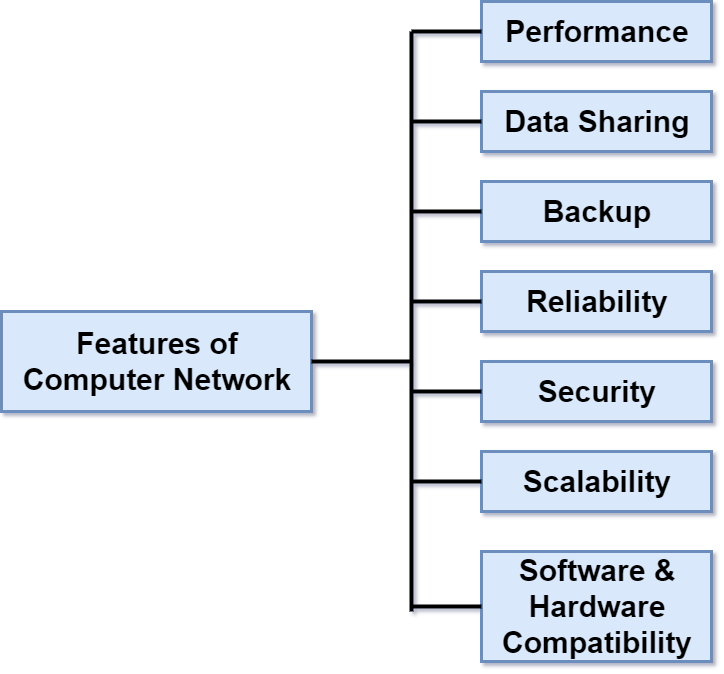
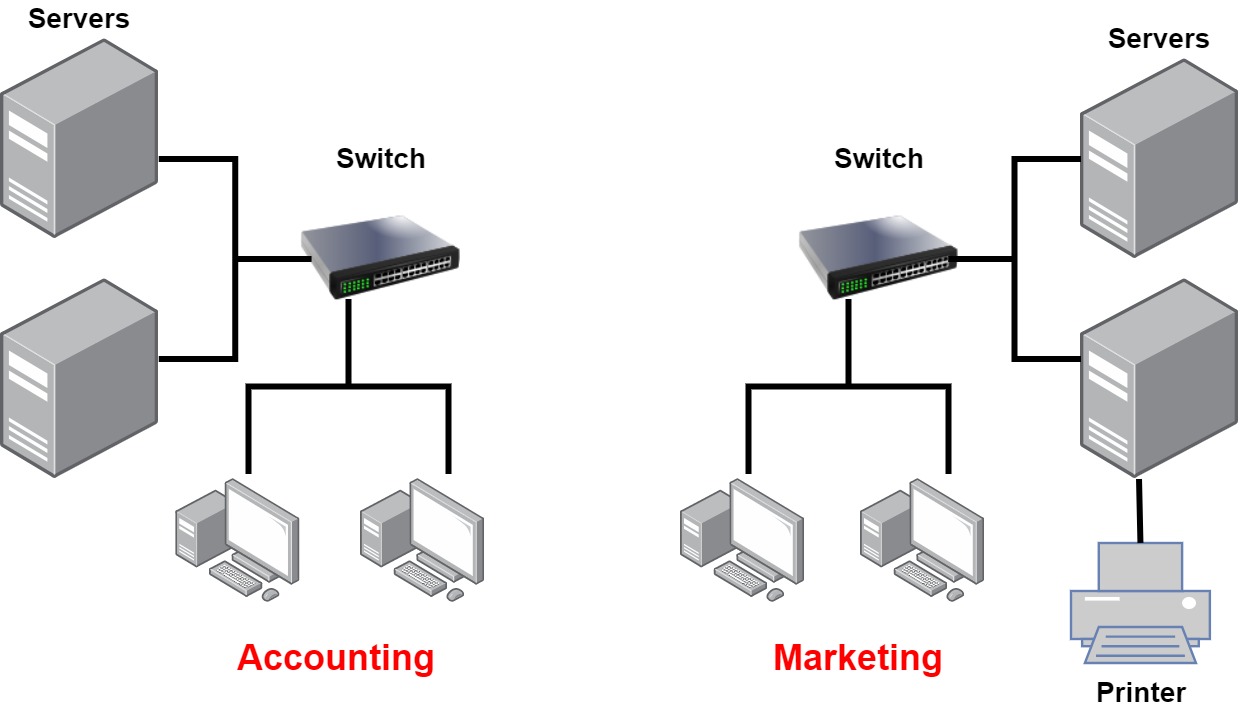
Q: What is a Computer Network?  
A: A computer network is a connection network between two or more nodes using [Physical Media](https://lms.clarusway.com/mod/lesson/view.php?id=1839" \o "Physical Media) Links viz., cable, or wireless to exchange data over pre-configured services and Protocols. A computer network is a collective result of – Electrical Engineering, Computer Science, Telecommunication, Computer Engineering, and Information Technology involving their theoretical as well as practical aspects into action. The most widely used Computer Network of Today is the Internet which supports the World Wide Web (WWW).

