CAPITULO 1

INTRODUCCIÓN A LAS REDES DE DATOS

ASISTENCIA

CALIFICACIONES

Contenido

1. Componentes, dispositivos e interfaces de red
2. Clasificación de las redes
3. Métricas de desempeño de red y tráfico
4. Redes convergentes y redes confiables
5. Modelo de referencia de interconexión de sistemas abiertos (OSI)
6. Protocolo de control de transmisión/protocolo de internet (TCP/IP)

Globally Connected

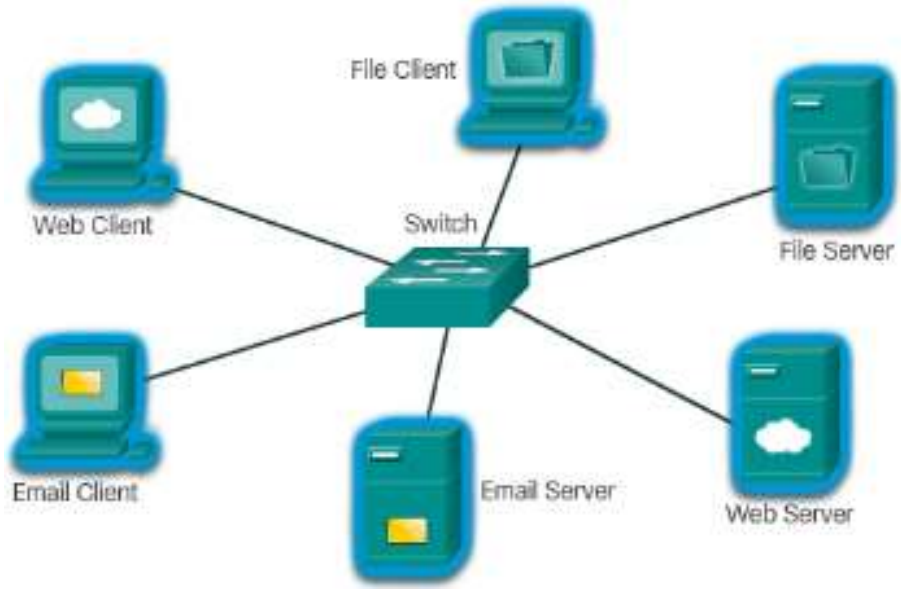
Networking Today

- Network has no boundary and supports the way we:
  - Learn
  - Communicate
  - Work
  - Play

Globally Connected

Providing Resources in a Network

- Networks of Many Sizes
  - Small Home / Office Networks
  - Medium to Large Networks
  - World Wide Network
- Clients and Servers
  - Clients request and display information
  - Servers provide information to other devices on the network
- Peer-to-Peer
  - Computers can be both server and client at the same time.
  - What are the advantages?
  - What are the disadvantages?



Network Components

- End Devices
  - Either the source or destination of a message
  - Name some end devices
- Intermediary Network Devices
  - Connect multiple individual networks to form an internetwork
  - Connect the individual end devices to the network
  - Ensure data flows across the network
  - Provide connectivity
- Network Media
  - Provide the pathway for data transmission
  - Interconnect devices
  - Name the three types of media

Network Components

- Network Representations
  - What do the symbols represent?
- Topology Diagrams
  - Physical
  - Logical

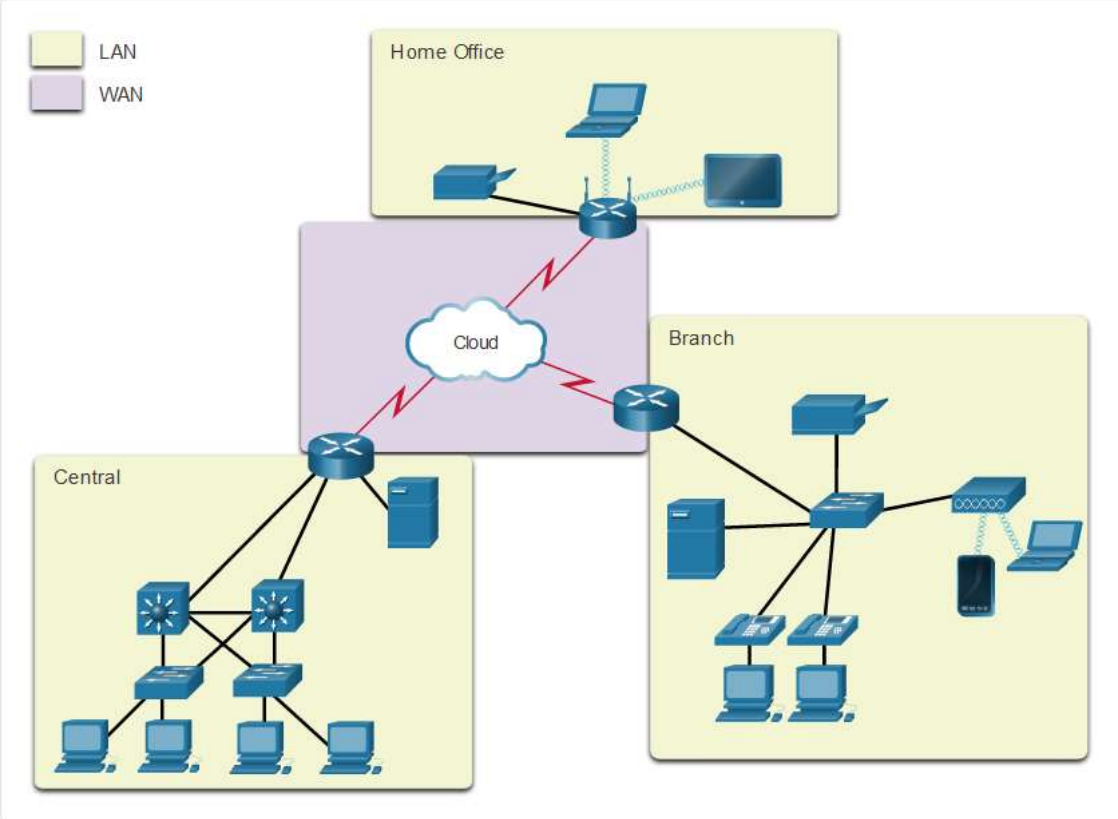
LANs and WANs

Network infrastructures vary greatly in terms of:

- Size of the area covered
- Number of users connected
- Number and types of services available
- Area of responsibility

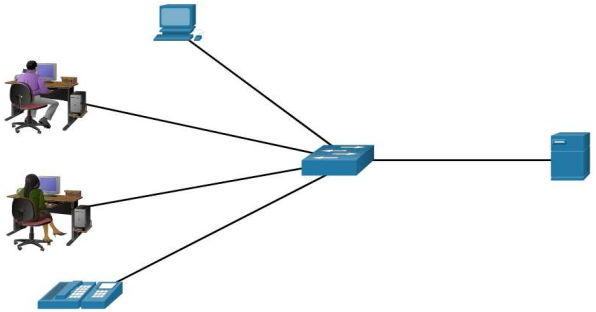
Two most common types of networks:

- Local Area Network (LAN)
- Wide Area Network (WAN).

