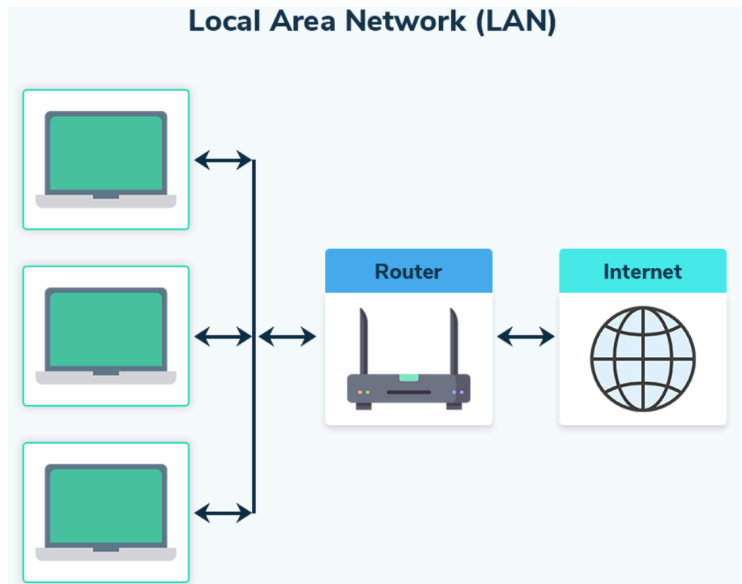


Types of Networks

When it comes to networking, there is no one-size-fits-all policy. Familiarizing yourself with each network will give you a better ability to choose, troubleshoot, and protect your network.

1. Local Area Network (LAN)

A LAN, or local area network, is a network where all the devices used to connect with one another and the internet are housed under one roof. Networks within a home or office, for example, are a LAN.

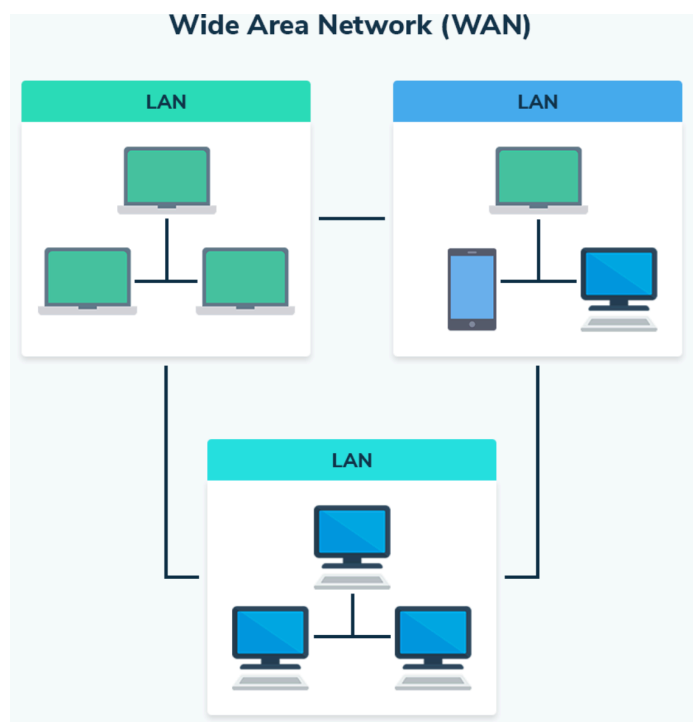


2. Wide Area Network (WAN)

A WAN extends beyond a single building and connects multiple LANs regardless of location.

WANs are popular among companies with branches strewn across the country or the world needing fast and secure networking capabilities. In essence, a WAN is a constellation of LANs or a network of networks.

In fact, the Internet itself is considered a WAN as it connects all devices regardless of location.



