Certified Information Systems Security Professional (CISSP) Certification Training Course

CISSP® is a registered trademark of (ISC)² ®

Domain 04: Communications and Network Security

Learning Objectives

By the end of this lesson, you will be able to:

- Evaluate OSI, TCP/IP, and UDP communication protocols to improve protocol selection and troubleshooting
- Examine SDN and SD-WAN concepts to enhance network agility and management
- Assess different transmission media to select the best fit for network environments
- Identify and assess the key features of endpoint security for safeguarding devices against cyber threats
- Investigate and assess different types of network attacks to strengthen preventive measures and response strategies

Overview of Communication Models

Introduction to Communication

It is the process of transferring information from one system or device to another.

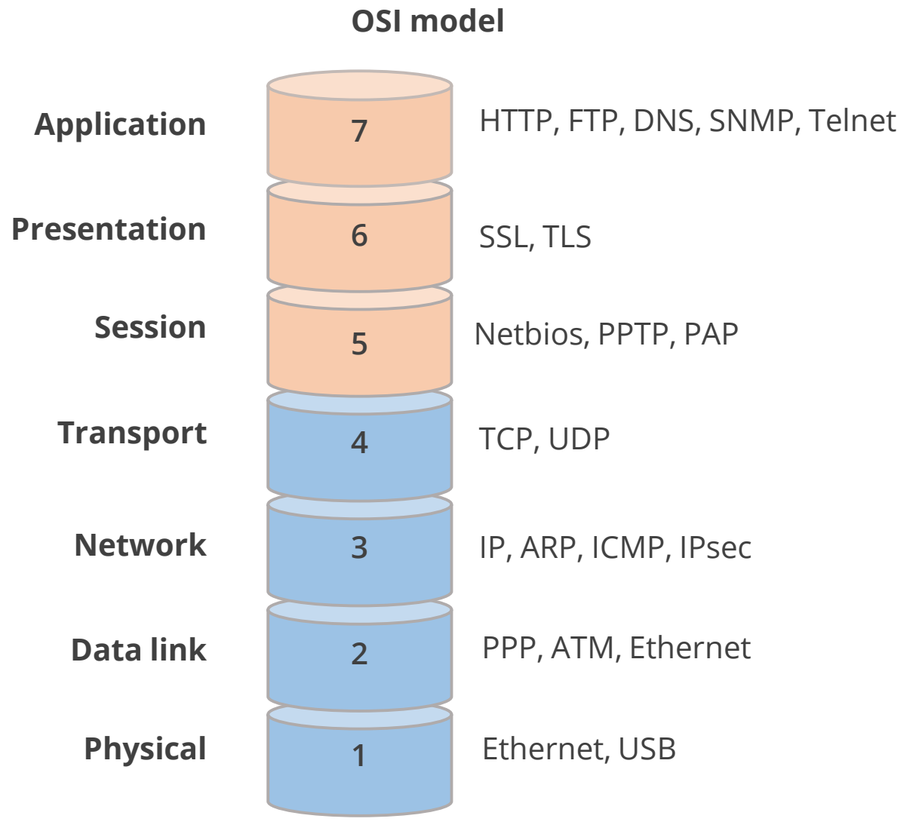
Various communication protocols define communication.

- The protocols can be grouped into stacks, family, or suite.
- OSI and TCP/IP models are the most popular communication models.
- Communication is divided into different layers by both the models.
- Security can be addressed more efficiently using the layered approach.

Open Systems Interconnection (OSI)

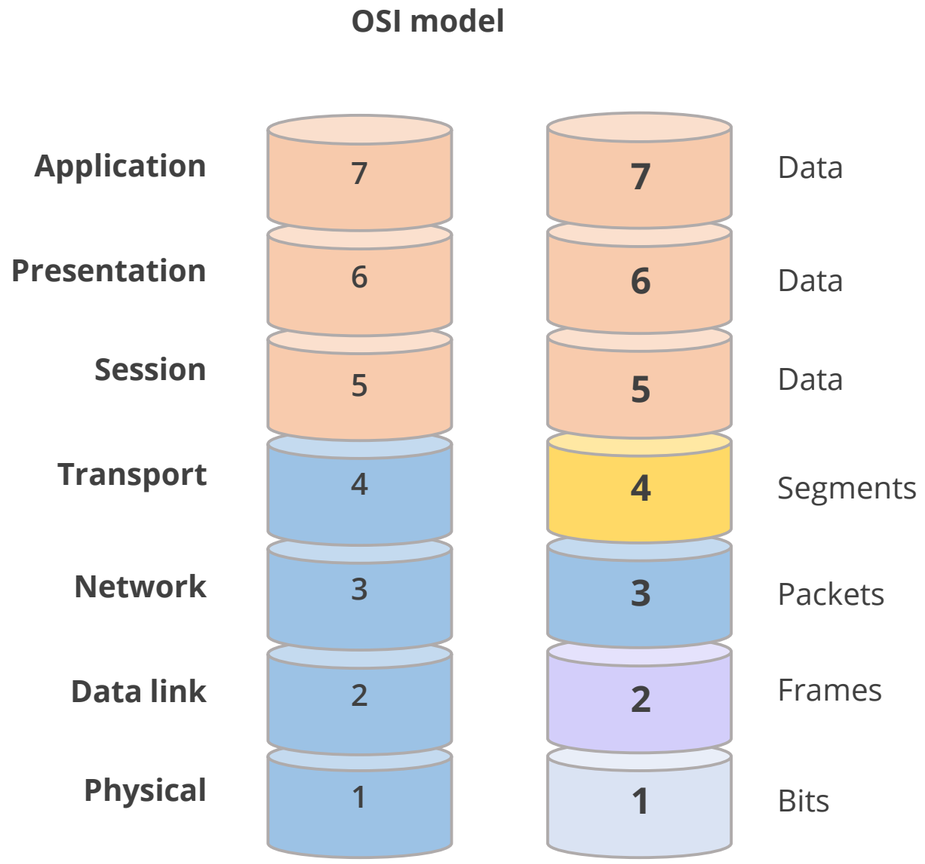
This model serves as a standard framework for network communications and allows different and dissimilar networks to communicate seamlessly.

It explains how data is transmitted between computers.



Open Systems Interconnection (OSI)

- Each layer communicates with the same layer's software or hardware on other computers.
- The four lower layers (transport, network, data link, and physical) handle end-to-end data flow through the network.
- The three upper layers (application, presentation, and session) focus on providing services to the applications.
- Data is encapsulated with protocol information as it moves down the layers before network transit.



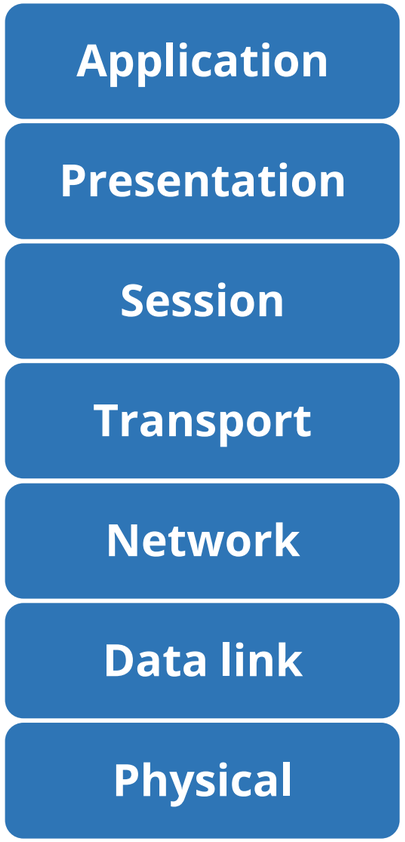
OSI Layers

7	**Application**	Provides the contents of the letter, representing the data the user interacts with, such as emails or web browsers
6	**Presentation**	Translates data into a format the receiving computer can understand, like a person opening and translating a letter
5	**Session**	Ensures mail is delivered to the correct mailbox by establishing, maintaining, and ending communication with the receiving device
4	**Transport**	Verifies that data arrives safely like a security check, preventing errors and damage to the data
3	**Network**	Determines the best route for data like the system the post office uses to find the optimal path to its destination
2	**Data link**	Prepares data by packaging it and adding a delivery address, just like the sorting process at the post office
1	**Physical**	Delivers data like a mail truck, using cables and wires to transport it from one computer to another

Working of the OSI Model

The following explains the process of data transmission and management through its layered approach:

- Data is sent from a source computer to a destination computer.
- Each protocol operates in a specific layer.
- Each protocol in the source computer has a job allocated.
- When the data packet reaches the destination computer, it moves up the model.
- Each protocol detaches and examines only the data that was attached by its protocol counterpart at the source computer.
- Each layer at the individual destination sees and deals only with the data that was packaged by its counterpart on the sending side.



Working of the OSI Model

The following illustration explains how data travels in the model:

1 Data travels down the stack

Host A	
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data link
1	Physical

2 Data travels through the network

Host B	
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data link
1	Physical

3 Data travels up the receiving stack

OSI Model: Physical Layer

It defines the physical connection between a computer and network.

- It converts the bits into voltages or light impulses for transmission.
- It defines rules by which bits are passed from one system to another on a physical communication medium.
- It specifies types of signaling, such as analog or digital, electrical or optical characteristics of signals, asynchronous or synchronous, simplex, full, or half duplex.

OSI Model: Physical Layer

- It defines the topology (star, bus, and ring).
- It provides services to the data link layer.
- It has only two responsibilities:
  - Sending and receiving bits
  - Defining standard interfaces

Examples

EIA-232 (RS-232), Synchronous Optical Network (SONET), ISDN, and DSL are some of the standard interfaces at this layer.

Network Topologies

It defines the way the network devices are organized to facilitate communications.

	**Bus**	All transmissions of the network nodes travel the full length of the cable and are received by all other stations.
	**Ring**	The network nodes are connected by unidirectional transmission links to form a closed loop.
	**Hierarchical**	It is a bus-type topology. In this topology, branches can have multiple nodes.
	**Star**	The nodes of a network are connected directly to a central LAN device.
	**Mesh**	All the nodes are connected to every other node in a network.

Transmission Media

They are used for transmitting data from a source to destination.

- They are situated beneath the physical layer and are managed by it.
- They are also called as communication channels.

Types of Cabling

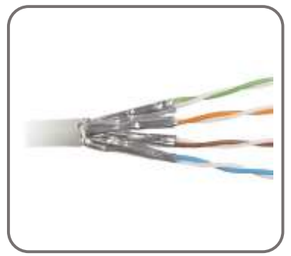
Data transmission happens over cables.

Unshielded twisted pair

Coaxial cable

Types of cables

Shielded twisted pair



Fiber optic cable

Twisted Pair

It consists of two copper wires twisted together, which reduces electrical interference.

- It can be used for both analog and digital transmissions.
- The maximum length for a twisted pair cable is 100 meters, and it uses an RJ-45 connector.
- It can span a distance of 100 meters, beyond which a device is needed to amplify the signals.
- Shielded twisted pair is shielded and provides better immunity to electromagnetic interference (EMI).
- Unshielded twisted pair is unshielded and is more susceptible to EMI and crosstalk.

Coaxial Cable

It is a type of electrical cable consisting of a central conductor, an insulating layer, a metallic shield, and an outer insulating layer.

- It is expensive and resistant to electromagnetic interference (EMI).
- Thinnet and thicknet are two main types currently used in LANs.
- Thinnet (10Base2) can span a distance of up to 185 meters and provides throughput of up to 10 Mbps.
- Thicknet (10Base5) can span a distance of up to 500 meters and provides a throughput of up to 10 Mbps (megabits per second).

Fiber Optic Cable

It is a physical medium capable of conducting modulated light transmission.

- It carries signals as light waves, enabling higher transmission speeds and longer distances due to reduced attenuation.
- It is usually reserved for connections between the backbone and devices in large networks.
- It is the most reliable and expensive option.
- It has a higher transmission speed that allows signals to travel over longer distances.

It can span distances of over 1.24 miles, after which a device is needed to amplify the signals.

Cabling Problems

These can significantly impact network performance and reliability. Some of the common issues include:

Electromagnetic interference(EMI)

- It is caused by surrounding devices or wiring characteristics such as motors, computers, fluorescent lights, and microwave ovens.

Attenuation (signal loss)

- It occurs as the signal travels.
- It increases with higher frequencies.
- It can also be caused by cable breaks and malfunctions.

Cross talks

- It happens when electrical signals spill over into adjacent wires.
- UTP cables are more vulnerable to these issues compared to STP cables.

OSI Model: Data Link Layer

It defines the protocol that computers must follow to access the network for transmitting and receiving messages.

- It establishes the communication link between individual devices over a physical link or channel.
- It determines hardware (physical or MAC) addresses as well as the communication process that occurs within a media type.
- It also formats the message into data frames and adds a customized header containing the hardware destination and source address.

OSI Model: Data Link Layer

It provides services to the network layer and has the following sub-layers:

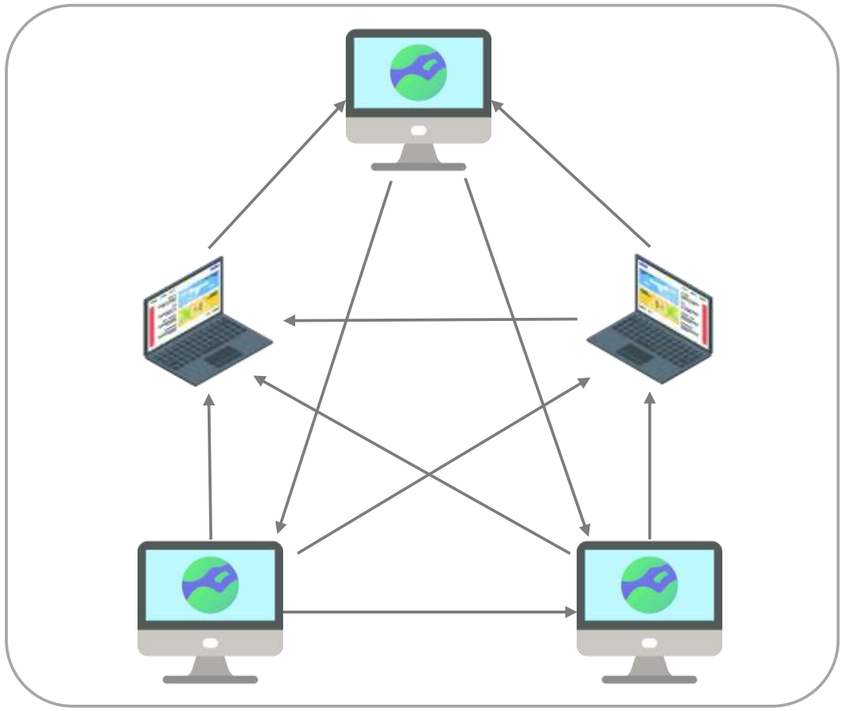
- **Media access control (MAC) layer**: It controls the way a system on the network gains access to the data and gets permission to transmit it.
- **Logical link control (LLC) layer**: It controls frame synchronization, error check, and flow.

Examples

Address resolution protocol (ARP), serial line internet protocol (SLIP), and point-to-point protocol (PPP)

Collision Domain

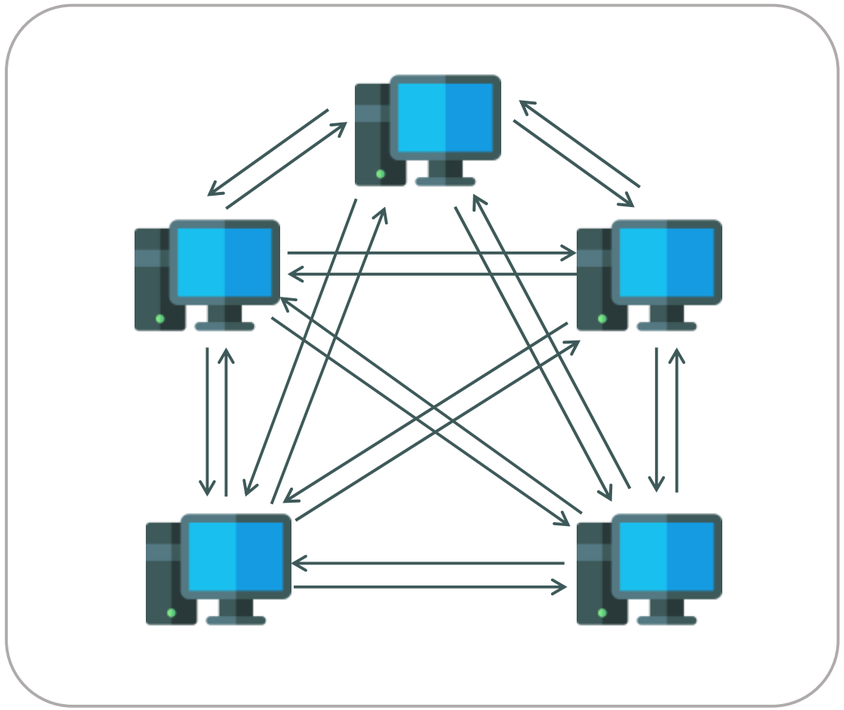
It is a group of computers that are contending for the same shared communication medium.



It is typically found in networks connected by a hub, repeater, or wireless access points.

Broadcast Domain

It is a set of computing nodes that can receive all layer 2 (data link layer) broadcast frames.

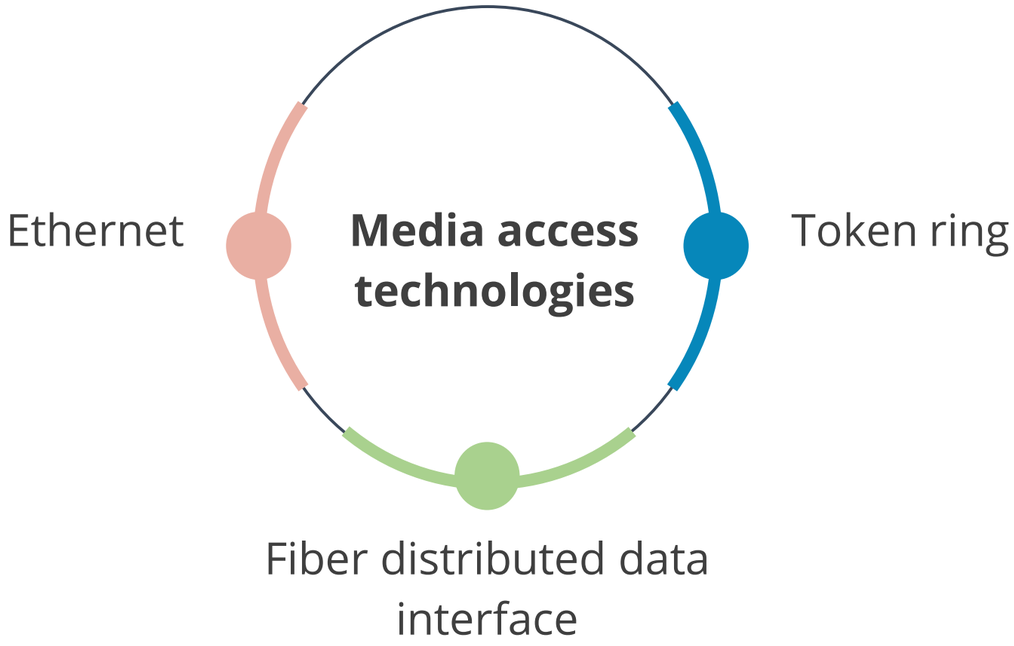


It consists of nodes interconnected by switches, bridges, or hubs but with no routers in between.

Media Access Technologies

It deals with how systems communicate over the media.

- It is typically represented in protocols, network interface card (NIC) drivers, and interfaces.
- It sets up the rules for how systems communicate in a network and how errors are handled.
- The maximum transmission unit (MTU) defines how much data a frame can carry on a specific network.



Ethernet

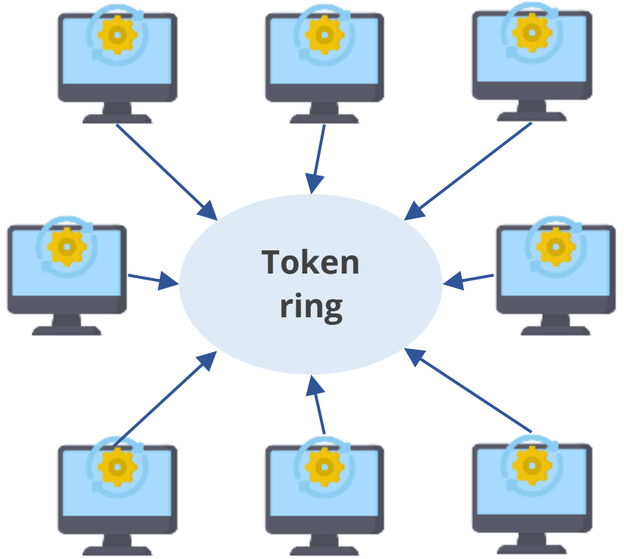
It is a set of technologies that enable several devices to communicate on the same network.

- It usually uses bus or star topology.
- It is defined by the 802.3 standard.
- It is a contention-based technology.
- It utilizes collision and broadcast domains.
- It uses carrier sense multiple access with collision detection (CSMA/CD).
- It supports full-duplex communication.
- It uses coaxial, twisted pair, or fiber-optic cabling types.

Token Ring

It is a LAN media access technology developed by IBM.

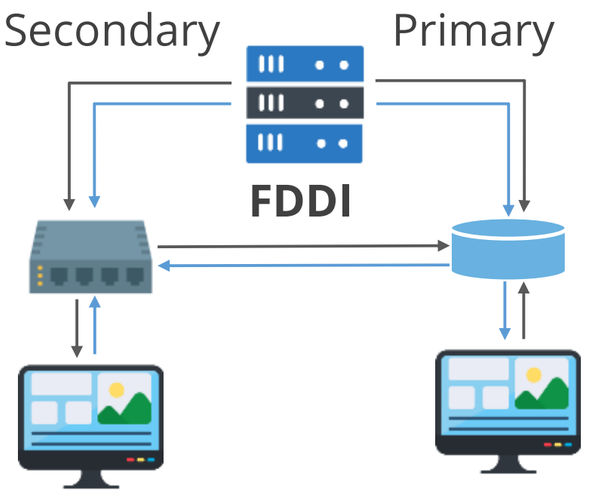
- It is defined by the 802.5 standard.
- It has a data transmission rate of up to 16 Mbps.
- It uses token-passing technology with a star-configured topology.
- Each computer is connected to the central hub known as a multiple access unit (MAU).
- An active monitor is used to remove frames that are continuously circulating the network.
- The beaconing mechanism ensures that if a computer detects a problem, it sends a beacon frame.



Fiber Distributed Data Interface (FDDI)

It is a high-speed, token-passing media access technology that operates on fiber-optic cabling.

- It has a transmission speed of up to 100 Mbps.
- It provides fault tolerance by incorporating a secondary counter-rotating ring.
- It is primarily used in backbone networks, such as metropolitan area networks (MAN).
- It can be deployed for distances up to 62.14 miles FDDI-2 offers fixed bandwidth, functioning like a broadband connection with quality of service (QoS) capabilities.



Copper distributed data interface (CDDI) operates over unshielded twisted pair (UTP) cabling and is used in LAN environments.

Media Sharing Technologies

It allows multiple systems to access the channel or medium in a way that prevents data corruption during transmission and enables traffic control during peak times.

The following techniques are utilized to manage data transmission and prevent collisions in shared communication channels:

Carrier sense multiple access with collision detection

Carrier sense multiple access with collision avoidance

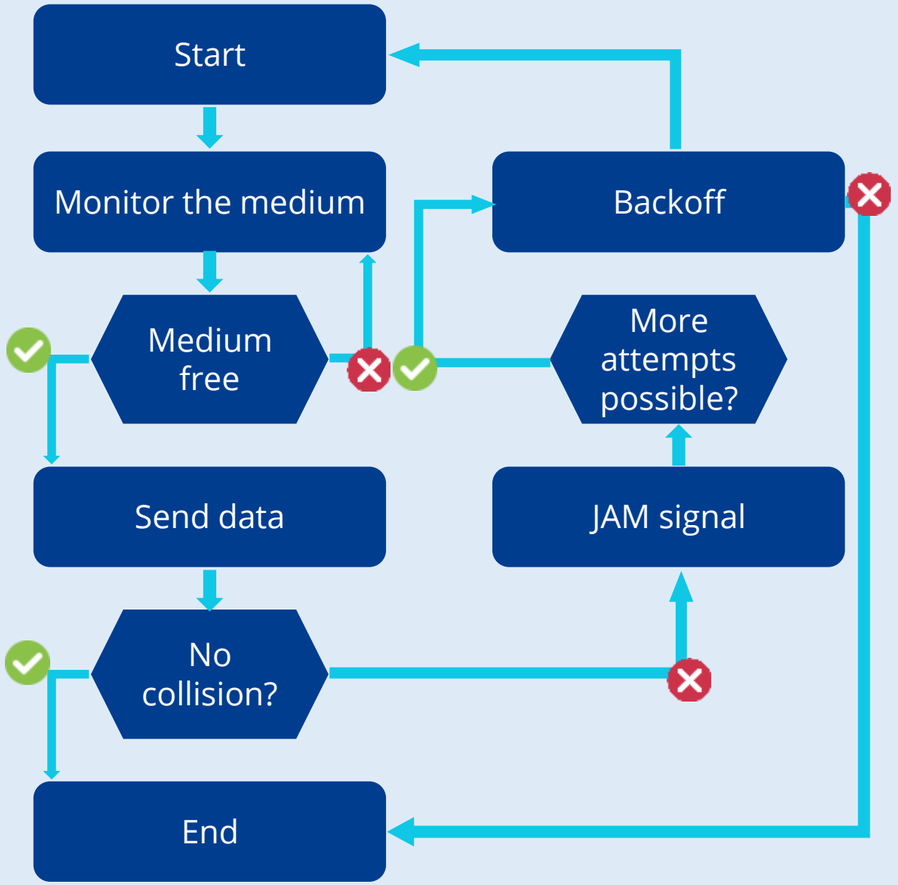
Token passing

Polling

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

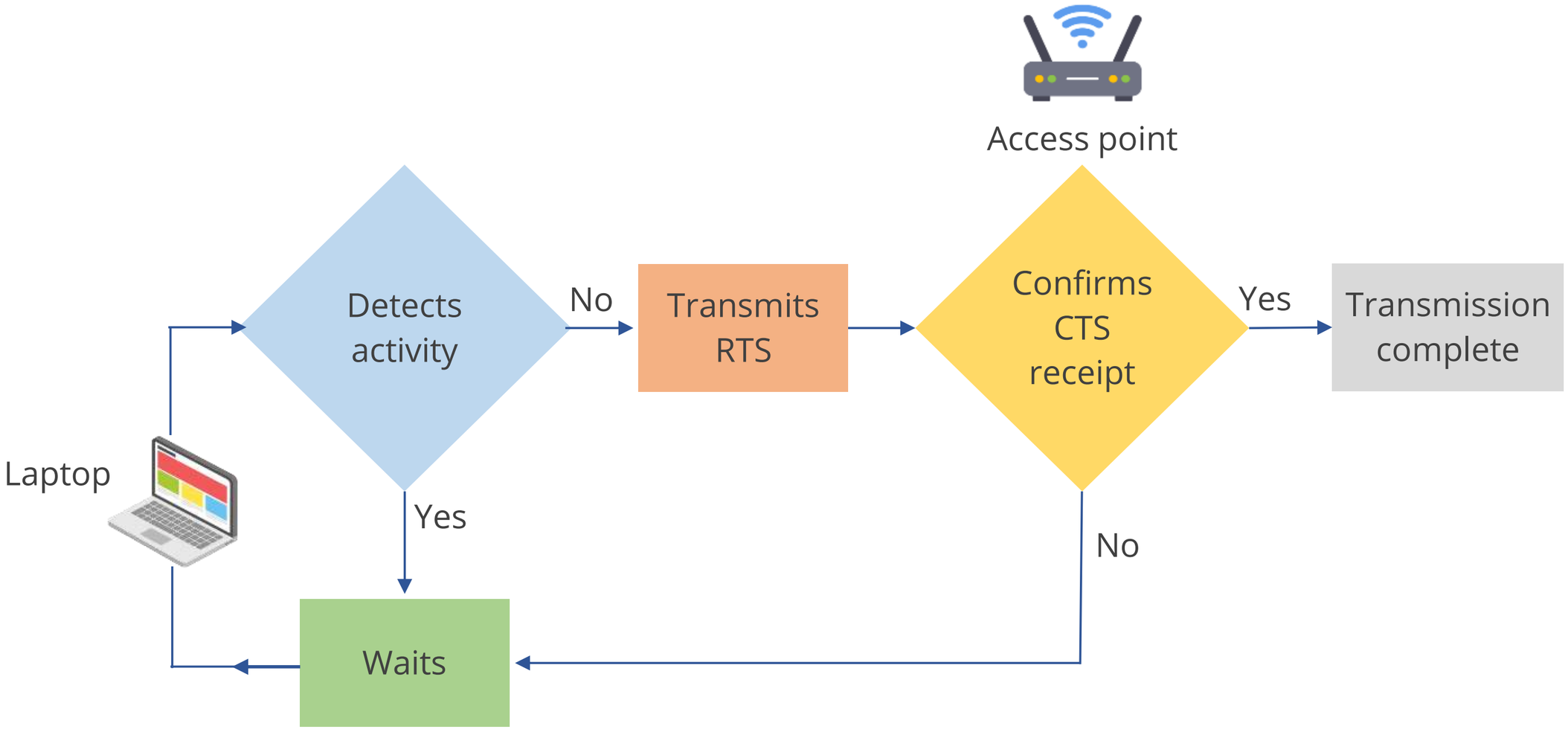
It is a protocol used to manage data transmission over Ethernet networks. Here's how it works:

- Systems monitor the network for transmission activity, and if they detect that the network is free, the computer transmits the data.
- If two devices transmit data simultaneously, a collision occurs.
- In a busy network, damaged cables, faulty connectors, or cables that are too long can cause too many collisions.
- If a collision happens, the devices in the network execute a random collision timer, called the back-off algorithm, to force a delay before they attempt to transmit data.



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

It is a protocol used primarily in wireless networks to prevent data collisions.



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

Here’s how it works:

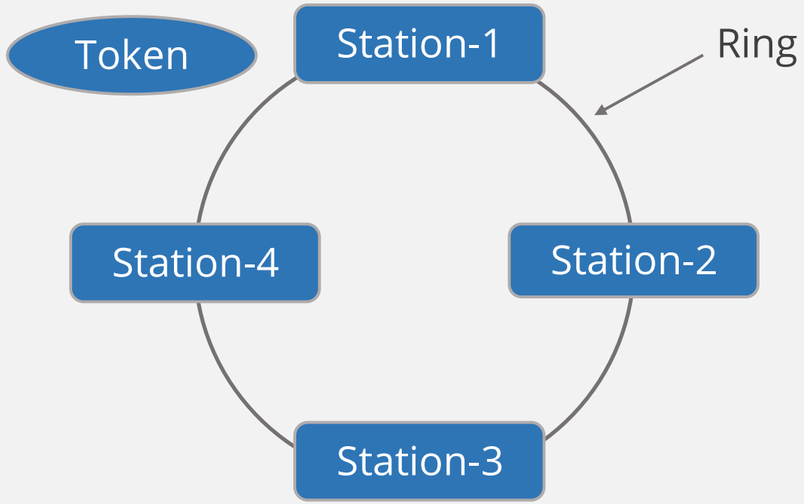
- Systems monitor the network for transmission activity. If the network is free, the computer sends a broadcast message, request-to-send (RTS), before transmitting data.
- Upon receiving the RTS, all the other systems are notified that the communication medium is in use, and they refrain from sending data.
- After the system finishes transmitting data, it sends a clear-to-send (CTS) message, indicating that the medium is free for others to use.

This keeps the communication structured and avoids collisions in wireless networks.

Token Passing

It is a 24-bit control frame that decides which computer is allowed to communicate and at what intervals.

- Only the computer holding the token is allowed to transmit data, while all other computers must wait for their turn.
- Only the computer that sent the data can remove the data from the token and release it, while the destination computer can only copy the data.
- Copper Distributed Data Interface (CDDI) works over UTP and is used in LAN environments.



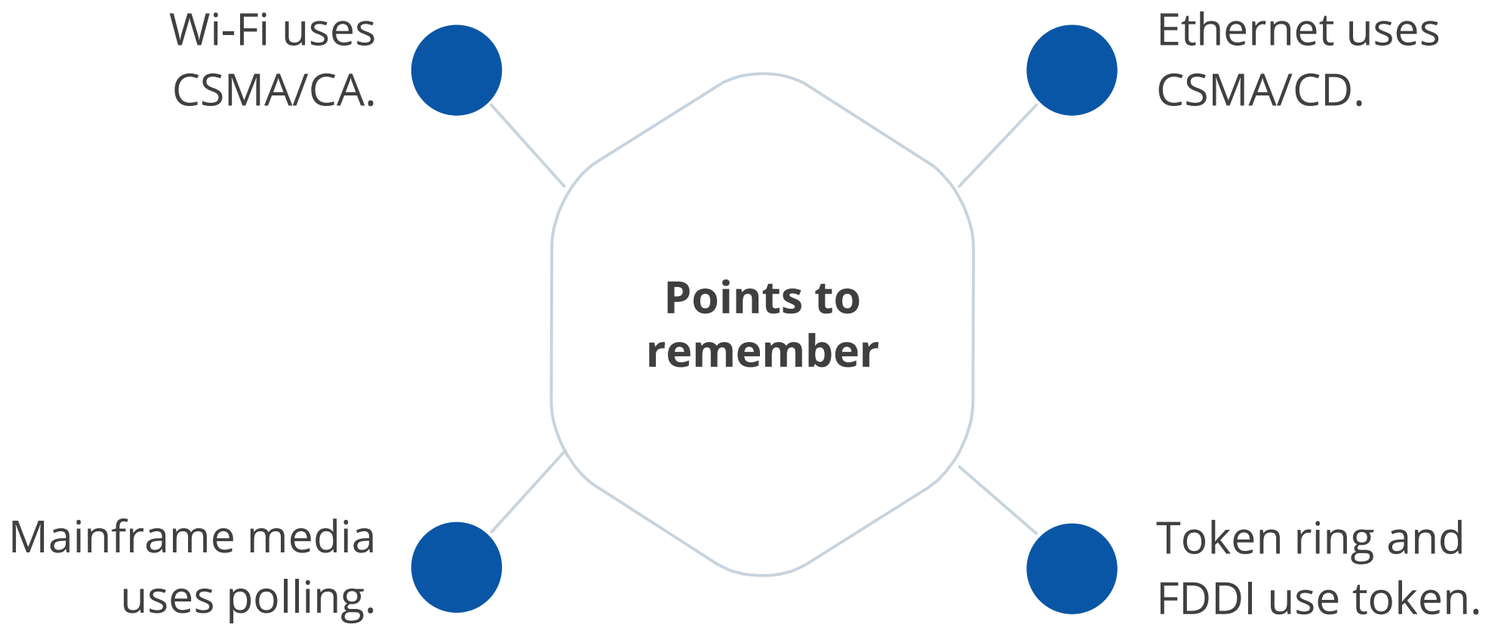
This method is used by token ring and FDDI.

Polling

It is a network communication method commonly used in mainframe environments.

- The systems are divided into primary stations and secondary stations.
- The primary stations poll the secondary stations at regular intervals to check for any data transmission.
- Secondary stations can only communicate when polled by the primary station.

Media Access Technologies

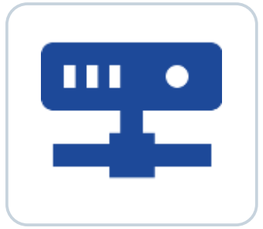


Hubs and Repeaters

These are basic networking devices used to extend and manage data transmission in networks.

Repeater

- It operates at the physical layer of the OSI model.
- Its primary function is to regenerate the signal before it becomes too weak or corrupted.
- This regeneration extends the length over which the signal can be transmitted on the same network.



Hubs

- It is essentially a multi-port repeater.
- It connects multiple wires coming from different branches.
- Since hubs cannot filter data, data packets are sent to all connected devices.

Switches

They are network devices that combine the functions of a repeater and a bridge.

- They amplify electrical signals like a repeater and include the intelligence of a bridge.
- They allow any device connected to one port by a switch to communicate with a device connected to another port with its virtual private link.
- They support full-duplex communication for simultaneous data transmission and reception.
- They operate at layer 2, layer 3, or layer 4.

Virtual Local Area Networks (VLANs)

They allow the ports on the same or different switches to be grouped so that the traffic is confined to the members of that group.

- They restrict broadcast, unicast, and multicast traffic.
- They create an isolated broadcast domain and a switch with multiple broadcast domains, like a router.
- They aid in isolating segments, reducing routing broadcasts, and segregating departmental functions.
- They can be segmented logically.

Virtual X LAN

It is a networking technology used in cloud computing, data centers, and multi-tenant environments to extend traditional VLANs across layer 3 networks, reducing complexity and overhead.

It provides a way to extend layer 2 networks across multiple physical data centers or cloud environments, enabling greater flexibility and scalability.

Virtual X LAN: Working

Encapsulation: It encapsulates layer 2 frames (ethernet frames) within a UDP packet, creating a VXLAN tunnel.

Tunneling: This tunnel is transmitted over an underlying transport network, such as IP.

Decapsulation: At the destination, this tunnel is decapsulated, and the original layer 2 frame is extracted.

Address Resolution Protocol (ARP)

It is a crucial protocol in networking, especially on LANs, such as home or office networks.

- It helps translate logical IP addresses, which identify devices on a network, into physical addresses.
- These physical addresses are called media access control (MAC) addresses, embedded in every network interface card (NIC).

ARP Functioning

IP address	MAC address
10.0.0.1	00-B0-D0-63-C2-26
10.0.0.2	00-B0-D0-63-C2-27
10.0.0.3	00-B0-D0-63-C2-28
10.0.0.4	??? 00-B0-D0-63-C2-29

4 ARP table is updated with 10.0.04 MAC address.

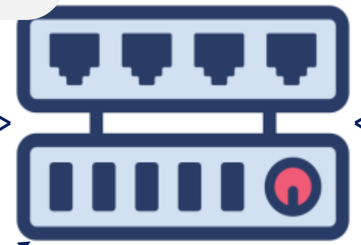
IP address 10.0.0.1
MAC address 00-B0-D0-63-C2-26

IP address 10.0.0.2
MAC address 00-B0-D0-63-C2-27

ARP query looking for MAC address of 10.0.0.4

2 ARP query looking for MAC address of 10.0.0.4

2 ARP query looking for MAC address of 10.0.0.4



IP address 10.0.0.4
MAC address 00-B0-D0-63-C2-29

2 ARP query looking for MAC address of 10.0.0.4

IP address 10.0.0.3
MAC address 00-B0-D0-63-C2-28

1 ARP request is broadcast to all systems and received by all four systems.

3 Only 10.0.0.4 will respond back with its MAC address.

ARP Cache Poisoning (ARP Spoofing)

It is a cyber attack that manipulates the address resolution protocol (ARP) for malicious purposes.

It disrupts normal network traffic by creating a false mapping between IP addresses and media access control (MAC) addresses.

ARP Cache Poisoning

IP address 10.0.0.1
MAC address 00-B0-D0-63-C2-26

IP address	MAC address
10.0.0.1	00-B0-D0-63-C2-26
10.0.0.2	00-B0-D0-63-C2-27
10.0.0.3	00-B0-D0-63-C2-28

4

ARP cache is poisoned with hackers' system MAC address.

IP address 10.0.0.2
MAC address 00-B0-D0-63-C2-27

ARP query looking for MAC address of 10.0.0.3

2

ARP query looking for MAC address of 10.0.0.3

2

1

ARP request is broadcast to all systems and received by all four systems.

2

ARP query looking for MAC address of 10.0.0.3

2

ARP query looking for MAC address of 10.0.0.3

IP address 10.0.0.4
MAC address 00-B0-D0-63-C2-29

IP address 10.0.0.3
MAC address 00-B0-D0-63-C2-28

3

The attacker responds with its MAC address claiming itself to be 10.0.0.3 and poisoning the cache.

OSI Model: Network Layer

It defines how the small packets of data are routed and relayed between end systems on the same network or interconnected networks.

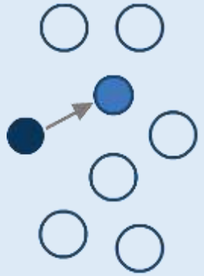
- It defines the most optimal path that a packet should take from the source to the destination.
- It establishes logical addressing so that any endpoint can be identified.
- It handles congestion in the network.
- It outlines how to fragment a packet into smaller packets to accommodate different media.
- It manages message routing, error detection, and control of node data traffic.
- It is primarily responsible for routing.
- It provides services to the transport layer.

Examples

IP, OSPF, ICMP, and RIP

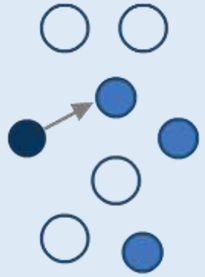
IP Addressing and Its Types

IP addressing enables network communication, and the internet layer provides different addressing types, allowing messages to be sent to one or more destination nodes.



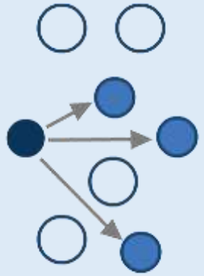
Unicast

Packet sent to a single IP address destination



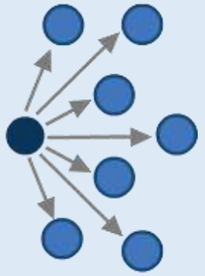
Anycast

Packet sent only to the nearest group of nodes



Multicast

Packet sent to a group of nodes on different networks



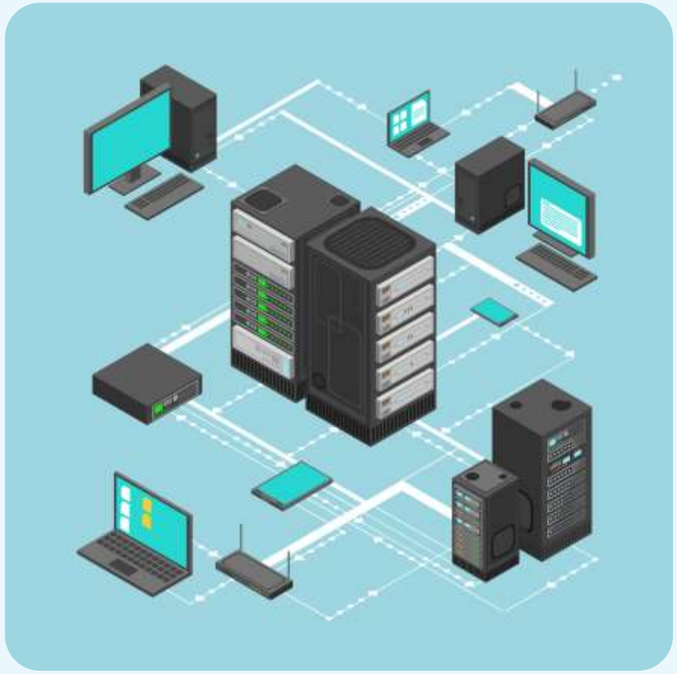
Broadcast

Packet sent to a network's broadcast address

Internet Control Message Protocol (ICMP)

It is a management protocol and messaging service provider for IP.

- Its primary function is to send messages between network devices.
- It can inform hosts of a better route to a destination.

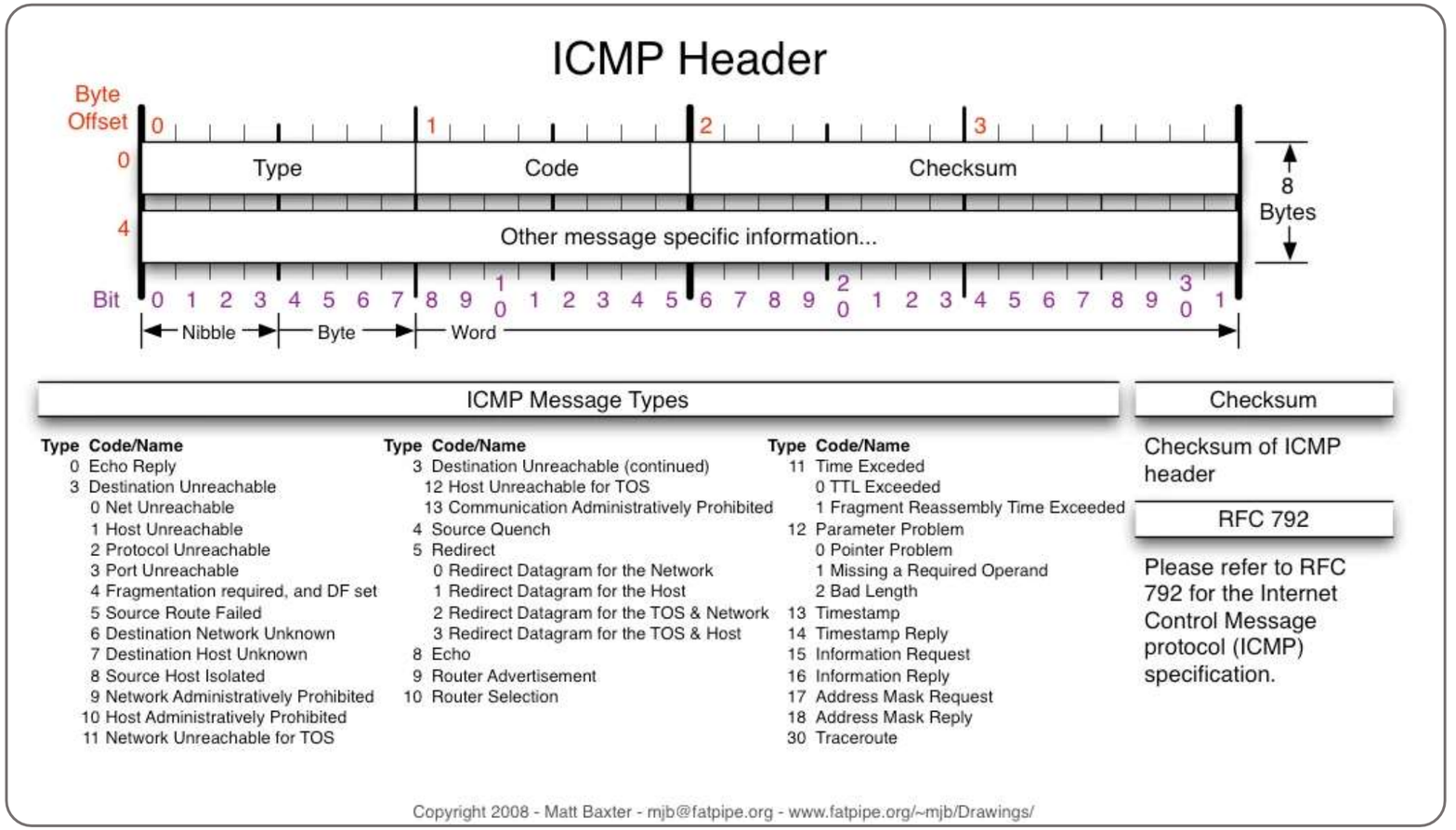


Example

PING is an ICMP utility used to check the physical connectivity of machines on a network.