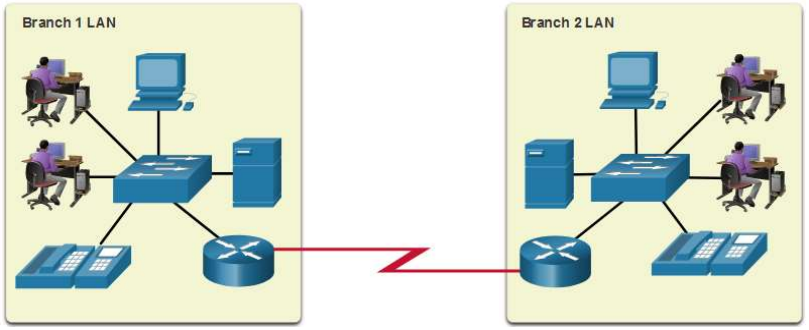


LANs and WANs (cont.)

A LAN is a network infrastructure that spans a small geographical area.



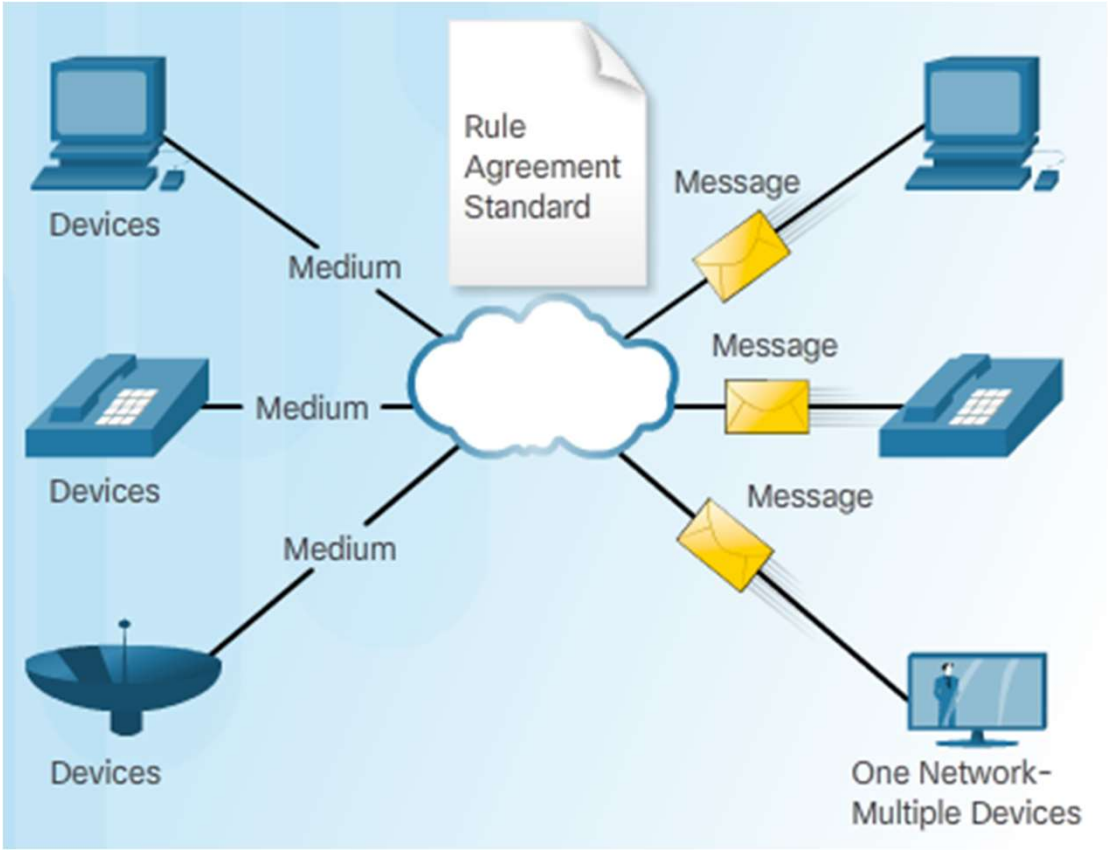
A WAN is a network infrastructure that spans a wide geographical area.



LAN	WAN
Interconnect end devices in a limited area.	Interconnect LANs over wide geographical areas.
Administered by a single organization or individual.	Typically administered by one or more service providers.
Provide high-speed bandwidth to internal devices.	Typically provide slower speed links between LANs.

