DevOps education program

Basics of networks

Lecture 3.1
Module 3. Networking Fundamentals

Serhii Zakharchenko

Module overview

Lection's topics

Lection 1

- Introduction
- Standards and models
- Transport layer details

Lection 2

- LAN addressing
- LAN technologies
- LAN devices

Lection 3

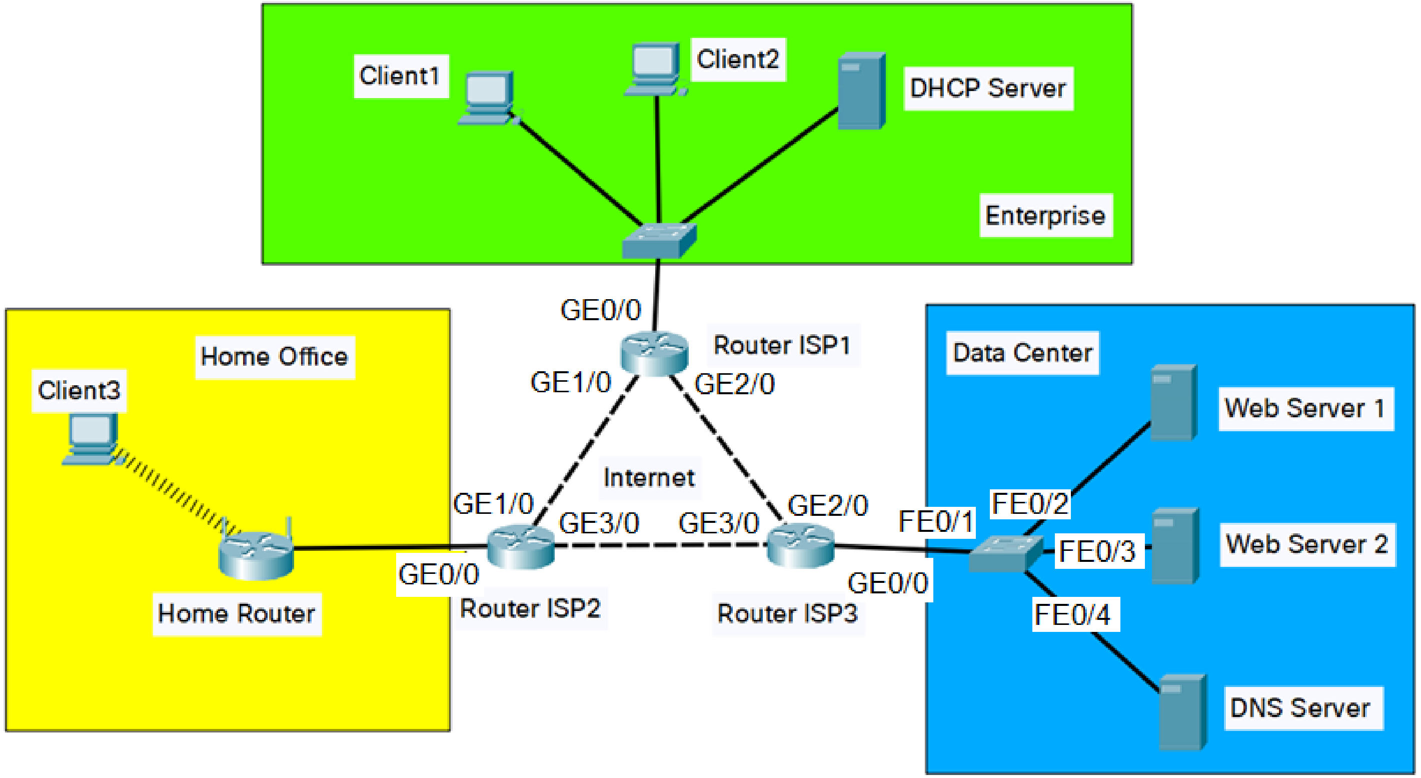
- Internet Protocol
- IPv4 address subnetting
- IP routing

Lection 4

- DHCP
- DNS
- NAT

Practical Tasks

- **Task 3.1** – Creating three separate networks: Home Office, Enterprise, Data Center.
- **Task 3.2** – Connecting separate networks thrue Internet
- **Task 3.3** – Routing configuration
- **Task 3.4** – DHCP, DNS and NAT configuration



Agenda

- Introduction
- Standards and models
- Transport layer details
- Q&A

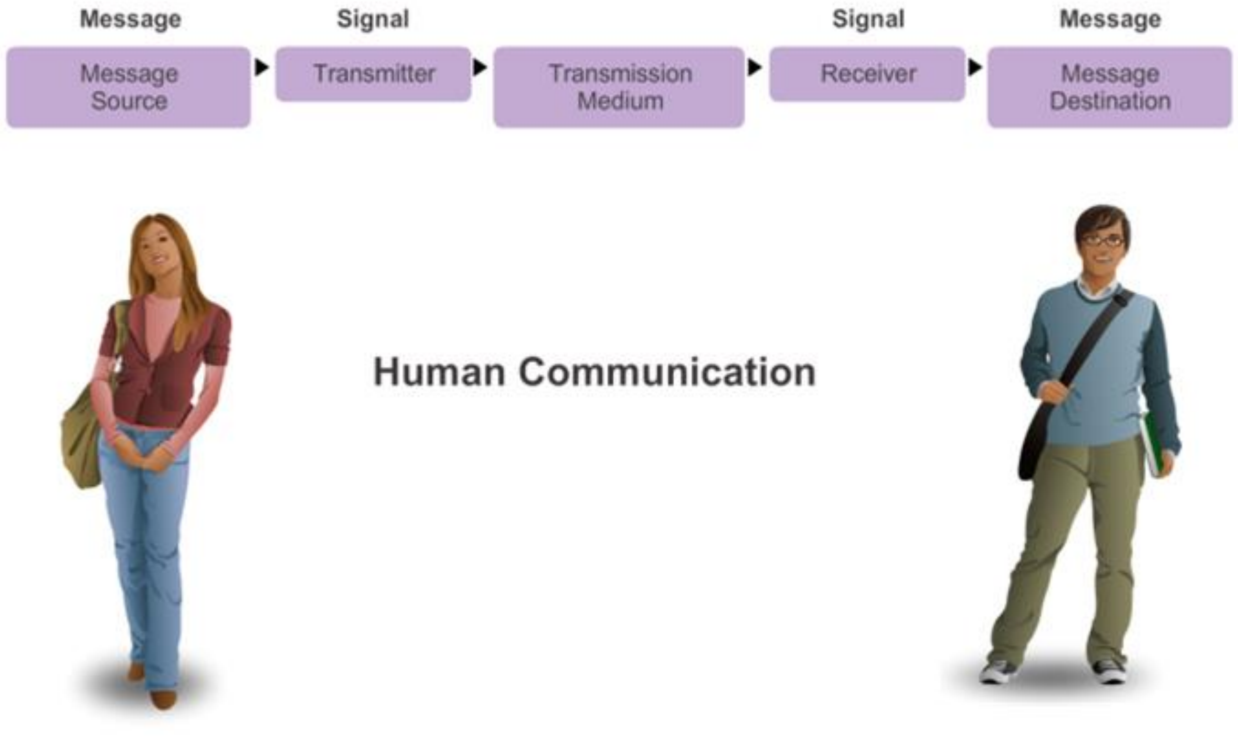
Introduction

Why Networks?

Communication

The elements of communication

- Communication begins with a **message**, or information, that must be sent from one individual or device to another. There are 3 common elements of communication:
  - **message source**
  - **the channel**
  - **message destination**
- Data or information networks capable of carrying many **different types** of communications



Networks of Many Sizes

Small Home Networks

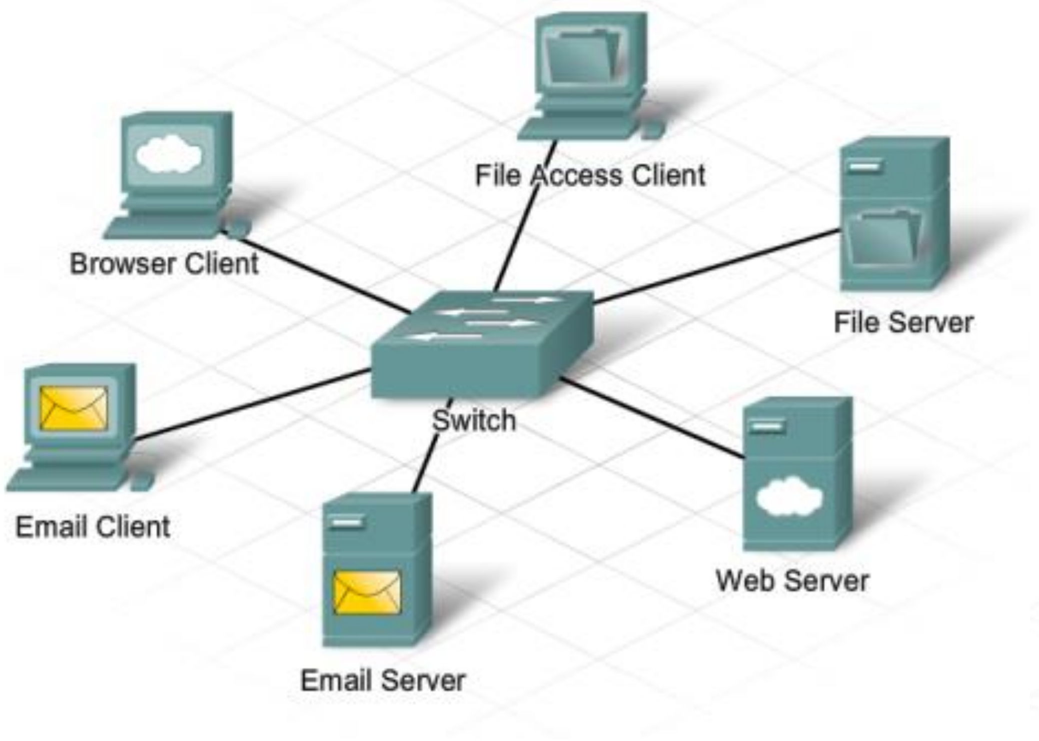
Small Office/Home Office Networks

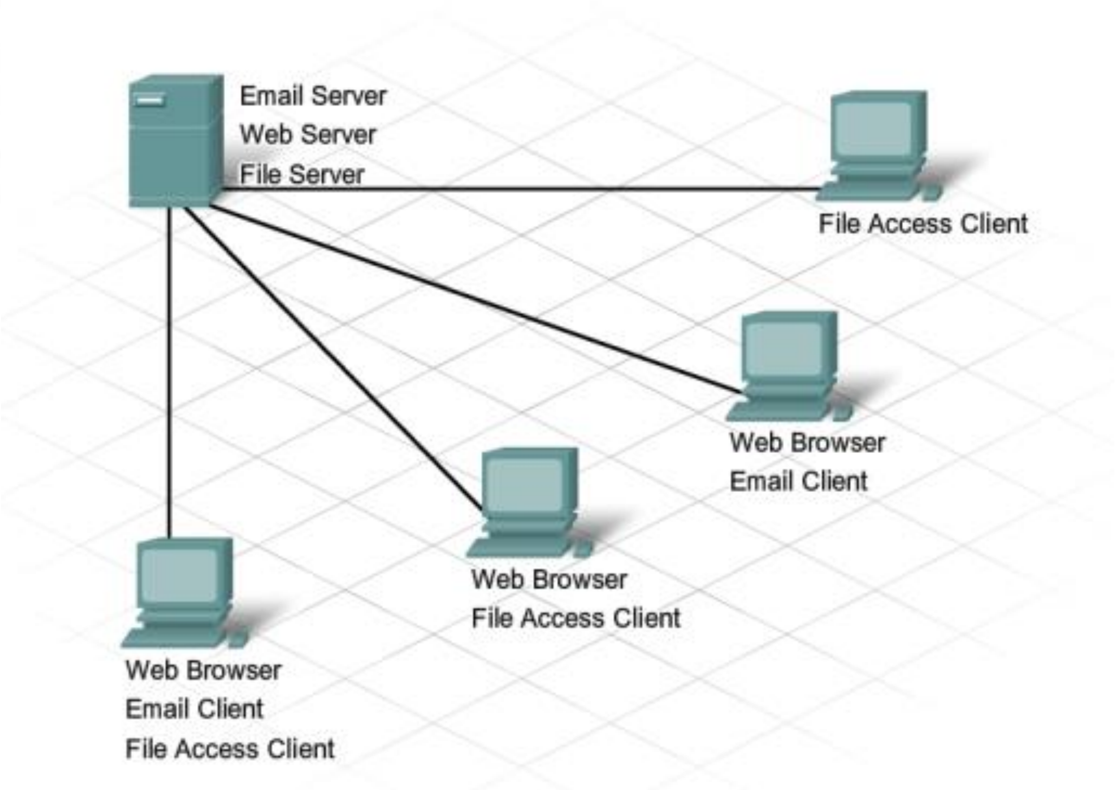
Medium to Large Networks

World Wide Networks

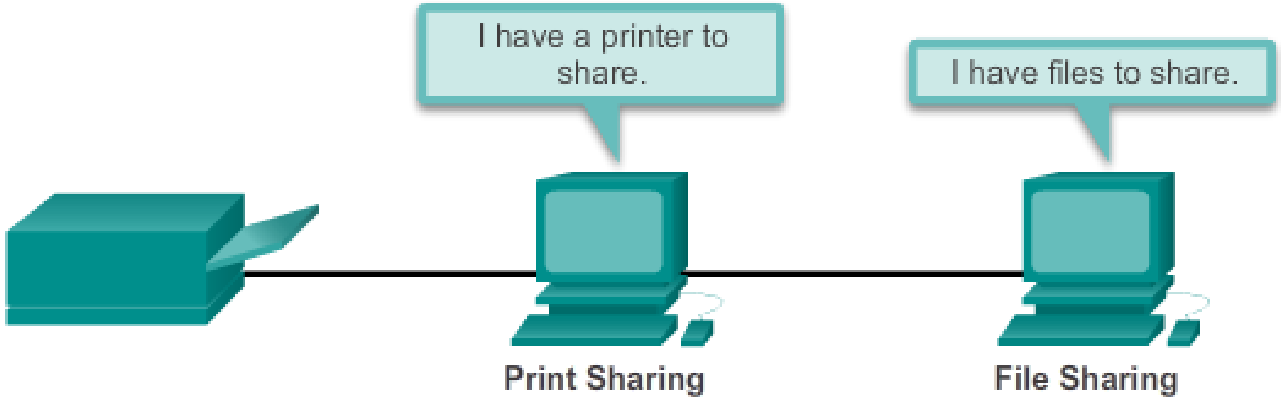
- **Small Home Networks** - simple networks installed in homes enable sharing of resources, such as printers, documents, pictures and music between a few local computers
- **Home office networks and small office networks** are often set up by individuals that work from a home or remote office and need to connect to a corporate network or other centralized resources.
- **Large/medium networks** in businesses and large organizations can be used to allow employees to provide consolidation, storage, and access to information on network servers.
- The **Internet** is the largest network in existence. In fact, the term Internet means a ‘network of networks’

Clients and Servers





Peer-to-Peer Networks



The advantages of peer-to-peer networking:

- Easy to set up
- Less complexity
- Lower cost since network devices and dedicated servers may not be required
- Can be used for simple tasks such as transferring files and sharing printers

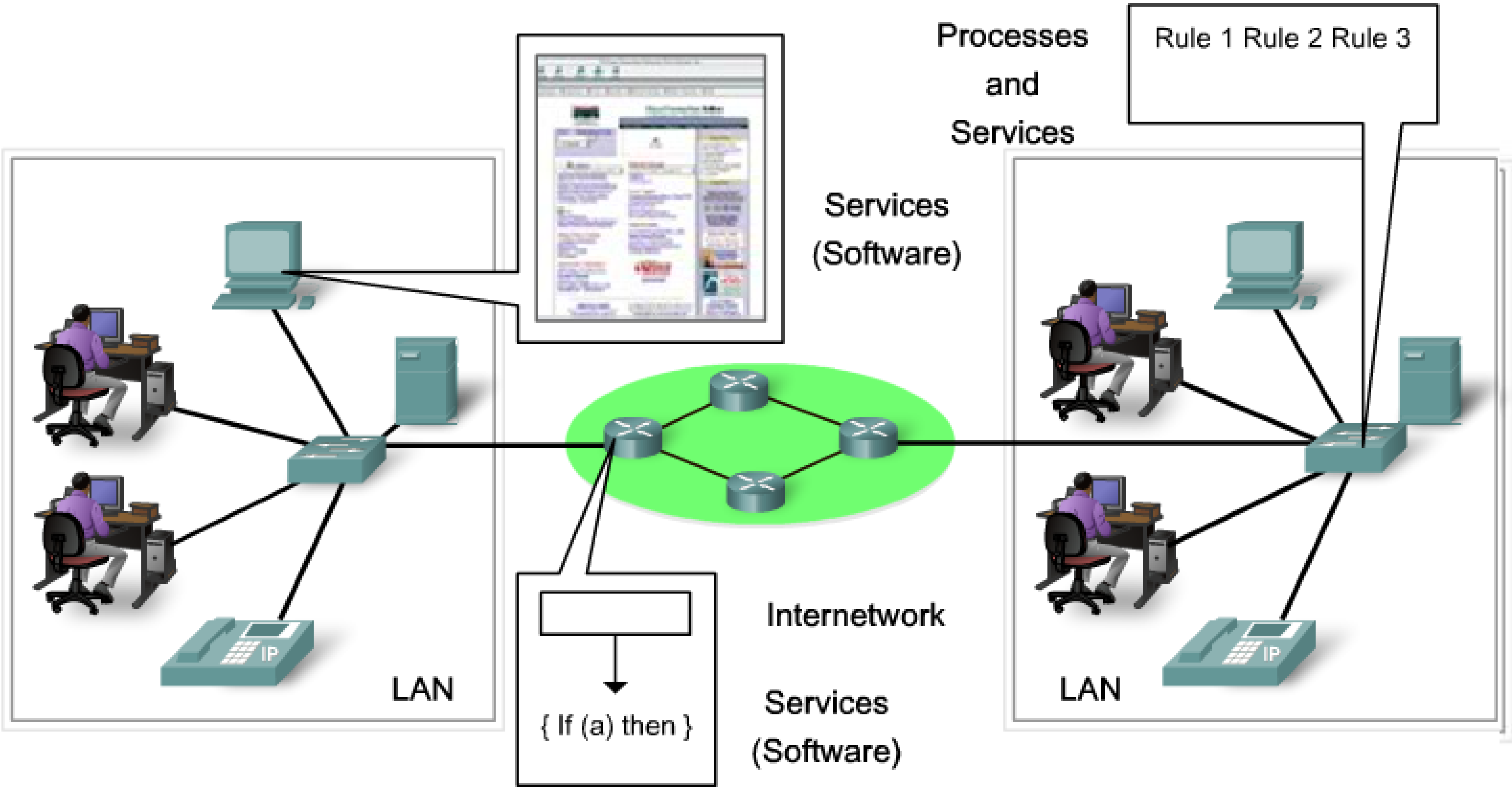
The disadvantages of peer-to-peer networking:

- No centralized administration
- Not as secure
- Not scalable
- All devices may act as both clients and servers which can slow their performance

Components of a Network

There are three categories of network components:

- **Devices**
- **Media**
- **Services.**



End Devices

Some examples of end devices are:

- Computers (workstations, laptops, servers)
- Network printers
- VoIP phones
- TelePresence endpoint
- Security cameras
- Mobile handheld devices (such as smartphones, tablets, PDAs, and wireless debit / credit card readers and barcode scanners)

Network Infrastructure Devices

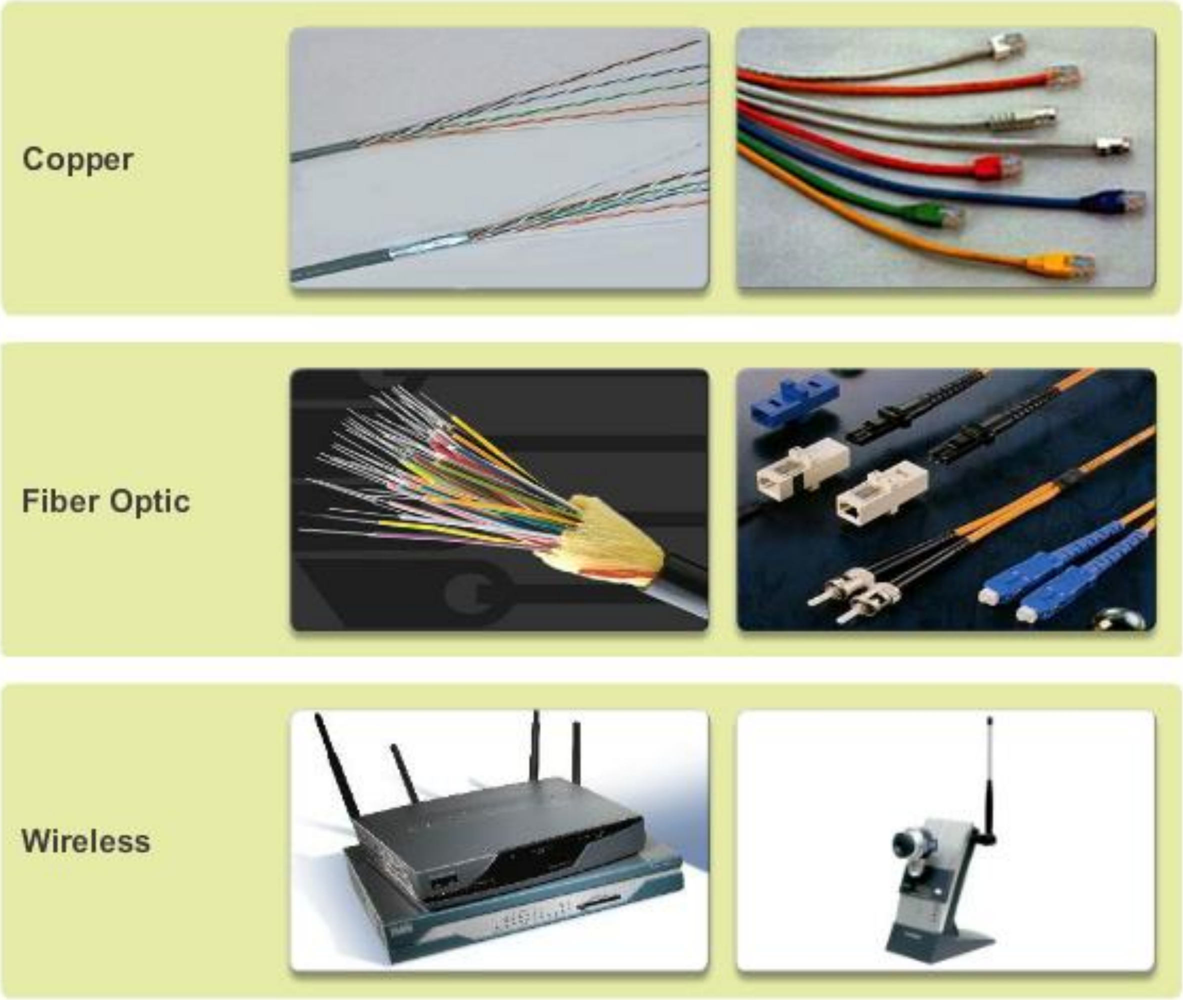
Examples of intermediary network devices are:

- Network Access Devices (switches, and wireless access points)
- Internetworking Devices (routers)
- Security Devices (firewalls)

Intermediary network devices functions:

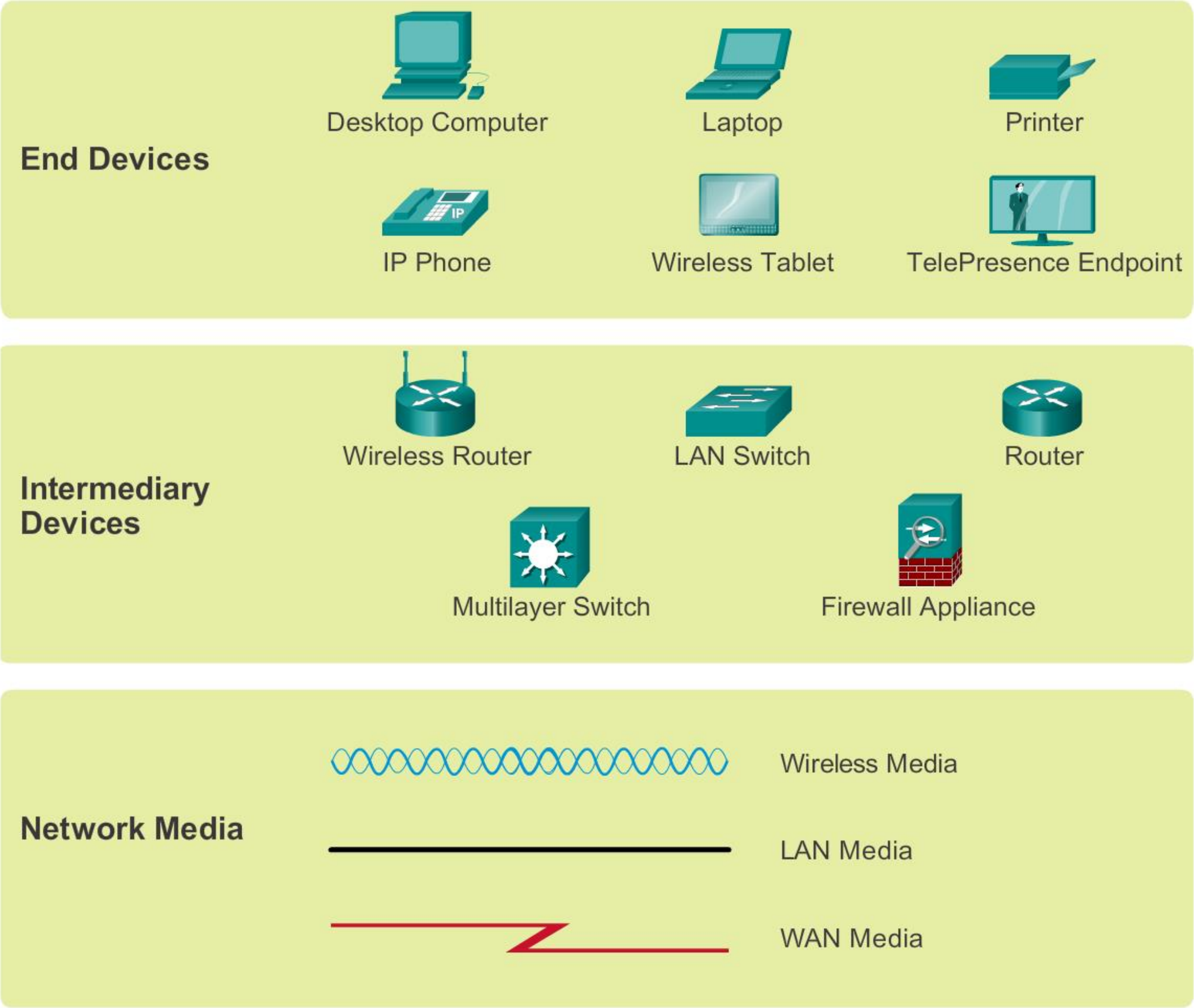
- Regenerate and retransmit data signals
- Maintain information about what pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to Quality of Service (QoS) priorities
- Permit or deny the flow of data, based on security settings

Network Media



CONFIDENTIAL | © 2021 EPAM Systems, Inc.

