Certified Information Systems Security Professional (CISSP) Certification Training Course

Domain 04: Communications and Network Security

Learning Objectives

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

- Analyze OSI, TCP/IP, and UDP communication protocols
- Explain the concepts of Software Defined Networking (SDN) and Software Defined Wide Area Networking(SD-WAN)
- Recognize and compare different transmission media
- List the features of endpoint security
- Explain VPN and different types of VPN protocols
- Analyze different types of network attacks

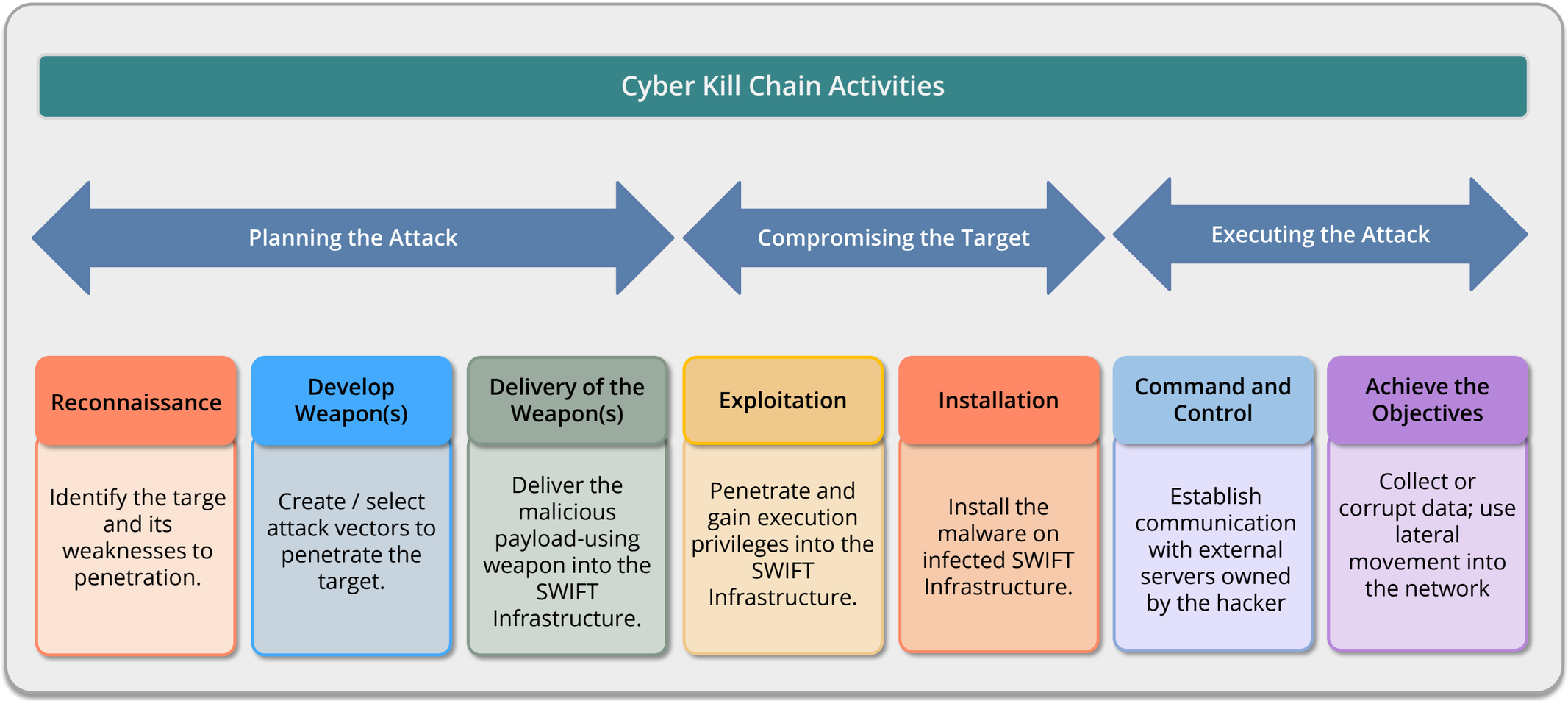
Introduction to Communications and Network Security

Case Study: Communications and Network Security

Kevin, who is preparing for his CISSP exam, read an internal case file on a recent spam attack on Nutri Worldwide Inc.

At the Minnesota plant, a vendor who had visited the plant used his laptop to complete a few transactions. He connected to the wireless after taking approvals. He used his flash drive to backup the transactions. The flash drive had viruses, and these entered the network through his laptop, causing the local server to crash. This had far-reaching effects.

Cyber Kill Chain Activities



Source: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Assess and Implement Secure Design Principles in Network Architecture

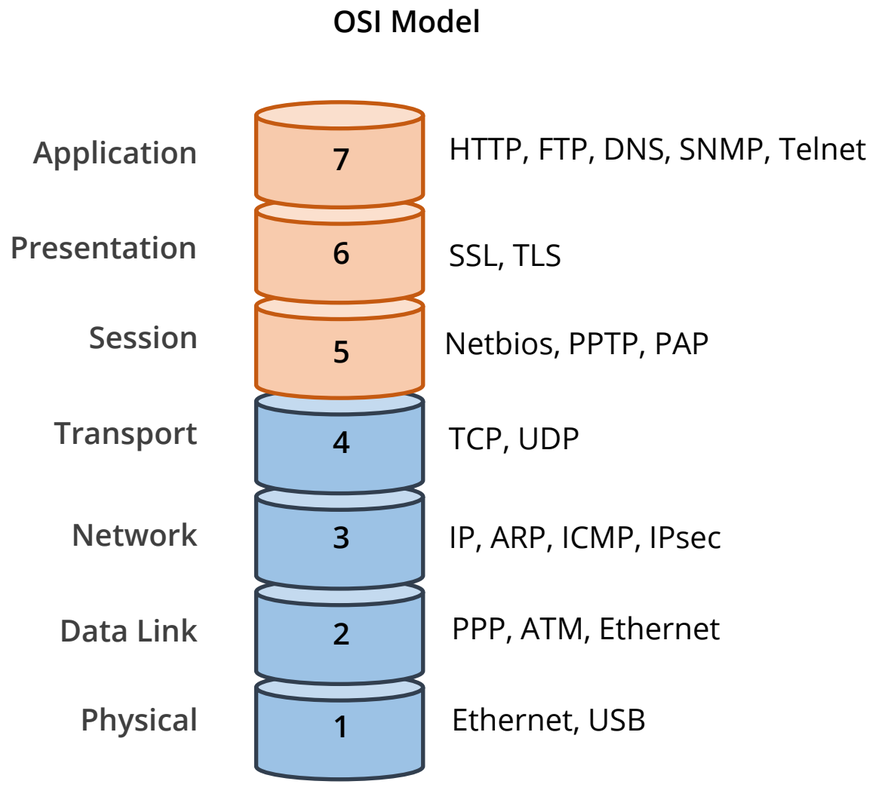
Introduction to Secure Network Architecture and Design

Various communication protocols define communication.

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

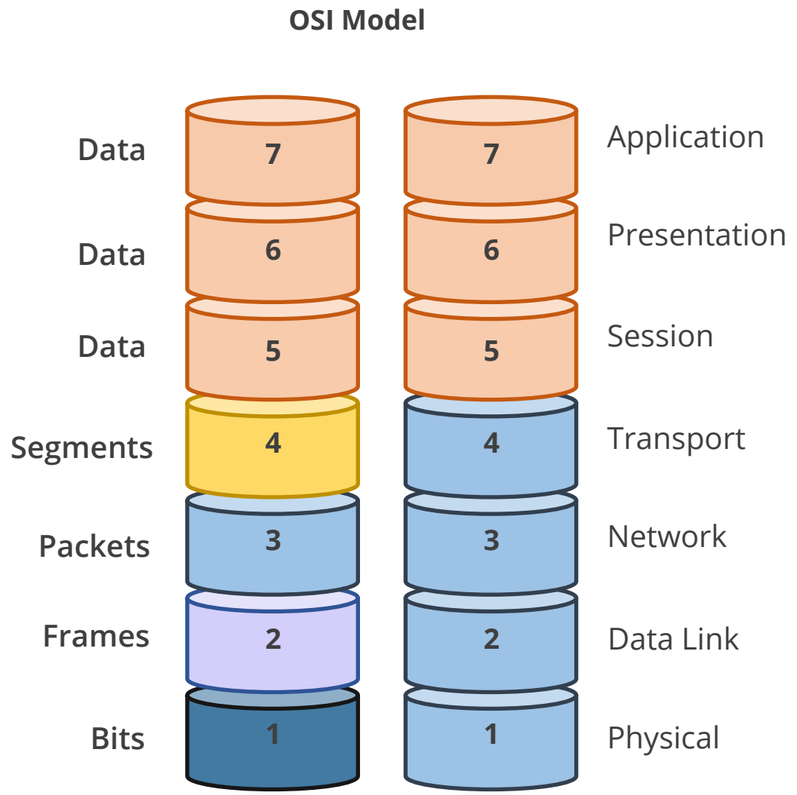
Open Systems Interconnection

- Open Systems Interconnection (OSI), a standard model for network communications, allows dissimilar networks to communicate.
- OSI describes how data and network information are communicated from one computer to another.
- Each layer communicates with the same layer's software or hardware on other computers.



Open Systems Interconnection

- The four lower layers (transport, network, data link, and physical) are concerned with the flow of data from end to end through the network.
- The three upper layers of the OSI model (application, presentation, and session) are more oriented toward services to the applications.
- Data is encapsulated with the necessary protocol information as it moves down the layers before network transit.



Open Systems Interconnection

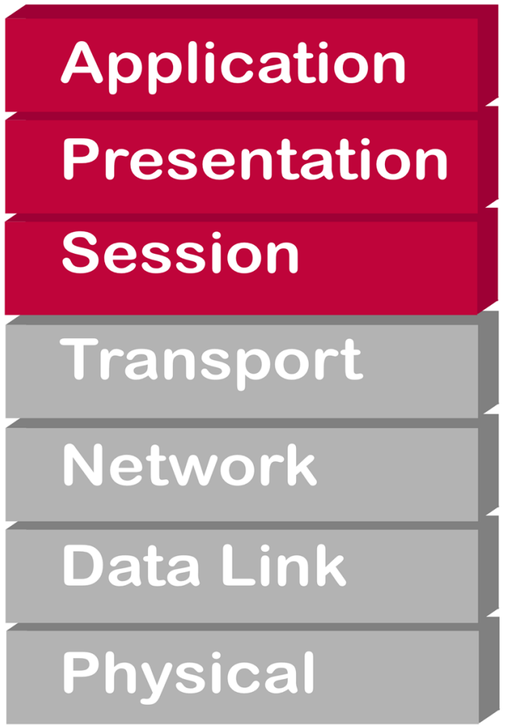
The seven layers in the OSI model and their functions are as follows:

7	Application	• Provides specific services for applications such as file transfer • Allows access to network's resources
6	Presentation	Translates, encrypts, and compresses data
5	Session	• Establishes, maintains, and manages sessions • Example: Synchronization of data flow
4	Transport	Provides end-to-end data transmission integrity
3	Network	• Switches and routes information units • Provides internetworking
2	Data Link	Provides transfer of units of information to the other end of the physical link Organizes bits into frames
1	Physical	• Transmits bit stream on physical medium • Provides mechanical and electrical specifications

Working of the OSI Model

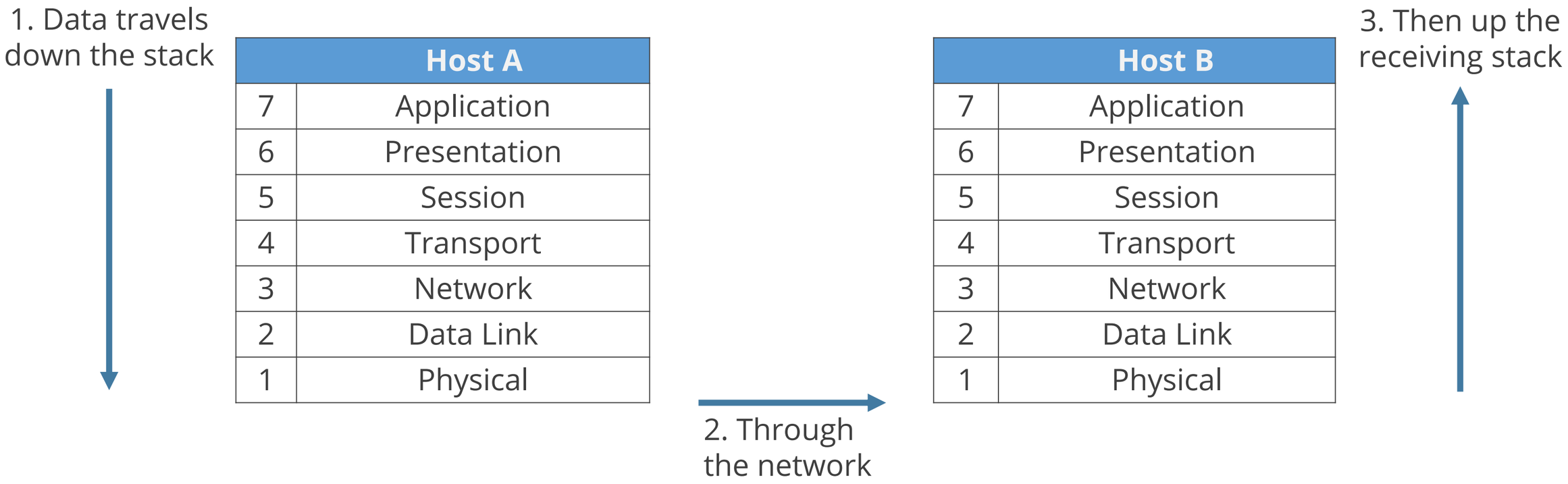
Data is sent from a source computer to a destination computer.

- 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.



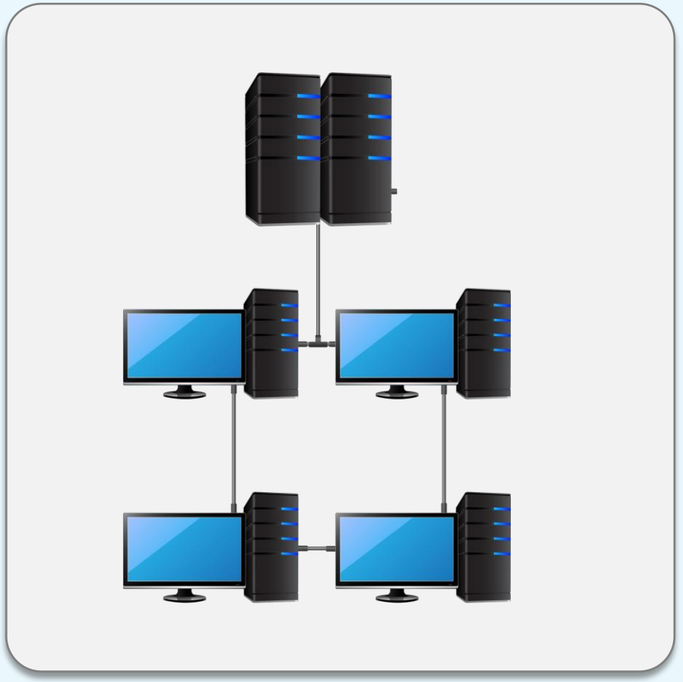
Working of the OSI Model

The following illustration explains how data travels in the OSI model:



Physical Layer

- Physical layer 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 defines types of signaling, such as analog or digital, electrical or optical characteristics of signals, asynchronous or synchronous, simplex, full, or half duplex.

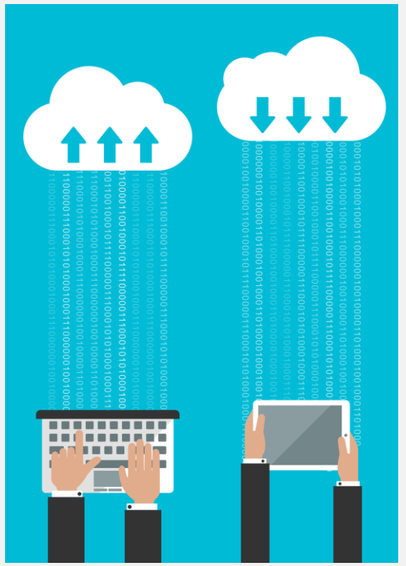


Physical Layer

- It defines the topology (Star, bus, and ring).
- The physical layer has only two responsibilities:
  - Sending and receiving bits
  - Defining standard interfaces

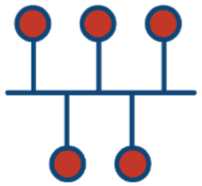
Example: EIA-232 (RS-232), Synchronous Optical NETwork (SONET), ISDN, DSL, and SONET are some of the standard interfaces at this layer.

- The physical layer provides services to the data link layer.



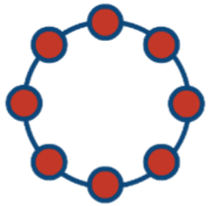
Network Topologies

Network topology defines the way the network devices are organized to facilitate communications.



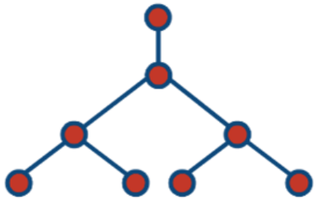
Bus

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 where branches with multiple nodes are possible.

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.

Data Link Layer

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

- This layer establishes the communication link between individual devices over a physical link or channel.
- The data link layer defines 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.

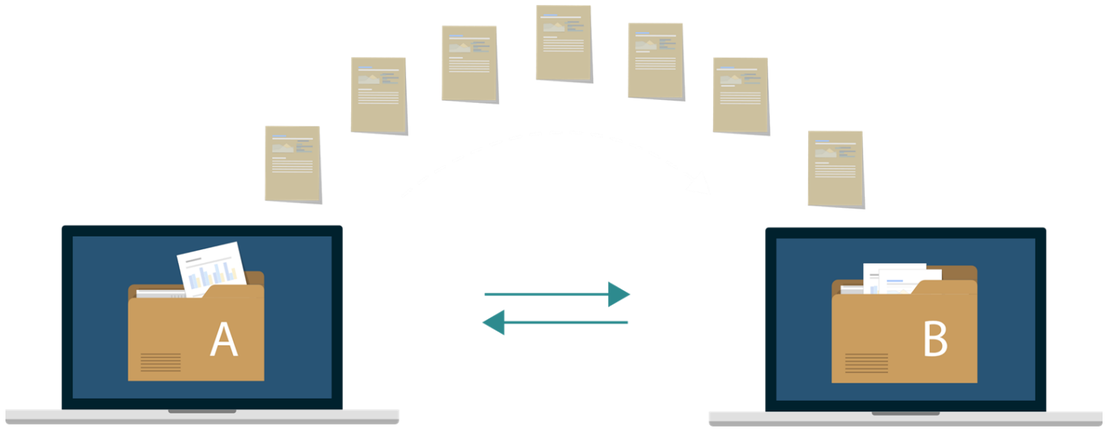
Data Link Layer

The data link layer has two 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.

Example: Address Resolution Protocol (ARP), Serial Line Internet Protocol (SLIP), and Point-to-Point Protocol (PPP)

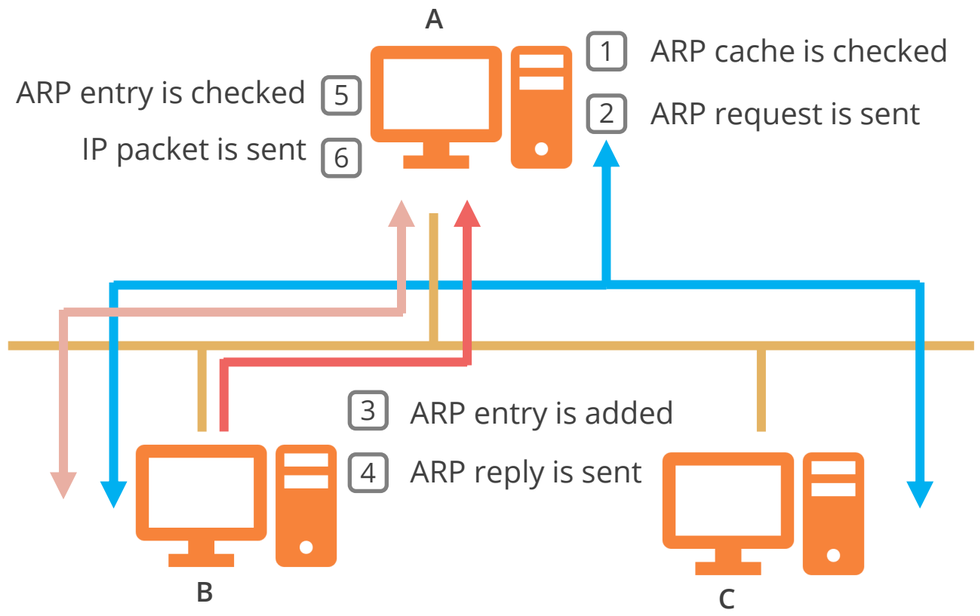
- The data link layer provides services to the network layer.



Address Resolution Protocol

Address resolution protocol helps match an IP address to a Media Access Control (MAC) address.

- Interrogates the network by sending out a broadcast seeking a network node that has a particular IP address
- Maintains a dynamic table, known as the ARP cache, of the translations between IP and MAC addresses



VLANs

Virtual Local Area Networks (VLANs) allow the ports on the same or different switches to be grouped so that the traffic is confined to the members of that group.

- VLAN restricts broadcast, unicast, and multicast traffic.
- A VLAN creates an isolated broadcast domain and a switch with multiple broadcast domains, like a router.
- It aids in isolating segments, reduces routing broadcasts, and segregates department functions.
- It can be segmented logically.

Network Layer

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

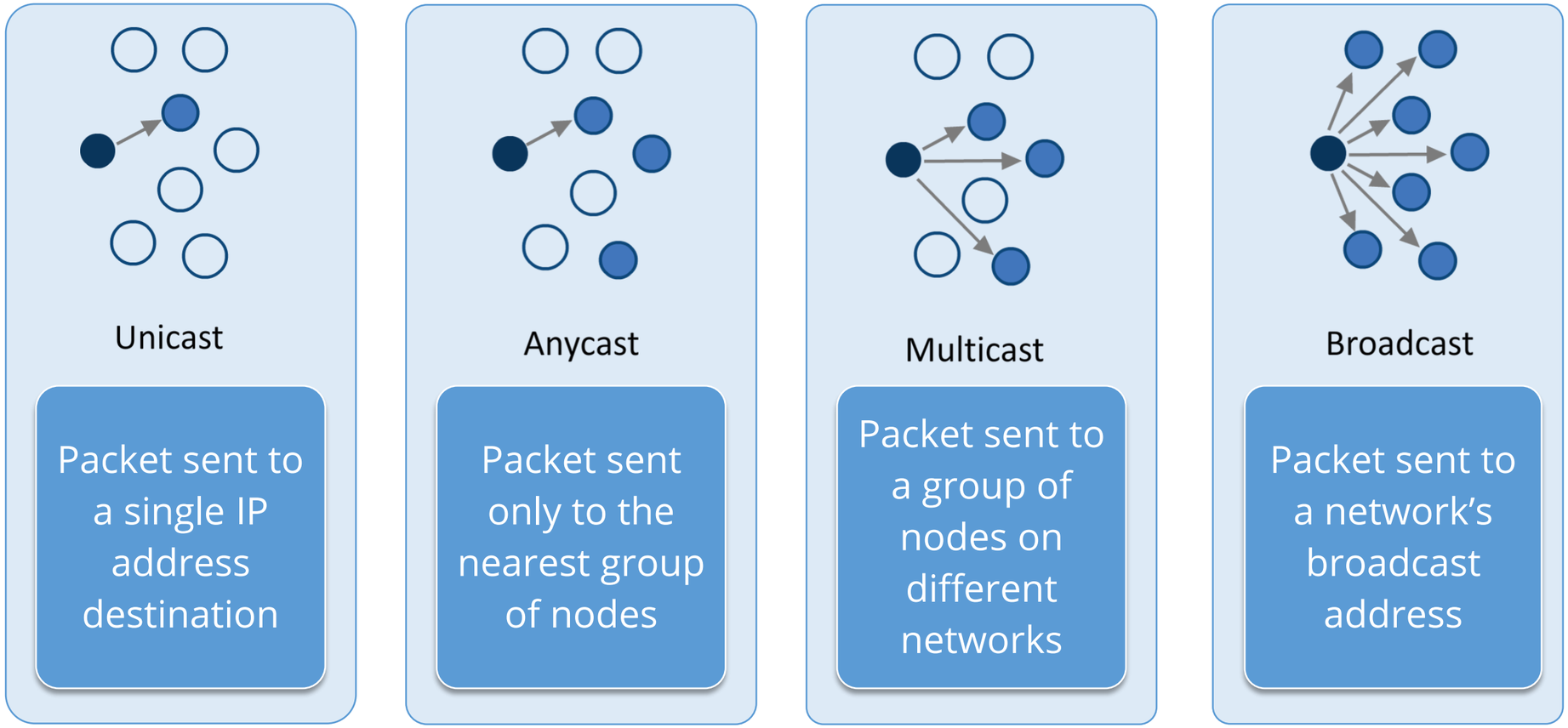
- Defines the most optimal path the packet should take from the source to the destination
- Defines logical addressing so that any endpoint can be identified
- Handles congestion in the network
- Defines how to fragment a packet into smaller packets to accommodate different media
- Manages message routing, error detection, and control of node data traffic
- Is primarily responsible for routing

  Examples: IP, OSPF, ICMP, and RIP

- Provides services to the transport layer

Types of IP Addressing

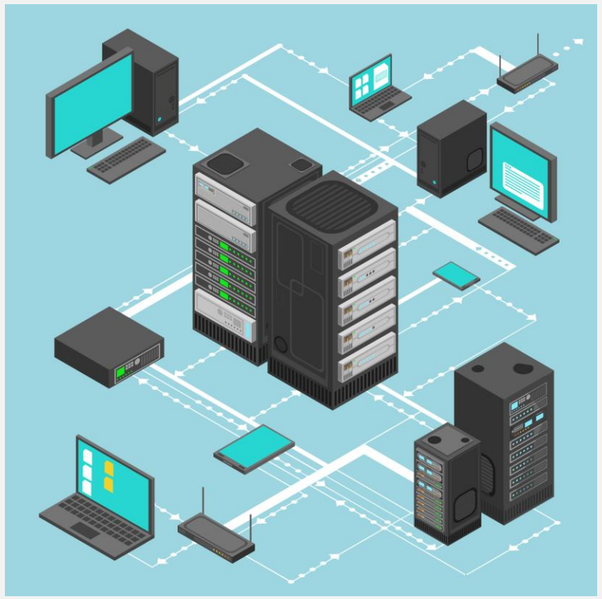
The Internet layer provides different addressing types, resulting in messages sent to one or more destination nodes.



