ASSIGNMENT FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 2: Networking Infrastructure**		
Submission date		**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	Nguyễn Trọng Duy	**Student ID**	GCD17313
Class	GCD1001	**Assessor name**	Đặng Quang Hiển
Student declaration I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.			
		Student's signature	Duy

Grading grid

P1	P2	P3	P4	P5	P6	P7	P8	M1	M2	M3	M4	D1	D2	D3
✓	✓	✓	✓											

Contents

LO1 Examine networking principles and their protocols 3

P1 Discuss the benefits and constraints of different network types and standards. 3

Definition 3

Networking standards: 4

Protocols: 10

IEEE 802.x 19

Different Types of Networks: 21

P2 Explain the impact of network topology, communication and bandwidth requirements. 31

• Definition: Physical & Logical Topology 31

-Logical e.g. Ethernet, Token Ring; 31

-physical e.g. star, ring, bus, mesh, tree, ring. 35

Types of Topologies with Examples of topology with diagrams (Mesh, Star, Bus, Ring, Tree, Hybrid) 35

List some standard organizations and standards names 43

P3 Discuss the operating principles of networking devices and server types. 47

----Discuss at least 2 operating principles of a selected network devices 47

Networking device 47

• List server types 54

P4 Discuss the inter-dependence of workstation hardware with relevant networking software. 62

Workstation: 62

--Hardware e.g. network card, cabling; permissions; system bus; local-system architecture e.g. memory, processor, I/O devices. 62

--Networking Software: web, mail, file, DHCP, DNS, application, MISA, accounting software, network monitoring system 63

Web 63

mail,.. 64
file, ... 65

LO1 Examine networking principles and their protocols

P1 Discuss the benefits and constraints of different network types and standards.

Different types of networks, standards and protocols available

Definition

Networking standards provide the criteria for data communication that are required for networking technologies and processes to function together. Standards aid in the creation and maintenance of open markets by allowing providers to compete on the basis of product quality while remaining compatible with existing market items. In today's world, there are many various types of networks, standards, and protocols that may be used in businesses and homes.

At different tiers of data transfer, a variety of standards may be employed at the same time

. The following the commonly used standards at each layer are

Application layer – HTTP, HTML, POP, H.323, IMAP

- **Transport layer –** TCP, SPX
- **Network layer –**IP, IPX
- **Data link layer –** Ethernet IEEE 802.3, X.25, Frame Relay
- **Physical layer –**RS-232C (cable), V.92 (modem)

Some instances of various network types, standards, and protocols...

Role of networks:

---Different Type Networks Standard:

Network Standards

Networking standards:

Conceptual models::

OSI model

The OSI Model (Open System Interconnection Model) is a conceptual modeling framework created by the International Organization for Standardization to allow diverse communication systems to communicate using standard protocols. It is used to describe and standardize the communication functions of a network system as well as the functions of a telecommunications system or computer without regard to its internal structure and technology. In layman's terms, OSI establishes a standard for computer systems to interact with one another.

Its purpose is to make various communication systems interoperable using common communication protocols.

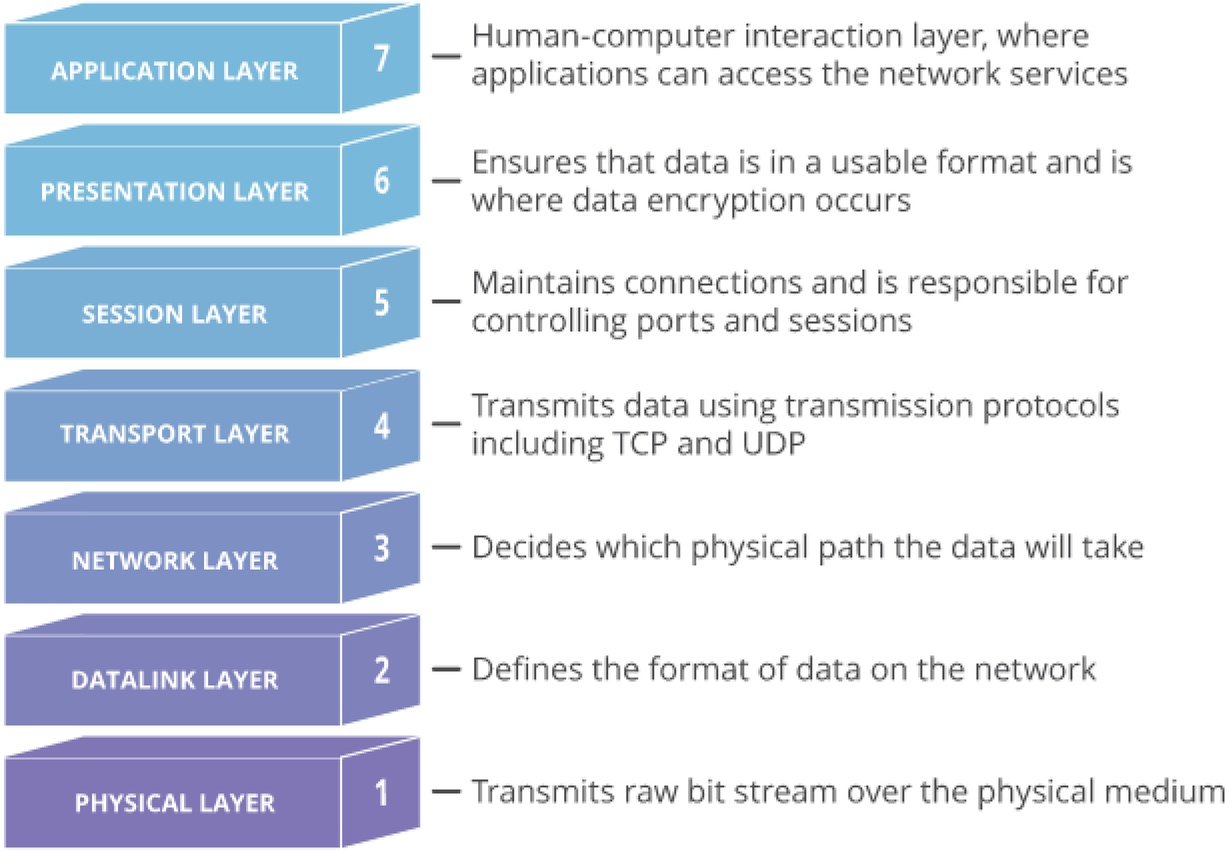
To facilitate interoperability across diverse devices and applications, the OSI model breaks down computing functions into a standard set of rules and constraints.

OSI was developed in 1984 by the International Organization for Standardization at a period when network computing was still in its infancy (ISO). The OSI Model is still used to describe network architecture today, despite the fact that it does not always map precisely to real systems.

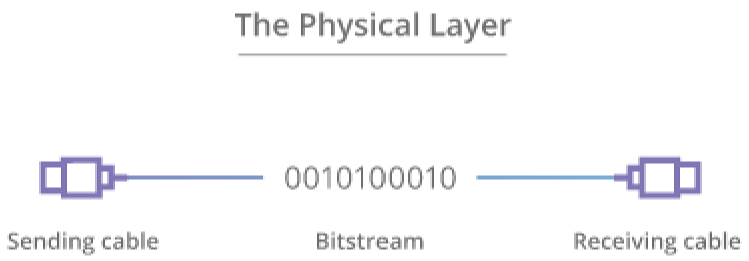
The OSI Model may be thought of as a standard for computer networks. It is based on the idea of separating the data flow in a communication system into seven levels of abstraction: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

From the physical implementation of moving bits on a medium to the top-level data representation of a distributed application, each layer overlaps the previous. Each intermediary layer provides functionality to the layer above it while also being served by the layer below it. Software implements functional levels using established communication protocols.

(https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/, n.d.)


APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATALINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium

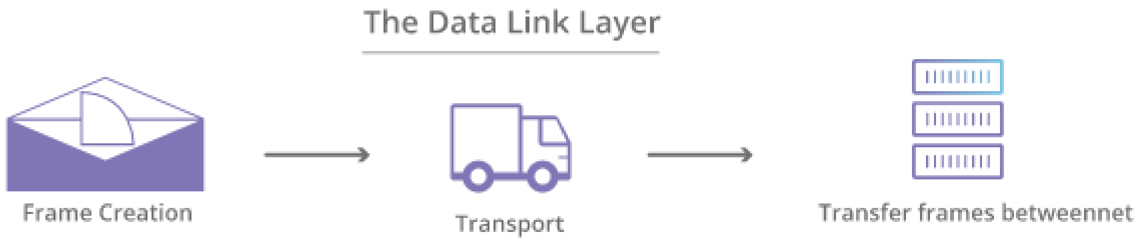
Layer 1: Physical layer



(https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/, n.d.)

Between a device and a physical transmission media, the physical layer is responsible for the transmission and receipt of unstructured raw data. The digital bits are converted into electrical, radio, or optical signals. Voltage levels, voltage change timing, physical data rates, maximum transmission lengths, modulation system, channel access mechanism, and physical connections are all defined by layer specifications. For wireless devices, this comprises pin layout, voltages, line impedance, cable specs, signal timing, and frequency. The physical layer controls bit rate and can specify transmission modes such as simplex, half duplex, and full duplex. A network topology can be used to explain the components of a physical layer. Physical layer specifications are contained in the Bluetooth, Ethernet, and USB standards, which are all widely used. The CAN standard is an example of a lesser-known physical layer specification.

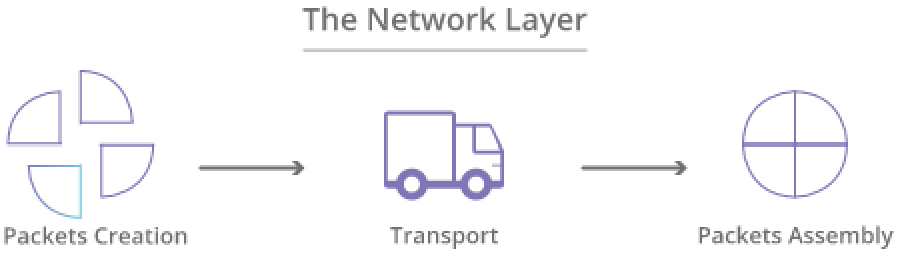
Layer 2: Data link layer



(https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/, n.d.)

Node-to-node data transport is provided by the data link layer, which is a link between two directly linked nodes. It identifies and, in certain cases, corrects problems in the physical layer. It specifies the procedure for establishing and terminating a physical connection between two devices. It also specifies the flow control protocol between them.

Layer 3: Network layer

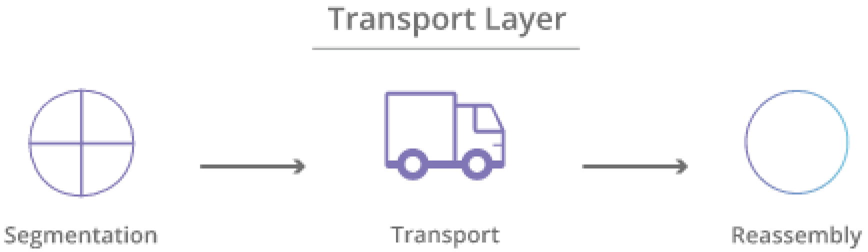


(https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/, n.d.)

The network layer offers the functional and procedural methods of moving packets between nodes in "various networks." A network is a medium to which many nodes can be connected, on which each node has an address, and on which nodes connected to it can send messages to other nodes connected to it by simply providing the message's content and the destination node's address, and letting the network figure out how to deliver the message to the destination node, possibly via intermediate nodes. If a message is too big to be sent from one node to another across the data connection layer between those nodes, the network may divide the message into numerous pieces at one node, send the fragments separately, then reassemble the fragments at a different node. It has the option to report delivery issues, although it is not required to do so.

Message delivery at the network layer is not always guaranteed to be reliable; a network layer protocol may, but is not required to, offer reliable message delivery.

Layer 4: Transport layer

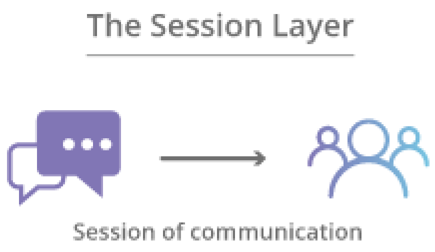


(https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/, n.d.)

The transport layer is responsible for transporting variable-length data sequences from a source to a destination host while ensuring service quality.

Flow control, segmentation/desegmentation, and error control are all methods used by the transport layer to govern the dependability of a specific link. Some protocols are based on state and connections. This implies that the transport layer can keep track of the segments and retransmit those that don't make it. If no failures occur, the transport layer may additionally transmit acknowledgement of successful data transmission before sending the following packet. The message received from the application layer is segmented by the transport layer. The process of splitting a big message into smaller pieces is known as segmentation.

Layer 5: Session layer

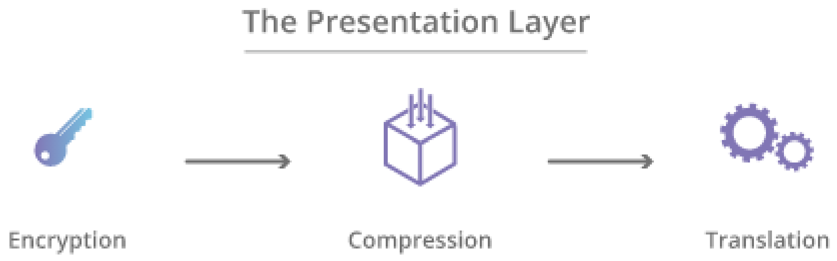


(https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/, n.d.)

The session layer manages computer conversations (connections). It creates, manages, and closes connections between the local and remote applications. It offers protocols for checkpointing, suspending, resuming, and terminating a session in full-duplex, half-duplex, or simplex mode. This layer is responsible for gently ending a session in the OSI model. This layer also handles session checkpointing and recovery, which isn't common in the Internet Protocol Suite. In application contexts that leverage remote procedure calls, the session layer is frequently built explicitly.

The session layer is no longer used in current TCP/IP systems and has been replaced by the TCP protocol.

Layer 6: Presentation layer



(https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/, n.d.)

Though the presentation service offers a mapping between application-layer entities, the presentation layer builds context between them, even if the application-layer entities may employ distinct syntax and semantics. Presentation protocol data units are wrapped into session protocol data units and delivered down the protocol stack if a mapping is provided.

By translating between application and network formats, this layer enables independence from data representation. The presentation layer converts data into the format required by the application. This layer prepares data for transmission across a network. It's also known as the syntactic layer. Compression functions might be included in the presentation layer. The Transfer Syntax is negotiated by the Presentation Layer.

Protocols:

Network protocol definition

- List some protocols : TCP/IP, HTTP,DNS,ICMP

TCP/IP,

TCP/IP model;

The TCP/IP (Transmission Control Protocol/Internet Protocol) model, which is a functional model developed to tackle specific communication issues, assists you in determining how a computer will connect to the internet and how data will be transmitted between them. When many computer networks are linked together, it aids in the creation of a virtual network.

The TCP/IP model's goal is to allow communication across long distances using particular, standard protocols.

The Department of Defense (DoD) conceived and developed it in 1960, and it is based on standard protocols. TCP/IP (Transmission Control Protocol/Internet Protocol) is the acronym for Transmission Control Protocol/Internet Protocol.

TCP/IP Stack is a paradigm for providing an end-to-end, extremely reliable byte stream across an unpredictable internet.

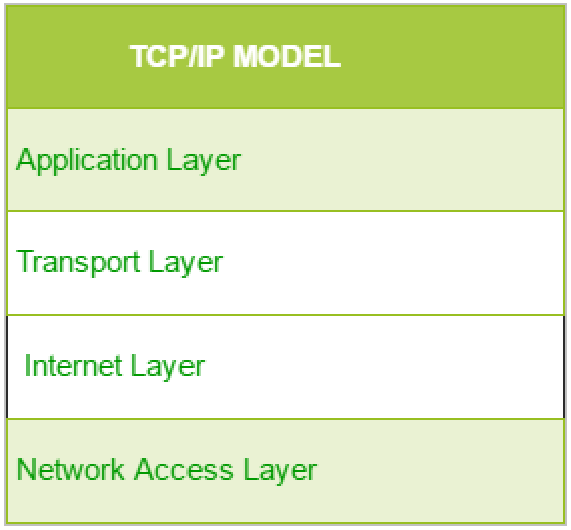
OSI is a protocol-agnostic model for defining all types of network communication.

TCP/IP is a simplified version of the OSI model.

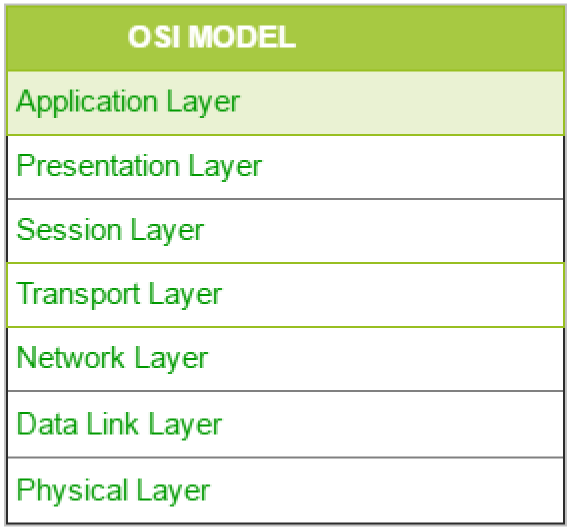
It has four layers, as opposed to the OSI model's seven. The layers are as follows:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

(https://www.geeksforgeeks.org/tcp-ip-model/, n.d.)



TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer



OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

HTTP,

The Hypertext Transfer Protocol (HTTP) is a networked, collaborative, hypermedia information system application-layer layer protocol in the Internet protocol suite concept.

HTTP is an application layer protocol that operates on top of other layers of the network protocol stack to convey data between networked devices.

A typical HTTP flow contains a client machine specification that specifies sending a request to a server, which then provides a response message on how the client's request data will be generated and delivered to the server, as well as how the servers reply to these requests.