Network Representations



Types of Networks

Classification Criteria

- The size of the area covered
- The number of users connected
- The number and types of services available

The two most common types of network infrastructures are:

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

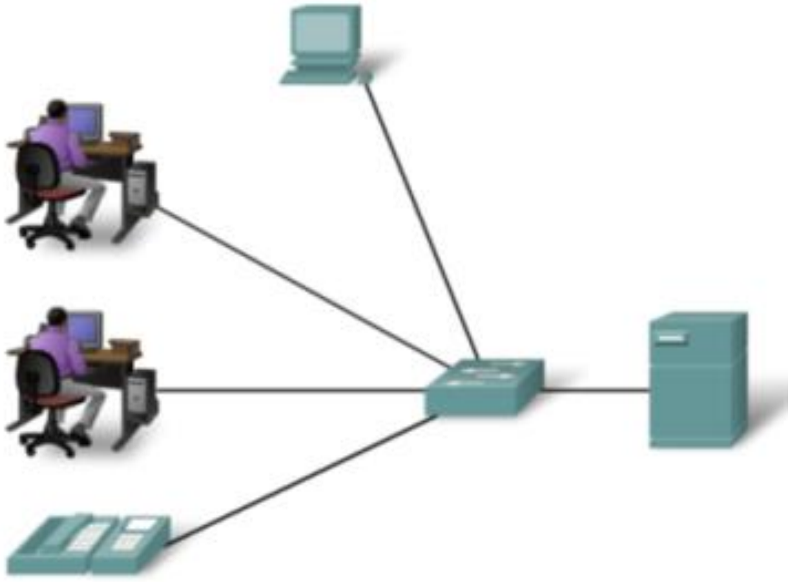
Other types of networks include:

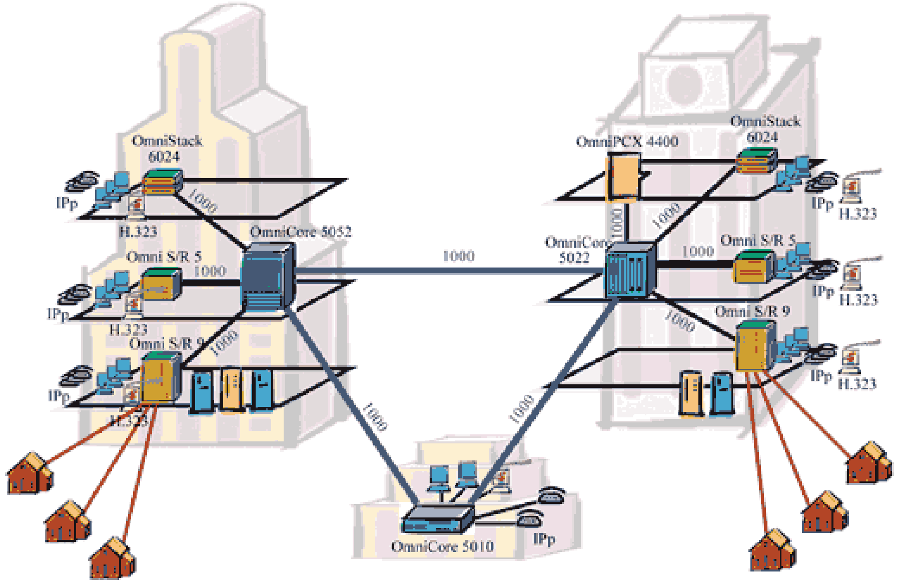
- **Metropolitan Area Network** (MAN)
- **Wireless** LAN (WLAN)
- **Storage Area Network** (SAN)

Local Area Networks (LAN)

A network infrastructure that provides access to users and end devices in a **small geographical area**.

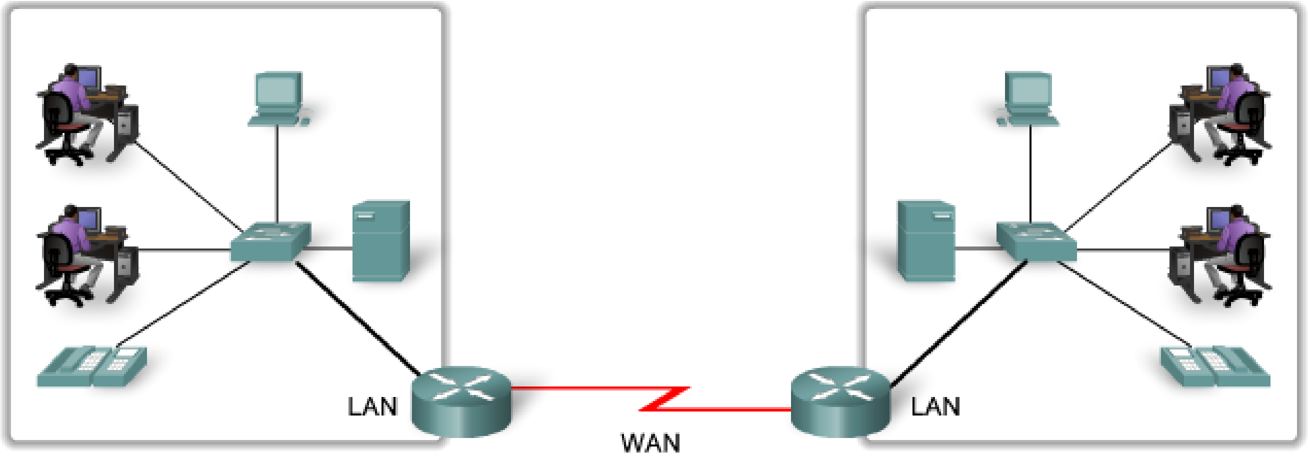
- LANs interconnect end devices in a **limited area** such as a home, school, office building, or campus.
- A LAN is usually **administered by a single organization** or individual. The administrative control that governs the security and access control policies are enforced on the network level.
- LANs provide **high speed bandwidth** to internal end devices and intermediary devices.





Wide Area Networks (WAN)

A network infrastructure that provides access to other networks over a **wide geographical area**. Individual organizations usually **lease** connections through a telecommunications service provider network.



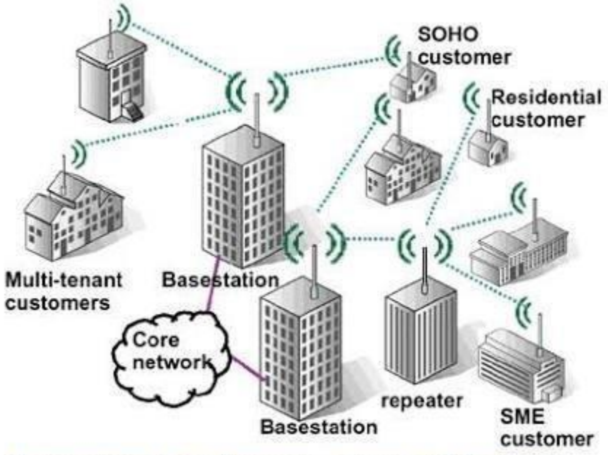
- WANs interconnect LANs over **wide geographical areas** such as between cities, states, provinces, countries, or continents.
- WANs are usually administered by **multiple service providers**.
- WANs typically provide **slower speed** links between LANs.

Other types of networks

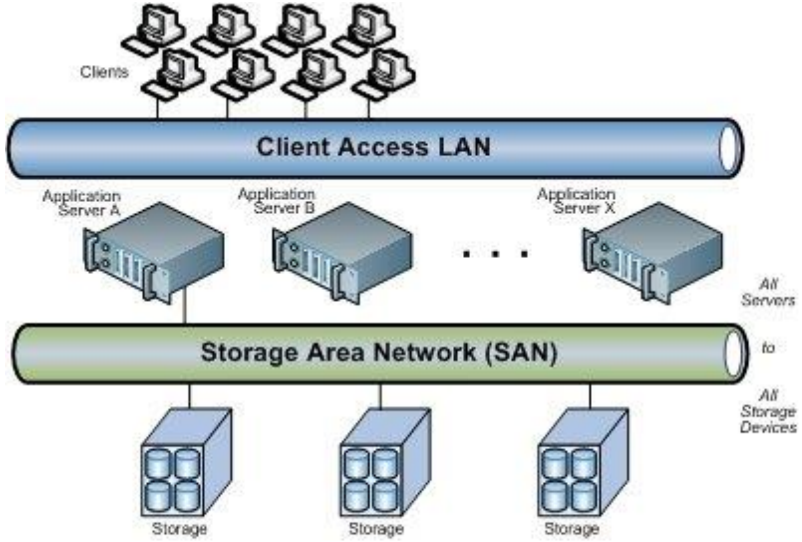
- **Metropolitan Area Network (MAN)** - A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city). MANs are typically operated by a single entity such as a large organization.

- **Wireless LAN (WLAN)** - Similar to a LAN but wirelessly interconnects users and end points in a small geographical area.

- **Storage Area Network (SAN)** - A network infrastructure designed to support file servers and provide data storage, retrieval, and replication. It involves high-end servers, multiple disk arrays (called blocks), and Fiber Channel interconnection technology.



Metropolitan Area Network - www.certiology.com

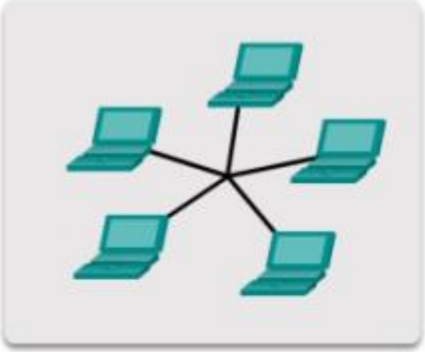


Physical and logical topology

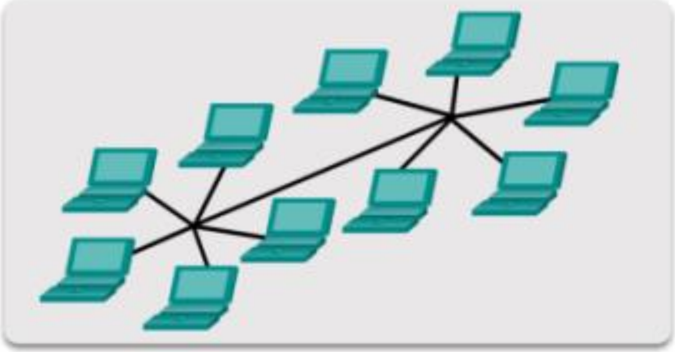
- **Physical topology**: Refers to the **physical connections** and identifies how end devices and infrastructure devices such as routers, switches, and wireless access points are interconnected. Physical topologies are usually **point-to-point** or **star**.
- **Logical topology**: Refers to the way a network **transfers frames** from one node to the next. This arrangement consists of virtual connections between the nodes of a network. These logical signal paths are defined by data link layer protocols. The logical topology of point-to-point links is relatively simple while shared media offers deterministic and a non-deterministic media access control methods.

Physical LAN and WAN Topologies

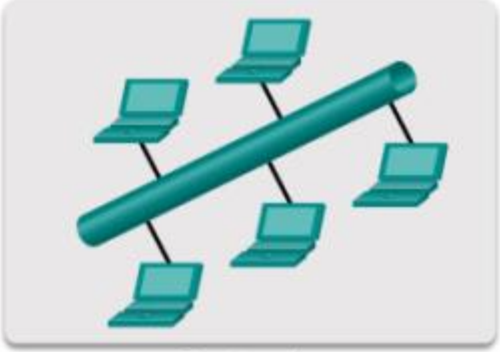
Physical LAN Topologies



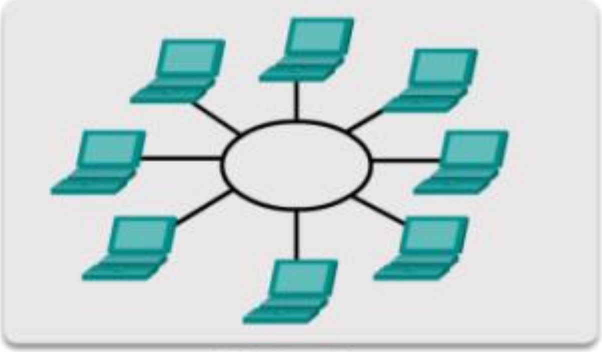
Star topology



Extended star topology

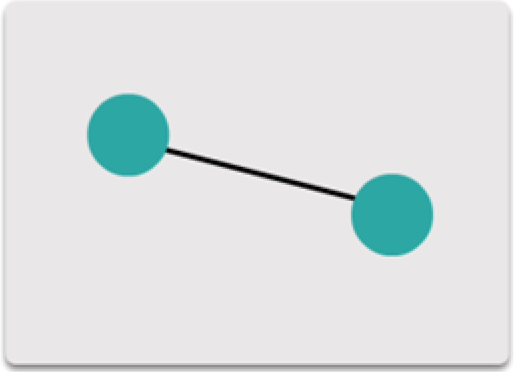


Bus topology

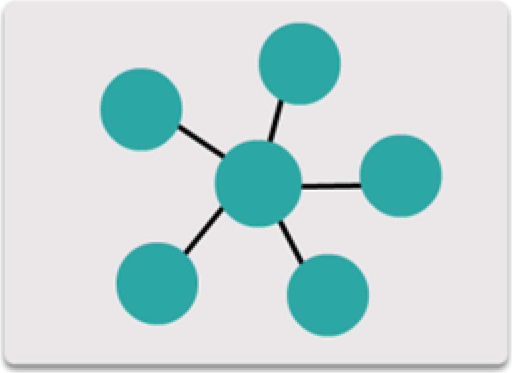


Ring topology

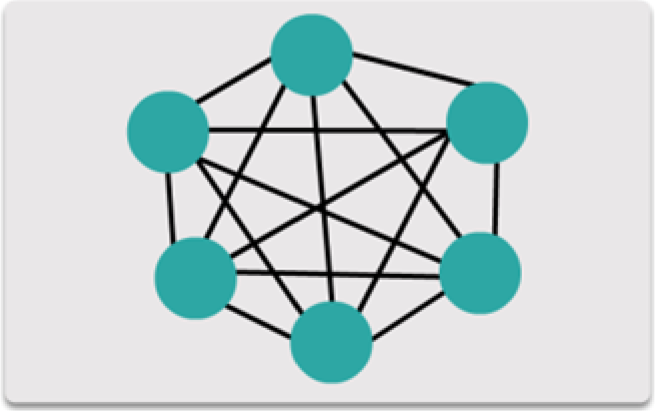
Physical WAN Topologies



Point-to-point topology



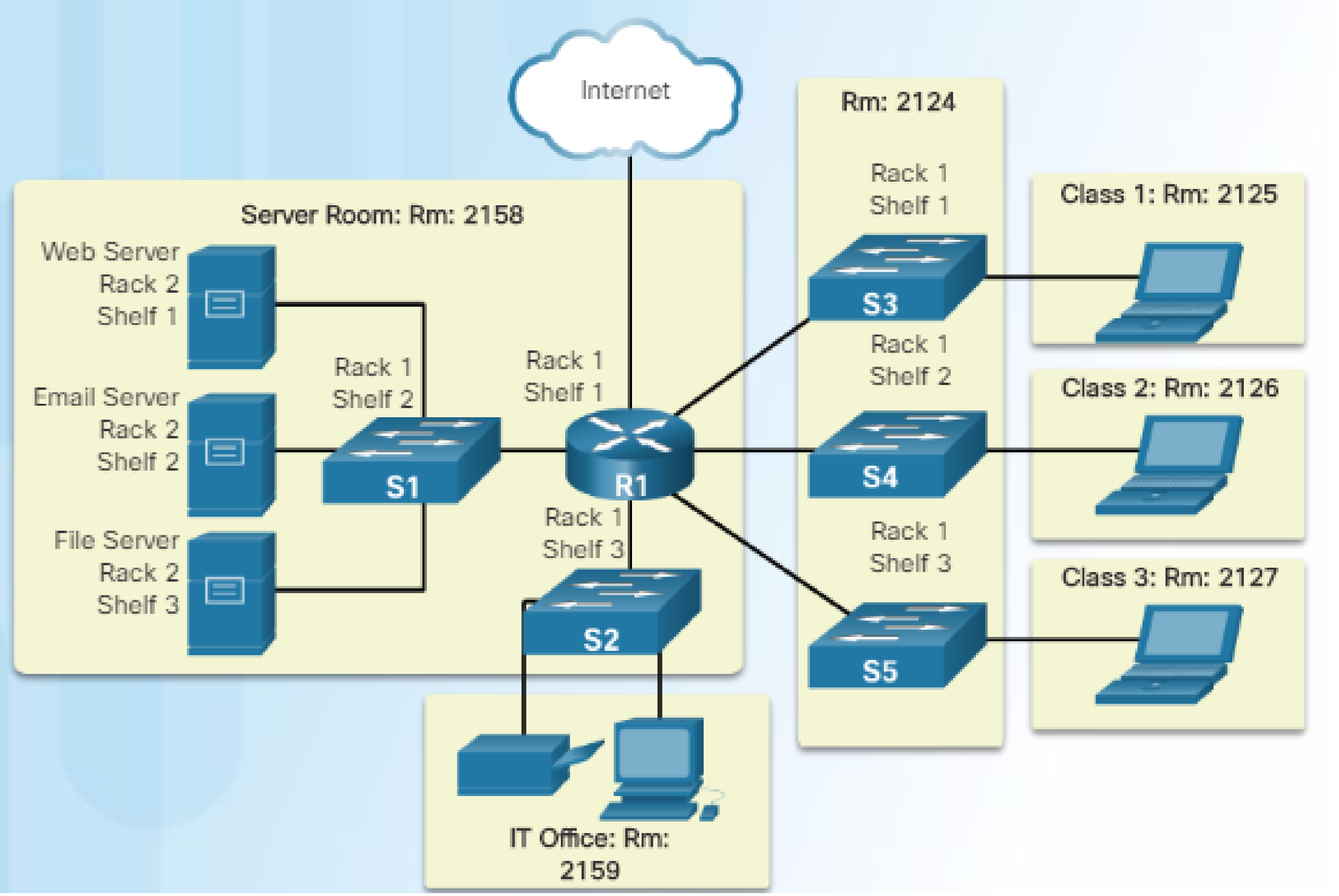
Hub and spoke topology



Full mesh topology

Physical topology diagrams

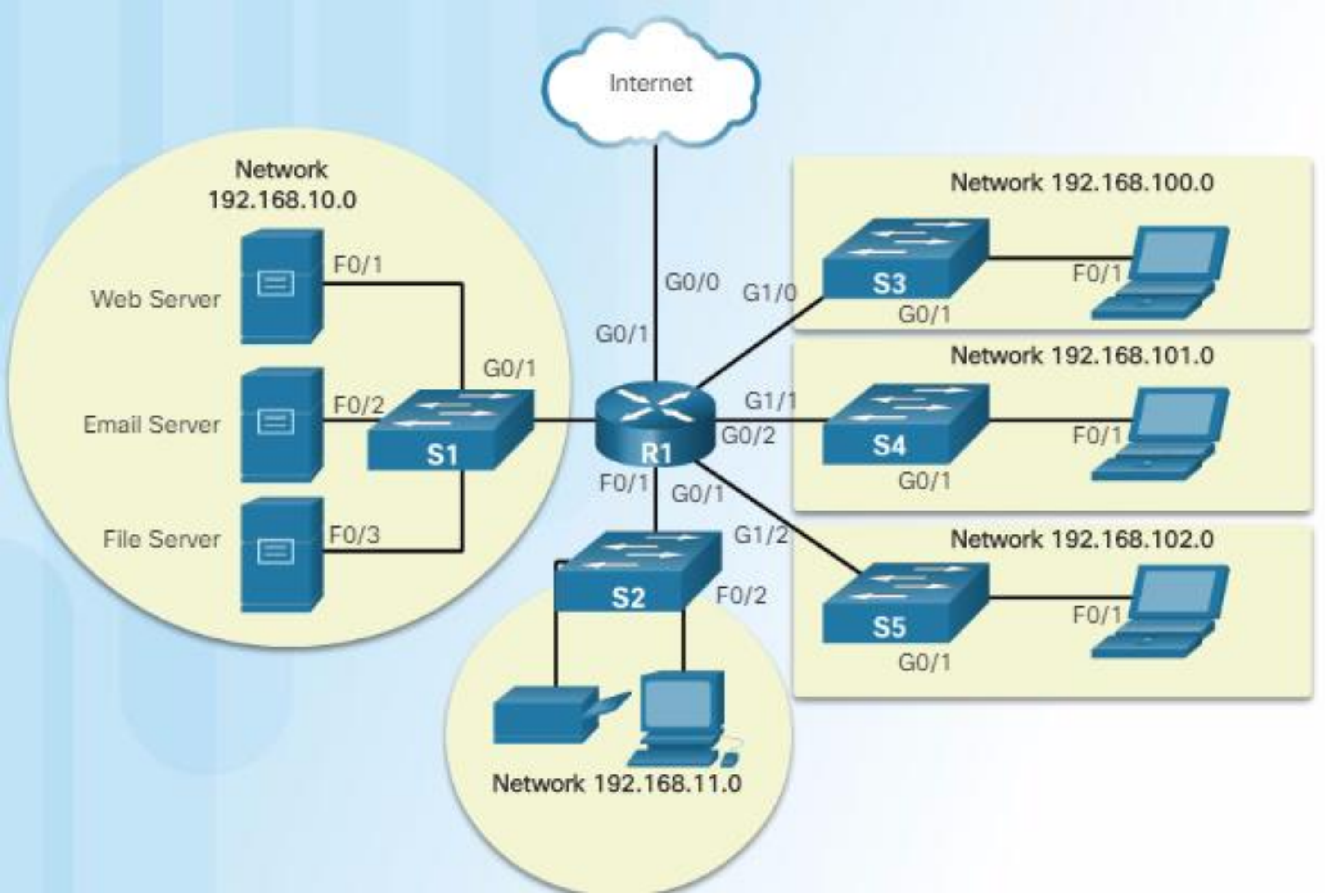
- identify the physical location of intermediary devices, configured ports, and cable installation.



© 2021 EPAM Systems, Inc.

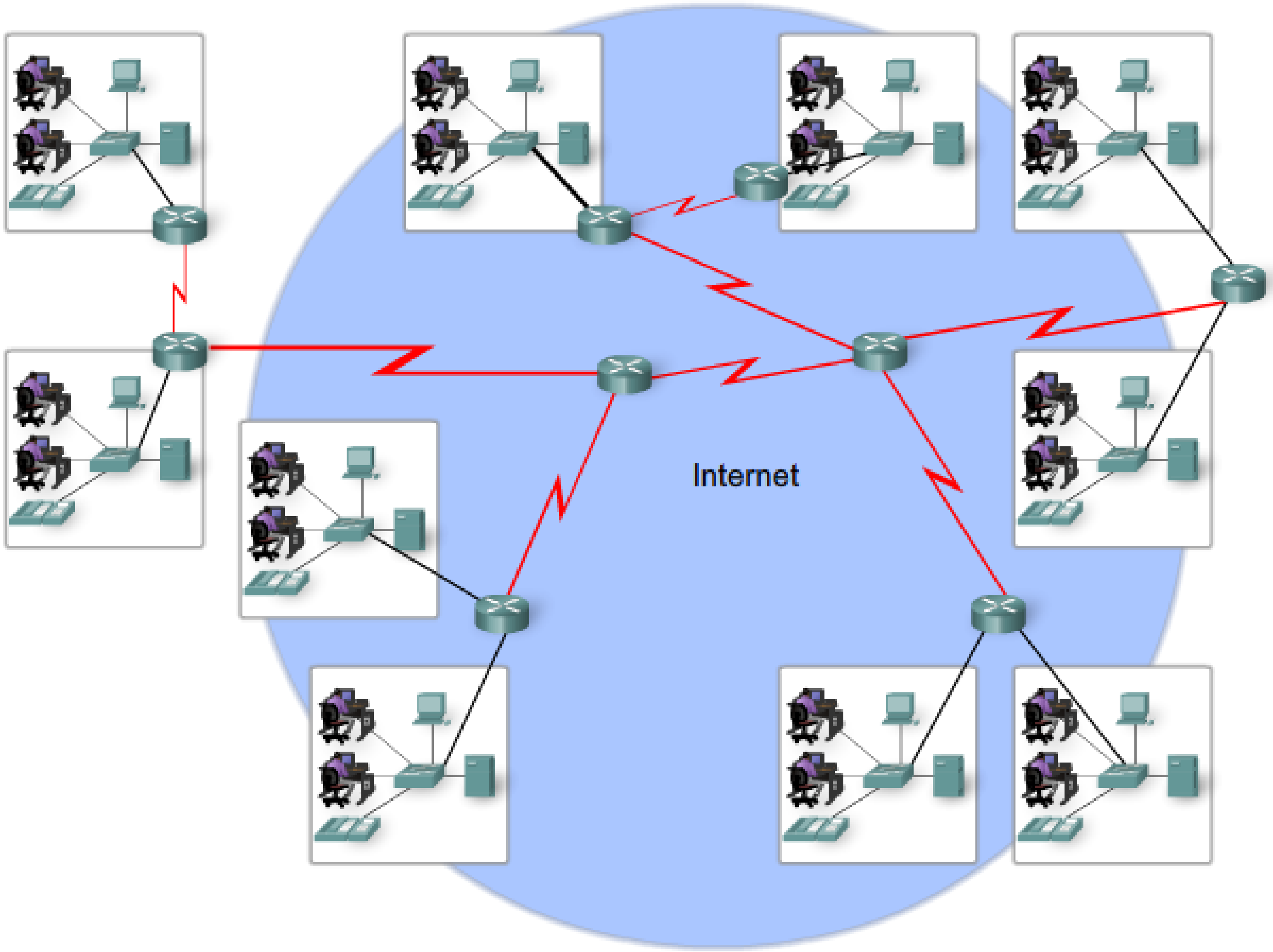
Logical topology diagrams

- Identify devices, ports, and IP addressing scheme.



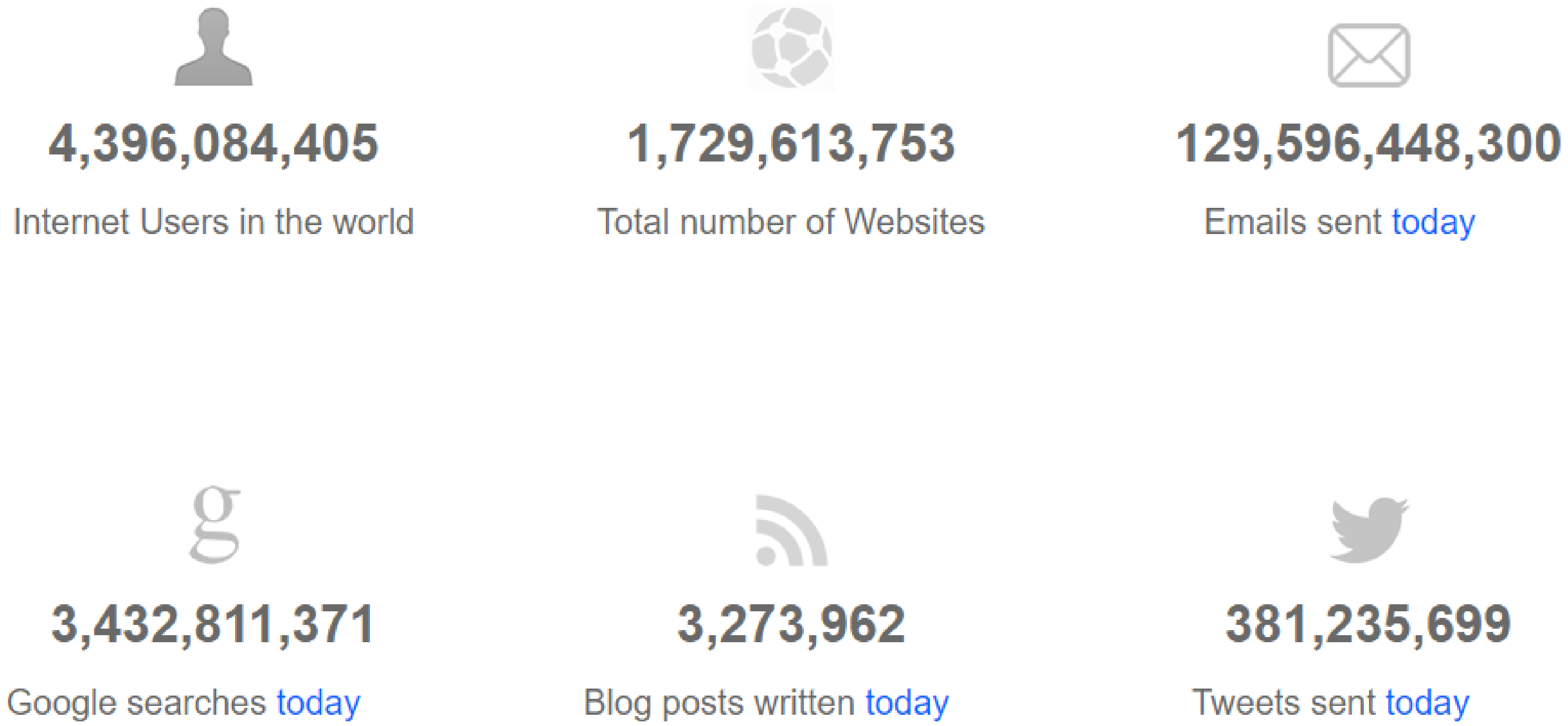
The Internet

LANs and WANs may be connected into internetworks.