Internet Control Message Protocol (ICMP)

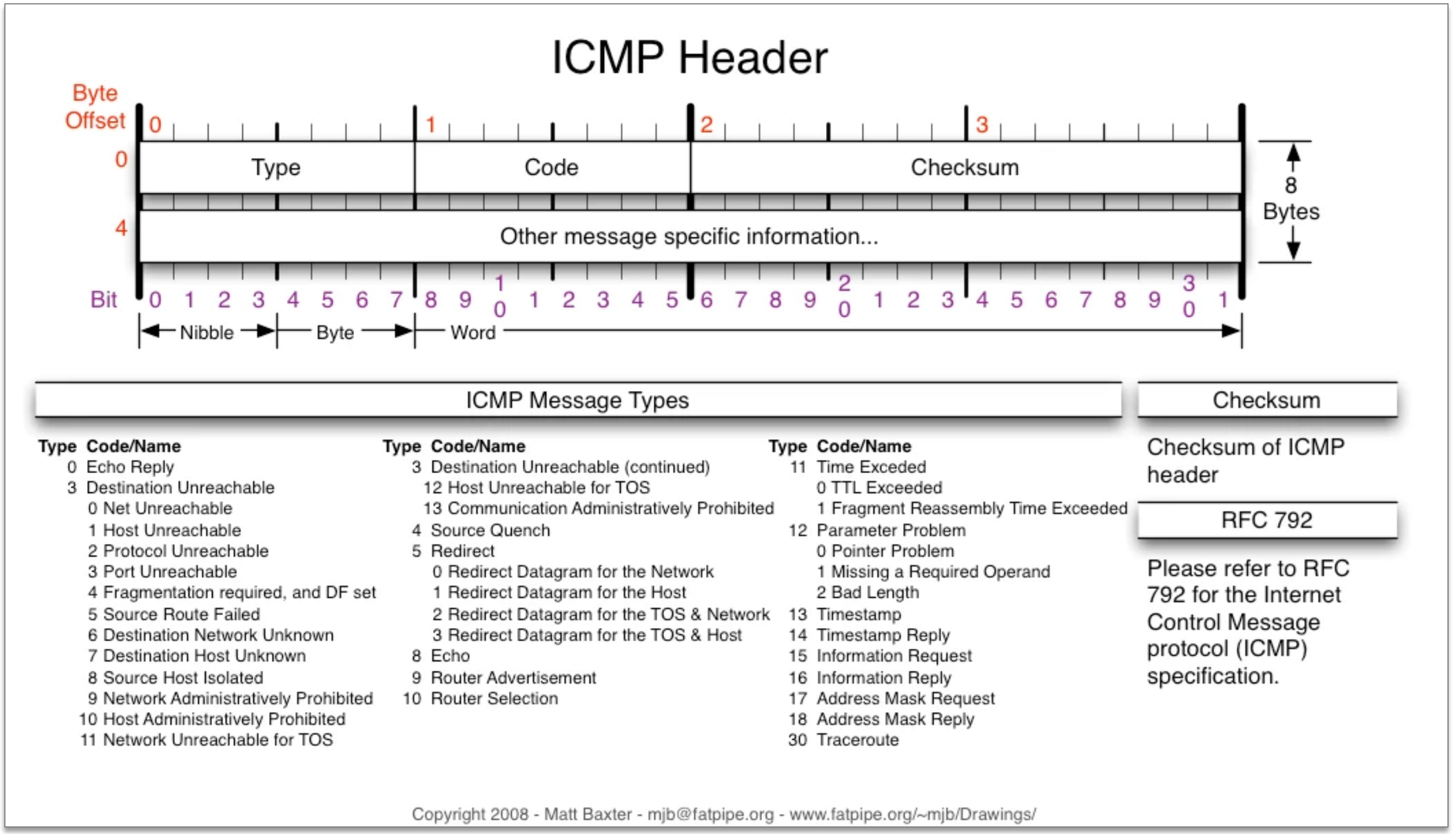
ICMP is a management protocol and messaging service provider for IP.

- Its primary function is to send messages between network devices.
- It can inform hosts on a better route to a destination.
- PING is an ICMP utility used to check the physical connectivity of machines on a network.



Internet Control Message Protocol (ICMP)

ICMP is illustrated below:



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS

Type	Code/Name
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection

Type	Code/Name
11	Time Exceeded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

Checksum of ICMP header

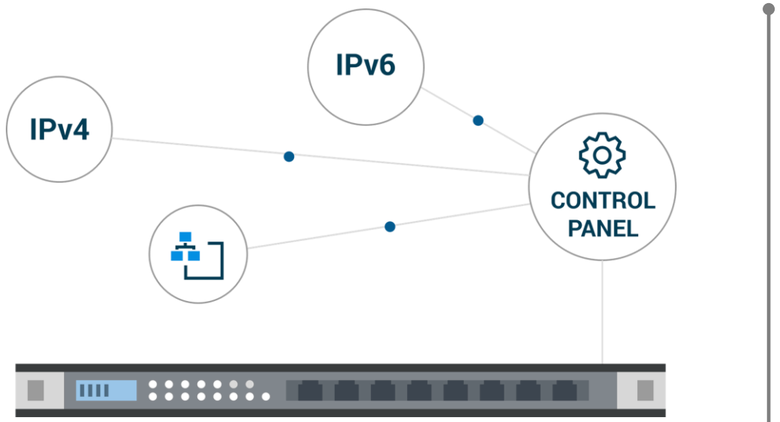
RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

Internet Protocol

Internet protocol is a network layer protocol which handles addressing and routing.

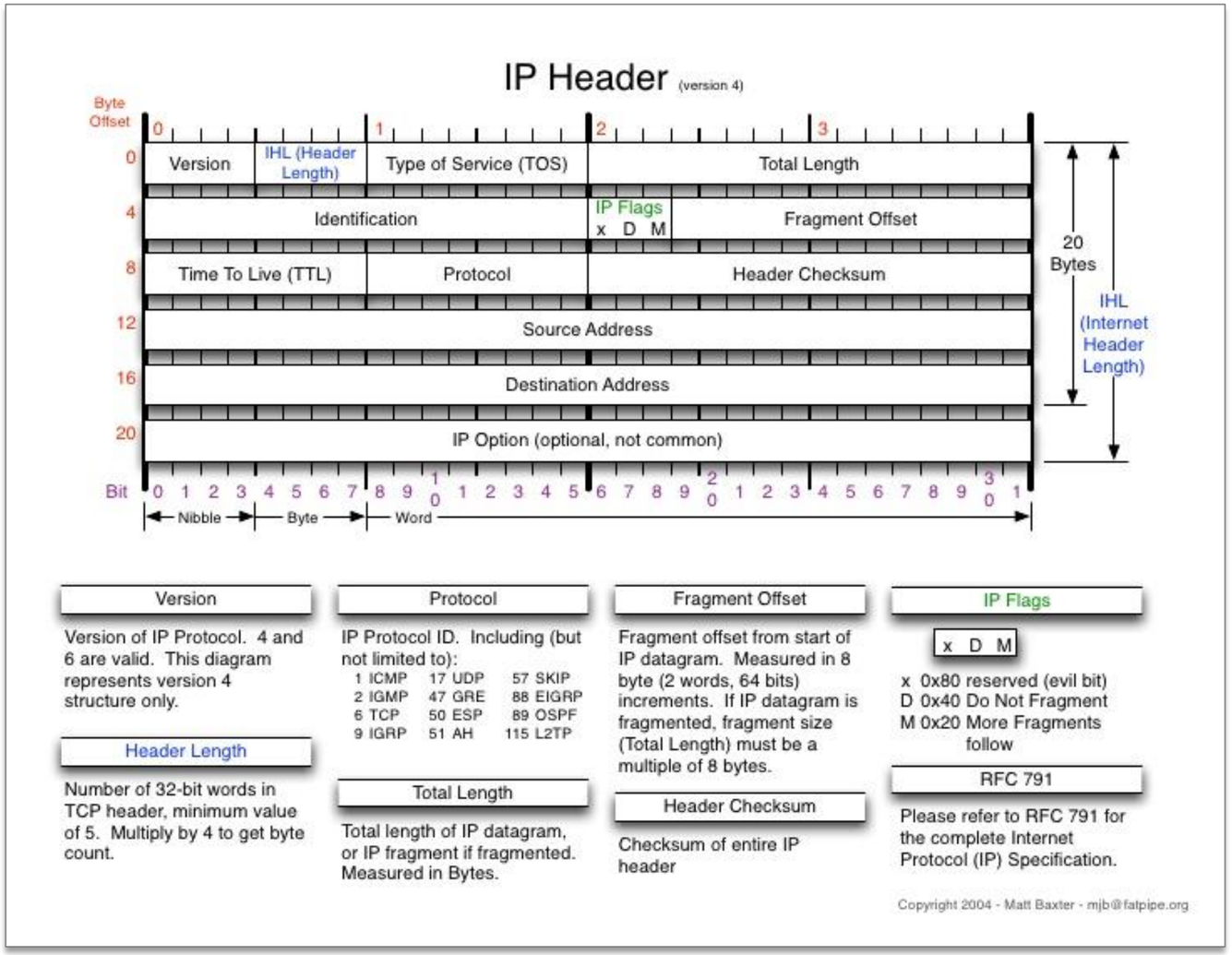
IP specifies the packet format or datagrams and the addressing scheme.



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

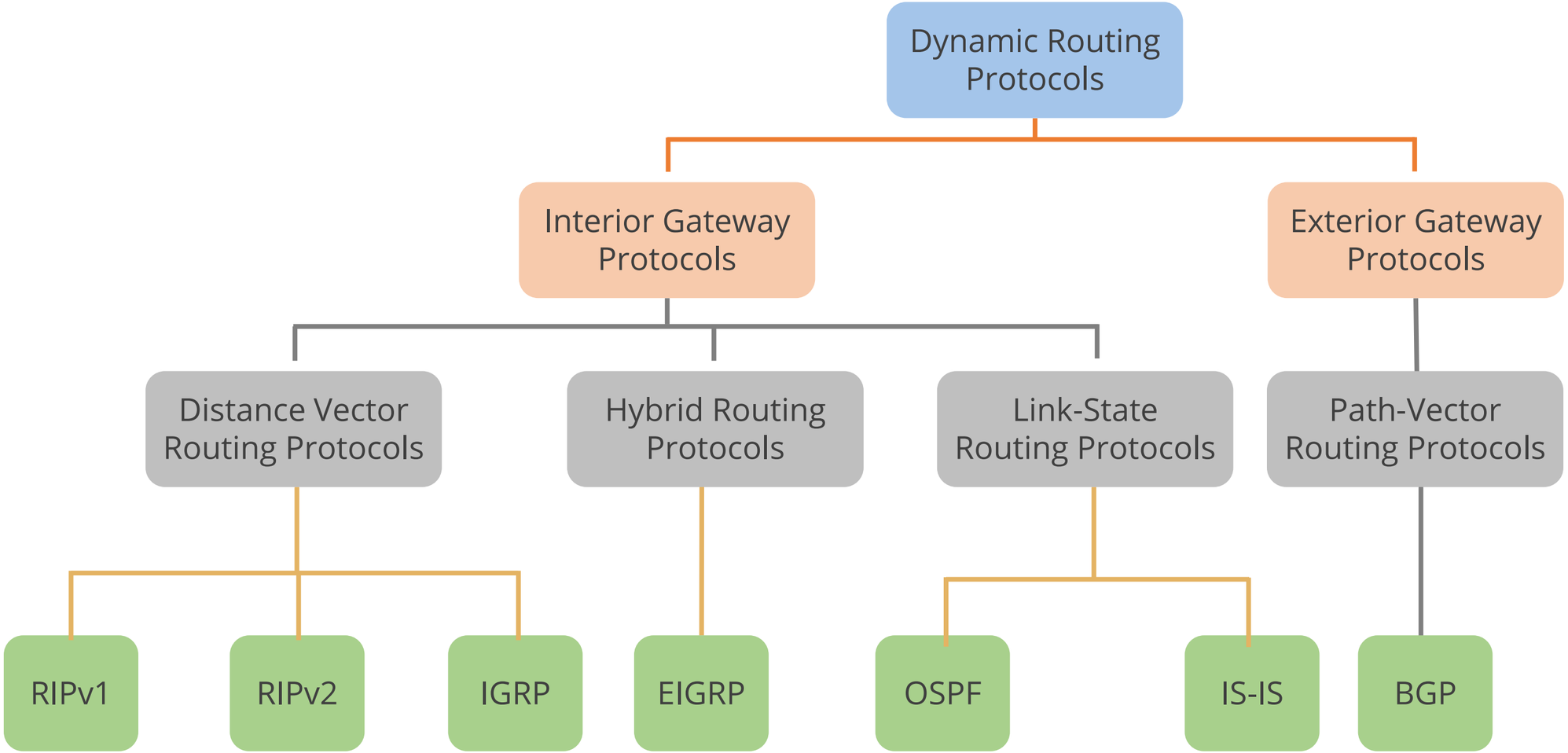
Internet Protocol

Working of internet protocol is shown below:



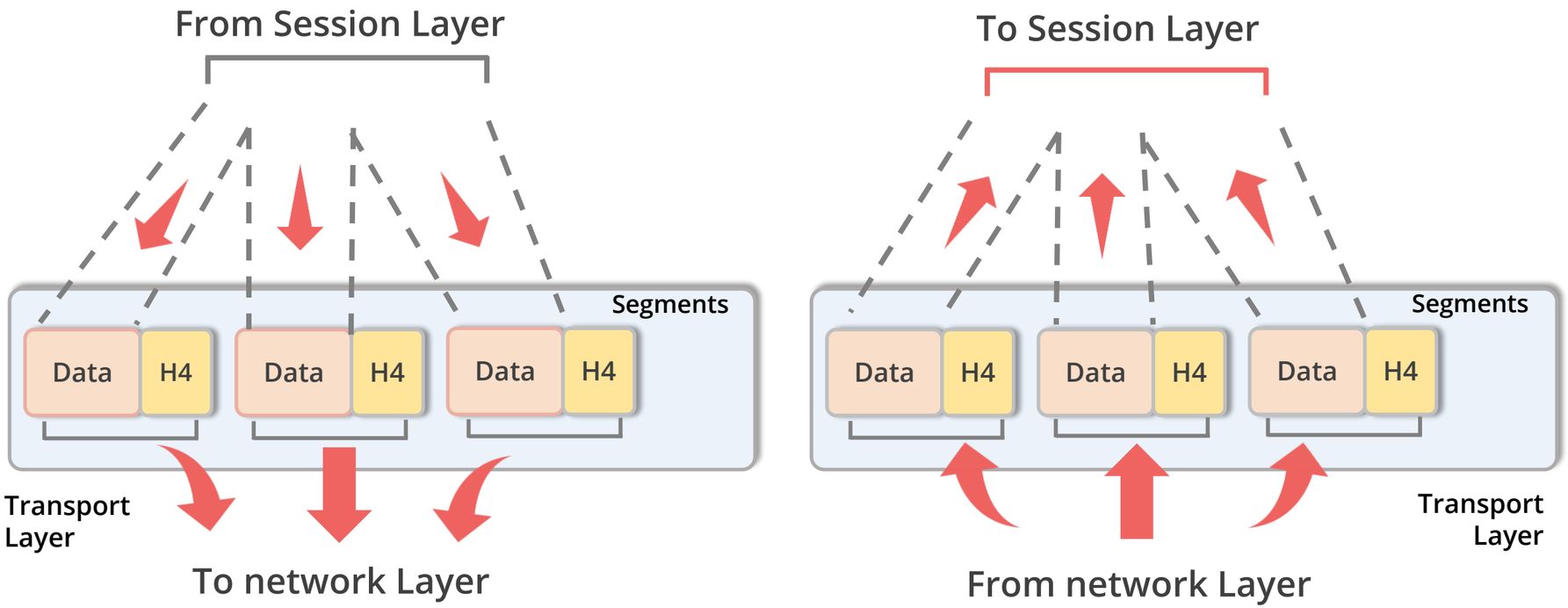
Hierarchy of Routing Protocols

Hierarchy of different routing protocols is illustrated in the figure below:



Transport Layer

Transport layer 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.



Transport Layer

The transport layer:

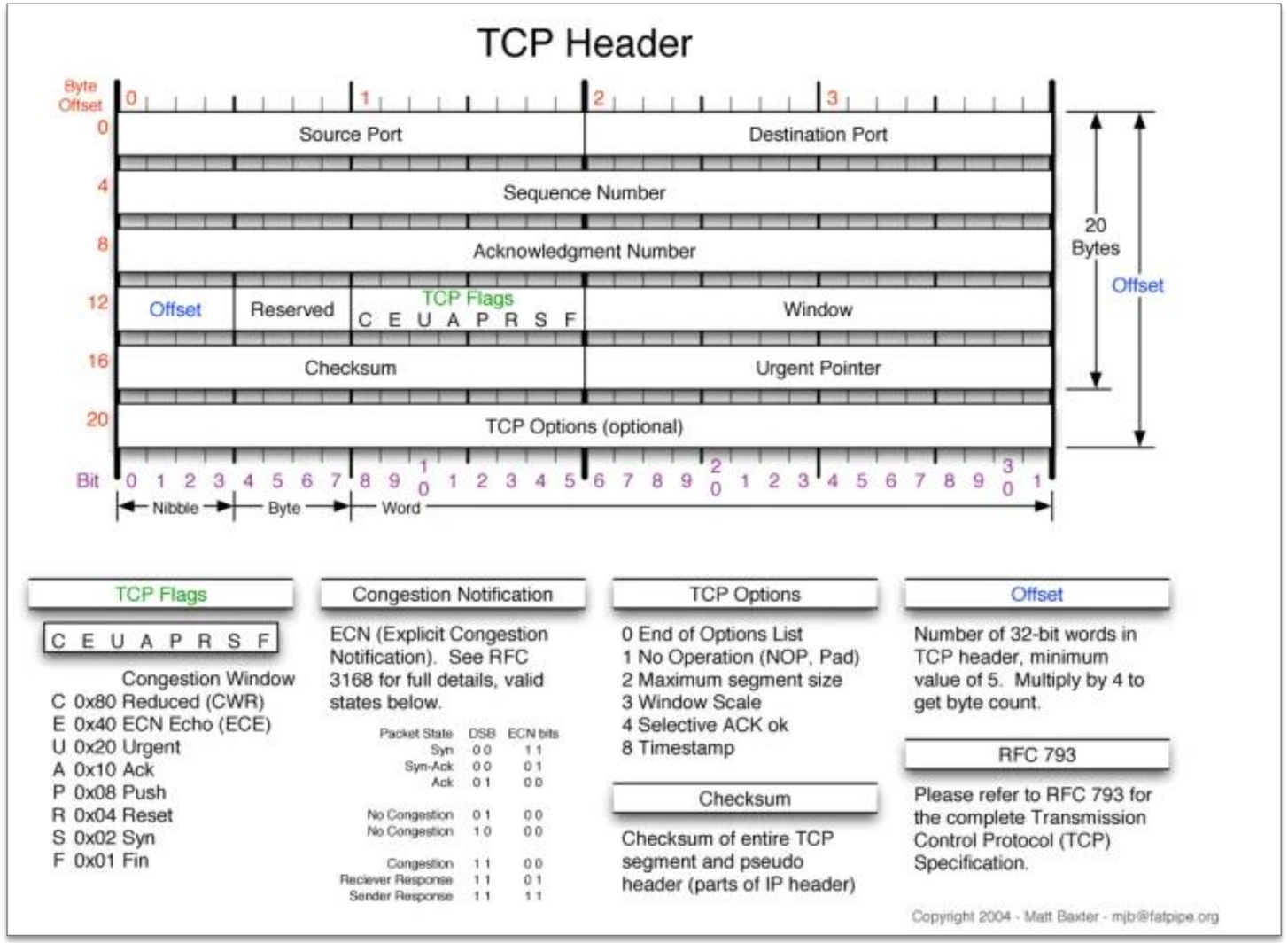
- Establishes a logical connection between the sending host and destination host on a network
- Ensures that the data units are delivered free of errors
- Ensures that data units are delivered in sequence
- Ensures that there is no loss or duplication of data units
- Provides connectionless or connection-oriented service
- Is responsible for providing mechanisms for multiplexing upper-layer applications, session establishment, and the teardown of virtual circuits

  Example: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

- Provides services to the session layer

Transmission Control Protocol (TCP)

TCP provides a complete duplex and reliable connection. It is costly in terms of network overhead and is slower than UDP.

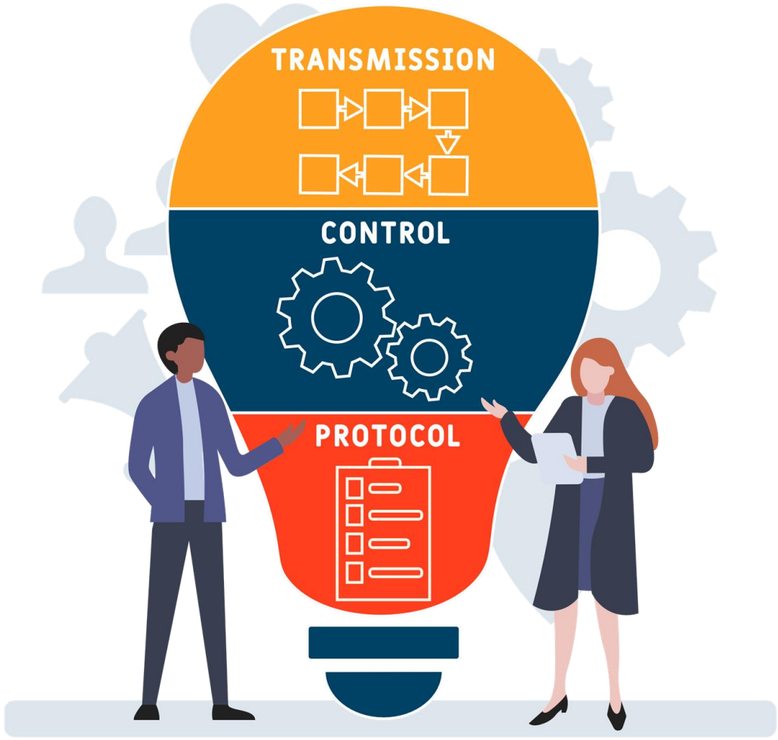


Transmission Control Protocol (TCP): Goals

Reliable data transport is addressed by TCP to ensure the following goals are achieved:

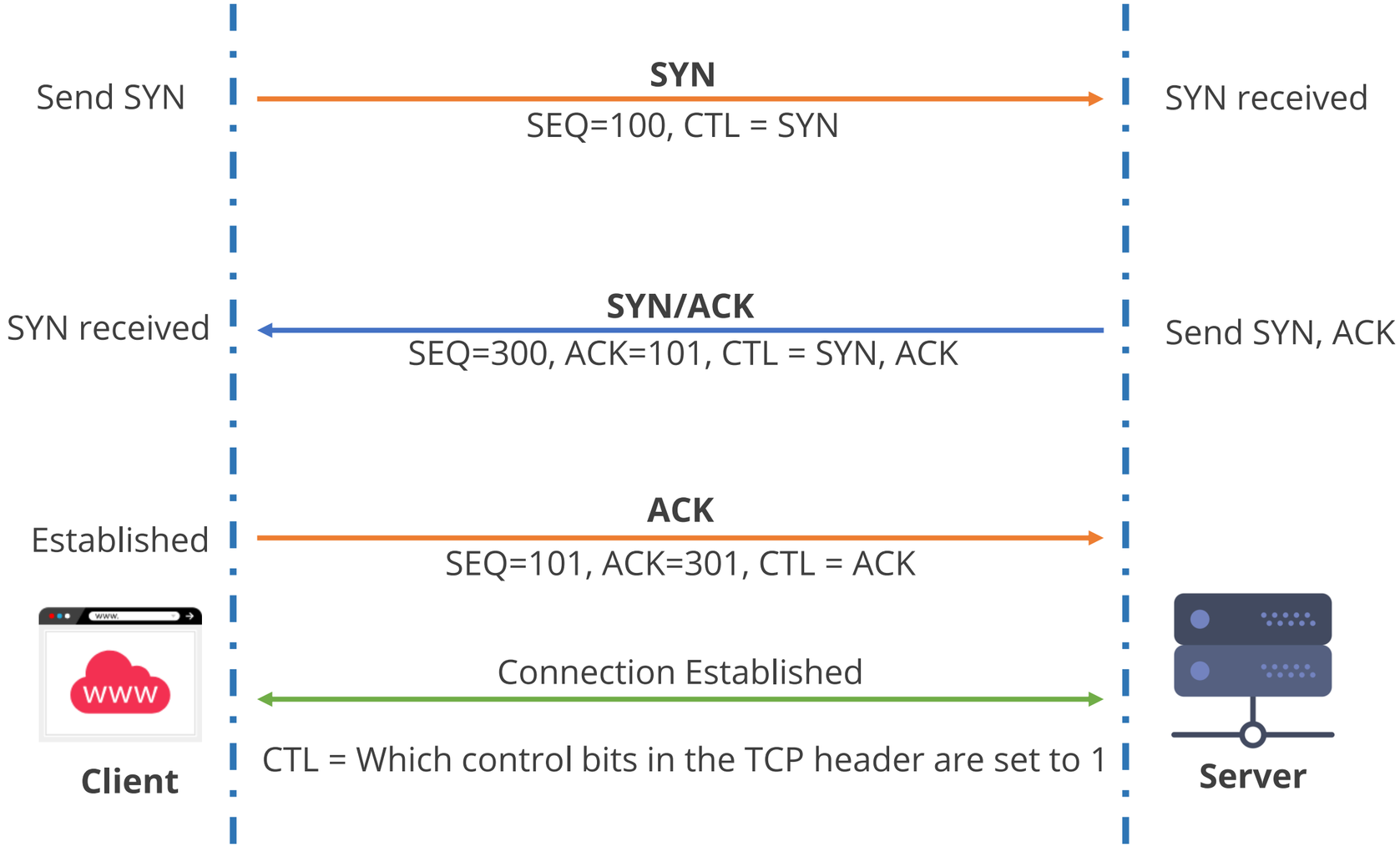
- An acknowledgment is sent back to the sender.
- Any unacknowledged segments are retransmitted.
- Segments are sequenced back in their proper order.
- A manageable data flow is maintained.
- Port types are reserved or well-known ports (0 to 1023), registered ports (1024 to 49151), and dynamic ports (49152 to 65535).

Example: 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.

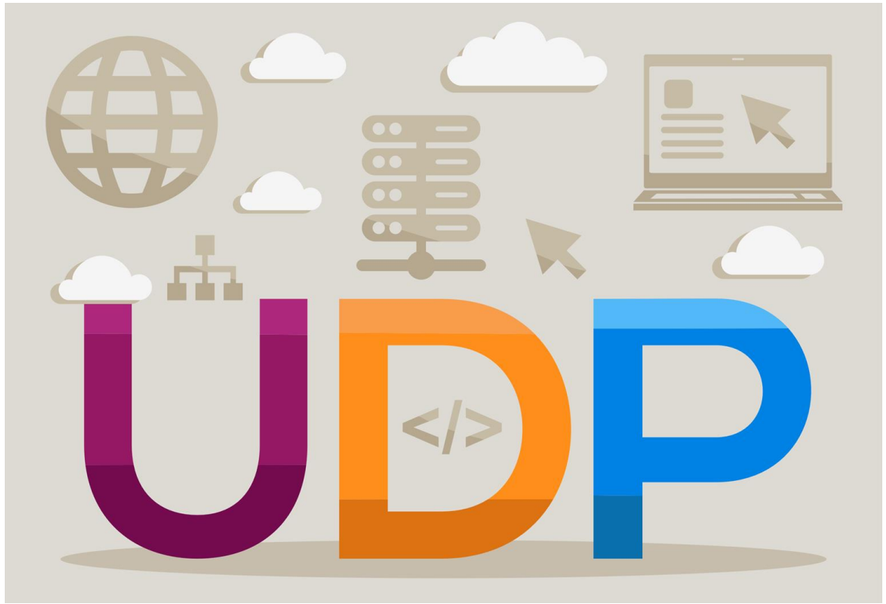


User Datagram Protocol (UDP)

UDP is like TCP.

