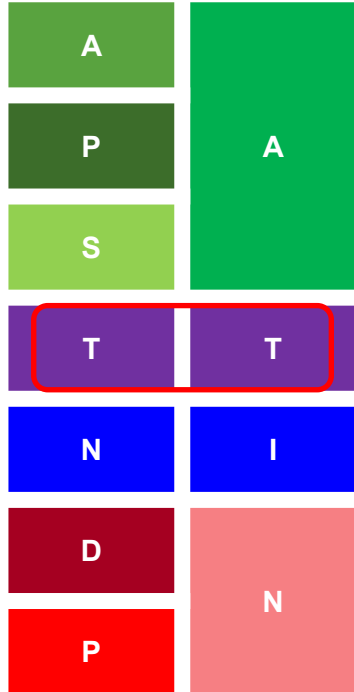


TNE20003 - Internet and Cybersecurity for Engineering Applications

Transport Layer Services



What happens at the Transport Layer?????



Topic Title	Topic Objective
The Client Server Relationship	Explain client and server interaction.
TCP and UDP	Compare TCP and UDP transport layer functions.
Port Numbers	Explain how TCP and UDP use port numbers.

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

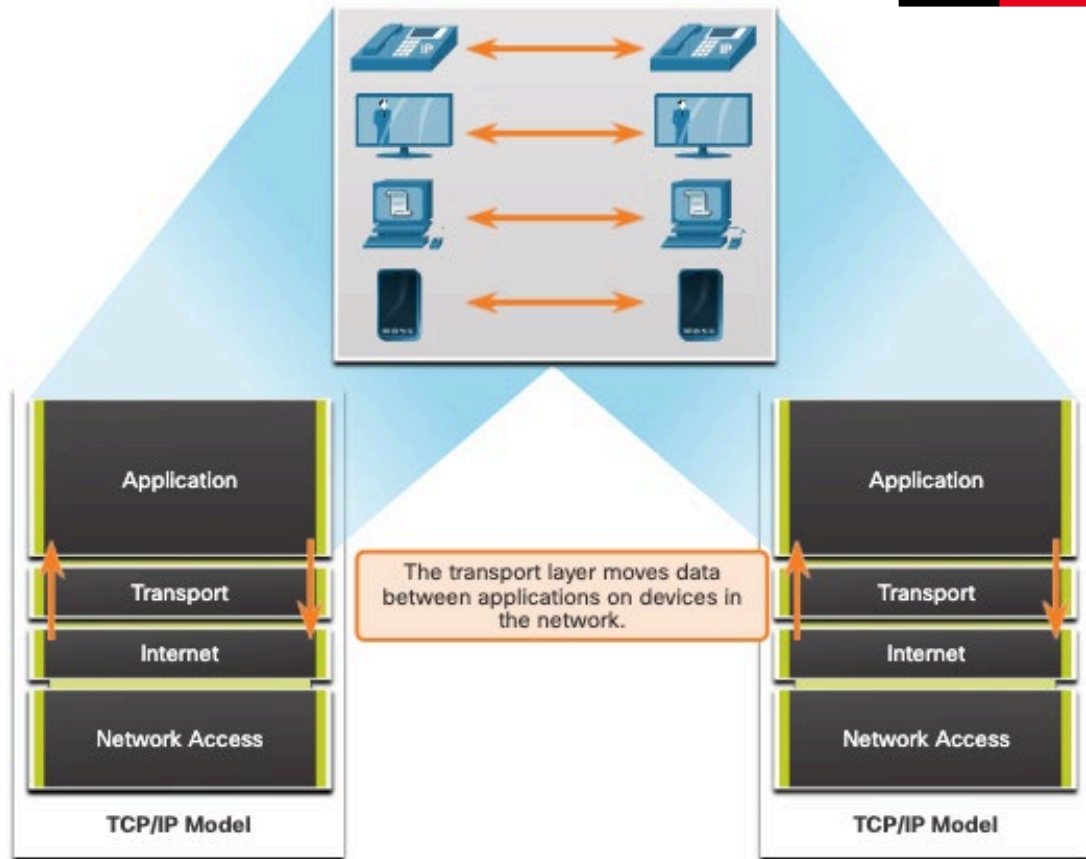
- Tracking the individual communication between applications on the source and destination hosts
- Segmenting data for manageability and reassembling segmented data into streams of application data at the destination
- Identifying the proper application for each communication stream

Transportation of Data

Role of the Transport Layer

The transport layer is:

- responsible for logical communications between applications running on different hosts.
- The link between the application layer and the lower layers that are responsible for network transmission.



Transportation of Data

Transport Layer Responsibilities

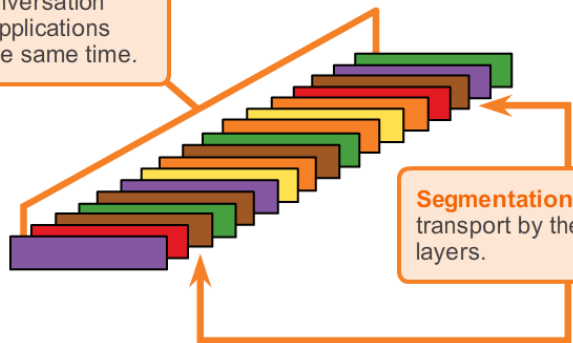
The transport layer has the following responsibilities:

- Tracking individual conversations
- Segmenting data and reassembling segments
- Adds header information
- Identify, separate, and manage multiple conversations
- Uses segmentation and multiplexing to enable different communication conversations to be interleaved on the same network

Transport Layer Services



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



Segmentation facilitates data transport 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.

The Client Server Relationship

The Client Server Relationship

Client and Server Interaction

- We use network services available over networks and the internet to communicate with others and to perform routine tasks
- A server is a host running a software application (or server service) that provides services to other hosts (clients)
- There are millions of servers on the internet. Clients and servers interact following agreed standards and protocols

Type	Description
Email	The email server runs email server software. Clients use mail client software, such as Microsoft Outlook, to access email on the server.
Web	The web server runs web server software. Clients use browser software, such as Windows Internet Explorer, to access web pages on the server.
File	The file server stores corporate and user files in a central location. The client devices access these files with client software such as the Windows File Explorer.

