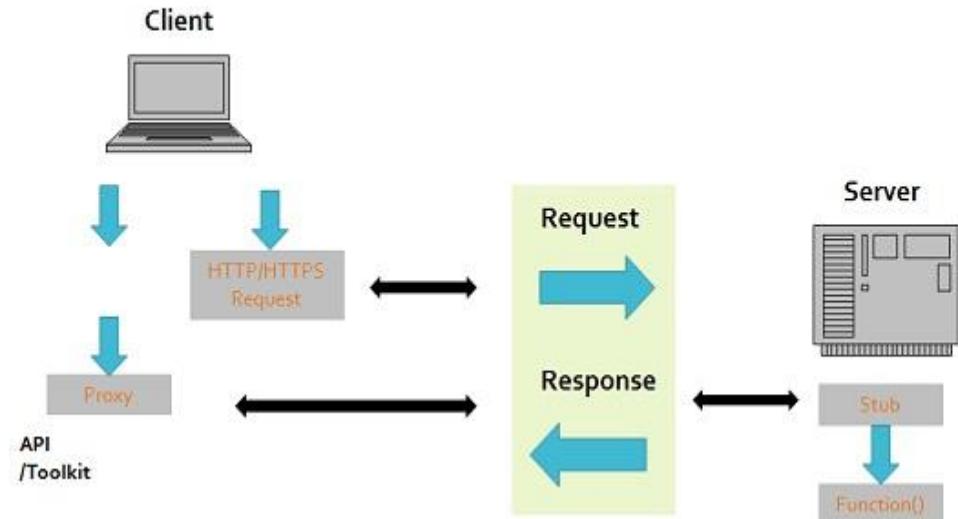


Web Services

Introduction

- Web service is a standardized medium to circulate communication between the client and server applications on the World Wide Web.
- A web service is a software module that is designed to perform a certain set of tasks.

Web Services



Image

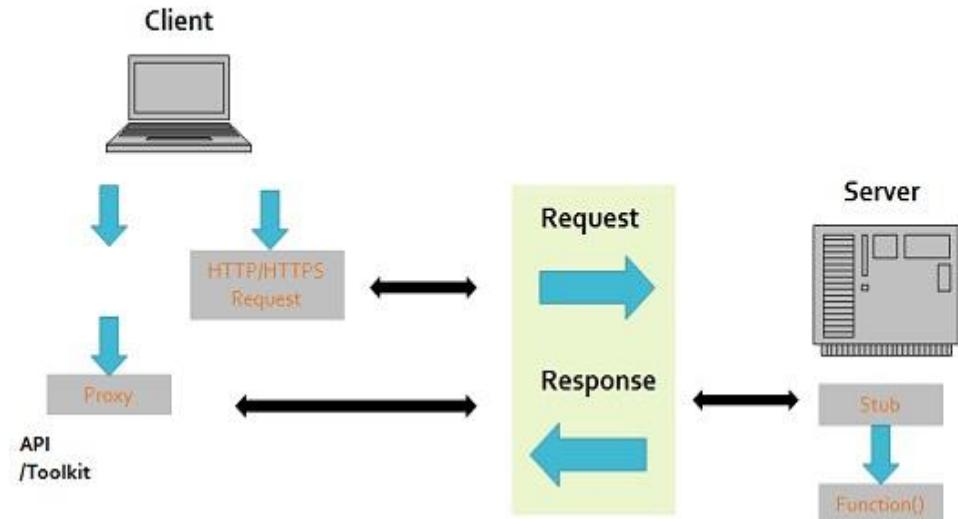
Source: <https://documentation.alphasoftware.com/pages/Guides/Services/Web%20Service%20Client/>

Web Services

Introduction

- A web service is a client server application or application component for communication
- A web service communicate over network between two devices
- It is a software system for interoperable machine to machine communication
- A web service is a collection of open protocols and standards used for exchanging data between applications or systems

Web Services



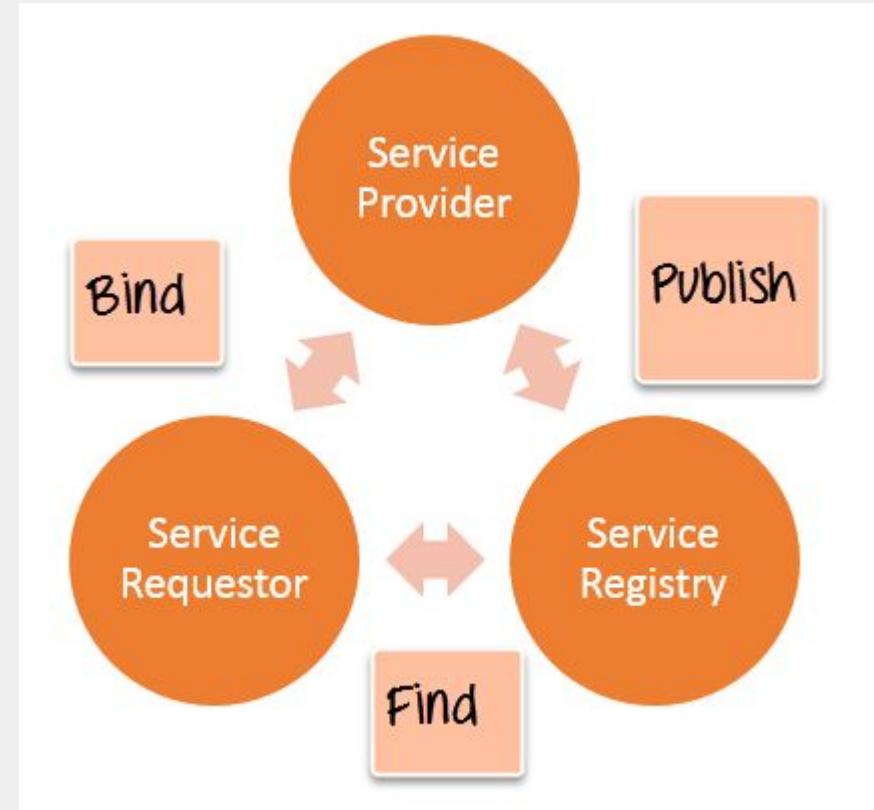
Image

Source:<https://documentation.alphasoftware.com/pages/Guides/Services/Web%20Services%20Client/>

Web Services

Web Services Architecture

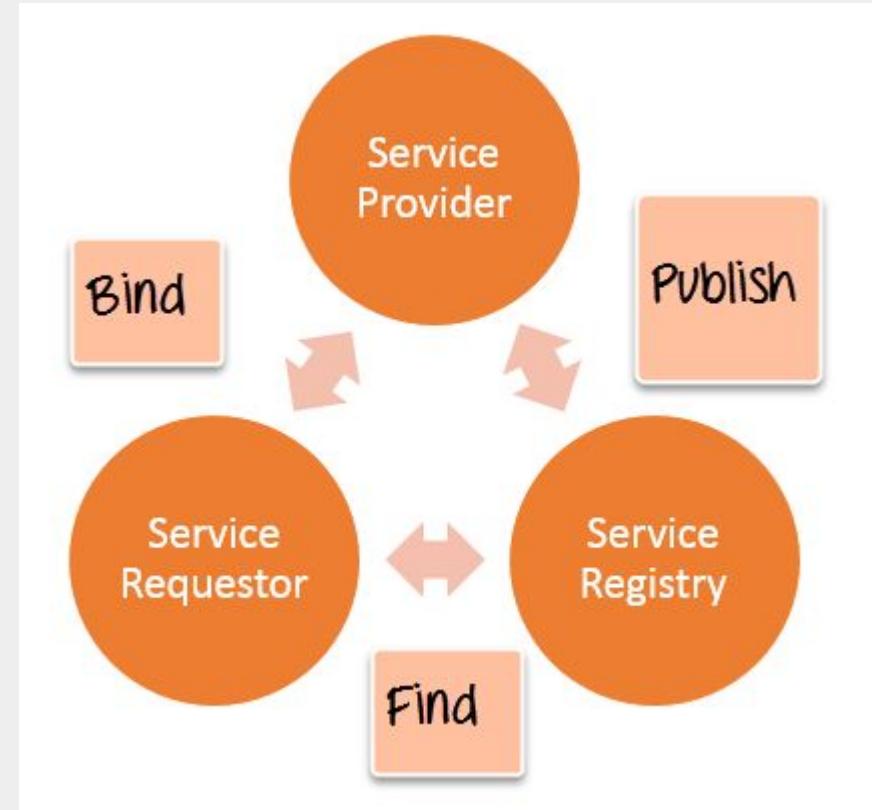
- Provider
- Requestor
- Broker - The broker is nothing but the application which provides access to the UDDI. The UDDI, as discussed in the earlier topic enables the client application to locate the web service.(UDDI stands for Universal Description, Discovery, and Integration.)



Web Services

Web Services Architecture

- Publish - A provider informs the broker (service registry) about the existence of the web service by using the broker's publish interface to make the service accessible to clients
- Find - The requestor consults the broker to locate a published web service
- Bind - With the information it gained from the broker(service registry)

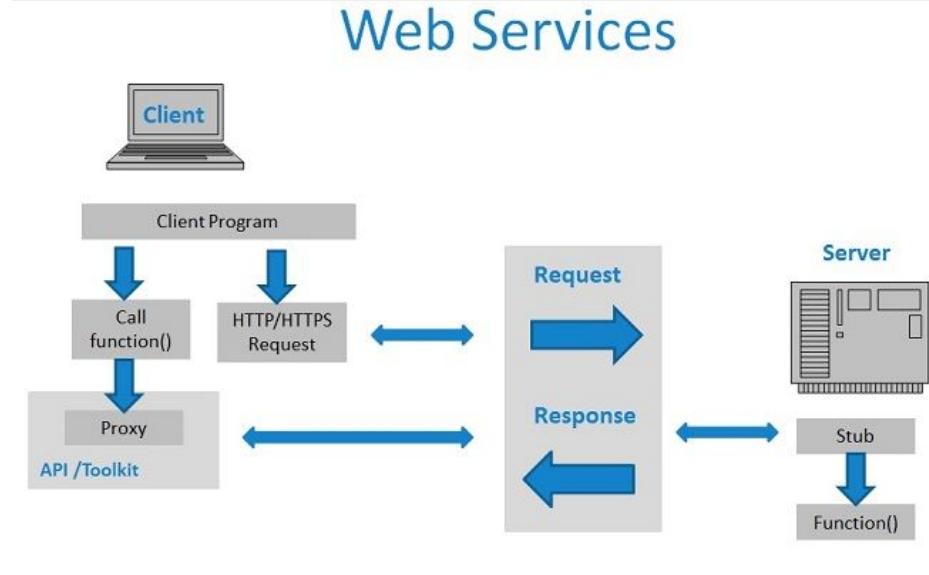


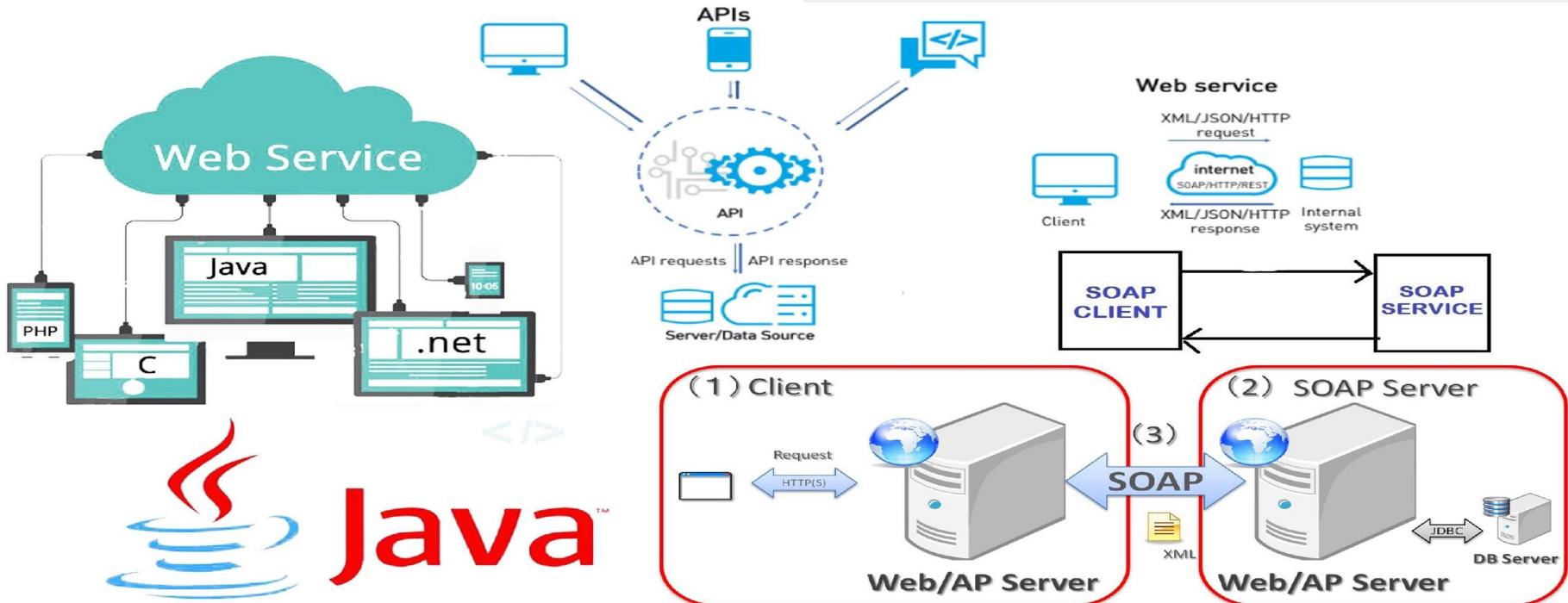
Web Services

Types of Web Services

There are mainly two types of web services.

1. SOAP stands for Simple Object Access Protocol
2. SOAP a XML-based protocol for accessing web services
3. SOAP is platform and language independent
4. SOAP is a W3C recommendation for communication between two applications





SOAP Web services

Web Services

Types of Web Services

- **REST** stands for **R**epresentational **S**tate **T**ransfer. REST is an architectural style not a protocol.
 - Restful Web Service is a lightweight, maintainable, and scalable service that is built on the REST architecture.
 - Restful Web Service, expose API from your application in a secure, uniform, stateless manner to the calling client.

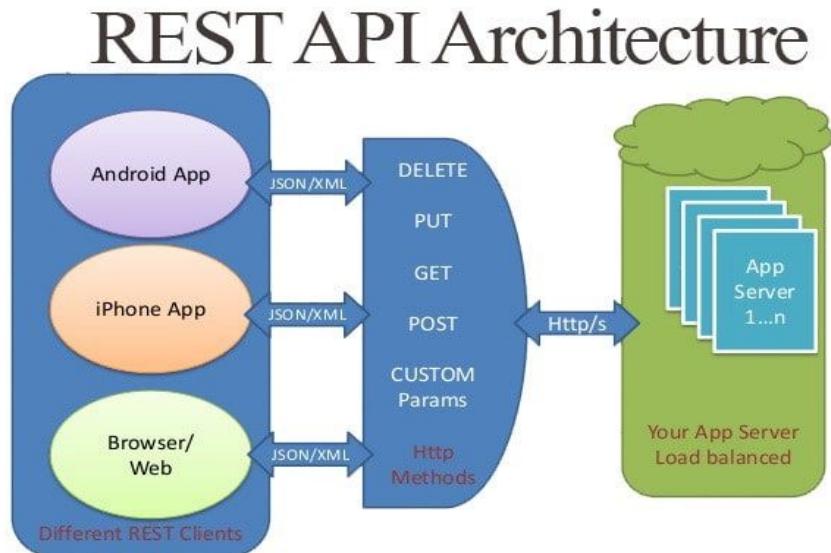
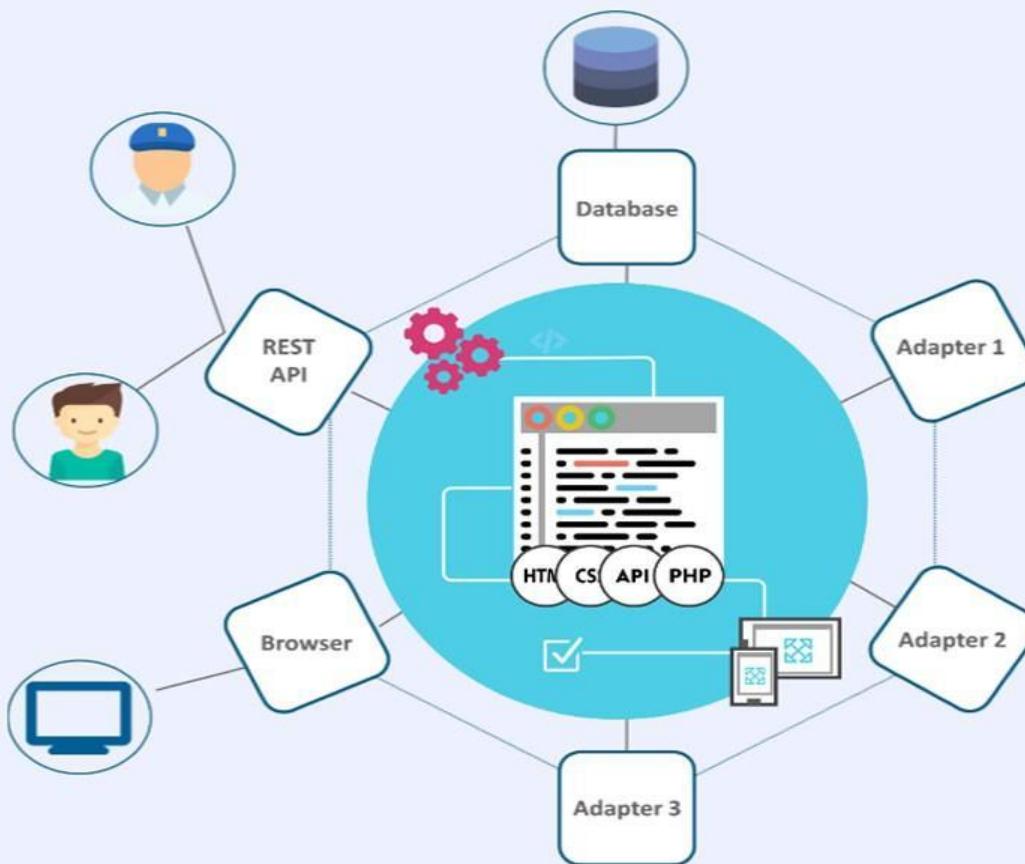


Image Source



Web Services

Web Services API

Advantages

Type	Advantages	Description
SOAP	Security	SOAP defines its own security known as WS Security
	Language and Platform independent	SOAP web services can be written in any programming language and executed in any platform
RESTful	Fast	RESTful Web Services are fast
	Language and Platform independent	It is also language and platform independent
	Can use SOAP	RESTful web services can use SOAP web services as the implementation
	Permits different data format	RESTful web service permits different data format such as Plain Text, HTML, XML and JSON

Disadvantages

Disadvantages	Description
Slow	SOAP uses XML format that must be parsed to be read. It defines many standards that must be followed while developing the SOAP applications. So it is slow and consumes more bandwidth and resource.
WSDL Dependent	SOAP uses WSDL and doesn't have any other mechanism to discover the service

Proxy Services

www.temok.com

Introduction

- A proxy server is a server (a computer system or an application) that acts as an intermediate for requests from clients looking for resources from other servers.
- Monitoring and Filtering
- Improving performance
- Translation
- Accessing services anonymously
- Security

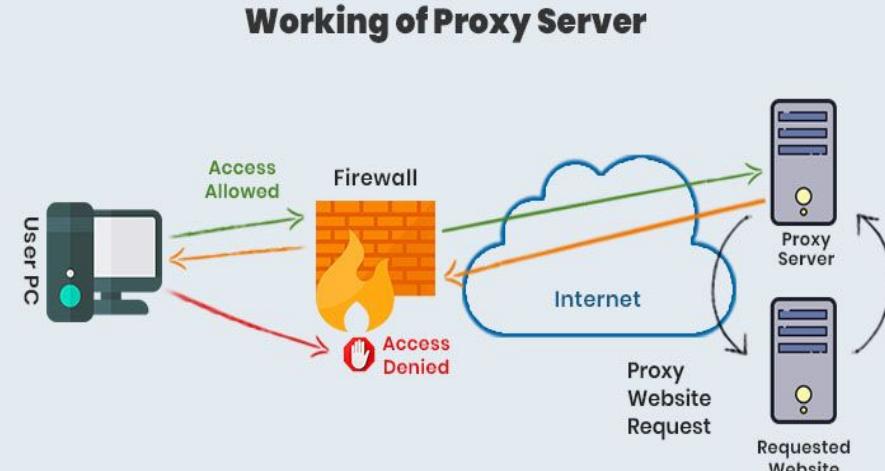


Image Sources:

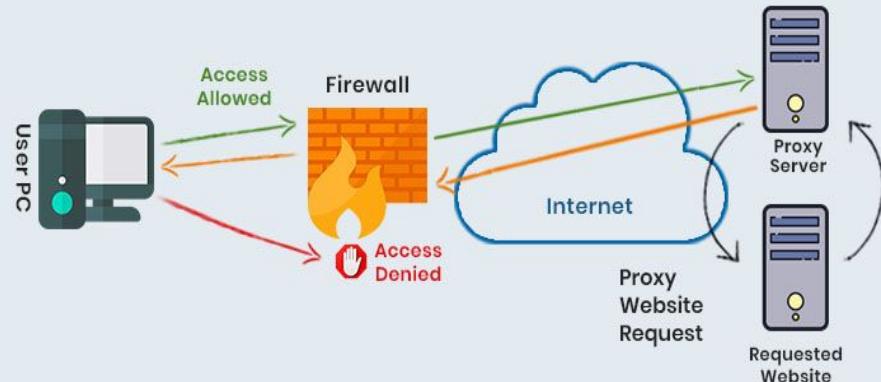
<https://www.temok.com/blog/wp-content/uploads/2019/08/Featured.jpg>

Disadvantages

Introduction

- Monitoring and Filtering
 1. Proxy servers allow us to do several kind of filtering such as:
 2. Content Filtering
 3. Filtering encrypted data
 4. Bypass filters
 5. Logging and eavesdropping

Working of Proxy Server



How Proxy Server Works

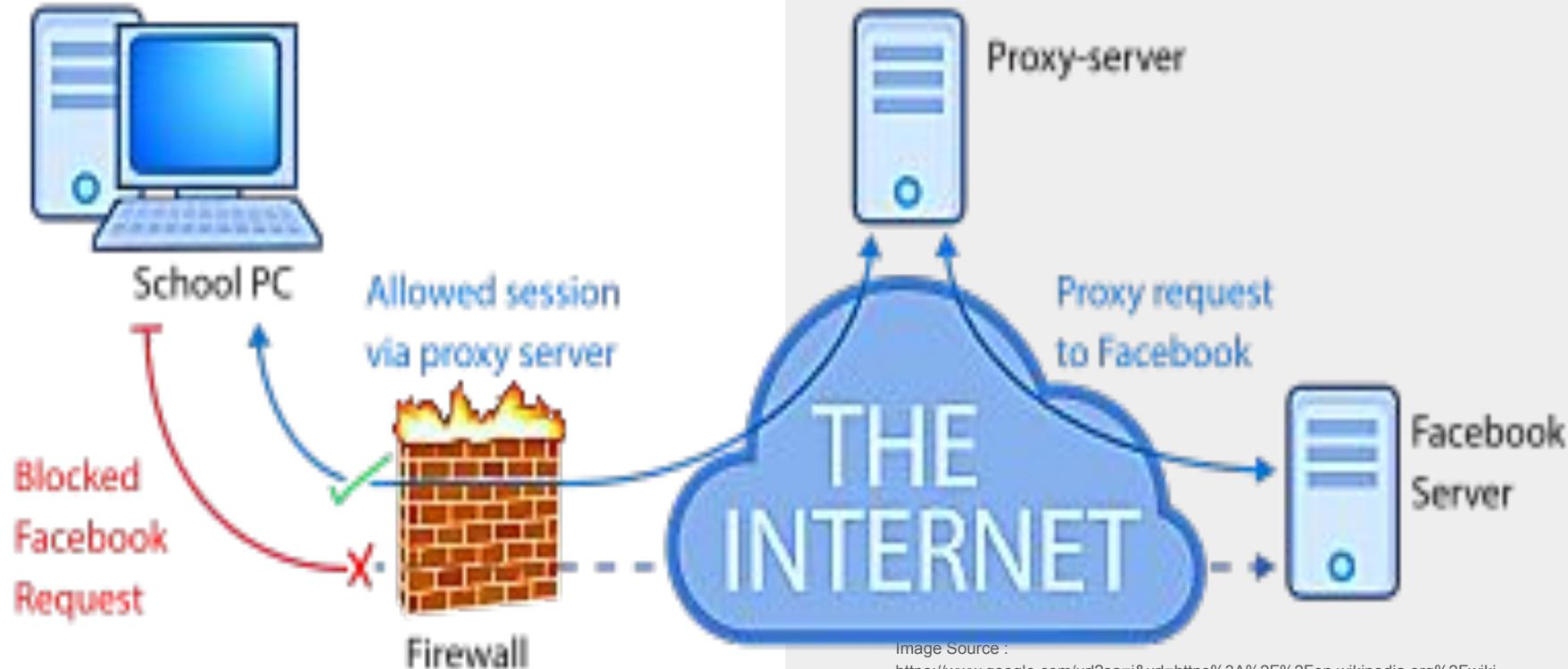


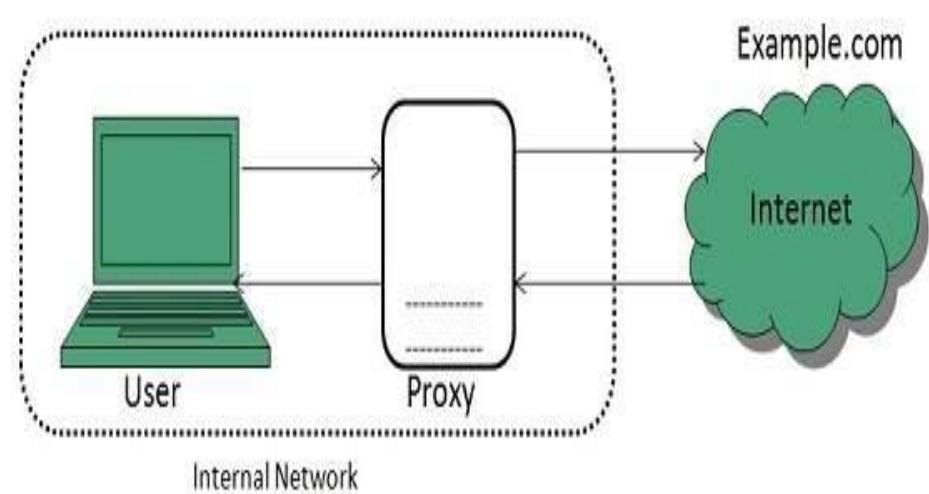
Image Source :

[https://www.google.com/url?sa=i&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FProxy_\(computing\)&q=AO_Ver_24_0_H1_Google_LinuxH3_1_1532007000](https://www.google.com/url?sa=i&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FProxy_(computing)&q=AO_Ver_24_0_H1_Google_LinuxH3_1_1532007000)

Types of proxy servers

Forward Proxy

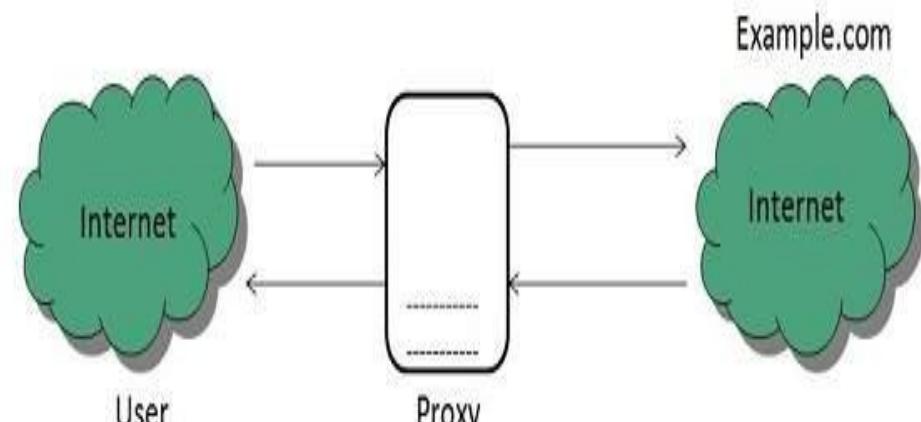
- In this the client requests its internal network server to forward to the internet.



Types of proxy servers

Open Proxy

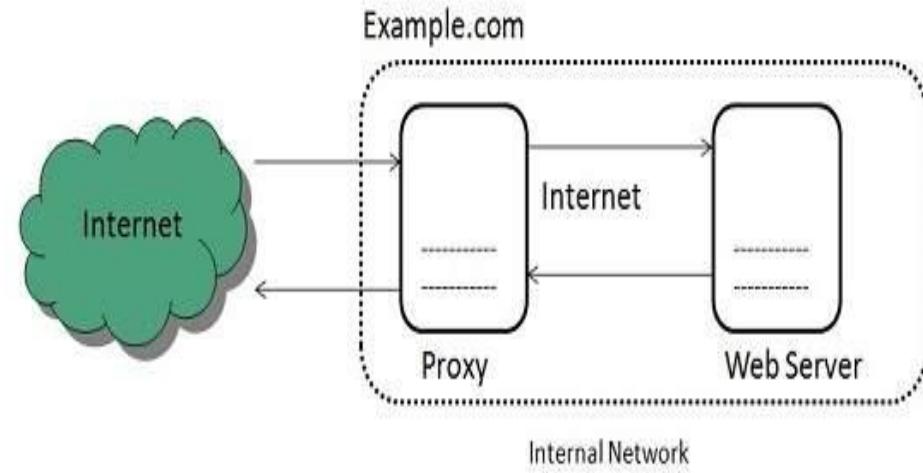
- Open Proxies helps the clients to conceal their IP address while browsing the web.



Types of proxy servers

Reverse Proxy

- In this the requests are forwarded to one or more proxy servers and the response from the proxy server is retrieved as if it came directly from the original Server.



Install and configure Linux server environment

In this section, we will discuss:

- Configuration Plan
- Public and data directory
- Host file
- SWAT
- Password

Configuration Plan

Server Role

- Servers will be purpose-built devices.
- A server will run the services that are necessary to perform its role.
- It is the “Role-Specific” section containing
- guidelines for specific common server roles.



Image Source:

<https://medium.com/viithisys/10-steps-to-secure-linux-server-for-production-environment-a135109a57c5>

Configuration Plan

Vulnerable Services

- Many services have inherent security vulnerabilities.
- Because they do not encrypt sensitive traffic.



Image Source: <https://blog.trendmicro.com/linux-is-secureright/>

Configuration Plan

Picking a Platform

- Use an advanced server-oriented system when at all possible.

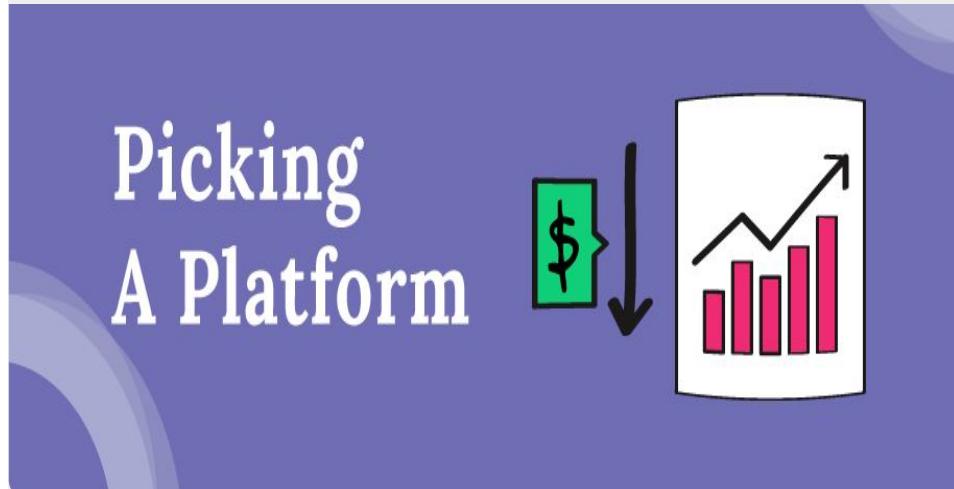


Image Source: <https://snowballfundraising.com/free-nonprofit-crm-software/>

Configuration Plan

Network and Access Control

- It is essential to plan network architecture and configuration ahead of time.
- Using a “least access necessary” model, plan what network sectors need access to this machine.



Image Source: <https://www.bioenabletech.com/network-access-control.html>

Configuration Plan

Users and Authentication

- Recognize potential users and access levels ahead of time.
- Decide what users need what roles and what groups will be needed to manage those roles.



Image Source:

https://developer.orange.com/orange_explains/user-authentication-methods/

Public and data directory

Public folder

- A public folder is a function of a software application.
- It is the only one that handles data of any type, that allows an operator to share files with other operators and devices within the same network or the same computer.
- Different features and setups depending on the application in public folder.

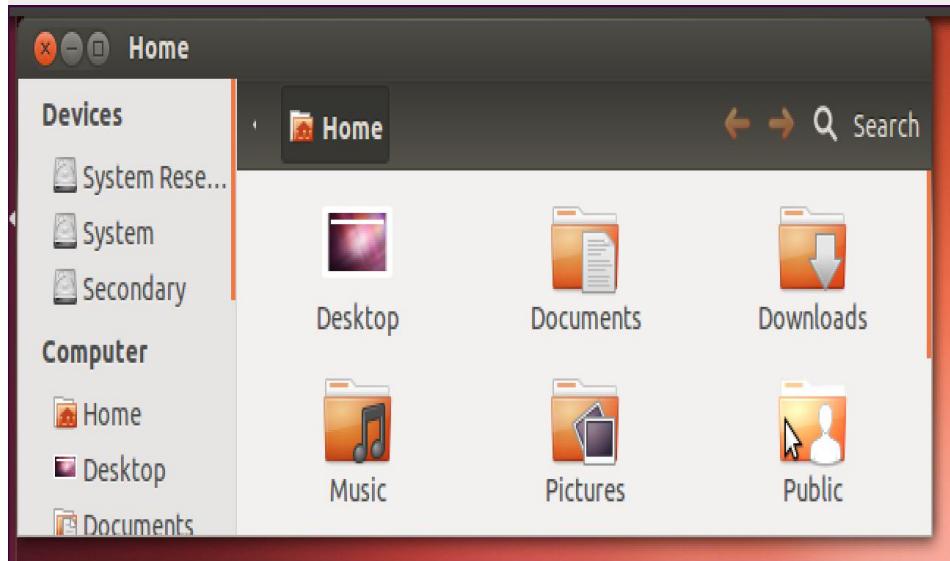


Image Source:

<https://www.howtogeek.com/116309/use-ubuntus-public-folder-to-easily-share-files-between-computers/>

Public and data directory

Data directory

- Data directory initialization can be done automatically, after installing MySQL then will initialize data directory.

```
shell> mkdir MySQL-files
```

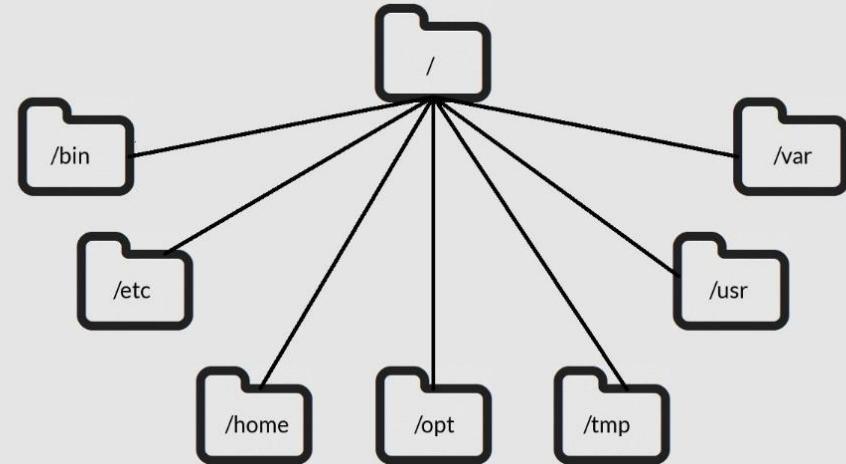


Image Source:

<https://www.linuxtrainingacademy.com/linux-directory-structure-and-file-system-hierarchy/>

Host file

Concept

- All operating systems with the support of the network have a hosts file in order to translate hostnames to IP addresses.
- These are the simple text file located in the etc folder on Linux and Mac OS.



Image Source: <https://vitux.com/linux-hosts-file/>

Host file

Applications

- Block a website
- Handle an attack or resolve a prank
- Create a duplicate for locations on your local server
- Override addresses that your DNS server provides
- Control access to network traffic



The Hosts File on Linux

Image Source: <https://vitux.com/linux-hosts-file/>

SWAT

What is it ?

- SWAT is a web-based application that helps to configure Samba. used to configure the settings on your samba server using GUI (graphic user interface).



Image Source:

<https://thehackernews.com/2015/02/samba-service-hit-by-remote-code.html>

SWAT

Functions

- Globals
 - Provides access to the global parameters in smb.conf. You can work at one of two levels, which shows only the more important options listed, or Advanced, which shows every available parameter.



Image Source:

<https://thehackernews.com/2015/02/samba-service-hit-by-remote-code.html>

SWAT

Functions

- Shares
 - We can create, edit, or drop shares.
 - Edit an existing share. We need to pick it from the combo box, then click on Choose Share; clicking on Delete Share will delete it.



Image Source:

<https://thehackernews.com/2015/02/samba-service-hit-by-remote-code.html>

SWAT

Functions

- Printers
 - It works like shares but works with printers instead.



Image Source:

<https://thehackernews.com/2015/02/samba-service-hit-by-remote-code.html>

SWAT

Functions

- Wizard
 - It lets you do a quick server configuration. Choose either a standalone server, a domain controller, or a domain member.



Image Source:

<https://thehackernews.com/2015/02/samba-service-hit-by-remote-code.html>

SWAT

Functions

- Status
 - It shows you which services are running, active shares, and open files. You can click on Auto Refresh so that the page will refresh on its own every interval (30 secs by default).



Image Source:

<https://thehackernews.com/2015/02/samba-service-hit-by-remote-code.html>

SWAT

Functions

- View
 - You can view the current configuration file. You can click on the View button to see it either in the normal view or the full view.



Image Source:

<https://thehackernews.com/2015/02/samba-service-hit-by-remote-code.html>

SWAT

Functions

- Password
 - It is used to create, delete, enable, or disable local Samba users and change passwords for a local or remote server.



Image Source:

<https://thehackernews.com/2015/02/samba-service-hit-by-remote-code.html>

Password

Need of passwords

- In Linux, regular operators and super operators can access services via password authentication.
- By default, the root user account password is locked in Ubuntu Linux for safety reasons.
- As a result, you cannot log in using root user or use a command such as ‘su –’ to become a Super operator.



Image Source: <http://tecdistro.com/how-to-reset-root-password-in-linux/>

Password

Guidelines for use

- Passwords should consist of 6 to 8 characters including one or more from each of the following sets:
 - Lowercase alphabetic
 - Uppercase alphabetic
 - Digits 0 thru 9
 - Punctuation marks



Image Source: <http://tecdistro.com/how-to-reset-root-password-in-linux/>

Install & configure the different types of network devices in a network

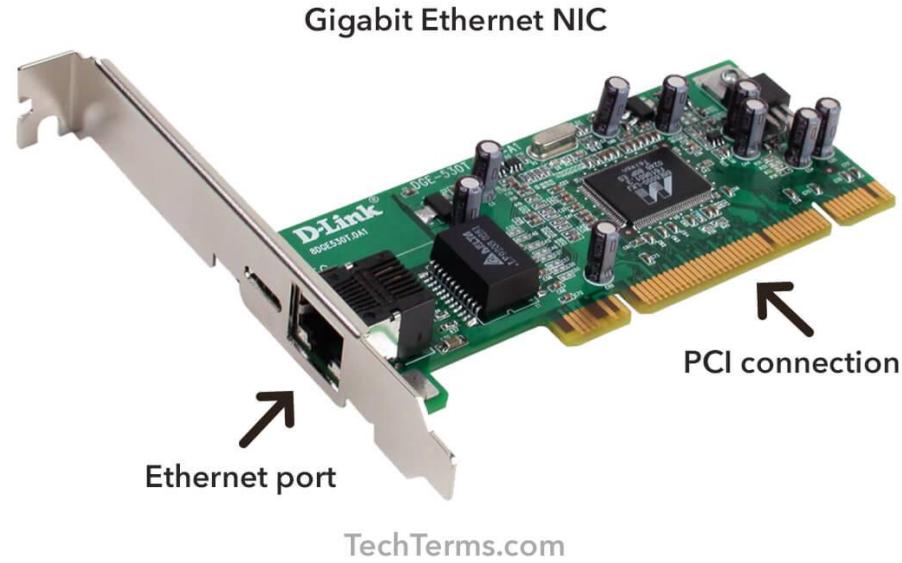
In this section, we will discuss:

- Functions of Network Interface Card (NIC)
- Repeaters
- Hub
- Switches
- Routers
- Bridges.
- Internet Service Provider

Network Devices

Functions of Network Interface Card (NIC)

- It is an electronic device that joins a computer to a computer network, usually a LAN.
- The NIC contains the electronic circuitry required to connect using a wired connection (e.g., Ethernet) or a wireless connection (e.g., WiFi).



Network Devices

Repeaters

- Repeaters receive network signals on one port, amplify them, and repeat them out the other port.
- Since they operate only at the Physical layer of the OSI model, repeaters can intersect different media types but cannot convert protocols.
- The purpose of a repeater is to extend the maximum distance of a single network segment.

Repeater Mode

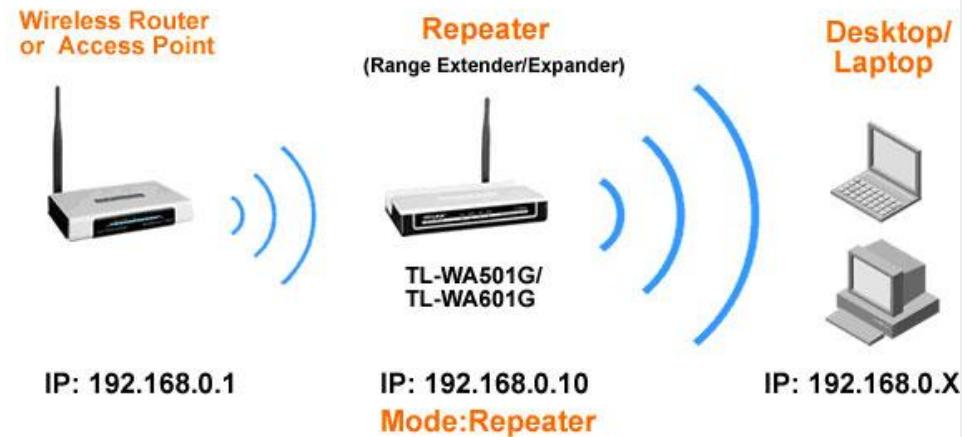


Image Source: <https://www.tp-link.com/ae/support/faq/151/>

Network Devices

Hub

- A hub (also called a concentrator) serves as a central joining point for several network devices.
- At a basic level, a hub is nothing more than a multiport repeater.
- A hub repeats what it obtains on one port to all other ports.