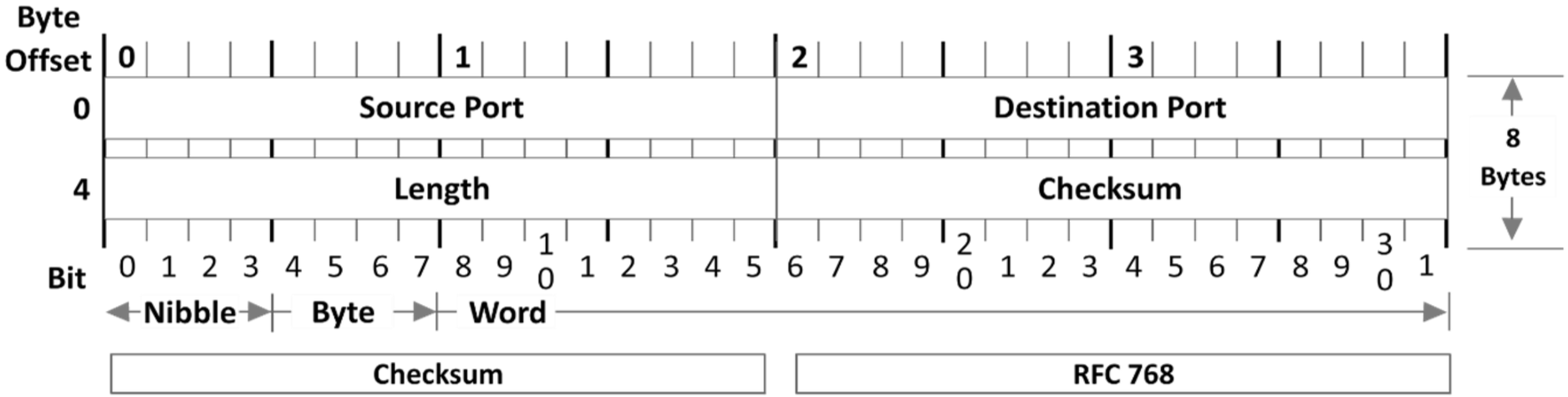
- It gives only **best effort** delivery.
- It is referred to as an unreliable protocol.
- It is considered a connectionless protocol.

Example: DNS, TFTP, and VoIP



User Datagram Protocol (UDP)

User Datagram Protocol(UDP) is illustrated below:



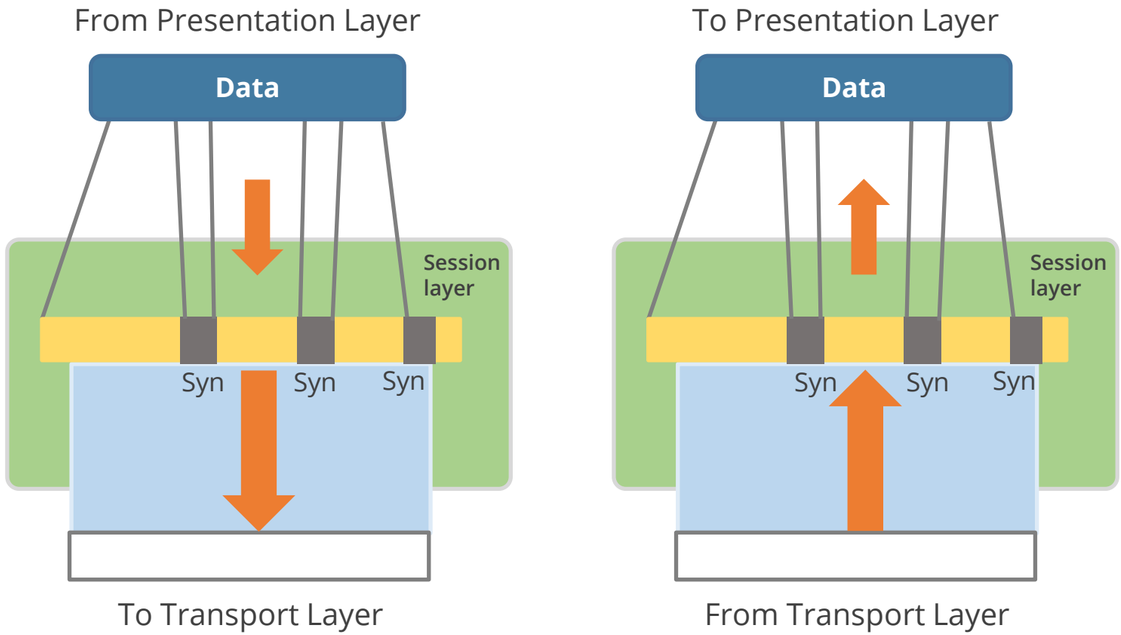
TCP Vs. UDP

	TCP	UDP
	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 acknowledgement of data and can retransmit if the user requests	Neither takes acknowledgement nor retransmits the lost data

Session Layer

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

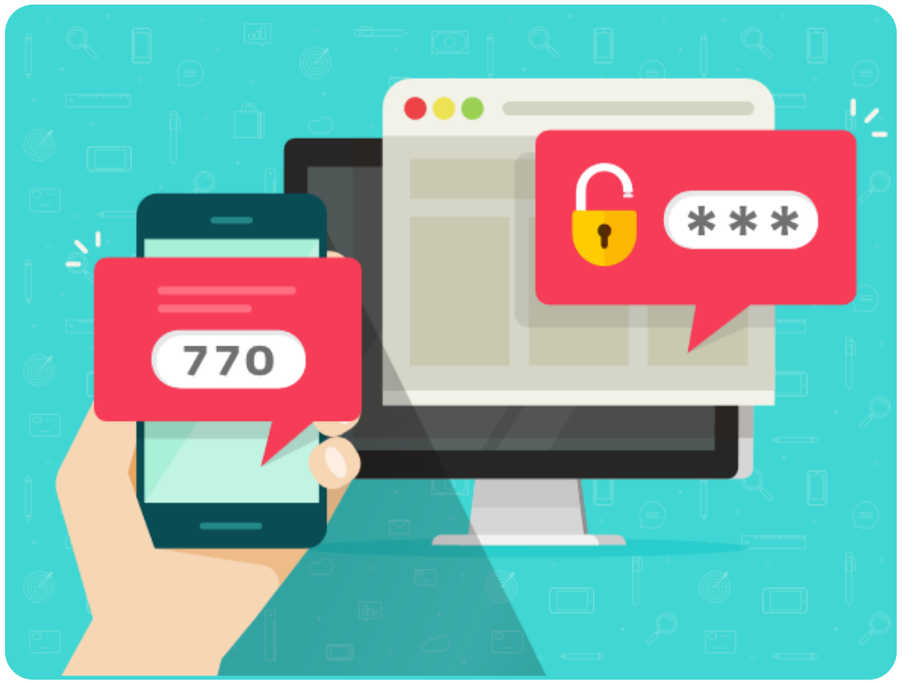
- The session layer offers three different modes:
  - Simplex
  - Half duplex
  - Full duplex



Session Layer

- This layer splits up a communication session into three different phases:
  - Connection establishment
  - Data transfer
  - Connection release

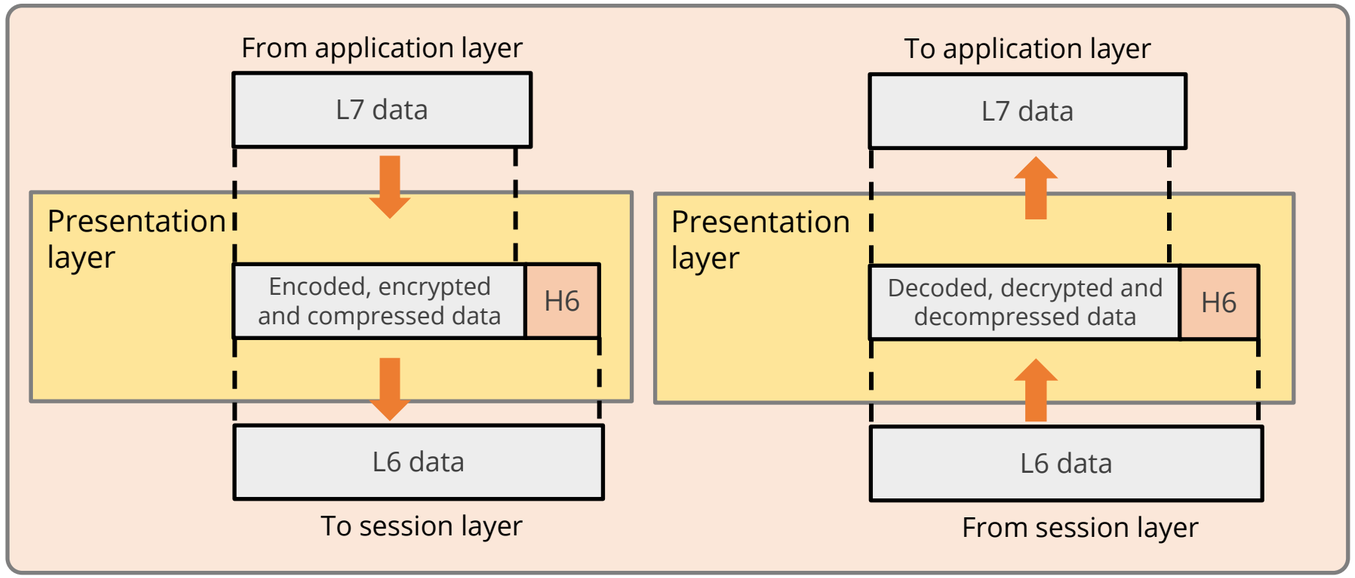
  Example: NFS, SQL, and RPC
- The session layer provides services to the presentation layer.



Presentation Layer

- Presentation layer presents data and provides services to the application layer.
- It is responsible for defining how information is presented to the user in the interface (application layer) that they are using.
- This layer provides a common means of representing data.
- It acts as a translator, 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.

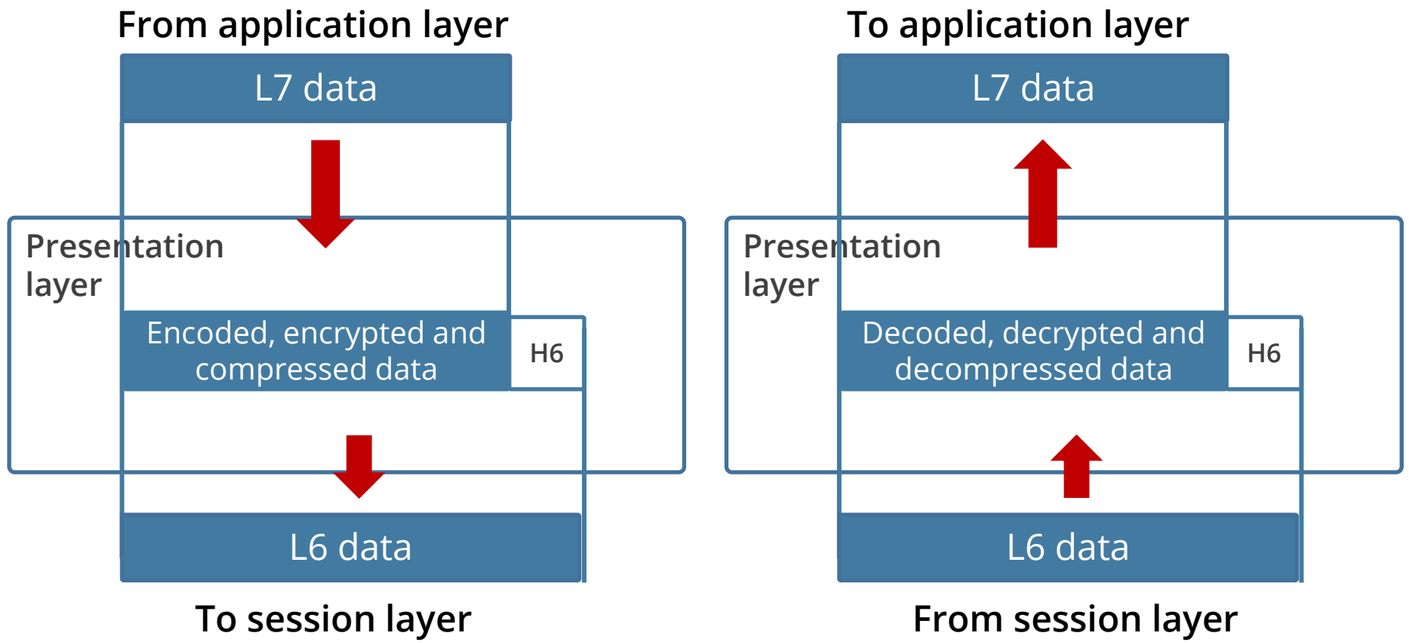
Example: ASCII, BMP, GIF, JPEG, WAV, AVI, and MPEG



Presentation Layer

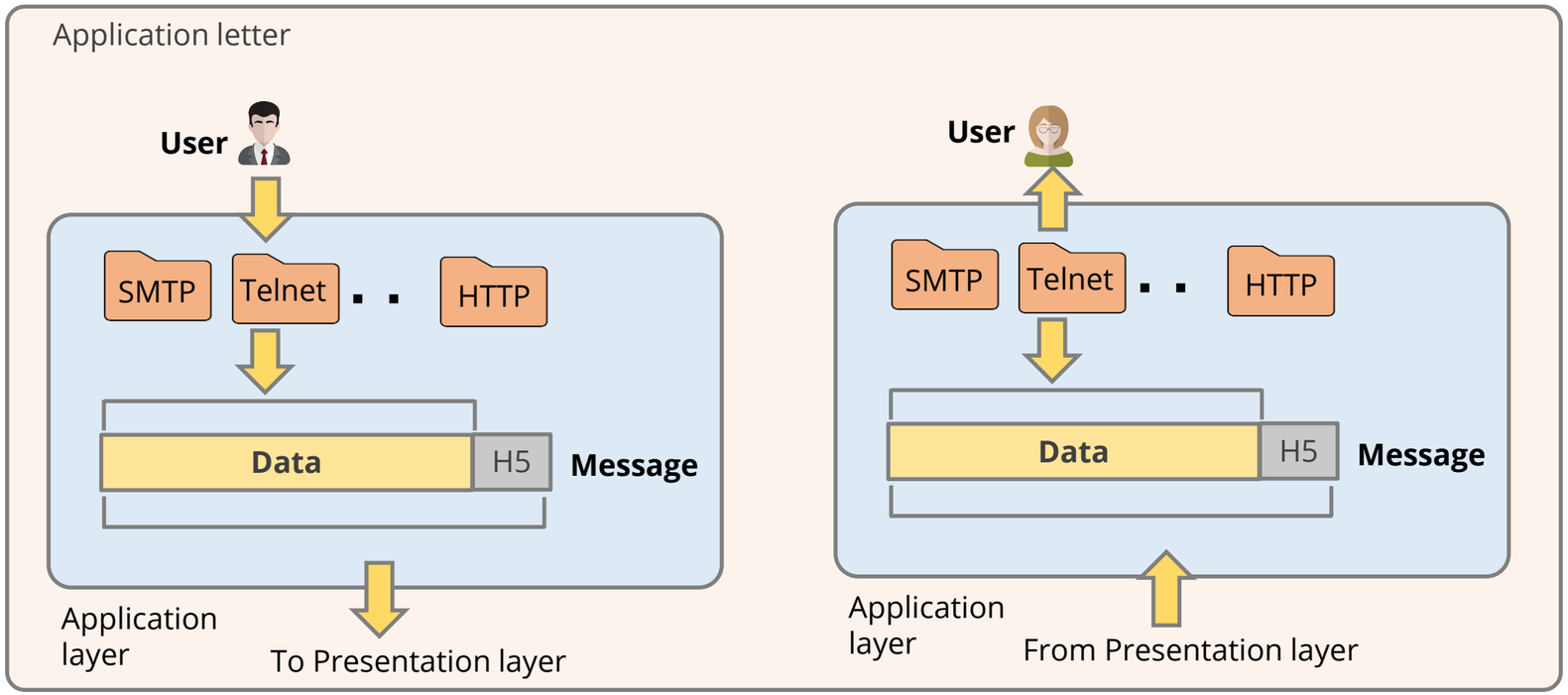
Its functions are:

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



Application Layer

- Application layer supports the components that deal with the communication aspects of an application.
- It is at this point that the data is in a visual form a user can truly understand rather than binary zeros and ones.
- It does not include applications, rather only protocols that support the applications.
- It deals with properly processing and formatting the data before it moves to the layer below.



Application Layer

- This layer 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).

Application	Represents data to user plus 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

Network Access Layer

Network Access Layer

- The host and the network data exchange are monitored by this layer.
- OSI layer's physical and data link layers match this layer.
- It defines protocols for the physical transmission of data and oversees hardware addressing.

Example: Ethernet and Point-to-Point Protocol (PPP)

Internet Layer

Internet Layer

Internet layer designates the protocols related to the logical transmission of packets over the network. The OSI network layer matches the internet layer.

The functions of Internet Layer:

- Giving node IP address
- Handling routing of packets
- Controlling communication flows between hosts

Example: Internet Protocol (IP) and Address Resolution Protocol (ARP)

Host-to-Host Layer

Host-to-host Layer

Host-to-host layer defines protocols for setting up the level of transmission service.

The functions of host-to-host layer:

- End-to-end communications
- Error-free delivery of the data
- Data packet sequencing
- Data integrity

Example: Transmission Control Protocol and User Datagram Protocol

Application Layer

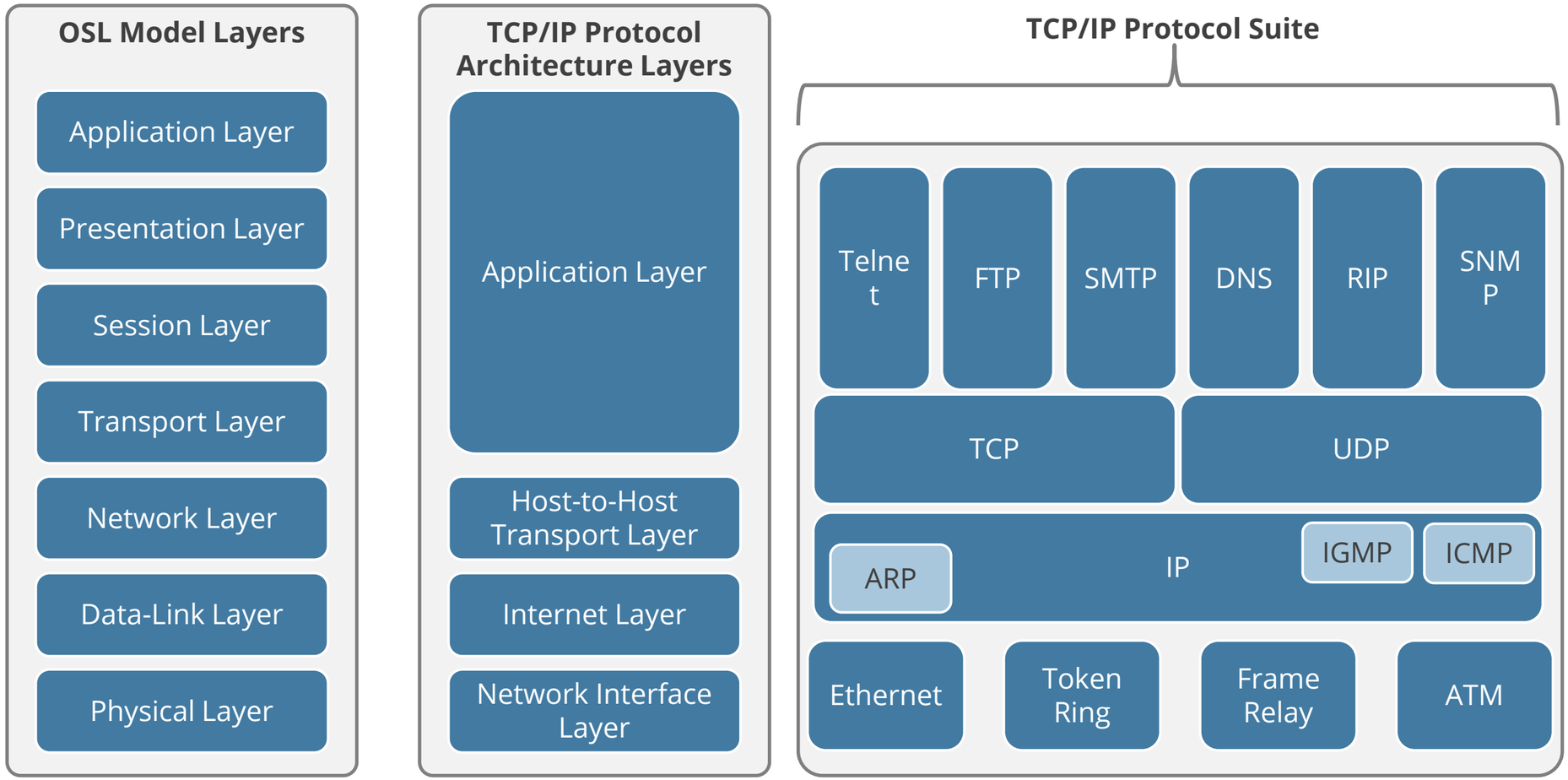
Application Layer

- Application layer is user data created by the application that is communicated to other processes or applications on it or another host.
- The OSI application, presentation, and session layers match with this layer.

Examples: HTTP and FTP

Comparison of OSI and TCP/IP Models

The TCP/IP model is very similar to the OSI model, however with fewer layers.



Introduction to IP Addressing

All hosts on the Internet have a logical and numerical ID called an Internet Protocol (IP) address.

- 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.
- IP addressing provides an unreliable datagram service.
- IP address includes network and host.

IP ADDRESS

IPv4 and IPv6

There are two versions of IP in use, IP Version 4 (IPV4) and IP Version 6 (IPV6).

- IPV4 version provides best effort packet delivery.
- Network addresses in IPv4 are 32 bits in length and are expressed as a dot-decimal.

Example: 192.168.0.100

- IPv6 address space is 128-bit.
- The new address space provides the potential for a maximum of 2128, or about 3.403×1038 addresses.
- IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons.

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

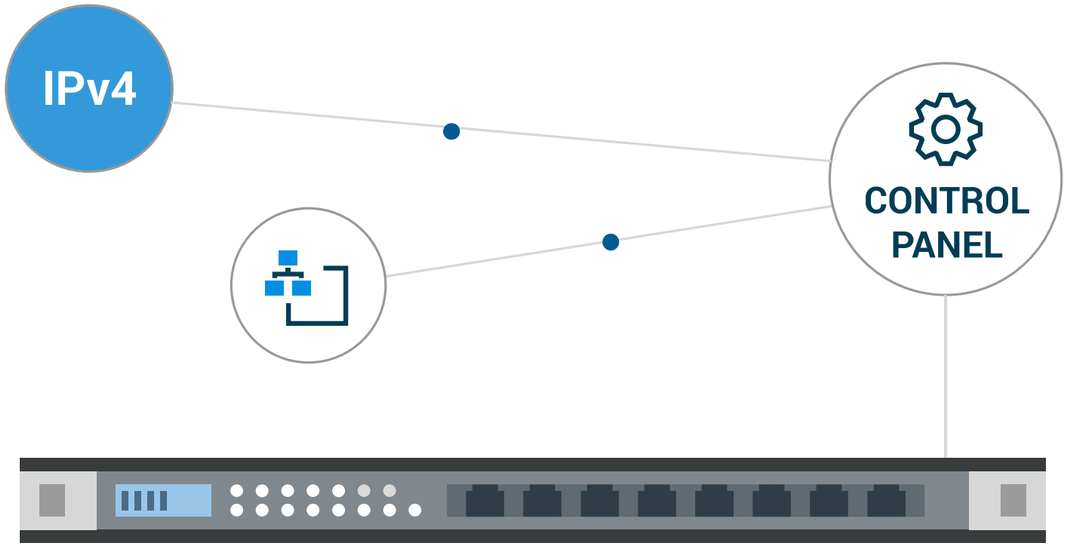
IPv4

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

IPv4 version provides best effort packet delivery.

- Network addresses in IPv4 are 32 bits in length and are expressed as dot-decimal.

Example: 192.168.0.100



Classful IP Addressing

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

- The network number: first 8 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	2 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

Class A is an 8-bit network address.

- Has 24-bit host address
- IP ranges from 1.0.0.0 to 126.255.255.255
- Implied net mask of 255.0.0.0
- Contains 16,777,214 nodes
- 126 networks created

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	2 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

Class B is a 16-bit network address.

- Has 16-bit host address
- IP ranges from 128.0.0.0 to 191.255.255.255
- Implied net mask is 255.255.0.0
- Contains 65,534 nodes
- 16,382 networks created

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	2 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

Class C is a 24-bit network address.

- Has 8-bit host address
- IP ranges from 192.0.0.0 to 223.255.255.255
- Implied net mask is 255.255.255.0
- Contains 254 nodes
- Over 2 million networks created

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**	**2 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	2 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**

Classless Inter-Domain Routing

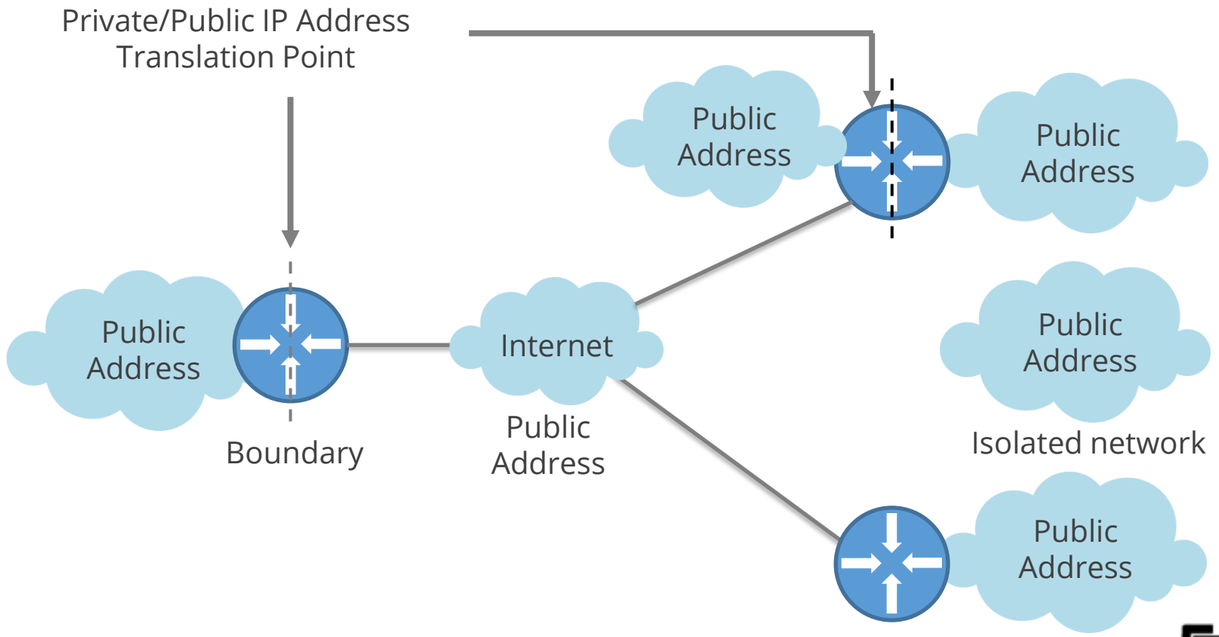
Classless Inter-Domain Routing (CIDR) is a method for allocating IP addresses and routing Internet Protocol packets.