Internet Live Stats

- https://www.internetlivestats.com/



4,396,084,405

Internet Users in the world

1,729,613,753

Total number of Websites

129,596,448,300

Emails sent today

3,432,811,371

Google searches today

3,273,962

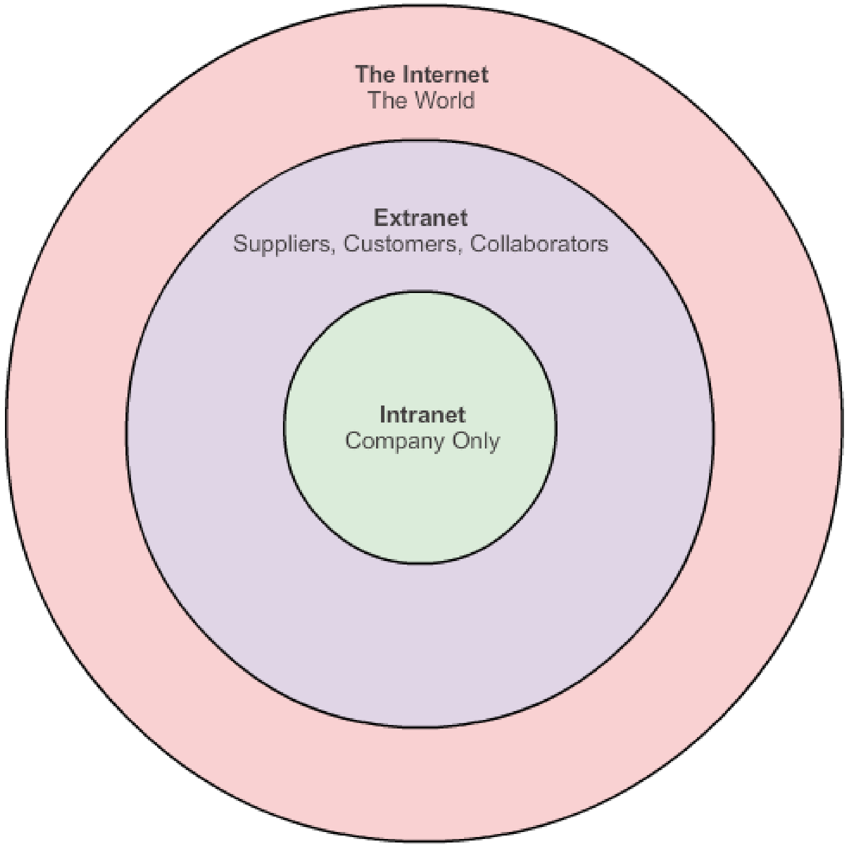
Blog posts written today

381,235,699

Tweets sent today

Intranet and Extranet

- **Intranet** is a term often used to refer to a **private** connection of LANs and WANs that belongs to an organization and is designed to be accessible only by the organization's members, employees, or others with **authorization**.
  - For example, schools may have intranets that include information on class schedules, online curriculum, and discussion forums.
- An organization may use an **extranet** to provide secure and safe access to individuals who work for a **different organizations but** require company data. Examples of extranets include:
  - A company providing access to outside suppliers/contractors.
  - A hospital providing a booking system to doctors so they can make appointments for their patients.
  - A local office of education providing budget and personnel information to the schools in its district.

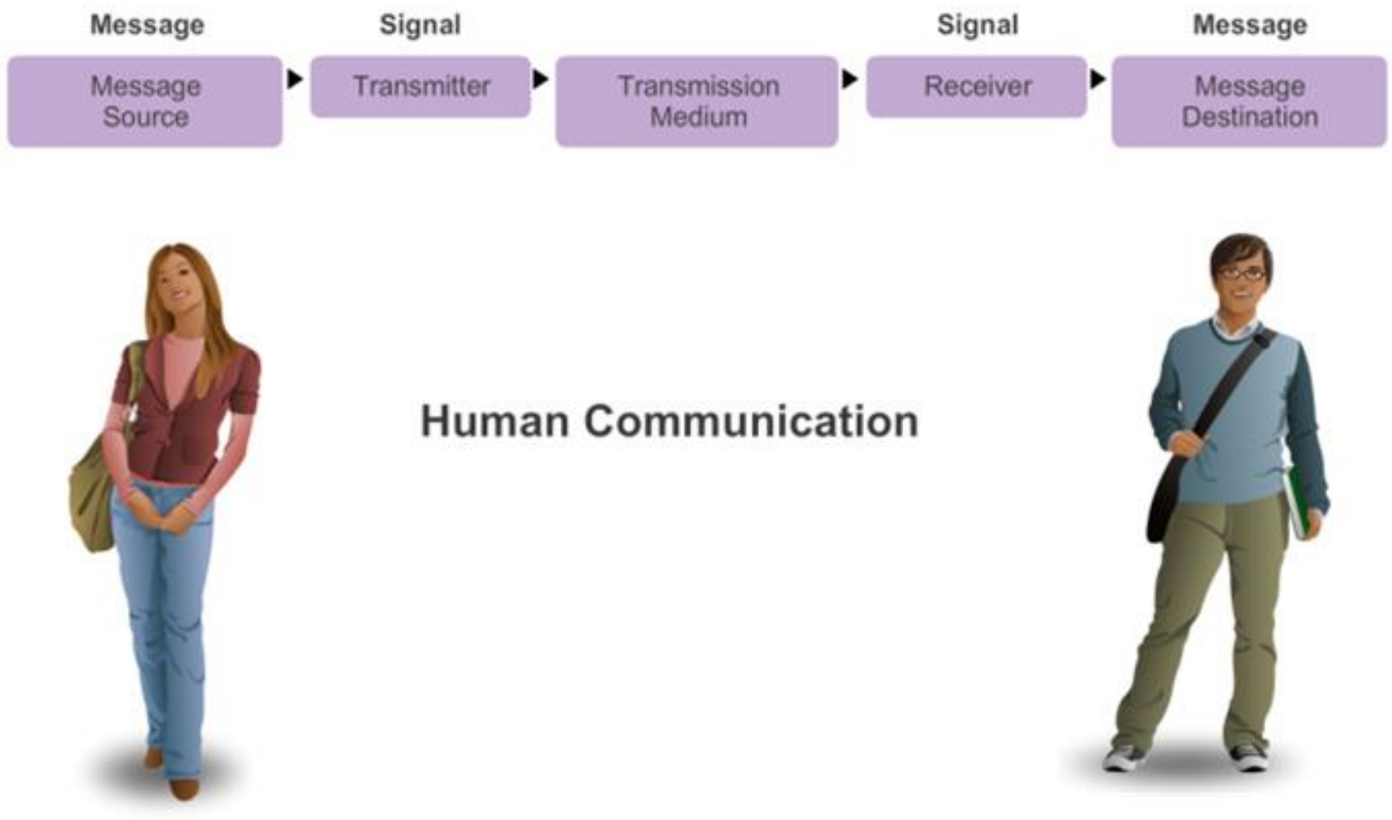


Standards and models

The Communication Rules

Establishing the Rules

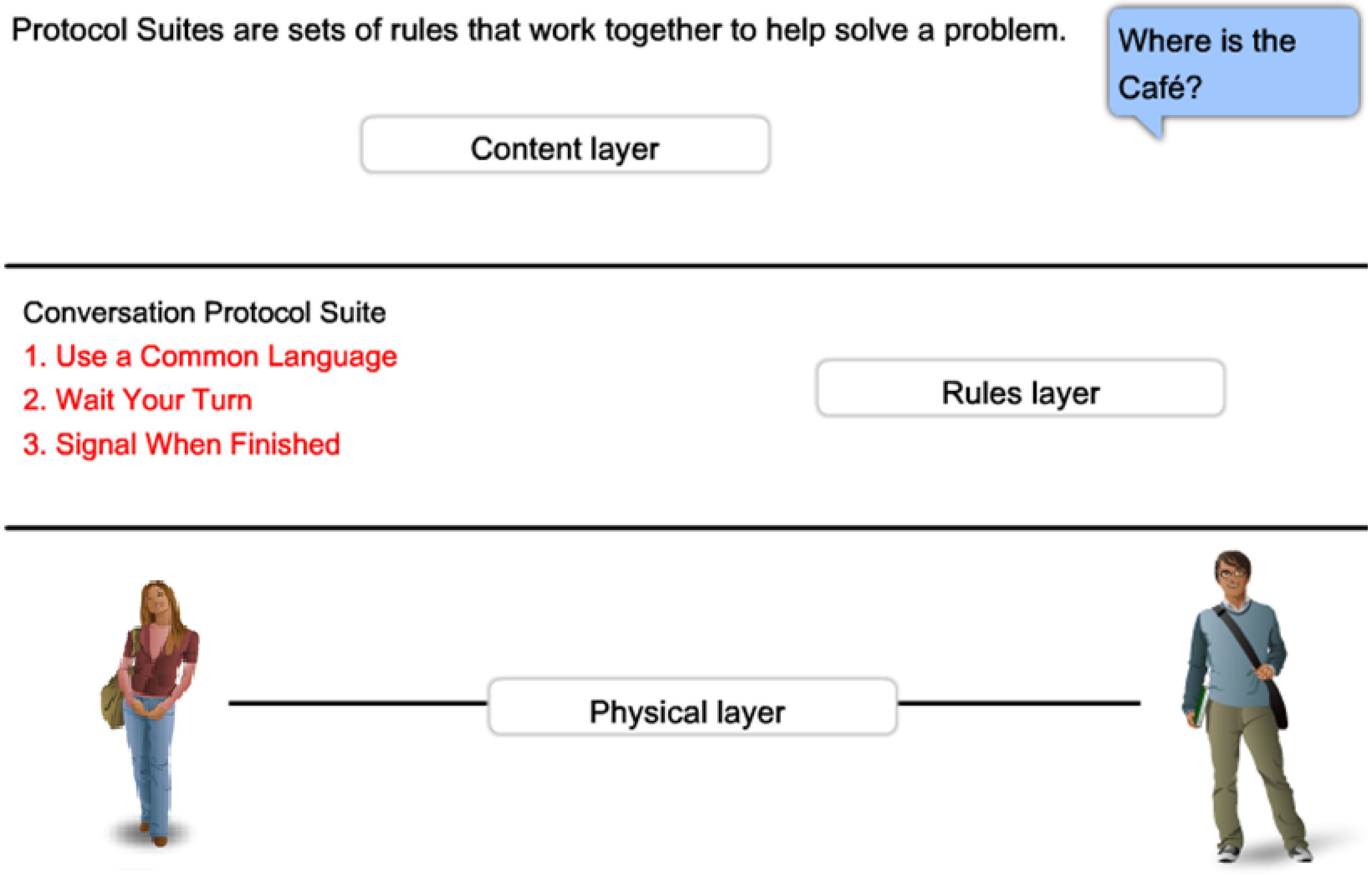
- An identified sender and receiver
- Agreed upon method of communicating (face-to-face, telephone, letter, photograph)
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgement requirements



Communication Protocols

- All communication, whether face-to-face or over a network, is governed by predetermined rules called **protocols**.
- A group of inter-related protocols that are necessary to perform a communication function is called a **protocol suite**.
- Protocols are implemented in **software** and **hardware** that is loaded on each host and network device.
- The protocols are viewed as a layered **hierarchy**, with each higher level service depending on the functionality defined by the protocols shown in the lower levels.

Communication Protocols Example



Protocol Suites are sets of rules that work together to help solve a problem.

Where is the Café?

Content layer

Conversation Protocol Suite

1. Use a Common Language
2. Wait Your Turn
3. Signal When Finished

Rules layer

Physical layer

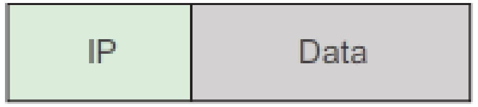
Network Protocols

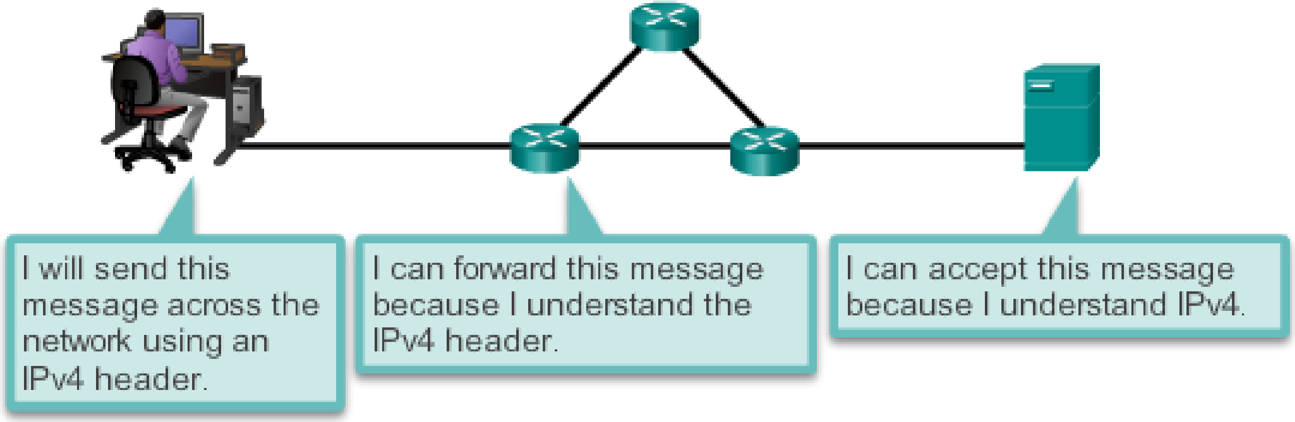
Networking protocols define a common format and set of rules for exchanging messages between devices. For example, describe the following processes:

- 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

Network Protocols

How the message is formatted or structured



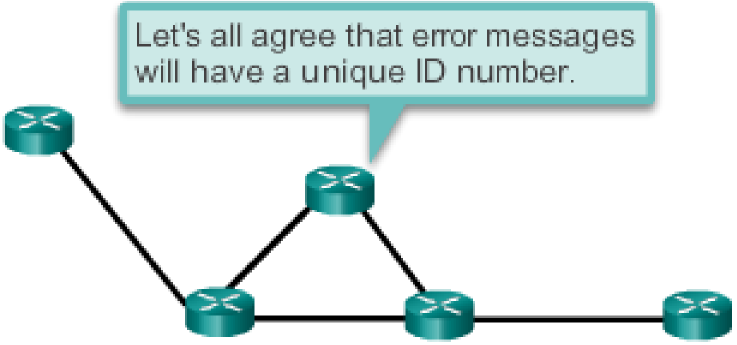


I will send this message across the network using an IPv4 header.

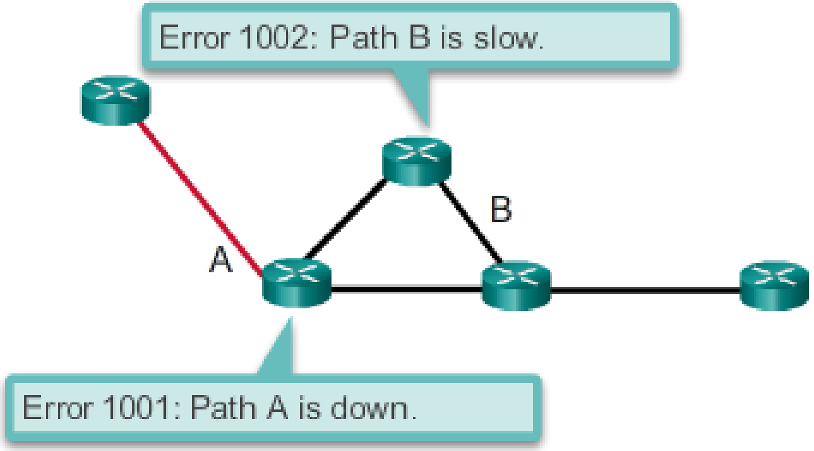
I can forward this message because I understand the IPv4 header.

I can accept this message because I understand IPv4.

How and when error and system messages are passed between devices



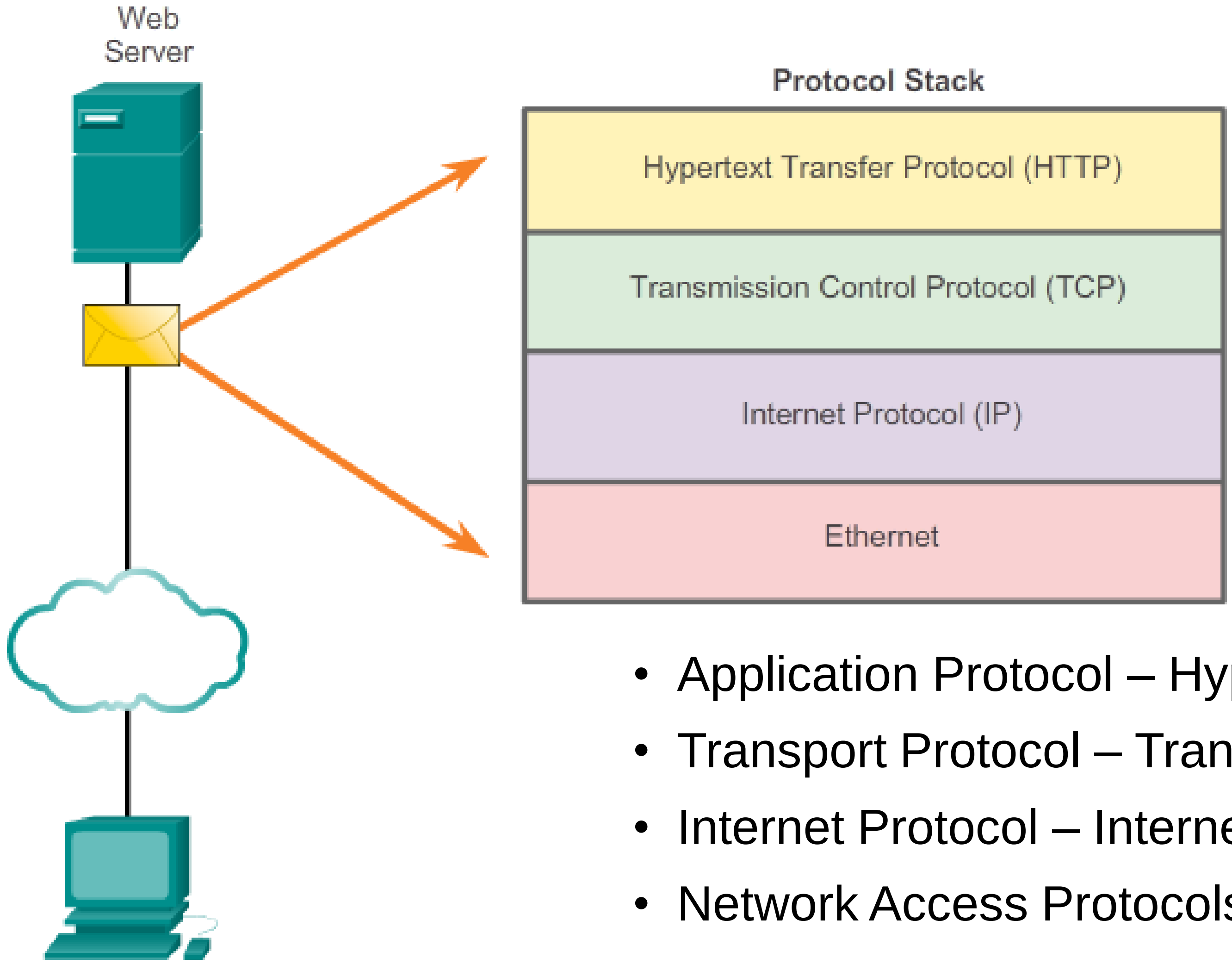
Let's all agree that error messages will have a unique ID number.



Error 1002: Path B is slow.

Error 1001: Path A is down.

Interaction of Protocols


Web Server
Protocol Stack
Hypertext Transfer Protocol (HTTP)
Transmission Control Protocol (TCP)
Internet Protocol (IP)
Ethernet

- Application Protocol – Hypertext Transfer Protocol (HTTP)
- Transport Protocol – Transmission Control Protocol (TCP)
- Internet Protocol – Internet Protocol (IP)
- Network Access Protocols – Data Link & Physical layers

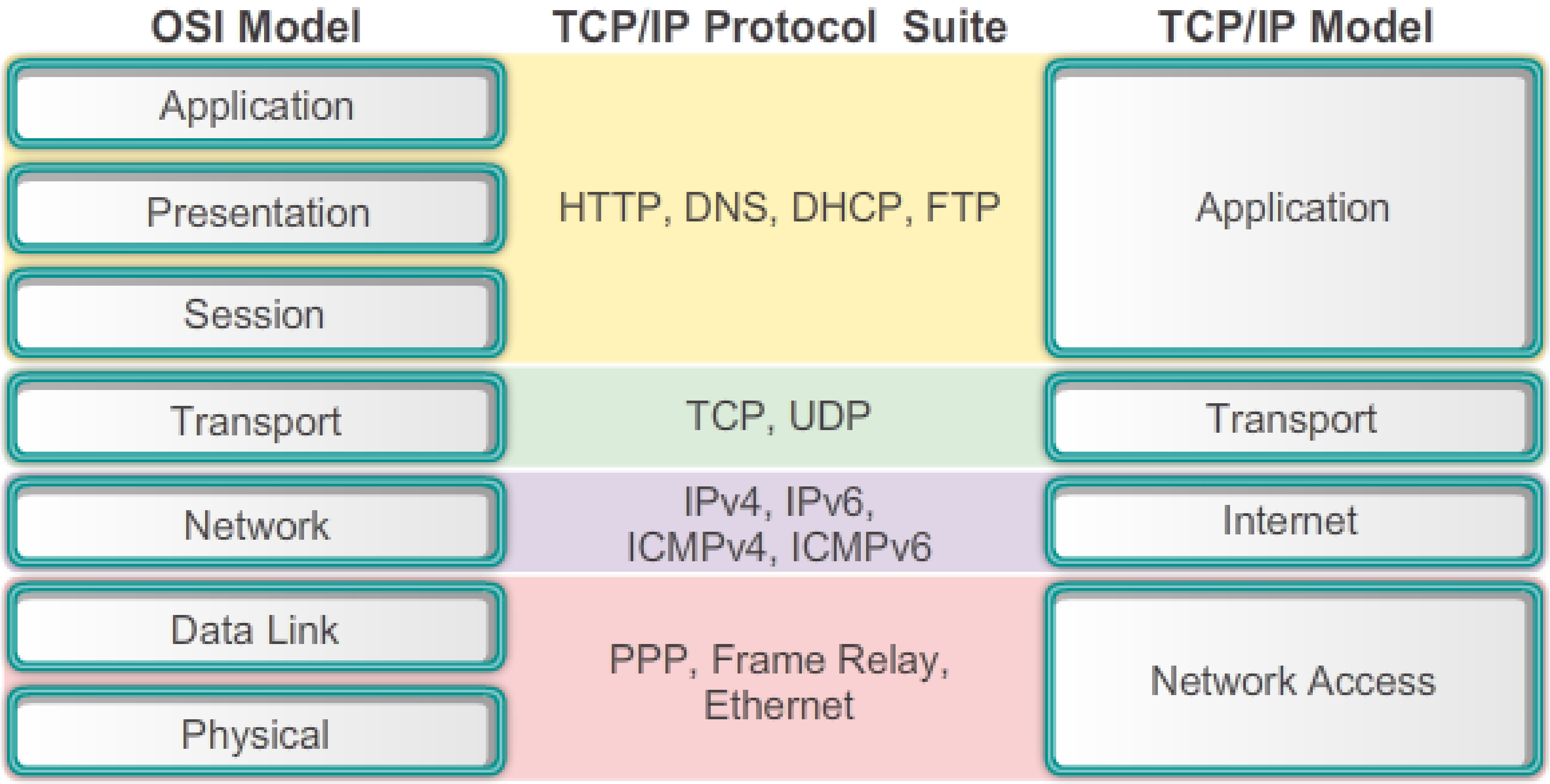
Protocols and Protocol Suite

- A protocol suite is a set of protocols that work together to provide comprehensive network communication services.
- A protocol suite may be specified by a standards organization or developed by a vendor.
- The protocols IP, HTTP, and DHCP are all part of the Internet protocol suite known as Transmission Control Protocol/IP (TCP/IP).
- The TCP/IP protocol suite is an open standard, meaning these protocols are freely available to the public, and any vendor is able to implement these protocols on their hardware or in their software.

Networking Models Types

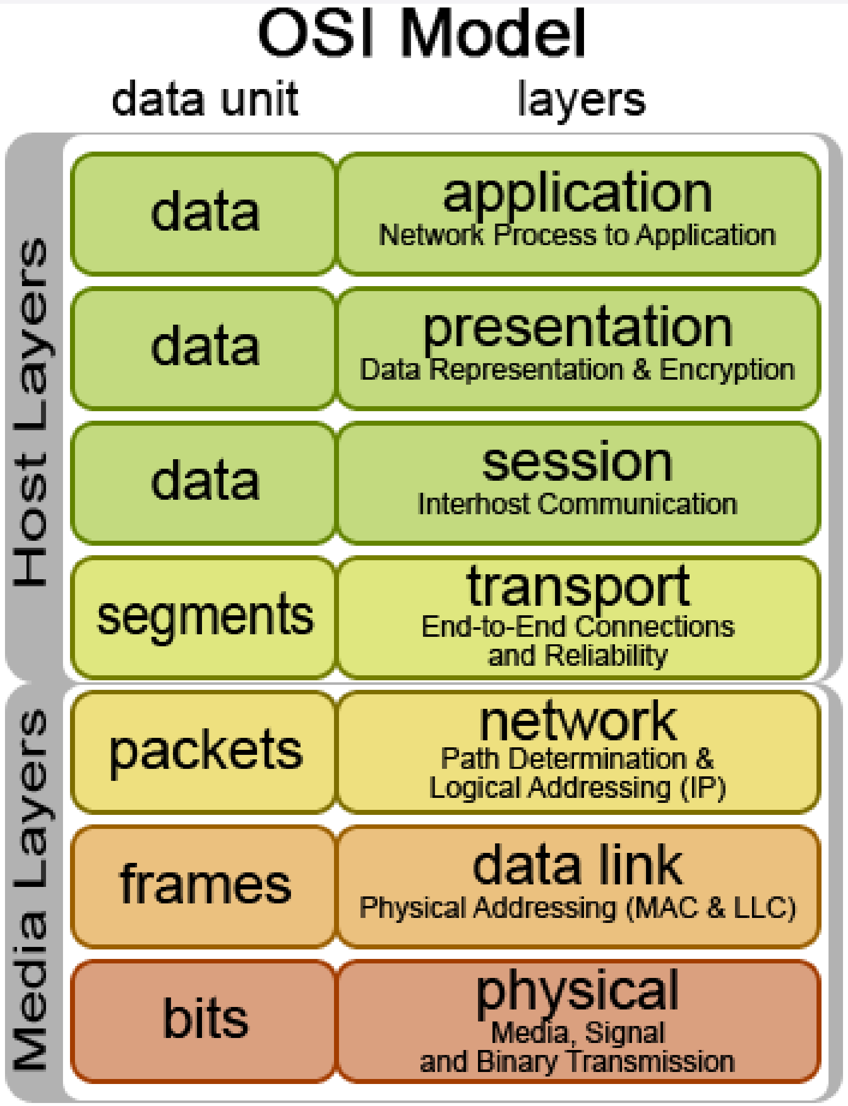
- **Reference model** - This model provides consistency within all types of network protocols and services by describing *what* has to be done at a particular layer, but not prescribing *how* it should be accomplished. The primary purpose of a reference model is to aid in clearer understanding of the functions and processes involved.
- **Protocol model** - This model closely matches the structure of a particular protocol suite. The TCP/IP model is a protocol model, because it describes the functions that occur at each layer of protocols within the TCP/IP suite.

