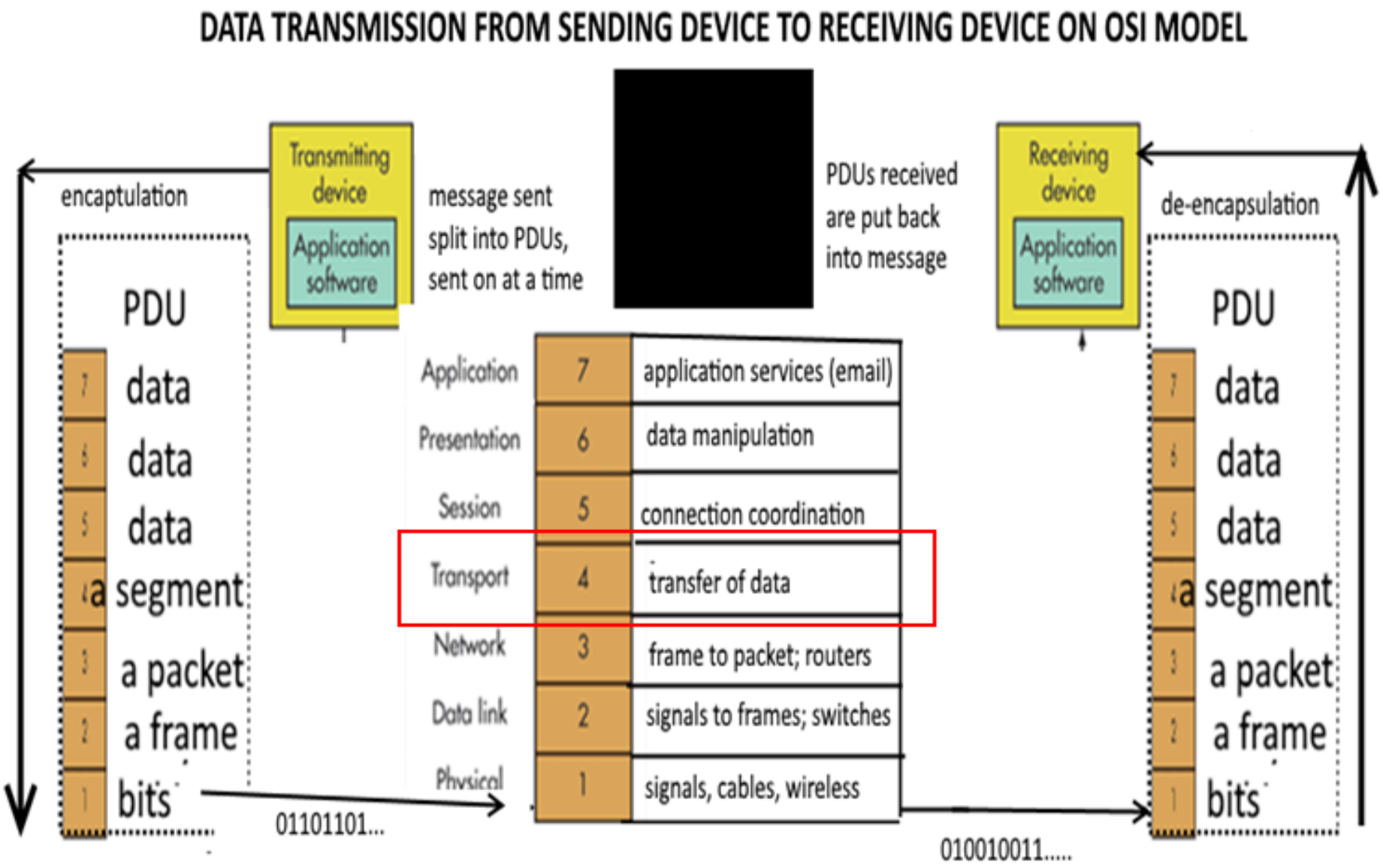
Chapter 7
Transport Layer

7.0 Introduction
7.1 Transport Layer Protocols
7.2 TCP and UDP
7.3 Summary

Transport Layer



Role of the Transport Layer

The transport layer is responsible for establishing a temporary communication session between two applications and delivering data between them.