Active Hubs

- Need a power source
- Power added to the signal when passed though port
- Prevents weakening of signal by multiple devices being attached
- Repeats signal to all hosts connected to hub

lynda.com

Image Source:
<https://www.lynda.com/Windows-Server-tutorials/Exploring-hubs/408231/435884-4.html>

Network Devices

Types of hub

- **Active Hub** – It is usually powered and amplifies and cleans up the signal it receives, thus doubling the effective segment distance limitation for the specific topology.
- **Passive Hub** – Typically it is unpowered and makes only physical, electrical connections. Usually, the maximum segment distance of a topology is shortened because the hub takes some power away from the signal strength in order to do its job.



2. Passive Hub

- Act as connection point, not as repeater.
- Do not require electricity to run.
- Inexpensive and easy to configure.

Image Source: <https://www.slideshare.net/patelgopal1044/network-d>

Switches

What is a Switch

- Switches are key building blocks for any network.
- They can connect multiple devices such as computers , printers , access points & servers etc. on same network within a building or campus .



Image Source:

<https://www.indiamart.com/proddetail/networking-switches-dlink-and-digisol-1103-6001622.html>

Switches

Role of switches in networking

- Switching in a computer network is achieved by using switches.
- Network switches operates at layer 2 (Data Link Layer) in the OSI Model
- It is operated in a full duplex mode.



Image Source:

<https://www.indiamart.com/proddetail/networking-switches-dlink-and-digisol-1103-6221622.html>

Switches

Types of switches (Unmanaged Switches)

- These are the switches that are used in home networks and small businesses.
- They do not need to be configured as they work on home /small networks .
- They require small cabling and they are least expensive too.



Switches

Types of switches (Managed Switches)

- These are the switches used in large organizations containing a large network.
- These are costly but their scalability makes them an ideal option for a network that is going.
- They are achieved by setting a simple network management protocol(SNMP)



Switches

Types of switches (LAN Switches)

- These are also known as Ethernet switches or Data switches.
- They are used to reduce network congestion or bottleneck by distributing a package of data only to its intended recipient



Switches

Types of switches (PoE Switches)

- PoE switches are used in PoE technology which stands for Power over Ethernet.
- Technology that integrate data and power on the same cable allowing power devices to receive data in parallel to power



Image Source:

<https://www.wifi-stock.com/details/zq-poes-8-7.html/products/switches/unmanage>

Switches

Advantages of switching

- Increases the bandwidth of the network.
- Reduces the workload of individual PC as it sends the information to only that device which has been addressed.
- Increases the overall performance of the network by reducing the traffic on the network.



Image Source:

<https://www.indiamart.com/proddetail/networking-switches-dlink-and-digisol-1103-6221622.html>

Switches

Disadvantages of switching

- It is expensive as compared to network bridges.
- It cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switches are required to handle multicast packets



Image Source:

<https://www.indiamart.com/proddetail/networking-switches-dlink-and-digisol-1103-6001622.html>

Routers

What is a Router

- The Router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks.
- Some popular companies that develop routers are cisco , ibm , hp , asus , juniper d-link etc.



Routers

What is a Router

- Is used in LAN and WAN Environments.
- It shares information with other routers. in networking
- It uses the RIP(Routing Information Protocol) to transfer the data across the network.
- It is more expensive than other network devices like switches and hubs.



Routers

Features of Routers

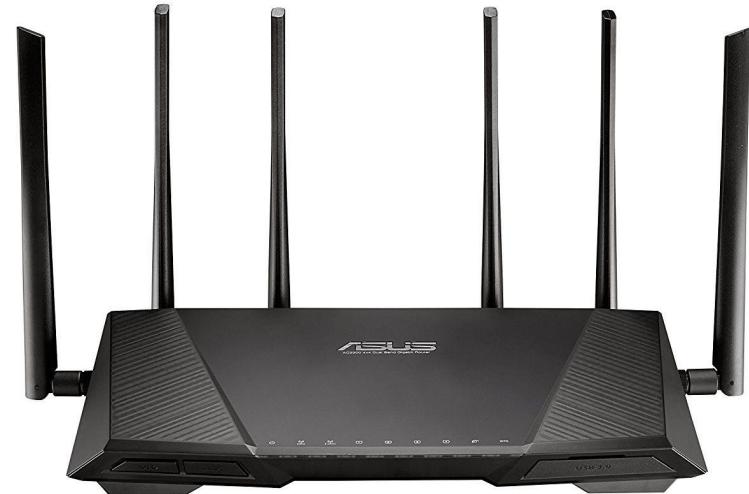
- A router works on the third layer (network layer) of OSI model
- It allows the users to connect to several LAN and WAN .
- Routers are capable of routing the traffic in a large networking system by subnetting .
- Routers provide the redundancy as it always works in master and slave mode.



Routers

Types of Routers (Wireless Router)

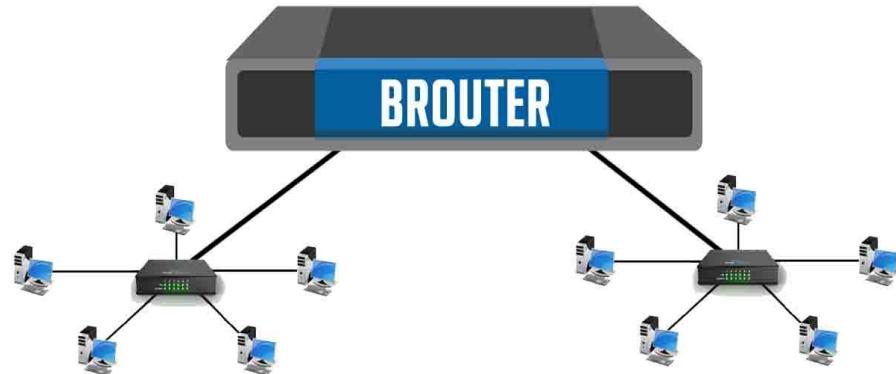
- They used to offer a wifi connectivity to laptop , smartphones and other devices.
- Wireless routers are capable of generating a wireless signal in your home or office.
- If the connection is indoors , the range of wireless router is 150 feet and when the connection is outdoors ,the range is upto 300 feet.



Routers

Types of Routers (BRouter)

- It is the combination of bridge and the router.
- It allows the transferring the data between network like a bridge and like a router , it can also route the data within the network to the individual systems.



Routers

Types of Routers (Core Router)

- It is a router that can route the data within a network, but it is not able to route the data between the networks.
- It is a computer communication system device and the backbone of networks, as it helps to link all network devices.
- It is used by Internet Service Providers (ISPs).



Carrier Routing System-X (CRS-X)

Routers

Types of Routers (Edge Router)

- An edge router is a lower-capacity device that is placed at the boundary of a network.
- It is also known as an access router.
- It allows a internal network to connect to the external network.
- It uses bgp(border gateway protocol) for communication.



Routers

Types of Routers (Broadband Router)

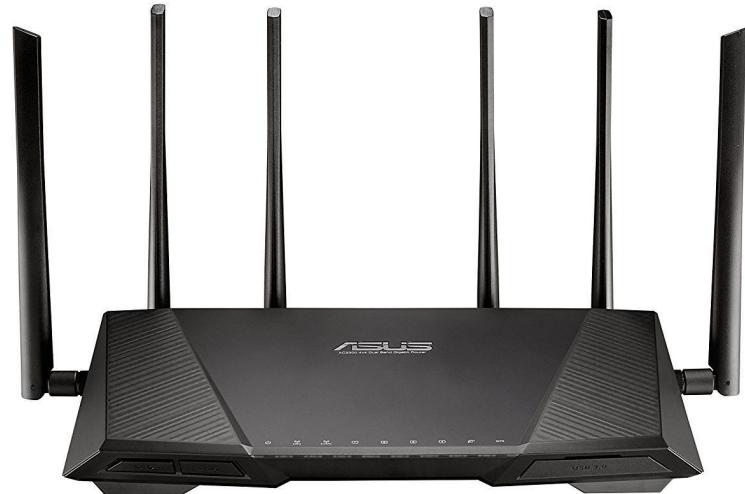
- Broadband routers are used to provide high speed internet access to computers.
- It is needed when you connect to the internet through phone and use voice over IP technology (VOIP).
- It is configured and provided by the Internet Service Provider (ISP).



Routers

Advantages of Routers

- Security
- Performance enhancement
- Reliability
- Networking Range



Routers

Disadvantages of Routers

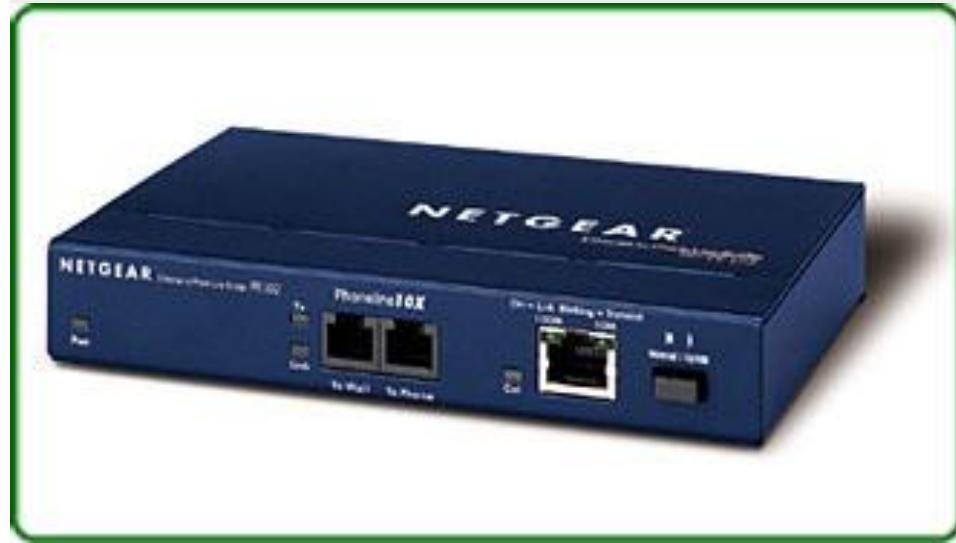
- They operate on routable network protocols.
- They are expensive.
- They are slower as they need to analyse from layer 1 through layer 3 of OSI model.



Bridges

What is bridges

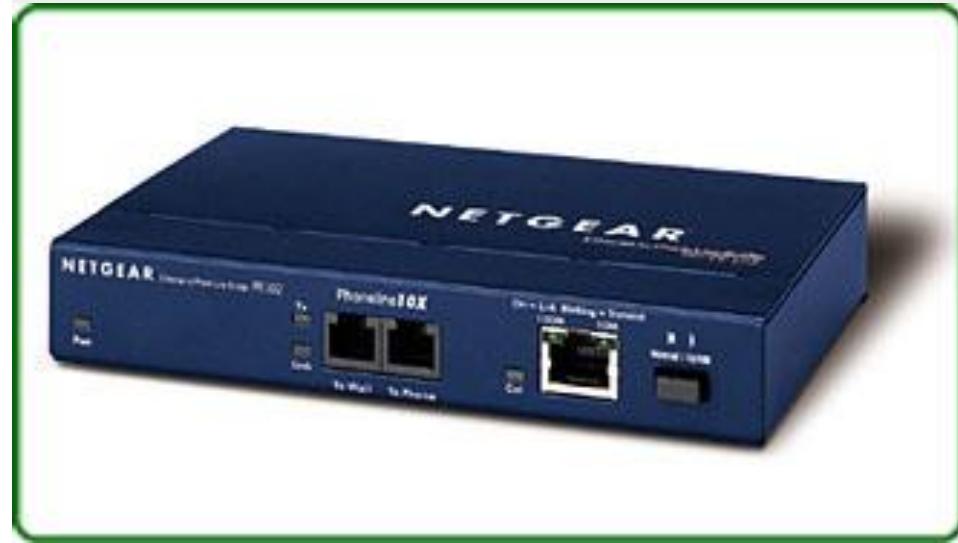
- A networking Bridge is a device that divides a network into the segments.
- Each segment represent a separate collision domain , & each collision domain has its own separate bandwidth
- A Bridge works at layer 2 (Data link layer) of the OSI Model.



Bridges

Types of bridges (Transparent Bridge)

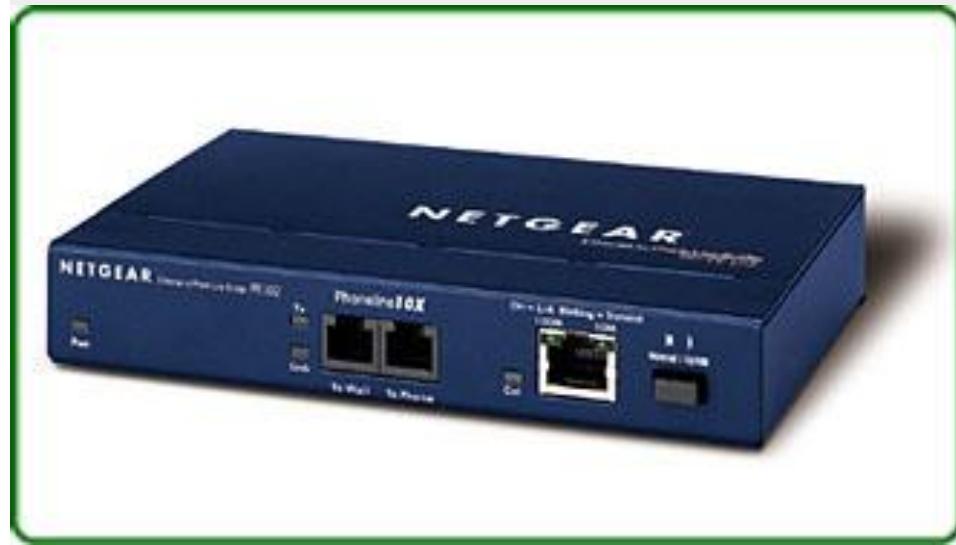
- It is an Invisible bridge in the computer network.
- The main function of this bridge is to block or forward the data depending on the MAC address.
- The other devices within the network are unaware of the existence of bridges.



Bridges

Types of bridges (Translational Bridge)

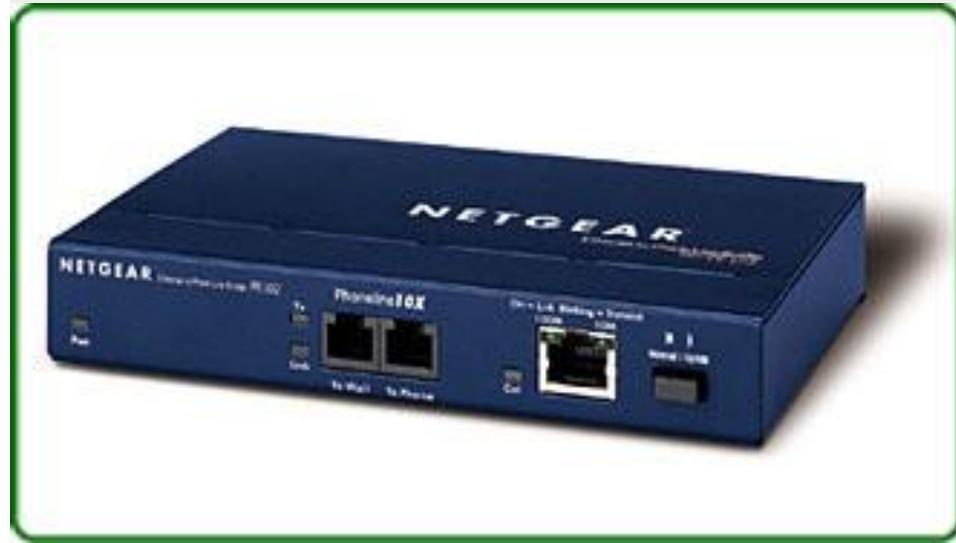
- It plays a key role in changing a networking system from one type to another.
- These bridges are used to connect two different networks like token ring and Ethernet.
- This bridge can add or remove the data based on traveling direction, and fields from the frames as needed.



Bridges

Types of bridges (Source-Route Bridge)

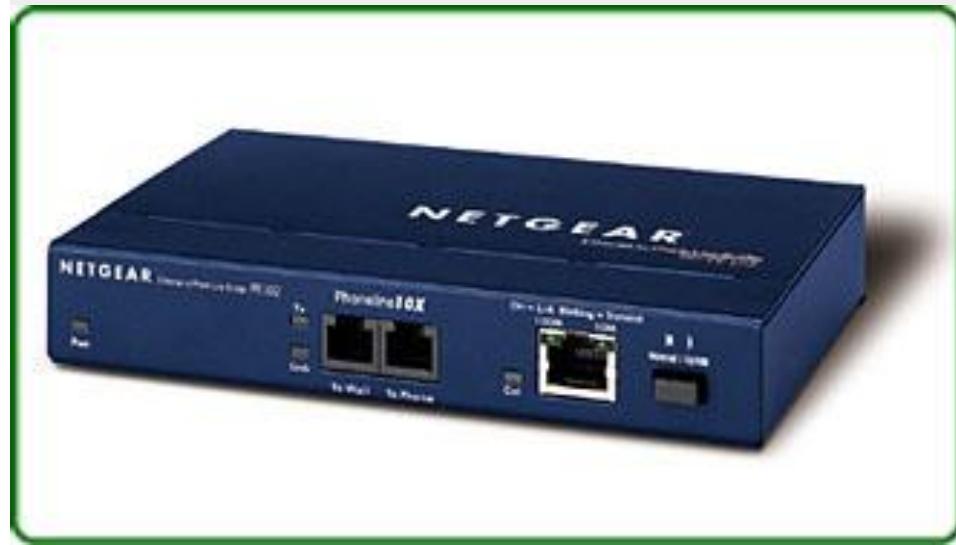
- It is a one type of technique used for token ring network and it is designed by IBM.
- The total frame route is embedded in one frame so it allow the bridge to make precise decision of how the frame is forwarding using a network.
- In this method two similar network segments are connected to data link layer.



Bridges

Functions of Bridges

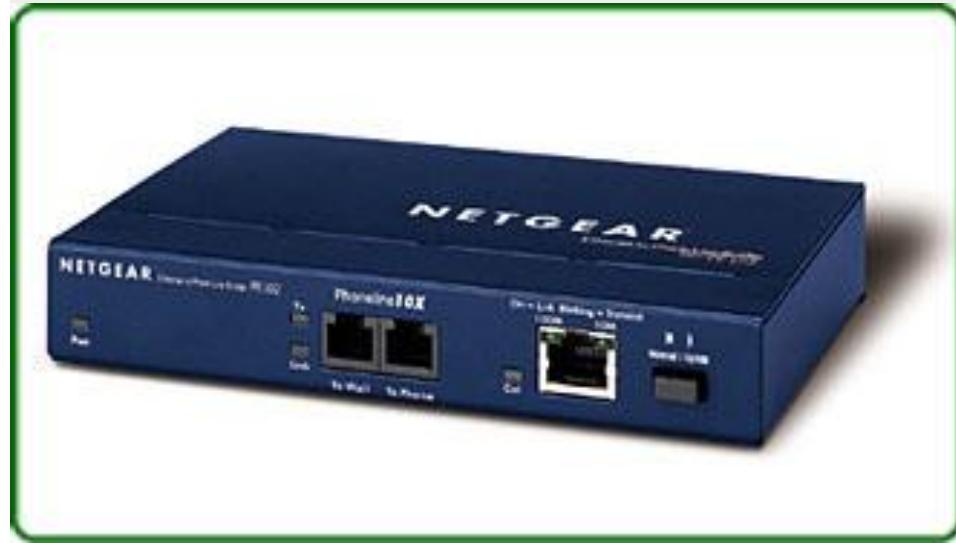
- It is used to divide the local area network into several segments.
- In the osi model it works under the data link layer
- It is used to store the address of MAC in PC used in a network.



Bridges

Advantages of Bridges

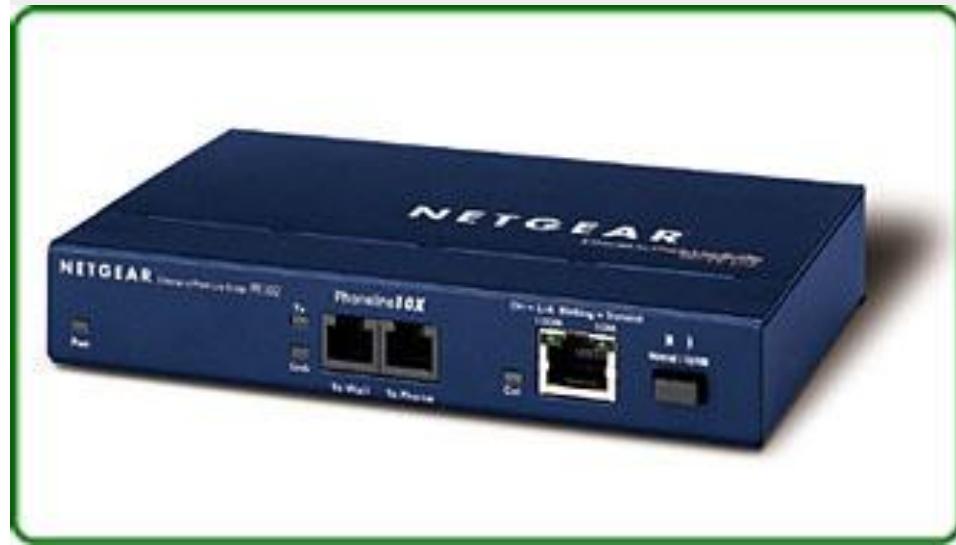
- It acts as a repeater to extend a network.
- Collisions can be reduced.
- Bridges increases the available bandwidth to individual nodes.
- It avoids waste bandwidth
- The length of the network can be increased



Bridges

Disadvantages of Bridges

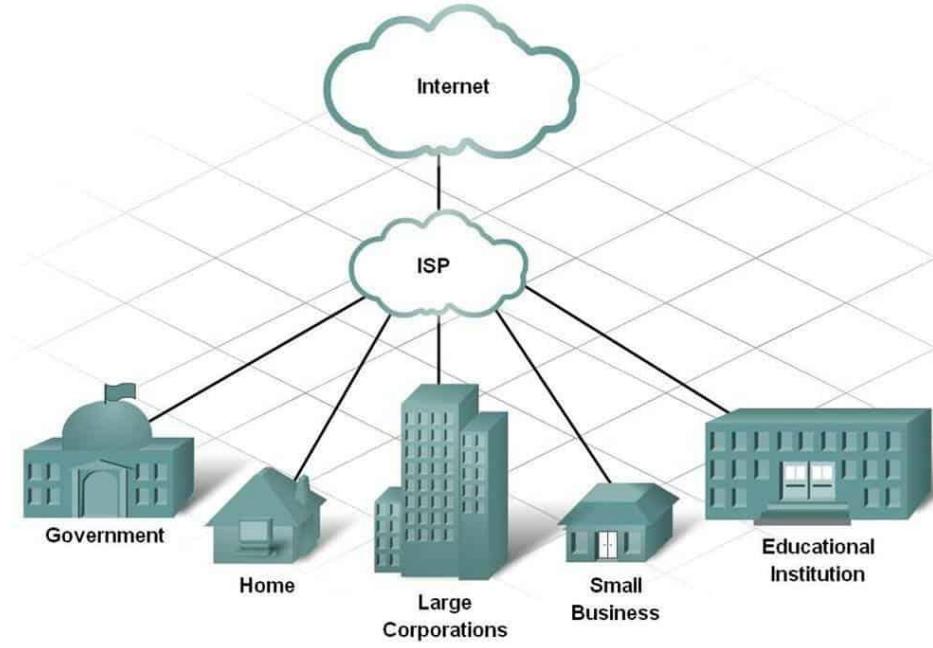
- It is unable to read specific IP address because they are more troubled with the mac address.
- They cannot help while building the network between the different architectures of network.
- It does not handle more variable and complex data load which occurs from WAN.



Internet Service Provider

What is ISP

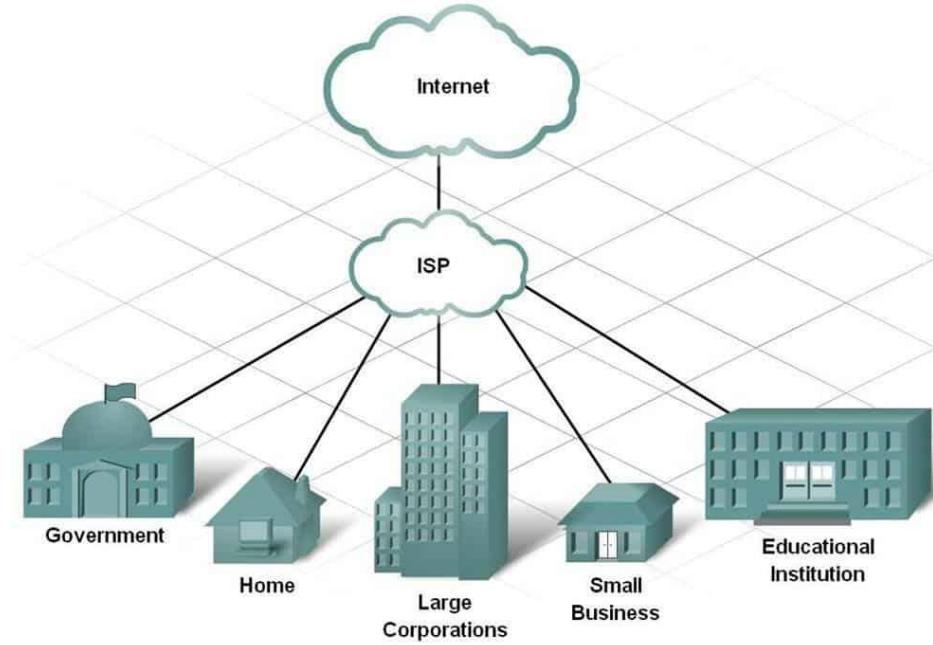
- An Internet Service Provider (ISP) is a company that provides customers with internet access.
- An Internet Service Provider (ISP) is also known as Internet Access Provider (IAP).
- ISPs also provide their customers with the ability to communicate with one another.



Internet Service Provider

Types of ISPs (Dial-up Internet Access)

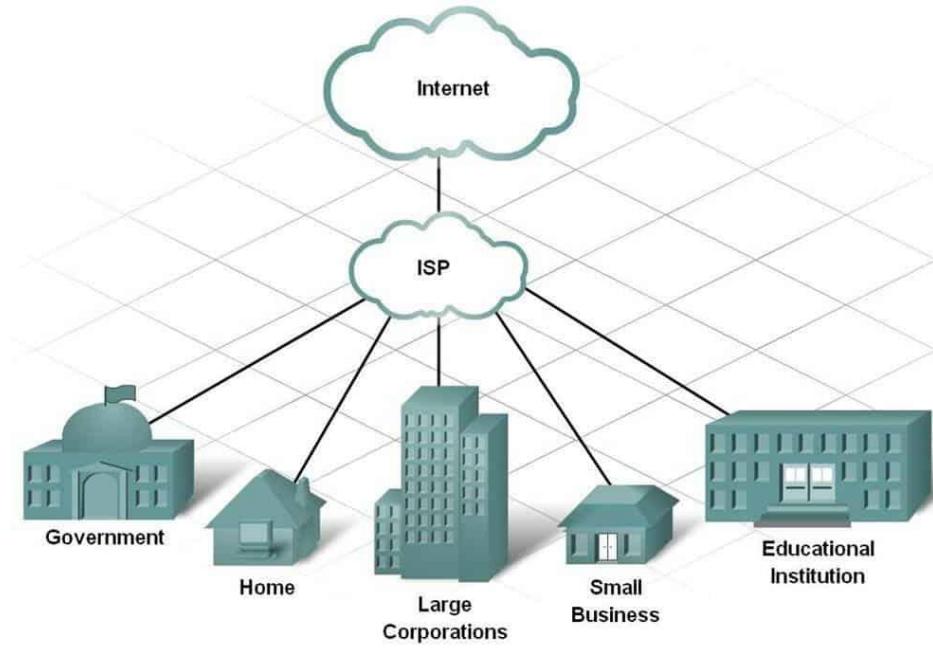
- It is the oldest technology to provide internet access by modem to modem connection using telephone lines.
- This method has become outdated today due to slow connection speed.



Internet Service Provider

Types of ISPs (DSL)

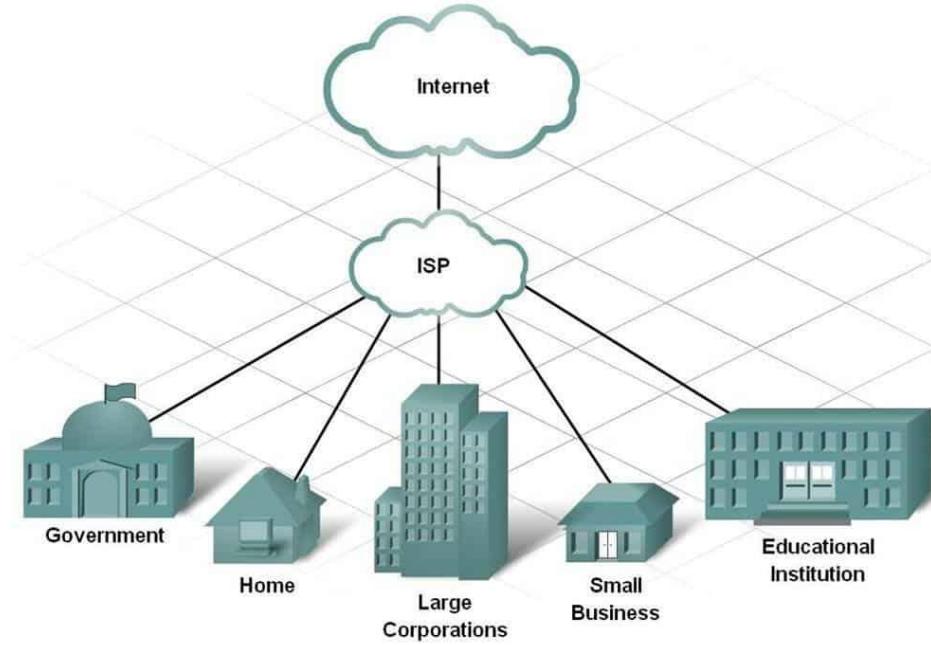
- DSL stands for 'Digital Subscriber Line' is an advanced version of Dial-up internet access method.
- This method offers Asymmetric Digital Subscriber(ADSL), where upload speed is less than download speed, and Symmetric Digital Subscriber (SDSL), where upload and download speed are equal.



Internet Service Provider

Types of ISPs (Wireless Broadband)

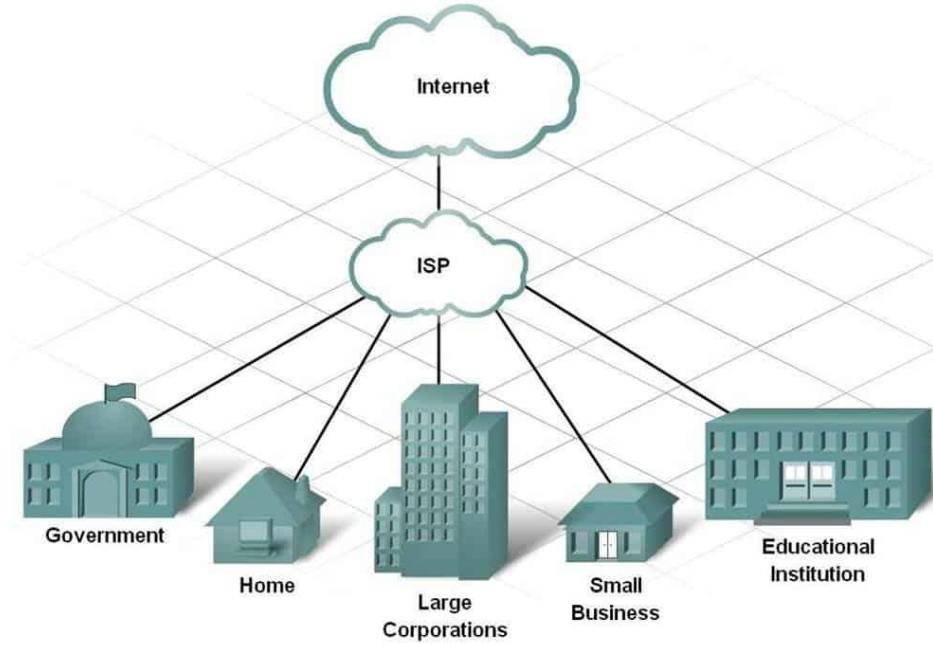
- WiBB is a modern broadband technology for internet access.
- It allows high-speed wireless internet within a large area.



Internet Service Provider

Types of ISPs (Wifi Internet)

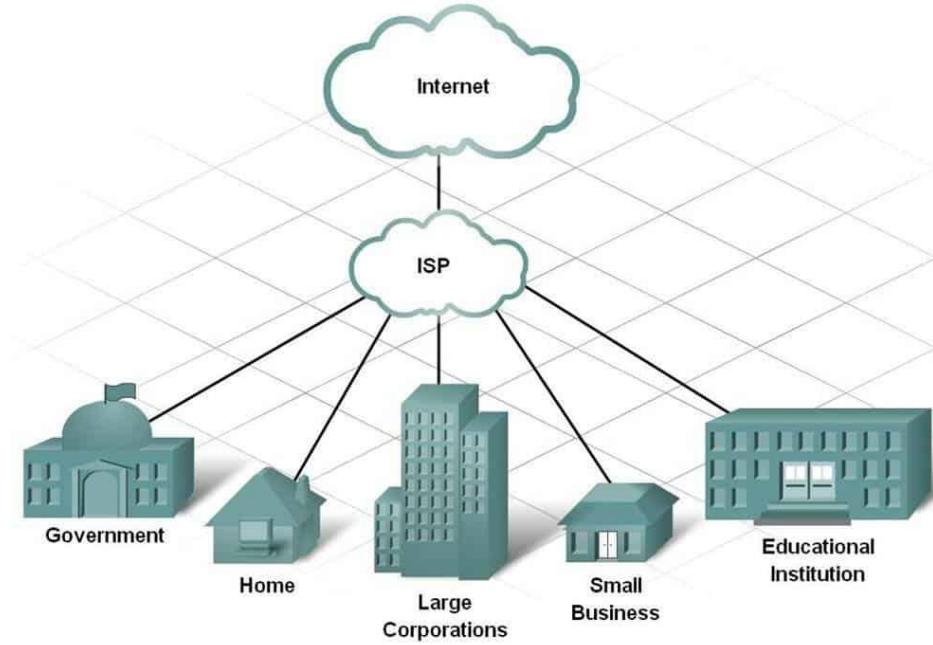
- Wifi stands for ‘Wireless fidelity’.
- It is a wireless networking technology that provides wireless high-speed internet connections using Radio waves.
- It is commonly used in public places such as hotels, airports, restaurants, etc.



Internet Service Provider

Types of ISPs (ISDN)

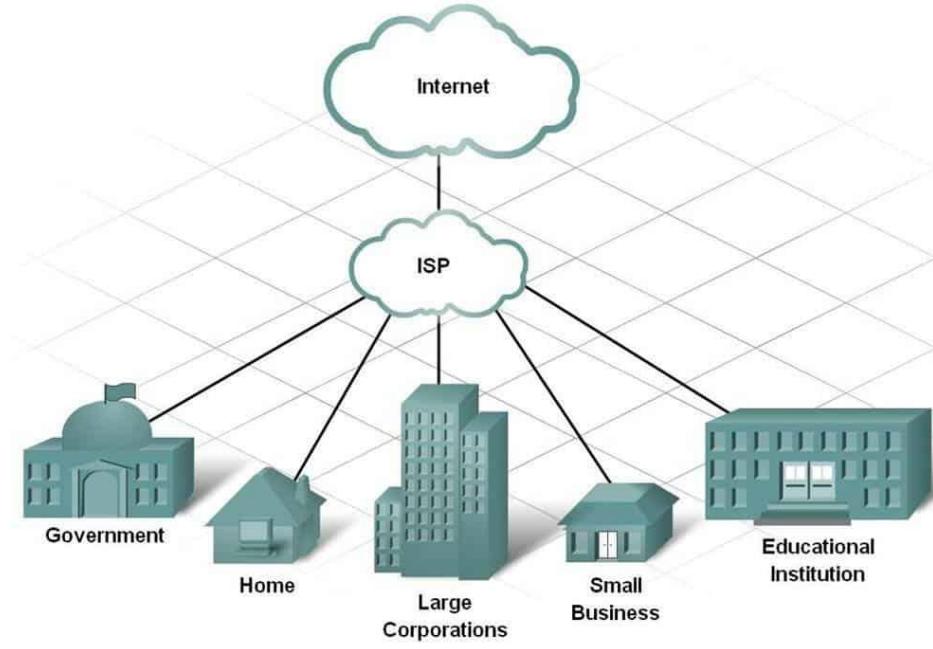
- ISDN stands for Integrated Services Digital Network.
- It is a telephone system network which integrates a high quality digital transmission of voice and data over the same standard phone line.



Internet Service Provider

Types of ISPs (Ethernet)

- It is a wired LAN (Local Area Network) where computers are connected within a primary physical space.
- It enables devices to communicate with each other via a protocol (a set of rules or common network language).
- It may provide different speed such as 10 Mbps, 100 Mbps and 10 Gbps.



Configure and manage network security

In this section, we will discuss:

- Modern Network Security
- Threats and the basics of securing a network
- Secure Administrative Access
- LAN security considerations.
- Network Security Devices.

Modern Network Security

Why Internet Security

- Cybersecurity refers to the practice of reducing cyber risk through the protection of the entire information technology (IT) infrastructure, including systems, applications, hardware, software, and data.
- It is very important in today's world.



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Modern Network Security

Importance of Cyber Security

- Cyber-attacks (Unauthorized access to your Systems)
- Data breaches (Exposure of sensitive business, customer, & supplier data)
- Identity thefts (the theft of logins, passwords, and other sensitive, personally identifiable data)



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Modern Network Security

Cyber Security Practise Areas

- Data Security
- Application Security
- Network Security
- Operational Security
- Cloud Security



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Modern Network Security

Cyber Security Practise Areas

- Identity and Access Management(IAM)
- Privileged Access Management(PAM)
- Vulnerability Management (VM)
- Enterprise Mobility Management (EMM)
- Business Continuity (BC) and Disaster Recovery (DR).



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Threats and the Basics of securing a network

Common Network Security Threats

- Computer Viruses
- DOS (Denial of service) attack
- Trojan Horse
- Adware and Spyware
- Computer Worm
- Phishing
- Rootkit
- SQL Injection attack
- Malware



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Threats and the Basics of securing a network

Cyber Security Best Practices

- Audit your existing IT ecosystem
- Complete a gap Analysis
- Used a risk based approach to cyber security
- Take the advantages of modern cyber security software
- Implement robust identity and access management



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Threats and the Basics of securing a network

Cyber Security Best Practices

- Use privileged access management
- Employ vulnerability scanning
- Use of Cyber Security Frameworks



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Threats and the Basics of securing a network

Network security Models

- Firewalls
- Antivirus Software
- Passwords
- Cryptography
- Algorithms



Threats and the Basics of securing a network

Firewalls

- A firewall is a software program or hardware that stops the hackers, viruses and worms that try to reach computer.
- It scans every message and blocks that information that does not meet the security norms.



Threats and the Basics of securing a network

Benefits of Firewalls

- Shield from Vulnerable services.
- Logging and statistics on network usage, and misuse of it.
- Policy enforcement.



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Threats and the Basics of securing a network

Authentication

- User Identification and Password.
- A signed digital certificate or even a fingerprint.
- User's voice, hand configuration, fingerprint, etc.



Threats and the Basics of securing a network

Intrusion Detection System

- Intrusion Detection System (IDS) are mainly concentrated on recognizing possible occurrences, logging information and reporting attempts.



Threats and the Basics of securing a network

Antivirus software

- Antivirus software is a program or set of programs that are designed to prevent, search for, detect and remove software viruses and other malicious software like worms, trojans, adware, etc.



Threats and the Basics of securing a network

Benefits of Antivirus software

- Scan specific files or directories.
- Allows to schedule scans to automatically run for you.
- Allows you to initiate scan of a particular file or entire computer or of a CD or flash drive at any time.
- Removes any malicious code detected.
- Show you the 'health' of your computer.



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Threats and the Basics of securing a network

Some popular Antivirus software

- Norton
- Kaspersky
- McAfee
- BullGuard
- Avast Antivirus
- Panda Cloud Antivirus
- Quick Heal Antivirus
- AVG



Threats and the Basics of securing a network

Cryptography

- The term cryptography means the concept of encryption and decryption together.
- Cryptography is the method in which plain text message is encoded that is called ciphertext at the transmitters end, which is then conveyed to the receiver. The receiver then decrypts to get the original message back.



Threats and the Basics of securing a network

Techniques of Cryptography

- Symmetric Key Cryptography : In this the significant component used is equal for both encoding and decoding.
- Asymmetric Key Cryptography : In this the key element used is unlike for both encryption as well as decryption.



Threats and the Basics of securing a network

Some Populars Encryption Algorithms

- Triple DES
- RSA
- Blowfish
- Twofish
- AES



Image Source:

<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Secure Administrative Access

Techniques for secure administrative access

- Setting User modes passwords
- Setting Privilege mode passwords
- Encryption Passwords in config files
- Setting access privilege levels
- Restrict telnet to the Device



Secure Administrative Access

Techniques for secure administrative access

- Restrict web browser access to the Device.
- Restrict SNMP access to the Device.



Secure Administrative Access

User Mode Passwords

- **Console (con) port** Access for the console cable. Figure shows a typical console port on a router.
- **Auxiliary (AUX) port** A console-like access that can be attached to an external modem for a dial-up connection.

```
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
!
line con 0 ???????<-Console connection
login
line aux 0 ???????<-AUX connection
login
line vty 0 4 ??????<-Virtual terminal connections
login
end
```

Secure Administrative Access

User Mode Passwords

- **Virtual terminal (vty) ports** The access points for Telnet sessions.

```
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
!
line con 0 ???????<-Console connection
login
line aux 0 ???????<-AUX connection
login
line vty 0 4 ??????<-Virtual terminal connections
login
end
```

Secure Administrative Access

Privilege Mode Passwords

- **1** User exec mode only (prompt is `router>`), the default level for login
- **15** Privileged exec mode (prompt is `router#`), the Enable mode
- **0** Seldom used, but includes five commands: `disable`, `enable`, `exit`, `help`, and `logout`

<code>mode</code>	Indicates the configuration level being assigned. This includes all router configuration modes, including exec, configure, and interface.
<code>level</code>	Indicates the level being defined.
<code>command</code>	Indicates the command to be included. If you specify exec mode, then the command must be an <code>exec mode</code> command.
<code>reset</code>	Resets the privilege level of the command to the default privilege level.

Secure Administrative Access

Privilege Mode Passwords

- The Syntax is

```
privilege mode {level /level command  
| reset command}
```

```
Rtr1(config)#privilege exec level 7 ping  
Rtr1(config)#privilege exec level 7 show startup-config  
Rtr1(config)#privilege exec level 7 show ip route  
Rtr1(config)#privilege exec level 7 show ip int brief  
Rtr1(config)#enable secret level 7 tEST7
```

LAN Security Considerations.