Networking Models



OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

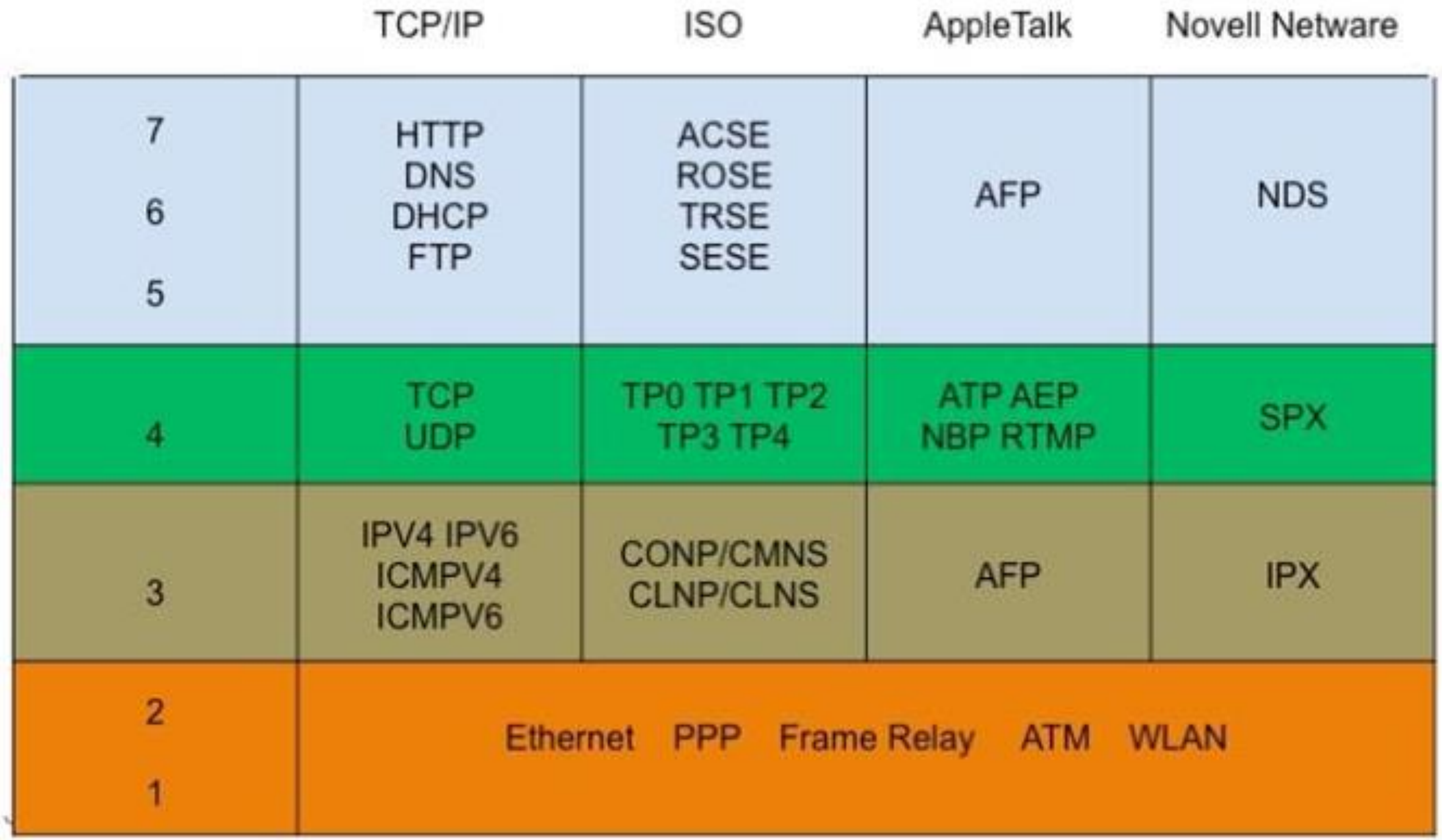
International Organization for Standardization



OSI Model

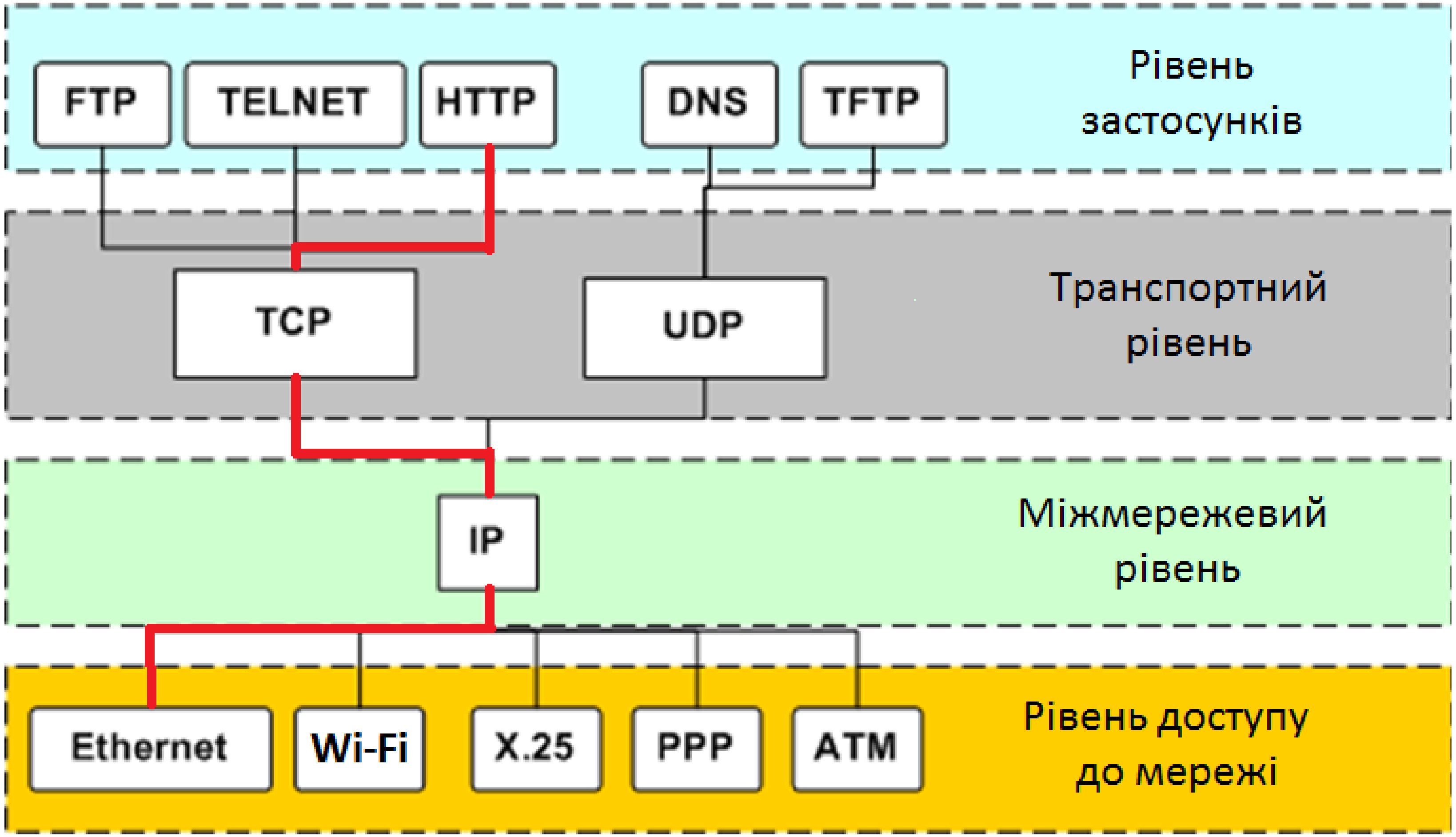
	data unit	layers
Host Layers	data	**application** Network Process to Application
	data	**presentation** Data Representation & Encryption
	data	**session** Interhost Communication
	segments	**transport** End-to-End Connections and Reliability
Media Layers	packets	**network** Path Determination & Logical Addressing (IP)
	frames	**data link** Physical Addressing (MAC & LLC)
	bits	**physical** Media, Signal and Binary Transmission

Protocol Suites and Industry Standards

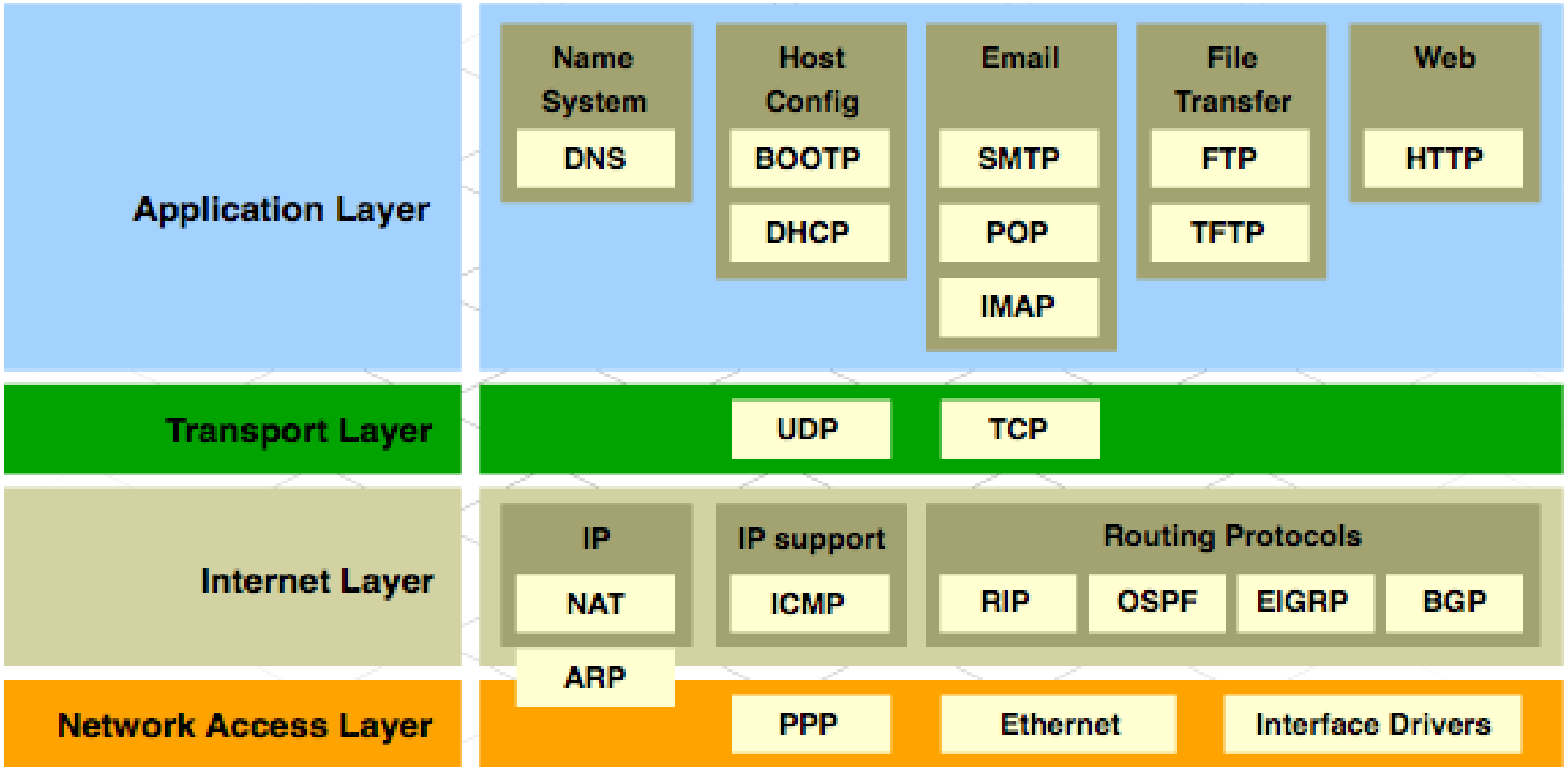


	TCP/IP	ISO	AppleTalk	Novell Netware
7 6 5	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
4	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
3	IPV4 IPV6 ICMPV4 ICMPV6	CONP/CMNS CLNP/CLNS	AFP	IPX
2 1	Ethernet PPP Frame Relay ATM WLAN			

TCP/IP stack


FTP
TELNET
HTTP
DNS
TFTP
Рівень застосунків
TCP
UDP
Транспортний рівень
IP
Міжмережевий рівень
Ethernet
Wi-Fi
X.25
PPP
ATM
Рівень доступу до мережі

TCP/IP Protocol Suite and Communication



Application Layer

- Name System: DNS
- Host Config: BOOTP, DHCP
- Email: SMTP, POP, IMAP
- File Transfer: FTP, TFTP
- Web: HTTP

Transport Layer

- UDP
- TCP

Internet Layer

- IP: NAT, ARP
- IP support: ICMP
- Routing Protocols: RIP, OSPF, EIGRP, BGP

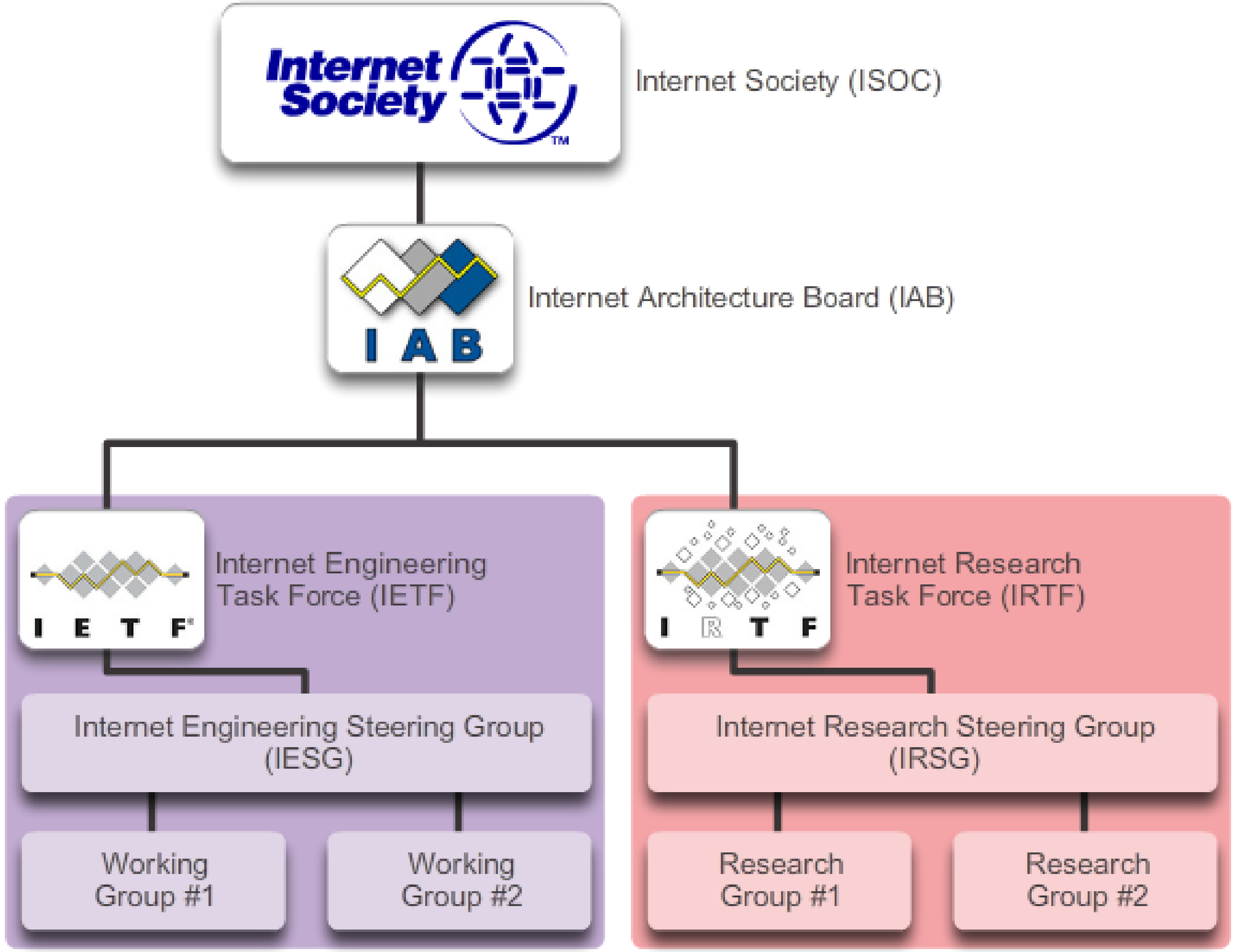
Network Access Layer

- PPP
- Ethernet
- Interface Drivers

Standards Organizations

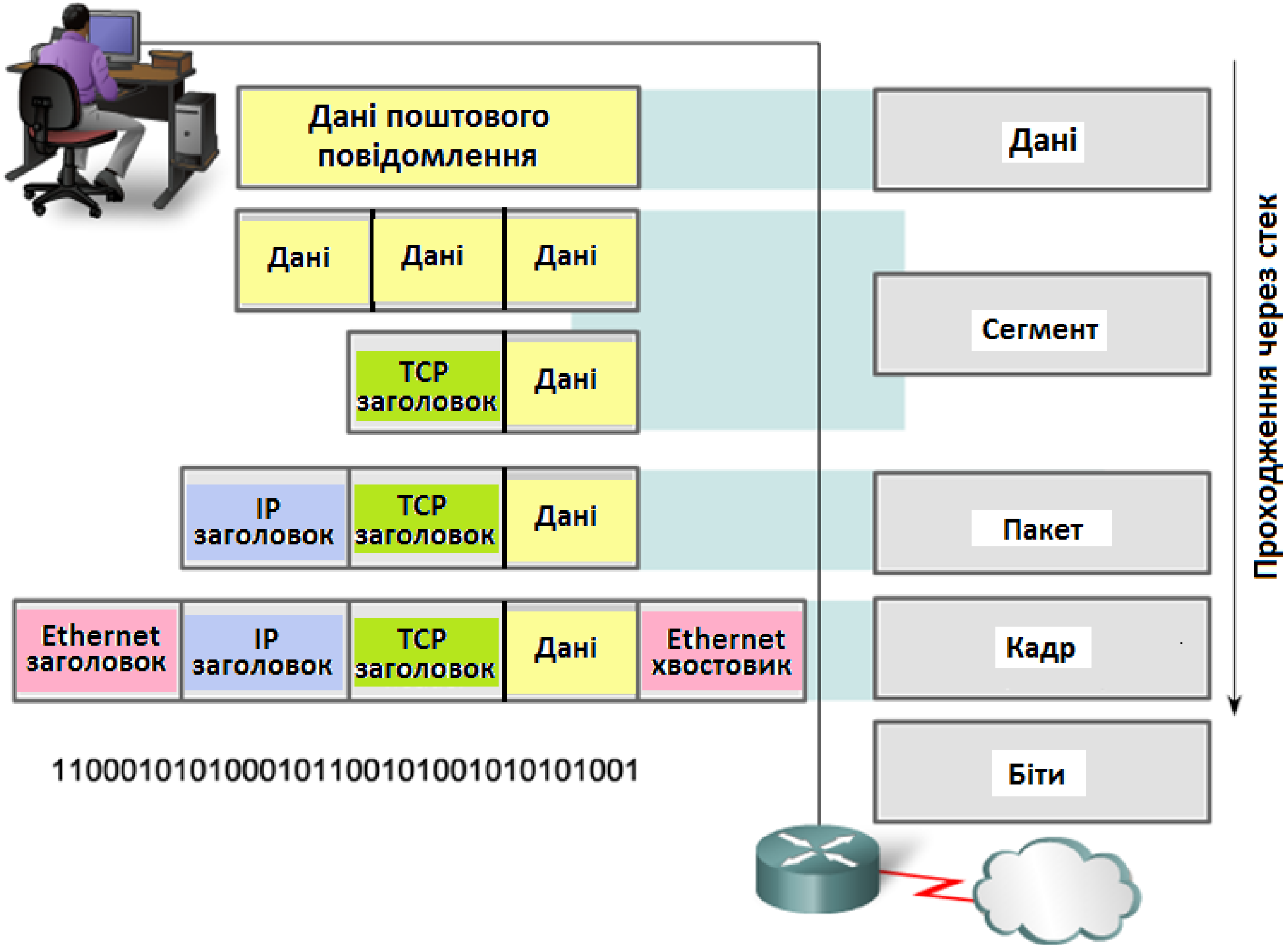
CONFIDENTIAL | © 2021 EPAM Systems, Inc.

ISOC, IAB, IETF, IRTF



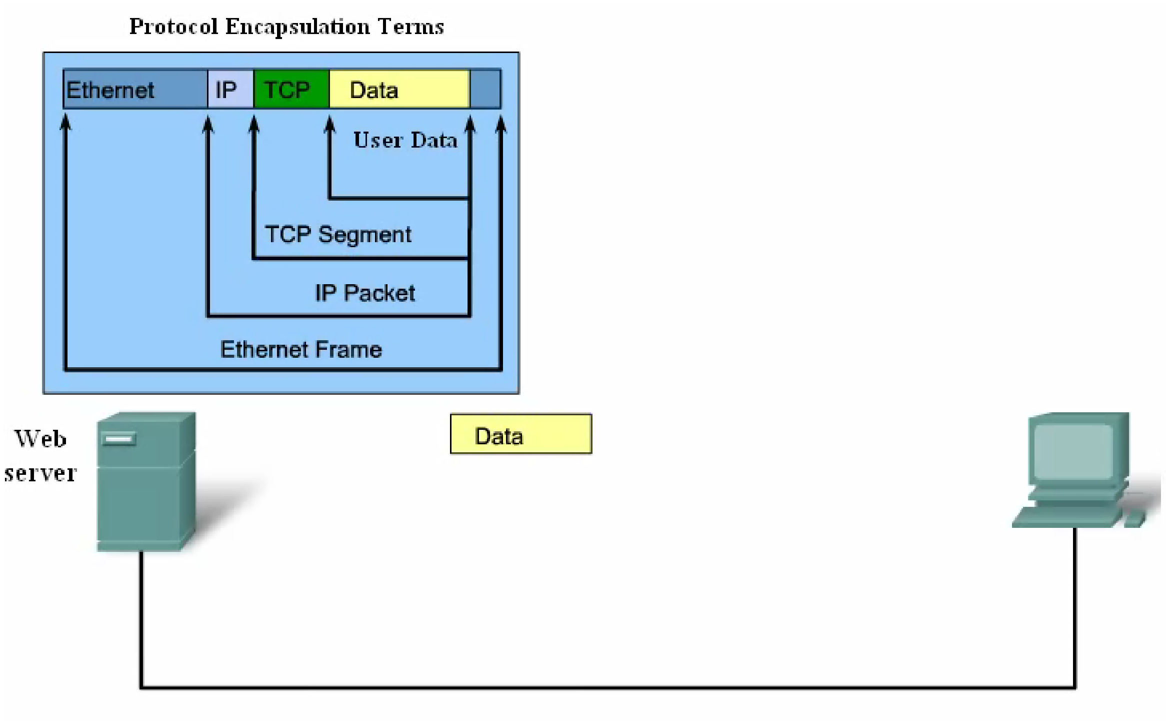
Internet Society
Internet Society (ISOC)
IAB
Internet Architecture Board (IAB)
IETF
Internet Engineering Task Force (IETF)
Internet Engineering Steering Group (IESG)
Working Group #1
Working Group #2
IRTF
Internet Research Task Force (IRTF)
Internet Research Steering Group (IRSG)
Research Group #1
Research Group #2

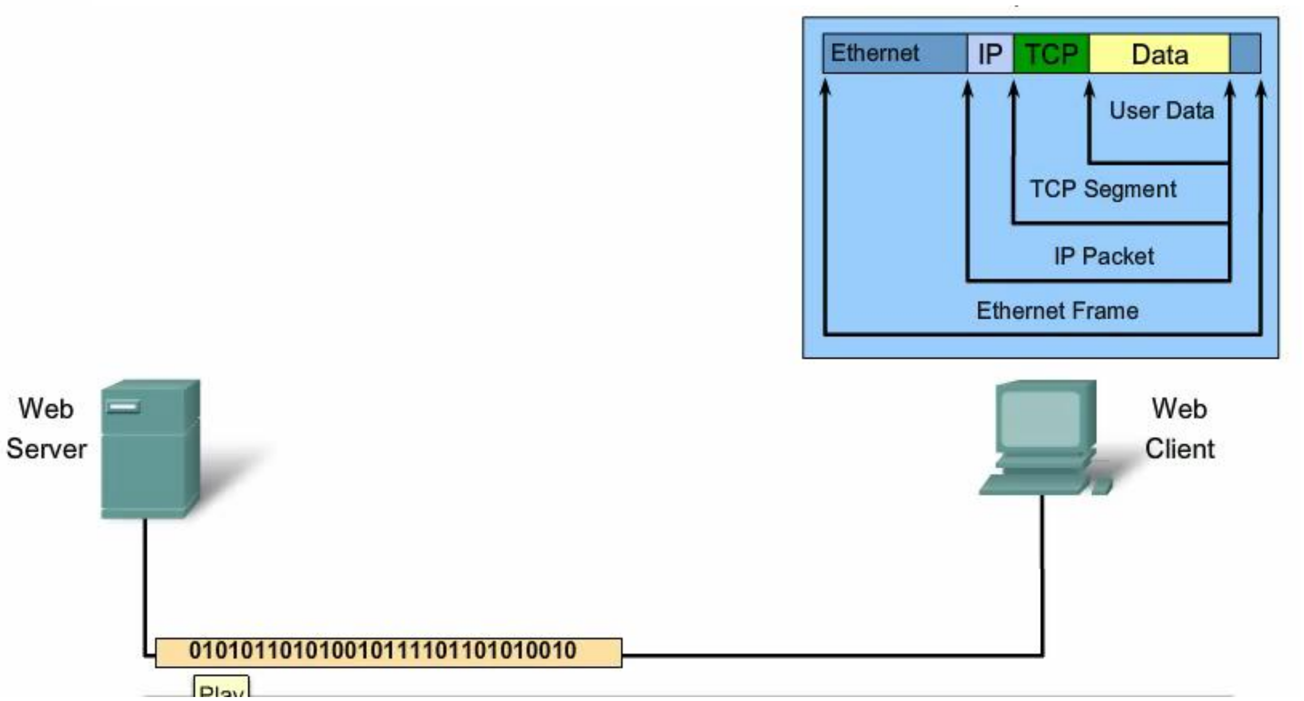
TCP/IP model in action



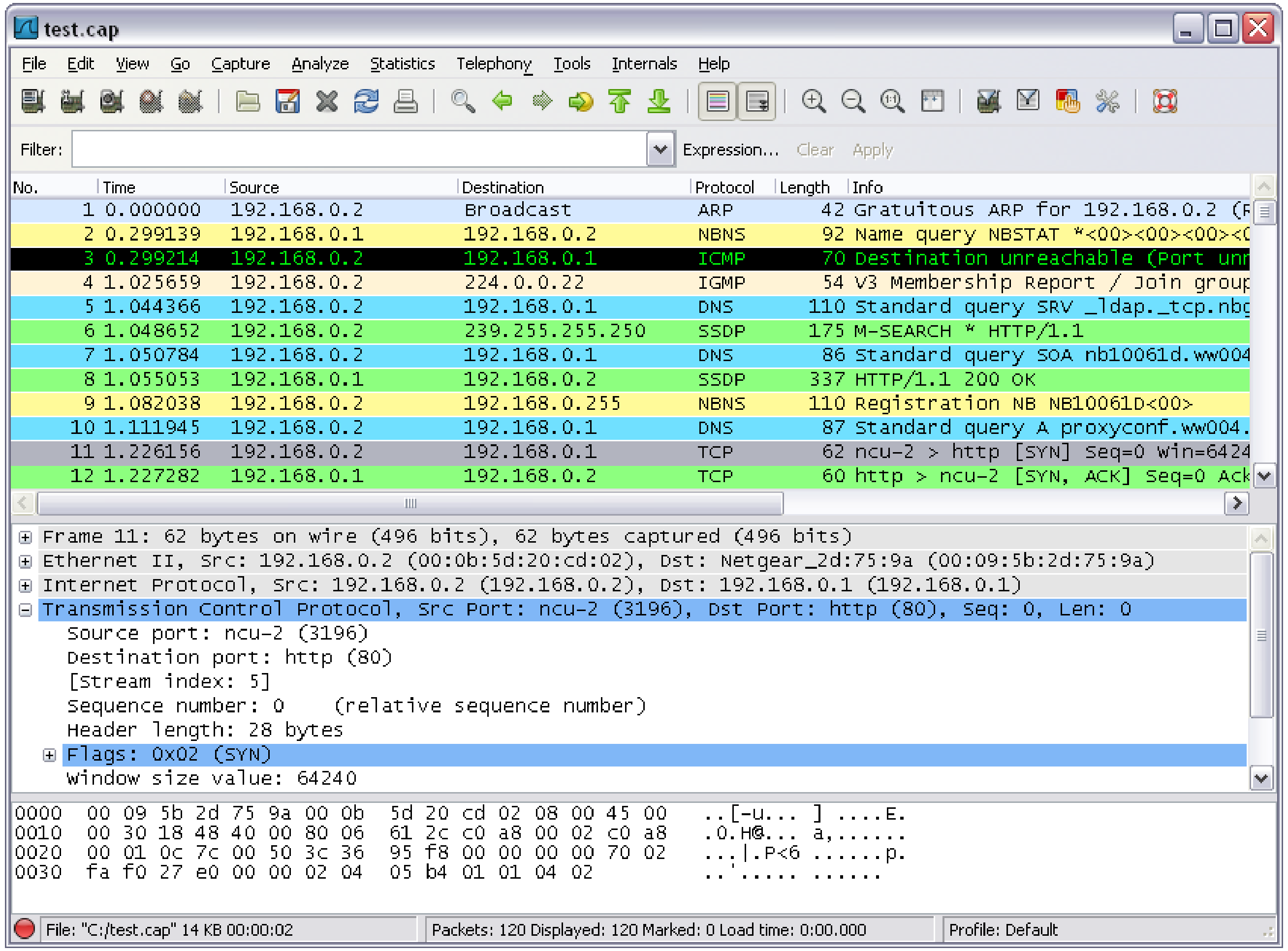
- **Data** - The general term for the PDU used at the Application layer
- **Segment** - Transport Layer PDU
- **Packet** - Internetwork Layer PDU
- **Frame** - Network Access Layer PDU
- **Bits** - A PDU used when physically transmitting data over the medium