Internet Control Message Protocol (ICMP)

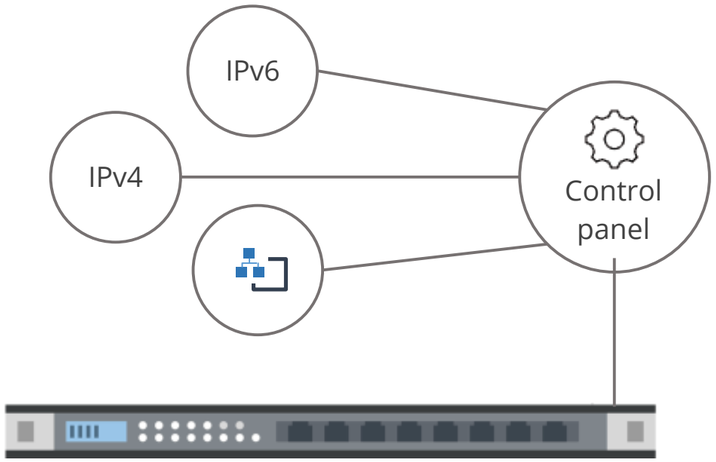
The format of the ICMP header is explained in the diagram below:



Internet Protocol (IP)

It is a network layer protocol that handles addressing and routing.

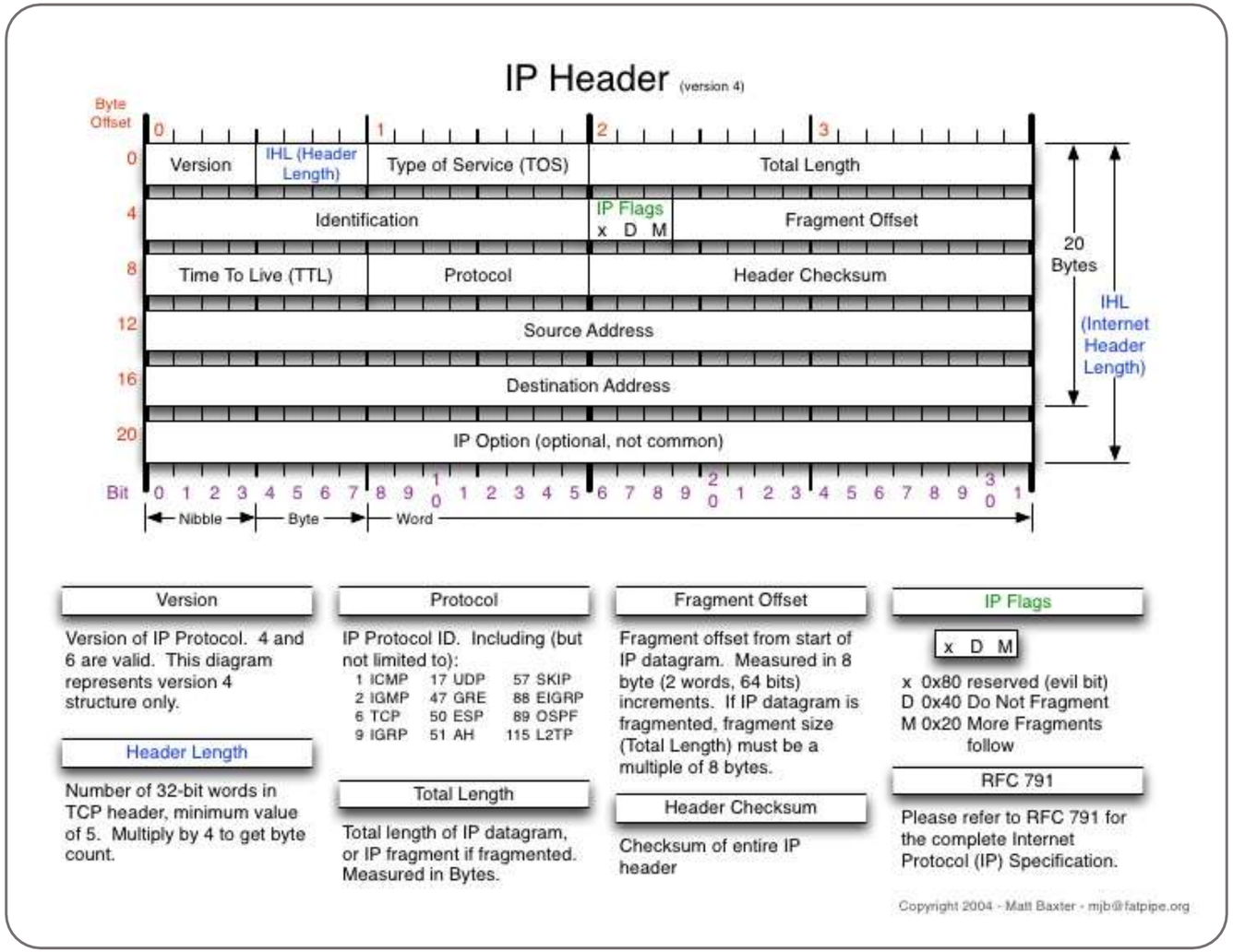
It specifies the packet format or datagrams and the addressing scheme.



The two types of IP versions are IPv4 (32-bit address) and IPv6 (128-bit address).

Internet Protocol (IP)

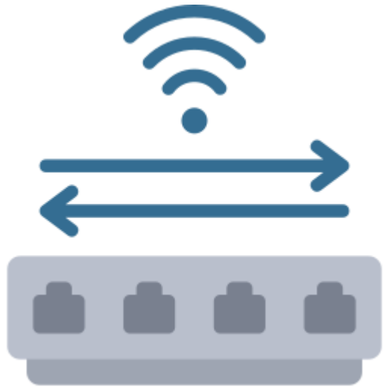
Its operation is illustrated below:



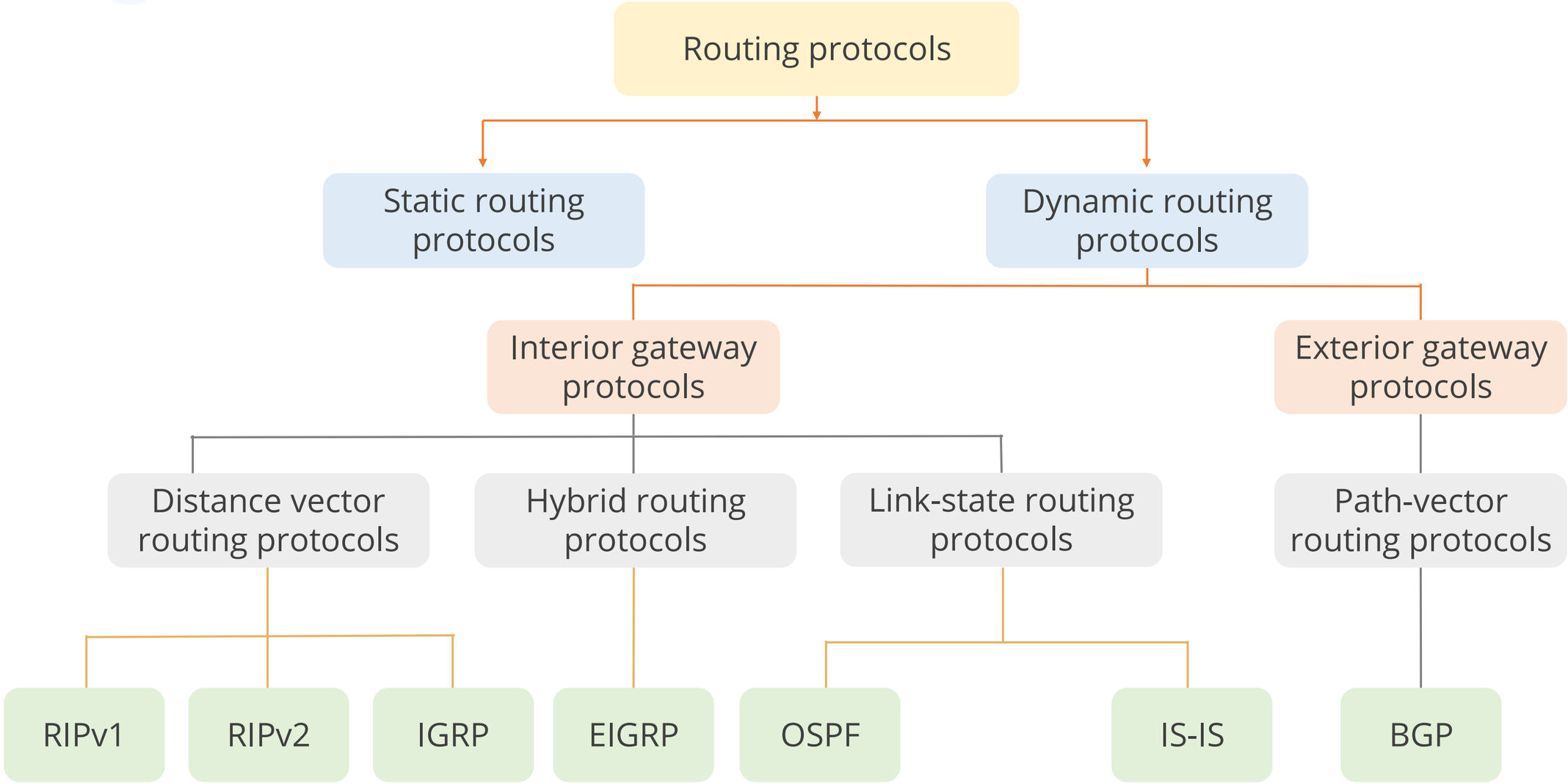
Routers

These are network traffic management devices used to connect different network segments together.

- They work at the network layer of the OSI model, routing traffic using network addresses and routing protocols for optimal paths.
- They examine each packet, check the destination address, and use algorithms and tables to decide where to send the packet next.



Hierarchy of Routing Protocols

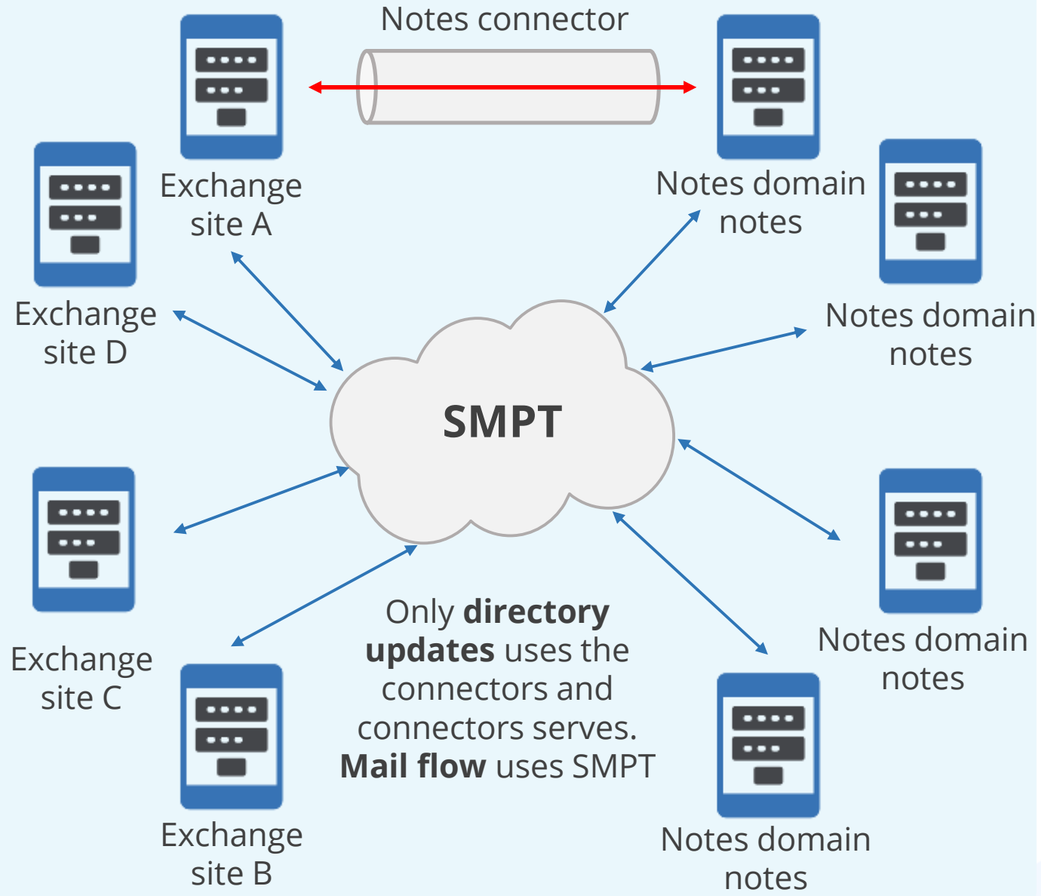


Gateway

- It regulates traffic between two dissimilar networks, while routers regulate traffic between similar networks.
- It performs more complex functions than the router.
- It is needed when one environment uses a protocol that the other does not understand, requiring translation between different communication standards.

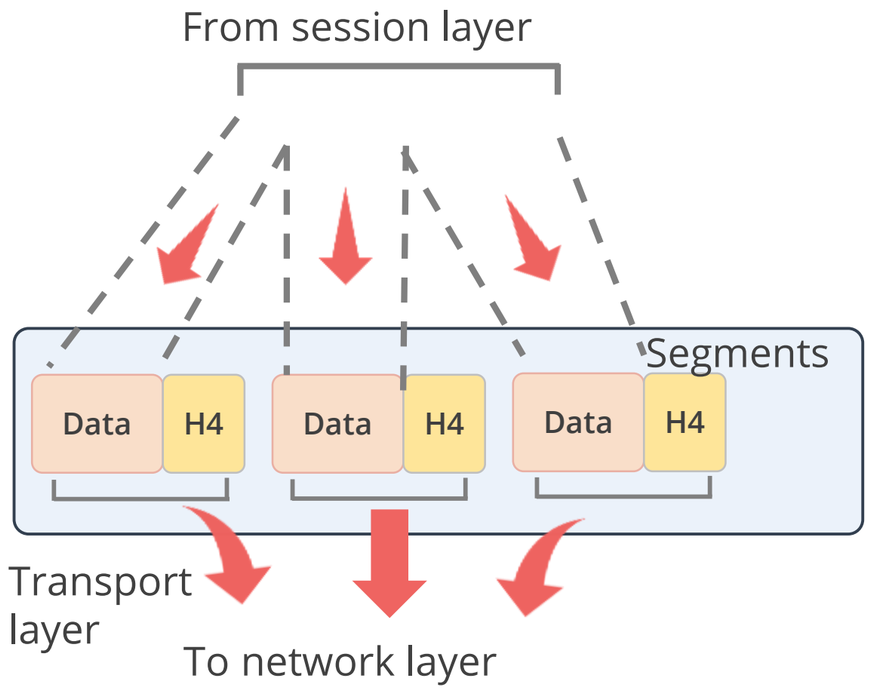
Examples

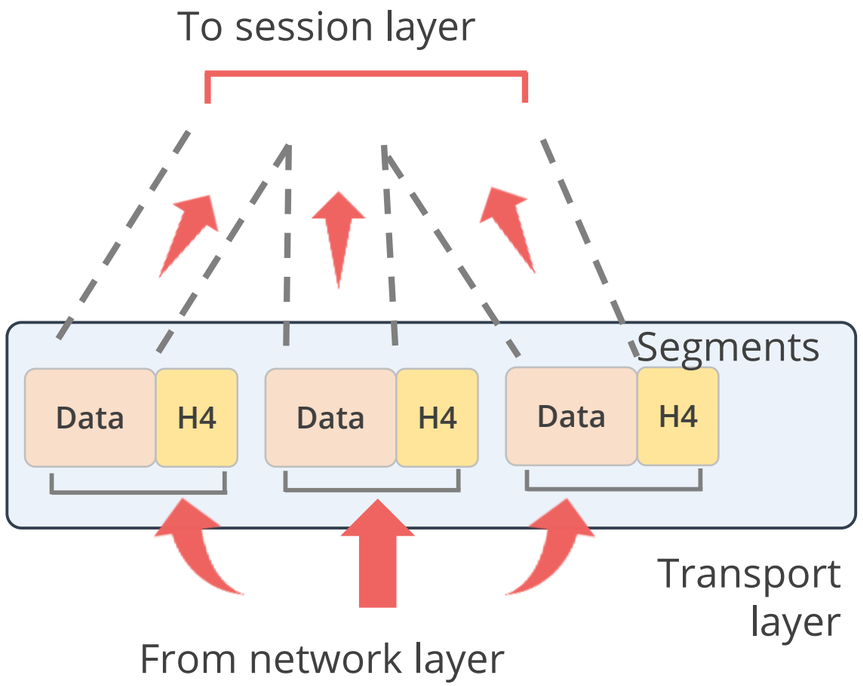
Connect voice and data network and connect IPX with IP network



OSI Model: Transport Layer

It defines how to address the physical locations and devices on the network, how to make connections between nodes, and how to handle the networking of messages.





OSI Model: Transport Layer

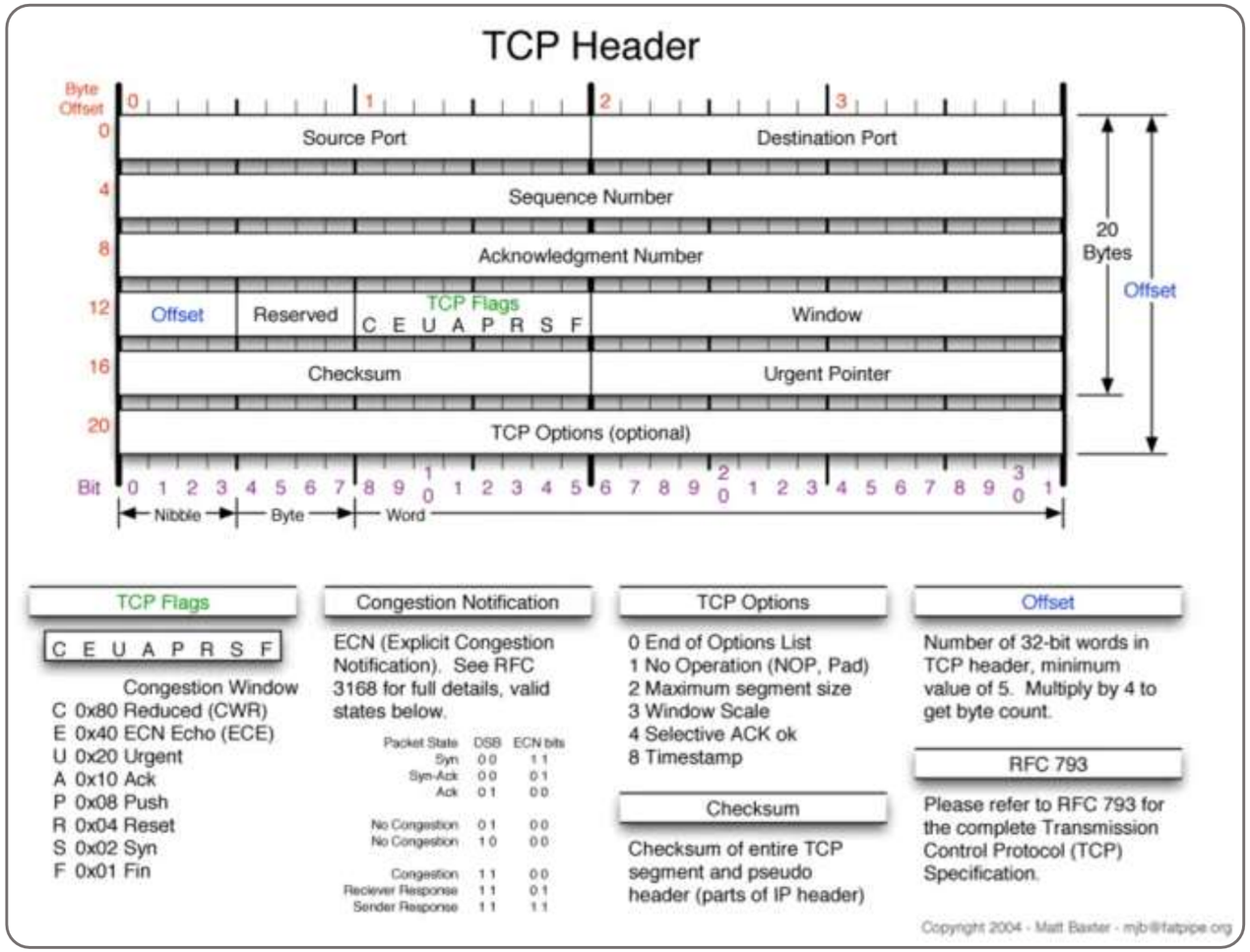
- It establishes a logical connection between the sending and destination hosts on a network.
- It ensures that data units are delivered free of errors and in the correct sequence.
- It prevents loss or duplication of data units.
- It provides either connectionless or connection-oriented service.
- It offers mechanisms for multiplexing upper-layer applications, establishing sessions, and tearing down virtual circuits.
- It provides services to the session layer.

Examples

Transmission control protocol (TCP) and User datagram protocol (UDP)

Transmission Control Protocol (TCP)

It provides a full-duplex and reliable connection but is more costly in terms of network overhead and slower than UDP.



Transmission Control Protocol (TCP): Goals

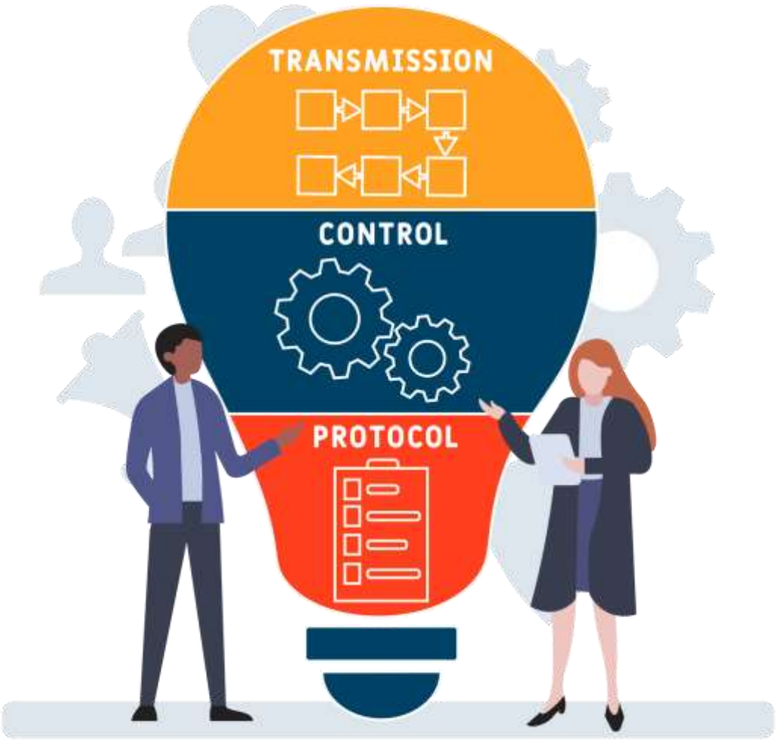
It ensures reliable data transport by performing the following:

- Sending back an acknowledgment to the sender
- Retransmitting any unacknowledged segments
- Sequencing the segments back to their proper order
- Maintaining a manageable data flow

Port types are reserved for well-known ports (0 to 1023), registered ports (1024 to 49151), and dynamic ports (49152 to 65535).

Examples

HTTP, FTP, and Telnet



TCP Handshake Process

A TCP three-way handshake is used to create a connection between a local host or client and server.

Send SYN

SYN

SEQ=100, CTL = SYN

SYN received

SYN received

SYN/ACK

SEQ=300, ACK=101, CTL = SYN, ACK

Send SYN, ACK

Established

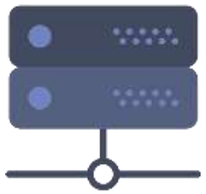
ACK

SEQ=101, ACK=301, CTL = ACK

Client

Connection established

CTL refers to which control bits in the TCP header are set to 1



Server

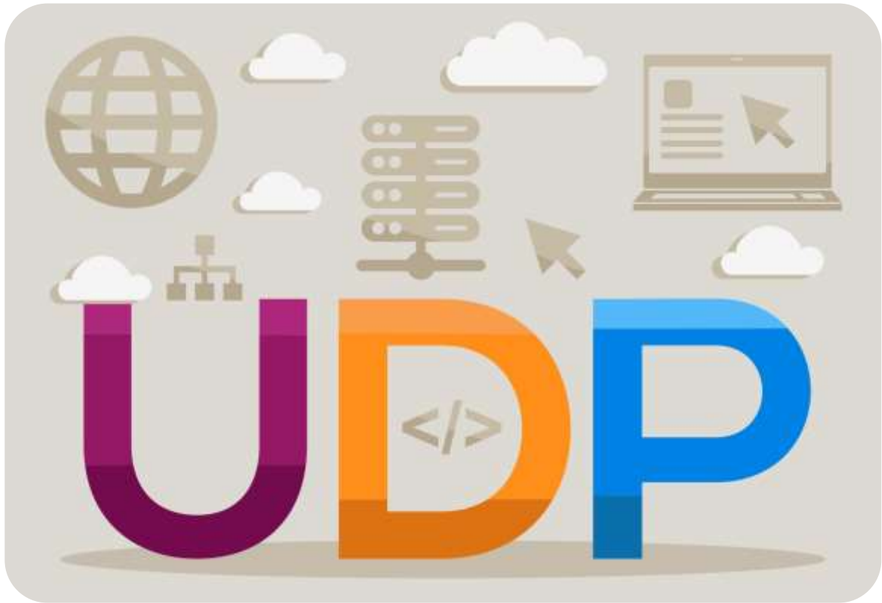
User Datagram Protocol (UDP)

It is like TCP and gives only best-effort delivery.

- It is referred to as an unreliable protocol.
- It is considered a connectionless protocol.

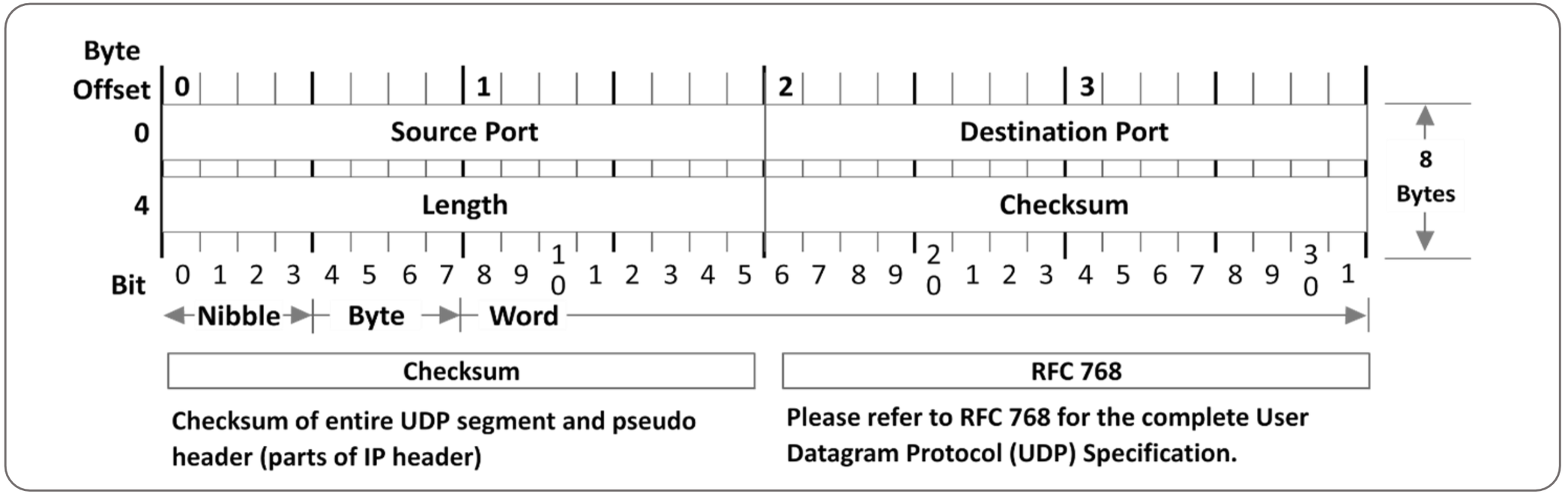
Examples

DNS, TFTP, and VoIP



User Datagram Protocol (UDP)

It is illustrated below:



TCP Flags

These are control bits in the TCP header that provide crucial information about network connection states and play a key role in establishing, managing, and terminating TCP connections.

SYN (Synchronize)

Initiates a connection

ACK (Acknowledge)

Confirms the receipt of data

FIN (Finish)

Indicates the end of the data transmission from one side of the connection

RST (Reset)

Terminates an existing connection abruptly

PUSH (Push)

Requests the immediate delivery of data

URG (Urgent)

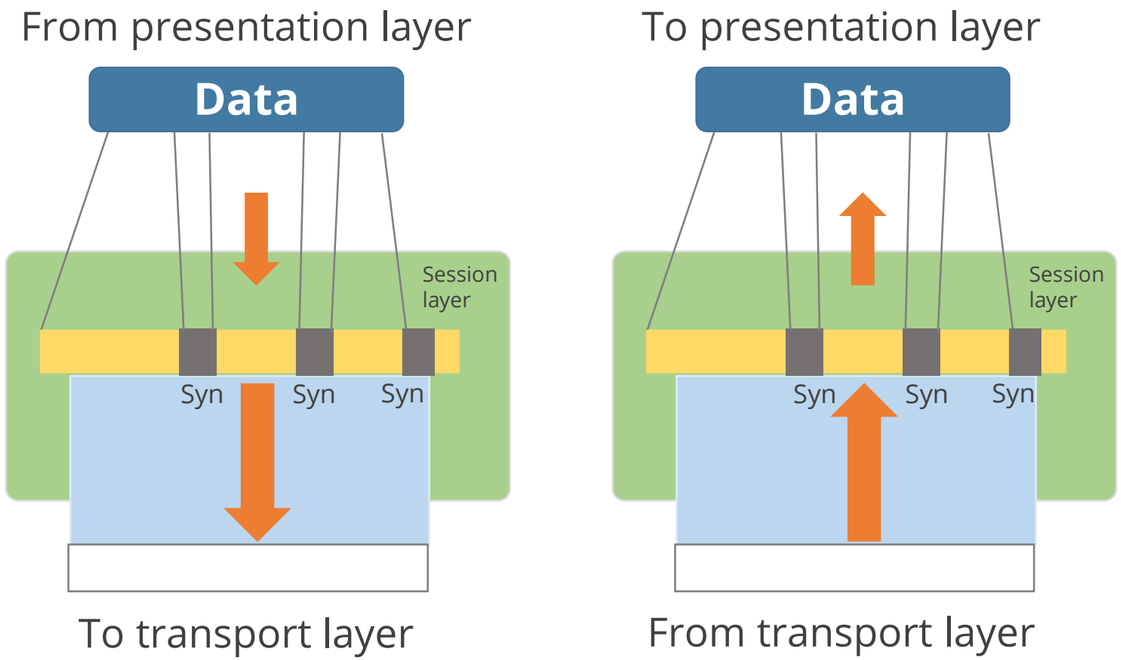
Indicates that urgent data follows in the packet

TCP vs. UDP

	TCP	UDP
Role	Establishes connection between the computers before transmitting data	Sends data directly to the destination computer without checking whether the system is ready to receive or not
Connection	Connection-oriented protocol	Connectionless protocol
Speed	Slow	Fast
Reliability	Highly reliable	Unreliable
Header size	20 bytes	8 bytes
Acknowledgement	Takes acknowledgment of data and can retransmit the user requests	Neither takes acknowledgement nor retransmits the lost data

OSI Model: Session Layer

It makes the initial contact with other computers and sets up the lines of communication.



It offers three different modes:

- Simplex
- Half duplex
- Full duplex

OSI Model: Session Layer

This layer splits up a communication session into three different phases:

- Connection establishment
- Data transfer
- Connection release

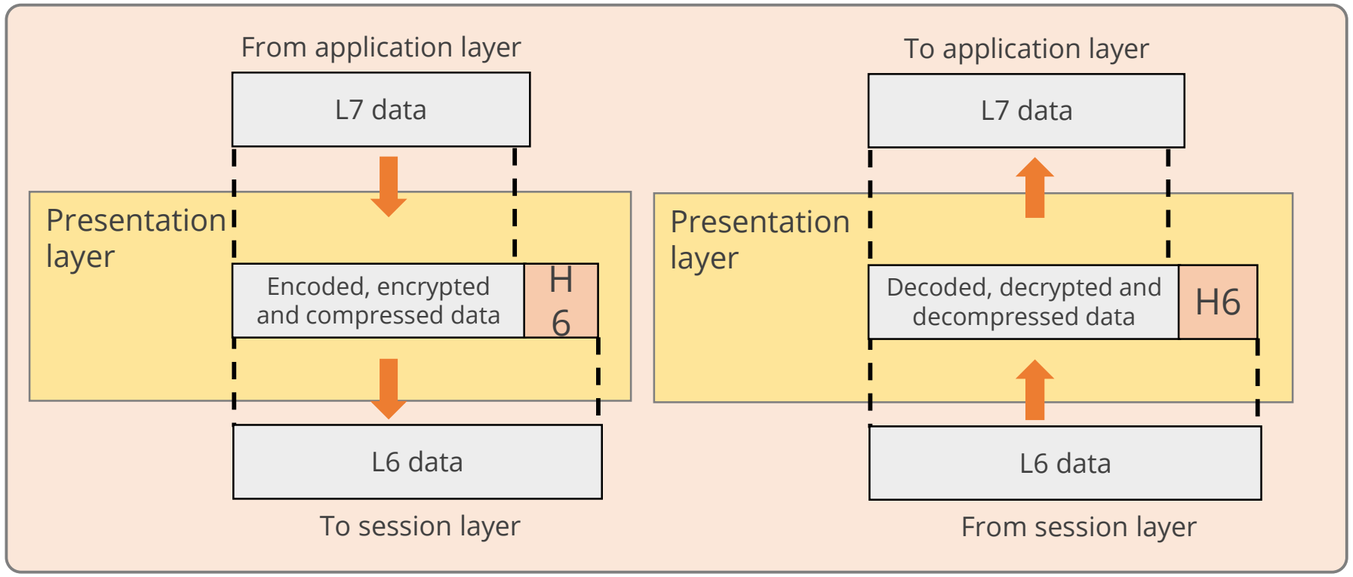
Examples

NFS, SQL, and RPC

It provides services to the presentation layer.

OSI Model: Presentation Layer

It is responsible for defining how information is presented to the user in the interface (application layer) that they are using.



- It presents data and provides services to the application layer.
- It provides a common means of representing data.
- It acts as a translator and no protocols work in this layer.
- It is not concerned with the meaning of the data but with the syntax and format of the data.

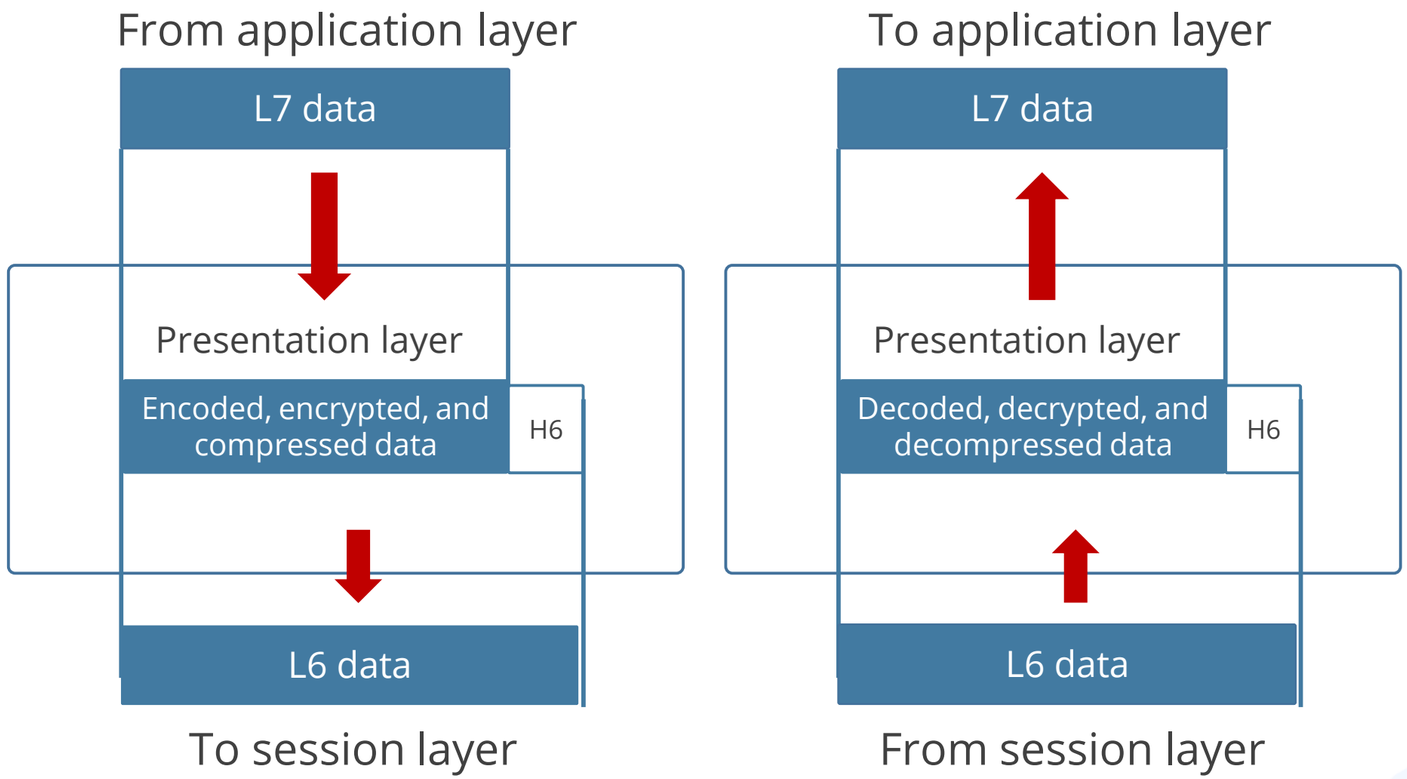
Examples

ASCII, BMP, GIF, JPEG, WAV, AVI, and MPEG

OSI Model: Presentation Layer

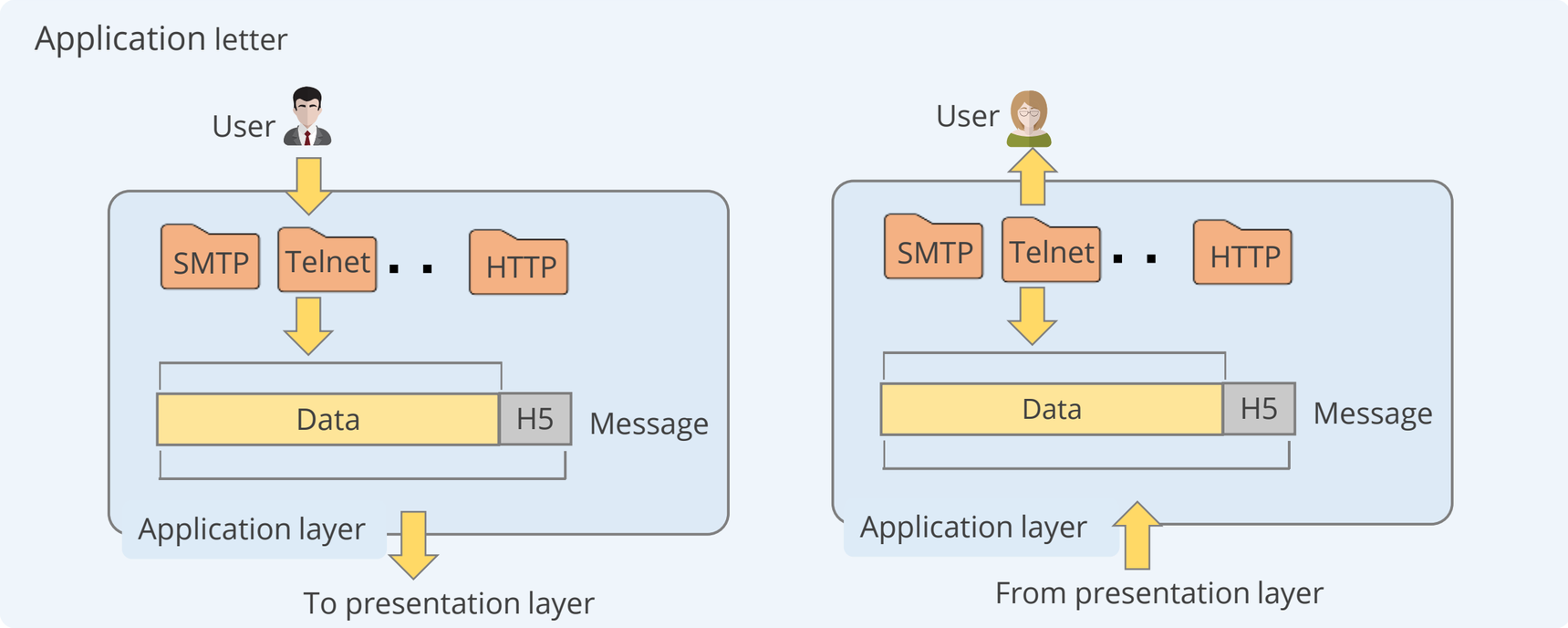
Its functions are:

- Protocol conversion
- Data translation
- Compression
- Encryption
- Character set conversion



OSI Model: Application Layer

It supports the components responsible for the communication aspects of an application.



- It presents data in a visual form that users can understand, rather than as binary zeros and ones.
- It encompasses protocols that support applications but does not include the applications themselves.
- It handles the proper processing and formatting of data before it moves to the layer below.

OSI Model: Application Layer

- It interfaces with the operating system and other applications.
- It communicates data between files, messages, and other network activities.
- It handles file transfer, virtual terminals, network management, and fulfilling network requests of applications.

Examples

Telnet, FTP, web browsers, email, and DNS

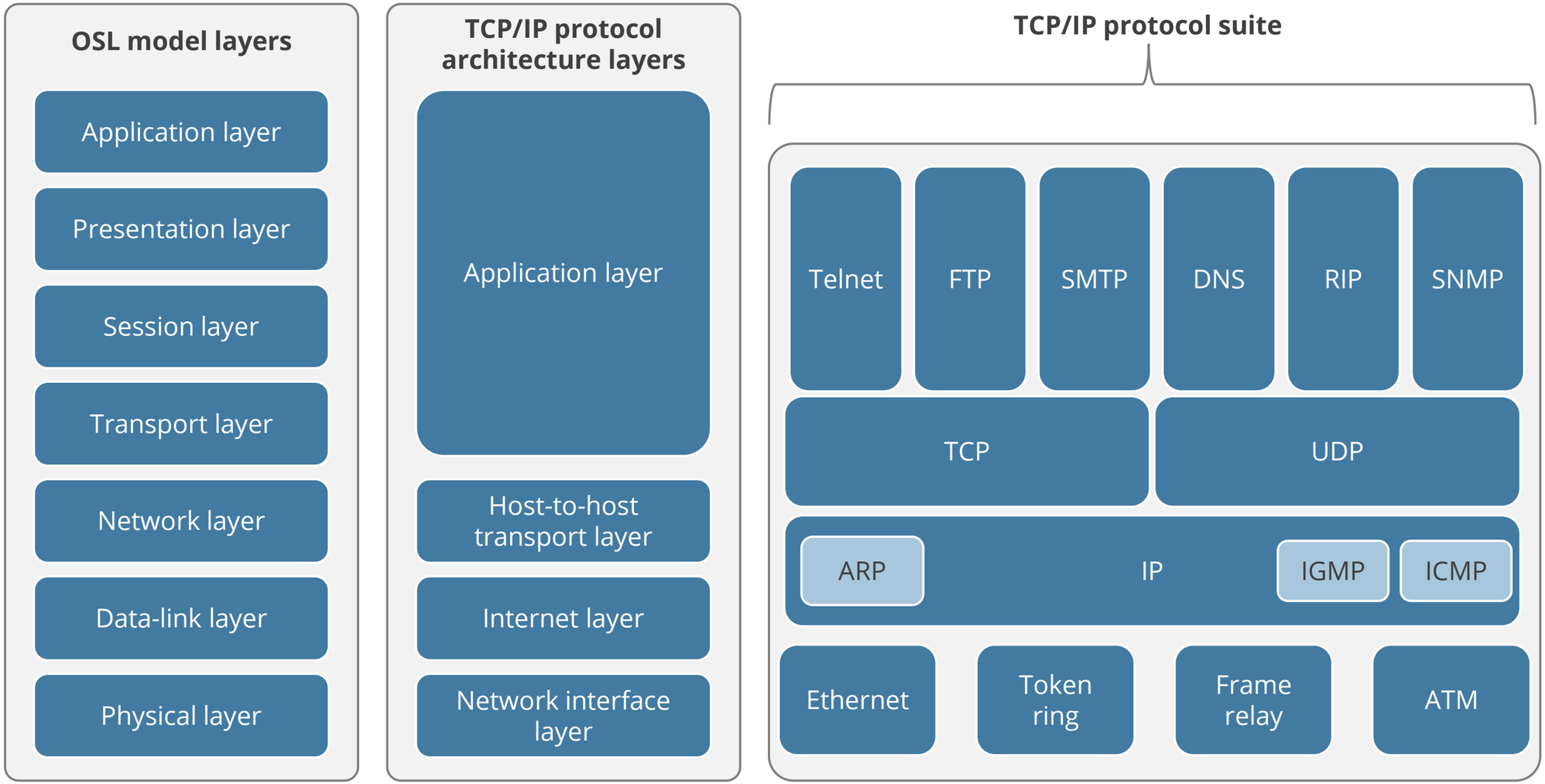
Transmission Control Protocol or Internet Protocol (TCP/IP) Model

TCP/IP is the common name for the suite of protocols originally developed by the Department of Defense (DOD). The following are its layers:

Application	Represents data to the user along with encoding and dialog control
Host-to-host	Supports communication between diverse devices across diverse networks
Internet	Determines the best path through the network
Network access	Controls the hardware devices and media that make up the network

Comparison of OSI and TCP/IP Models

This model is very similar to the OSI model, however with fewer layers.