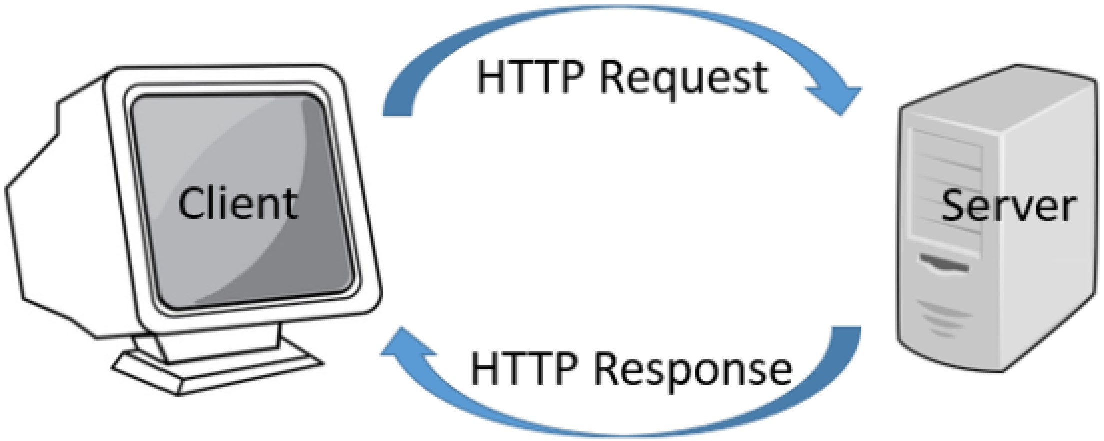
Tim Berners-Lee started developing HTTP in 1989 at CERN, and it was described in a brief text detailing the behavior of a client and a server using the initial HTTP protocol version, which was called 0.9.

Since 1990, it has been the cornerstone of data communication for the World Wide Web (i.e. internet), and it is used to load web pages with hypertext documents that include hyperlinks to other resources that the user can quickly access, for example, by clicking or touching the screen in a web browser.

HTTP is a stateless protocol that may be extended to serve additional purposes by modifying its request methods, error codes, headers, to use TCP/IP-based communication protocol for delivering data (HTML files, picture files, query results, and so on) across the Internet. TCP 80 is the default port, although other ports can be used as well.

It establishes a common language for computers to speak with one another.

(https://innovationm.co/http-protocol/, n.d.)



DNS,

It was simpler to associate individual IP addresses with specific computers when the internet was extremely tiny, but it didn't last long as more devices and people joined the developing network.

As the Internet expanded in popularity, this became an untenable position.

Feinler took time off his time for Christmas and only addressed queries before 6 p.m at California time.

It's still possible to access a website by typing a specific IP address into a browser, but back then, as now, consumers preferred an address made up of easy-to-remember words, similar to what we now call a domain name (like networkworld.com).

Those identities and addresses were allocated by one individual in the 1970s and early 1980s — Elizabeth Feinler at Stanford — who kept a master list of every Internet-connected machine in a text file called HOSTS.TXT.

In 1983, Paul Mockapetris, a researcher at USC, was tasked with coming up with a compromise among multiple suggestions for dealing with the problem. He basically ignored them all and developed his own system, which he dubbed DNS. While it's obviously changed quite a bit since then, at a fundamental level it still works the same way it did nearly 40 years ago.

When you open a web browser and go to a website, All computers on the Internet, from your smart phone or laptop to the servers that serve content for massive retail websites, find and communicate with one another by using numbers. These numbers are known as IP addresses.

The Domain Name System (DNS) is the phonebook of the Internet.

You don't have to remember and enter a long number. Instead, you can enter a domain name like example.com and still end up in the right place.

Domain names such as nytimes.com and espn.com allow people to access content on the internet. Internet Protocol (IP) addresses are used to communicate between web browsers. DNS converts domain names to IP addresses, allowing browsers to access resources on the Internet.

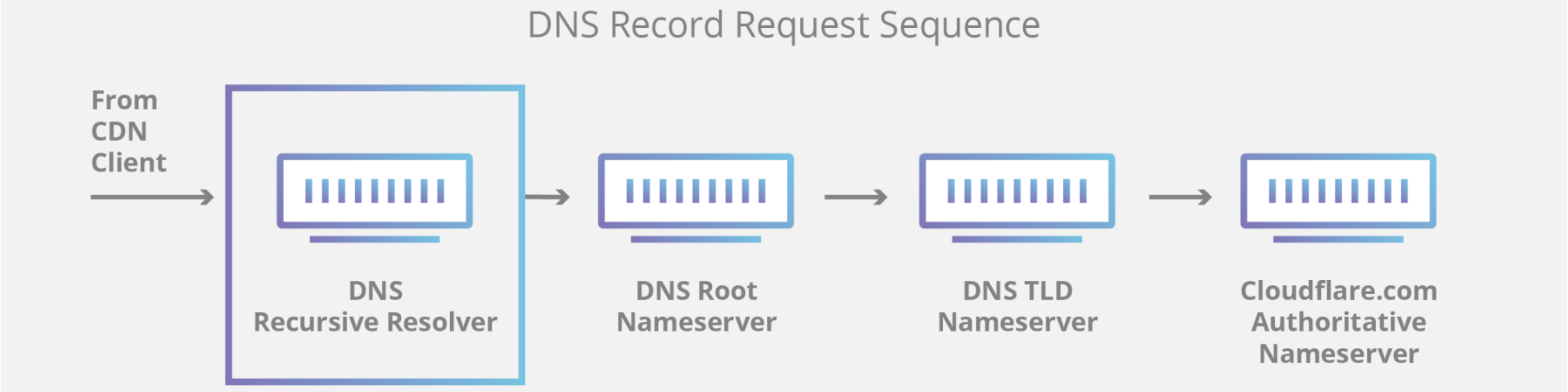
Each Internet-connected device has a unique IP address that other machines use to locate it. DNS servers minimize the need for people to learn IP addresses like 192.168.1.1 (in IPv4) or more complicated modern alphanumeric IP addresses like 2400:cb00:2048:1::c629:d7a2 (in IPv6)

A DNS server such as Amazon Route 53, is a globally distributed service that converts human-readable names such as www.example.com into numeric IP addresses such as 192.0.2.1 that computers use to connect to one another. The DNS system on the Internet manages the mapping between names and numbers in a similar way to a phone book. DNS servers convert requests for names into IP addresses, allowing users to choose which server they want to visit when they input a domain name into their browser. Queries are the term for these requests.

Types of DNS Services

--Authoritative DNS: An authoritative DNS service is a service that allows developers to control their public DNS names by providing an updating method. It then responds to DNS requests by converting domain names to IP addresses, allowing computers to interact with one another. Authoritative DNS has final authority over a domain and is responsible for supplying IP address information to recursive DNS servers. Amazon Route 53 is a DNS scheme that is authoritative.

(https://www.cloudflare.com/learning/dns/what-is-dns/, n.d.)



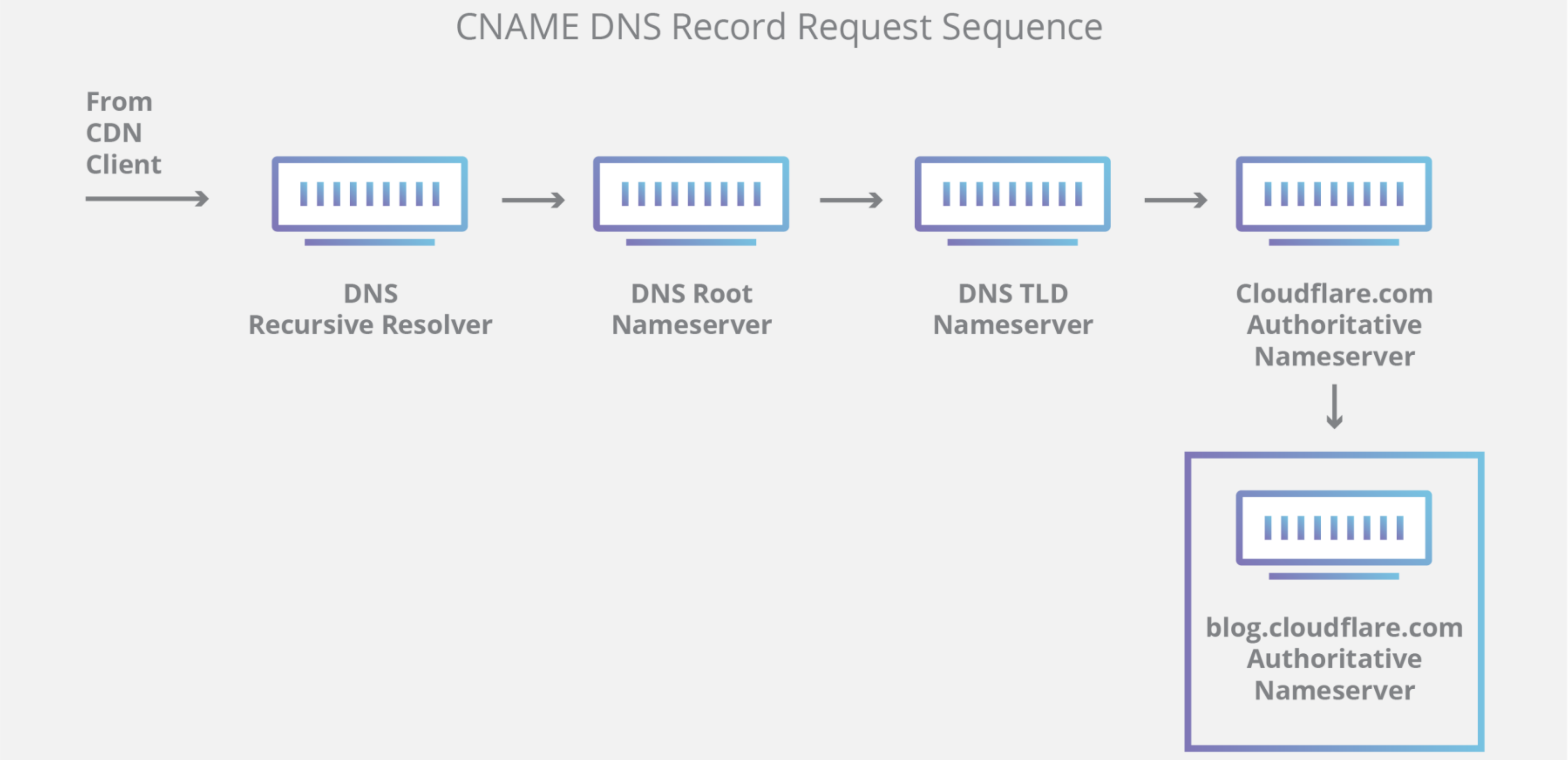
--Recursive DNS:

In most cases, recursive DNS clients do not query authoritative DNS services directly. Instead, they usually link to a resolver, also known as a recursive DNS server, which is a different sort of DNS service. A recursive DNS service functions similarly to a hotel concierge: it does not hold any DNS records, but it works as a middleman to obtain DNS information on your behalf.

When a recursive DNS caches or stores the DNS reference for a length of time, it responds to a DNS query by delivering the source or IP information. If it can't discover the information, it sends the query to one or more authoritative DNS servers.

Although the Domain Name System (DNS) is one of the internet's pillars, most individuals outside of networking are likely unaware that they use it every day to accomplish their jobs, check their email, and spend time on their cellphones.

(https://www.cloudflare.com/learning/dns/what-is-dns/, n.d.)


CNAME DNS Record Request Sequence
From CDN Client
DNS Recursive Resolver
DNS Root Nameserver
DNS TLD Nameserver
Cloudflare.com Authoritative Nameserver
blog.cloudflare.com Authoritative Nameserver

ICMP

Unlike the Internet Protocol (IP), ICMP does not use a transport layer protocol like TCP or UDP.

The most common application of ICMP is to report mistakes.

One of the most common uses of the Internet Control Message Protocol (ICMP) is to see if data is arriving to its destination in a timely manner. As a result, ICMP is an important part of the error reporting process as well as testing to see how well a network transmits data. It is a network level protocol that devices within a network use to communicate problems and information about network connectivity issues back to the source of the compromised data transmission.

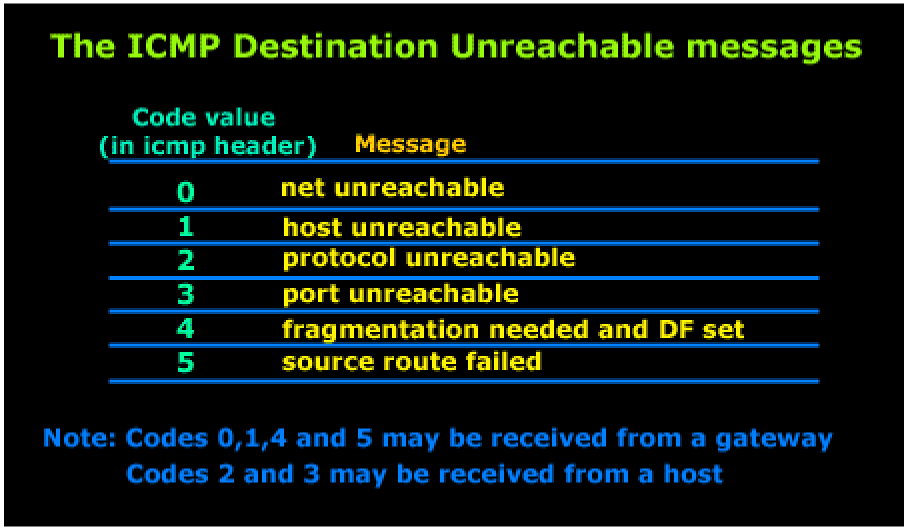
It transmits control signals such source route failure, destination network inaccessible, and source quench. It has an 8-byte header and a variable-size data portion in its data packet format.

When two devices are linked via the internet, for example, ICMP can be used to convey errors from the receiving device to the sending device if some of the data does not arrive as expected. Extremely huge data packets could be too much for a router to handle. The router will then discard the data packet and send an ICMP message to the sender advising it of the problem.

A device such as a router, uses ICMP to communicate with the source of a data packet about transmission problems. If a datagram is not delivered, for example, ICMP may send a message to the host with details to help the host figure out what went wrong with the transmission. It's a workplace policy that emphasizes direct communication.

As a result, ICMP is a connectionless protocol, meaning that one device does not need to establish a connection with another before delivering an ICMP message. TCP is used to send normal IP traffic, therefore any two devices exchanging data will first perform a TCP handshake to guarantee that both devices are ready to receive data. This is not how ICMP establishes a connection. Targeting a specific port on a device is likewise not possible using the ICMP protocol.

(http://dhngoc.blogspot.com/2013/07/icmp-destination-unreachable-message.html, n.d.)

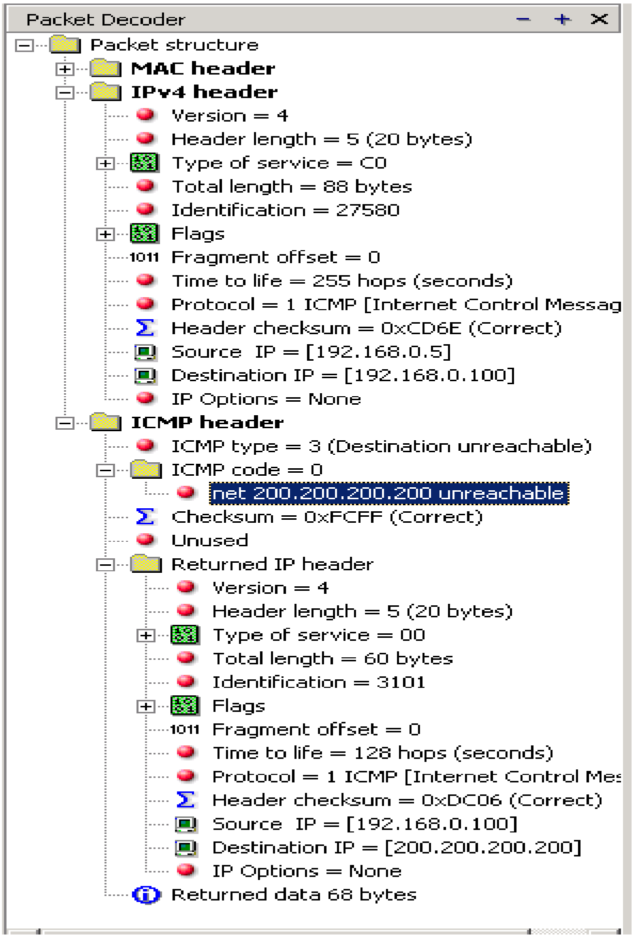


The ICMP Destination Unreachable messages

Code value (in icmp header)	Message
0	net unreachable
1	host unreachable
2	protocol unreachable
3	port unreachable
4	fragmentation needed and DF set
5	source route failed

Note: Codes 0,1,4 and 5 may be received from a gateway
Codes 2 and 3 may be received from a host

(http://dhngoc.blogspot.com/2013/07/icmp-destination-unreachable-message.html, n.d.)