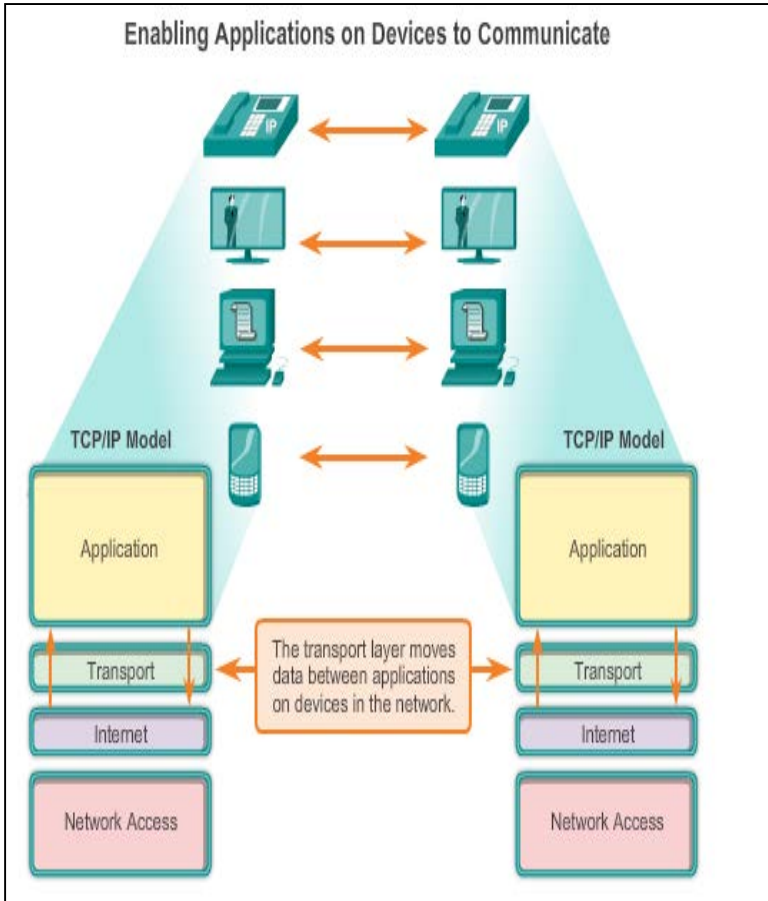
TCP/IP uses two protocols to achieve this:

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

Role of the Transport Layer

Primary Responsibilities of Transport Layer Protocols

- Tracking individual communication between applications on the source and destination hosts
- Segmenting data
- Reassembling segmented data at the destination
- Identifying the proper application for each communication stream