Understand Types of Network Devices

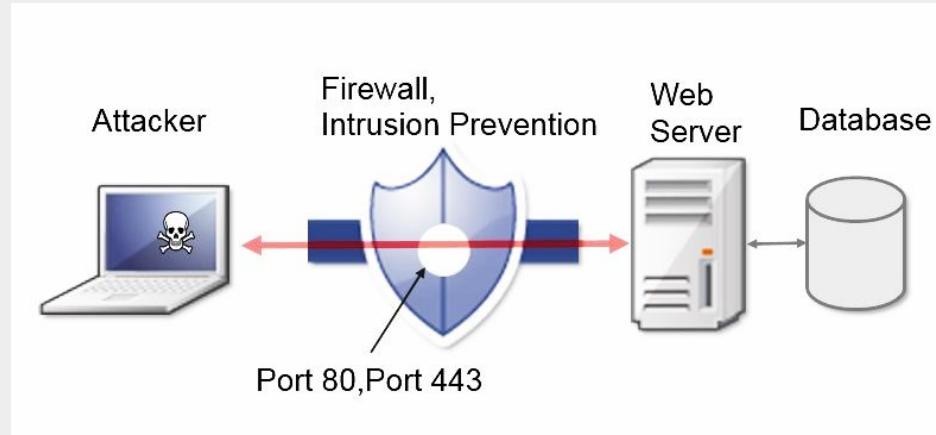
- To build a strong network and defend it, you need to understand the devices that comprise it. Here are the main types of network devices; viz. Hub, Switch, Router, Gateway



LAN Security Considerations.

Know Network Defenses

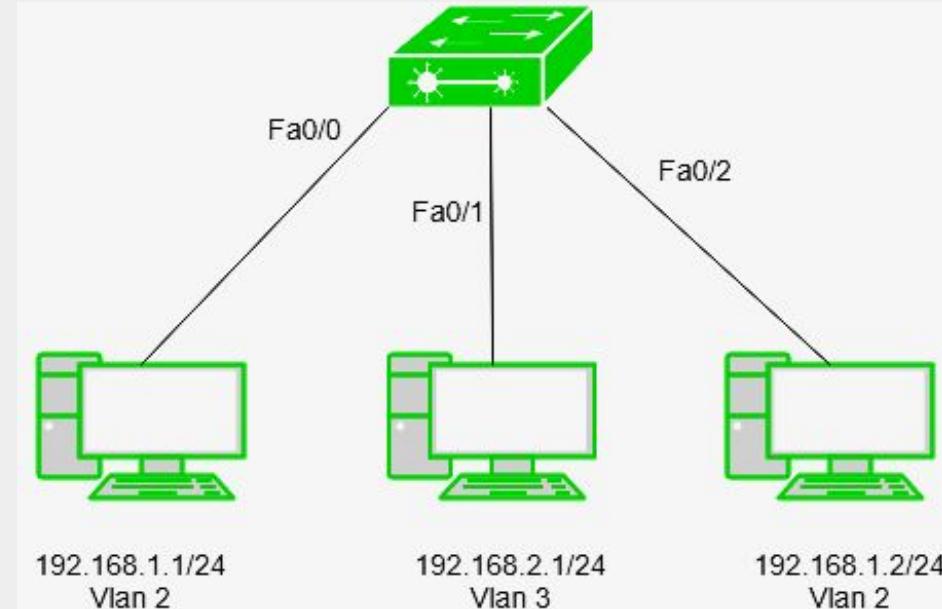
- Using the proper devices and solutions can help you defend your network. Here are the most common ones you should know about; Firewall, IDS, IPS, NAC, Web Filters, Load Balancers, Proxy Server, Anti DDoS, Spam Filter



LAN Security Considerations.

Segregate Your Network

- Network segmentation involves segregating the network into logical or functional units called zones.
- You can separate them using routers or switches or using virtual local area networks (VLANs), which you create by configuring a set of ports on a switch to behave like a separate network.



LAN Security Considerations.

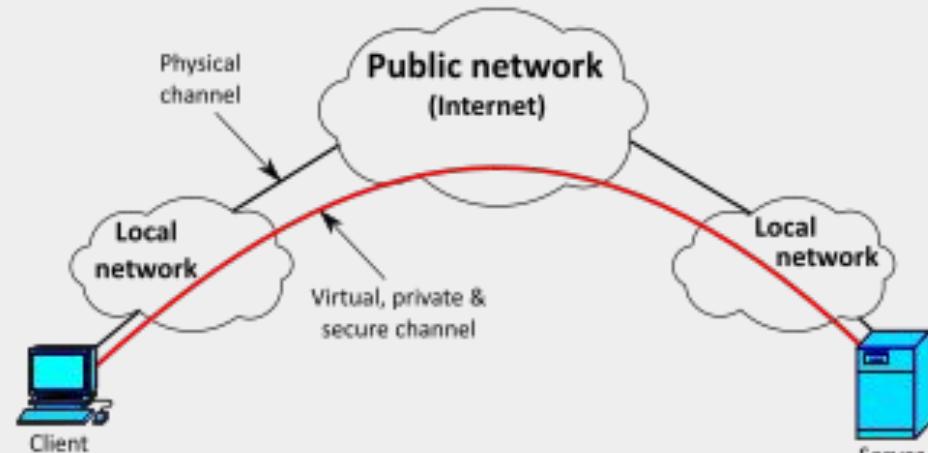
Segregate Your Network (Continue)

- Segmentation is also useful in data classification and data protection.
- Virtualization is another way to segment a network.
- Segmentation limits the potential damage of a compromise to whatever is in that one zone.

LAN Security Considerations.

Segregate Your Network (Continue)

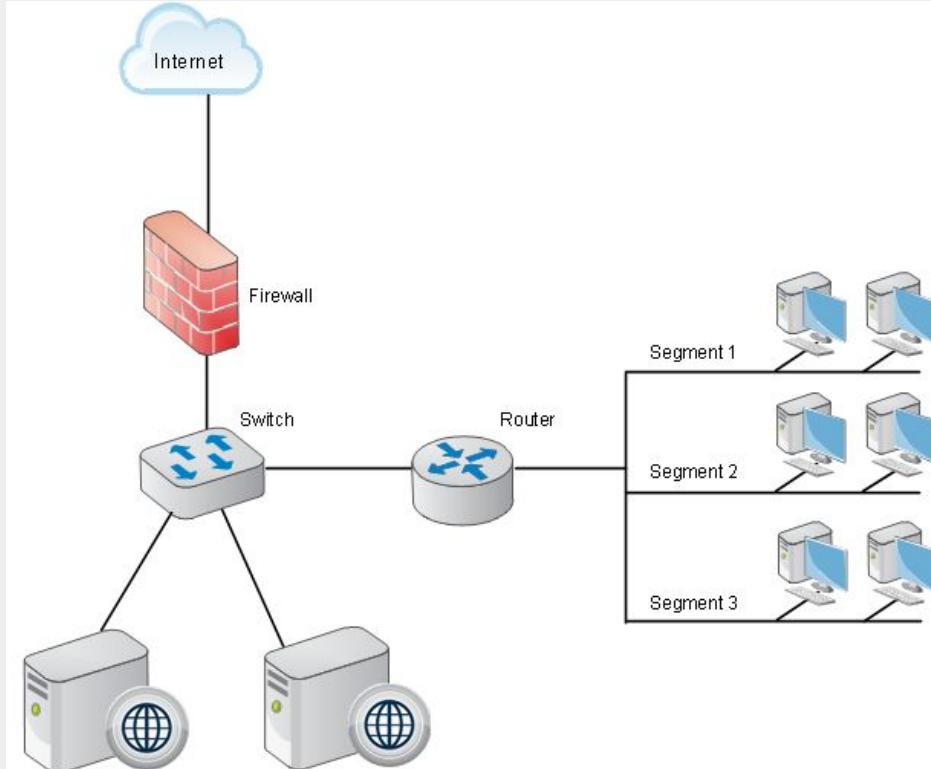
- Types of Network Segments:
 - Public Networks
 - Semi-private Networks
 - Private Networks
 - Demilitarized Zone (DMZ)
 - Software-Defined Networking (SDN)



LAN Security Considerations.

Place Your Security Devices Correctly

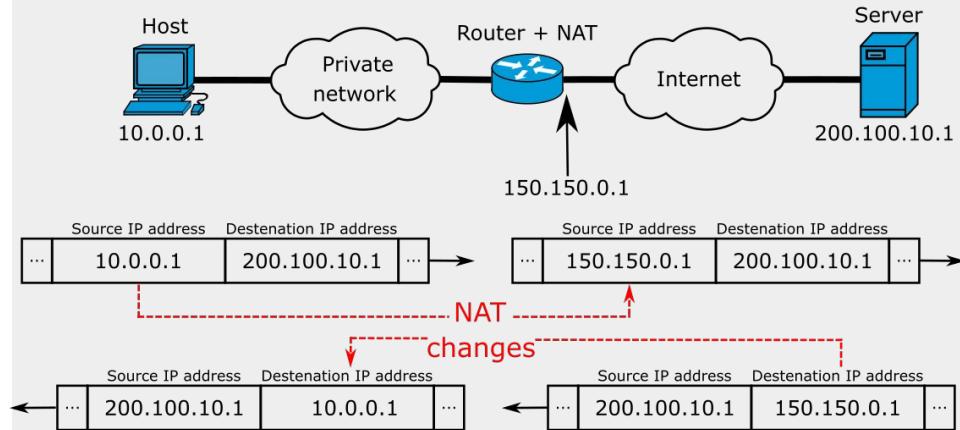
- As you design your network segregation strategy, you need to determine where to place all your devices
- To determine where to place other devices, you need to consider the rest of your network configuration



LAN Security Considerations.

Use Network Address Translation

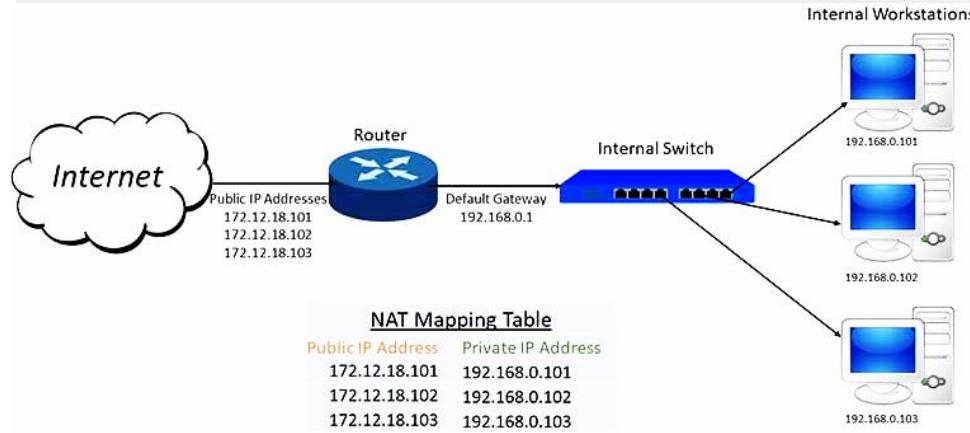
- Network address translation (NAT) enables organizations to compensate for the address deficiency of IPv4 networking.
- NAT translates private addresses (internal to a particular organization) into routable addresses on public networks such as the internet.



LAN Security Considerations.

Use Network Address Translation (Continue)

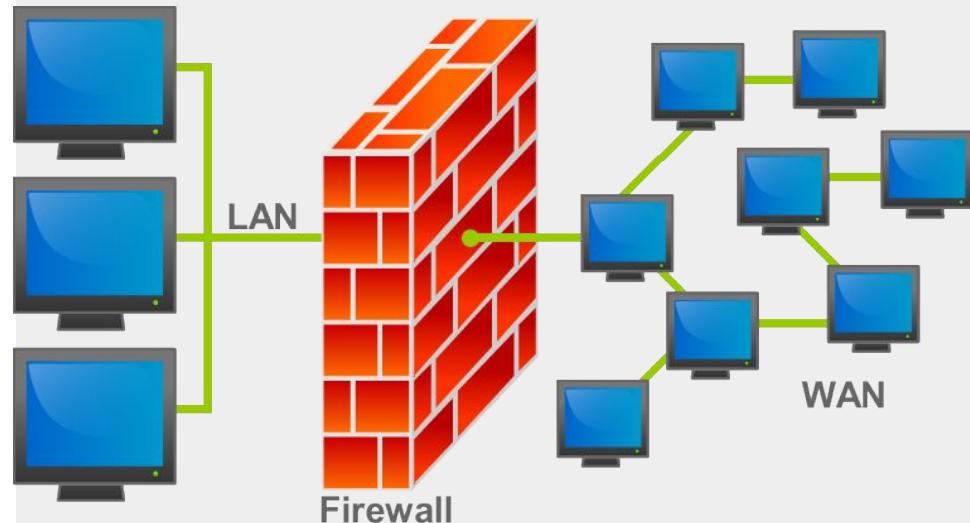
- In particular, NAT is a method of connecting multiple computers to the internet (or any other IP network) using one IP address.
- NAT complements firewalls to provide an extra measure of security for an organization's internal network



LAN Security Considerations.

Don't Disable Personal Firewalls

- Personal firewalls are software-based firewalls installed on each computer in the network. They work in much the same way as larger border firewalls
- Instead of disabling personal firewalls, simply configure a standard personal firewall according to your organization's needs



LAN Security Considerations.

Use Centralized Logging and Immediate Log Analysis

- Record suspicious logins and other computer events and look for anomalies
- This helps you reconstruct what happened during an attack
- You can take steps to improve your threat detection process and quickly block attacks in the future

Time	DoS Mode	DoS Source	Virtual Server	Event	Type	Action	Attack ID
2016-06-13 18:14:37	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:36	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:35	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:34	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:33	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:32	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:31	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:30	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:29	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:28	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:27	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:26	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:25	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Allow	3510932495
2016-06-13 18:14:24	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Drop	3510932495
2016-06-13 18:14:22	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Drop	3510932495
2016-06-13 18:14:21	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Drop	3510932495
2016-06-13 18:14:20	Enforced	Aggregate	/Common\span-virtual-all	Attack Sampled	UDP flood	Drop	3510932495

LAN Security Considerations.

Use Web Domain Whitelisting

- Limiting users to browsing only the websites you've explicitly approved helps in two ways
 - First, it limits your attack surface
 - Second, whitelisting limits hackers' options for communication after they compromise a system

Blacklisting



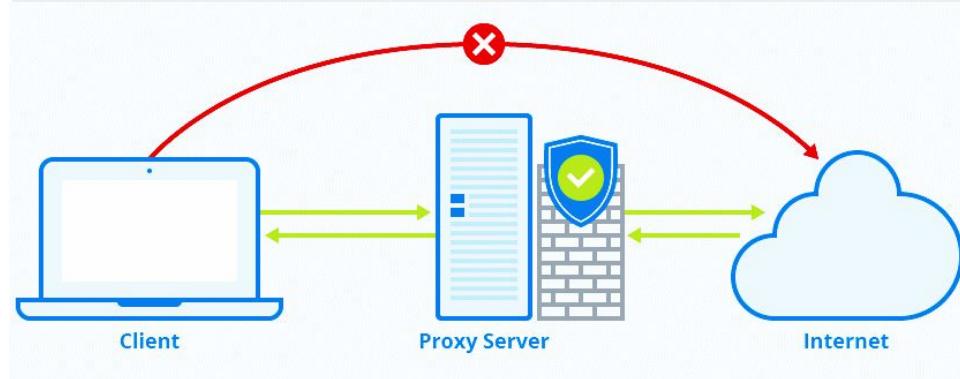
Whitelisting



LAN Security Considerations.

Route Through a Proxy Server

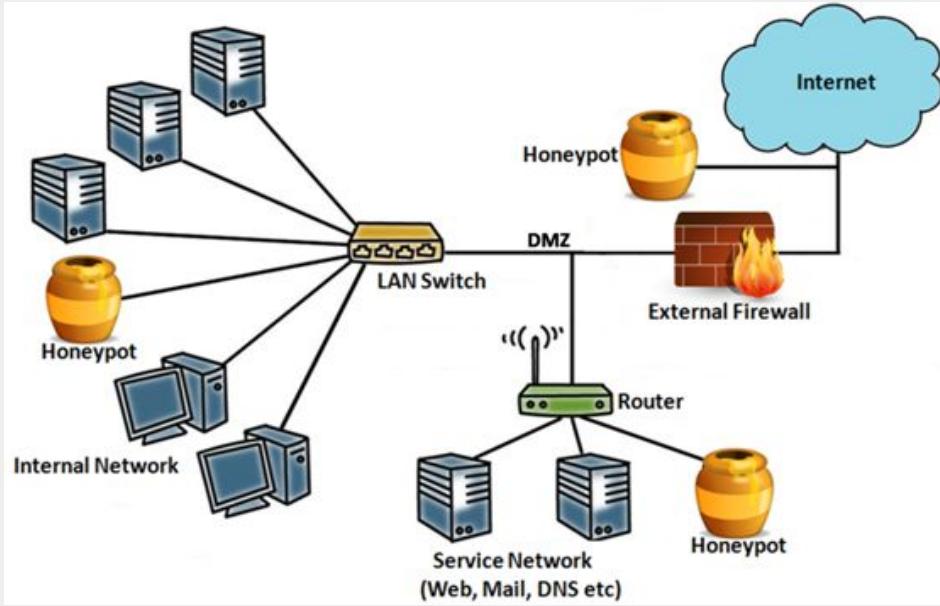
- All outbound web access should be routed through an authenticating server where access can be controlled and monitored
- Using a web proxy helps ensure that an actual person, not an unknown program, is driving the outbound connection



LAN Security Considerations.

Use Honeypots and Honeynets

- A Honeypot is a separate system that appears to be an attractive target but is in reality a trap for attackers
- A Honeynet is the next logical extension of a honeypot — it is a fake network segment that appears to be a very enticing target



LAN Security Considerations.

Protect Your Network from Insider Threats

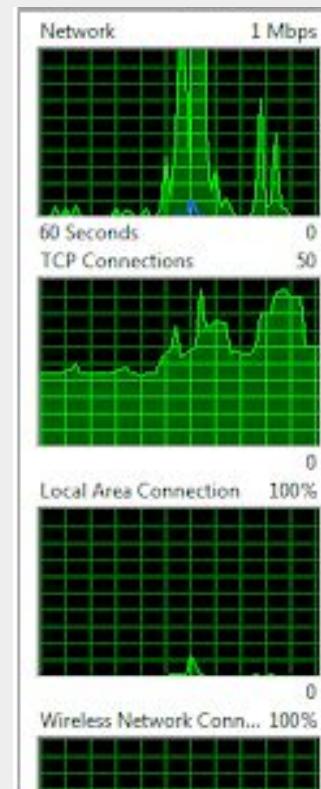
- To deal with insider threats, you need both prevention and detection strategies
- The most important preventive measure is to establish and enforce the least-privilege principle for access management and access control



LAN Security Considerations.

Monitor and Baseline Network Protocols

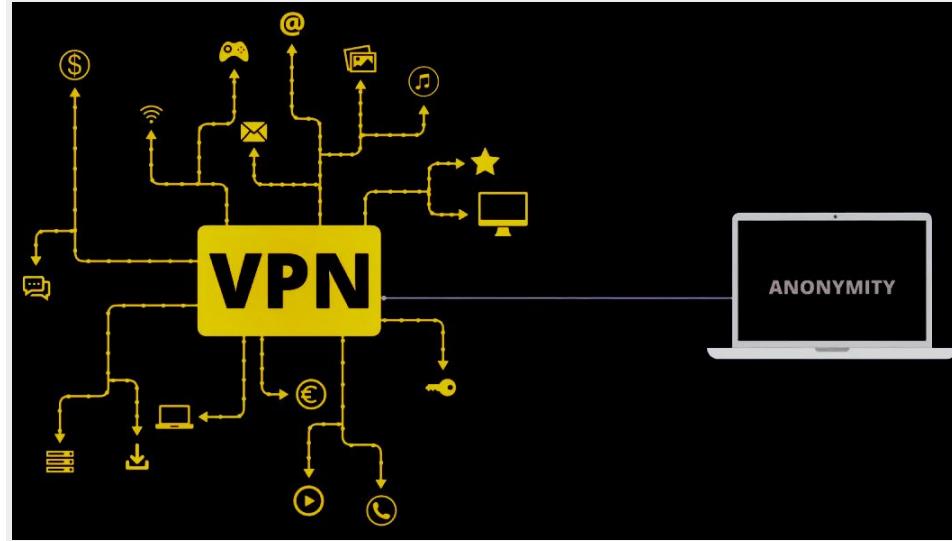
- You should monitor the use of different protocol types on your network to establish baselines both the organization level and a user level



LAN Security Considerations.

Use VPNs

- A virtual private network (VPN) is a secure private network connection across a public network
- With a VPN, the remote end appears to be connected to the network as if it were connected locally
- To improve security, VPNs usually encrypt data



LAN Security Considerations.

Use Multiple Vendors

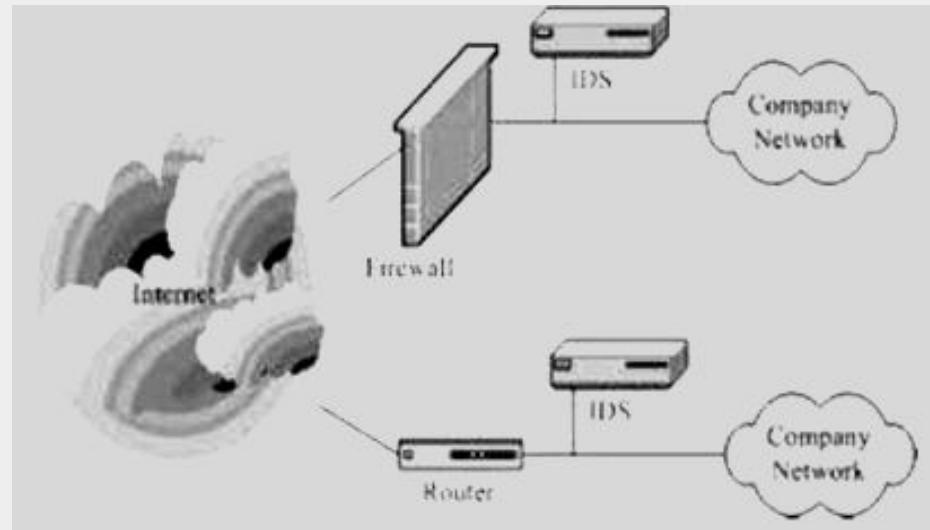
- In addition to diversity of controls, you should strive for diversity of vendors
- Each vendor uses the same malware detection algorithms in all its products, if your workstation, network and firewall antimalware solutions all come from vendor A, then anything missed by one product will be missed by all others



LAN Security Considerations.

Use Your Intrusion Detection System Properly

- To get the most value from your IDS, take advantage of both ways it can detect potentially malicious activities
 - Anomaly Detection
 - Misuse Detection



LAN Security Considerations.

Automate Response to Attacks

- Many network devices and software solutions can be configured to automatically take action when an alarm is triggered, which dramatically reduces response time.



LAN Security Considerations.

Automate Response to Attacks (Continue)

- Suggested Actions:
 - Block IP
 - Terminate Connection
 - Collect additional information
 - Look for the point of initial access
 - Determine how malicious software was deployed



LAN Security Considerations.

Physically Secure Your Network Equipment

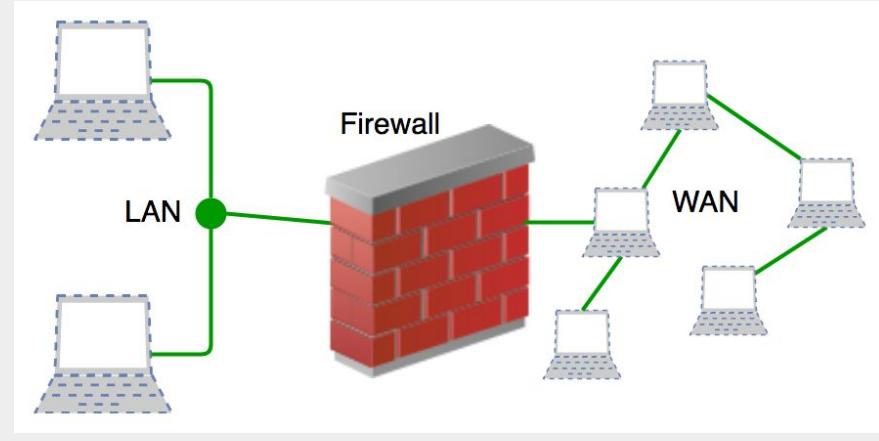
- Physical controls should be established and security personnel should ensure that equipment and data do not leave the building.
- Moreover, direct access to network equipment should be prohibited for unauthorized personnel.



Network Security Devices

Firewall

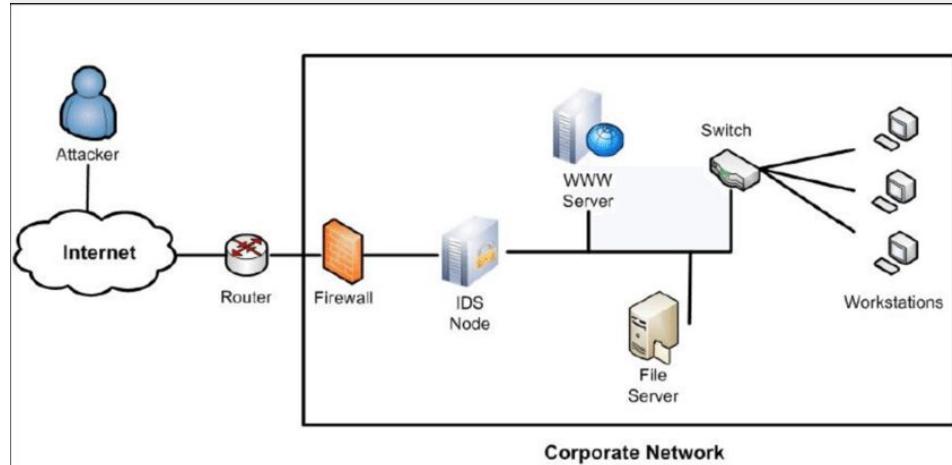
- One of the first lines of defense in a network
- A firewall isolates one network from another.
- Firewalls either can be standalone systems or included in other devices
- You can find both hardware and software firewall solutions



Network Security Devices

Intrusion Detection System (IDS)

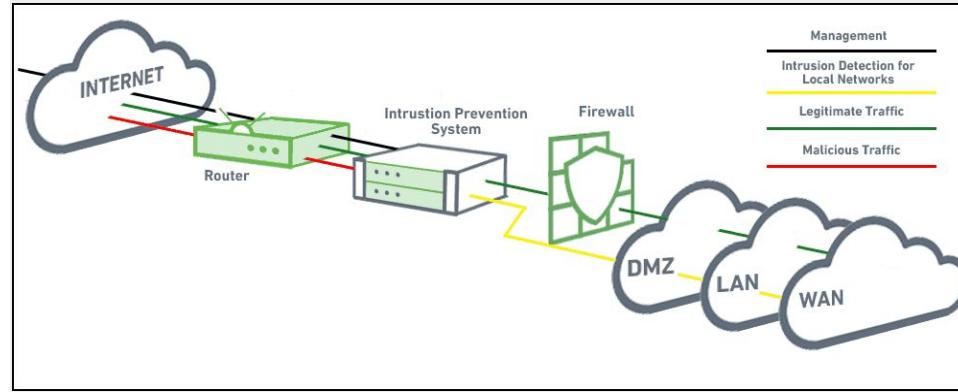
- An IDS enhances cybersecurity by spotting a hacker or malicious software on a network so you can remove it promptly to prevent a breach or other problems
- Use the data logged about the event to better defend against similar intrusion incidents in the future



Network Security Devices

Intrusion prevention system (IPS)

- An IPS is a network security solution that can not only detect intruders, but also prevent them from successfully launching any known attack.
- Intrusion prevention systems combine the abilities of firewalls and intrusion detection systems



Network Security Devices

Network Access Control (NAC)

- Involves restricting the availability of network resources to endpoint devices that comply with your security policy
- NAC is most useful when the user environment is fairly static and can be rigidly controlled



Network Security Devices

Web Filters

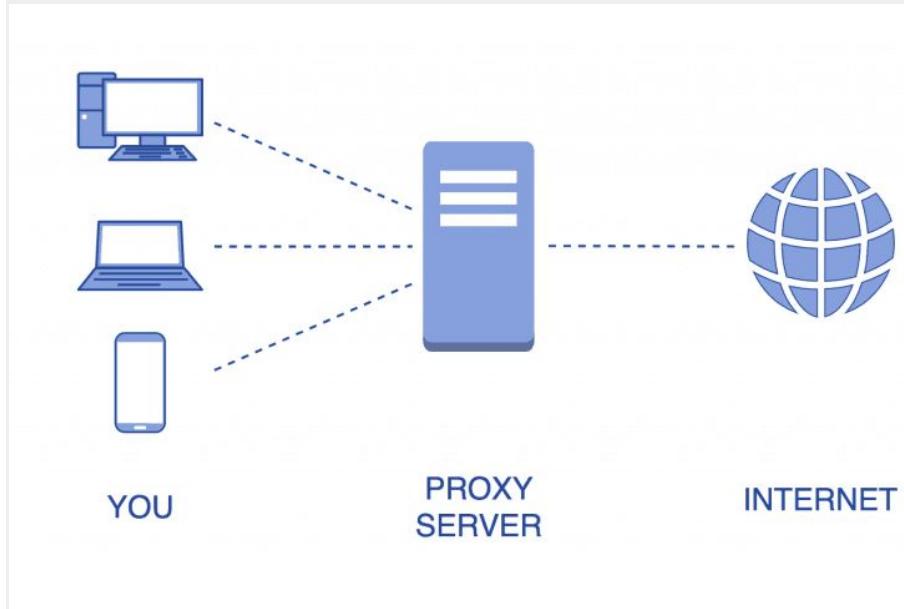
- Web filters are solutions that prevent user browser from loading certain pages from particular websites.
- There are different web filters designed for individual, family, institutional and enterprise use



Network Security Devices

Proxy Server

- Proxy servers act as negotiators for requests from client software seeking resources from other servers.
- A client connects to the proxy server, requesting some service (for example, a website); the proxy server evaluates the request and then allows or denies it.
- In organizations, proxy servers are usually used for traffic filtering and performance improvement



Network Security Devices

Anti-DDoS Devices

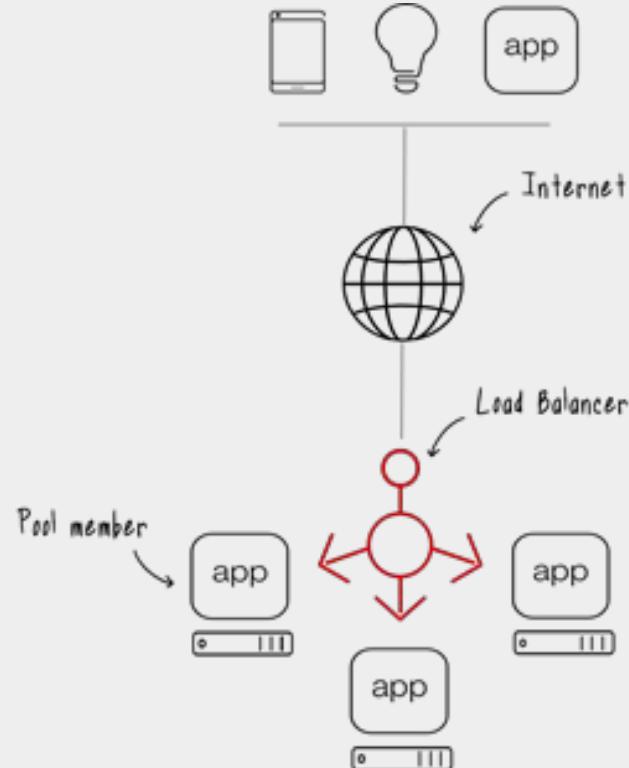
- Anti-DDoS devices detect distributed denial of service (DDoS) attacks in their early stages, absorb the volume of traffic and identify the source of the attack.



Network Security Devices

Load Balancers

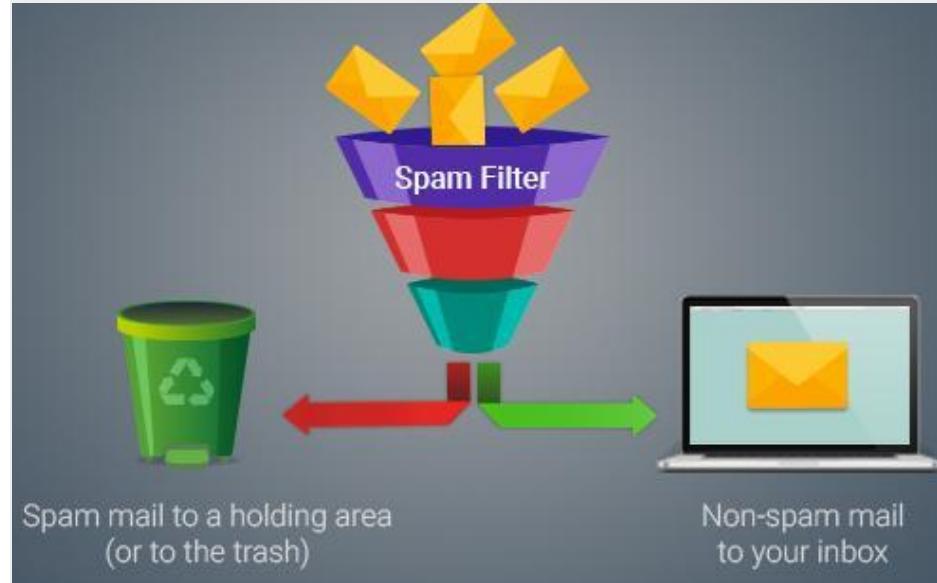
- Load balancers are physical units that direct computers to individual servers in a network based on factors such as server processor utilization, number of connections to a server or overall server performance



Network Security Devices

Spam Filter

- Spam filters detect unwanted email and prevent it from getting to a user's mailbox. Spam filters judge emails based on policies or patterns designed by an organization or vendor



Able to Configure and
Perform Remote Accessing
& Routing

In this section, we will discuss:

- Overview of Remote Access
- VPN Concepts.
- Remote Access Authentication Protocol
- TCP/IP Routing

Overview of Remote Access

Introduction

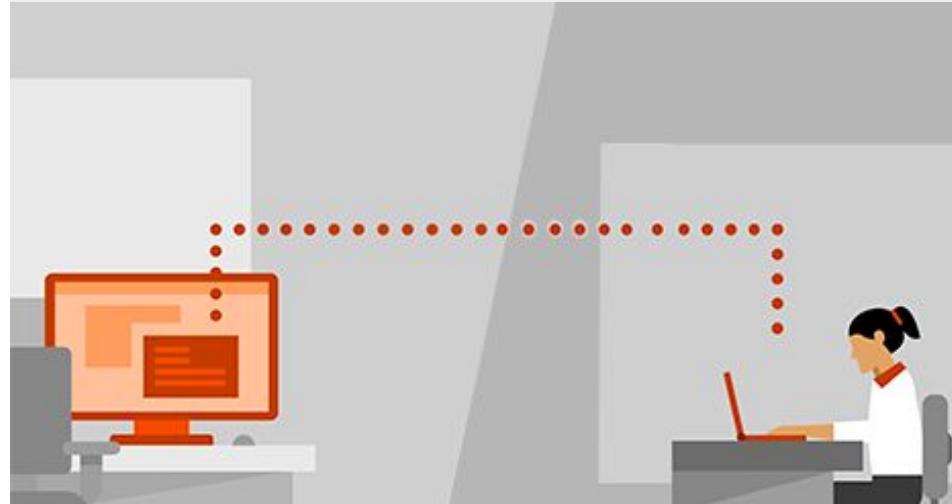
- Remote access is the ability for an authorized person to access a computer or a network from a geographical distance through a network connection.
- Remote access enables users to connect to the systems they need when they are physically far away.



Overview of Remote Access

Introduction (Continue)

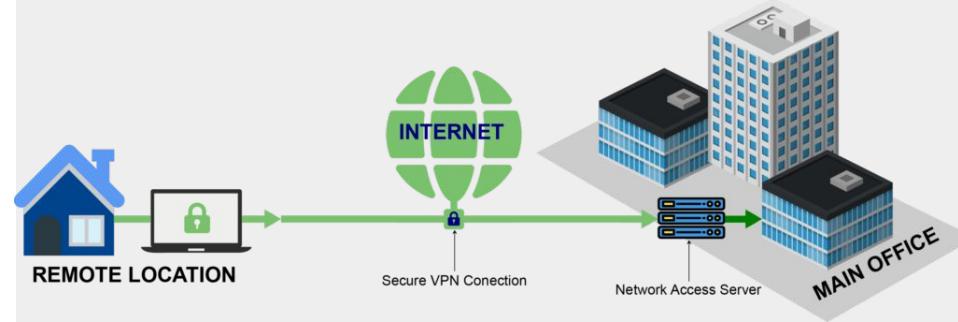
- Remote access enables remote users to access files and other system resources on any devices or servers that are connected to the network at any time.
- Increases employee productivity and enabling them to better collaborate with colleagues around the world.



Overview of Remote Access

Introduction (Continue)

- One common method of providing remote access is via a remote access VPN connection.
- A VPN creates a safe and encrypted connection over a less secure network, such as the internet.



Overview of Remote Access

How Remote Access Works

- Remote access is usually accomplished with a combination of software, hardware and network connectivity.
- Remote access VPNs are used to connect individual users to private networks.
- With a remote access VPN, each user needs a VPN client capable of connecting to the private network's VPN server.



Overview of Remote Access

How Remote Access Works (Continue)

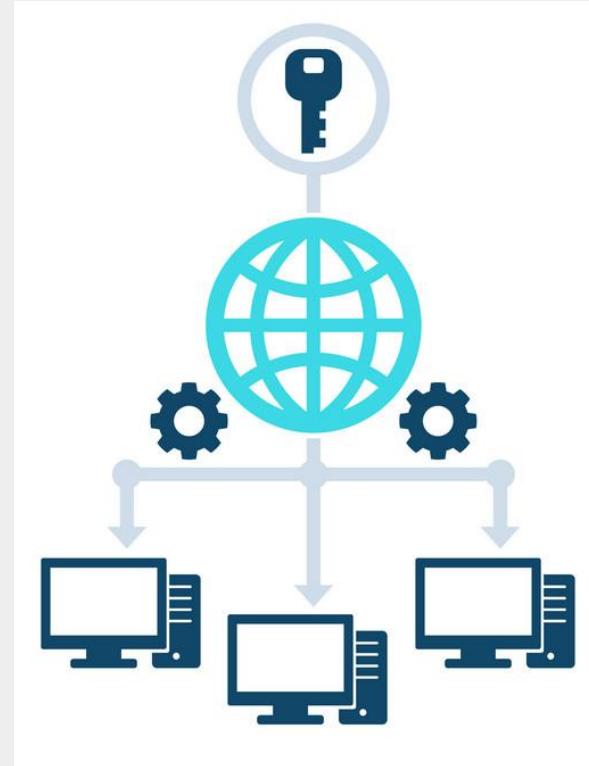
- When a user is connected to the network via a VPN client, the software encrypts the traffic before it delivers it over the internet.
- The VPN server, or gateway, is located at the edge of the targeted network and decrypts the data and sends it to the appropriate host inside the private network.



Overview of Remote Access

How Remote Access Works (Continue)

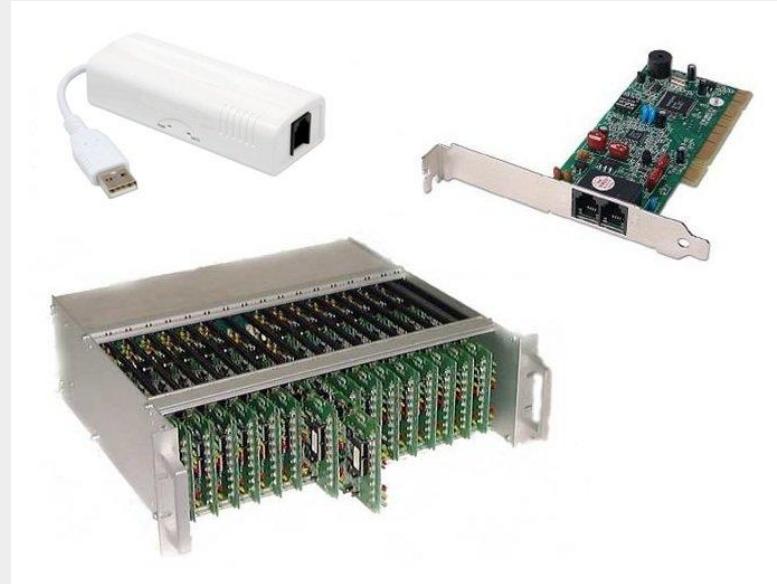
- In addition, organizations can use multifactor authentication to verify a user's identity by combining multiple credentials unique to one person.



Overview of Remote Access

Types of Remote Access

- Traditionally, enterprises use modems and dial-up technologies to allow employees to connect to office networks via telephone networks connected to remote access servers.



Dial Up Modem Technology

Overview of Remote Access

Types of Remote Access (Continue)

- Broadband provides remote users with high-speed connection options to business networks and to the internet.
- There are several types of broadband, including Cellular Internet, DSL, Cable Broadband, Satellite internet, Fiber Optics broadband



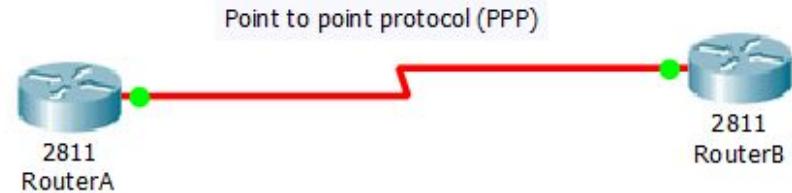
<https://internet-access-guide.com/wp-content/uploads/2011/08/Use-Type-Of-Mobile-Broadband-Routers.jpg>

<https://fios.verizon.com/beacon/wp-content/uploads/2016/06/Broadband-Modem-Back-805x330.jpg>

Overview of Remote Access

Remote Access Protocols

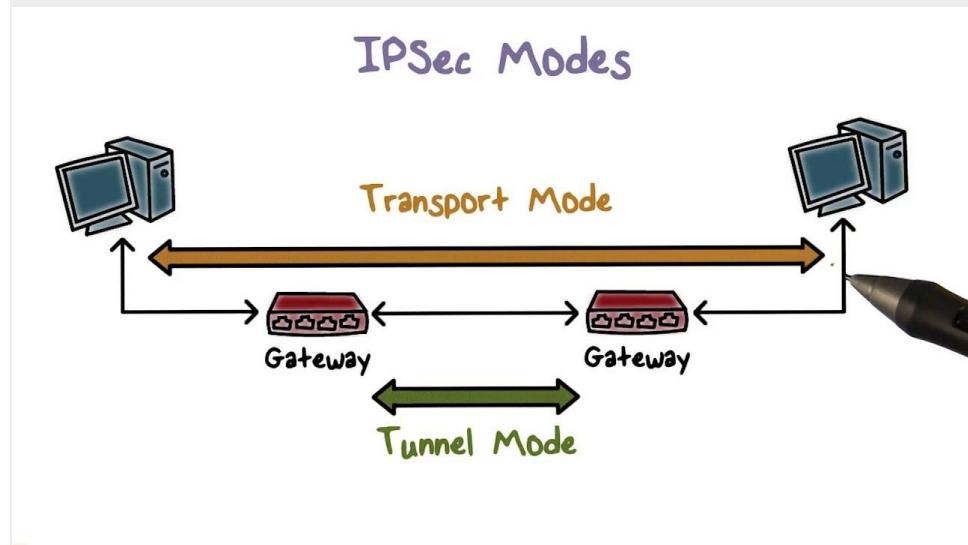
- Common remote access and VPN protocols include the following:
- Point-to-Point Protocol (PPP) enables hosts to set up a direct connection between two endpoints.