Implications of Multi-Layer Protocols

TCP/IP protocol suite consists of various layers with many individual protocols.

The following are the benefits and limitations of multi-layer protocols:

Advantages

- Encryption can be incorporated on various layers.
- Higher layers support wide range of protocols.

Disadvantages

- Filters can be evaded.
- Unauthorized access to the system can happen due to covert channels.

Quick Check

During a network troubleshooting session, a technician needs to resolve IP addresses to MAC addresses to ensure proper data packet delivery. At which layer of the OSI model are ARP and RARP functioning to facilitate this process?

A. Physical layer

B. Data link layer

C. Network layer

D. Transport layer

IP Addressing

Introduction to IP Address

It is a logical and numerical identifier assigned to each host on the internet, allowing for unique identification and communication between devices.

- Each data packet is assigned an IP address of the sender and the recipient.
- Each device receives the packet and makes routing decisions based on the packet’s destination IP address.
- It provides an unreliable datagram service.
- It includes both network and host.

IP Address

IP Address: Types

There are two versions of IP in use, IP version 4 (IPv4) and IP version 6 (IPv6).

IPv4

- Its space is 32-bit.
- It provides best-effort packet delivery.
- The network addresses are expressed as a dot-decimal.

Example

192.168.0.100

IPv6

- Its space is 128-bit.
- This space provides the potential for a maximum of 2128, or about 3.403×1038 addresses.
- It is represented as eight groups of four hexadecimal digits separated by colons.

Example

FE80:0000:0000:0000:0202:B3FF:FE1E:8329

Classful IP Addressing

The entire available IP address space is divided into two parts:

- **The network number**: The first eight bits of an IP address
- **The host address**: The remaining 24 bits of an IP address

Class	Subnet mask	Network bit field	Host bit field	Number of networks	Hosts per network	Start address	End address	CIDR notation
Class A	255.0.0.0	8	24	128	16 million	0.0.0.0	127.255.255.255	/8
Class B	255.255.0.0	16	6	16,000	65,000	128.0.0.0	191.255.255.255	/16
Class C	255.255.255.0	24	8	Two million	254	192.0.0.0	223.255.255.255	/24
Class D	Reserved for multicast group					224.0.0.0	239.255.255.255	
Class E	Reserved for future use, research, or development purpose					240.0.0.0	255.255.255.255	

Class A

It has an 8-bit network address and a 24-bit host address.

- Its IP ranges from 1.0.0.0 to 126.255.255.255.
- It has an implied netmask of 255.0.0.0, allowing for 126 networks to be created.
- Each network can contain up to 16,777,214 nodes.

Class	Subnet mask	Number of networks	Hosts per network	Start address	End address
Class A	**255.0.0.0**	**128**	**16 million**	**0.0.0.0**	**127.255.255.255**
Class B	255.255.0.0	16,000	65,000	128.0.0.0	191.255.255.255
Class C	255.255.255.0	Two million	254	192.0.0.0	223.255.255.255
Class D	Reserved for multicast group			224.0.0.0	239.255.255.255
Class E	Reserved for future use, research, or developmental purposes			240.0.0.0	255.255.255.255

Class B

It has a 16-bit network address and a 16-bit host address.

- Its IP ranges from 128.0.0.0 to 191.255.255.255.
- It has an implied netmask of 255.255.0.0, allowing for 16,382 networks to be created.
- Each network can contain up to 65,534 nodes.

Class	Subnet mask	Number of networks	Hosts per network	Start address	End address
Class A	255.0.0.0	128	16 million	0.0.0.0	127.255.255.255
Class B	**255.255.0.0**	**16,000**	**65,000**	**128.0.0.0**	**191.255.255.255**
Class C	255.255.255.0	Two million	254	192.0.0.0	223.255.255.255
Class D	Reserved for multicast group			224.0.0.0	239.255.255.255
Class E	Reserved for future use, research, or developmental purposes			240.0.0.0	255.255.255.255

Class C

It has a 24-bit network address and an 8-bit host address.

- Its IP ranges from 192.0.0.0 to 223.255.255.255.
- It has an implied netmask of 255.255.255.0, allowing for over two million networks to be created.
- Each network can contain up to 254 nodes.

Class	Subnet mask	Number of networks	Hosts per network	Start address	End address
Class A	255.0.0.0	128	16 million	0.0.0.0	127.255.255.255
Class B	255.255.0.0	16,000	65,000	128.0.0.0	191.255.255.255
Class C	**255.255.255.0**	**Two million**	**254**	**192.0.0.0**	**223.255.255.255**
Class D	Reserved for multicast group			224.0.0.0	239.255.255.255
Class E	Reserved for future use, research, or developmental purposes			240.0.0.0	255.255.255.255

Class D and Class E

Class D is reserved for multicast.

- IP ranges from 224.0.0.0 to 239.255.255.255

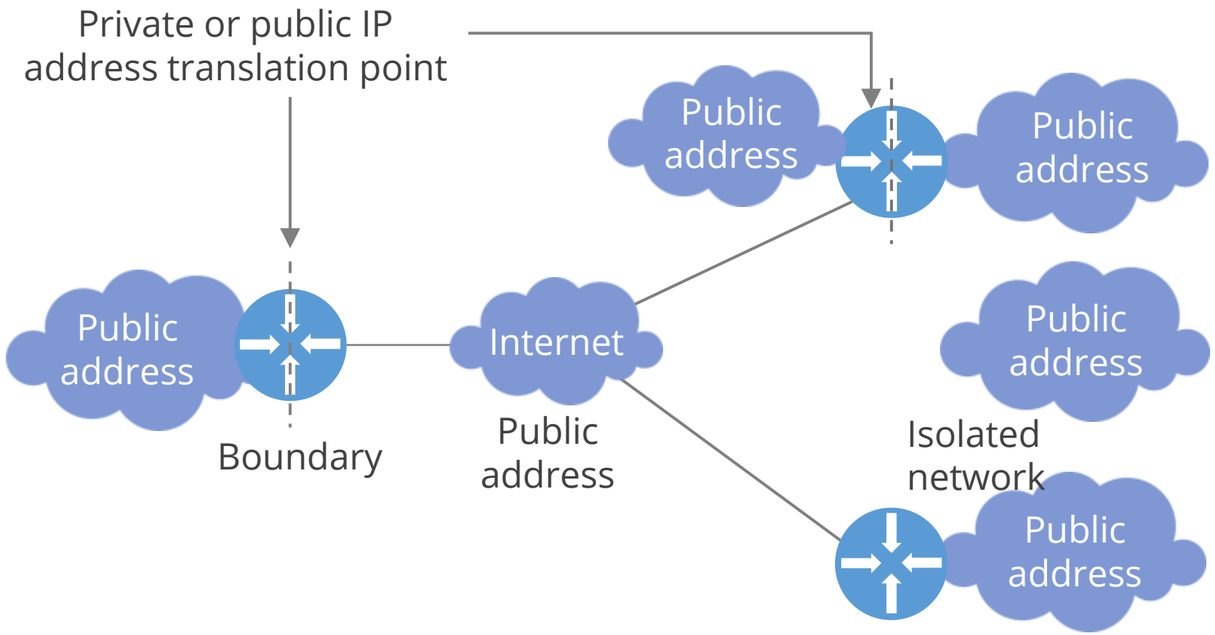
Class E is reserved for research purposes.

- IP ranges from 240.0.0.0 to 255.255.255.255

Class	Subnet mask	Number of networks	Hosts per network	Start address	End address
Class A	255.0.0.0	128	16 million	0.0.0.0	127.255.255.255
Class B	255.255.0.0	16,000	65,000	128.0.0.0	191.255.255.255
Class C	255.255.255.0	Two million	254	192.0.0.0	223.255.255.255
Class D	**Reserved for multicast group**			**224.0.0.0**	**239.255.255.255**
Class E	**Reserved for future use, research, or developmental purposes**			**240.0.0.0**	**255.255.255.255**

Private Networks

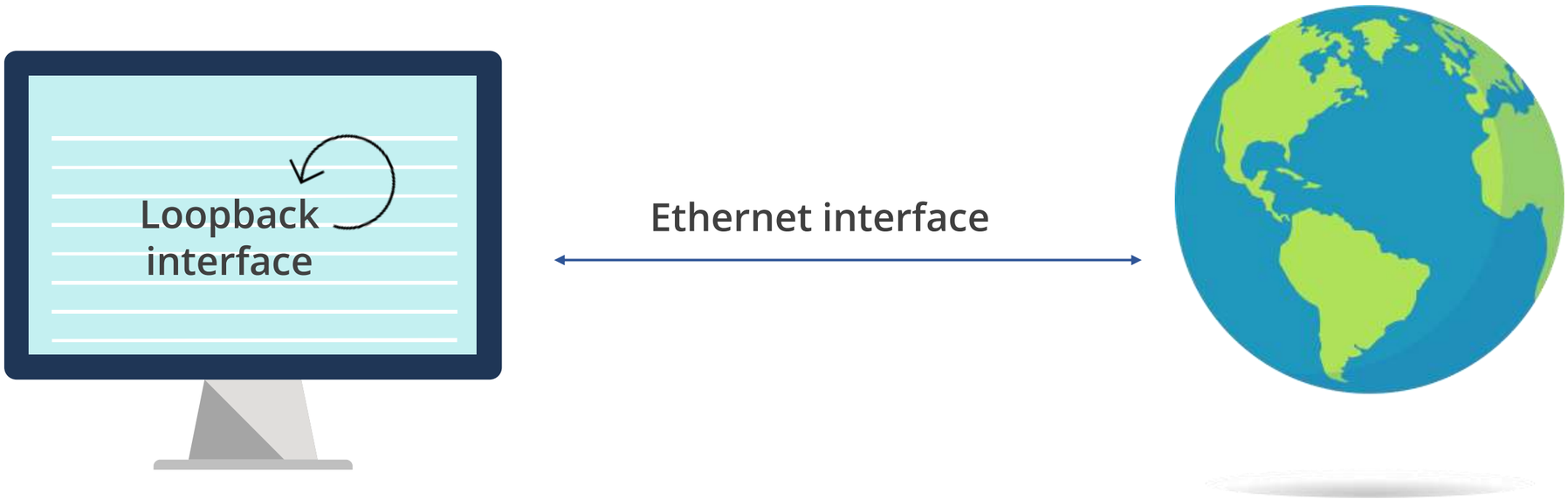
They are not available for general use and allow access to a guest machine by an address that is not publicly accessible.



- Organizations are encouraged to assign private network IP addresses to nodes in their internal networks.
- The address blocks reserved for them are:
  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255

Loopback Address

It is a special address that signifies a node's own address.

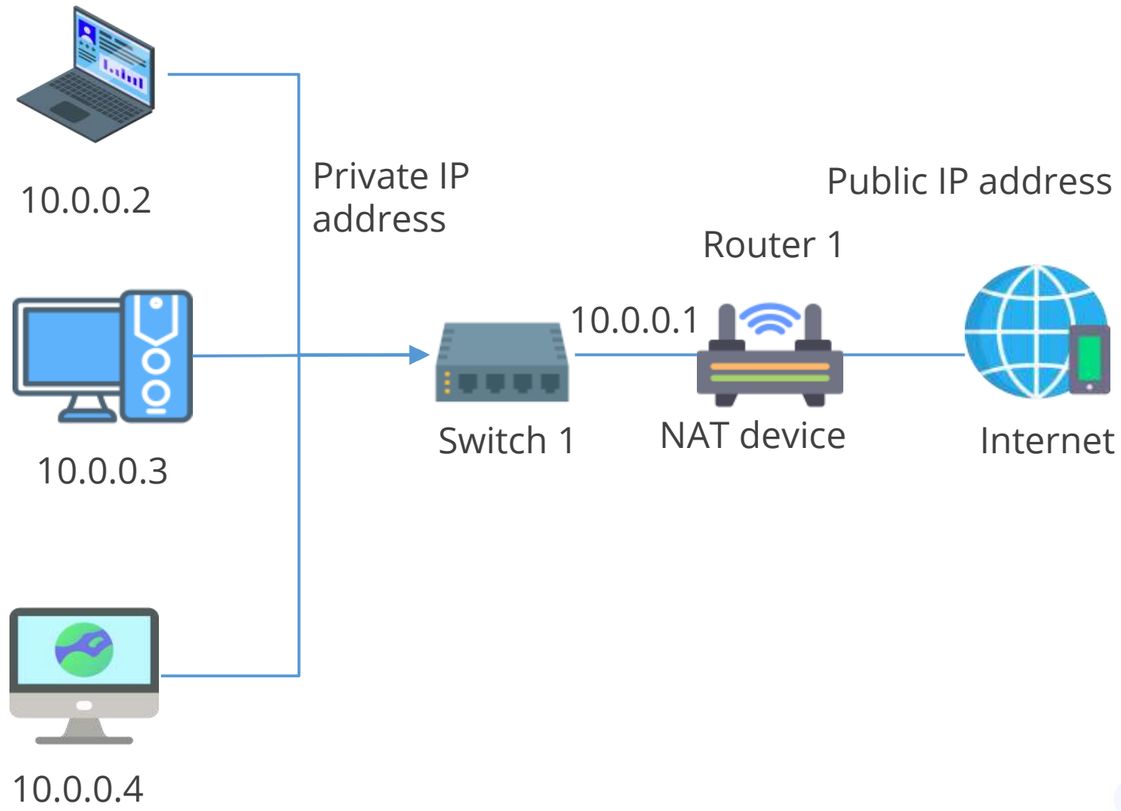


Loopback address 127.0.0.1 points back to the issuing computer.

Network Address Translations

It is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

It enables private IP networks that use unregistered IP addresses to connect to the internet.

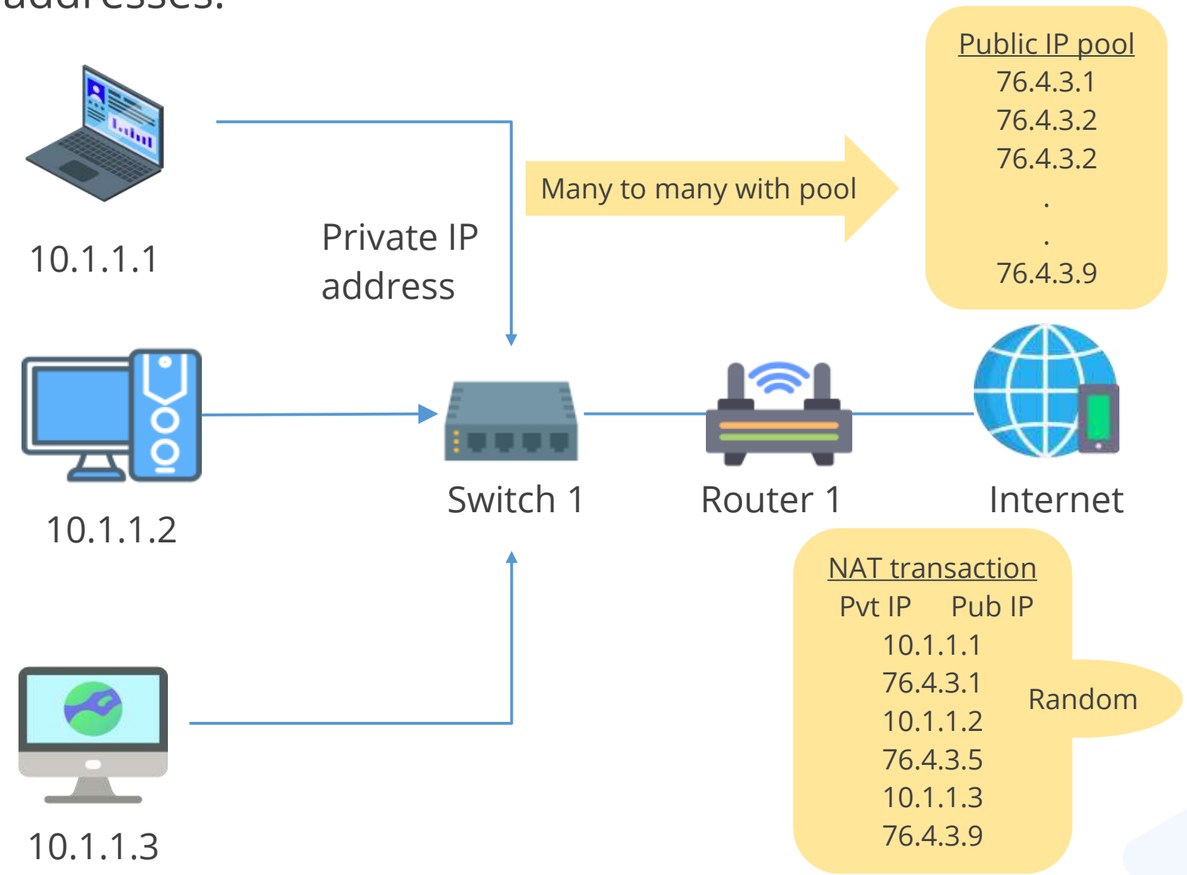


One internet-routable IP address of a NAT gateway can be used for an entire private network.

Dynamic NAT

This technique maps an internal, private IP address to a public IP address selected from a pool of registered public IP addresses.

- It is used in outbound connection.
- It is often used when translating addresses for end-user workstations.
- It keeps track of internal or external address mappings.

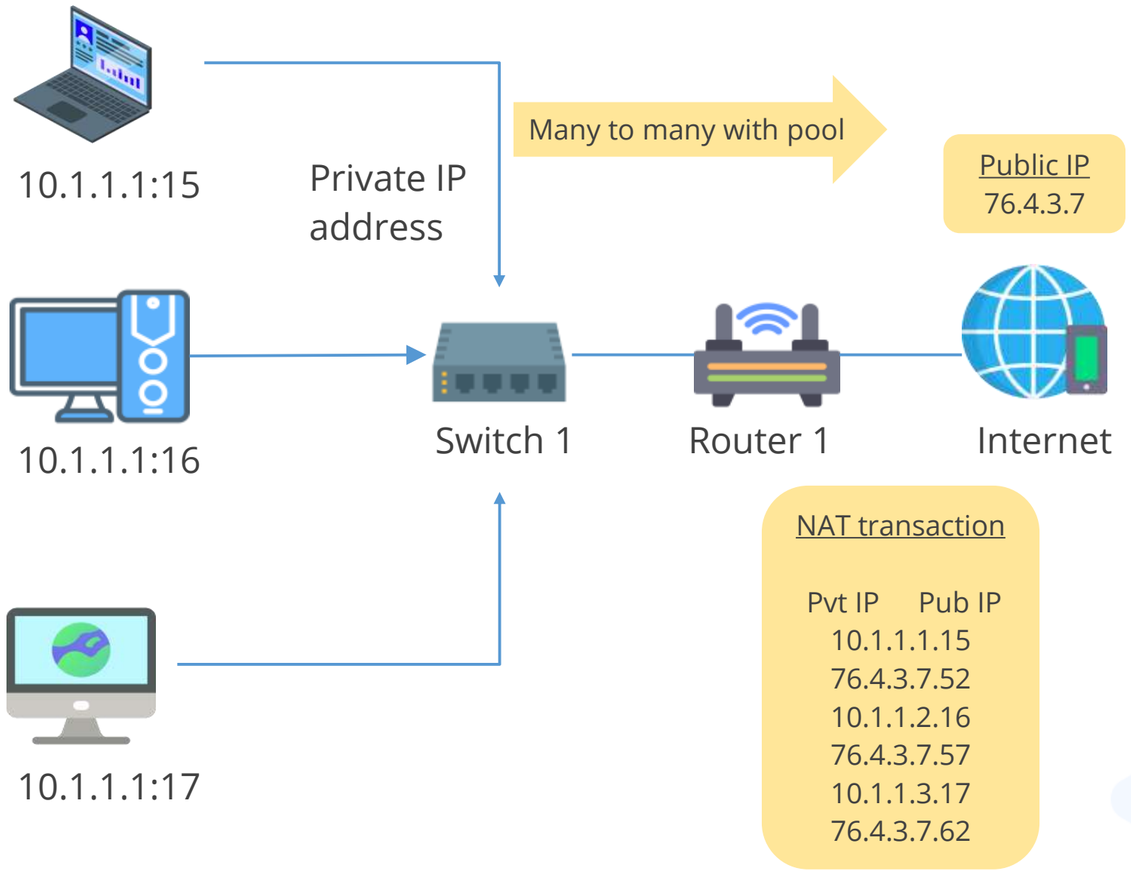


Dynamic Port Address Translation (PAT)

This technique allows many different internal and private addresses to share a single external IP address.

It is used in outbound connections.

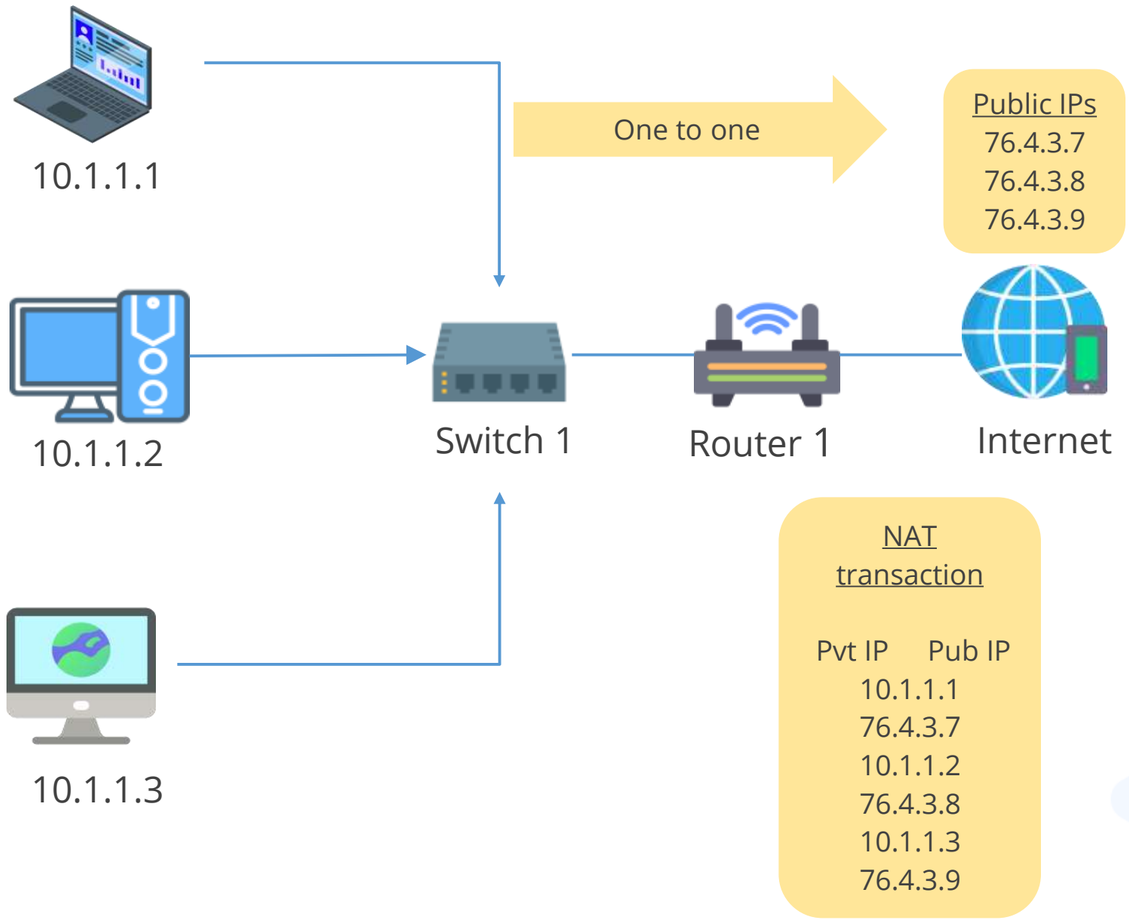
The devices performing PAT replace the source IP address with the NAT IP address and substitute the source port field with a port from an available connection pool.



Static NAT

This technique maps an internal, private address to an external, public address and the same public address is consistently used for that private address.

- It is used in inbound connections.
- It is often employed when hosting services that the public needs to access, such as a web server, behind a firewall.



Hexadecimal Format

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

IPv6 Address Structure

It is made of 128-bits divided into eight 16-bit blocks where each block is then converted into four-digit hexadecimal numbers separated by colons.

Binary representation:
0010000000000001 0000000000000000
0011001000111000 1101111111100001
0000000001100011 0000000000000000
0000000000000000 1111111011111011

Hexadecimal equivalent:
2001:0000:3238:DFE1:0063:0000:0000:FEFB.

Even after converting into the hexadecimal format, the address remains long.

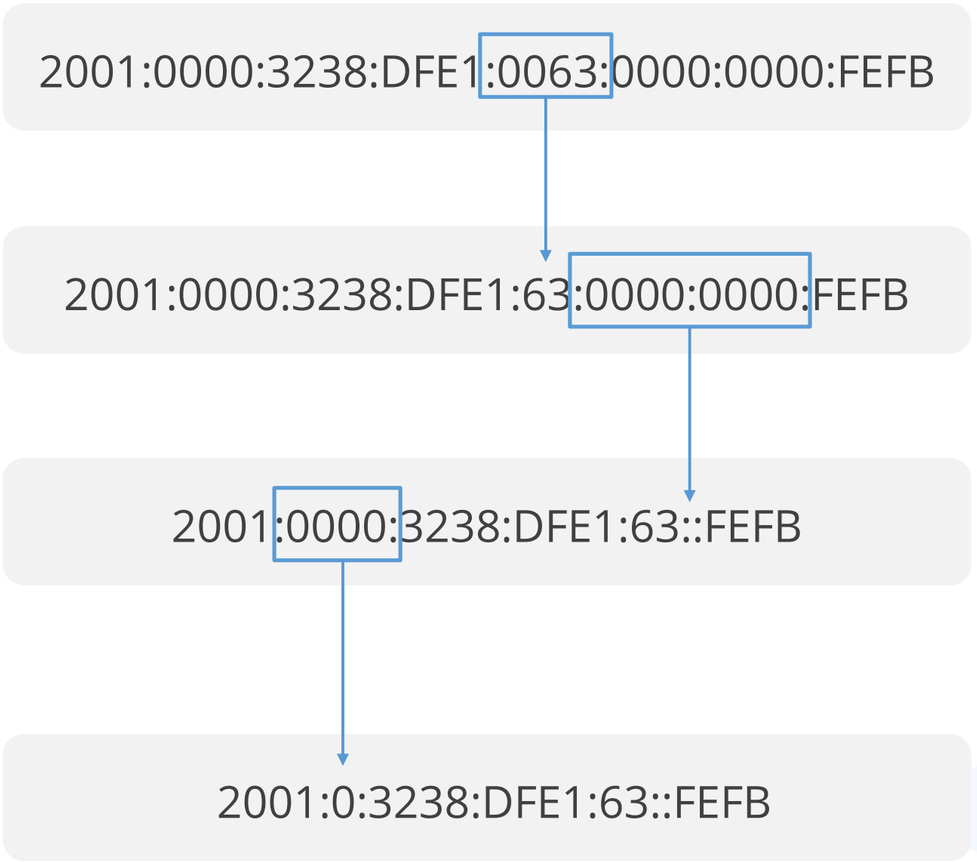
IPv6 Address Structure

There are some rules to be followed to shorten the address:

Rule 1: Discard leading zero(s)
In block 5, 0063, the leading two zeros can be omitted.

Rule 2:

- If two or more blocks contain consecutive zeros, omit them all and replace them with a double colon sign (::).
- Consecutive blocks of zeros can be replaced by :: only once.
- If there are still blocks of zeros in the address, they can be shrunk down to a single zero.



IPv6 Address Terminology: Prefix and Prefix Length

Prefix

- It is the network portion of an IPv6 address.
- In an IPv4 address, this is sometimes called the network portion of the address, or the network prefix.

IPv6

Prefix length

- It is the number of the most significant or leftmost bits that define the prefix.
- This is equivalent to the subnet mask in IPv4.
- IPv6 addresses are 128 bits, so the prefix length can be /0 to /128.

IPv6 Address Terminologies: Interface ID

- It is equivalent to the host portion of an IPv4 address.
- IPv6 uses this term because any type of device can have an IP address, not just a host computer.
- A device with an IPv6 interface may range anywhere from a common server or client computer to an espresso machine or a biomedical sensor.
- The term interface is used because an IP address (IPv4 or IPv6) is assigned to an interface, and a device may have multiple interfaces.

IPv6 Address Terminologies: Node or Device

It refers to any entity that can have an IPv6 address, including traditional devices like computers and printers, as well as other types such as webcams, embedded devices, and Internet of Things (IoT) devices.

IPv6 Address Types

Global unicast address (GUA)

- It is a globally unique and routable IPv6 address.
- It is equivalent to a public IPv4 address.
- It begins with either a hexadecimal 2 or 3.
- It can be either a source or destination IPv6 address.

Example

2001:db8:cafe:1::100

Link-local unicast address (LLA)

- It is a unicast address that is local only on that link. The term link refers to a logical network segment or a subnet.
- It is not routable beyond the local subnet.
- It is created automatically by the host operating system.
- It can be either source or destination IPv6 addresses.
- It usually begins with fe80.

Example

fe80::a299:9bff:fe18:50d1

6to4 Tunneling Method

It is a system that allows IPv6 packets to be transmitted over an IPv4 network without the need to configure explicit tunnels.

- It serves as a transparent mechanism used as a transport layer between IPv6 nodes.
- It does not facilitate interoperation between IPv4-only hosts and IPv6-only hosts.
- It performs the following three functions:
  - Assigns a block of IPv6 address space to any host or network that has a global IPv4 address
  - Encapsulates IPv6 packets inside IPv4 packets for transmission over an IPv4 network using 6in4
  - Routes traffic between 6to4 and native IPv6 networks

IPv6 vs. IPv4

Feature	IPv6	IPv4
IP address size	It has an IP address size of 128 bits.	It has an IP address size of 32 bits.
Total address range	It has a total range of 340 undecillion possible addresses.	It has a total range of 4.3 billion possible addresses.
Example	2001:db8::ff00:42:8329.	123.45.67.89.
Scalability of multicast routing	The scalability of multicast routing is improved by adding a scope field to the multicast address.	It offers no options for scalability.
Anycast address	An anycast address is used to send a packet to any one node in a group of nodes.	It has no options for anycast.
Extensions for support	It includes extensions to support authentication, data integrity, and confidentiality.	It has no extensions available for support.

Quick Check

Your company is rolling out IPv6 across its global network. They assign Global Unicast Addresses (GUAs) to devices for internet communication. Which of the following is true about GUAs?

A. GUAs are like IPv4 private addresses and not publicly routable.

B. GUAs are publicly routable and need security controls similar to IPv4 public addresses.

C. GUAs automatically encrypt all internet traffic.

D. GUAs must be translated to an IPv4 address using Network Address Translation (NAT) to communicate with other IPv6 hosts.

Implementing Network Security Devices

Network Security Devices

They are tools used to protect a network from unauthorized access or attacks. Some of the key security devices include:

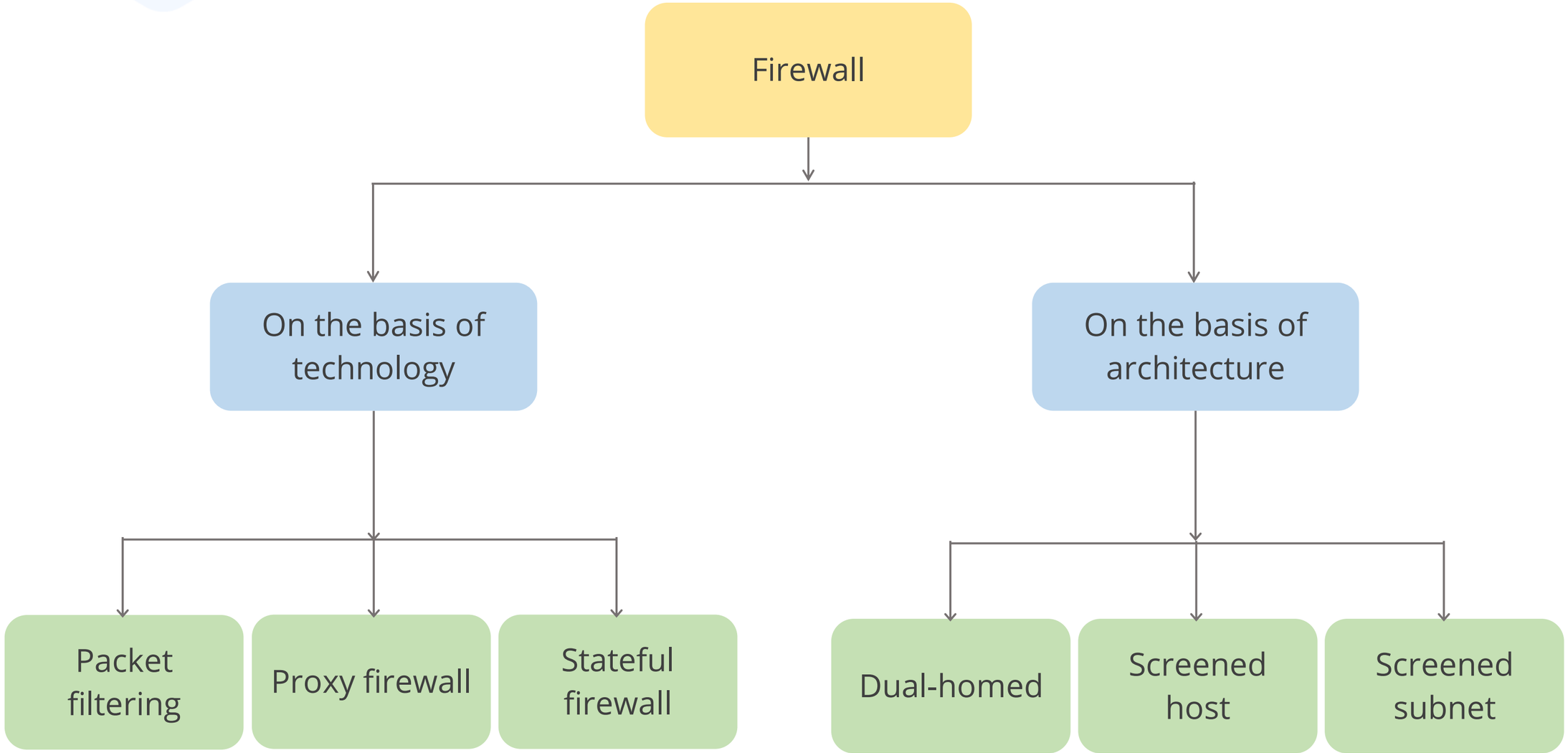
- Firewalls
- Web-application firewall
- Intrusion detection and prevention system
- Proxy server
- Load balancer
- Network access control

Firewall

It can be hardware, software, or a combination of both, and its purpose is to enforce a set of network security policies across network connections.

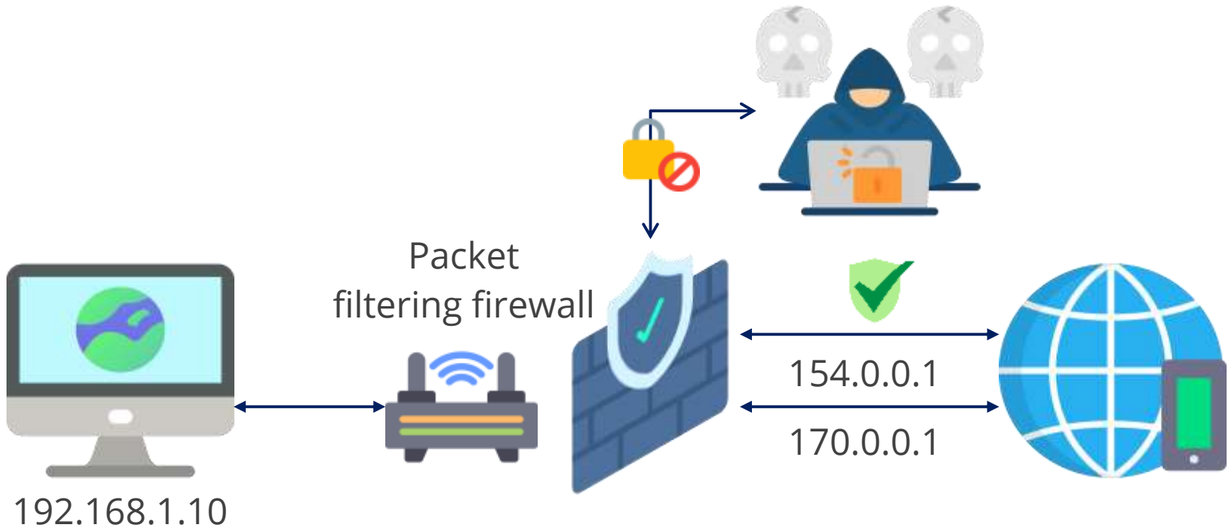
- It is used to restrict access between one network and another.
- It operates from the network layer to the application layer of the OSI model.

Types of Firewall



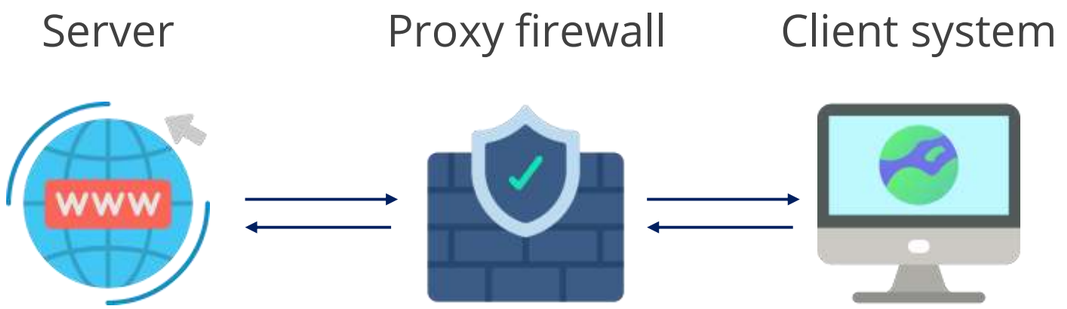
Packet Filtering Firewall

- It operates at the network and the transport layer of the OSI model.
- It is categorized as a stateless firewall.
- It makes decisions based on the source and destination IP addresses, port numbers, protocol type, and direction of traffic.
- It can manage inbound, outbound, or both types of traffic.
- Its operation is based on rule-based access control.



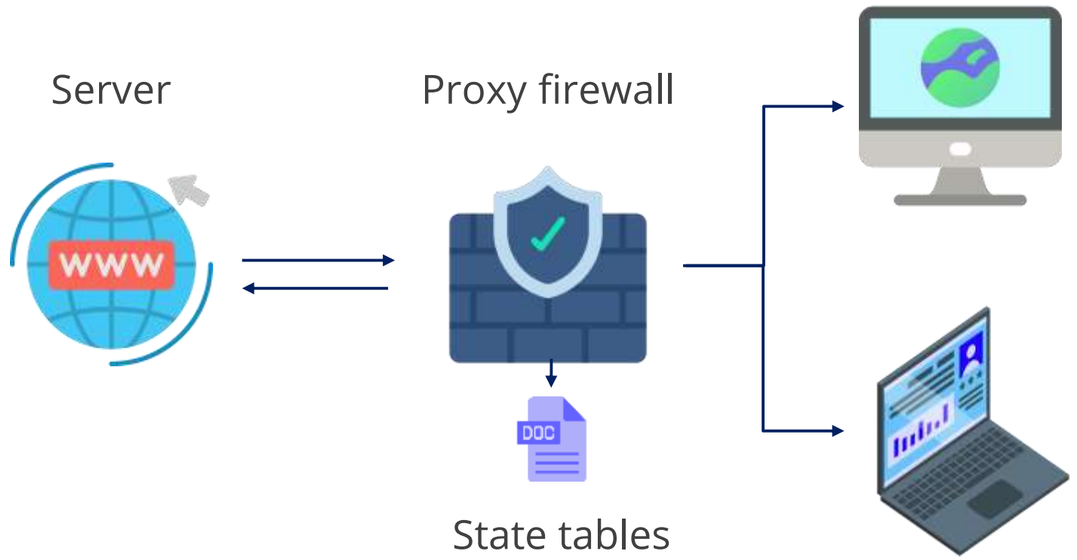
Proxy Firewall

- It intercepts and inspects the packets before it is delivered to the destination.
- It breaks the connection between the peers.
- It works at the application layer.



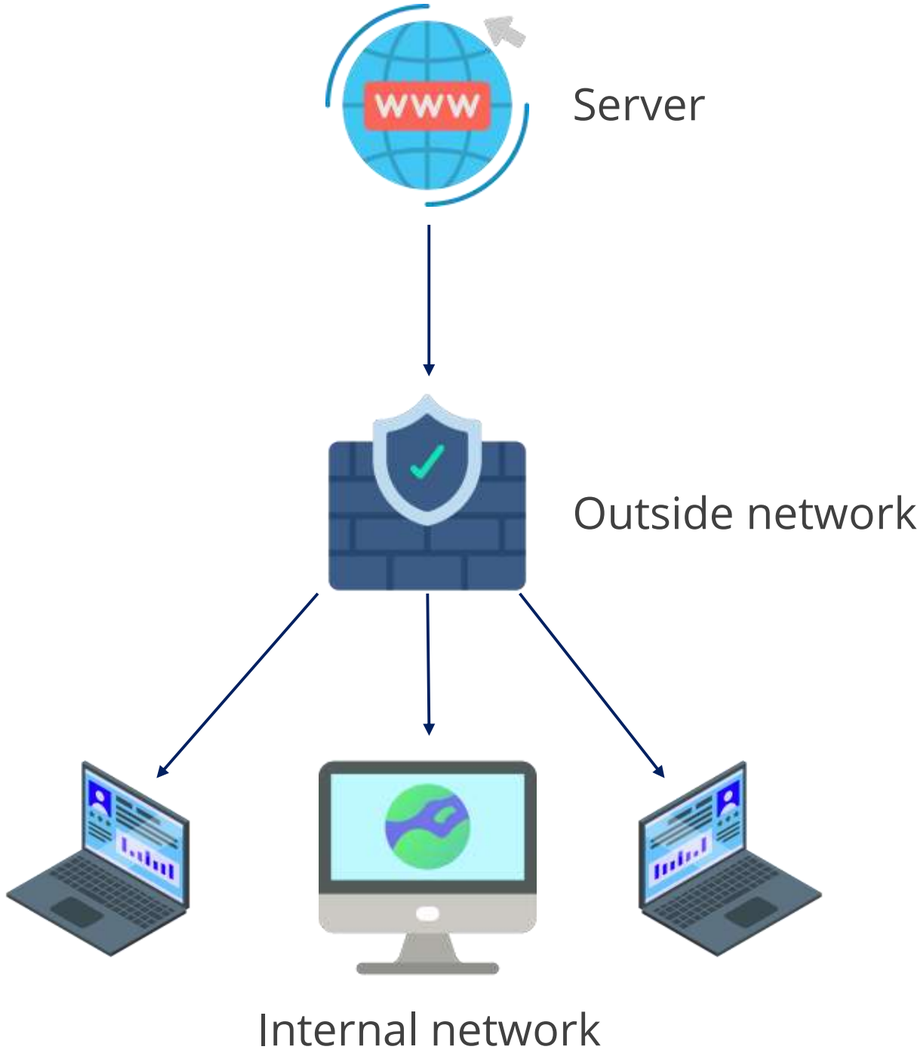
Stateful Firewall

- It limits network-based information on the destination, source address, and state table content.
- It maintains a state table of all connections, deeply inspecting the first packet but not the subsequent connections.
- It provides a high degree of security and does not introduce a performance hit.
- It gives transparency and scalability to the user.



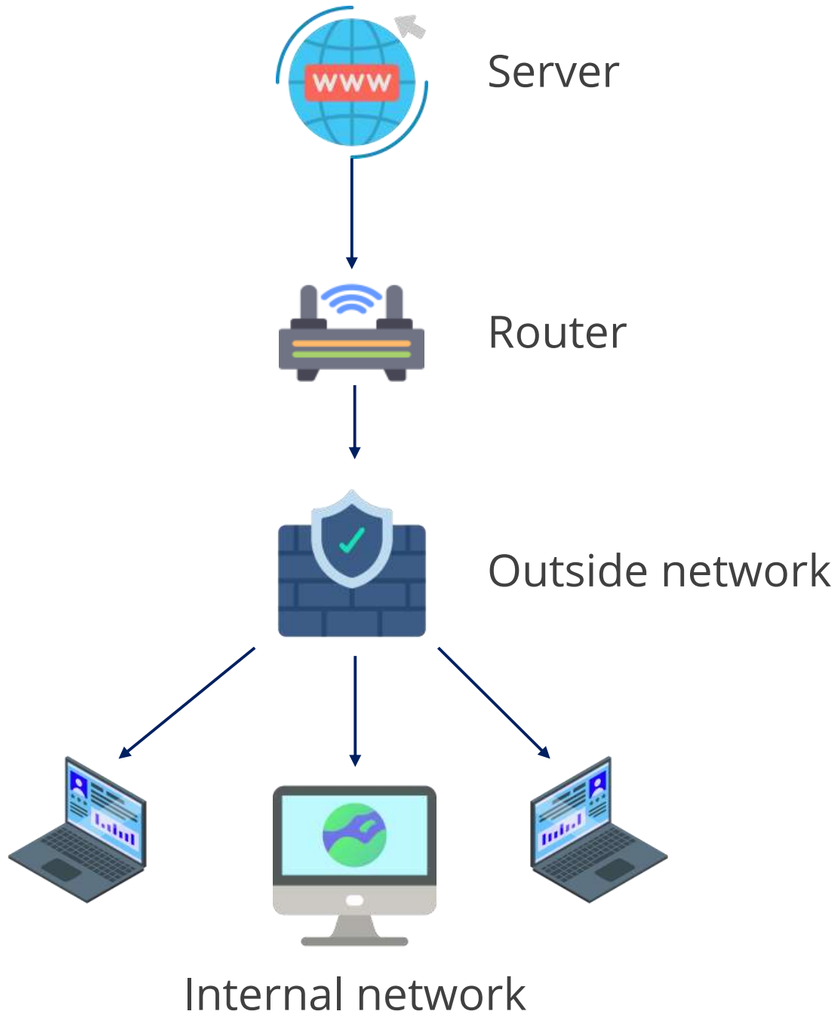
Dual-Homed Firewall

- It has two interfaces, inside and outside.
- A single firewall layer protects the internal network in SOHO (small office , home office or small remote location) environments, allowing direct traffic access.