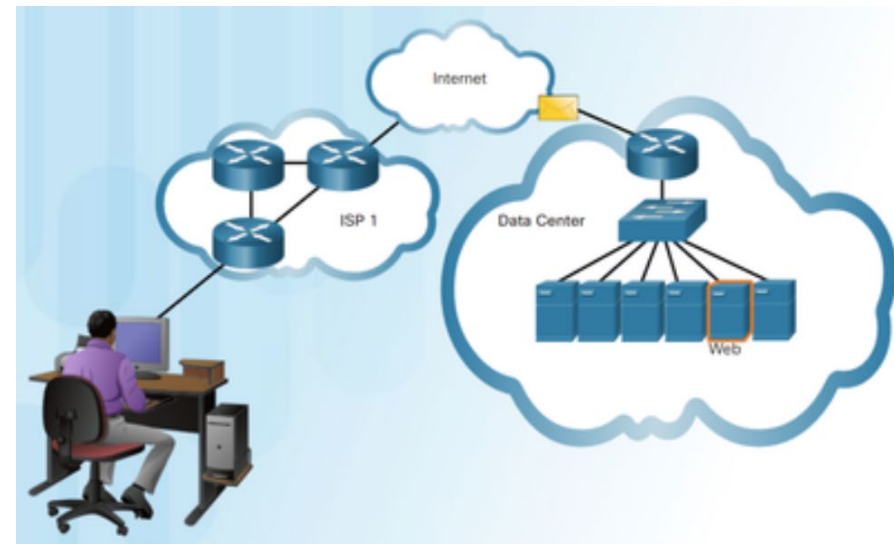
The Client Server Relationship

Client Requests a Web Page

A client/server system is illustrated by the interaction between a web client and a web server:

1. A person uses a web browser to access a web server by sending a request, for example, requesting a web page.
2. The server receives the request and responds by sending the requested web page back to the client.

A web server is usually in a part of the network with other servers called a server farm, or within a data center.



The Client Server Relationship

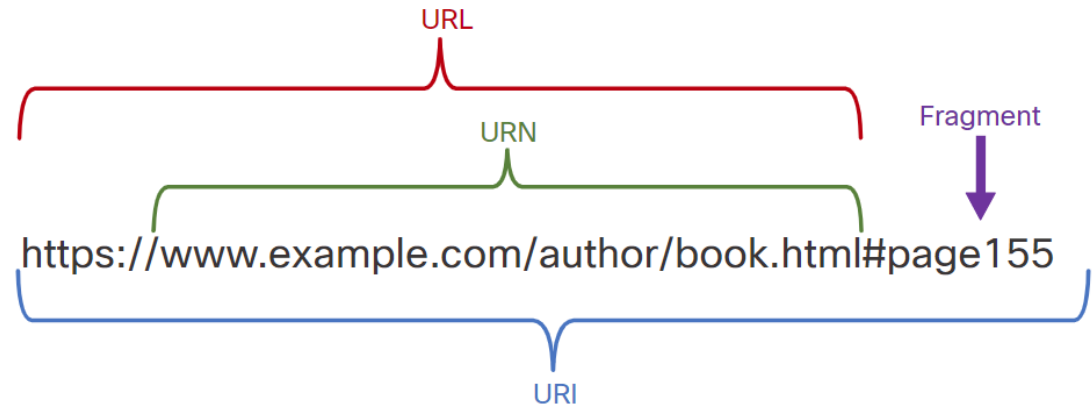
URI, URN, and URL

Uniform Resource Name - identifies only the namespace of the resource without reference to the protocol

Uniform Resource Locator - defines the network location of a specific resource on the network.

Components in the example URL:

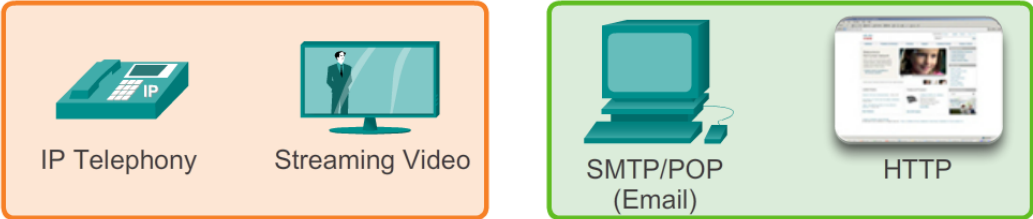
- **Protocol/scheme** - HTTPS or other protocols such as FTP, SFTP, mailto, and NTP
- **Hostname** - www.example.com
- **Path and file name** - /author/book.html
- **Fragment** - #page155



TCP and UDP

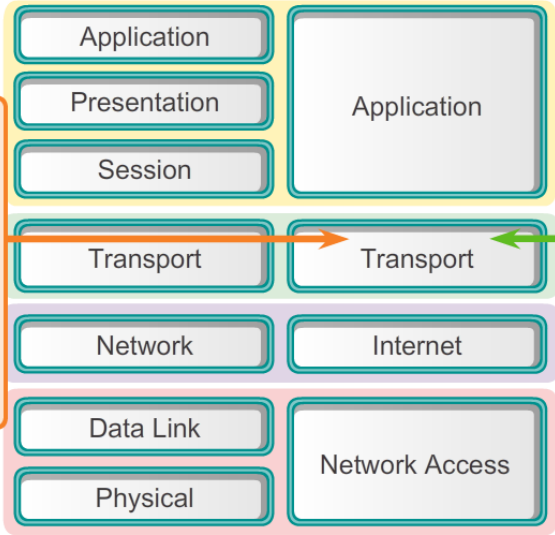
Transportation of Data

Transport Layer Reliability



OSI Model

TCP/IP Model



UDP

- Required protocol properties:
- Fast
 - Low overhead
 - Does not require acknowledgements
 - Does not resend lost data
 - Delivers data as it arrives

