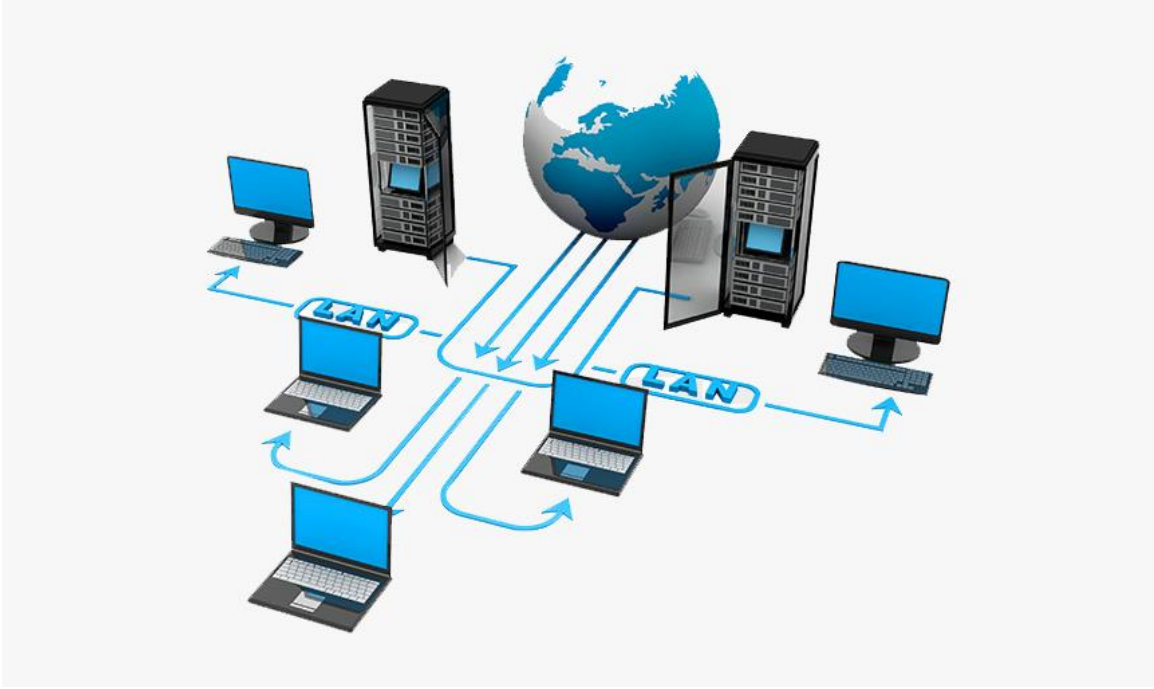
معلومات مفيدة لاختبار وظيفة (اخصائي حاسب آلي)

حسب تجربتي سابقة في اختبار (**اخصائي حاسب آلي**) في احدى مؤسسسات الحكومية، هذا معلومات كان جزء من اختبار.

Compter Networking



Types of Ethernet Cabling

In fact, Ethernet cabling is an important topic on Cisco's CCNA exam. So what do you need to know about Ethernet cabling? Let's find out.

Types of Ethernet Cabling

To start off with, **you should know that not all Ethernet cabling is the same.** If you go to a store you may find a variety of **"categories"** of cabling. These categories tell you the quality of the cabling. The quality determines, essentially, how much the cable can handle. Here are the categories that you need to know:

1. **Cat 3**–used for voice cabling and 10Mb Ethernet

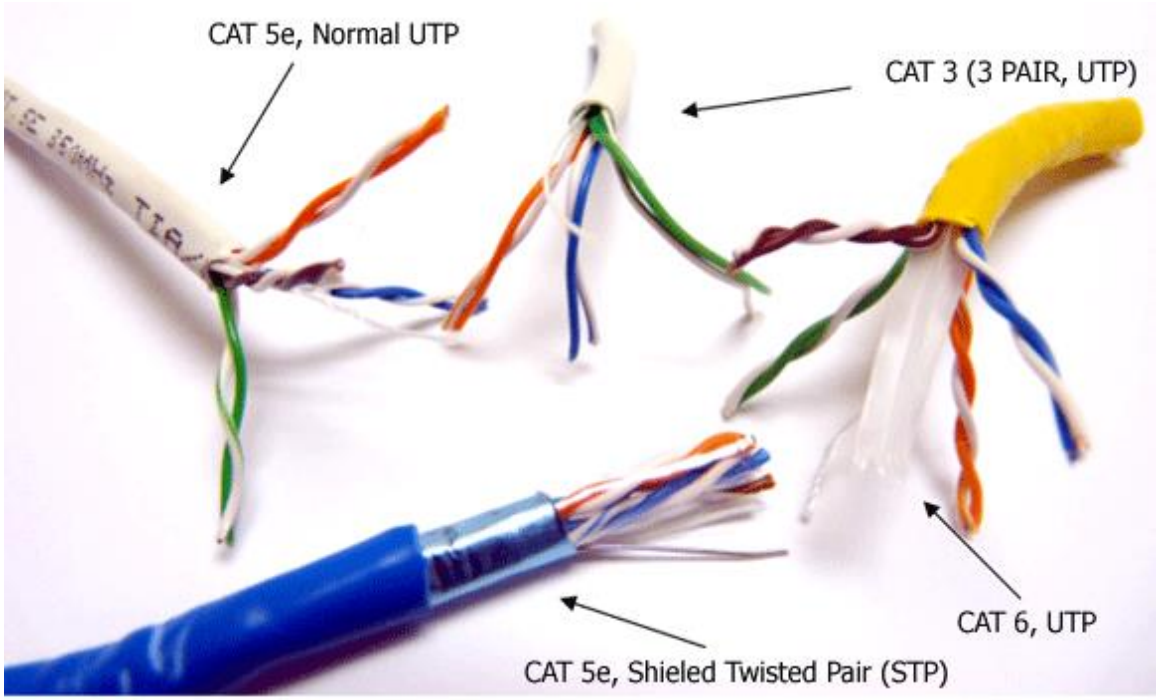
2. **Cat 5**–used for 10/100Mb Ethernet and works for voice as well

3. **Cat 5E**–Enhanced Cat 5 cabling that helps to prevent cross-talk, works for 10/100Mb and 1000Mb (or Gigabit Ethernet)

4. **Cat 6**–Like Cat 5E but with larger gauge wires, works for 10/100/1000Mb. **This cable is better than Cat 5e for Gigabit Ethernet.**

5. **Cat 7**–Also called Class F, this is fully-shielded cabling and supports up to 600Mhz. This is a relatively new type of cabling and isn't used much.

What the CAT3, CAT5 and CAT6 Look Like



Most companies today **are still using and even installing Category 5e as it works for the 100Mb Fast-Ethernet in use on almost every desktop PC**. Plus, it is economical compared to the higher categories of cabling. If you go to a computer store and buy an Ethernet cable, 99% of the time it will be a Cat 5e cable.

Ethernet Cabling Standards

Ethernet Type	Bandwidth	Cable Type	Maximum Distance
10Base-T	10Mbps	Cat 3/Cat 5 UTP	100m
100Base-TX	100Mbps	Cat 5 UTP	100m
100Base-TX	200Mbps	Cat 5 UTP	100m
100Base-FX	100Mbps	Multi-mode fiber	400m
100Base-FX	200Mbps	Multi-mode fiber	2Km
1000Base-T	1Gbps	Cat 5e UTP	100m
1000Base-TX	1Gbps	Cat 6 UTP	100m
1000Base-SX	1Gbps	Multi-mode fiber	550m
1000Base-LX	1Gbps	Single-mode fiber	2Km
10GBase-T	10Gbps	Cat 6a/Cat 7 UTP	100m
10GBase-LX	10Gbps	Multi-mode fiber	100m
10GBase-LX	10Gbp	Single-mode fiber	10Km

https://blog.router-switch.com/2016/01/cisco-ccna-part-types-of-ethernet-cabling/

Network OS (Network Operating System)

What is network OS software?

A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations, personal computers and, in some instances, older terminals that are connected on a local area network (LAN). The software behind a NOS allows multiple devices within a network to communicate and share resources with each other.

The composition of hardware that typically uses a NOS includes a number of personal computers, a printer, a server and file server with a local network that connects them together. The role of the NOS is to then provide basic network services and features that support multiple input requests simultaneously in a multiuser environment.

Due to earlier versions of basic operating systems not being designed for network use, network operating systems emerged as a solution for single-user computers.

Types of network operating systems

There are **two basic types** of network operating systems, the peer-to-peer NOS and the client/server NOS:

1. Peer-to-peer network operating systems allow users to share network resources saved in a common, accessible network location. In this architecture, all devices are treated equally in terms of functionality. Peer-

to-peer usually works best for small to medium LANs and is cheaper to set up.

2. Client/server network operating systems provide users with access to resources through a server. In this architecture, all functions and applications are unified under one file server that can be used to execute individual client actions regardless of physical location. Client/server tends to be most expensive to implement and requires a large amount of technical maintenance. An advantage to the client/server model is that the network is controlled centrally, makes changes or additions to technology easier to incorporate.

Common features of network operating systems

Features of network operating systems are typically associated with user administration, system maintenance and resource management functionality. This includes:

1. Basic support for operating systems like protocol and processor support, hardware detection and multiprocessing.
2. Printer and application sharing.
3. Common file system and database sharing.
4. Network security capabilities such as user authentication and access control.
5. Directory
6. Backup and web services.
7. Internetworking.

https://www.techtarget.com/searchnetworking/definition/network-operating-system

Advantages

1. Centralized servers are highly stable.
2. Security is server managed.
3. Upgradation of new technologies and hardware can be easily integrated into the system.
4. It is possible to remote access to servers from different locations and types of systems.