The sending and receiving process





Using Wireshark to View Network Traffic



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	Broadcast	ARP	42	Gratuitous ARP for 192.168.0.2 (R
2	0.299139	192.168.0.1	192.168.0.2	NBNS	92	Name query NBSTAT *<00><00><00><0
3	0.299214	192.168.0.2	192.168.0.1	ICMP	70	Destination unreachable (Port unr
4	1.025659	192.168.0.2	224.0.0.22	IGMP	54	V3 Membership Report / Join group
5	1.044366	192.168.0.2	192.168.0.1	DNS	110	Standard query SRV _ldap._tcp.nbg
6	1.048652	192.168.0.2	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
7	1.050784	192.168.0.2	192.168.0.1	DNS	86	Standard query SOA nb10061d.ww004
8	1.055053	192.168.0.1	192.168.0.2	SSDP	337	HTTP/1.1 200 OK
9	1.082038	192.168.0.2	192.168.0.255	NBNS	110	Registration NB NB10061D<00>
10	1.111945	192.168.0.2	192.168.0.1	DNS	87	Standard query A proxyconf.ww004.
11	1.226156	192.168.0.2	192.168.0.1	TCP	62	ncu-2 > http [SYN] Seq=0 Win=6424
12	1.227282	192.168.0.1	192.168.0.2	TCP	60	http > ncu-2 [SYN, ACK] Seq=0 Ack