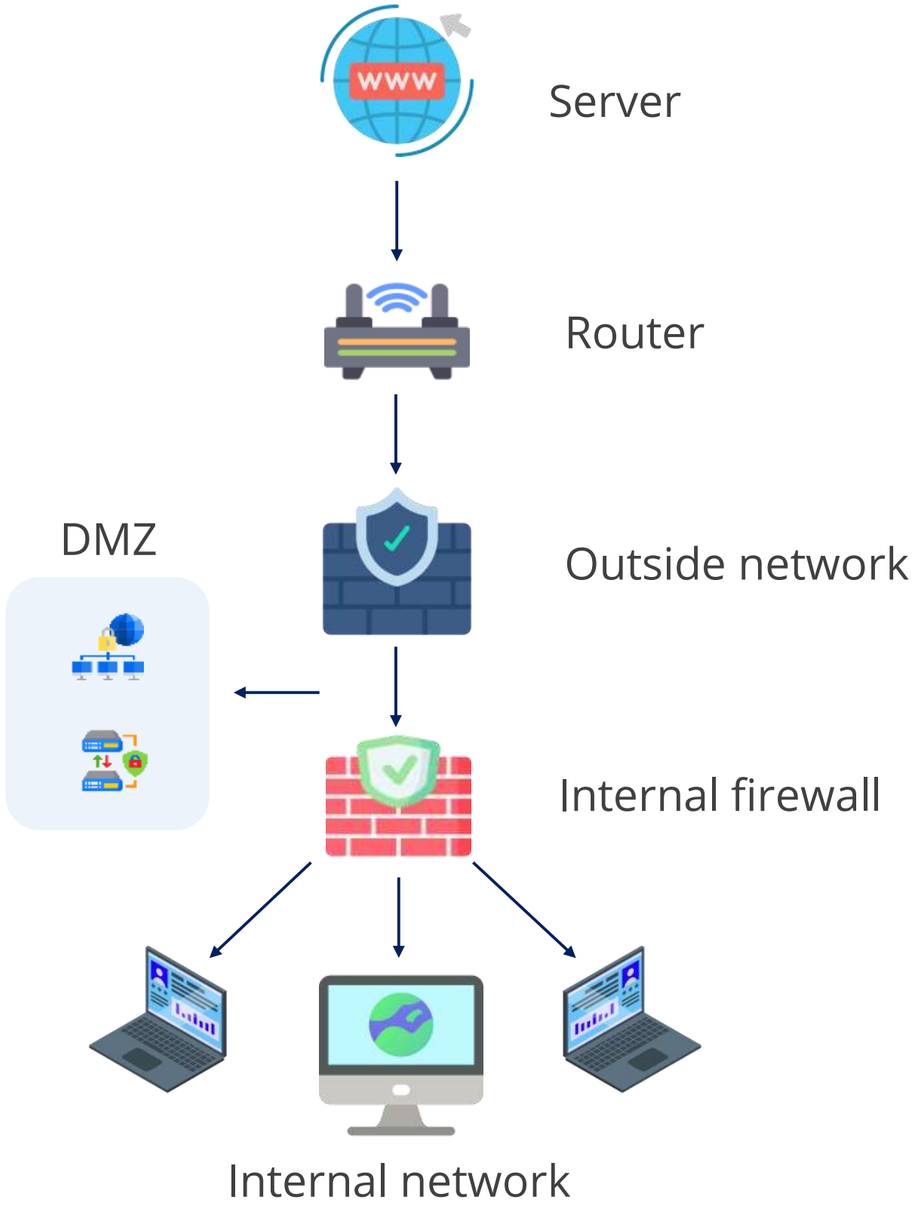
Screened Host Firewall

- A device is connected to the internet router that segregates the internal network.
- The internet router connects only to the firewall, which inspects and forwards traffic to the internal network.
- Internet traffic is initially filtered by the outer router via packet filtering.
- The traffic that makes it past this phase is sent to this firewall and drops the denied packets.



Screened Subnet Firewall

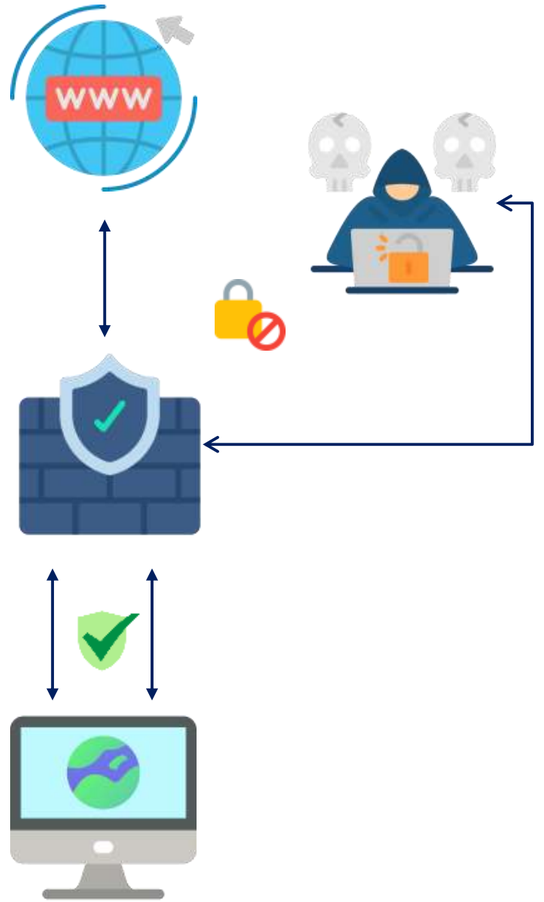
- It adds another layer of protection to the screened-host architecture.
- It passes the connection through another firewall, instead of routing internet traffic after the screened host firewall.
- It creates a DMZ segment in the network.
- It provides multiple layers of protection.



Firewall Rules

They are an established set of rules that firewalls rely on to filter out traffic and protect networks and devices from attacks. Rules can be based on:

- Directions (inbound and outbound)
- Allow and deny rules
- Port numbers, protocol types, and IP address



Firewall Rules

Inbound or outbound rules	• **Outbound rules:** Dictate what internal network can access externally • **Inbound rules:** Regulate incoming traffic to determine what external requests can access the network
Explicit allow and explicit deny	• In firewall configurations, sequence of rules is crucial for effective security. • **Explicit deny rules:** Serve as the first line of defense, blocking specific traffic types or sources that should never gain entry • **Explicit allow rules:** Specify what's allowed after establishing denial criteria
Port number, protocol, and IP address	• **Port numbers:** Specify which ports are open for communication (such as port 80 for HTTP) • **Protocol types:** Determine allowed communication protocols (such as TCP and UDP) • **IP address:** Consider source or destination of the IP address being used

Access Control List

It's a list of rules that defines who (users or groups) can access a specific resource and what actions (read, write, execute) they are allowed to perform.

- Acts as a digital bouncer, controlling access to resources (files, folders, networks, systems)
- Consists of entries, often called access control entries (ACEs), which specify permissions

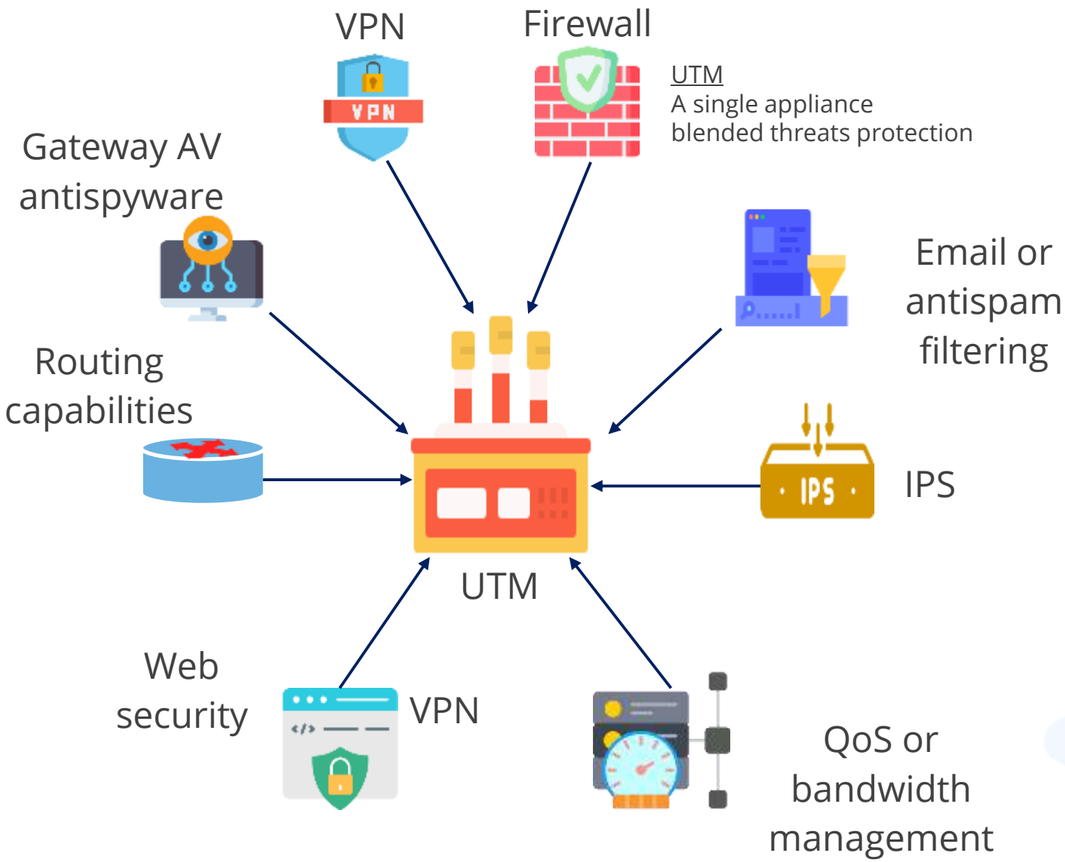
Next-Generation Firewalls

While intrusion detection software was initially developed as a stand-alone application, its functionality was quickly incorporated into a new generation of firewalls.

It combines security controls into single agent and management platforms.

Examples

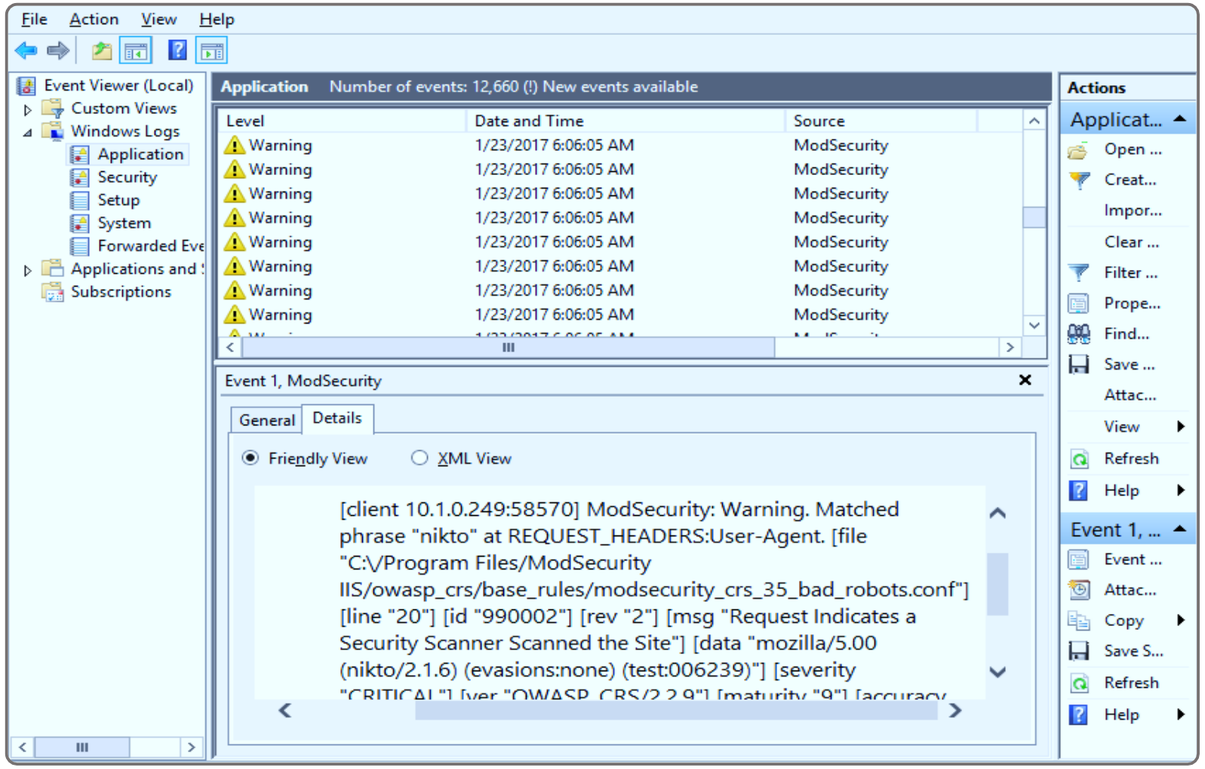
Firewall, anti-malware, network intrusion prevention, spam filtering, content filtering, data loss prevention, VPN, and cloud access gateway



Web Application Firewalls (WAFs)

They are specifically designed to safeguard software running on web servers and their backend databases against code injection and denial of service (DoS) attacks. They can:

1. Inspect code in HTTP packets
2. Match suspicious code to vulnerability database
3. Be implemented as software on host or as appliance



Web Application Firewalls (WAFs)

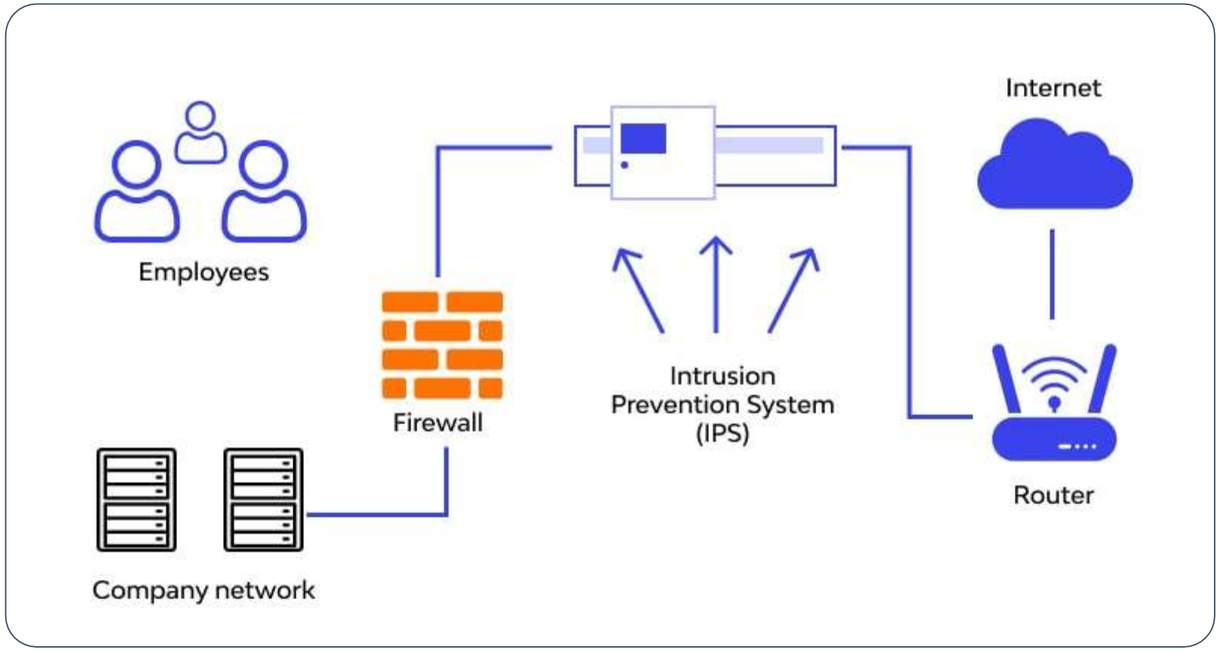
They can be deployed as appliance or web server plug-in software. The following are examples of WAF products:

Examples

- ModSecurity is an open-source WAF for Apache, Nginx, and IIS sponsored by Trustwave.
- NAXSI is an open-source module for the Nginx web server software.
- Imperva is a commercial web security company specialized in data centers.

Intrusion Detection and Prevention System

An intrusion detection system (IDS) detects unauthorized intrusions in a network, server, or system and identifies suspicious activity, sending an alarm to the network administrator.



An intrusion prevention system detects and prevents any malicious traffic or activity from gaining access to the target.

Components of IDS and IPS

Sensor

Collects network and user activity traffic and sends it to the analyzer

Analyzer

Looks for suspicious activities from collected data and alerts admin interface

Administrator interface

Manages and monitors the IDS via user interface

Signature database

Recognizes a collection of patterns and definitions of known suspicious or malicious activity

IDS and IPS Technology

Signature based

- It is also called knowledge-based pattern matching.
- It is developed by vendors based on known attack patterns.
- Its effectiveness depends on regular updates with new signatures.
- It is weak against new attacks as it can only recognize previously known attacks.

Profile or anomaly based

- It is a behavior-based IDS.
- It does not use predefined signatures.
- It learns the network traffic to create a baseline, post which any traffic pattern that meets a threshold variation triggers an alert.
- It can detect zero-day attacks and slow attacks.

Rule based

- It detects intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether any activity is suspicious or not.
- The rules used are specific to a machine and operating system.

False Positive and False Negative

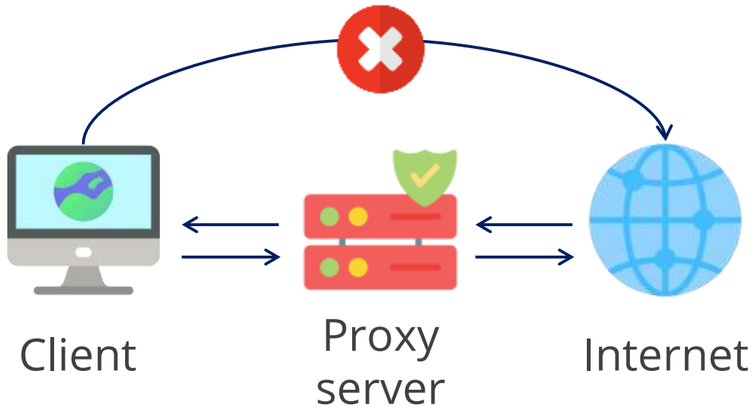
These parameters help evaluate the effectiveness of an IDS and IPS.

Detection	IDS detected it	IDS didn’t detect it
Malicious traffic	True positive (Attack and alert)	False negative (Attack and no alert)
Normal traffic	False positive (No attack and alert)	True negative (No attack and no alert)

Proxy Server

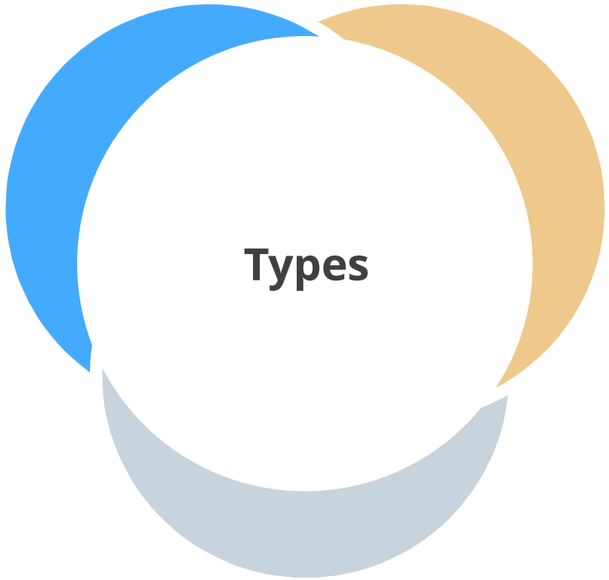
It is a server that sits between a client application, such as a web browser and a real server.

- Intercepts all requests to the real server and forwards the request to the real server if unable to fulfil the requests itself
- Acts as intermediary between clients that need to communicate
- Caches the responses it receives so that requests from other clients are served faster



Types of Proxy Servers

Forward proxy



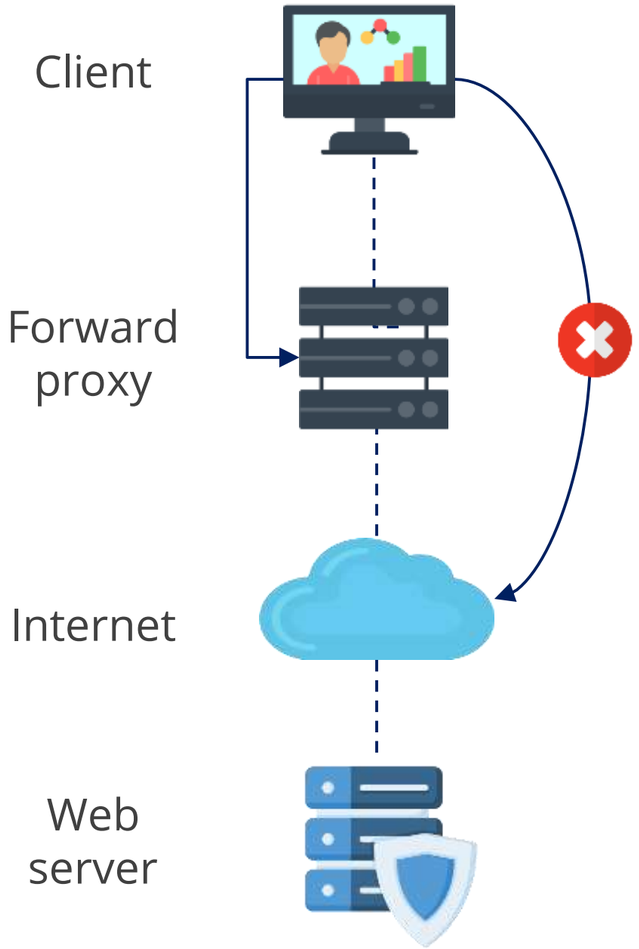
Transparent proxy

Reverse proxy

Forward Proxy

It is a computer on the LAN that allows connecting to the outside network without compromising the security of the internal network.

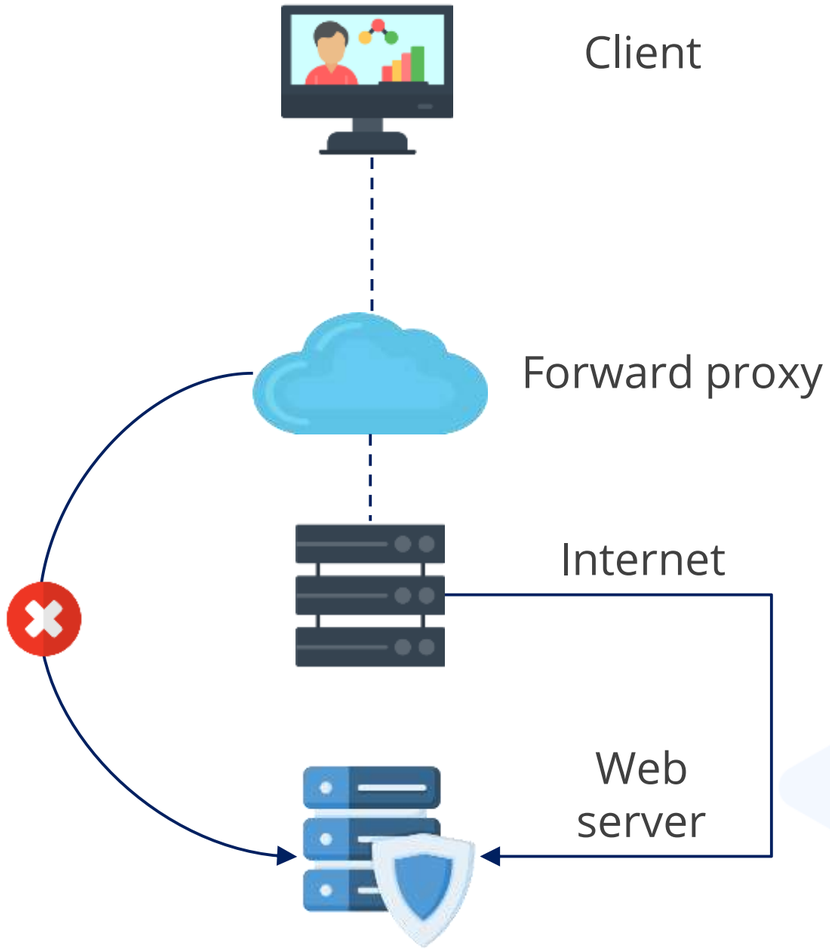
It is a proxy configured to handle requests from a group of clients under a local administrator's control to an unknown external or arbitrary group of resources.



Reverse Proxy

It is a server that sits in front of web servers and forwards client (such as a web browser) requests to those web servers.

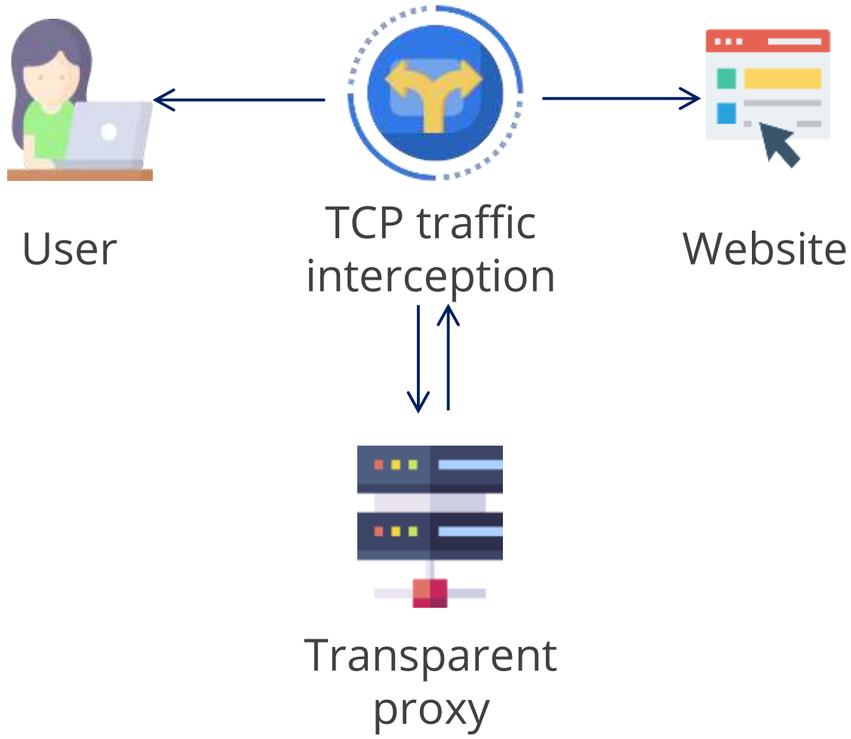
- It is configured to handle remote or arbitrary client requests to a group of known resources under the control of the local administrator.
- It is a single-entry point that serves multiple backend servers.



Transparent Proxy

In this proxy deployment, the user's client software (typically a browser) is unaware that it is communicating with a proxy.

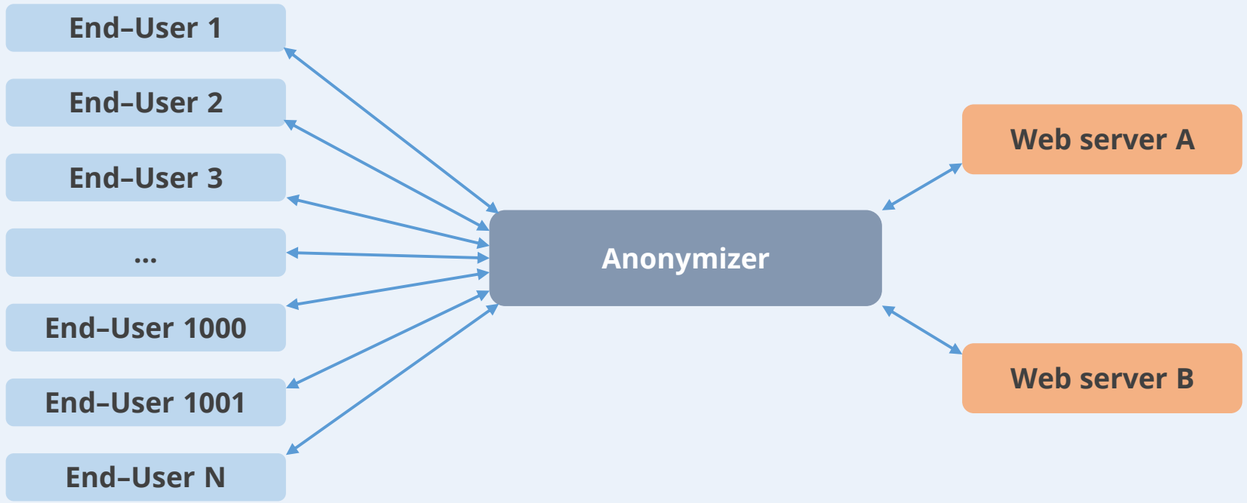
- Users request internet content as usual, without any special client configuration, and the proxy serves their requests.
- These are intermediary systems that sit between a user and a content provider.



Other Proxy Types

- Anonymizing proxy
- Caching proxy
- Content filtering proxy
- Open proxy
- Web proxy

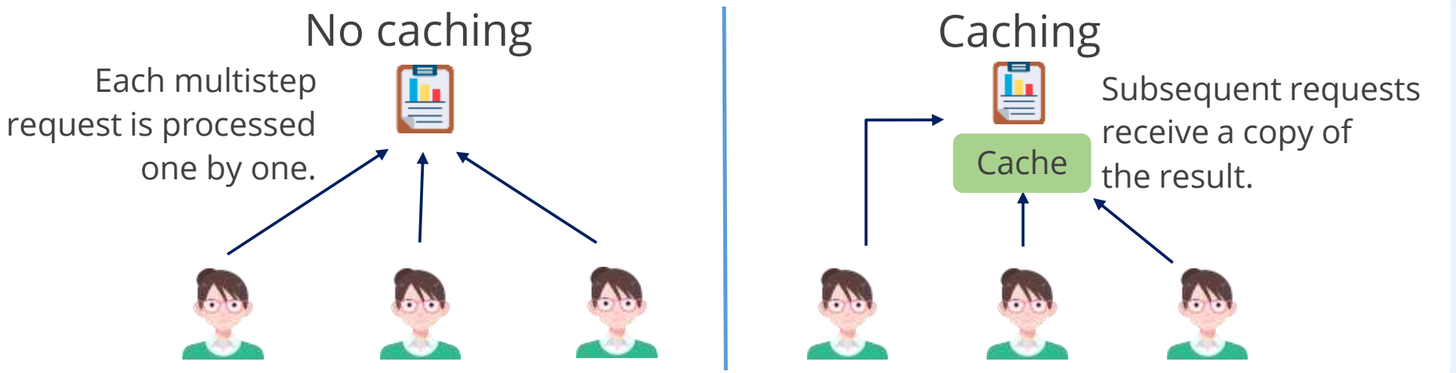
- It is designed to hide information about the requesting system and make a user's web browsing experience anonymous.
- It is used by individuals concerned about personal data transfer across the internet and the use of cookies and other mechanisms to track browsing activity.



Other Proxy Types

- Anonymizing proxy
- Caching proxy
- Content filtering proxy
- Open proxy
- Web proxy

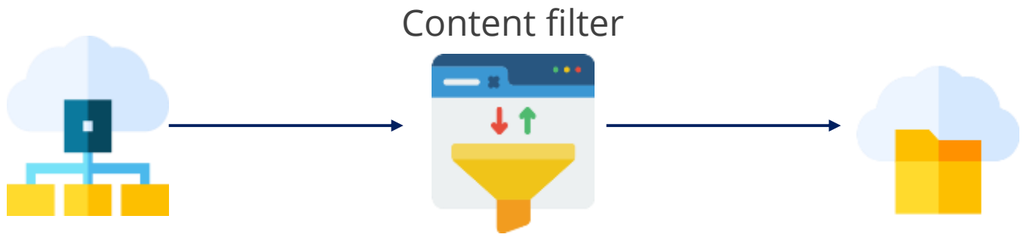
- It keeps local copies of popular client requests and is used in large organizations to reduce bandwidth usage and increase performance.
- When a request is made, it first checks its cache, and if it finds a copy of the requested content, it serves the client request without contacting the destination server.



Other Proxy Types

- Anonymizing proxy
- Caching proxy
- Content filtering proxy
- Open proxy
- Web proxy

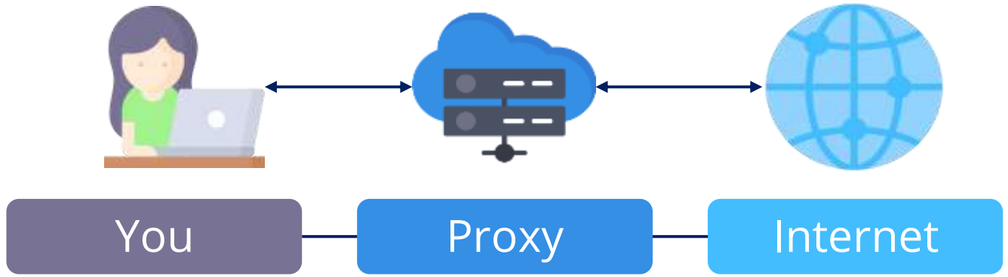
- It examines each client request and compares it to an established acceptable use policy (AUP).
- It filters the requests in numerous ways (by requested URL, destination system, domain name, or keywords in the content).
- It supports user-level authentication to control and monitor the access and log and analyze any activity through the proxy.



Other Proxy Types

- Anonymizing proxy
- Caching proxy
- Content filtering proxy
- Open proxy
- Web proxy

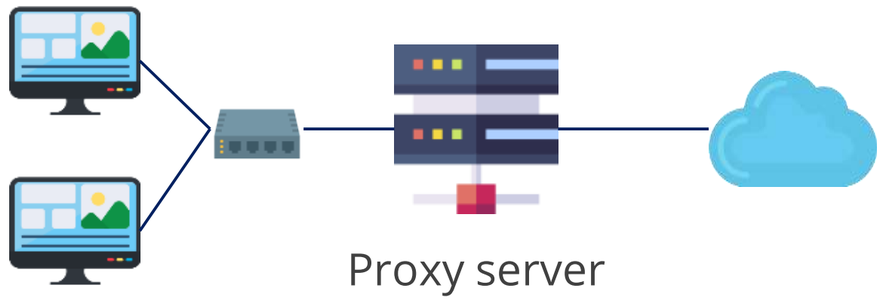
- It is available to any internet user and also has some anonymizing capabilities.
- It has been the subject of some controversy with internet privacy and freedom on one side of the argument, and law enforcement, corporations, and government entities on the other.



Other Proxy Types

- Anonymizing proxy
- Caching proxy
- Content filtering proxy
- Open proxy
- Web proxy

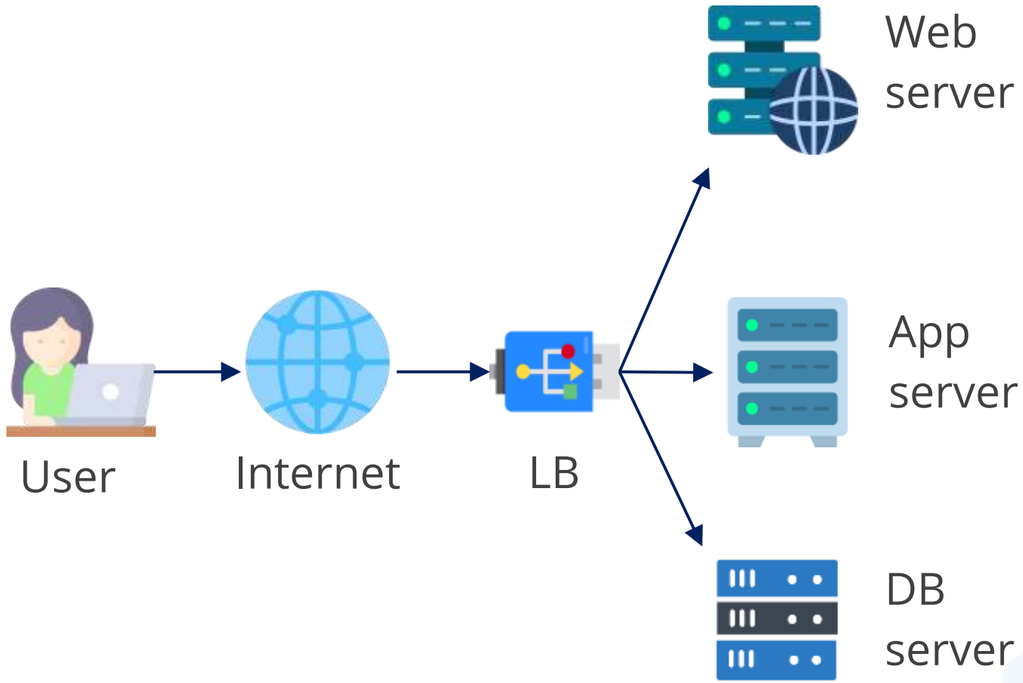
- It is solely designed to handle web traffic and is also called a web cache.
- Most web proxies are essentially specialized caching proxies.



Load Balancer

It is a device that distributes network or application traffic across server clusters to improve responsiveness and increase availability of applications.

- It sits between the client and server farm accepting incoming network and application traffic and distributing it across multiple backend servers.
- It reduces individual server load and prevents one application server from single-point failures by balancing application requests across multiple servers.



Load Balancer Scheduling

Its goal is to maximize the performance of a parallel system, by transferring tasks from busy processors to other less busy or idle processors.

The two prominent load-balancing algorithms are:

Round robin

- It involves sending each new request to the next server in rotation.
- It sends all requests to servers in equal amounts, regardless of server load.

Affinity based scheduling

- It keeps a host connected to the same server across a session.
- It benefits applications like web applications in both directions.

Load Balancer Redundancy

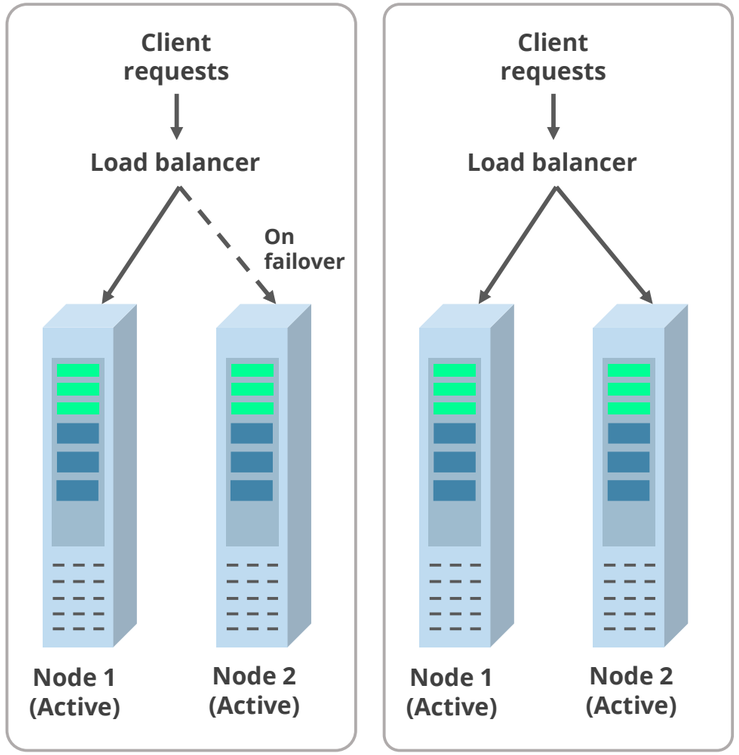
It involves deploying multiple load balancers to achieve high availability, reliability, and fault tolerance in a network. The following are its types:

Active-passive

- The primary load balancer actively balances while the secondary load balancer passively observes.
- The secondary load balancer steps in if the primary system fails.

Active-active

- All the load balancers are active, sharing the duties.
- Though it enhances performance, it is also important to watch the overall load.



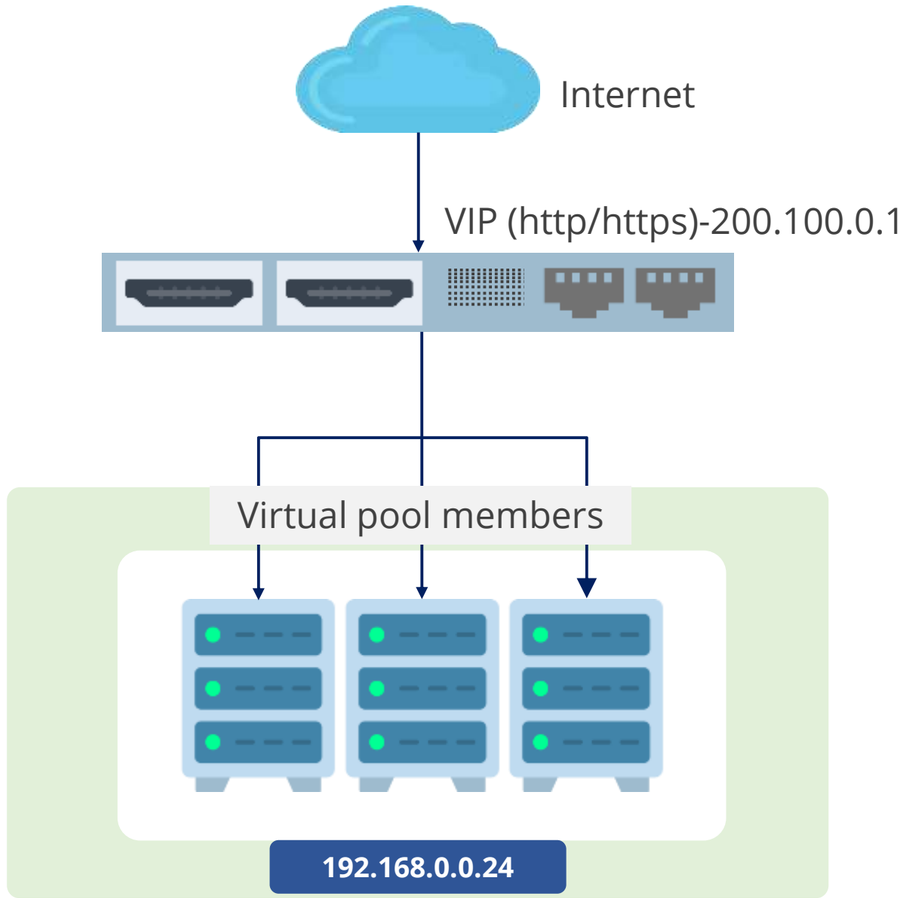
Active-passive system

Active-active system

Load Balancer: Virtual IP (VIP)

It is the load-balancing instance to which the world directs its browsers to access a site.

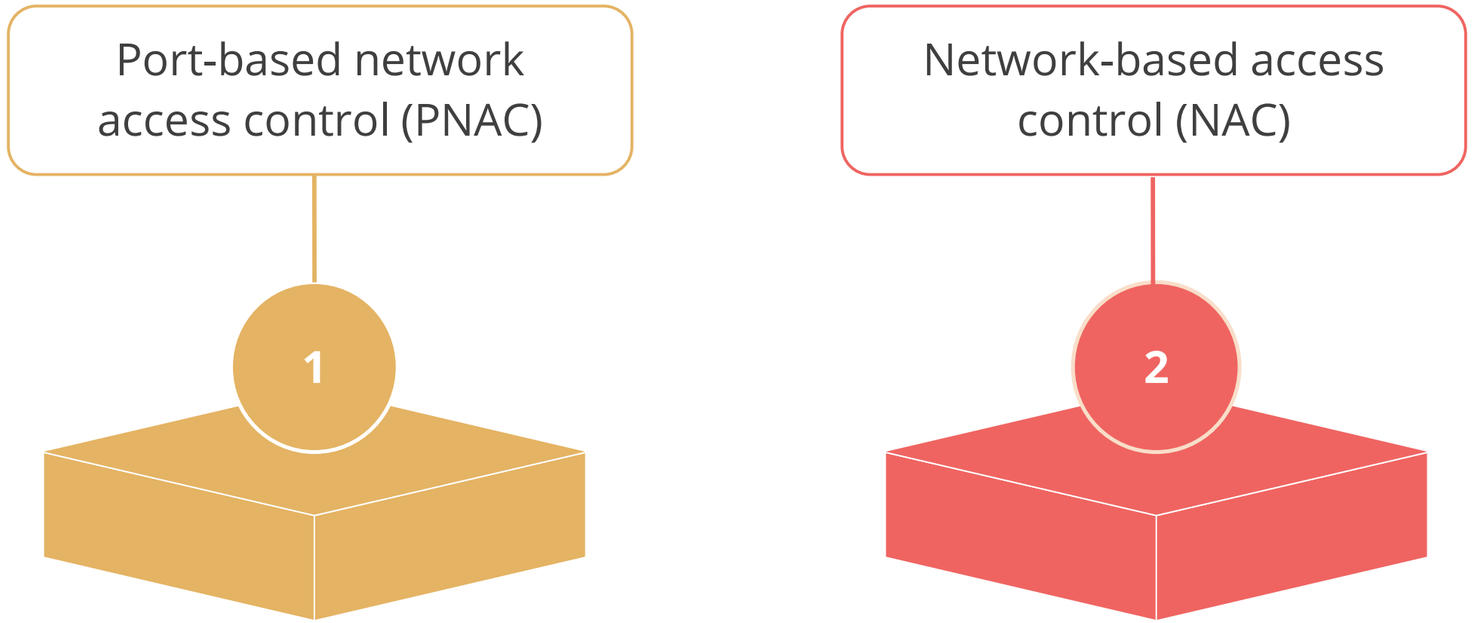
- It has an IP address which must be publicly available for use.
- It usually connects with a TCP or UDP port number, such as TCP port 80 for web traffic.