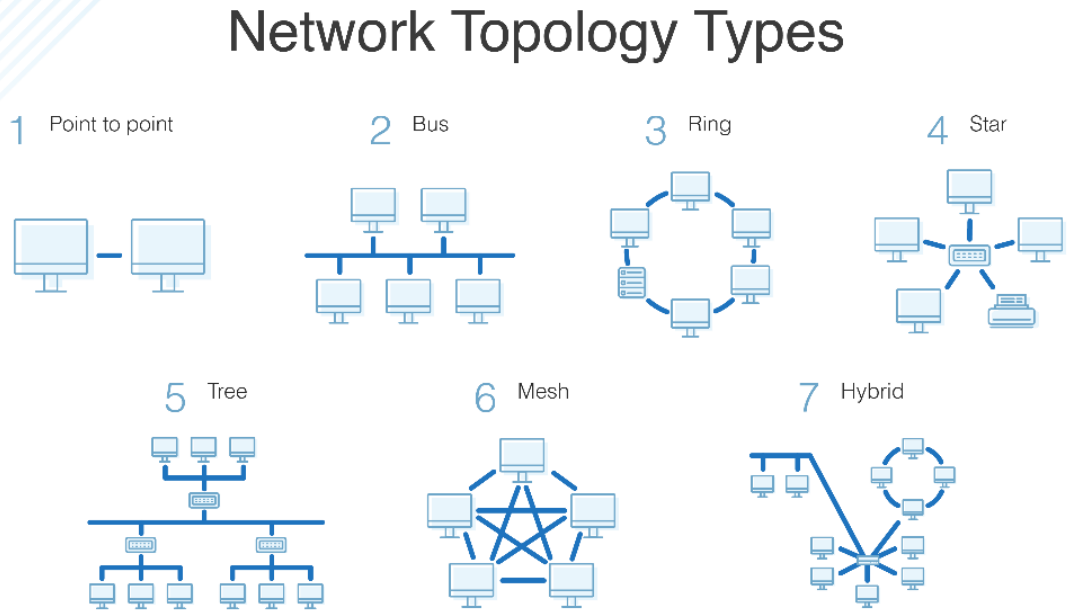
Disadvantages

1. High cost of buying and running a server.
2. Dependency on a central location for most operations.
3. Regular maintenance and updates are required.

Network Topology

What's the Most Common Type of Network Topology?

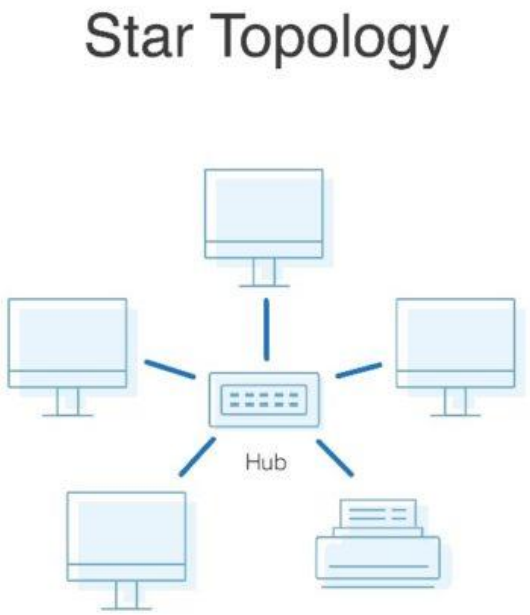
Building a local area network (LAN) topology can be make-or-break for your business, as you want to set up a resilient, secure, and easy-to-maintain topology. There are several different types of network topology and all are suitable for different purposes, depending on the overall network size and your objectives.



As with most things, there's no "right" or one-size-fits-all option. With this in mind, I'll walk you through the most common network topology definitions to give you a feel for the advantages and disadvantages of each.

What Is **Star Topology**?

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps prevent data loss.



Advantages of Star Topology

Star topologies are common since they allow you to conveniently manage your entire network from a single location. Because each of the nodes is independently connected to the central hub, should one go down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network layout.

Additionally, devices can be added, removed, and modified without taking the entire network offline.

On the physical side of things, the structure of the star topology uses relatively little cabling to fully connect the network, which allows for both straightforward setup and management over time as the network expands or contracts. The simplicity of the network design makes life easier for administrators, too, because it's easy to identify where errors or performance issues are occurring.

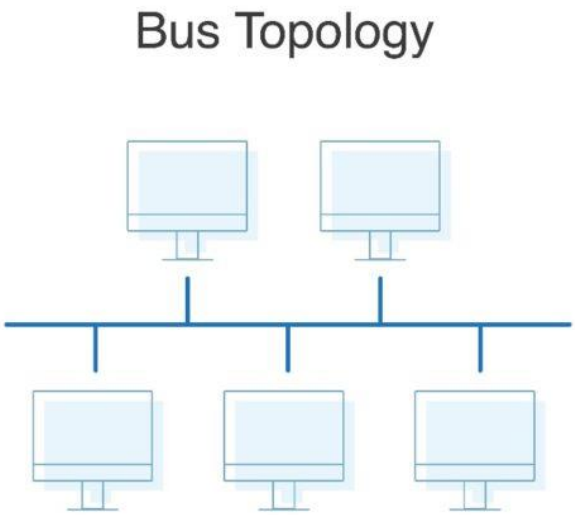
Disadvantages of Star Topology

On the flipside, if the central hub goes down, the rest of the network can't function. But if the central hub is properly managed and kept in good health, administrators shouldn't have too many issues.

The overall bandwidth and performance of the network are also limited by the central node's configurations and technical specifications, making star topologies expensive to set up and operate.

What Is **Bus Topology**?

A bus topology orients all the devices on a network along a single cable running in a single direction from one end of the network to the other—which is why it's sometimes called a "line topology" or "backbone topology." Data flow on the network also follows the route of the cable, moving in one direction.



Advantages of Bus Topology

Bus topologies are a good, cost-effective choice for smaller networks because the layout is simple, allowing all devices to be connected via a single coaxial or RJ45 cable. If needed, more nodes can be easily added to the network by joining additional cables.

Disadvantages of Bus Topology

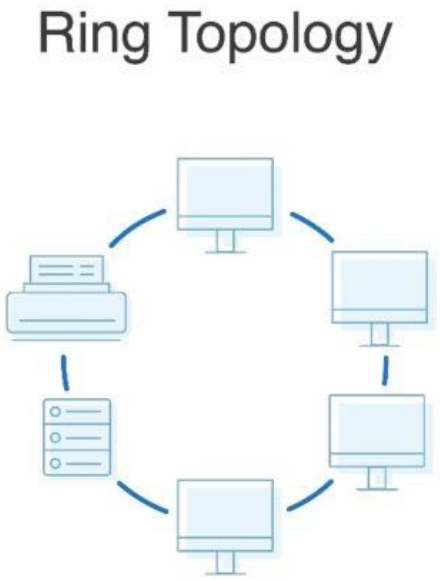
However, because bus topologies use a single cable to transmit data, they're somewhat vulnerable. If the cable experiences a failure, the whole network goes down, which can be time-consuming and expensive to restore, which can be less of an issue with smaller networks.

Bus topologies are best suited for small networks because there's only so much bandwidth, and every additional node will slow transmission speeds.

Furthermore, data is "half-duplex," which means it can't be sent in two opposite directions at the same time, so this layout is not the ideal choice for networks with huge amounts of traffic.

What Is **Ring Topology**? Single vs. Dual

Ring topology is where nodes are arranged in a circle (or ring). The data can travel through the ring network in either one direction or both directions, with each device having exactly two neighbors.



Pros of Ring Topology

Since each device is only connected to the ones on either side, when data is transmitted, the packets also travel along the circle, moving through each of the intermediate nodes until they arrive at their destination. If a large network is arranged in a ring topology, repeaters can be used to ensure packets arrive correctly and without data loss.

Only one station on the network is permitted to send data at a time, which greatly reduces the risk of packet collisions, making ring topologies efficient at transmitting data without errors.

By and large, ring topologies are cost-effective and inexpensive to install, and the intricate point-to-point connectivity of the nodes makes it relatively easy to identify issues or misconfigurations on the network.

Cons of Ring Topology

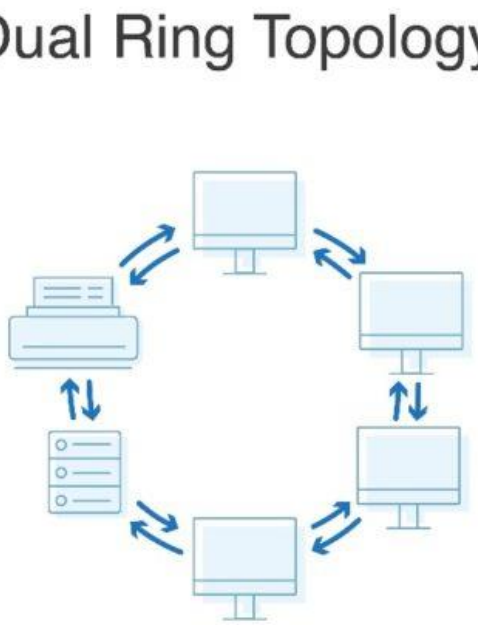
Even though it's popular, a ring topology is still vulnerable to failure without proper network management. Since the flow of data transmission moves unidirectionally between nodes along each ring, if one node goes down, it can take the entire network with it. That's why it's imperative for each of the nodes to be monitored and kept in good health. Nevertheless, even if you're vigilant and attentive to node performance, your network can still be taken down by a transmission line failure.

The question of scalability should also be taken into consideration. In a ring topology, all the devices on the network share bandwidth, so the addition of more devices can contribute to overall communication delays. Network administrators need to be mindful of the devices added to the topology to avoid overburdening the network's resources and capacity.

Additionally, the entire network must be taken offline to reconfigure, add, or remove nodes. And while that's not the end of the world, scheduling downtime for the network can be inconvenient and costly.

What Is **Dual-Ring Topology**?

A network with ring topology is half-duplex, meaning data can only move in one direction at a time. Ring topologies can be made full-duplex by adding a second connection between network nodes, creating a dual ring topology.

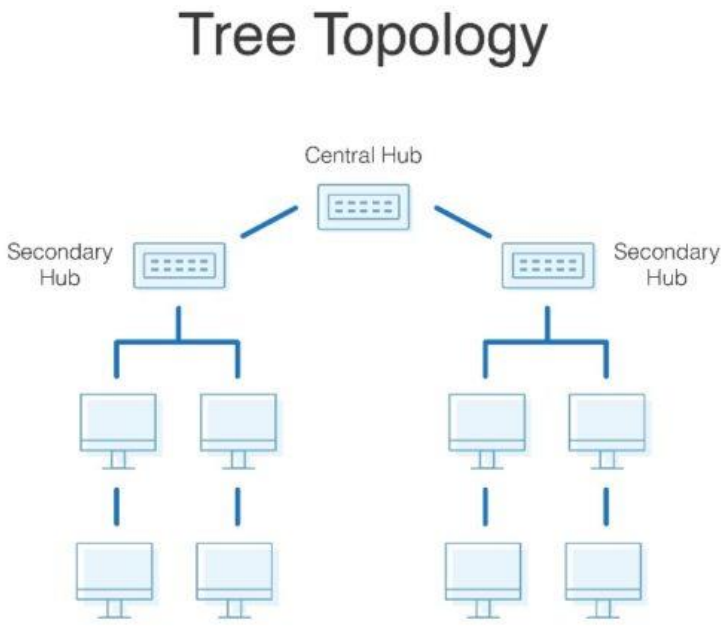


Advantages of Dual-Ring Topology

The primary advantage of dual ring topology is its efficiency: because each node has two connections on either side, information can be sent both clockwise and counterclockwise along the network. The secondary ring included in a dual-ring topology setup can act as a redundant layer and backup, which helps solve for many of the disadvantages of traditional ring topology. Dual ring topologies offer a little extra security, too: if one ring fails within a node, the other ring is still able to send data.