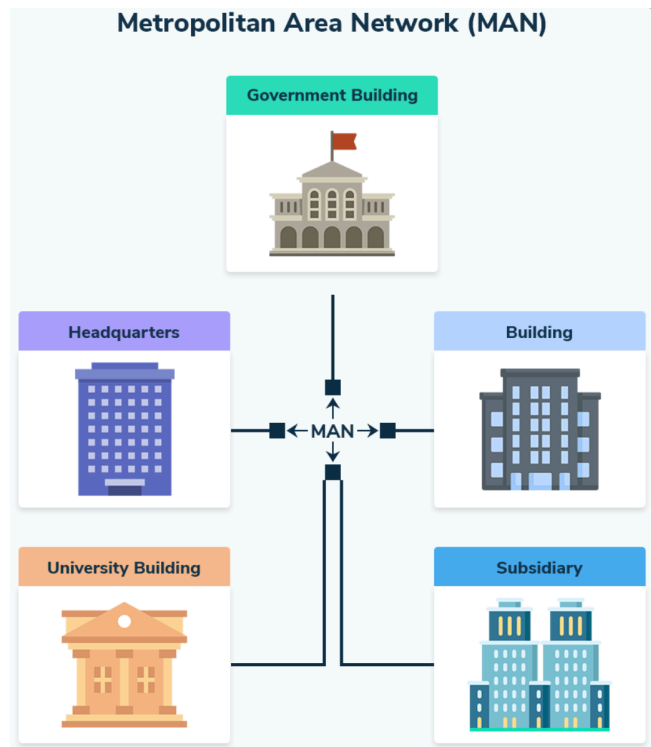
3. Metropolitan Area Network (MAN)

A Metropolitan Area Network (MAN) is an extensive computer network that spans a metropolitan area or campus. Its size and scope fall between a LAN and a WAN.

MANs are often used to connect multiple offices of a single organization within a city, provide connectivity for city-wide services, or link educational campuses.

Due to their proximity, they will likely share a physical infrastructure, such as high-capacity fiber optics.

WANs, by contrast, may need to rely on different technologies, backbones, and internet providers to facilitate connections.



4. Personal Area Network (PAN)

If you've ever airdropped files to a friend or connected your earbuds to your computer via Bluetooth, you've used a personal area network.

A PAN connects devices close to one another—within a few feet—via wired and non-wired connections such as Bluetooth.

Typically, PANs do not connect to the Internet but are device-to-device connections within the same room.



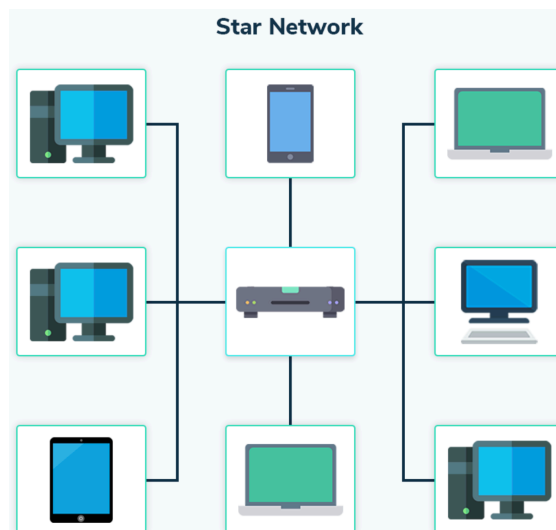
Introduction to Networking Topologies

Network topologies are different from network types in that topologies are node arrangements that facilitate data sharing. Here are some common—and not-so-common—network topologies.

1. Star

The most common topology, the star topology, requires every node on the network to connect to a central device such as a hub, switch, or router.

Most LANs use the star topology. Should the network devices wish to communicate with one another, data must be sent to the central hub first and then routed to its ultimate destination.

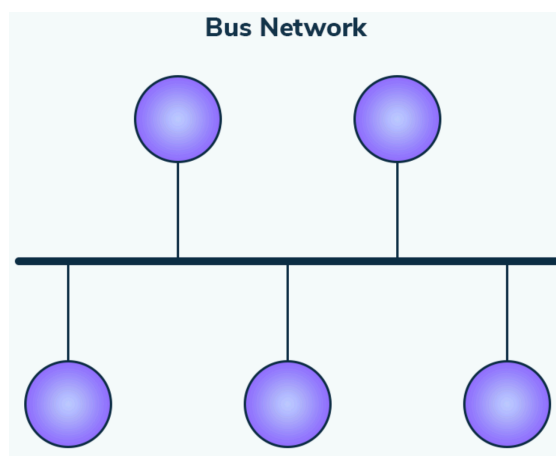


2. Bus

In a bus network topology, every node is connected to the same cable called the “bus.”

Sharing the same cable means that every time a message comes into the bus topology, every node connected to the cable will receive that message. A disadvantage of this setup is that having one cable connect to every device on a network creates a single point of failure.