Network Access Control

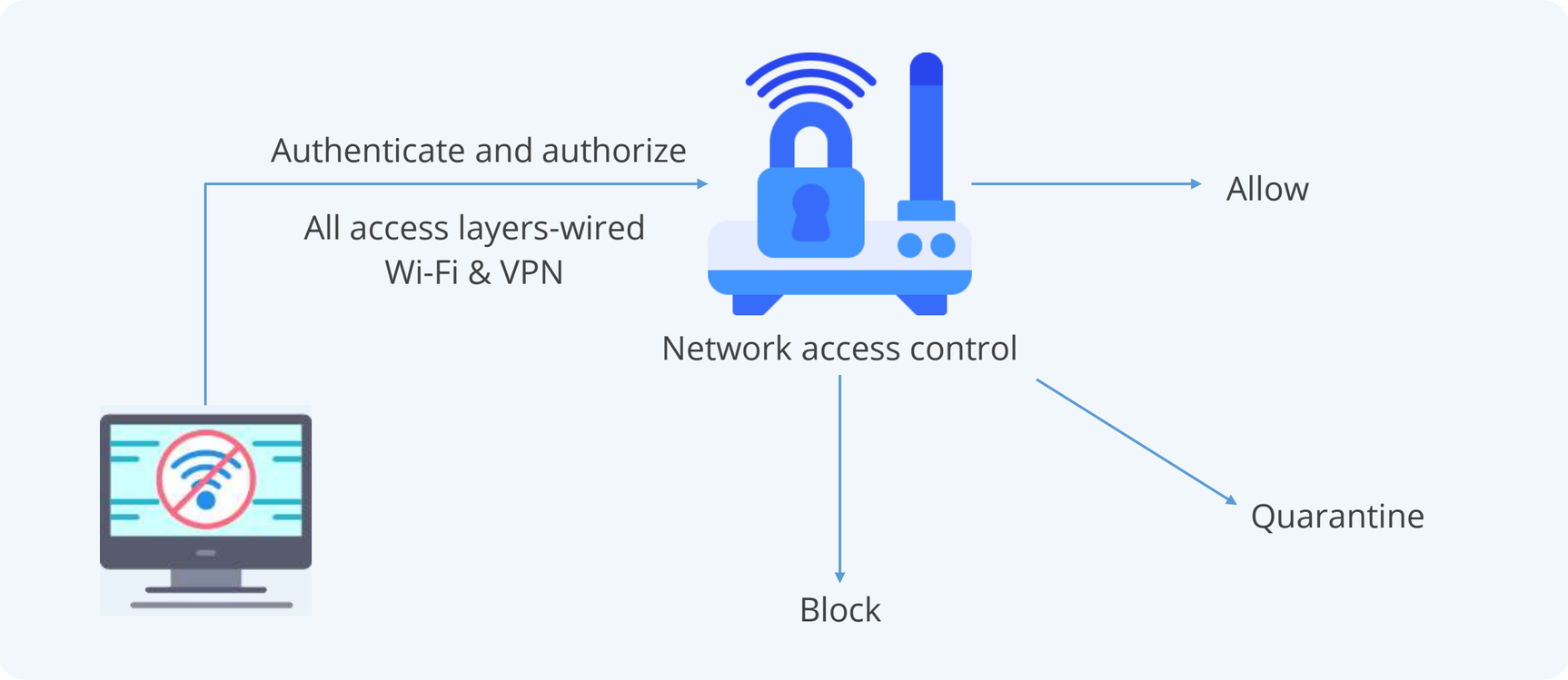
It is a security solution that regulates device access to a network, ensuring only authenticated and compliant devices connect, thereby enhancing network security.

The different types of network access control are:



Network-Based Access Control

It is a concept of controlling access to an environment through strict adherence to and implementation of security policy.

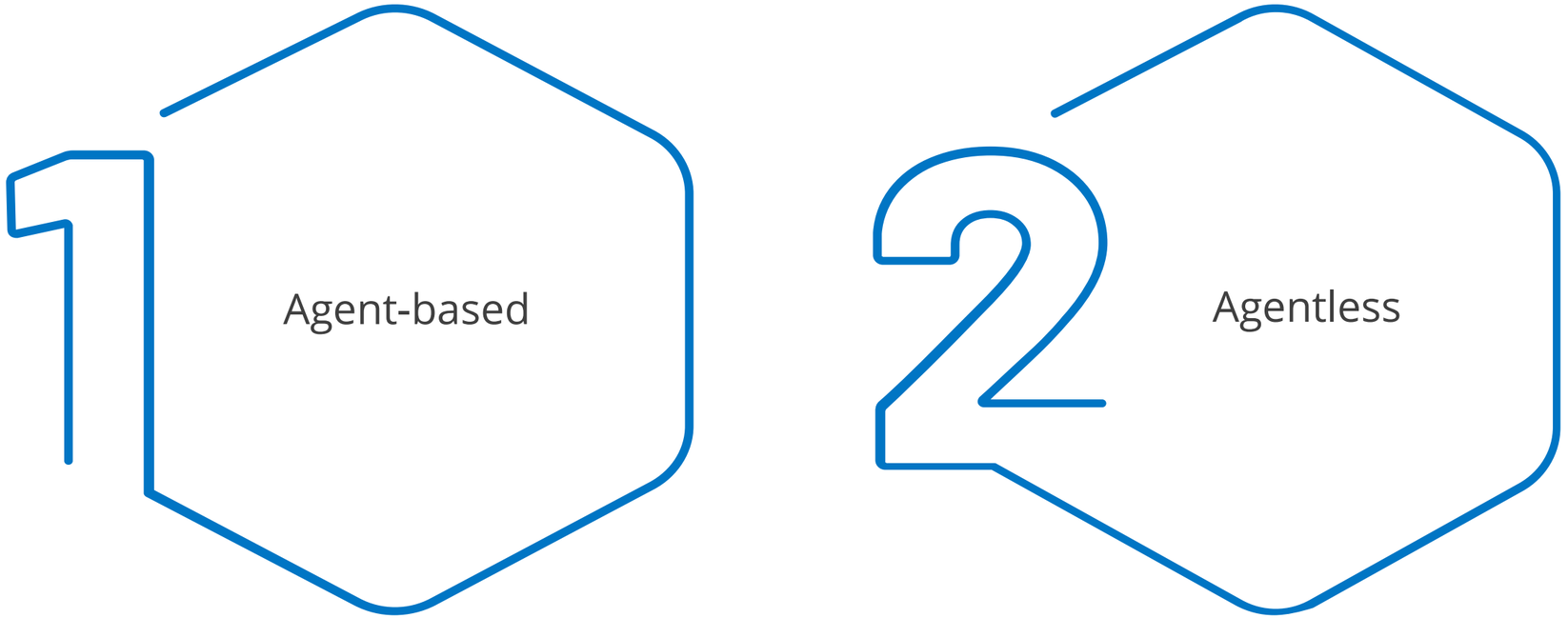


It strengthens the security of a proprietary network by restricting access to network resources for endpoint devices.

Network-Based Access Control: Posture Assessment

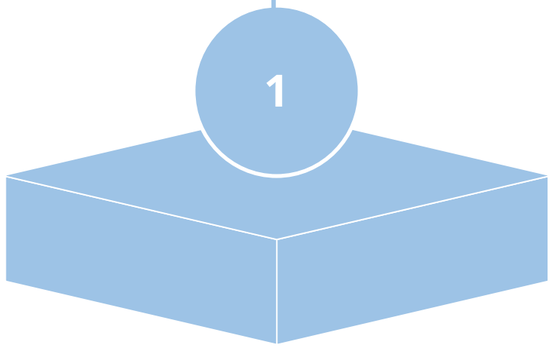
It is the process by which host health checks are performed against a client device to verify compliance with the health policy.

Posture assessment can be:

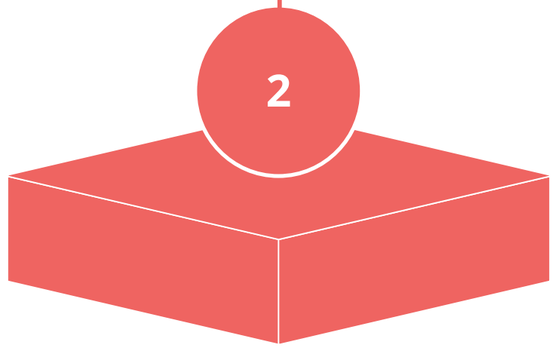


Goals of Network-Based Access Control

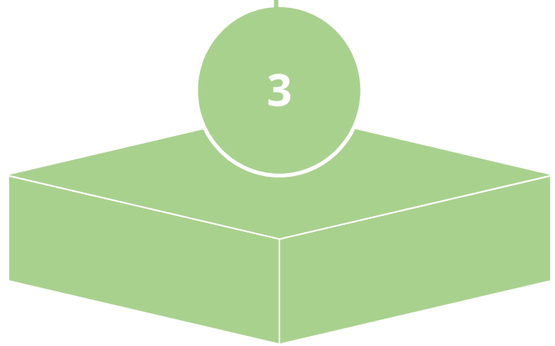
Prevent or reduce zero-day attacks



Enforce security policy through out the network



Use identities to perform access control



Network-Based Access Control: Implementation

The following policies guide the implementation of network access control and are applied before allowing device or user connections.

Pre-admission policy

Requires a system to meet all current security requirements (patch application and antivirus updates) before it is allowed to communicate with the network

Post admission policy

Allows and denies access based on user activity, which is based on a predefined authorization matrix

They are the actions taken before and after a device accesses a network, each with specific functions and objectives for security and compliance.

Network-Based Access Control: Agents

It is a software that examines a host before allowing it to connect to the network.

Types of NAC agents include:

Permanent agents

- They are permanently deployed to hosts or provided on a need basis by the endpoint at the time of use.
- Pre-deployed agents at the endpoints act as the gateway to NAC functionality.
- One of the first checks is agent integrity, then machine integrity.

Dissolvable agents

- These agents are deployed upon request and later discarded after use.
- These agents, in essence, disappear after use.

Port-Based Network Access Control

It ensures port security using the following methods:

Physical port security

- Provides secure access to physical switch ports and switch hardware
- Physically disconnects the unused ports
- Disables switch port using the management software

MAC filtering

- Configures permitted MACs
- Limits number of MAC changes

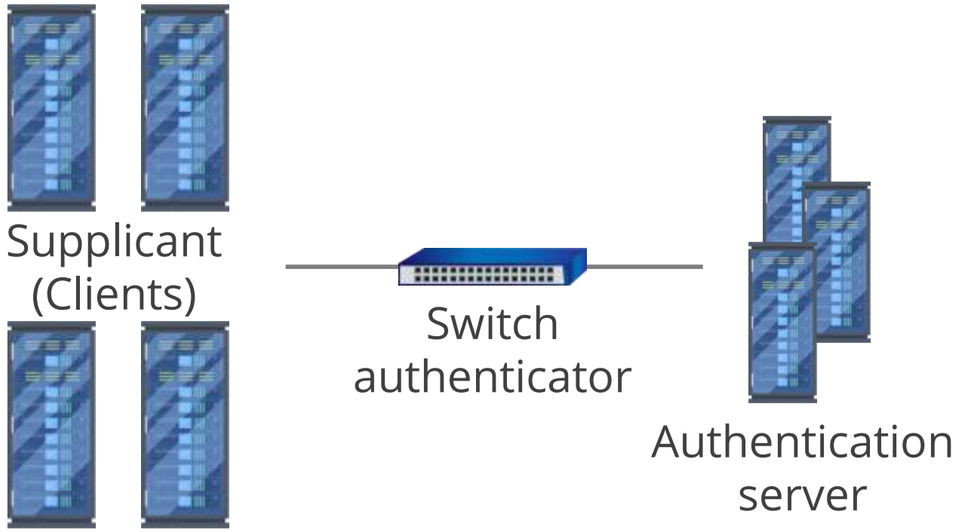
Dynamic host configuration protocol (DHCP) snooping

- Inspects traffic arriving on access ports
- Ensures ARP packets use valid IP addresses via dynamic ARP inspection (DAI)

IEEE 802.1x

It is a crucial network access control (NAC) standard used for authentication and control of network resources, essential for network security. It involves three parties:

- **Supplicant**: Client device (such as laptop) that wants to be authenticated to LAN or WLAN
- **Authentication server**: Trusted server that authenticates the supplicant, typically a RADIUS server
- **Authenticator**: Device that provides a data link between the supplicant and authentication server and allows or blocks traffic between them

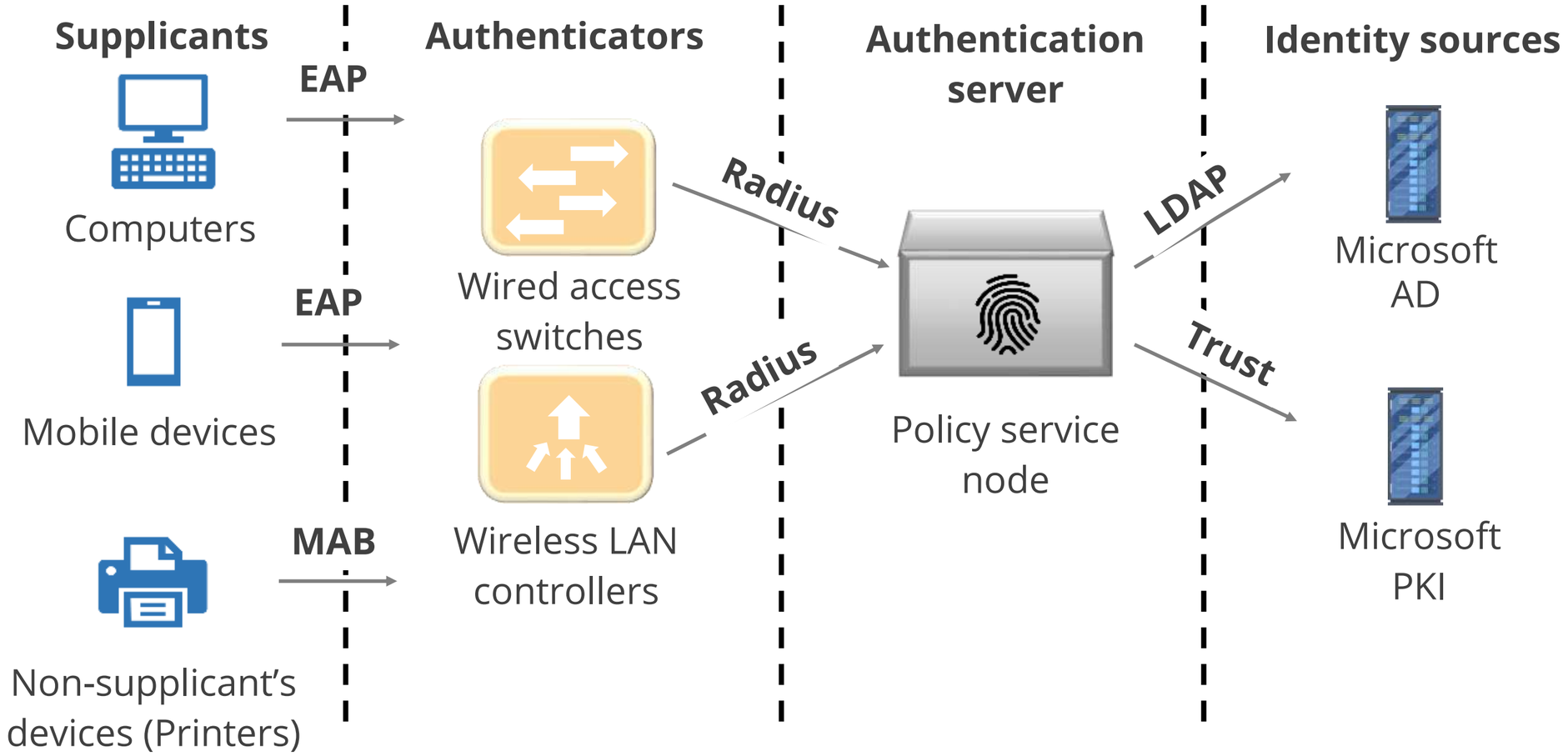


Examples

Wireless access point or an ethernet switch

Source: https://www.tp-link.com/us/configuration-guides/configuring_802_1x/?configurationId=18220

802.1x Architecture



Source: https://sudonull.com/post/31574-Configuring-8021X-on-Cisco-Switches-Using-Failover-NPS-Windows-RADIUS-with-AD

Quick Check

Your organization has recently implemented an 802.1x network access control (NAC) solution. However, you notice that some users are experiencing intermittent connectivity issues. Which of the following is most likely the cause of the connectivity problems?

A. Incorrectly configured supplicant software on user devices

B. Overloaded authentication server

C. Faulty network infrastructure components

D. Insufficient NAC policy enforcement

Implementing Remote Access

Introduction to Remote Access Technologies

They are the data networking technologies that are focused on providing access to a remote user into a network.

Advantages of remote access technologies:

Reduce networking costs

Build efficient ties

Provide flexible work styles

Remote Access Technologies

The following are its different types:

- Dial-up connection
- Digital subscriber line (DSL)
- Integrated service digital network (ISDN)
- Virtual private network (VPN)
- Internet protocol security (IPSec)

Dial-Up Connection

It uses the public switched telephone network (PSTN) facilities to establish a connection to an internet service provider (ISP) by dialing a telephone number on a telephone line.

The connections take place over point-to-point protocol, which has authentication capabilities.

Modem

It is a device that modulates an outgoing digital signal into an analog signal and demodulates the incoming analog signal into digital signals.

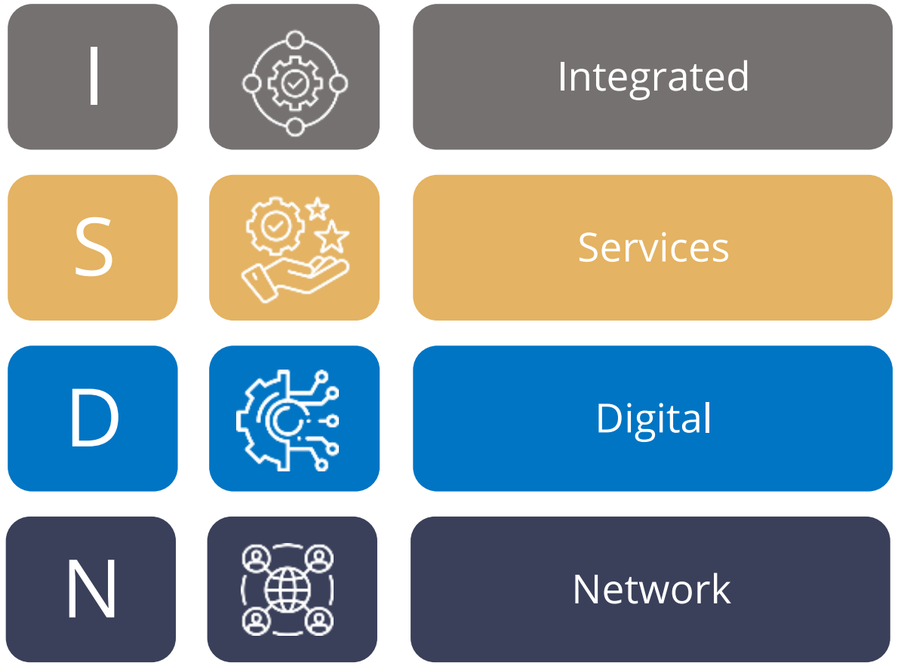
Digital Subscriber Line (DSL)

It is a high-speed connection technology used to connect a home or office to a service provider network.

- It provides six to 20 times higher bandwidth than ISDN.
- It uses existing phone lines and provides a 24-hour connection to the internet at rates up to 52 Mbps.
- It provides faster transmission rates as it uses all the frequencies available on a voice-grade UTP line.
- It always remains on and doesn’t need a dial-up.

Integrated Service Digital Network (ISDN)

It is a set of telecommunications services that can be used over public and private telecommunications networks.



It provides a digital, point-to-point, circuit-switching medium and establishes a circuit.

Types of ISDN

It provides the following two basic services:

Basic rate interface (BRI)

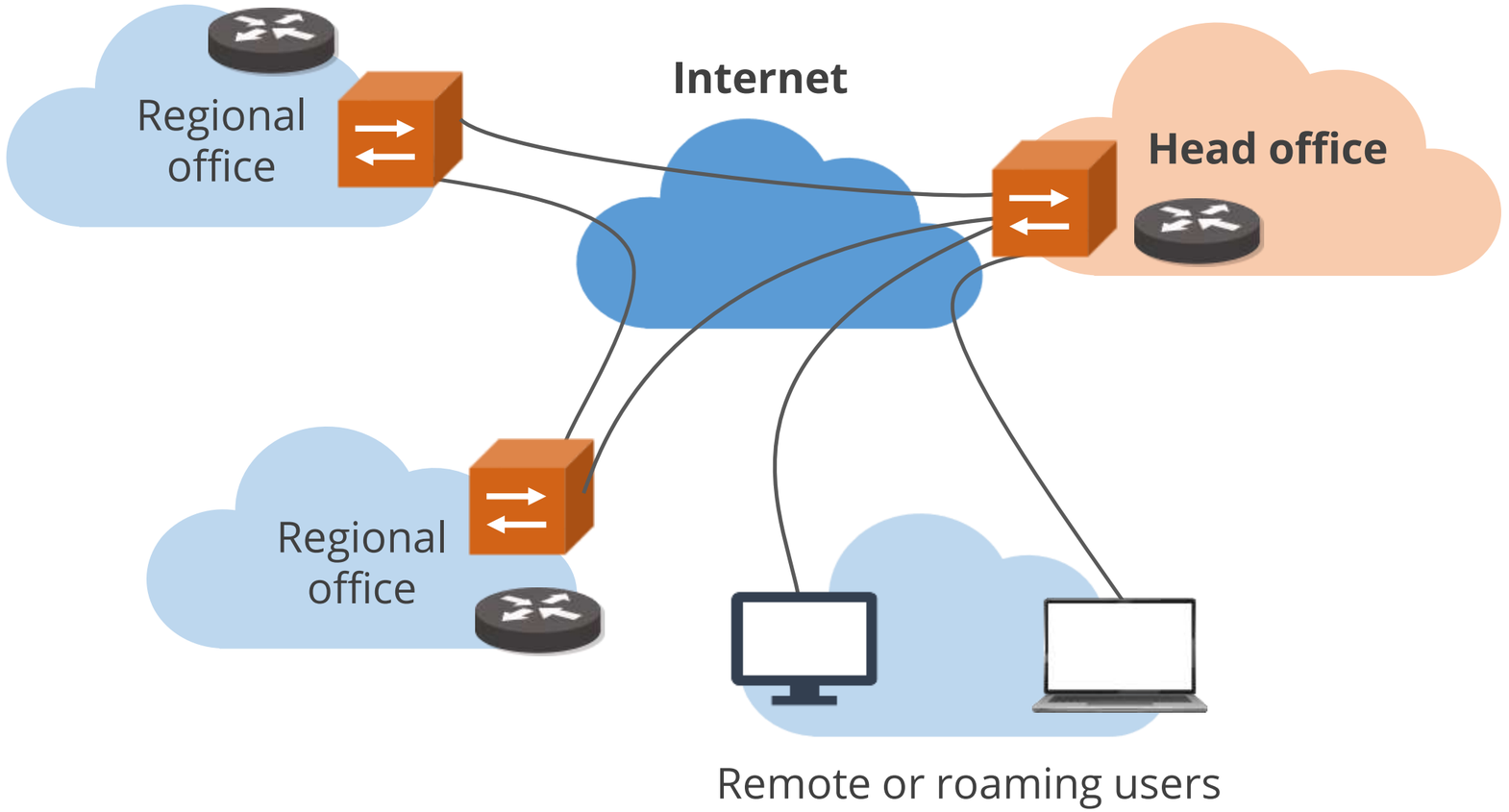
- Has two B channels for data transfer and one D channel that provides call setup, connection management, error control, and caller ID
- Has bandwidth of around 144Kbps
- Suitable for small offices and home offices

Primary rate interface (PRI)

- Has 23 B channels and one D channel
- Has total bandwidth of 1.544Mbps
- Suitable for companies that require higher bandwidth compared to BRI ISDN

Virtual Private Network (VPN)

It is a private network that uses a public network (usually internet) to connect remote sites or users together.



VPN Security

It has the following components:

Authentication: Ensuring that the data originates at the source that it claims

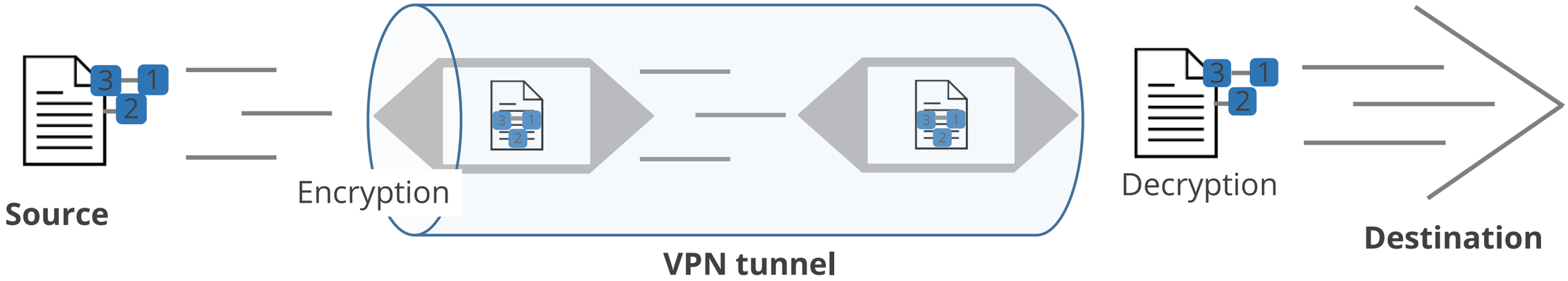
Access control: Restricting unauthorized users from gaining admission to the network

Confidentiality: Preventing anyone from reading or copying data as it travels across the internet

Integrity: Making sure that no one tampers with data as it travels across the internet

VPN Tunnel

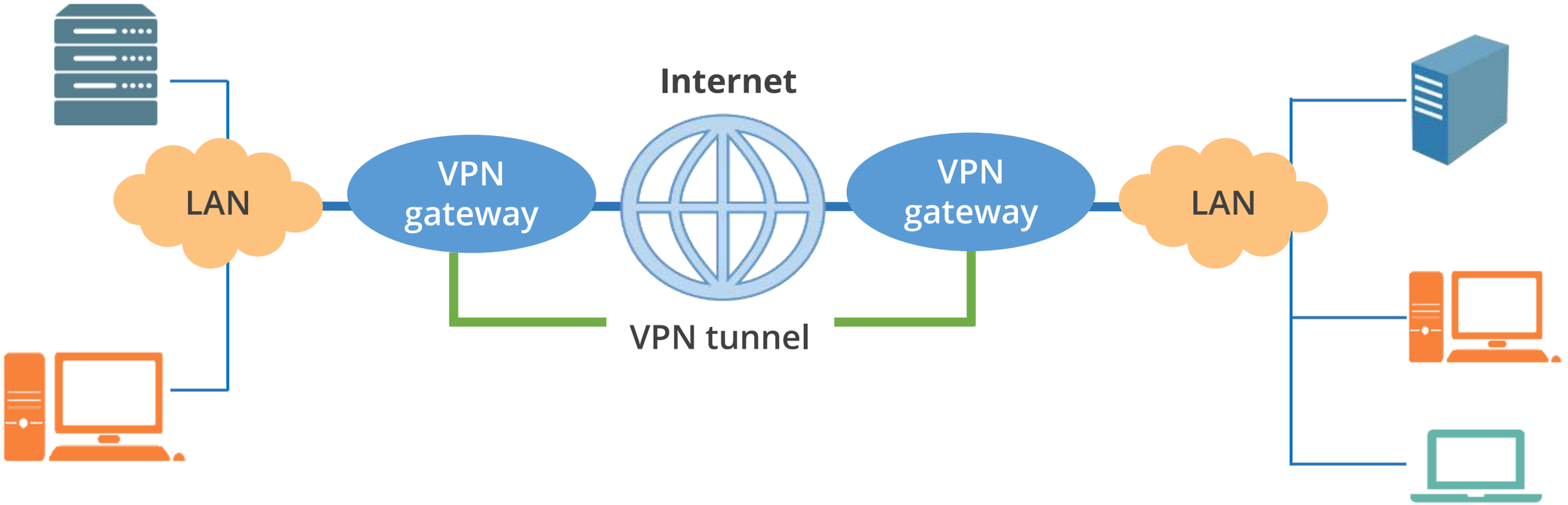
It is a tunnel that connects the user to the VPN server.



- To keep a data packet secure, it is wrapped in an encrypted outer packet through a process called encapsulation.
- At the VPN server, the outer packet is removed to access the data of the inner packet.

Types of VPN: Site-to-Site

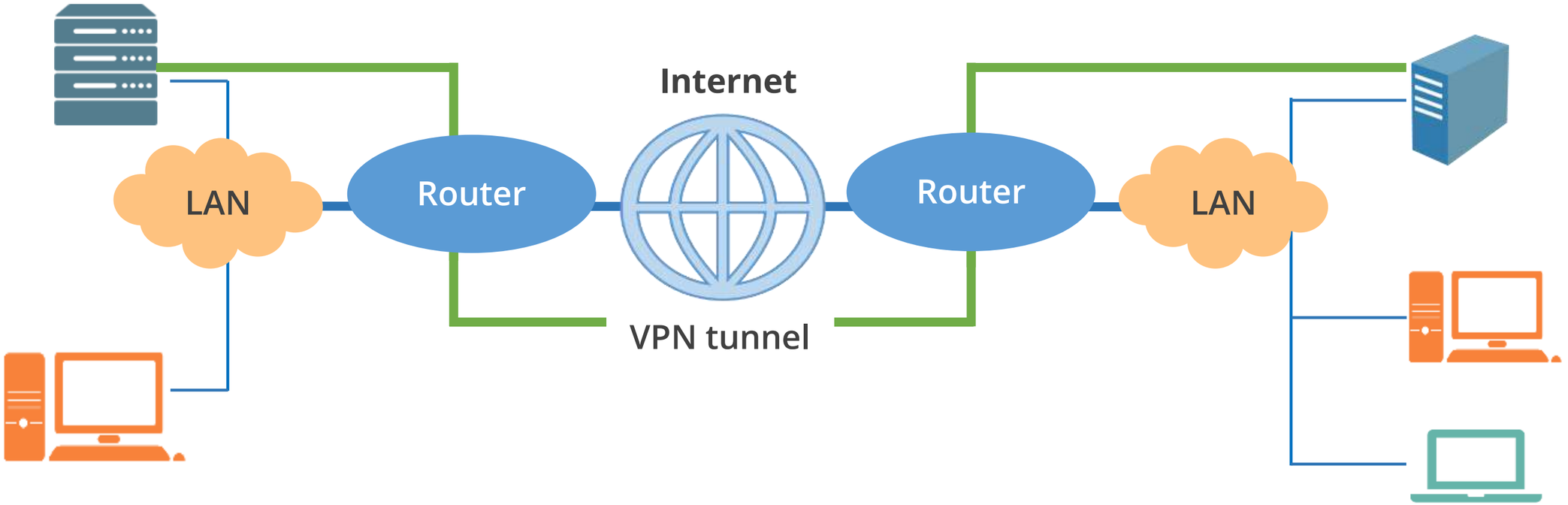
It allows a company to connect its remote sites to the corporate backbone securely over a public medium like the internet.



It is also called intranet VPN.

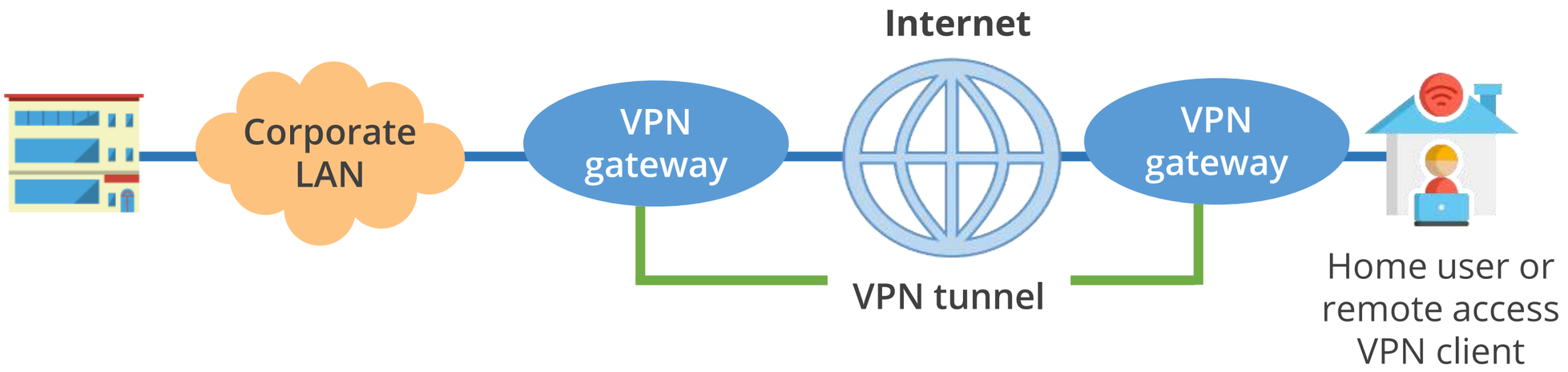
Types of VPN: Host-to-Host

It is like a site-to-site in concept except that the endpoints of the tunnel are two individual hosts.



Types of VPN: Host-to-Site

It allows remote users like telecommuters to securely access the corporate network wherever and whenever they need to.

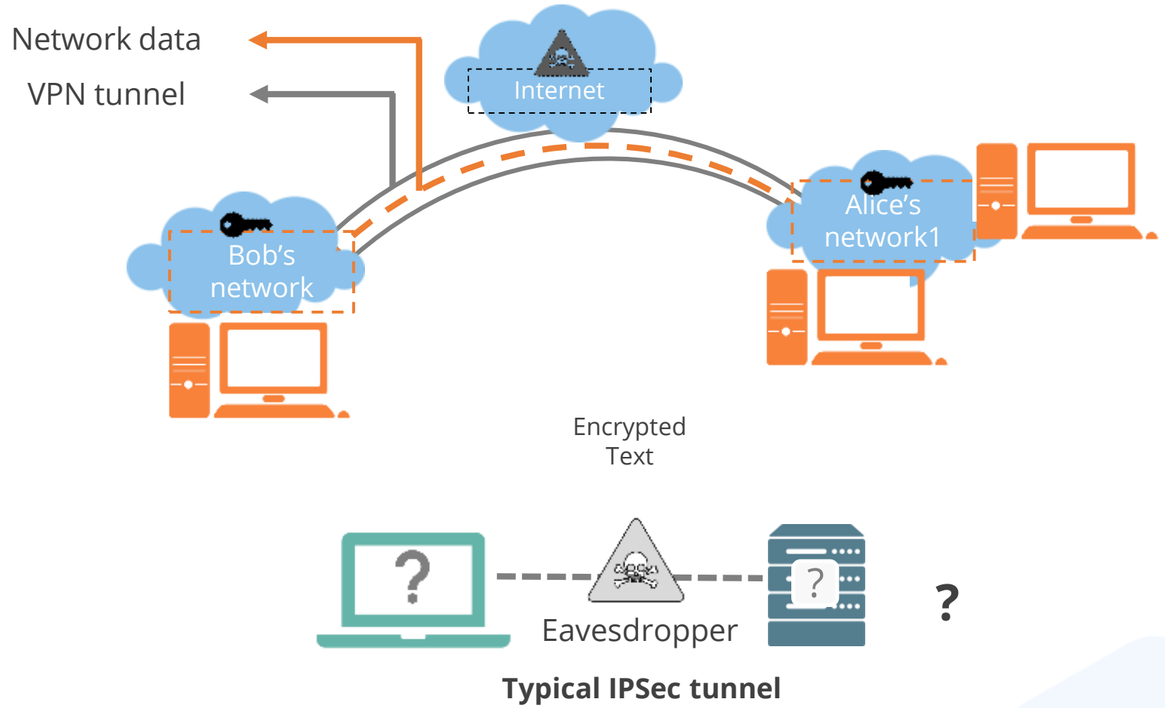


They are also called remote-access VPNs.

Internet Protocol Security (IPSec)

It is a protocol suite used for securing internet protocol (IP) communications.

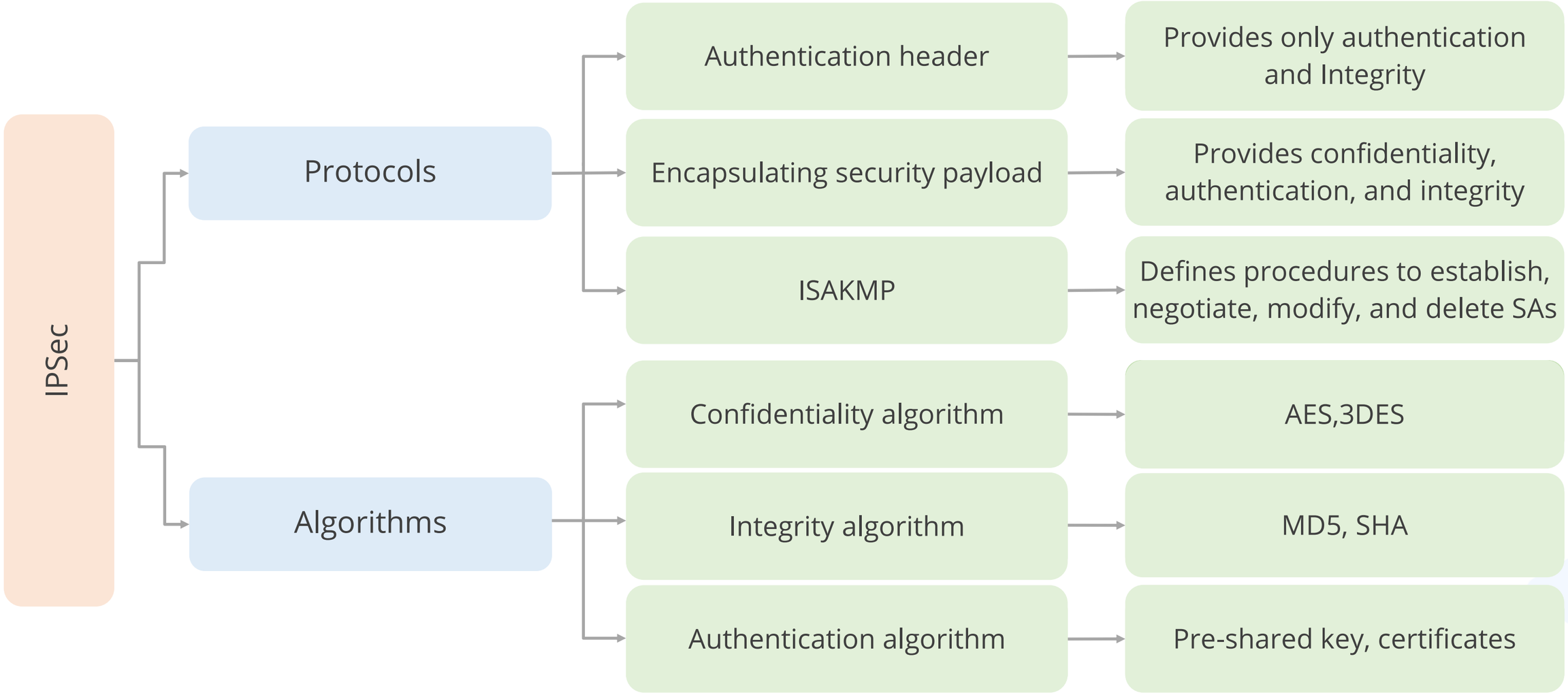
- They mutually authenticate agents at the beginning of the session and negotiate cryptographic keys to be used during the session.
- A cryptographic layer is added to both IPv4 and IPv6 using a suite of protocols.
- Each IP packet of a communication session is authenticated and encrypted.
- It provides VPNs and is used for creating a secure connection between client and server networks.



Typical IPSec tunnel

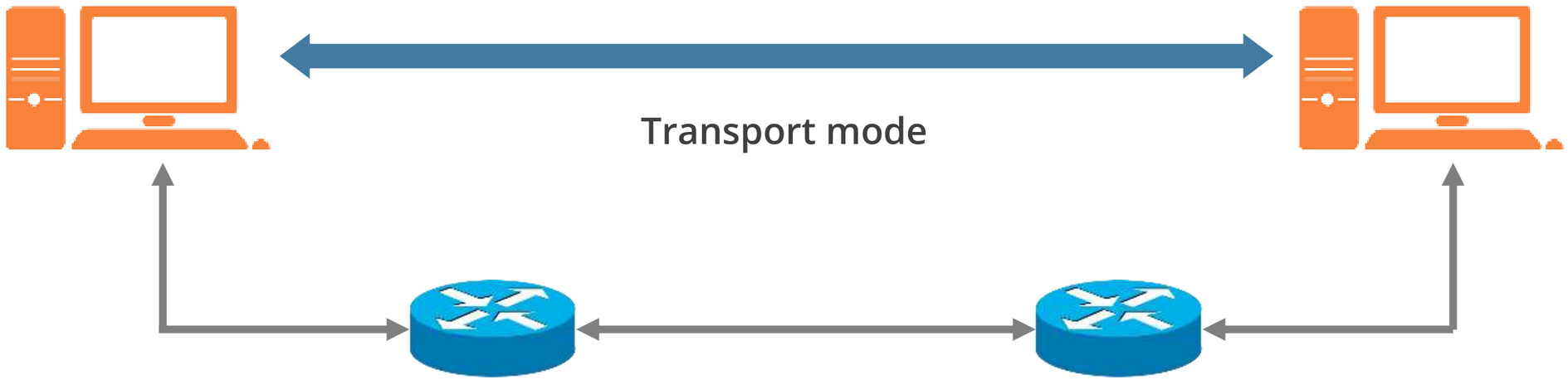
Internet Protocol Security (IPSec)

Some of the protocols and algorithms used by IPSec are:



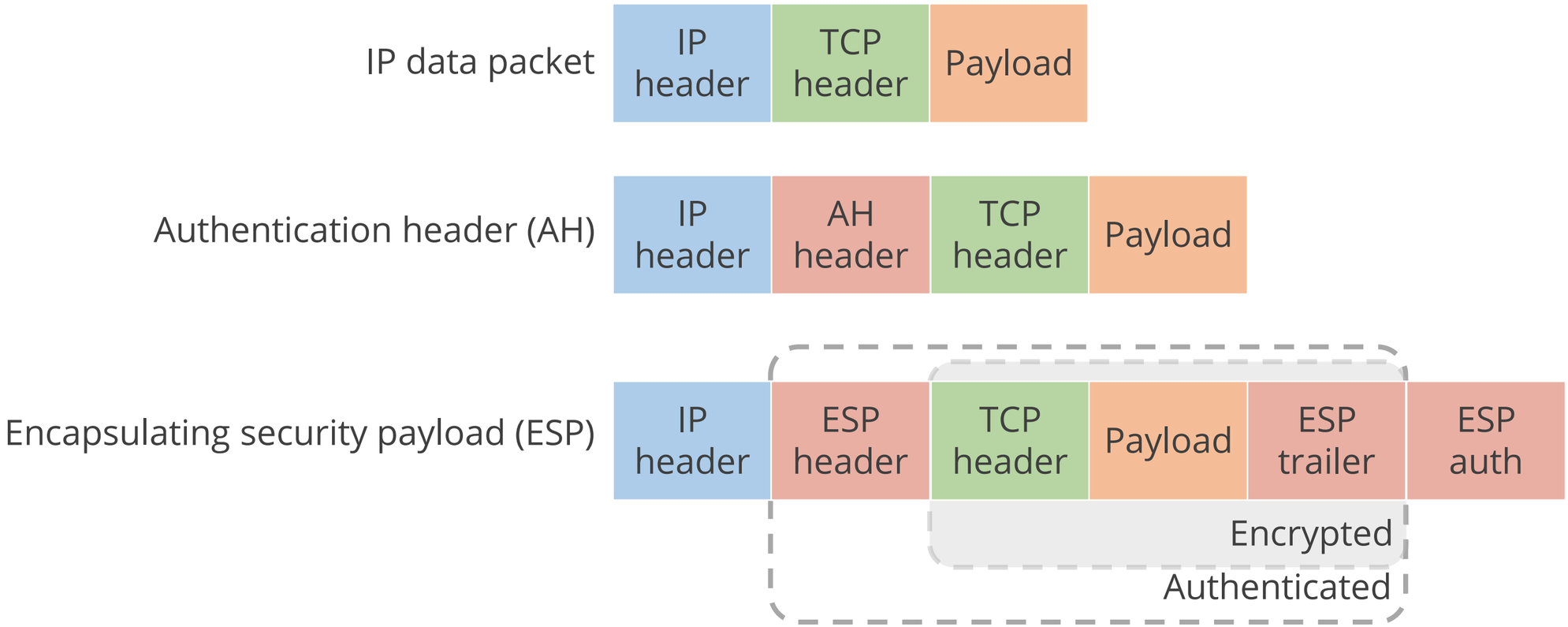
IPSec Modes: Transport Mode

In this mode, only the data is encrypted and is designed for peer-to-peer communication.



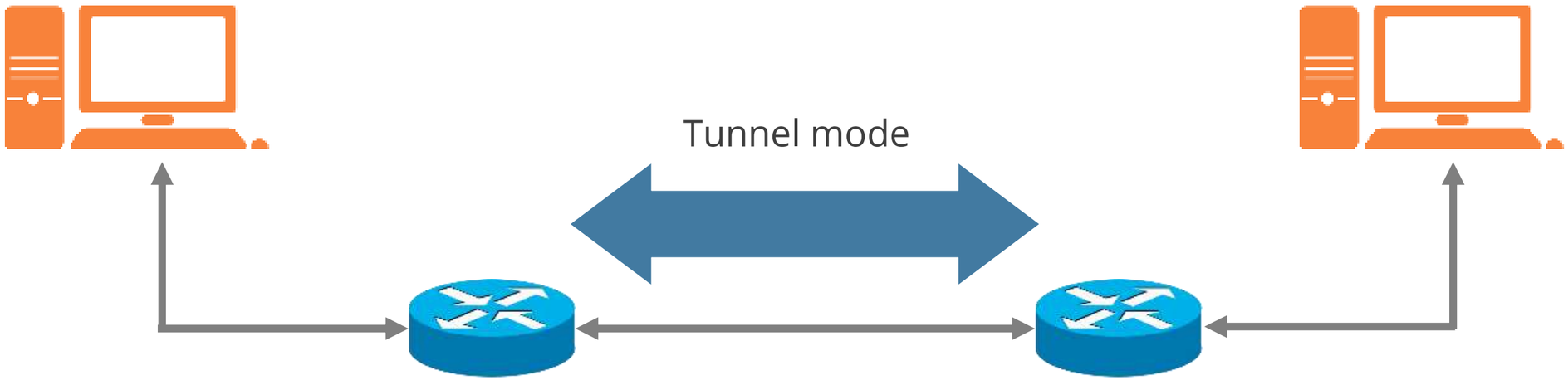
IPSec Modes: Transport Mode

It safeguards the payload of an IP packet, leaving the IP header untouched, primarily used for securing traffic between connected hosts or servers.



