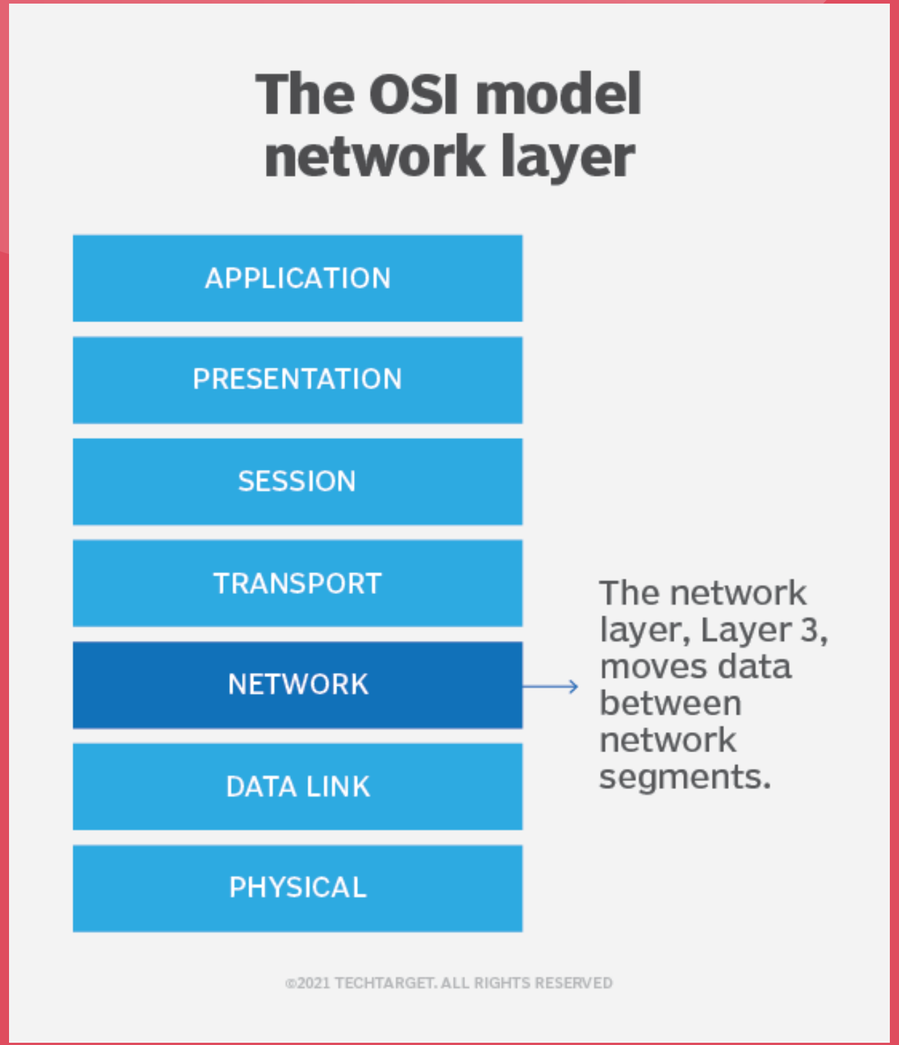
DELHI
TECHNOLOGICAL
UNIVERSITY

NETWORK LAYER

INDEX

Introduction

The network layer is the third layer in the OSI model of computer networks. Its main function is to transfer network packets from the source to the destination. It is involved both the source host and the destination host. At the start, it accepts a package from the transport layer, encapsulates it in a datagram, and then delivers the packet to the data link layer so that it can further be sent to the receiver. At the destination, the datagram is decapsulated, and the package is extracted and delivered to the corresponding transport layer.

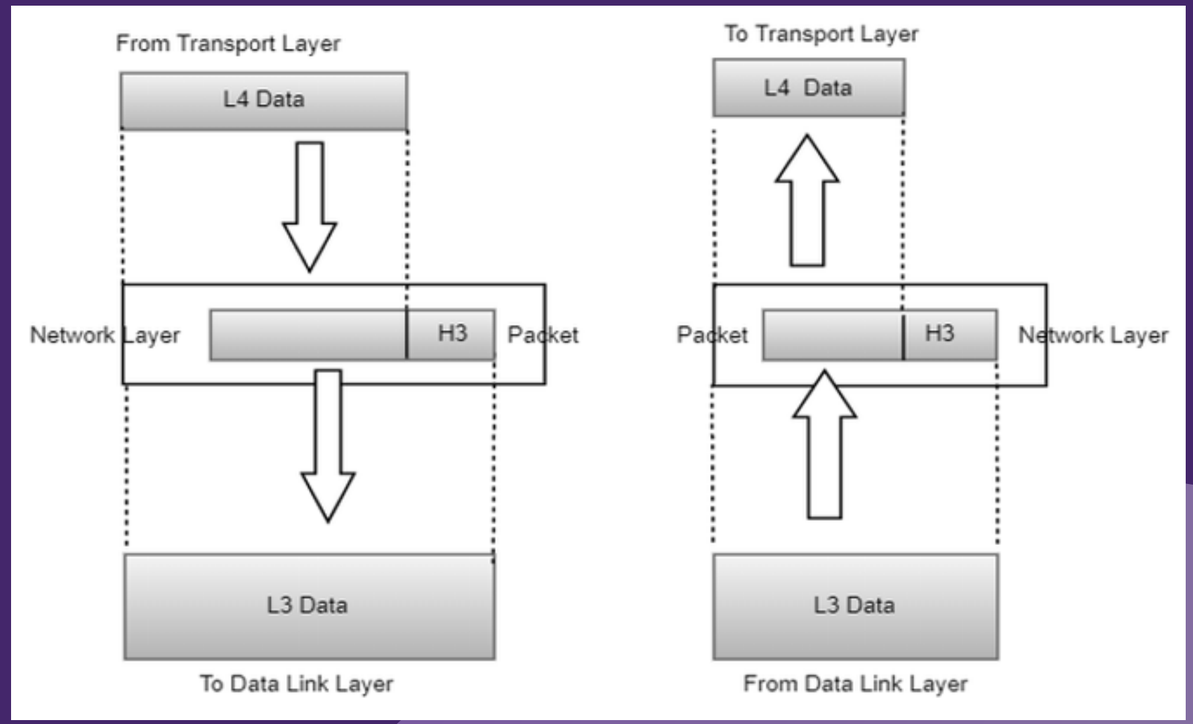


Functions of the Network Layer

1. Logical addressing: The network layer provides a unique logical address to each device on the network, which is used to identify and communicate with that device.

2. Routing: The network layer determines the most efficient path for data to travel through the network from source to destination, taking into account factors such as network congestion and the availability of different routes.

3. Congestion Control: The network layer helps prevent network congestion by regulating the flow of data through the network, based on the capacity and availability of network resources.



4. Packet fragmentation and reassembly: The network layer may fragment large data packets into smaller packets that can be transmitted through the network more efficiently. It also reassembles these packets at the receiving end.

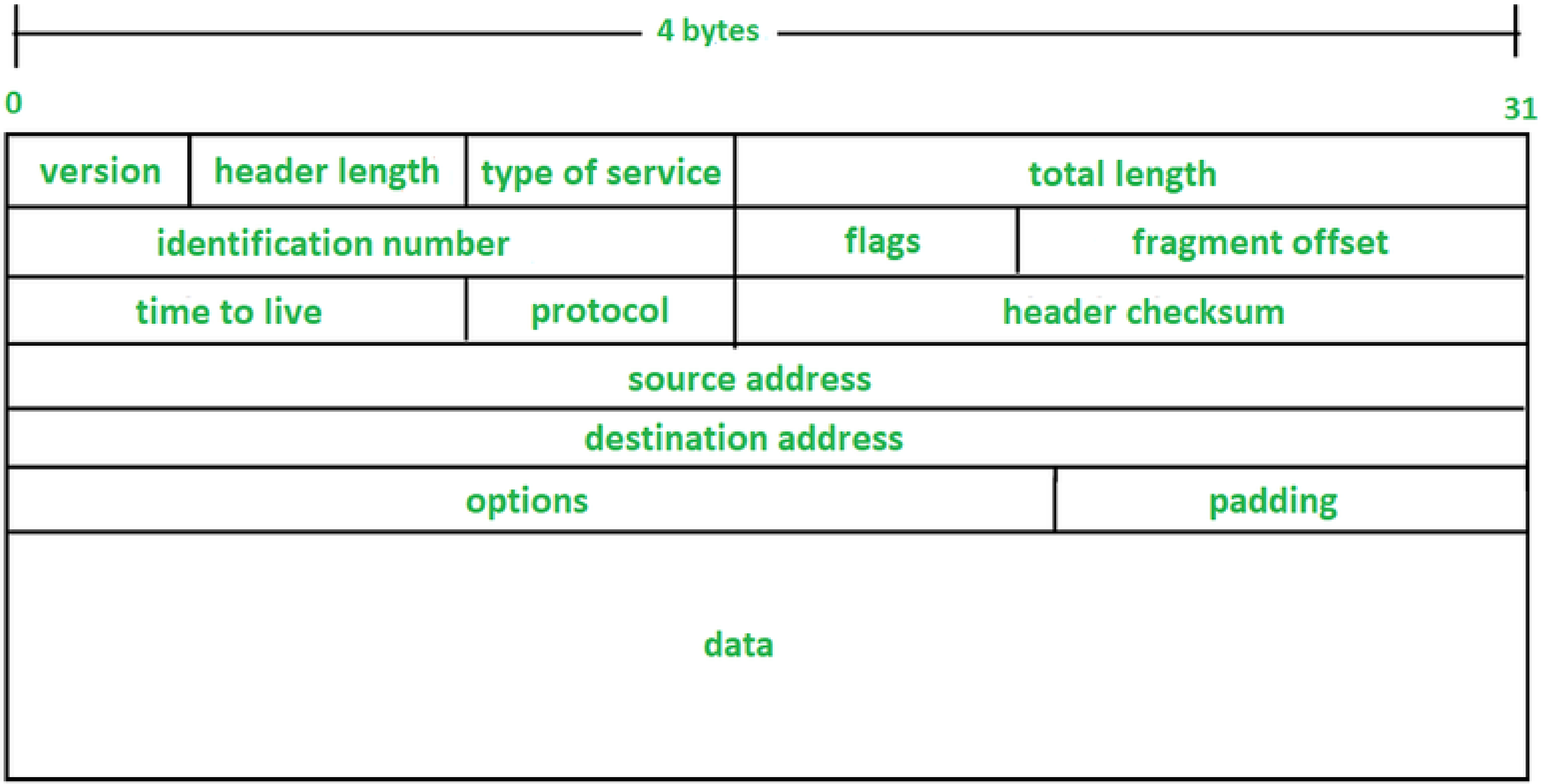
LOGICAL ADDRESSING

The network layer provides logical addressing for devices in a network, which is used to identify the source and destination devices during communication. This addressing scheme is typically hierarchical, with each device on the network having a unique logical address.