What Is **Tree Topology**?

The tree topology structure gets its name from how the central node functions as a sort of trunk for the network, with nodes extending outward in a branch-like fashion. However, where each node in a star topology is directly connected to the central hub, a tree topology has a parent-child hierarchy to how the nodes are connected. Those connected to the central hub are connected linearly to other nodes, so two connected nodes only share one mutual connection. Because the tree topology structure is both extremely flexible and scalable, it's often used for wide area networks to support many spread-out devices.



Pros of Tree Topology

Combining elements of the star and bus topologies allows for the easy addition of nodes and network expansion. Troubleshooting errors on the

network is also a straightforward process, as each of the branches can be individually assessed for performance issues.

Cons of Tree Topology

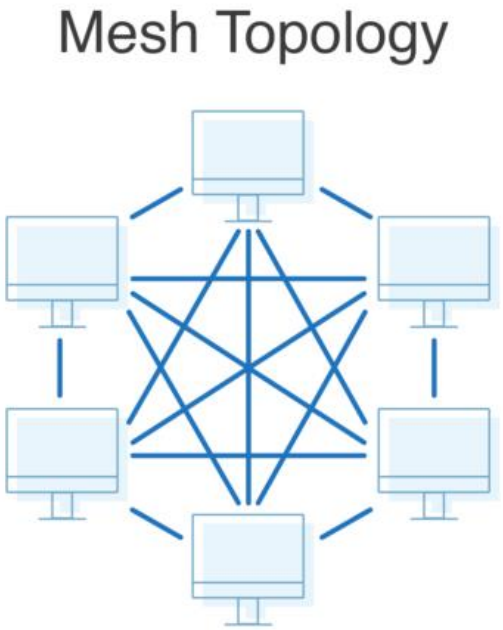
As with the star topology, the entire network depends on the health of the root node in a tree topology structure. Should the central hub fail, the various node branches will become disconnected, though connectivity within—but not between—branch systems will remain.

Because of the hierarchical complexity and linear structure of the network layout, adding more nodes to a tree topology can quickly make proper management an unwieldy, not to mention costly, experience. Tree topologies are expensive because of the sheer amount of cabling required to connect each device to the next within the hierarchical layout.

What Is **Mesh Topology**?

A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected. Mesh networks can be full or partial mesh. Partial mesh topologies are mostly interconnected, with a few nodes with only two or three connections, while full-mesh topologies are—surprise!—fully interconnected.

The web-like structure of mesh topologies offers two different methods of data transmission: routing and flooding. When data is routed, the nodes use logic to determine the shortest distance from the source to destination, and when data is flooded, the information is sent to all nodes within the network without the need for routing logic.



Advantages of Mesh Topology

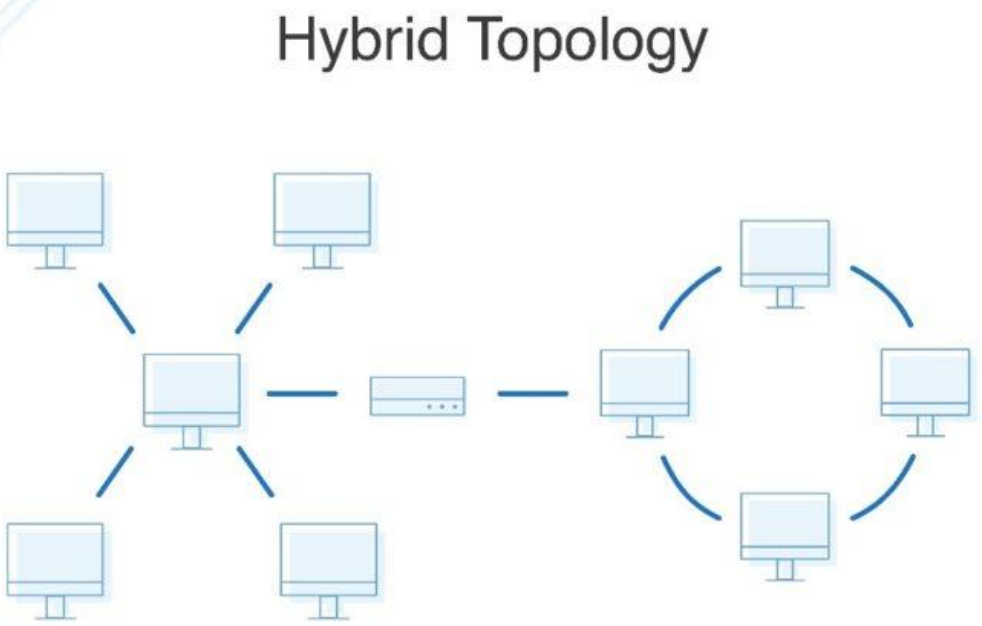
Mesh topologies are reliable and stable, and the complex degree of interconnectivity between nodes makes the network resistant to failure. For instance, no single device going down can bring the network offline.

Disadvantages of Mesh Topology

Mesh topologies are incredibly labor-intensive. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time-consuming to set up. As with other topology structures, the cost of cabling adds up fast, and to say mesh networks require a lot of cabling is an understatement.

What Is **Hybrid Topology**?

Hybrid topologies combine two or more different topology structures—the tree topology is a good example, integrating the bus and star layouts. Hybrid structures are most commonly found in larger companies where individual departments have personalized network topologies adapted to suit their needs and network usage.



Advantages of Hybrid Topology

The main advantage of hybrid structures is the degree of flexibility they provide, as there are few limitations on the network structure itself that a hybrid setup can't accommodate.

Disadvantages of Hybrid Topology

However, each type of network topology comes with its own disadvantages, and as a network grows in complexity, so too does the experience and know-

how required on the part of the admins to keep everything functioning optimally. There's also the monetary cost to consider when creating a hybrid network topology.

Which Topology Is Best for Your Network?

No network topology is perfect, or even inherently better than the others, so determining the right structure for your business will depend on the needs and size of your network. Here are the key elements to consider:

- Length of cable needed
- Cable type
- Cost
- Scalability

Cable Length

Generally, the more cable involved in network topology, the more work it'll require to set up. The bus and star topologies are on the simpler side of things, both being fairly lightweight, while mesh networks are much more cable- and labor-intensive.

Cable Type

The second point to consider is the type of cable you'll install. Coaxial and twisted-pair cables both use insulated copper or copper-based wiring, while fiber-optic cables are made from thin and pliable plastic or glass tubes. Twisted-pair cables are cost-effective but have less bandwidth than coaxial cables. Fiber-optic cables are high performing and can transmit data far faster than twisted-pair or coaxial cables, but they also tend to be far more expensive to install, because they require additional components like optical receivers. So, as with your choice of network topology, the wiring you select depends on the needs of your network, including which applications you'll be running, the transmission distance, and desired performance.

Cost

As I've mentioned, the installation cost is important to account for, as the more complex network topologies will require more time and funding to set

up. This can be compounded if you're combining different elements, such as connecting a more complex network structure via more expensive cables (though using fiber-optic cables in a mesh network is overdoing it, if you ask me, because of how interconnected the topology is). Determining the right topology for your needs, then, is a matter of striking the right balance between installation and operating costs and the level of performance you require from the network.

Scalability

The last element to consider is scalability. If you anticipate your company and network expanding—or if you'd like it to be able to—it'll save you time and hassle down the line to use an easily modifiable network topology. Star topologies are so common because they allow you to add, remove, and alter nodes with minimal disruption to the rest of the network. Ring networks, on the other hand, have to be taken entirely offline for any changes to be made to any of the nodes.

How to Map Network Topology

When you're starting to design a network, topology diagrams come in handy. They allow you to see how the information will move across the network, which, in turn, allows you to predict potential choke points. Visual representation makes it easier to create a streamlined and efficient network design, while also acting as a good reference point if you find yourself needing to troubleshoot errors.

A topology diagram is also essential for having a comprehensive understanding of your network's functionality. In addition to assisting with the troubleshooting process, the bird's-eye view provided by a topology diagram can help you visually identify the pieces of the infrastructure your network is lacking, or which nodes need monitoring, upgrading, or replacing.

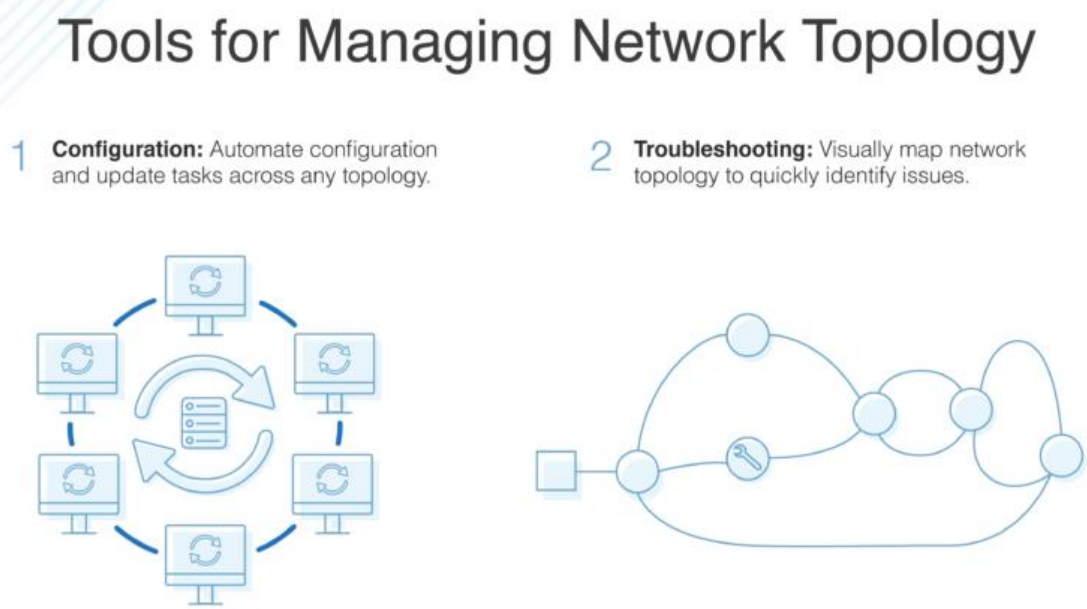
The good news is you don't have to do it manually: you can easily create a map of your network topology with tools.

What Tools Help Manage and Monitor Networks?

There are a few network topology mapping products on the market. One of the more common ones is Microsoft Visio, which lets you "draw" your network by adding different nodes and devices to a canvas-like interface. While this can work for smaller networks, drawing each additional node quickly becomes unwieldy if you're working with a multitude of devices and topologies spread across an entire company. Other options, like Lucidchart and LibreOffice Draw, are either free or offer free trials, and while they're viable options, especially if the cost is a concern, they don't come with a full set of premium network mapping tools to make managing a network easier and less time-consuming.