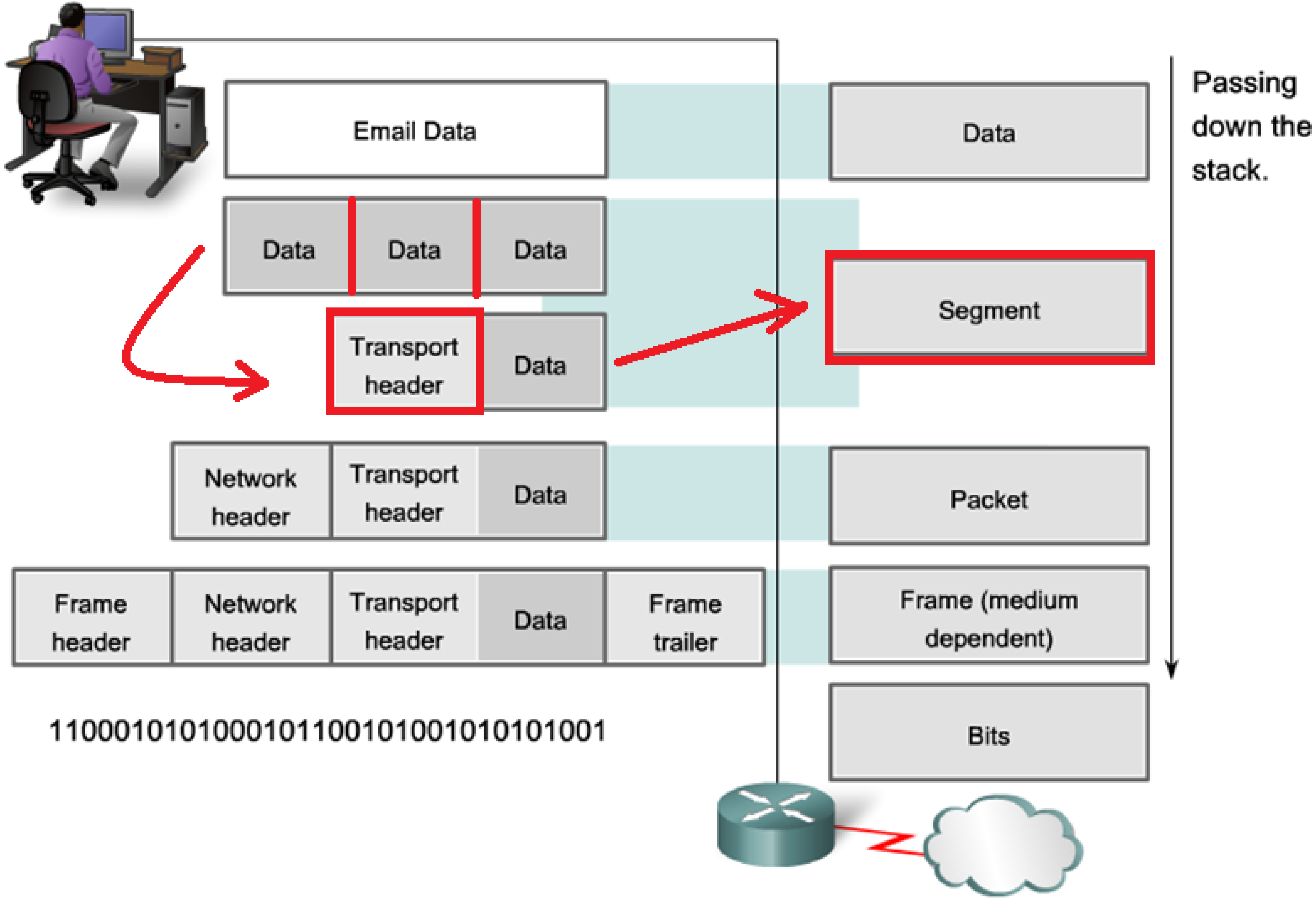
```
⊞ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊟ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: ncu-2 (3196)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size value: 64240
```

```
0000   00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010   00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020   00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030   fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

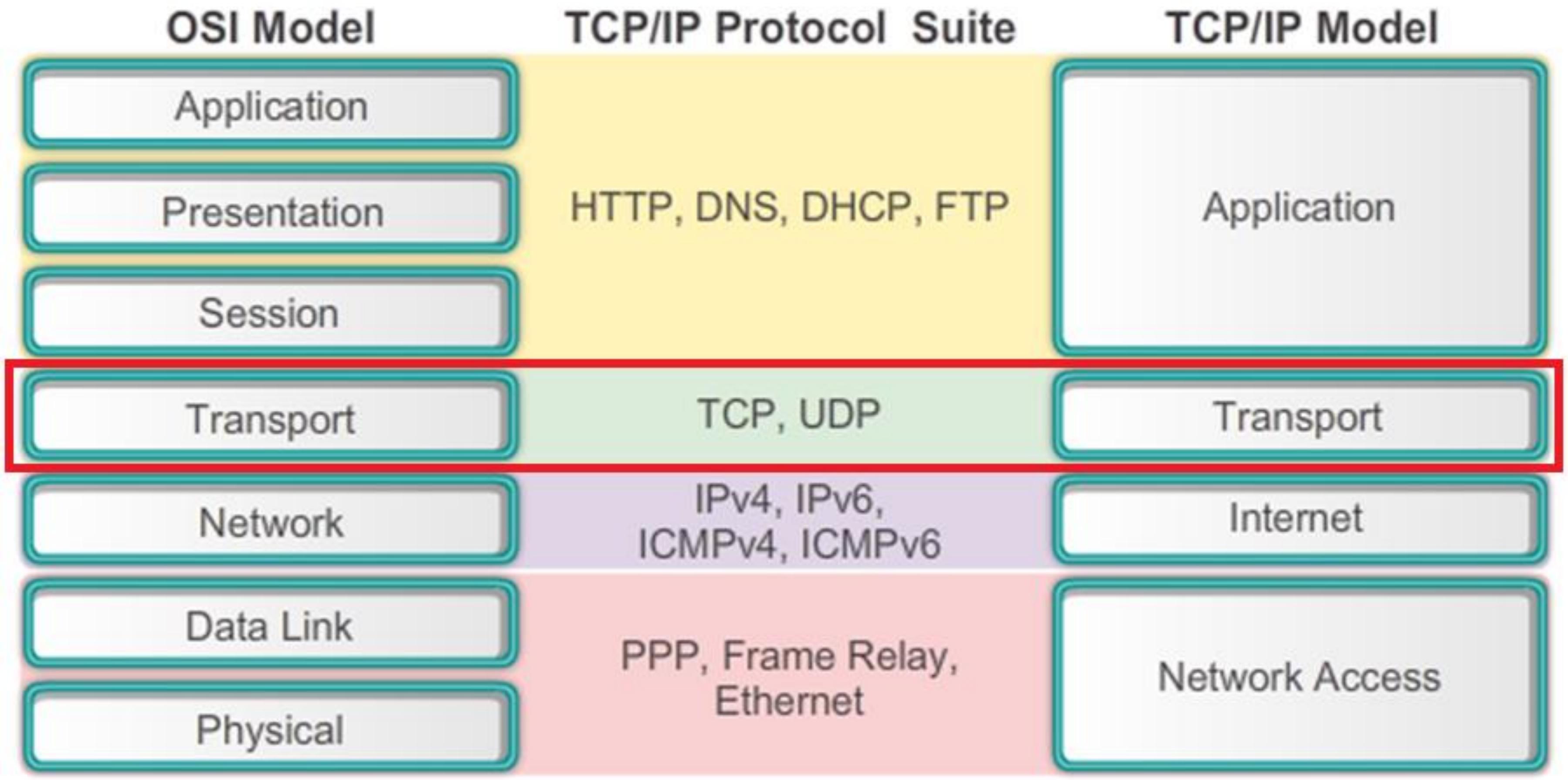
File: "C:/test.cap" 14 KB 00:00:02 | Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.000 | Profile: Default

Transport layer details

Protocol data units (PDU) and encapsulation



Networking Models



OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

Role of the Transport Layer

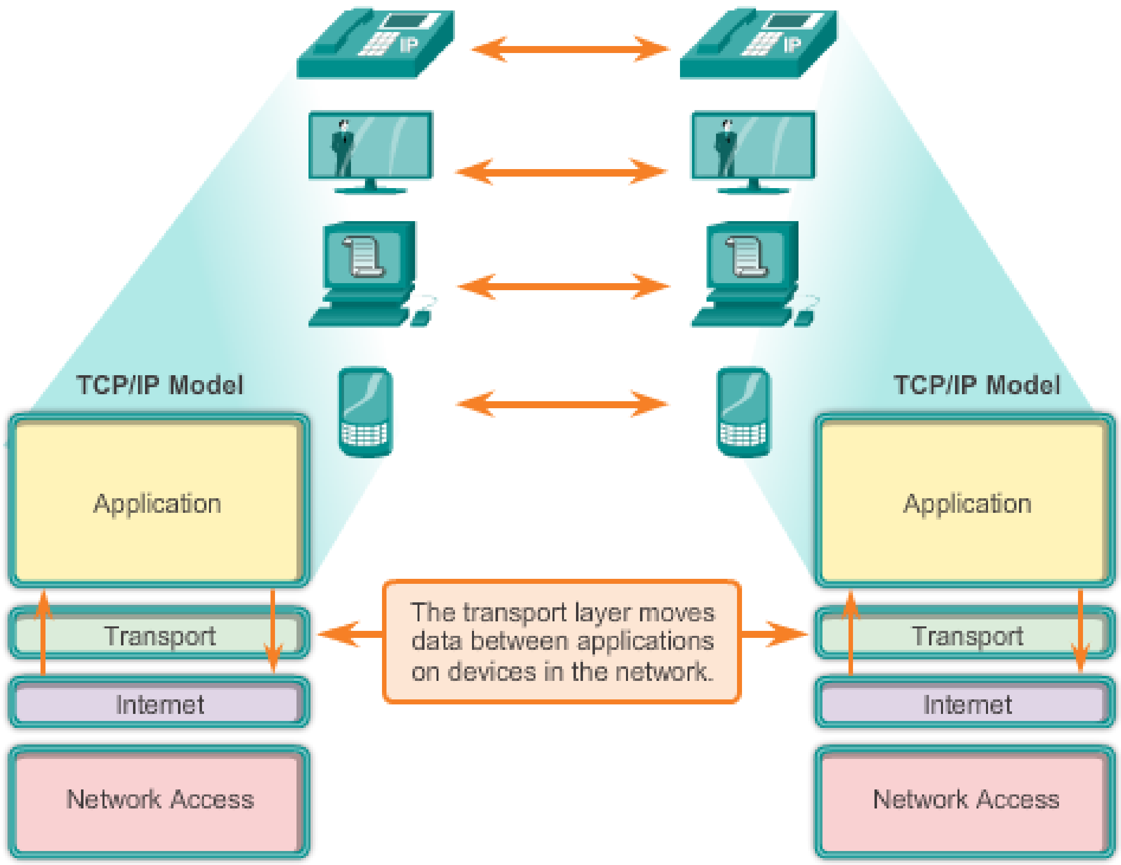
The **Transport Layer** is responsible for establishing a temporary communication session between two applications and delivering data between them. TCP/IP uses two protocols to achieve this:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

Primary Responsibilities of Transport layer Protocols

- **Tracking the individual communication** between applications on the source and destination hosts
- **Segmenting data** for manageability and reassembling segmented data into streams of application data at the destination
- **Identifying the proper application** for each communication stream

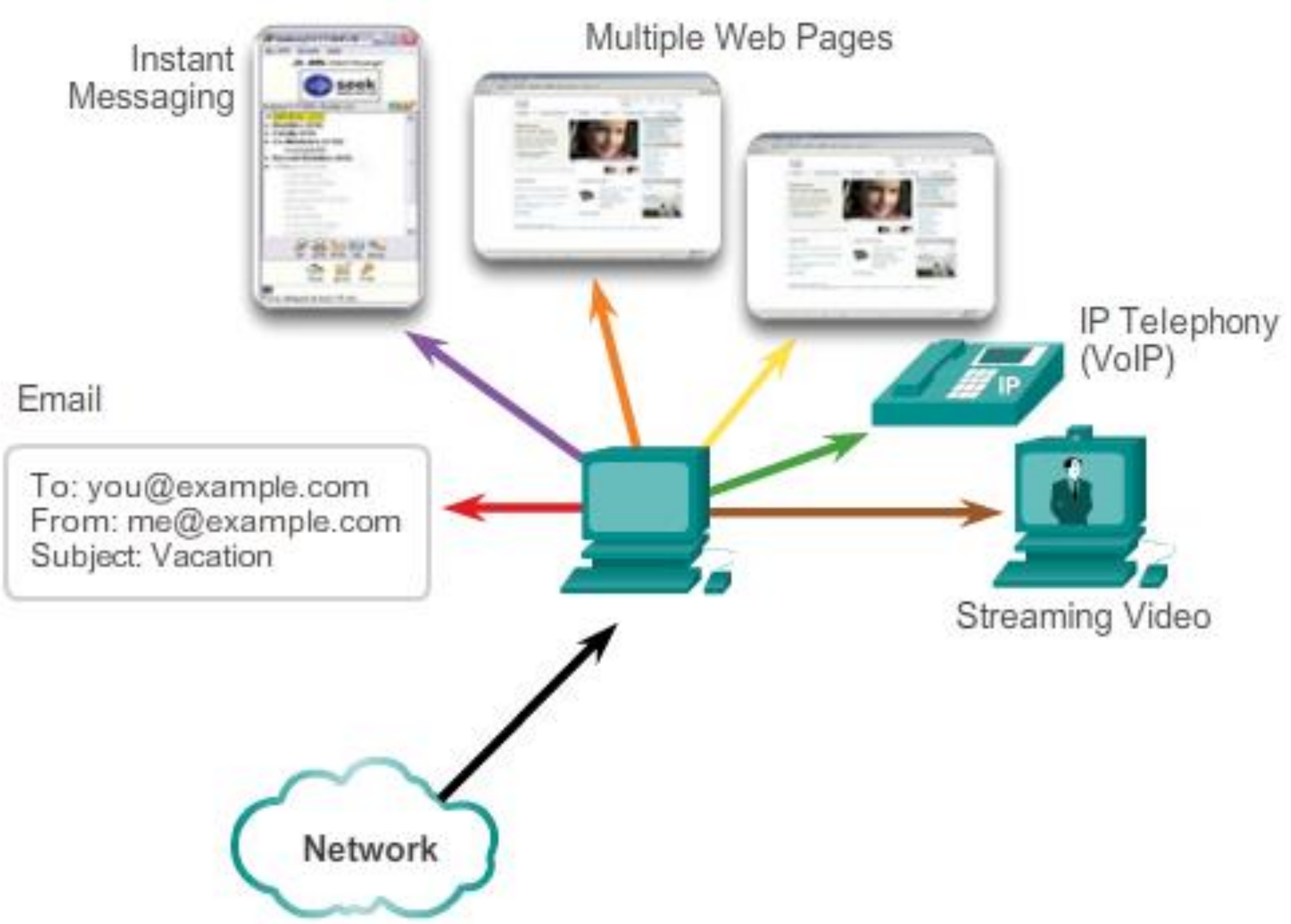
Enabling Applications on Devices to Communicate



The transport layer moves data between applications on devices in the network.

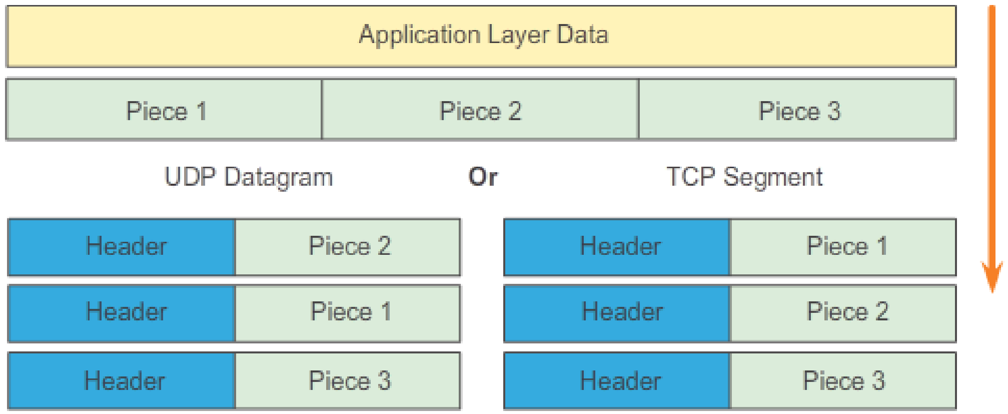
Tracking Individual Conversations

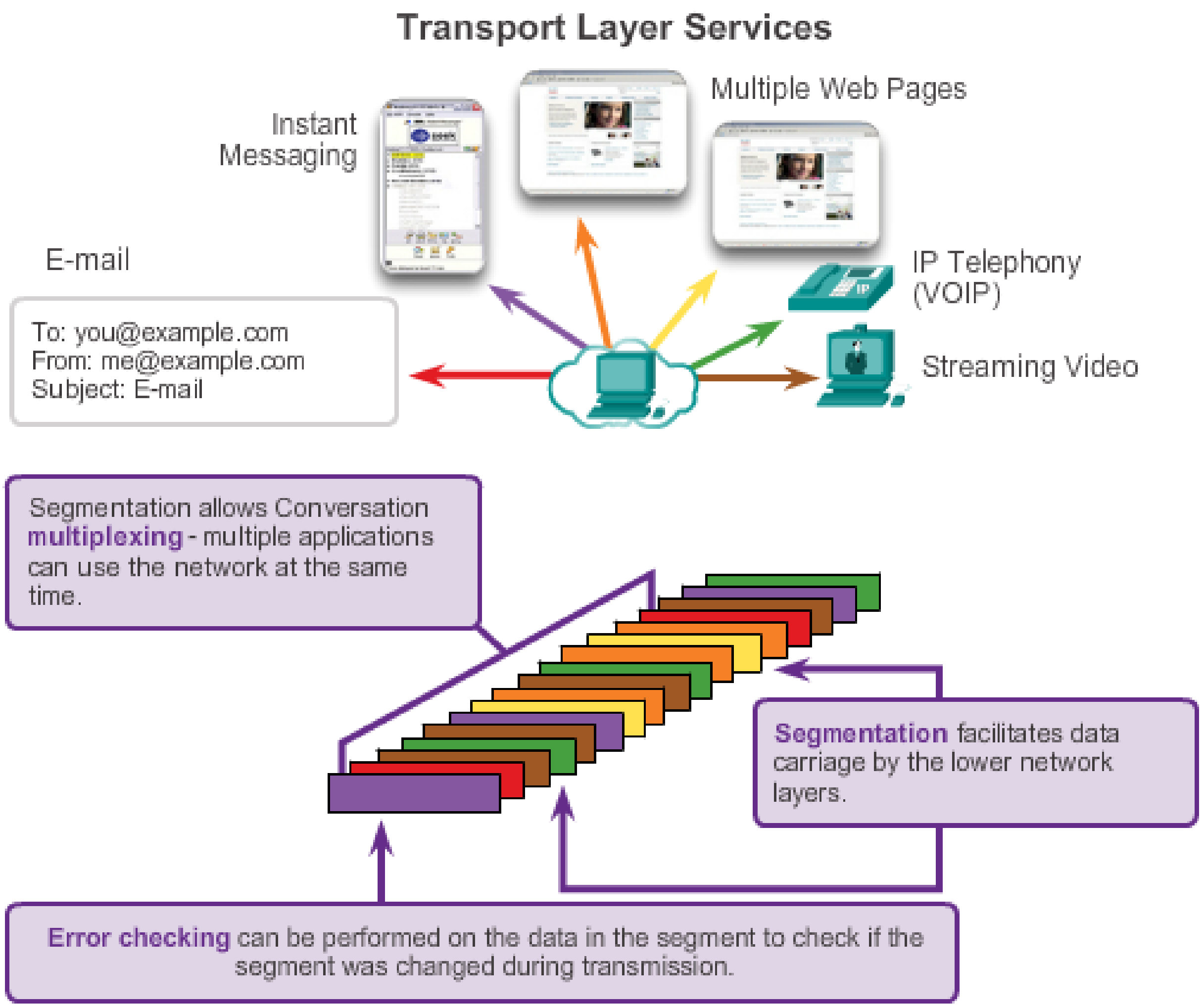
- At the transport layer, each set of data flowing between a source application and a destination application is known as a **conversation**.
- A host may have **multiple** applications that are communicating across the network **simultaneously**.
- Each of these applications communicates with one or more applications on one or more remote hosts. It is the responsibility of the transport layer to **maintain** and **track** these multiple conversations.



Segmenting data

- Enables many different communications, from many different users, to be interleaved (multiplexed) on the same network, at the same time.
- Provides the means to both **send** and **receive** data when running multiple applications.
- Header added to each segment to identify it.




Transport Layer Services

To: you@example.com
From: me@example.com
Subject: E-mail

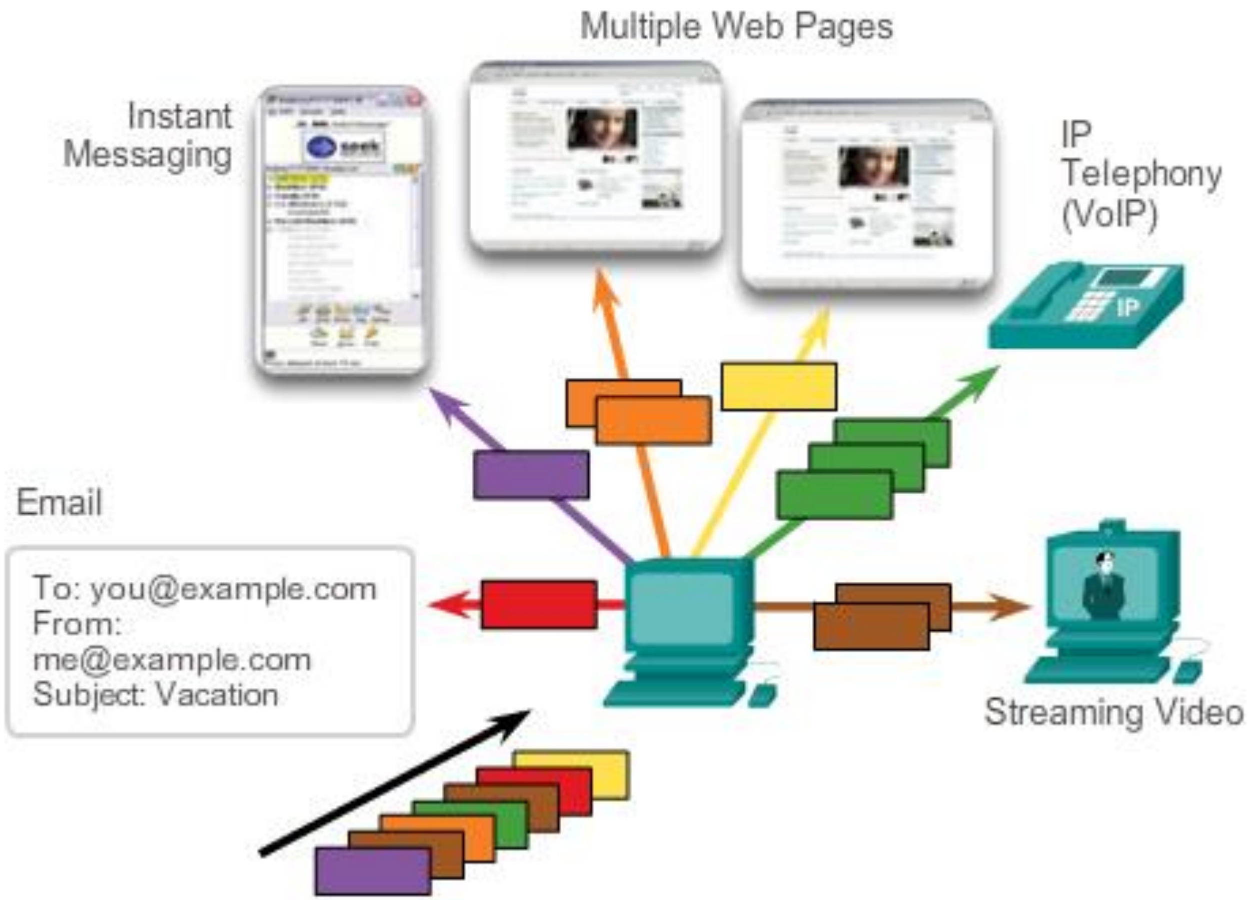
Segmentation allows Conversation **multiplexing** - multiple applications can use the network at the same time.

Segmentation facilitates data carriage by the lower network layers.

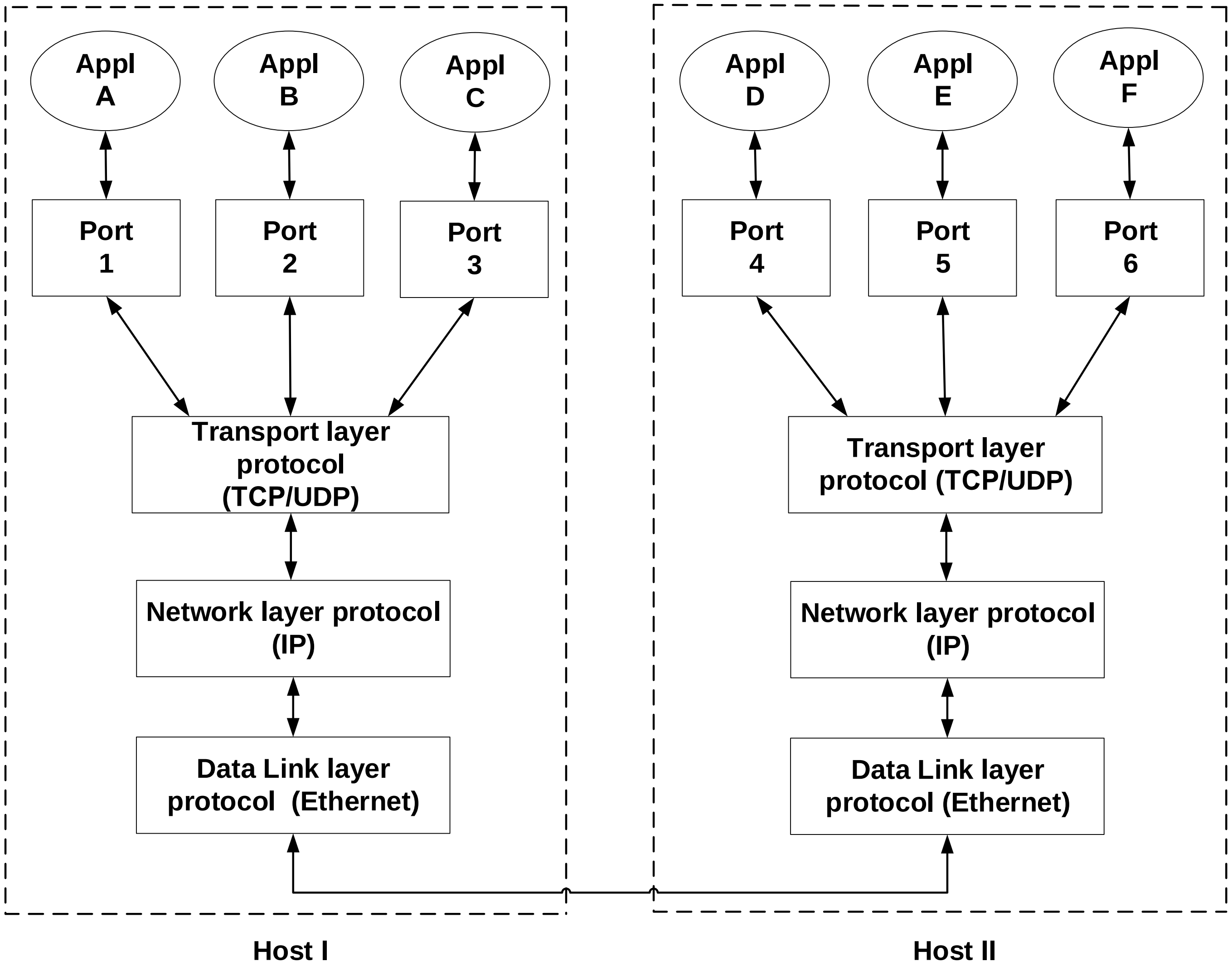
Error checking can be performed on the data in the segment to check if the segment was changed during transmission.

Identifying the Applications

- To pass data streams to the proper applications, the transport layer must **identify** the target application.
- To accomplish this, the transport layer assigns each application an identifier.
- This identifier is called a **port number**.



Data transfer via transport layer


Appl A
Appl B
Appl C
Port 1
Port 2
Port 3
Transport layer protocol (TCP/UDP)
Network layer protocol (IP)
Data Link layer protocol (Ethernet)
Host I
Appl D
Appl E
Appl F
Port 4
Port 5
Port 6
Transport layer protocol (TCP/UDP)
Network layer protocol (IP)
Data Link layer protocol (Ethernet)
Host II

Transport Layer Reliability

Different applications have different transport reliability requirements

TCP/IP provides two transport layer protocols, **TCP and UDP**

Transmission Control Protocol (TCP)

- Provides reliable delivery ensuring that all of the data arrives at the destination.
- Uses acknowledged delivery and other processes to ensure delivery
- Makes larger demands on the network – more overhead

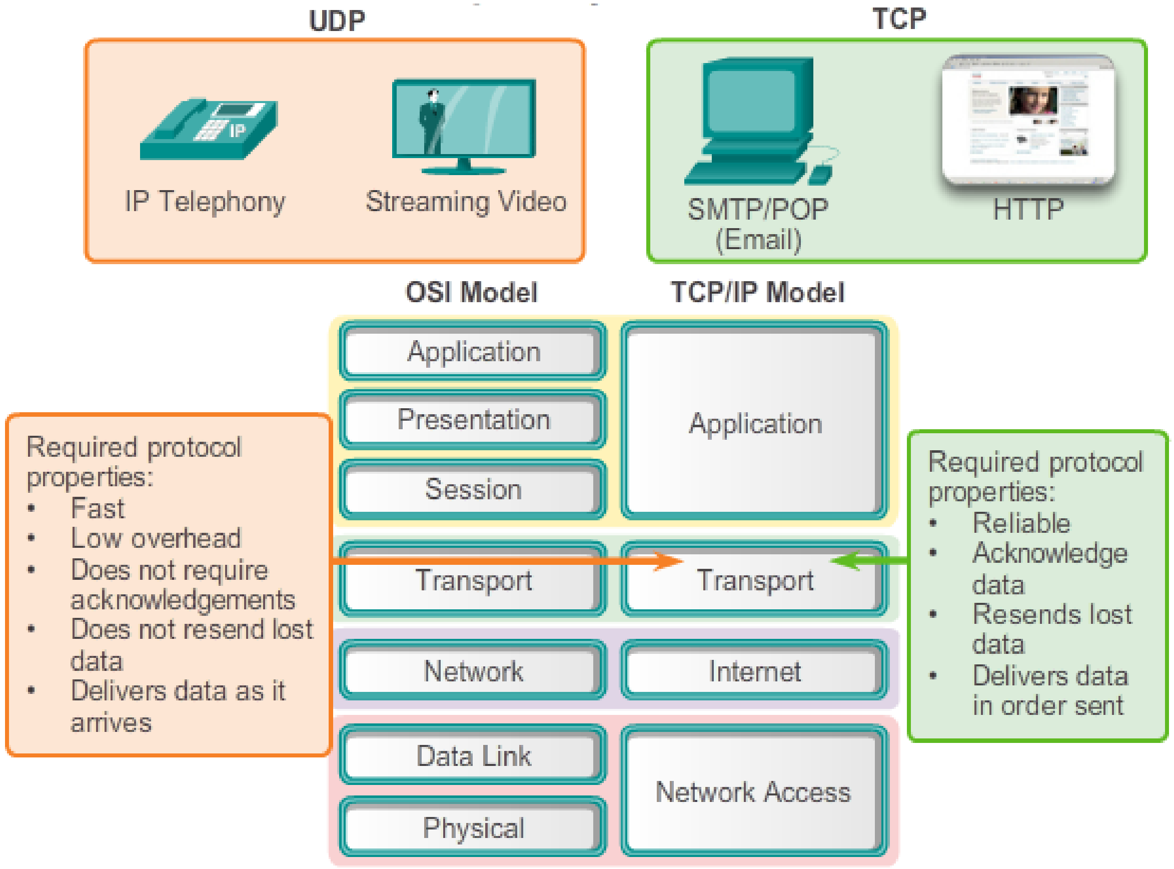
User Datagram Protocol (UDP)

- Provides just the basic functions for delivery – no reliability
- Less overhead

TCP versus UDP

There is a **trade-off** between the value of reliability and the burden it places on the network.

Application developers choose the transport protocol based on the requirements of their applications.

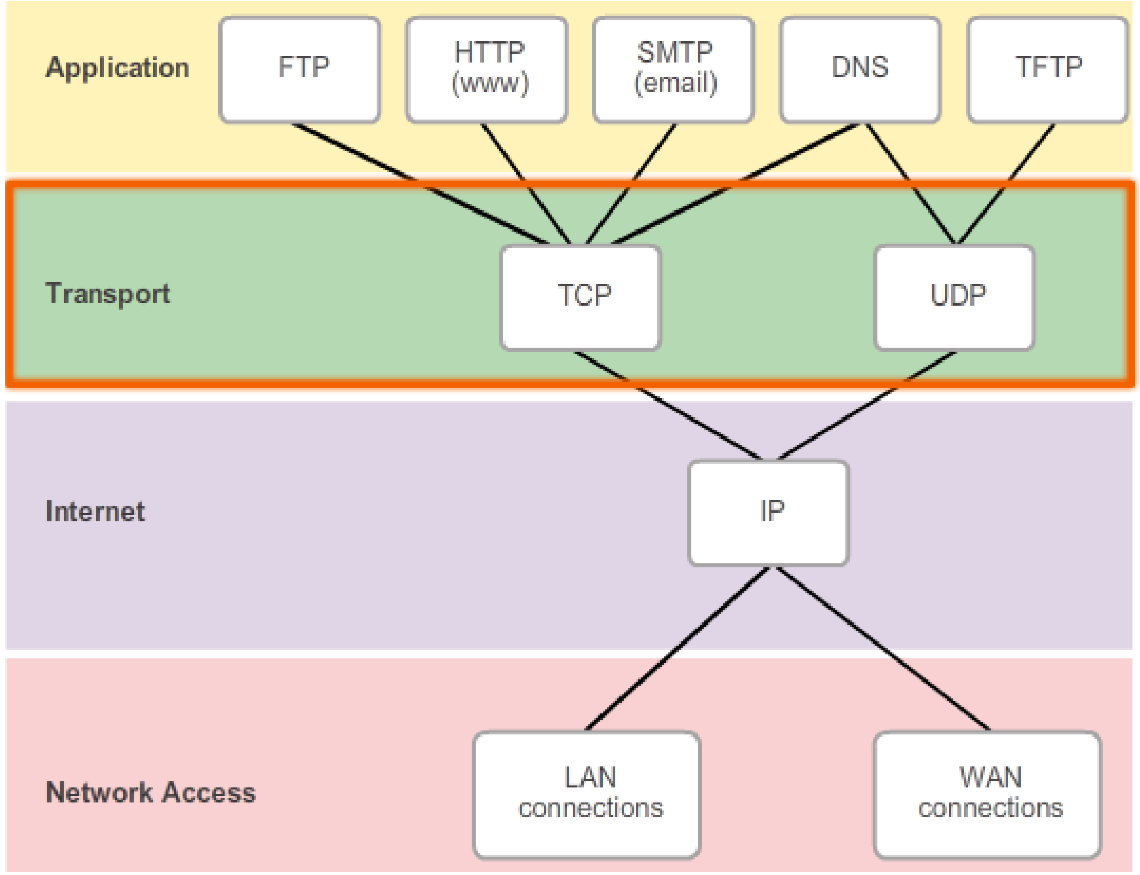


Required protocol properties:

- Fast
- Low overhead
- Does not require acknowledgements
- Does not resend lost data
- Delivers data as it arrives

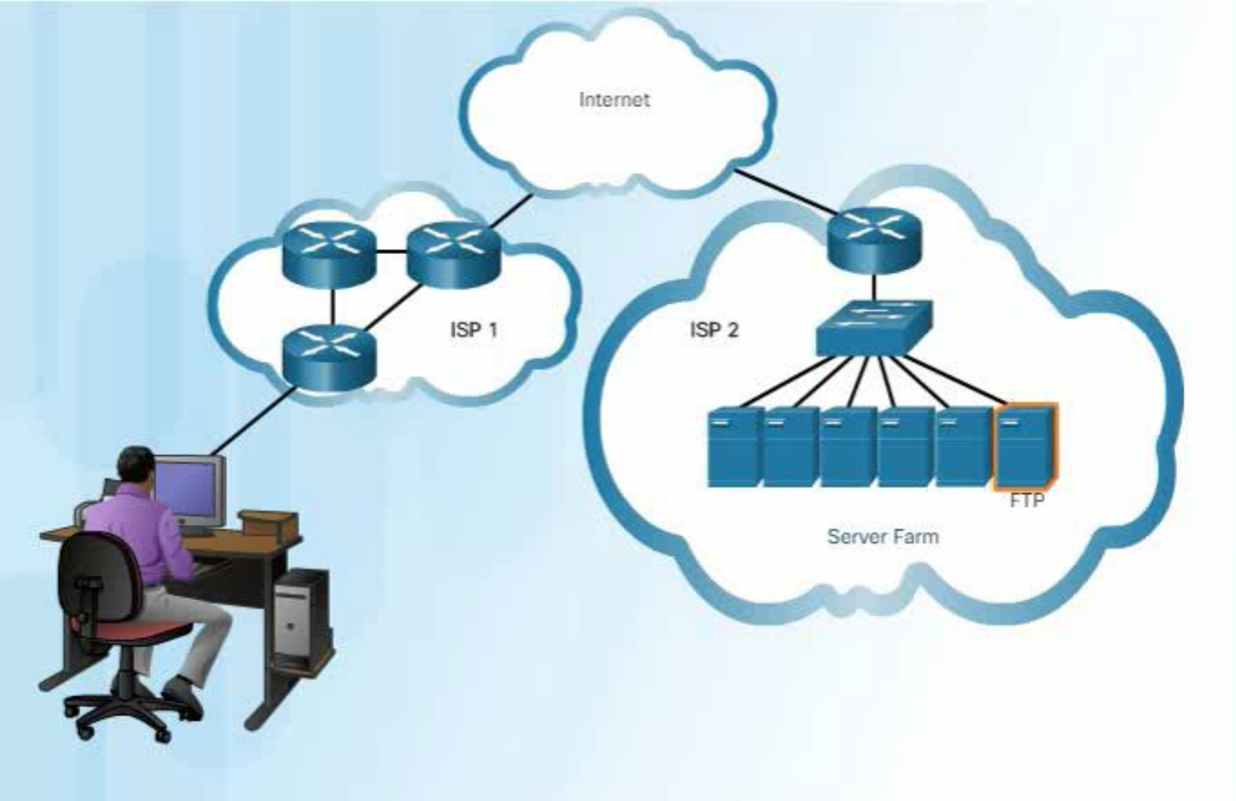
Required protocol properties:

- Reliable
- Acknowledge data
- Resends lost data
- Delivers data in order sent



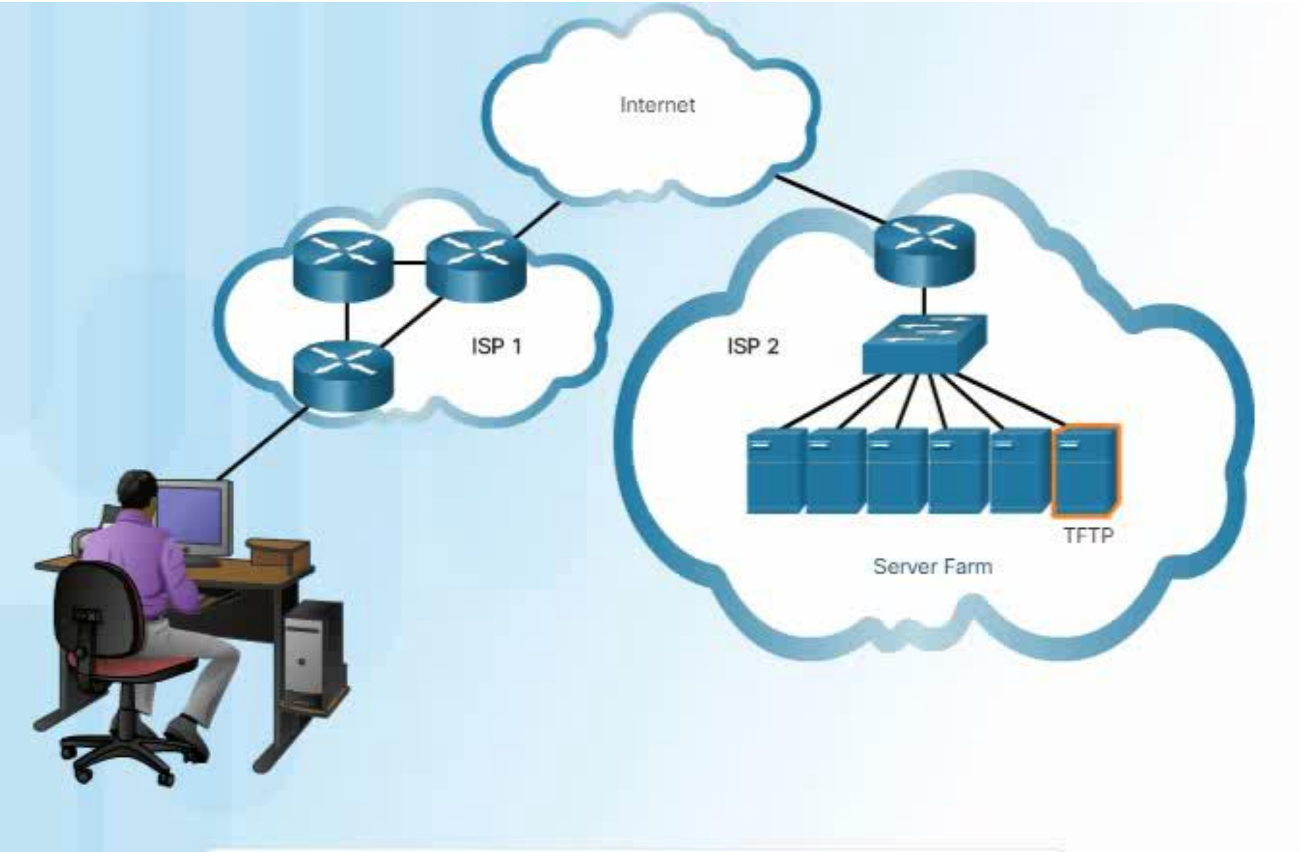
TCP

- TCP is considered a **reliable** transport protocol, which means that TCP includes processes to ensure reliable delivery between applications through the use of **acknowledged** delivery.
- With TCP, the three basic operations of reliability are:
  - Tracking transmitted data segments