- CIDR intends to slow the growth of routing tables on routers across the Internet and to help slow the rapid exhaustion of IPv4 addresses.
- CIDR disposes the rigid scheme of class A, B, and C networks.
- CIDR permits the creation of variable length subnet mask from 8 bits to 31 bits.
- CIDR leads to an efficient allocation of the available IP addresses on Internet.
- CIDR notation is a syntax for specifying IP addresses and their associated routing prefixes.

Example: 192.168.1.3/23

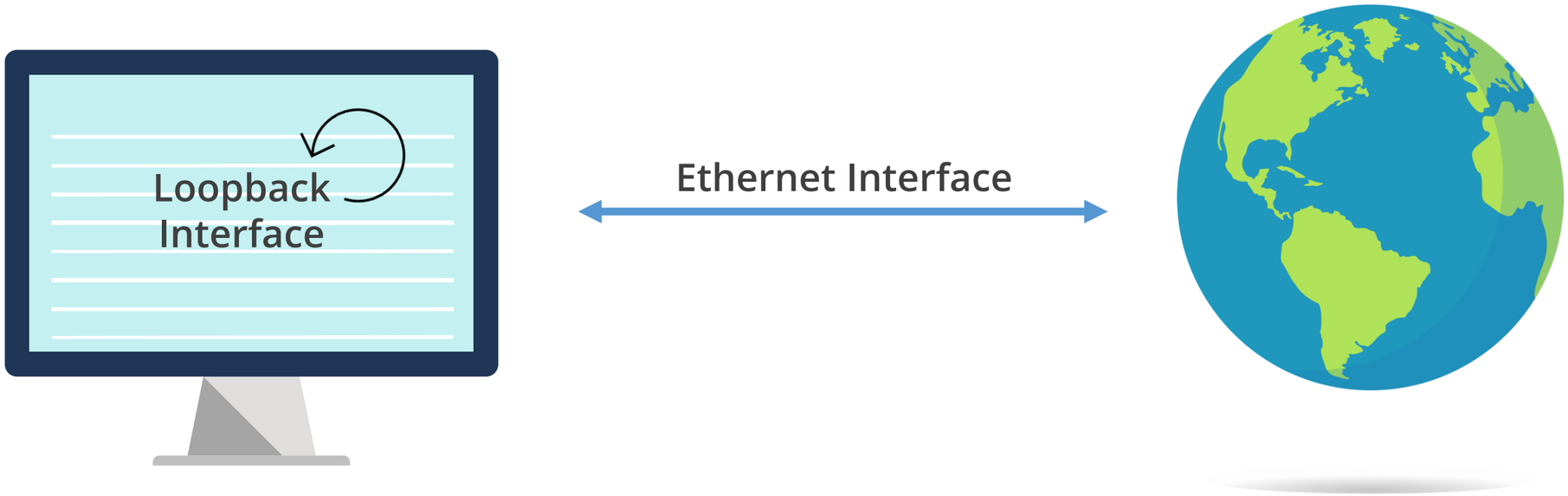
Private Networks and Loopback Address

- All network addresses are not available for general use.
- Private networks 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 private network 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



Private Networks and Loopback Address

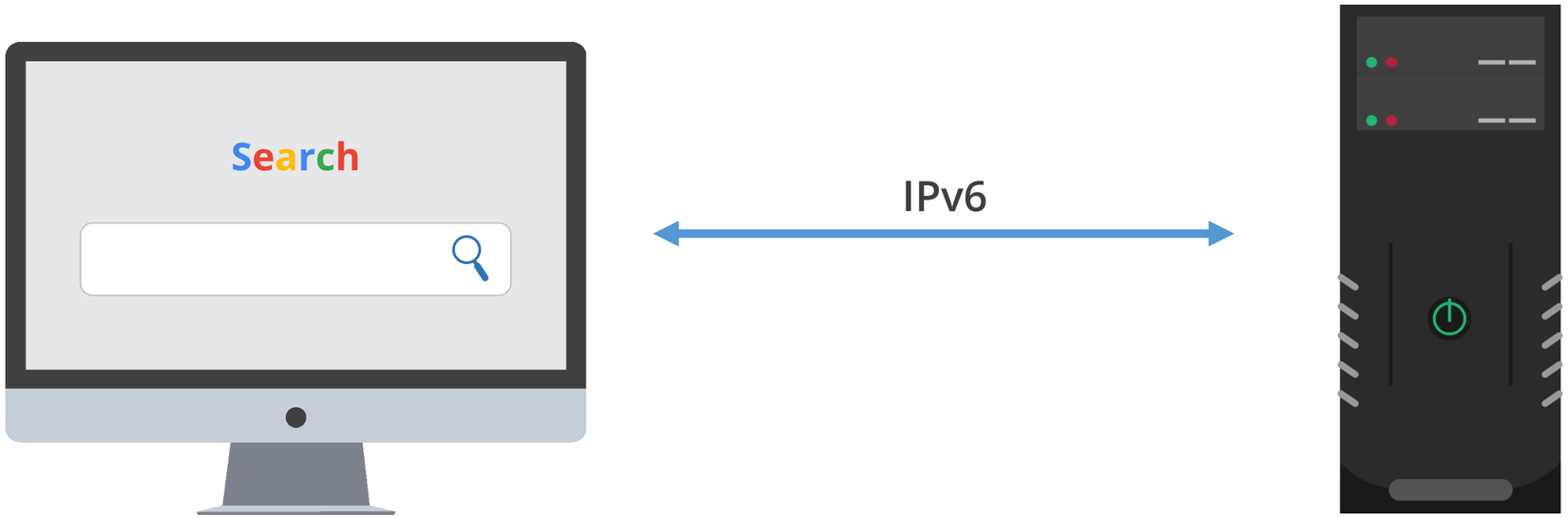
- A loopback address is a special address used to signify a node's address.
- Loopback addresses 127.0.0.1 point back to the issuing computer.



IPv6

- IPv6 address space is 128 bit.
- The new address space provides the potential for a maximum of 2^{128} or about 3.403×10^{38} addresses.
- IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons.

  Example: FE80:0000:0000:0000:0202:B3FF:FE1E:8329
- It allows scoped addresses, end-to-end secure transmission, and authentication.
- It has more flexibility, routing capabilities, and allows QoS.



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

- An IPv6 address is made of 128 bits divided into eight 16 bit blocks.
- Each block is then converted into 4 digit hexadecimal numbers separated by colon symbols.
- For example, given below is a 128-bit IPv6 address represented in the binary format and divided into eight 16-bit blocks:
  - 0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011
- Hexadecimal equivalent of an IPv6 above 128 bits is 2001:0000:3238:DFE1:0063:0000:0000:FEFB.
- Even after converting into the hexadecimal format, IPv6 address remains long.

IPv6 Address Structure

- IPv6 provides some rules to shorten the address.
  - **Rule 1**: Discard leading zero(s):

    In Block 5, 0063, the leading two zeros can be omitted:

    2001:0000:3238:DFE1:63:0000:0000:FEFB
  - **Rule 2**: If two or more blocks contain consecutive zeros, omit them all and replace them with double colon sign (::) as shown:

    2001:0000:3238:DFE1:63::FEFB
- Consecutive blocks of zeros can be replaced only once by **::**.
- If there are still blocks of zeros in the address, they can be shrunk down to a single zero:

  2001:0:3238:DFE1:63::FEFB

IPv6 Address Terminology

Prefix

- The prefix 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.

Prefix length

- The prefix length 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

- The interface ID is equivalent to the host portion of an IPv4 address.
- IPv6 uses the term interface ID 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

An IPv6 node or device is anything that can have an IPv6 address, including traditional devices such as computers and printers along with other types of devices, such as webcams, embedded devices, and Internet of Things (IoT) devices.

Node or device

IPv6 Address Types

Global Unicast Address (GUA)

- An IPv6 global unicast address (GUA) is a globally unique and routable IPv6 address
- Equivalent to a public IPv4 address
- Begins with either a hexadecimal 2 or 3.
- GUA can be either a source or destination IPv6 address
- Example of a global unicast address: 2001:db8:cafe:1::100

Link-Local Unicast Address

- A unicast address that is local only on that link. The term link refers to a logical network segment or a subnet
- Limited to the link and are not routable beyond the local subnet
- Typically created automatically by the host operating system
- Can be either source or destination IPv6 addresses
- Usually begin 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.
- 6to4 is simply a transparent mechanism used as a transport layer between IPv6 nodes.
- 6to4 does not facilitate interoperation between IPv4-only hosts and IPv6-only hosts.
- 6to4 performs 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

IPv6

- IP address size of 128 bits
- Has a total range of 340 undecillion possible addresses
  - 20021:db8::ff00:42:8329
- The scalability of multicast routing is improved by adding a scope field to the multicast address
- Anycast address is used to send a packet to any one node in a group of nodes
- Extensions to support authentication, data integrity, and data confidentiality

IPv4

- IP address size of 32 bits
- Has a total range of 4.3 billion possible addresses
  - 123.45.67.89
- No options of scalability
- No options of anycast
- No extensions available for support

Discussion

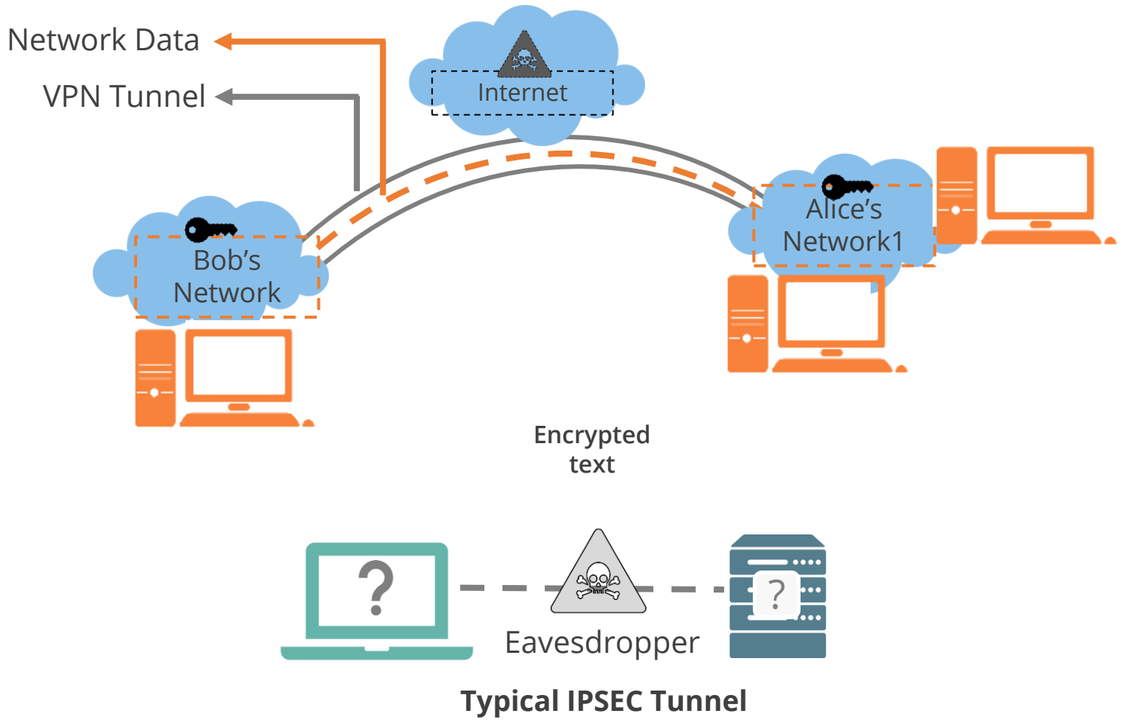
Discussion

What are the main responsibilities of the Internet Assigned Numbers Authority (IANA)?

Internet Security Protocol (IPsec)

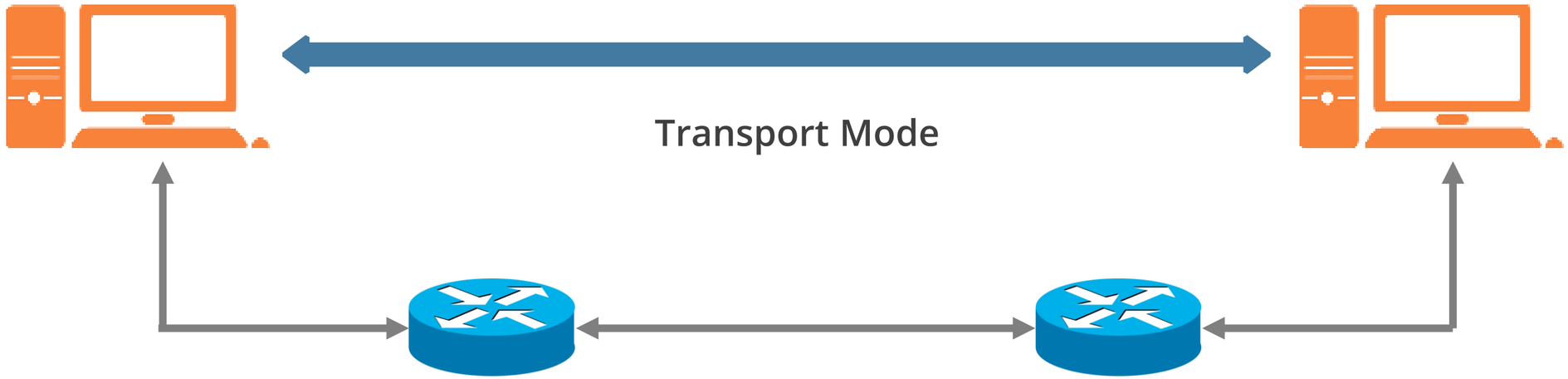
Internet Protocol Security (IPsec) is a protocol suite used for securing Internet Protocol (IP) communications.

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



Typical IPSEC Tunnel

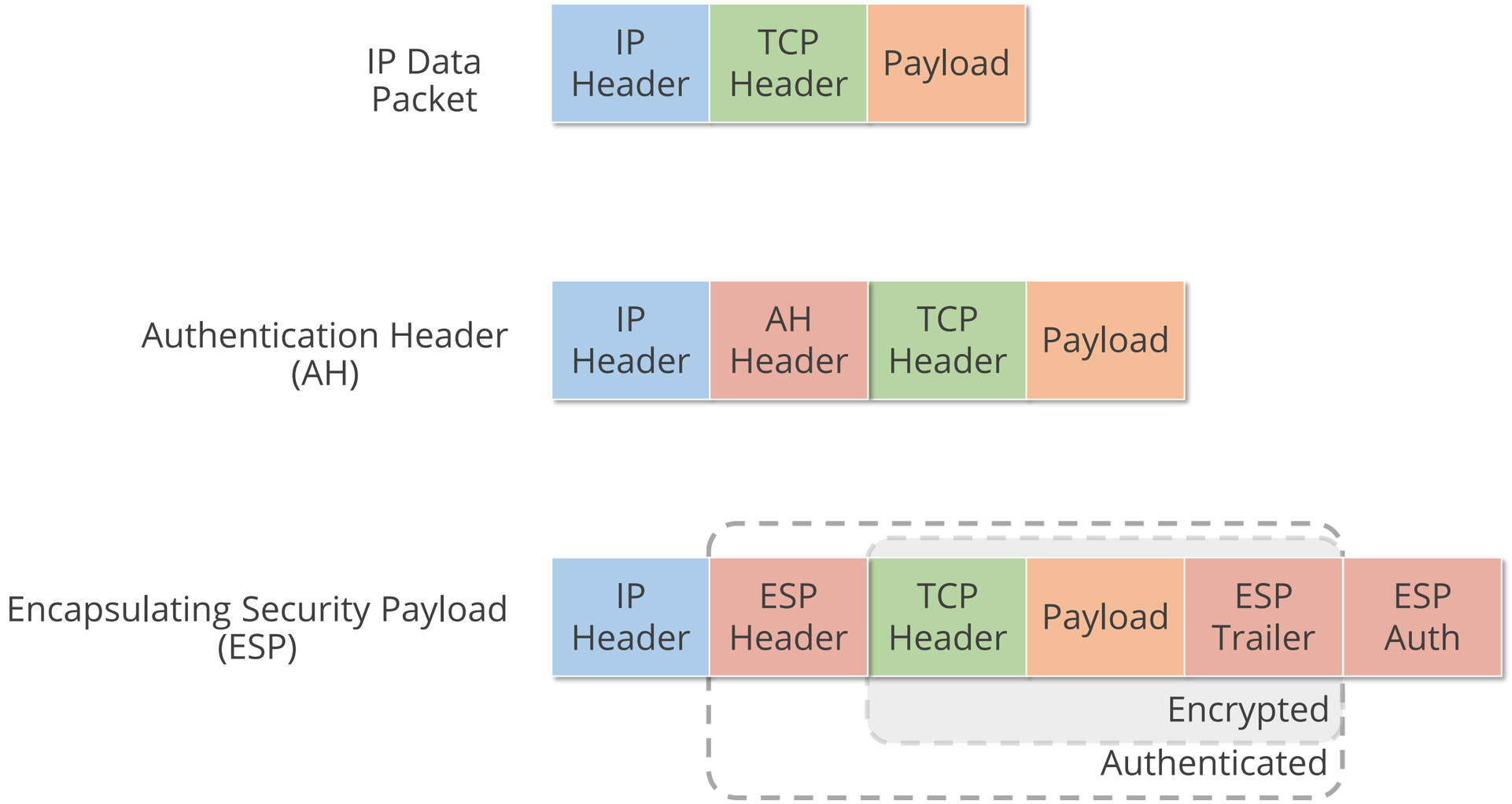
IPsec Modes: Transport Mode



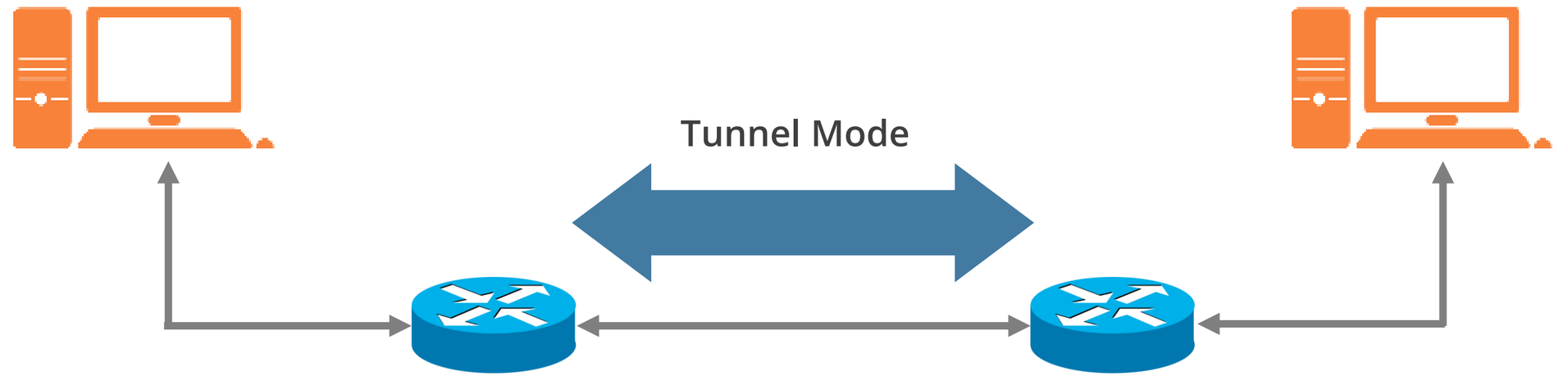
In transport mode, only the data is encrypted.

It is designed for peer-to-peer communication.

IPsec Modes: Transport Mode



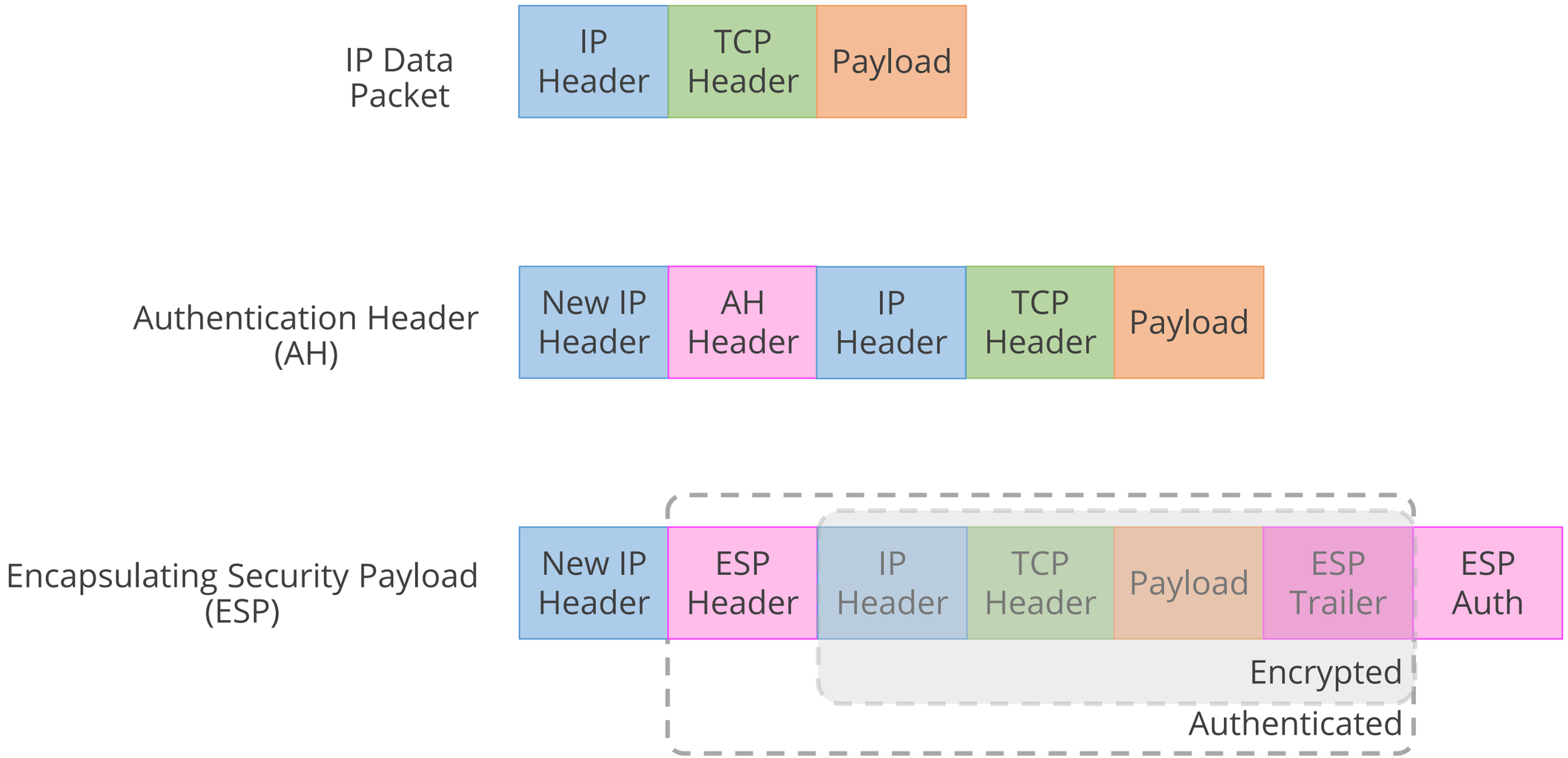
IPsec Modes: Tunnel Mode



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

It is designed for gateway-to-gateway communication.

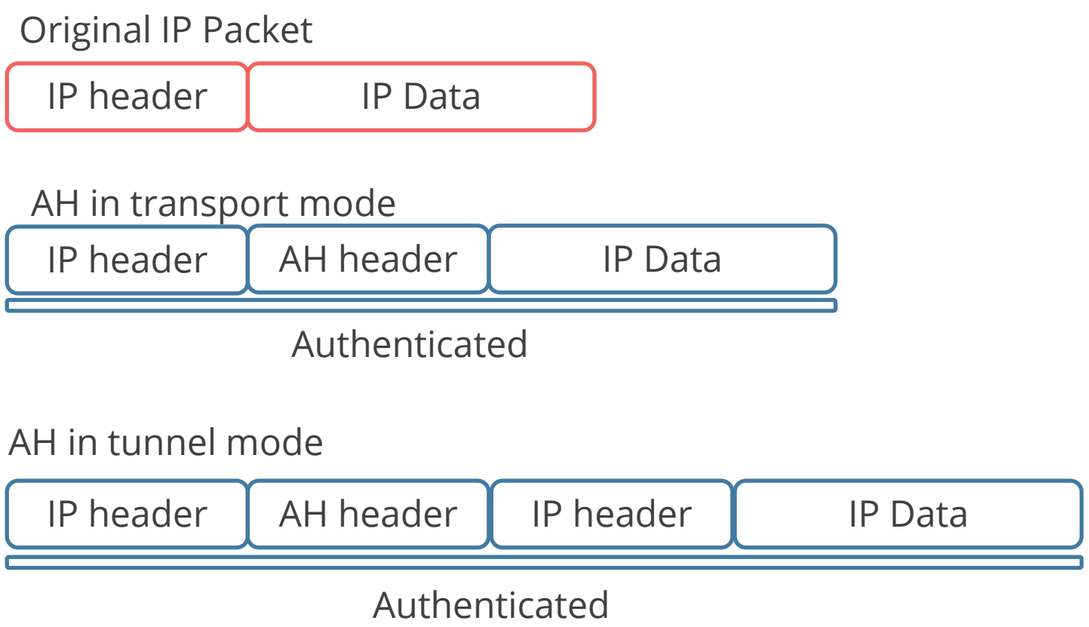
IPsec Modes: Tunnel Mode



IPsec Security Protocols: Authentication Header (AH)

AH is an authentication protocol.