 - Interview Q&A

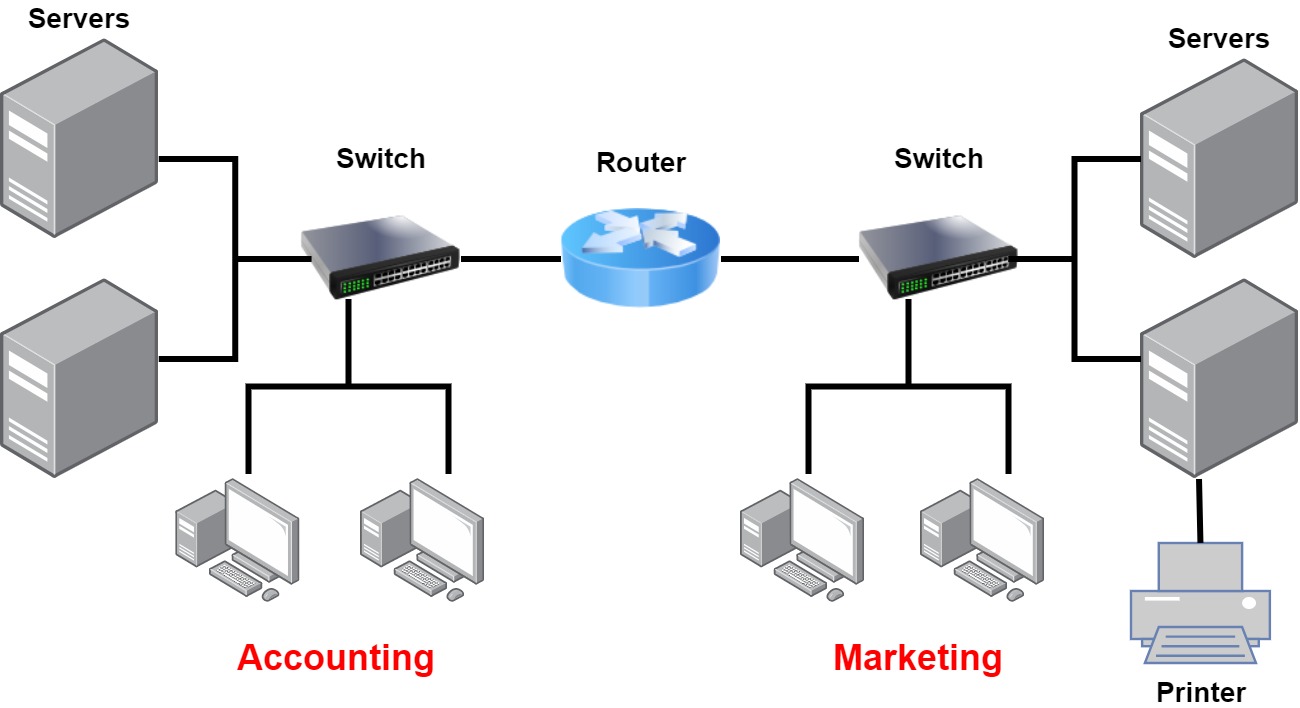


Q: Explain what is LAN?  
A: A LAN or Local Area Network is the network between devices that are located within a small physical location. It can be either wireless or wired. One LAN differs from another based on the following factors:  
**Topology:** The arrangement of nodes within the network  
**Protocol:** Refer to the rules for the transfer of data  
**Media:** These devices can be connected using optic fibers, twisted-pair wires, etc.