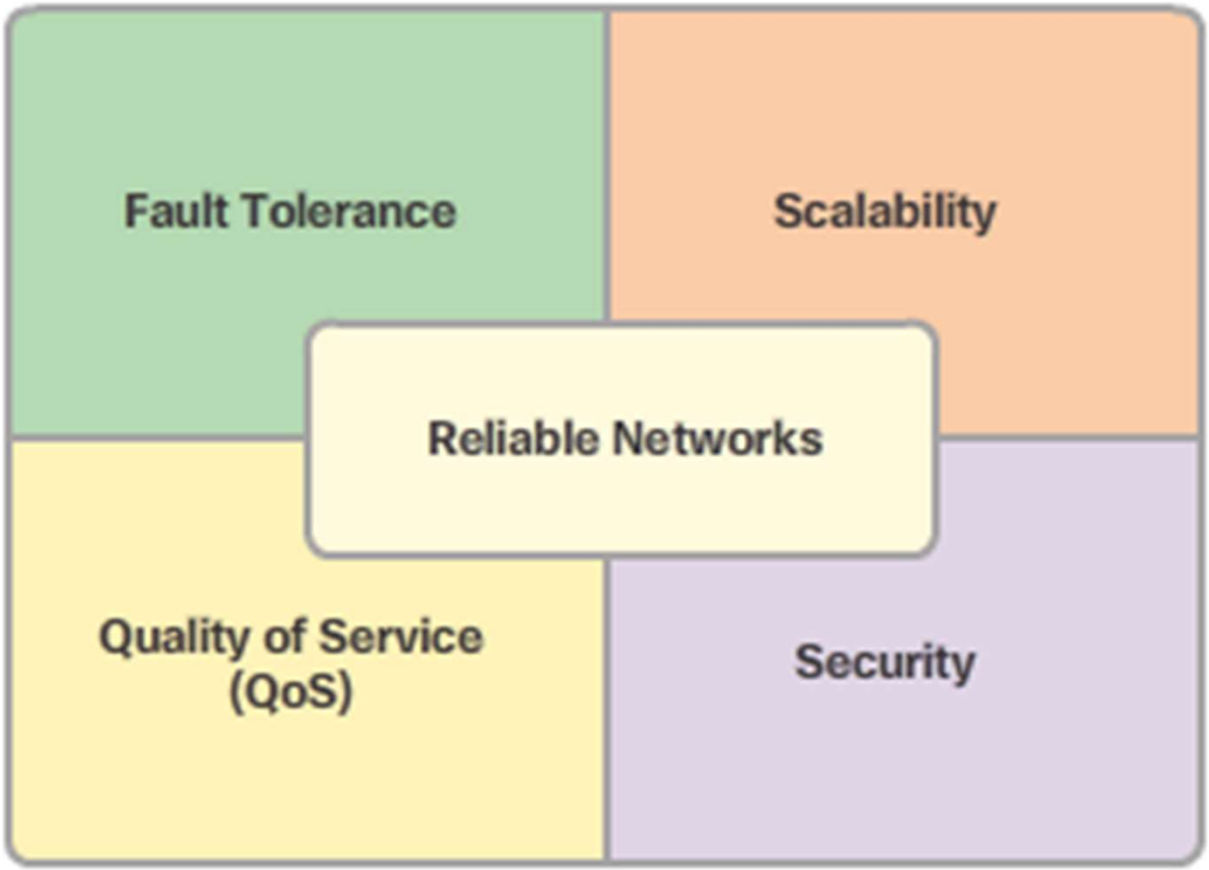
Converged Networks

- Traditional Separate Networks
  - Each network with its own rules and
- The Converging Network
  - Capable of delivering data, voice, and video over the same network infrastructure



Reliable Network

- Four Basic Characteristics of Network Architecture
  - Fault Tolerance
  - Scalability
  - Quality of Service (QoS)
  - Security



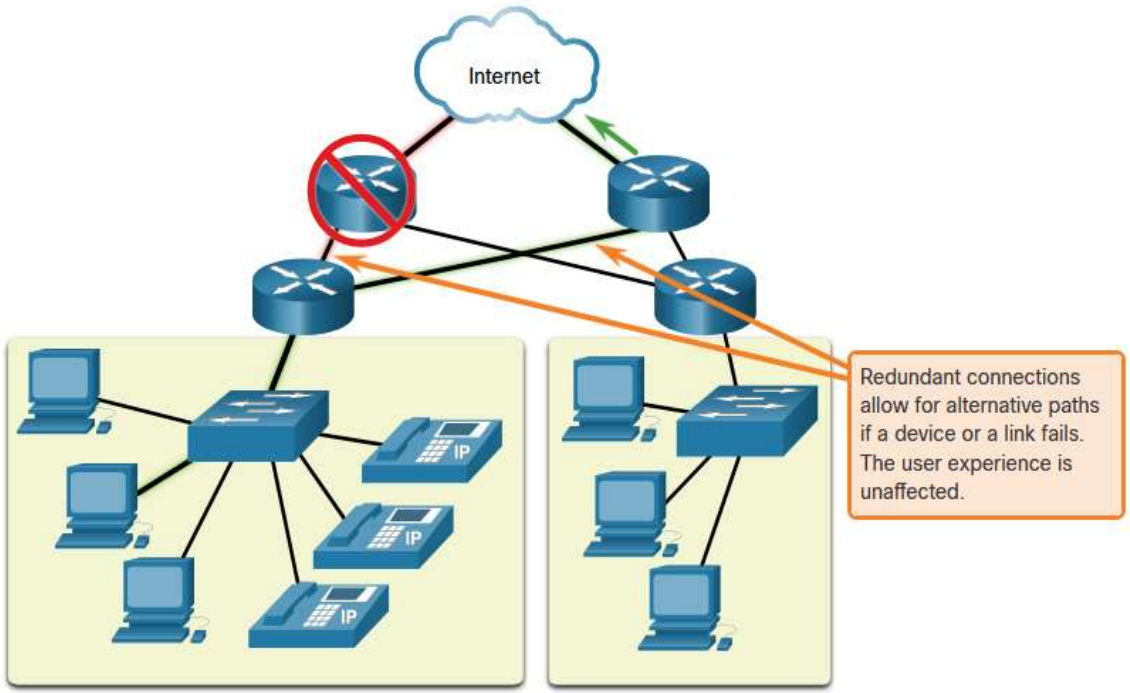
Fault Tolerance

A fault tolerant network limits the impact of a failure by limiting the number of affected devices. Multiple paths are required for fault tolerance.

Reliable networks provide redundancy by implementing a packet switched network:

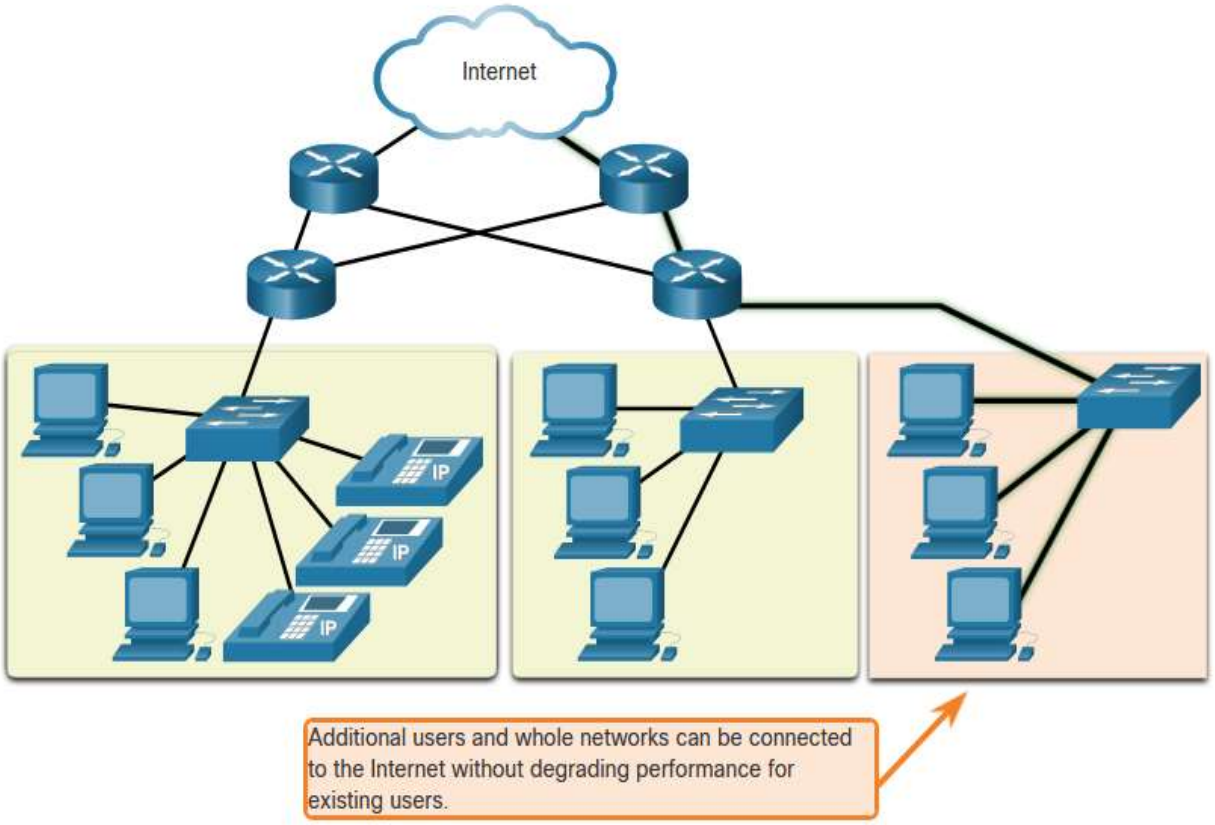
- Packet switching splits traffic into packets that are routed over a network.
- Each packet could theoretically take a different path to the destination.