But bus topologies aren’t all negative. Some positives include being simple and easy to deploy and scale, and reliable as long as the cable does not fail.



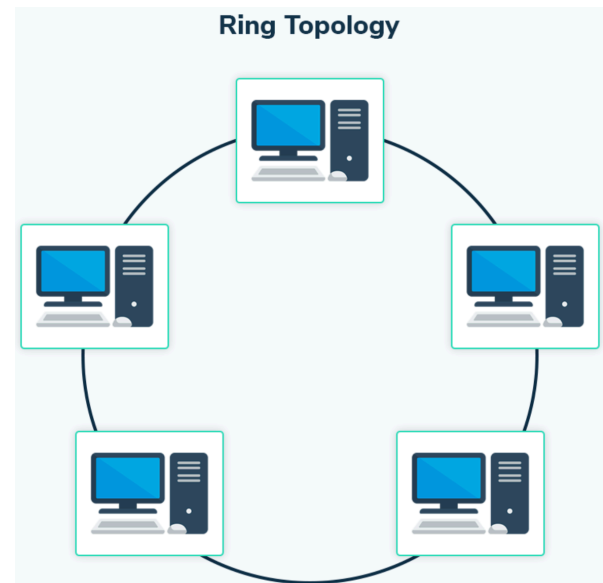
3. Ring

Every node on a ring topology relies on other nodes on the network to pass along information.

Every device on a ring network is connected to two nodes. Ring topologies can pass information one way meaning every node must cooperate to pass that information along to ensure it reaches its destination on the network, while other rings are bidirectional.

Some advantages of this topology include minimal collisions, cost, ease of implementation, and a high data transmission speed.

The crucial disadvantage is obvious: if one node fails to do its job, all communication breaks down.

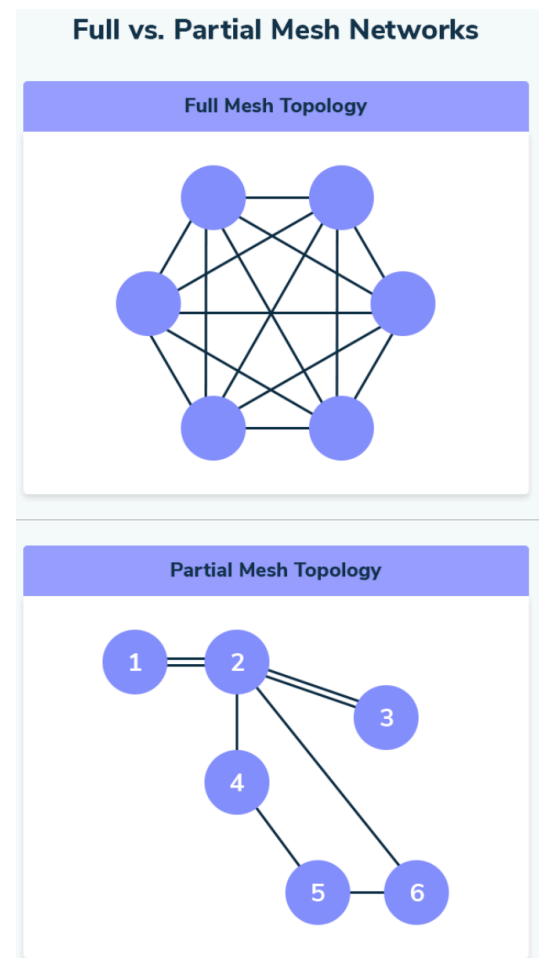


4. Mesh

A mesh network is a highly interconnected topology where every node is connected to another.

This means every node can take multiple routes when communicating with one another. There is also a partial mesh network where only some nodes can directly connect.

Some benefits of a mesh network include increased stability, range, and direct communication. The negatives of a mesh networks may be the cost, scalability, and complexity of setting up and managing them.