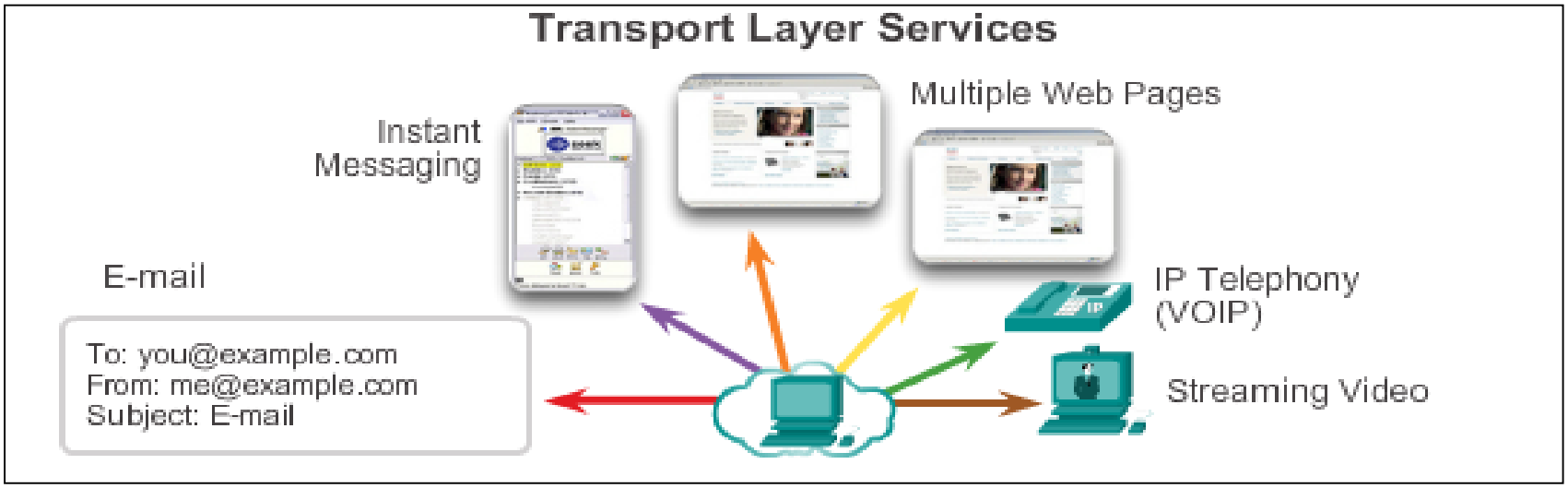


Multiplexing/Demultiplexing

- a *socket* is the interface through which a process communicates with the transport layer
- each process can use one or many sockets
- the transport layer in a receiving machine receives segments from its network layer
- delivering segments to the correct socket is called *demultiplexing*
- assembling segments and passing them to the network layer is called *multiplexing*
- multiplexing and demultiplexing are needed whenever a communications channel is *shared*

Conversation Multiplexing

- Sending one big chunk of data in a network can jam a network
- segmenting the data into smaller chunks enables many different communications to be multiplexed on the same network
- Data can be sent and received at the same time



Transport Layer Reliability

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

TCP (Transmission Control Protocol)

- Provides reliable delivery; ensures that all of the data arrives at the destination.
- Uses acknowledged delivery to ensure delivery
- More overhead.

UDP (User Datagram Protocol)

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

TCP or UDP – which to use

- Depends on level of reliability desired
- Depends on the requirements of applications.

RFC

- A **Request for Comments** (**RFC**) is,
- a type of publication
- authored by engineers and computer scientists
- submitted either for peer review or simply to convey new concepts

TCP – Transmission Control Protocol

- Connection-oriented – it creates a session between the source and destination
- Reliable delivery – it re-transmits lost or corrupt data
- Ordered data reconstruction – it reconstructs numbering and sequencing of segments
- Flow control – it regulates the amount of data transmitted
- it tracks the session