Overview of Remote Access

Remote Access Protocols (Continue)

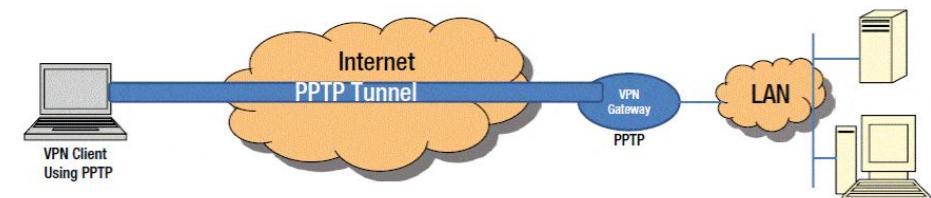
- IPsec - Internet Protocol Security is a set of security protocols used to enable authentication and encryption services to secure the transfer of IP packets over the internet.



Overview of Remote Access

Remote Access Protocols (Continue)

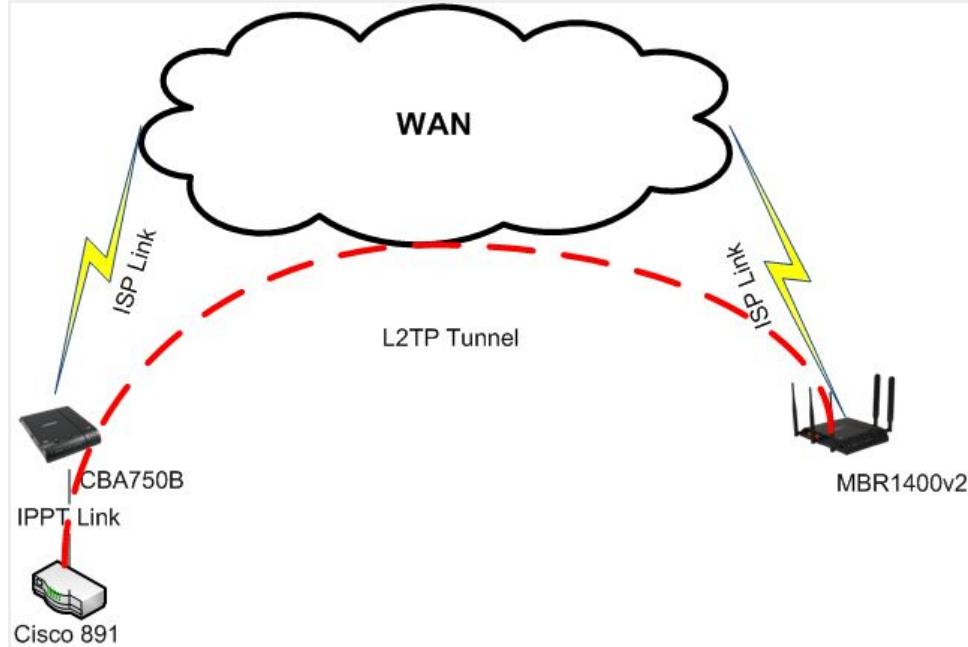
- Point-to-Point Tunneling (PPTP) is one of the oldest protocols for implementing virtual private networks.
- Although PPTP is not very secure, it persists in some cases



Overview of Remote Access

Remote Access Protocols (Continue)

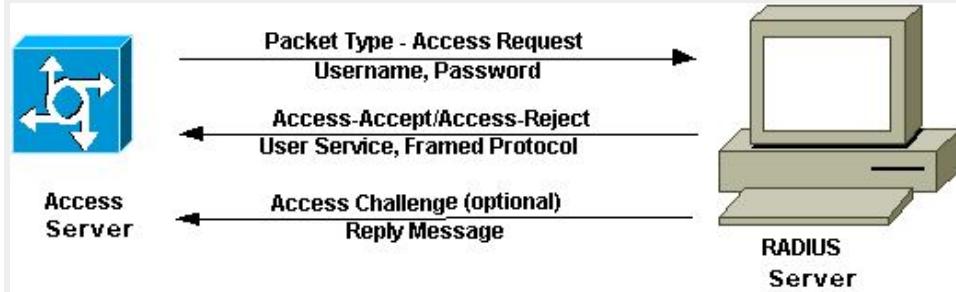
- Layer Two Tunneling Protocol (L2TP) is a VPN protocol that does not offer encryption or cryptographic authentication for the traffic that passes through the connection.
- As a result, it is usually paired with IPsec, which provides those services.



Overview of Remote Access

Remote Access Protocols (Continue)

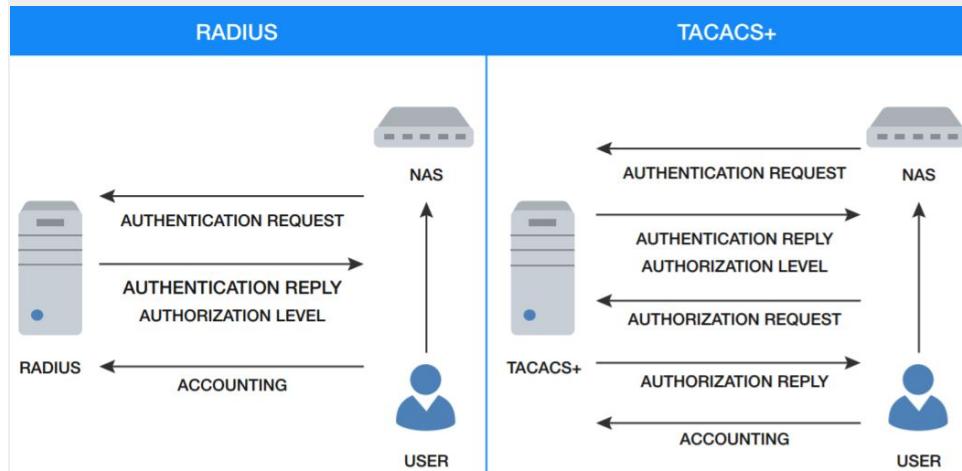
- Remote Authentication Dial-In User Service (RADIUS) enable remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.



Overview of Remote Access

Remote Access Protocols (Continue)

- Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that was originally common to UNIX networks that enables a remote access server to forward a user's password to an authentication server to determine whether access to a given system should be allowed.

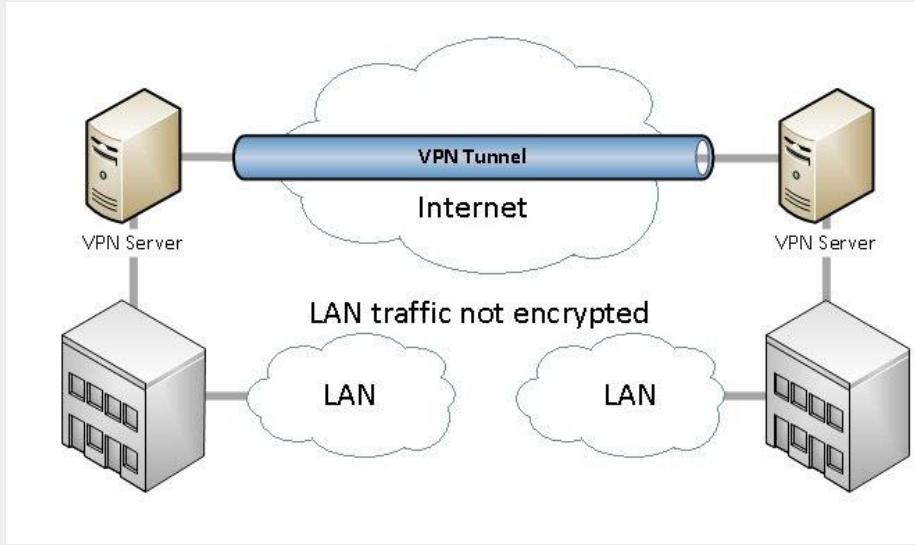


<https://i0.wp.com/www.networkhunt.com/wp-content/uploads/2017/10/RADIUS-VS-TACACS-packet-flow.png?fit=1101%2C579&ssl=1>

VPN Concepts

Introduction

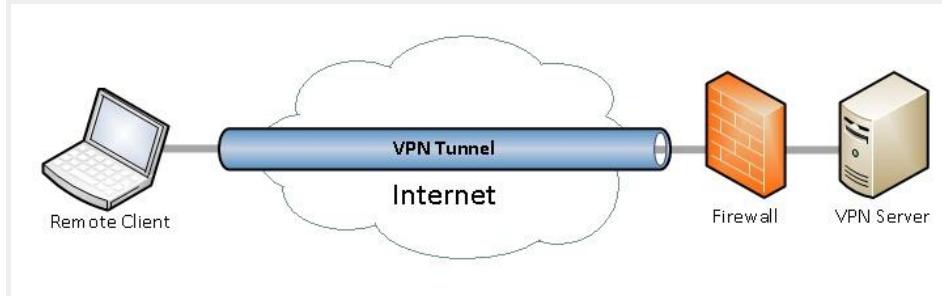
- A VPN is a private network that uses a public network to connect remote sites or users together.
- A VPN's purpose is providing a secure and reliable private connection between computer networks over an existing public network, typically the internet.



VPN Concepts

Introduction (Continue)

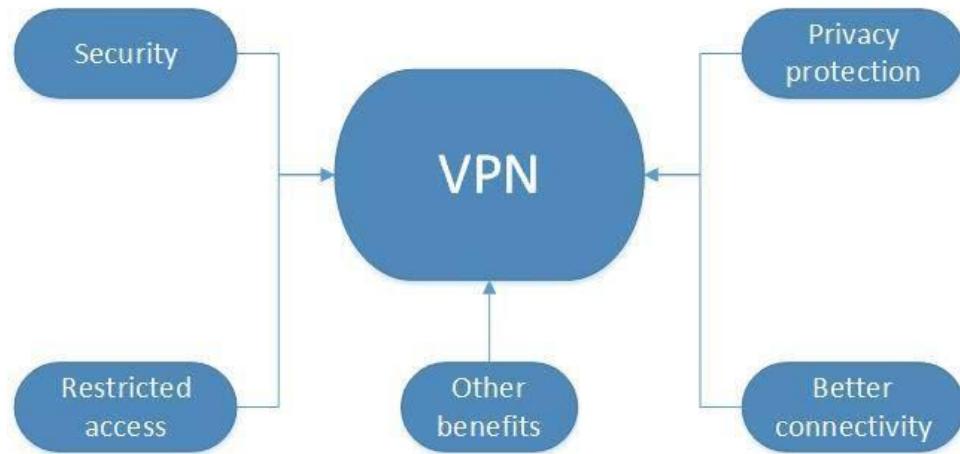
- It uses "virtual" connections routed through the internet from the business's private network to the remote site or person.
- VPNs help ensure security — anyone intercepting the encrypted data can't read it.



VPN Concepts

VPN Benefits

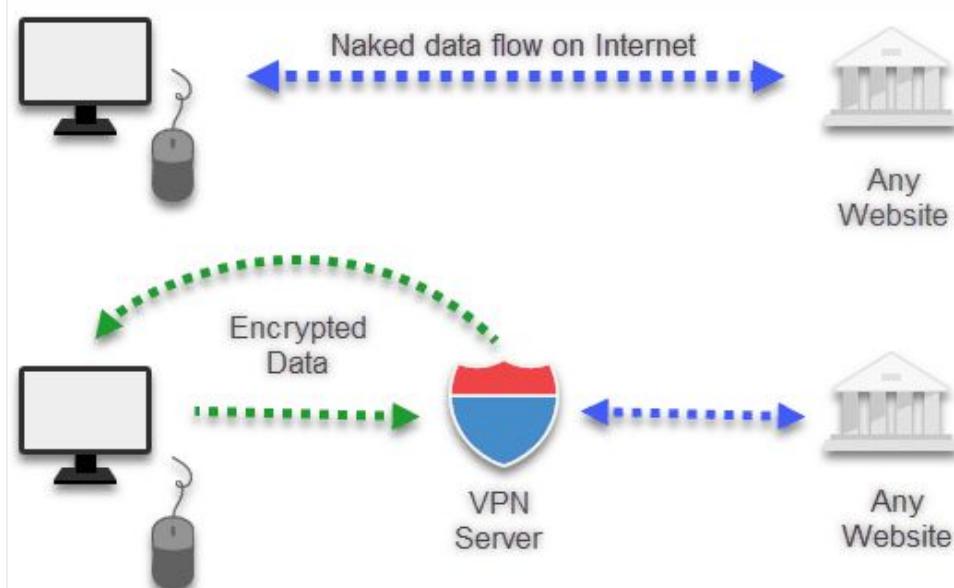
- Extended connections across multiple geographic locations without using a leased line
- Improved security for exchanging data
- Improved productivity for remote employees



VPN Concepts

VPN Benefits (Continue)

- Flexibility for remote offices and employees to use the business intranet over an existing internet connection as if they're directly connected to the network
- Savings in time and expense for employees to commute if they work from virtual workplaces



VPN Concepts

Desired VPN Features

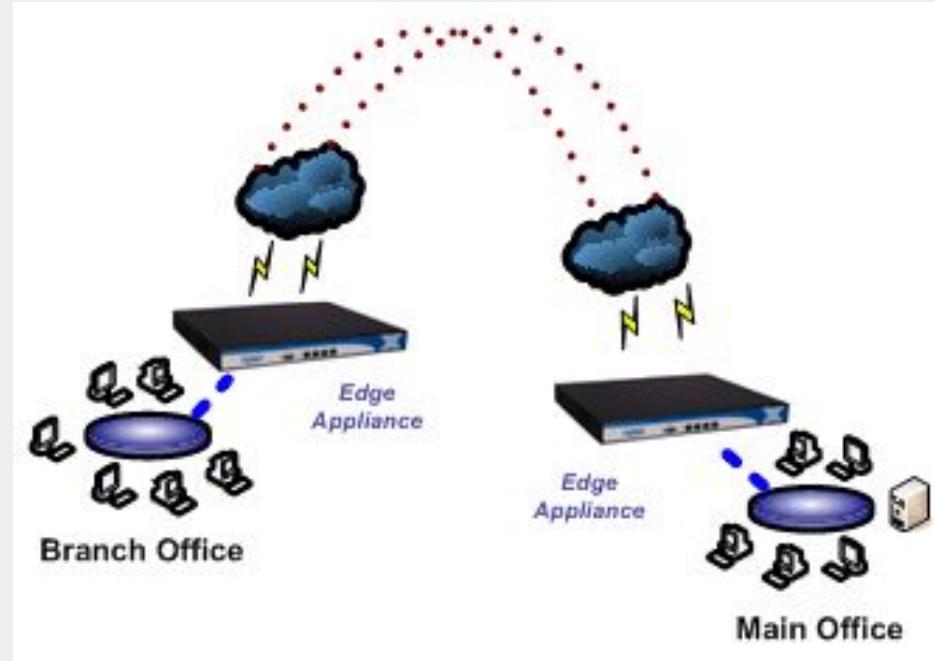
- Security
 - The VPN should protect data while it's traveling on the public network. If intruders attempt to capture the data, they should be unable to read or use it.



VPN Concepts

Desired VPN Features (Continue)

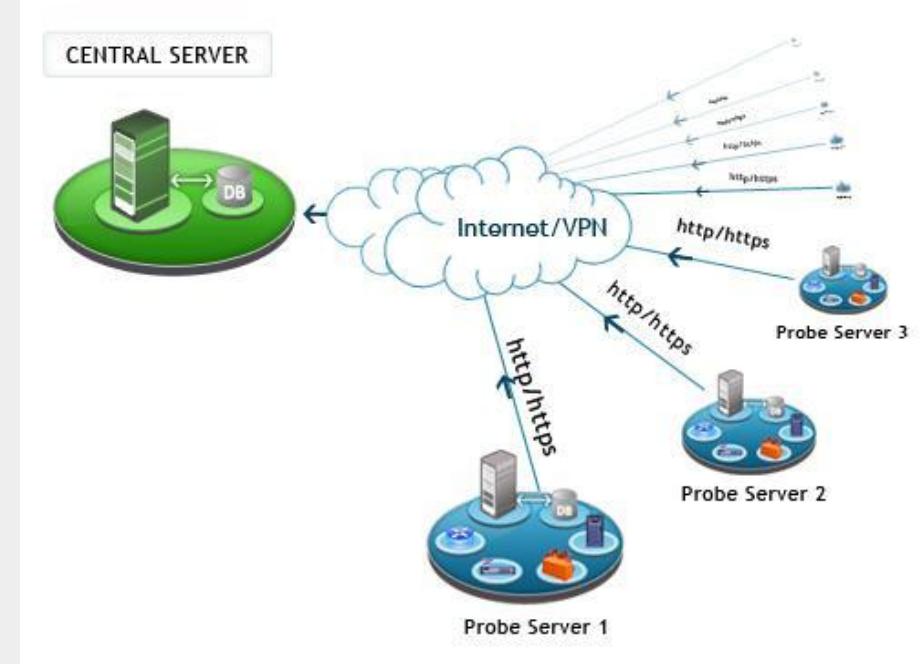
- Reliability
 - Employees and remote offices should be able to connect to the VPN with no trouble at any time (unless hours are restricted)
 - And, the VPN should provide the same quality of connection for each user even when it is handling its maximum number of simultaneous connections.



VPN Concepts

Desired VPN Features (Continue)

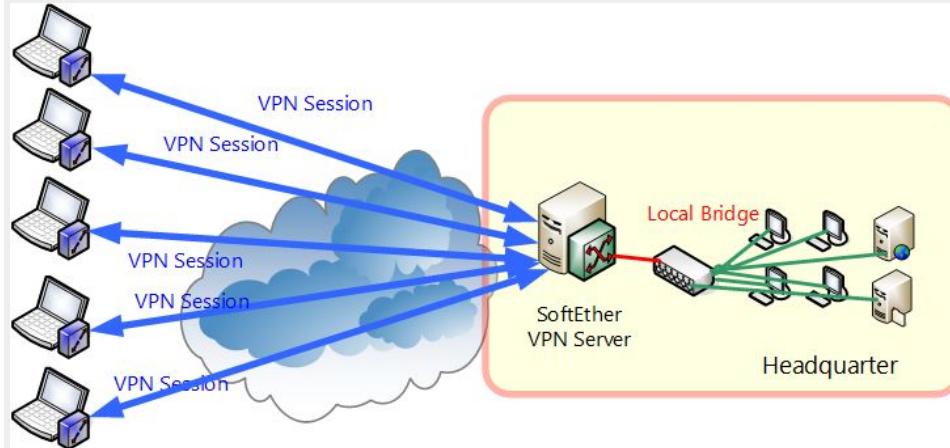
- Scalability
 - As a business grows, it should be able to extend its VPN services to handle that growth without replacing the VPN technology altogether.



VPN Concepts

Types of VPN

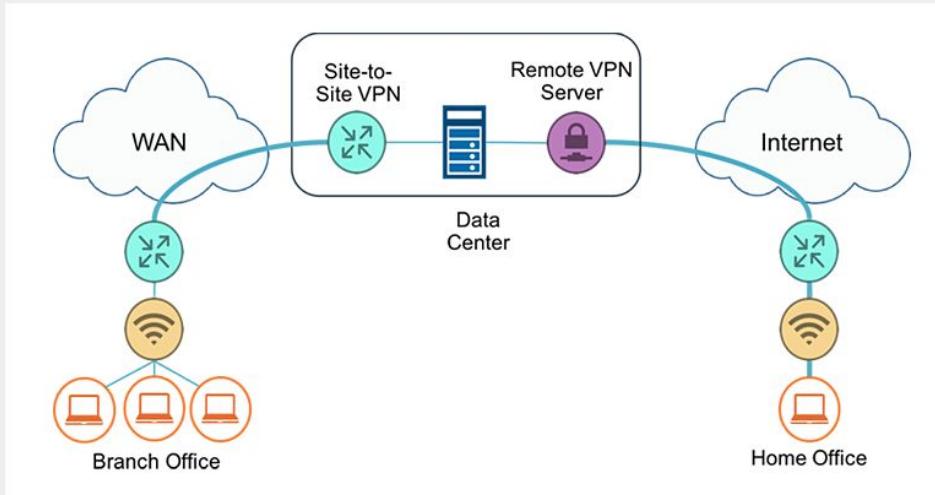
- **Remote-Access VPN** allows individual users to establish secure connections with a remote computer network.
- Large corporations or businesses with knowledgeable IT staff typically purchase, deploy and maintain their own remote-access VPNs.



VPN Concepts

Types of VPN (Continue)

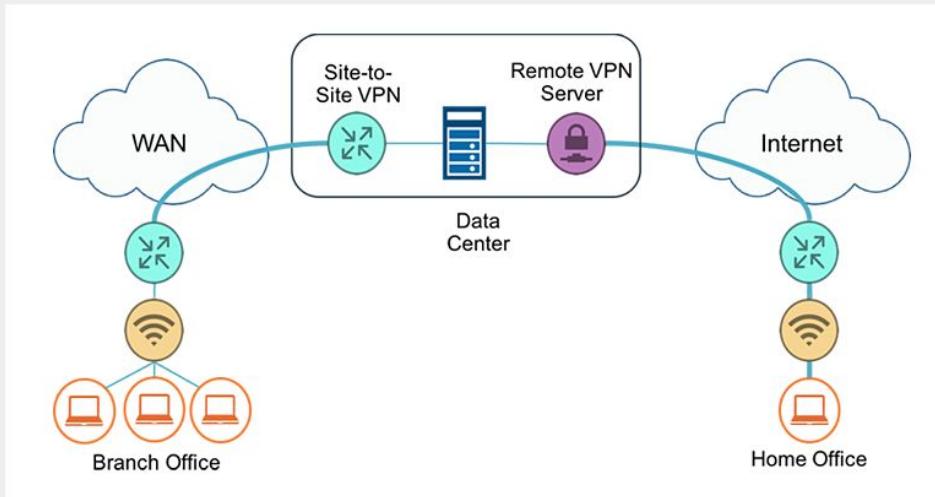
- There are two components required in a remote-access VPN.
- The first is a network access server also called a remote-access server (RAS)
- The other required component of remote-access VPNs is client software.



VPN Concepts

Types of VPN (Continue)

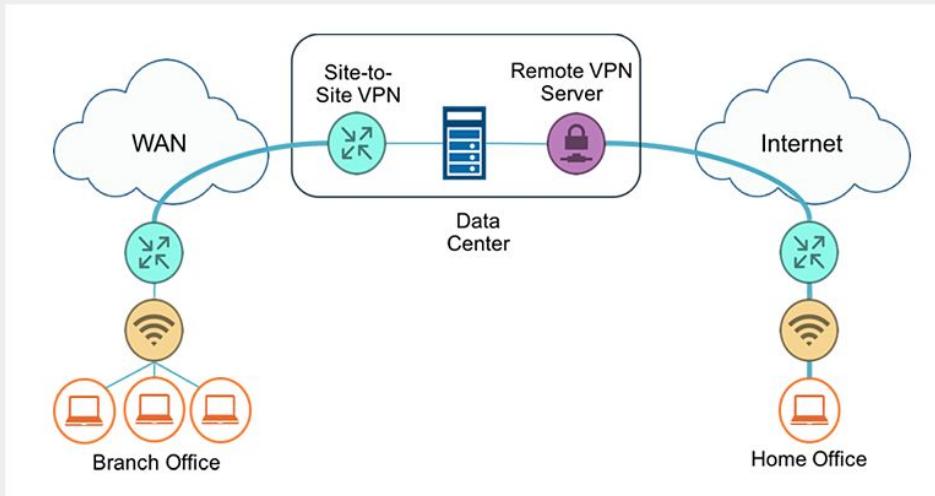
- A **site-to-site VPN** allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the internet.
- Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations.



VPN Concepts

Types of VPN (Continue)

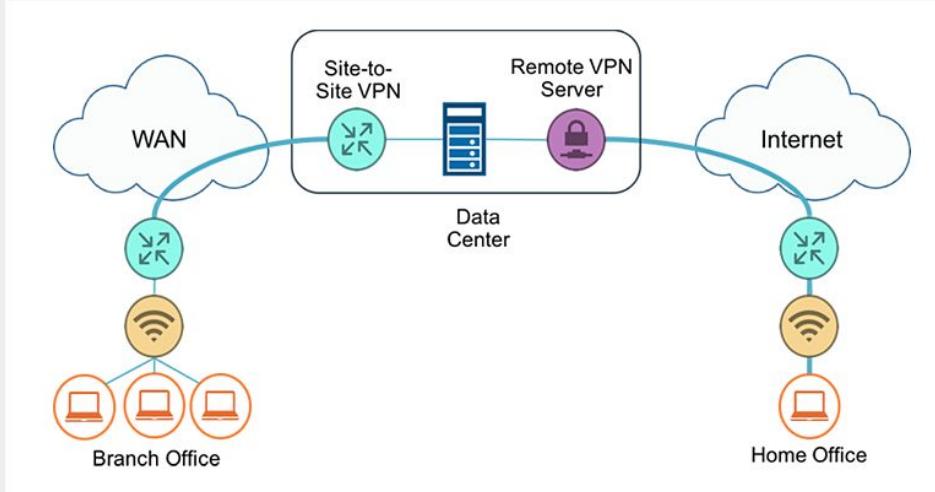
- There are two types of site-to-site VPNs:
 - **Intranet-based:** If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect each separate LAN to a single WAN.



VPN Concepts

Types of VPN (Continue)

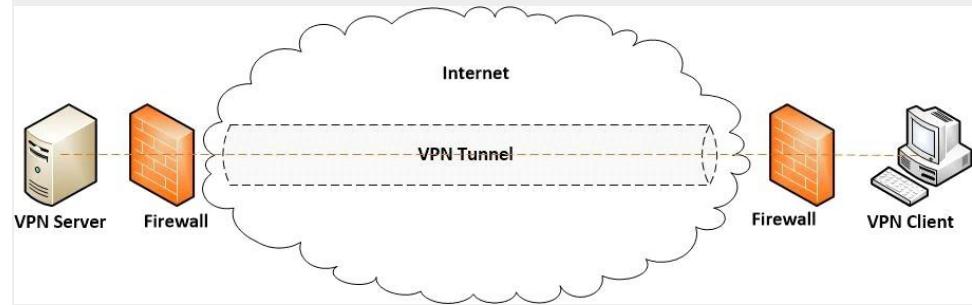
- **Extranet-based:** When a company has a close relationship with another company (such as a partner, supplier or customer), it can build an extranet VPN that connects those companies' LANs.



VPN Concepts

VPN Tunneling

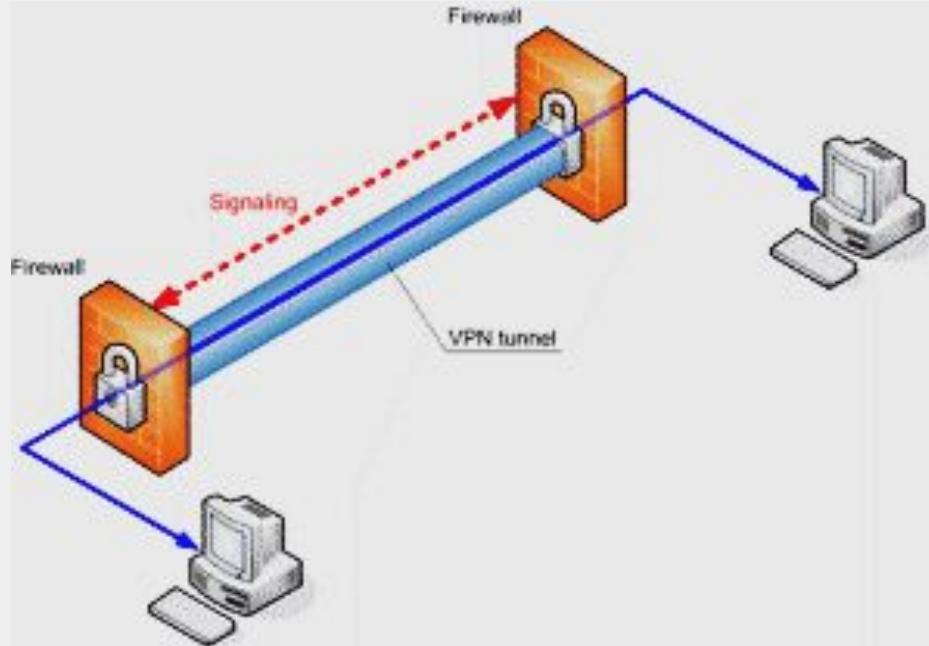
- Most VPNs rely on tunneling to create a private network that reaches across the internet.
- Tunneling is the process of placing an entire packet within another packet before it's transported over the internet.
- That outer packet protects the contents from public view and ensures that the packet moves within a virtual tunnel.



VPN Concepts

VPN Tunneling (Continue)

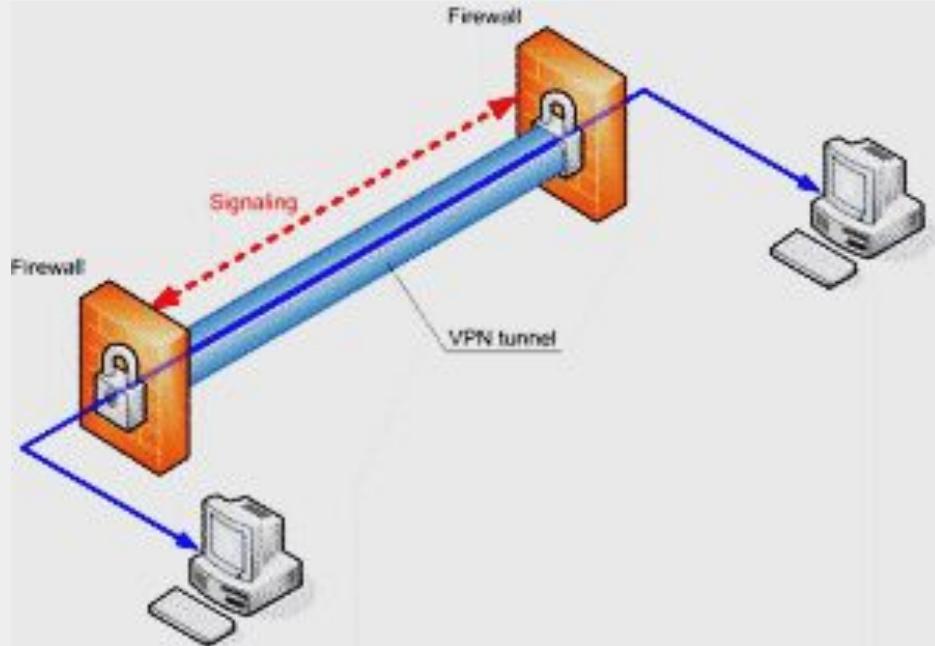
- This layering of packets is called encapsulation. Computers or other network devices at both ends of the tunnel, called tunnel interfaces, can encapsulate outgoing packets and reopen incoming packets.
- Also called an encapsulation protocol, a tunneling protocol is a standardized way to encapsulate packets



VPN Concepts

VPN Tunneling (Continue)

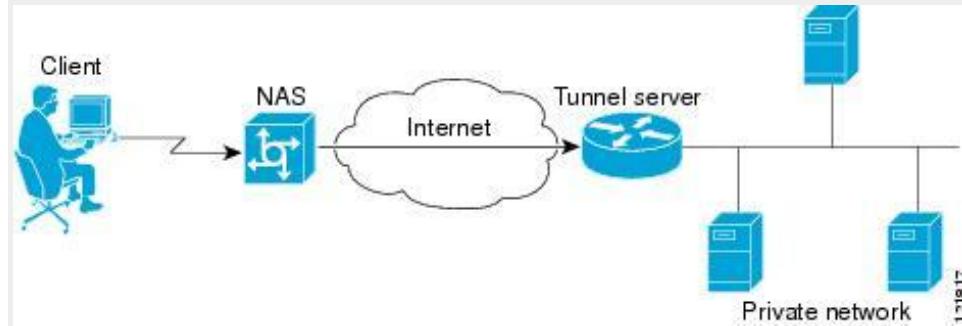
- Some VPNs, such as ExpressVPN have a split tunneling feature. This means you can choose which apps send data through the VPN and which use your regular, local connection.



VPN Concepts

Equipment used for VPN

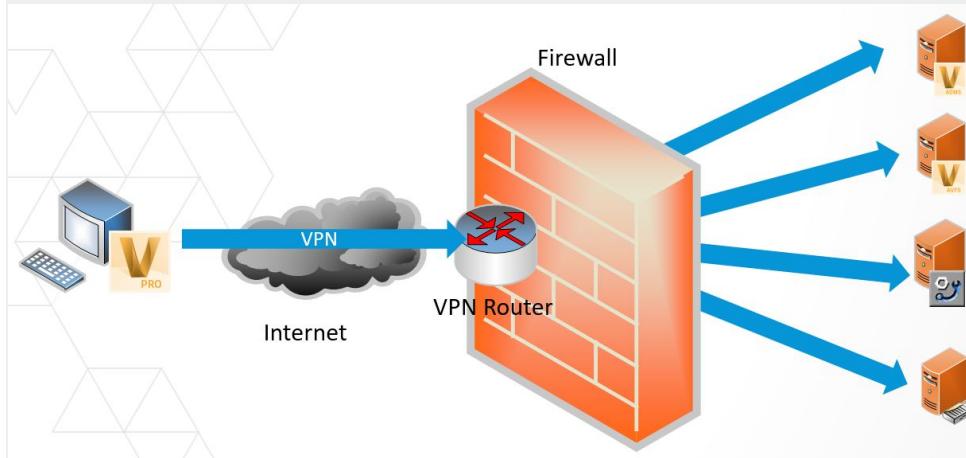
- Network Access Server
 - NAS is responsible for setting up and maintaining each tunnel in a remote-access VPN



VPN Concepts

Equipment used for VPN (Continue)

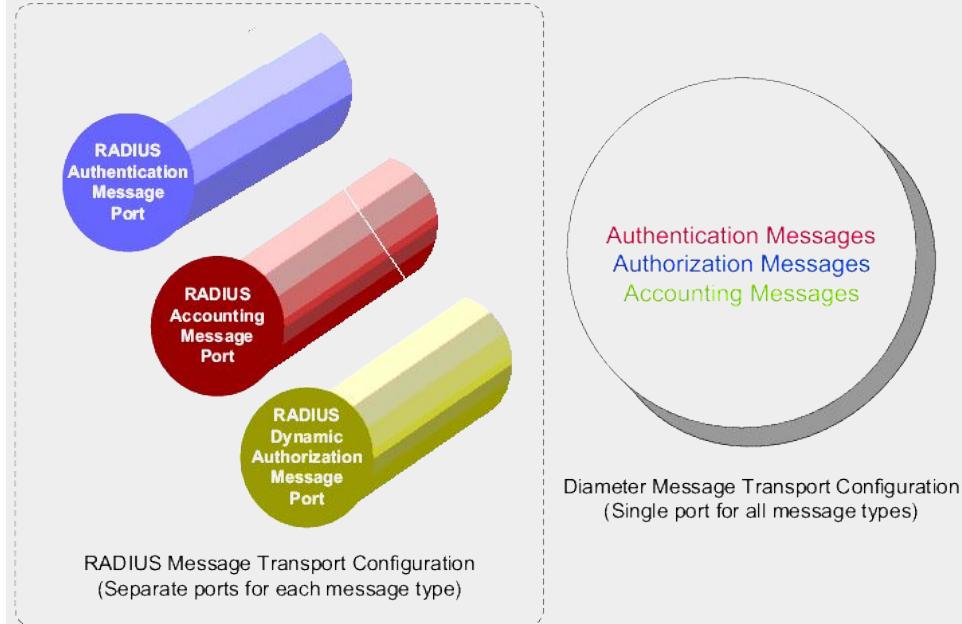
- Firewall
 - A firewall provides a strong barrier between your private network and the internet.



VPN Concepts

Equipment used for VPN (Continue)

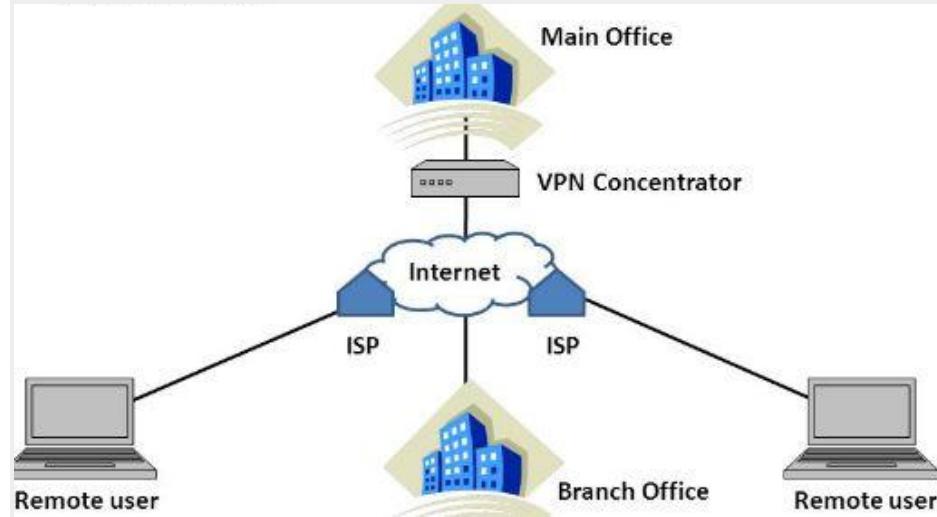
- AAA Server
 - The acronym stands for the server's three responsibilities: authentication, authorization and accounting.



VPN Concepts

Equipment used for VPN (Continue)

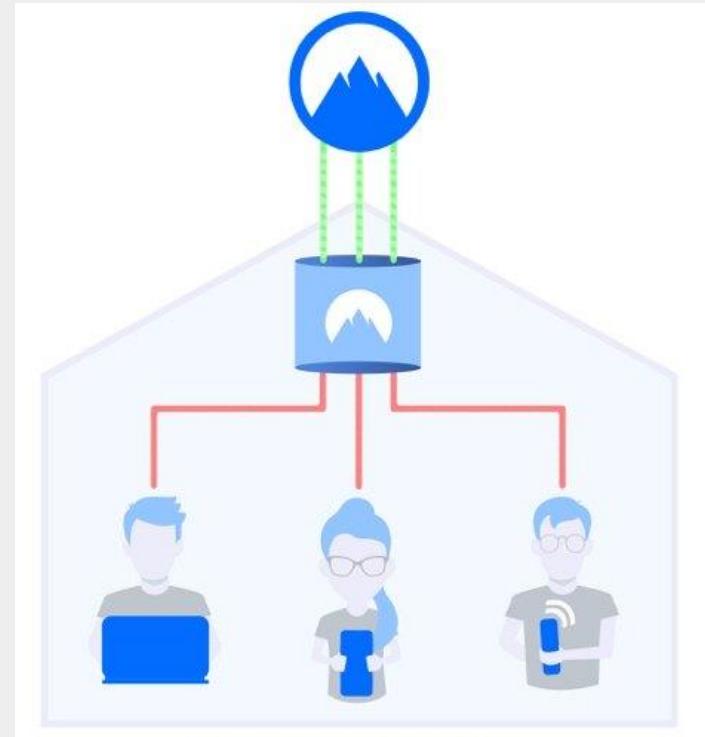
- VPN Concentrator
 - This device replaces an AAA server installed on a generic server. The hardware and software work together to establish VPN tunnels and handle large numbers of simultaneous connections.



VPN Concepts

Equipment used for VPN (Continue)

- VPN-enabled/VPN-optimized Router
 - This is a typical router that delegates traffic on a network, but with the added feature of routing traffic using protocols specific to VPNs.



VPN Concepts

Equipment used for VPN (Continue)

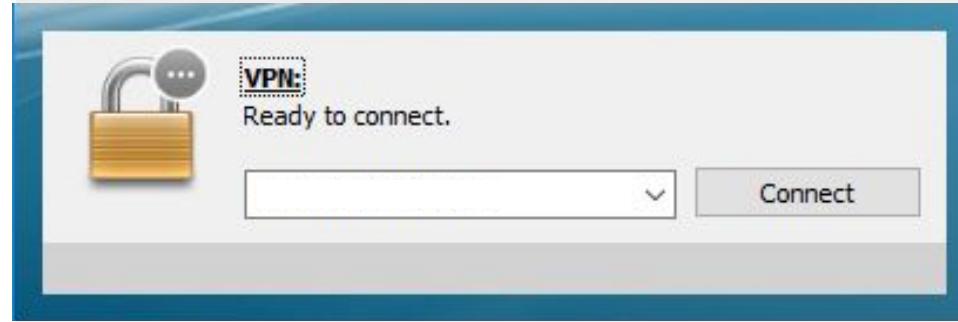
- VPN-enabled Firewall
 - This is a conventional firewall protecting traffic between networks, but with the added feature of managing traffic using protocols specific to VPNs.



VPN Concepts

Equipment used for VPN (Continue)

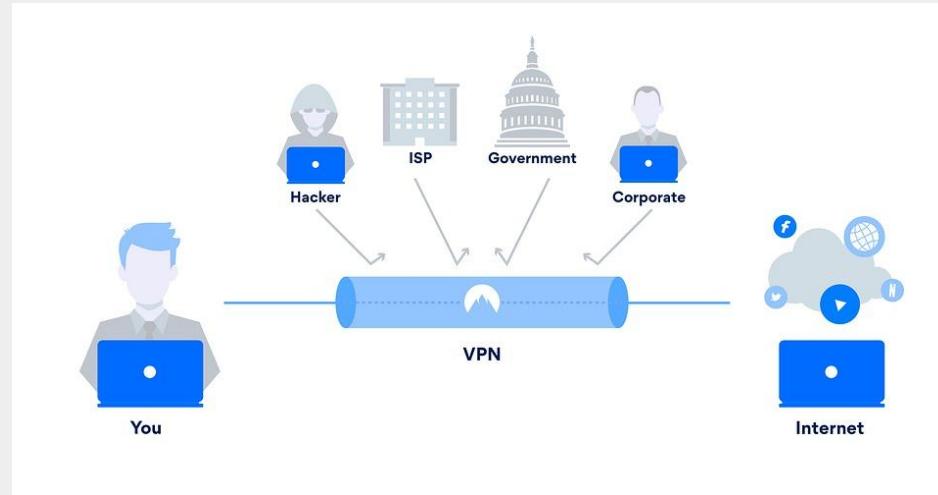
- VPN Client
 - This is software running on a dedicated device that acts as the tunnel interface for multiple connections. This setup spares each computer from having to run its own VPN client software.



VPN Concepts

VPN Security

- In a VPN, the computers at each end of the tunnel encrypt the data entering the tunnel and decrypt it at the other end.
- A **site-to-site VPN** could use either internet protocol security protocol (IPSec) or generic routing encapsulation (GRE)



VPN Concepts

VPN Security (Continue)

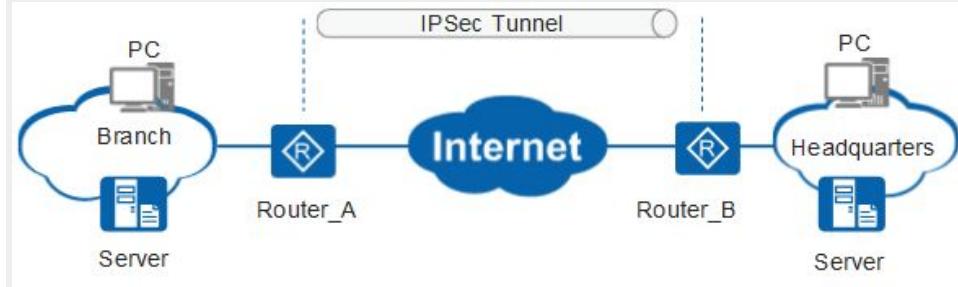
- GRE
 - Provides the framework for how to package the passenger protocol for transport over the internet protocol (IP).
 - It includes information on what type of packet you're encapsulating and the connection between sender and receiver.