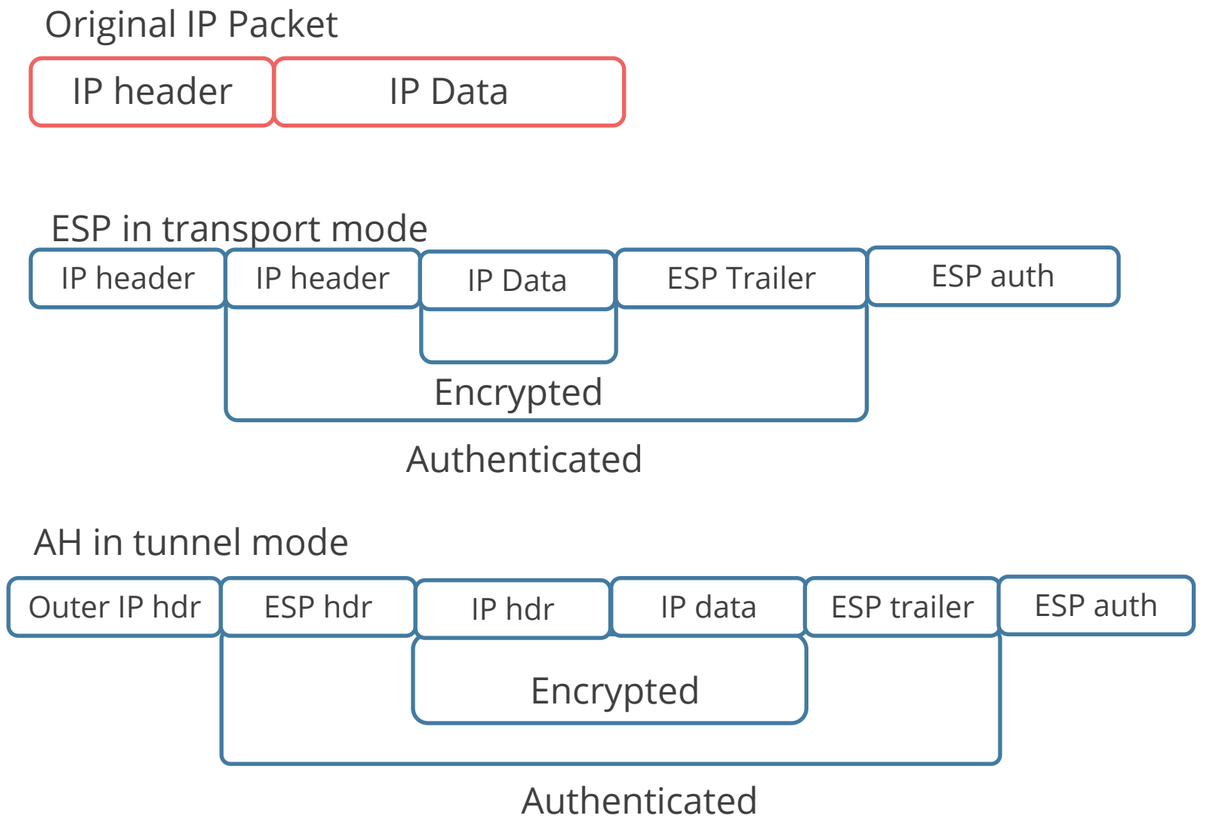
- It provides authentication and integrity for every packet of network data.
- It acts as a digital signature for the data.
- Confidentiality is not offered.
- It authenticates the IP packet data and parts of the IP header.
- In transport mode, after the original IP header, the AH protocol inserts an AH header.
- In tunnel mode, the AH header is inserted before the original, inner and IP header but after the outer header.



IPsec Security Protocols: Encapsulating Security Payload (ESP)

ESP is an authentication and encryption protocol.

- It provides confidentiality by encryption of data packets.
- Authentication and integrity are provided optionally.
- In transport mode, the ESP protocol, an ESP header, is inserted after the original IP header.
- In tunnel mode, the ESP header is inserted before the original, inner IP header but after the outer header.
- All data is encrypted and or or authenticated after the ESP header.



Components of IPsec Process: SA and ISAKMP

Security Association (SA)	• Used for negotiating ESP or AH parameters • One-way or simplex connection • Two SAs: One for each direction are used if two systems communicate via ESP or AH • The security parameter index (SPI) is a unique 32-bit number that identifies each simplex SA connection
Internet Security Association and Key Management Protocol (ISAKMP)	• Manages the SA process • Provides a key exchange framework

Components of the IPsec Process: IKE

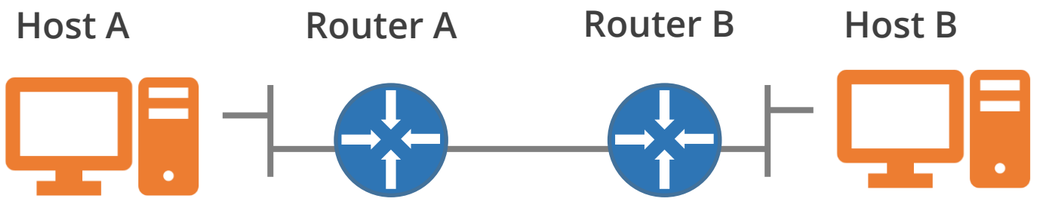
Internet Key Exchange (IKE)

- Has a variety of encryption algorithms like AES, DES, MD%, and SHA-1 can be employed by IPsec
- Negotiates the algorithm selection process
- Eliminates the need to manually specify all the IPsec security parameters
- Allows specifying a lifetime for the IPsec security association
- Allows encryption keys to change during IPsec sessions
- Allows IPsec to provide anti-replay services
- Permits Certification Authority (CA) support for a manageable, scalable IPsec implementation
- Allows dynamic authentication of peers

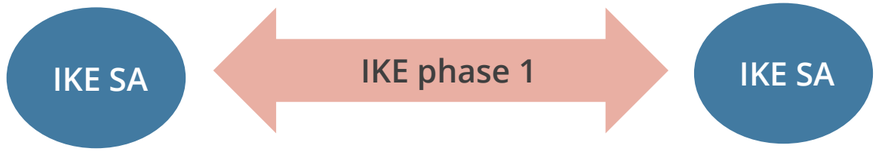
IPsec Process

The steps in the IPsec process are as follows:

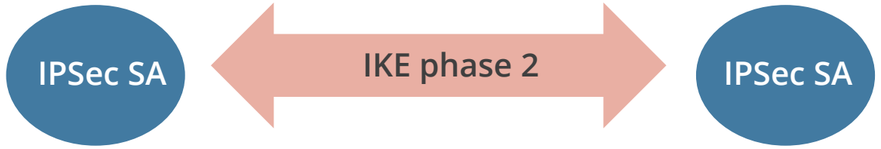
Step 1 : "Interesting traffic" initiates the IPSec Process



Step 2 : IKE phase 1



Step 3 : IKE phase 1



Step 4 : Data Transfer

Step 5 : IPSec tunnel termination

Secure Access Protocols: PGP

- A freeware for securing e-mail communication
- Mainly uses RSA public key encryption and key management
- Uses IDEA symmetric bulk encryption and MD5 hashing
- Supports conventional and PGP public key certificates

Secure Access Protocols: S-HTTP

- S-HTTP (Secure Hypertext Transport Protocol) is used to protect individual messages encrypted with a symmetric session key at the application layer (HTTP).
- The web server creates a session key which is sent to the client after encrypting with the client's public key.

Secure Access Protocols: HTTPS

HTTPS (Hypertext Transport Protocol over SSL) encrypts all information that passes over the connection at the session layer.

Unlike S-HTTP, SSL can be applied to non-HTTP traffic.

Secure Access Protocols: SSL

- Mostly used for e-commerce
- The digital certificate is sent by the server to the client
- The server's public key is verified by CA
- The client generates a symmetric session key
- Using the server’s public key, the session key is encrypted and sent to the server
- Supports asymmetric RSA, symmetric DES, 3DES, & IDEA, and MD5 hashing

Business Scenario

To improve the security of the communication channels, Hilda Jacobs was asked to provide suggestions for securing communication. Kevin worked with Hilda on this assignment, and they produced their report.

The report suggested that all site-to-site communication over the public network or internet should use IPSec. Administrators will have to use SSH instead of Telnet for the administration of network devices or servers over the network. SSH provides more a secure communication channel as compared to Telnet.

Question: What is the major disadvantage of using Telnet?

Business Scenario

To improve the security of the communication channels, Hilda Jacobs was asked to provide suggestions for securing communication. Kevin worked with Hilda on this assignment, and they produced their report.

The report suggested that all site-to-site communication over the public network or internet should use IPSec. Administrators will have to use SSH instead of Telnet for the administration of network devices or servers over the network. SSH provides more a secure communication channel as compared to Telnet.

Question: What is the major disadvantage of using Telnet?

Answer: Telnet communication is unencrypted, and an attacker can easily sniff the data including passwords.

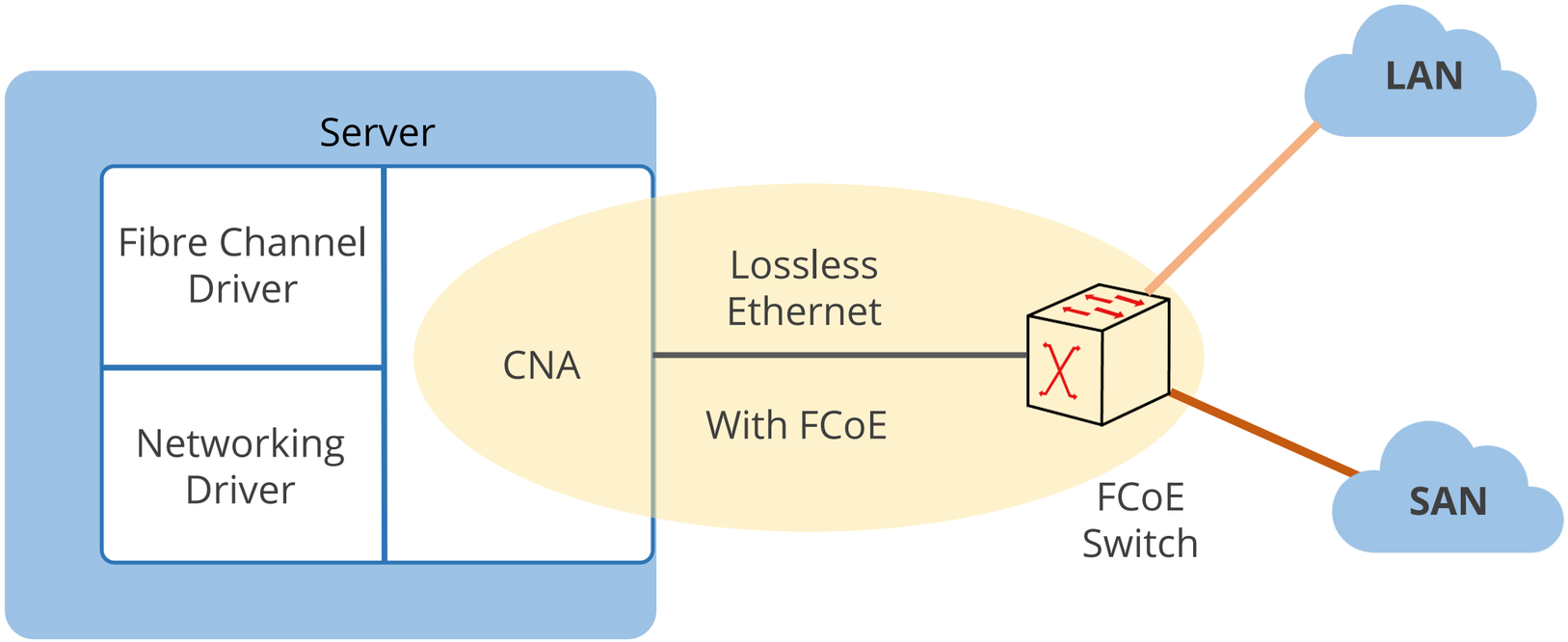
Multi-Protocol Label Switching

Multi-protocol label switching (MPLS) is a mechanism that directs data from one network node to the next based on the short path labels.

- The labels identify virtual links or paths between distant nodes rather than endpoints.
- MPLS can encapsulate packets of various network protocols.
- MPLS operates at a layer 2.5.

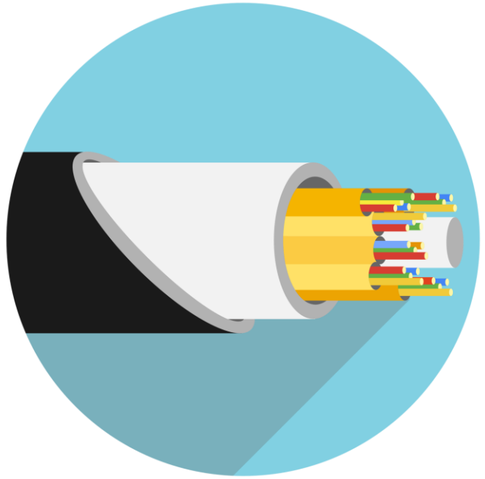
Fiber Channel over Ethernet and Internet Small Computer System Interface

Fiber Channel over Ethernet (FCoE) is a computer network technology that enables Fiber Channel communications to run directly over Ethernet.



Fiber Channel over Ethernet and Internet Small Computer System Interface

It converges storage and IP protocols on a single cable transport and interface by moving Fiber Channel traffic across existing high-speed Ethernet infrastructure.



Internet Small Computer System Interface (iSCSI) is a transport layer protocol that defines how Small Computer System Interface (SCSI) packets should be transported over a TCP/IP network.

Implications of Multi-Layer Protocols

TCP/IP protocol suite consists of various layers with many individual protocols and is also known as Multi-layer protocol.

Following are the advantages and disadvantages of Multi-layer protocol:

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 due to issues of covert channels

Micro-Segmentation

Micro-segmentation is a network technique to create distinct security zones in data centers and cloud environments to isolate workloads from one another and then define security controls to secure them individually.

Micro-Segmentation

Benefits of micro-segmentation:

Reduce network attack surface

By limiting attackers movement from one potentially compromised workload to another

Improve breach containment

By blocking unsanctioned activities and drastically improving threat detection and response times with real-time alerts

Strengthen regulatory compliance

By isolating segments that specifically store regulated data such as PII and PHI

Achieve zero trust with micro-segmentation

By creating and enforcing granular policies

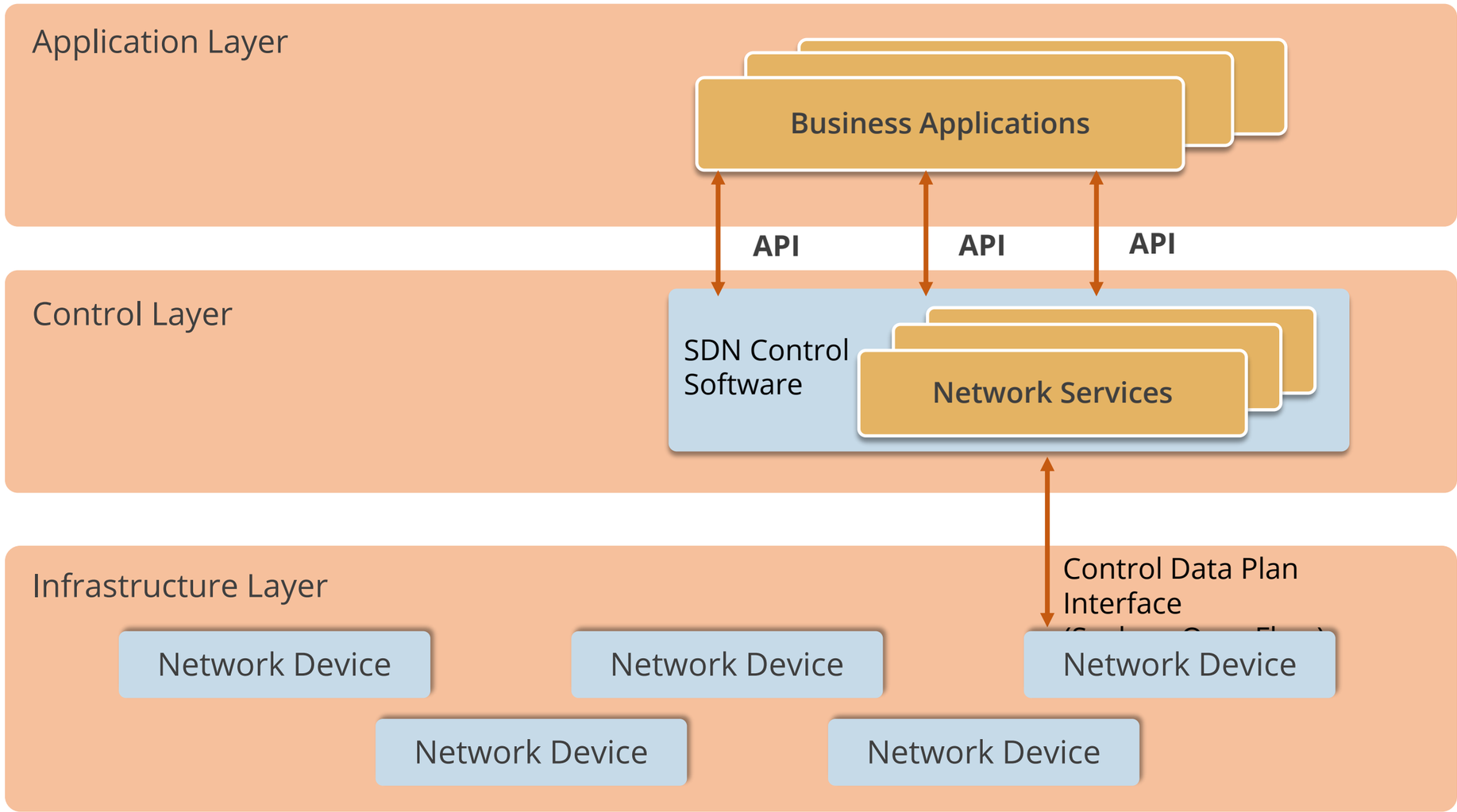
Software-Defined Networking (SDN)

- Software-Defined Networking(SDN) allows network administrators to programmatically initialize, control, change, and manage network behavior dynamically via open interfaces and abstraction of lower-level functionality.

- SDN aims at separating the infrastructure layer (i.e., hardware and hardware-based settings) from the control layer (i.e., network services of data transmission management).

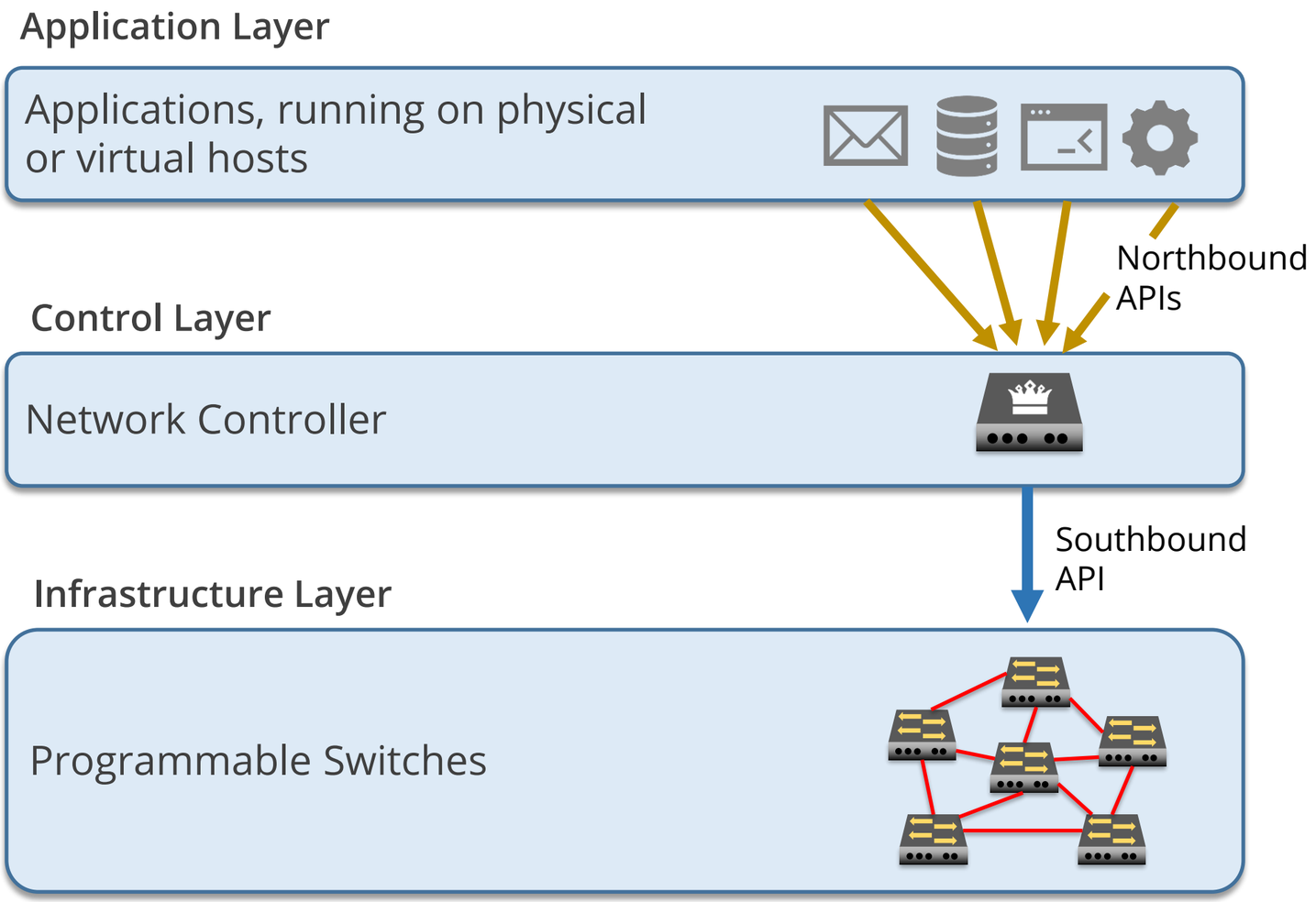
Software-Defined Networking (SDN)

The SDN architecture is illustrated below :



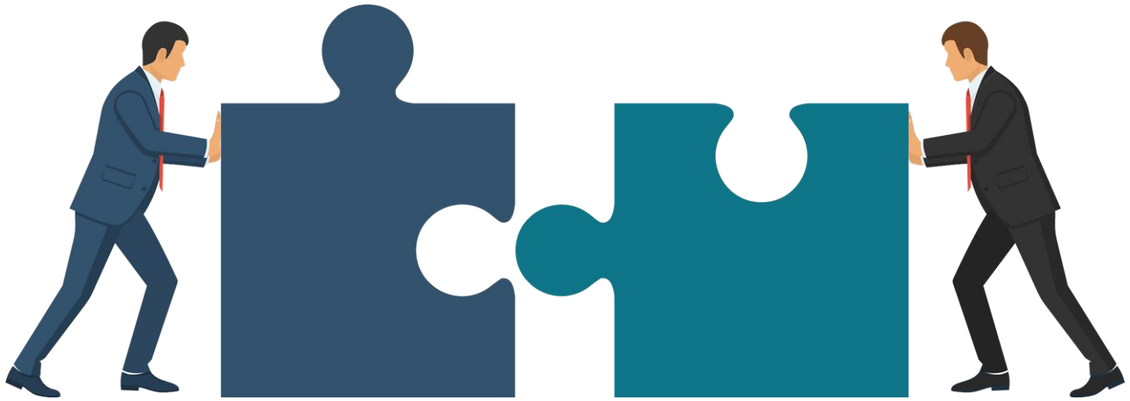
Software-Defined Networking (SDN)

The SDN architecture concept is given below :



Software-Defined Wide Area Network (SD-WAN)

- SD-WAN combines Software-Defined Network (SDN) and a Wide-Area Network (WAN).
- SD-WAN simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism.

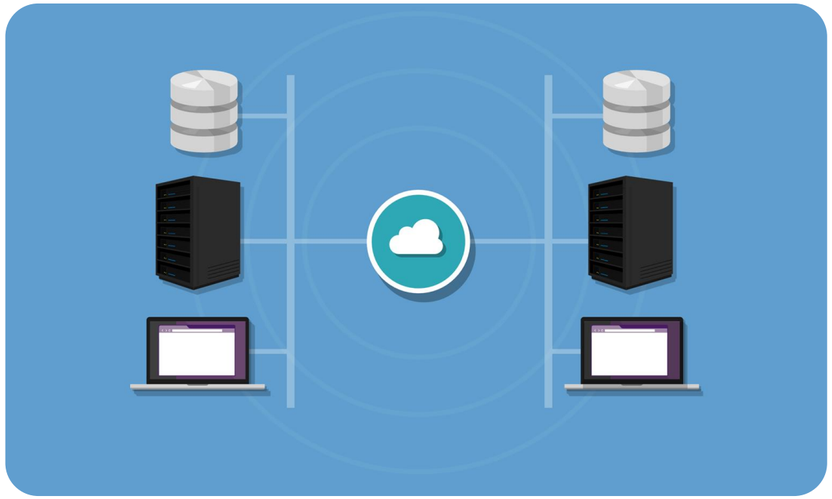


Source: https://www.gartner.com/imagesrv/media-products/pdf/cisco/Cisco-1-5W2DWHZ.pdf

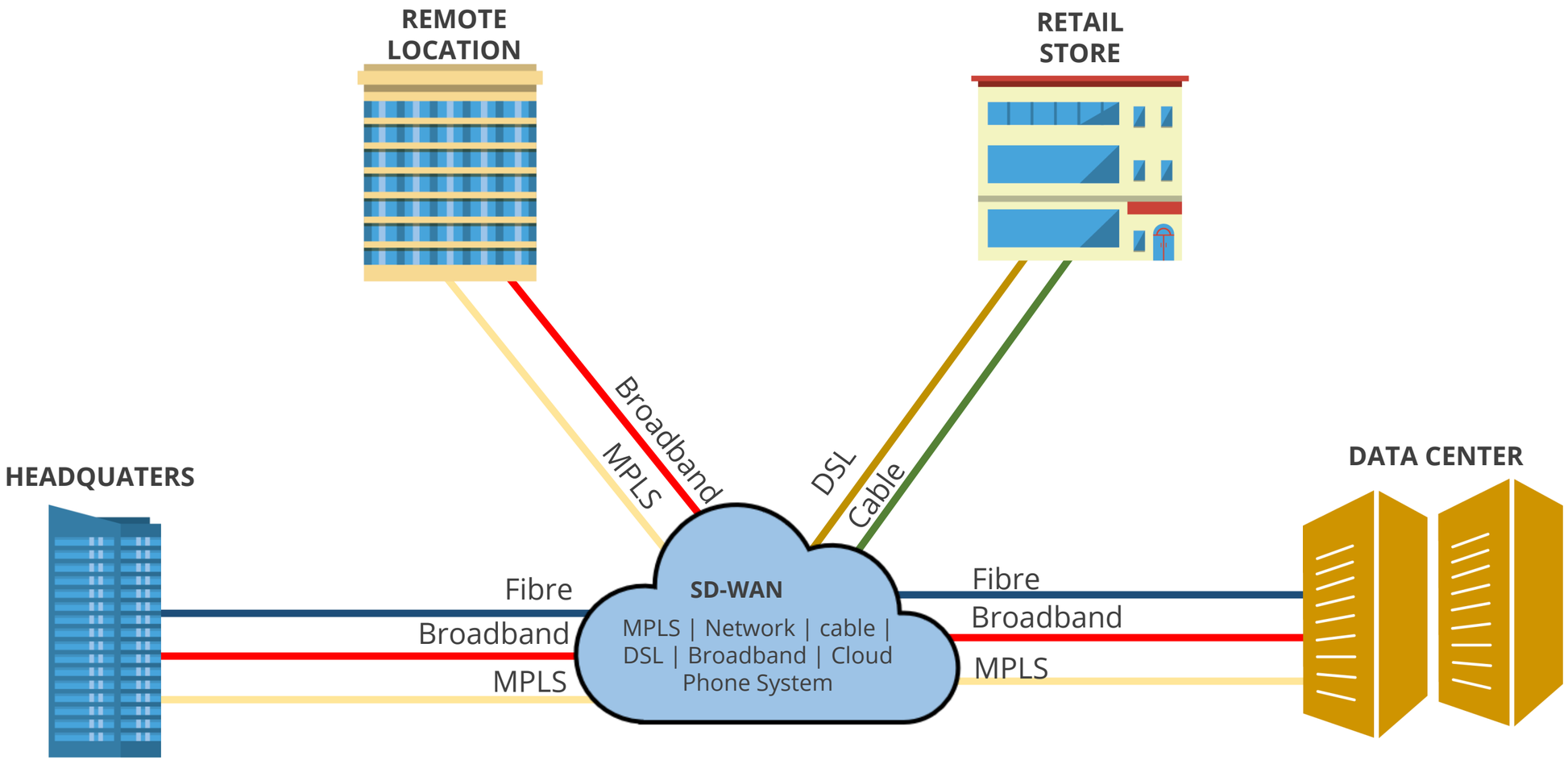
Software-Defined Wide Area Network (SD-WAN)

Characteristics

- The ability to support multiple connection types, such as MPLS, Last Mile Fiber Optic Network or through high speed cellular networks e.g. 4G LTE and 5G wireless technologies
- The ability to do dynamic path selection for load sharing and resiliency purposes
- The ability to easily configure and manage with help of a simple interface
- The ability to support VPNs, and third party services such as WAN optimization controllers, firewalls, and web gateways



SD-WAN



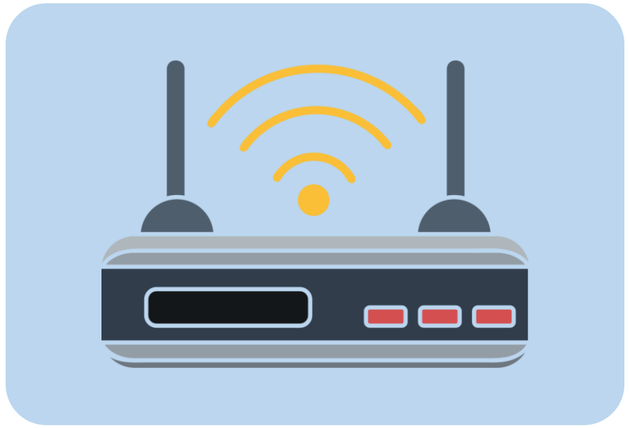
Source: https://www.bboxservices.com/resources/blog/bbns/2019/05/24/what-is-sd-wan-and-why-is-it-so-important

Wireless Technologies

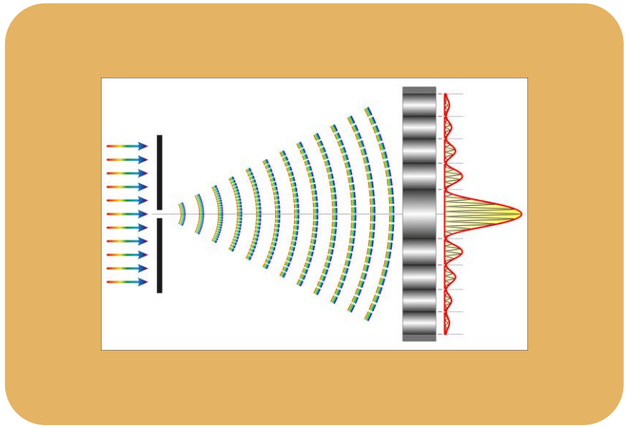
Wireless technology is the fastest-growing area of network connectivity.