Due to variations in network topology and the different ways networks can behave—including their unique security issues, pressure points, and management challenges—it's often useful to automate configuration and management tasks using network software.

Network Configuration



First, consider using a network configuration management tool. This kind of tool can help you configure your network correctly and automate repetitive tasks to take the pressure off the network administrator. As your organization or network grows, the network topology may become more layered or more complex, and it can become harder to deploy configurations across the entire network with certainty. However, with configuration management tools, the complicated network topology is no issue: tools can usually auto-detect each node on the network, allowing you to deploy standard configurations that may be required for compliance reasons, or flag any configurations outside what is expected.

Network configuration management tools can also highlight vulnerabilities, so you can correct these issues and keep your network more secure. Finally, these kinds of tools should also display the lifecycle of the devices on your network, alerting you to devices coming to their end-of-service or end-of-life points, so you can replace them before problems begin to arise.

Network Performance Troubleshooting

You should use network management software to track overall performance. A performance manager can keep track of network issues, outages, and performance issues. A performance management tool will also have the functionality to set network performance baselines and establish a clear picture of how your network typically behaves when healthy. Then, by setting alerts when your network performs unexpectedly or outside of these baselines, you can quickly track, pinpoint, and troubleshoot issues.
With complex network topologies, it may be hard to figure out exactly which part of the network is having issues. Some performance managers will create a visual display of your network topology, so you can see the entire network in a one-map overview. This can show you how your network is laid out, bring your attention to changes in the topology, and flag where problems are arising. To get started understanding your network topology, you can try a tool like Network Topology Mapper free for 14 days. This tool automatically discovers and generates detailed topology maps of your network and can create multiple map types without having to rescan your network every time.

What to Know About Network Topology Today

The best advice I can give regarding network topology is that you should be deeply familiar with the needs and usage requirements of your network. The total number of nodes on the network is one of the primary considerations to account for, as this will dictate whether it's feasible to use a simpler topology, or whether you'll have to make the investment in a more complicated network structure.

As I mentioned earlier, no one topology is "best." Each offers its own set of perks and drawbacks, depending on the network environment you're working with or attempting to set up. For this reason, I would avoid jumping to immediate conclusions about any of the network topologies based solely on the descriptions here. Before deciding, try using a network topology

mapping tool to sketch the layout you're thinking about using. Network Topology Mapper, my personal favorite, lets you plot the entire structure of your network in a way that's both easy to use and easy to parse, and it offers a 14-day free trial.

https://www.dnsstuff.com/what-is-network-topology

Port Number in Networking

Common port number in networking

Port number	Service
20	File Transfer Protocol(FTP)
23	Telnet
25	Simple Mail Transfer Protocol(SMTP)
53	Domain Name System(DNS)
80	Hypertext Transfer Protocol(HTTP)
161	Simple Network Management Protocol (SNMP)
443	HTTP Secure(HTTPS)

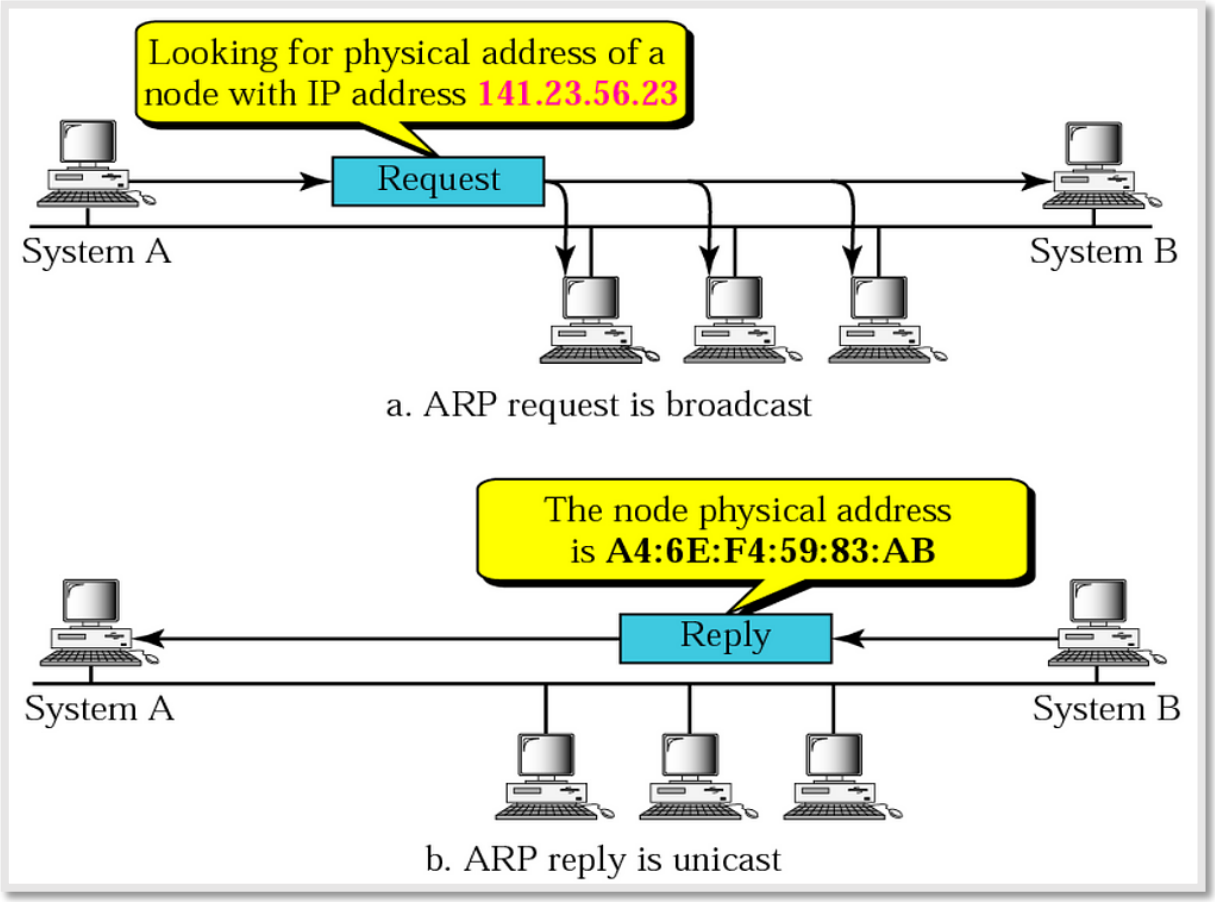
Popular Protocols and Their Common Ports

Protocol	Name	Common Well-Known Port(s)
HTTP	Hypertext Transfer Protocol, Web services	TCP:80
HTTPS	Hypertext Transfer Protocol, Secure Web Services	TCP:443
Telnet	Unencrypted method to log onto a remote computer	TCP:23
SSH	Secure Shell: Encrypted method to log on to a remote computer	TCP:22
DNS Queries	Domain Name System: Request asking for an IP address associated with a name	UDP:53
DHCP	Dynamic Host Configuration Protocol: IP address management	UDP:67, 68
FTP	File Transfer Protocol	TCP:21, 20
TFTP	Trivial File Transfer Protocol	UDP:69
SFTP	SSH File Transfer Protocol, or Secure File Transfer Protocol	TCP:22
SMTP	Simple Mail Transfer Protocol	TCP:25
POP	Post Office Protocol v3	TCP:110
IMAP	Internet Message Access Protocol	TCP:143
SNMP	Simple Network Management Protocol	TCP:161
RDP	Remote Desktop Protocol	TCP:3389
NTP	Network Time Protocol	UDP:123
SIP	Session Initiation Protocol	TCP/UDP:5060, TCP:5061
SMB	Server Message Block	TCP:445
LDAP	Lightweight Directory Access Protocol	TCP/UDP:389
LDAPS	Lightweight Directory Access Protocol over TLS/SSL	TCP:636
H.323	Protocols for audio and video over networks	UDP:1719, TCP:1720, & more

Address Resolution Protocol (ARP)

It is a communication protocol used to find the MAC Address of a device from the available IP address.

What Does ARP Do and How Does It Work?



When a new computer joins a local area network (**LAN**), it will receive a unique IP address to use for identification and communication.

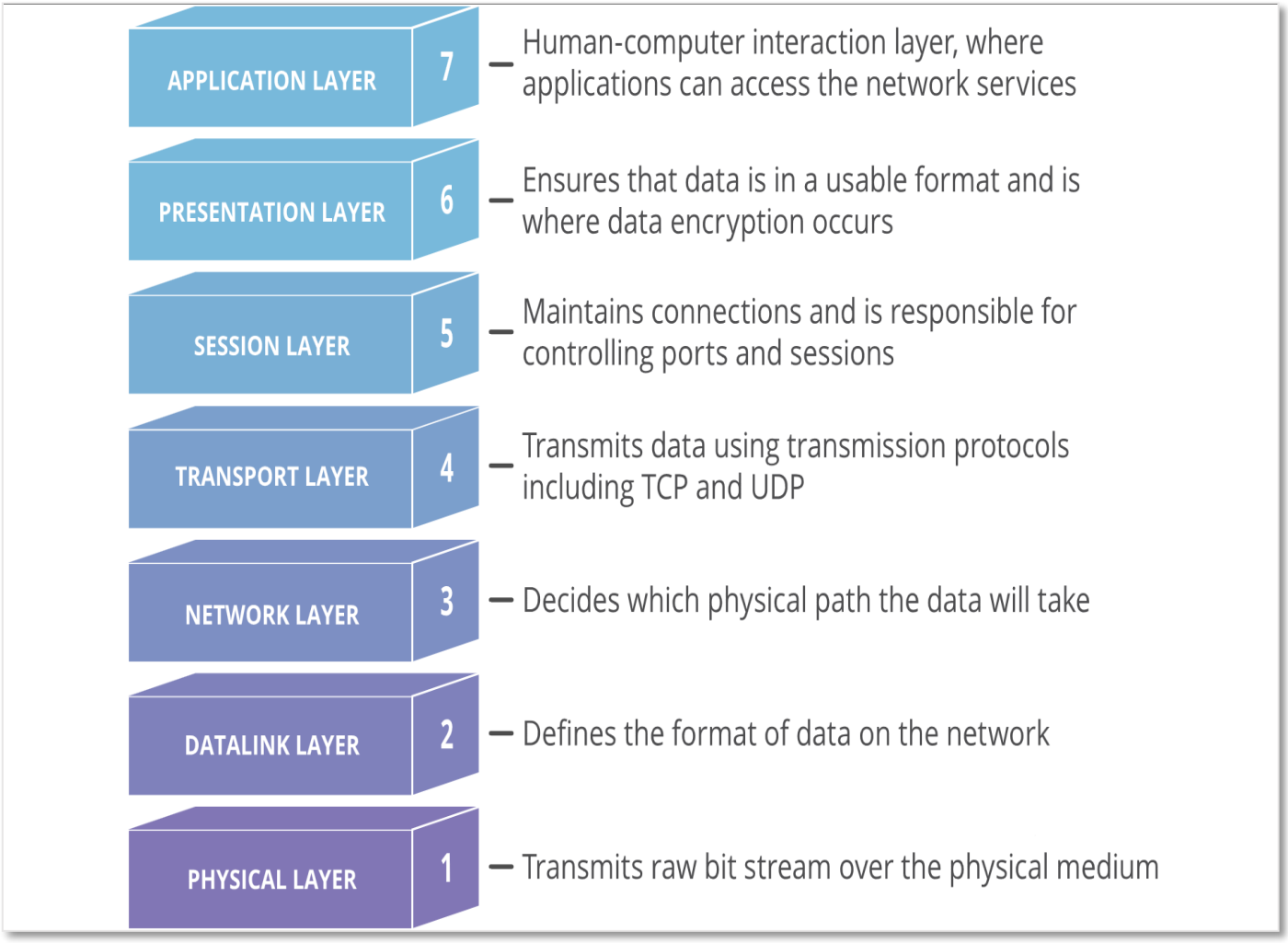
Packets of data arrive at a gateway, destined for a particular host machine. The gateway, or the piece of hardware on a network that allows data to flow from one network to