- Interview Q&A

Two separate LANs

A network with two LANs



Common Network Components

**Node, Stations, and Hosts:** A **node** is any device that can connect to a network. The term **node** can be used to describe *endpoint devices*, such as *computers, laptops, servers, IP phones, smartphones, or printers*, and *connecting or forwarding devices*, such as *switches* and *routers*. A **node** on a wireless network is often called a ***station*.**

The term **host** is often used in *TCP/IP networking* to mean an *end system device*, such as a *computer*, with a unique IP address on the network.

**Workstations:** Workstation is a client **machine** used to deploy an **application** or **server**. They are usually powerful **computers** that have more than one CPU and its resources are available to other users on the network. Workstations are often equipped with systems for end-users to use daily.

**Servers:** Servers are also powerful **computers**. They are “at the service” of the network and run specialized software known as the network operating system to maintain and control the network. Servers are highly specialized and handle important labor-intensive jobs. In order to get better performance, a single task is often assigned to a dedicated server. Here’s a list of common dedicated servers: **File Server** - Stores and manages files.

* **Mail Server** - It's the network’s post office; handles email functions
* **Print Server** - Manages printers on the network
* **Web Server** - Manages web-based activities by running Hypertext Transfer Protocol (HTTP) for storing web content and accessing web pages
* **Application Server** - Manages network applications
* **Telephony Server** - Handles the call center and call routing
* **Proxy Server** - Handles tasks in the place of other machines on the network, particularly an internet connection.

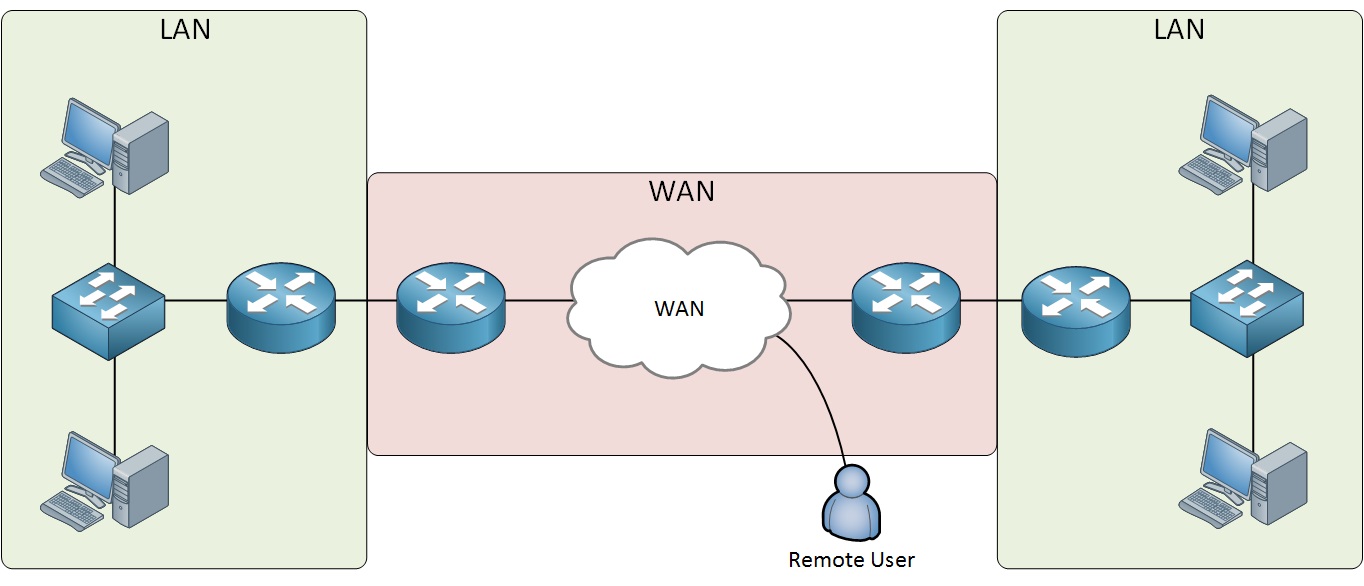
Q: What do you mean by a Node?  
A: The intersection point in a network is called a Node. Nodes can send or receive data/ information within a network. For example, if two computers are connected to form a network, there are 2 nodes in that network. Similarly, in the case of adding more computers, there will be more nodes and so on. It is not necessary for a node to be a computer, it can be any communication device such as a printer, servers, modems, etc..