The various types of wireless technologies are given below.

Wireless Standards



WLAN Operational Modes



Spread-Spectrum Technologies

IEEE Wireless Standards and Spread-Spectrum Technologies

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.

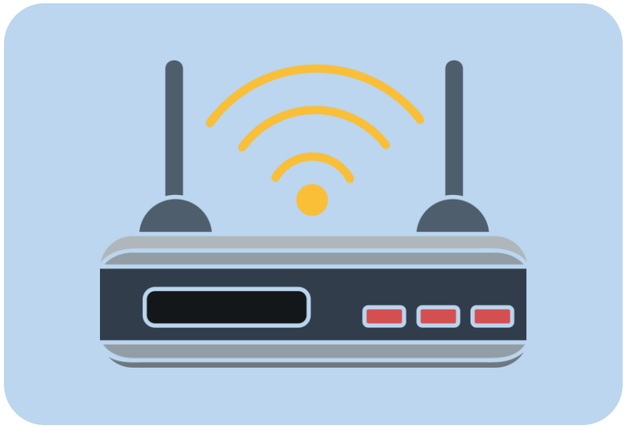
Spread-Spectrum Technologies:

Spread spectrum uses a radio transmission mode that broadcasts signals over a range of frequencies.

IEEE Wireless Standards and Spread-Spectrum Technologies

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

Frequency-Hopping Spread Spectrum (FHSS)



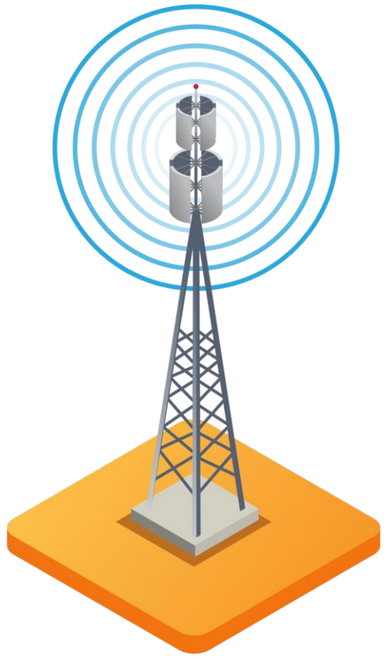
Direct Sequence Spread Spectrum (DSSS)

Wireless Standards

Standard	Year Introduced	Band Frequency	Max 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 & 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

Cellular Network

A cellular network or mobile network is a radio network distributed over land areas called cells



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

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

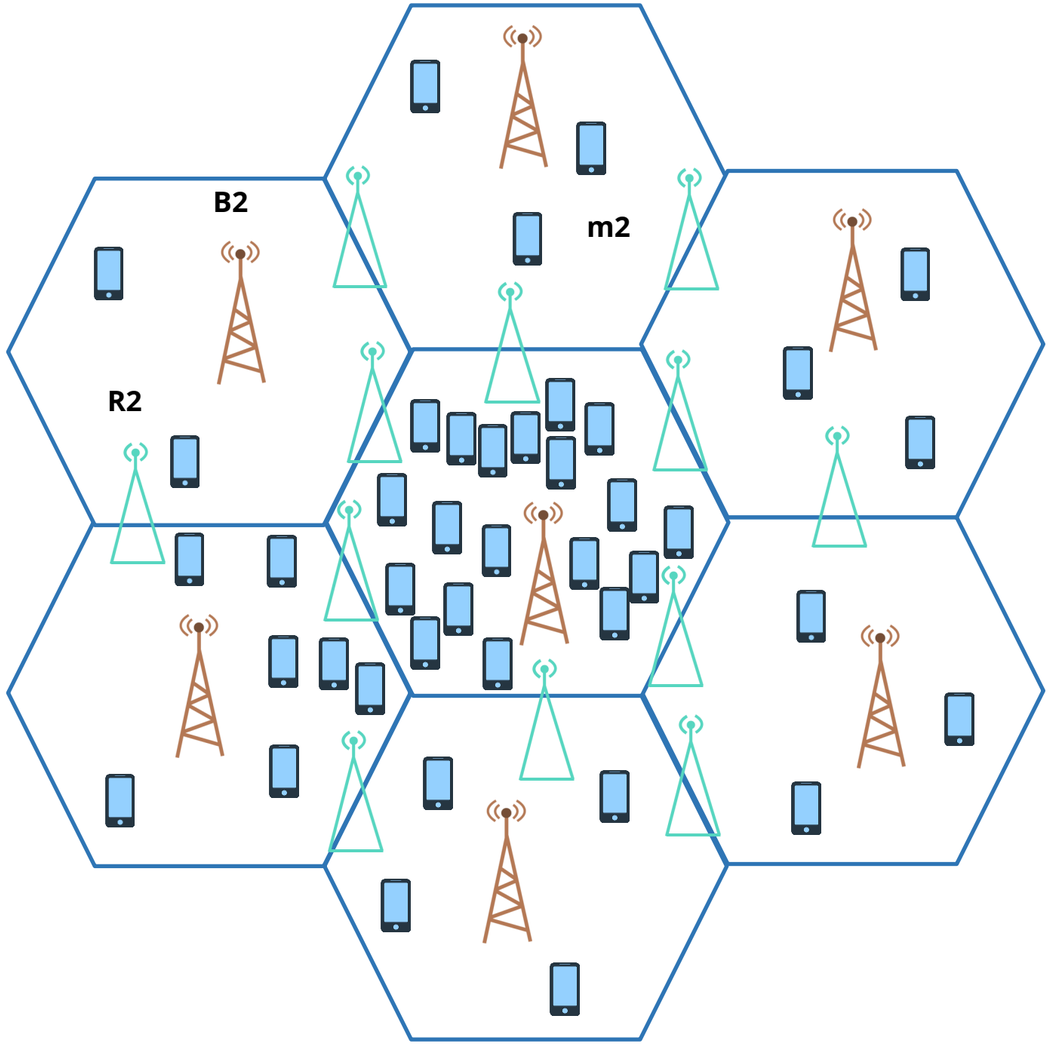
Cellular Network

A topology of a cellular network is shown below:

Base Station

Relay Station

Cell Phone



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

Content Delivery Network (CDN)

A Content Delivery Network (CDN) 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 of CDN :

Performance

- Shorter distance to users will not only reduce latency but also minimize packet loss resulting in a much better performance.

Availability

- Requests are always routed to the nearest available location.
- If one server is not available, requests are automatically sent to the next available server.

Content Delivery Network (CDN)

Benefits of CDN :

Security

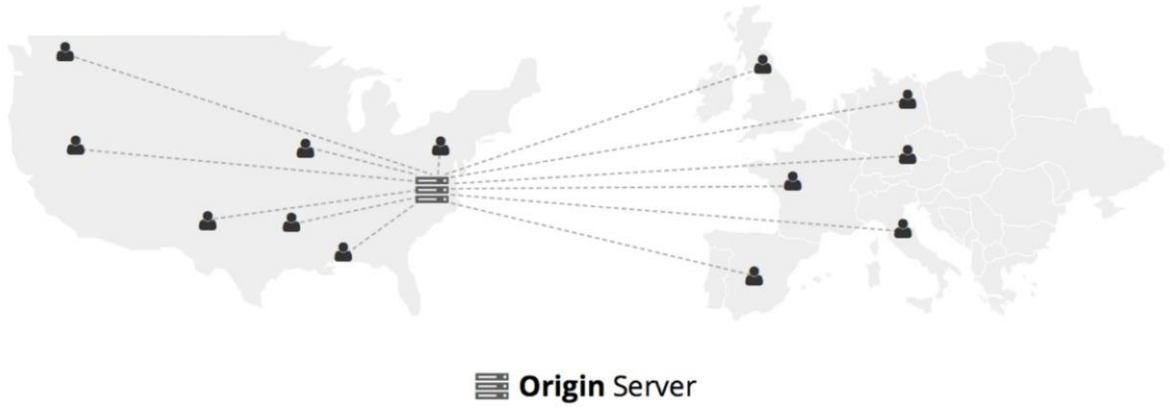
- Most CDNs should protect content providers and users by mitigating against a wide array of attacks including DDoS attacks and web-based exploits (SQL injection, cross-site scripting, and local or remote file-inclusion attacks).

Intelligence

- CDN can also offer valuable analytical information to discover trends about end user connectivity, device types, and browsing experiences across the globe.
- This data can give critical, actionable insights, and intelligence into their user base.

Without CDN

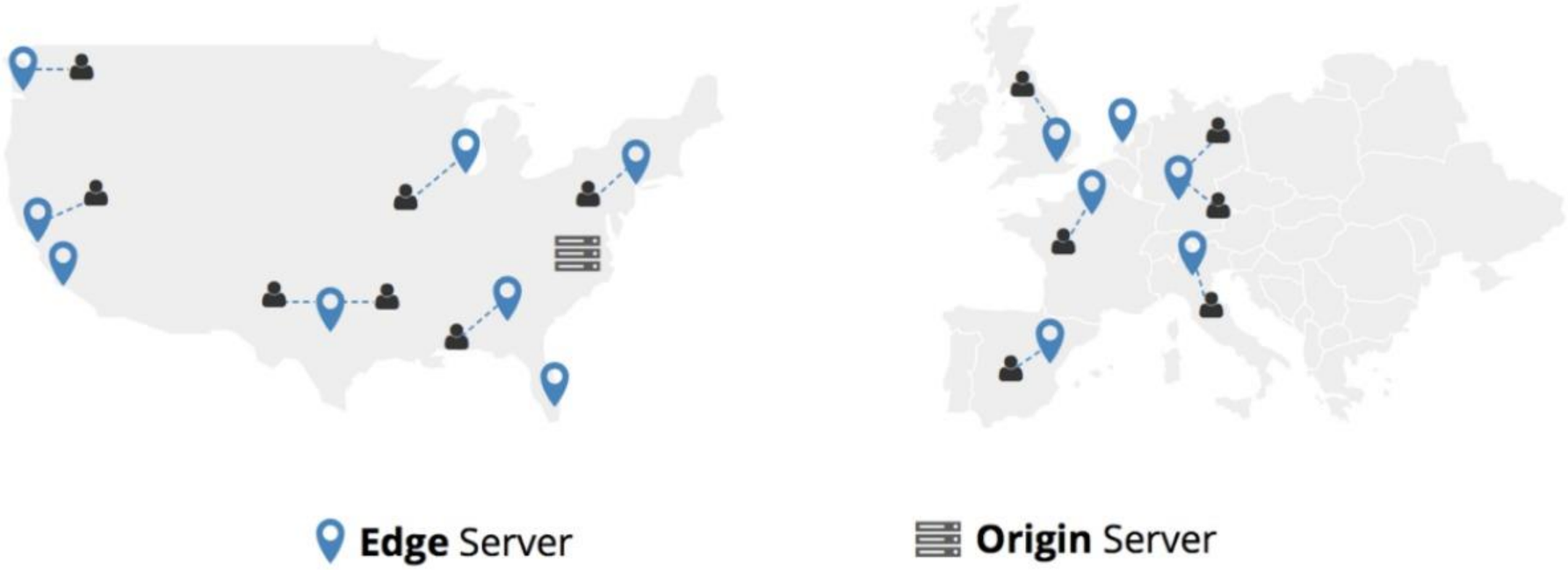
- No matter where a user is based geographically, information must be requested from the origin server which can be a great distance away from the user.
- This could severely impact the performance of the application.



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

With CDN

- When using a CDN, edge servers distribute static website data to visitors that are close to their geographic region.
- The connection is fast because it’s between Internet nodes that are close together.
- This means fewer hops and a faster flow of data.

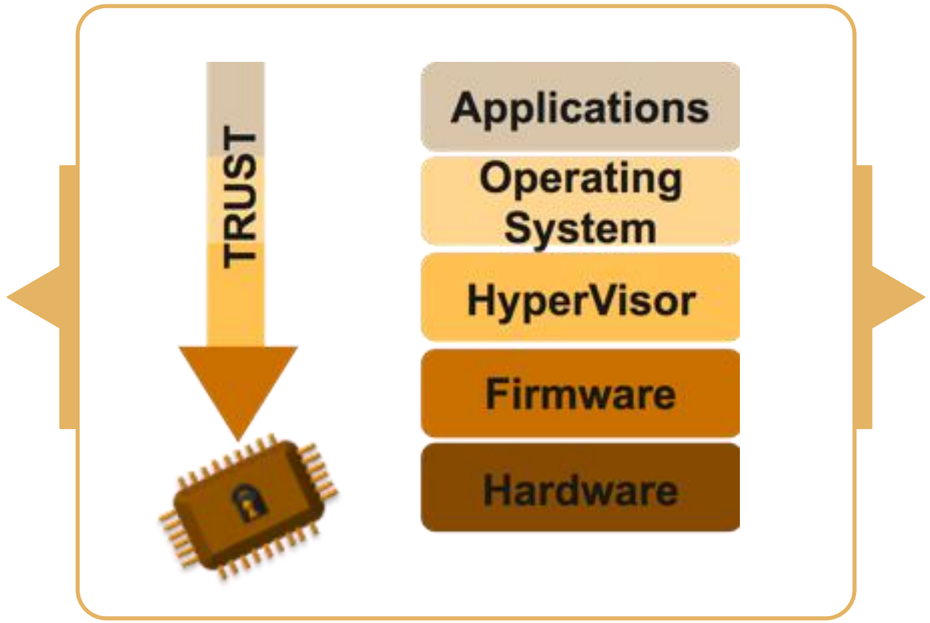


Source: https://img-medianova.mncdn.com/wp-content/uploads/sites/8/2020/05/cdn3.png

Secure Network Components

Root of Trust

The security of the applications depends on the layer below. Each layer has to trust the layer below.

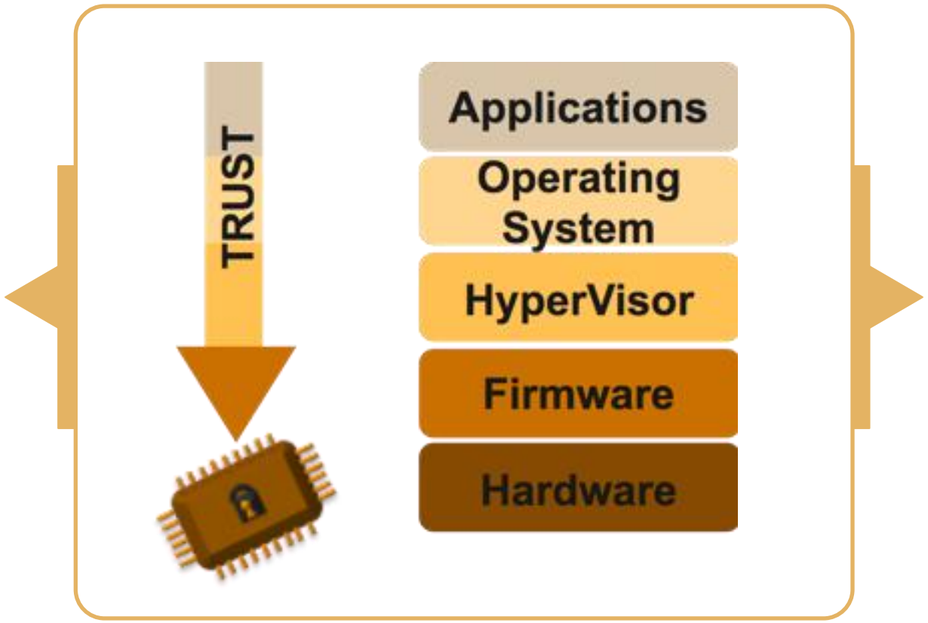


Security starts with hardware and the creation of a **Root of Trust (RoT)** in each device.

Source: https://aws.amazon.com/blogs/iot/using-a-trusted-platform-module-for-endpoint-device-security-in-aws-iot-greengrass/

Root of Trust

The RoT is ideally based on a hardware-validated boot process to ensure the system can only be started using code from an **immutable** source.



The **TPM** is often used as the basis for a hardware Root of Trust which contains the keys used for cryptographic functions and enables a secure boot process.

Source: https://aws.amazon.com/blogs/iot/using-a-trusted-platform-module-for-endpoint-device-security-in-aws-iot-greengrass/

List of Networking Devices

The different types of networking devices that coexist on the internetwork are:

Hubs and Repeaters

- Operate in OSI physical layer
- Amplify the data signal to extend the length of a network segment

Bridges

- Operate in OSI data link layer
- Amplify the data signals and make intelligent decisions as to where to forward the data

List of Networking Devices

Switches

- Operate in the data link layer, OSI layer 2, and network layer, OSI layer 3
- Sends the data packet only to the specific port where the destination MAC address is located

Routers

- Operate at the network layer, layer 3, of the OSI model
- Add more intelligence to the process of forwarding packets

Wireless Access Points

- Operate at the data link layer, OSI layer 2, and network layer, layer 3
- Allow wireless devices to connect to a wired network using Wi-Fi, bluetooth, or related standards

WAN Switching and Devices

Here are some of the devices related to WAN switching:

Circuit-switched networks:
Example: Telephone

Packet-switched networks
Examples: Frame Relay and Voice over IP (VoIP)

Router

Multiplexer

WAN switches

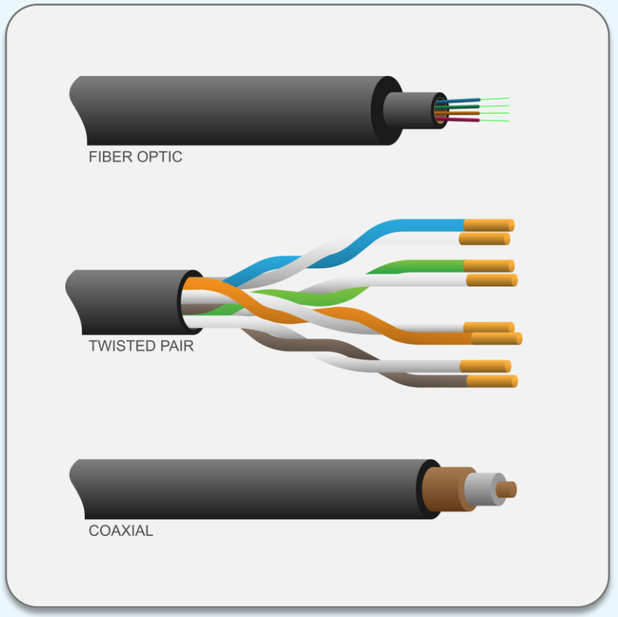
Transmission Media

Transmission media is used for transmitting data from a source to destination.
Following are the classes and types of transmission media:

Transmission media is used for transmitting data from a source to destination.

Following are the classes and types of transmission media:

- Unshielded twisted pair
- Shielded twisted pair
- Coaxial cable
- Fiber-optic cable

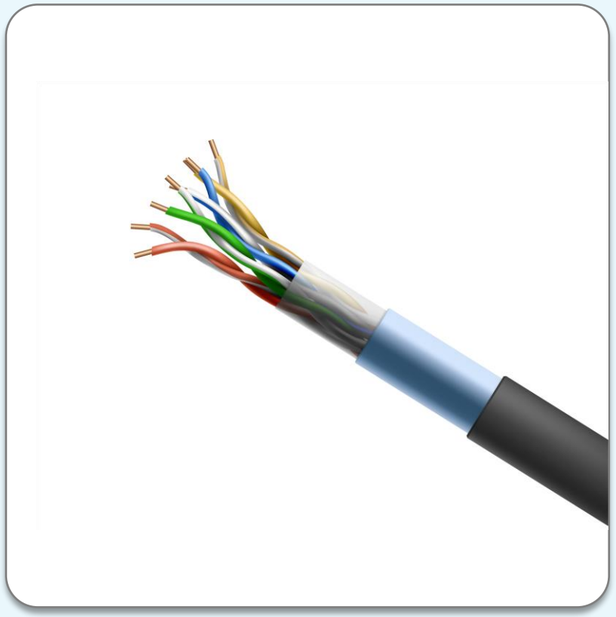


Twisted Pair

Twisted pair consists of two insulated wires that are arranged in a regular spiral pattern.

Wires can be shielded (STP) or unshielded (UTP).

- **Category 1**: Used for telephone communications and not suitable for transmitting data
- **Category 2**: Specified in the EIA or TIA-586 standard to be capable of handling data rates of up to 4 million bits per second (Mbps)
- **Category 3:** Used in 10Base-T networks and specified to be capable of handling data rates of up to 10 Mbps
- **Category 4:** Used in Token Ring networks and able to transmit data at speeds of up to 16 Mbps

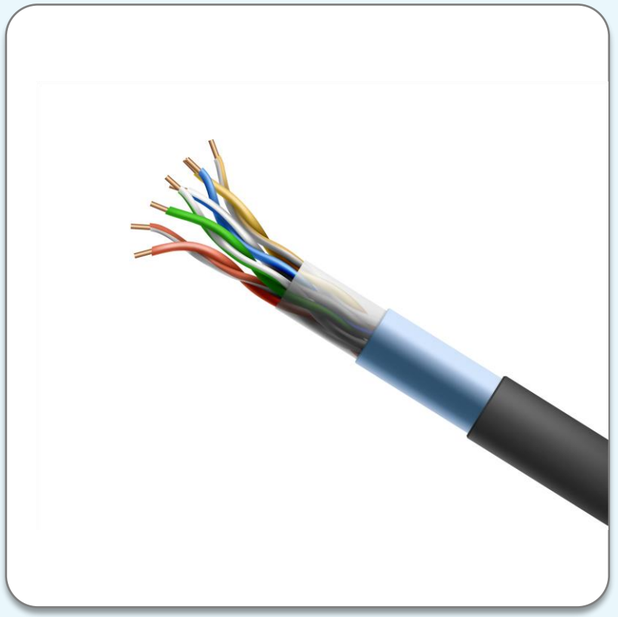


Twisted Pair

Twisted pair consists of two insulated wires that are arranged in a regular spiral pattern.

Wires can be shielded (STP) or unshielded (UTP).

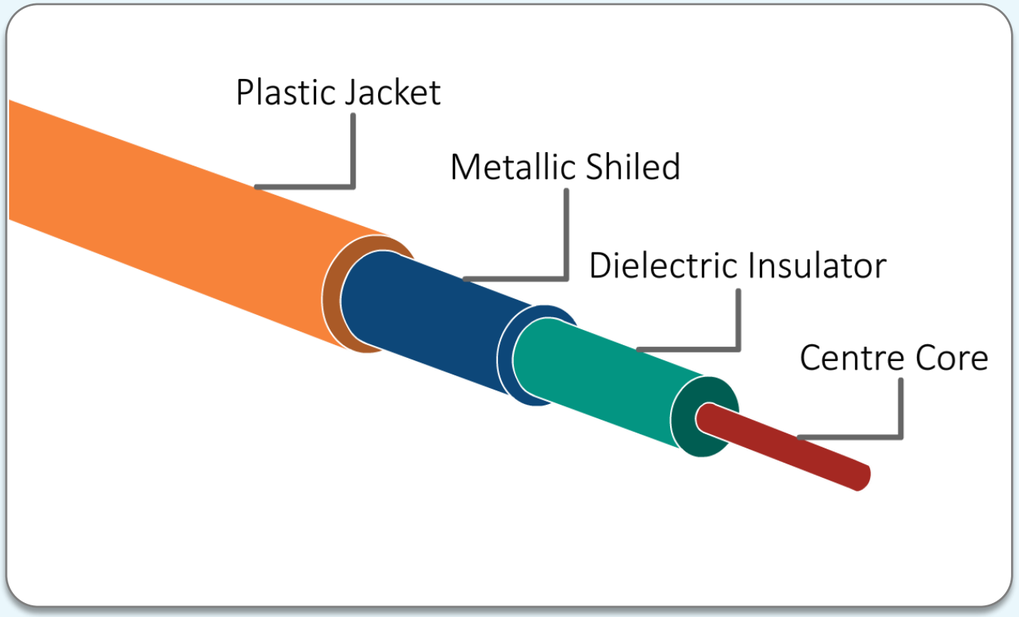
- **Category 5:** Consists of four twisted pairs in a single jacket
- **Category 6:** Backward compatible with Category 5 and 5e
- **Category 7:** More stringent than Category 6 cabling



Coaxial Cable Box

Coaxial cable box consists of a hollow outer cylindrical conductor.