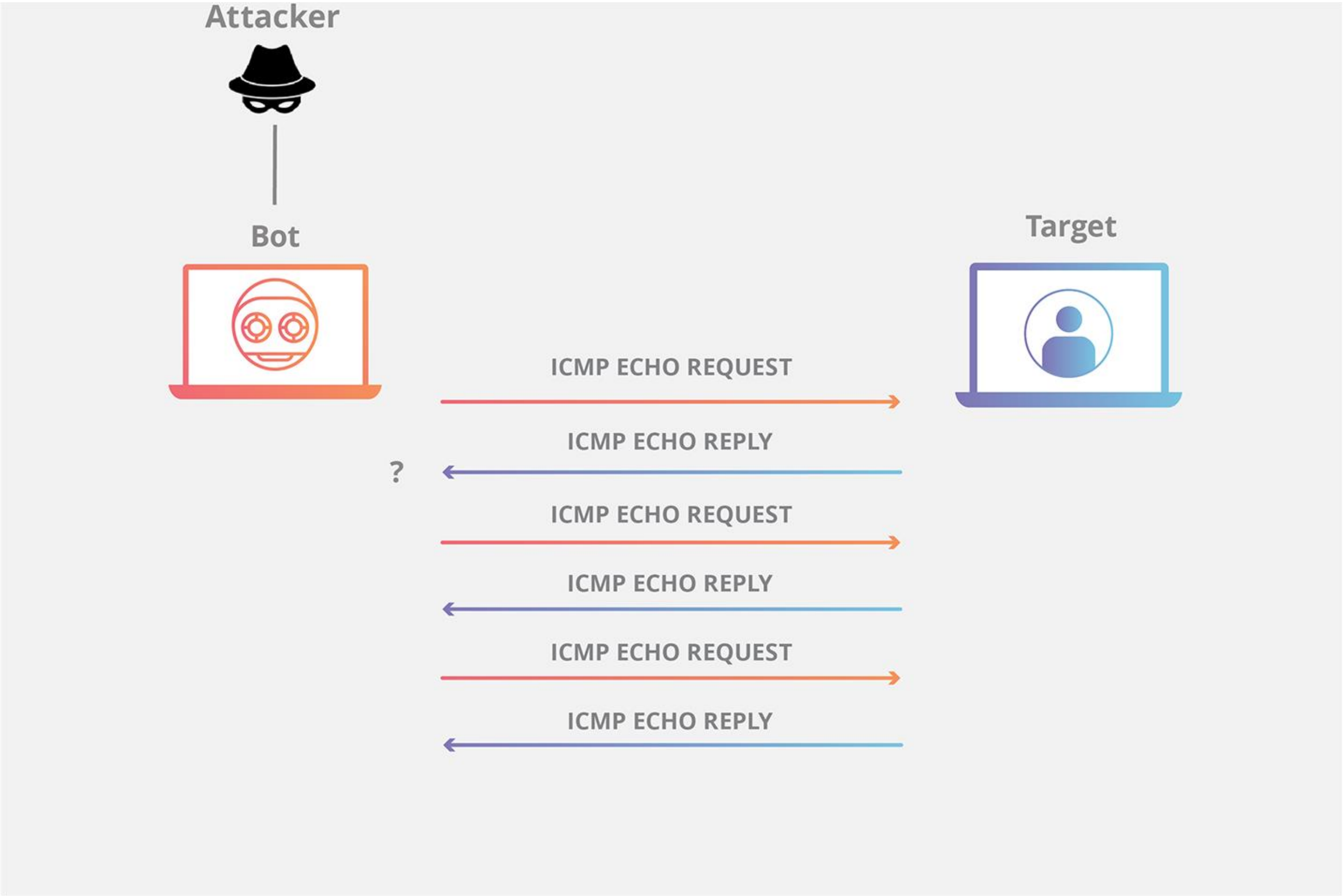


Packet Decoder

```
Packet structure
    MAC header
    IPv4 header
        Version = 4
        Header length = 5 (20 bytes)
        Type of service = C0
        Total length = 88 bytes
        Identification = 27580
        Flags
        Fragment offset = 0
        Time to life = 255 hops (seconds)
        Protocol = 1 ICMP [Internet Control Messag
        Header checksum = 0xCD6E (Correct)
        Source  IP = [192.168.0.5]
        Destination IP = [192.168.0.100]
        IP Options = None
    ICMP header
        ICMP type = 3 (Destination unreachable)
        ICMP code = 0
            net 200.200.200.200 unreachable
        Checksum = 0xFCFF (Correct)
        Unused
        Returned IP header
            Version = 4
            Header length = 5 (20 bytes)
            Type of service = 00
            Total length = 60 bytes
            Identification = 3101
            Flags
            Fragment offset = 0
            Time to life = 128 hops (seconds)
            Protocol = 1 ICMP [Internet Control Me:
            Header checksum = 0xDC06 (Correct)
            Source  IP = [192.168.0.100]
            Destination IP = [200.200.200.200]
            IP Options = None
        Returned data 68 bytes
```

It can, however, be used to carry out distributed denial-of-service (DDoS) assaults.

(https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/, n.d.)

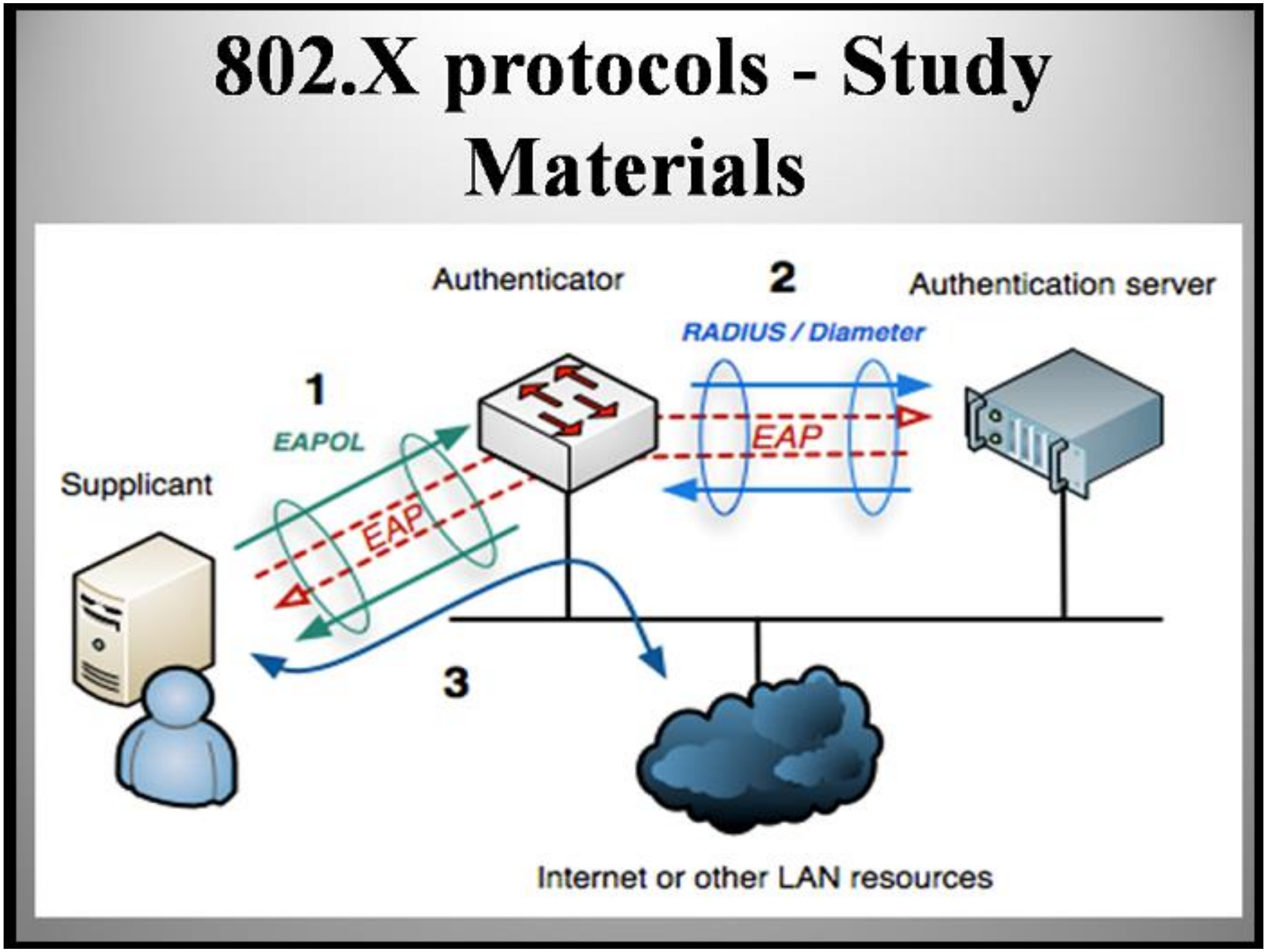


standards::

IEEE 802.x

IEEE 802.1X is an IEEE Standard protocol for port-based Network Access Control that outlines how to enable authentication for devices that connect to other devices on local area networks (LANs) for port-based Network Access Control (PNAC). It's a networking protocol that's part of the IEEE 802.1 group. It provides a mechanism for network switches and access points to delegate authentication to a specialized authentication server, such as a RADIUS server, so that device authentication on a network can be managed and updated centrally rather than distributed across multiple pieces of networking hardware to devices wishing to connect to a LAN or WLAN.

(https://examsdaily.in/802-x-protocols-study-materials, n.d.)



802.1X is a security protocol that dates back to the days of all-wired networking and is now used to safeguard both wired and wireless networks. Because it relies on a centralized authentication server, the protocol is more commonly seen in business LANs than in small residential networks.

Although the standard's name might remind you of the IEEE 802.1X standards that make up Wi-Fidefines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802.11, which is known as "EAP over LAN" or EAPOL. EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless and Fiber Distributed Data Interface (ANSI X3T9.5/X3T12 and ISO 9314) in 802.1X-2004. The EAPOL was also modified for use with IEEE 802.1AE ("MACsec") and IEEE 802.1AR (Secure Device Identity, DevID) in 802.1X-2010 to support service identification and optional point to point encryption over the internal LAN segment.

Different Types of Networks:

****The most common types of network infrastructures are:

1. Local Area Network (LAN)

As the name suggests, ‘local’ means in the same area or building, however a LAN can be very large (eg, spread across the university campus).

A local network with high speed but short transmission line and can only operate in a certain area.

LANs are used to connect a group of computers and devices for them to communicate with each other. For example, offices, buildings, universities, ...

Computers connected to the network are broadly classified as either servers or workstations.

LAN works with TCP / IP protocol.

(htt16)

BENEFIT:

-Having large bandwidth

-Running online applications connected through the network such as conferences, movie shows ...

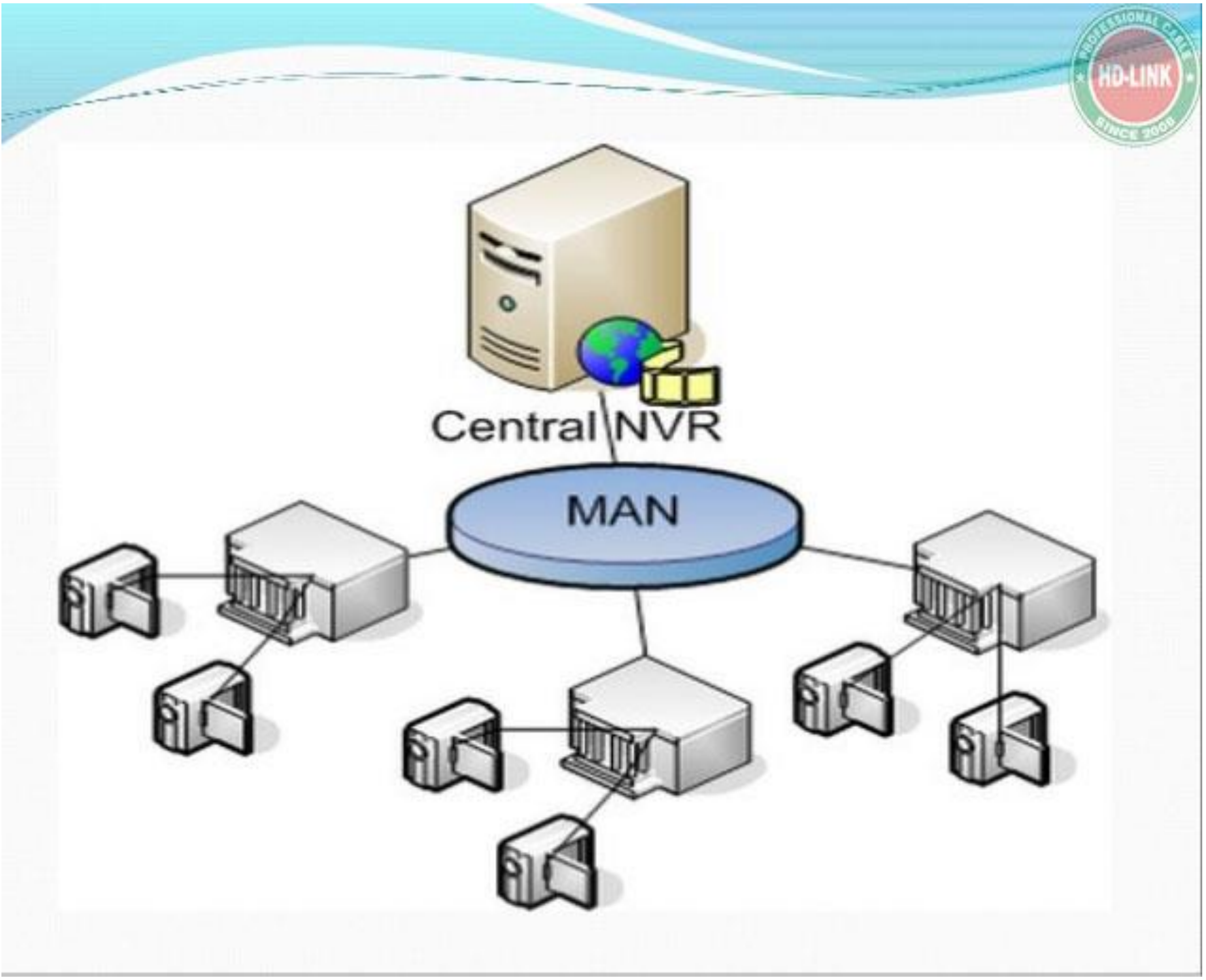
-The range of connections is relatively small but low cost and simple network management.

2. Metropolitan Area Network (MAN)

MAN network is a network model that is connected from multiple LANs together through cables, transmission media, ... Connection scope is to expand the connection area like a large campus or even. entire town or city.

These networks are many local networks that are interconnected. These networks typically cover a large geographic area but less than an area covered by wide area networks.

The main objects using the MAN network model are organizations and enterprises that have many branches or departments connected to each other. The purpose of using MAN network for enterprise is because this network model will help to provide businesses with many types of value-added services at the same time on a voice-data-video connection. Above all, this service also allows the deployment of professional applications easily.



(htt17)

BENEFIT:

-The main feature of the Man network is the average bandwidth but the range of connections is relatively large

-The installation cost is higher than LAN. At the same time, the way of network management is more complex.

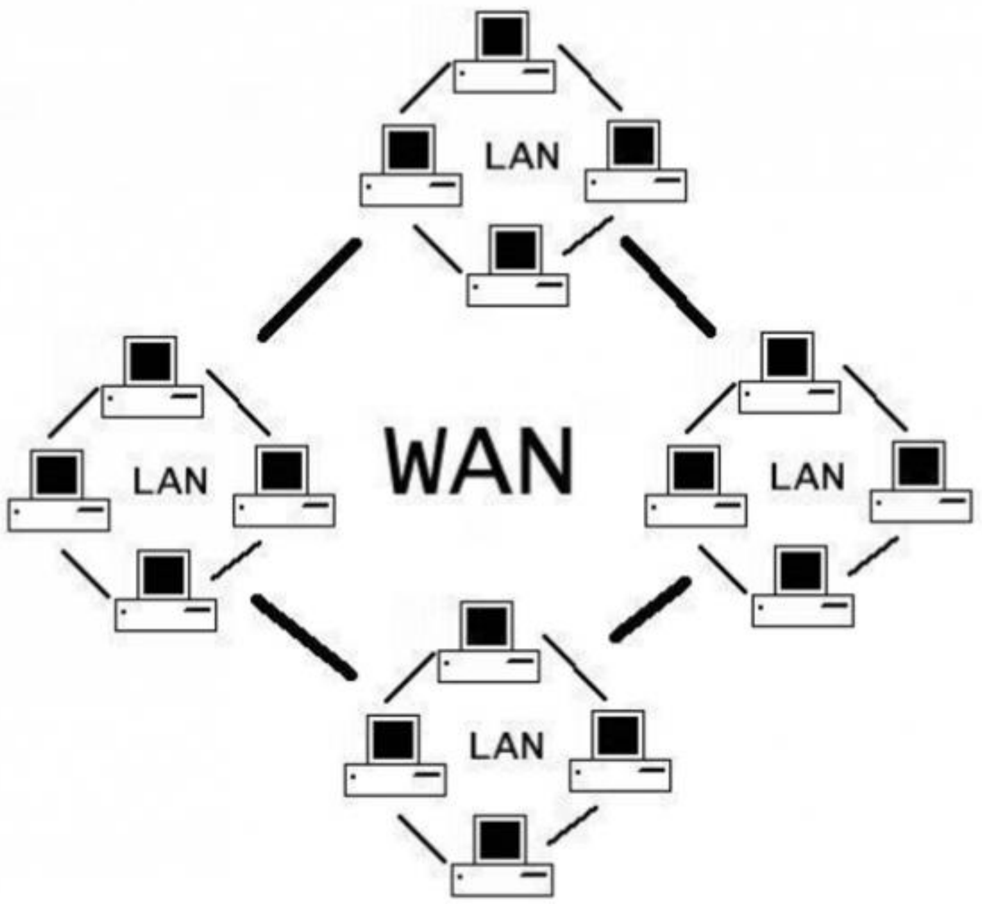
3. Wide Area Network/ Metropolitan Area Network (WAN)

WAN network is a combination of LAN and MAN network connected together and used for telecommunications and computer networks extending over a large geographical area via satellite, fiber optic cable or wire cable.

Large organizations like government, education, and enterprise use WAN to share information such as employees, customers, students, suppliers, buyers, etc. from different geographical regions.

This wide area network can both be connected to a private network and can create a large connection, covering an entire country or globally.

The protocol used mainly in the WAN is TCP / IP protocol. The transmission line of the WAN network is available by changing through each installation location. Because it is the backbone connecting countries or continents.



Como são "conectadas" duas redes LAN e WAN

(htt18)

BENEFIT:

WAN gives users the following advantages:

-The ability to control user access

-Good security.

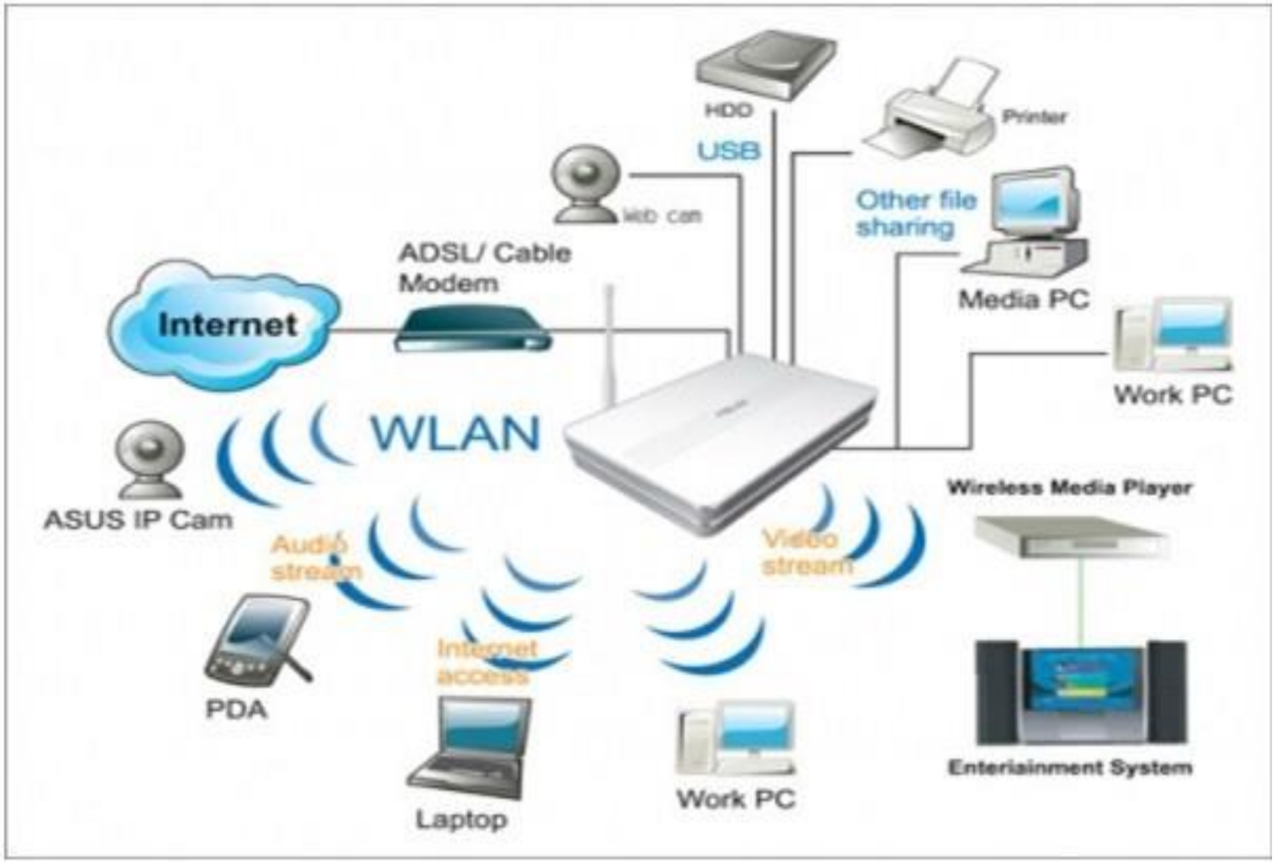
-Ability to store and share information.