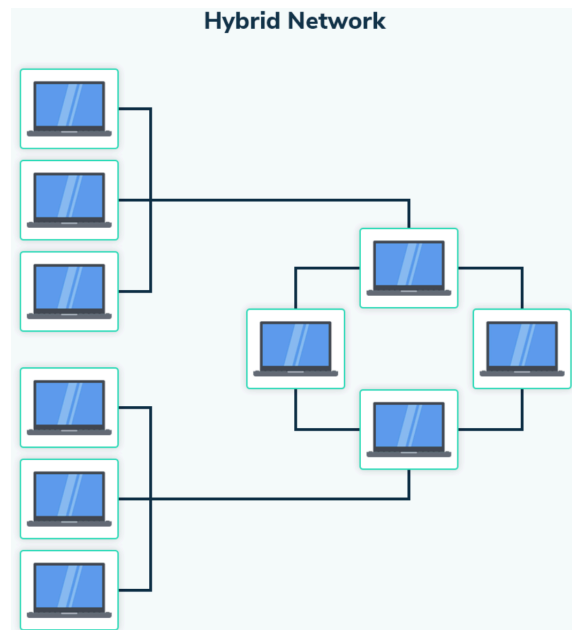


5. Hybrid

Sometimes, organizations can't rely on one topology for all their networking needs, opting to implement a hybrid topology strategy.

This hybrid strategy uses multiple topologies for their networking needs.

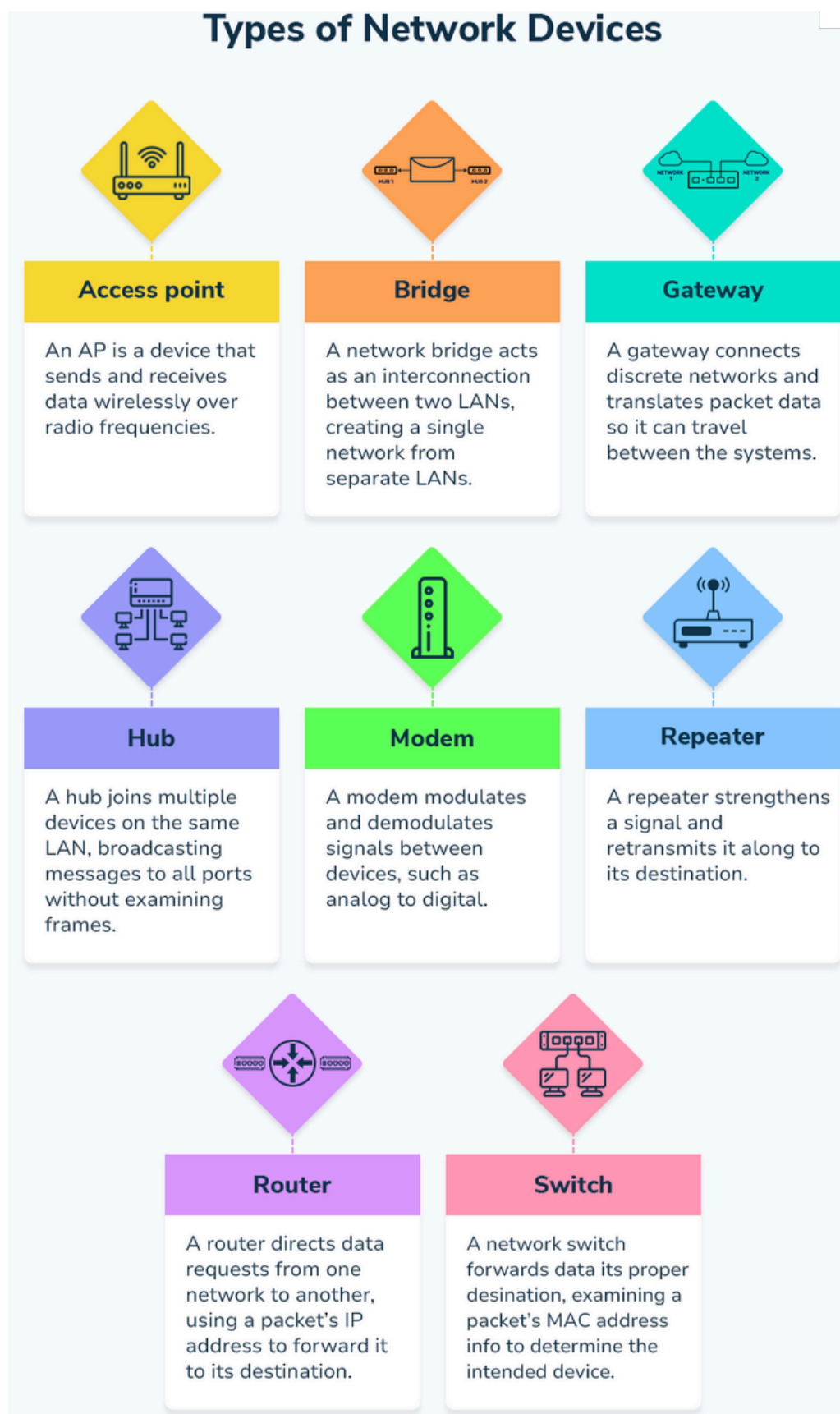
Perhaps an organization near you uses a star topology for most of their everyday networking needs but also needs to configure a wireless mesh network should a network cable fail to connect to an access point.