UDP – User Datagram Protocol

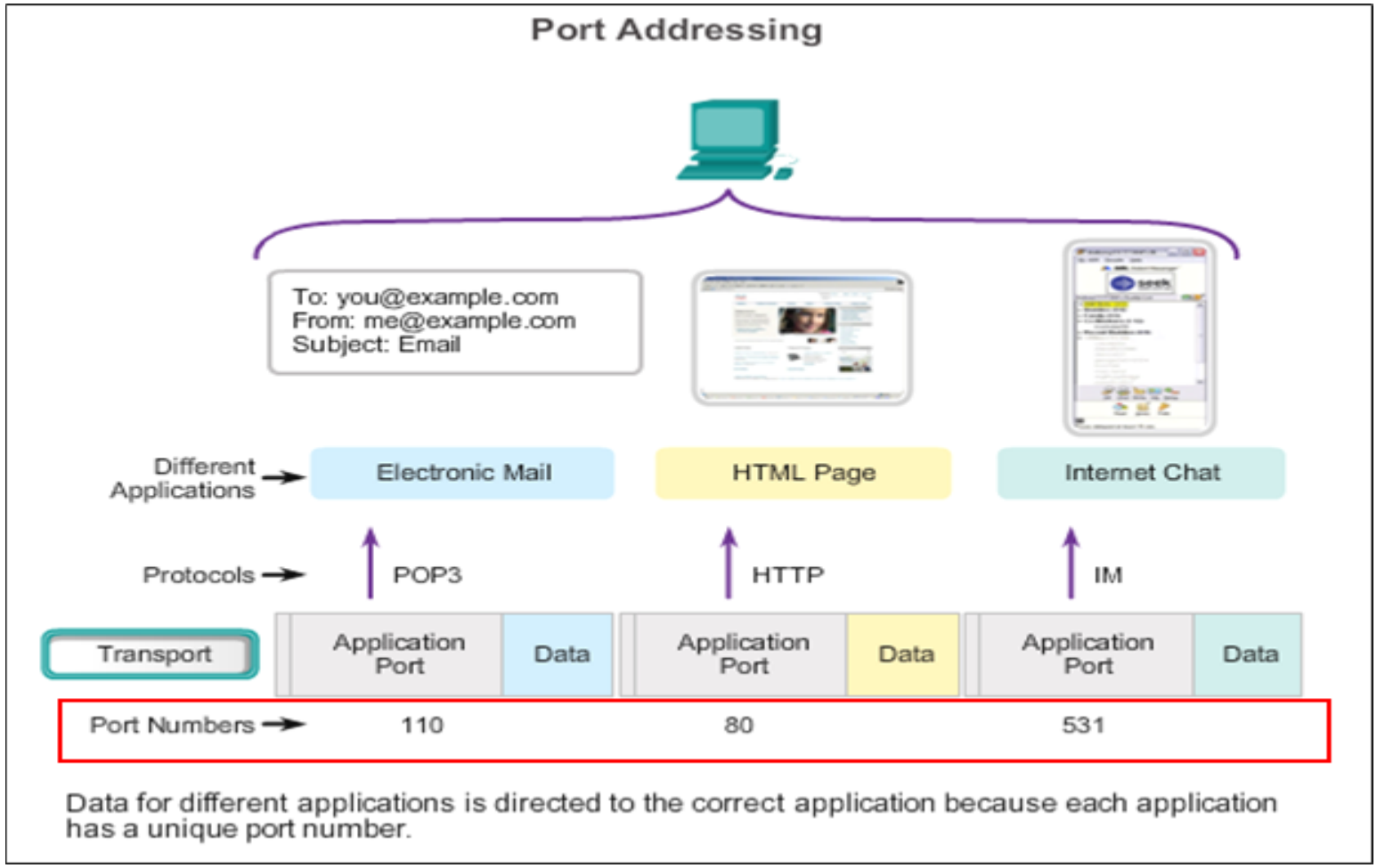
- Connectionless
- Unreliable delivery
- No ordered data reconstruction
- No flow control
- Stateless protocol

Applications that use UDP:

- Domain Name System (DNS)
- Video Streaming
- VoIP

Separating Multiple Communications

TCP and UDP use port numbers to differentiate between applications.



TCP and UDP Port Addressing

The TCP layer requires a port number to be assigned to each message. This way it can determine the type of service being provided.

These ports are merely reference numbers used to define a service.

For instance, port 23 is used for telnet services, and HTTP uses port 80 for providing web browsing service. There is a group called the IANA (Internet Assigned Numbers Authority) that controls the assigning of ports for specific services.

There are some ports that are assigned, some reserved and many unassigned which may be utilized by application programs. Port numbers are straight unsigned integer values which range up to a value of 65535.