-Employees and customers can use the network together.

-Two network users in two different locations can store and share information with each other.

4. Wireless LAN /Wireless Local Area Network (WLAN)

Similar to a LAN, except this network also known as a wireless network has a router which allows some computers to connect wirelessly to each other.



(htt19)

****** Other types less common of network infrastructures are:**

Storage Area Network (SAN)

A storage area network (SAN), or storage network, is a computer network that provides access to store aggregated, block-level data. SAN is primarily designed and used to connect servers to systems of storage devices, such as disk arrays and tape libraries from servers so devices appear to the operating system. as direct attached storage.

Where servers access a block-level storage system built on SANs that provide file-level access and are called shared disk file systems. In addition to SAN, NAS (Network Attached Storage) and CAS (Content Addressed Storage) is other networked storage technologies in which the NAS allows the server to access data at the file level and the CAS allows content level access.

A SAN is typically a dedicated network of storage devices that cannot be accessed through a local area network (LAN).

The heart of the SAN network is a switch. Formally, how is the LAN structure like, the SAN network is like that. Switches will be connected to servers and storage devices such as tapes, drives and even NAS devices. Connected technology can be SCSI (outdated), Fiber Channel (popular now). present) and iSCSI (emerging technology).

Controller Area Network (CAN)

A controller area network was originally designed for multiplex (combining analogue and digital signals over a shared medium) over electrical wiring in automobiles. It is a vehicle bus standard used for microcontrollers and devices to communicate with applications without a computer.

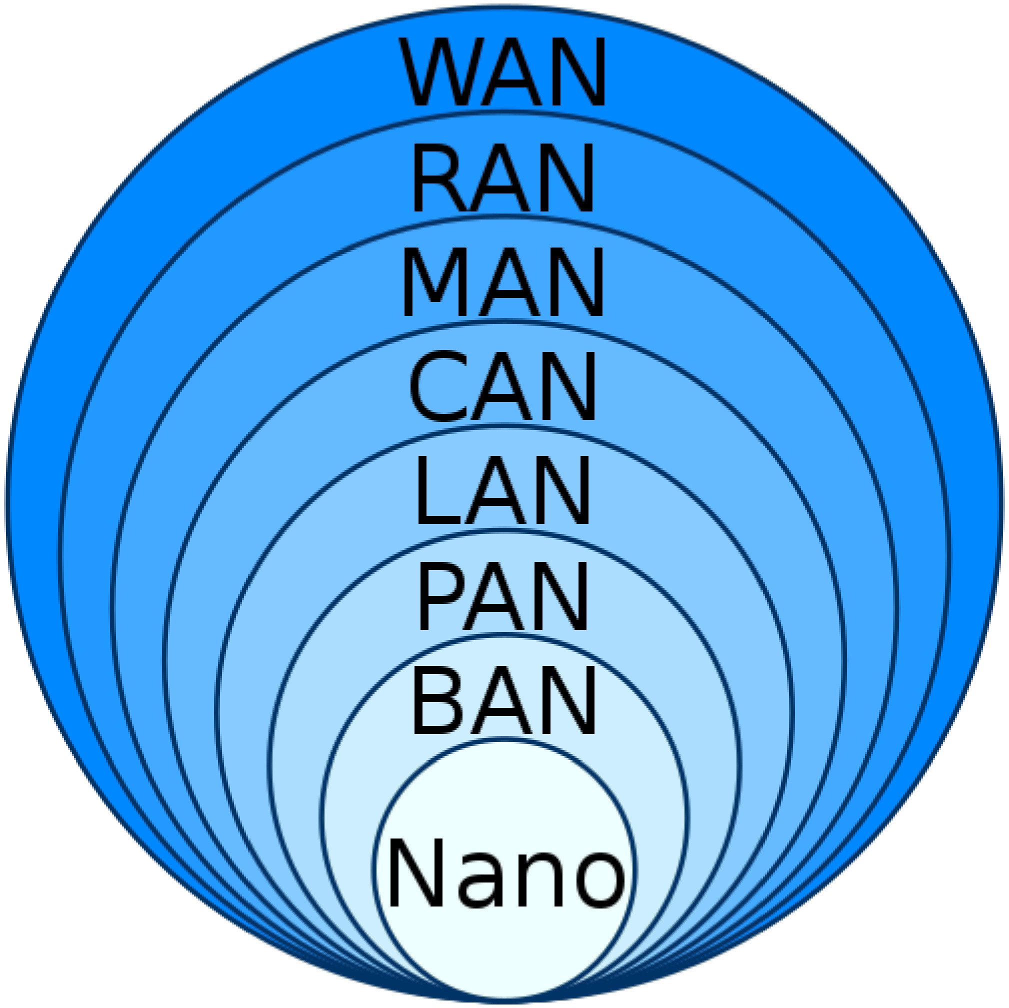
Desk Area Network (DAN)

A DAN is an architecture for multimedia workstations based around asynchronous transfer mode (ATM) technology which transfers data in small 'packets' over a network to ensure no specific type of data hogs resources. DAN is designed to interconnect workstations, multimedia devices and connections to other networks. Multimedia devices used to be connected directly to workstations, however with a DAN these devices are now connected to the network.

Personal Area Network (PAN)

A PAN is used to transmit data to personal devices such as PC's, phones or tablets. These networks can be also used for communication between personal devices or connecting to other networks such as the internet. It has very Short distance wireless network.

(https://en.wikipedia.org/wiki/Personal_area_network, n.d.)



The benefits and disadvantages of a personal area network (PAN).

-PANs are time-saving, cost-effective, and practical.

-Bluetooth is a short-range solution (tens of meters) and is not appropriate for long-distance wireless connections.

-Some PANs have a negative reputation for interfering with other wireless networking technologies that use the same radio channels.

-Bluetooth networks are reasonably safe, but data transfer speeds are modest.

• List some standard organizations and standards names

- Benefit of the network

- Constraint of the network

P2 Explain the impact of network topology, communication and bandwidth requirements.

Topology

• Definition: Physical & Logical Topology

- Provides different configurations that are used to create a network
- Is a pattern of network devices and describes the way in which these devices are connected.
- Topologies can be physical or logical.
- Physical topology refers to the actual physical structure of the network, while a logical topology determines the way in which the data actually passes through the network from one device to other.

-Logical e.g. Ethernet, Token Ring;

Ethernet::
Ethernet is defined as the 802.3 protocol by the Institute of Electrical and Electronics Engineers (IEEE). But simply saying "Ethernet" is a lot easier, and perhaps that's how you figure out who's in charge of that vital Internet.

Ethernet, as previously said, is a classic technology for constructing and connecting networks. It refers to how network devices format and send data to other network devices in a shared connected local area network (LAN). The most often used nowadays, or wide area network (WAN), is an interconnected network of computers in a limited area, such as an office, a university campus, or even your house, that connects many computers or other devices like printers, scanners, and so on.

You could even be linked after reading this. It enables devices to interact with one another via a protocol, which is a collection of rules or a universal network language.

Fiber optic cables are used in a wired network to accomplish this. It is done using wireless network technologies in a wireless network.

Ethernet can detect, receive, and process data in the same LAN or campus network. An Ethernet cable is a data transmission cable that is encased.

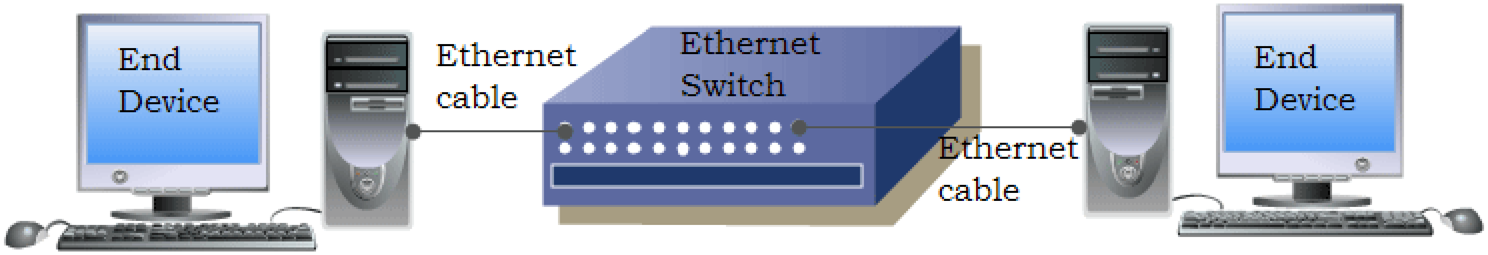
Instead of connecting wirelessly, connected devices can utilize Ethernet to access the geographical local area network. End users ranging from corporations to gamers rely on Ethernet connectivity for a variety of reasons, including stability and security.

Ethernet is less susceptible to disruptions than wireless LAN (WLAN) technology.

Because devices must connect through physical cable and rectangular Ethernet ports, it can also give a better level of network security and control than wireless technologies. Outsiders will have a hard time accessing network data or stealing bandwidth from idle devices as a result of this.

Different topologies, such as star, bus, and ring, are used in Ethernet networks.

(https://www.computernetworkingnotes.com/ccna-study-guide/basic-concepts-of-ethernet-lan-explained.html, n.d.)



Token Ring:

A token-ring network is a computer networking technology that was formerly used to establish a local area network (LAN) that uses a token to transport data in one way over a set number of sites by using a token. IBM introduced and developed the access method in 1984, and it was standardized and conforming to the IEEE 802.5 standard in 1989.

The token is a mark of authority for transmission line control. When the token arrives at that location, it allows any sending station in the network (ring) to send data.

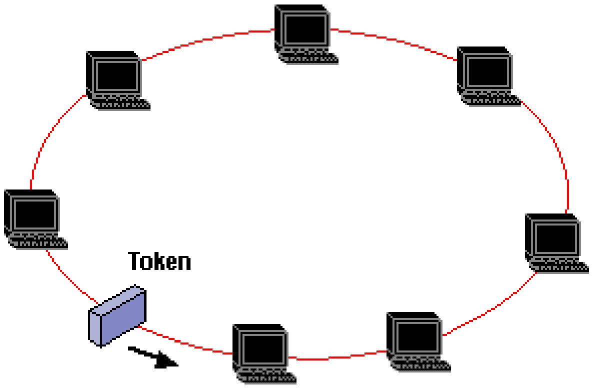
Although the Token Ring MAU is a central hub, it does not work in the same way as a shared Ethernet hub. Token Ring is more deterministic, ensuring that all users receive regular transmission turns. When using Ethernet, all users strive to be the first to connect to the network.

Using twisted wire connection, all stations link to a central wiring hub known as the "Multistation Access Unit" (MAU). The majority of Token Ring commercial networks have now transitioned to Ethernet.

Stations in a token-ring network are physically linked to a wiring concentrator, such as the IBM® 8228 Multistation Access Unit, in a star-wired ring topology. The concentrator Token Ring access method links up to 255 nodes in a star topology at 4, 16, or 100 nodes and serves as a logical ring around which data is transported (Mbps). Shielded twisted pair (STP) cabling is used to link each station to the concentrator. Using twisted wire connection, all stations link to a central wiring hub known as the "Multistation Access Unit" (MAU). The majority of Token Ring commercial networks have now transitioned to Ethernet.

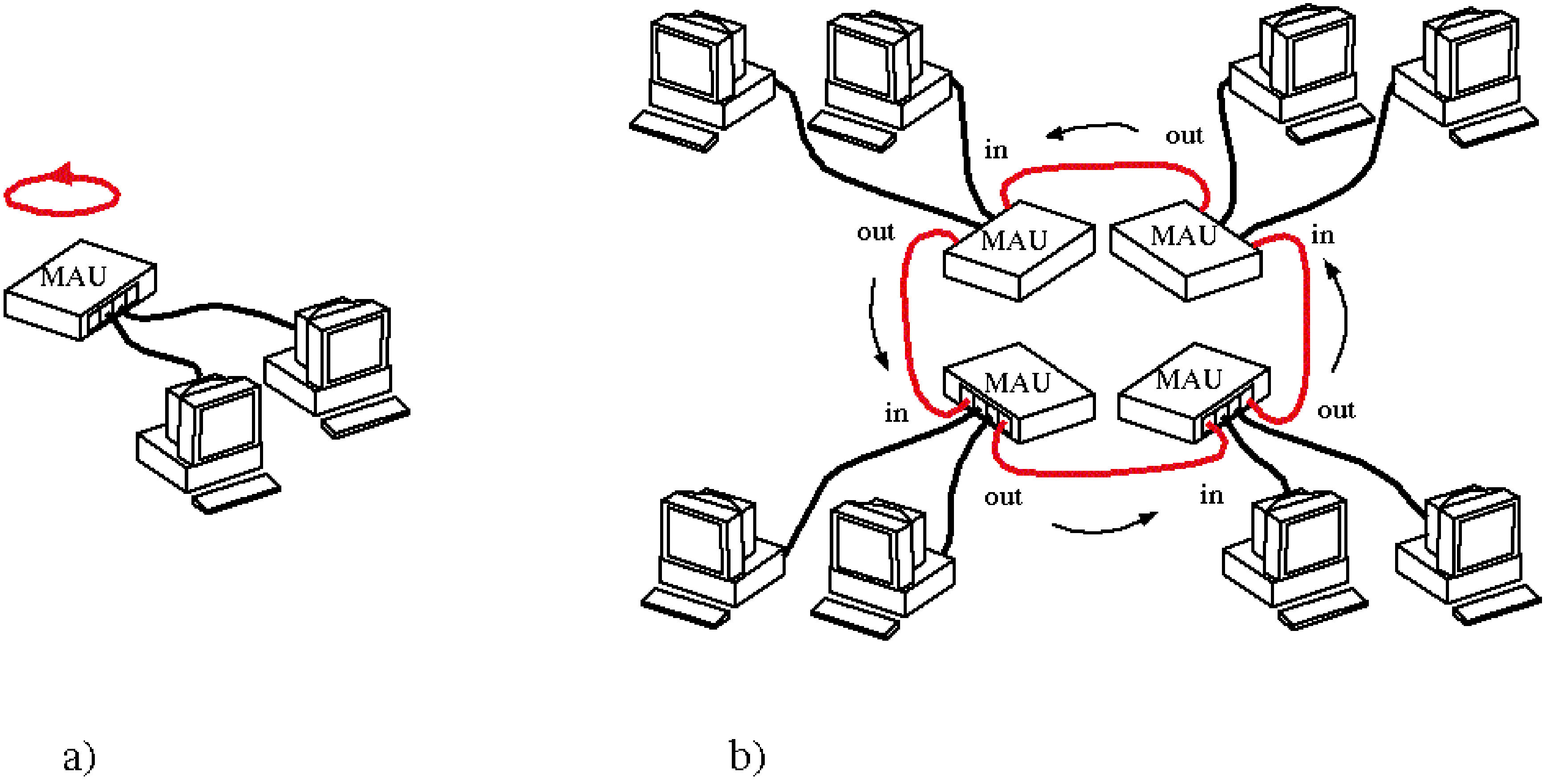
It makes use of a token, which is a three-byte frame that is transferred around a logical ring of workstations or servers. Token passing is a channel access mechanism that provides equal access to all stations while avoiding the collisions that can occur with contention-based access methods.

Token Ring was a popular technology, especially in business settings, although it was eventually surpassed by subsequent Ethernet variants.



(https://www.pctechguide.com/networking/token-ring-networks, n.d.)

(https://commons.wikimedia.org/wiki/File:Token_ring.png, n.d.)



-physical e.g. star, ring, bus, mesh, tree, ring.

Types of Topologies with Examples of topology with diagrams (Mesh, Star, Bus, Ring, Tree, Hybrid)

1. Bus:::

-All devices are linked together by a backbone/trunk connection.

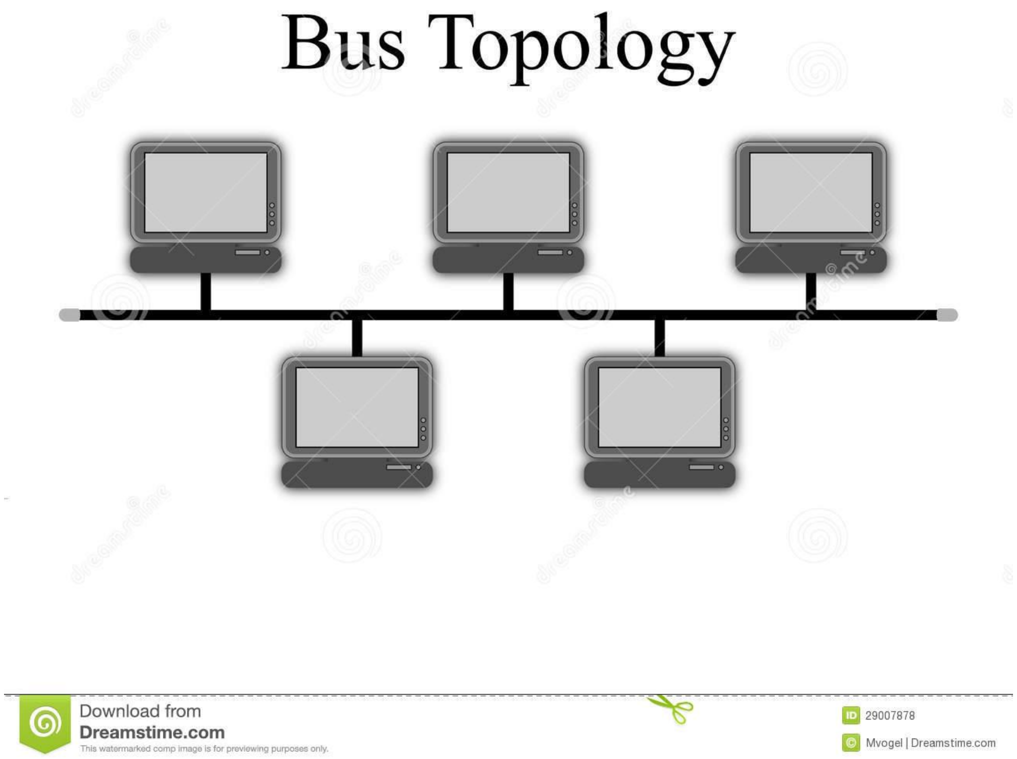
-Works in a daisy chain form

-Medium is shared, which results in collisions

-At one end, the server is located, while the devices are located in various locations.