Bus and ring topologies aren't nearly as popular as they once were. The main topologies we use are star, mesh, and hybrid topologies.

Introduction to Network Hardware

To create network types and topologies, you'll have to use some of the following hardware.



Router	A router allows you to connect with networks on the internet using an IP address to forward packets.
Switches	Switches use a MAC address to forward packets within a LAN. Switches need to connect with a router to access the Internet.
Hub	Similar, though not as intelligent as a switch, a hub connects internal devices by broadcasting messages to all connected devices and ports. For the most part, hubs can be replaced by switches.
Bridge	A bridge connects two LANS, creating one network in turn.
Modem	While most modern modems are built into routers, modems modulate signals to and from the Internet that otherwise would be unintelligible to a router. Think of a modem as a translator for networking devices.
WAP	A WAP or wireless access point is a switch for wireless devices, allowing them to connect to and communicate within a network.
Firewall	A firewall uses rules to filter traffic coming in and out of your internal network. A firewall is built into most home routers. However, most enterprises will use firewall-specific hardware.

Other common pieces of network hardware include:

- **Hosts:** A network host is any network device communicating on a network (computer, printer, etc.).
- **Servers:** Network servers are powerful machines designed to handle various networking tasks such as identity and access management, and data storage.

Introduction to IP Addressing and Subnetting

If you want to connect to the Internet or communicate within a network, you'll need an IP address. Here's a quick primer on everything related to IP addresses.

What Are IP Addresses?

An IP address is a unique string of numbers (IPv4) or numbers and letters (IPv6) used to identify a device connected to the Internet.

IP stands for Internet Protocol, a set of rules to format data efficiently to send through the Internet.

Every time you connect to a router, you're provided a new private IP address that the router will use to identify you. Your private IP address is known only within your local network.

Your router also has a public IP address, which it then used to connect to the Internet. Your public IP address does not change as it's assigned by your ISP (Internet Service Provider).

Subnetting

Subnetting is a way to make a network smaller. Imagine if you had hundreds or thousands of devices in a network.

Making sure that all the data generated by these devices is quickly routed would be difficult. So, to make routing easier, devices are grouped via subnetting.

The process of subnetting involves creating a subnet mask. A subnet mask is akin to an IP address, but it's only used for internal routing purposes.

NAT

NAT stands for network address translation.

Due to the finite amount of public IP addresses, not every device can have its own public IP address.

NAT translates a private IP address to a public one to access the internet—and vice versa. Slowly, we are transitioning to using IPv6 addresses, which are plentiful and would allow every device to have its own public IP address.

But until then, we'll be stuck using IPv4 and relying on our router to use NAT to translate our private IP address so that we may connect to the internet.

All devices within a LAN have their private IP address but share a single public IP address thanks to NAT.

IPv4 Address Classes

In the IPv4 IP address space, there are five classes: A, B, C, D and E. Each class has a specific range of IP addresses. Primarily, class A, B, and C are used by the majority of devices on the Internet. Class D and class E are for special uses.

There are three main private IPv4 address classes. The type of address class you'll use depends on the size of the network you're on.

Class A Public IP Range: 1.0.0.0 to 127.0.0.0

Class A Private IP Range: 10.0.0.0 to 10.255.255.255

This range is used by large businesses that have many devices that want to connect to the internet.

Class B Public IP Range: 128.0.0.0 to 191.255.0.0

Class B Private IP Range: 172.16.0.0 to 172.31.255.255

Medium-sized businesses use the Class B range of IP addresses.

Class C Public IP Range: 192.0.0.0 to 223.255.255.0

Class C Private IP Range: 192.168.0.0 to 192.168.255.255

The class C range is the range you use when on your home network or in a small business.

Network admins need to choose their network class wisely to ensure each device they want to connect to their network can do so.