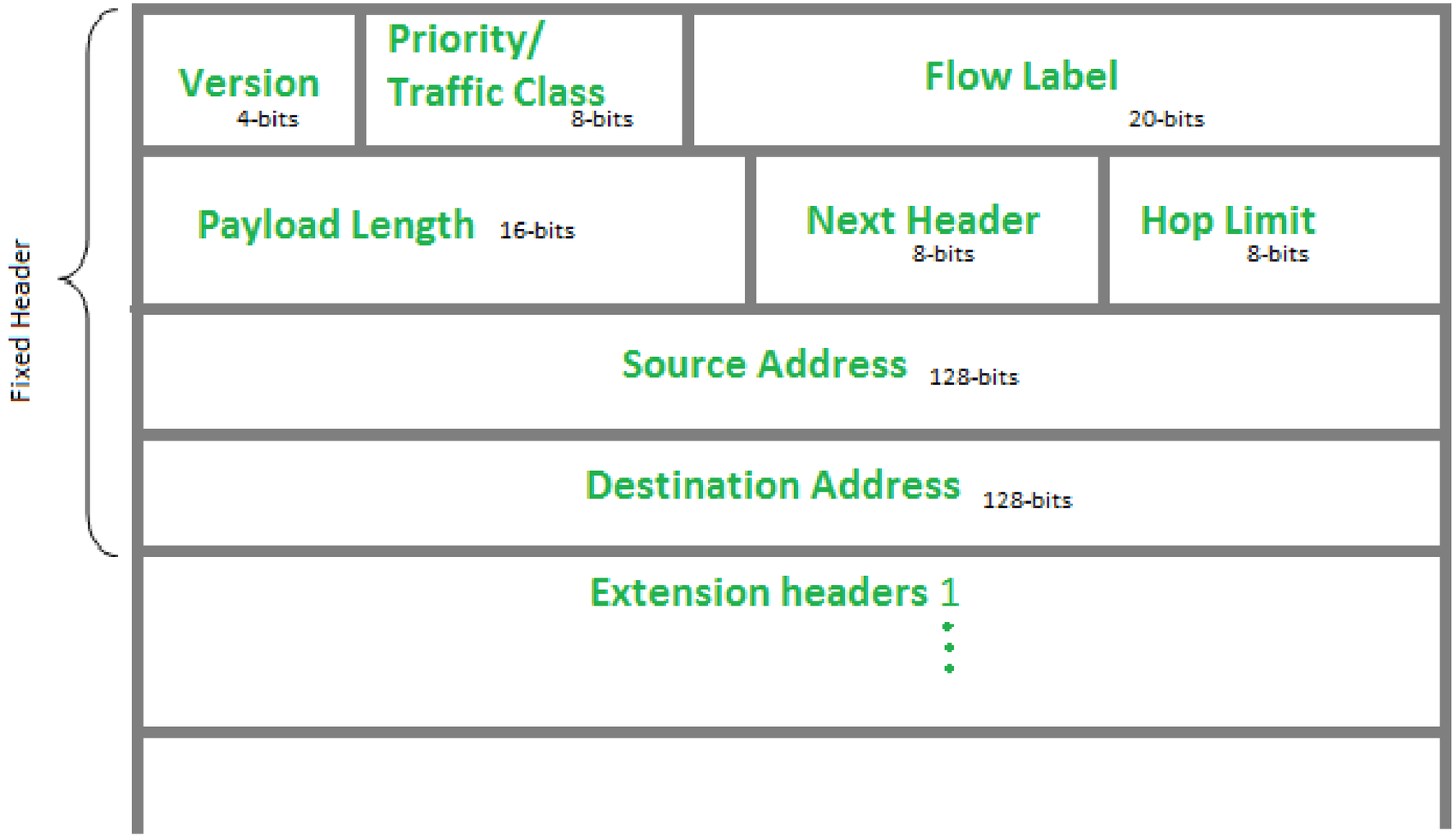
In the Internet Protocol (IP), which is the most widely used protocol at the network layer, the logical address is known as an IP address. An IP address is a 32-bit number (IPv4) or 128-bit number (IPv6) that is divided into two parts: the network address and the host address. The network address identifies the network to which the device is connected, while the host address identifies the specific device on that network.

For example, in the IPv4 address 192.168.1.100, the first three octets (192.168.1) represent the network address, while the last octet (100) represents the host address. Devices on the same network will have the same network address but different host addresses.

IPv4 Header Format



IPv6 Header Format



Routing in Network Layer

- Routing is the process of selecting a path for traffic in a network to travel from its source to its destination. In the network layer of the OSI model, routing is a key function that determines the best path for packets to take across an internetwork, such as the Internet.

- Routing in the network layer is typically performed by routers, which are specialized network devices that forward packets between networks. Routers use routing algorithms to determine the best path for packets to take based on a variety of factors, such as the network topology, the current network traffic load, and the destination address of the packet.

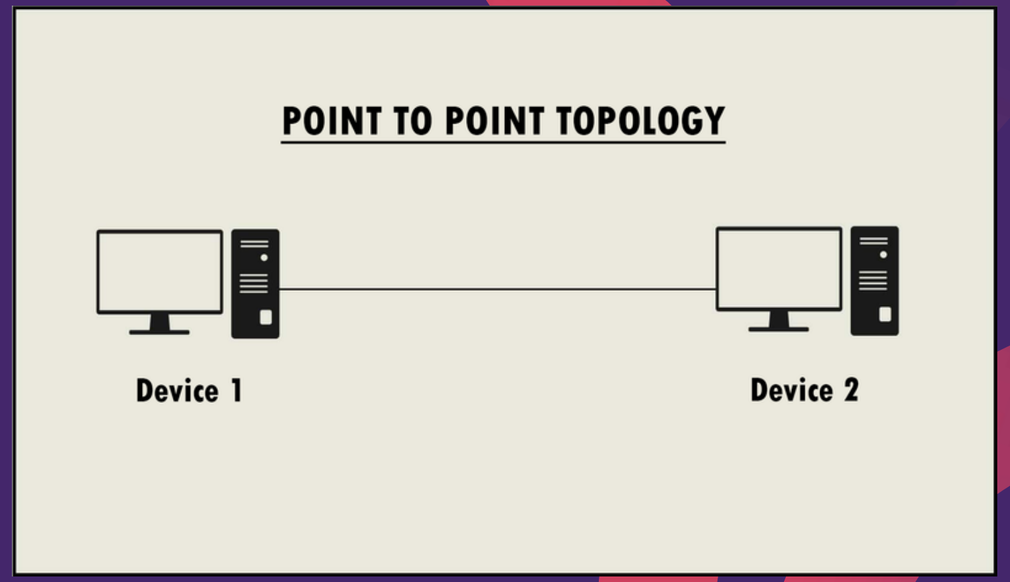
- There are two main types of routing algorithms used in the network layer: **distance-vector routing** and **link-state routing**. In distance-vector routing, routers exchange information about the distance and direction to all reachable destinations. In link-state routing, routers exchange information about the entire topology of the network, including the state of each link.

PROTOCOLS IN NETWORK LAYER

1. Internet Protocol (IP): IP is the primary protocol used by the Internet for transmitting data between devices. It provides logical addressing and routing services, and it is responsible for breaking data into packets and reassembling them at their destination.
2. Internet Control Message Protocol (ICMP): ICMP is a protocol used by network devices to communicate error messages and other control information. It is used by routers to send error messages back to the source device when packets cannot be delivered.
3. Address Resolution Protocol (ARP): ARP is a protocol used to map IP addresses to MAC addresses. It allows devices to find the hardware address of a device on the same network segment.
4. Reverse Address Resolution Protocol (RARP): RARP is a protocol used to map MAC addresses to IP addresses. It is used by diskless workstations to obtain their IP address from a server.
5. Internet Group Management Protocol (IGMP): IGMP is a protocol used by hosts to join and leave multicast groups. It is used by routers to forward multicast traffic to only those devices that have expressed an interest in receiving it.

Point to Point Network

Point-to-point connections, sometimes called point-to-point link, P2P links, private line, or leased line, securely connect two locations using a Layer 2 data connection, building a closed network. Data on these connections don’t travel on the public internet, where it could be vulnerable to hackers or cyberattacks. Point-to-point connections are extremely secure, so much so that only limited data encryption may be necessary when using them. However, if an extremely high degree of security is required, think government or finance, some carriers offer encryption with their point-to-point services.



When Is Point-to-Point the Right Choice?

- Point-to-point connections are available in a range of service levels, but they're most commonly used for high bandwidth (the amount of data that can be transmitted in a specific window of time) and low latency (the delay between the user's action and the network's response). Point-to-point connections also have minimal packet loss, which occurs when small units of data or "packets" never reach their destination.

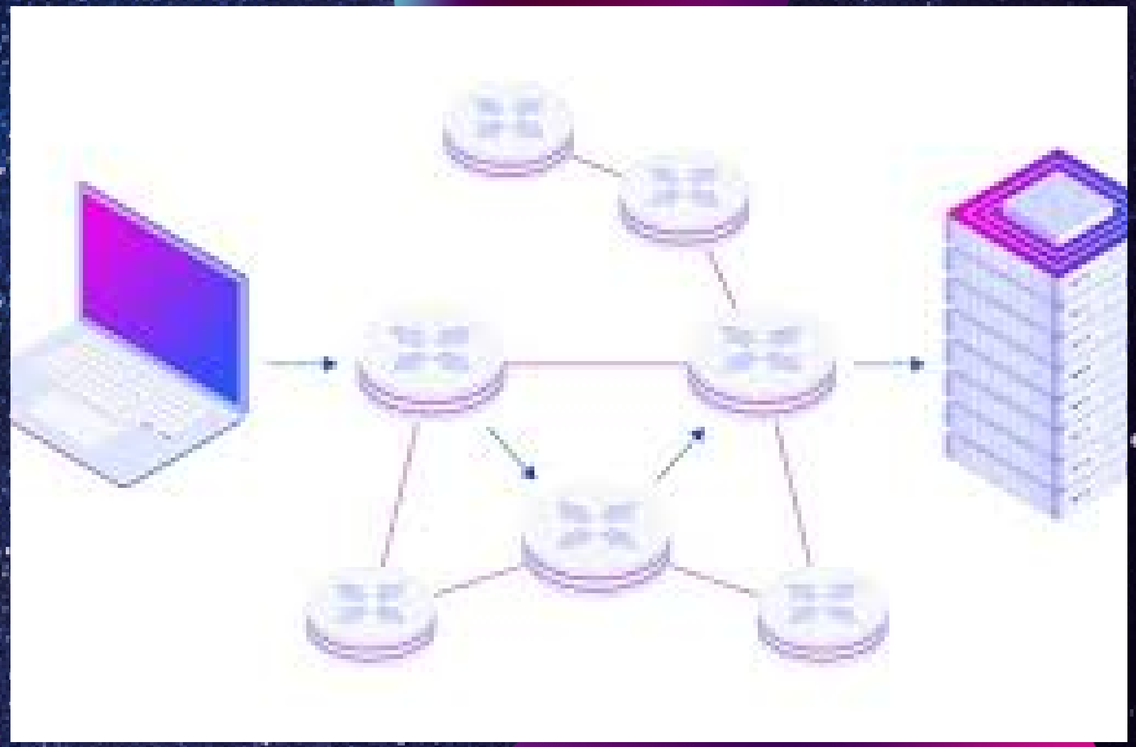
- Point-to-point connections can deliver these high service levels because data always travel back and forth in the same way across a dedicated route. When businesses use the public internet, their data may be routed differently at different times or rerouted to reach its destination. With a point-to-point connection, data travels a predictable path, meeting customer expectations (and provider promises) for a high quality of service (QoS).