This is not possible with circuit-switched networks which establish dedicated circuits.



Reliable Network

Scalability



A scalable network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users.

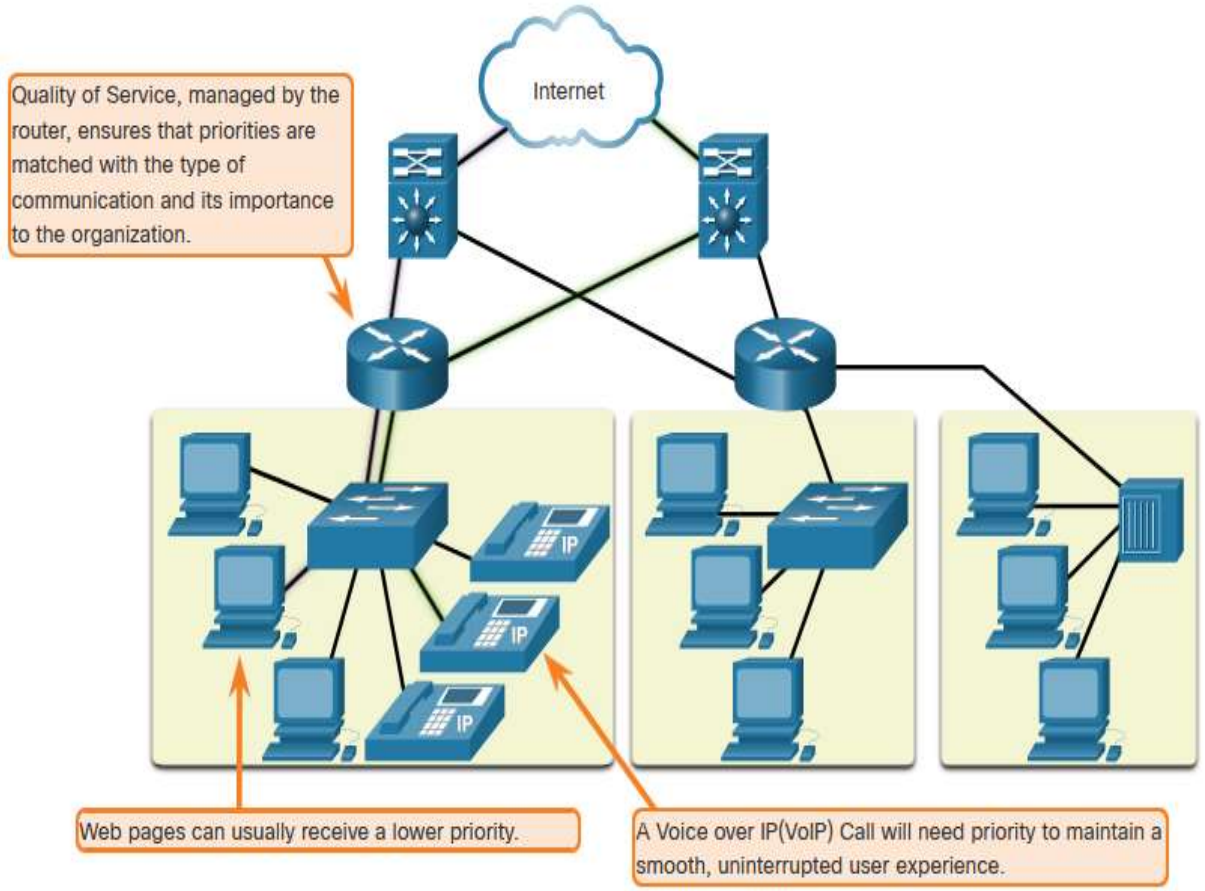
Network designers follow accepted standards and protocols in order to make the networks scalable.

Quality of Service

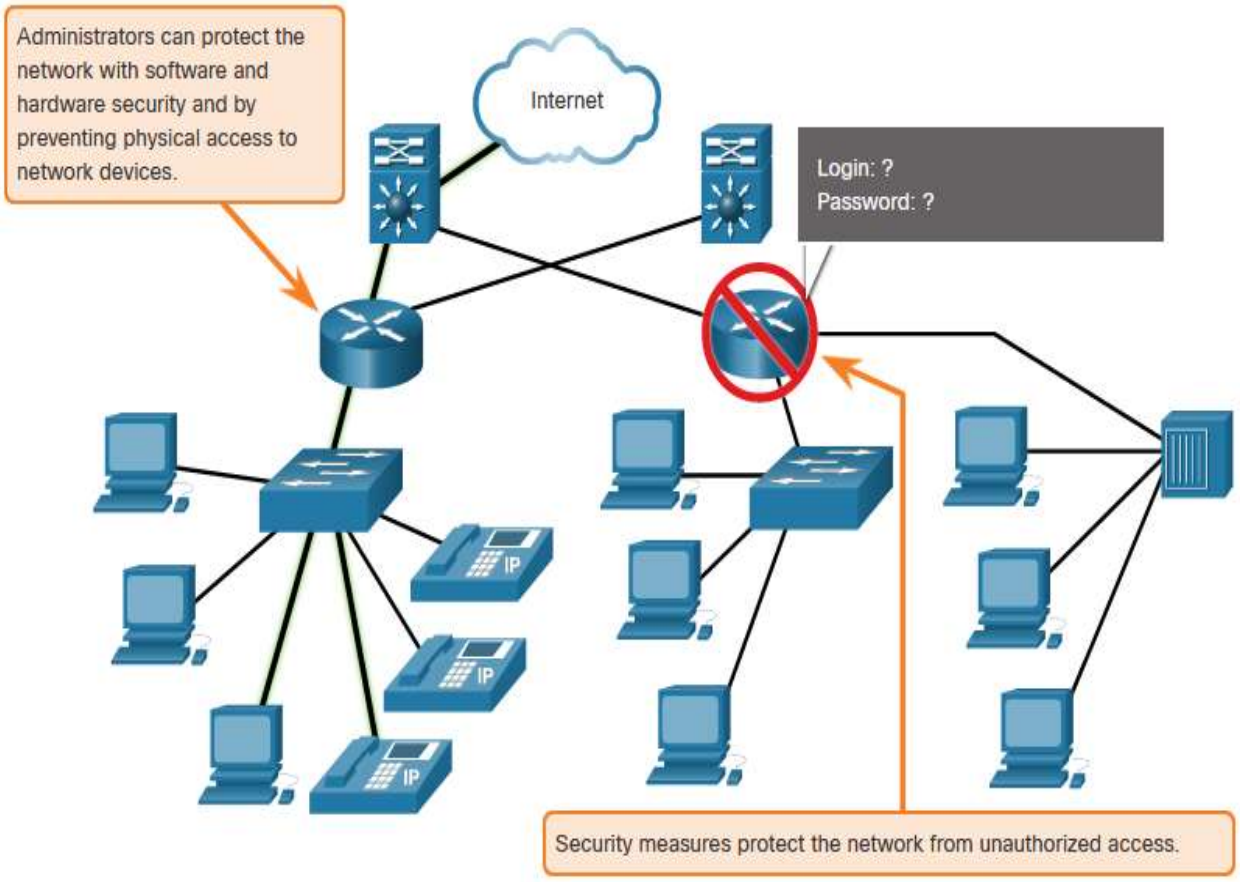
Voice and live video transmissions require higher expectations for those services being delivered.