-50 ohm terminators are utilized

-Data transmission is not the responsibility of the devices



(https://www.dreamstime.com/royalty-free-stock-photos-bus-topology-diagram-image29007878, n.d.)

2. **Star**

-Each gadget is connected via wire to a central device known as a hub.

• Benefits:

– Easy to install, configure, maintain, and grow

– Centralized management

– Adding or removing a device does not affect the entire network

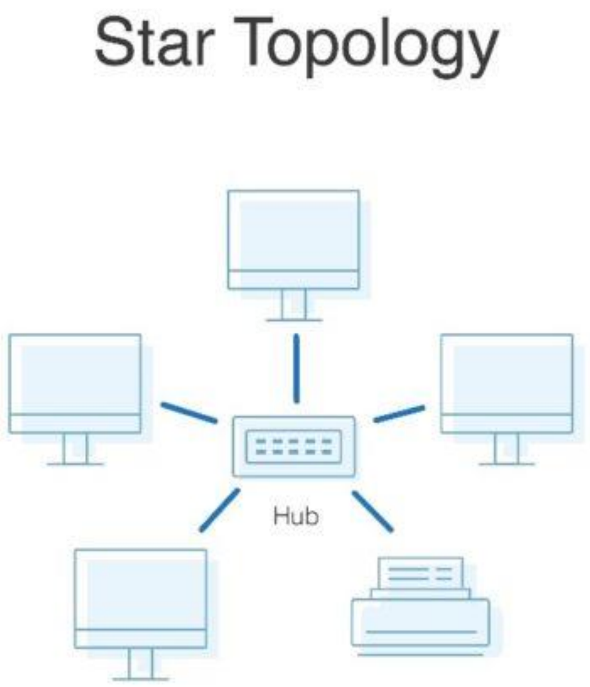
• Disadvantages:

- More wire is required

- When a hub fails, the entire network suffers.

- It Is More Expensive

(https://thietbikythuat.com.vn/mang-lan-la-gi-vi-sao-nen-su-dung-mang-lan/star-topology/, n.d.)



3.Ring

The devices are linked together in a closed loop.

Media is available to all devices on an equal basis.

The device waits for its turn to send data.

Token Ring networks are the most frequent.

• Advantages:

- Reliable and provides faster service

- There are no collisions

• Disadvantages:

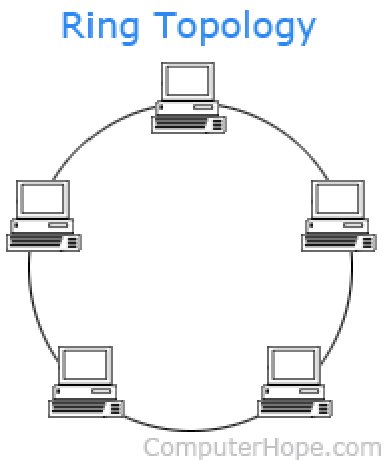
- Handles a high volume of traffic

– When compared to bus topology, more cabling is required

– A single malfunctioning item impacts the entire network

- The addition of devices has an impact on the network.

(https://www.computerhope.com/jargon/r/ringtopo.htm, n.d.)



4, Mesh

Used to link LANs in WANs.

Every gadget communicates with the others.

Routers can be used to discover the optimum communication path.

• Advantages:

- Helps to increase fault tolerance

- A single link failure does not affect the entire network.

- There is no need for centralized management.

• Disadvantages:

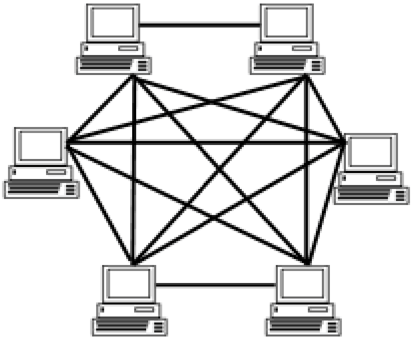
— Difficult to set up and maintain

- Each connectivity from one device to another need its own network interface card (NIC).

– Expensive

(https://www.computerhope.com/jargon/m/mesh.htm, n.d.)

Mesh Topology



ComputerHope.com

5. Tree

Combines the benefits of both a linear bus and a star topology.

The root hub is connected to all of the devices.

Twisted pair cable is a typical type of cable.

Smaller computers are the lowest level gadgets.

• Advantages:

– Easy to expand the network

– Each device has its own point-to-point wiring

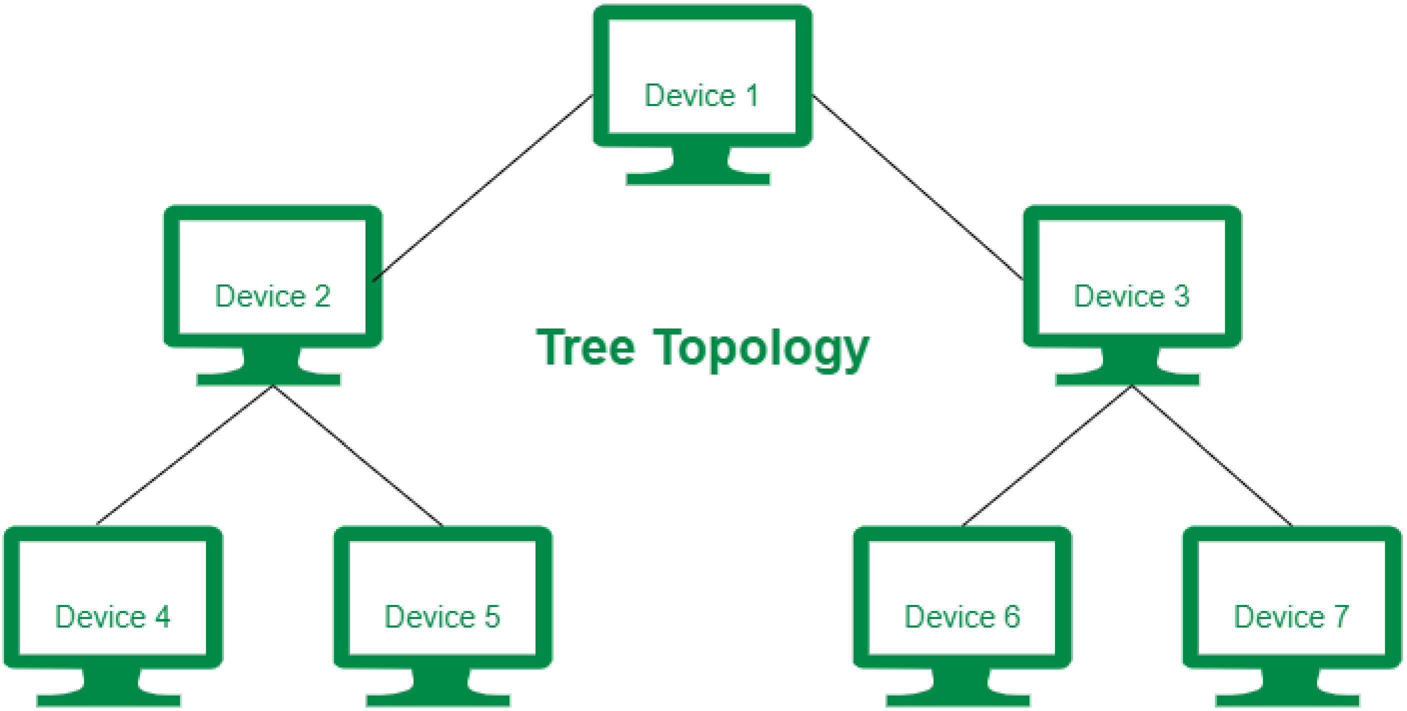
• Disadvantages:

– Difficult to configure

– If the backbone goes down, the entire network falls down

– More expensive

(https://www.geeksforgeeks.org/difference-between-ring-topology-and-tree-topology/, n.d.)



6. Hybrid

A hybrid topology is a network that combines two or more topologies in such a way that the resulting network does not conform to any of the conventional forms.

• Benefits:

– Can be used to build bigger networks

– Can handle a lot of traffic

– Fault detection is simple

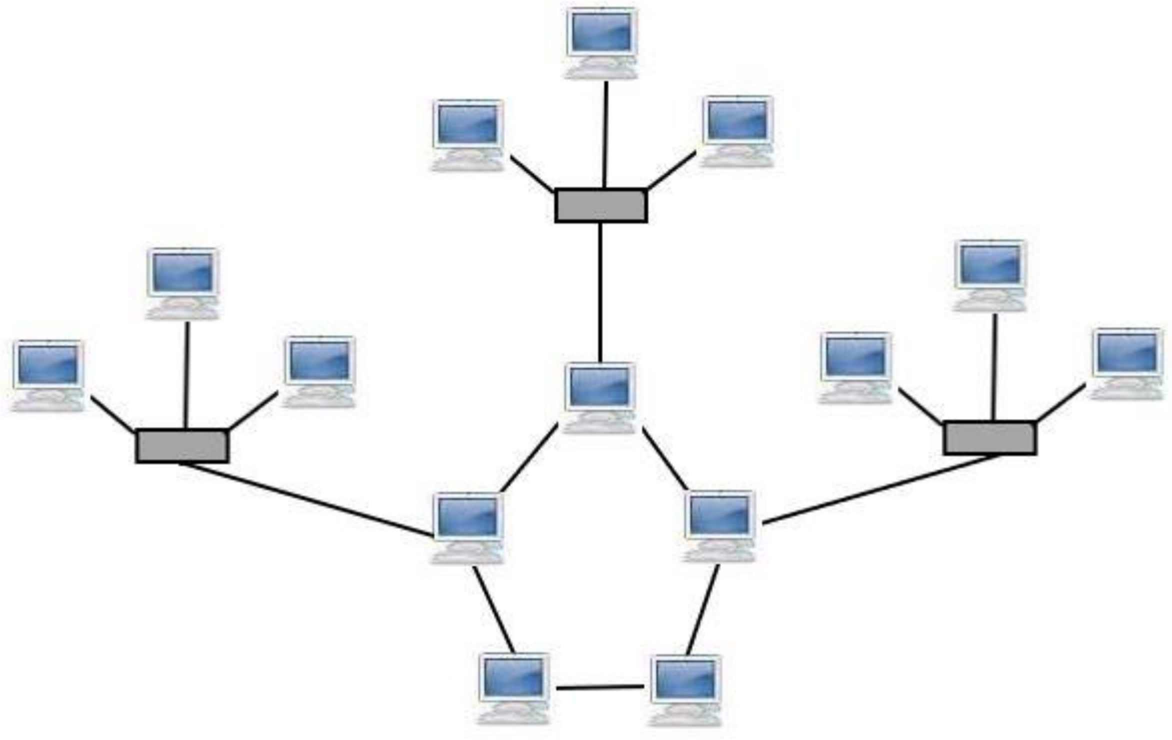
• Disadvantages:

– Difficult to install and configure

– More costly than other topologies

– More cabling is necessary

(https://www.computerhope.com/jargon/h/hybrtopo.htm, n.d.)



ICMP

List some standard organizations and standards names

ISO. – International Organization for Standardization

IEC. – International Electrotechnical Commission

ITU. – The International Telecommunication Union

ANSI. - American National Standards Institute

NIST. - National Institute of Standards and Technology

Ecma International. - Ecma International (previously called ECMA)

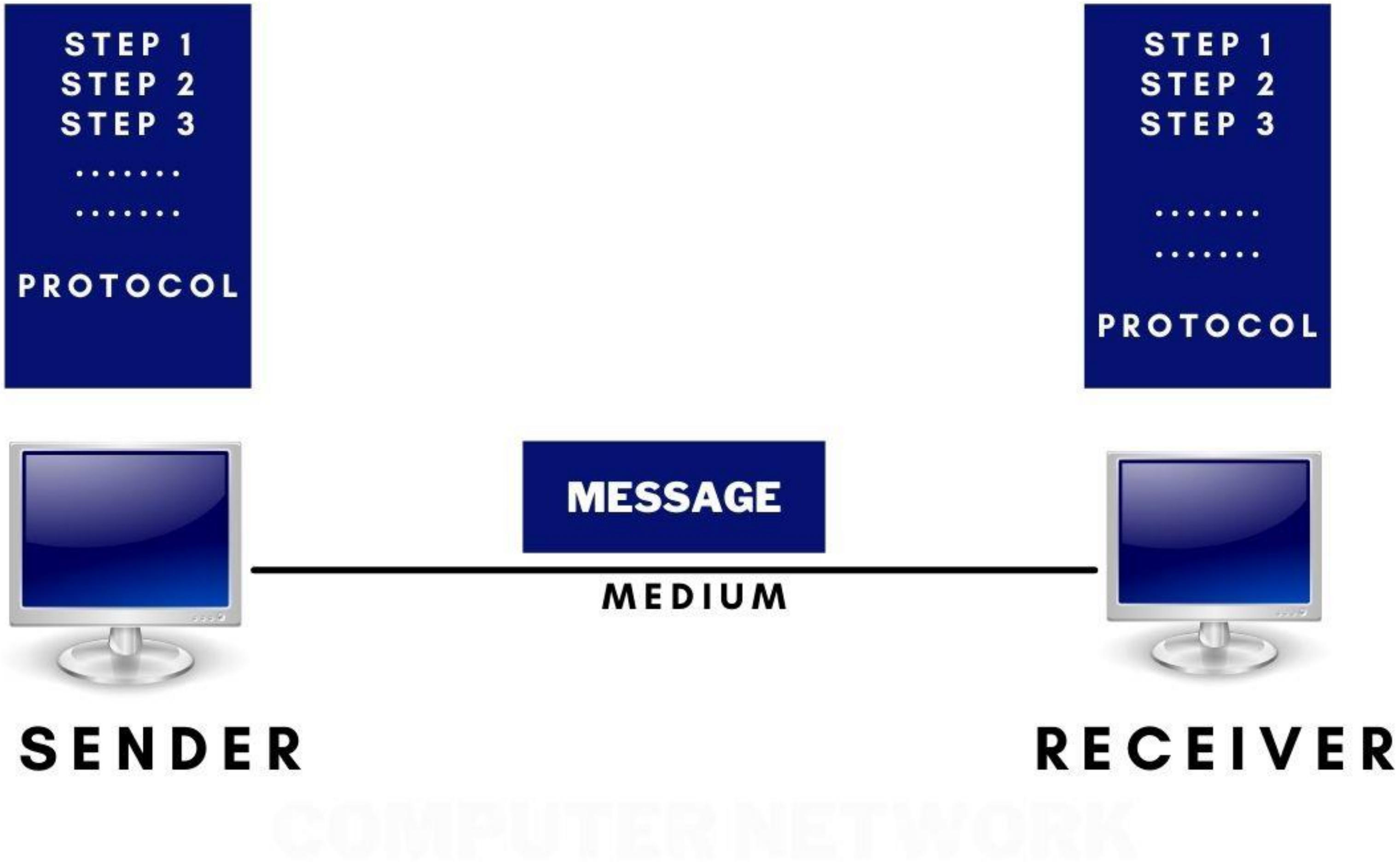
(https://en.wikipedia.org/wiki/List_of_technical_standard_organizations, n.d.)

2. Communication and Bandwidth

• Define commutations in terms of networking

A computer network or data network is a telecommunications network that allows computers to exchange data, that allows application programs to talk to each other regardless of the hardware and operating systems where they are run.

(https://www.quora.com/What-is-data-communication, n.d.)



Network communications (Internet working) defines a set of protocols (that is, rules and standards) that refers to the transmission of this digital data between two or more computers, and a computer network or data network is a telecommunications network that allows computers to exchange data, that allows application programs to talk to each other regardless of the

Application programs can communicate via the internet regardless of their actual network connectivity.

Cable or wireless media is used to make a physical link between networked computing devices. The Internet is the most well-known computer network.

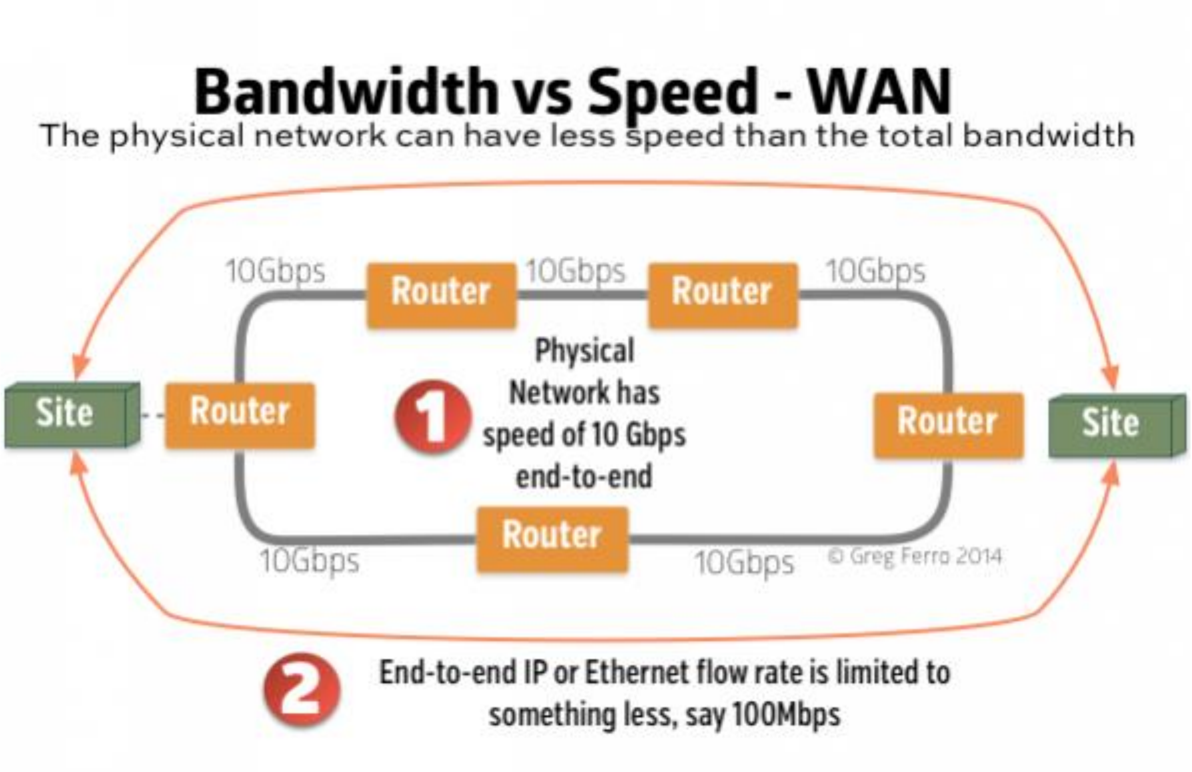
• Rules of communication

Transmission Control Protocol (TCP) and Internet Protocol (IP) are the two fundamental protocols that make up the TCP/IP internetworking technology (IP).