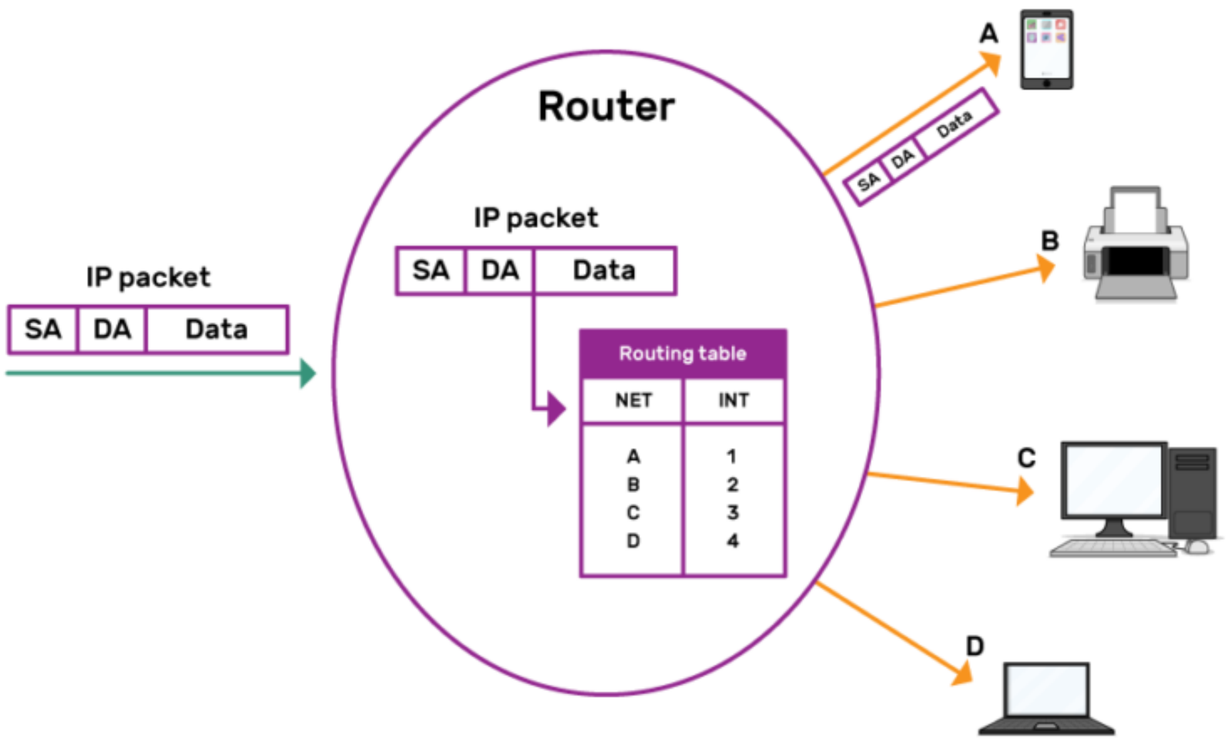
- Examples: The link between the TV and the remote control
- The link between the air conditioner and the remote control
- A LAN (local area network) is a network that connects two computers.

Routing in Computer Networks

WHAT IS ROUTING?

Routing is the process of path selection in any network. A computer network is made of many machines, called nodes, and paths or links that connect those nodes. Communication between two nodes in an interconnected network can take place through many different paths. Routing is the process of selecting the best path using some predetermined rules.

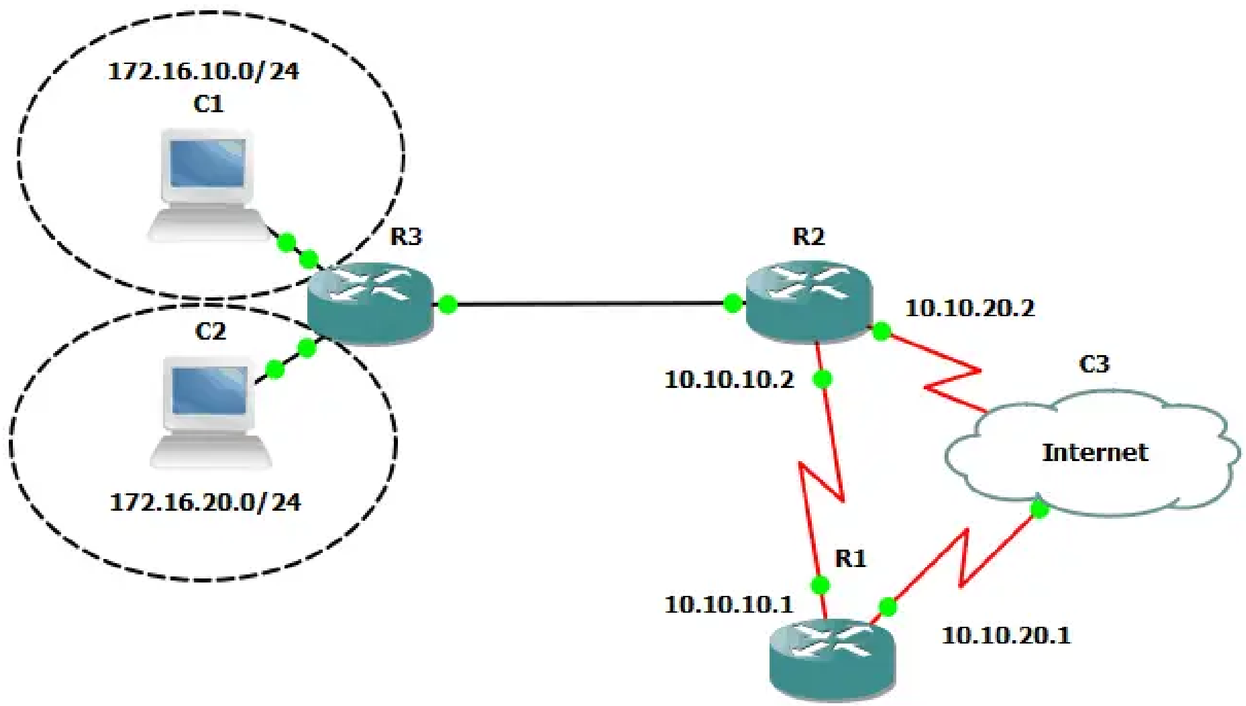




HOW ROUTING WORKS ?

Data moves along any network in the form of data packets. Each data packet has a header that contains information about the packet's intended destination. As a packet travels to its destination, several routers might route it multiple times. Routers perform this process millions of times each second with millions of packets.

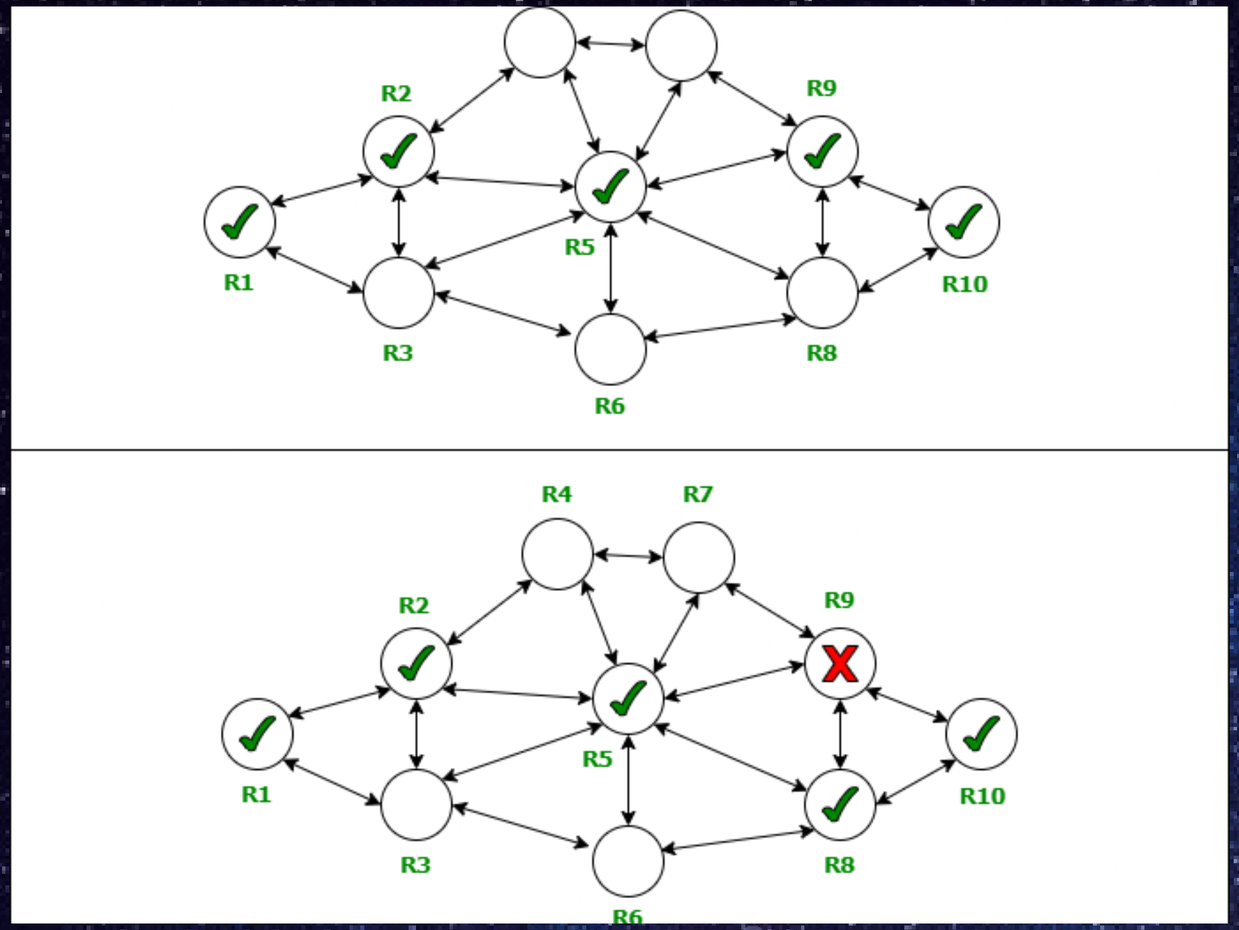
When a data packet arrives, the router first looks up its address in a routing table. Then the router forwards or moves the packet onward to the next point in the network.



STATIC ROUTING

In static routing, a network administrator uses static tables to manually configure and select network routes. Static routing is helpful in situations where the network design or parameters are expected to remain constant.