- Interview Q&A

Wide Area Network (WAN)

Our own networks are called **LANs** (Local Area Network). We own and operate these networks. It’s called a **“local”** area network since all devices that make up the LAN are close to each other. Perhaps in one building or a few buildings close to each other (called a **campus**).

When we need to access other remote networks or give others access to our LAN, we need a **WAN (Wide Area Network)**. As the name implies, WANs cover *large geographical areas*. This could be a network between two cities or as large as the **Internet**.



Below is the list of some differences between WAN and LANs:

* WANs usually need a router.
* WANs span larger geographic areas and/or can link diverse locations.
* WANs are usually slower.
* We can choose when and how long we connect to a WAN. A LAN is all or nothing—our workstation is connected to it either permanently or not at all.
* WANs can utilize either private or public data transport media such as phone lines.
* Q: What is WAN?
* A: WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are located in different regions and countries.
* - Interview Q&A

**Physical Network Topologies**

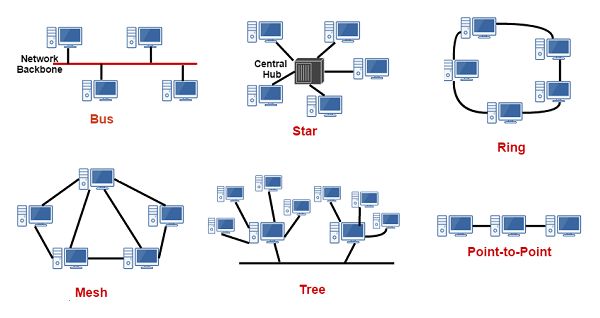
Network topology is the arrangement of the various nodes of a computer network. Essentially, it is the topological structure of a network and may be depicted physically or logically which are the two basic categories of network topologies.

The shape of the cabling layout used to link devices is called the **physical topology** of the network.

In opposition to the Physical Topology, the **logical topology** is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices.

Here’s a list of the topologies mostly used nowadays:

Bus Star Ring Mesh Tree Point-to-point Point-to-multipoint Hybrid



Q: What do you mean by network topology?  
A: Network topology specifies the layout of a computer network. It shows how devices and cables are connected to each other. Some types of topologies are: Bus, Star, Ring, Mesh, etc.

- Interview Q&A

Q: Describe star topology  
A: Star topology consists of a central hub that connects the nodes. This is one of the easiest way to setup and maintain.

- Interview Q&A

Q: What is the disadvantage of a star topology?  
A: One major disadvantage of star topology is that once the central hub or switch damaged, the entire network becomes unusable.

- Interview Q&A

Q: What are some drawbacks of implementing a ring topology?  
A: In case one workstation on the network suffers a malfunction, it can bring down the entire network. Another drawback is that when there are adjustments and reconfigurations needed to be performed on a particular part of the network, the entire network has to be temporarily brought down as well.

- Interview Q&A

Q: What is mesh topology?  
A: Mesh topology is a setup wherein each device is connected directly to every other device on the network. Consequently, it requires that each device has at least two network connections.