• Define Bandwidth ::Bandwidth requirements for the networks

Signal processing, wireless communications, modem data transfer, digital communications, and electronics all use a different notion of bandwidth.

(https://etherealmind.com/basics-difference-bandwidth-speed/, n.d.)


Bandwidth vs Speed - WAN
The physical network can have less speed than the total bandwidth
10Gbps
Router
10Gbps
Router
10Gbps
Site
Router
1
Physical Network has speed of 10 Gbps end-to-end
Router
Site
10Gbps
Router
10Gbps
© Greg Ferro 2014
2
End-to-end IP or Ethernet flow rate is limited to something less, say 100Mbps

The term "bandwidth" is used in computers to describe the amount of data that may be sent. The greatest quantity of analog signal data that can be communicated and transferred through an internet connection in a given length of time and on a given path. Bandwidth is measured in hertz and can be classified as network bandwidth, data bandwidth, or digital bandwidth. The frequency range between the lowest and highest achievable frequencies while maintaining a well-defined signal power impairment threshold. The exact bit rate that can be obtained is determined by both the signal bandwidth and the channel noise.

Bandwidth is commonly confused with internet speed, although it refers to the quantity of data that can be delivered across a connection in a given length of time (measured in megabits per second) (Mbps).

3. Discuss the impact of topology on banwidth requirement

P3 Discuss the operating principles of networking devices and server types.

----Discuss at least 2 operating principles of a selected network devices

• List network devices

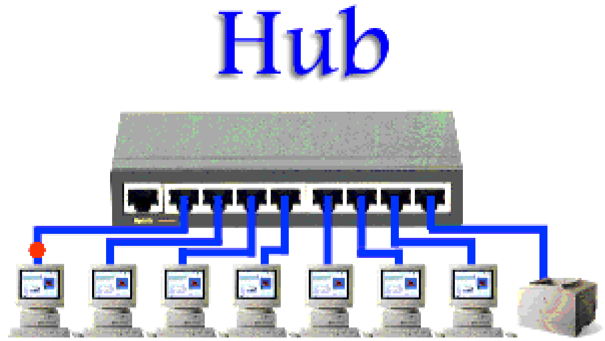
Intermediate Devices: Servers; hub, routers; repeaters; switches; bridges; access point (wireless/wired), wireless router; gateway multilayer switch, firewall, HIDS,;; wireless devices; content filter, Load balancer, Modem, Packet shaper, VPN concentrator.

Networking device

-Hub

A hub (also known as an Ethernet hub, active hub, network hub, repeater hub, multiport repeater, or simply hub) is a physical hardware device layer networking device that connects numerous devices to form a single network segment.

(https://community.fs.com/blog/do-you-know-the-differences-between-hubs-switches-and-routers.html, n.d.)



It contains many input/output (I/O) ports, with a signal inserted at any port's input appearing at every port's output save the original incoming signal.

They're often used to connect computers in a local area network (LAN). It has a lot of ports in it. One of these ports is plugged in by a machine that wants to connect to the network. When a data frame arrives at a port, it is broadcast to all other ports, regardless of whether or not it is headed for a specific destination.

A hub works at the physical layer (layer 1) of the OSI model. A repeater hub also participates in collision detection, forwarding a jam signal to all ports if it detects a collision.

In addition to standard 8P8C ("RJ45") ports, some hubs may also come with a BNC or an Attachment Unit Interface (AUI) connector to allow connection to legacy 10BASE2 or 10BASE5 network segments.

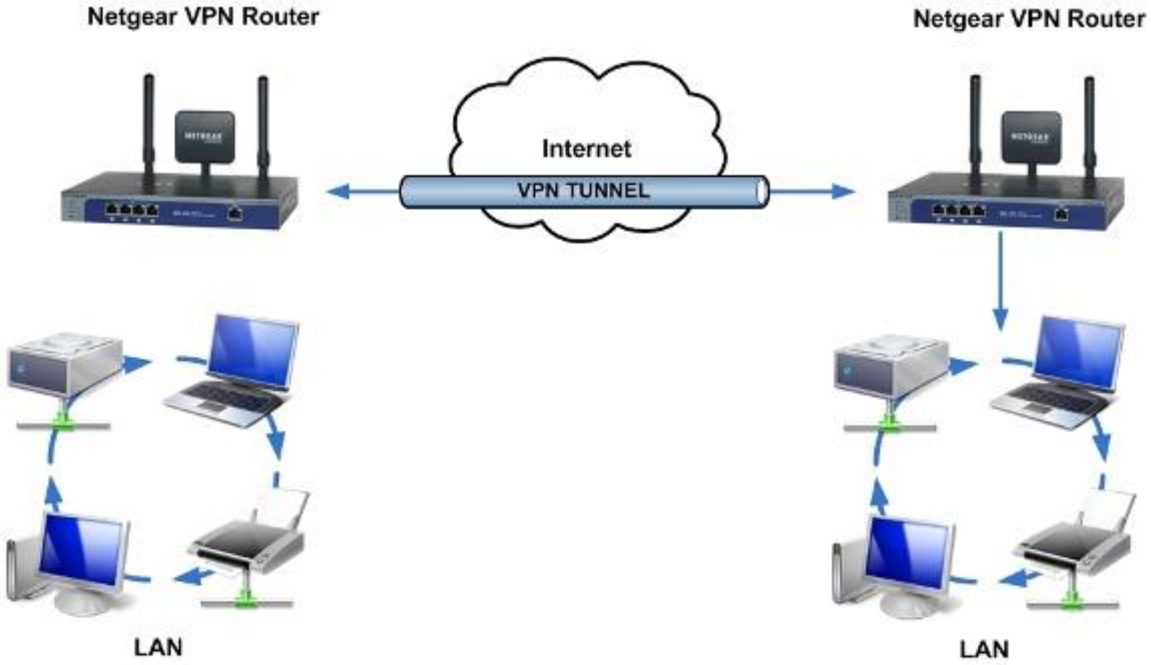
Hubs are now largely obsolete, having been replaced by network switches except in very old installations or specialized applications. As of 2011, connecting network segments by repeaters or hubs is deprecated by IEEE 802.3.

-Router

A router is a network switching networking device that may route network packets to other networks or devices depending on their addresses.

They're utilized for a variety of purposes, including Internet access, network coupling, and VPN connections between branch offices and a central office (Virtual Private Network).

(https://kb.netgear.com/1128/What-is-VPN-Virtual-Private-Networking, n.d.)



They interact via various access protocols, such as Ethernet, ATM, or DSL, depending on the model.

The switching of data packets through the router in the OSI layer model is dependent on the network layer address (layer 3). Multi-protocol routers, in addition to routers that utilize the Internet protocol (IP), may support a variety of additional network protocols.

Routers use packets to route and steer network data, which can include files, messages, and simple transfers such as web interactions. They are in charge of receiving, analyzing, and forwarding data packets between computer networks that are linked.

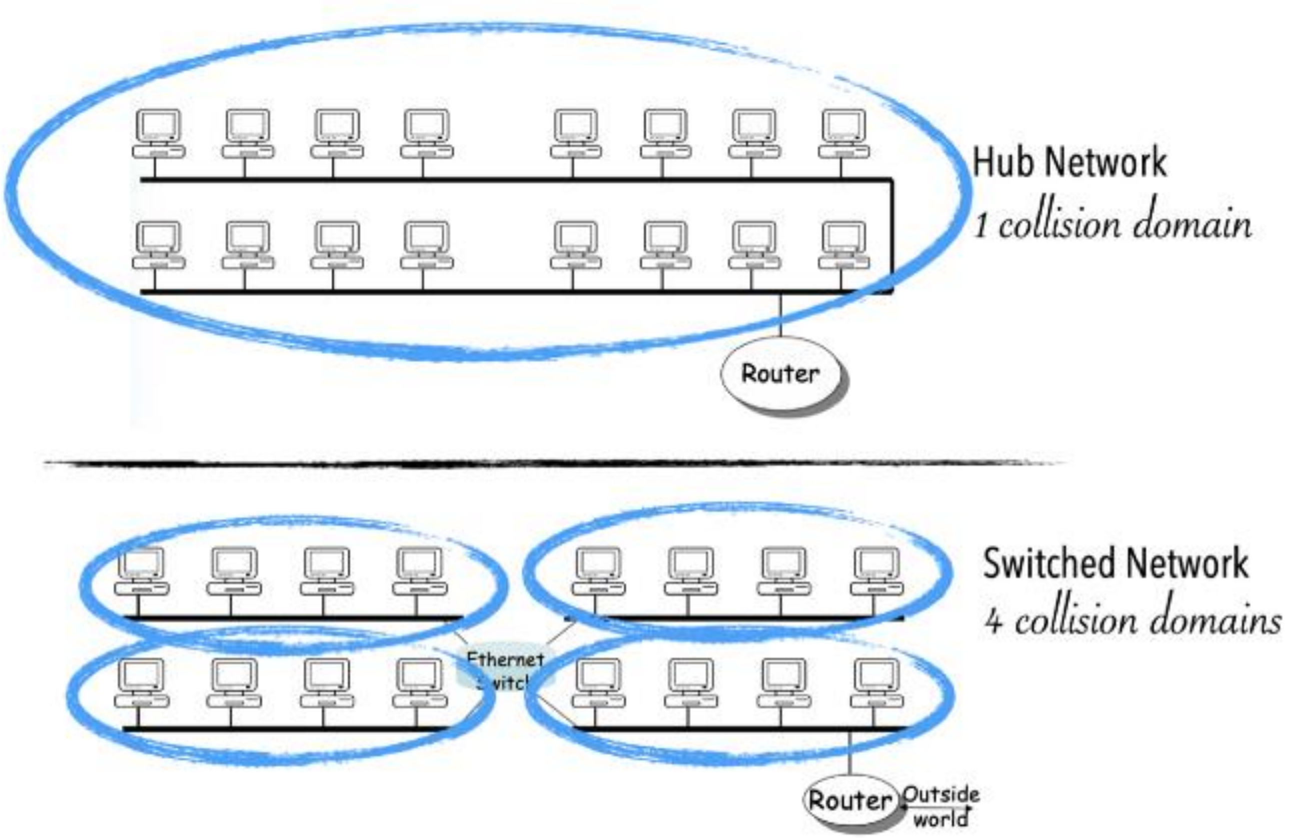
One of the layers, or sections, of the data packets contains identifying information such as sender, data type, size, and, most significantly, the destination IP (Internet protocol) address. This layer is read by the router, which prioritizes the data and selects the optimal path for each transmission.

When a data packet comes, the router looks at the destination address, examines its routing tables to determine the best route, and then sends the packet down that path.

-Switch

A network switch (also known as a switching hub, a bridging hub, or a MAC bridge according to the IEEE) is a networking data link layer hardware device that connects networking devices on a computer network by using packet switching to receive and forward data to the destination device via a multiport network bridge that uses MAC addresses to forward data packets at the OSI data link layer (layer 2) of the OSI model.

(https://avocado89.medium.com/networking-router-vs-switch-vs-hub-dbe75660c77e, n.d.)



By implementing routing capability, certain switches may also route data at the network layer (layer 3) and receive data over the network.

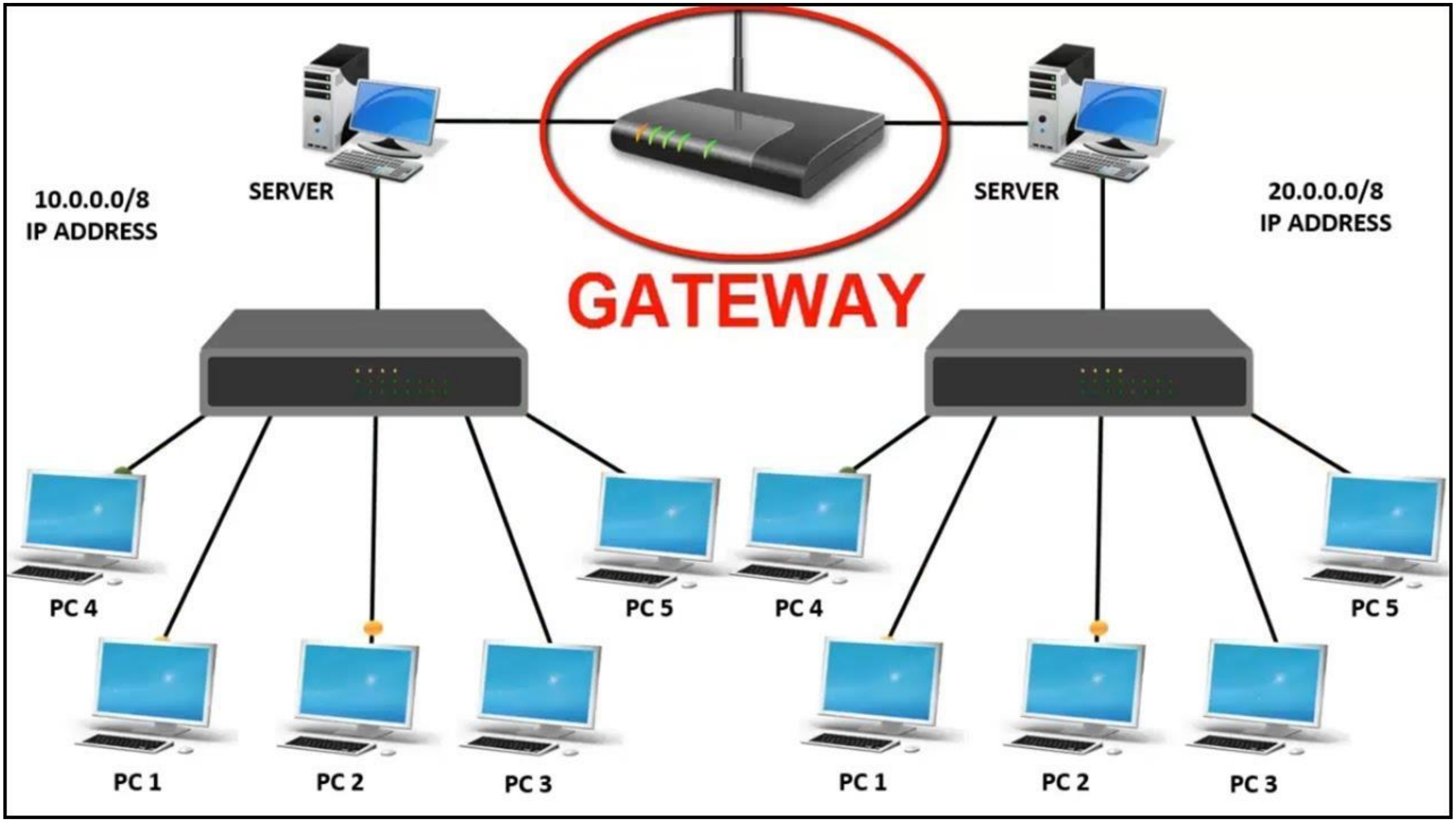
Such switches are commonly known as layer-3 switches or multilayer switches.

Like a hub, a switch also has many ports, to which computers are plugged in. However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding devices. Thus, it supports both unicast and multicast communications.

Gateway

In a telecommunications network, a gateway is a piece of networking hardware or software that allows data to be sent from one network to another. In contrast to routers and switches, gateways link many networks using a single protocol and may operate at any of the seven levels of the open system interconnection paradigm (OSI).

(https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3Dai5bFPVToMU&psig=AOvVaw2JcaIgmDRz2UryRcPoaIxD&ust=1640870955492000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCLCwseaOifUCFQAAAAAdAAAAABAc, n.d.)

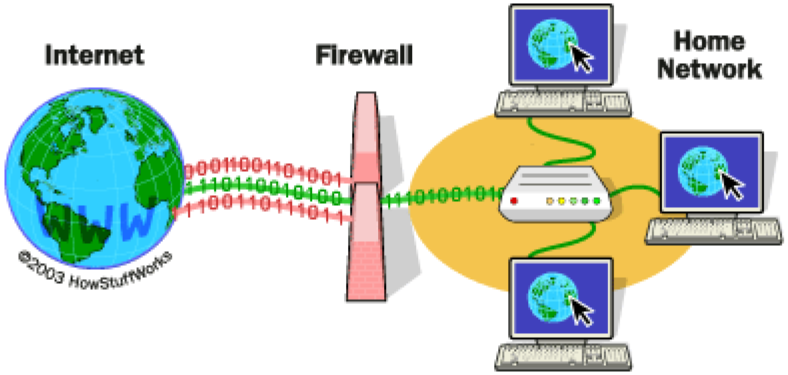


Firewall

A firewall is a network security device that can monitors incoming and outgoing messege network traffic and allows or disallows data packets according to a set of security rules.

Its take goal is to create a barrier between your internal network and incoming traffic from other sources on the internet, that harmful traffic like viruses and hackers can't get in.

(https://computer.howstuffworks.com/firewall.htm, n.d.)