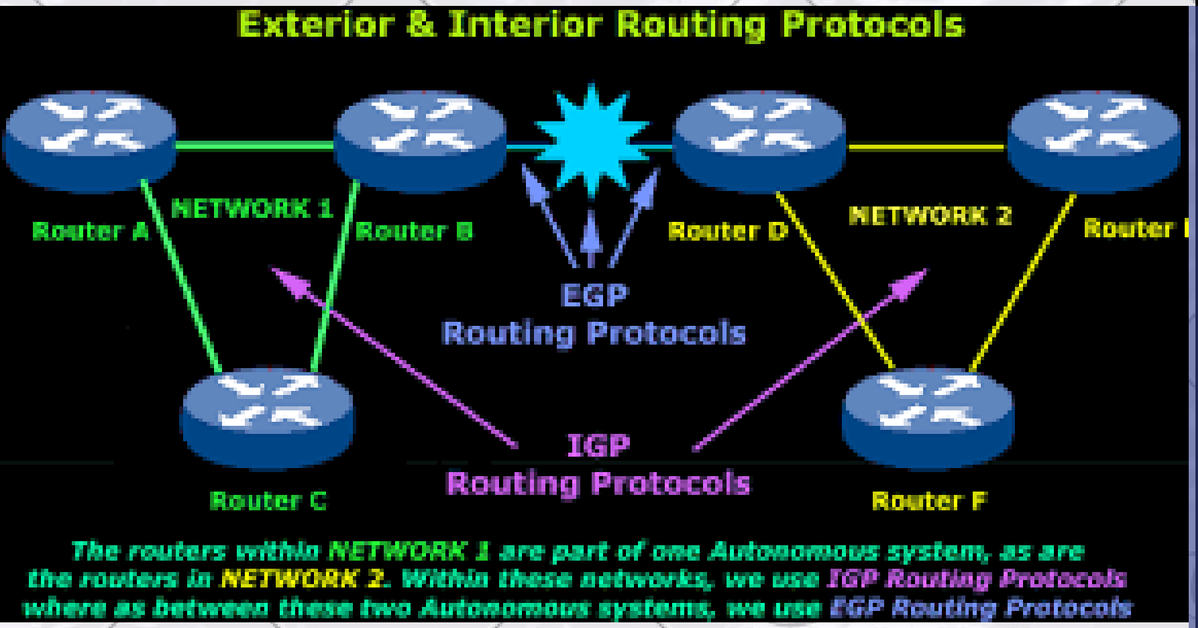
The static nature of this routing technique comes with expected drawbacks, such as network congestion. While administrators can configure fallback paths in case a link fails, static routing generally decreases the adaptability and flexibility of networks, resulting in limited network performance.



DYNAMIC ROUTING

In dynamic routing, routers create and update routing tables at runtime based on actual network conditions. They attempt to find the fastest path from the source to the destination by using a dynamic routing protocol, which is a set of rules that create, maintain, and update the dynamic routing table.

The biggest advantage of dynamic routing is that it adapts to changing network conditions, including traffic volume, bandwidth, and network failure.



MAIN ROUTING PROTOCOLS

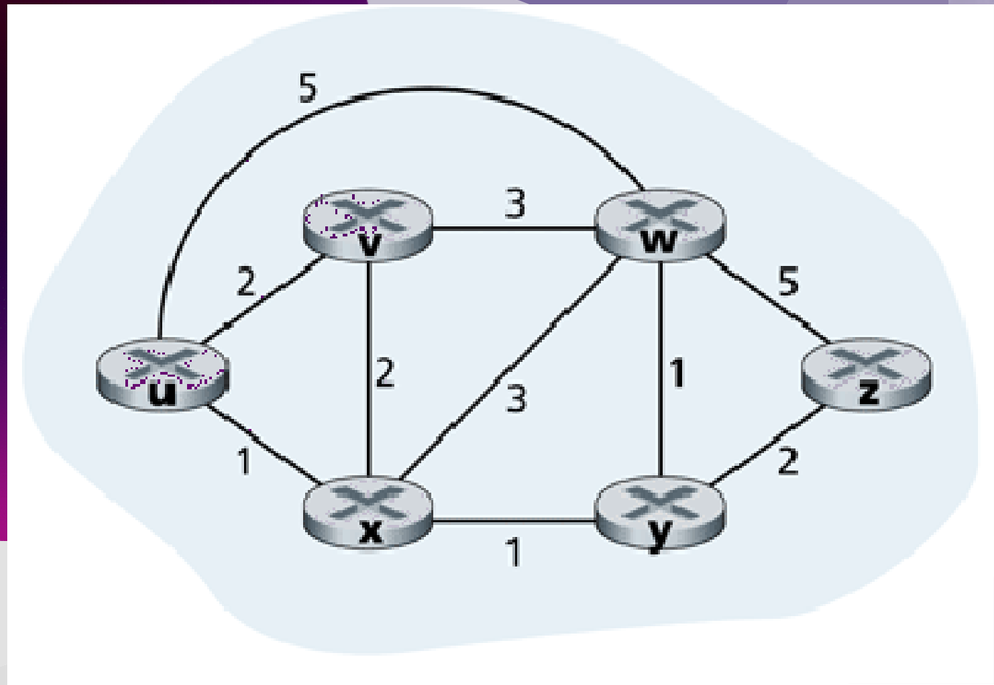
A routing protocol is a set of rules that specify how routers identify and forward packets along a network path. Routing protocols are grouped into two distinct categories: interior gateway protocols and exterior gateway protocols.

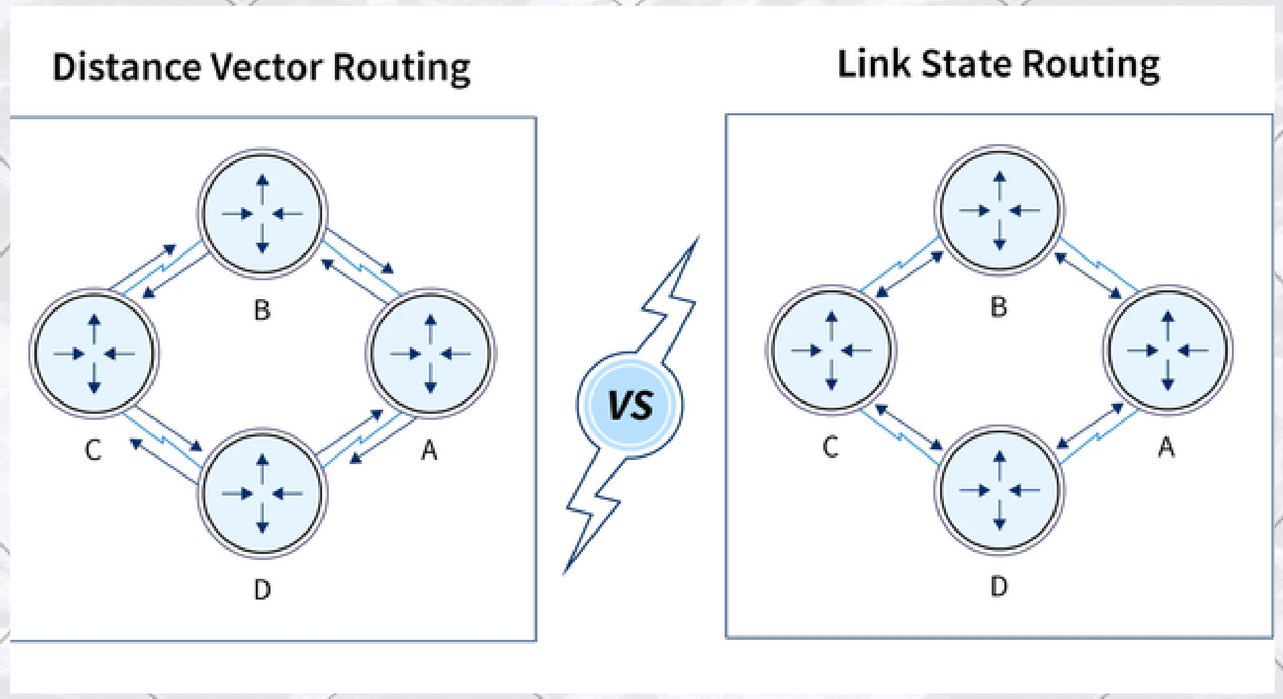
Routing protocols work by exchanging routing information between routers and updating their routing tables based on the information received. The routing tables contain information about the network topology, including the available paths and their associated metrics such as bandwidth, delay, and hop count.

ROUTING ALGORITHMS

Routing algorithms are software programs that implement different routing protocols. They work by assigning a cost number to each link; the cost number is calculated using various network metrics. Every router tries to forward the data packet to the next best link with the lowest cost.

- Static Routing Algorithm
- Dynamic Routing Algorithm

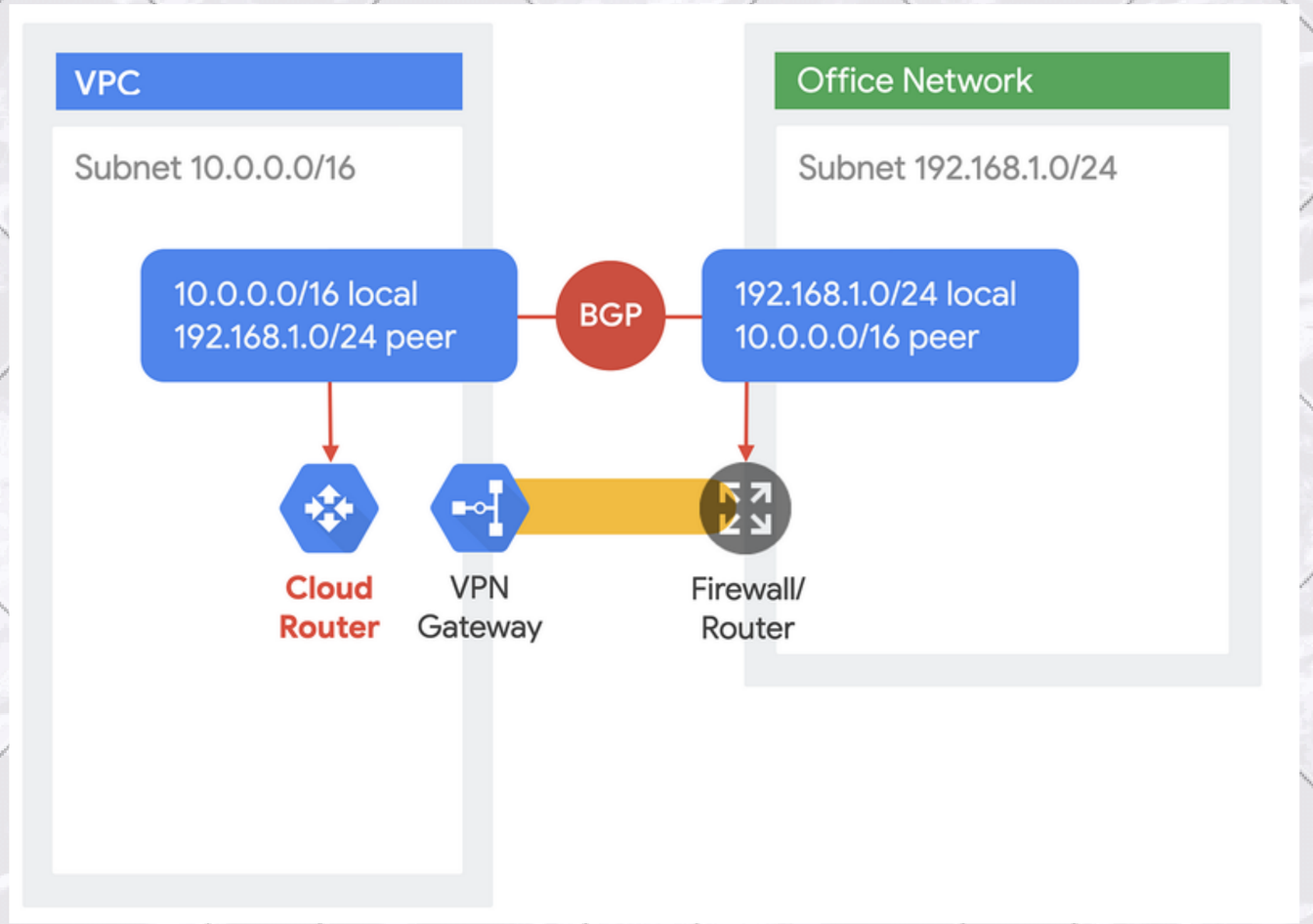




EXAMPLE OF ROUTING ALGORITHM

The **Distance Vector Routing algorithm** requires all routers to periodically update each other about the best path information they have found. Each router sends information about the current assessment of the total cost to all known destinations. Eventually, every router in the network discovers the best path information for all possible destinations.