Introduction to Networking Protocols

Without rules for networking, data could never be transferred correctly. There are protocols for each type of interaction.

Some of the most common [networking protocols include](#):

- **HTTP:** Unencrypted hypertext transfer protocol used to access web servers
- **HTTPS:** Encrypted hypertext transfer protocol
- **FTP:** File transfer protocol used to transfer data
- **SMTP:** Simple mail transfer protocol, is used for sending email between mail servers
- **SSH:** Secure shell is used for sending commands to a computer over an unsecured network
- **DNS:** Domain name translation is used to translate IP addresses of websites to human readable names and vice versa

Each protocol has its own logical port number. Ports allow computers to understand one another as they help differentiate traffic. Ports aren't physical locations but virtual destinations where protocols take place.

Well-Known Ports: Unencrypted vs Encrypted

Must-know commonly used ports to memorize



OSI Reference Model

The OSI model is the standardized language computers use to talk to one another. While the current OSI model is a little dated, it's still widely used to understand how the internet works and to help with network troubleshooting.

There are seven layers to the OSI model:








1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Data being received to your host device must move through all of the OSI layers, starting with the Physical (data travelling through a modem) to the Application (what you use to access the data).

Likewise, sending information through a network or the internet requires the data to move from the Application layer to the Physical before heading to its final destination.

Each layer is explained in the infographic below.

The 7-Layer OSI Model

No.	Layer	Function	Data unit	Hardware	Protocols
7	Application 	Human-computer interaction through applications that access network services	Message/data	Gateway	UPnP, DHCP, DNS, HTTP, HTTPS, NFS, NTP, POP3, SMTP, SNMP, FTP, Telnet, SSH, TFTP, IMAP
6	Presentation 	Data formatting and encryption/decryption	Message/data	Gateway redirector	TLS, SSL, AFP
5	Session 	Inter-host communication	Message/data	Gateway	NetBIOS, RPC, SMB, Socks
4	Transport 	Data transmission	TCP: segment; UDP: datagram	Gateway	TCP, UDP, SCTP
3	Network 	Path determination and logical addressing	Packet, datagram	Router, Brouter	ARP, IP, NAT, ICMP, IPsec, ICMP (ping)
2	Data Link 	Physical addressing	Frame, cell	Switch, bridge, NIC	ARP, Ethernet, L2TP, LLDP, MAC, NDP, PPP, PPTP, VTP, VLAN
1	Physical 	Binary signal transmission over physical media	Bit, frame	Cables, modem, hub, repeater, NIC, multiplexer	Ethernet, IEEE802.11, ISDN, USB, Bluetooth

Introduction to Network Security

The Internet isn't inherently secure.

To harden systems and ensure that your data isn't compromised, cyber security professionals use the following network security tools:

- **Firewalls**, which use rules to filter traffic in and out of a network;
- **IDS**, or intrusion detection systems, which monitor network traffic and issue notifications when identifying suspicious traffic;
- **IPS**, or intrusion prevention system, which works similarly to an IDS but can take automatic action to block suspicious traffic;
- **SIEM**, or security information and event management system, used to collect logs from all devices connected to your network to monitor your network traffic;
- **VPN**, or virtual private network, that connects you from your network to a remote network;
- **VLAN**, or virtual local area networks, used to group devices together and create a network within a network (e.g., creating networks for each company department)