Have you ever watched a live video with constant breaks and pauses? This is caused when there is a higher demand for bandwidth than available – and QoS isn't configured.

- Quality of Service (QoS) is the primary mechanism used to ensure reliable delivery of content for all users.
- With a QoS policy in place, the router can more easily manage the flow of data and voice traffic.



Network Security



There are two main types of network security that must be addressed:

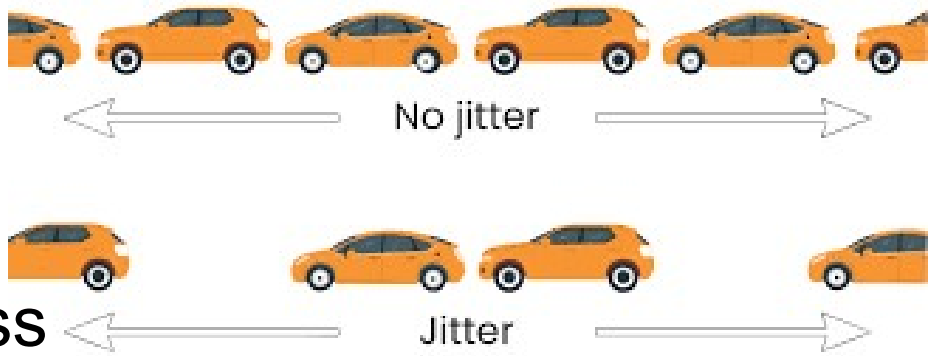
- Network infrastructure security
  - Physical security of network devices
  - Preventing unauthorized access to the devices
- Information Security
  - Protection of the information or data transmitted over the network

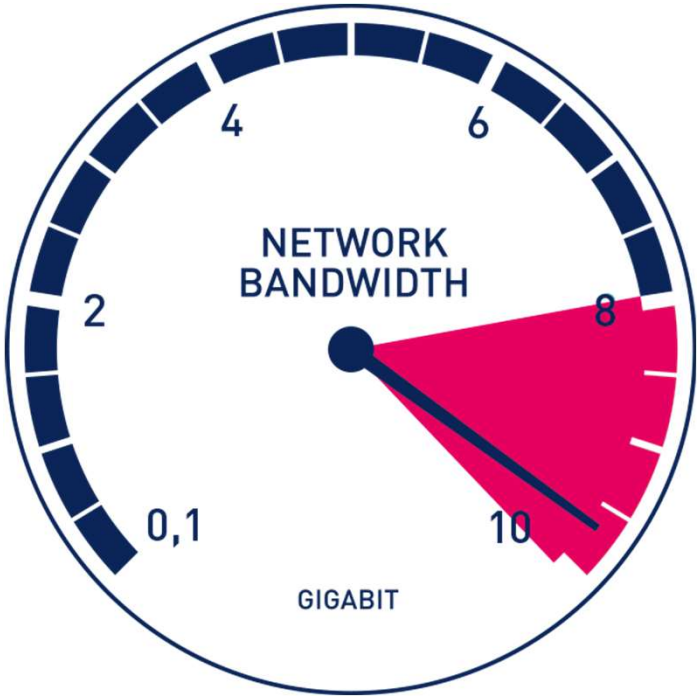
Three goals of network security:

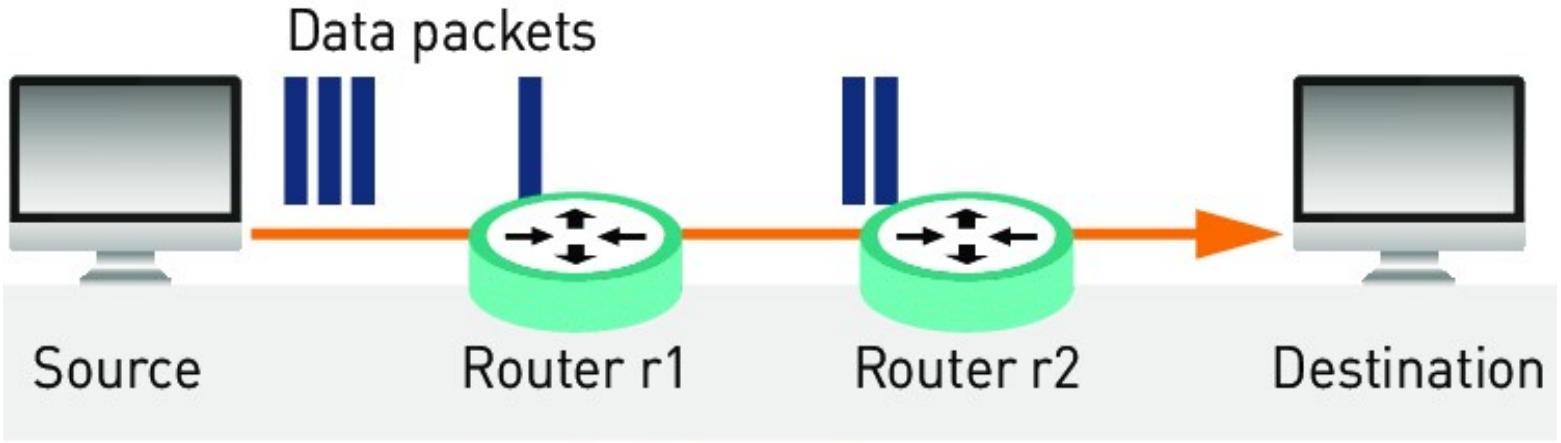
- Confidentiality – only intended recipients can read the data
- Integrity – assurance that the data has not be altered with during transmission
- Availability – assurance of timely and reliable access to data for authorized users