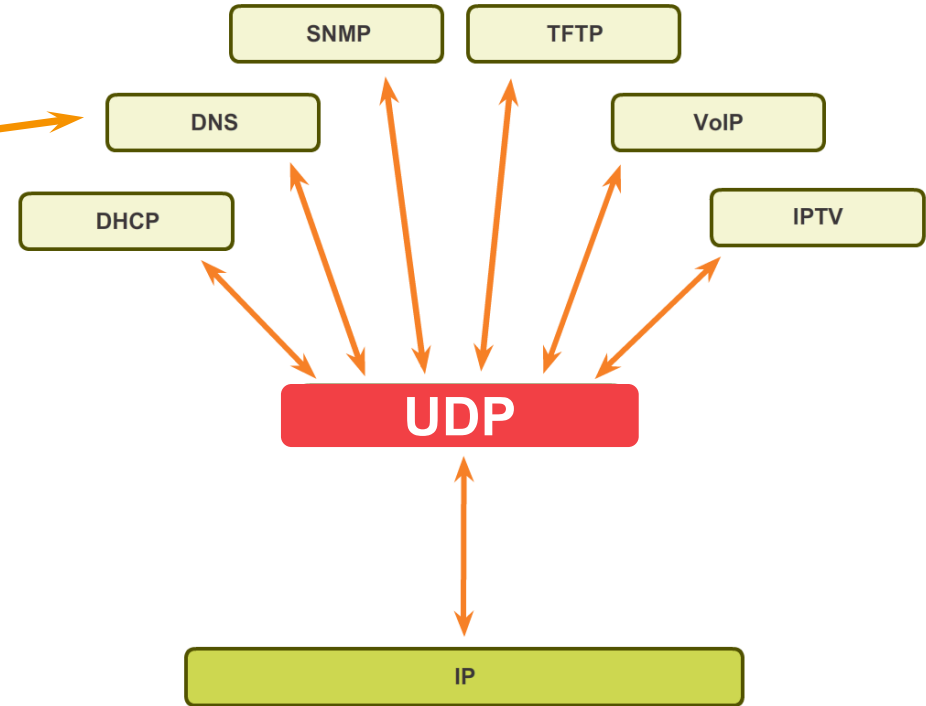
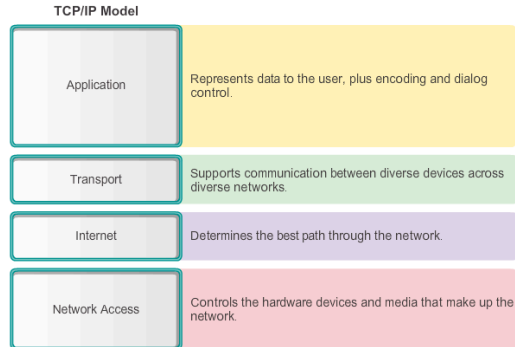
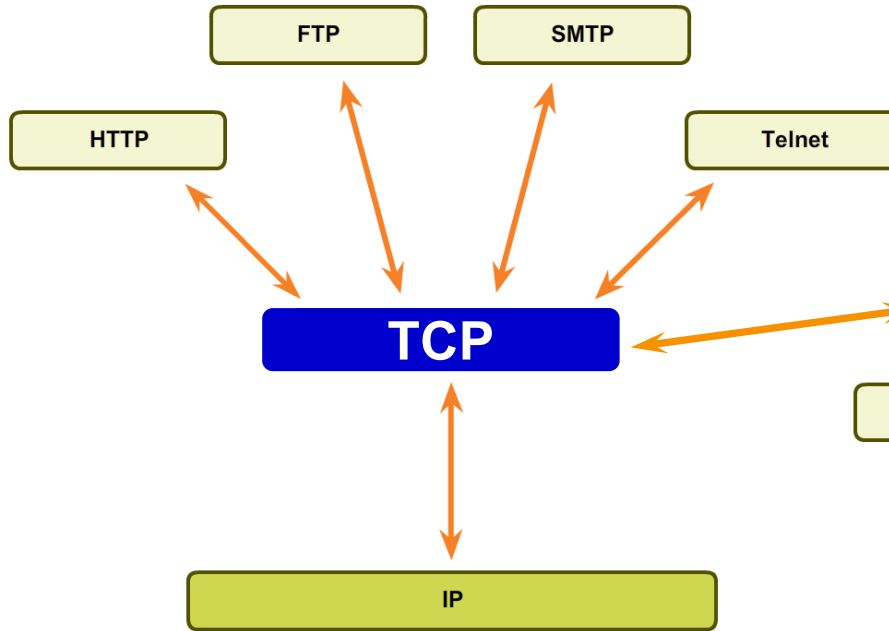
TCP

- Required protocol properties:
- Reliable
 - Acknowledge data
 - Resends lost data
 - Delivers data in order sent

Application developers choose the appropriate transport layer protocol based on the nature of the application.

Transportation of Data

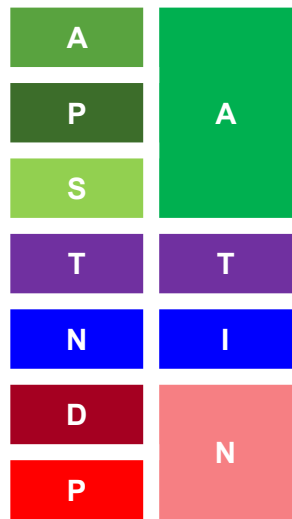
Common Applications



TCP and UDP

Protocol Operations

A web server and a web client use specific protocols and standards in the process of exchanging information to ensure that the messages are received and understood. The various protocols necessary to deliver a web page function at the four different layers of the TCP/IP model are as follows:



- **Application Layer Protocol** - Hypertext Transfer Protocol (HTTP) governs the way that a web server and a web client interact.
- **Transport Layer Protocol** - Transmission Control Protocol (TCP) ensures that IP packets are sent reliably, and any missing packets are resent.
- **Internetwork Layer Protocol** - The most common internetwork protocol is Internet Protocol (IP) which is used to identify end hosts and to route packets to destination host.
- **Network Access Layer** - The specific protocol at the network access layer, such as Ethernet, depends on the type of media and transmission methods used in the physical network.

Port Numbers

Port Numbers

Multiple Separate Communications

TCP and UDP transport layer protocols use port numbers to manage multiple, simultaneous conversations.

The source port number is associated with the originating application on the local host whereas the destination port number is associated with the destination application on the remote host.