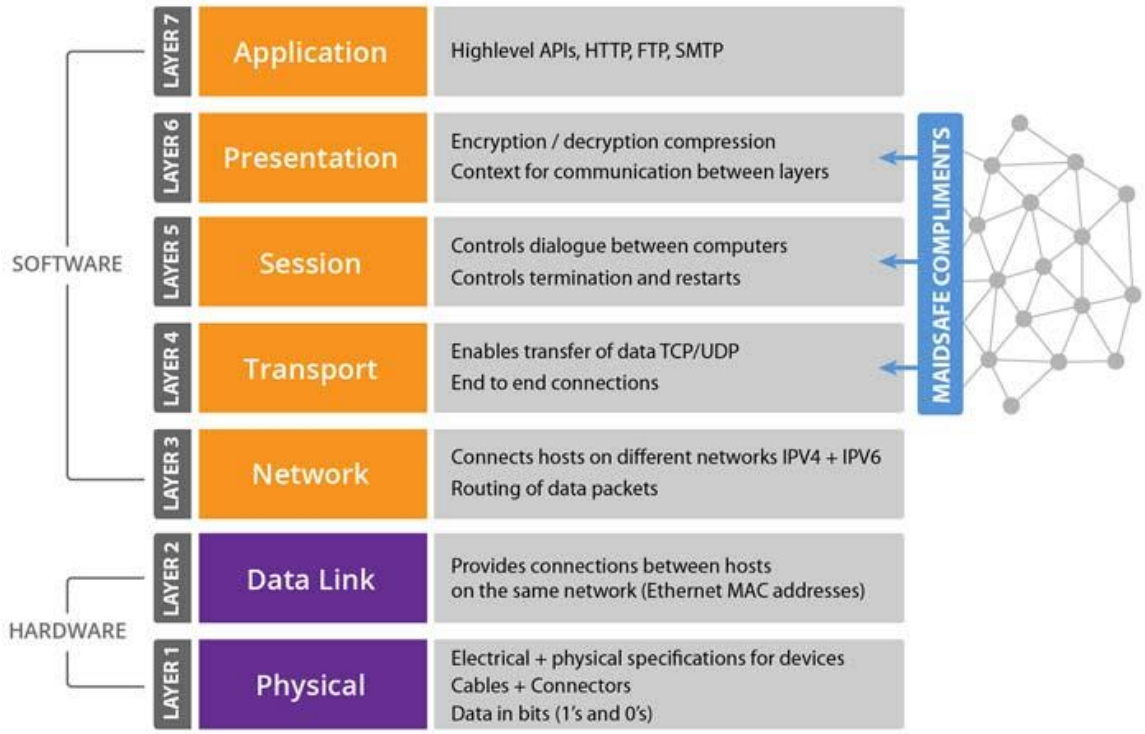
another, asks the ARP program to find a MAC address that matches the IP address. The ARP cache keeps a list of each IP address and its matching MAC address. The ARP cache is dynamic, but users on a network can also configure a static ARP table containing IP addresses and MAC addresses.

ARP caches are kept on all operating systems in an IPv4 Ethernet network. Every time a device requests a MAC address to send data to another device connected to the LAN, the device verifies its ARP cache to see if the IP-to-MAC-address connection has already been completed. If it exists, then a new request is unnecessary. However, if the translation has not yet been carried out, then the request for network addresses is sent, and ARP is performed.

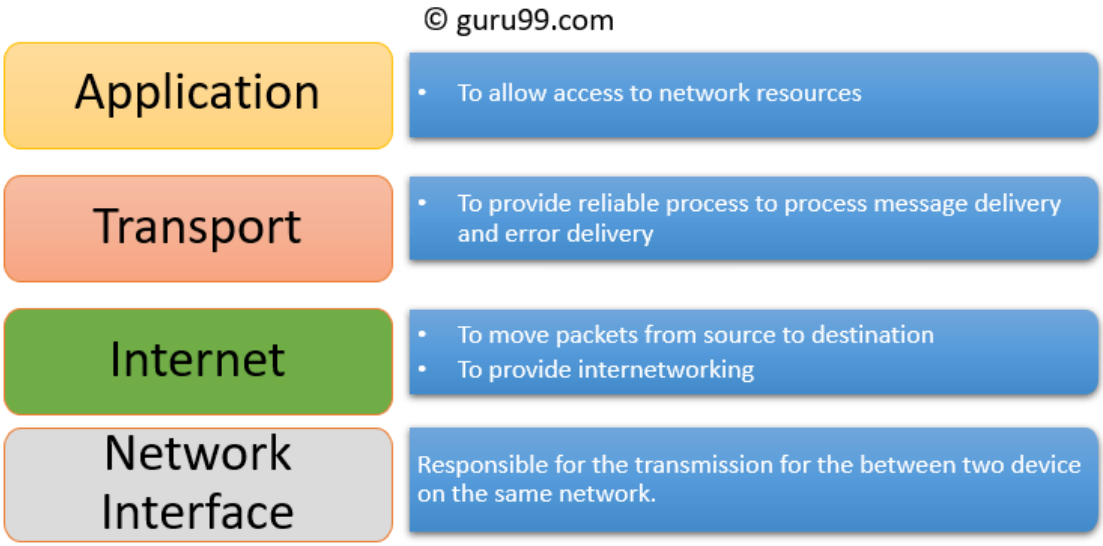
https://www.fortinet.com/resources/cyberglossary/what-is-arp

OSI Model


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

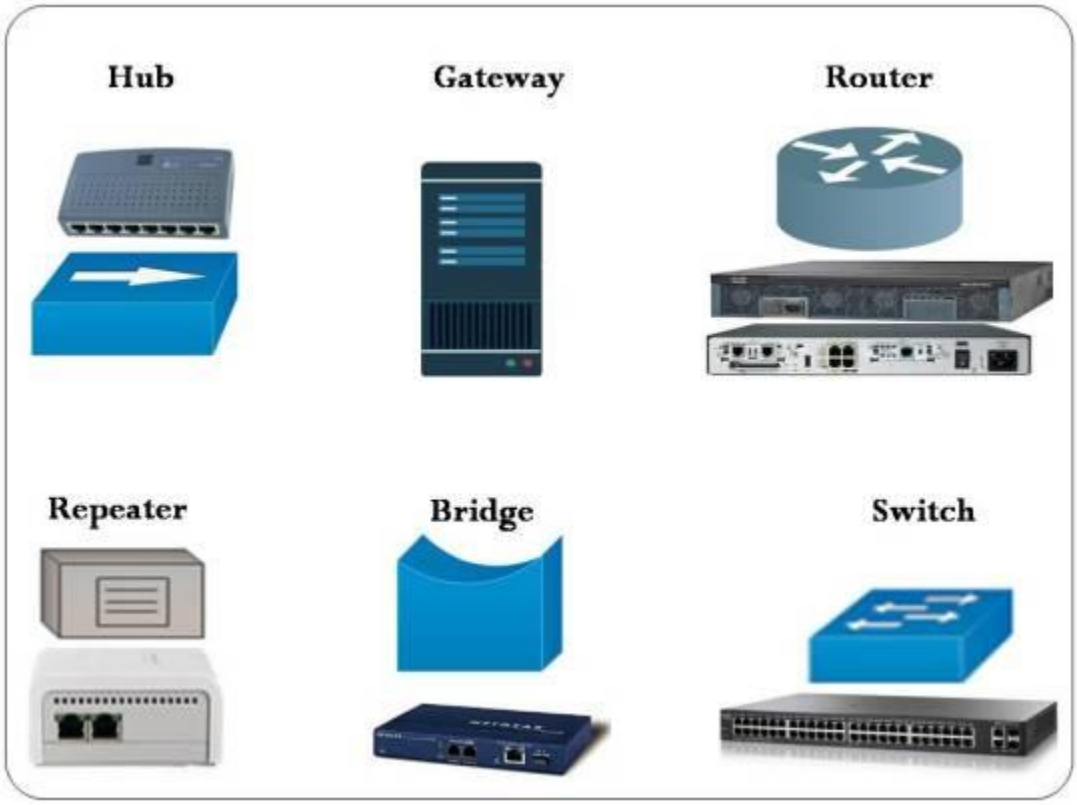

LAYER 7
Application
Highlevel APIs, HTTP, FTP, SMTP
LAYER 6
Presentation
Encryption / decryption compression
Context for communication between layers
LAYER 5
Session
Controls dialogue between computers
Controls termination and restarts
LAYER 4
Transport
Enables transfer of data TCP/UDP
End to end connections
LAYER 3
Network
Connects hosts on different networks IPV4 + IPV6
Routing of data packets
LAYER 2
Data Link
Provides connections between hosts
on the same network (Ethernet MAC addresses)
LAYER 1
Physical
Electrical + physical specifications for devices
Cables + Connectors
Data in bits (1's and 0's)
SOFTWARE
HARDWARE
MAIDSAFE COMPLIMENTS

TCP/IP layer


© guru99.com
Application
To allow access to network resources
Transport
To provide reliable process to process message delivery and error delivery
Internet
To move packets from source to destination
To provide internetworking
Network Interface
Responsible for the transmission for the between two device on the same network.