- Interview Q&A

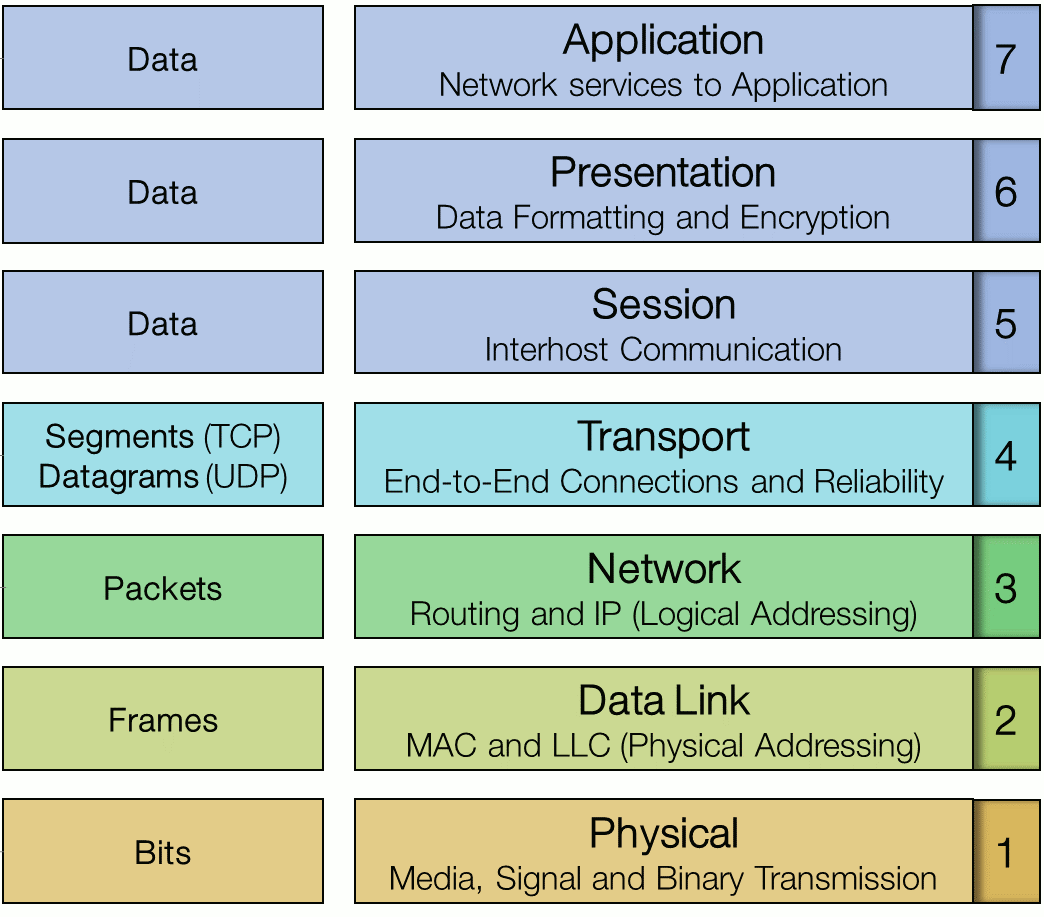
Q: What is one advantage of mesh topology?  
A: In the event that one link fails, there will always be another available. Mesh topology is actually one of the most fault-tolerant network topology.

- Interview Q&A

What is the OSI Reference Model?

**OSI** stands for *Open System Interconnection*. **The OSI Model** defines how **data is transferred** from one computer to another computer regardless of the operating system or vendor of the hardware.

The OSI Network Layers



**Physical Layer**

The physical layer of the OSI model (layer 1) is responsible for the transmission and receipt of bits from one node to another. It specifies the follDevices operating at the physical layer include:

* **Transceiver** - the part of a network interface that sends and receives signals over the network media.
* **Media Converter** - converts one media signaling type to another.
* **Repeater** - amplifies the signal to extend the maximum allowable distance for a media type.
* **Hub** - a multiport repeater, deployed as the central point of connection for nodes wired in a star topology.
* **Modem** - a device that converts between digital and analog signal transmissions (**MO**dulator-**DEM**odulator).

**Data Link Layer**

The data link layer (layer 2) is responsible for transferring data between noConnectivity devices found at the data link layer include:

* **Network adapter (or Network Interface Card [NIC])** - joins a host computer to network media (cabling or wireless) and enables it to communicate over the network by assembling and disassembling frames.
* **Bridge** - joins two network segments while minimizing the performance reduction of having more nodes on the same network.
* **Basic switch** - a multiport bridge that creates links between nodes more efficiently.
* **Wireless Access Point (AP)** - allows nodes with wireless network cards to communicate and joins wireless networks to wired ones

des on the same network segment

**Network Layer**

The network layer (layer 3) is responsible for moving data around a network of networks, known as an internetwork or internet.

The main appliance working at layer 3 is the **router**. Other devices include **Layer 3 switches** (combining the function of switches and routers) and basic firewalls.

**Transport Layer**

The first 3 layers of the OSI model are primarily involved with moving **frames** and **datagrams** between nodes and networks. At the *transport layer* (also known as the end-to-end or host-to-host layer) the content of the packets starts to become significant.

Devices working at the transport layer (or above) include multilayer switches and security appliances such as more advanced firewalls and Intrusion Detection Systems (IDS).

**Session Layer**

Most application protocols require the exchange of multiple messages between the client and the server. This exchange of such a sequence of messages is called a **session** or **dialog**. The session layer (layer 5) represents the dialog control functions that administer the process of establishing the dialog, managing data transfer, and then ending (or "tearing down") the session.