Source Port (16)

Destination Port (16)



TCP and UDP Port Numbering

Port Number Range	Port Group
0 to 1023	Well-known Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

Registered TCP Ports:

1863	MSN Messenger
2000	Cisco SCCP (VoIP)
8008	Alternate HTTP
8080	Alternate HTTP

Registered UDP Ports:

1812	RADIUS Authentication Protocol
5004	RTP (Voice and Video Transport Protocol)
5040	SIP (VoIP)

Registered TCP/UDP Common Ports:

1433	MS SQL
2948	WAP (MMS)

Well-known TCP Ports:

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

Well-known UDP Ports:

69	TFTP
520	RIP

Well-known TCP/UDP Common Ports:

53	DNS
161	SNMP
531	AOL Instant Messenger, IRC

Port Numbers

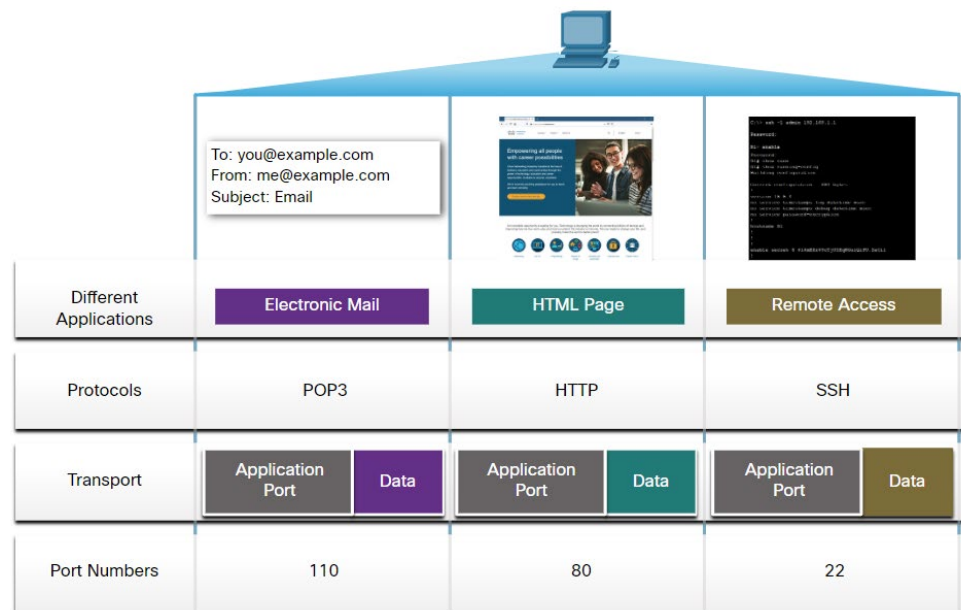
Destination and Source Port Numbers

The source port number is associated with the originating application on the local sending host.

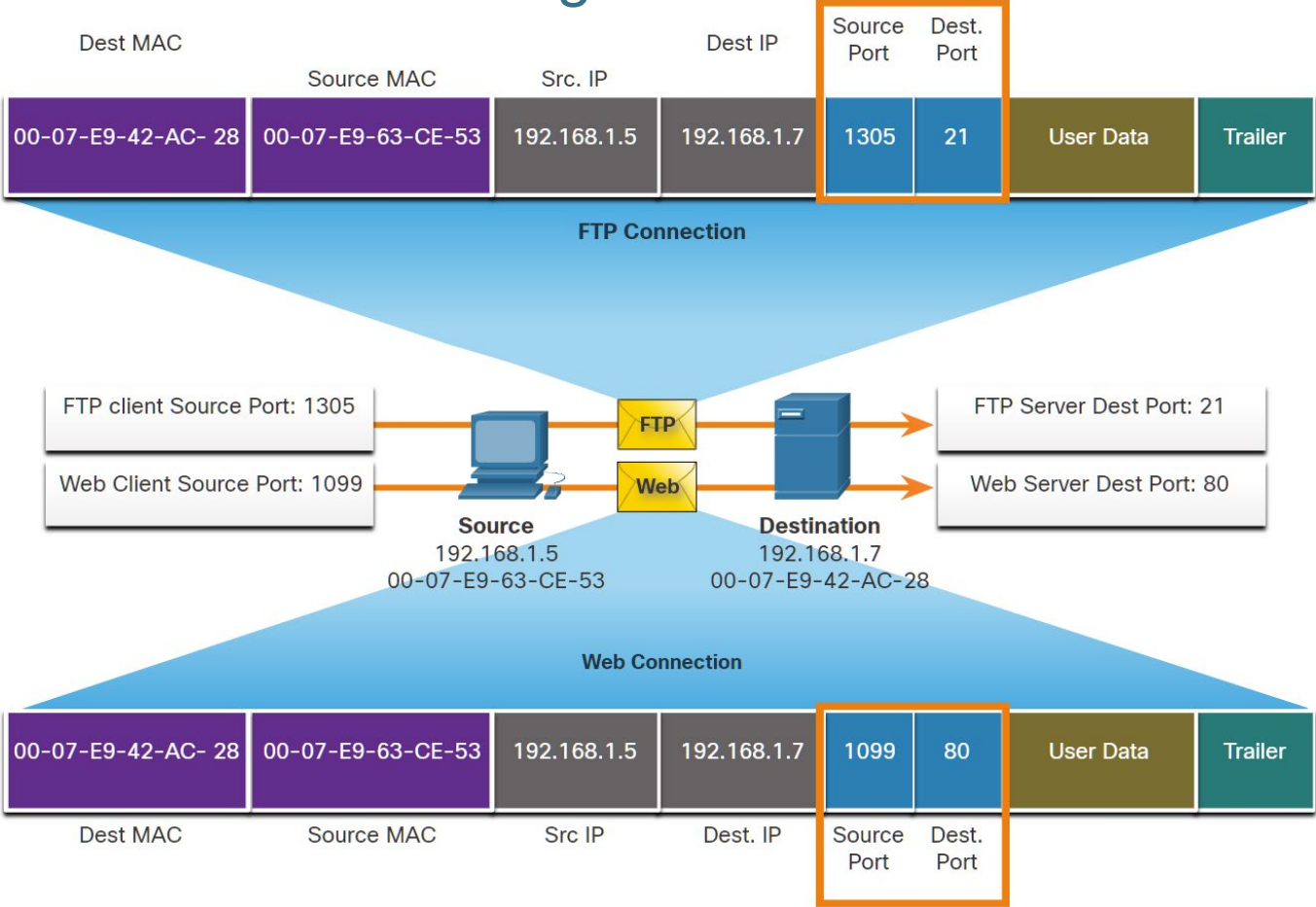
The destination port number is associated with the destination application on the remote host.