OSI Model	TCP/IP Model
Application Layer	Application layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data link layer	Link Layer
Physical layer	

Network Devices



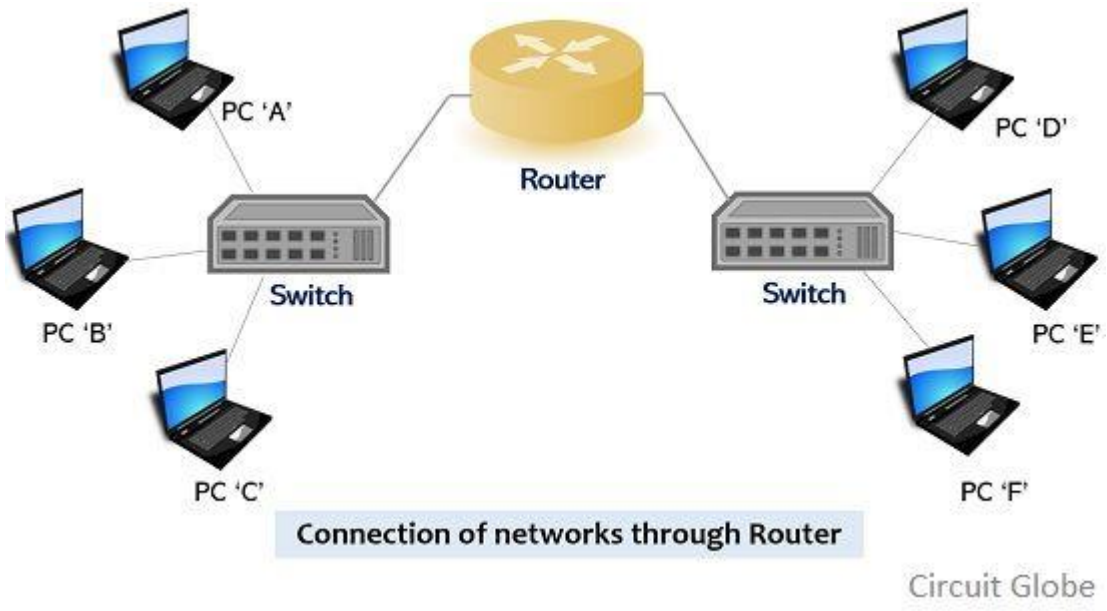
Here is **the common network device** list:

1. Hub
2. Switch
3. Router
4. Bridge
5. Gateway
6. Modem
7. Repeater
8. Access Point

Router

The router is a device that controls the traffic in the network. It connects two similar or dissimilar networks. The router works in both local area network (LAN) and wide area network (WAN). As a router is used in WAN so it is more expensive than any other network device. It can connect LAN and WAN networks. The main purpose of the router is to find a congestion-free path and then travels data through that path. Congestion free path means a path where packets of data are less. The router also connects two networks that have a large distance i.e. one network is in the USA and the other network is in India so the router wirelessly connects these two networks. The data transmission rate is high in the router. The router has an algorithm by which it can find a free congestion path. It works in both wired and wireless network.

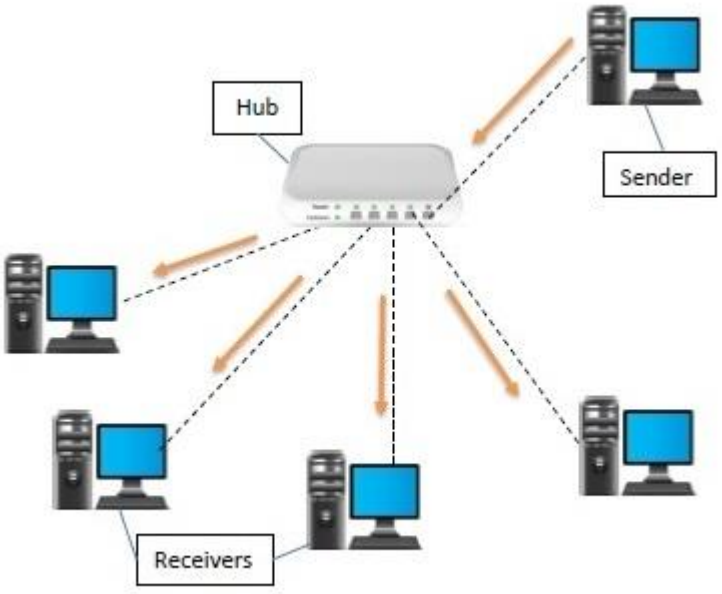
There is one dedicated person needed to maintain a router. There is a security issue while transferring data to long distance. The data can be stolen in the way.



Hub

Hub is used to connect two computers. If computer A wants to send data to computer B then computer A sends data to the hub and then the hub broadcast the data to all the computers attached to the hub. Computer B then receives the data and other computers ignore the data. Hub is less intelligent, and has less cost. It is used in local area network (LAN).

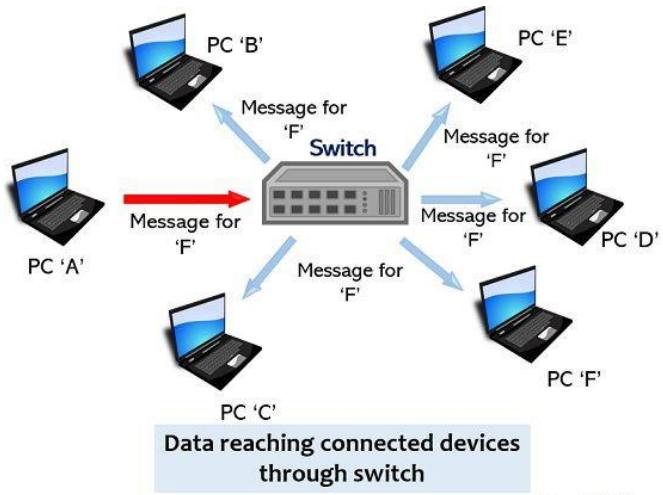
The new connection is made easily by attaching the computer to the network. Hub has the transmission mode of half-duplex meaning that one computer either sends or receive a message at a time. Computers cannot send and receive data simultaneously. If there occurs any problem in the hub then the whole network stops working. Hub cannot provide extra security.



Switch

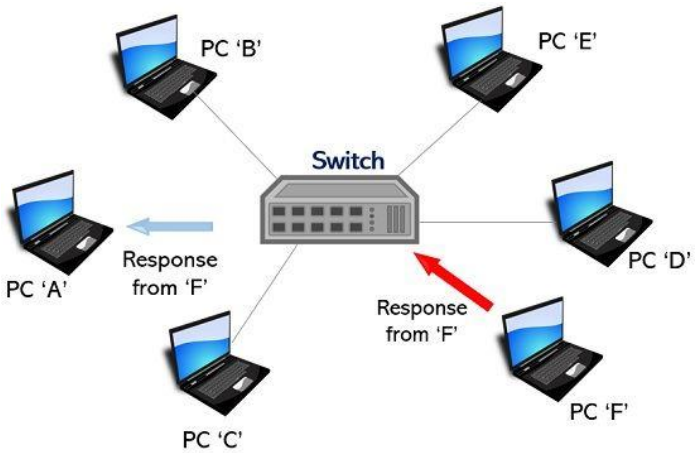
The switch is used to connect multiple computers in the network. It sends a private message from the sender to the receiver. It stores the MAC address of all the connected devices and upon receiving a message from the sender it first checks the MAC address of the message and then sends the message to the receiver that matches the MAC address.

Switch do unicast meaning it sends a message to only one receiver and not a broadcast message. It has high security than a hub. Also, the switch uses full-duplex transmission mode meaning computers can send/receive a message simultaneously. It is also difficult to set up a switch in the network.



Data reaching connected devices through switch

Circuit Globe



Response reaching the location through switch

Circuit Globe

Access Point (AP)

An access point (AP) is used to connect a wired network to a wireless computing device. Suppose there are four computers, a printer and a scanner is connected to a wired network. And there is another wireless network with four laptops. Now laptop computer cannot access the printer in a wired network. So to make this type of connection from wireless to wired network access points are used. The shape of AP looks like a modem. Old AP devices had antennas connected to them while new AP device comes with inbuilt antennas within device.

Modem

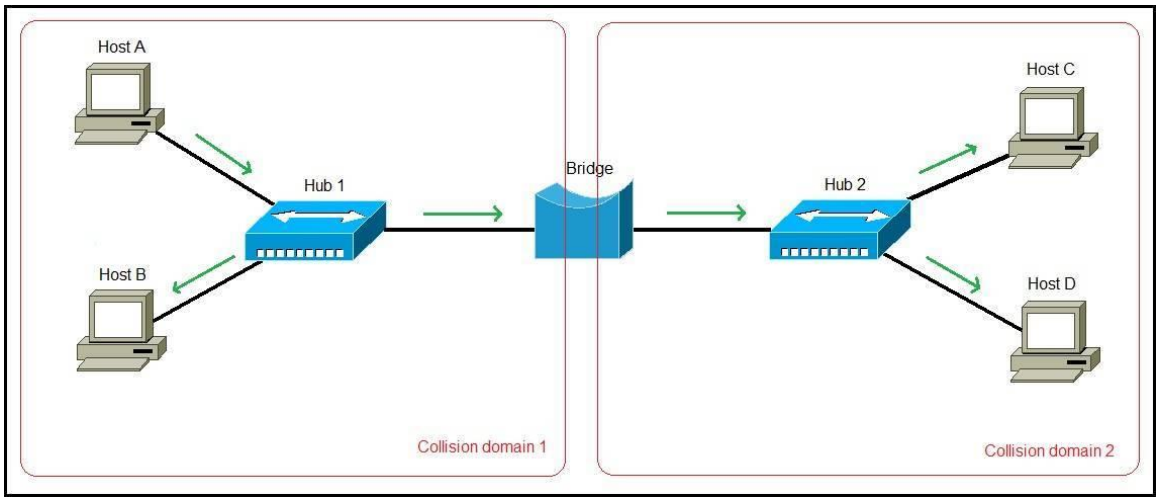
A modem is a short form of modulator-demodulator. It provides internet to the network that is connected through a hub or switch. A modem converts the digital data from our computer to the analogue data that is understandable by the telephone cables. The modem also converts analogue data from cables to the digital form that is understandable by the computer.

Modem receives/sends data from/to coaxial cables. The broadband or DSL network uses a modem.

Bridge

The bridge is a device that connects two LAN's. It works on both physical and data link layers of the OSI model. Suppose you have to make the connection of two LAN's through the bridge. When the connection is made then the bridge stores all the MAC addresses and port numbers of destinations computers in the LAN. When any computer wants to send data then the bridge checks the MAC address from the receiver and then find the LAN that has that MAC address. Then bridge transfer data to that LAN that has that MAC address matched.