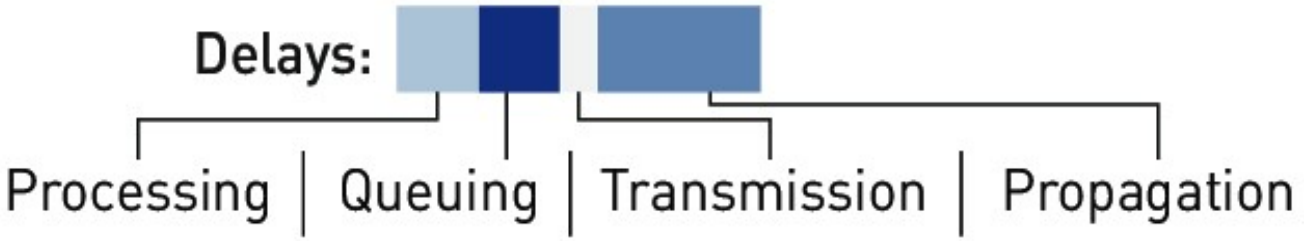
Métricas de desempeño

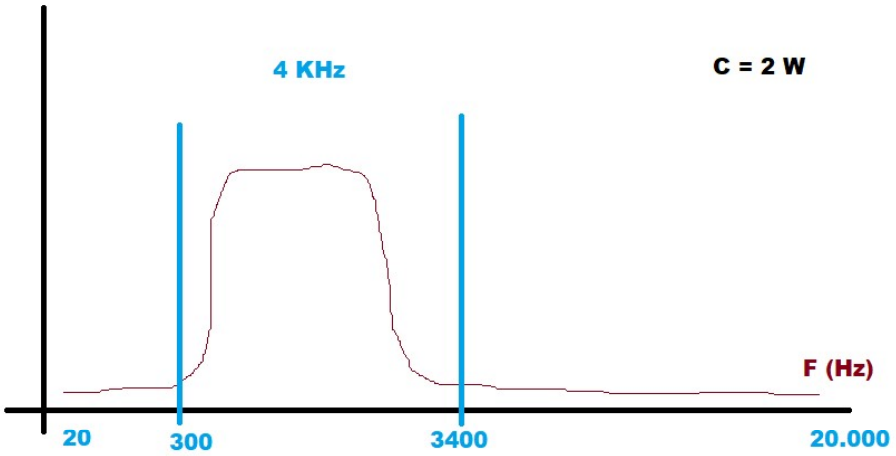
- Bandwidth
- Delay
- Jitter
- Packet loss











UTP --> categoría

- 5 = 100 MHz
- 6 = 250 MHz
- 6a = 500 MHz

- 10 Mbps
- 100 Mbps
- DSL = 5 Mps
- FTTH = 50 Mbps
- FO = 10 Gbps
- Mux = WDM = 3.2 Tbps

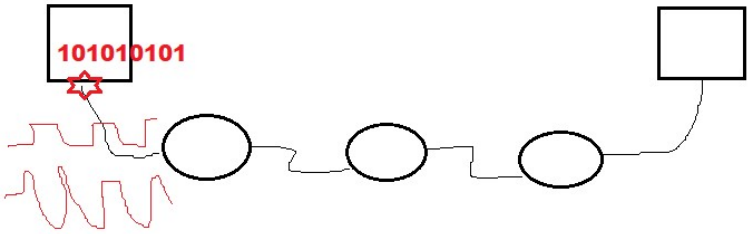
DELAY

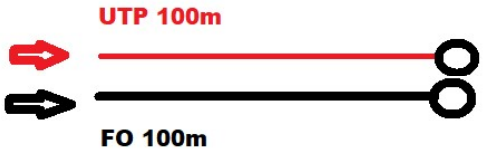
Esquemas de medición:

1. RTT
2. OWD

Componentes:

1. Transmisión
2. Propagación
3. Procesamiento
4. Encolamiento

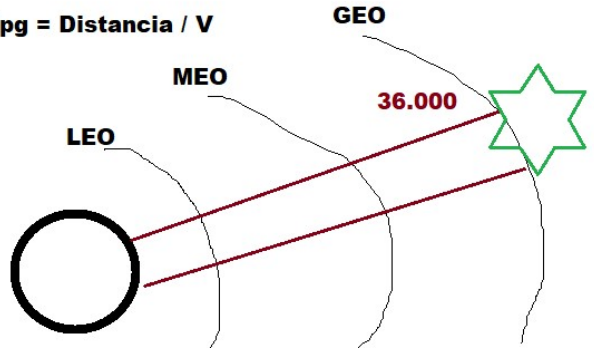




Rpg1 = 72000 / 300000 = 240 ms

Rpg2 = 600 / 200000 = 3 ms

Rpg = Distancia / V



ROOT SERVERS

DNS

Ecuador --> Raiz F

Rpg3 = 20000 / 200000 = 100 ms

+RAICES

Rpg4 = 1200 / 200000 = 6 ms

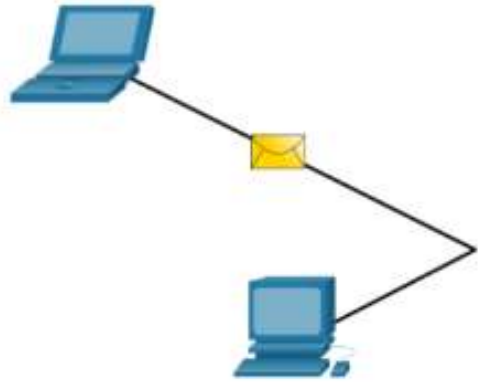
Protocols

- **Rules that Govern Communications**
- **Network Protocols**
  - The role of protocols
  - How the message is formatted or structured
  - The process by which networking devices share information about pathways with other networks
  - How and when error and system messages are passed between devices
  - The setup and termination of data transfer sessions
- Protocol Interaction
  - Example: web server and client

The Rules

Communications Protocols

- All communications are governed by protocols.
- Protocols are the rules that communications will follow.
- These rules will vary depending on the protocol.



Network Protocol Overview

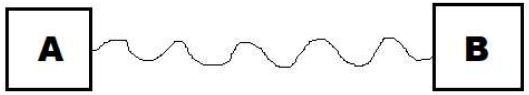
Network protocols define a common set of rules.

- Can be implemented on devices in:
  - Software
  - Hardware
  - Both
- Protocols have their own:
  - Function
  - Format
  - Rules

Protocol Type	Description
Network Communications	enable two or more devices to communicate over one or more networks
Network Security	secure data to provide authentication, data integrity, and data encryption
Routing	enable routers to exchange route information, compare path information, and select best path
Service Discovery	used for the automatic detection of devices or services