Source Port - dynamically generated by the sending device to identify a conversation between two devices. This process allows multiple conversations to occur simultaneously.

Destination Port - The client places a destination port number in the segment to tell the destination server what service is being requested. The server responds to the request and sends information back to the sending device using the source port.



TCP and UDP Port Addressing



TCP and UDP Port Addressing (Cont.)

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

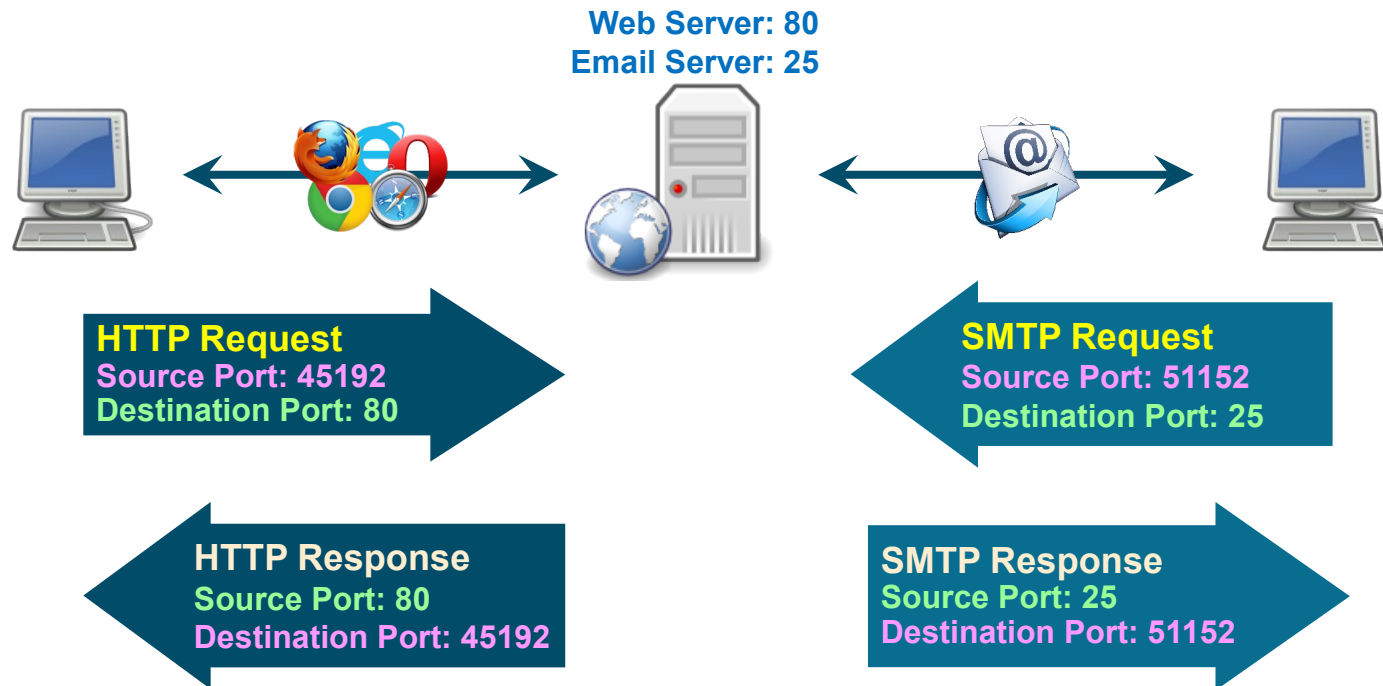


```
C:\> netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	192.168.1.124:3126	192.168.0.2:netbios-ssn	ESTABLISHED
TCP	192.168.1.124:3158	207.138.126.152:http	ESTABLISHED
TCP	192.168.1.124:3159	207.138.126.169:http	ESTABLISHED
TCP	192.168.1.124:3160	207.138.126.169:http	ESTABLISHED
TCP	192.168.1.124:3161	sc.msn.com:http	ESTABLISHED
TCP	192.168.1.124:3166	www.cisco.com:http	ESTABLISHED

TCP Server Processes



Transport Layer Role and Services