Sessions can work in three modes:

* **One-way/simplex** - only one system is allowed to send messages; the other receives only.
* **Two-Way Alternate (TWA)/half-duplex** - the hosts establish some system for taking turns to send messages, such as exchanging a token.
* **Two-Way Simultaneous (TWS)/duplex** - either host can send messages at any time.

In summary, this layer primarily manages applications’ data by separating from each other application. For instance, multiple web browser sessions at the same time on your desktop are handled by the help of session layer

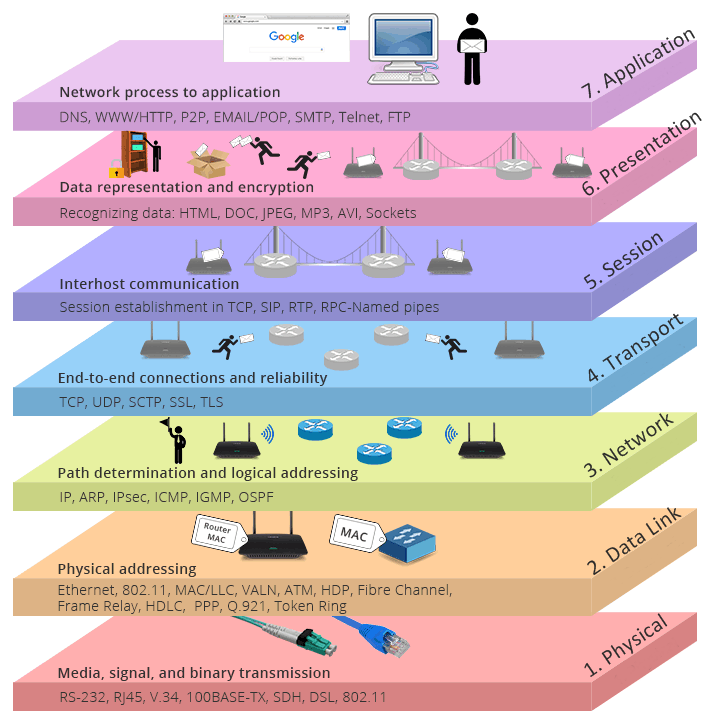
**Presentation Layer**

The presentation layer (layer 6) transforms data between the format required for the network and the format required for the application

**Application Layer**

The application layer (layer 7) is at the top. An application layer protocol doesn’t encapsulate any other protocols or provide services to any protocol. An application layer protocol provides an interface for software applications on network hosts that have established a communication channel using the lower-level protocols to exchange data. For example, one of the most utilized services provided by the application layer is file transfer.

The OSI Reference Model



Q: What is data encapsulation?  
A: Data encapsulation is the process of breaking down information into smaller manageable chunks before it is transmitted across the network. These chunks are wrapped with protocol information at each layer of the OSI model. In this process, the source and destination addresses are attached into the headers, along with parity checks.

- Interview Q&A

Q: What is ethernet?  
A: Ethernet is a network technology used in LAN and WAN that connects devices using cables for the transmission of data. It provides services on the Physical and Data Link layers of the OSI Model.

- Interview Q&A

Common Network Connectivity Devices

Network Interface Card

Today, it is almost impossible or at least very rare that a computer without **network interface card (NIC)** hardware can connect over a network. NIC is a circuit board that is installed in a computer to provide a dedicated network connection to the computer. It is also called **network in**Q: What is NIC?  
A: NIC is short for Network Interface Card. This is a peripheral card that is attached to a PC in order to connect to a network. Every NIC has its own MAC address that identifies the PC on the network.

- Interview Q&A**terface controller, network adapter**, or **LAN adapter**.

Hub

Hub is an elementary networking device, as it provides very simple functionality of establishing a connection between several devices. It does not have **segmentation capability**. Hub does not perform any filtration which means that each chunk of data is transmitted to all the connected end devices even if it is not a destined device. That is the reason it is said to be an unintelligent device. Today, hubs are considered obsolete and **switches** are commonly used instead.

Bridge

The bridge is also a networking device that connects two different LAN operating on the same protocol. Furthermore, it is used for *splitting* the larger LAN into smaller networks. The bridge allows the traffic to pass through only if the transmission is sent to a station on the opposite side. They are outdated now and switches are preferred to bridges.