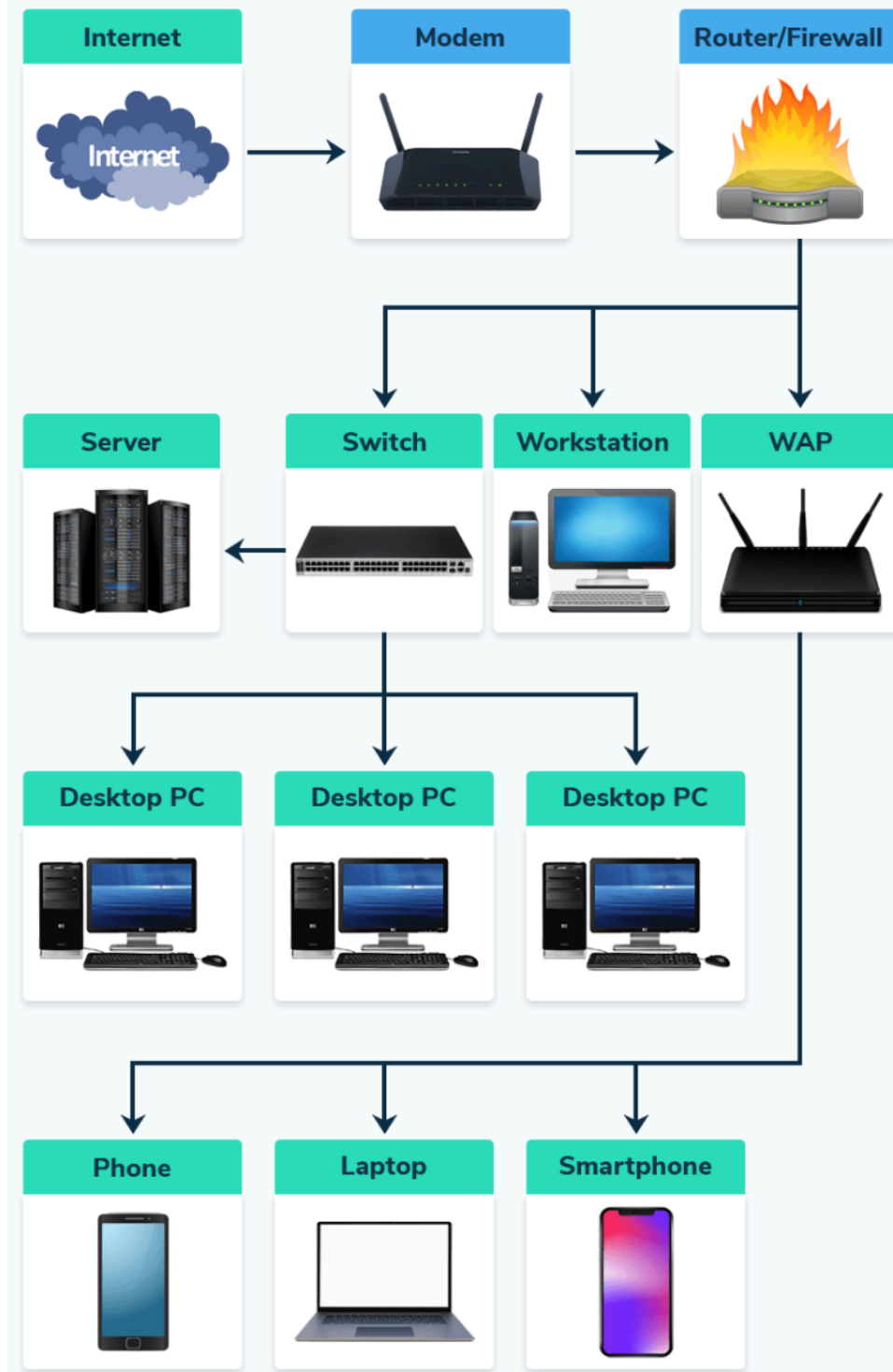
Bringing a Network Together

Understanding how each network component interacts with the others can be challenging. To better understand how networks function, even professionals use network diagrams to create easy-to-understand visuals.

This is a diagram of the network architecture we might see in the home or a small business.

When visualized, it's easier to understand what devices we have on our network and how they communicate.

Network Diagram



Questions:

What is the full form of OSI?

- ☐ a) optical service implementation
- ☐ b) open service Internet
- ☐ c) open system interconnection
- ☐ d) operating system interface

How many layers are there in the ISO OSI reference model?

- ☐ a) 7
- ☐ b) 5
- ☐ c) 4
- ☐ d) 6

What are nodes in a computer network?

- ☐ a) the computer that routes the data
- ☐ b) the computer that terminates the data
- ☐ c) the computer that originates the data
- ☐ d) all of the mentioned

Which of the following devices forwards packets between networks by processing the routing information included in the packet?

- ☐ a) firewall
- ☐ b) bridge
- ☐ c) hub
- ☐ d) router

Which layer does the data link layer take packets from and encapsulate them into frames for transmission?

- ☐ a) transport layer
- ☐ b) application layer
- ☐ c) network layer
- ☐ d) physical layer

Which of this is not a network edge device?

- ☐ a) Switch
- ☐ b) PC
- ☐ c) Smartphones
- ☐ d) Servers

Which type of network shares the communication channel among all the machines?