• List server types

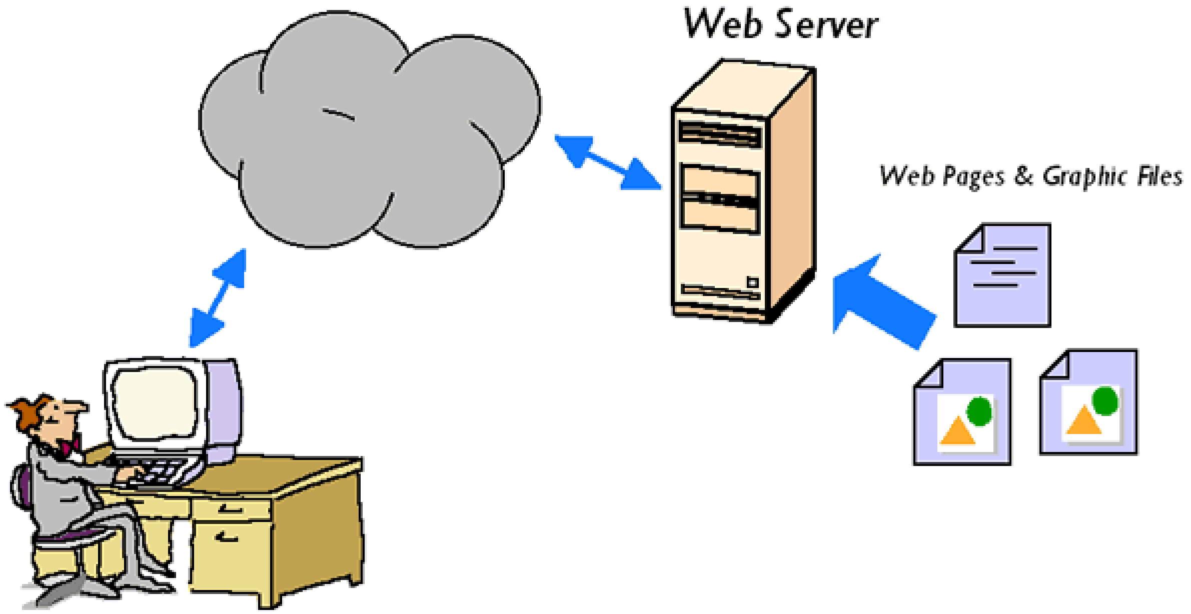
End devices: Web, mail, file, database combination, DHCP, DNS

virtualisation, terminal services server.

-Web

A web server is software and hardware that responds to client requests over the World Wide Web using HTTP (Hypertext Transfer Protocol) and other protocols. A web server's primary responsibility is to show website content by storing, processing, and distributing webpages to users.

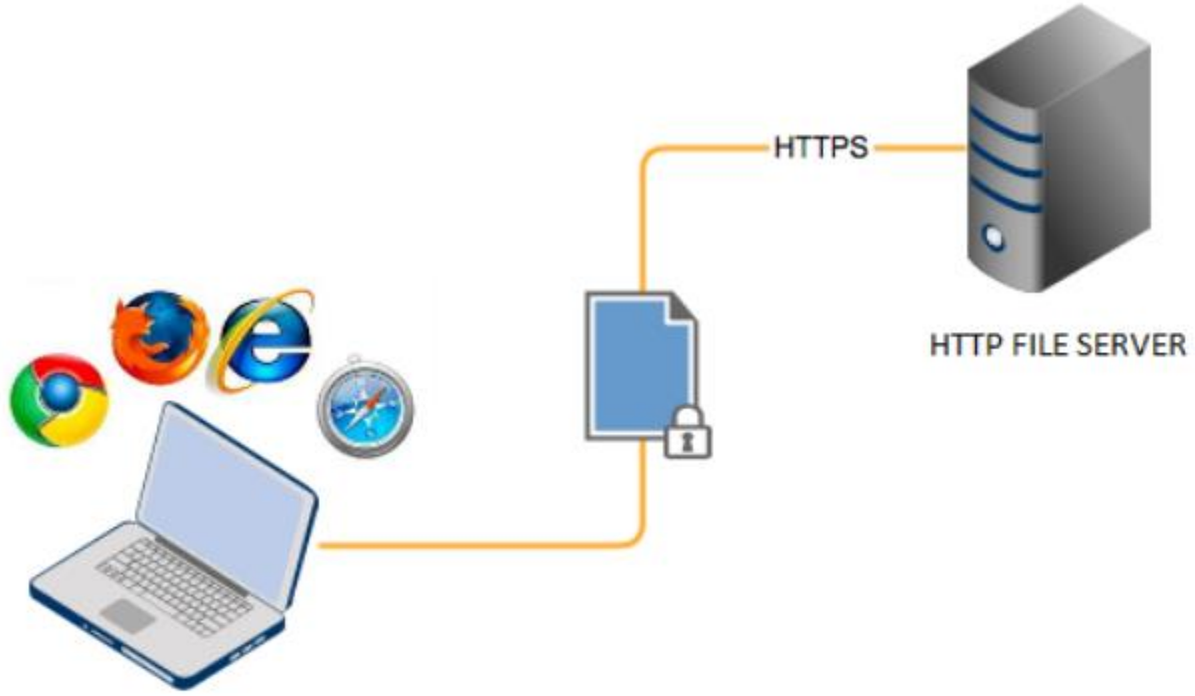
(https://firerox.org/web-server-la-gi/, n.d.)



-file

In a computer network, a file server is the central server that offers the file system, or at least portions of the file system, to connected clients. As a result, the file server gives users a central location to store files on the internal data medium that is available to all authorized clients.

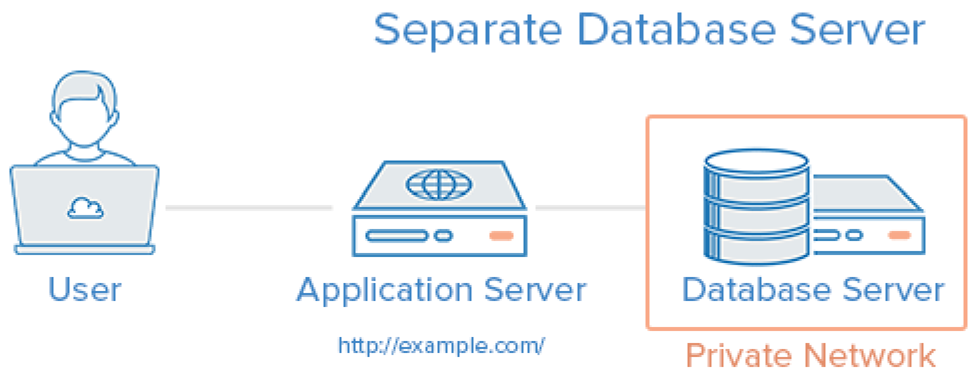
(https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.svnhostingcomparison.com%2Ffile-server-la-gi%2F&psig=AOvVaw3Qm6t4LveHJg652hQPZfsV&ust=1640707769764000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCJj0oYWvhPUCFQAAAAAdAAAAABAD, n.d.)



-database

Database servers are computers connected to a network and specialized to database storage and data retrieval. In a client/server computer context, the database server is a critical component. It is where the database management system (DBMS) and databases are stored.

(https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.digistar.vn%2F5-mo-hinh-pho-bien-de-cai-dat-server-cho-ung-dung%2F&psig=AOvVaw3gpntHvQipHTfHSFSiLKyH&ust=1640707937294000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCKjsvMuvhPUCFQAAAAAdAAAAABAD, n.d.)

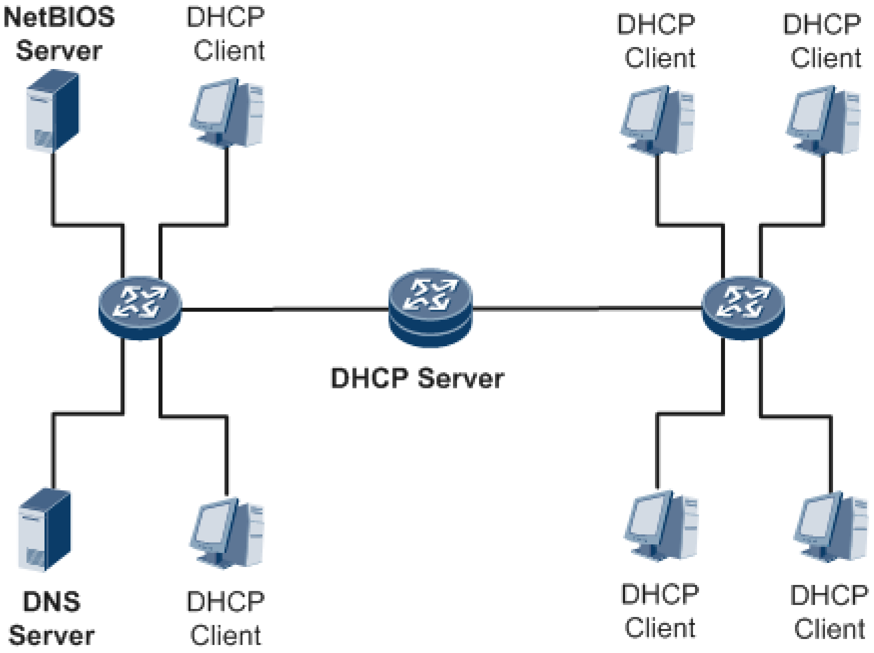


DHCP server

A DHCP (Dynamic Host Configuration Protocol) server is a network server that assigns IP addresses, default gateways, and other network information to client devices on a daily basis. It employs Dynamic Host Configuration Protocol, which automatically assigns IP addresses to devices on the network, to respond to broadcast queries from clients. We will be able to access the internet using the IP addresses supplied by the DHCP protocol, which is a standard protocol. It also guarantees that no two or more devices have the same IP address and gives configuration information such as DNS, subnet mask, and default gateway.

(https://www.google.com/url?sa=i&url=https%3A%2F%2Fsupport.huawei.com%2Fenterprise%2Fen%2Fdoc%2FEDOC1100143196%2F24a20adf%2Fconfiguring-a-dhcp-

server&psig=AOvVaw30ty7TD8u244grHsZtD2eF&ust=1640872426611000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCOjn46SUifUCF, n.d.)



The method DHCP works is simple: when a tool needs to enter the network, it sends a message of invitation to a router, and the router assigns it an available IP address.

The router serves as a DHCP server in small or domestic network configurations. A fervent server handles IP allocation since a router cannot manage a large number of devices in a large network.

For Assist PCs, laptops, phones, and tablets in swiftly establishing a network connection...

Manage IP addresses in an extremely scientific manner, eliminate overlapping IPs on many devices, and automate all networked device configurations.

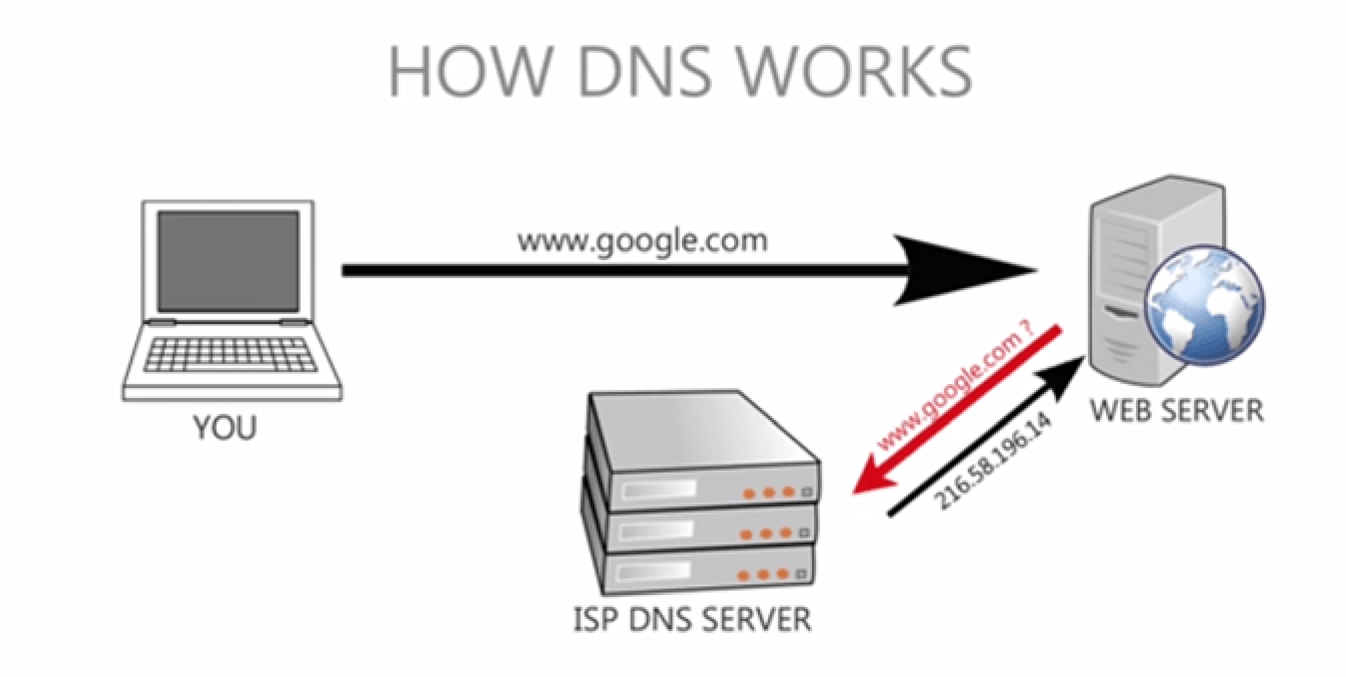
Between stations, easily manage IP addresses and TCP/IP specifications.

Network administrators may change IP settings and parameters to enhance infrastructure.

Devices may simply switch from one network to another and get new IP addresses right away.

DNS server

(https://digi9.net/212/danh-sach-cac-dns-server-thong-dung-tai-viet-nam/, n.d.)



DNS (Domain Name Service) is a domain name service that turns IP addresses into download resources from the Internet's web servers and listings, allowing web browsers to find the right IP address. The nameserver URL supplied there will be shown in the browser. When attempting to visit a website, you should normally type in the domain name. When consumers type in domain names like 'google.com' or 'facebook.com' into their web browsers, they get a lot of results.

DNS is in charge of determining the right IP address for such sites. To access the web page information, the browser utilizes that address to interact with the origin server or the CDN compilation server.

All of this is made possible by the DNS server, which is a computer dedicated to responding DNS requests.

However, in order to download material for a web page, the web browser has to know the correct IP address.

Networking software:

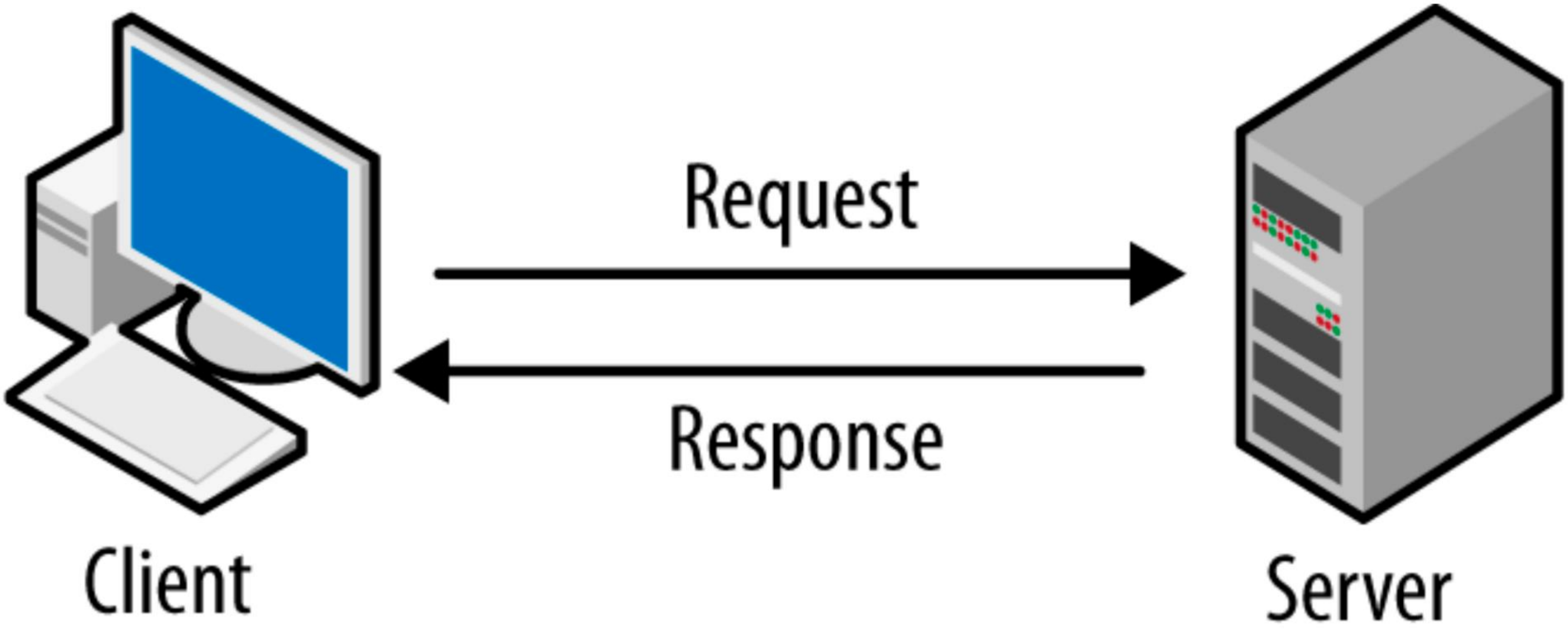
Client software, server software, client operating system, server operating system, Firewall.

-Client software,

Client software is a piece of software that is installed on your computer and can connect with other software across a network in the internet of world wide web.

Client software, on the other hand, does not require a network connection to execute on your computer.

(https://www.google.com/url?sa=i&url=https%3A%2F%2Fmadooei.github.io%2Fcs421_sp20_homepage%2Fclient-server-app%2F&psig=AOvVaw3AKBrOrEQa-l1ZK2OQkDmf&ust=1640708422644000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCLDw9aixhPUCFQAAAAAdAAAAABAD, n.d.)