In **Link State Routing**, every router discovers all other routers in the network. Using this information, a router creates a map of the complete network and then calculates the shortest path for any data packet.



HOW HAS ROUTING EVOLVED ?

Routing has evolved to meet the requirements of advances in network technology. Routing is no longer just about switching data packets between autonomous systems and the internet.

We now have cloud infrastructure with computing resources and hardware hosted by third-party cloud providers. These cloud resources are connected virtually to create a virtual network of resources that businesses can use to host and run applications. Many organizations now have hybrid networks that consist of both on-premises networks with internal hardware and cloud networks.

Computer Networks

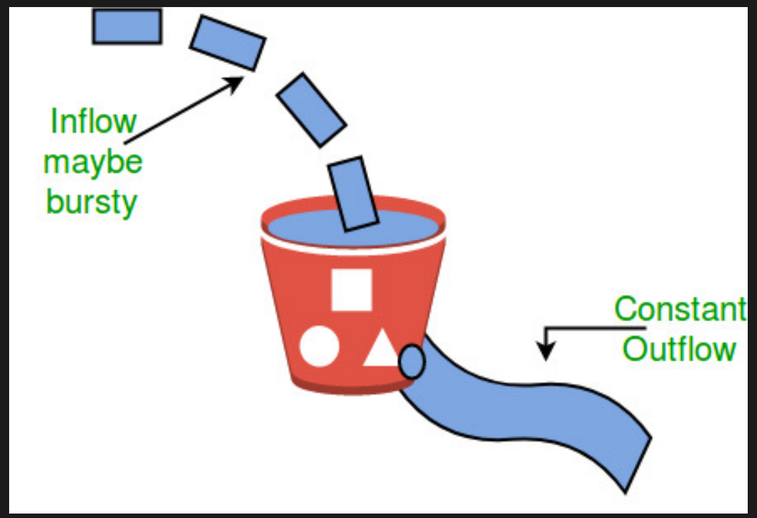
CONGESTION CONTROL

Agenda

1. Congestion
2. Congestion control
3. Open loop congestion control
4. Closed loop congestion control
5. Congestion control in TCP
6. Congestion control in Frame Relay

Congestion

Congestion happens in any system that involves waiting. For example, congestion happens on a freeway because any abnormality in the flow, such as an accident during rush hour, creates blockage.

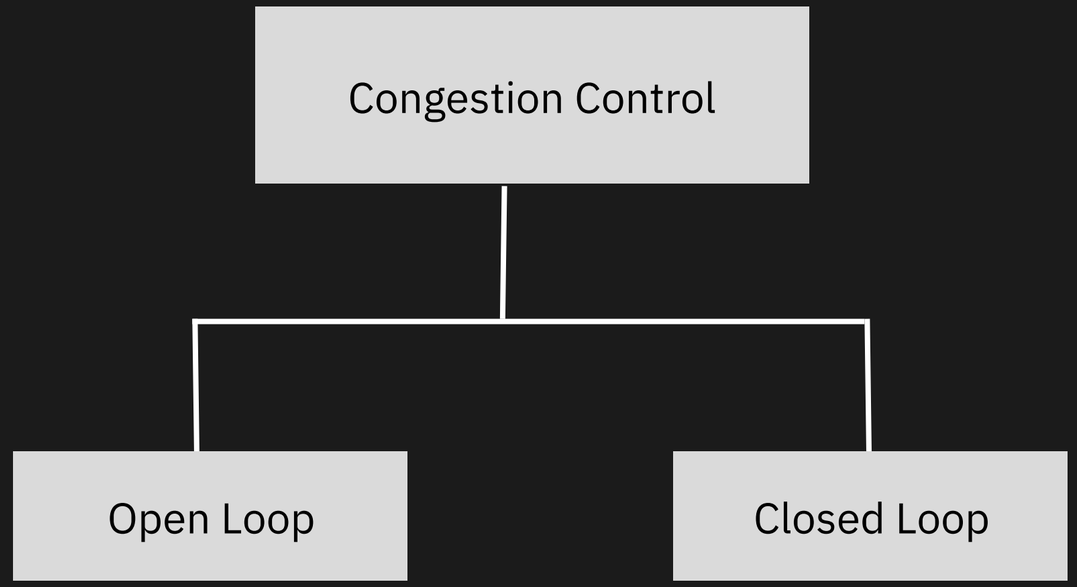


An important issue in a packet-switched network is **congestion.** Congestion in a network may occur if the **load** on the network-the number of packets sent to the network-is greater than the *capacity* of the network-the number of packets a network can handle.

Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

Congestion Control

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal)



- Retransmission policy
- window policy
- acknowledgment policy
- discard policy
- admission policy

- Back Pressure
- Choke packet
- Implicit signalling
- Explicit signalling

Open Loop Control

Retransmission Protocol

If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion.

Window Policy

The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control.

Acknowledgment Policy

The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.

Open Loop Control

DISCARDING POLICY

A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.

ADMISSION POLICY

An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network

CLOSED LOOP CONTROL

BACKPRESSURE

The technique of *backpressure* refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes.

CHOKE PACKET

A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke packet methods. In backpres- sure, the warning is from one node to its upstream node. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly.

IMPLICIT SIGNALLING

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested.

EXPLICIT SIGNALLING

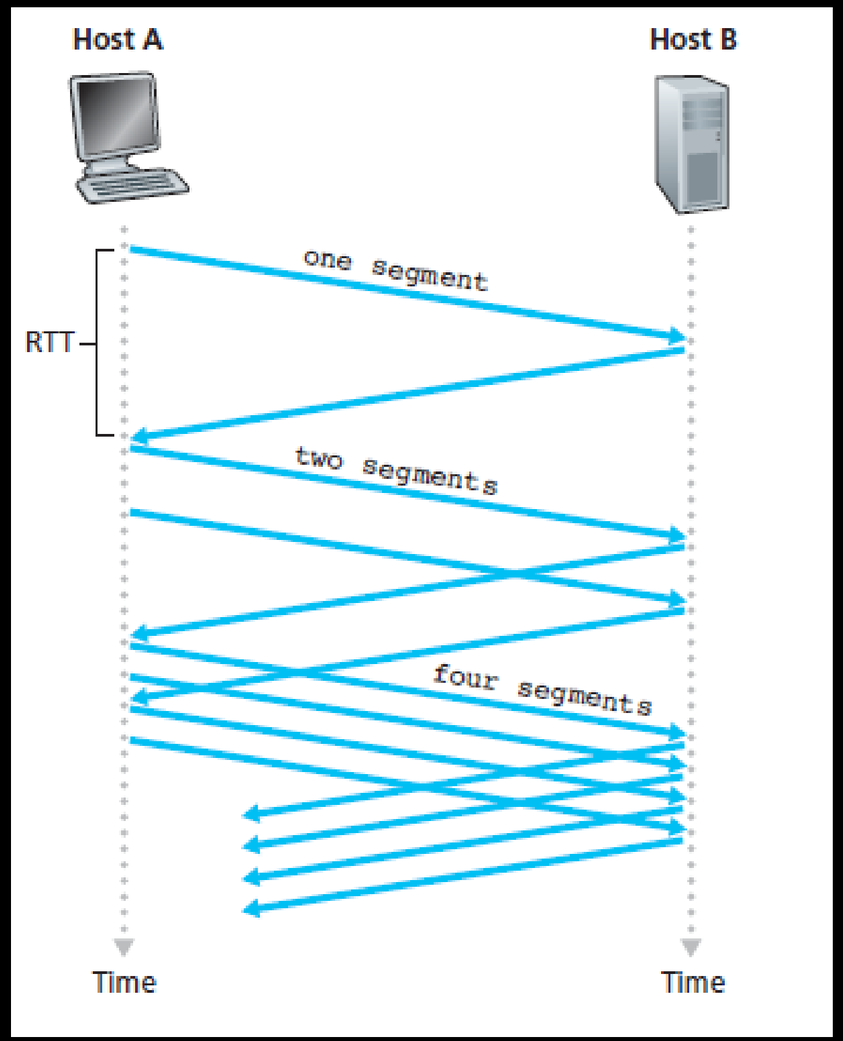
The node that experiences congestion can explicitly send a signal to the source or desti- nation. The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data.

Congestion Control in TCP

TCP's general policy for handling congestion is based on three phases:

Slow Start

Exponential Increase One of the algorithms used in TCP congestion control is called slow start. This algorithm is based on the idea that the size of the con- gestion window *(cwnd)* starts with one maximum segment size (MSS). The MSS is determined during connection establishment by using an option of the same name.



Congesiton Avoidance

Additive Increase If we start with the slow-start algorithm, the size of the congestion window increases exponentially. To avoid congestion before it happens, one must slow down this exponential growth.

CP defines another algo- rithm called congestion avoidance, which undergoes an additive increase instead of an exponential one. When the size of the congestion window reaches the slow-start threshold, the slow-start phase stops and the additive phase begins.

Congestion Detection

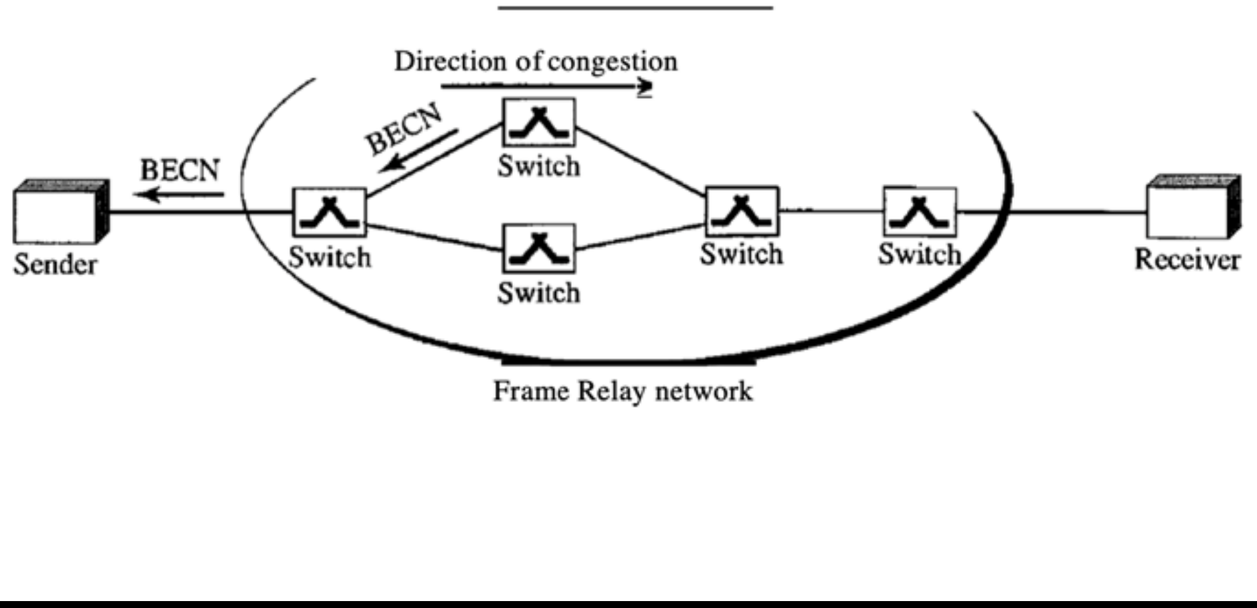
Multiplicative Decrease If congestion occurs, the congestion window size must be decreased. The only way the sender can guess that congestion has occurred is by the need to retransmit a segment. However, retransmission can occur in one of two cases: when a timer times out or when three ACKs are received. In both cases, the size of the threshold is dropped to one-half, a multiplicative decrease

Congestion Avoidance in Frame Relay

For congestion avoidance, the Frame Relay protocol uses 2 bits in the frame to explicitly warn the source and the destination of the presence of congestion.