VPN Concepts

VPN Security (Continue)

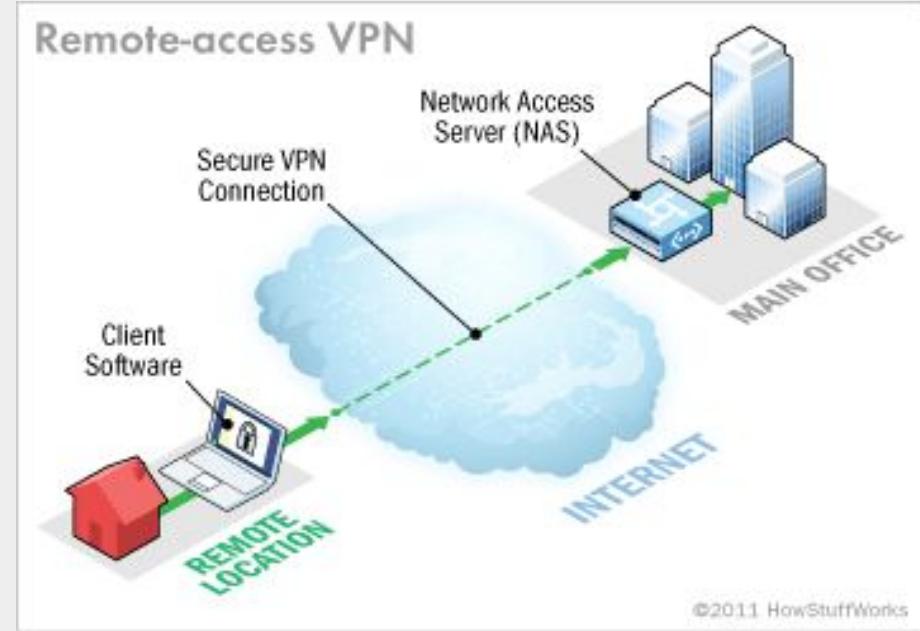
- IPSec
 - A widely used protocol for securing traffic on IP networks, including the internet. IPSec can encrypt data between various devices, including router to router, firewall to router, desktop to router, and desktop to server.



VPN Concepts

VPN Security (Continue)

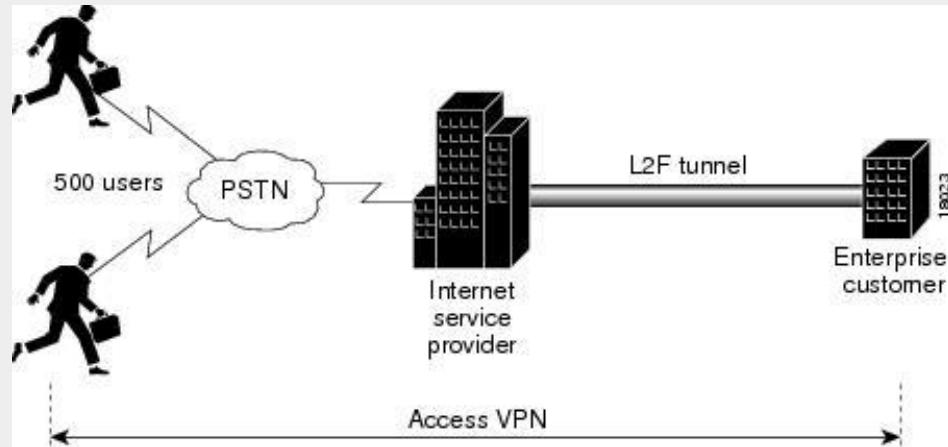
- In a **remote-access VPN**, tunneling typically relies on Point-to-point Protocol (PPP) which is part of the native protocols used by the internet.



VPN Concepts

VPN Security (Continue)

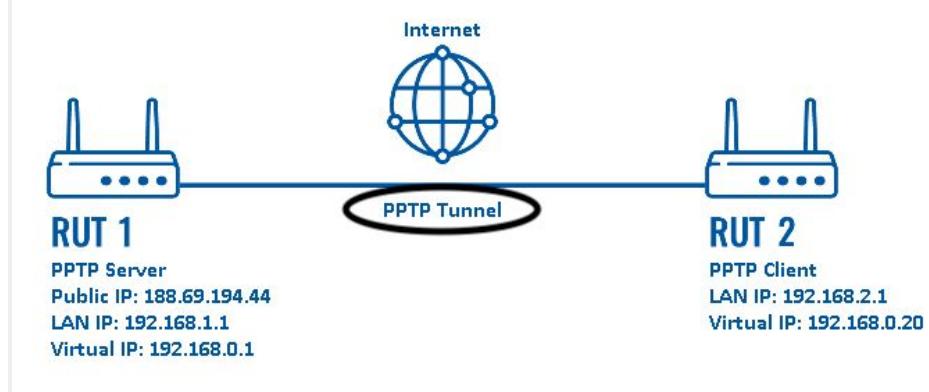
- L2F (Layer 2 Forwarding)
 - Developed by Cisco; uses any authentication scheme supported by PPP



VPN Concepts

VPN Security (Continue)

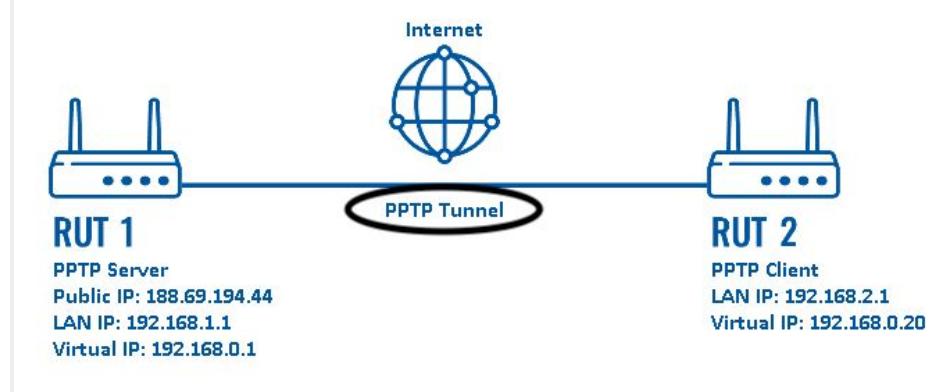
- PPTP (Point-to-point Tunneling Protocol)
 - Supports 40-bit and 128-bit encryption and any authentication scheme supported by PPP



VPN Concepts

VPN Security (Continue)

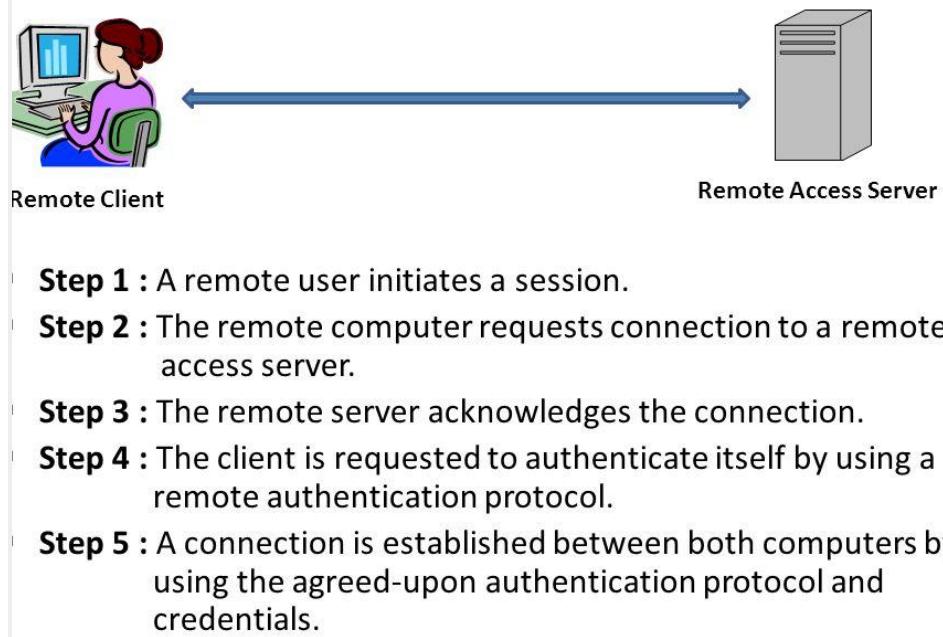
- L2TP (Layer 2 Tunneling Protocol)
 - Combines features of PPTP and L2F and fully supports IPSec; also applicable in site-to-site VPNs



Remote Access Authentication Protocol

Remote Access Authentication Protocol

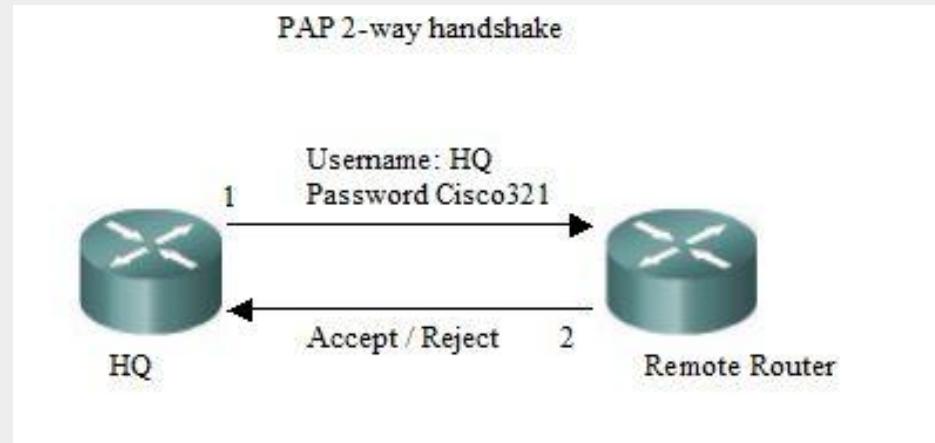
- There are simply two methods to authenticate PPP links namely Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP)
- From these two authentication protocols, PAP is less secured as the password is sent in clear text and is performed only at the initial link establishment.



Remote Access Authentication Protocol

Password Authentication Protocol (PAP)

- PAP is a password Authentication Protocol used by PPP links to validate users.
- PAP authentication requires the calling device to enter the username and password.
- If the credentials match with the local database of the called device or in the remote AAA database then it is allowed to access otherwise denied.

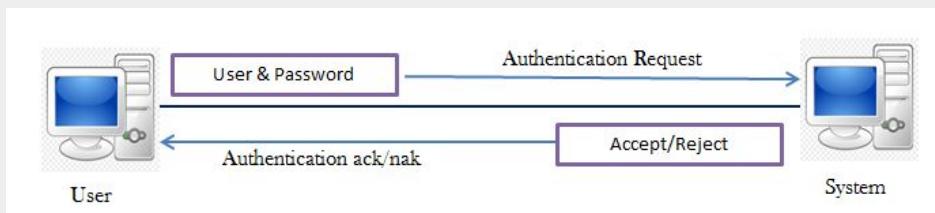


Remote Access Authentication Protocol

Password Authentication Protocol (PAP) (Continue)

Some of the features of PAP are:

- The password is sent in clear text.
- All network operating system support PAP.
- It uses two-way Handshake Protocol.
- It is non-interactive.
- PAP supports both one-way authentication (unidirectional) and two-way authentication (bidirectional).

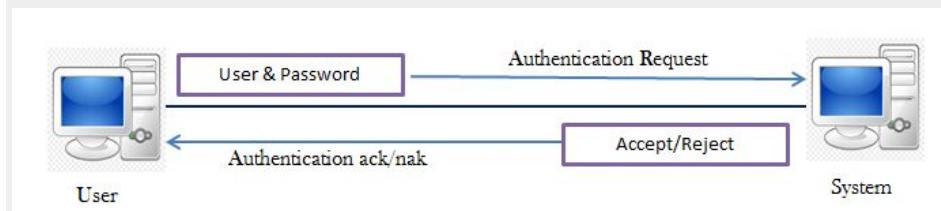


Remote Access Authentication Protocol

Password Authentication Protocol (PAP) (Continue)

PAP is usually used in following scenarios:

- When the application doesn't support CHAP.
- Circumstances where it is necessary to send a plain text password to stimulate a login at the called device (remote host).
- When there is occurrence of incompatibilities between different vendors of CHAP.

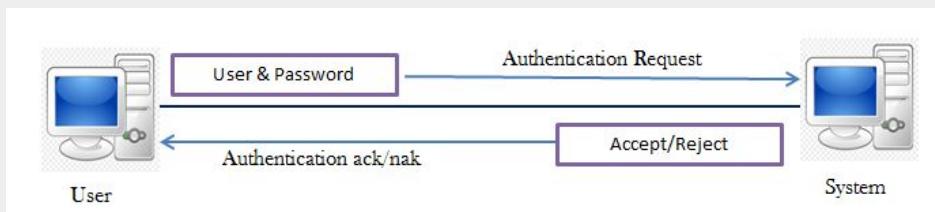


Remote Access Authentication Protocol

Password Authentication Protocol (PAP) (Continue)

Advantage of PAP over CHAP

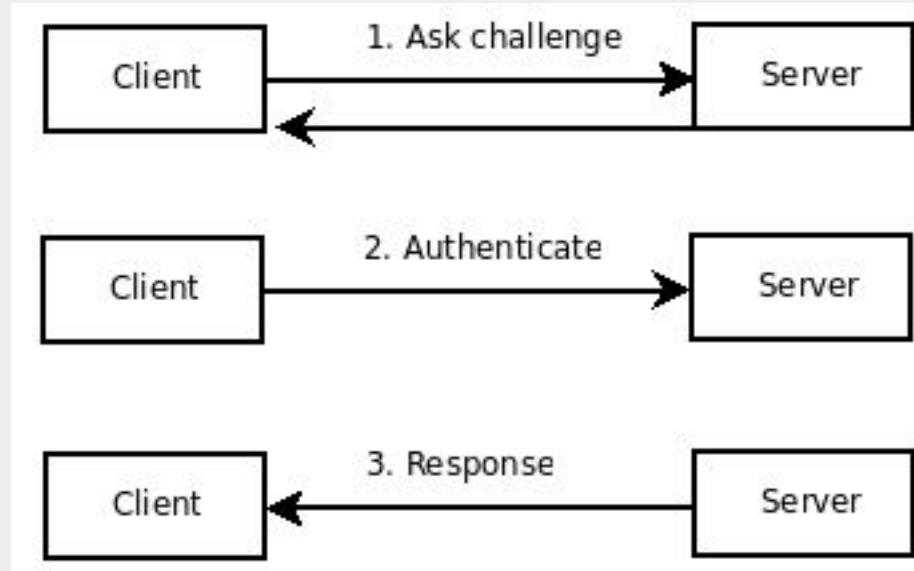
- The only advantage PAP holds over CHAP is that it is supported by all the network operating system vendors therefore it can be said that PAP is used where CHAP is not supported.



Remote Access Authentication Protocol

Challenge Handshake Authentication Protocol (CHAP)

- Challenge Handshake Authentication Protocol (CHAP) is a Point-to-point protocol (PPP) authentication protocol.
- It is used at the initial startup of the link.
- Also, it performs periodic checkups to check if the router is still communicating with the same host.



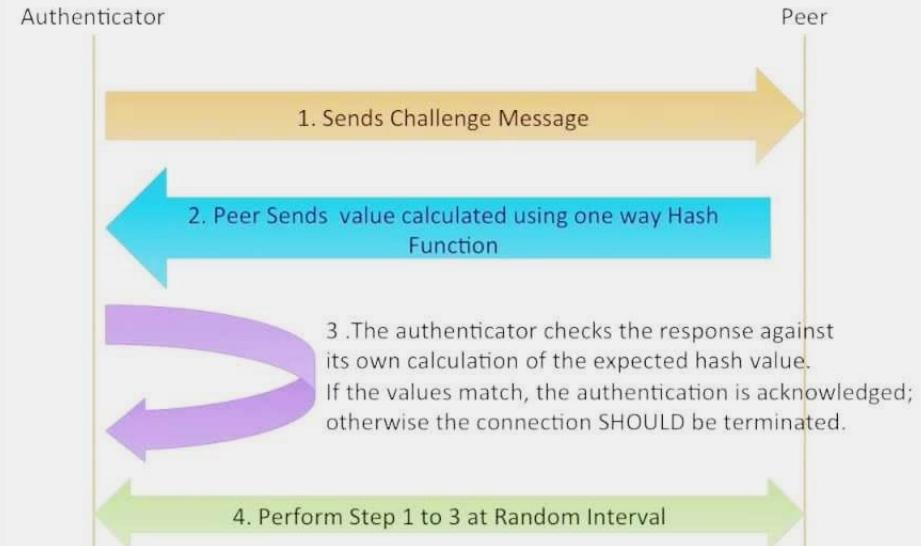
Remote Access Authentication Protocol

Challenge Handshake Authentication Protocol (CHAP) (Continue)

Features:

- It uses 3-way handshaking protocol.
- It uses one-way hash function called MD5.
- It also authenticates periodically to check if the communication is taking place with the same device or not.
- Also, it provides more security than PAP
- CHAP requires to know the plaintext of the secret.

3 Way Handshake



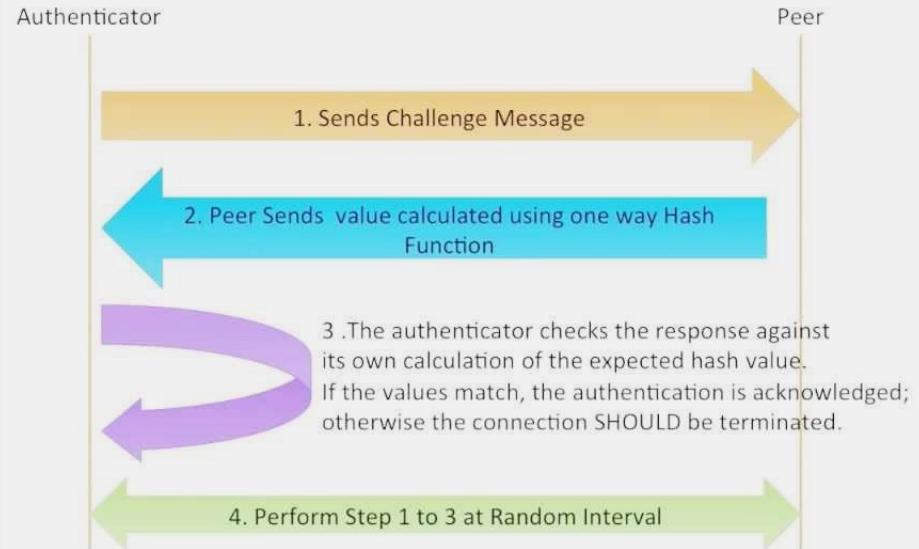
Remote Access Authentication Protocol

Challenge Handshake Authentication Protocol (CHAP) (Continue)

CHAP packets:

- Challenge Packet
- Response Packet
- Success Packet
- Failure Packet

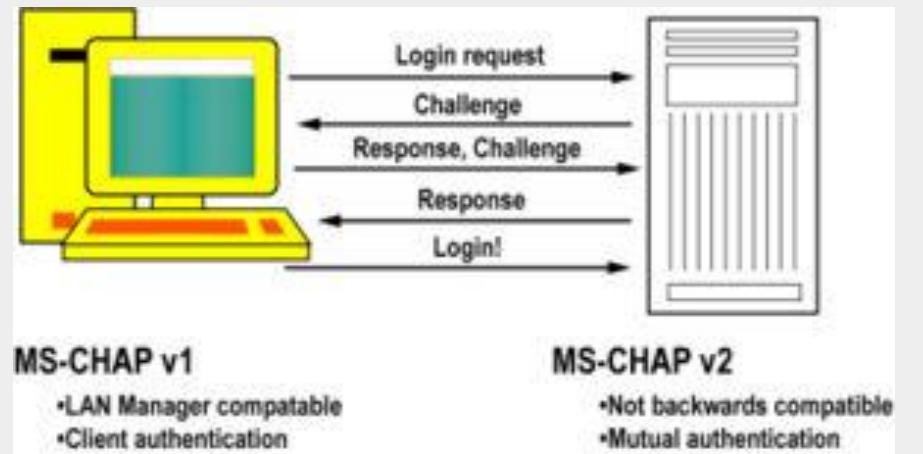
3 Way Handshake



Remote Access Authentication Protocol

MS-CHAP

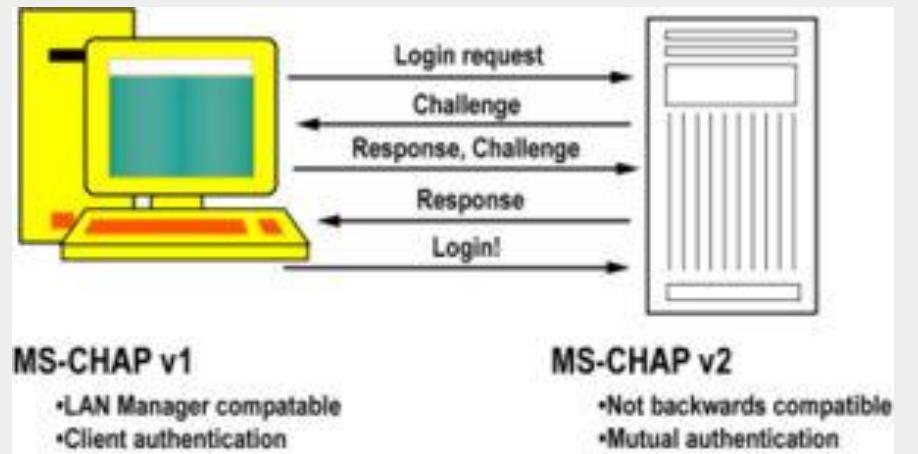
- MS-CHAP is the Microsoft version of the Challenge-Handshake Authentication Protocol, CHAP.
- The protocol exists in two versions, MS-CHAPv1 and MS-CHAPv2.



Remote Access Authentication Protocol

MS-CHAP (Continue)

- MS-CHAP is used as one authentication option in Microsoft's implementation of the PPTP protocol for virtual private networks.
- It is further used as the main authentication option of the Protected Extensible Authentication Protocol (PEAP).



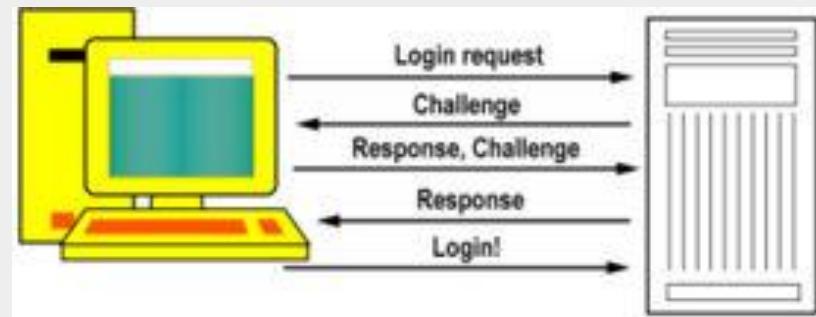
https://lh3.googleusercontent.com/proxy/tXVHpOxZtNflmJT7ZKHEuXSklSikO1hiyxLsBmTsl4aZ1zlzbdRsMMXVDL_pkluYyP6wd_YNhQlZA2WJqXe17D16jxipcP4uVGvwVNNMrlTq1sa-CgL-EhcLBzRgK5dg_3akCjyEH0UpQ-t3QigKZiMz4n2vnvlKDenxBycXdZwMn5_5Cge1Cm

Remote Access Authentication Protocol

MS-CHAP (Continue)

Compared with CHAP

- Provides an authenticator-controlled password change mechanism
- Provides an authenticator-controlled authentication retry mechanism
- Defines failure codes returned in the Failure packet message field



MS-CHAP v1

- LAN Manager compatible
- Client authentication

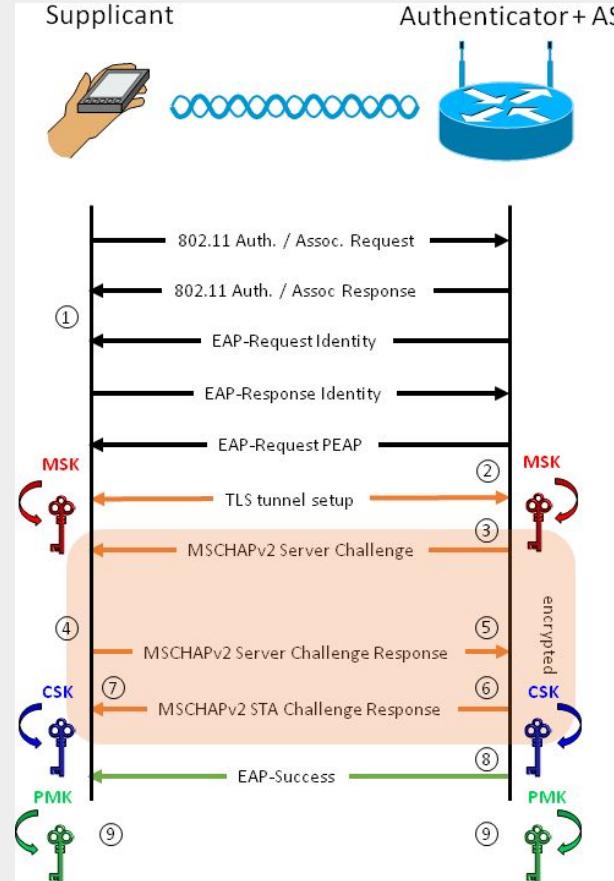
MS-CHAP v2

- Not backwards compatible
- Mutual authentication

Remote Access Authentication Protocol

MS-CHAP v2

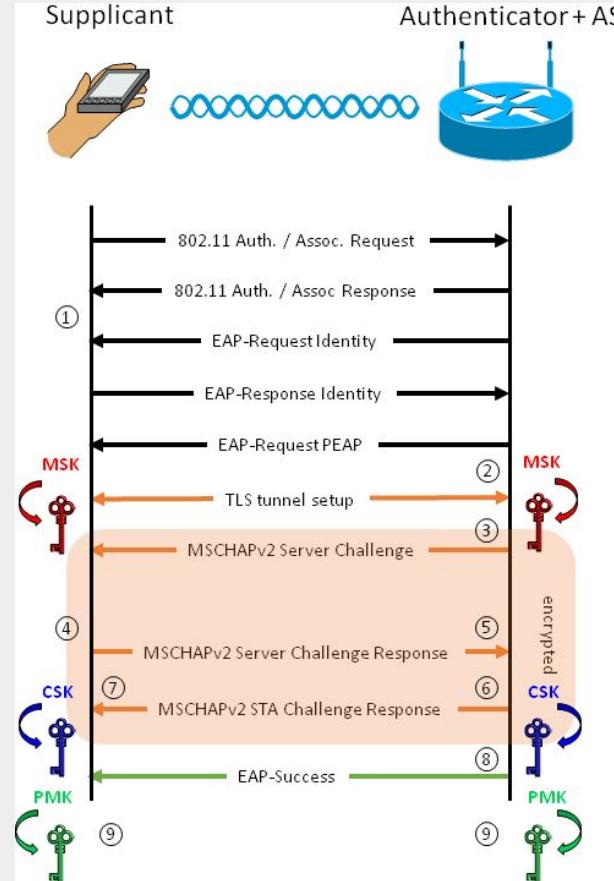
- MS-CHAP v2 is a Microsoft authentication protocol that, like CHAP, avoids sending passwords in clear-text.
- MS-CHAP v2 communicates users' requests to change their passwords to a RADIUS server.



Remote Access Authentication Protocol

MS-CHAP v2 (Continue)

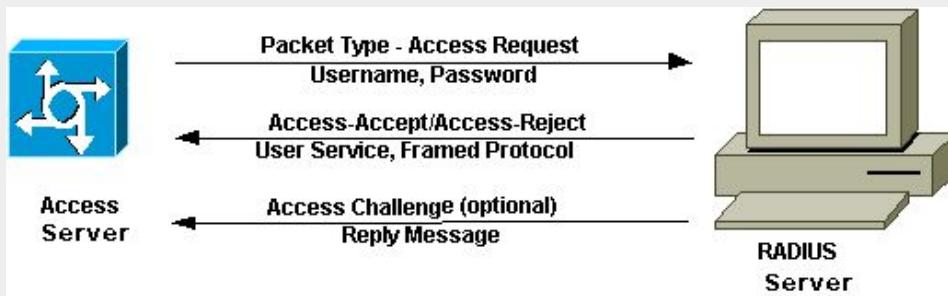
- Steel-Belted Radius Carrier must be able to perform a digest operation similar to CHAP to support MS-CHAP v2.
- Native User passwords are stored in the Steel-Belted Radius Carrier database.



Remote Access Authentication Protocol

RADIUS

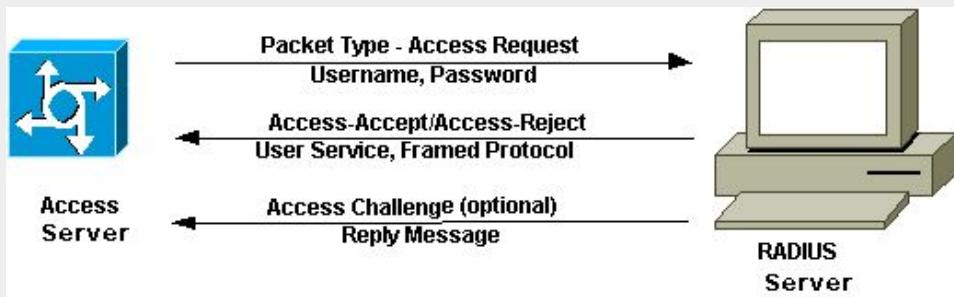
- The Remote Authentication Dial-In User Service (RADIUS)
- Developed in 1991 as an access server authentication and accounting protocol.
- RADIUS is the underlying authentication and access protocol used by the majority of network and computing systems.
- RADIUS is commonly used to facilitate roaming between ISPs.



Remote Access Authentication Protocol

RADIUS (Continue)

- Communication between a network access server (NAS) and a RADIUS server is based on the User Datagram Protocol (UDP).
- RADIUS is a client/server protocol.

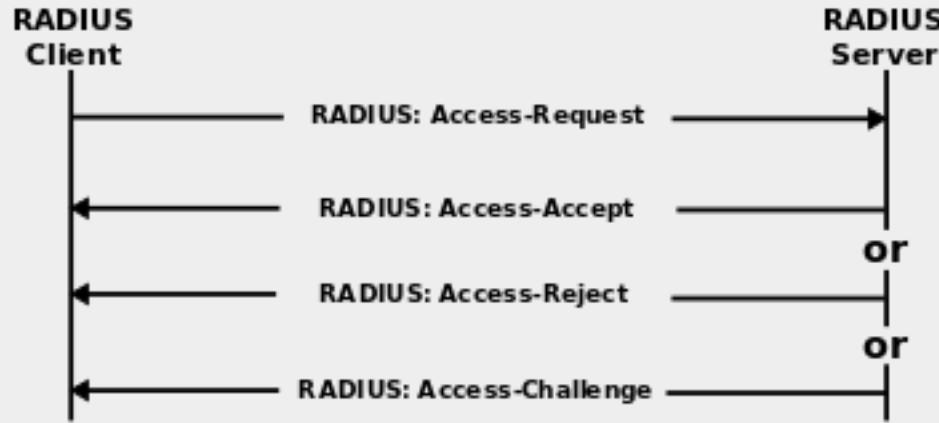


Remote Access Authentication Protocol

RADIUS (Continue)

How it works?

1. User initiates PPP authentication to the NAS.
2. NAS prompts for username and password (if Password Authentication Protocol [PAP]) or challenge (if Challenge Handshake Authentication Protocol [CHAP]).
3. User replies.

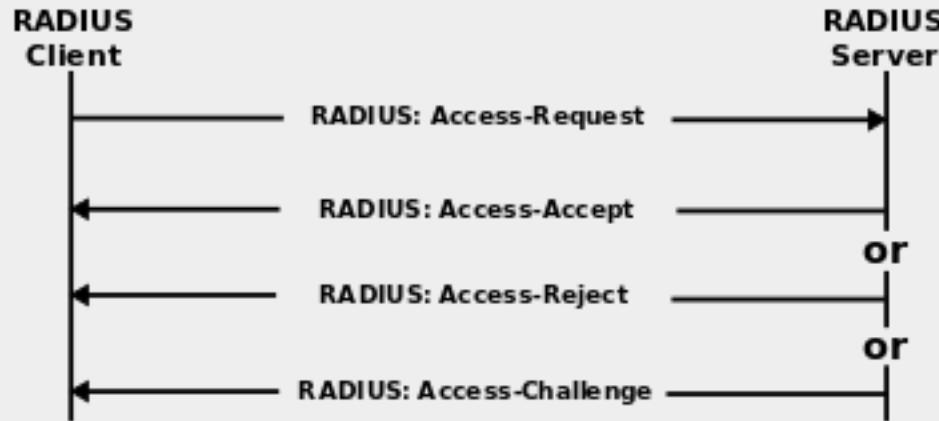


https://upload.wikimedia.org/wikipedia/commons/thumb/5/50/Drawing_RADIUS_1812.svg/350px-Drawing_RADIUS_1812.svg.png

Remote Access Authentication Protocol

RADIUS (Continue)

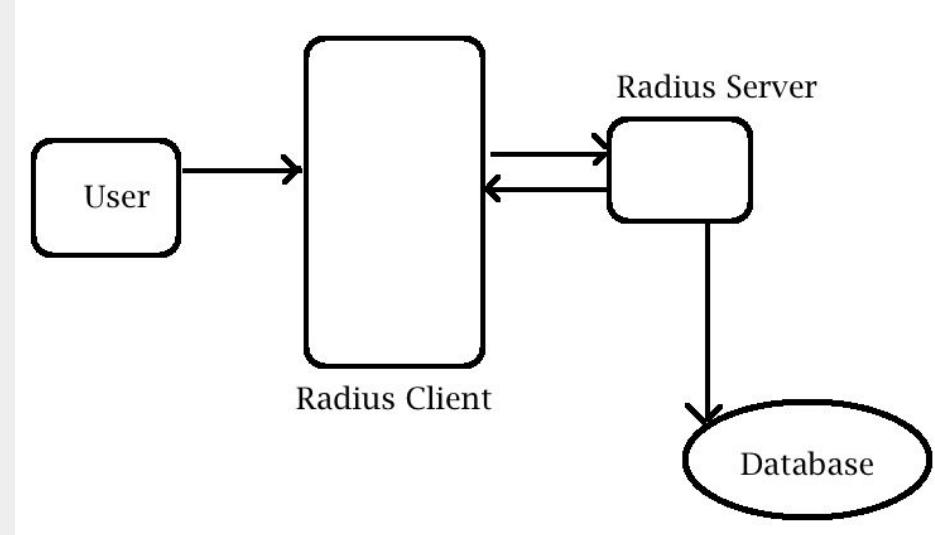
4. RADIUS client sends username and encrypted password to the RADIUS server.
5. RADIUS server responds with Accept, Reject, or Challenge.
6. The RADIUS client acts upon services and services parameters bundled with Accept or Reject.



Remote Access Authentication Protocol

RADIUS (Continue)

- The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms.

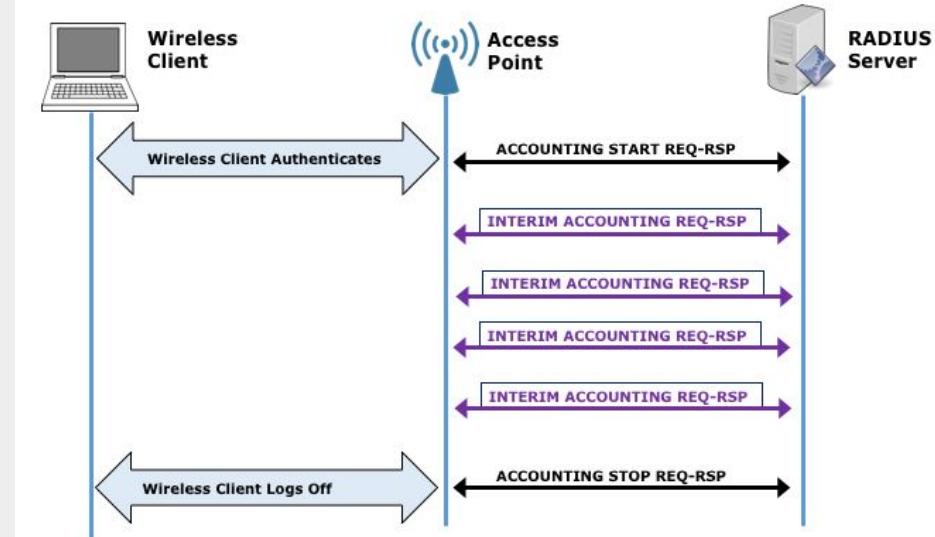


Remote Access Authentication Protocol

RADIUS (Continue)

Accounting

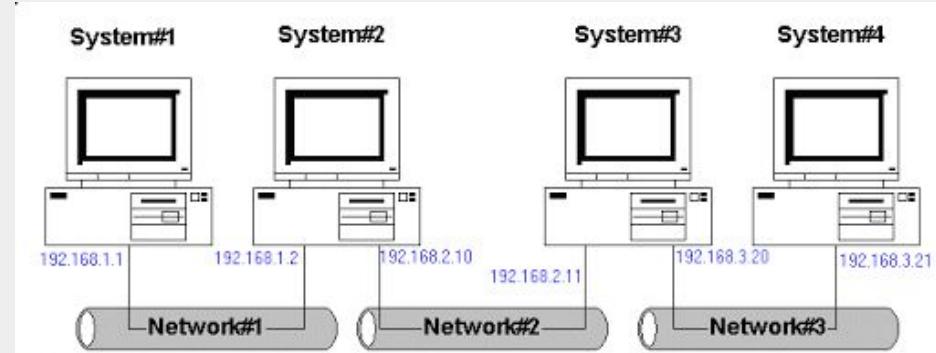
- The accounting features of the RADIUS protocol can be used independently of RADIUS authentication or authorization.
- The RADIUS accounting functions allow data to be sent at the start and end of sessions, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session.



TCP/IP Routing

Introduction

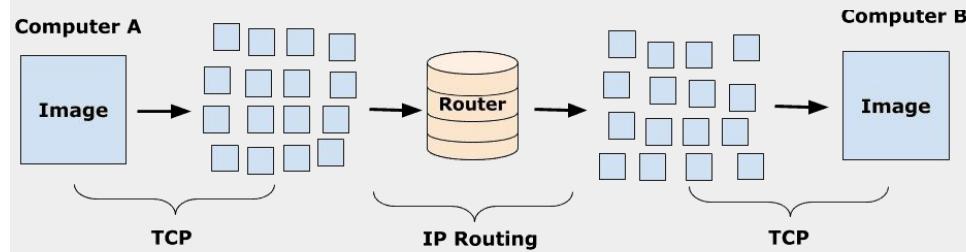
- TCP/IP must support routing capabilities, if not, information sent out to the Internet may never be delivered to its proper destination.
- Since TCP/IP is the protocol used for the Internet, it is a necessity that the protocol supports the immense size.



TCP/IP Routing

Introduction (Continue)

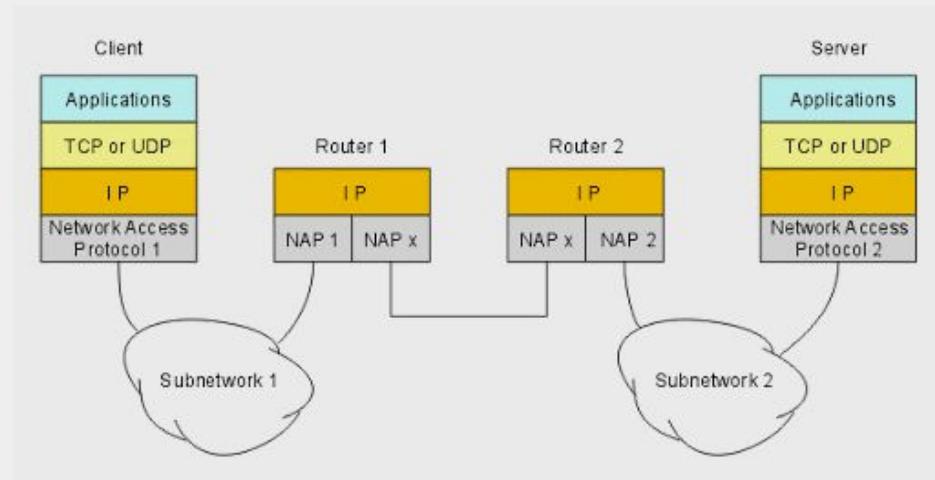
- Routers use routing tables which designate where specific IP Address ranges exist.
- The benefit is to determine which direction the frames must be sent in order to reach their destination.
- Multiple destinations allow for redundancy of delivery if a path should fail.



TCP/IP Routing

Introduction (Continue)

- It is also possible to determine which path is best if there are multiple paths to reach the same destination.
- When one connection fails, the routers can detect the failure and react appropriately to maintain communications.

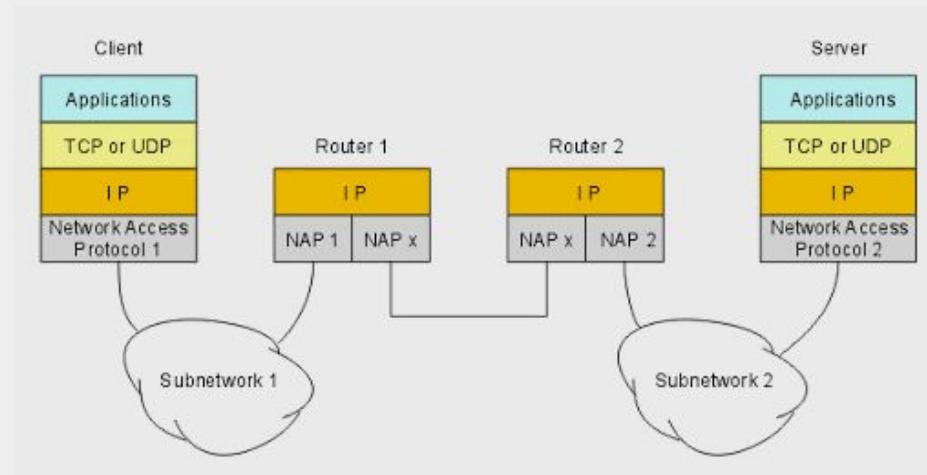


TCP/IP Routing

Introduction (Continue)

There are five basic routing protocols to manage the routers to maintain communications for all the networks.