Switch

Like hubs, a switch is used to connect multiple hosts together, but it has many advantages over a hub. A switch is an **OSI Layer 2** device, which means that it can inspect received traffic and make forwarding decisions. Each port on a switch is a separate collision domain and can run in a full-duplex mode.

Q: What is the difference between a hub and a switch?  
A: A hub acts as a multiport repeater. However, as more and more devices connect to it, it would not be able to efficiently manage the volume of traffic that passes through it. A switch provides a better alternative that can improve the performance especially when high traffic volume is expected across all ports.

- Interview Q&A

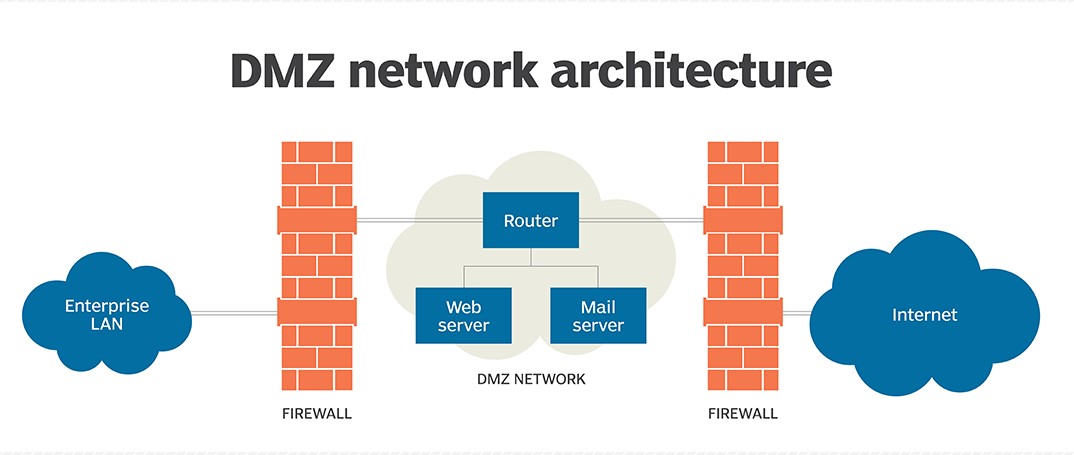
Router

A **router** is a network device used to connect many, sometimes disparate, network segments together, combining them into what we call an internetwork. A well-configured router can make intelligent decisions about the best way to get network data to its destination. It gathers the information it needs to make these decisions based on a network’s particular performance data. As routers use IP addresses to make forwarding decisions, they are considered **Layer 3** devices.

**Note:** **Routers**can have many different names: **Layer 3 switch** and **multilayer switch** are the most common, besides the name router, of course. Remember, if you hear just the word **switch**, that means a **Layer 2**device. **Routers, Layer 3 switches**, and **multilayer switches** are all **Layer 3** devices

Firewall

For networks, security is crucial! A **firewall** protects your LAN resources from invaders that prowl the Internet for unprotected networks while simultaneously preventing all or some of your LAN’s computers from accessing certain services on the Internet. You can employ them to filter packets based on rules that you or the network administrator create and configure to strictly delimit the type of information allowed to flow in and out of the network’s Internet connection. Firewalls operate at *multiple layers of the OSI model*. Some firewalls can operate up to the *Application layer*.



Q: Explain what is a firewall?  
A: A firewall is a network security system which is used to monitor and control the network traffic based on some predefined rules. Firewalls are the first line of defense and establish barriers between the internal and external networks in order to avoid attack from untrusted external networks. Firewalls can be either hardware, software or sometimes both.

- Interview Q&A

IDS/IPS

**Intrusion detection systems (IDSs)** and **intrusion prevention systems (IPSs)** are very important in today’s networks. They are network security appliances that monitor networks and packets for malicious activity. An **IDS** is considered *monitor mode* and just records and tells you about problems, whereas an **IPS** can work in real-time to *stop threats* as they occur. The main difference between them is that an IPS works inline to actively prevent and block intrusions that are detected based on the rules you set up. IPSs can send an *alarm, create correlation rules and remediation, drop malicious packets, provide malware protection*, and *reset the connection* of offending source hosts.