Example

Error checking



Hola chicos

Checksum

-100

4682 4

6

8

2

20

Hola chicos

Hola chicas xxx

+100

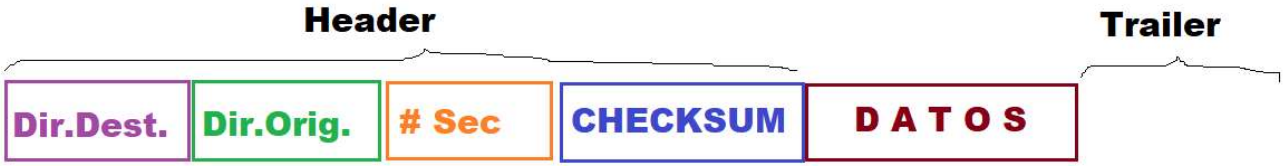
4582 4

5

8

2

19



TCP vs UDP

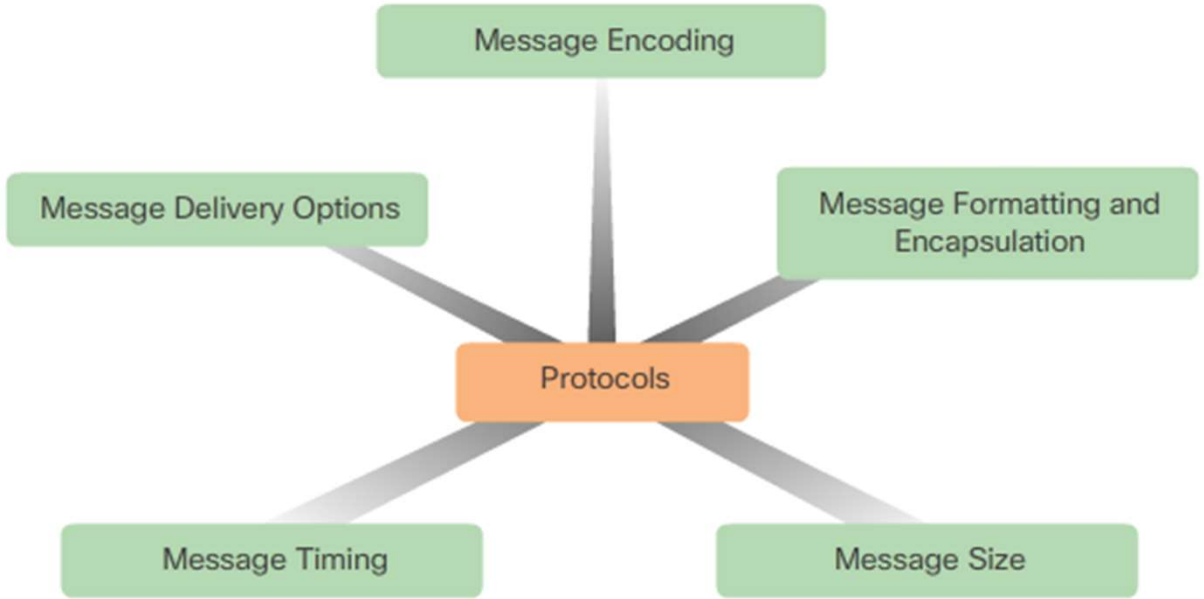
FTP TFTP

HTTP GQUIC

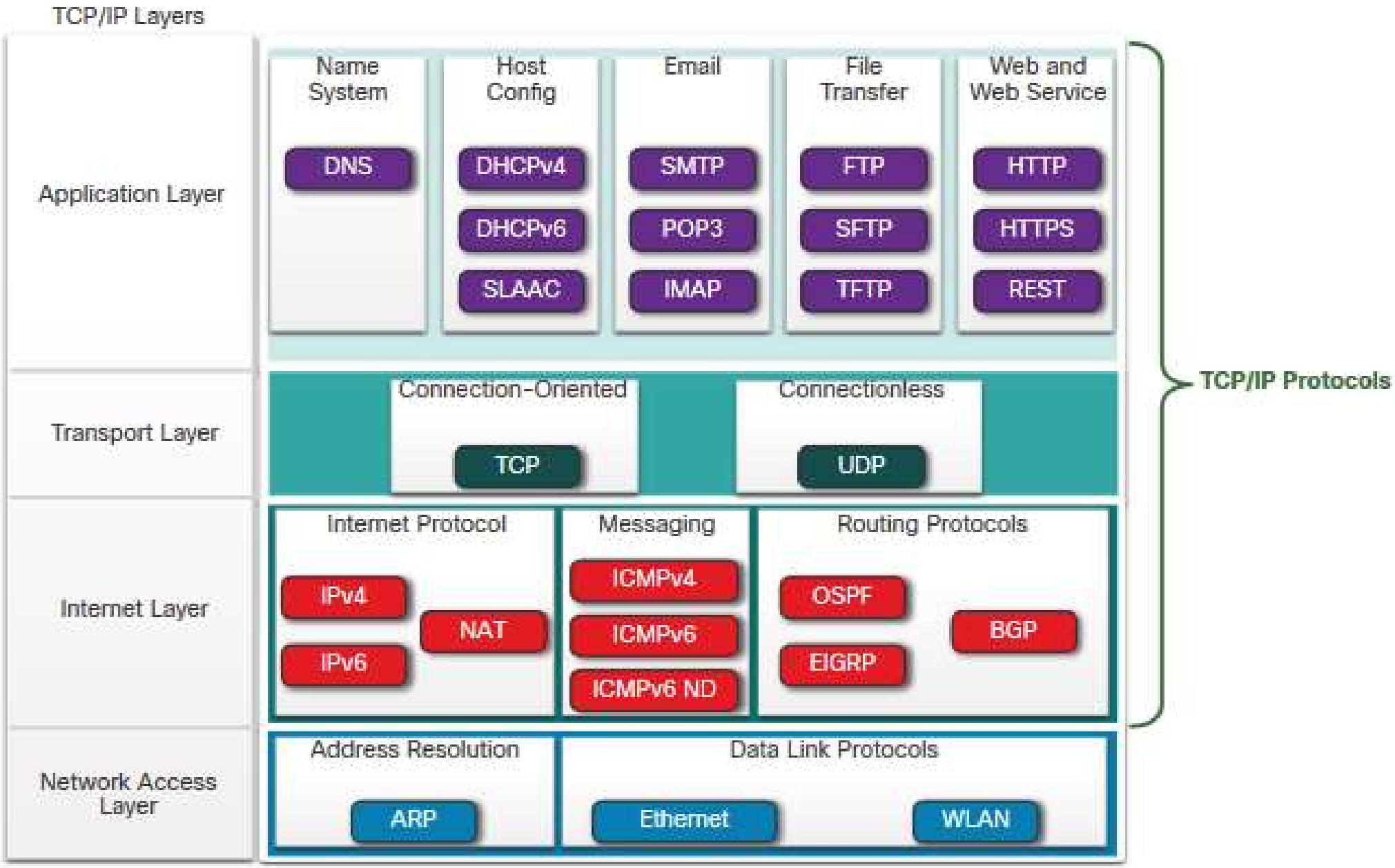
Rules of Communication

The Rules

- Rule Establishment
  - Identified sender and receiver
  - Common language and grammar
  - Speed and timing of delivery
  - Confirmation or acknowledgment requirements
- Message Encoding
  - Process of converting information into another acceptable form
- Message Formatting and Encapsulation
- Message Size
- Message Timing
  - Access method
  - Flow control
  - Response timeout
- Message Delivery Options
  - Unicast
  - Multicast
  - Broadcast