- It is expensive and resistant to Electromagnetic Interference (EMI).
- Two types of coaxial cables are currently used in LAN: 50-ohm cable and 75-ohm cable.
- Coax can come in two types for LANs: thinnet and thicknet.
- There are two common types of coaxial cable transmission methods: baseband and broadband.



Fiber-Optic Cable Box

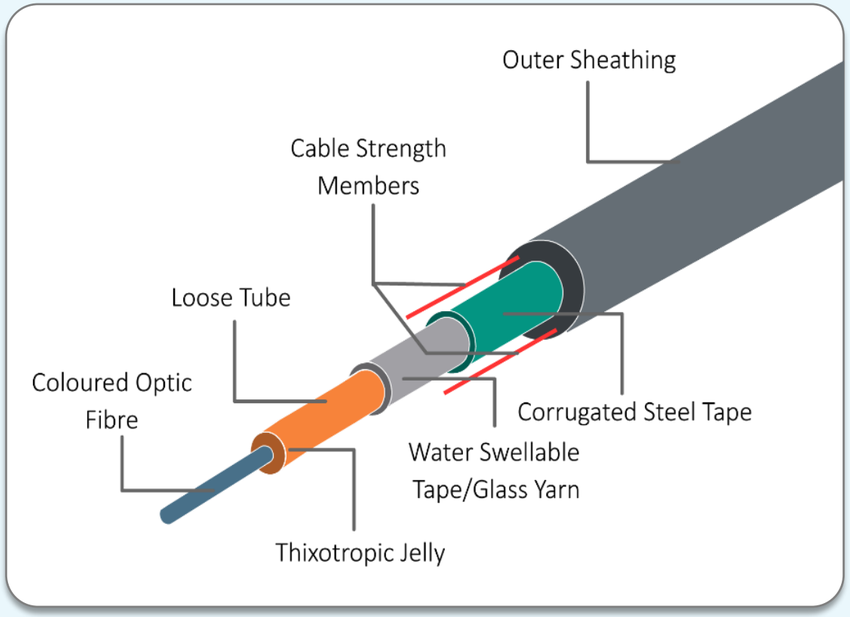
Fiber-optic cable box is a physical medium that can conduct modulated light transmission.

There are two types of light sources:

- Light-Emitting Diodes (LEDs)
- Diode lasers

There are two types of optical fibers:

- Multimode fiber
- Single-mode fiber

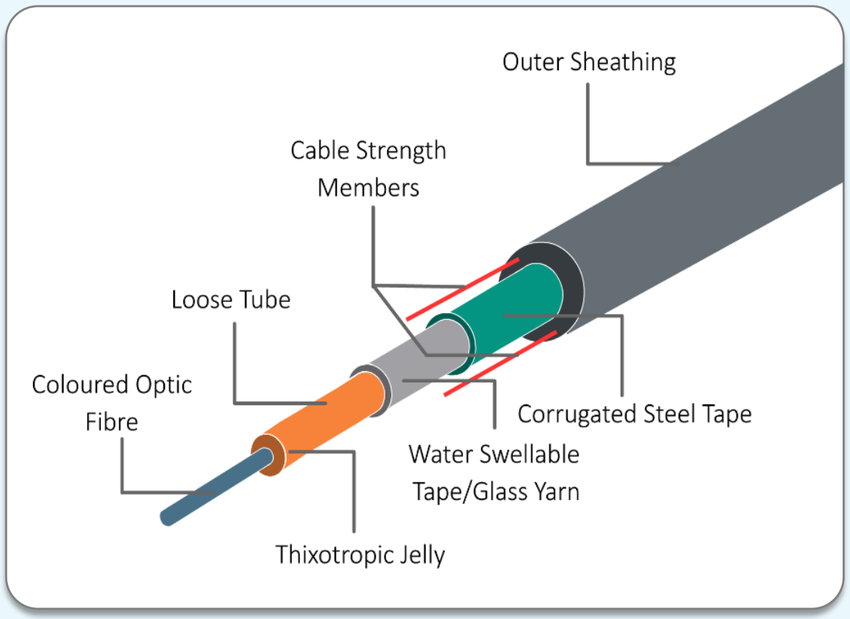


Fiber-Optic Cable Box

Fiber-optic cable box is a physical medium that can conduct modulated light transmission.

Fiber-optic cable has three basic physical elements:

- Core
- Cladding
- Jacket



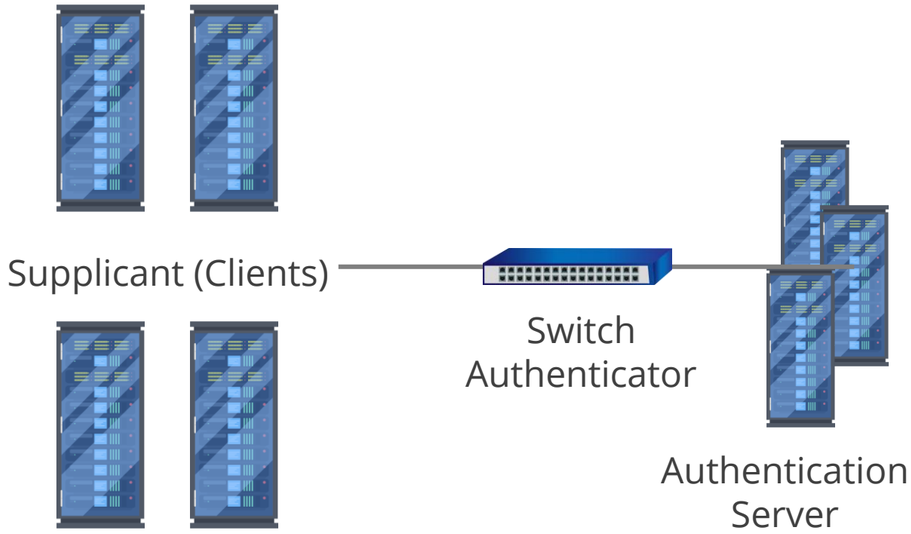
Network Access Control (NAC) Devices

- **Network Access Control (NAC)** solutions ensure that only endpoint devices in compliance with security policy can access specific network resources.
- IEEE **802.1X** is a standard for Port-based Network Access Control (**PNAC**) that defines how devices provide authentication to connect with other devices on Local Area Networks (LANs).
- Instead of network switches and access points, the authentication duties are performed by specialized authentication server, like a RADIUS server.
- This allows for devices to be managed and updated centrally, rather than distributed across multiple pieces of networking hardware.

802.1x NAC

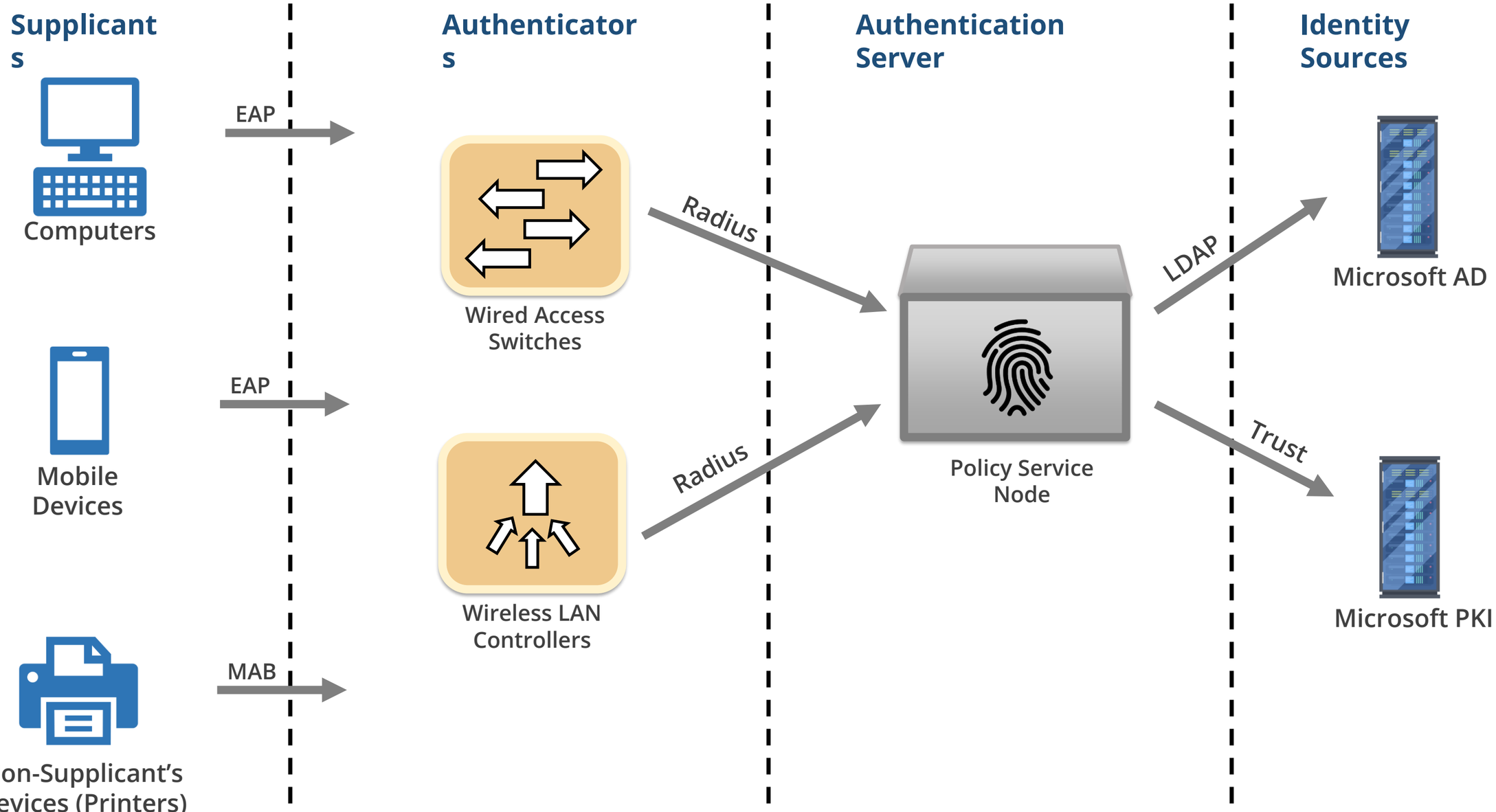
- **Supplicant**: The client device (such as laptop) that wants to be authenticated to LAN or WLAN
- **Authentication server**: The trusted server that authenticates the supplicant, typically a RADIUS server
- **Authenticator**: The device that provides a data link between the supplicant and the authentication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

  Example: 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

Endpoint Security

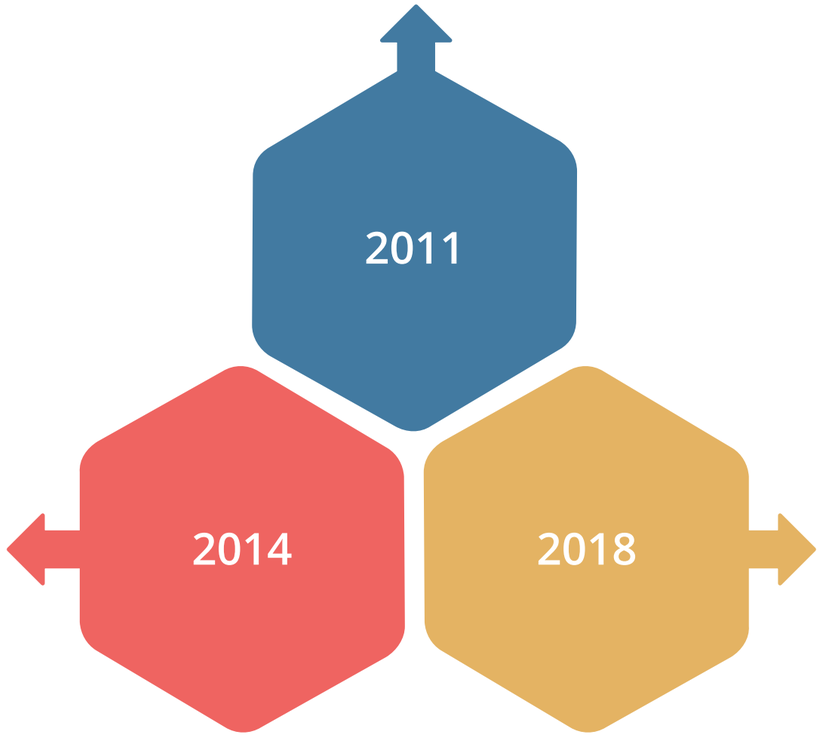
Endpoint security is the practice of securing endpoints of user devices such as desktops, laptops, and mobile devices from cyberattacks.

Features:

- Centralized endpoint management platform
- Advanced anti-malware and antivirus protection
- Proactive web security to ensure safe browsing on the Internet
- Data classification and data loss prevention to prevent data exfiltration
- Integrated firewall to block hostile network attacks
- Email gateway to block phishing and social engineering attacks
- Insightful and actionable threat forensics to allow administrators to quickly isolate infected devices
- Insider threat protection to safeguard against unintentional or malicious actions

Endpoint Security

Mobile Device Management (MDM)
BYOD device management



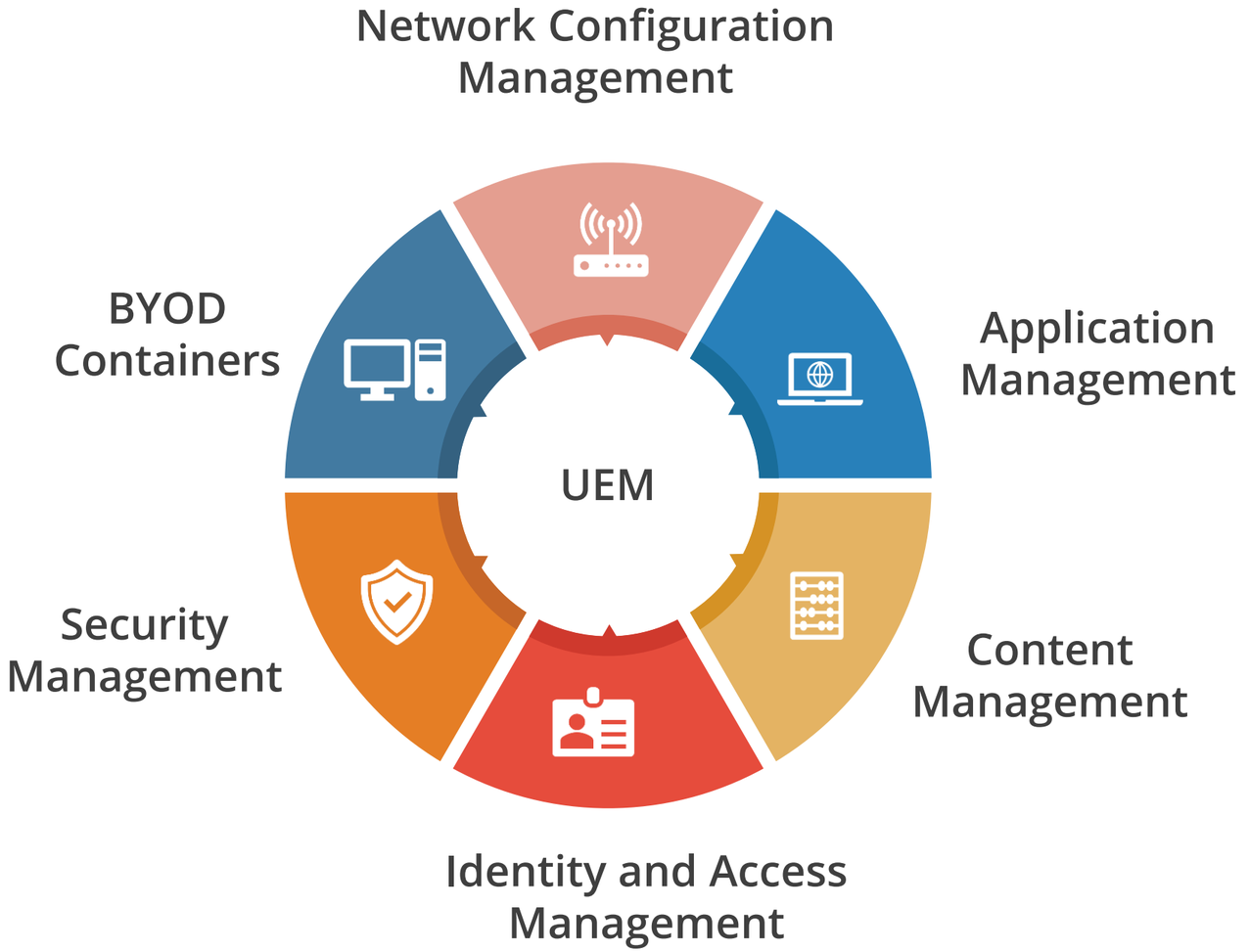
Enterprise Mobility Management (EMM)

- App management
- Managed configurations
- Email management
- Secure content management

Unified Endpoint Management (UEM)
All business devices including IoT

Unified Endpoint Management

Unified Endpoint Management (UEM) is an approach to securing and controlling mobile devices, such as smartphones, tablets, and laptops, in a connected, cohesive manner from a single console.



Source: https://www.hexnode.com/blogs/what-is-unified-endpoint-management-uem/

Network Address Translation

Network Address Translation (NAT) converts a private IP address of the inside, trusted network to a registered **real** IP address seen by the outside, untrusted network.

The Internet Assigned Numbers Authority (IANA) has reserved three blocks of the IP address space for private Internet addresses:

10.0.0.0 through 10.255.255.255

192.168.0.0 through 192.168.255.255

172.16.0.0 through 172.31.255.255

Implement Secure Communication Channels According to Design

Voice over IP

Voice over IP (VoIP) 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.

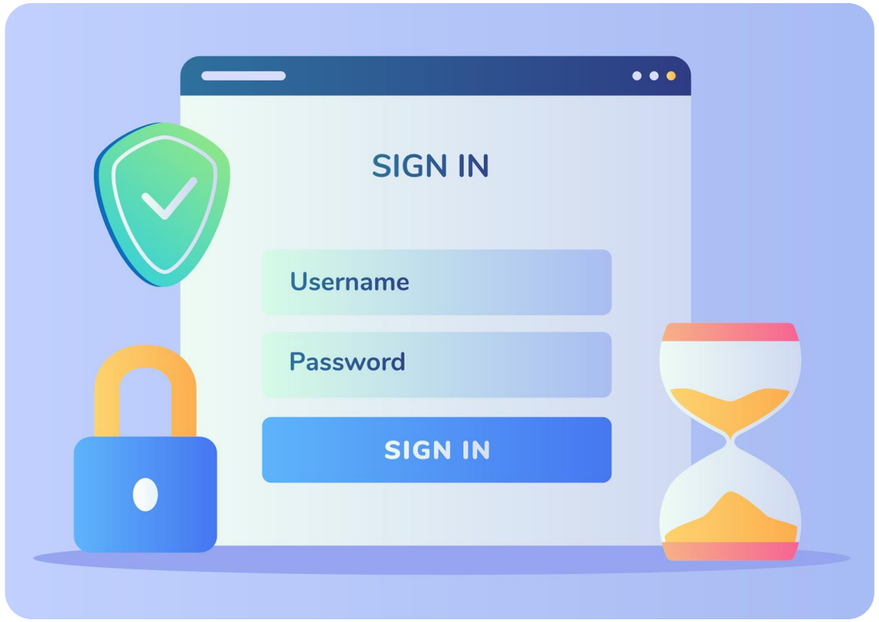
VoIP combines many types of data, such as voice, audio, and video, into a single IP packet

Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) is an application layer protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video, and messaging applications.

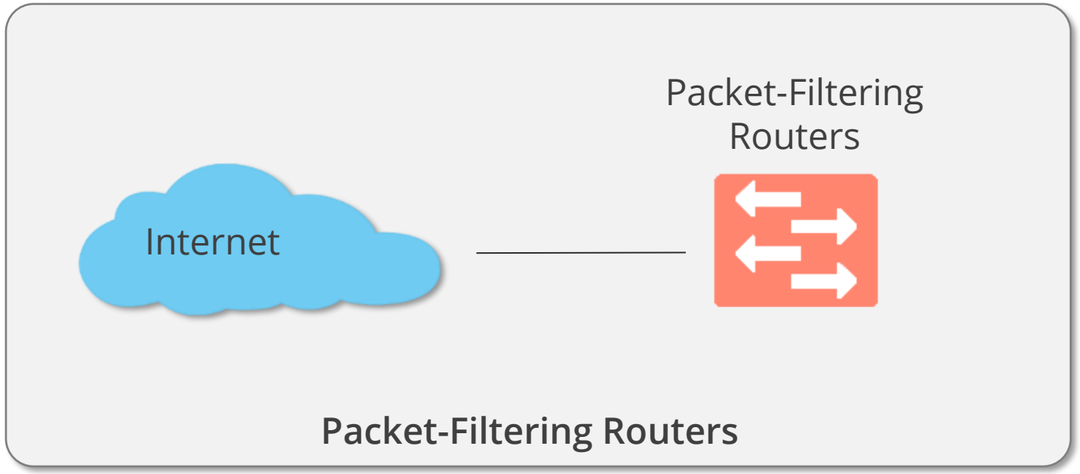
Some of the risks of using SIP are

- Denial of Service (DoS) attacks
- Vishing
- Viruses and malware
- Eavesdropping
- Spam over Internet Technology (SPIT)

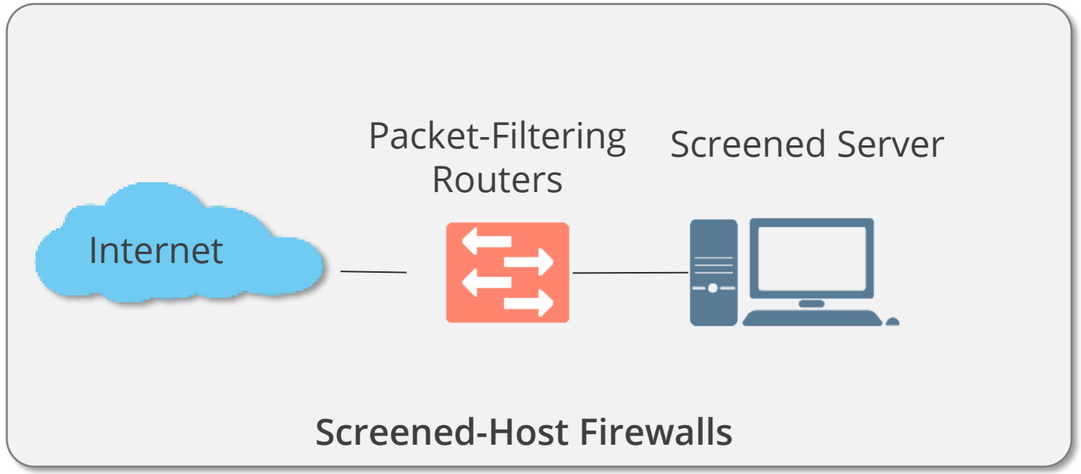


Firewall Architectures

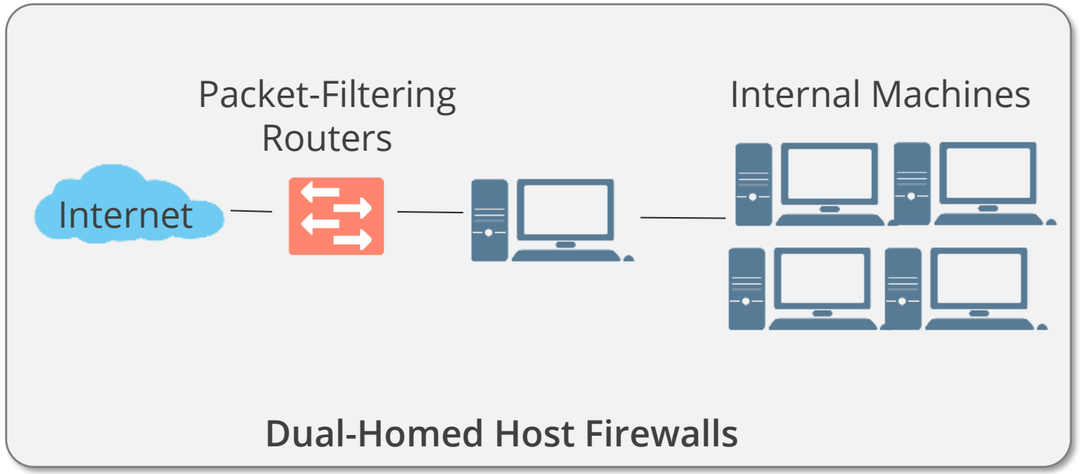
The four types of firewall architectures are:



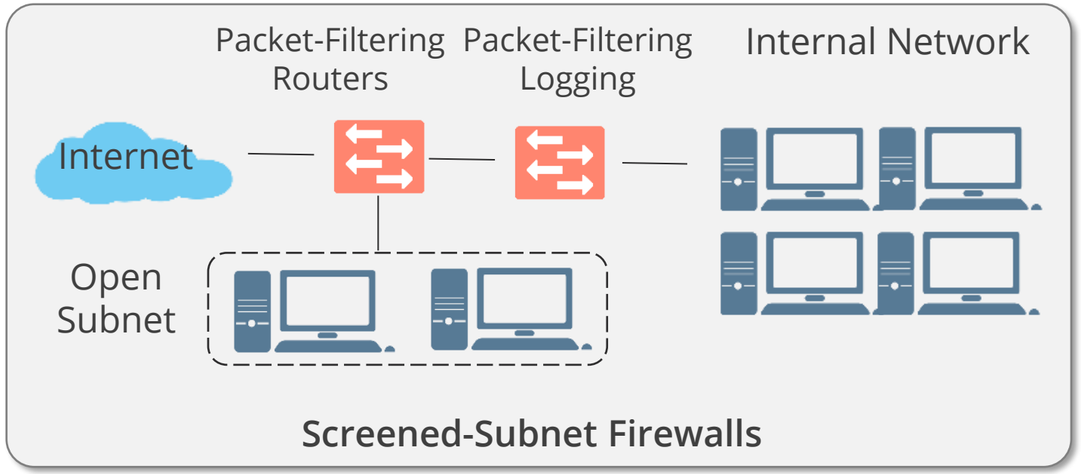
Packet-Filtering Routers



Screened-Host Firewalls



Dual-Homed Host Firewalls

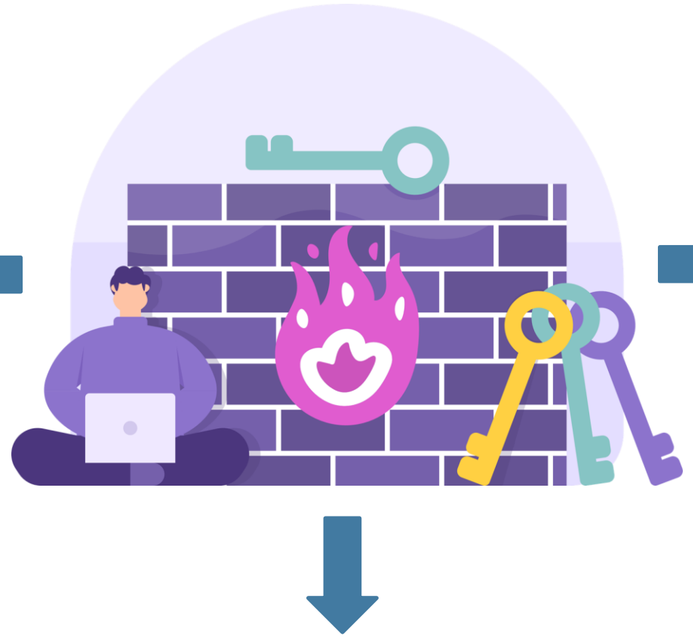


Screened-Subnet Firewalls

Packet Filtering Firewall

Packet filtering firewall examines the source and destination address of the incoming data packet. A packet-filtering router:

Allows or denies access to specific applications or services based on the access control lists



Can be configured to allow access to only authorized application port or service numbers

Operates at the Network Layer of the OSI model

Application-Level Gateway

Application-level gateway usually is a host computer that runs proxy server software.