IPSec Modes: Tunnel Mode

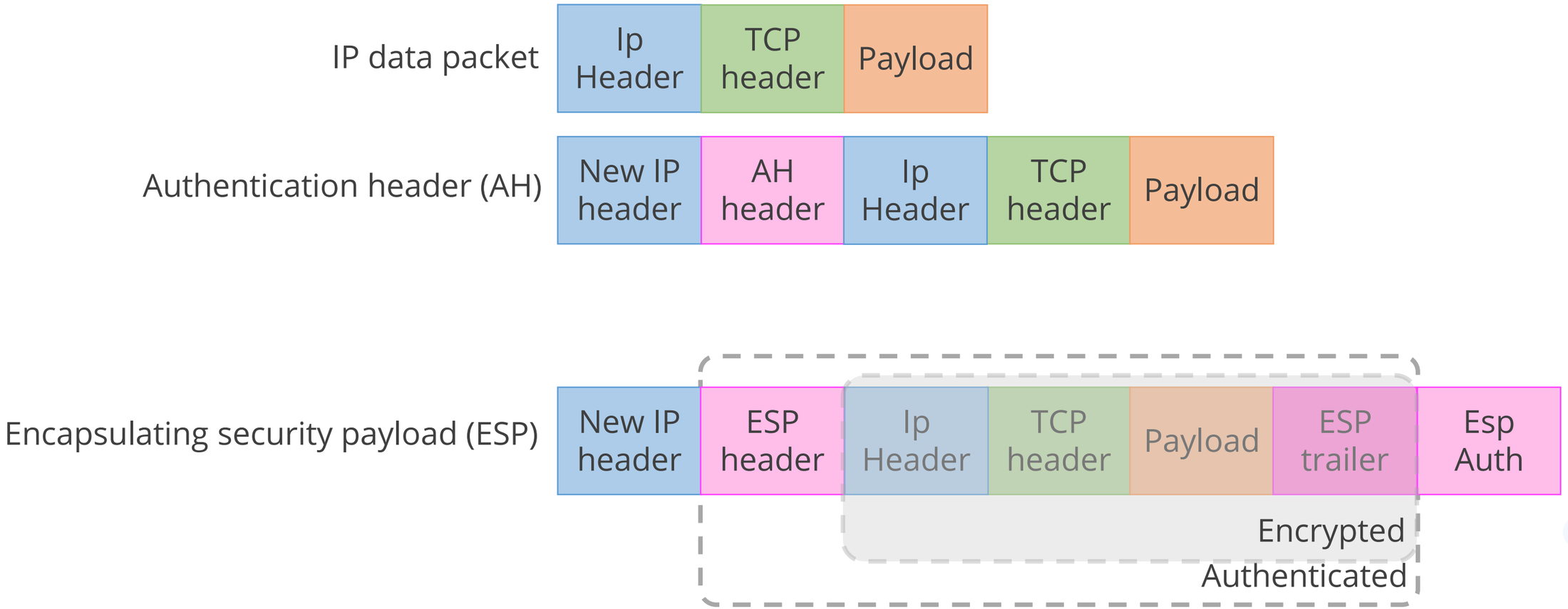
In this mode, the entire data packet including the header is encrypted.



It is designed for gateway-to-gateway communication.

IPSec Modes: Tunnel Mode

It encapsulates the original IP packet, including header and payload, for secure communication between networks and remote access scenarios in site-to-site VPNs.



IPSec Process

The steps in the process are as follows:

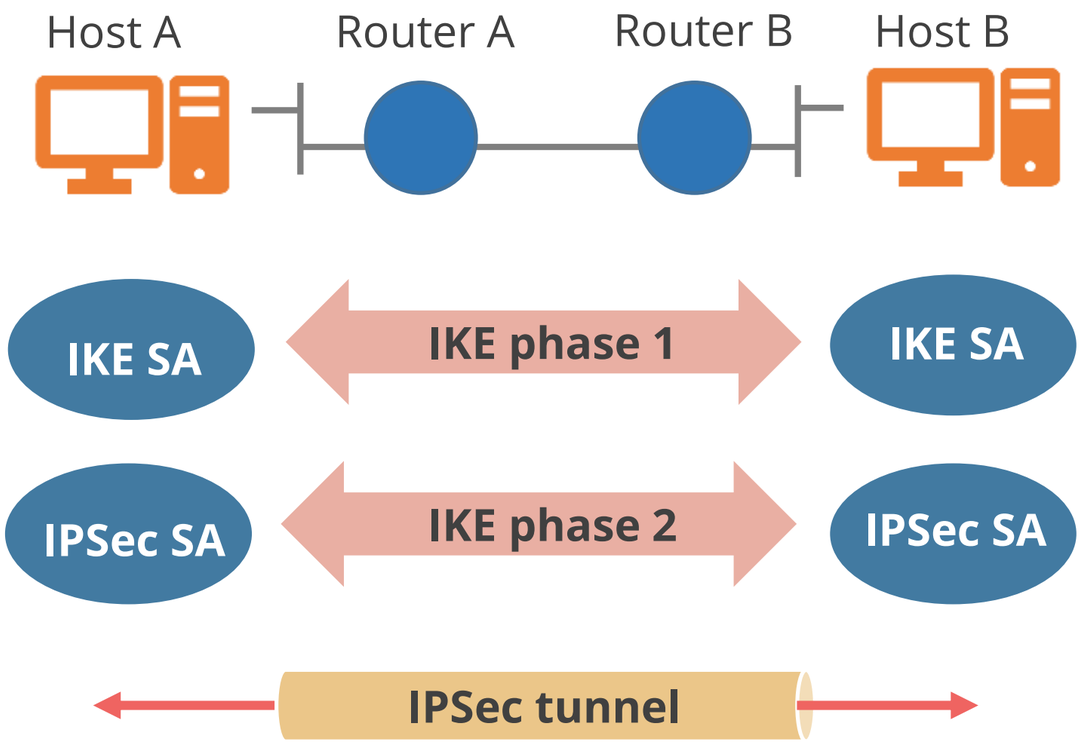
Step 1: Traffic that needs to be protected initiates the IPSec process

Step 2 : IKE phase 1

Step 3 : IKE phase 2

Step 4: Data transfer

Step 5 : IPSec tunnel termination



Quick Check

Bob wants to send data to Nancy through a VPN tunnel and ensure the data is transmitted securely. What techniques are used in a Virtual Private Network (VPN) to ensure this security?

A. Encapsulation

B. Wrapping

C. Transform

D. Encoding

Implementing Voice over Internet Protocol (VoIP)

Voice over IP (VoIP)

It is a category of hardware and software that enables people to use the internet as the transmission medium for telephone calls by sending voice data in packets using IP.

It is a packet switching technology that combines many types of data (voice, audio, and video) into a single IP packet.

VoIP Components

IP telephony device	Voice mail system	Voice gateway	Call processing manager
A phone that has necessary software allowance to work as a network device	A storage space for messages, providing user directory lookups and call-forwarding function	A gateway that carries out packet routing, providing access to legacy voice systems and backup calling process	A server that notifies both sender and receiver that the channel is active

Session Initiation Protocol (SIP)

It is an application layer protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video, and messaging applications.

VoIP Attacks

Identity and service theft

Stealing service from a service provider, or use service while passing the cost to another person

Vishing (VoIP phishing)

Calling by faking a trustworthy organization (such as a bank) and requesting confidential and often critical information

Viruses and malware

Exploiting softphones and software that are vulnerable to worms, viruses, and malware, just like any internet application

Denial of service attack

Flooding a target with unnecessary SIP call-signaling messages, thereby degrading the service

Spam over internet telephony (SPIT)

Clogging voice mail of mail system by sending SPAM messages to mail system

VoIP Security Controls

1. Develop appropriate architecture
2. Use VOIP-ready firewall
3. Avoid using soft phones
4. Apply encryption selectively
5. Maintain current patch levels
6. Install antivirus and update regularly

Secure VoIP

The following security mechanisms enhance the safety of voice and video communications over IP networks:

Secure real-time transport protocol (SRTP)	Provides confidentiality, integrity, and replay protection for voice and video communications through encryption and dynamic key management
Session initiation protocol secure (SIPS)	Secures SIP signaling using transport layer security (TLS) to enhance VOIP security by ensuring confidentiality, integrity, and authentication
Secure VoIP (SVoIP)	Integrates encryption and authentication to protect VoIP communications from eavesdropping and tampering

Phreaking Attack

It is a specific type of attack directed toward the telephone system.

Different types of technology are used to circumvent the telephone system to:

- Make free long-distance calls
- Tap phone lines
- Alter the function of telephone service
- Steal specialized services
- Cause service disruptions

Phreaker is someone who breaks into the telephone network illegally.

Phreaking Attack: Types

Black box

- It manipulates line voltages to steal long-distance services.
- It is often a custom-built circuit board with a battery and wire clips.

Red box

- It simulates tones of coins being deposited into a pay phone.
- It is often a small tape recorder.

Blue box

- It simulates 2600 Hz tones to interact directly with telephone network trunk systems (backbone).
- It is usually a whistle, tape recorder, or digital tone generator.

White box

- It controls the phone system.
- It is a dual-tone multi-frequency (DTMF) generator, either custom-built or a tool that most telephone repair personnel use.

Quick Check

The IT security manager is responsible for ensuring the security of a VoIP system. Which of the following security measures should be prioritized to protect the VoIP system against common threats?

A. Implement strong encryption protocols to secure voice communications and ensure confidentiality.

B. Use static IP addresses for all VoIP devices to simplify network management.

C. Disable firewall rules on the network to ensure that all VoIP traffic can flow freely without interference.

D. Require all employees to use personal mobile phones for VoIP calls to reduce the number of devices connected to the VoIP system.

Implementing Email Security

Email Security

Email is a digital method used to exchange messages and attachments between people and organizations over internet or computer networks.

- Email security encompasses methods and technologies that protect accounts, information, and users from threats.
- It guards against unauthorized access, phishing, and spam, acting like a shield for the inbox.

Sender Policy Framework (SPF)

It is an email authentication protocol designed to combat email spoofing;
a tactic commonly used in phishing attacks.

- It acts as a whitelist for email senders.
- The domain owner of an email address publishes an SPF record in their domain name system (DNS).
- The record specifies which email servers are authorized to send emails on behalf of the domain.

SPF: Working

SPF record setup

The domain owner publishes an SPF record in the DNS, listing the authorized mail servers allowed to send emails for that domain.

Email received

When an email arrives, the receiving mail server checks the SPF record of the sender's domain.

SPF check

The mail server compares the IP address of the sender with the authorized servers listed in the SPF record.

Not a match

Match

SPF fail

If there is no match, the email might be flagged as suspicious, though SPF results alone do not necessarily mean spam.

SPF pass

If the sender's IP address matches an authorized server, the email is considered legitimate.

Domain Keys Identified Email (DKIM)

It is an email authentication protocol that works with SPF to enhance email security.

- It adds cryptographic verification to prevent tampering.
- It allows senders to digitally sign emails, and recipients' servers validate the signatures for authenticity.

DKIM Process

Digital signing

When an email is sent through a DKIM-enabled server, a digital signature is added using a cryptographic key pair: a private key on the sending server and a public key in the domain's DNS records.

Verification

When the receiving mail server gets a mail, it retrieves the sender's public key from the DNS record and uses it to verify the digital signature.

Authentication

If verification is successful, it means the signature matches the sender's domain, and the email is likely authentic, ensuring it originated from the claimed domain.

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

This is also an email authentication protocol that enhances email security.

- It works alongside SPF and DKIM to specify how mail servers should handle failed authentication.
- It empowers domain owners to take actions when authentication fails and instructs email receivers on handling unauthenticated messages.
- It acts as the final layer of defense in the email authentication trio, alongside SPF and DKIM.

DMARC: Working

1

SPF check

- The receiving mail server uses SPF to validate that the email is from the IP address listed in the DNS records of the sending domain.
- If the sending IP address is not listed, email fails this check.

2

DKIM check

- The receiving mail server uses DKIM to verify the email header's digital signature against the sender's public DNS key.
- If the signature does not match, the email fails this check.

DMARC: Working

3

DMARC policy retrieval: The receiving mail server retrieves the DMARC policy from the sender domain's DNS records, which specifies actions if SPF or DKIM checks fail.

4

Policy enforcement: Based on DMARC policy, the receiving mail server decides whether to deliver the email to recipient’s inbox, send it to spam folder, or reject it.

5

Reporting: DMARC allows the sender to specify an email address to receive the verification reports.

Secure/Multipurpose Internet Mail Extensions (S/MIME)

This is a widely used standard for securing email communication through digital signatures and encryption.

- **Encryption:** The recipient's public key encrypts the email content, making it unreadable to anyone without the corresponding private key.
- **Digital signatures:** It allows the digital signing of emails using a private key to create a unique signature attached to the email.

It utilizes a public-key cryptography system to achieve this.

Pretty Good Privacy (PGP)

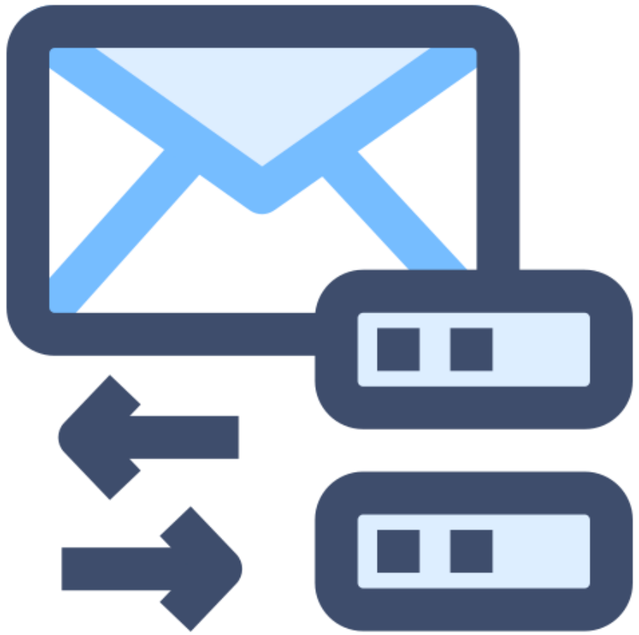
This is a software program that encrypts and decrypts emails, files, and even entire disk partitions.

- It offers versatile cryptographic privacy and authentication for various types of data.
- It revolves around a pair of keys: an openly shared public key and a closely guarded private key.
- It enables the sender to use the recipient's public key to send an encrypted message.
- It ensures that only the recipient with a corresponding private key can decrypt the message.
- It does not rely on PKI infrastructure.

Email Gateway

It acts as a security checkpoint for email communications, scanning all incoming and outgoing emails for potential threats.

- Serves as a crucial line of defense against various email threats, such as spam, malware, and phishing attacks
- Allows policies to be created based on attachments, malicious URLs, and content to prevent them from entering the mail server
- Uses data loss prevention to stop sensitive data and personally identifiable information (PII) from leaving the network via email



Quick Check

After a security breach exposes sensitive information through phishing emails, the IT security manager must prioritize actions to enhance email security and reduce future phishing risks. What actions should be taken?

A. Implement email filtering to block unknown senders and mark emails as spam

B. Conduct regular employee training on recognizing phishing attempts and safe email practices

C. Enforce monthly password changes to reduce unauthorized access

D. Disable email attachments by default to block potentially malicious files

Implementing Wi-Fi

Wireless Technologies

It is the fastest-growing area of network connectivity. The various types are given below:

Wireless standards

WLAN
operational modes

Spread-spectrum
technologies

Wireless Technologies: Components

Wireless network

- It is a computer network based on 802.11 standard, that uses wireless data connections between network nodes.
- It uses electrical waves to carry data from one node to another.

Wireless access point (WAP)

- It is a networking hardware device that allows a Wi-Fi device to connect to a wired network.
- It is also referred to as just access point (AP).

IEEE Wireless Standards

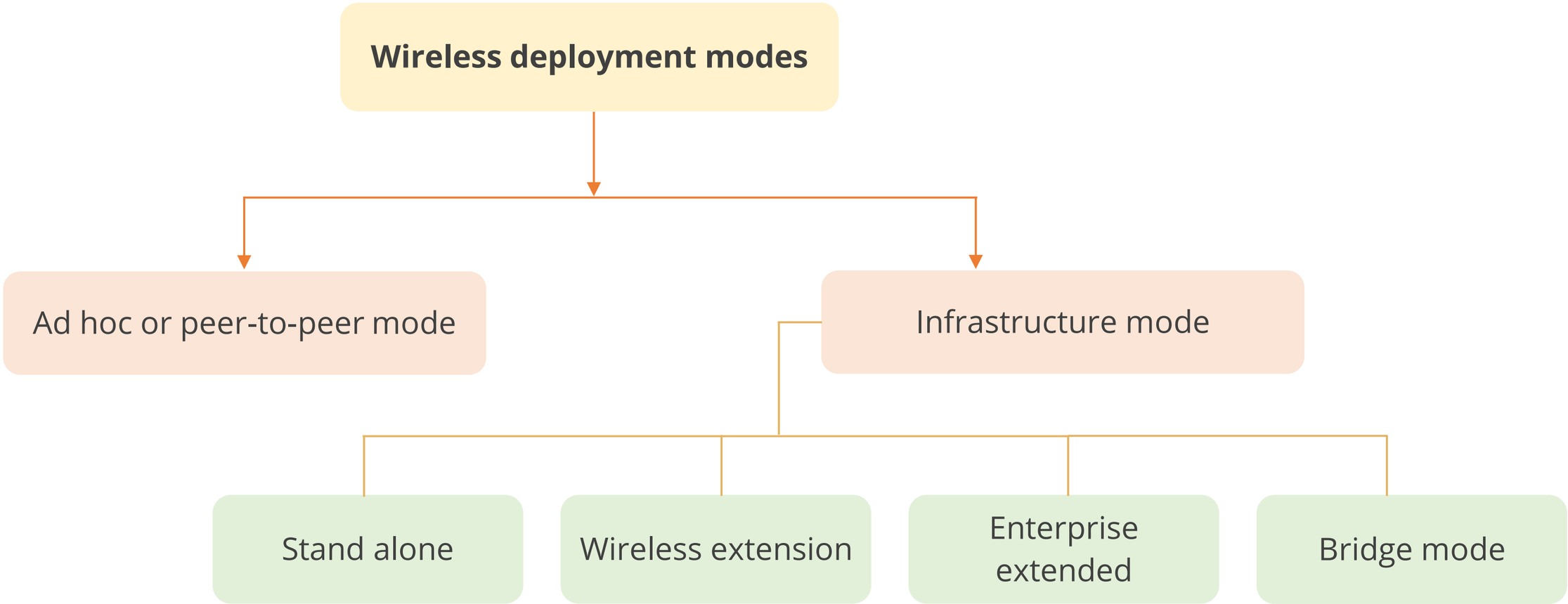
IEEE 802.11 refers to a family of specifications for WLANs developed by a working group of the IEEE.

It also generically refers to the IEEE committee responsible for setting various wireless LAN standards.

Wireless Standards

Standard	Year introduced	Band frequency	Maximum data transfer	Modulation
802.11a	1999	5 GHz	54 Mbps	DSSS, FHSS
802.11b	1999	2.4 GHz	11 Mbps	OFDM
802.11g	2003	2.4 GHz	54 Mbps	DSSS
802.11n	2009	2.4 and 5 GHz	600 Mbps	OFDM
802.11ac	2013	5 GHz	1.3 Gbps	MIMO-OFDM
802.11ax	2021	2.4, 5 (Wi-Fi 6), 6 GHz (Wi-Fi 6E)	10 Gbps	OFDMA, MU-MIMO

Wireless Deployment Modes



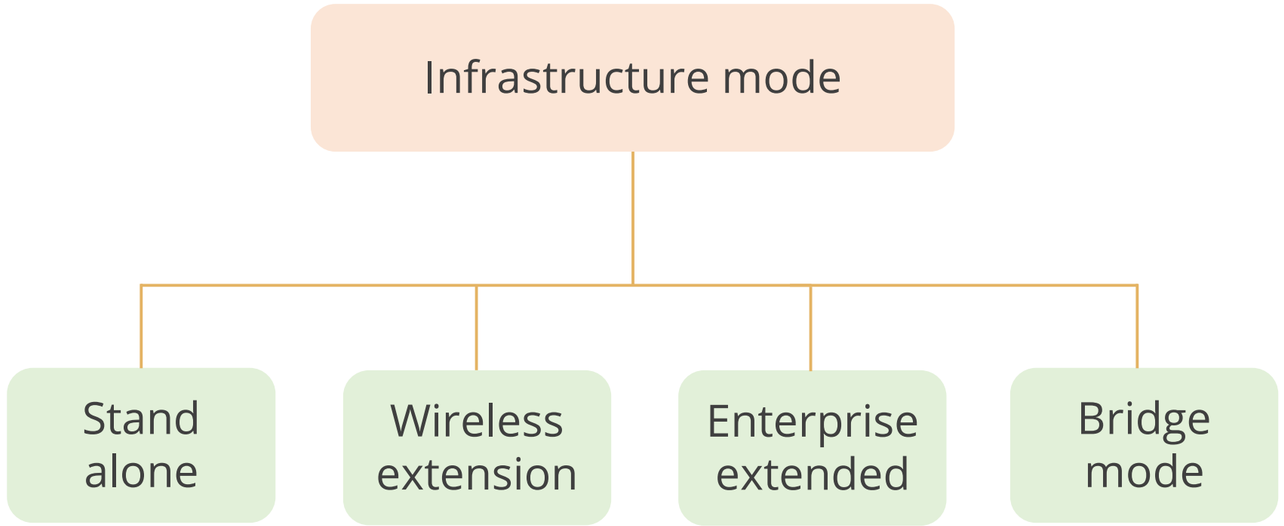
Wireless Deployment Modes: Ad Hoc Mode

It means that any two wireless networking devices, including two wireless network interface cards (NICs), can communicate without a centralized control authority.

This mode refers to a wireless network structure where devices can communicate directly with each other.

Wireless Deployment Modes: Infrastructure Mode

In this deployment mode:



- A wireless access point is required
- Wireless NICs on systems can’t interact directly
- Restrictions of the wireless access point for wireless network access are enforced

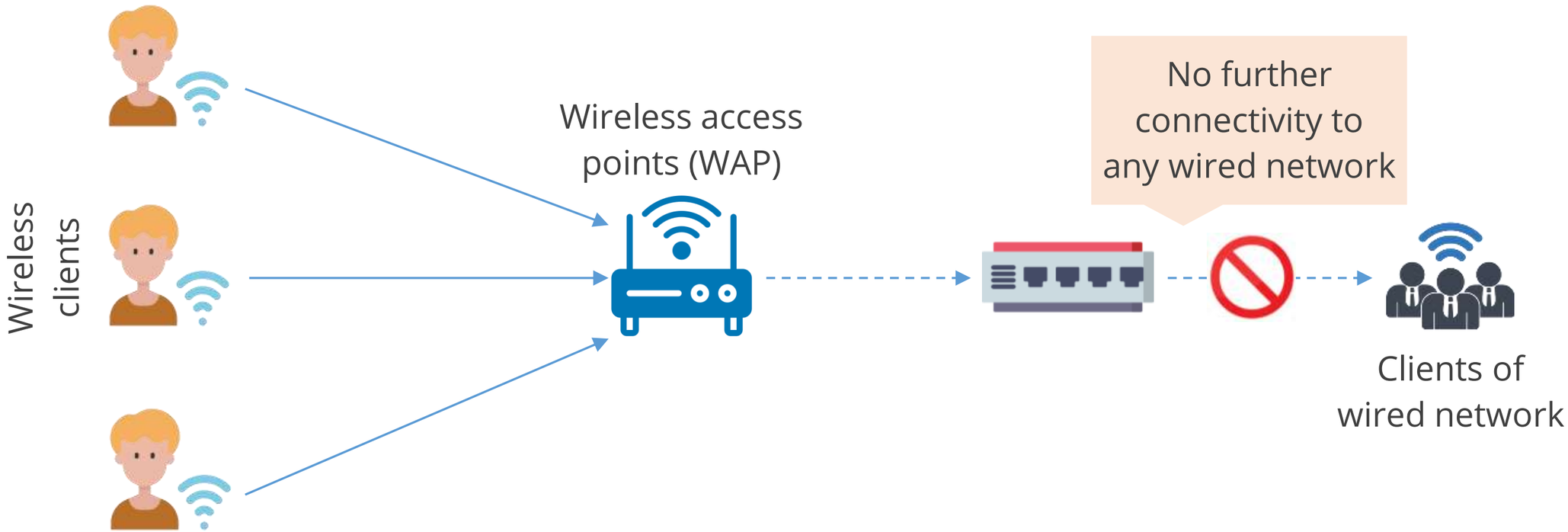
Infrastructure Mode: Stand-Alone

It occurs when there is a wireless access point connecting wireless clients to each other but not to any wired resources.

The wireless access point serves as a wireless hub exclusively.

Infrastructure Mode: Stand-Alone

A stand-alone infrastructure setup can be seen below:

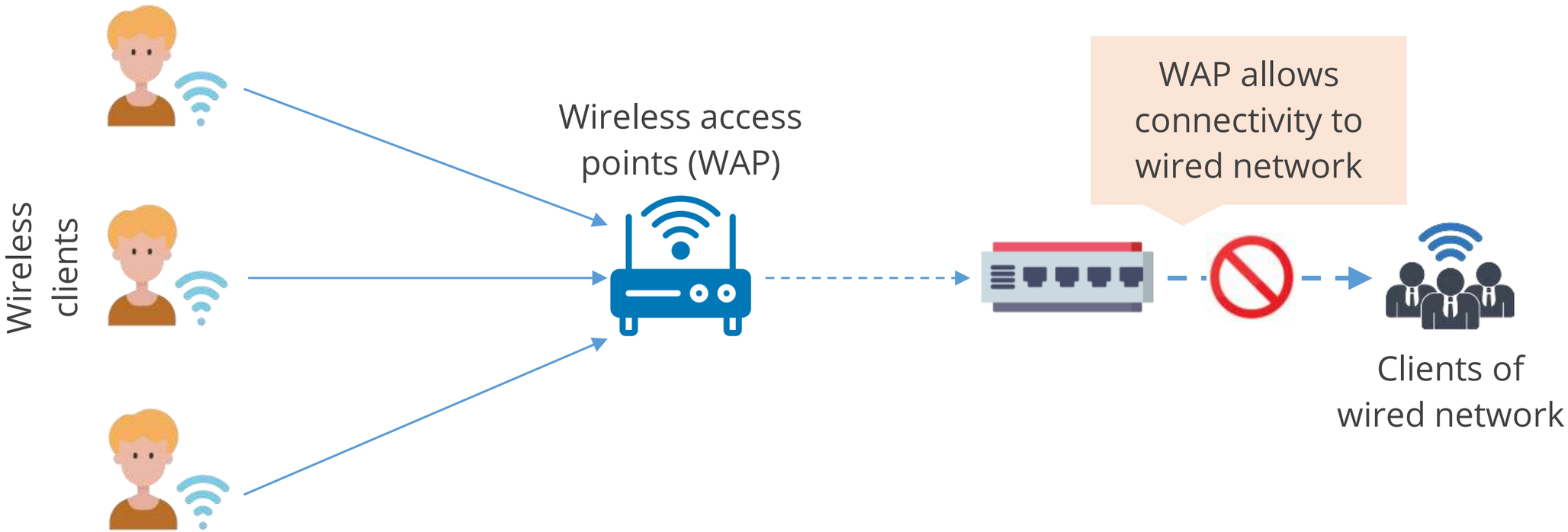


Infrastructure Mode: Wireless Extension

It occurs when the wireless access point acts as a connection point to link the wireless clients to the wired network.

Infrastructure Mode: Wireless Extension

A wireless extension infrastructure setup can be seen below:

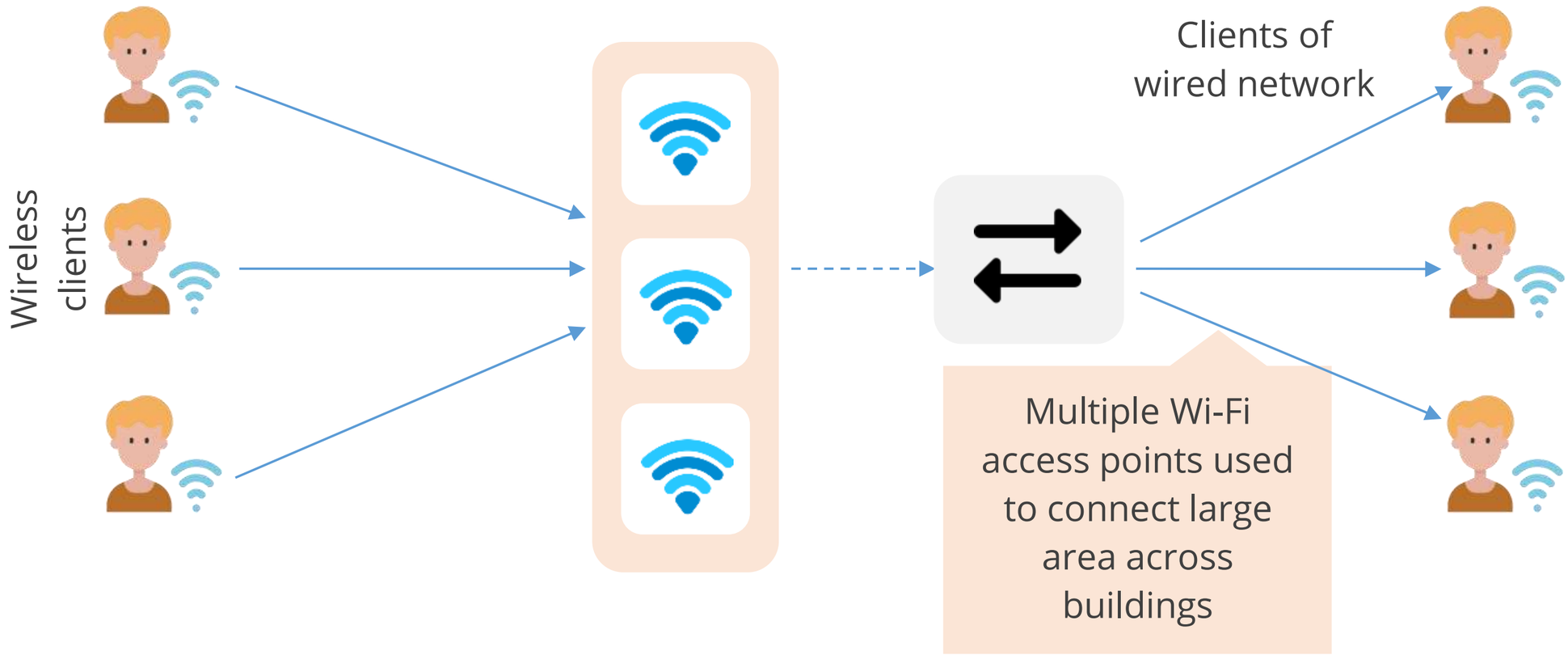


Infrastructure Mode: Enterprise Extended

It occurs when multiple wireless access points (WAPs) are used to connect a large physical area to the same wired network.

Infrastructure Mode: Enterprise Extended

An enterprise extended infrastructure setup can be seen below:



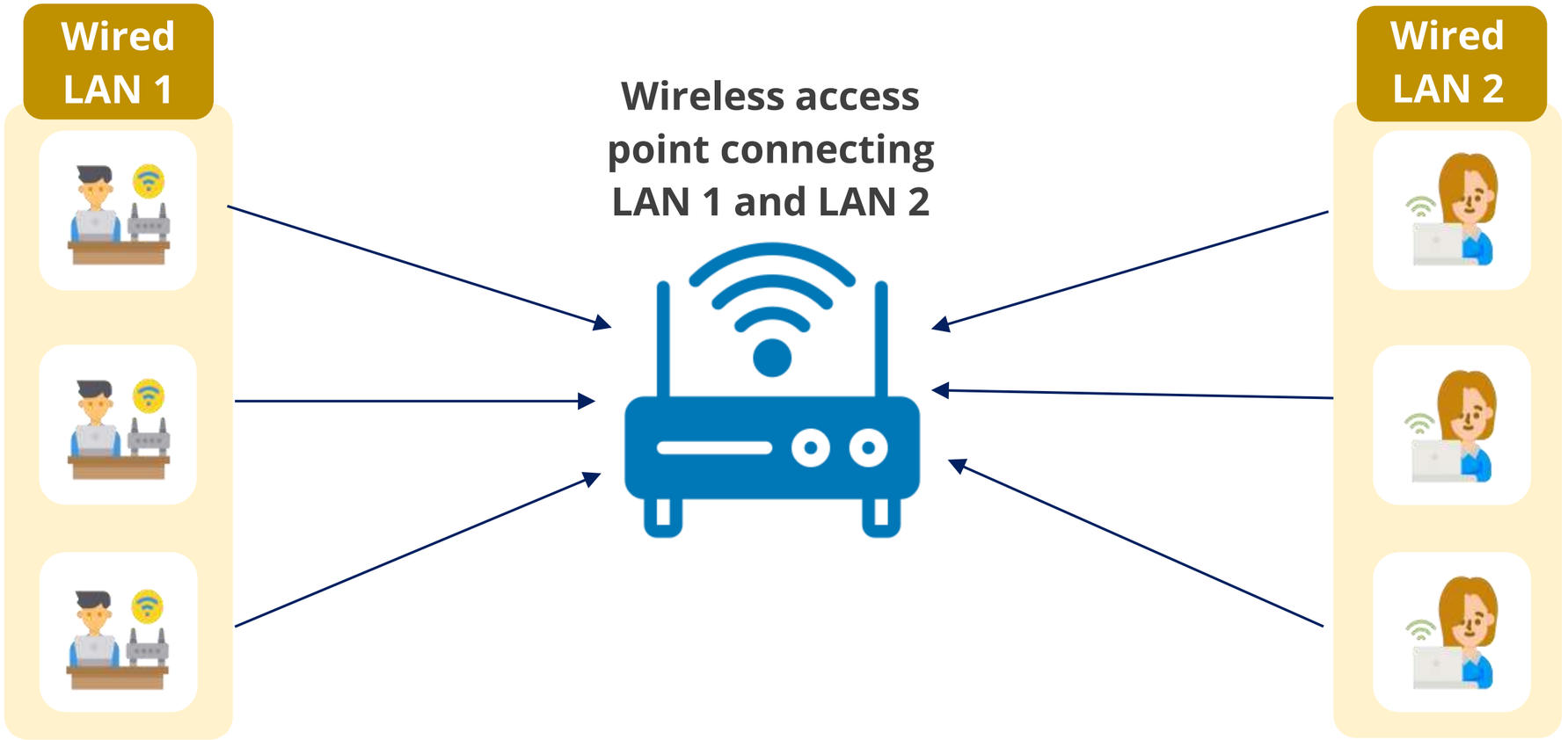
Infrastructure Mode: Bridge Mode

It often uses dedicated wireless bridges and is used when wired bridges are inconvenient, such as when linking networks between floors or buildings.

It is used when a wireless connection is needed to link two wired networks.

Infrastructure Mode: Bridge Mode

A bridge mode infrastructure setup can be seen below:



Service Set Identifier (SSID)

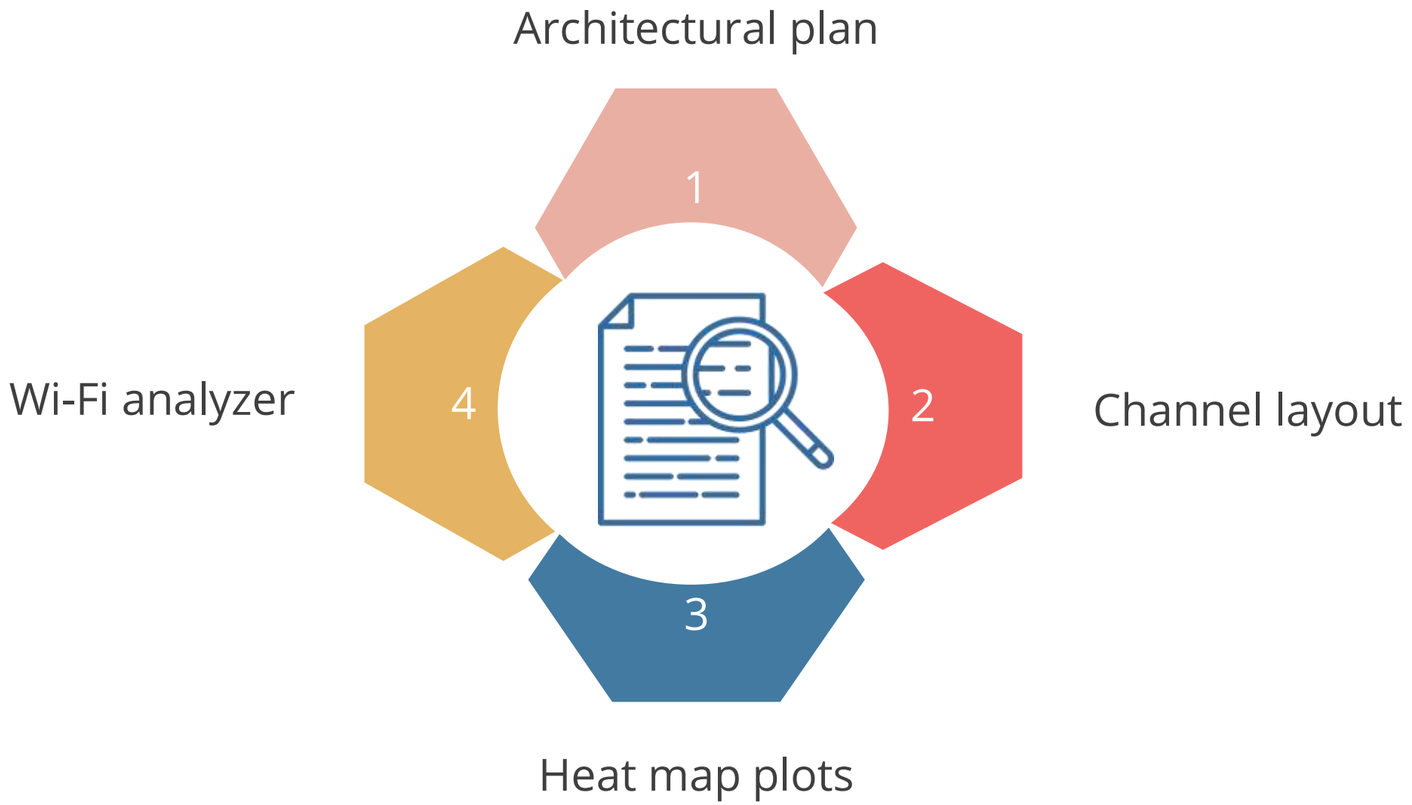
It’s a unique ID made up of case-sensitive letters, numbers, and special characters like dashes, periods, and spaces, used for uniquely identifying Wi-Fi networks.

According to the 802.11 wireless local area networks (WLAN) standard, an SSID can be as long as 32 characters.

Securing SSID

Wireless Network Installation Considerations

Site surveys and heat maps help with wireless network installation by giving the user an idea of:



Wireless Attacks

Evil twin

- It mimics a legitimate Wi-Fi access point to eavesdrop on wireless communications.
- It targets the wireless protocol using substitute hardware that appears as a stronger connection to users.

Rogue AP

- It is installed on a secure network without explicit authorization from the network administrator.
- It can be added by either a well-meaning employee or a malicious attacker.

Jamming

- It is a form of denial of service that specifically targets the radio spectrum aspect of wireless.
- It can manipulate things behind the scenes, enabling actions such as attachment to a rogue AP.

Wireless Attacks

Wi-Fi protected setup

- It exploits the simplified wireless network configuration.
- It can reveal the PIN, allowing unauthorized access to the network by obtaining the WPA/WPA2 passphrase.

Disassociation

- It disassociates a host from the network using the deauthentication frame in the IEEE 802.11 (Wi-Fi) standard.
- It allows anyone to exploit the deauthentication frame due to the protocol's design.

War driving

- It searches for wireless networks, typically from a moving vehicle using a laptop or smartphone.
- It involves driving slowly around an area to locate Wi-Fi signals, often with one person driving while others searching for networks.

Securing Wireless Network

The following methods can help secure wireless networks from unauthorized access and potential threats:

Use encryption

Use WPA2 authentication

Use antivirus, antispyware, and firewall

Turn off SSID broadcast

Use WPA3 authentication

Secure Encryption Protocol

These protocols are used to secure the data traveling over a wireless network.

Wired equivalency privacy (WEP)

- It is defined by the IEEE 802.11 standard and aims to prevent hackers from snooping on wireless data between clients and access points.
- It utilizes a static shared secret key of 40 bits that is common to all wireless access points and devices.
- It uses the RC4 algorithm for encryption to secure wireless communications.

Wi-Fi protected access (WPA)

- It improves on WEP by using unique keys for each host instead of a static key for all communications.
- It employs a single passphrase to authorize association with the base station, which, if too short, can be easily guessed.
- A passphrase of 14 characters or more is generally recommended for better security.

Secure Encryption Protocol

WPA2 or 802.11i

- It is a new method for securing wireless networks that is still considered secure.
- It introduces a new encryption scheme called Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), based on AES encryption.
- It facilitates seamless roaming, allowing clients to move between access points on the same Wi-Fi network without needing to reauthenticate.

WPA 3

- It standardizes a 128-bit cryptographic suite and disallows obsolete security protocols.
- It employs CCMP-128 and AES-128 for encryption.
- It uses Simultaneous Authentication of Equals (SAE), where each device transmits its authentication credentials in a one-off message, eliminating the reuse of encryption keys and requiring a new code for every interaction.

Spread Spectrum Technology

It is a technique used in wireless telecommunications to spread a signal across a wider bandwidth than the minimum necessary to transmit it. It helps in:

- Securing communications
- Increasing resistance to interference, noise, and jamming
- Improving communication performance
- Enhancing security and spectrum utilization

Spread-Spectrum Technologies

The two different spread spectrum technologies for 2.4 GHz wireless LANs are:

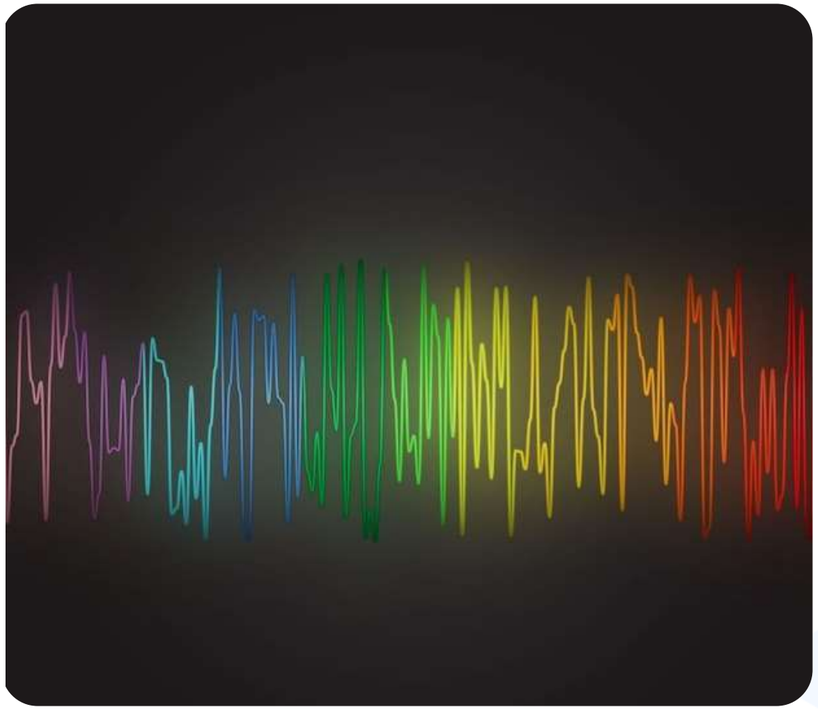
Frequency-Hopping Spread Spectrum (FHSS)

Direct Sequence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS)

It is a telecommunications technique that enhances wireless communication security and reliability by rapidly switching carrier frequencies at specific intervals.

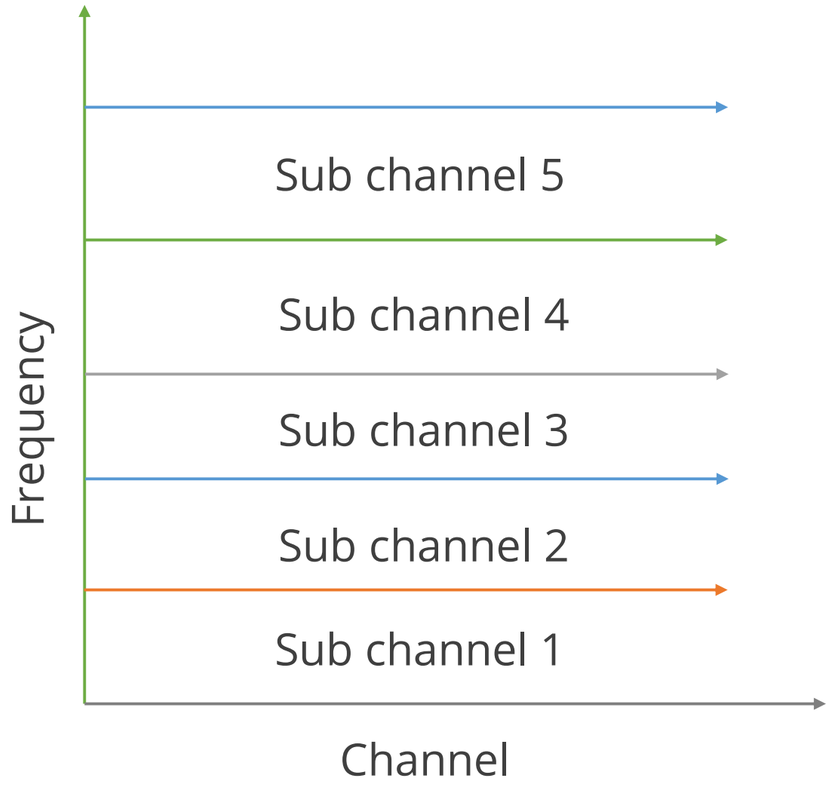
- Bandwidth is divided into smaller subchannels.
- The sender and receiver operate on one subchannel for a set time, then switch.
- The sender transmits data on different frequencies sequentially.
- The FHSS algorithm defines the frequencies and hop sequence.
- The sender and receiver hop between frequencies based on this sequence.
- Multiple sender-receiver pairs can use the same frequencies with unique hop sequences.



Frequency Hopping Spread Spectrum (FHSS)

Examples

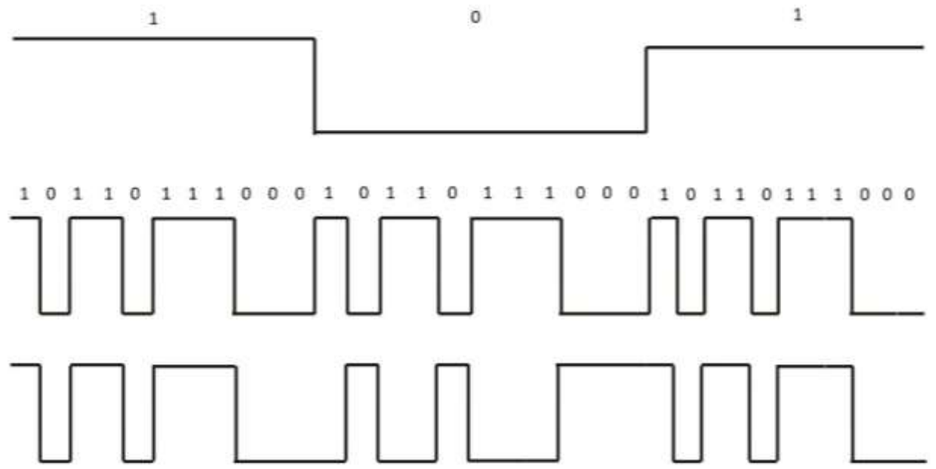
- Susan and a user share a hop sequence of 1, 5, 3, 2, 4.
- Nicole and Ed have a sequence of 4, 2, 5, 1, 3.
- Susan sends her first message on frequency 1, while Nicole sends hers on frequency 4 simultaneously.
- Susan's subsequent messages are sent on frequencies 5, then 3, and so on.
- The user’s device listens on frequency 1 for half a second, then switches to frequency 5, continuing this pattern
- This process continues until all pieces of data reach the device.