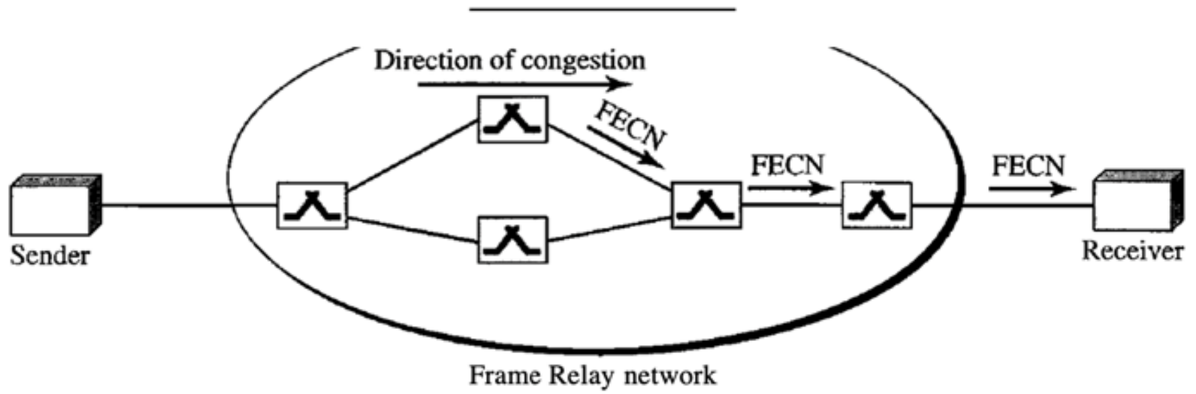
BECN

The backward explicit congestion notification (BECN) bit warns the sender of congestion in the network.



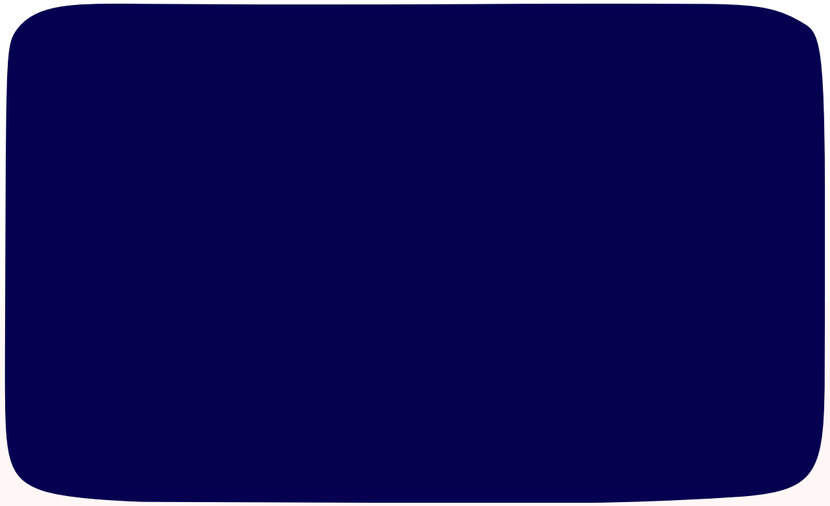
FECN

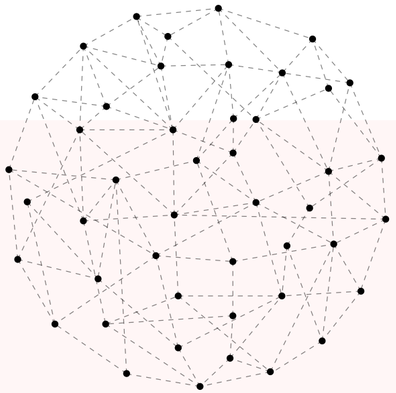
The forward explicit congestion notification (FECN) bit is used to warn the receiver of congestion in the network.



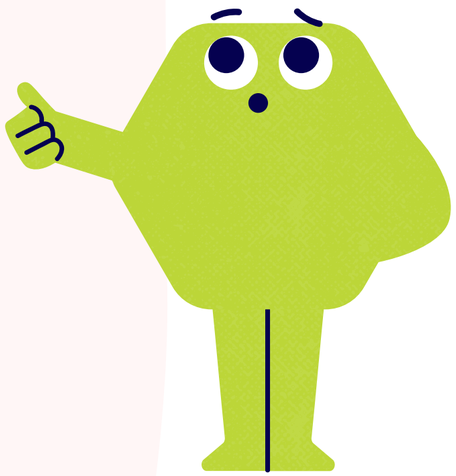
INTERNETWORKING TCP / IP

A DETAILED STUDY





CONTENTS



WHAT IS INTERNETWORKING?

- Internetworking refers to the process of connecting two or more separate computer networks to enable communication and data exchange between them.
- It involves the use of hardware and software components that allow different network types and protocols to work together seamlessly.

- The goal of Internetworking is to create a single, global communication infrastructure that connects networks of different types and sizes.
- This allows organizations and individuals to communicate and exchange information regardless of their location or the network they are using.

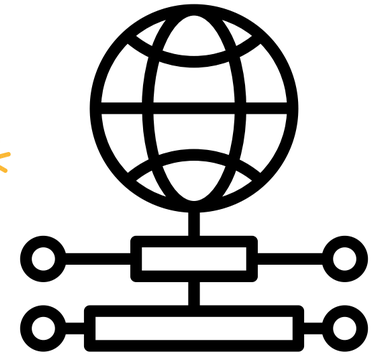
What is TCP/IP ?

TCP/IP is a set of communication protocols that define how data is transmitted over the internet. It is the foundation of the internet and enables us to send and receive data across the world quickly and reliably.

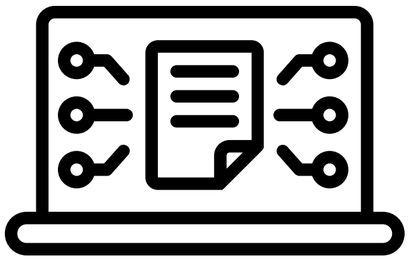
1. Transmission Control Protocol (TCP)

- **Transmission Control Protocol (TCP) is a standard that defines how to establish and maintain a network conversation by which applications can exchange data.**
- **TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules that define the Internet. The Internet Engineering Task Force (IETF) defines TCP in the Request for Comment (RFC) standards document number 793.**
- **TCP breaks data into packets, reassembles them at the destination, and ensures they are delivered correctly.**

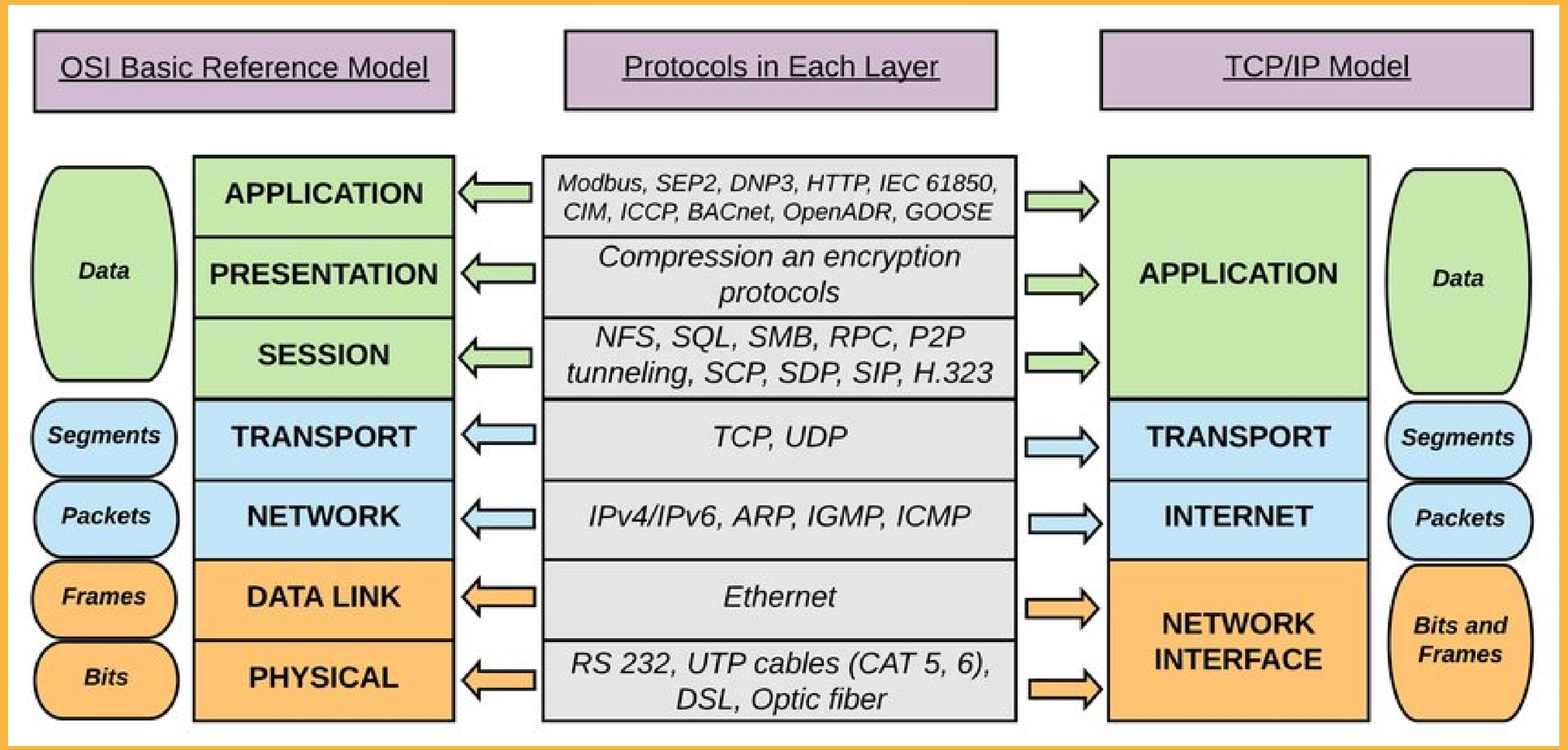
2. Internet Protocol (IP)



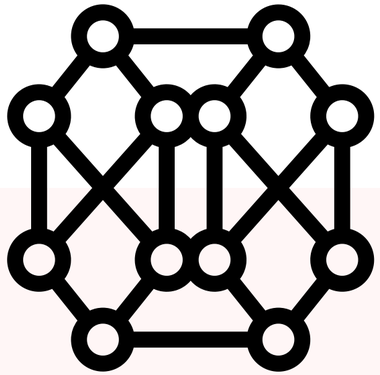
- **The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets.**
- **IP information is attached to each packet, and this information helps routers to send packets to the right place.**
- **Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.**
- **Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.**