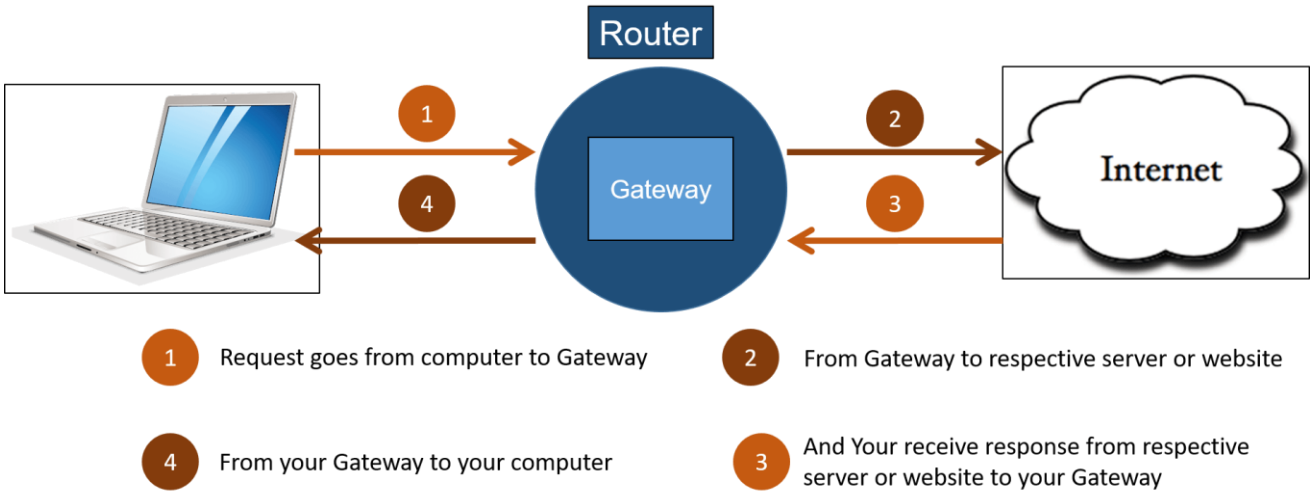
Bridge broadcast the message like hub and repeater. In bridge data collision not occurs. The bridge is an intelligent device. Bridge connects two similar networks but not connect networks that are different. The bridge is a slower device and is expensive also.



Gateway

Gateway is a network device that connects dissimilar computers. It also connects similar networks but in most cases, it connects dissimilar devices. Sometimes switch also behaves as a gateway. Suppose a computer in the LAN network wants some data. If that data is present in the LAN then it will be provided by the gateway but if the data is not present in the LAN then the gateway will connect to the WAN and gets and transfer data to that computer.

Gateway works in all 7 layers of the OSI model. You cannot access the internet without using the gateway. It is expensive to buy a gateway and it provides some security. It is difficult to maintain a gateway and is less intelligent. The data transfer rate is slow in the gateway.



NIC

NIC is a short form of the network interface card. You cannot connect to the internet without NIC. NIC stores the MAC address of the computer but when you connect your computer to the internet then it uses an IP address or LAN address to identify the computer. There are two types of NIC:-

Internal NIC: Internal NIC is attached to the motherboard and it is connected to the Rj45 cable.

External NIC: External NIC is connected via USB or by wireless connection to the computer.

Security is weak by using NIC.

Network Devices – Type your name here

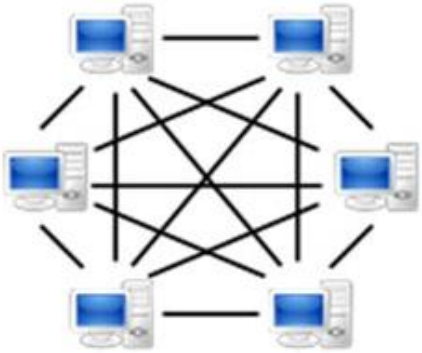
Lookup the following **network devices** to find an image, then type an explanation of how the device is used.

Use your textbooks and the internet, but you must also acknowledge all the sources of information.

No	Description	Image
1	**Server** A computer that is set up to host files that can be accessed by other computers on the same network or over the internet.	
2	**Hub** The hub/concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.	
3	**Switch** An Ethernet switch is a device that provides a central connection point for cables from everything on the network. Most switches are active, that is they electrically amplify the signal as it moves from one device to another.	
4	**Router** Routers are network gateways. They move network packets from one network to another, and many can convert from one network protocol to another as necessary. Routers select the best path to route a message, based on the destination address of the packet.	
6	**Bridge** A bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).	
7	**Cables** Cables are wires that information or power can travel through. Used to either share information between computers or provide electricity from a power supply	

What do you mean by **peer-to-peer**?

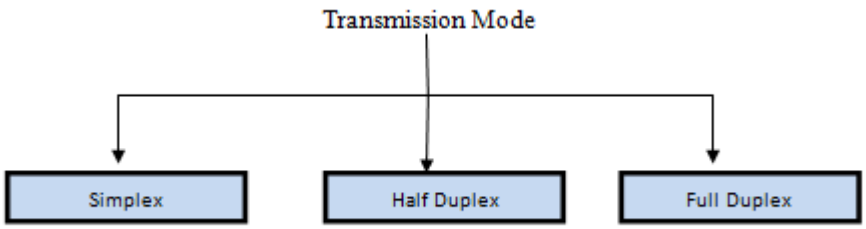
In peer-to-peer (P2P) networking, **a group of computers are linked together with equal permissions and responsibilities for processing data**. Unlike traditional client-server networking, no devices in a P2P network are designated solely to serve or to receive data.

A **server** based network	A **peer-to-peer** based network.
	

Data Transmission Modes

Transmission

There are three modes of transmission, namely: simplex, half duplex, and full duplex. The transmission mode defines the direction of signal flow between two connected devices.



Comparison Chart

Basis for Comparison	Simplex	Half Duplex	Full Duplex
Direction of Communication	Unidirectional	Two-directional, one at a time	Two-directional, simultaneously
Send / Receive	Sender can only send data	Sender can send and receive data, but one a time	Sender can send and receive data simultaneously
Performance	Worst performing mode of transmission	Better than Simplex	Best performing mode of transmission
Example	Keyboard and monitor	Walkie-talkie	Telephone

Simplex

In simplex transmission mode, the communication between sender and receiver occurs in only one direction. The sender can only send the data, and the receiver can only receive the data. The receiver cannot reply to the sender.

Simplex transmission can be thought of as a one-way road in which the traffic travels only in one direction—no vehicle coming from the opposite direction is allowed to drive through.

To take a keyboard / monitor relationship as an example, the keyboard can only send the input to the monitor, and the monitor can only receive the input and display it on the screen. The monitor cannot reply, or send any feedback, to the keyboard.

Half Duplex

The communication between sender and receiver occurs in both directions in half duplex transmission, but only one at a time. The sender and receiver can both send and receive the information, but only one is allowed to send at any given time. Half duplex is still considered a one-way road, in which a vehicle traveling in the opposite direction of the traffic has to wait till the road is empty before it can pass through.

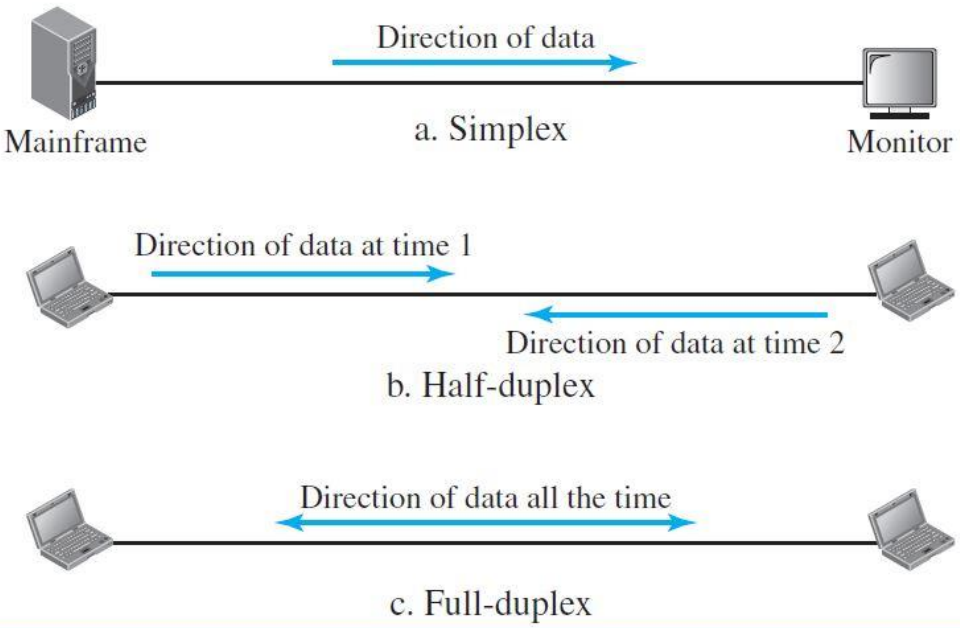
For example, in walkie-talkies, the speakers at both ends can speak, but they have to speak one by one. They cannot speak simultaneously.

Full Duplex

In full duplex transmission mode, the communication between sender and receiver can occur simultaneously. The sender and receiver can both transmit and receive at the same time. Full duplex transmission mode is like a two-way road, in which traffic can flow in both directions at the same time.

https://teachcomputerscience.com/simplex-half-duplex-full-duplex/

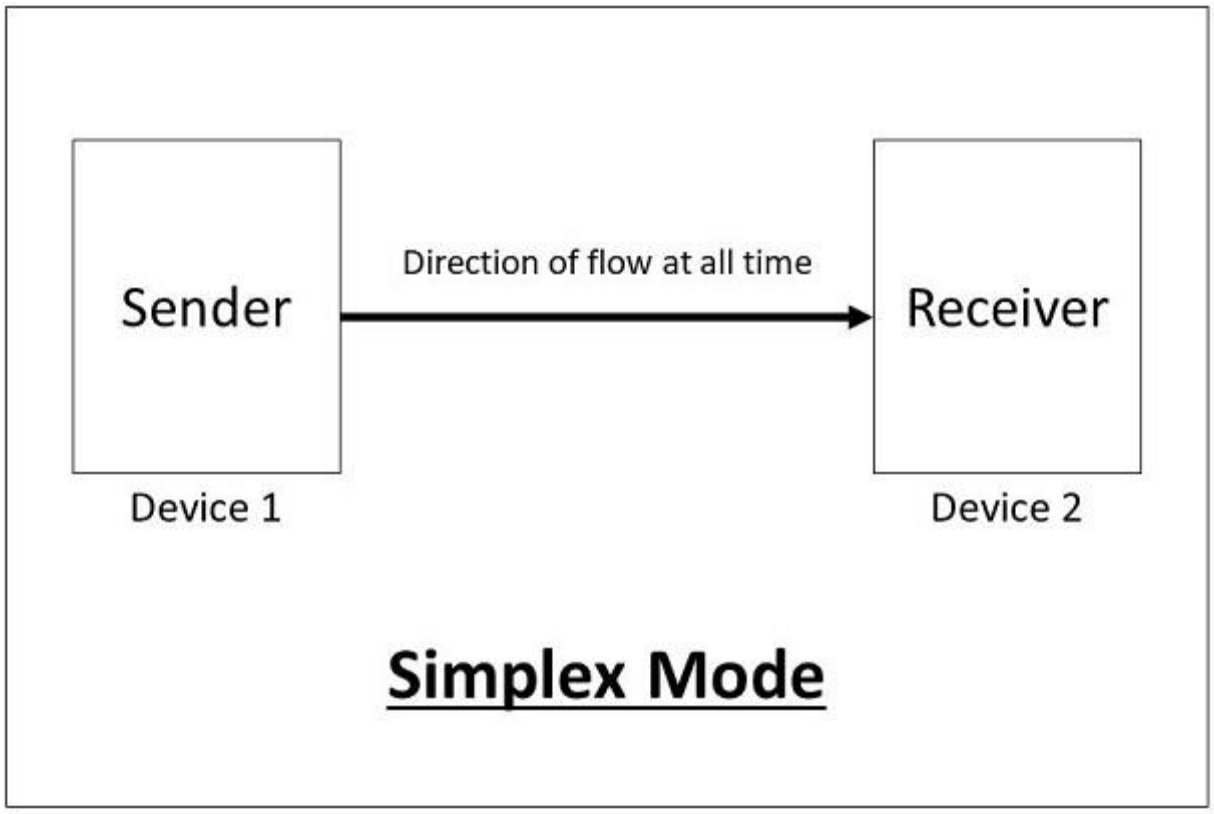
Figure 1.2 *Data flow (simplex, half-duplex, and full-duplex)*