Direct Sequence Spread Spectrum

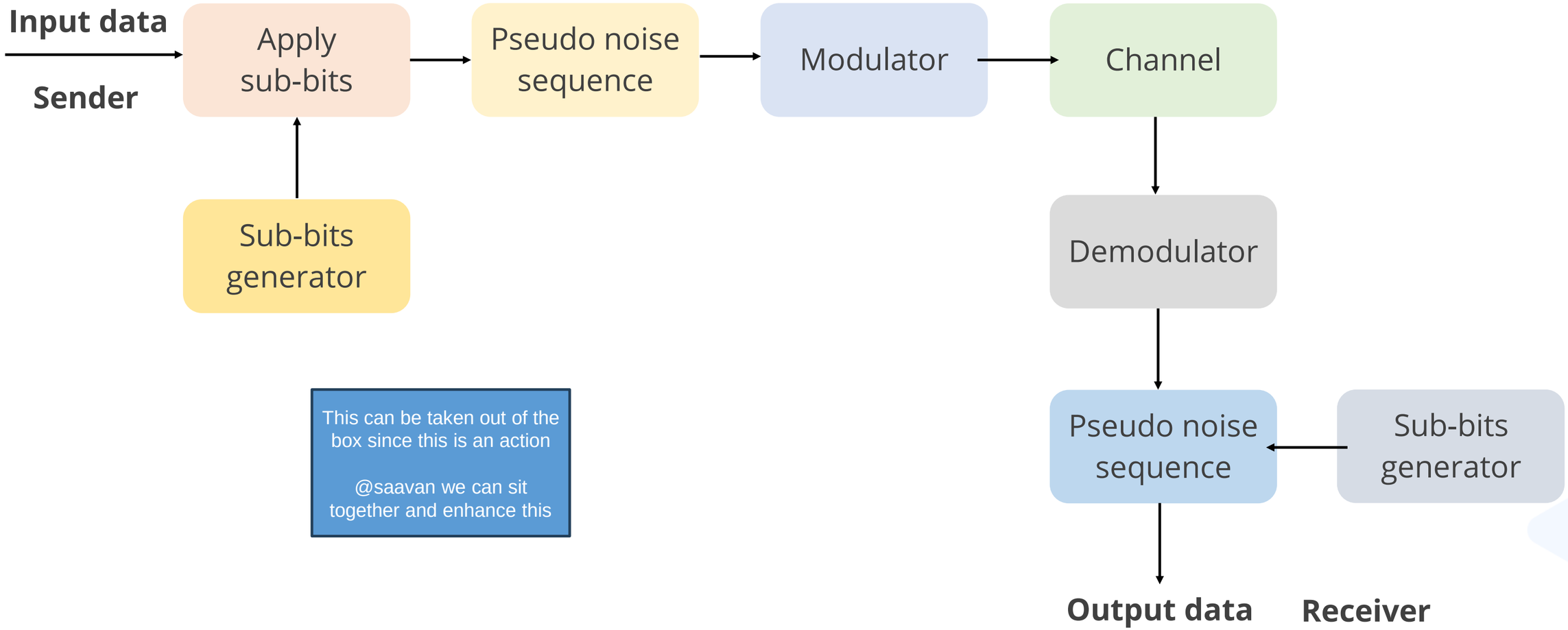
It works by applying sub-bits to a message.

- The sending system uses sub-bits to generate a different data format before transmission.
- The receiving end uses these sub-bits to reassemble the signal into the original format.
- The sub-bits are called chips, and their application sequence is the chipping code.
- When the sender’s data is combined with the chip, the signal appears as random noise to anyone unaware of the chipping sequence.
- This sequence is sometimes referred to as a pseudo-noise sequence.



Direct Sequence Spread Spectrum

The working of a DSSS can be seen below:



This can be taken out of the box since this is an action

@saavan we can sit together and enhance this

FHSS vs. DSSS

FHSS Spectrum	DSSS Spectrum
Moves data by changing frequencies	Applies sub-bits to a message
Uses a narrow band carrier that frequently changes across a wide band, utilizing only a portion of the total bandwidth at any given time	Utilizes all available frequencies, continuously employs the full bandwidth, and spreads signals across a wider frequency range
Sends data across different frequencies one by one and has a lower data throughput than DSSS	Sends data across all frequencies at once and has a higher data throughput than FHSS
Uses 802.11 standard that provides a data throughput of only one to two Mbps with FHSS	Uses 802.11b standard that provides a data throughput of up to 11 Mbps with DSSS

Bluetooth

- It is a short-range wireless communications technology.
- It uses radio waves for communication.
- It is based on a low-cost, low-power, short-range radio link.
- Its speed is 2.4 GHZ and range is between 10 to 98 feet.

Bluetooth Attacks

Blue jacking

- It is an attack in which someone sends unsolicited messages to a Bluetooth-enabled device.
- It requires the target to be within the Bluetooth range for the attack to work.
- It lets hackers send unsolicited data to phones.

Blue snarfing

- It lets hackers access a wireless device through a Bluetooth connection.
- It occurs without the user's permission and often leads to information theft or device damage.
- It allows hackers to steal data with the help of a Bluetooth connection.

Blue bugging

- It allows individuals to access a device with a discoverable Bluetooth connection.
- It lets an attacker take full control of the device once it accesses a rigged link.
- It allows hackers to read and send messages, access the victim’s phonebook, and eavesdrop on calls.

Bluetooth Attacks: Countermeasures

01 Use Bluetooth for those activities that are not sensitive or confidential.

02 Change the default PINs on the devices.

03 Do not leave devices in discovery mode.

04 Turn off Bluetooth when it’s not in active use

Radio Frequency Identification (RFID)

It is the use of radio waves to read and capture information stored on a tag attached to an object.

A tag can be read from up to several feet away and does not need to be within direct line-of-sight of the reader to be tracked.

RFID: Risks

While it provides numerous benefits, it also introduces security risks, including data theft, misuse of information, and potential breaches.

The following are some of the key risks:

- **Unauthorized access:** Refers to intruders gaining access to sensitive data
- **Data privacy concerns:** Involves the exposure of personal or confidential information
- **Supply chain vulnerabilities:** Indicates that RFID tags may be tampered with or replaced
- **Physical interference:** Occurs when jamming devices disrupt RFID signals
- **Electronic pickpocketing:** Happens when RFID devices are read without physical contact

RFID Controls

Management controls

Management oversight

Examples

Policies

Operational controls

Admin and user control

Examples

Physical controls

Technical controls

Technology-based usage monitoring

Examples

Access control monitoring

Cellular Network

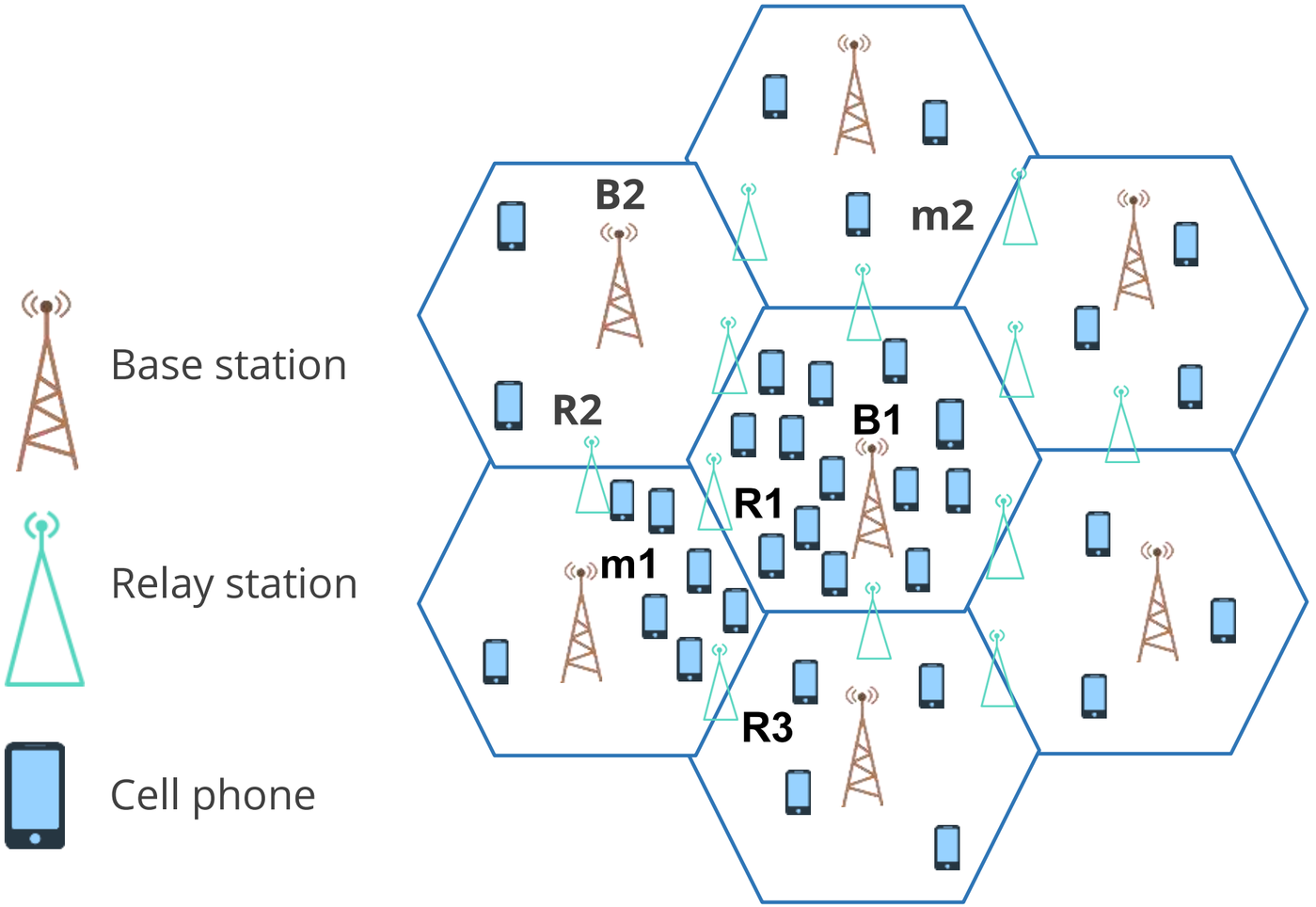
It is a radio network distributed over land areas called cells.

Each cell is served by at least one fixed-location transceiver known as a cell site or base station.

It uses a different set of frequencies from neighboring cells to avoid interference and provides guaranteed bandwidth within each cell.

Cellular Network

A topology of a cellular network is shown below:



Source: https://arxiv.org/pdf/1406.5258.pdf

Cellular Wireless Technologies

Generation	1G	2G	3G	4G	5G
Launch	1979	1991	2001	2009	2019
Technology	Analog	GSM	WCDMA	LTE, WiMAX	SDN
Switching	Circuit	Circuit, packet	Packet	All packet	All packet
Data rate	14.4 Kbps	64 Kbps	2 Mbps	100-300 Mbps	1-10 Gbps
Purpose	Voice calls	SMS, MMS	Video calls	HD video, web conferencing	IoT

Quick Check

You are setting up a new wireless network for your office and need to ensure that it complies with the standard wireless LAN specifications. Which of the following specifications should you use?

A. IEEE 802.3

B. IEEE 802.7

C. IEEE 802.11

D. IEEE 802.15

Implementing Mobile Device Management

Mobile Devices

Mobile devices such as cell phones, tablets, and computers have become a dominant part of everyday life.

- These devices store information such as contact list, passwords, emails, and texts.
- Attacks on these mobile devices can take private information such as bank information, login information, and other data.

Mobile Device Security

It protects data from security threats that can lead to data breaches, unauthorized access to sensitive data, and even data loss.

Security breaches can happen due to user error or a stolen or misplaced device.

Mobile Device Connection Method

Cellular	• It uses mobile telephony circuits, today typically fourth-generation (4G) or LTE (long term evolution) in nature, although some 3G services still exist. • Its key strength is its robust nationwide coverage, providing strong signals almost anywhere with reasonable population density.
Wi-Fi	• It is the radio communication method developed under the Wi-Fi alliance. • These systems exist on 2.4- and 5-GHz frequency spectrums and networks are constructed by the concerned enterprise as well as third parties.
Satellite Communication	• It uses terrestrial transmitters and receivers and satellites in orbit to transfer the signals. • It is expensive, and for high-density urban areas, both cost and line-of-sight issues make this a more expensive option.

Mobile Device Deployment Models

They explain the process of how the employees are supplied with mobile devices and applications. It can be:

01 Corporate owned, business only (COBO)

02 Choose your own device (CYOD)

03 Virtual desktop infrastructure (VDI)

04 Corporate owned, personally-enabled (COPE)

05 Bring your own device (BYOD)

Mobile Device Deployment Models

Bring your own device (BYOD)	It refers to employees using personal devices to connect to their organizational networks to access work-related systems and potentially sensitive or confidential data.
Corporate owned business only (COBO)	It is the corporate-owned deployment model where the company supplies employees with a mobile device that is restricted to company-only use.
Corporate owned, personally-enabled (COPE)	It is the model where employees are supplied a mobile device that is chosen and paid for by the organization, but they are given permission to use it for personal activities.

Mobile Device Deployment Models

Choose your own device	It allows people to select the mobile devices they would like to use, typically from a limited number of options.
Virtual desktop infrastructure	It brings control to the mobile environment associated with non-corporate-owned equipment.

Enterprise Mobility Management (EMM)

It is a class of management software that applies security policies to the use of mobile devices and applications in the enterprise.

It helps in visibility over use and configuration.

It helps in managing enterprise-owned devices and BYOD.

Enterprise Mobility Management (EMM)

It is a centralized platform for managing and securing mobile devices within an organization, providing a centralized approach to control, monitor, and protect their applications and data.

The main functions of an EMM product site are as follows:

Mobile Device Management (MDM)

- Involved in network enrollment
- Helps in managing device functions

Mobile Application Management (MAM)

Involved in installing and monitoring of corporate apps and data

Unified Endpoint Management (UEM)

Aims for visibility across PC, laptop, smartphone, tablet, and even IoT devices

Mobile Device Management (MDM)

It is the technology used in managing mobile devices that are used in organizations to access sensitive business data.

It includes:

- Storing essential information about mobile devices
- Deciding which applications can be present on the devices
- Locating devices
- Securing devices if lost or stolen

MDM Policy Controls

It implements the following controls:

1. Device locking with a strong password
2. Device locking automatically after a certain period of inactivity
3. Locking the device remotely if lost or stolen
4. Encrypting data on the device
5. Wiping device automatically after a certain number of failed login attempts
6. Managing applications

Mobile Access Control Systems

The following authentications control mobile access, ensuring the security and privacy of a smartphone:

Password

Pin

Swipe pattern

Biometric

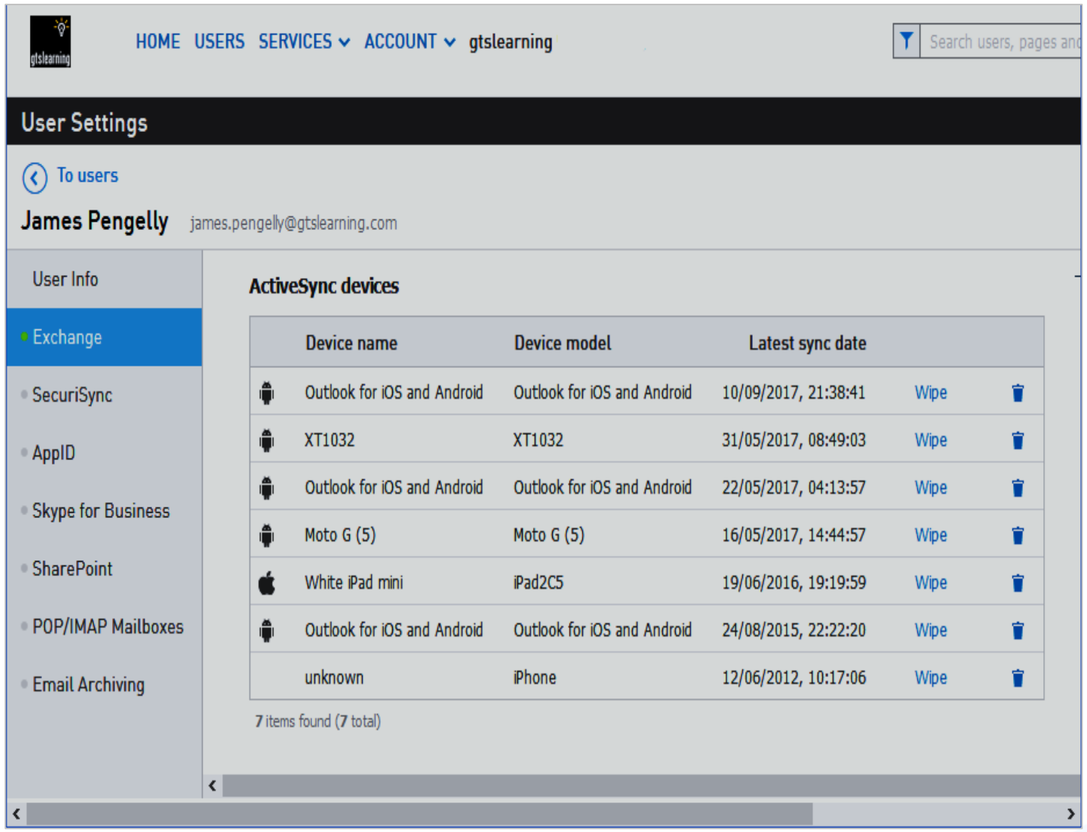
Context-aware authentication helps a user unlock the smartphone in case of password loss.

Remote Wipe

It sets the device to factory defaults or clears storage in case the smartphone gets stolen.

- It is initiated from the enterprise management software.
- It is triggered when the thief enters the wrong password multiple times.

The thief might be able to keep the device away from receiving the wipe command.



The screenshot here shows the corporate messaging service by Intermedia.

Full Device Encryption of Mobile Device

It is a security feature that encrypts all data stored on a device, making it unreadable unless a correct decryption key is used. The various levels of encryption in an iOS device are:

Secure erase encryption

The OS deletes the key to make the data inaccessible rather than wiping each storage location.

Data protection

It is used as a second round of encryption using a key derived from and protected by the user's credential.

Full Device Encryption of Mobile Device

Encryption on an Android device depends on the version of software installed on the device.

- By default, user data is encrypted at file-level from Android version 10.
- External storage devices are used to extend device storage capacity.
- MicroSD HSM is a small device designed to store extra essentials.

Location Service

It uses network attributes to help a user determine the physical position of a device when it is lost.

Global positioning system (GPS)

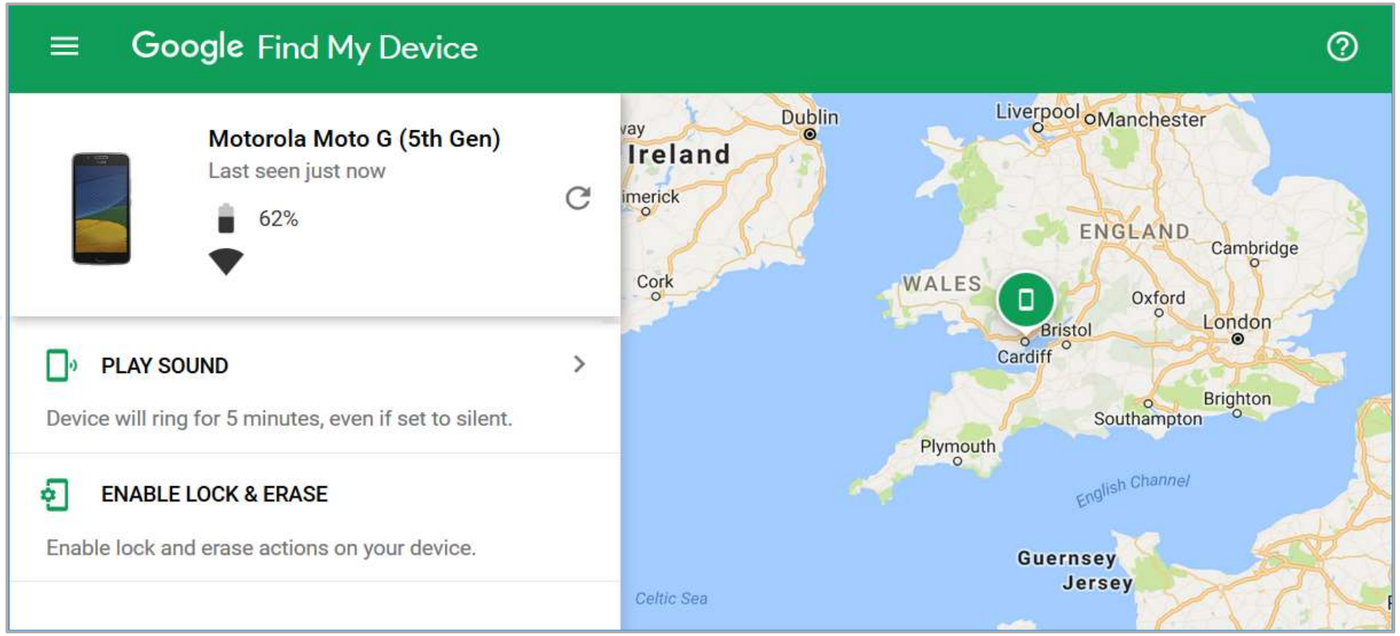
It makes use of two location systems:

Indoor positioning system (IPS)

Geofencing

It applies location-based policies automatically and helps disable on-board cameras or video through MDM or EMM controls, creating a virtual boundary.

Using **Find My Device** to locate an Android smartphone



GPS Tagging

It is the process of including the geographical identification metadata in a device.

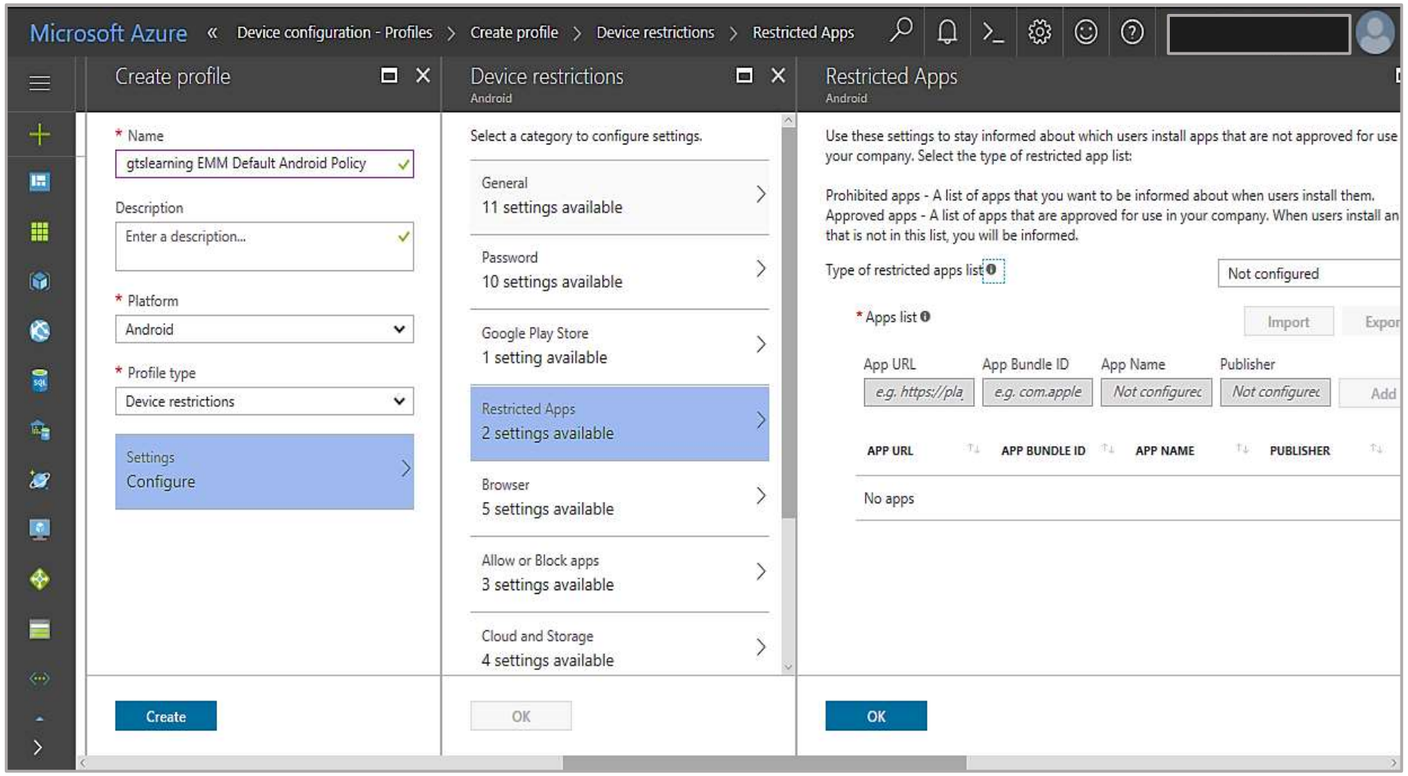
GPS data is highly sensitive and therefore it is a risk to personal information.

It helps in tracking the movements of a person and assists social engineering.

MDM prevents GPS tagging by controlling device configurations, restricting app access to GPS data, encrypting information, and enforcing compliance policies

Application Management

MDM or EMM use policies to provide better management of applications on a device.



Android allows third-party application stores to install untrusted applications into a device with the user's consent, known as **sideloading**.

Content Management

It helps resolve data ownership and privacy issues when privately owned corporate devices are used for any other tasks. It uses containerization to:

Set up a corporate workspace separated from the employee’s private applications and data

Enforce storage segmentation to ensure separation of data

Implement content management or DLP policies

Risks to Mobile Security

They involve subverting the security measures on the device, posing a risk for enterprise management agents.

Rooting

- It allows users to gain access to the root account on Android devices.
- It uses custom firmware or ROM.

Jailbreaking

- It allows access to root account on iOS devices.
- It is accomplished by restarting the device with a patched kernel.

Carrier unlocking

- It removes restrictions that tie a device to a single carrier.
- It is usually done in both iOS and Android.

Implementing Secure Network Designs

Network Infrastructure

It refers to hardware and software resources that facilitate network connectivity, communication, operations, and management within an enterprise network.

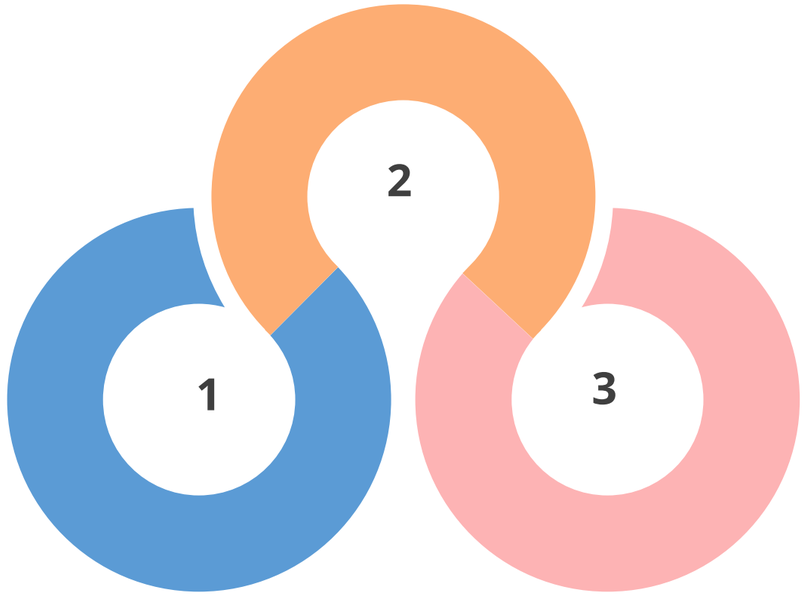
It comprises networking devices, protocols, and routing mechanisms that function together in an interconnected environment.

Secure network design involves implementing security measures to protect the network against unauthorized access, cyberattacks, and data breaches.

Secure Network Design

It provisions the assets and services underpinning business workflows with the properties of:

Integrity

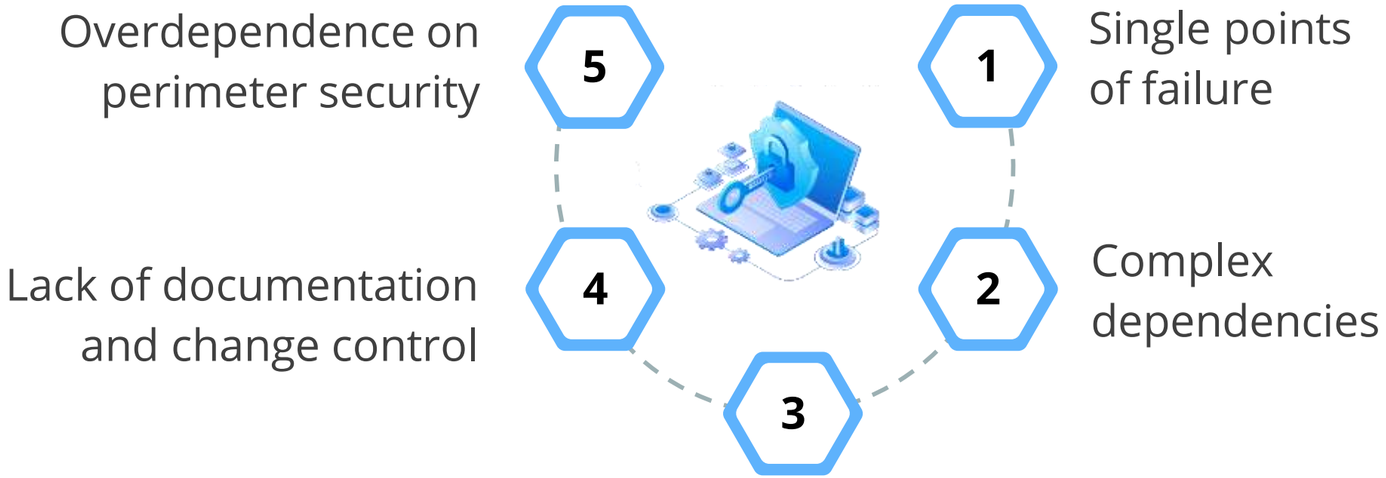


Confidentiality

Availability

Weak Network Design

It makes the network more susceptible to undetected intrusions or catastrophic service failures. Typical weaknesses include:

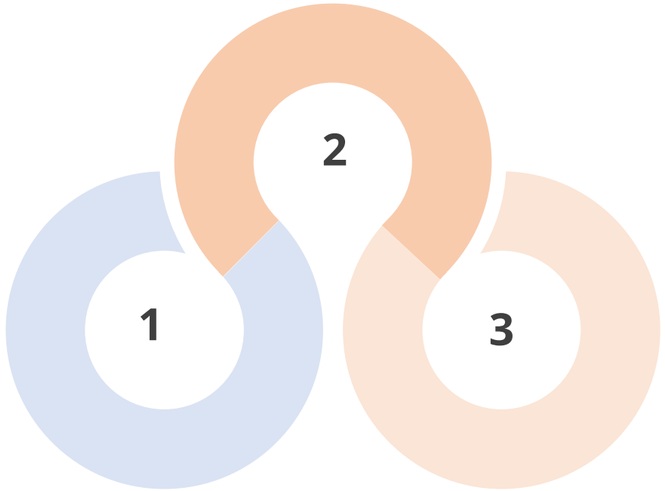


Refer to Cisco’s SAFE Architecture for best practice design and architecture guides

Network Architecture

It is designed to support the following business workflows:

Email mailbox server

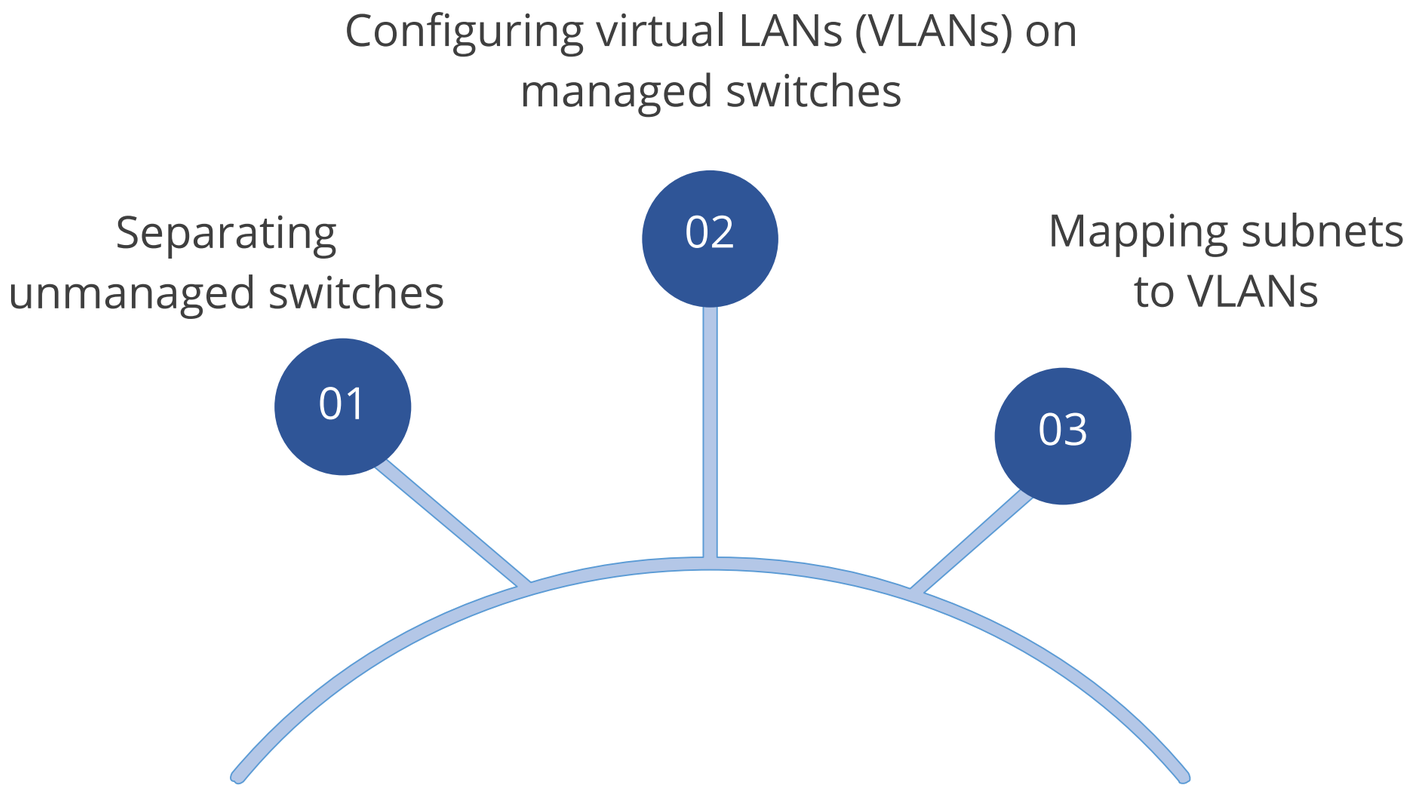


Access

Mail transfer server

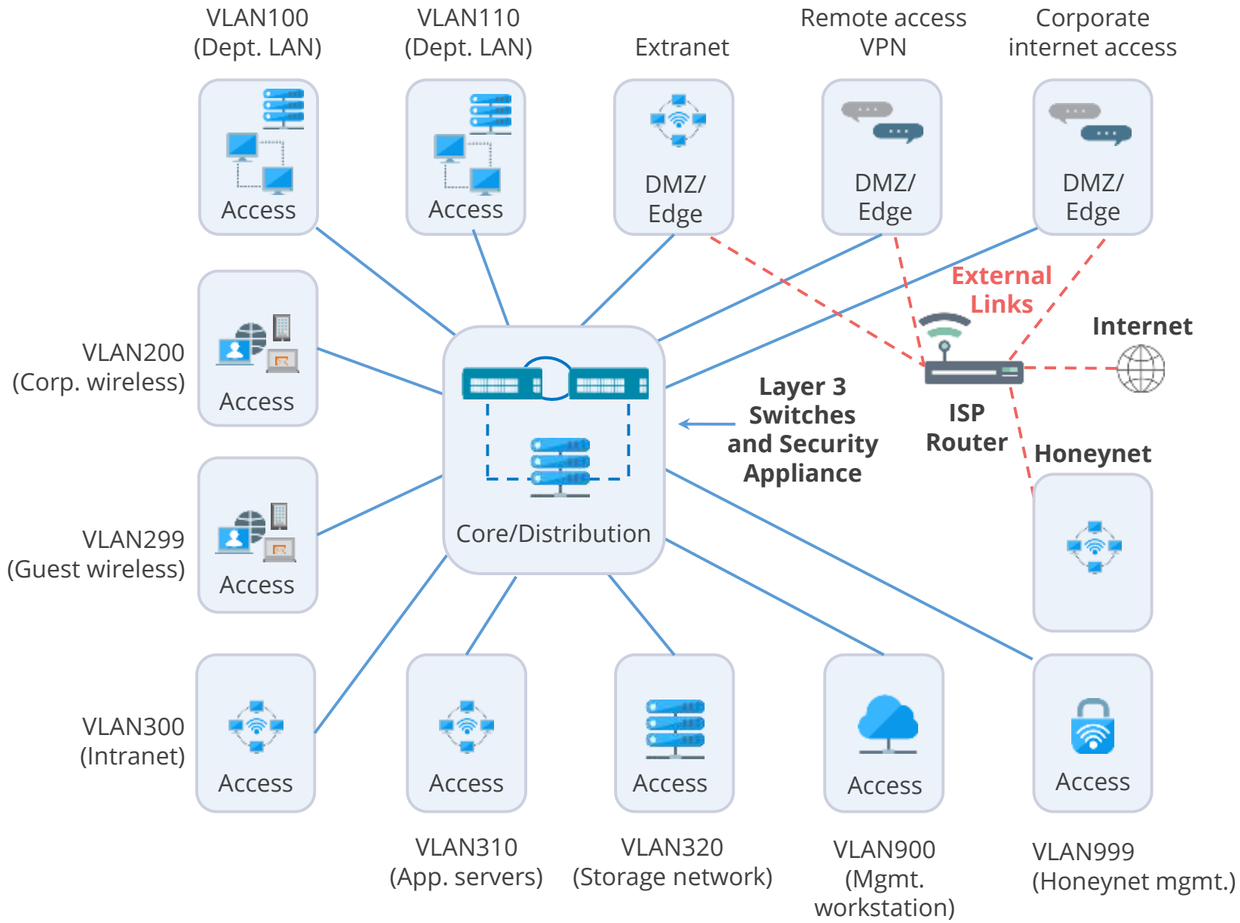
Network Segmentation

It allows all the hosts attached to the segment to use layer 2 forwarding to communicate freely with one another. It is implemented by:



Network Topology and Zones

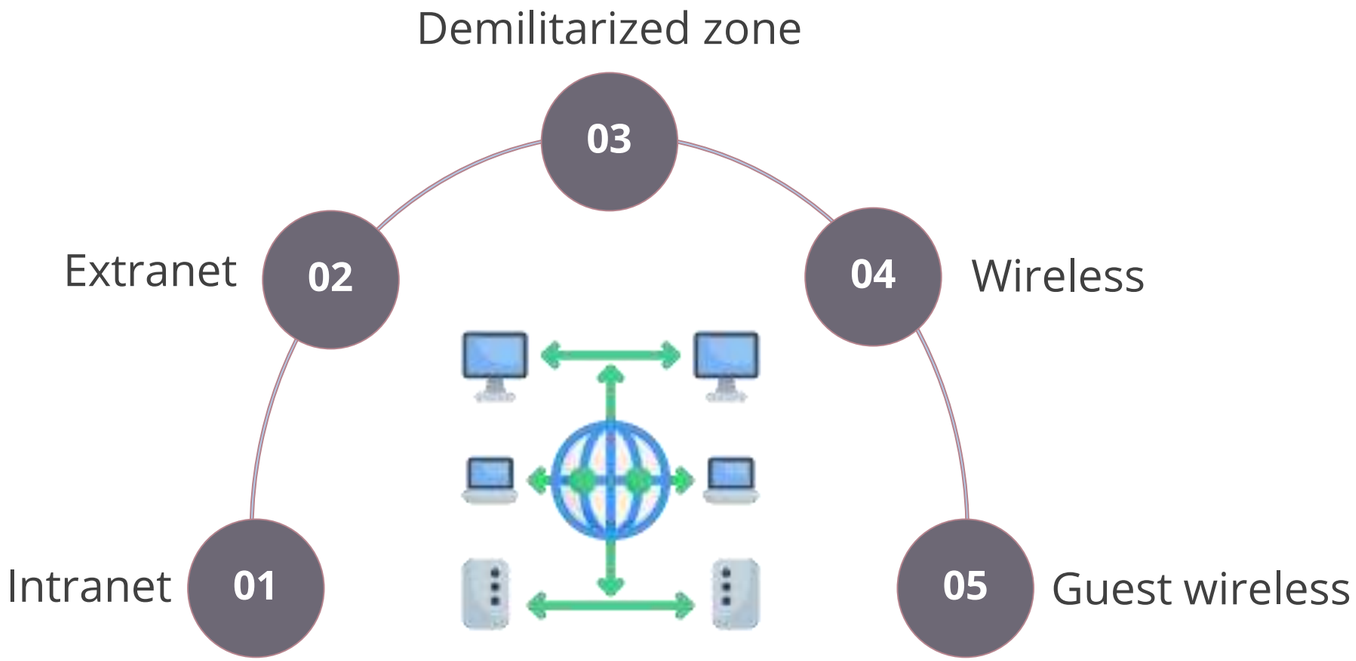
A topology is a description of how a computer network is physically or logically organized.



A zone is an area of the network where the security configuration is the same for all hosts within it.

Types of Network Zone

It divides a campus network or data center into zones with each zone having a different security configuration. The main zones are as follows:



Intranet

It is a network that offers the same functionality as the internet for users but operates entirely within a trusted area, controlled and secured by system and network administrators.

- It is referred to as campus or corporate networks and is used every day in companies around the world.
- It makes the content on the intranet web servers unavailable over the internet to untrusted users.

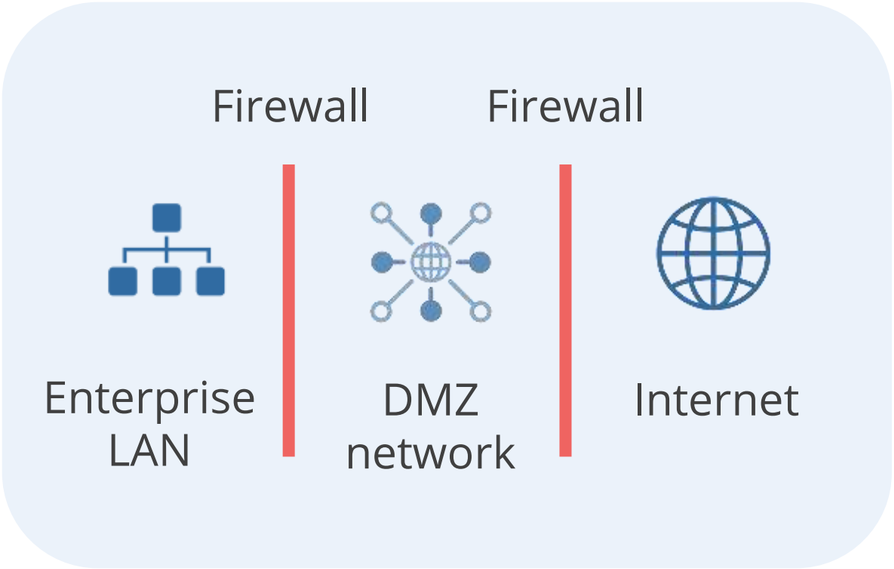
Extranet

It is an extension of a selected portion of a company’s intranet to external partners such as customers, suppliers, and other trusted groups.

- It shares the information using a common set of internet protocols to facilitate operations.
- It uses public networks to extend the reach beyond a company’s own internal network, using some form of security, typically a VPN.

Demilitarized Zones (DMZs)

It is a network security buffer zone between a trusted internal network and an untrusted external network, protecting it from unauthorized access and potential attacks.



01 Internet-facing hosts are placed in one or more DMZs, also known as perimeter or edge networks.

02 Traffic cannot pass directly through DMZ.

03 When communication between hosts on either side of a DMZ is required, a host within the DMZ acts as a proxy.

Types of Demilitarized Zones (DMZs)

Different types of DMZ are used for different functions.

01

Proxy DMZ

02

Communication DMZ

03

VPN DMZ

04

Cloud applications DMZ

05

Multi-tier DMZ

Wireless Network

It is the transmission of packetized data by means of a physical topology that does not use direct physical links.

- It should have separate zones where access to the internal zone can be controlled through MAC filtering.
- It should be configured to accept connections only from specific MAC addresses.