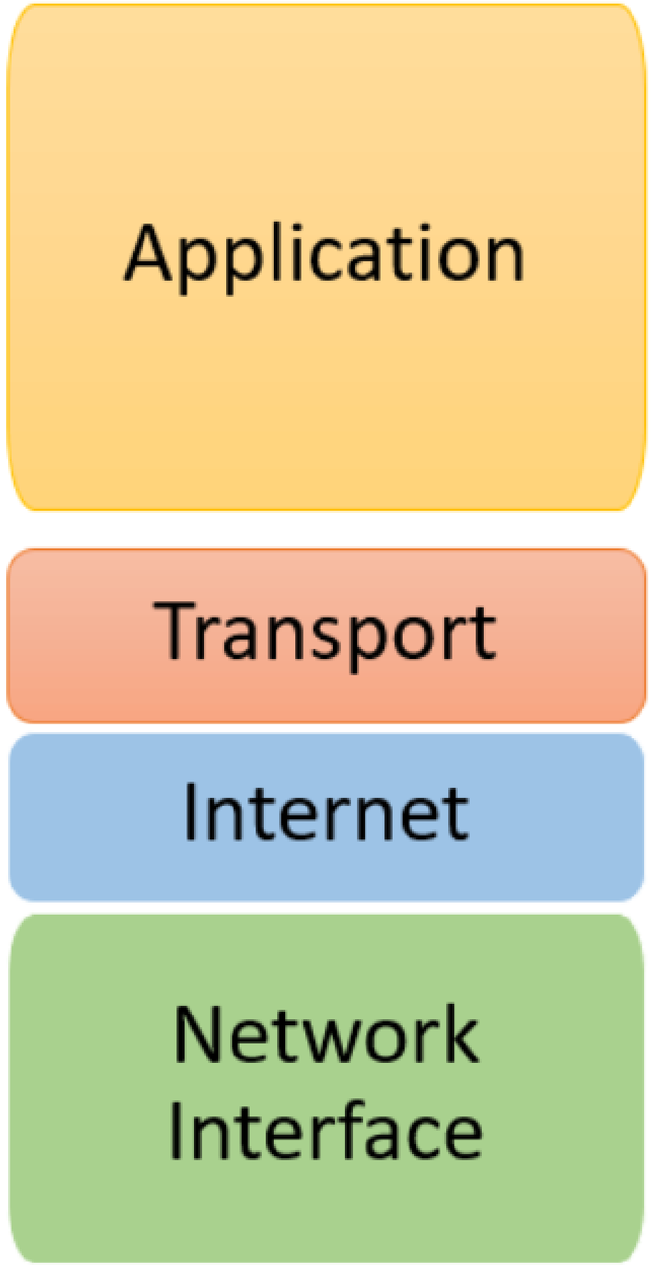


OSI V/S TCP/IP


OSI Basic Reference Model
Protocols in Each Layer
TCP/IP Model
Data
Segments
Packets
Frames
Bits
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL
Modbus, SEP2, DNP3, HTTP, IEC 61850, CIM, ICCP, BACnet, OpenADR, GOOSE
Compression an encryption protocols
NFS, SQL, SMB, RPC, P2P tunneling, SCP, SDP, SIP, H.323
TCP, UDP
IPv4/IPv6, ARP, IGMP, ICMP
Ethernet
RS 232, UTP cables (CAT 5, 6), DSL, Optic fiber
APPLICATION
TRANSPORT
INTERNET
NETWORK INTERFACE
Data
Segments
Packets
Bits and Frames

Layers of TCP/IP

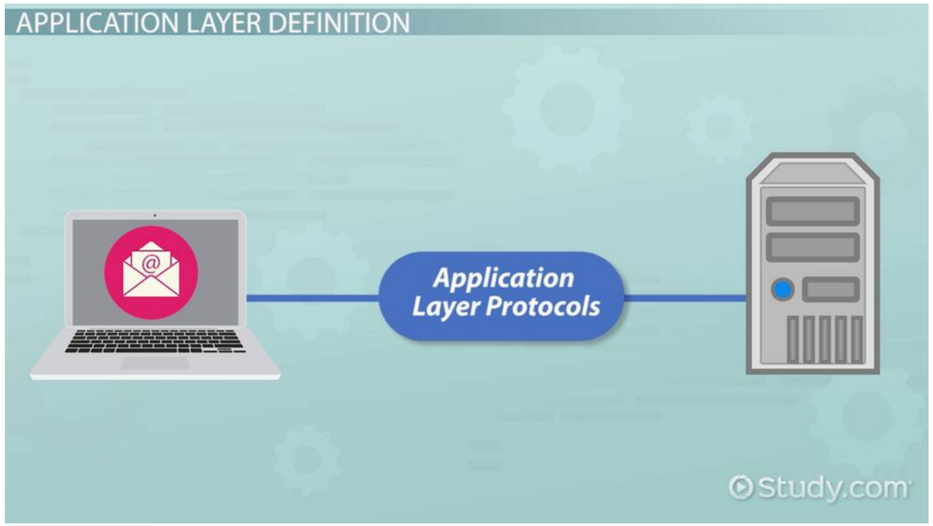




TCP/IP Conceptual Layers

Application Layer

- The application layer is the highest abstraction layer of the TCP/IP model that provides the interfaces and protocols needed by the users. It combines the functionalities of the session layer, the presentation layer, and the application layer of the OSI model.



The functions of the application layer are:

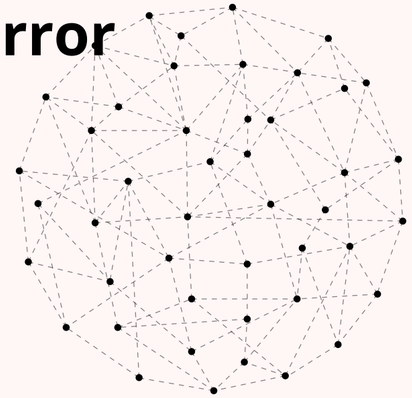
- It facilitates the user to use the services of the network.
- It is used to develop network-based applications.
- It provides user services like user log-in, naming network devices, formatting messages, and e-mails, transfer of files, etc.
- It is also concerned with error handling and recovery of the message as a whole.

Transport Layer

The transport layer is responsible for error-free, end-to-end delivery of data from the source host to the destination host.
It corresponds to the transport layer of the OSI model.

The functions of the transport layer are:

- It facilitates the communicating hosts to carry on a conversation.
- It provides an interface for the users to the underlying network.
- It can provide for a reliable connection. It can also carry out error checking, flow control, and verification.



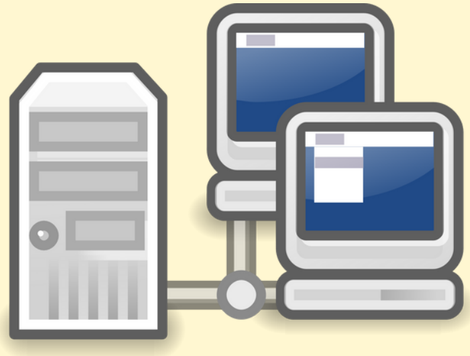
Internet Layer

- **An internet layer is the second layer of TCP/IP layer of the TCP/IP model. It is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer till they reach the destination irrespective of the route they take.**
- **The Internet layer offers the functional and procedural method for transferring variable-length data sequences from one node to another with the help of various networks.**

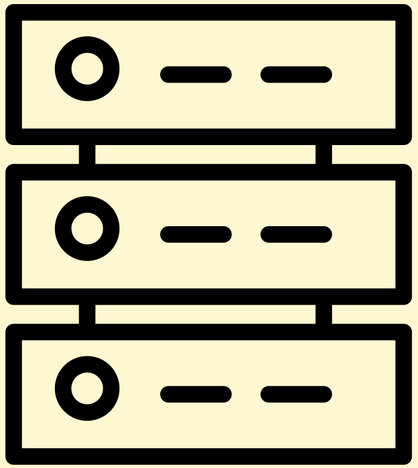
Layer-management protocols that belong to the network layer are:

1. **Routing protocols**
2. **Multicast group management**
3. **Network-layer address assignment.**

Network Interface Layer



- Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer.
- It helps you to define details of how data should be sent using the network.
- It also includes how bits should optically be signaled by hardware devices that directly interface with a network medium, like coaxial, optical, coaxial, fiber, or twisted-pair cables.

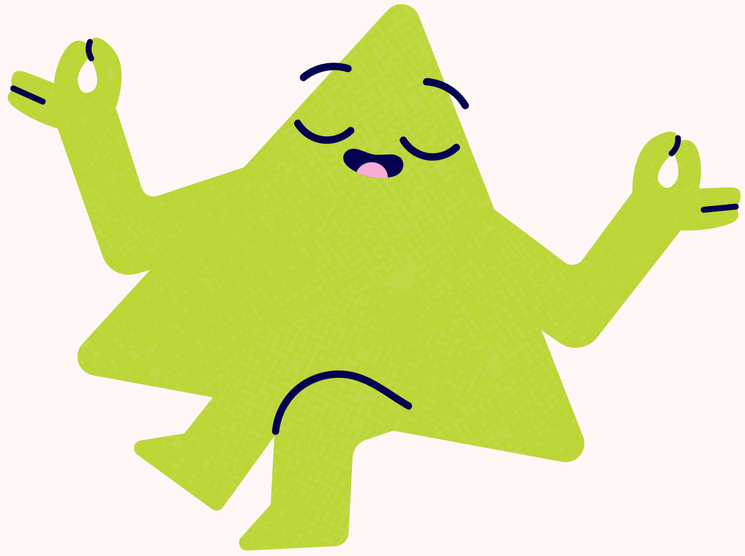


- A network layer is a combination of the data line and defined in the article on the OSI reference model. This layer defines how the data should be sent physically through the network.
- This layer is responsible for the transmission of the data between two devices on the same network.

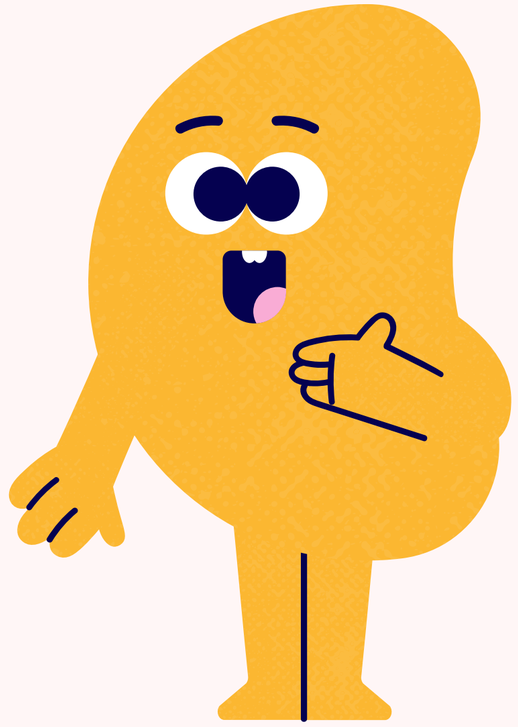
CONCLUSION

- The TCP/IP model is a communication protocol stack that defines how data is transmitted over a network.
- It consists of four layers: the application layer, transport layer, internet layer, and network access layer.
- At the application layer, protocols such as HTTP, FTP, SMTP, and DNS are used to facilitate communication between applications.
- The transport layer provides end-to-end communication services between the source and destination hosts and is responsible for error detection and correction.
- The internet layer deals with routing and packet forwarding across multiple networks.

Overall, the TCP/IP model is a widely used and important model for networking, and it forms the basis for modern internet communication.