  - Acknowledging received data
  - Retransmitting any unacknowledged data
- TCP breaks up a message into small pieces known as **segments**. The segments are numbered in sequence. TCP keeps track of the number of segments that have been sent to a specific host from a specific application.



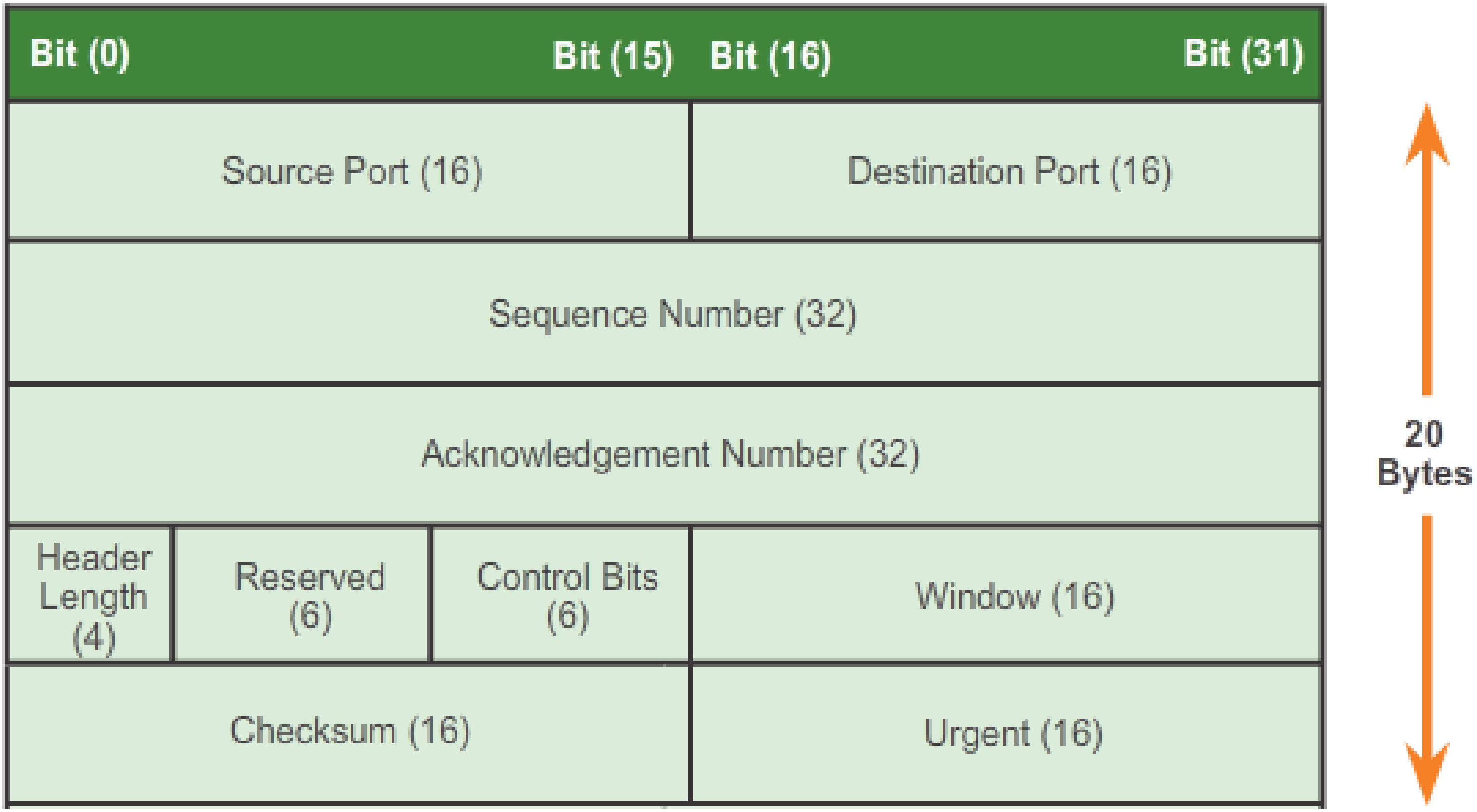
UDP

- UDP provides just the basic functions for delivering data segments between the appropriate applications, with very little overhead and data checking.
- UDP is known as a **best-effort** delivery protocol. In the context of networking, best-effort delivery is referred to as unreliable, because there is no acknowledgement that the data is received at the destination.
- Imposing overhead to ensure reliability for some applications could reduce the usefulness of the application and can even be detrimental to the application. In such cases, UDP is a better transport protocol.



Transmission Control Protocol (TCP)

- **RFC 793**
- **Connection-oriented** – creating a session between source and destination
- **Reliable delivery** – retransmitting lost or corrupt data
- **Ordered data reconstruction** – numbering and sequencing of segments
- **Flow control** - regulating the amount of data transmitted
- **Stateful protocol** – keeping track of the session



Bit (0)		Bit (15)	Bit (16) Bit (31)
Source Port (16)			Destination Port (16)
Sequence Number (32)			
Acknowledgement Number (32)			
Header Length (4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)			Urgent (16)

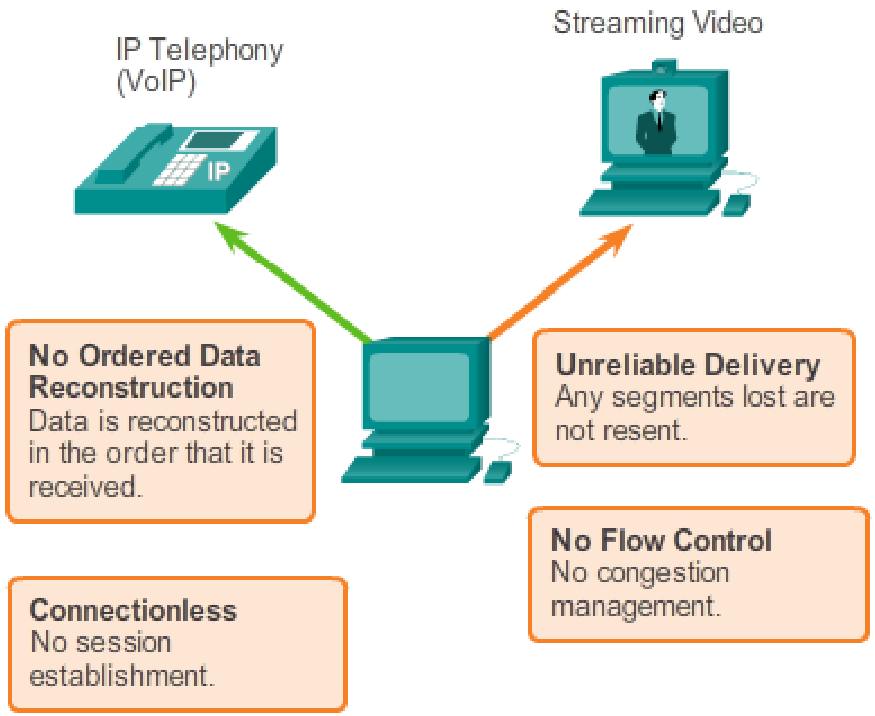
20 Bytes

User Datagram Protocol (UDP)

- RFC 768
- Connectionless
- Unreliable delivery
- No ordered data reconstruction
- No flow control
- Stateless protocol

Applications that use UDP:

- Domain Name System (DNS)
- Video Streaming
- Voice over IP (VoIP)
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- IP telephony or Voice over IP (VoIP)
- Online games

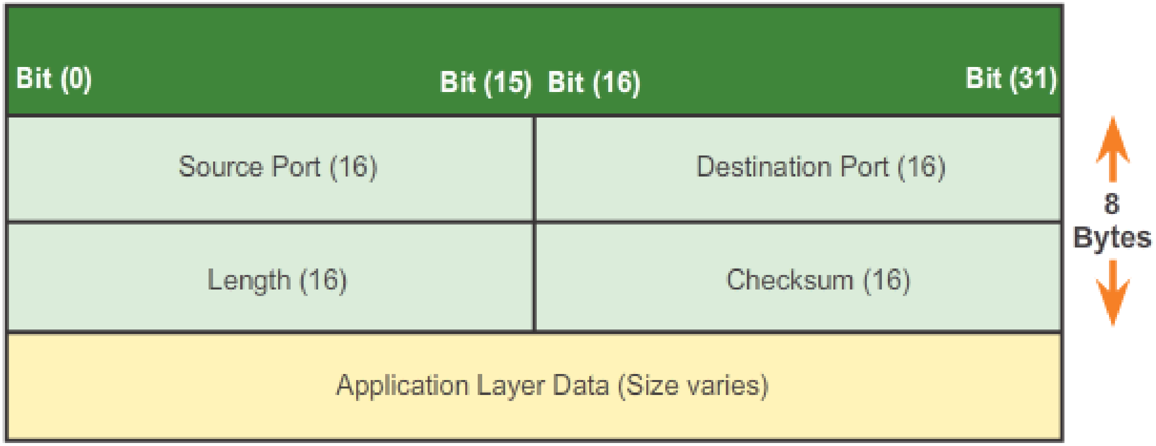


No Ordered Data Reconstruction
Data is reconstructed in the order that it is received.

Unreliable Delivery
Any segments lost are not resent.

No Flow Control
No congestion management.

Connectionless
No session establishment.

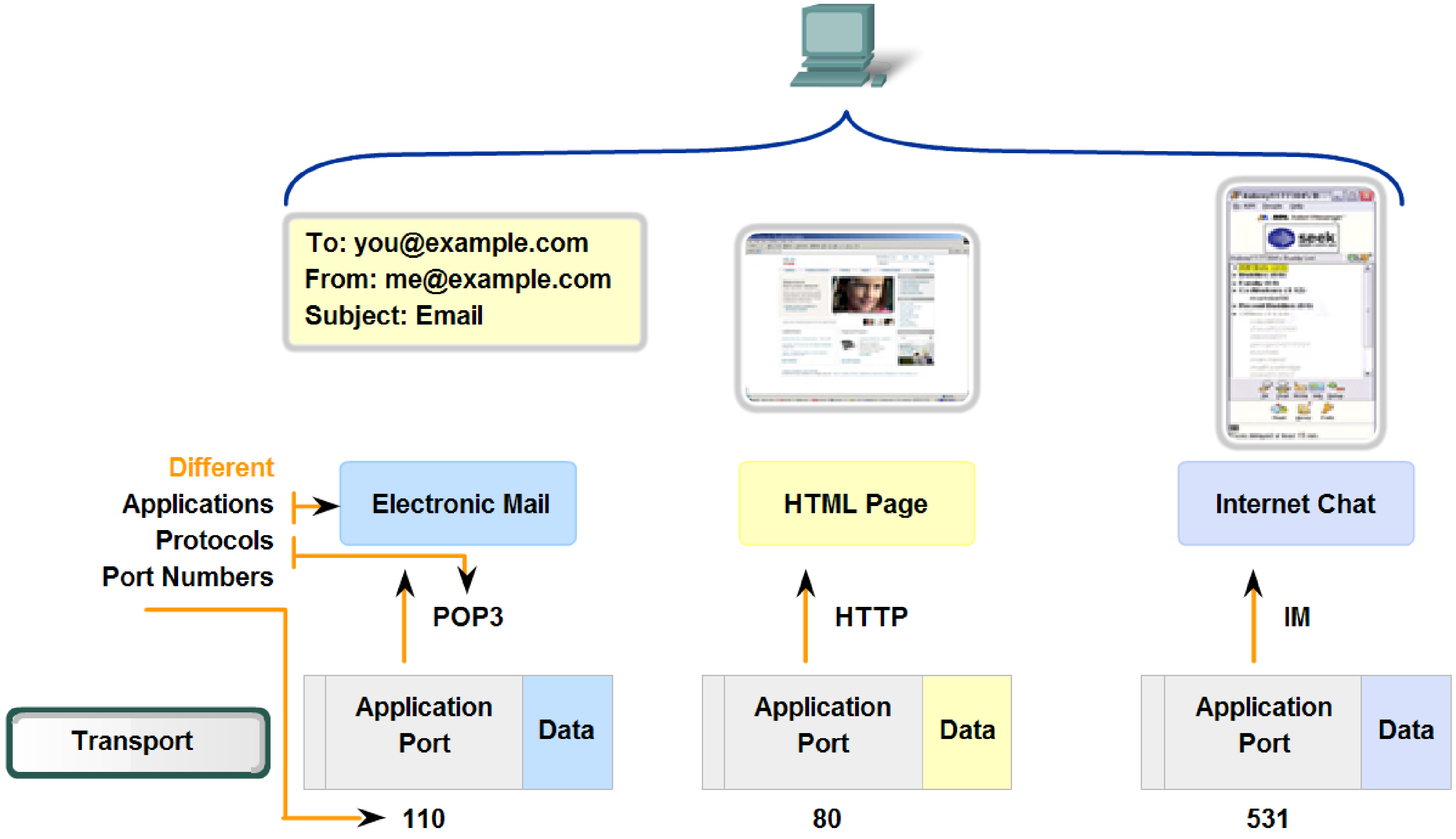


Bit (0) … Bit (15)	Bit (16) … Bit (31)
Source Port (16)	Destination Port (16)
Length (16)	Checksum (16)
Application Layer Data (Size varies)	

Identifying the Conversations

- To differentiate the segments and datagrams for each application, both TCP and UDP have header fields that can uniquely identify these applications. These unique identifiers are the **port numbers**.
- In the header of each segment or datagram, there is a **source** and **destination** port.
- Port numbers are assigned in various ways. While **server processes** have **static port** numbers assigned to them, **clients dynamically** choose a **port** number for each conversation
- The **combination** of the Transport layer **port number** and the Network layer **IP address** assigned to the host uniquely identifies a particular process running on a specific host device. This combination is called a **socket**.

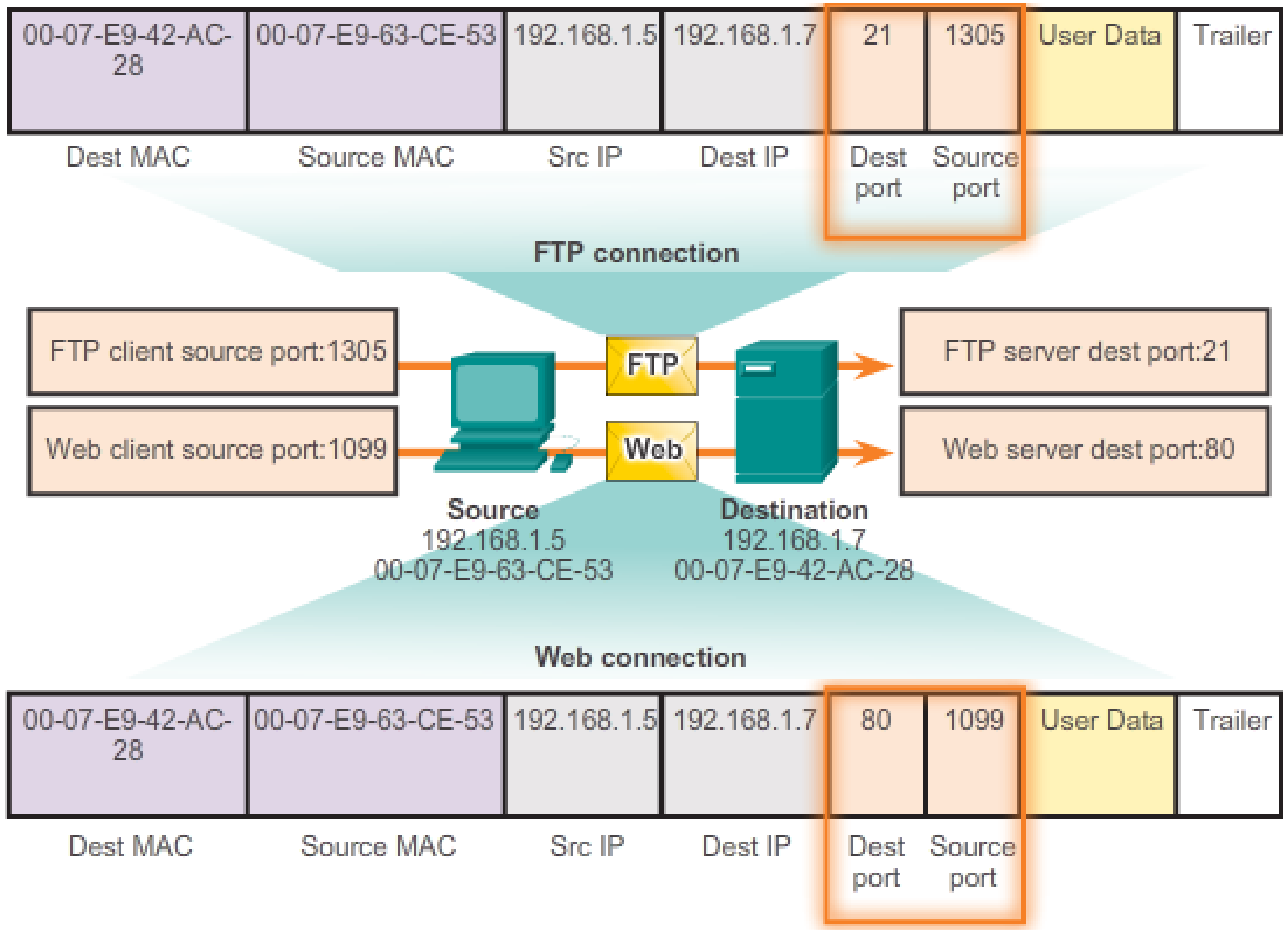
Identifying the Conversations with port numbers



To: you@example.com
From: me@example.com
Subject: Email

CONFIDENTIAL | © 2021 EPAM Systems, Inc.

TCP and UDP Port Addressing



Dest MAC	Source MAC	Src IP	Dest IP	Dest port	Source port		
00-07-E9-42-AC-28	00-07-E9-63-CE-53	192.168.1.5	192.168.1.7	21	1305	User Data	Trailer

FTP connection

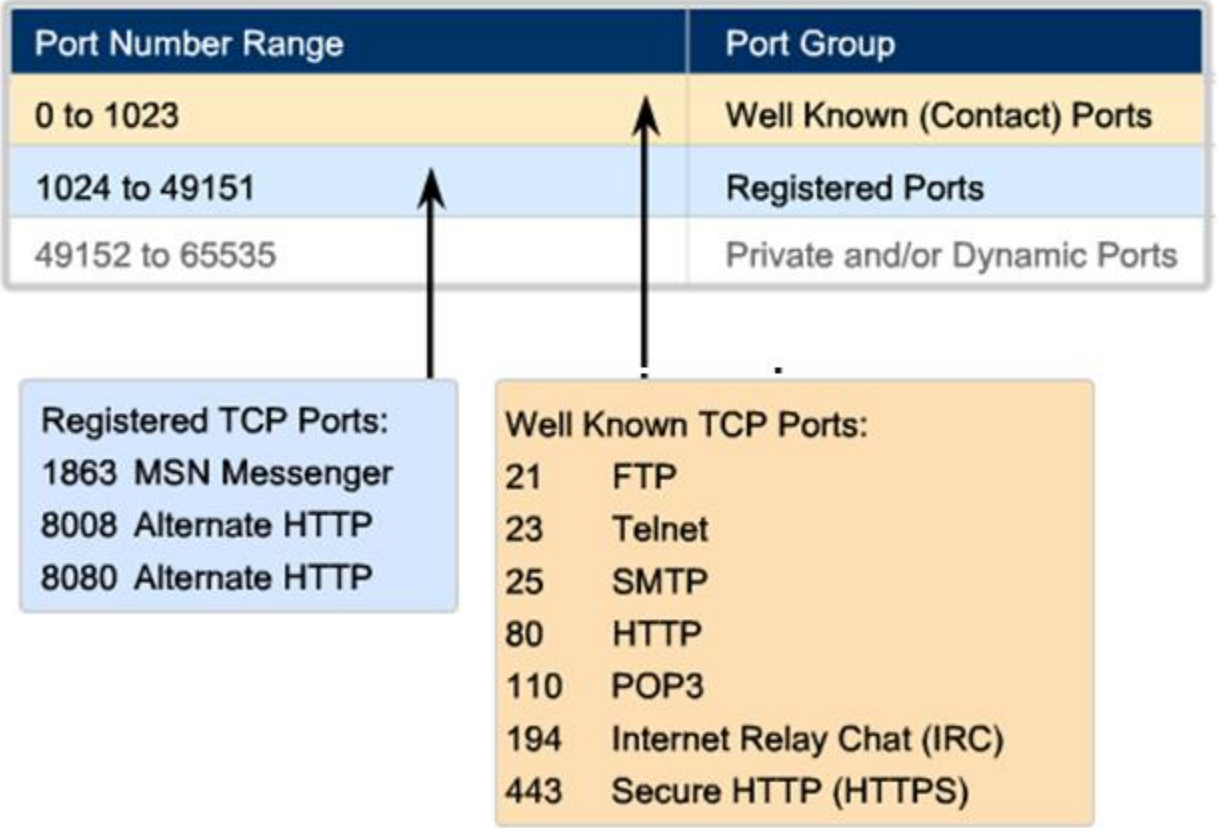
Web connection

Dest MAC	Source MAC	Src IP	Dest IP	Dest port	Source port		
00-07-E9-42-AC-28	00-07-E9-63-CE-53	192.168.1.5	192.168.1.7	80	1099	User Data	Trailer

CONFIDENTIAL | © 2021 EPAM Systems, Inc.

TCP and UDP Port addressing

- **Well-known Ports (Numbers 0 to 1023)** - These numbers are reserved for **services and applications**. They are commonly used for applications such as HTTP (web server), Internet Message Access Protocol (IMAP)/Simple Mail Transfer Protocol (SMTP) (email server) and Telnet.
- **Registered Ports (Numbers 1024 to 49151)** - These port numbers are assigned to user processes or applications. These processes are primarily **individual applications** that a user has chosen to install. When not used for a server resource, these ports may also be used dynamically selected by a client as its source port.
- **Dynamic or Private Ports (Numbers 49152 to 65535)** - Also known as ephemeral ports, these are usually assigned dynamically to client applications when the client initiates a connection to a service.



Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

Registered TCP Ports:

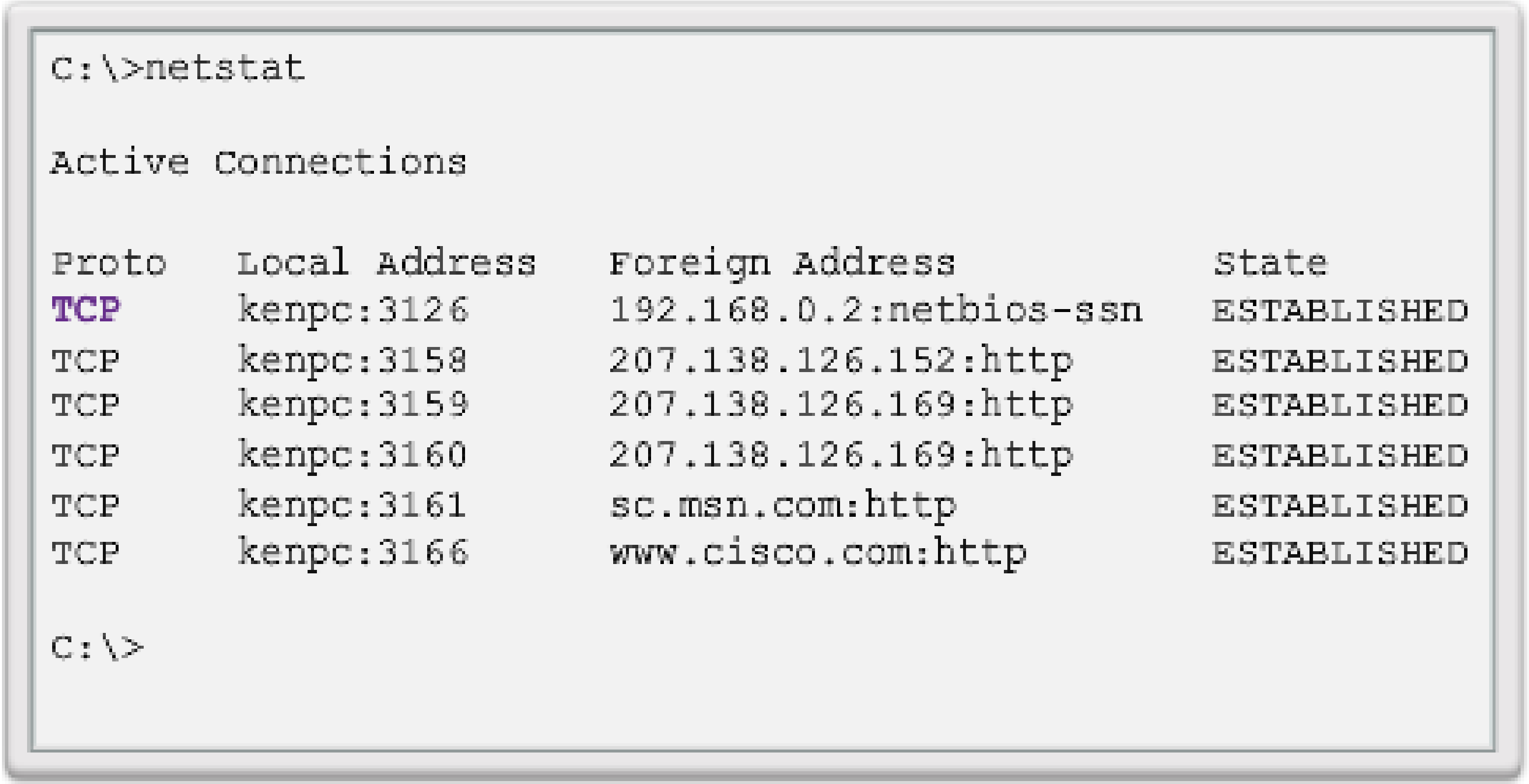
1863	MSN Messenger
8008	Alternate HTTP
8080	Alternate HTTP

Well Known TCP Ports:

21	FTP
23	Telnet
25	SMTP
80	HTTP
110	POP3
194	Internet Relay Chat (IRC)
443	Secure HTTP (HTTPS)

TCP and UDP Port Addressing

Netstat used to examine TCP connections that are open and running on a networked host



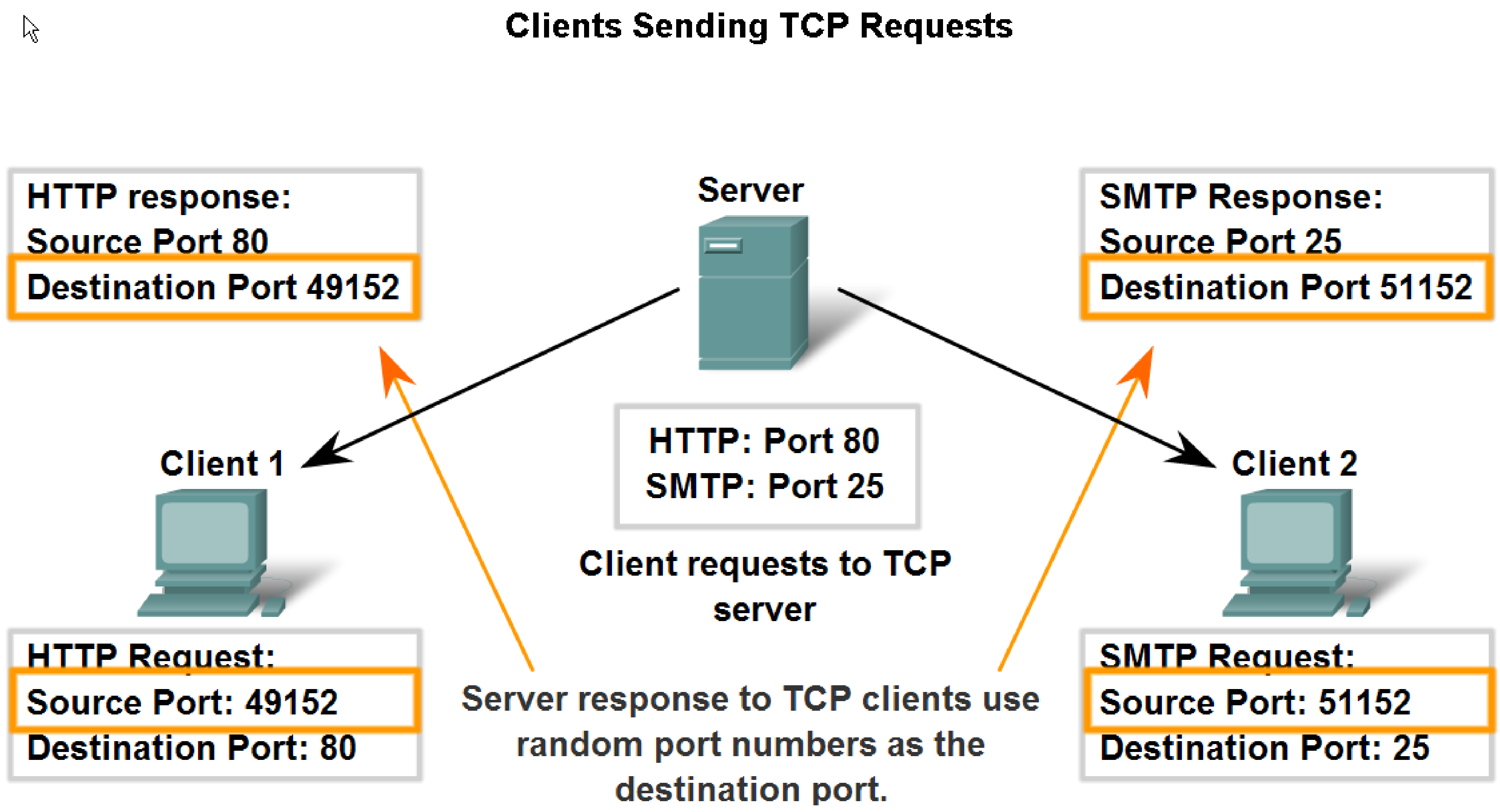
```
C:\>netstat