TCP SEGMENT & HEADER FIELDS

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) Code Bits (6)		Window (16)		
Checksum (16)		Urgent (16)		
Options (0 or 32 if any)				
APPLICATION LAYER DATA SEGMENT (Size varies)				

↑
20
Bytes
↓

*What does
TCP have
that UDP
does not ?*

UDP SEGMENT & HEADER FIELDS

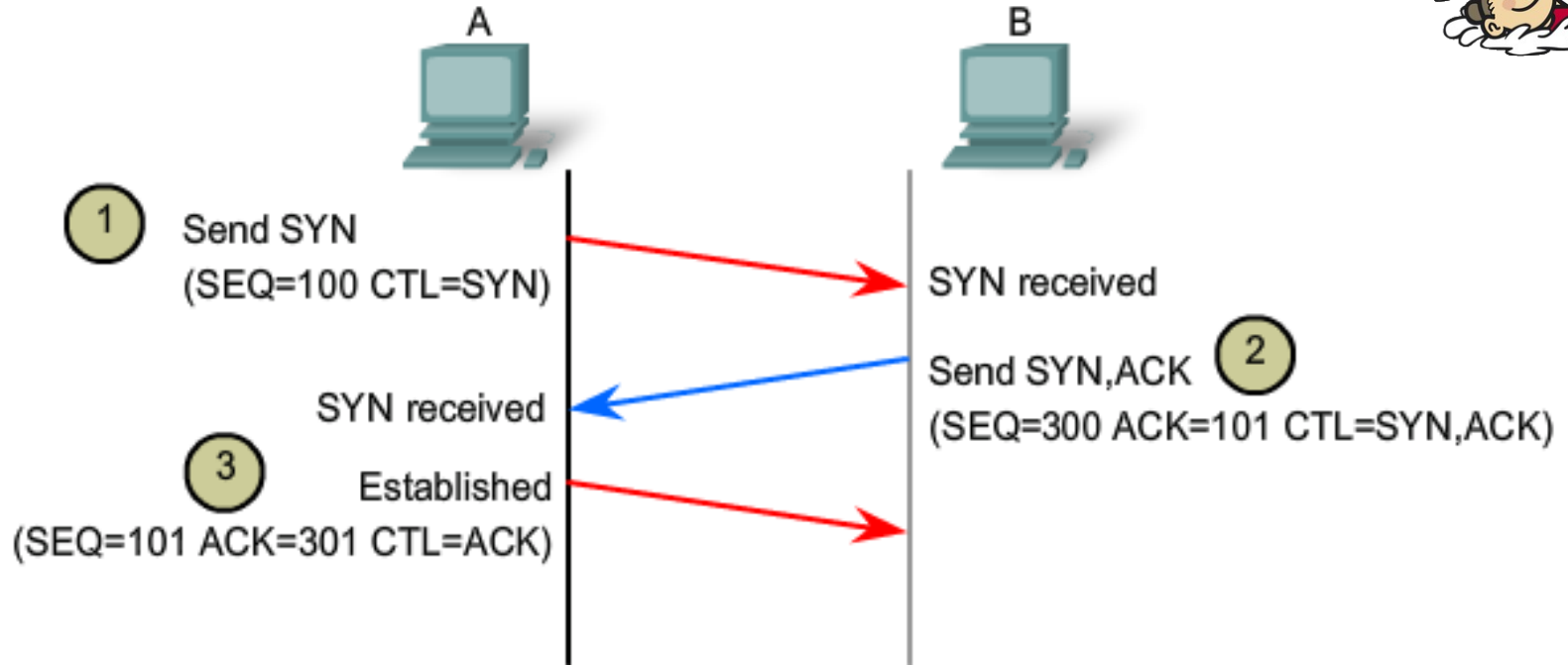
Bit (0)		Bit (15) Bit (16)		Bit (31)	
Source Port (16)			Destination Port (16)		
Length (16)			Checksum (16)		
APPLICATION LAYER DATA SEGMENT (Size varies)					

↑
8
Bytes
↓

Three Way Handshake



TCP Connection Establishment

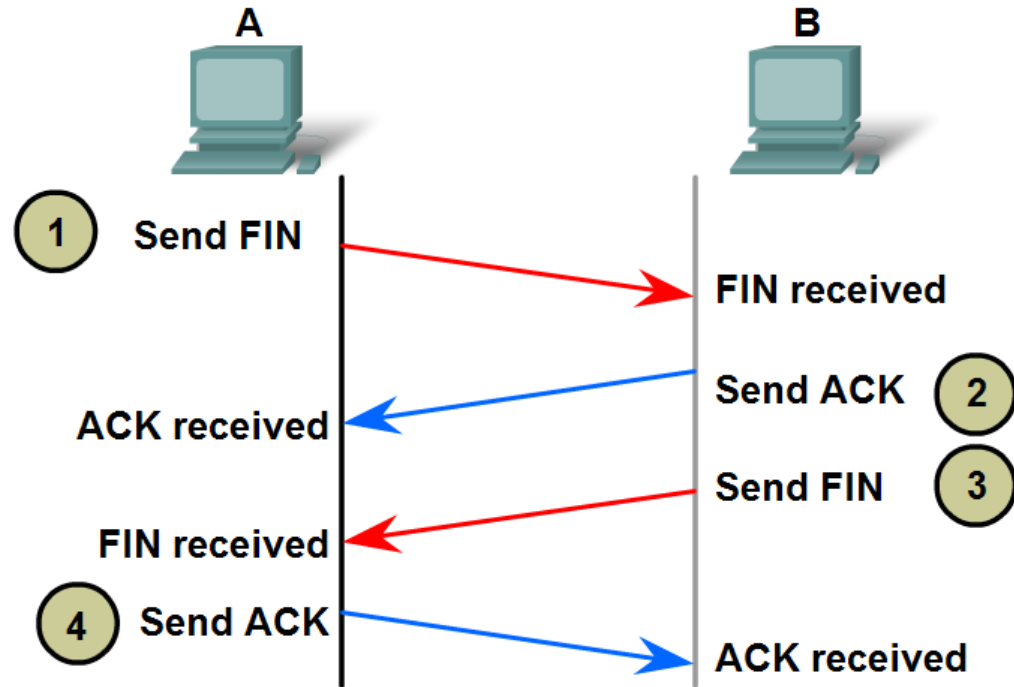


CTL = Which control bits in the TCP header are set to 1

Three Way Handshake



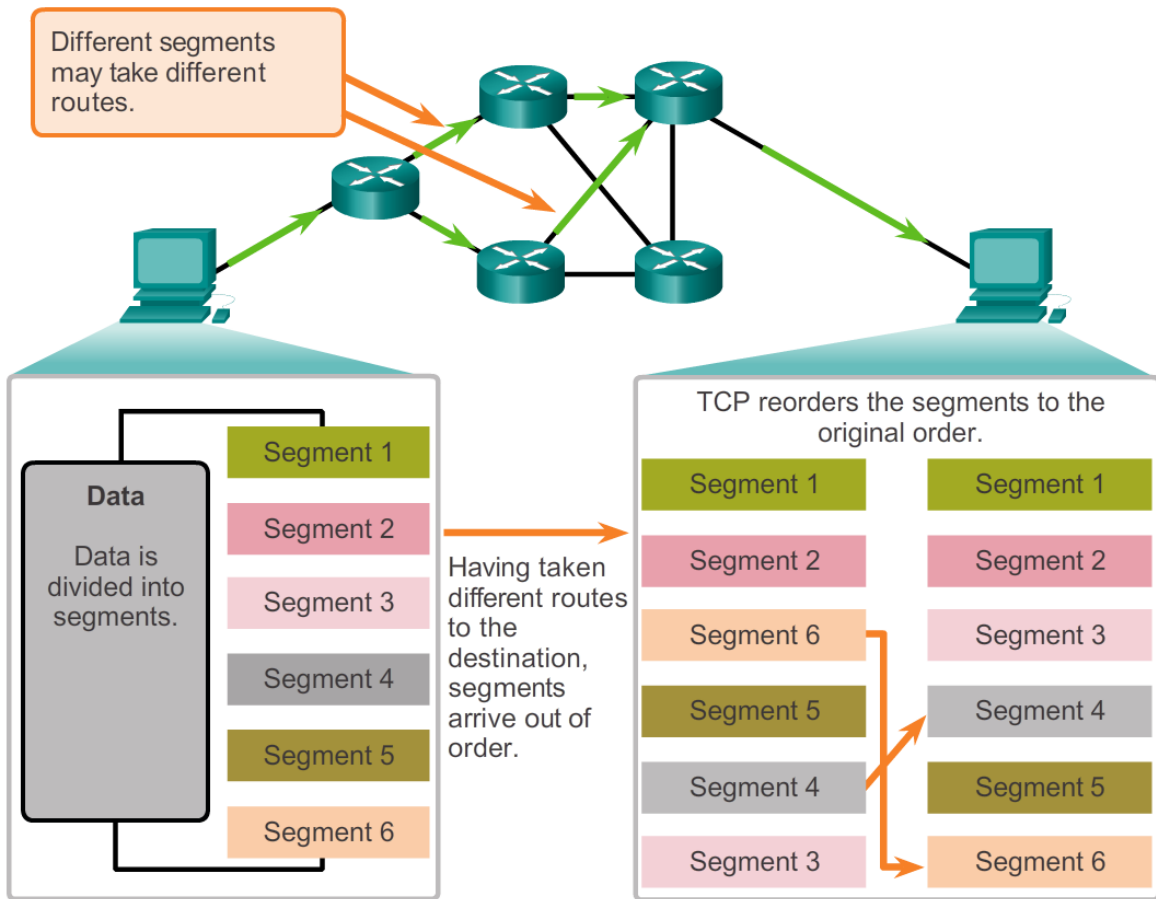
TCP Connection Termination



Reliability and Flow Control

TCP Reliability: Ordered Delivery

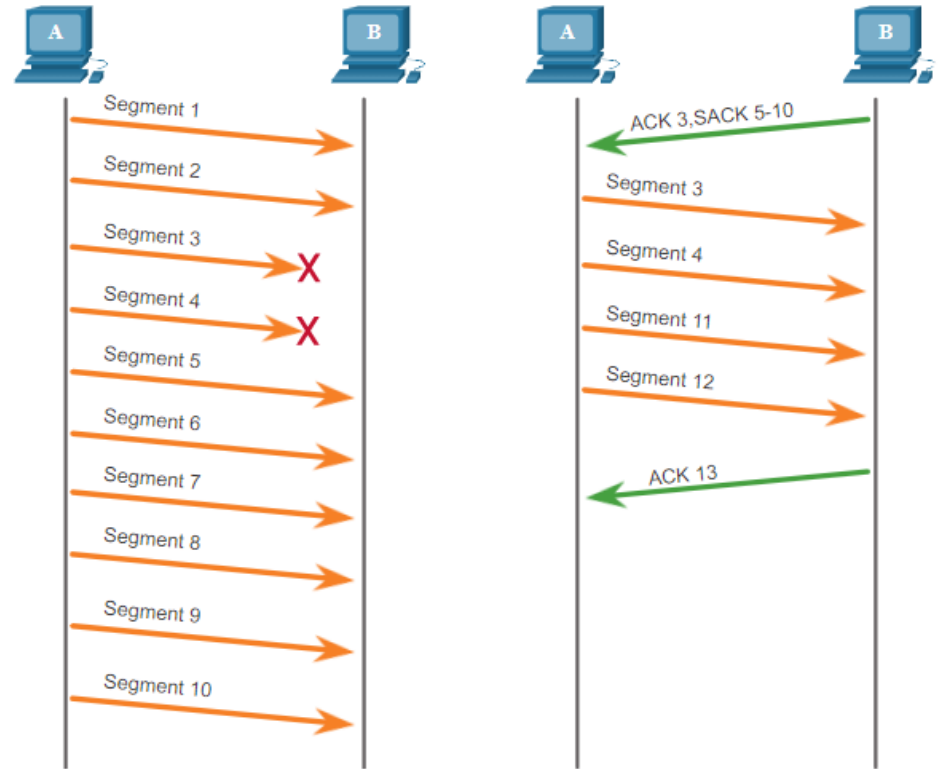
Sequence numbers are used to reassemble segments into their original order.



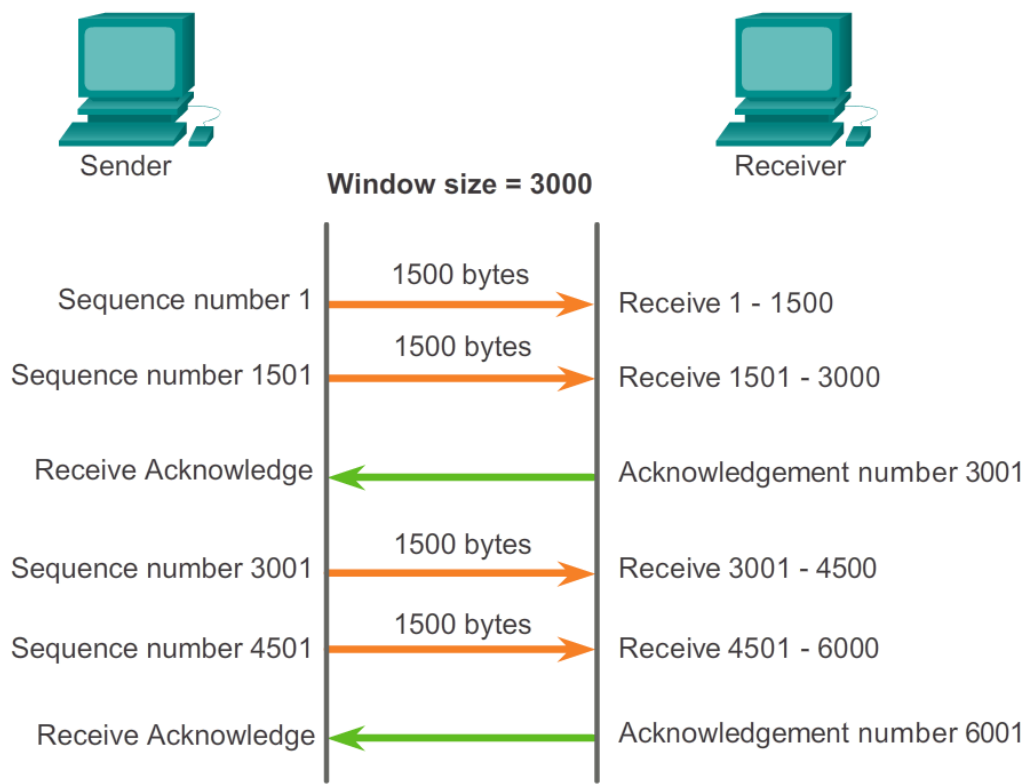