Thank you



IP Packet and IP Address

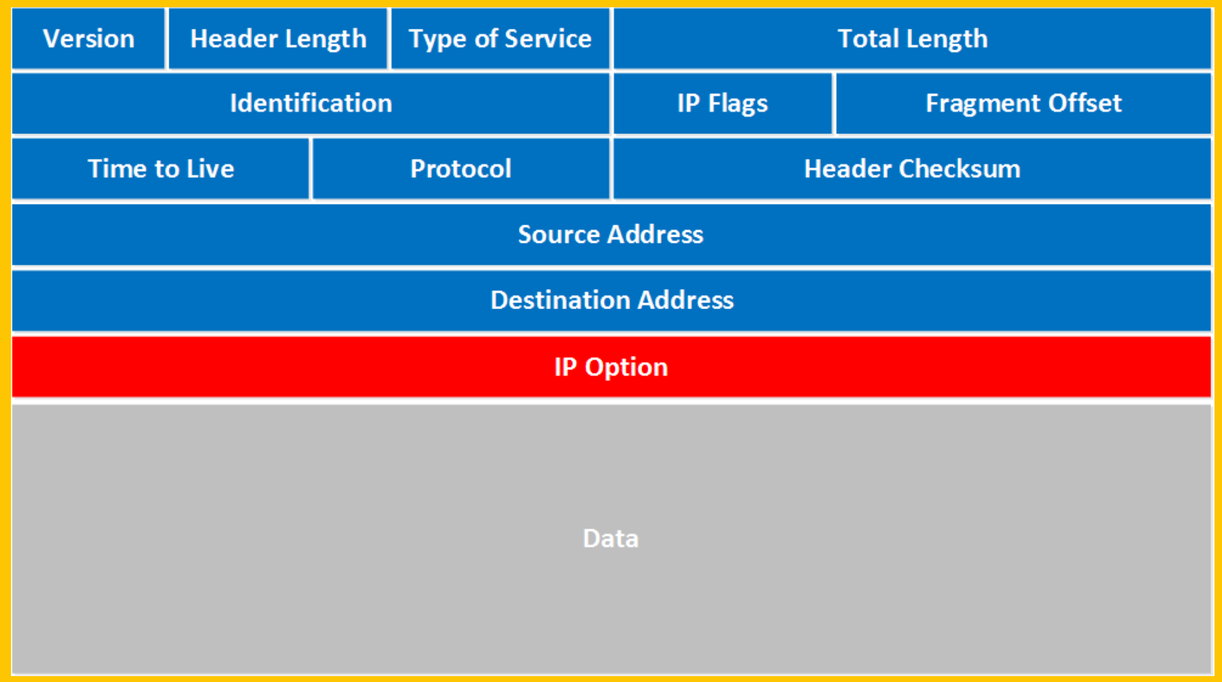
START

Definition of IP packet

- IP stands for Internet Protocol, which is a set of rules that govern how data is sent and received over the Internet
- An IP packet is a unit of data that is encapsulated within an IP header and contains the data being transmitted over the Internet..

Structure of an IP Packet

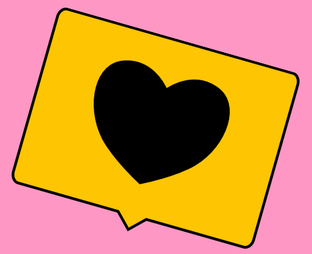
- An IP packet is composed of two main parts: the header and the payload.
- The header contains information such as the source and destination IP addresses, version of IP, time-to-live (TTL), and more.
- The payload is the actual data being transmitted, such as a file, email, or web page.



IP Address

- An IP address is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- It serves as the address of the device and allows it to send and receive data over the Internet.
- There are two types of IP addresses namelyIPv4
- IPv6

IPv4 vs IPv6



IPv4

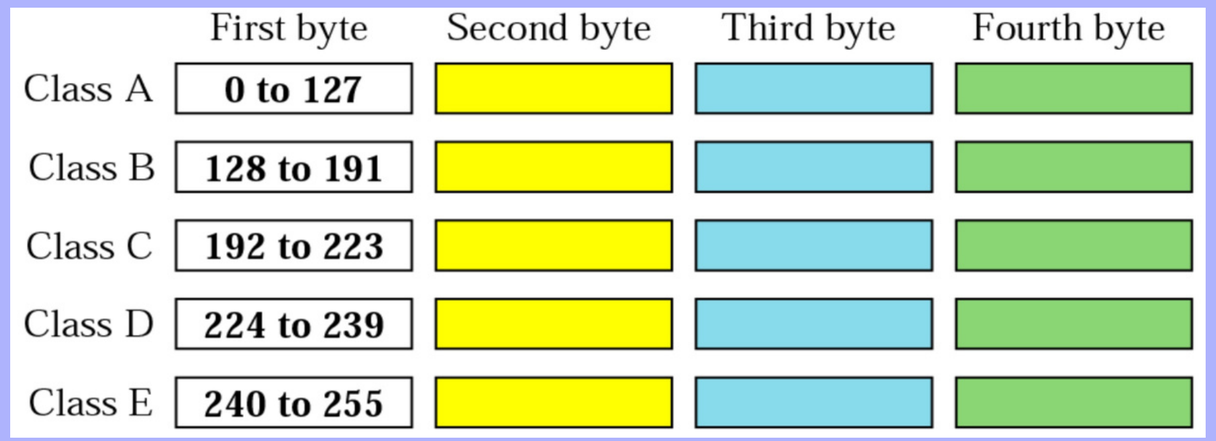
- IPv4 is a 32-bit address.
- IPv4 has 5 different classes of IP address that includes Class A, B, C, D, and E.
- It generates 4 billion unique addresses
- The IP address is represented in decimal.

IPv6

- IPv6 is a 128-bit address.
- IPv6 does not contain classes of IP addresses.
- It generates 340 undecillion unique addresses
- The representation of the IP address in hexadecimal.

IPv4 Address Classes

- IPv4 addresses are divided into five classes: A, B, C, D, and E.
- Each class has a specific range of addresses and is used for different purposes, such as Class A for large networks, Class B for medium-sized networks, and Class C for small networks.



Private vs. Public IP Addresses

Private Addresses

- Private IP addresses are used within private networks, such as home or office networks, and are not routable over the Internet.
- The private network is typically short-range.
-

Public Addresses

- Public IP addresses are assigned by Internet Service Providers (ISPs) and are routable over the Internet, allowing devices to communicate with each other globally.
- The public network was never intended to span long distances.

Conclusion

- IP packets and IP addresses are fundamental components of the Internet Protocol and are essential for the communication of data over the Internet.
- Understanding how IP packets and IP addresses work is crucial for networking professionals to design, configure, and troubleshoot IP-based networks.

IPv 4 and IPv 6

Introduction to IP addressing

- **Definition of IP addressing: IP addressing is the process of assigning unique numerical identifiers to every device connected to a network that uses the Internet Protocol for communication.**
- **Importance of IP addressing in networking: IP addressing is essential for enabling communication between devices on a network and for routing traffic across the internet.**
- **Brief history of IP addressing: IP addressing was first introduced in 1981 with the development of IPv4, which has been the standard protocol for internet communication for many years.**

IPv4 Overview: The Basics

What is IPv4 and how it works: IPv4 is a 32-bit address scheme that allows for 4.3 billion unique IP addresses. It uses a hierarchical addressing structure that consists of network addresses and host addresses.

Characteristics of IPv4 addresses: IPv4 addresses are divided into five classes (A, B, C, D, and E) and can be either public or private. They are also subject to address exhaustion, as the number of available IPv4 addresses is limited.

Limitations of IPv4 addressing scheme: The limitations of IPv4 addressing, such as address exhaustion, have led to the development of IPv6 as a replacement.

IPv6 Overview: The Basics

- **What is IPv6 and how it works: IPv6 is a 128-bit address scheme that allows for 340 undecillion unique IP addresses. It uses a simplified addressing structure that consists of a global routing prefix and a unique interface identifier.**
- **Characteristics of IPv6 addresses: IPv6 addresses are structured differently than IPv4 addresses and have a larger address space, which allows for more efficient routing and network management.**
- **Advantages of IPv6 addressing scheme: IPv6 offers several advantages over IPv4, including a larger address space, simplified addressing structure, and built-in security features.**

Key differences between IPv4 and IPv6

- Number of bits used in IPv4 and IPv6 addresses: IPv4 addresses are 32 bits in length, while IPv6 addresses are 128 bits in length.
- Address space differences between IPv4 and IPv6: IPv4 allows for 4.3 billion unique addresses, while IPv6 allows for 340 undecillion unique addresses.
- Routing and forwarding differences between IPv4 and IPv6: IPv6 has a more efficient routing and forwarding mechanism than IPv4, which improves network performance.

Addressing Differences between IPv4 and IPv6

- **IPv4 address classes and classful addressing: IPv4 addresses are divided into five classes (A, B, C, D, and E) and use classful addressing to allocate IP addresses to networks.**
- **IPv6 address structure and hierarchy: IPv6 addresses use a hierarchical addressing structure that consists of a global routing prefix and a unique interface identifier.**
- **IPv6 address types and uses: IPv6 addresses can be either global or link-local and are used for various purposes, such as routing, host addressing, and multicast.**

Routing Differences between IPv4 and IPv6

- **Routing protocols used in IPv4: IPv4 uses routing protocols such as RIP, OSPF, and BGP for routing.**
- **Routing protocols used in IPv6: IPv6 uses routing protocols such as OSPFv3, BGP4+, and IS-IS for routing.**
- **Differences in routing table structures between IPv4 and IPv6: IPv6 has a simpler and more efficient routing table structure than IPv4, which allows for faster routing.**

Security Differences between IPv4 and IPv6

- **Security issues and vulnerabilities in IPv4: IPv4 is subject to several security issues, such as IP spoofing, packet sniffing, and denial of service attacks.**
- **Security features and improvements in IPv6: IPv6 includes several built-in security features, such as IPsec, which provides authentication and encryption of network traffic.**
- **Address configuration and security in IPv6: IPv6 includes a stateless address autoconfiguration (SLAAC) mechanism that allows for automatic configuration of IP addresses without the need for a central DHCP server. This mechanism also includes security features to prevent address spoofing and other attacks.**
- **Transitioning from IPv4 to IPv6: The transition from IPv4 to IPv6 presents unique security challenges and requires careful planning and implementation to ensure a secure and smooth transition.**

Deployment Status of IPv6

- Adoption rates of IPv6: While IPv6 has been available for many years, adoption rates have been slow due to various factors, such as cost, complexity, and compatibility issues.

IPv6 deployment strategies: Organizations can adopt various strategies for deploying IPv6, such as dual-stack deployment, tunneling, and translation.

Current status and future prospects of IPv6: Despite slow adoption rates, IPv6 is expected to eventually replace IPv4 as the dominant protocol for internet communication, as the need for more IP addresses and improved network performance continues to grow.

Conclusion

Summary of key points: IPv4 and IPv6 are two different protocols used for internet communication, with significant differences in their addressing, routing, and security mechanisms.

Importance of understanding IPv4 and IPv6: As the world becomes increasingly connected, it is important for network engineers and administrators to understand the differences between IPv4 and IPv6 to ensure efficient and secure network communication.

Final thoughts and future directions: The transition from IPv4 to IPv6 will continue to be an important issue in networking and will require ongoing efforts from industry and government to ensure a smooth and secure transition.