- ☐ a) anycast network
- ☐ b) multicast network
- ☐ c) unicast network
- ☐ d) broadcast network

Which topology requires a multipoint connection?

- ☐ a) Ring
- ☐ b) Bus
- ☐ c) Star
- ☐ d) Mesh

Which of the following networks extends a private network across public networks?

- ☐ a) virtual private network
- ☐ b) local area network
- ☐ c) storage area network
- ☐ d) enterprise private network

Which layer is responsible for process to process delivery in a general network model?

- ☐ a) session layer
- ☐ b) data link layer
- ☐ c) transport layer
- ☐ d) network layer

What is the term for the data communication system within a building or campus?

- ☐ a) MAN
- ☐ b) LAN
- ☐ c) PAN
- ☐ d) WAN

Which network topology requires a central controller or hub?

- ☐ a) Ring
- ☐ b) Bus
- ☐ c) Star
- ☐ d) Mesh

If a link transmits 4000 frames per second, and each slot has 8 bits, what is the transmission rate of the circuit using Time Division Multiplexing (TDM)?

- ☐ a) 500kbps
- ☐ b) 32kbps
- ☐ c) 32bps
- ☐ d) 500bps

Which layer provides the services to user?

- ☐ a) physical layer
- ☐ b) presentation layer
- ☐ c) session layer
- ☐ d) application layer

Which of the following is used in an attempt to render a computer resource unavailable to its intended users?

- ☐ a) botnet process
- ☐ b) worms attack
- ☐ c) virus attack
- ☐ d) denial-of-service attack

Which topology does the Internet resemble?

- ☐ a) Ring
- ☐ b) Bus
- ☐ c) Star
- ☐ d) Mesh

Which device is used to connect different network segments in a computer network?

- ☐ a) Repeater
- ☐ b) Router
- ☐ c) Bridge
- ☐ d) Modem

In a computer network, what is the main function of the application layer?

- ☐ a) To provide network services to the applications
- ☐ b) To transmit data between network devices
- ☐ c) To package data for transfer
- ☐ d) To route data between networks

Which command can be used to view the current IP configuration of a device?

- ☐ a) ipconfig
- ☐ b) ifconfig
- ☐ c) Both ipconfig and ifconfig
- ☐ d) netstat

Which layer of the OSI model is responsible for establishing, managing, and terminating sessions between applications?

- ☐ a) Session Layer
- ☐ b) Transport Layer
- ☐ c) Application Layer
- ☐ d) Presentation Layer

In the TCP/IP model, which layer corresponds to the OSI model's Physical and Data Link layers?

- ☐ a) Application
- ☐ b) Transport
- ☐ c) Internet
- ☐ d) Network Interface

The process of encapsulation involves data moving from which layer to which layer?

- ☐ a) Application to Physical
- ☐ b) Physical to Application
- ☐ c) Transport to Network
- ☐ d) Network to Transport

Which command can be used to display the current TCP/IP network configuration?

- ☐ a) ipconfig /all
- ☐ b) netstat -r
- ☐ c) arp -a
- ☐ d) tracert

A device is unable to connect to any network. Which OSI layer should be investigated first?

- ☐ a) Application
- ☐ b) Presentation
- ☐ c) Network
- ☐ d) Physical

If a computer can connect to local devices but not to the Internet, what might be misconfigured?

- ☐ a) IP address
- ☐ b) Subnet mask
- ☐ c) Default gateway
- ☐ d) MAC address

What is the standard Ethernet frame size for most networks?

- ☐ a) 64 bytes to 1518 bytes
- ☐ b) 128 bytes to 1024 bytes
- ☐ c) 1500 bytes to 2000 bytes
- ☐ d) 100 bytes to 1500 bytes

How does a switch determine the destination of an Ethernet frame?

- ☐ a) By using the source IP address
- ☐ b) By using the destination MAC address
- ☐ c) By using the source MAC address
- ☐ d) By broadcasting to all ports except the source

A computer can access local network devices but not the internet.
What should be checked on the switch?

- ☐ a) VLAN configurations
- ☐ b) Port speed settings
- ☐ c) Power settings
- ☐ d) Firmware updates

What is the function of an IP subnet mask?

- ☐ a) To separate the network address from the host address
- ☐ b) To encrypt IP addresses
- ☐ c) To detect IP conflicts
- ☐ d) To assign IP addresses automatically