Active Connections

Proto   Local Address    Foreign Address             State
TCP     kenpc:3126       192.168.0.2:netbios-ssn     ESTABLISHED
TCP     kenpc:3158       207.138.126.152:http        ESTABLISHED
TCP     kenpc:3159       207.138.126.169:http        ESTABLISHED
TCP     kenpc:3160       207.138.126.169:http        ESTABLISHED
TCP     kenpc:3161       sc.msn.com:http             ESTABLISHED
TCP     kenpc:3166       www.cisco.com:http          ESTABLISHED

C:\>
```

Role of port numbers in establishing TCP sessions



Clients Sending TCP Requests

Server

HTTP: Port 80
SMTP: Port 25

Client requests to TCP server

Client 1

HTTP response:
Source Port 80
Destination Port 49152

HTTP Request:
Source Port: 49152
Destination Port: 80

Client 2

SMTP Response:
Source Port 25
Destination Port 51152

SMTP Request:
Source Port: 51152
Destination Port: 25

Server response to TCP clients use random port numbers as the destination port.

TCP Connection, Establishment and Termination

Three-Way Handshake

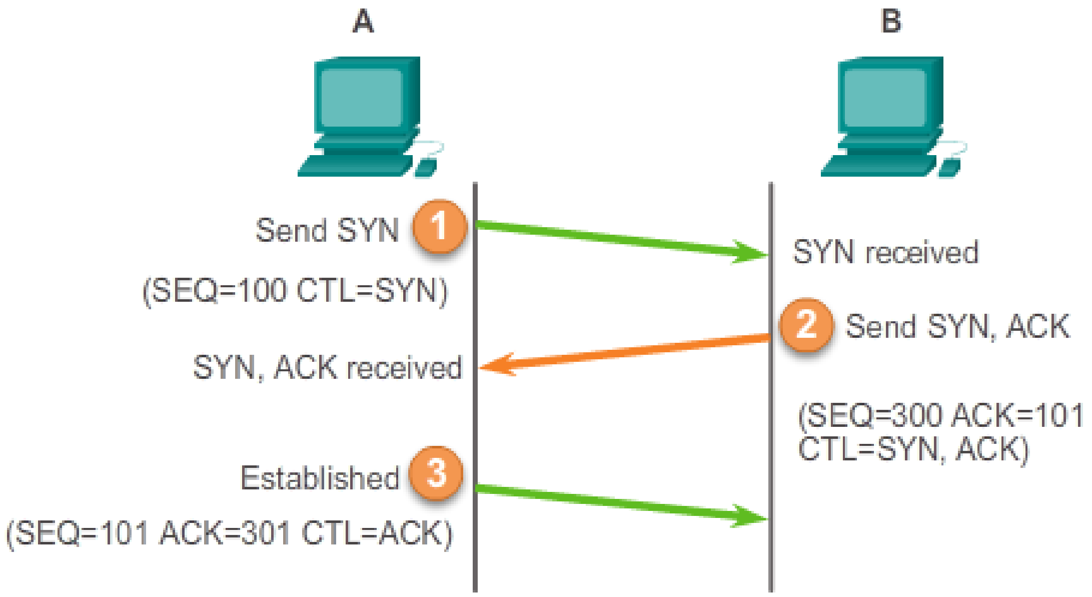
- Establishes that the destination device is present on the network.
- Verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use for the session.
- Informs the destination device that the source client intends to establish a communication session on that port number.

TCP Three-Way Handshake

Step 1: The initiating client requests a client-to-server communication session with the server.

Step 2: The server acknowledges the client-to-server communication session and requests a server-to-client communication session.

Step 3: The initiating client acknowledges the server-to-client communication session.



A

B

1 Send SYN

(SEQ=100 CTL=SYN)

SYN received

2 Send SYN, ACK

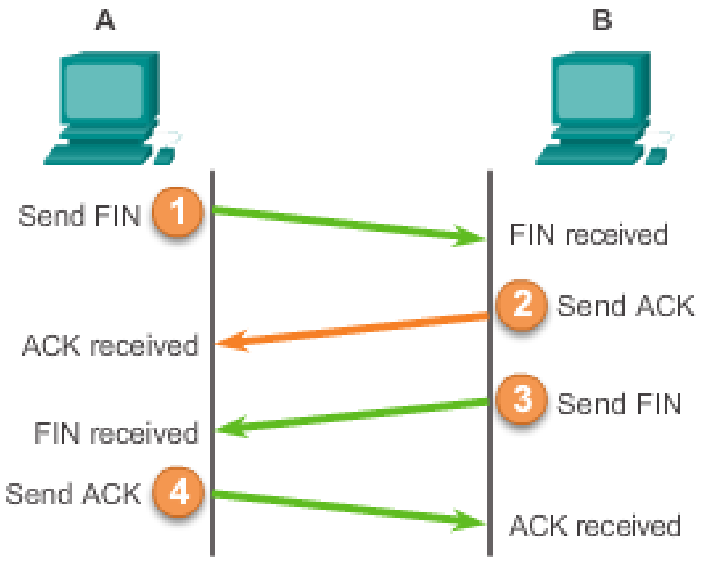
SYN, ACK received

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

3 Established

(SEQ=101 ACK=301 CTL=ACK)

CTL = Which control bits in the TCP header are set to 1
A sends ACK response to B.



A

B

Send FIN 1

FIN received

2 Send ACK

ACK received

3 Send FIN

FIN received

Send ACK 4

ACK received

A sends ACK response to B.

TCP segment header control information

URG - Urgent pointer field significant

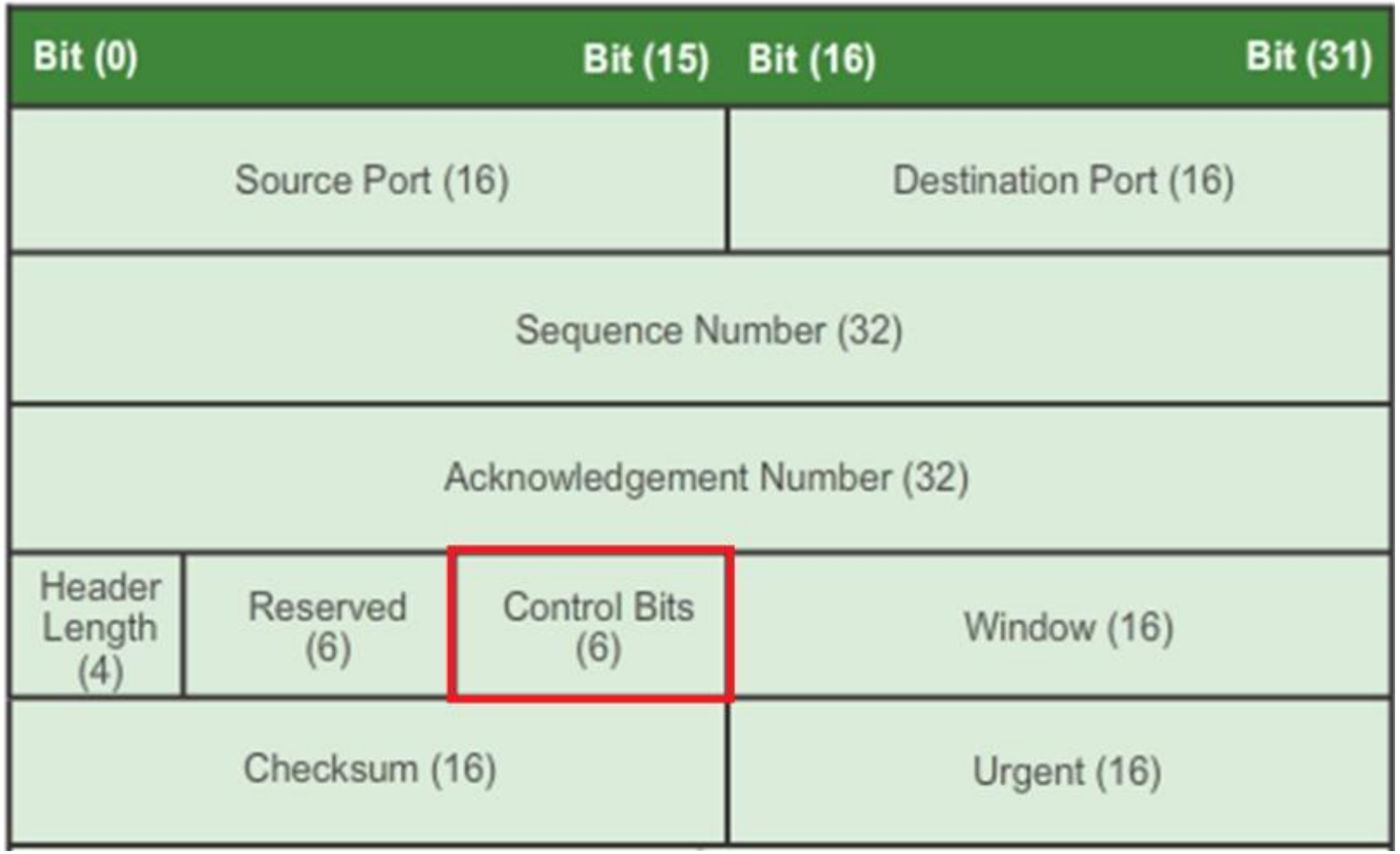
ACK - Acknowledgement field significant

PSH - Push function

RST - Reset the connection

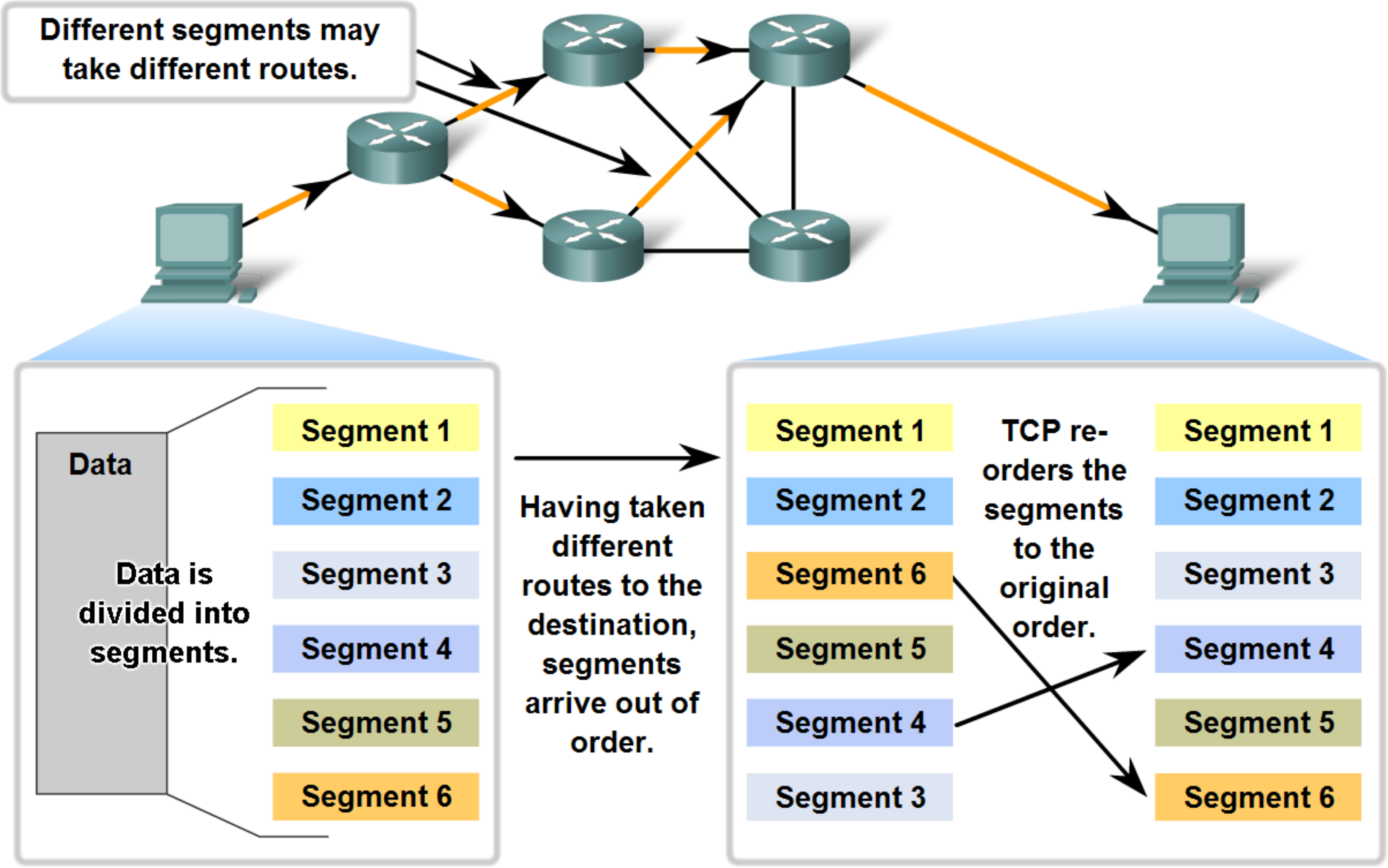
SYN - Synchronize sequence numbers

FIN - No more data from sender



Bit (0)		Bit (15)	Bit (16)	Bit (31)
Source Port (16)			Destination Port (16)	
Sequence Number (32)				
Acknowledgement Number (32)				
Header Length (4)	Reserved (6)	Control Bits (6)	Window (16)	
Checksum (16)			Urgent (16)	

Resequencing Segments to Order Transmitted



Different segments may take different routes.

Data

Data is divided into segments.

Segment 1
Segment 2
Segment 3
Segment 4
Segment 5
Segment 6

Having taken different routes to the destination, segments arrive out of order.

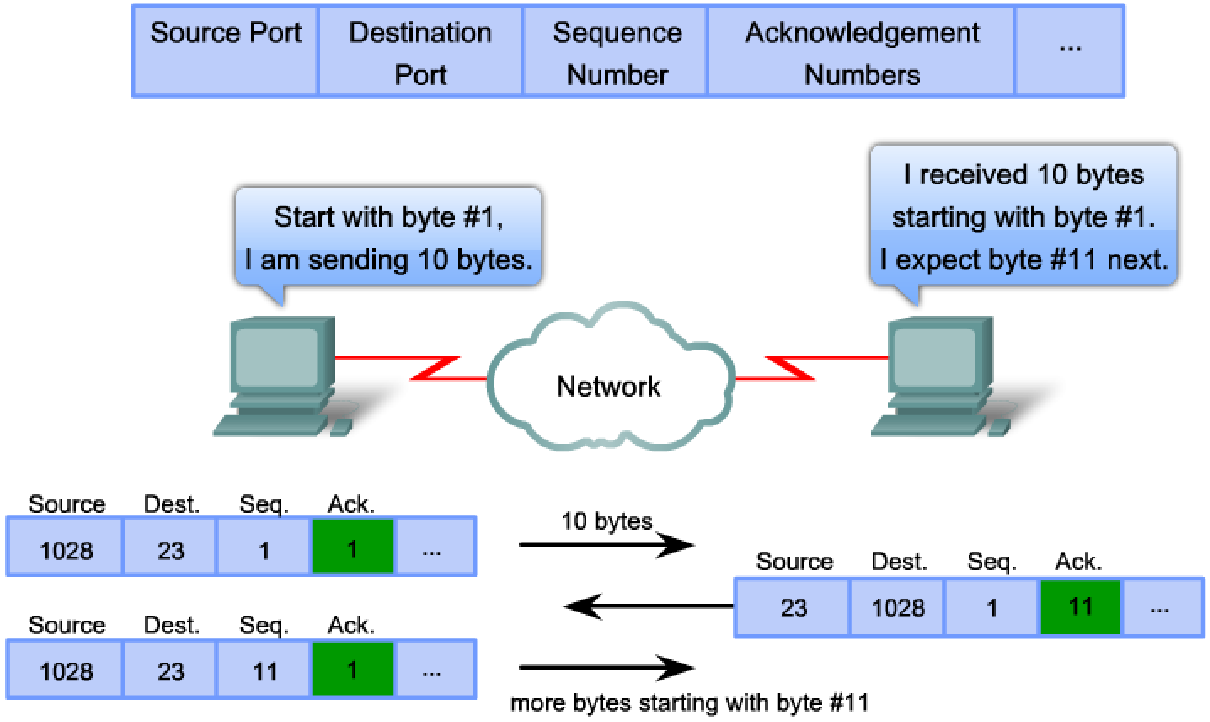
Segment 1
Segment 2
Segment 6
Segment 5
Segment 4
Segment 3

TCP re-orders the segments to the original order.

Segment 1
Segment 2
Segment 3
Segment 4
Segment 5
Segment 6

Managing TCP Sessions

Expectational acknowledgement



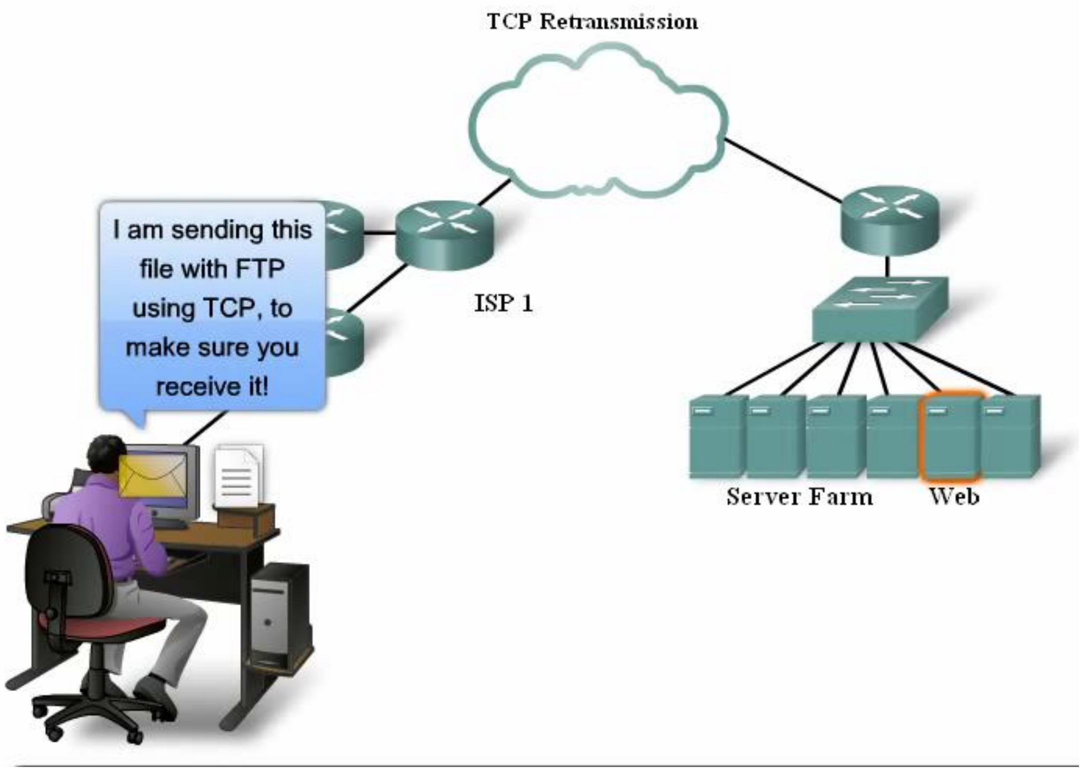
Source Port	Destination Port	Sequence Number	Acknowledgement Numbers	...

Source	Dest.	Seq.	Ack.	
1028	23	1	1	...

Source	Dest.	Seq.	Ack.	
23	1028	1	11	...

Source	Dest.	Seq.	Ack.	
1028	23	11	1	...

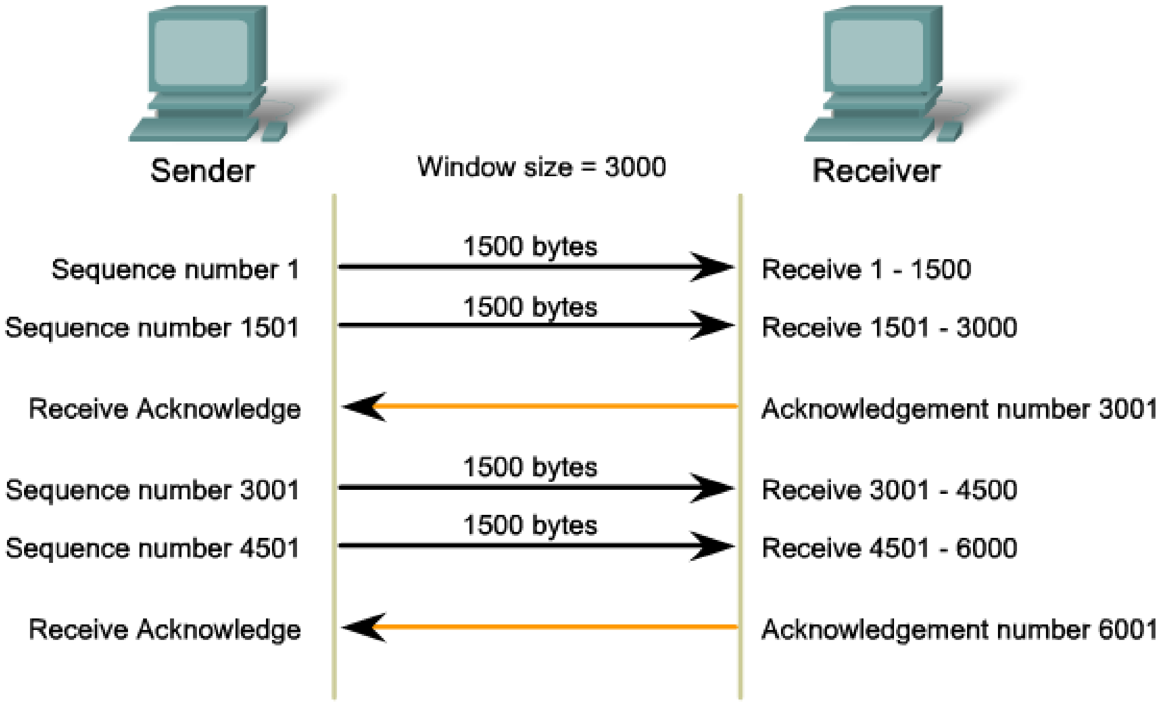
TCP **Retransmission**



TCP Retransmission
I am sending this file with FTP using TCP, to make sure you receive it!
ISP 1
Server Farm
Web

epam CONFIDENTIAL | © 2021 EPAM Systems, Inc.

TCP Flow Control



Sender

Window size = 3000

Receiver

Sequence number 1 — 1500 bytes → Receive 1 - 1500

Sequence number 1501 — 1500 bytes → Receive 1501 - 3000

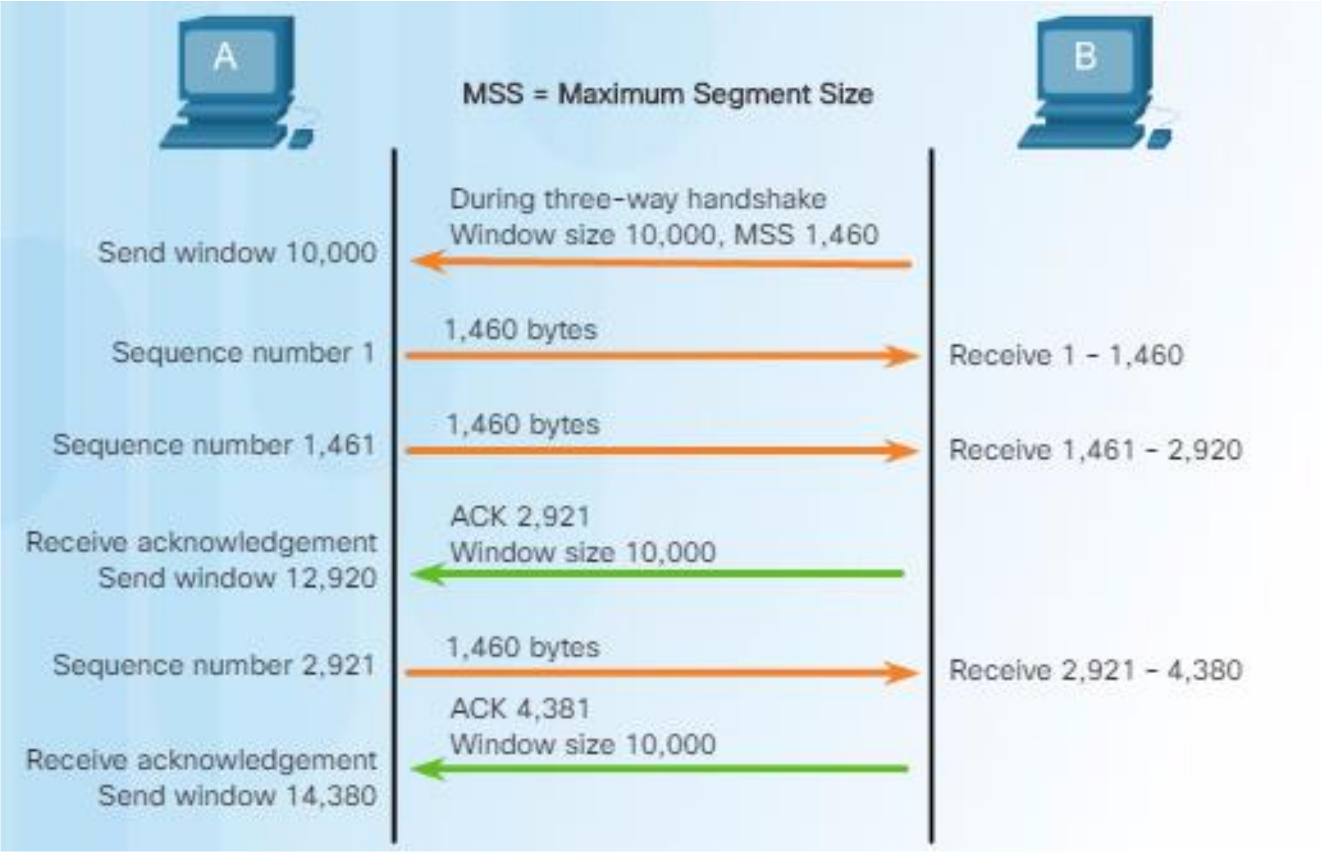
Receive Acknowledge ← Acknowledgement number 3001

Sequence number 3001 — 1500 bytes → Receive 3001 - 4500

Sequence number 4501 — 1500 bytes → Receive 4501 - 6000

Receive Acknowledge ← Acknowledgement number 6001

The window size determines the number of bytes sent before an acknowledgment is expected.



A

MSS = Maximum Segment Size

B

Send window 10,000 ← During three-way handshake Window size 10,000, MSS 1,460

Sequence number 1 — 1,460 bytes → Receive 1 - 1,460

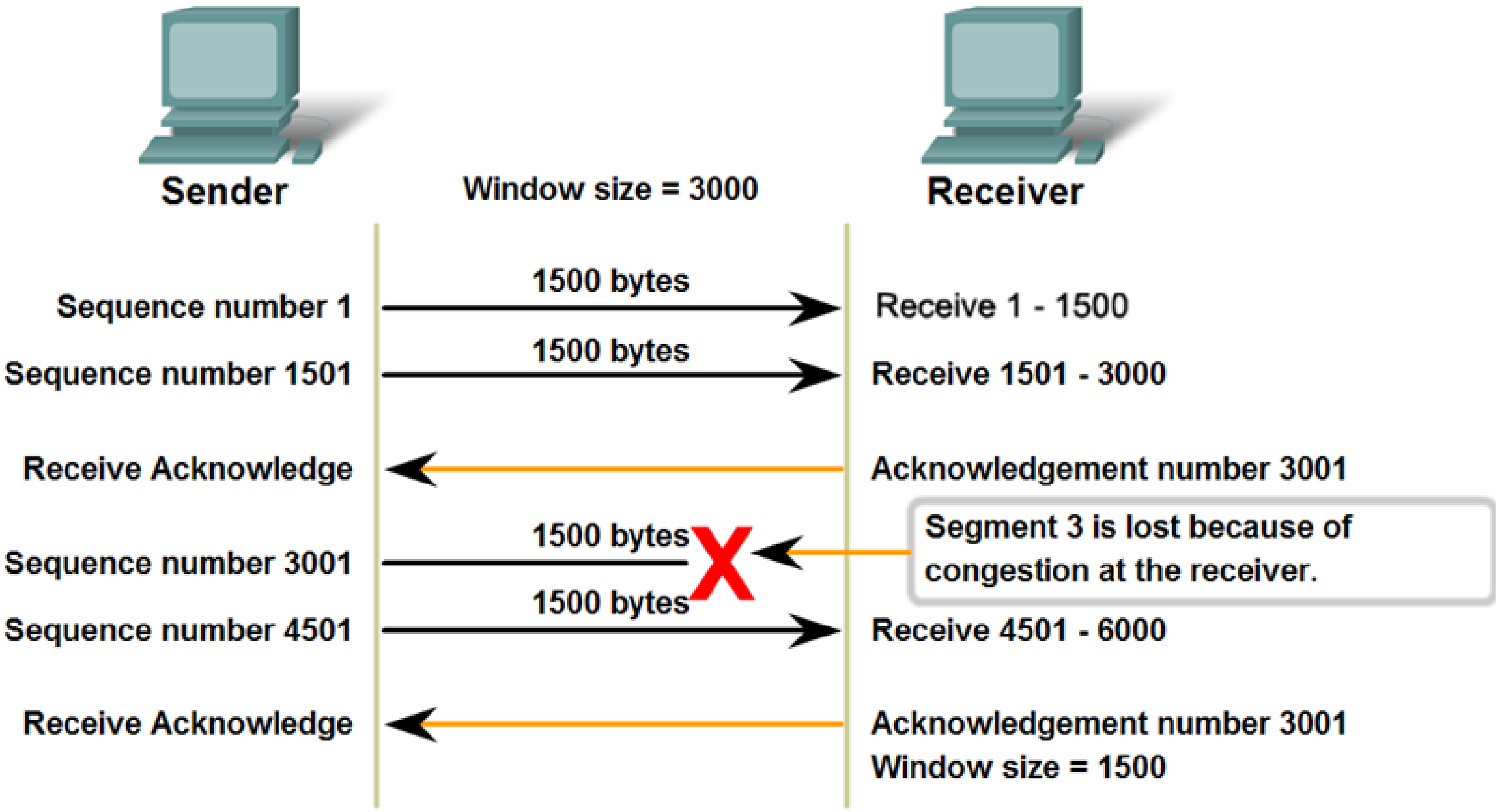
Sequence number 1,461 — 1,460 bytes → Receive 1,461 - 2,920

Receive acknowledgement Send window 12,920 ← ACK 2,921 Window size 10,000

Sequence number 2,921 — 1,460 bytes → Receive 2,921 - 4,380

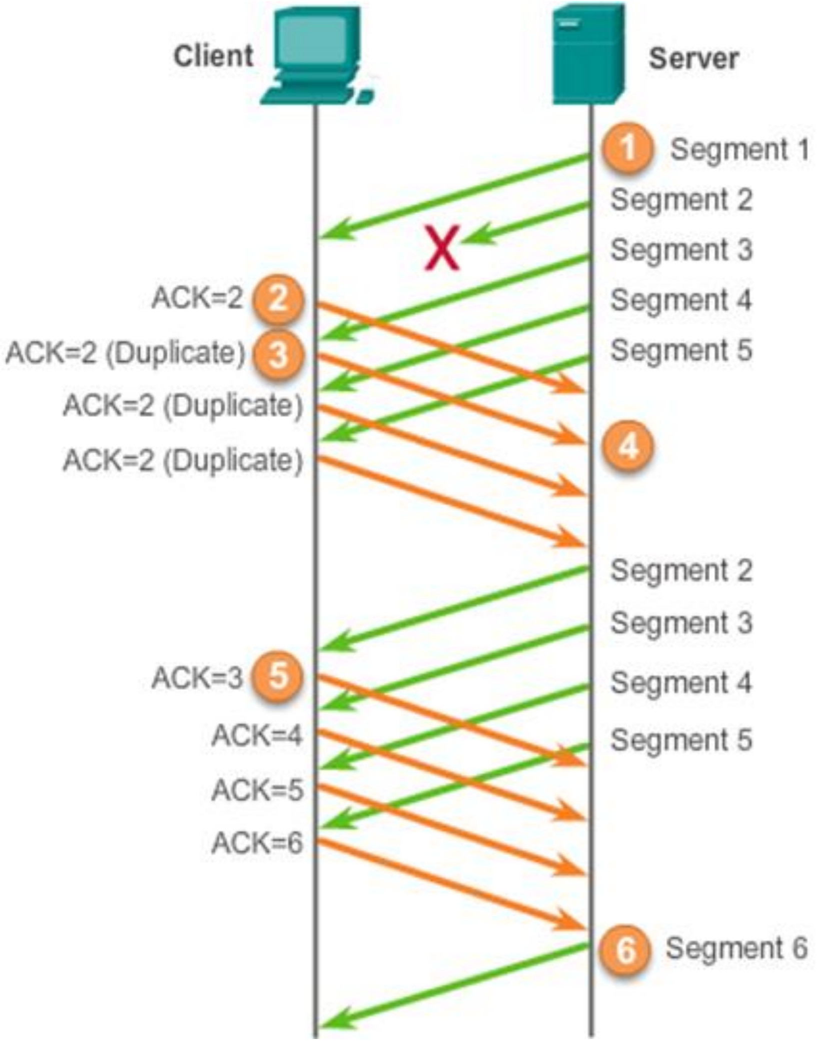
Receive acknowledgement Send window 14,380 ← ACK 4,381 Window size 10,000

Segment lost TCP reaction



Segment 3 is lost because of congestion at the receiver.

If segments are lost because of congestion, the Receiver will acknowledge the last received sequential segment and reply with a reduced window size.



Q&A

Thank you!