- Border Gateway Protocol (BGP)
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Interior Gateway Routing Protocol (IGRP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

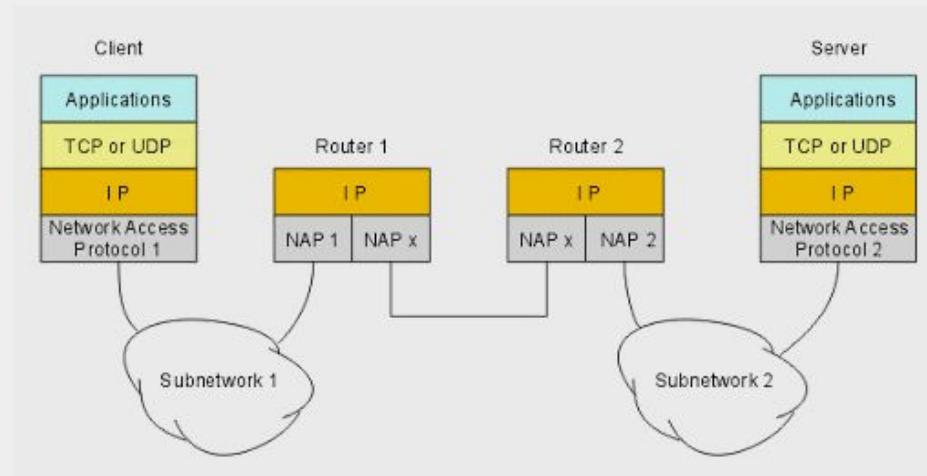


TCP/IP Routing

Protocol Types

Although there are many types of routing protocols, three major classes are in widespread use on IP networks:

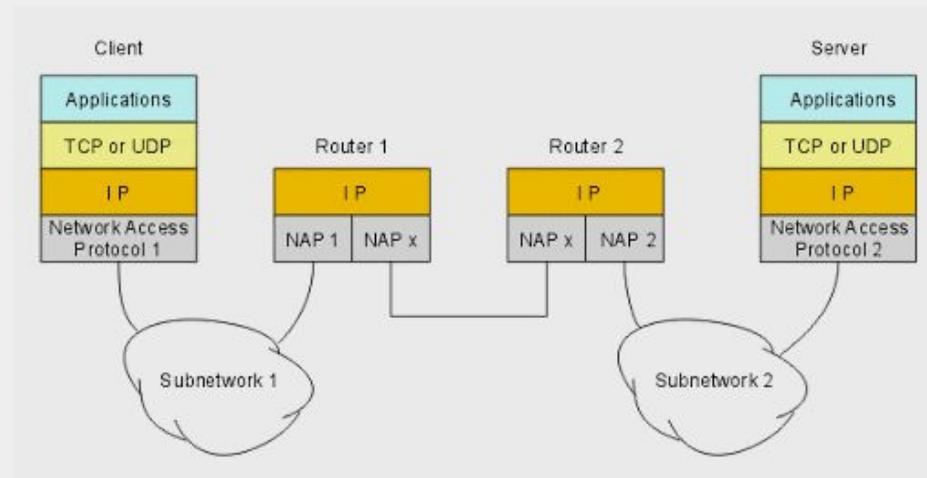
- Interior gateway protocols type 1, link-state routing protocols, such as OSPF and IS-IS



TCP/IP Routing

Protocol Types (Continue)

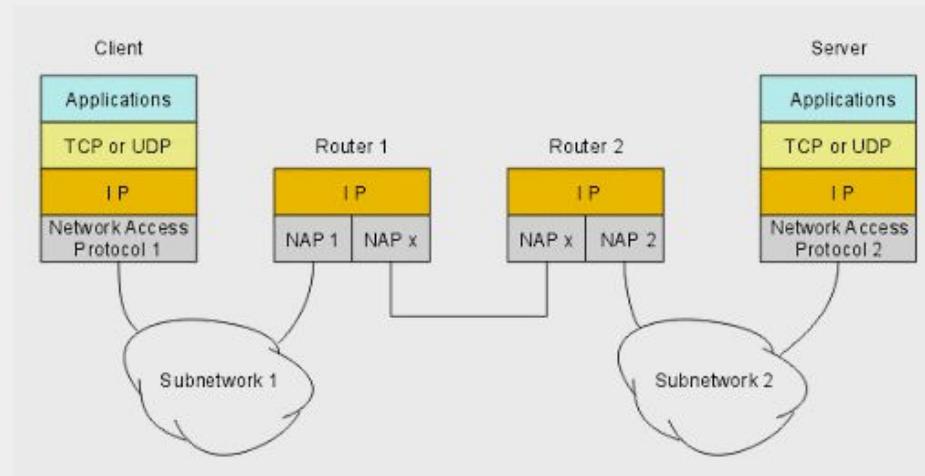
- Interior gateway protocols type 2, distance-vector routing protocols, such as Routing Information Protocol, RIPv2, IGRP.



TCP/IP Routing

Protocol Types (Continue)

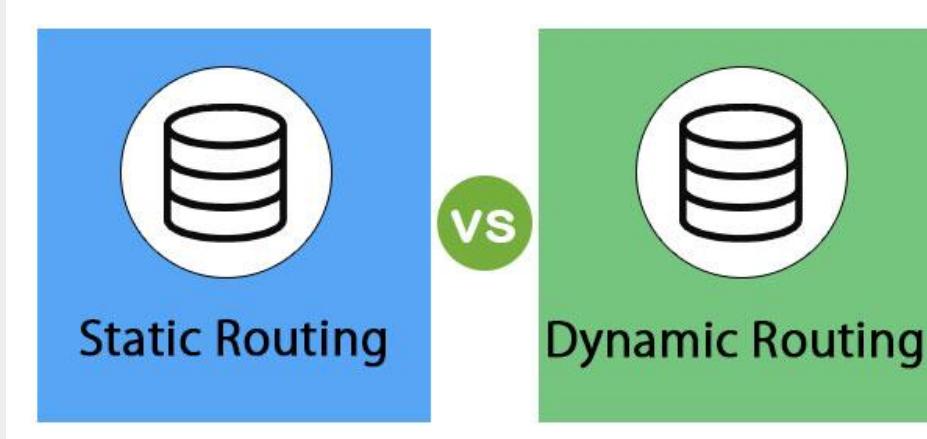
- Exterior gateway protocols are routing protocols used on the Internet for exchanging routing information between Autonomous Systems, such as Border Gateway Protocol (BGP), Path Vector Routing Protocol.
- Exterior gateway protocols should not be confused with Exterior Gateway Protocol (EGP), an obsolete routing protocol.



TCP/IP Routing

Static and Dynamic Routing

- In TCP/IP, routing can be one of two types: static or dynamic.
- With static routing, you maintain the routing table manually using the route command.
- Static routing is practical for a single network communicating with one or two other networks.



TCP/IP Routing

Static and Dynamic Routing (Continue)

- With dynamic routing, daemons update the routing table automatically.
- Routing daemons continuously receive information broadcast by other routing daemons, and so continuously update the routing table.

Static  Dynamic
Route Route

TCP/IP Routing

Static and Dynamic Routing (Continue)

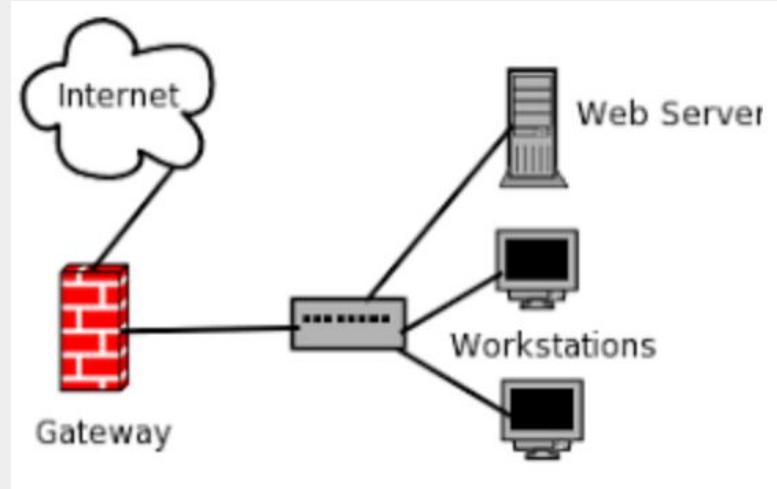
- These two types of routing can be used not only for gateways, but for other hosts on a network as well.
- Static routing works the same for gateways as for other hosts.
- Dynamic routing daemons, however, must be run in the passive (quiet) mode when run on a host that is not a gateway.

Static  Dynamic
Route Route

TCP/IP Routing

Gateways

- Gateways are a type of router.
- Gateways, however, route at the network level.
- Gateways receive IP datagrams from other gateways for delivery to hosts on the local network, and route IP datagrams from one network to another.



TCP/IP Routing

Gateways (Continue)

- To pass on information, the gateway receives datagrams through one network interface and sends them out through the other network interface.
- Gateways periodically verify their network connections through interface status messages.



TCP/IP Routing

Gateways (Continue)

- Gateways route packets according to the destination network, not according to the destination host.
- That is, a gateway machine is not required to keep track of every possible host destination for a packet.
- Instead, a gateway routes packets according to the network of the destination host.

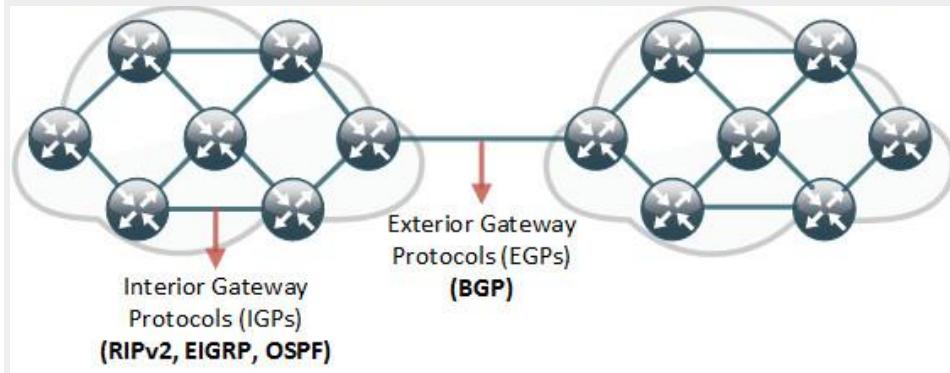


TCP/IP Routing

Gateways (Continue)

Interior Gateways

- Interior gateways are gateways that belong to the same autonomous system. They communicate with each other using the RIP, RIPng, OSPF, HELLO

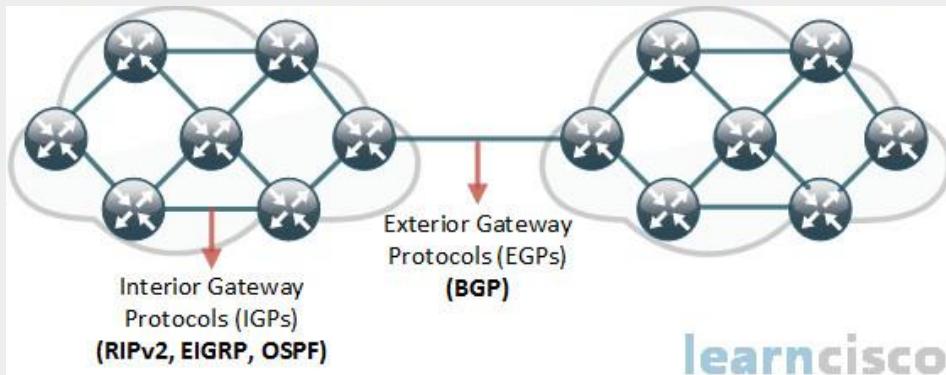


TCP/IP Routing

Gateways (Continue)

Exterior Gateways

- Exterior gateways belong to different autonomous systems. They use the Exterior Gateway Protocol (EGP), the Border Gateway Protocol (BGP), or BGP4+.



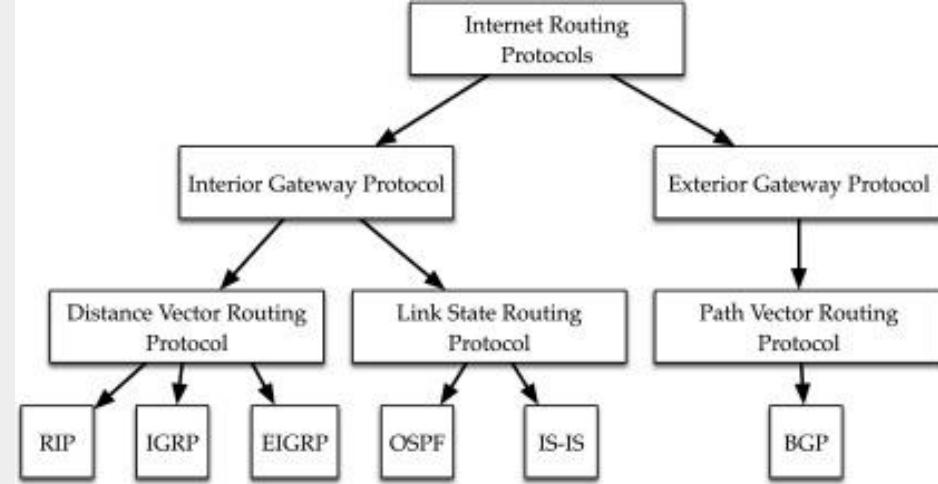
learnCisco

TCP/IP Routing

Gateway Protocols

HELLO Protocol (HELLO)

- HELLO is one protocol that the interior gateways use to communicate among themselves. HELLO calculates the shortest path to other networks by determining the path that has the least delay time.

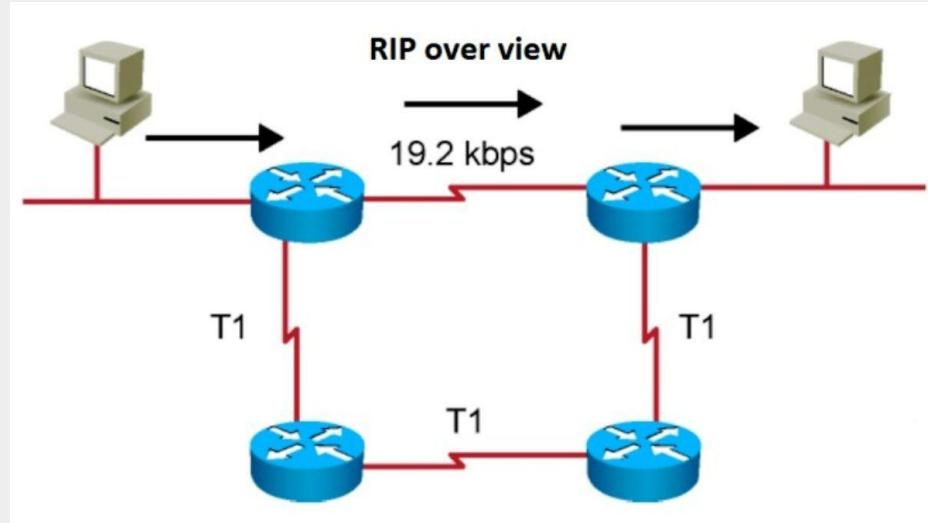


TCP/IP Routing

Gateway Protocols (Continue)

Routing Information Protocol (RIP)

- Routing Information Protocol is a protocol that the interior gateways use to communicate among themselves.
- Like the HELLO Protocol, RIP calculates the shortest path to other networks.
- Unlike HELLO, RIP estimates distance not by delay time, but by hop counts.

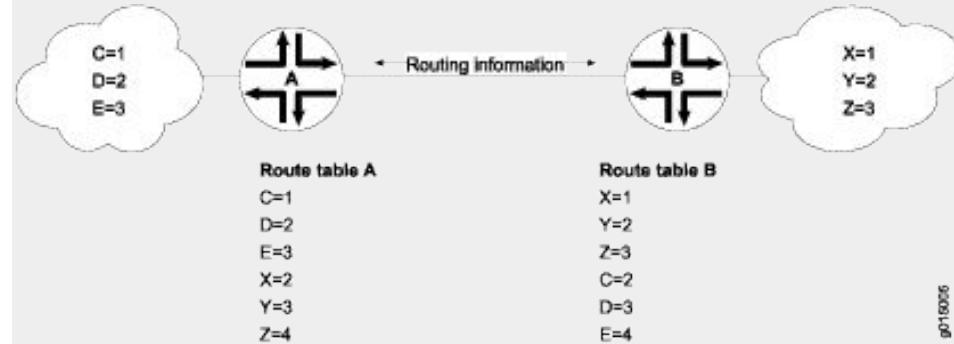


TCP/IP Routing

Gateway Protocols (Continue)

Routing Information Protocol Next Generation

- RIPng is the RIP protocol that is enhanced to support IPv6.

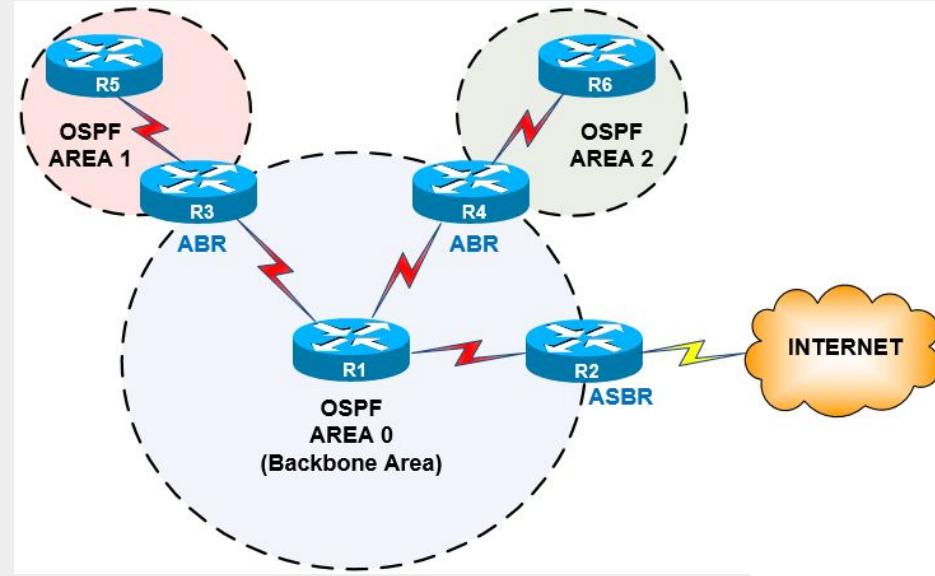


TCP/IP Routing

Gateway Protocols (Continue)

Open Shortest Path First (OSPF)

- OSPF is a protocol that the interior gateways use to communicate among themselves.
- It is a link-state protocol that is better suited than RIP for complex networks with many routers.
- It provides equal cost multipath routing.



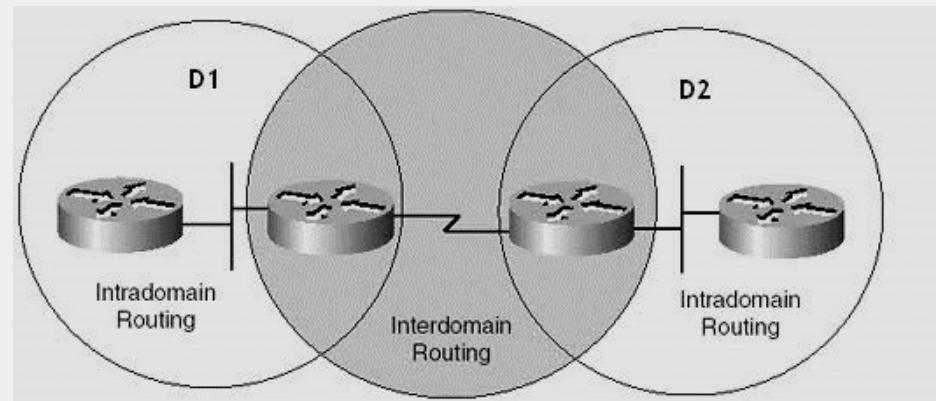
<https://www.firewall.cx/images/stories/ospf-operation-basic-advanced-concepts-ospf-areas-roles-theory-overview1.png>

TCP/IP Routing

Gateway Protocols (Continue)

Exterior Gateway Protocol (EGP)

- The exterior gateways can use the Exterior Gateway Protocol to communicate among themselves.
- The EGP does not calculate the shortest path to other networks.
- Instead, it merely indicates whether a particular network is reachable or not.

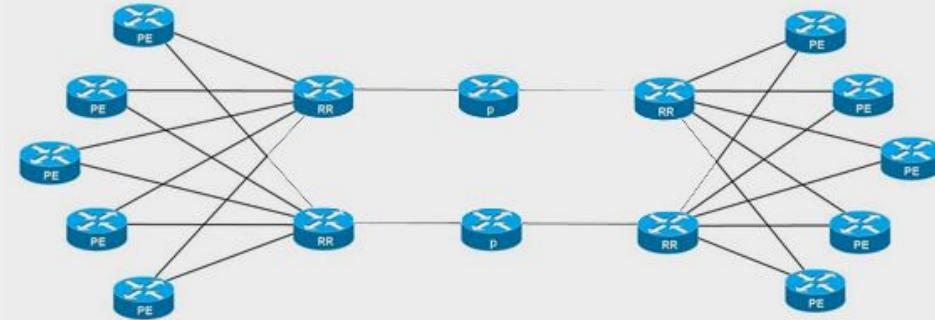


TCP/IP Routing

Gateway Protocols (Continue)

Border Gateway Protocol (BGP)

- The exterior gateways can use this protocol to communicate among themselves.
- It exchanges reachability information between autonomous systems providing more capabilities than EGP.
- BGP uses path attributes to provide more information about each route as an aid in selecting the best route.

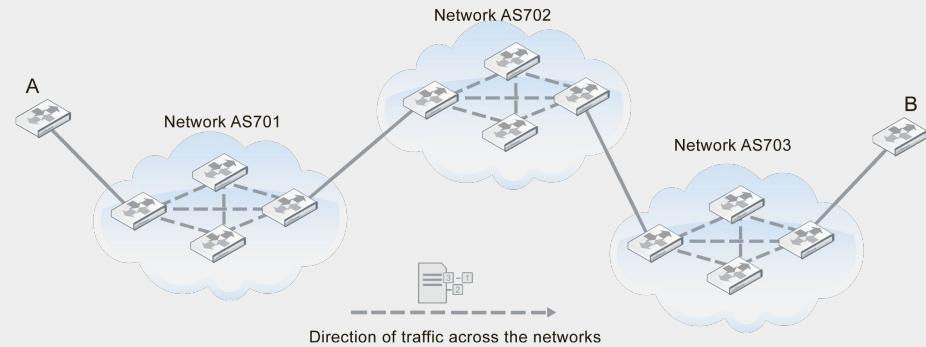


TCP/IP Routing

Gateway Protocols (Continue)

Border Gateway Protocol 4+

- BGP4+ is the BGP protocol version 4, which supports IPv6 and has other enhancements over past versions of the protocol.

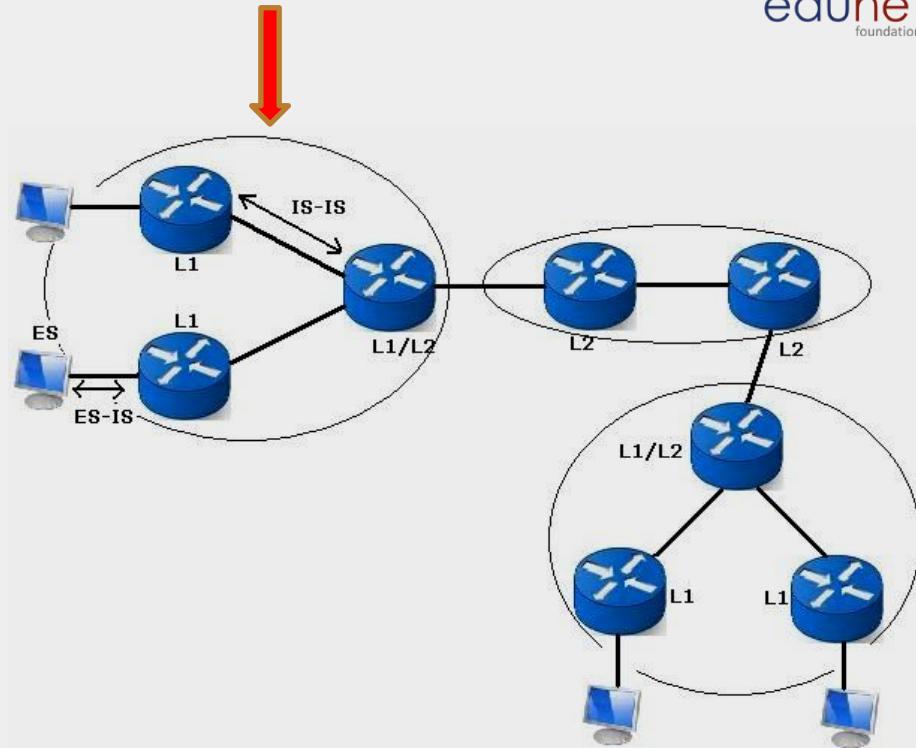


TCP/IP Routing

Gateway Protocols (Continue)

Intermediate System to Intermediate System (IS-IS)

- Interior gateways use IS-IS protocol to communicate among themselves. It is a link-state protocol that can route IP and ISO/CLNP packets and, like OSPF, uses a "shorter path first" algorithm to determine routes.



Able to get familiarize with
internet and E-Commerce
sites

In this section, we will discuss:

- Introduction to Search Engines
- Popular Search engines
- Concept of Favourites Folder
- What is an Electronic Mail
- Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM
- Introduction to video chatting tools
- Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages
- IT Act & Law Introduction to Cyber Security.

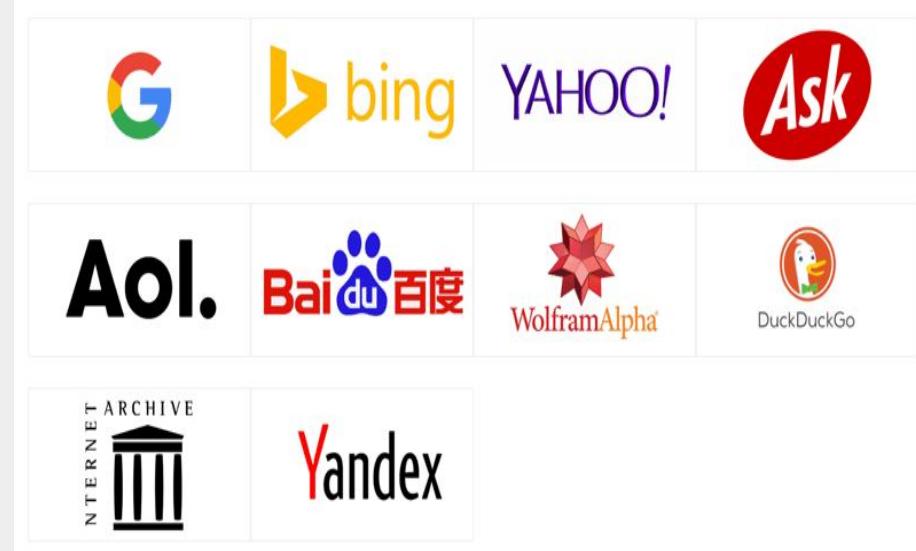
In this section, we will discuss:

- Introduction to Cyber Laws & IT Act.
- Importance of privacy and techniques to manage it.
- Definition of E commerce, Types, scope and benefits of Ecommerce.
- Difference between E commerce and traditional commerce.
- Capabilities requirements and Technology issues for E commerce.
- Types of E commerce web sites.
- Building business on the net.
- Concepts of online Catalogues, Shopping carts, Checkoutpages.
- Payment and Order Processing, Authorization, Chargeback and other payment methods.
- Security issues and payment gateways.

Introduction to Search Engines

Introduction

- Search Engine refers to a huge database of internet resources
- such as web pages, newsgroups, programs, images etc.
- It helps to locate information on World Wide Web.



Introduction to Search Engines

Search Engine Components

Generally there are three basic components of a search engine

- Web Crawler
- Database
- Search Interfaces

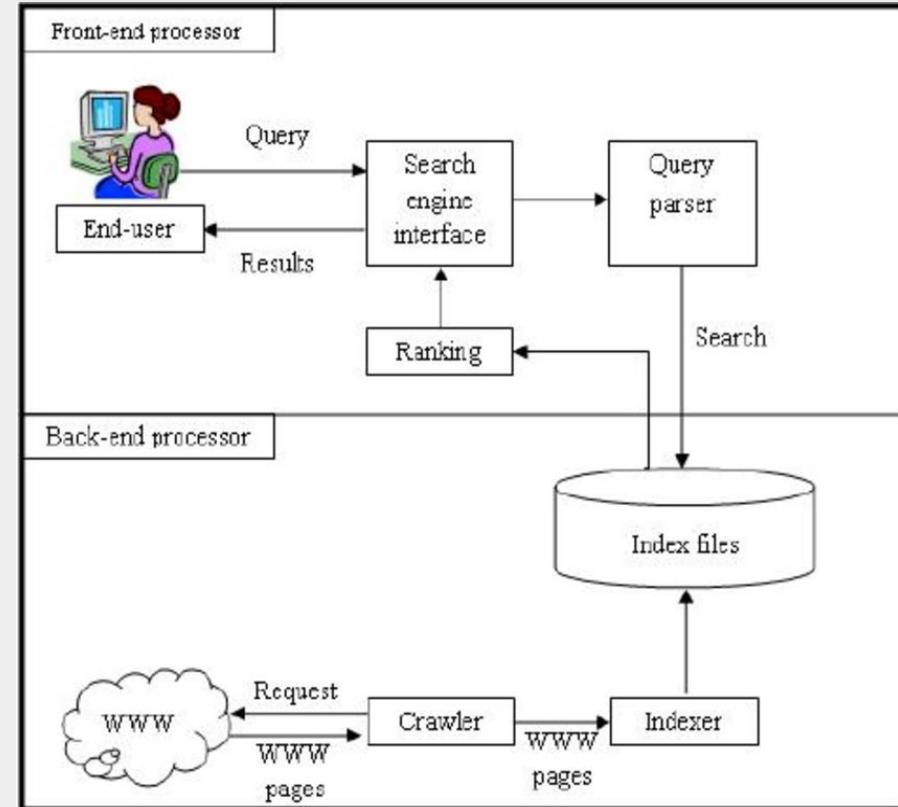


Image Source:

https://www.researchgate.net/figure/Architecture-and-main-components-of-standard-search-engine-model_fig1_220717128

Introduction to Search Engines

Search Engine Components

Web crawler:

- It is also known as spider or bots.
- It is a software component that traverses the web to gather information.

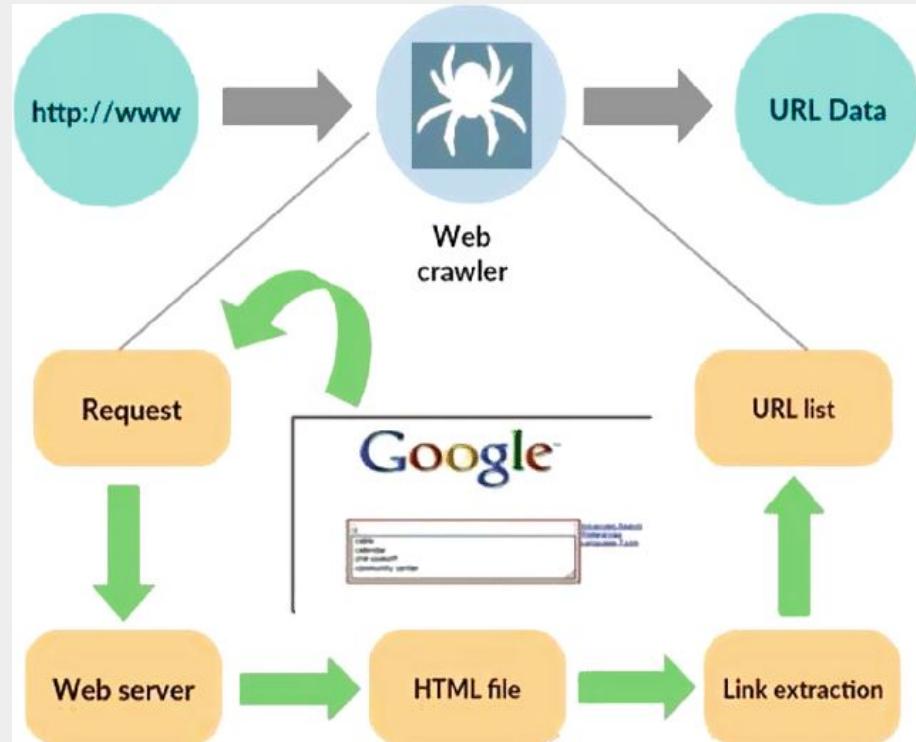


Image Source:

https://www.researchgate.net/figure/Working-model-of-web-crawler_fig1_316089973

Introduction to Search Engines

Search Engine Components

Database

- All the information on the web is stored in database.
- It consists of huge web resources.



Introduction to Search Engines

Search Engine Components

Search Interfaces

- This component is an interface between user and the database.
- It helps the user to search through the database.

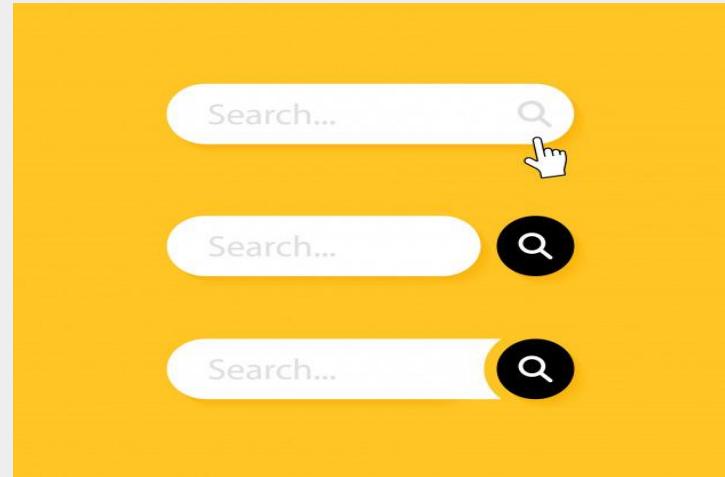


Image Source:

https://www.freepik.com/premium-vector/set-search-bar-web-ui-design-element-web-site-browsers-text-field-search-button_7216994.htm

Introduction to Search Engines

Architecture

The search engine architecture comprises of the three basic layers listed below:

- Content collection and refinement.
- Search core
- User and application interfaces

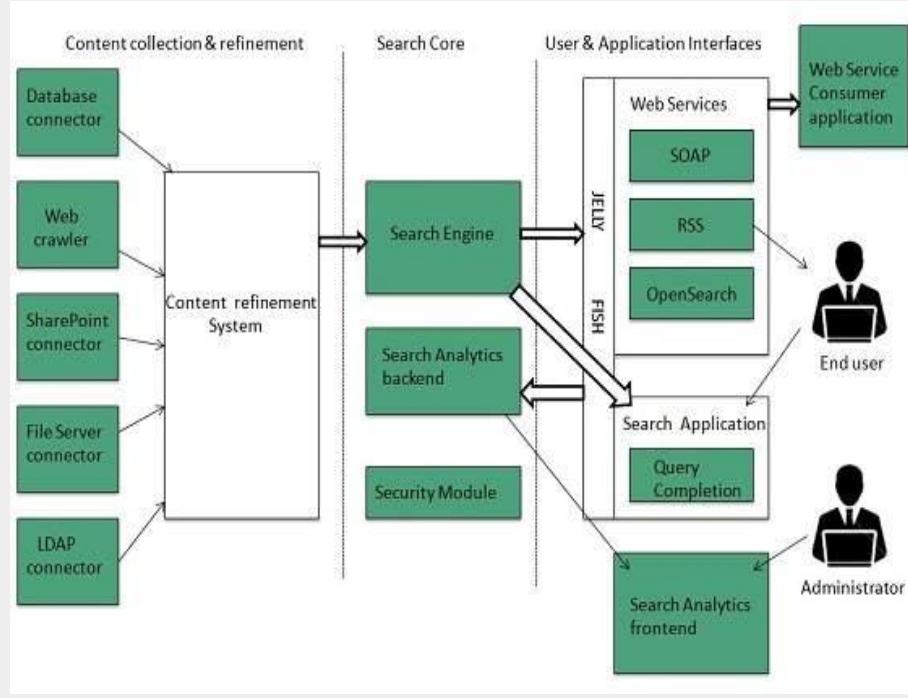


Image Source:

https://www.tutorialspoint.com/internet_technologies/search_engines.htm

Introduction to Search Engines

Search Engine Examples

- Google
- Bing
- Yahoo
- Ask
- DuckDuckGo etc...

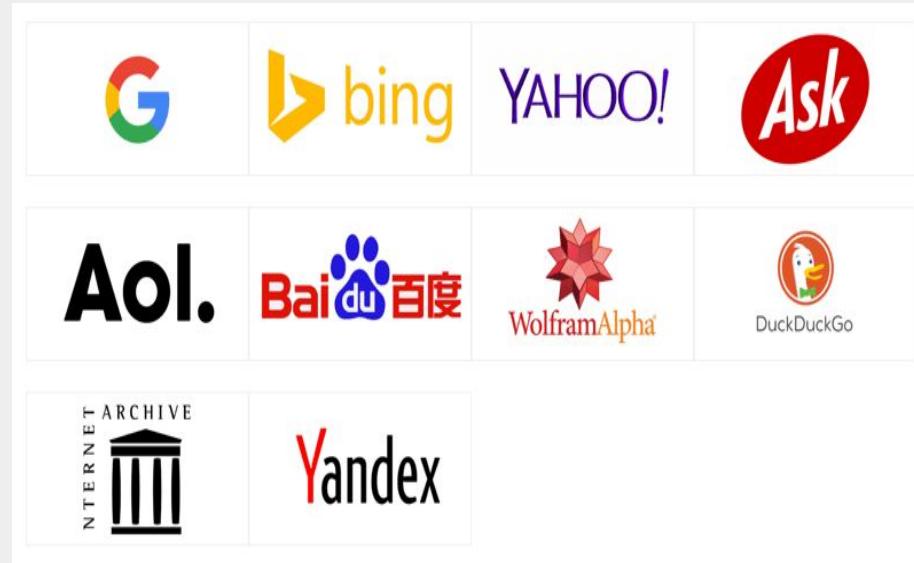


Image Source:

https://www.freepik.com/premium-vector/set-search-bar-web-ui-design-element-web-site-browsers-text-field-search-button_7216994.htm

Popular Search engines

Popular Search engines

- Google is the best search engine with a worldwide market share between 70.83% and 91.98%.
- Bing search market share is between 2.55% and 12.61%
- Yahoo market share is between 1.66% and 2.83%.

Search Engine Market Share Worldwide - April 2020

	NETMARKETSHARE	STATISTA	STATCOUNTER
GOOGLE	70.83%	87.35%	91.98%
BING	12.61%	5.53%	2.55%
BAIDU	11.83%	0.7%	1.44%
YAHOO!	2.30%	2.83%	1.66%
YANDEX	1.41%	0.76%	0.45%
DUCKDUCKGO	0.42%	N/A	N/A

RELIABLESOFT.NET

@RELIABLESOFTNET

Popular Search engines

Popular Search engines

- Baidu has a global market share between 0.7% and 11.83% but it is the most popular search engine in China.
- Yandex, Russia's most popular search engine has a global market share between 0.45% and 1.41%.
- DuckDuckGo market share is around 0.42%.

Search Engine Market Share Worldwide - April 2020

	NETMARKETSHARE	STATISTA	STATCOUNTER
GOOGLE	70.83%	87.35%	91.98%
BING	12.61%	5.53%	2.55%
BAIDU	11.83%	0.7%	1.44%
YAHOO!	2.30%	2.83%	1.66%
YANDEX	1.41%	0.76%	0.45%
DUCKDUCKGO	0.42%	N/A	N/A

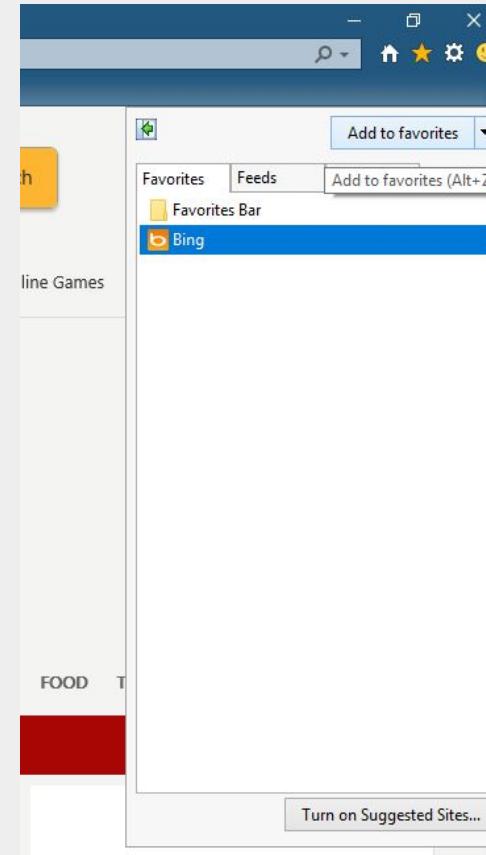
RELIABLESOFT.NET

@RELIABLESOFTNET

Concept of Favourites Folder

Internet Explorer

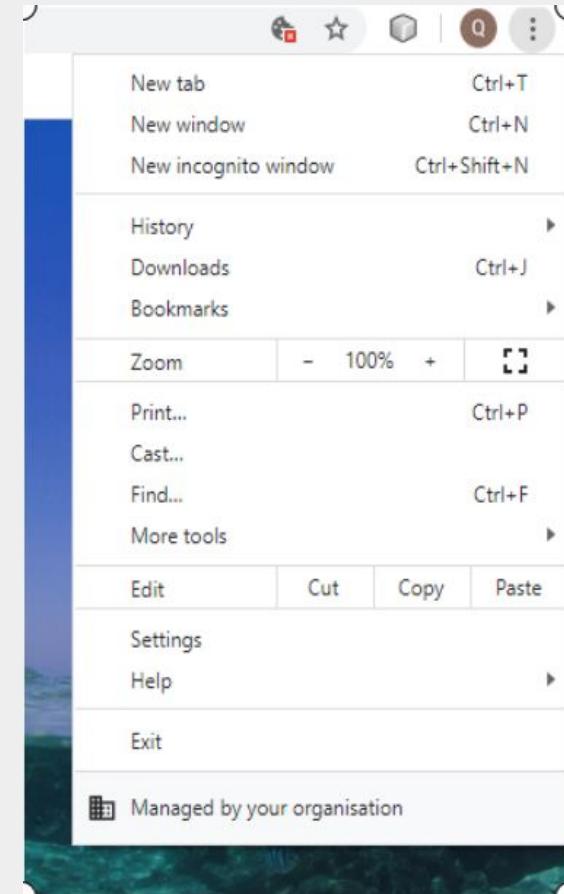
- The web browsers like Firefox have been designed with an option to save webpage addresses in the form of bookmarks.
- internet explorer saves these web pages under the name “favourites”.
- Hence, there is no difference between bookmarks and favourites.



Concept of Favourites Folder

Internet Explorer

- Favourites can be saved and used by the user themselves.
- You can often identify a Favorites folder by a star or heart icon.
- Most applications allow you to simply drag items into the Favorites folder to add them to your favorites.
- While "favorites" may refer to a wide variety of items, the purpose of a favorites folder is always to provide easy access to frequently used items.



What is an Electronic Mail

Definition

- Email is a service which allows us to send the message in electronic mode over the internet.
- It offers an efficient, inexpensive and real time mean of distributing information among people.



What is an Electronic Mail

History

- The first example of email can be found on computers at MIT in a program called “MAILBOX”, all the way back in 1965.
- The system was quite effective, but only if the people wishing to communicate with each other were regularly using the same computer.



What is an Electronic Mail

History continued...