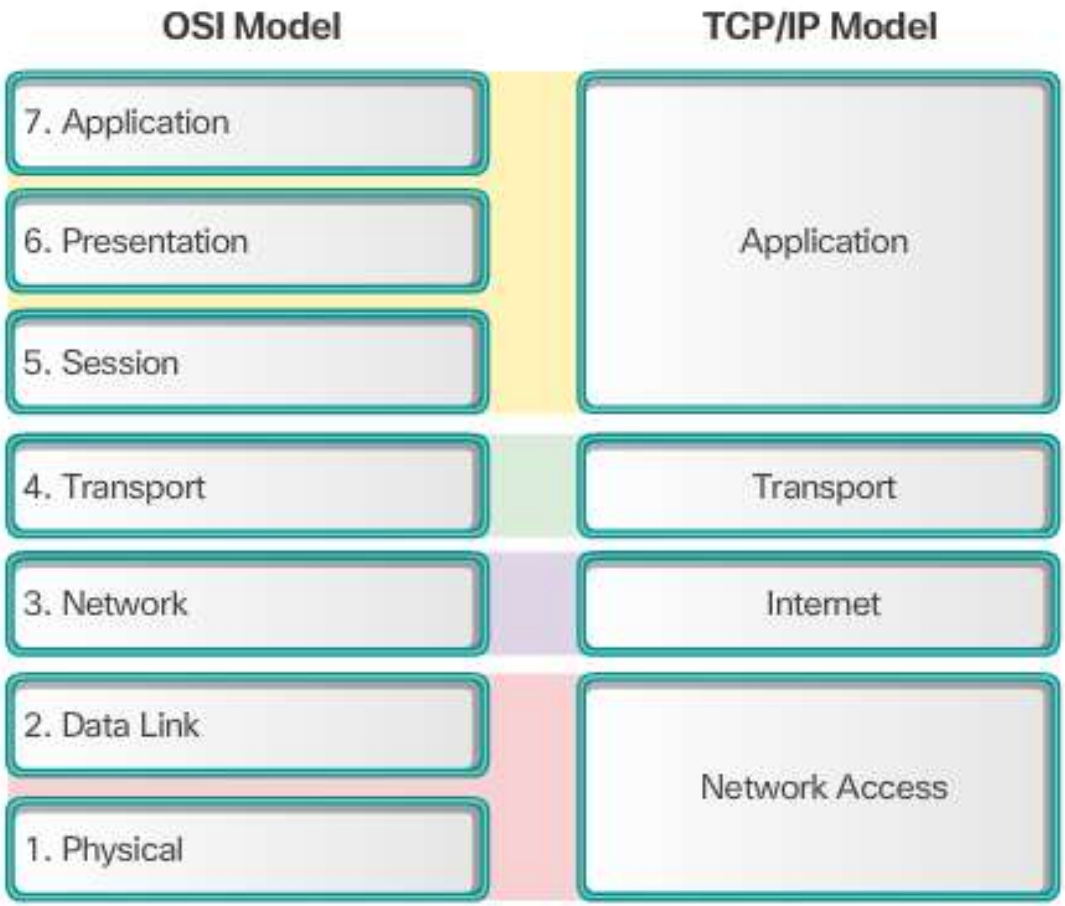


Protocol Suites



Reference Models

- The Benefits of Using a Layered Model
  - Name some benefits
- The OSI Reference Model
  - Provides list of functions
  - Describes interactions between layers
- OSI Model and TCP/IP Model Comparison
  - Similar: transport and network layers
  - Contrast: relationship between layers

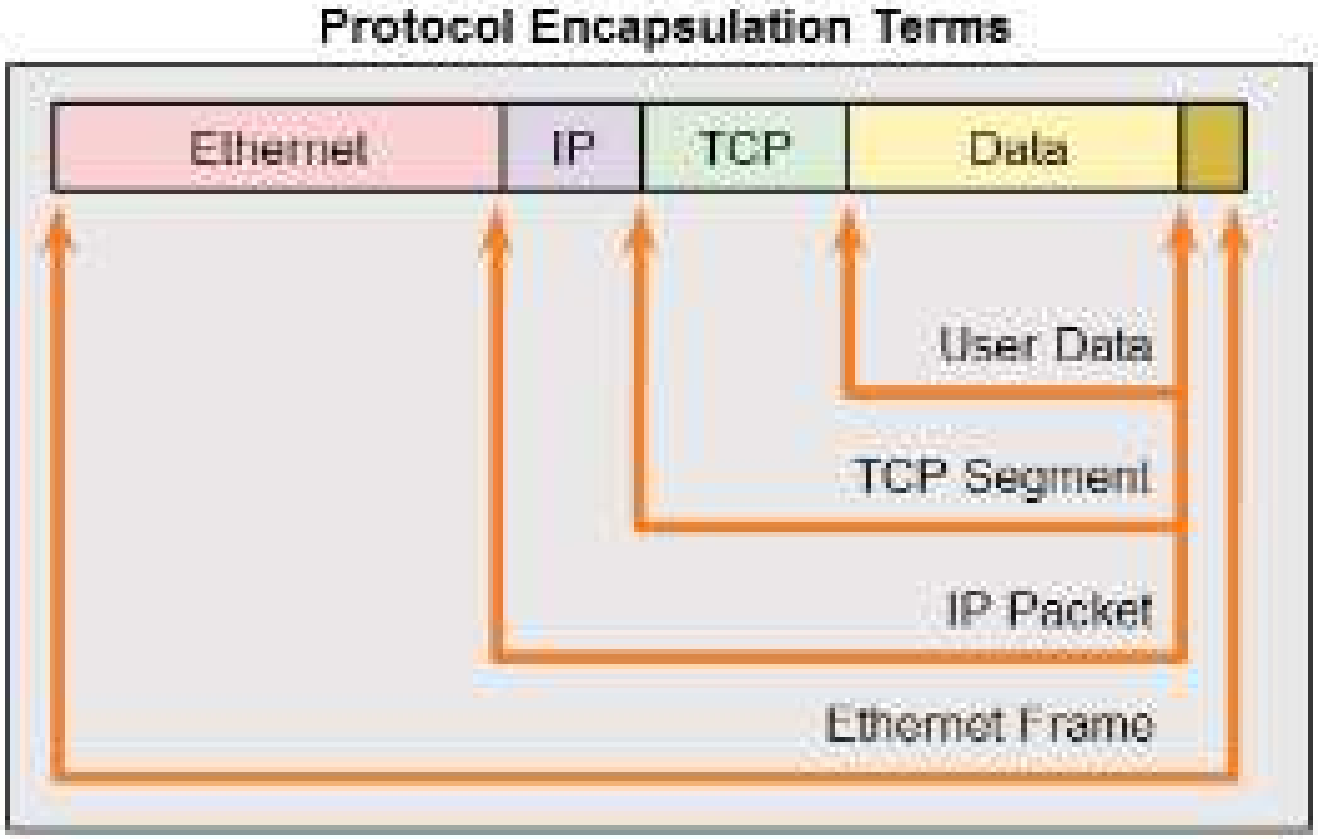


The OSI Reference Model

OSI Model Layer	Description
7 - Application	Contains protocols used for process-to-process communications.
6 - Presentation	Provides for common representation of the data transferred between application layer services.
5 - Session	Provides services to the presentation layer and to manage data exchange.
4 - Transport	Defines services to segment, transfer, and reassemble the data for individual communications.
3 - Network	Provides services to exchange the individual pieces of data over the network.
2 - Data Link	Describes methods for exchanging data frames over a common media.
1 - Physical	Describes the means to activate, maintain, and de-activate physical connections.

Data Transfer in the Network

Data Encapsulation



Protocol Wrapper Dependencies and Network Layers