Q: What is TCP/IP?  
A: TCP/IP is short for Transmission Control Protocol / Internet Protocol. This is a set of protocol layers that is designed to make data exchange possible on different types of computer networks, also known as heterogeneous network.

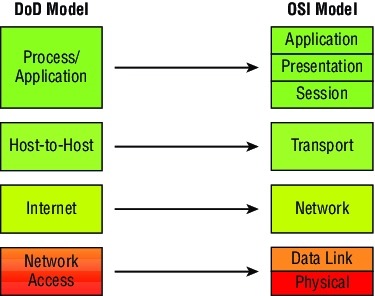
- Interview Q&A

TCP/IP and the DoD Model

The Department of Defense created TCP/IP to ensure and preserve data integrity. The DoD model is a condensed version of the OSI model and only has four layers that are:

* Process/Application layer
* Host-to-Host layer
* Internet layer
* Network Access Layer

The DoD and OSI models are identical in design and concept and have similar functions in similar layers.



**1. Process/Application layer**

The Application layer of the DoD model is equivalent to the upper three layers of the OSI model, i.e., Session layer, Presentation layer, and Application layer. The Process/Application layer of the DoD model provides the following capabilities:

* Enable applications to communicate with each other.
* Provides access to the services that operate at the lower layers of the DoD model.
* It contains a protocol that implements user-level functions such as mail delivery, file transfer, and remote login.

**2. Host-to-Host layer**

A host-to-host layer of the DoD model performs the same functions as the Transport Layer of [the OSI reference model](https://lms.clarusway.com/mod/lesson/view.php?id=1837" \o "The OSI Reference Model). It handles issues such as flow control, reliable end-to-end communication, and ensuring error-free delivery of the data. Protocols that operate on the Host-to-Host layer are TCP and UDP.

**3. Internet layer**

Internet layer of the DoD model performs the same functions as the Network layer of [the OSI reference model](https://lms.clarusway.com/mod/lesson/view.php?id=1837" \o "The OSI Reference Model). It handles the packaging, addressing, and routing of packets among multiple networks. This layer also establishes a connection between two computers to exchange the data.

**4. Network Access Layer**

The Network Access layer of the DoD model is equivalent to the lower two layers (Data Link, and Physical) of the OSI model. The hardware connected to Network access layer are:

* Network medium: Cables like coaxial, twisted pair. Today, mostly, we use a wireless medium such as Bluetooth, WI-FI.
* Network Interface Card (NIC) has two types of addresses.
  + MAC Address- It is a 48 bits physical address.
  + IP Address – It is a 32 bits logical address.

Key features of TCP and UDP

The below table highlights some of the key concepts that you should keep in mind regarding these two protocols.

| **TCP** | **UDP** |
| --- | --- |
| Sequenced | Unsequenced |
| Secure | Unsecure |
| Connection-oriented | Connectionless |
| Slow | Fast |
| Guaranteed transmission | No guarantee |
| Flow control | No flow control |
| Reliable | Unreliable |
| Virtual circuit | No virtual circuit |
| High overhead | Low overhead |
| Acknowledgment | No acknowledgment |
| Windowing flow control | No windowing or flow control |
| 20 bytes header | 8 bytes header |

IP Terminology

**Done:**Go through the activity to the end

IP Terminology

Throughout this section, you’ll learn several important terms vital to your understanding of the **Internet Protocol**. Here are a few to get you started:

* **Bit** - A bit is one binary digit, either a 1 or a 0.
* **Nibble** - A nibble is 4 bits.
* **Byte** - A byte is 8 bits.
* **Octet** - An octet, made up of 8 bits, is just an ordinary 8-bit binary number. In this section, the terms byte and octet are completely interchangeable.
* **Network Address** - This is the designation used in routing to send packets to a remote network—for example, 10.0.0.0, 172.16.0.0, and 192.168.10.0.
* **IP Address** - A logical address used to define a single host; however, IP addresses can be used to reference many or all hosts as well. If you see something written as just IP, it is referring to IPv4. IPv6 will always be written as IPv6.
* **Broadcast Address** - The broadcast address is used by applications and hosts to send information to all hosts on a network. Examples include 255.255.255.255, which designates all networks and all hosts; 172.16.255.255, which specifies all subnets and hosts on network 172.16.0.0; and 10.255.255.255, which broadcasts to all subnets and hosts on network 10.0.0.0.