- In 1969, the US Department of Defense implemented ARPANET (Advanced Research Projects Agency Network), a network connecting numerous computers across the department for the purpose of communication within the organisation.
- On October 29th 1969, the first message was sent from computer to computer on ARPANET.
- It looked like this:

29 Oct 69	2100	LOADED	0P. PROG#AM	CSK
		FOR	BEN BARKER	
		BBN		
	2230	TALKED TO SRF		CSK
		HOST TO HOST		
		LEFTTOP IMP PROGRAM	CSK	
		RUNNING AFTER SENDING		
		A HOST DEAD MESSAGE		
		TO IMP.		

Image Source: <https://phrasee.co/a-brief-history-of-email/>

What is an Electronic Mail

History continued...

- It was 1971 when Ray Tomlinson invented and developed electronic mail, as we know it today, by creating ARPANET's networked email system.
- When sending a message from one computer to another within a network, how would one indicate where the message was intended to go?
- Ray Tomlinson had the answer:



What is an Electronic Mail

History continued...

- The “@” symbol, which was probably his most enduring contribution to the internet.
- Indicating a destination for a message became as simple as addressing it: “username@name of computer”, which is essentially how email has been addressed ever since.



What is an Electronic Mail

History continued...

- By 1976 75% of all ARPANET traffic was electronic mail.
- Approx: With over 2.6 billion active users and over 4.6 billion email accounts in operation, email is the most important and widely used communications medium on the internet.



Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM.

Email Addressing

- Each user of email is assigned a unique name for his email account.
- This name is known as E-mail address.
- Different users can send and receive messages according to the e-mail address.
- E-mail is generally of the form `username@domainname`.

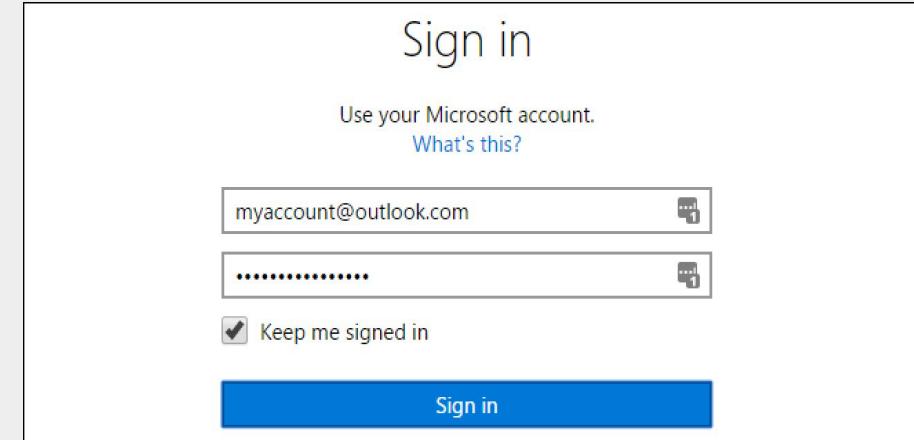


Image Source:

<https://www.howtogeek.com/277170/how-to-change-the-primary-email-address-for-your-microsoft-account/>

Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM.

Email Addressing continued...

- The user name and the domain name are separated by @ (at) symbol.
- E-mail addresses are not case sensitive.
- Spaces are not allowed in e-mail addresses

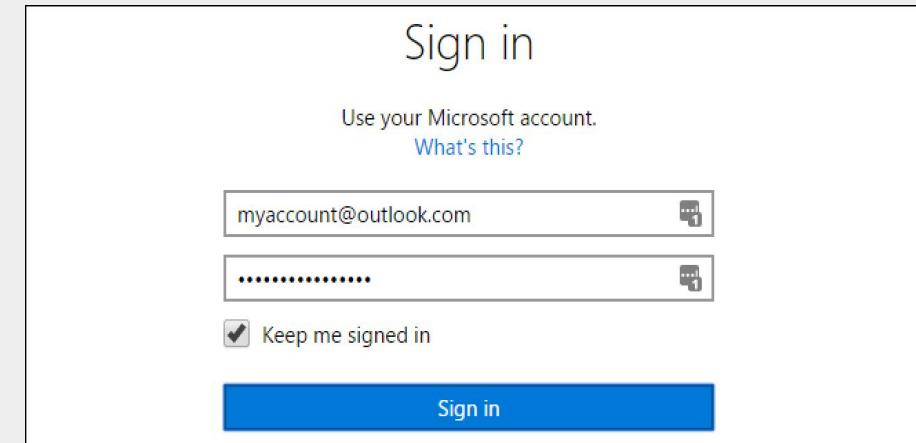


Image Source:

<https://www.howtogeek.com/277170/how-to-change-the-primary-email-address-for-your-microsoft-account/>

Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM.

BCC and CC

- BCC stands for Black Carbon Copy. It is used when we do not want one or more of the recipients to know that someone else was copied on the message.
- CC stands for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.

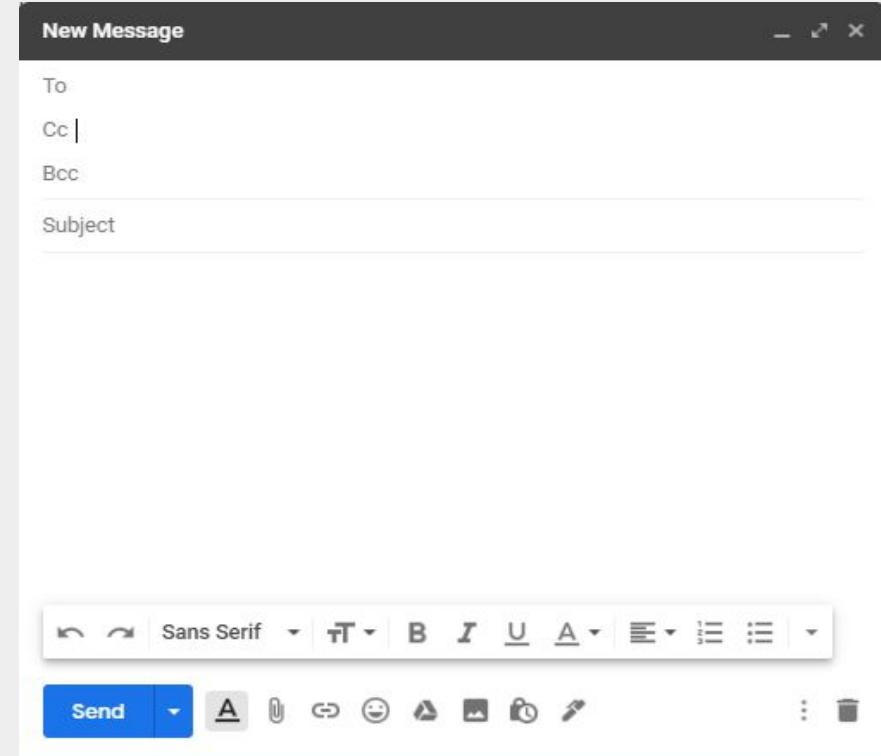


Image Source:

https://www.tutorialspoint.com/internet_technologies/e_mail_overview.htm

Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM.

Inbox

- Inbox is an area where you can see all the received mails.

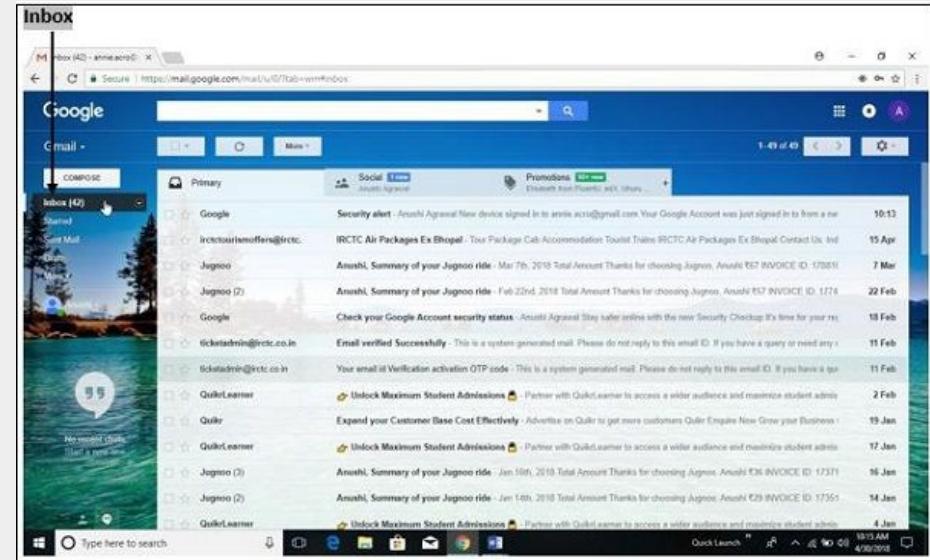


Image Source:

https://www.tutorialspoint.com/computer_concepts/computer_concepts_mailbox_inbox_outbox.htm

Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM.

Outbox

- Outbox is an area where the outgoing messages or messages which are in process of sending or which are failed to send are stored.

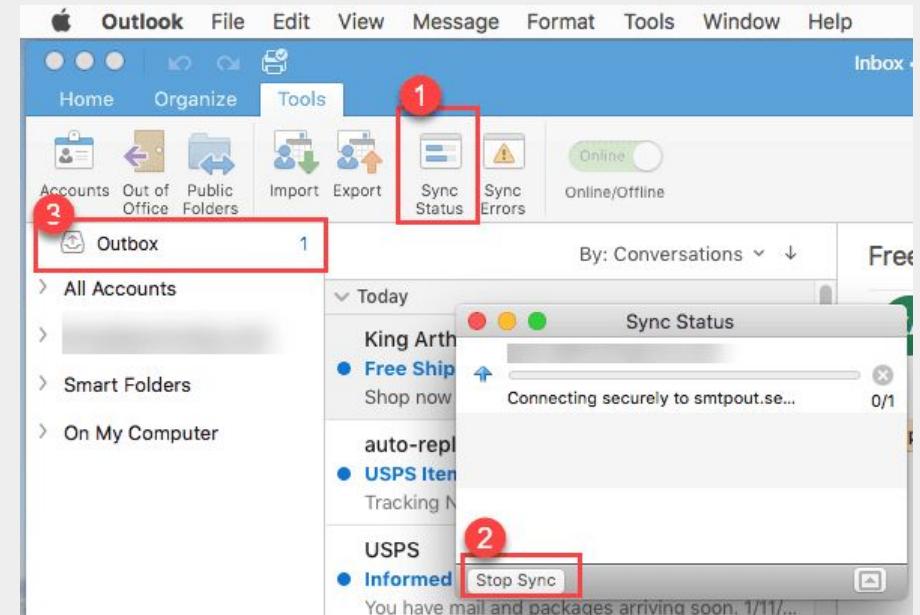


Image Source:

<https://www.slipstick.com/outlook/mac/delete-messages-stuck-outlook-mac-outbox/>

Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM.

Address book

- The Webmail Address Book is a convenient tool for storing the email addresses and other contact information of people you frequently email.
- The Address Book screen displays the Name, Email Address, and Phone number of each contact, that you have added to your address book.

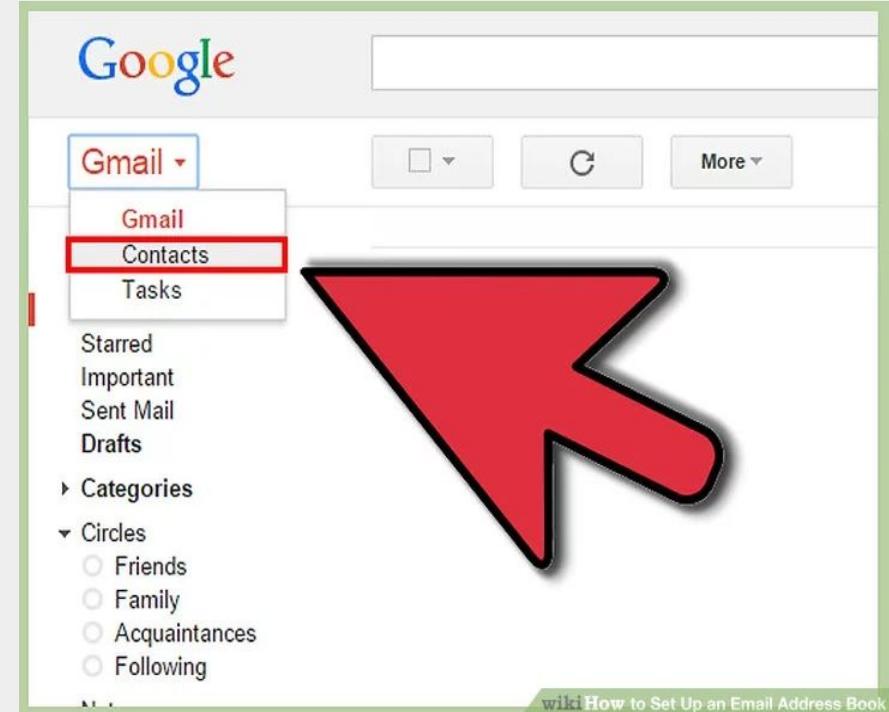


Image Source: <https://www.wikihow.com/Set-Up-an-Email-Address-Book>

Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM.

SPAM

- Email spam, also referred to as junk email, is unsolicited messages sent in bulk by **email (spamming)**.
- The name comes from **Spam** luncheon meat by way of a **Monty Python sketch** in which Spam is ubiquitous, unavoidable, and repetitive

Subject	Sender	Date
U.S. check this out man...	Nelida Romans	Thursday 14.59.37
U.S. Help me!	Oswaldo MANNING	Thursday 12.47.93
U.S. Have Arthritis pains? There is help for you	Orna	Thursday 03.45.36
U.S. down on her, and	Reginald Stubbs	Wednesday 06.02.06
U.S. natural enlargement	diane george	Tuesday 16.37.15
U.S. No Subject	Miran dickhaul	Monday 10.38.58
U.S. only Younger have Shocking sexuality other	Kristie Sapp	Monday 01.07.32
U.S. PedoSex Threat	Ranika kim	06.02.2006 16.27
U.S. PERSONAL	aren0005	06.02.2006 04.56
U.S. We need to render the delight of having the best	Christina Gadnungs	06.02.2006 02.10
U.S. Find more savings online	Breneth draper	06.02.2006 22.30
U.S. faster cheaper meds	Lisa White	06.02.2006 16.37
U.S. Breaking News	Dex H. Edwards	06.02.2006 14.40
U.S. We have your wanted meds at low prices only	Ivana hyatt	04.02.2006 06.59
U.S. 100% cum entaden_ 1079439	Issei Ross	03.02.2006 03.34
U.S. Enjoy your wanted meds	Tracey slams	03.02.2006 02.26
U.S. Custom Your Washington Mutual Online Banking	Washington Mutual On.	03.02.2006 22.03
U.S. PINEAPPLE SYSTEM, MACROMEDIA, SYMANTEC, PC GAMES,	Valerie been	02.02.2006 19.11
U.S. Finished	Cecilia Fuller	02.02.2006 05.57
U.S. You can save more thru ordering meds on our site	mel swick	02.02.2006 01.21
U.S. The most insane action	Katrina Souza	31.01.2006 08.19
U.S. You don't have to be fat... Noel	Koester	28.01.2006 03.22

Introduction to video chatting tools.

Video Chatting Tools

- Video Chat is an online visual, face to face communication performed with other internet users by using a dedicated software and a webcam.
- Skype is the most popular video chat allow users to connect users from different parts of the world.
- A user needs a strong internet connection, computer system, the Skype application.



Image Source: <https://www.skype.com/en/features/group-video-chat/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Introduction to Internet Security

Internet security refers to securing communication over the internet. It includes specific security protocols such as:

- Internet Security Protocol (IPSec)
- Secure Socket Layer (SSL)



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Introduction to Internet Security Cont..

Internet Security Protocol

- It consists of a set of protocols designed by Internet Engineering Task Force (IETF).
- It provides security at network level and helps to create authenticated and confidential packets for IP layer.



Image Source: <https://blog.360totalsecurity.com/en/internet-security-stand-ahead/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Introduction to Internet Security Cont..

Secure Socket Layer (SSL)

- It is a security protocol developed by Netscape Communications Corporation.)
- It provides security at transport layer. It addresses the following security issues: Privacy, Integrity, Authentication.



Image Source: <https://blog.360totalsecurity.com/en/internet-security-stand-ahead/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attacks

- Internet security threats impact the network, data security and other internet connected systems.
 - Cyber criminals have evolved several techniques to threat privacy and integrity of bank accounts, businesses, and organizations.



Image Source

<https://www.globalrailwayreview.com/article/85919/growth-of-big-data-and-cyber-threats/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Following are some of the internet security threats:

- Mobile worms
- Malware
- PC and Mobile ransomware
- Large scale attacks like Stuxnet that attempts to destroy infrastructure.

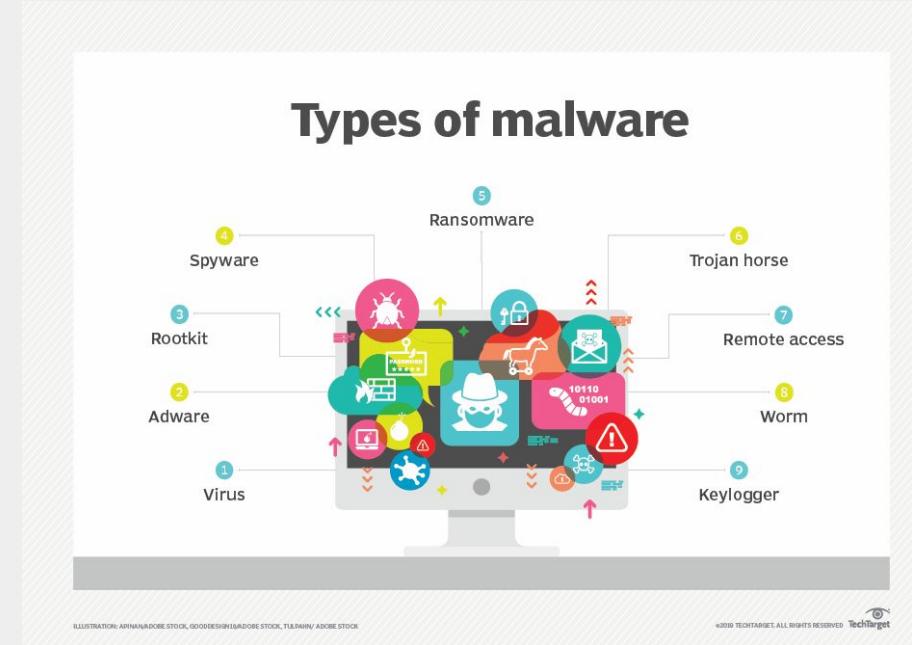


Image Source: <https://searchsecurity.techtarget.com/definition/malware>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Following are some of the internet security threats:

- Hacking as a Service
- Spam
- Phishing



Image Source:

<https://www.globalrailwayreview.com/article/85919/growth-of-big-data-and-cyber-threats/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Attack:

- A cyber-attack is an exploitation of computer systems and networks.
- It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.



Image Source:

<https://www.csionline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Attack:

Cyber-attacks can be classified into the following categories:

- Web based attacks
- System based attacks

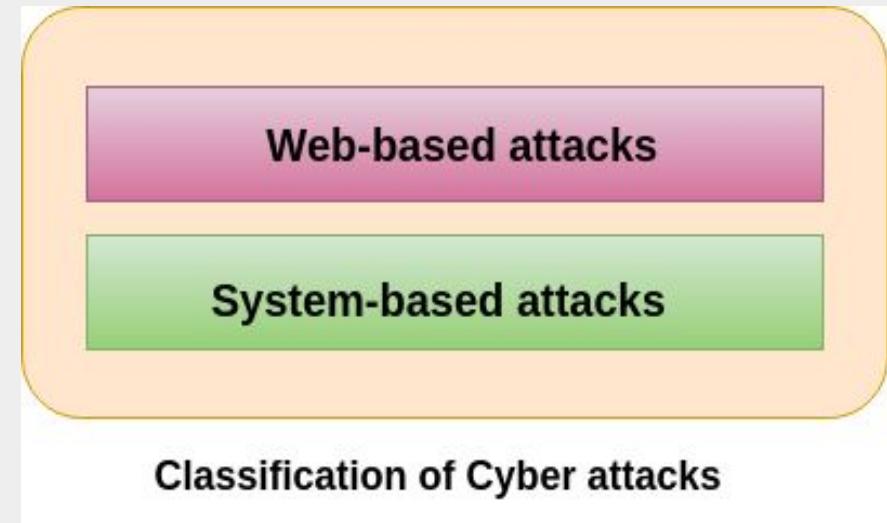


Image Source: <https://www.javatpoint.com/types-of-cyber-attacks>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Web-based attacks:

- These are the attacks which occur on a website or web applications.
- Some of the important web-based attacks are as follows-

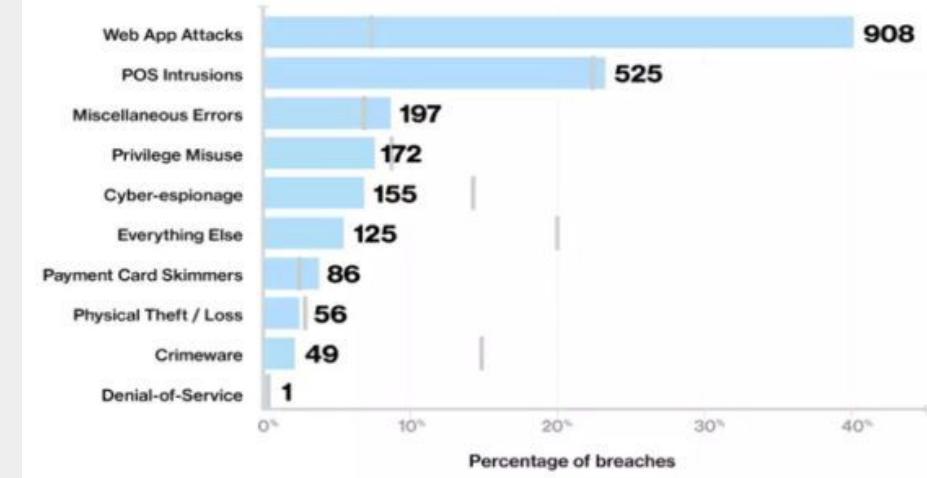


Image Source:

<https://ntrepidcorp.com/cyber-security/web-based-data-breach-law-firms-care/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Injection attacks:

- It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
- Example- SQL Injection, code Injection, log Injection, XML Injection etc.

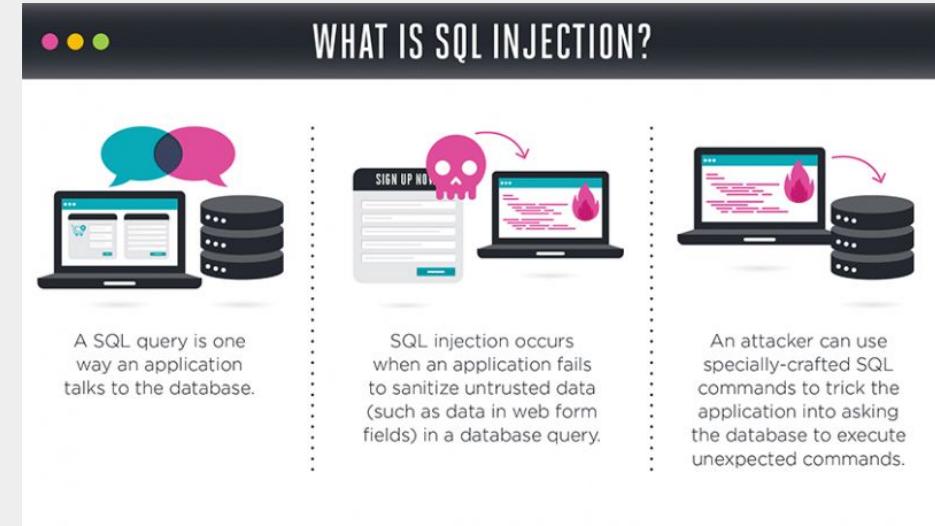


Image Source: <https://www.veracode.com/security/sql-injection>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

DNS Spoofing

- Is a type of computer security hacking.
- Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer.
- The DNS spoofing attacks can go on for a long period of time without being detected.

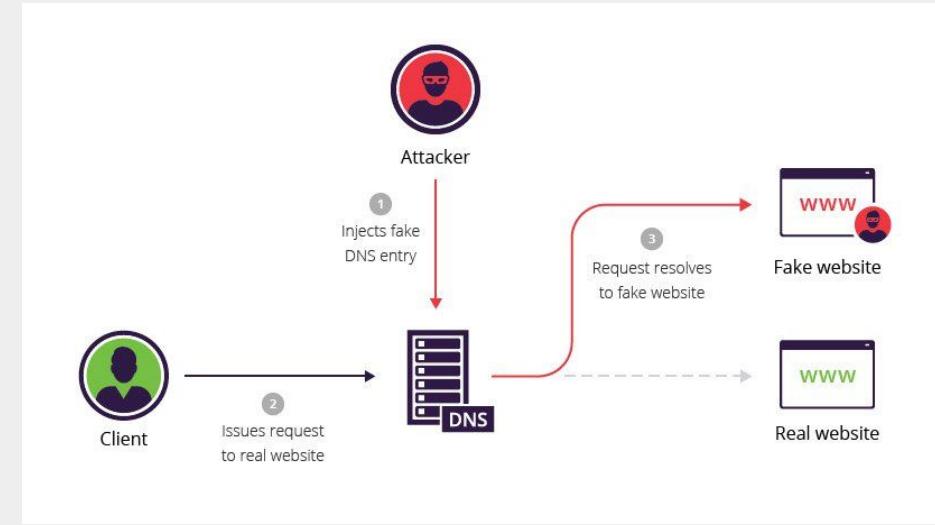


Image Source: <https://www.imperva.com/learn/application-security/dns-spoofing/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Session Hijacking:

- It is a security attack on a user session over a protected network.
- Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.



Image Source: <https://www.geeksforgeeks.org/session-hijacking/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Phishing:

- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number.
- It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.



Image Source:

<https://www.laninfotech.com/phishing-emails-why-theyre-a-threat-how-to-protect-your-business/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Brute force:

- It is a type of attack which uses a trial and error method.
- This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number.

```
[80][http-get-form] host: 192.168.100.155 login: admin password: password
[80][http-get-form] host: 192.168.100.155 login: admin password: p@ssword
[80][http-get-form] host: 192.168.100.155 login: admin password: 12345
[80][http-get-form] host: 192.168.100.155 login: admin password: 1234567890
[80][http-get-form] host: 192.168.100.155 login: admin password: Password
[80][http-get-form] host: 192.168.100.155 login: admin password: 123456
[80][http-get-form] host: 192.168.100.155 login: admin password: 1234567
[80][http-get-form] host: 192.168.100.155 login: admin password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155 login: admin password: 123
[80][http-get-form] host: 192.168.100.155 login: admin password: 1
[80][http-get-form] host: 192.168.100.155 login: admin password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Denial of Service:

- It is an attack which meant to make a server or network resource unavailable to the users.
- It accomplishes this by flooding the target with traffic or sending it information that triggers a crash.
- It uses the single system and single internet connection to attack a server.

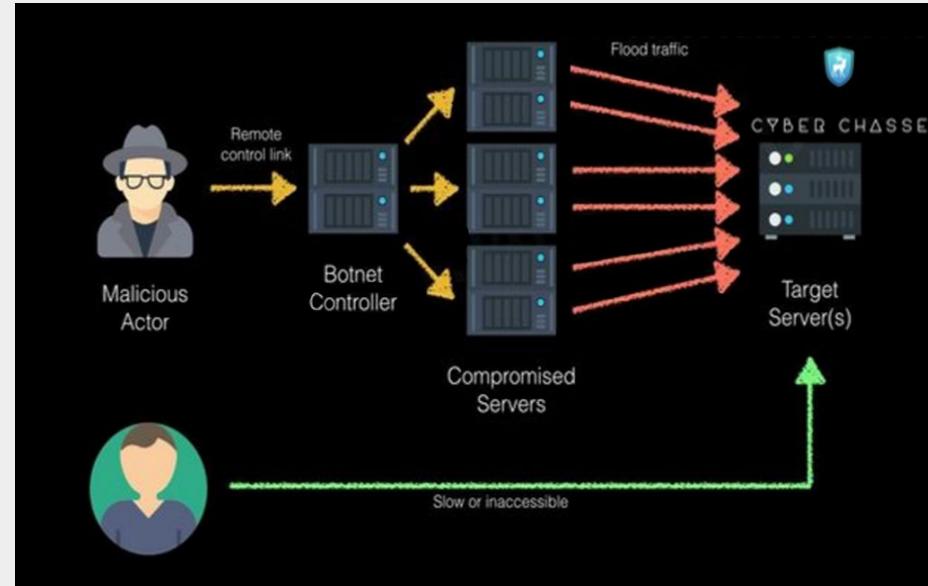


Image Source: <https://cyberchasse.com/denial-of-service-attacks/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

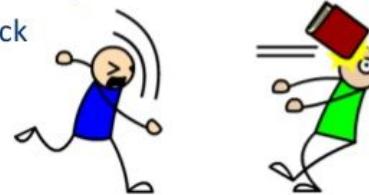
Dictionary attacks:

- This type of attack stored the list of a commonly used password and validated them to get original password.

Dictionary Attacks: Process Overview

Windows Dictionary Attack Process

1. Identify domains
2. Enumerate domain controllers
3. Enumerate domain users
4. Enumerate domain lockout policy
5. Create a dictionary
6. Perform Attack

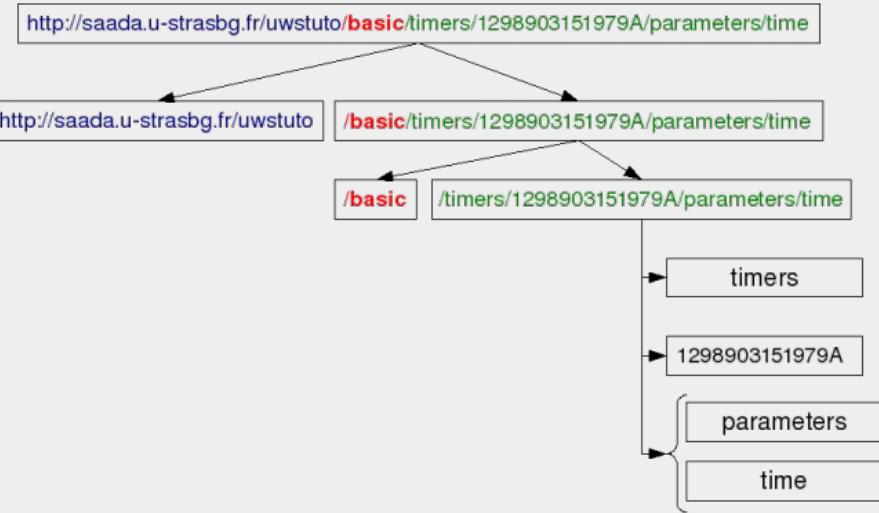


Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

URL Interpretation:

- It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

File Inclusion attacks:

- It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

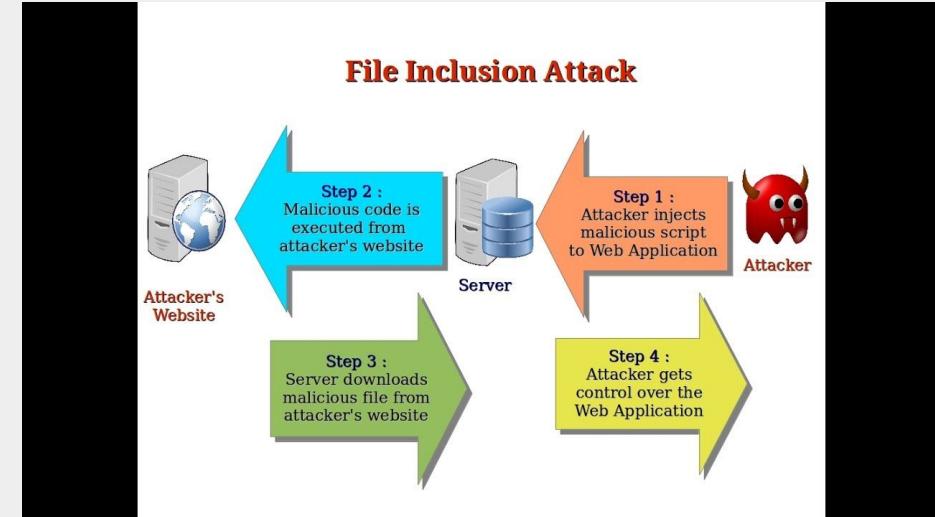


Image Source: <http://iotsecuritynews.com/remote-file-inclusion-local-file-inclusion/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Man in the middle attacks:

- It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

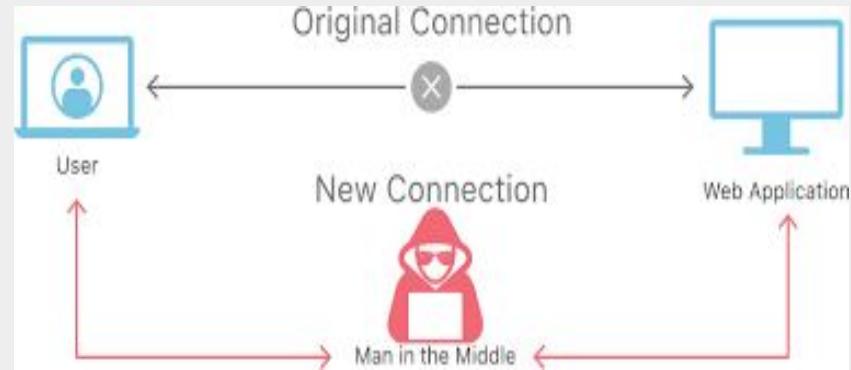


Image Source:

<https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

System-based attacks:

- These are the attacks which are intended to compromise a computer or a computer network.
- Some of the important system-based attacks are as follows-

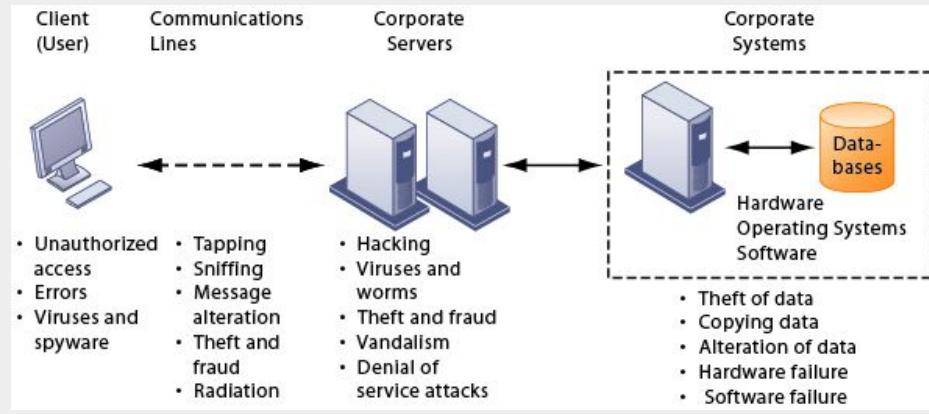


Image Source:

<https://www.globalrailwayreview.com/article/85919/growth-of-big-data-and-cyber-threats/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Virus:

- It is a type of malicious software program that spread throughout the computer files without the knowledge of a user.
- It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed.



Image Source:

<https://www.npr.org/2012/06/02/154188937/flame-sheds-light-on-politics-of-cyberwarfare>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Worm:

- It is a type of malware whose primary function is to replicate itself to spread to uninfected computers.
- It works same as the computer virus.
- Worms often originate from email attachments that appear to be from trusted senders.



Image Source: <https://blog.emsisoft.com/en/28154/computer-worms/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Trojan horse:

- It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent
- It appears to be a normal application but when opened/executed some malicious code will run in the background.



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Backdoors:

- It is a method that bypasses the normal authentication process.
- A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.



Image Source: <https://www.cbronline.com/what-is/what-is-a-backdoor/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Threats and attack Continued

Bots:

- A bot (short for "robot") is an automated process that interacts with other network services.
- Some bots program run automatically, while others only execute commands when they receive specific input.
- Common examples of bots program are the crawler, chatroom bots, and malicious bots.



Image Source:

<https://theconversation.com/beaten-by-bots-training-ai-for-first-person-shooter-games-11176>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types

- Malicious software, commonly known as malware, is any software that brings harm to a computer system.
- Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission.

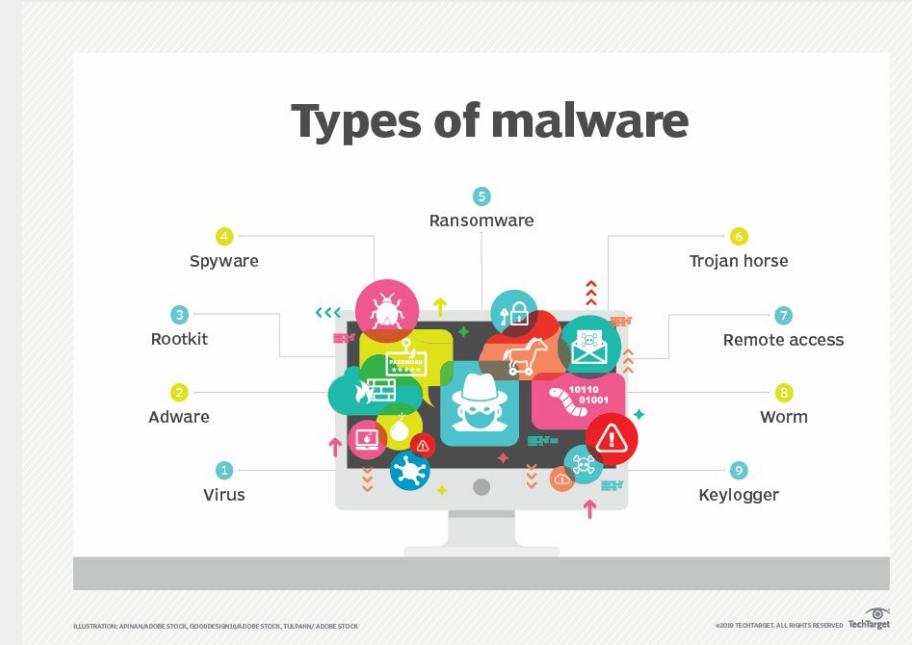
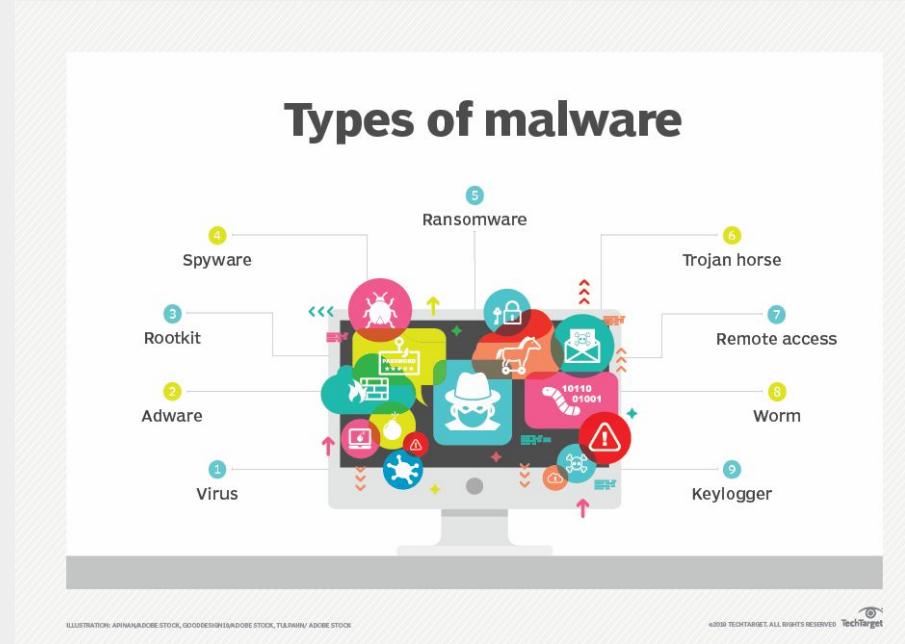


Image Source: <https://searchsecurity.techtarget.com/definition/malware>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

- Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs.



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

Types of Malware:

Viruses :

- A Virus is a malicious executable code attached to another executable file.
- The virus spreads when an infected file is passed from system to system.
- Opening a file can trigger a virus.



Image Source:

<https://www.npr.org/2012/06/02/154188937/flame-sheds-light-on-politics-of-cyberwarfare>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

Worms :

- Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas.
- Worms usually slow down networks.



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

Spyware:

- Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

Trojan horse:

- A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game.



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

Logic Bombs:

- A logic bomb is a malicious program that uses a trigger to activate the malicious code.
- The logic bomb remains non-functioning until that trigger event happens.
- Once triggered, a logic bomb implements a malicious code that causes harm to a computer.

Logic Bombs



- Embedded in some legitimate program
- "Explode" or perform malicious activities when certain conditions are met.



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

Ransomware:

- Ransomware grasps a computer system or the data it contains until the victim makes a payment.
- Ransomware encrypts data in the computer with a key which is unknown to the user.
- The user has to pay a ransom (price) to the criminals to retrieve data.



Image Source:

<https://securityintelligence.com/ransomware-101-what-is-ransomware-and-how-can-you-protect-your-business/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

Backdoors:

- A backdoor bypasses the usual authentication used to access a system.
- The purpose of the backdoor is to grant the cyber criminals future access to the system



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

Rootkits:

- A rootkit modifies the OS to make a backdoor.
- Attackers then use the backdoor to access the computer distantly.
- Most rootkits take advantage of software vulnerabilities to modify system files.

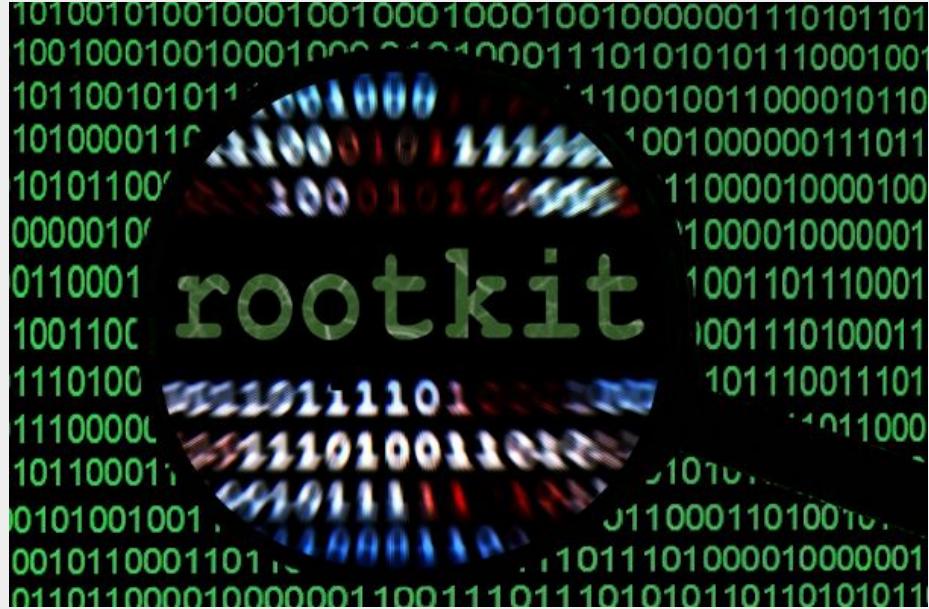


Image Source:

<https://www.pandasecurity.com/mediacenter/security/rootkits-the-invisible-threat-2/>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Malicious Software types cont..

Keyloggers:

- Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.



Image Source: <https://www.keylogger.org/keylogger.html>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Internet security products and their advantages

Internet Security Products:

- Bitdefender Total Security
- Kaspersky Total Security.
- Norton 360 Deluxe.
- Trend Micro Maximum Security.
- Avast Ultimate



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Internet security products and their advantages Cont...

- Webroot Internet Security Plus.
- ESET Smart Security Premium.
- McAfee Total Protection Multi-Device.
- Bullguard Premium Protection.
- Panda Dome Advanced.



Image Source:

<https://www.indiamart.com/proddetail/antivirus-software-19144772833.html>

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Internet security products and their advantages Cont...

Advantages:

- Protection from viruses and their transmission.
- Block spam and ads.

Benefits of Antivirus

- The key benefit to installing antivirus software is quite simply that it prevents a virus damaging your PC or network.
- Protects your PC or network from viruses and other forms of malware.
- Prevents downtime, i.e. valuable working time could be wasted if you can not access your PC due to a virus infection.
- Protects valuable information on your PC.

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Internet security products and their advantages Cont...

Advantages:

- Defense against hackers and data thieves.
- Ensures protection from removable devices.

Benefits of Antivirus

- The key benefit to installing antivirus software is quite simply that it prevents a virus damaging your PC or network.
- Protects your PC or network from viruses and other forms of malware.
- Prevents downtime, i.e. valuable working time could be wasted if you can not access your PC due to a virus infection.
- Protects valuable information on your PC.

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Internet security products and their advantages Cont...



Advantages:

- Protects your data and files.
- Supercharge your PC.

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Internet security products and their advantages Cont...

Advantages:

- Firewall protection from spyware and phishing attacks.
- Limit the access of websites to enhance web protection



Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages.

Internet security products and their advantages Cont...

Advantages:

- Keeping an eye on kids.
- Protects your password.

Advantages of Antivirus

- Having a good anti-virus program can be the difference between the life and death of your computer. With so many computer viruses in existence, protecting your computer's security should be one of your top priorities. Aside from just stopping viruses, most anti-virus programs have other features, such as firewalls, that will ensure the well-rounded safety and security of your valued computer.



IT Act & Law Introduction to Cyber Security

IT Act & Law

- The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the **Indian Parliament** (No 21 of 2000) notified on 17 October 2000.

IT Act, 2000

- Enacted on 17th May 2000- India is 12th nation in the world to adopt cyber laws
- IT Act is based on Model law on e-commerce adopted by UNCITRAL



IT Act & Law Introduction to Cyber Security

IT Act & Law continued...

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to ₹500,000

Objectives of the IT Act

To provide legal recognition for transactions:-

- ◆ Carried out by means of electronic data interchange, and other means of electronic communication, commonly referred to as "electronic commerce"
- ◆ To facilitate electronic filing of documents with Government agencies and E-Payments
- ◆ To amend the Indian Penal Code, Indian Evidence Act, 1872, the Banker's Books Evidence Act 1891, Reserve Bank of India Act, 1934
- ◆ Aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.

IT Act & Law Introduction to Cyber Security

IT Act & Law continued...

Section	Offence	Penalty
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to ₹100,000

IT Act 2000 Objectives

- ◆ Legal Recognition for E-Commerce
 - Digital Signatures and Regulatory Regime
 - Electronic Documents at par with paper documents
- ◆ E-Governance
 - Electronic Filing of Documents
- ◆ Amend certain Acts
- ◆ Define Civil wrongs, Offences, punishments
 - Investigation, Adjudication
 - Appellate Regime

IT Act & Law Introduction to Cyber Security

IT Act & Law continued...

Section	Offence	Penalty
66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to ₹200,000
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to ₹1,000,000

66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing Images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000

Image Source: https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

IT Act & Law Introduction to Cyber Security

IT Act & Law continued...

Section	Offence	Penalty
67B	Publishing child porn or predating children online	Imprisonment up to five years, or/and with fine up to ₹1,000,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.

India IT Act of 2000 (Information Technology Act)



Image Source:

<https://www.termsfeed.com/blog/india-it-act-of-2000-information-technology-act/>

IT Act & Law Introduction to Cyber Security

Cyber Security

- Cyber security is a potential activity by which information and other communication systems are protected from and/or defended against the unauthorized use or modification or exploitation or even theft.



IT Act & Law Introduction to Cyber Security

Cyber Security

- Likewise, cyber security is a well-designed technique to protect computers, networks, different programs, personal data, etc., from unauthorized access.



Image Source:

https://www.tutorialspoint.com/fundamentals_of_science_and_technology/cyber_crime_and_cyber_security.htm

Introduction to Cyber Laws & IT Act

Information Technology Act

- To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as electronic commerce or E-Commerce. The aim was to use replacements of paper-based methods of communication and storage of information.



Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Fblog.ipleaders.in%2Fwp-content%2Fuploads%2F2017%2F03%2Fcyberlaw1.jpg&imgrefurl=https%3A%2F%2Fblog.ipleaders.in%2Fneed-to-know-cyber-laws-india%2F&tbnid=VQhB59PrV2-RaM&vet=12ahUKEwi4uJyH5bzpAhWs0XMBHUoxDLsQMyEgEuiARD4AQ..i&d=3q2wkp_IUAAM&w=580&h=390&q=Introduction%20to%20Cyber%20Law&ws%20%20%26%20%20Act.&hl=en&ved=2ahUKEwi4uJyH5bzpAhWs0XMBHUoxDLsQMyEgEuiARD4AQ

Introduction to Cyber Laws & IT Act

Information Technology Act

- To facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.



Image Source:

Introduction to Cyber Laws & IT Act

Cyber Security

- Cybersecurity denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the Internet by cyber delinquents.



Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.eccouncil.org%2Fwp-content%2Fuploads%2F2020%2F03%2Fcybersecurity_trends.jpg&imgrefurl=https%3A%2F%2Fblog.eccouncil.org%2Fcybersecurity-trends-in-2020-the-threats-facing-the-industry%2F&tbnid=OLc2kXOpvUsqZM&vet=12ahUKEwjqk-nv6LzpAhUmBrcAHQcdDqwQMygHegUIARCGAg.i&docid=Dlaglf0AYEowaM&w=800&h=500&q=cyber%20security&hl=en&ved=2ahUKEwjqk-nv6LzpAhUmBrcAHQcdDqwQMygHegUIARCGAg

Introduction to Cyber Laws & IT Act

Cyber Security

- ISO 27001 (ISO27001) is the international Cybersecurity Standard that delivers a model for creating, applying, functioning, monitoring, reviewing, preserving, and improving an Information Security Management System.



Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.eccouncil.org%2Fwp-content%2Fuploads%2F2020%2F03%2Fcybersecurity_trends.jpg&imgrefurl=https%3A%2F%2Fblog.eccouncil.org%2Fcybersecurity-trends-in-2020-the-threats-facing-the-industry%2F&tbnid=OLc2kXOpvUsqZM&vet=12ahUKEwjqk-nv6LzpAhUmBrcAHQcdDqwQMygHegUIARCGAg.i&docid=Dlaglf0AYEowaM&w=800&h=500&q=cyber%20security&hl=en&ved=2ahUKEwjqk-nv6LzpAhUmBrcAHQcdDqwQMygHegUIARCGAg

Importance of privacy and techniques to manage it

List of techniques on Importance of Privacy

- Limit on Power
 - Respect for Individuals
 - Reputation Management
 - Maintaining Appropriate Social Boundaries
 - Trust



Image Source:

https://www.google.com/url?sa=i&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwjT_sygh73pAhXFgeYKhdsiDDcQjRx6BAgBEAQ&url=https%3A%2F%2Falcoytoday.com%2Fprivacy-policy-2%2F&pssig=AOvVaw0o9kKSNSlIStkR8a4whU_G&ust=1589879080987339

Importance of privacy and techniques to manage it

List of techniques on Importance of Privacy

- **Limit on Power:** Privacy is a limit on government power, as well as the power of private sector companies. The more someone knows about us, the more power they can have over us. Personal data is used to make very important decisions in our lives.



Image Source:

https://www.google.com/url?sa=i&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwjT_sygh73pAhXFgeYKHdsiDDCqJRx6BAgBEAQ&url=https%3A%2F%2Falcoytoday.com%2Fprivacy-policy-2%2F&pssig=AOvVaw0o9kKSnsIISTkR8a4whUG&ust=1588979080987339

Importance of privacy and techniques to manage it

List of techniques on Importance of Privacy

- **Respect for Individuals:** Privacy is about respecting individuals. If a person has a reasonable desire to keep something private, it is disrespectful to ignore that person's wishes without a compelling reason to do so.



Image Source:

https://www.google.com/url?sa=i&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwjT_sygh73pAhXFgeYKhdsiDDCqJRx6BAgBEAQ&url=https%3A%2F%2Falcoytoday.com%2Fprivacy-policy-2%2F&pssig=AOvVaw0o9kKSNsIISTkR8a4whUG&ust=1589879080987339

Importance of privacy and techniques to manage it

List of techniques on Importance of Privacy

- **Reputation Management:** Privacy enables people to manage their reputations. How we are judged by others affects our opportunities, friendships, and overall well-being. Although we can't have complete control over our reputations, we must have some ability to protect our reputations from being unfairly harmed.



Image Source:

[https://www.google.com/url?sa=i&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwjT_sygh73pAhXFgeYKHdsiDDCqJRx6BAgBEAQ&url=https%3A%2F%2falcoytoday.com%2Fprivacy-policy-2%2F&pssig=AOvVaw0o9kKSnsIISTkR8a4whUG&ust=1589879080987339](https://www.google.com/url?sa=i&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwjT_sygh73pAhXFgeYKHdsiDDCqJRx6BAgBEAQ&url=https%3A%2F%2Falcoytoday.com%2Fprivacy-policy-2%2F&pssig=AOvVaw0o9kKSnsIISTkR8a4whUG&ust=1589879080987339)

Importance of privacy and techniques to manage it

List of techniques on Importance of Privacy

- **Maintaining Appropriate Social Boundaries:** People establish boundaries from others in society. These boundaries are both physical and informational. We need places of solitude to retreat to, places where we are free of the gaze of others in order to relax and feel at ease.



Image Source:

https://www.google.com/url?sa=i&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwjT_sygh73pAhXFgeYKhdsiDDCqJRx6BAgBEAQ&url=https%3A%2F%2Falcoytoday.com%2Fprivacy-policy-2%2F&pssig=AOvVaw0o9kKSNsIISTkR8a4whUG&ust=1589879080987339

Importance of privacy and techniques to manage it

List of techniques on Importance of Privacy

- **Trust:** In relationships, whether personal, professional, governmental, or commercial, we depend upon trusting the other party. Breaches of confidentiality are breaches of that trust.



Image Source:

https://www.google.com/url?sa=i&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwjT_sygh73pAhXFgeYKHdsiDDCQjRx6BAGBEAQ&url=https%3A%2F%2Falcoytoday.com%2Fprivacy-policy-2%2F&pssig=AOvVaw0o9kKSNSlIStkR8a4whUG&ust=1589879080987339

E commerce

Definition of E-Commerce

- E-Commerce is also known as electronic commerce is the mode of buying and selling goods and services and transferring funds over an electronic method essentially on the internet. .



Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Ftrellis.co%2Fwp-content%2Fuploads%2F2019%2F02%2FBlog-Post-Banners-3.png&imrefurl=https%3A%2F%2Ftrellis.co%2Fblog%2Fthe-different-types-of-e-commerce%2F&tbnid=Yy4MjgE5gIxVHM&vet=12ahUKEwi09rbt1L3pAhXYBrcAHaZIBp4QMygBegUIARD8AQ.i.&docid=_1crvJpfpkK_rGM&w=700&h=350&q=e-commerce&hl=en&ved=2ahUKEwi09rbt1L3pAhXYBrcAHaZIBp4QMygBegUIARD8AQ

E commerce

Types of E-Commerce

- BUSINESS-TO-BUSINESS (B2B)
- BUSINESS-TO-CONSUMER (B2C)
- CONSUMER-TO-CONSUMER (C2C)
- CONSUMER-TO-BUSINESS (C2B)



Image Source:

[https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.thebalancesmb.com%2Fthmb%2F2-eB0QCqKZmzBBmKBFl0Y2sjh0%3D%2F1500x1000%2Ffilters%3Afill\(auto%2C1\)%2Ftypesofecommerce-5c40fab5c9e77c00019d7029.png&imgrefurl=https%3A%2F%2Fwww.thebalancesmb.com%2Flet-s-ask-the-basic-question-what-is-ecommerce-1141599&tbnid=mFa361trkIXngM&vet=12ahUKEwjJ9oqs1r3pAhXWxXMBHXa0CLkQMygAegUIARD7AQ](https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.thebalancesmb.com%2Fthmb%2F2-eB0QCqKZmzBBmKBFl0Y2sjh0%3D%2F1500x1000%2Ffilters%3Afill(auto%2C1)%2Ftypesofecommerce-5c40fab5c9e77c00019d7029.png&imgrefurl=https%3A%2F%2Fwww.thebalancesmb.com%2Flet-s-ask-the-basic-question-what-is-ecommerce-1141599&tbnid=mFa361trkIXngM&vet=12ahUKEwjJ9oqs1r3pAhXWxXMBHXa0CLkQMygAegUIARD7AQ..i&docid=kd3KuZyQOqP8VM&w=1500&h=1000&q=type%20of%20ecommerce&hl=en&ved=2ahUKEwjJ9oqs1r3pAhXWxXMBHXa0CLkQMygAegUIARD7AQ)

E-commerce

Types of E-Commerce

- **BUSINESS-TO-BUSINESS (B2B):** B2B e-commerce refers to all electronic transactions of goods and sales that are conducted between two companies. This type of e-commerce typically explains the relationship between the producers of a product and the wholesalers who advertise the product for purchase to consumers.



Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Fblog.feedspot.com%2Fwp-content%2Fuploads%2F2016%2F07%2FB2B-Marketing-Philippines.jpg&imgrefurl=https%3A%2F%2Fblog.feedspot.com%2Fb2b-marketing-blogs%2F&tbnid=83zPZW_v6t9aUm&vet=12ahUEwigqJCJ173pAhVbJ7cAHTOEDfwQMyg0egUIARCJAQ..i&docid=DZ-GKoqAlZLC&w=1000&h=679&q=B2B&hl=en&ved=2ahUKEwigqJCJ173pAhVbJ7cAHTOEDfwQMyg0egUIARCJAQ

E commerce

Types of E-Commerce

- **BUSINESS-TO-CONSUMER (B2C):B2C**

e-commerce deals with electronic business relationships between businesses and consumers. Many people enjoy this avenue of e-commerce because it allows them to shop around for the best prices, read customer reviews and often find different products that they wouldn't otherwise be exposed to in the retail world.



Image Source:

https://www.google.com/imgres?imgurl=http%3A%2F%2Fwww.study4business.com%2Fwp-content%2Fuploads%2F2018%2F10%2FAdvantages-and-disadvantages-of-B2C-2.jpg&imgrefurl=http%3A%2F%2Fwww.study4business.com%2Fbusiness%2Fadvantages-and-disadvantages-of-b2c%2F&tbnid=7Z3u8OWXKWfOnM&vet=10CBIQMyhsahcKEwjA3ami2L3pAhUAAAAAHQAAAAAQAg..&docid=ZSrJuyh1lxqm_M&w=890&h=500&q=B2C&hl=en&ved=0CBIQMyhsahcKEwjA3ami2L3pAhUAAAAAHQAAAAAQAg

E commerce

Types of E-Commerce

- **CONSUMER-TO-CONSUMER (C2C):** This level of e-commerce encompasses all electronic transactions that take place between consumers. Generally, these transactions are provided by online platforms (such as PayPal), but often are conducted through the use of social media networks (Facebook marketplace) and websites (Craigslist).

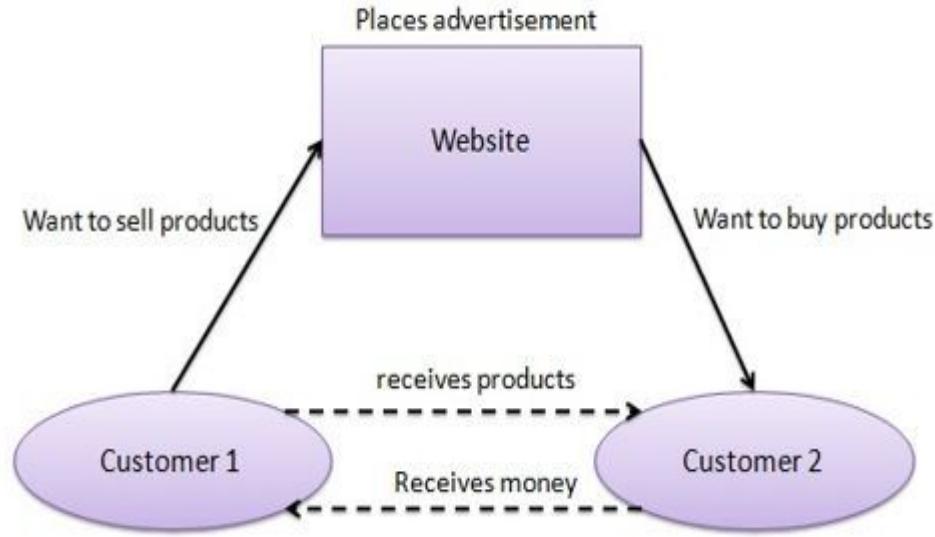


Image Source:

<https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.qsstudy.com%2Fwp-content%2Fuploads%2F2017%2F01%2FC2C-Commerce.jpg&imgrefurl=https%3A%2F%2Fwww.qsstudy.com%2Fbusiness-studies%2Fc2c-commerce&tbnid=mvBptG0wp1w4KM&vet=12ahUKEwjNsKGi2b3pAhXy5jgGHbBhBAcQMyhcegUIARDgAQ..i&docid=QnvMgVbrWlaDRM&w=480&h=250&q=C2C&hl=en&ved=2ahUKEwjNsKGi2b3pAhXy5jgGHbBhBAcQMyhcegUIARDgAQ>

E commerce

Types of E-Commerce

- CONSUMER-TO-BUSINESS (C2B):**
C2B e-commerce is when a consumer makes their services or products available for companies to purchase. An example of this would be a graphic designer customizing a company logo or a photographer taking photos for an e-commerce website.



Consumer - to - Business (C2B)

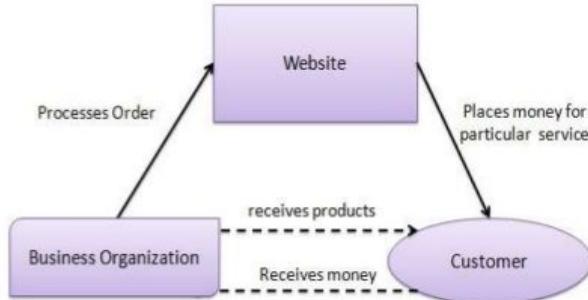


Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Fimage.slidesharecdn.com%2Fecommerce-170318034818%2F95%2Fecommerce-basic-concept-18-638.jpg&imgrefurl=https%3A%2F%2Fstandard.home.blog%2F2018%2F07%2F23%2Fc2b-model%2F&tbnid=O4bxH3sHny8vsM&vet=1ahUKEwiYluOP2r3pAhV6kksFHa9tAoAQMygQegUIARCQAg..i&docid=nI_05_0eW-XNQM&w=638&h=479&q=C2B&hl=en&ved=2ahUKEwiYluOP2r3pAhV6kksFHa9tAoAQMygQegUIARCQAg

E commerce

Scope of E-Commerce

- Reduction in the cost of broadband internet facilities to ensure more people come online.
- Encouraging more domain registrations and letting e-commerce websites maintain them at cheaper rates.
- Encouraging innovative schemes such as the COD (Cash on Delivery) in a country where credit card use is not prominent shows how we have eased into this particular niche.



Image Source:

https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwib3Li73b3pAhW0V3wkHeR-A4AQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.kindpng.com%2Fimgv%2FThRiTJJ_e-business-png-image-background-scop-e-of-e%2F&psig=AOvVaw1-YomRHR8z3E1egxrdo1T&ust=1589902219033436

E commerce

Scope of E-Commerce

- Bringing internet facilities to the rural areas in India as it remains a largely untapped resource and the possibilities are endless for a major boom in the e-commerce industry
- E-commerce can also spread to newer disciplines such as health services in these remote areas in India and help in offering health solutions to people who do not have the luxury of hospitals in their vicinity.



Image Source:

https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwib3Li73b3pAhW0V3wkHeR-A4AQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.kindpng.com%2Fimgv%2FThRiTJJ_e-business-png-image-background-scop-e-of-e%2F&psig=AOvVaw1-YomRHR8z3E1egxrdo1T&ust=1589902219033436

E commerce

Benefits of E-Commerce

- Faster transactions
- Reduces lead time
- Low operational costs
- Increases customer brand loyalty
- Customer self-service
- Easy accessibility to products and services
- 24*7 Marketplace
- No geographical restrictions



Image Source:

<https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.tekshapers.com%2Fassets%2Fckfinder%2Fuserfiles%2Fimages%2Fbenefit%2520of%2520ecommerce.png&imgrefurl=https%3A%2F%2Fwww.tekshapers.com%2Fblog%2F7-Benefits-of-Ecommerce-to-Organization&tbnid=YSSUhGhUNNIBMm&vet=12ahUKEwjawfSa373pAhUi2jgGHYsAB9wQMygBegUIARD4AQ..i&docid=AUi8LMiV3zOrwM&w=783&h=511&q=benefit%20of%20e-commerce&hl=en&ved=2ahUKEwjawfSa373pAhUi2jgGHYsAB9wQMygBegUIARD4AQ>

Difference between E-commerce and traditional commerce.

- E-commerce is the process of exchanging goods and services in the form of digital mode where the payment to the goods and services happens in electronic form.
- Traditional Commerce is the process of exchanging goods and services in the form of money directly. Traditional Commerce involves face to face and in person dealing with all the parties to perform the exchange of goods and services with predefined prices.

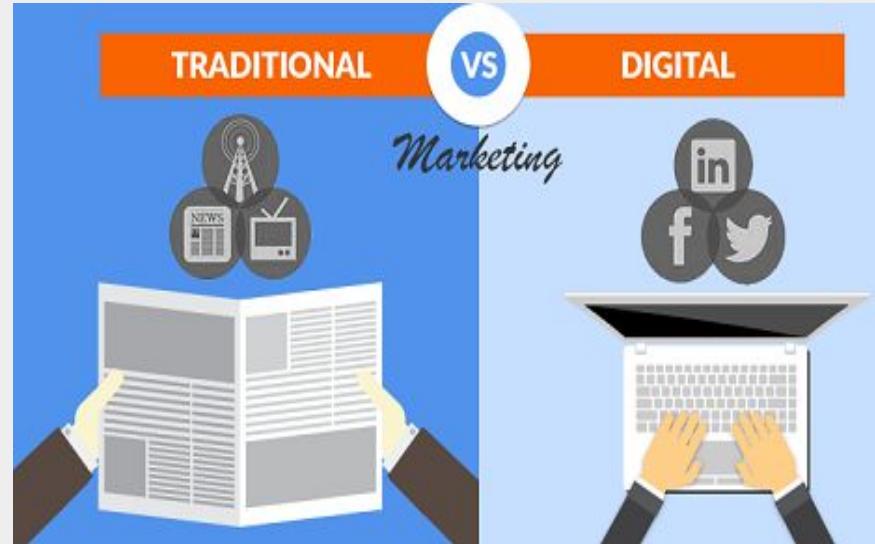


Image Source:
<http://cdn.differencebetween.net/wp-content/uploads/2018/01/Difference-between-Traditional-Commerce-and-Ecommerce.png>

Capabilities requirements and Technology issues for E commerce.

- Find out the market need and try to build the product according to the need.
- Write an effective advertisement copy and promote it in online portals.
- Design a user-friendly website.
- Use SEO services optimize search on your website



Image Source:

https://www.google.com/imgres?imgurl=http%3A%2F%2F1.bp.blogspot.com%2F5XTf7SrgA2A%2FVUzzvz79KsI%2FAAAAAAAAANI%2FZFLtW5OyP3s%2Fs640%2Fe-business-41.jpg&imgrefurl=http%3A%2F%2Ffatma103851.blogspot.com%2F2015%2F05%2Fe-commerce-applications-and-issues.html&tbnid=lc1zndOhUI3QfM&vet=12ahUKEwiquemO473pAhWJVisKHSLS5AmYQMygHegUIARD5AQ.i&docid=jRUVv3XJKo_G7M&w=600&h=354&q=%20Technology%20issues%20or%20E%20commerce.&hl=en&ved=2ahUKEwiquemO473pAhWJVisKHSLS5AmYQMygHegUIARD5AQ

Capabilities requirements and Technology issues for E commerce.

- Use upselling and cross-selling methods
- Gather referrals from friends, families, relatives, institutions, and strangers
- Create testimonials from happy customers
- Participate in industry meetings
- Publish blogs on the product and services



Image Source:

https://www.google.com/imgres?imgurl=http%3A%2F%2F1.bp.blogspot.com%2F5XTf7SrgA2A%2FVUzzvz79KsI%2FAAAAAAAAANI%2FZFLtW5OyP3s%2Fs640%2Fe-business-41.jpg&imgrefurl=http%3A%2F%2Ffatma103851.blogspot.com%2F2015%2F05%2Fe-commerce-applications-and-issues.html&tbnid=lc1zndOhUI3QfM&vet=12ahUKEwiquemO473pAhWJVisKHSLS5AmYQMygHegUIARD5AQ.i&docid=jRUVv3XJKo_G7M&w=600&h=354&q=%20Technology%20issues%20or%20E%20commerce.&hl=en&ved=2ahUKEwiquemO473pAhWJVisKHSLS5AmYQMygHegUIARD5AQ

Types of E commerce web sites

- Business-to-Business (B2B): Electronic transactions of goods and services between companies.
Example: A business sells SAS products to other businesses.
- Business-to-Consumer (B2C): Electronic transactions of goods and services between companies and consumers. Example: You buy a new t-shirt from an online store.

Top 7 E-commerce Websites in India



GoodWorkLabs
Technology Superstars

Image Source:

<https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwifjbK-5r3pAhWd6XMBHdJsBA8QjRx6BAgBEAQ&url=https%3A%2F%2Fwww.goodworklabs.com%2Ftop-five-e-commerce-websites-in-india%2F&psig=AOvVaw2umLC7HUNJMkA23WiidRBc&ust=1589904644218299>

Types of E commerce web sites

- Consumer-to-Consumer (C2C): Electronic transactions of goods and services between consumers, mostly through a third party. Example: You sell your old smartphone on eBay or Olx to another consumer.
- Consumer-to-Business (C2B): Electronic transactions of goods and services where individuals offer products or services to companies. Example: A Social media influencer offers exposure to their online audience in exchange for a fee.

Top 7 E-commerce Websites in India



GoodWorkLabs
Technology Superstars

Image Source:

<https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwifjbK-5r3pAhWd6XMBHdJsBA8QjRx6BAgBEAQ&url=https%3A%2F%2Fwww.goodworklabs.com%2Ftop-five-e-commerce-websites-in-india%2F&psig=AOvVaw2umLC7HUNJMkA23WiidRBC&ust=1589904644218299>

Building business on the net.

Start a business that fills a need

- Visit online forums to see what questions people ask and what problems they're trying to solve.
- Do keyword research to find keywords that a lot of people are searching, but don't have a ton of competition with other sites.
- Check out your potential competitors by visiting their sites and taking note of what they're doing to fill the demand. Then you can use what you've learned and create a product for a market that already exists -- and do it better than the competition.



Image Source:

https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwiJ7bvN7r3pAhV4jgGHbfSBkwQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.freepik.com%2Fpremium-vector%2Fpeople-are-building-business-internet_5570947.htm&psig=AOvVaw3CNQwbi7G_8Fv8OUDa0iDI&ust=1589906782909327

Building business on the net.

Write copy that sells

- Arouse interest with a compelling headline.
- Describe the problem your product solves.
- Establish your credibility as a solver of this problem.
- Add testimonials from people who have used your product.
- Talk about the product and how it benefits the user.
- Make an offer.
- Make a strong guarantee.
- Create urgency.
- Ask for the sale.



Image Source:

https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwiJ7bvN7r3pAhVk4jgGHbfSBkwQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.freepik.com%2Fpremium-vector%2Fpeople-are-building-business-internet_5570947.htm&psig=AOvVaw3CNQwbi7G_8Fv8OUdA0iDI&ust=1589906782909327

Building business on the net

Design and build your website

- Choose one or two plain fonts on a white background.
- Make your navigation clear and simple, and the same on every page.
- Only use graphics, audio or video if they enhance your message.
- Include an opt-in offer so you can collect e-mail addresses.
- Make it easy to buy -- no more than two clicks between potential customer and checkout.
- Your website is your online storefront, so make it customer-friendly.



Image Source:

https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwiJ7bvN7r3pAhV4jgGHbfSBkwQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.freepik.com%2Fpremium-vector%2Fpeople-are-building-business-internet_5570947.htm&psig=AOvVaw3CNQwbi7G_8Fv8OUdA0iDI&ust=1589906782909327

Building business on the net

Use search engines to drive targeted buyers to your site

- Pay-per-click advertising is the easiest way to get traffic to a brand-new site.
- It has two advantages over waiting for the traffic to come to you organically.
- First, PPC ads show up on the search pages immediately,
- And second, PPC ads allow you to test different keywords, as well as headlines, prices and selling approaches.



Image Source:

https://www.google.com/url?sa=i&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwiJ7bvN7r3pAhVk4jgGHbfSBkwQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.freepik.com%2Fpremium-vector%2Fpeople-are-building-business-internet_5570947.htm&psig=AOvVaw3CNQwbi7G_8Fv8OUdA0iDI&ust=1589906782909327

Building business on the net

Establish an expert reputation for yourself

- Give away free, expert content. Create articles, videos or any other content that people will find useful. Distribute that content through online article directories or social media sites.
- Include "send to a friend" links on valuable content on your website.
- Become an active expert in industry forums and social networking sites where your target market hangs out.



Image Source:

https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwiJ7bvN7r3pAhVk4jgGHbfSBkwQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.freepik.com%2Fpremium-vector%2Fpeople-are-building-business-internet_5570947.htm&psig=AOvVaw3CNQwbi7G_8Fv8OUDa0iDI&ust=1589906782909327

Building business on the net

Use the power of email marketing to turn visitors into buyer

- You're giving them something they've asked for.
- You're developing lifetime relationships with them.
- The response is 100 percent measurable.
- Email marketing is cheaper and more effective than print, TV or radio because it's highly targeted.



Image Source:

https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwiJ7bvN7r3pAhVk4jgGHbfSBkwQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.freepik.com%2Fpremium-vector%2Fpeople-are-building-business-internet_5570947.htm&psig=AOvVaw3CNQwbi7G_8Fv8OUdA0iDI&ust=1589906782909327

Building business on the net

Increase your income through back-end sales and upselling

- Offer products that complement their original purchase.
- Send out electronic loyalty coupons they can redeem on their next visit.
- Offer related products on your "Thank You" page after they purchase.



Image Source:

https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwiJ7bvN7r3pAhVk4jgGHbfSBkwQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.freepik.com%2Fpremium-vector%2Fpeople-are-building-business-internet_5570947.htm&psig=AOvVaw3CNQwbi7G_8Fv8OUdA0iDI&ust=1589906782909327

Concepts of online Catalogues, Shopping carts, Checkout pages.

Online catalogues

- An online product catalog is an important cornerstone for eCommerce retailers. Creating an immersive, information-rich experience helps eCommerce businesses build interest amongst online visitors and is key to converting potential customers into loyal shoppers.

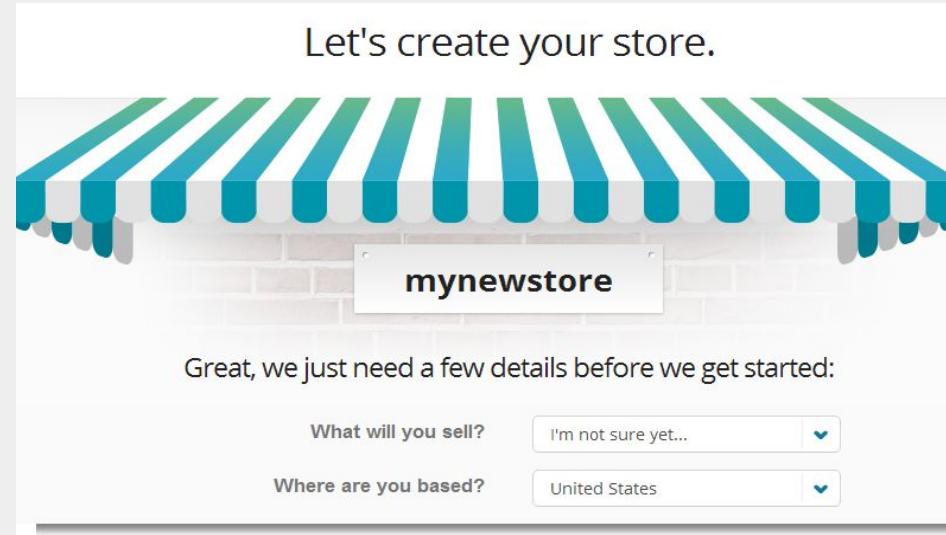


Image Source:

<https://www.google.com/imgres?imgurl=https%3A%2F%2Fecommerceinsiders.com%2Fwp-content%2Fuploads%2F2013%2F07%2Fstore-setup.png&imgrefurl=https%3A%2F%2Fecommerceinsiders.com%2Fecommerce-platform-solutions-online-product-catalog-best-1077%2F&tbnid=pqOsDEVv78OhAM&vet=12ahUKEwirip28873pAhWuBbcAHeRuBHIQMygCegUIARDwAQ..i&docid=kPTLae7VfnXKPM&w=797&h=472&q=what%20is%20online%20catalog%20in%20ecommerce&hl=en&ved=2ahUKEwirip28873pAhWuBbcAHeRuBHIQMygCegUIARDwAQ>

Concepts of online Catalogues, Shopping carts, Checkout pages.

Shopping Carts

- A shopping cart is a software used in eCommerce to assist visitors to make purchases online. Upon checkout, the software calculates the total of the order, including shipping and handling, taxes and other parameters the owner of the site has previously set. The shopping cart typically provides a means of collecting the shopper's payment information.



Image Source:

<https://www.google.com/imgres?imgurl=https%3A%2F%2Fi1.pngguru.com%2Fpreview%2F708%2F198%2F511%2Fshopping-cart-eCommerce-online-shopping-customer-shopping-cart-software-web-design-service-value-proposition-png-clipart.jpg&imgrefurl=https%3A%2F%2Fwww.pngguru.com%2Ffree-transparent-background-png-clipart-matix&tbnid=1mH9BGb0QukOeM&vet=12ahUKEwiRgfqf9L3pAhWf53MBHSTeBqsQMygZegQIARA..i&docid=AXqG8H63u1IDZM&w=800&h=477&q=what%20is%20shopping%20cart%20in%20ecommerce&hl=en&ved=2ahUKEwiRgfqf9L3pAhWf53MBHSTeBqsQMygZegQIARA->

Concepts of online Catalogues, Shopping carts, Checkout pages.

Checkout Pages

- A checkout page refers to any website pages shown to a customer during the step-by-step checkout process. Think of a checkout pages as the online version of a physical checkout counter in a grocery store. Checkout pages come in two types: one-page checkout and multi-page checkout.

The image shows a multi-page checkout process. Step 1: Billing Address. Step 2: Shipping Method, with 'Regular (1-6 wks)' selected. Step 3: Payment Method, with 'Credit Card' selected. Step 4: Review Your Order, showing a single item: a 'Card Pocket' in 'Blue Steel' color at \$59.95 USD. The total grand total is \$67.95 USD. A note says 'Our newsletters are infrequent, but rad. Want in?' and a 'PLACE ORDER' button is at the bottom.

Image Source:

<https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwi9pJOE9b3pAhVaT30KHVyIDV0QjRx6BAGBEAQ&url=https%3A%2F%2Fwww.bornngroup.com%2Fone-page-vs-multi-page-checkout-why-simplicity-is-everything%2F&psig=AOfvaw2uy7tuVWDNadVT46pW1Kn&ust=1589908549469532>

Payment and Order Processing

Payment & Order Processing

- **Merchant Account:** A merchant account is a type of bank account which can accept payments via credit cards, debit cards, net banking, third-party payment applications, etc. You or your company sign a contract with a bank to open a merchant account for your online business so that all payments derived from online sales are directly transferred to your business bank account.



Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.dixipay.com%2Fwp-content%2Fuploads%2F2013%2F12%2FDIXIPAY-Merchant-Account.png&imgrefurl=https%3A%2F%2Fwww.dixipay.com%2Fmerchant-account%2F&tbnid=ys1p_EhulaN__M&vet=12ahUKEwj1tdmw973pAhW_F7cAHaOYCu4QMyglegUIARChAg..i&docid=eOgA_fnUY0vjIM&w=434&h=356&q=merchant%20account&hl=en&ved=2ahUKEwj1tdmw973pAhW_F7cAHaOYCu4QMyglegUIARChAg

Payment and Order Processing

Payment & Order Processing

- **Payment Gateway:** A payment gateway is a software that is required to connect your merchant account to your online store. It's responsible for taking details from the online buyers regarding their payment mode, like credit/debit card details, net banking details etc, It is also responsible to process that payment so that it reaches to your bank account safely and securely.

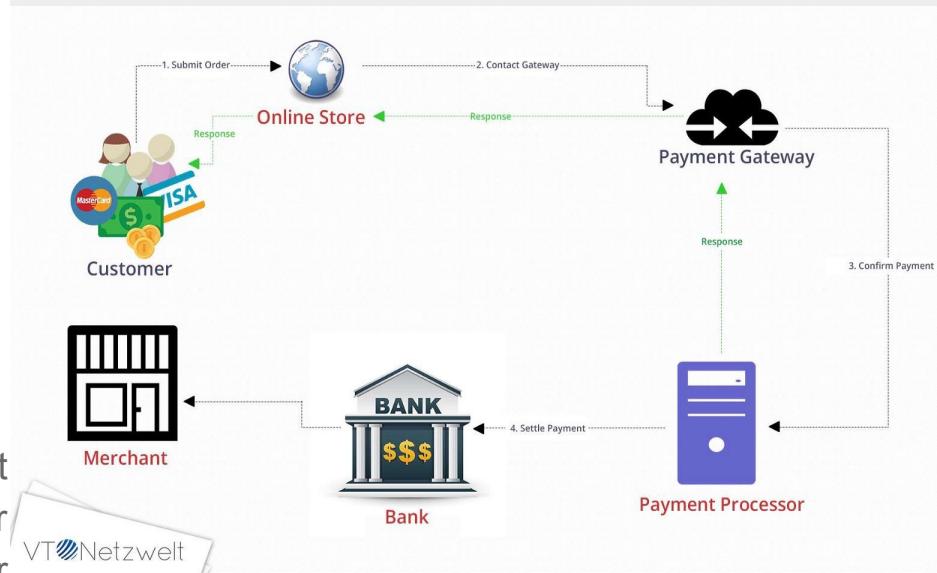


Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Fhackernoon.com%2Fn-images%2F0*AfCVg8qqjJBVWp7I.jpg&imgrefurl=https%3A%2F%2Fhackernoon.com%2F15-most-popular-payment-gateway-solutions-ad49342298b9&tbnid=HwCfDGf2c42VdM&vet=12ahUKEwiH18_T973pAhWXD7cAHVyjDkkQMygWegQIARA..i&docid=ZVJEfyLCCEMPZM&w=1600&h=900&q=payment%20gateway&hl=en&ved=2ahUKEwiH18_T973pAhWXD7cAHVyjDkkQMygWegQIARA-

Payment Authorization

Authorization

- A transaction performed by using a payment card to determine if the card holder has sufficient funds on his/her card to pay for a given transaction. An authorization will take only seconds, and allows the merchant to ensure that payment will be taken from the card.

Putting it all together: Authorization

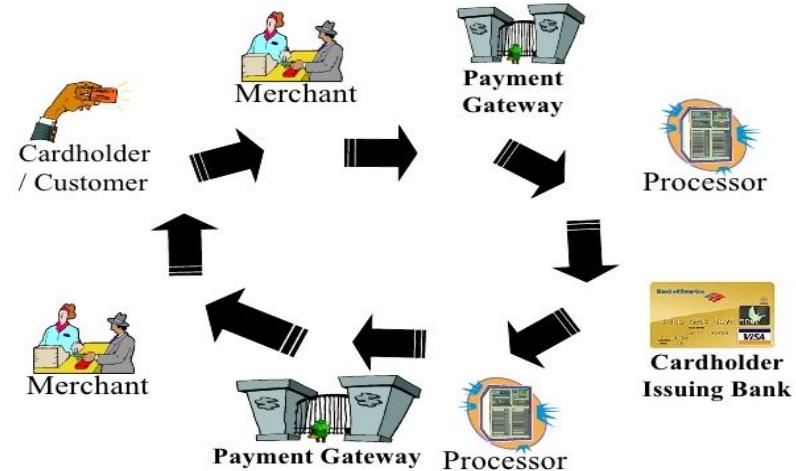


Image Source:

https://www.google.com/url?sa=i&source=imgrc&cd=&cad=rja&uact=8&ved=2ahUKEwi-tbCt-L3pAhXC7XMBHRIWARoQjRx6BAgBEAQ&url=https%3A%2F%2Fwww.slideshare.net%2Fsahilm87%2Fe-commerce-infrastructure&psig=AOvVawOE_2pu2z8Eo8VUwehcVXVp&ust=1589909441283585

Chargeback and other payment methods.

Chargeback & Other Payment Methods

- A Chargeback, in ordinary terms, means a reversal. It's more of a buyer protection measure. The customer gets their money back. Take for instance, if the products they receive are faulty, a chargeback is always the feasible remedy. In usual circumstances, this is the last thing a merchant wants to come across. It brings on board lots of frustrations, more precisely to the retailer.



Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Fblog.2checkout.com%2Fwp-content%2Fuploads%2F2019%2F04%2Fchargeback.jpg&imgrref=https%3A%2F%2Fblog.2checkout.com%2Fonline-payment-processing-challenges-overcome%2F&tbnid=rSf1JtW3mpAWJM&vet=12ahUKEwiijOqX-b3pAhU9B7cAHXJmBYcQMygGegUIARDaAQ..i&docid=tQs_02GU9TlffM&w=764&h=552&q=chargeback%20and%20other%20payment%20method%20in%20ecommerce&hl=en&ved=2ahUKEwiijOqX-b3pAhU9B7cAHXJmBYcQMygGegUIARDaAQ

Security issues and payment gateways

Security Issues

- privacy – information exchanged must be kept from unauthorized parties
- integrity – the exchanged information must not be altered or tampered with
- authentication – both sender and recipient must prove their identities to each other and
- non-repudiation – proof is required that the exchanged information was indeed received



Image Source:

https://www.google.com/imgres?imgurl=https%3A%2F%2Fmedia.springernature.com%2Fflw785%2Fspringer-static%2Fimage%2Fchp%253A10.1007%252F978-3-319-10091-3_10%2FMediaObjects%2F327051_8_En_10_Fig1_HTML.gif&imgrefurl=https%3A%2F%2Flink.springer.com%2Fchapter%2F10.1007%2F978-3-319-0091-3_10&tbnid=5IVs3Y31_XP7DM&vet=1ahUKEwigkOX3-b3pAhUbALcAHT7BArwQMygGegUIARCCAg..i&docid=r0u8lI-mrHlxCM&w=542&h=398&q=security%20issues%20in%20ecommerce&hl=en&ved=2ahUKEwigkOX3-b3pAhUbALcAHT7BArwQMygGegUIARCCAg