-Server software

Server software is designed to connect with the physical infrastructure of a server, which includes the CPU, memory, storage, I/O, and other communication interfaces. Server software may be classed in a variety of ways depending on the type of server and how it is used, on the following:

Web server software

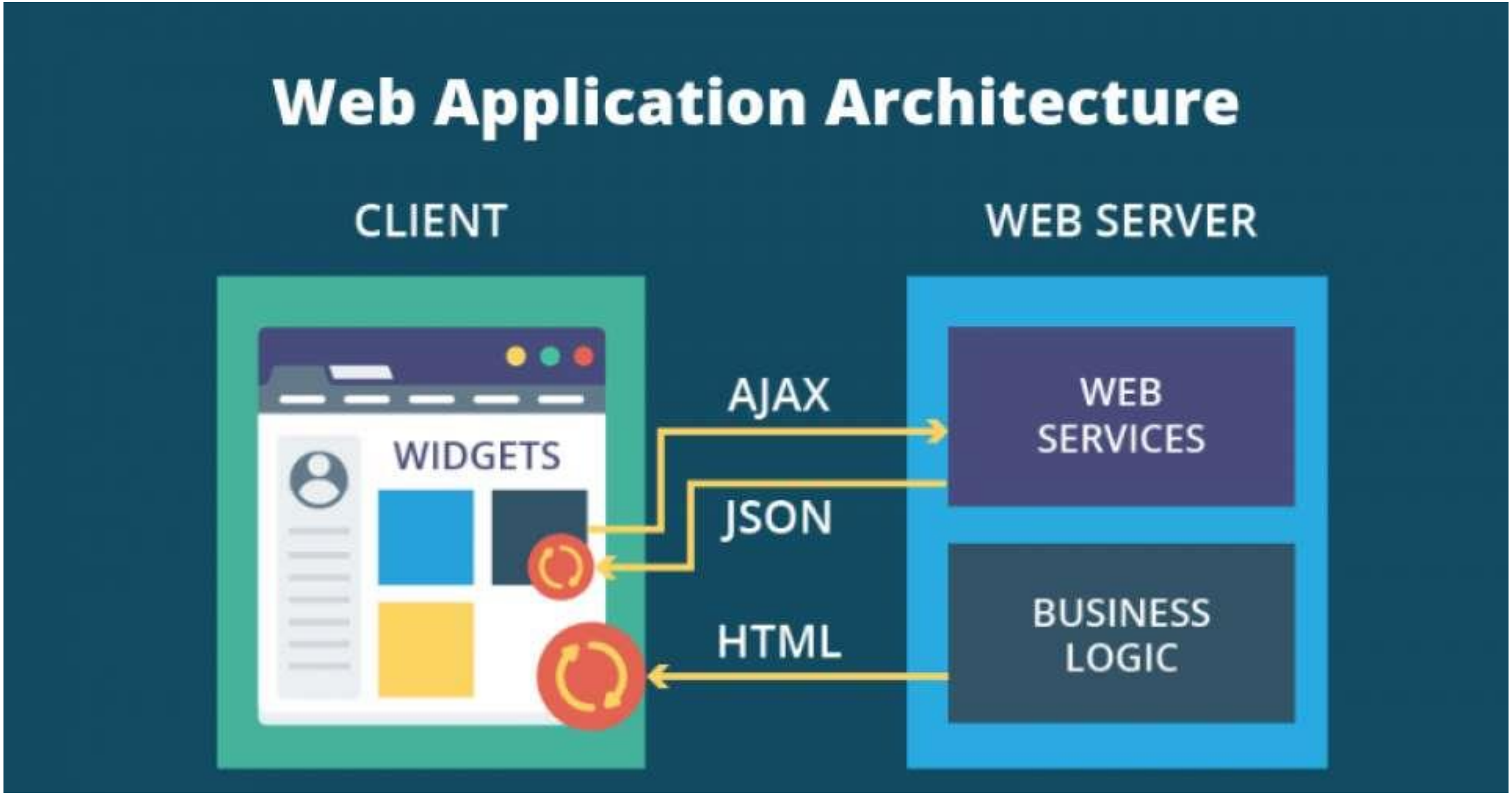
Application server software

Database server software

Cloud computing server software

File server software

(https://www.google.com/url?sa=i&url=https%3A%2F%2Fhackr.io%2Fblog%2Fweb-application-architecture-definition-models-types-and-more&psig=AOvVaw3vOtJB5Mmu_BRPUTlcsCm6&ust=1640708214216000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCLD40cSwhPUCFQAAAAAdAAAAABAf, n.d.)



Each of the aforementioned types of server software uses the server for different purposes and services, but they all have the same goal in mind: to make the most of the computer's natural capability and capabilities. Server software can also be for a physical, virtual, or cloud server that is based on a real server.

P4 Discuss the inter-dependence of workstation hardware with relevant networking software.

**Như kiểu giới thiệu cái Cisco Packet Tracer gồm những gì

Server selection:

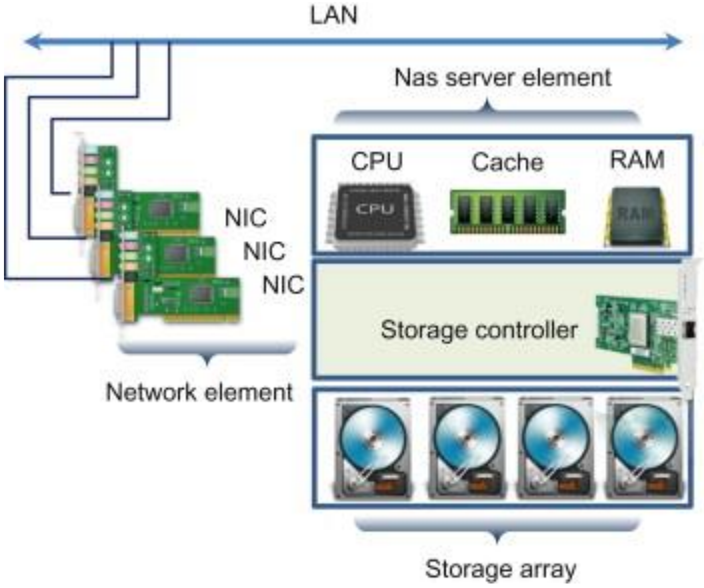
Cost, purpose, operating system requirement.

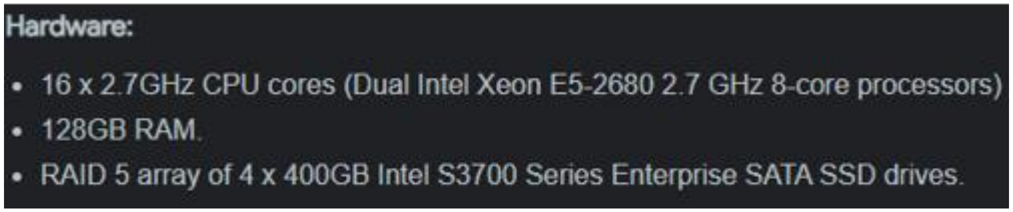
Workstation:

--Hardware e.g. network card, cabling; permissions; system bus; local-system architecture e.g. memory, processor, I/O devices.

CPU, RAM, DISK, NIC (network interface card)

(https://www.sciencedirect.com/topics/computer-science/network-attached-storage, n.d.)





Hardware:

- 16 x 2.7GHz CPU cores (Dual Intel Xeon E5-2680 2.7 GHz 8-core processors)
- 128GB RAM.
- RAID 5 array of 4 x 400GB Intel S3700 Series Enterprise SATA SSD drives.

--Networking Software: web, mail, file, DHCP, DNS, application, MISA, accounting software, network monitoring system

Web

In contrast to computer-based software applications that run locally on the operating system (OS) of the device, a web application (or web app) is application software that operates on a web server. The user uses a web browser with an active network connection to access web apps.

Apache HTTP Server

Nginx Web Server.

Lighttpd Web Server.

Apache Tomcat.

mail,

(https://en.wikipedia.org/wiki/List_of_mail_server_software, n.d.)

SMTP[edit]

agorum core

Apache James

Axigen

Citadel

POP/IMAP[edit]

agorum core

Apache James

Axigen

Bongo

Mail filtering[edit]

Anti-Spam SMTP Proxy

Axigen

Bogofilter

Clearswift Secure Email Gateway

Mail server packages

Mail-in-a-Box

iRedmail[4]

Modoboa[5]

file,

Plex Media Server. Image Source

Amahi Home Server

Windows Home Server

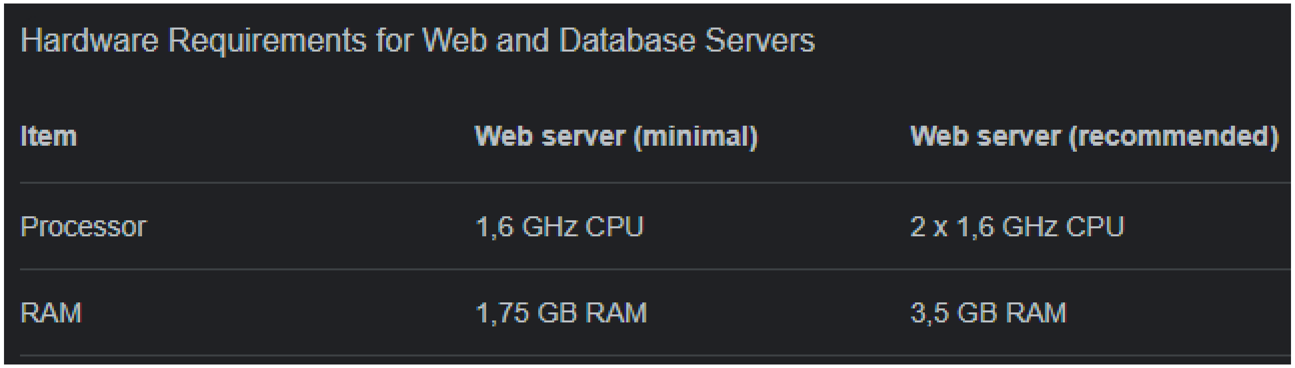
FreeNAS.

--Hardware vs Software

It’s need System requirements to run a software on a computer hardware

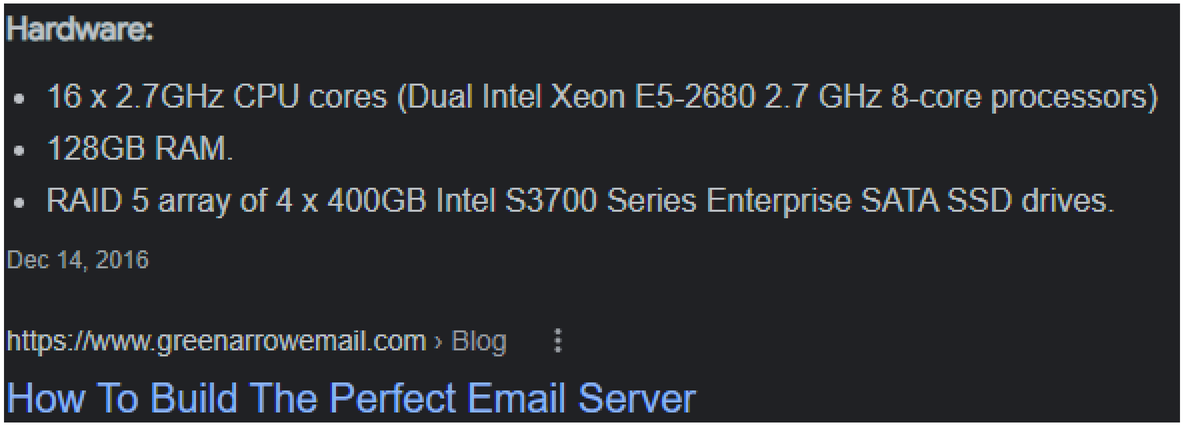
Definition:

All computer program requires the presence of specific hardware components or other software resources in order to function properly. These criteria are referred to as (computer) system requirements, and they are frequently utilized as a guideline rather than an absolute law. Most software has two sets of minimum and recommended system requirements. System requirements tend to rise over time as demand for more processing power and resources in newer versions of software grows. According to industry observers, this tendency is more important than technology developments in pushing updates to current computer systems. A second definition of the phrase "system requirements" is a broadening of the first, describing the criteria that must be satisfied in the design of a system or subsystem.



Hardware Requirements for Web and Database Servers

Item	Web server (minimal)	Web server (recommended)
Processor	1,6 GHz CPU	2 x 1,6 GHz CPU
RAM	1,75 GB RAM	3,5 GB RAM



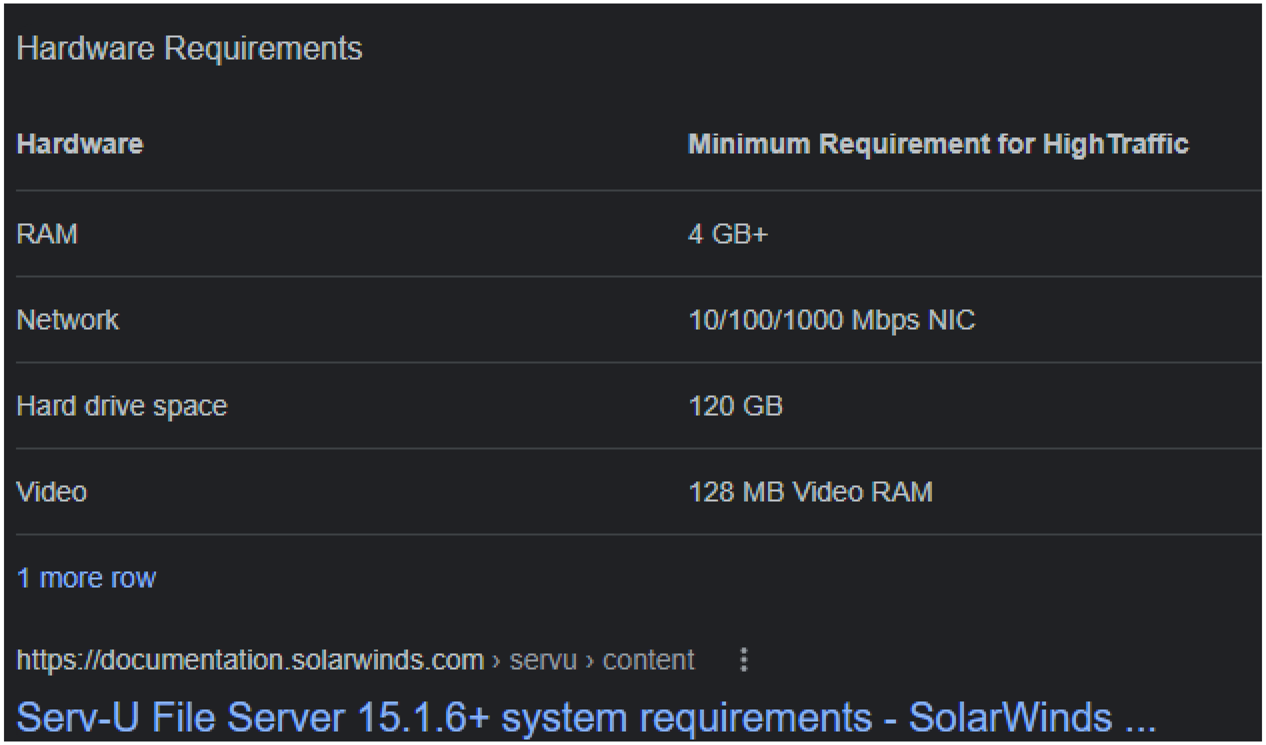
Hardware:

- 16 x 2.7GHz CPU cores (Dual Intel Xeon E5-2680 2.7 GHz 8-core processors)
- 128GB RAM.
- RAID 5 array of 4 x 400GB Intel S3700 Series Enterprise SATA SSD drives.

Dec 14, 2016

https://www.greenarrowemail.com › Blog

How To Build The Perfect Email Server



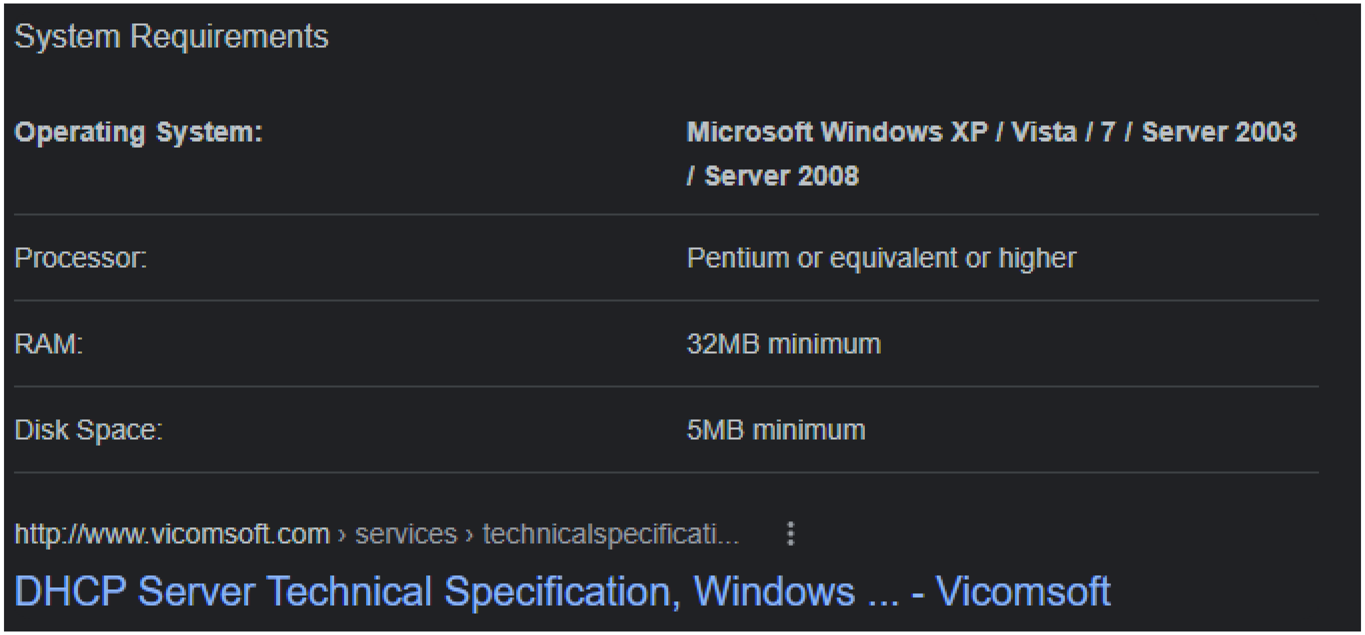
Hardware Requirements

Hardware	Minimum Requirement for High Traffic
RAM	4 GB+
Network	10/100/1000 Mbps NIC
Hard drive space	120 GB
Video	128 MB Video RAM

1 more row

https://documentation.solarwinds.com › servu › content

Serv-U File Server 15.1.6+ system requirements - SolarWinds ...



System Requirements

Operating System:	**Microsoft Windows XP / Vista / 7 / Server 2003 / Server 2008**
Processor:	Pentium or equivalent or higher
RAM:	32MB minimum
Disk Space:	5MB minimum

http://www.vicomsoft.com › services › technicalspecificati...

DHCP Server Technical Specification, Windows ... - Vicomsoft

➔ *Interdependence btw workstation hardware and software: 2.2. operating systems (Principles of network and system administrations)*

➔

➔ *Workstation Hardware: networking a beginner's guide. Chapter 3. Pag3 3.*

➔ *Understanding Networking. Networking: A Beginner's Guide. +chapter 14: Understanding Network Workstation Requirement*

• Explain what is meant by interdependencies

• Give examples of interdependency.

• Define workstation hardware

• Define networking software

Discuss and explain the interdepencies of workstation hardware with networking software. Derive an example form your discussion