According to the Direction of Exchange of Information:

1. Simplex

Simplex is the data transmission mode in which the data can flow only in one direction, i.e., the communication is unidirectional. In this mode, a sender can only send data but can not receive it. Similarly, a receiver can only receive data but can not send it.



This transmission mode is not so popular because we cannot perform two-way communication between the sender and receiver in this mode. It is mainly used in the business field as in sales that do not require any corresponding reply. It is similar to a one-way street.

For Example, Radio and TV transmission, keyboard, mouse, etc.

The advantages of using a Simplex transmission mode:

1. It utilizes the full capacity of the communication channel during data transmission.
2. It has the least or no data traffic issues as data flows only in one direction.

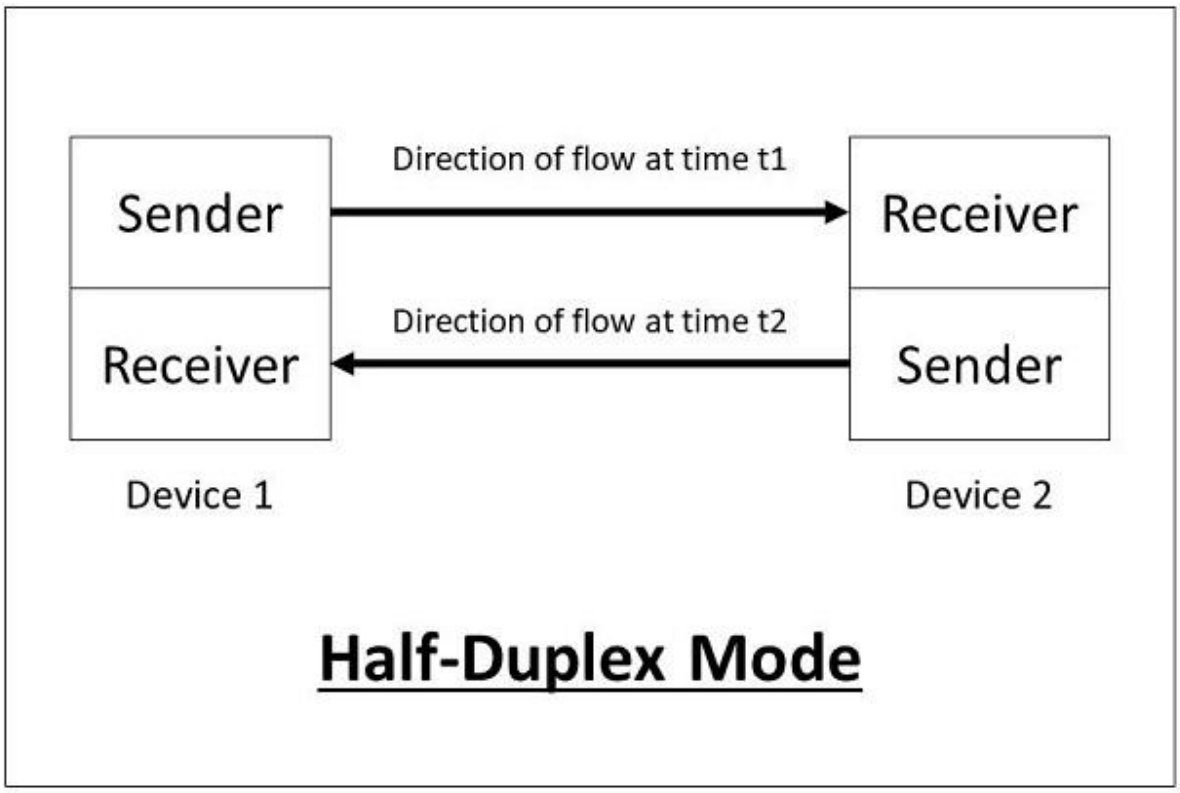
The disadvantages of using a Simplex transmission mode:

1. It is unidirectional in nature having no inter-communication between devices.
2. There is no mechanism for information to be transmitted back to the sender (No mechanism for acknowledgement).

2. Half–Duplex

Half-Duplex is the data transmission mode in which the data can flow in both directions but in one direction at a time. It is also referred to as Semi-Duplex. In other words, each station can both transmit and receive the data

but not at the same time. When one device is sending the other can only receive and vice-versa.



In this type of transmission mode, the entire capacity of the channel can be utilized for each direction. Transmission lines can carry data in both directions, but the data can be sent only in one direction at a time.

This type of data transmission mode can be used in cases where there is no need for communication in both directions at the same time. It can be used for error detection when the sender does not send or the receiver does not receive the data properly. In such cases, the data needs to be transmitted again by the receiver.

For Example, Walkie-Talkie, Internet Browsers, etc.

The advantages of using a half-duplex transmission mode:

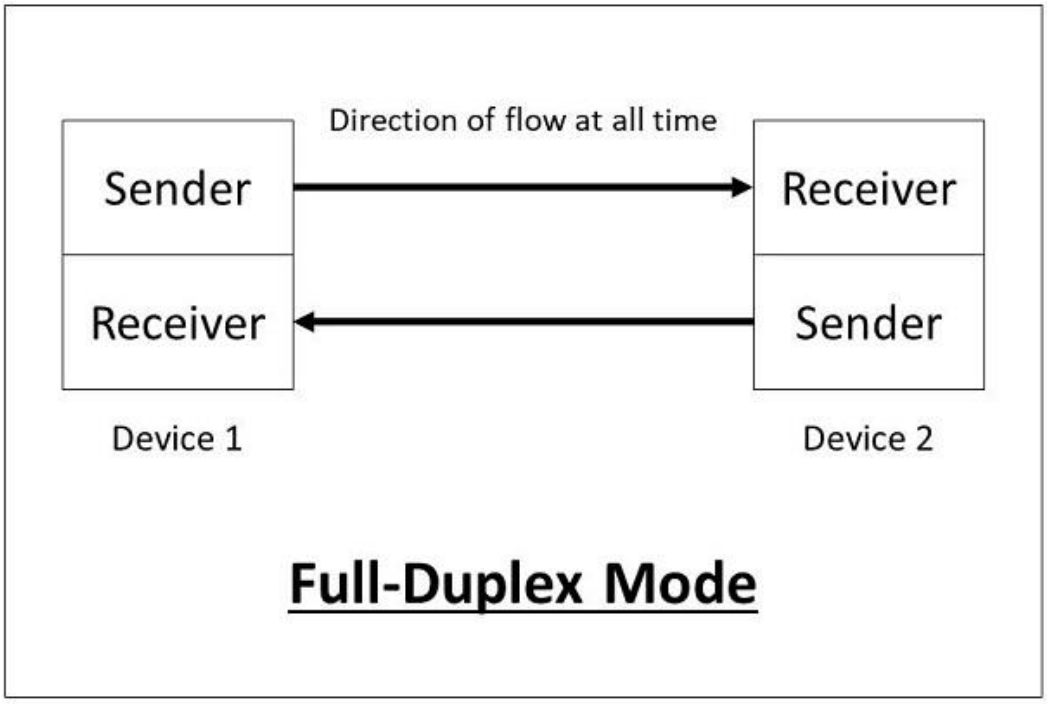
1. It facilitates the optimum use of the communication channel.
2. It provides two-way communication.

The disadvantages of using a half-duplex transmission mode:

1. The two-way communication can not be established simultaneously at the same time.
2. Delay in transmission may occur as only one way communication can be possible at a time.

3. Full–Duplex

Full-Duplex is the data transmission mode in which the data can flow in both directions at the same time. It is bi-directional in nature. It is two-way communication in which both the stations can transmit and receive the data simultaneously.



Full-Duplex mode has double bandwidth as compared to the half-duplex. The capacity of the channel is divided between the two directions of communication. This mode is used when communication in both directions is required simultaneously.

For Example, a Telephone Network, in which both the persons can talk and listen to each other simultaneously.

The advantages of using a full-duplex transmission mode:

1. The two-way communication can be carried out simultaneously in both directions.

2. It is the fastest mode of communication between devices.

The disadvantages of using a half-duplex transmission mode:

1. The capacity of the communication channel is divided into two parts. Also, no dedicated path exists for data transfer.

2. It has improper channel bandwidth utilization as there exist two separate paths for two communicating devices.

https://afteracademy.com/blog/what-are-the-data-transmission-modes-in-a-network

IP Address Classes

IP Address Classes					
Address Class	1st octet range (decimal)	1st octet bits (green bits don't change)	Network (N) and Host (H) parts of an address	Default subnet mask (decimal and binary)	Numbers of possible networks and hosts per network
A	1 - 127	00000000 - 01111111	N.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	126 nets (2^7-2) 16,777,214 hosts per net (2^24-2)
B	128 - 191	10000000 - 10111111	N.N.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16,382 nets (2^14-2) 65,534 hosts per net (2^16-2)
C	192 - 223	11000000 - 11011111	N.N.N.H	255.255.255.0 11111111.11111111.11111111.00000000	2,097,150 nets (2^21-2) 254 hosts per net (2^8-2)
D	224 - 239	11100000 - 11101111	Not for commercial use as a host		
E	240 - 255	11110000 - 11111111	Not for commercial use as a host		