TCP Reliability – Data Loss and Retransmission (Cont.)

Host operating systems today typically employ an optional TCP feature called selective acknowledgment (SACK), negotiated during the three-way handshake.

If both hosts support SACK, the receiver can explicitly acknowledge which segments (bytes) were received including any discontinuous segments.



Window Size and Acknowledgements



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

The **acknowledgement** number is the number of the next expected byte.

UDP Low Overhead vs. Reliability

UDP

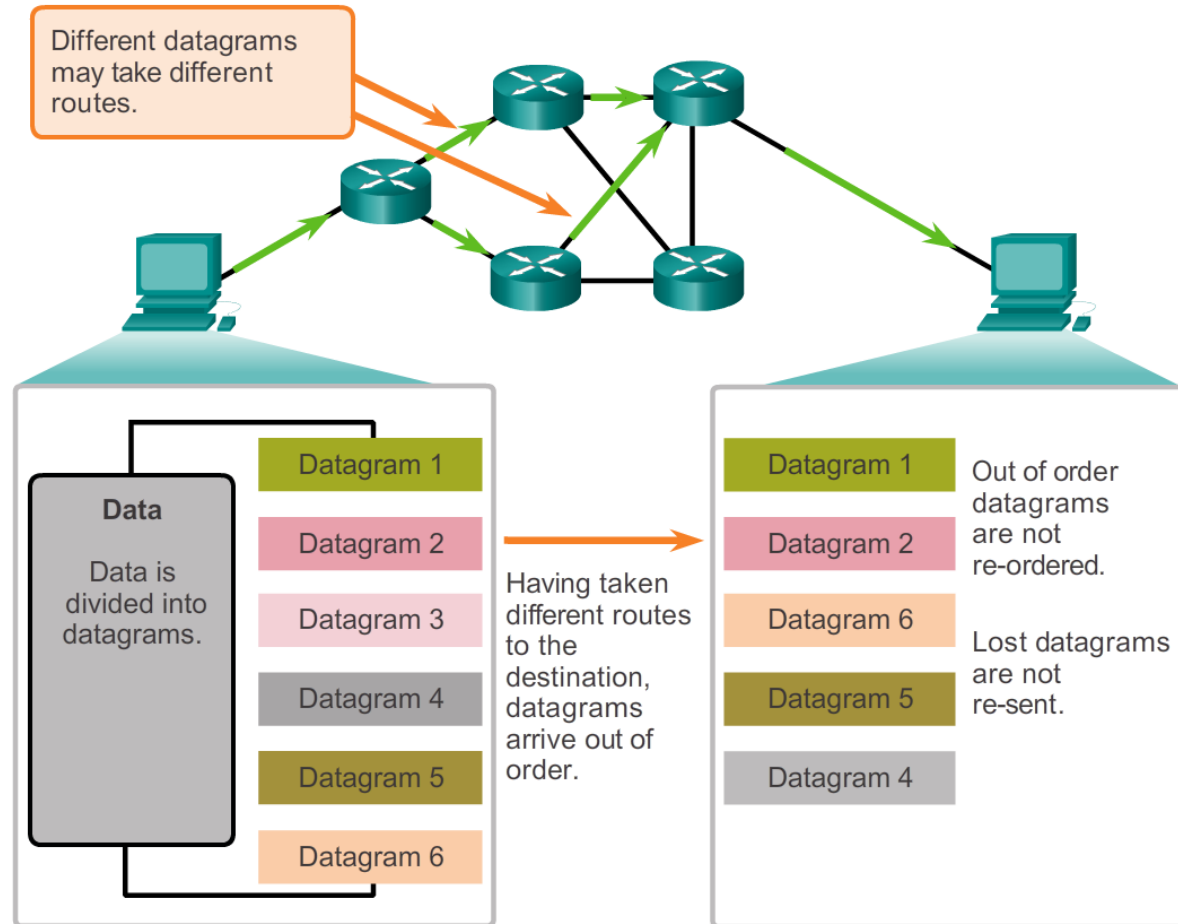
- Simple protocol that provides the basic transport layer function
- Used by applications that can tolerate small loss of data
- Used by applications that cannot tolerate delay

Used by:

- DNS
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- IP telephony or VoIP
- Online games



UDP: Connectionless and Unreliable



Transport Layer Services Summary

What Did I Learn in this Module?

- In the client/server model, the term server refers to a host running a software application that provides information or services to other hosts connected to the network. The client refers to a host running a software application makes a service request to a server.
- TCP and UDP are two network protocols operating at the Transport Layer.
- TCP provides mechanisms to ensure reliable data packets delivery with sequencing and acknowledgement. However, the acknowledgement slows down the packet delivery process.
- UDP is a 'best effort' delivery system that does not require acknowledgment of receipt.
- A port is a numeric identifier within each segment that is used to keep track of specific conversations between a client and server.
- Source port number is dynamically generated by the sending device as a return address.
- Destination port identifies the intended service requested by a client.
- Port numbers are in three categories: well-known ports, registered ports, and private ports.
- Command **netstat** lists the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state.