Inspects the packet up through the application layer and can make access decisions based on the content of the packets.

Controls the services a workstation uses on the Internet, and it aids in protecting the network from outsiders who may be trying to get information about the network's design.

Circuit-Level Gateway

Circuit-level gateway creates a virtual circuit between the workstation client (destination) and the server (host).

- Works at the session layer of the OSI model and does not carry out deep-packet inspection
- Takes decisions based upon protocol header and session information

Example: Socket Secure (SOCKS) creates a circuit between the client and server without requiring knowledge about the internetworking service, i.e., it does not have any application specific controls.

Stateful Inspection Firewall

Stateful inspection or dynamic packet filtering firewall intercepts the incoming packets at the network layer and uses an inspection engine to extract state-related information from upper layers.

Low-protocol records are kept at the IP level.

Packets are queued and analyzed at all OSI layers against the state table.

By examining the state and context of the incoming data packets, the connectionless protocols can be tracked easily.

Network Security Terms

Some important network security terms are given below:

DMZ

It is a buffer zone between an unprotected network and a protected network that allows for the monitoring and regulation of traffic between the two.

Bastion host

It is any computer fully exposed to attack by being on the public side of the DMZ, unprotected by a firewall or filtering router. Anything that provides perimeter access-control security is considered bastion host. Examples are firewalls and routers, web, mail, DNS, and FTP servers.

Endpoint security

It is an information security concept, which assumes that each device is responsible for its own security. It also includes the protection of a business's network from employee memory devices that may unknowingly contain malware.

Introduction to Remote Access

Remote access technologies can be defined as the data networking technologies that are uniquely focused on providing access to the remote user into a network.

Advantages of remote access technologies:

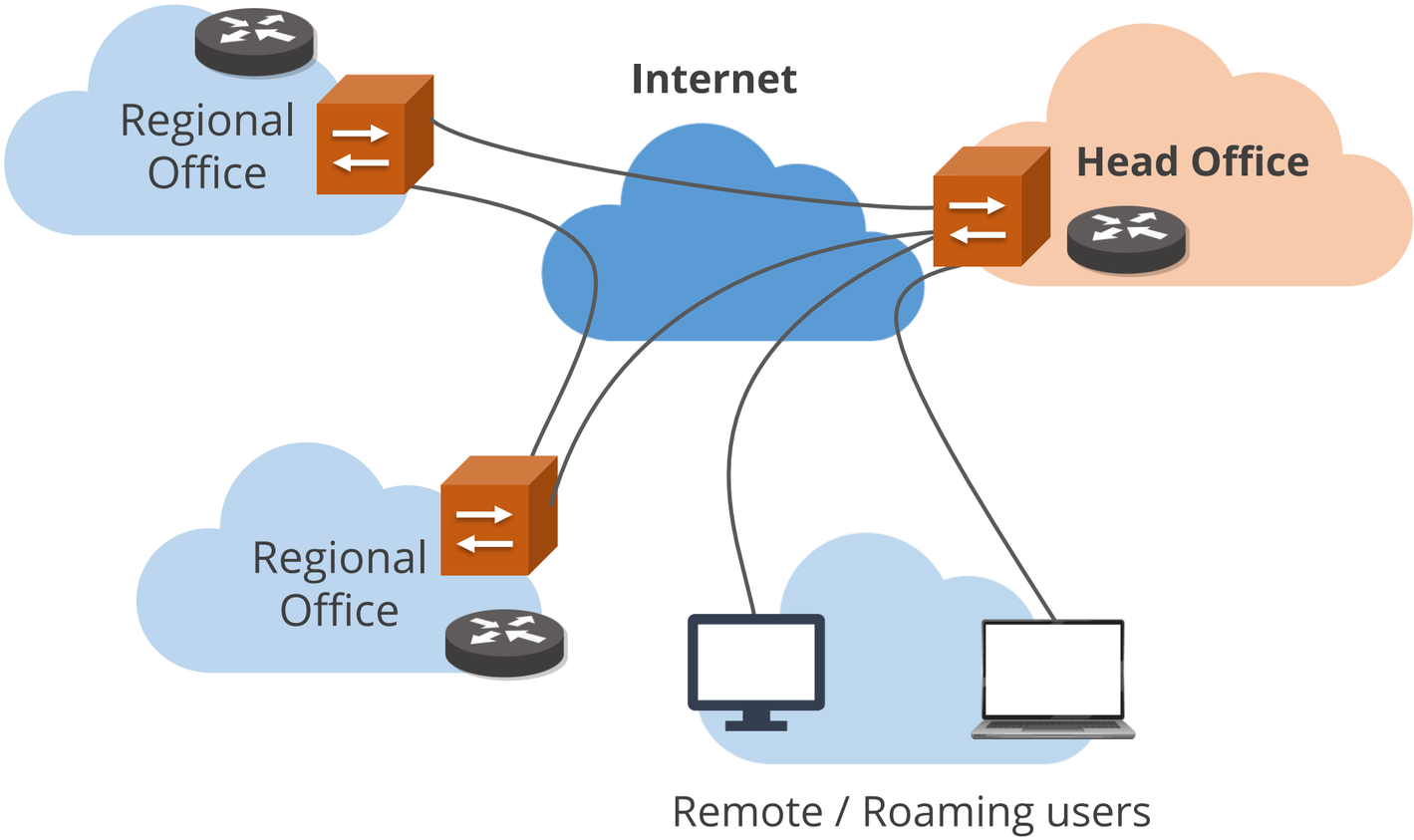
Reduce networking costs

Build efficient ties

Provide flexible work styles

Virtual Private Network

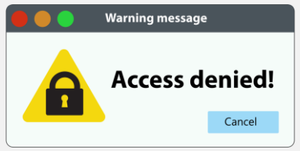
A **Virtual Private Network (VPN)** is a private network that uses a public network (usually the Internet) to connect remote sites or users together.



VPN Security

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

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

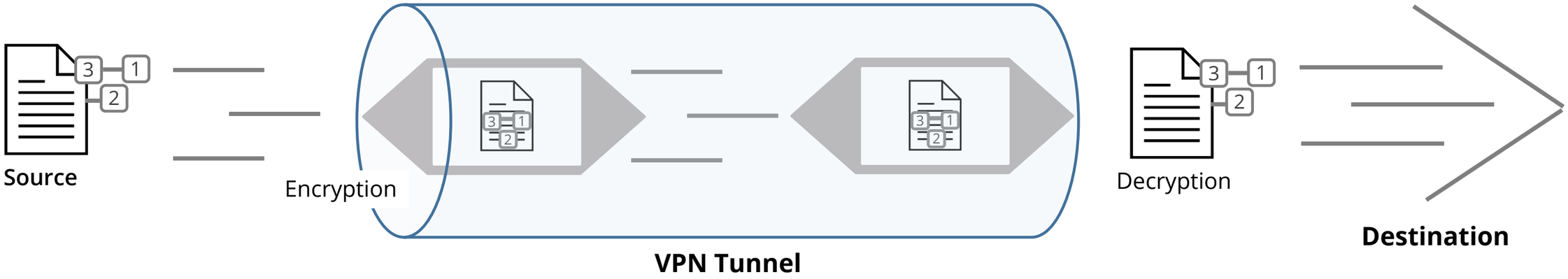


Confidentiality: Preventing anyone from reading or copying data as it travels across the internet

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

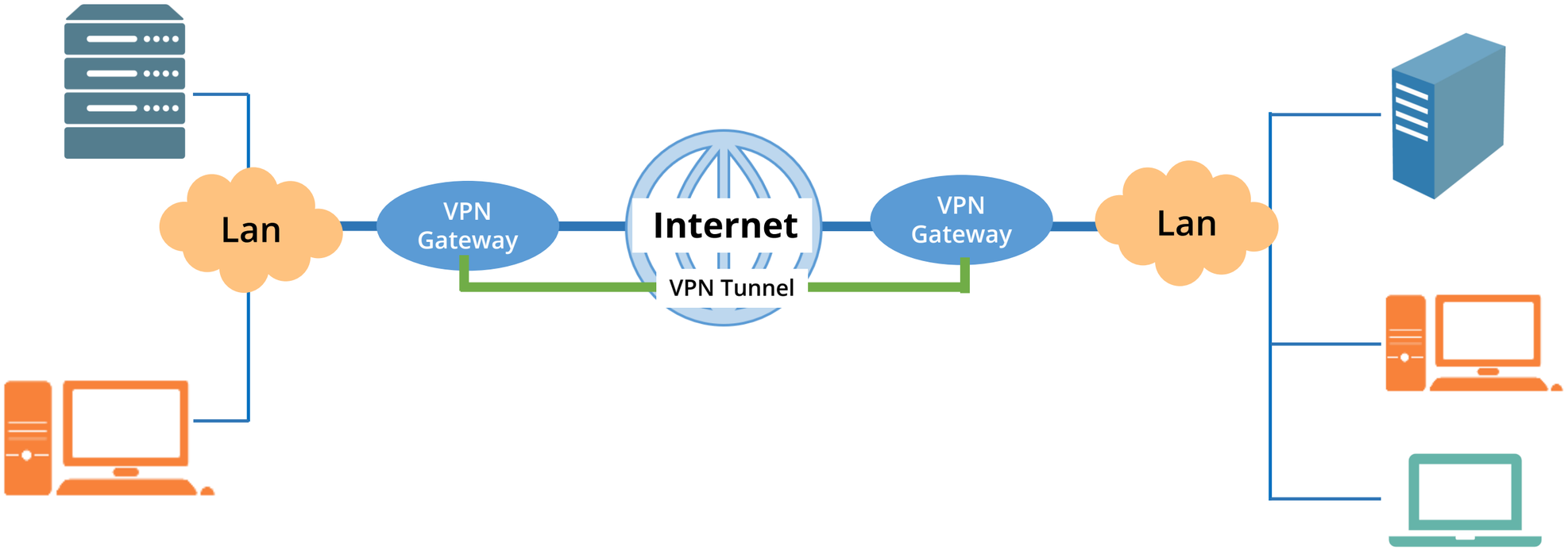
VPN Tunnel

- VPN is the tunnel that connects the user to the VPN server.
- To keep each data packet secure, it gets wrapped in an outer packet which is encrypted through a process known as encapsulation.
- This outer packet keeps the data secure during the transfer.
- At the VPN server, the outer packet is removed, to access the data of the inner packet.



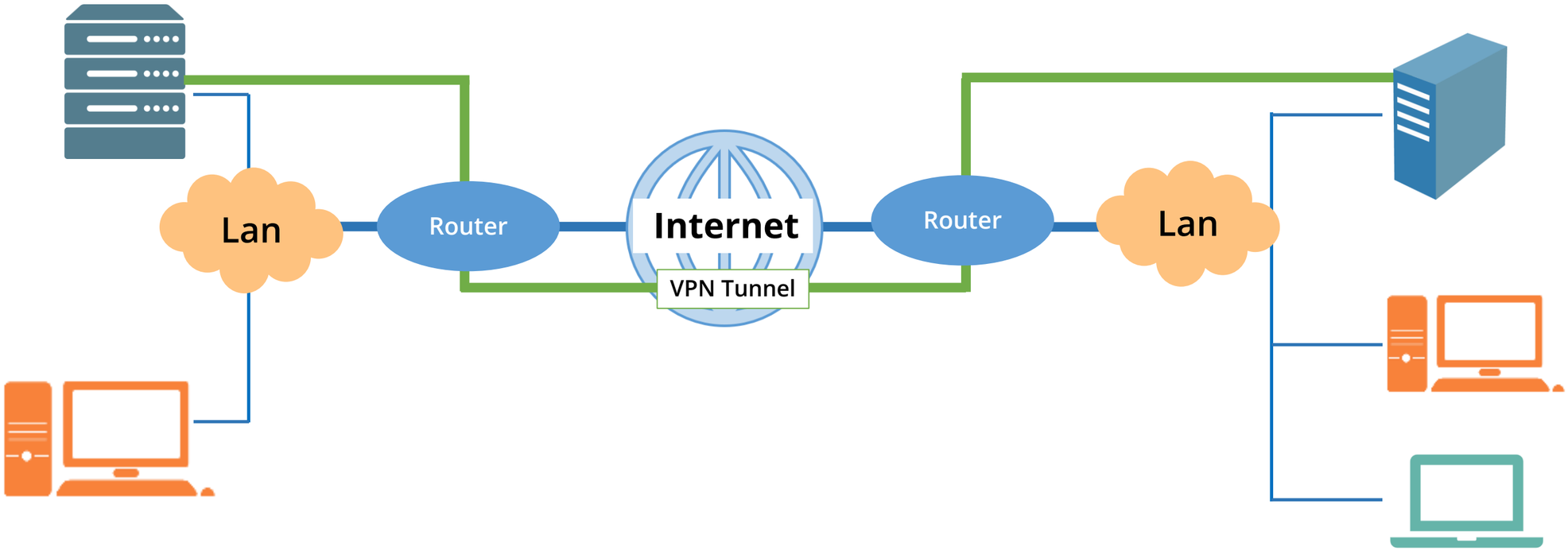
Types of VPN: Site-to-Site

Site-to-site VPNs, or intranet VPNs, allow a company to connect its remote sites to the corporate backbone securely over a public medium like the Internet.



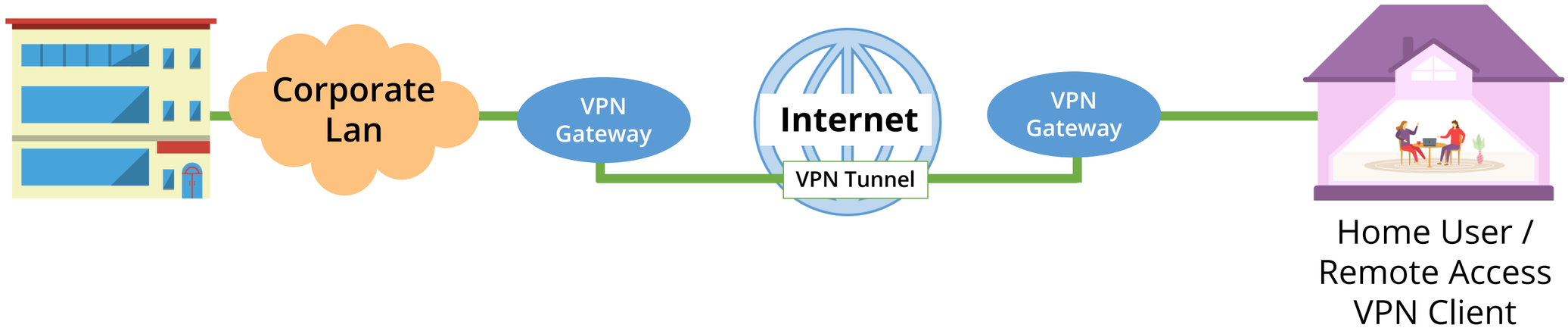
Types of VPN: Host-to-Host

A host-to-host VPN is somewhat like a site-to-site in concept except that the endpoints of the tunnel are two individual hosts.



Types of VPN: Host-to-Site

Host-to-site or remote-access VPNs allow remote users like telecommuters to securely access the corporate network wherever and whenever they need to.



VPN Protocols

The following are the five VPN protocols, their advantages, and disadvantages:

VPN Protocols

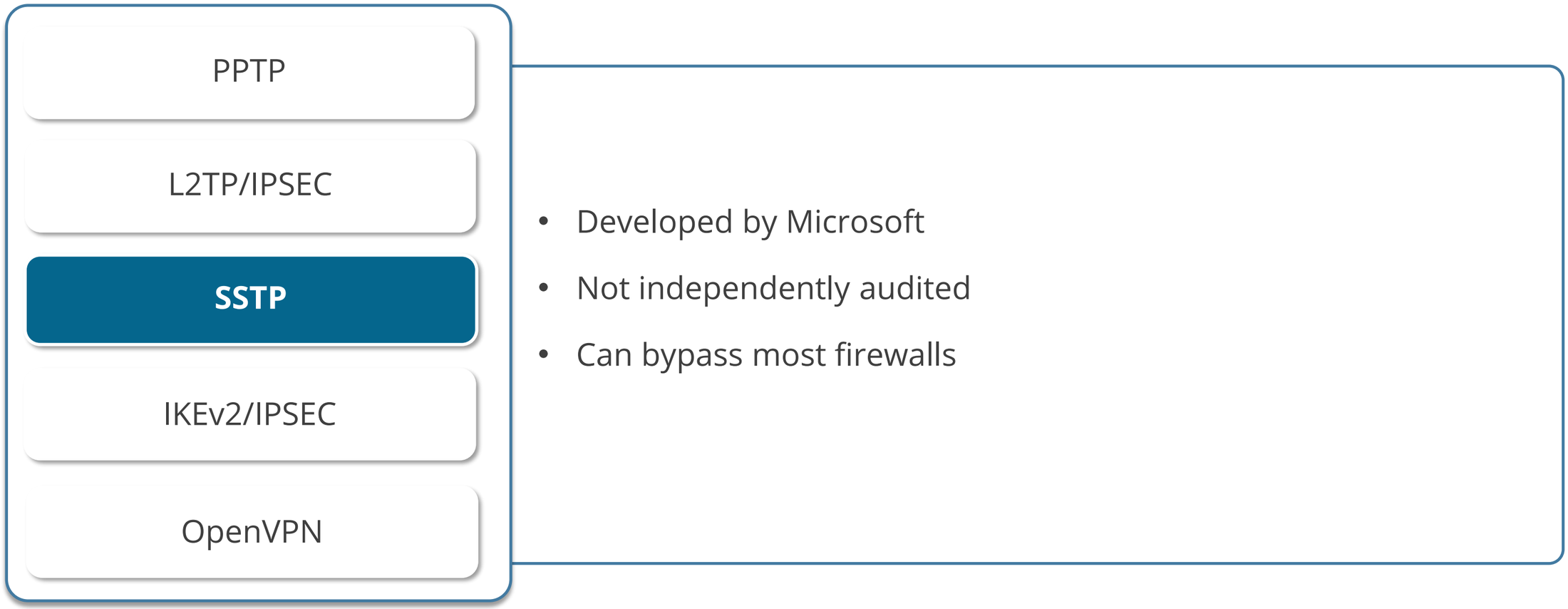
The following are the five VPN protocols, their advantages, and disadvantages:

- PPTP
- **L2TP/IPSEC**
- SSTP
- IKEv2/IPSEC
- OpenVPN

- Developed by IETF to replace PPTP
- Combined with IPsec for security
- Requires more overhead double encapsulation
- Supports non-TCP/IP protocols
- Can be blocked by firewalls
- Possibly compromised by the NSA

VPN Protocols

The following are the five VPN protocols, their advantages, and disadvantages:



VPN Protocols

The following are the five VPN protocols, their advantages, and disadvantages:

- PPTP
- L2TP/IPSEC
- SSTP
- **IKEv2/IPSEC**
- OpenVPN

- Based on the IPSec framework
- Jointly developed by Cisco and Microsoft
- Fast, stable, secure, and very easy to set up
- Supports a wide range of encryption protocols
- Useful for mobile devices

VPN Protocols

The following are the five VPN protocols, their advantages, and disadvantages:

- PPTP
- L2TP/IPSEC
- SSTP
- IKEv2/IPSEC
- **OpenVPN**

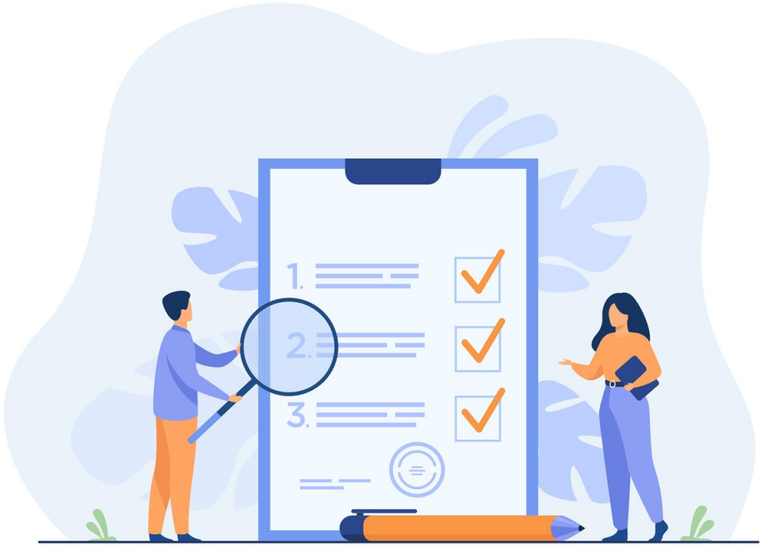
- Open-source protocol
- Runs on UDP and TCP protocols
- Has a highly reliable OpenVPN TCP protocol
- Lower latency and faster speed for OpenVPN UDP protocol
- Supports several encryption algorithms
- Relies upon third-party software to operate

VPN Protocols: A Comparison

Protocol	Speed	Encryption and Secure Browsing	Stability	Media Streaming	Compatible With
PPTP	FAST	POOR	MEDIUM	GOOD	Most OS and devices
L2TP/IPSEC	FAST	MEDIUM	GOOD	GOOD	Most OS and devices
SSTP	MEDIUM	GOOD	MEDIUM	MEDIUM	Windows
IKEv2/IPSec	FAST	GOOD	GOOD	GOOD	Most OS and devices
OpenVPN TCP	MEDIUM	GOOD	GOOD	MEDIUM	Most OS and devices
OpenVPN UDP	FAST	GOOD	MEDIUM	GOOD	Most OS and devices

VPN Protocols: Guidelines

- Choose OpenVPN when available, especially when the setup is handled by a third-party app.
- L2TP or IPSec is probably the most widely used alternative that offers decent security.
- SSTP is also a solid option for Windows users, assuming you trust proprietary tech from Microsoft.
- IKEv2 is a fast and secure alternative for the few devices that support it, particularly mobile devices.
- Only use PPTP as a last resort option.



Multimedia Collaboration

The various multimedia collaborations are mentioned below:

Remote or Virtual Meetings

Telecollaboration

Instant Messaging

Telepresence

Network Function Virtualization

- **Network function virtualization (NFV)** is a network architecture concept that uses virtualization to design, deploy, and manage networking services.
- NFV decouples network functions such as firewall management, intrusion detection, DNS, and NAT from proprietary hardware appliances and manages them as software in virtual machines (VMs).

Network Function Virtualization: Benefits

- Reduced vendor lock-in
- Reduced CapEx and OpEx through reduced equipment costs and reduced power consumption
- Faster time to deployment
- Improved scalability and resource management
- Greater flexibility and accelerated time to market for new products and updates

Network Attacks

The following are some of the types of network attacks:

Types	Description
DOS or DDOS	This attack is an attempt, on the part of the attacker, to incapacitate a target system or resource.
Teardrop	The attacker sends mangled packet fragments with overlapping and oversized payloads to a target system.
Ping of Death	The attacker sends a ping packet of length 65,535 bytes to the target system.
SYN Flood	It is a Denial-of-Service attack, where the attacker sends many SYN packets to the target system.
Sequence Number	An attacker attempts to hijack or disrupt an existing TCP session by injecting packets that pretend to originate from one of the two computers in the session.
Smurf	This attack consists of numerous forged ICMP echo requests.
DNS Poisoning	This is a computer hacking attack, where the data is introduced into a Domain Name System (DNS) name server's cache database.

Network Attacks

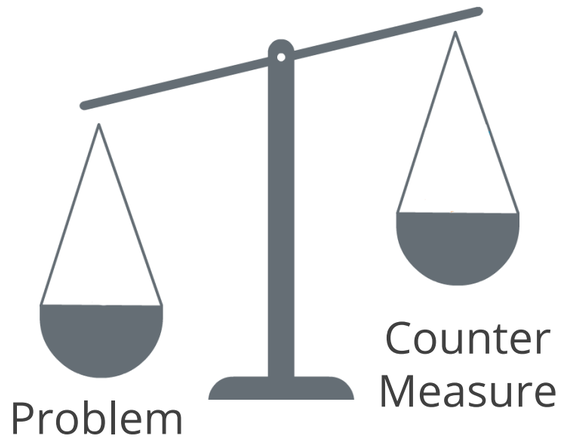
The following are some of the types of network attacks:

Types	Description
Rootkit	It is a tool or a collection of tools that an attacker can install on a compromised computer.
Worm	A worm is a type of malware that has the means for automatic self-replication.
Spam	Spam greatly adds to the volume of email traffic on the Internet.
Phishing	It is a type of spam where the contents of a message are designed to masquerade as a trustworthy organization.
Pharming	Pharming is a hacker's attack intended to redirect a website's traffic to another, bogus site.
IP Spoofing Attacks	This refers to the creation of Internet Protocol packets with a forged source IP address.
ARP Poisoning	An attacker sends fake Address Resolution Protocol (ARP) messages onto a Local Area Network compromising the victim’s ARP tables.
Masquerading	This is when one user pretends to be another user.

Network Attacks: Countermeasures

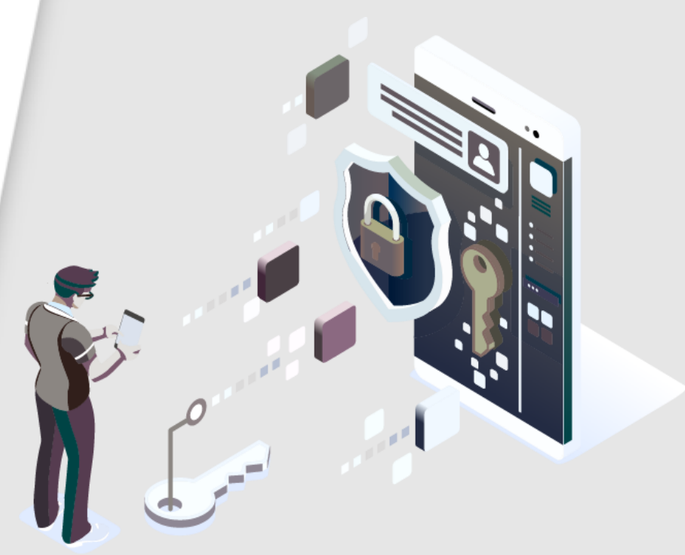
Some countermeasures for network attacks are:

- Implementing access control lists
- Firewalls
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Protection of network cabling
- Antivirus software
- Private addressing
- Close unnecessary ports and services
- Security patches
- Unified threat management (UTM)
- Gateways



Key Takeaways

- The Communications and Network Security domain involves developing a secure network architecture and design, securing network components, and communication channels.
- Security can be addressed more efficiently using the layered approach.
- The network communication model, such as OSI Model, provides a conceptual framework for communication between computers.
- The use of proper countermeasures provides confidentiality, integrity, availability, and authentication for transmissions over private and public communication networks.



This concludes **Communications and Network Security.**

The next domain is **Identity and Access Management (IAM).**