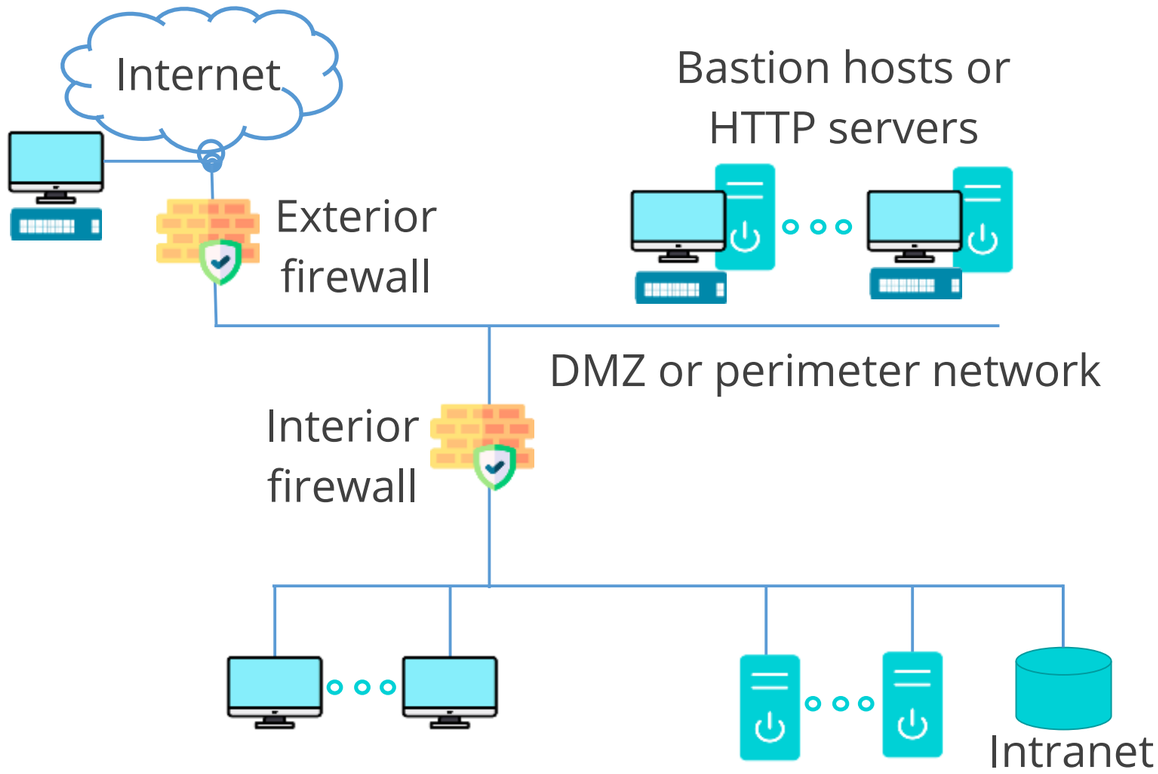
Guest Wireless

It is a separate network within an organization that provides internet access to authorized individuals without compromising the security of the main corporate network.

- It must be separated from the internal network using a wireless firewall, as MAC address authentication is ineffective for guests.
- Guest users should only access the internet gateway for web browsing and email.
- It uses captive portals, especially in businesses like hotels and restaurants, offering free Wi-Fi.
- Captive portals can require user authentication, facilitate payments, or display policies and agreements.

Bastion Host

It runs minimal services to reduce the attack surface on a network.



It is not configured with any data that could be a security risk to the internal network, such as user account credentials.

Segregation and Isolation

They are some of the most effective controls an organization can implement to mitigate the effect of a network intrusion.

If properly implemented, these controls are a preventative measure to protect sensitive information.

Types of Segregation

Physical separation

- Has separate physical equipment to manage different classes of traffic, including distinct switches, routers, and cables
- Offers the most secure method of traffic separation, but is also expensive
- Maintains separate physical paths in the outer sections of the network where internet connections are established

Virtualization

- Offers server isolation logically while still enabling physical hosting
- Allows running multiple servers on a single piece of hardware, utilizing more powerful machines in the enterprise
- Provides a certain level of isolation from the underlying hardware by operating through a hypervisor layer

Types of Segregation

Airgaps

- Refers to the physical separation between networks or systems to prevent unauthorized access or data transfer
- Isolates critical systems from external networks and reduces the risk of compromise
- Isolates a secure network or computer from all others, especially the internet, preventing unauthorized access

VLAN

- Enables port grouping on switches to limit traffic to specific group members
- Creates isolated broadcast domains and switches with multiple broadcast domains, similar to routers
- Aids in segmentation, reduces routing broadcasts and segregates department functions by logically segmenting the data

Micro-Segmentation

It is a network technique used to create distinct security zones in data centers and cloud environments to isolate workloads from one another.

Once workloads are isolated, security controls are defined to secure them individually.

Micro-Segmentation: Benefits

Reduces network attack surface

Limits attackers' movement from one potentially compromised workload to another

Improves breach containment

Blocks unsanctioned activities and drastically improves threat detection and response times with real-time alerts

Strengthens regulatory compliance

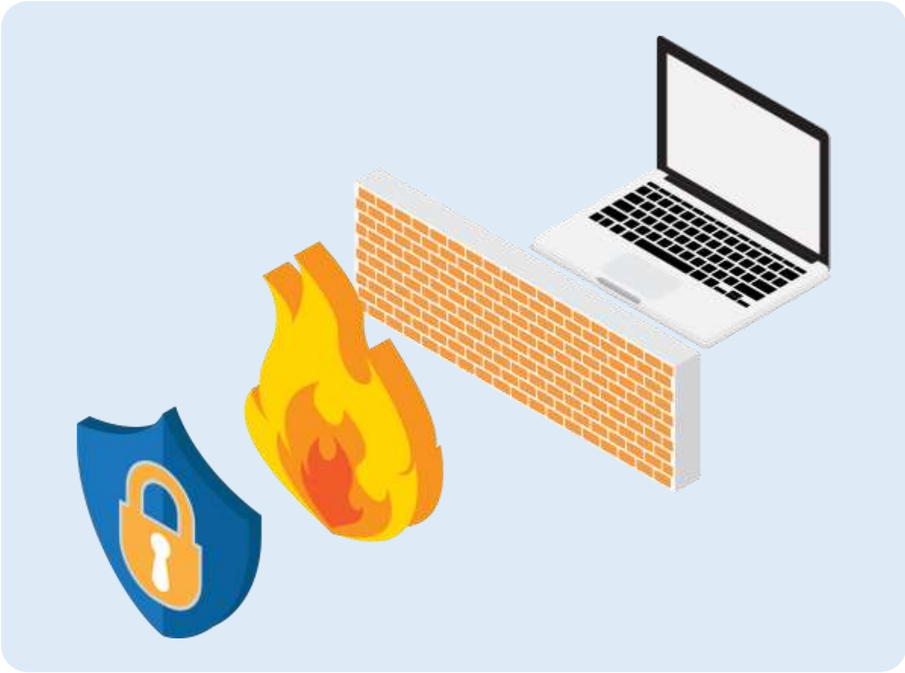
Isolates segments that specifically store regulated data such as PII and PHI

Achieves zero trust

Creates and enforces granular policies

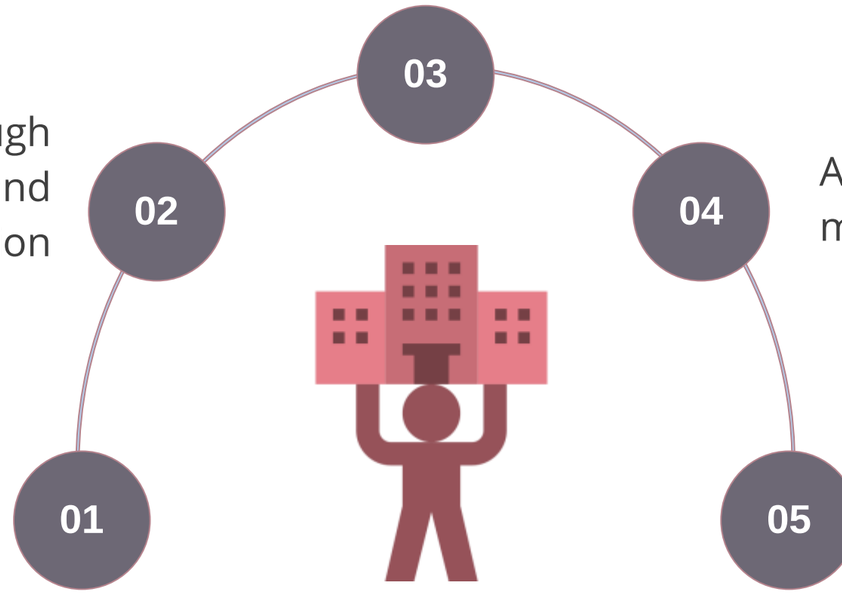
Network Function Virtualization

It is a network architecture concept that uses virtualization to design, deploy, and manage networking services.



It decouples network functions such as firewall management, intrusion detection, DNS, and NAT from proprietary hardware appliances and manages them as software in virtual machines.

Network Function Virtualization: Benefits



Improved scalability and resource management

Reduced CapEx and OpEx through reduced equipment costs and power consumption

Accelerated and flexible time to market for new products and updates

Reduced vendor lock-in

Faster deployment

Software-Defined Networking (SDN)

It allows network administrators to programmatically initialize, control, change, and manage network behavior dynamically via open interfaces and abstraction of lower-level functionality.

It separates the infrastructure layer (hardware and hardware-based settings) from the control layer (network services of data transmission management).

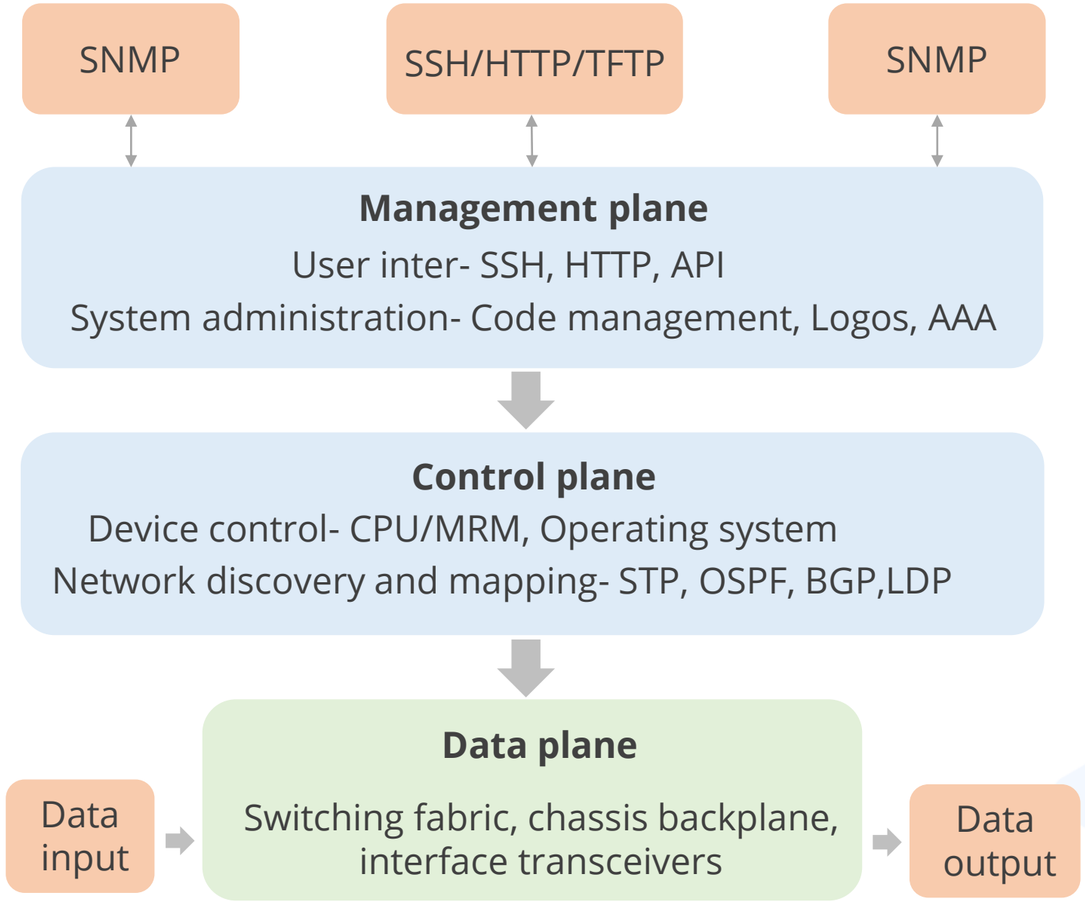
Software-Defined Networking (SDN)

The following are the different types of planes and their segregation based on the traffic they manage:

Control plane: It is the part of a network that carries signaling traffic and is responsible for routing.

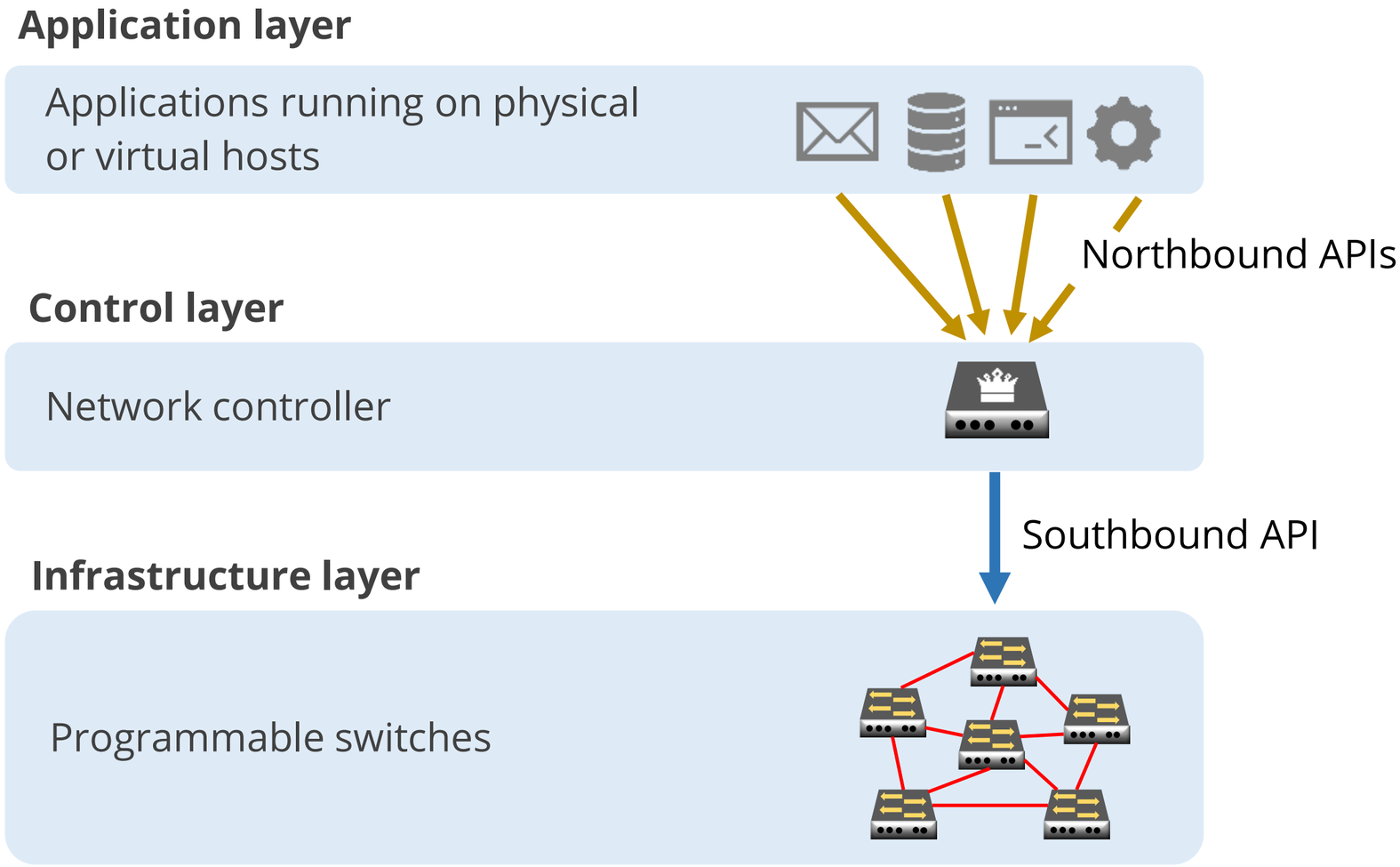
Management plane: It carries administrative traffic and is considered a subset of the control plane.

Data plane: It contains the traffic that the network carries.



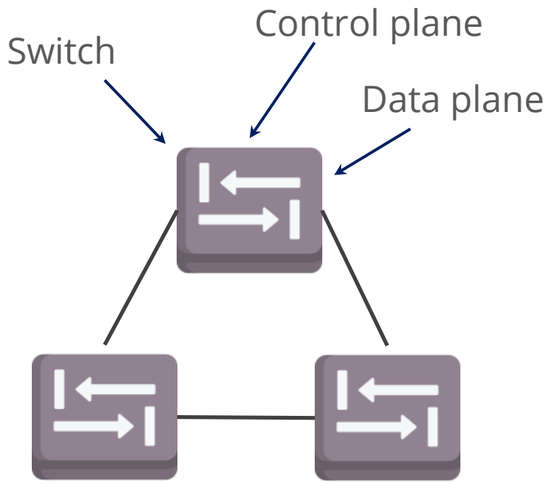
Software-Defined Networking (SDN)

The SDN architecture concept is given below:

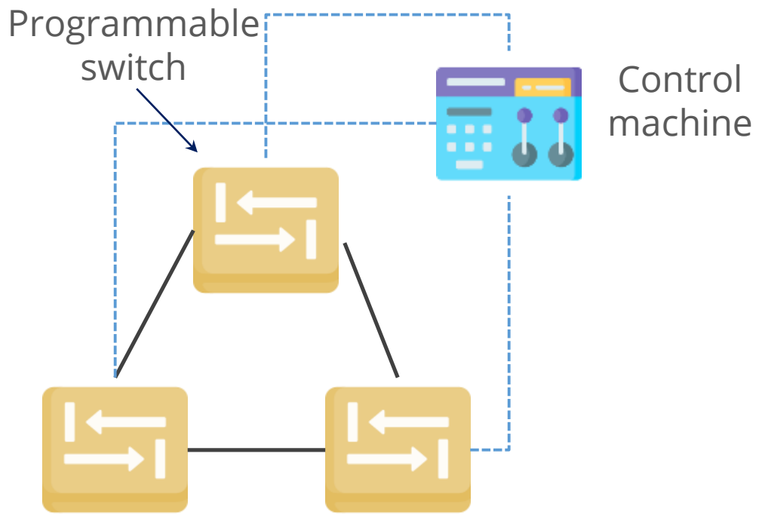


How SDN Is Different from Traditional Networking

Traditional network



Software-defined network



Traditional network

All three planes are implemented in the firmware of routers and switches.

Software-defined network

- It removes the control plane from network hardware and implements it in software.
- It enables programmatic access, making network administration much more flexible.

Content Delivery Network (CDN)

It is a large, geographically distributed network of specialized servers that accelerate the delivery of web content and rich media to internet-connected devices.

Content Delivery Network (CDN): Benefits

Performance

A shorter distance to users enhances performance by reducing latency and minimizing packet loss.

Availability

- Requests are always routed to the nearest available location.
- If the nearest server is unavailable, requests are automatically sent to the next available server.

Content Delivery Network (CDN): Benefits

Security

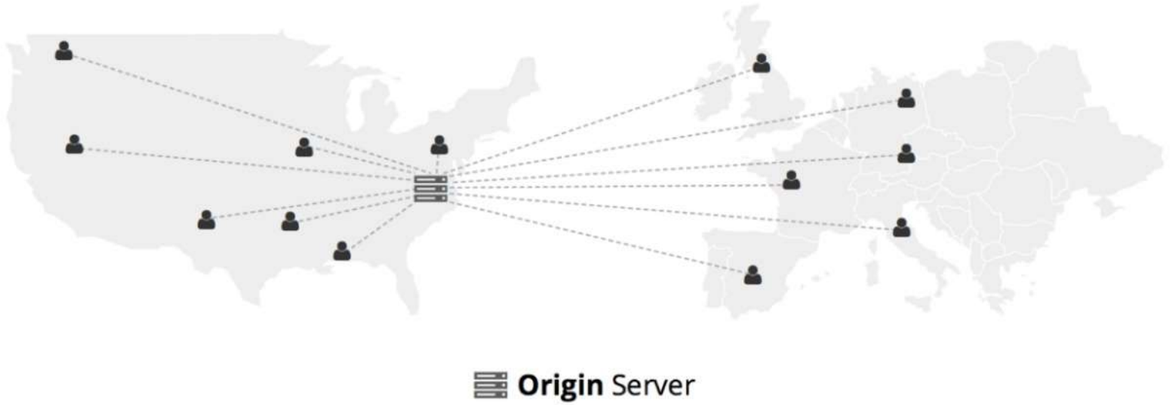
- It protects content providers and users by mitigating various attacks.
- The attacks may include DDoS attacks and web-based exploits such as SQL injection, cross-site scripting, and local or remote file inclusion.

Intelligence

- It provides valuable analytics to identify trends in end-user connectivity, device types, and global browsing experiences.
- It offers critical, actionable insights into their user base.

Importance of CDN

In the absence of a CDN, information must be requested from the origin server, no matter where a user is based geographically, which can be a great distance away from the user.



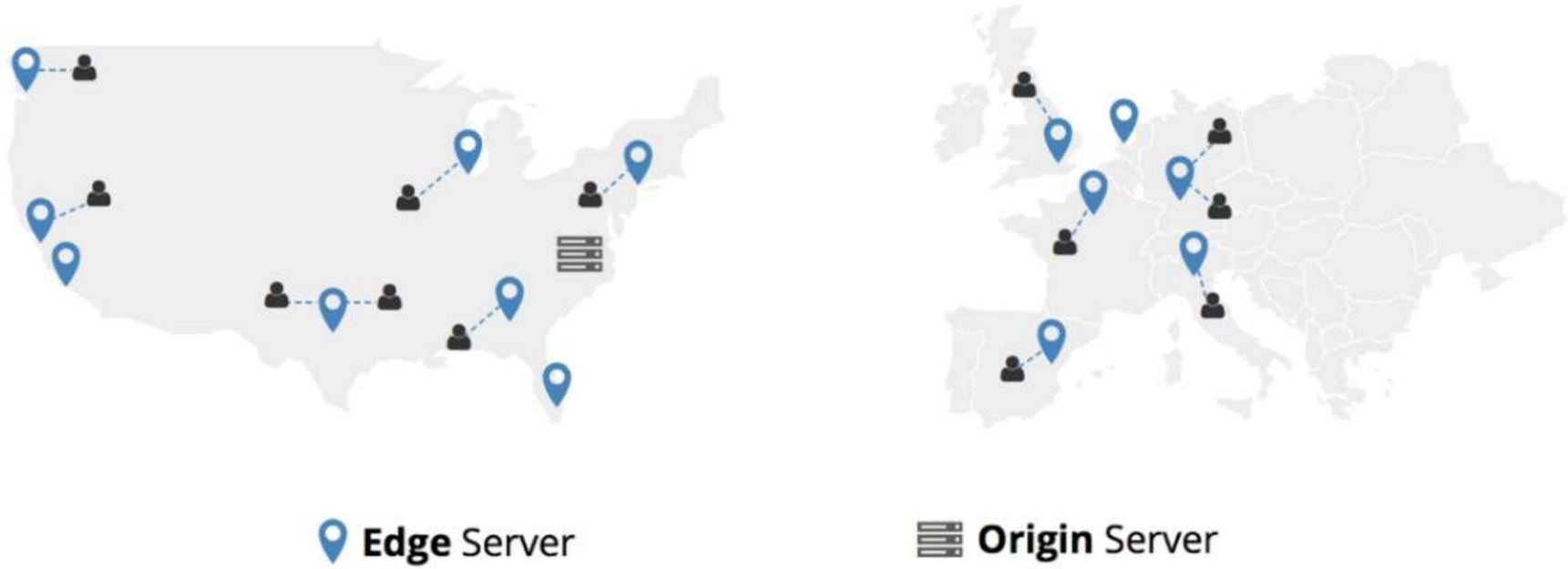
Without CDN

This could severely impact the performance of the application.

Source: https://img-medianova.mncdn.com/wp-content/uploads/sites/8/2020/05/cdn3.png

Importance of CDN

When using a CDN, edge servers distribute static website data to visitors that are close to their geographic region.



With CDN

The connectivity between the internet nodes that are close together means fewer hops and faster flow of data.

Source: https://img-medianova.mncdn.com/wp-content/uploads/sites/8/2020/05/cdn3.png

Quick Check

Your organization is considering implementing a CDN to enhance website performance. What is the primary benefit of using a CDN?

A. Increased website security

B. Reduced bandwidth costs

C. Improved search engine rankings

D. Enhanced website scalability

Secure Protocols

Secure Communication Protocol

It is a set of rules governing how data is securely transmitted between parties.

- It acts as a common language allowing different components to communicate using a known set of commands.
- It involves encryption to scramble data and authentication to verify identities.
- It has built-in security mechanisms to enforce security by default.

Secure Protocols

Domain Name System Security Extensions (DNSSEC)

- These are a set of cryptographic extensions to the DNS protocol that enable origin authentication of DNS data, authenticated denial of existence, and data integrity.
- They, however, do not address availability or confidentiality.

Secure Shell Protocol (SSH)

- It is an encrypted remote terminal connection program used for remote connections to a server.
- It employs asymmetric encryption but generally requires an independent source of trust with a server, such as manually receiving a server key, to function.
- It uses TCP port 22 as its default port.

Secure Protocols

Secure/Multipurpose Internet Mail Extensions (S/MIME)

- Multipurpose Internet Mail Extensions (MIME) is a standard for transmitting binary data via e-mail.
- S/MIME is a standard for public key encryption and signing of MIME data in e-mails.
- It offers cryptographic protections to e-mails and is built into most modern e-mail software to facilitate interoperability.

Secure Real-time Transport Protocol (SRTP)

- It is a network protocol for securely delivering audio and video over IP networks.
- It uses cryptography to provide encryption, message authentication, integrity, and replay protection to the RTP data.

Secure Protocols

Lightweight Directory Access Protocol (LADP)

- It is the primary protocol for transmitting directory information.
- It transmits traffic insecurely, by default, but can be secured using SSL/TLS, known as LDAP Secure (LDAPS).
- It uses a certificate from a trusted certificate authority (CA).
- It communicates over TCP port 636.

Simple Network management Protocol version 3 (SNMPv3)

- It is a standard for managing devices on IP-based networks, specifically addressing security concerns of SNMPv1 and SNMPv2.
- It operates as an application layer protocol within the IP suite, enabling management and monitoring of network devices, computers, and other IP-connected devices.
- All SNMP versions require ports 161 and 162 to be open on a firewall.

Secure Protocols

Internet Message Access Protocol over SSL/TLS (IMAPS)

- IMAPS does not secure data, including login credentials, by default.
- IMAPS uses SSL/TLS to encrypt the communication channel between the email client and the mail server.

Hypertext Transfer Protocol Secure (HTTPS)

- It encrypts communication between the browser and the website the user is visiting, making the data unreadable to eavesdroppers.

Secure Protocols

File Transfer Protocols Secure (FTPS)

- It is the implementation of FTP over an SSL/TLS-secured channel.
- It supports complete FTP compatibility and provides encryption protections enabled by SSL/TLS.
- It uses TCP ports 989 and 990.

SSH File Transfer Protocol (SFTP)

- It is the use of FTP over an SSH channel.
- It leverages the encryption protections of SSH to secure FTP transfers.
- It uses TCP port 22 since it relies on SSH.

Network Attack

Network Attack

It is an unauthorized and malicious attempt to disrupt, compromise, or gain access to computer systems, data, or communication within a network, often for malicious purposes.

In a server-side attack, the attackers target an organization’s servers holding confidential information.

Forms of Network Attacks

Passive attacks:
Involve monitoring network traffic to gather information without altering it

Active attacks:
Involve modifying network traffic or systems

Types of Network Attacks

Pivoting attack

DoS or DDoS attack

ARP poisoning

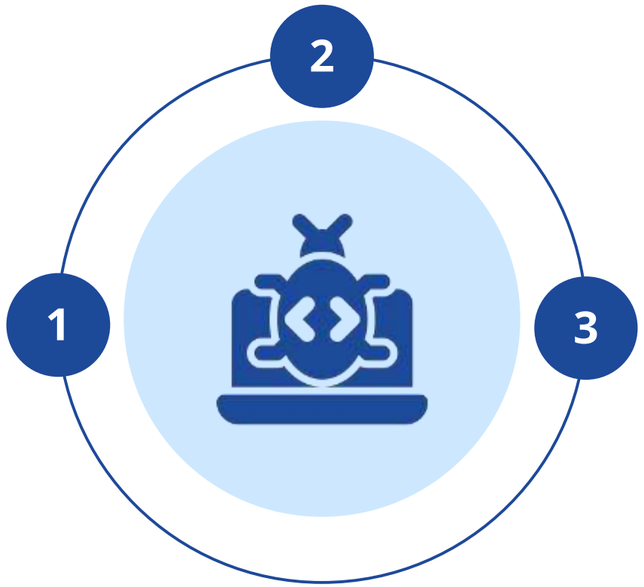
Smurf attack

Pivoting Attack

It is a technique used by attackers or ethical hackers (during penetration testing) to move laterally within a network.

Gaining foothold:
The attacker first gains access to a single system within the network.

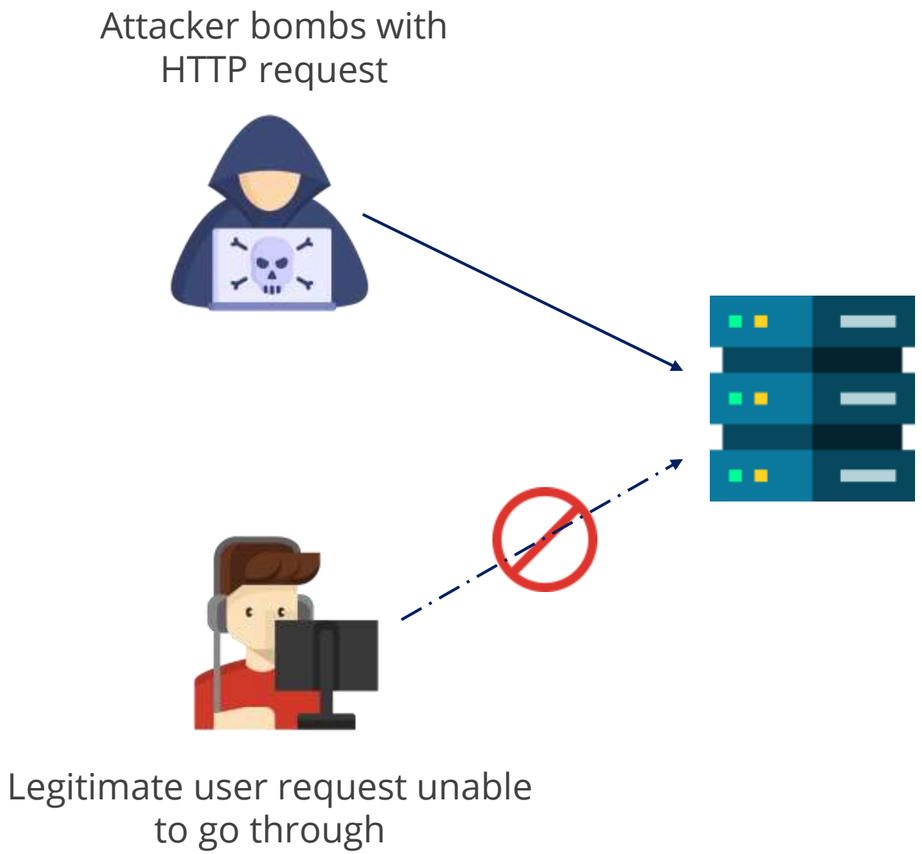
Using foothold:
Once inside the initial system, the attacker leverages its resources to further their reach.



Moving laterally:
With the compromised system as a pivot point, the attacker then launches attacks on other machines on the network.

Denial-of-Service (DoS) Attack

It makes a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of an internet-connected host.

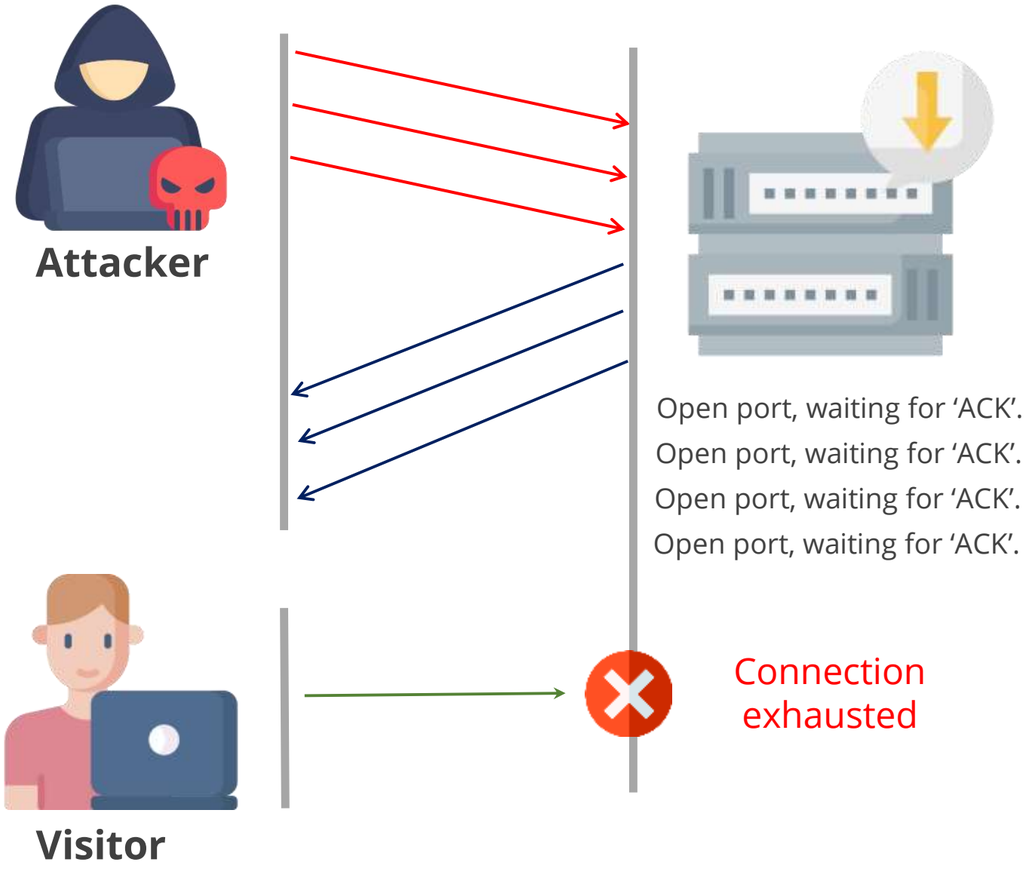


This can be accomplished by:

- Crashing the system
- Taking the system offline
- Sending an overwhelming number of requests that the machine cannot process

SYN Flood Attack

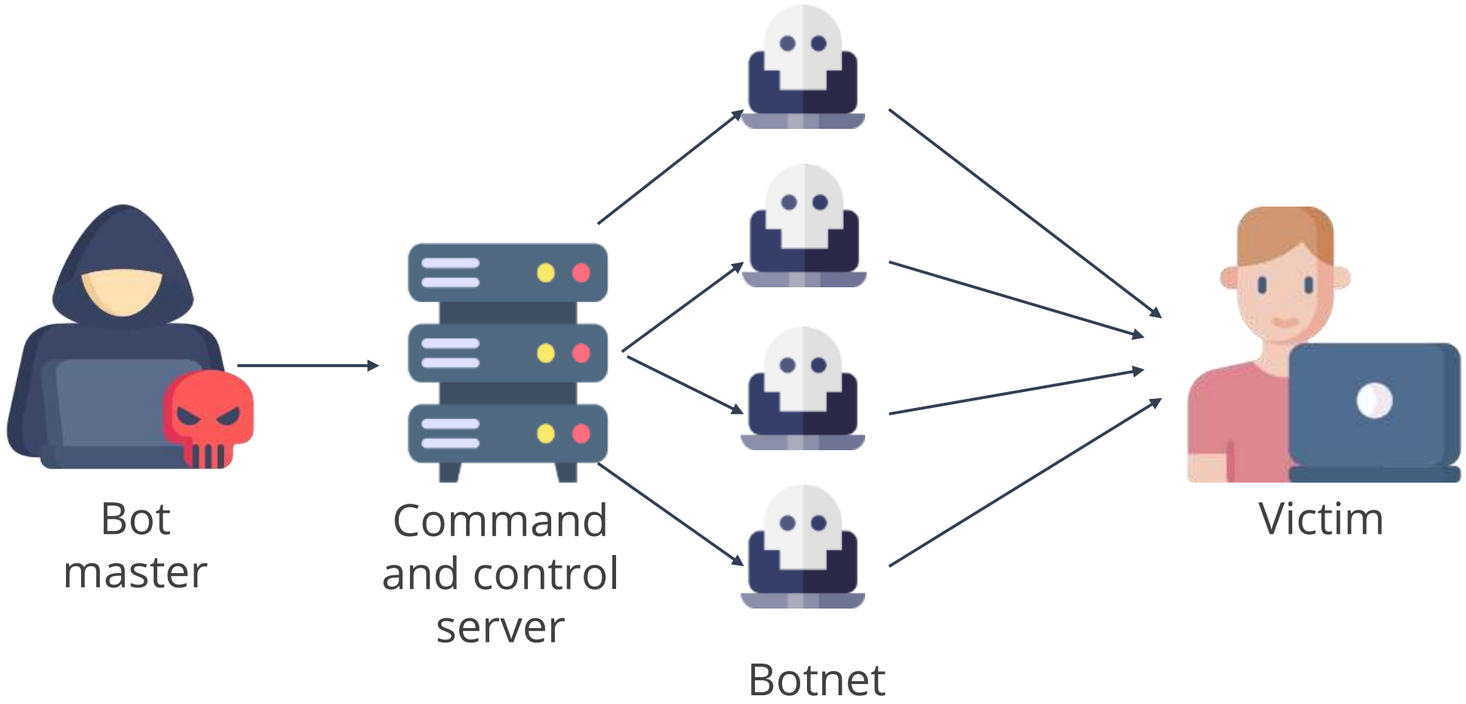
It is a type of denial-of-service (DoS) attack that aims to make a server unavailable to legitimate traffic by consuming all available server resources.



- The attacker repeatedly sends initial connection request (SYN) packets.
- This overwhelms all available ports on a targeted server, causing the targeted device to respond to legitimate traffic sluggishly or not at all.

Distributed Denial-of-Service (DDoS) Attack

The hacker begins by exploiting a computer system and making it the DDoS master, which then identifies other vulnerable systems and gains control over them.



Their main aim is to prevent legitimate users from accessing a system or site.

Types of DDoS Attacks

Network or volume-centric

- These attacks use bots and botnets to flood the network layers with seemingly legitimate traffic, causing network operations to become extremely slow or to not work at all.

Application layer-based

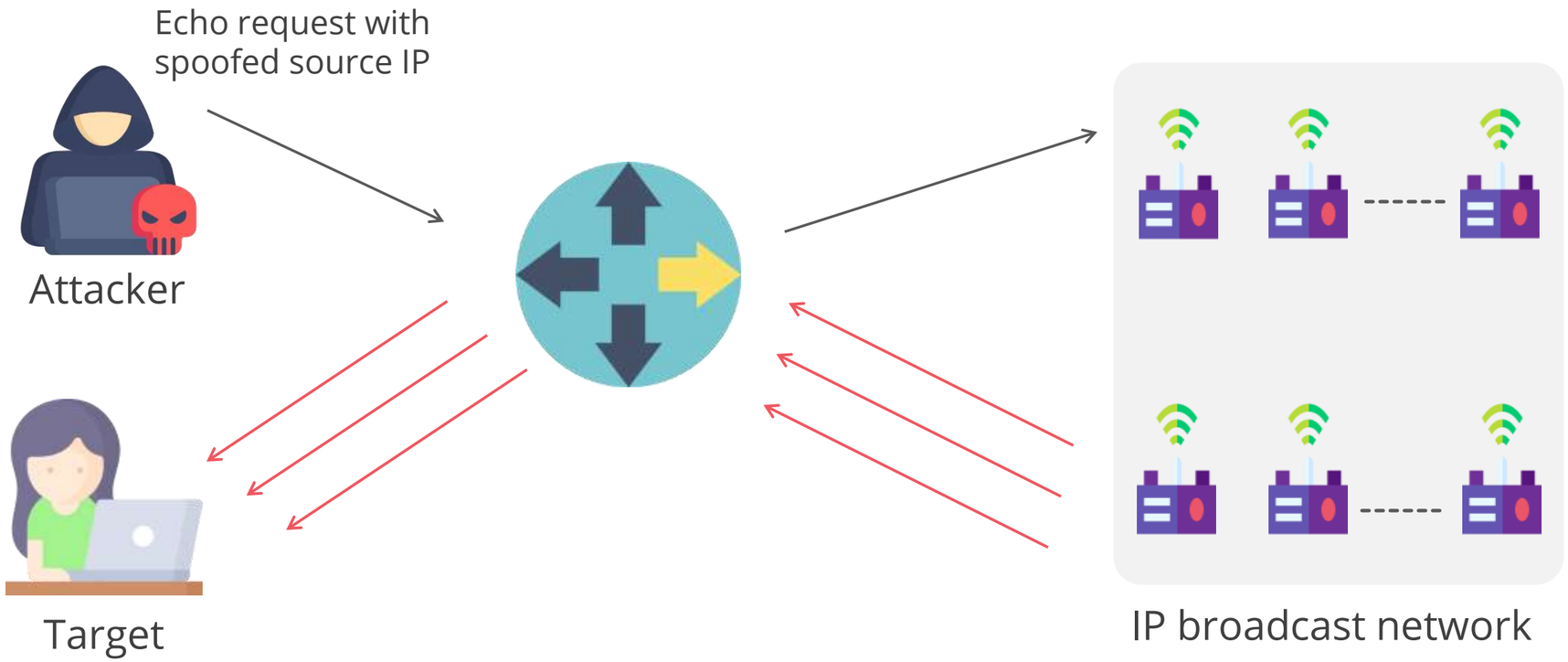
- These attacks exhaust resources by consuming too much of the application's resources.
- They also target the layer managing HTTP and SMTP communication.

DoS vs. DDoS Attack

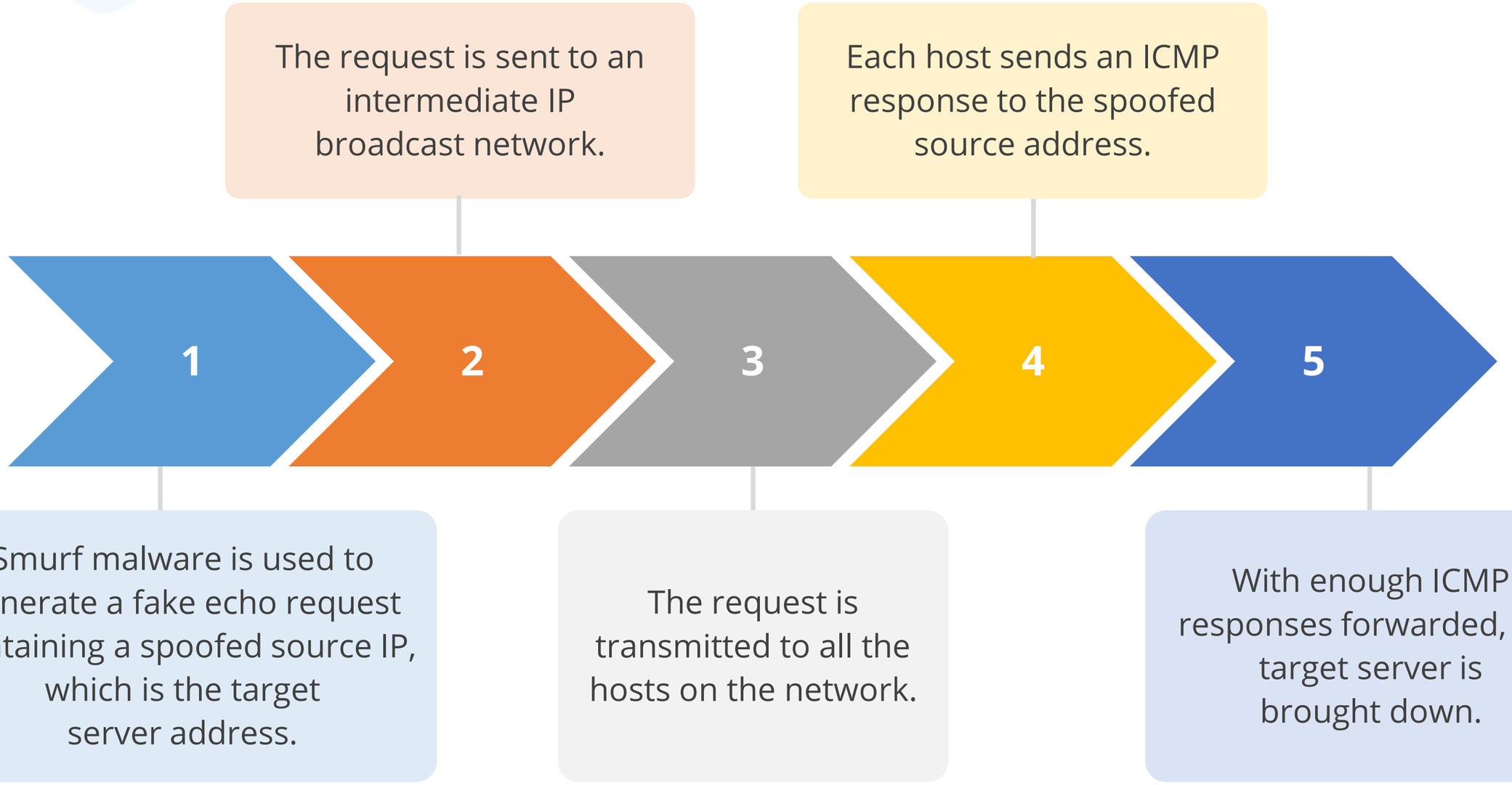
DoS attack	DDoS attack
A hacker uses a single internet connection to either exploit a software vulnerability or flood a target with fake requests.	A hacker launches attacks from multiple connected devices that are distributed across the internet.

Smurf Attack

It is a distributed denial-of-service (DDoS) attack in which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets.



Smurf Attack Flow



Network Attacks: Countermeasures

- Implementing access control lists
- Using firewalls
- Deploying intrusion detection system (IDS)
- Using an intrusion prevention system (IPS)
- Protecting network cabling
- Installing antivirus software
- Employing private addressing
- Closing unnecessary ports and services
- Deploying security patches
- Utilizing unified threat management (UTM)
- Configuring gateways

Key Takeaways

- The OSI model serves as a standard framework for network communications and allows different and dissimilar networks to communicate seamlessly.
- An IP address is a logical and numerical identifier assigned to each host on the internet, allowing for unique identification and communication between devices.
- Remote access technology focuses on providing access to a remote user into a network.
- VoIP enables people to use the internet as the transmission medium for telephone calls by sending voice data in packets using IP.
- Mobile device security protects data from security threats that can lead to data breaches, unauthorized access to sensitive data, and even data loss from mobile devices.

Thank You