TCP and UDP Port Addressing

Port Numbers

Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65533	Private and/or Dynamic Ports

Registered TCP Ports:

1863	MSN Messenger
2000	Cisco SCCP (VoIP)
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 (Cont.)

Registered UDP Ports:

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

Well Known UDP Ports:

69	TFTP
520	RIP

Registered TCP/UDP Common Ports:

1433	MS SQL
2948	WAP (MMS)

Well Known TCP/UDP Common Ports:

53	DNS
161	SNMP
531	AOL Instant Messenger, IRC

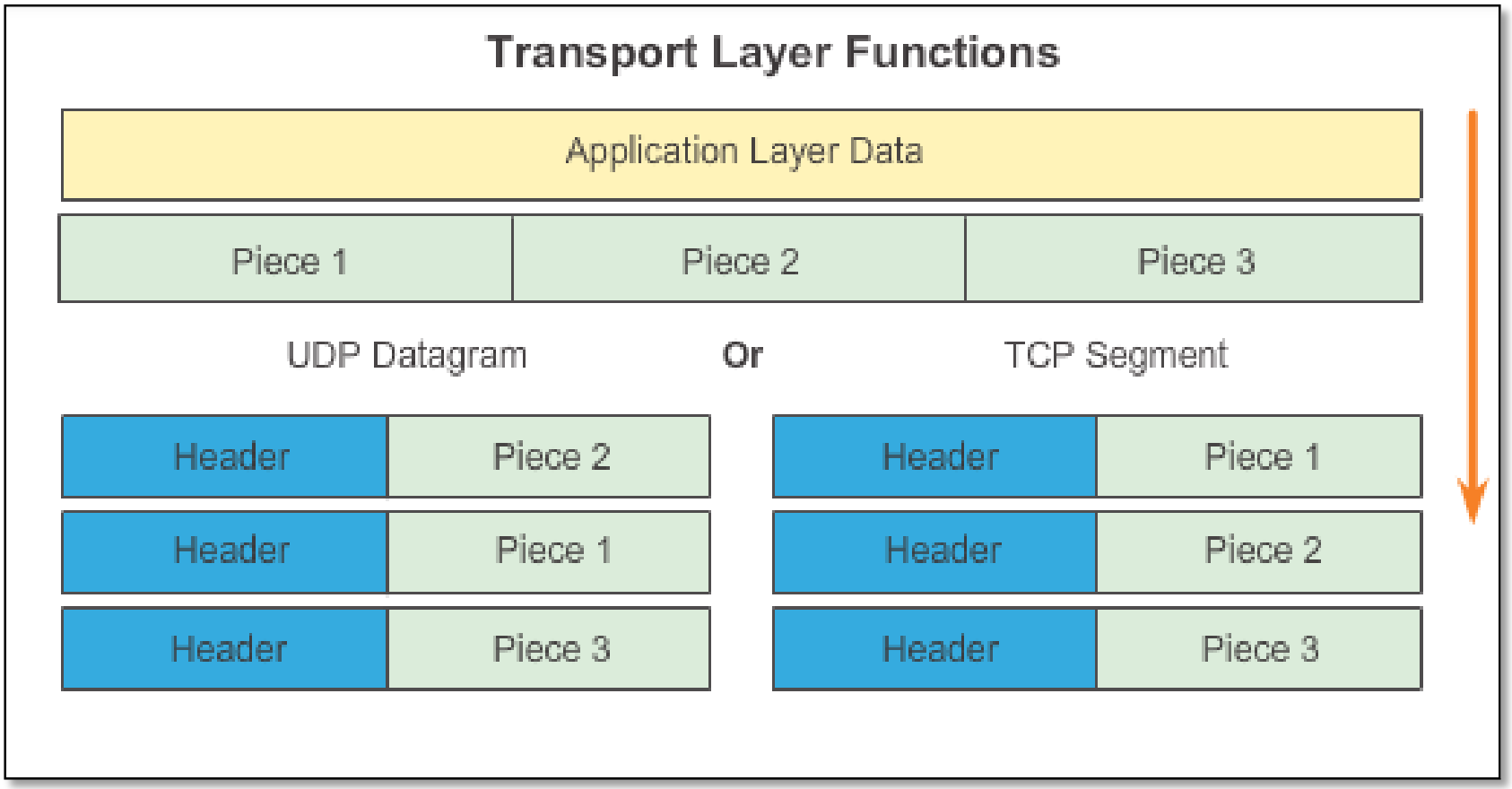
TCP and UDP Port Addressing

The ‘Netstat’ command 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     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:\>
```

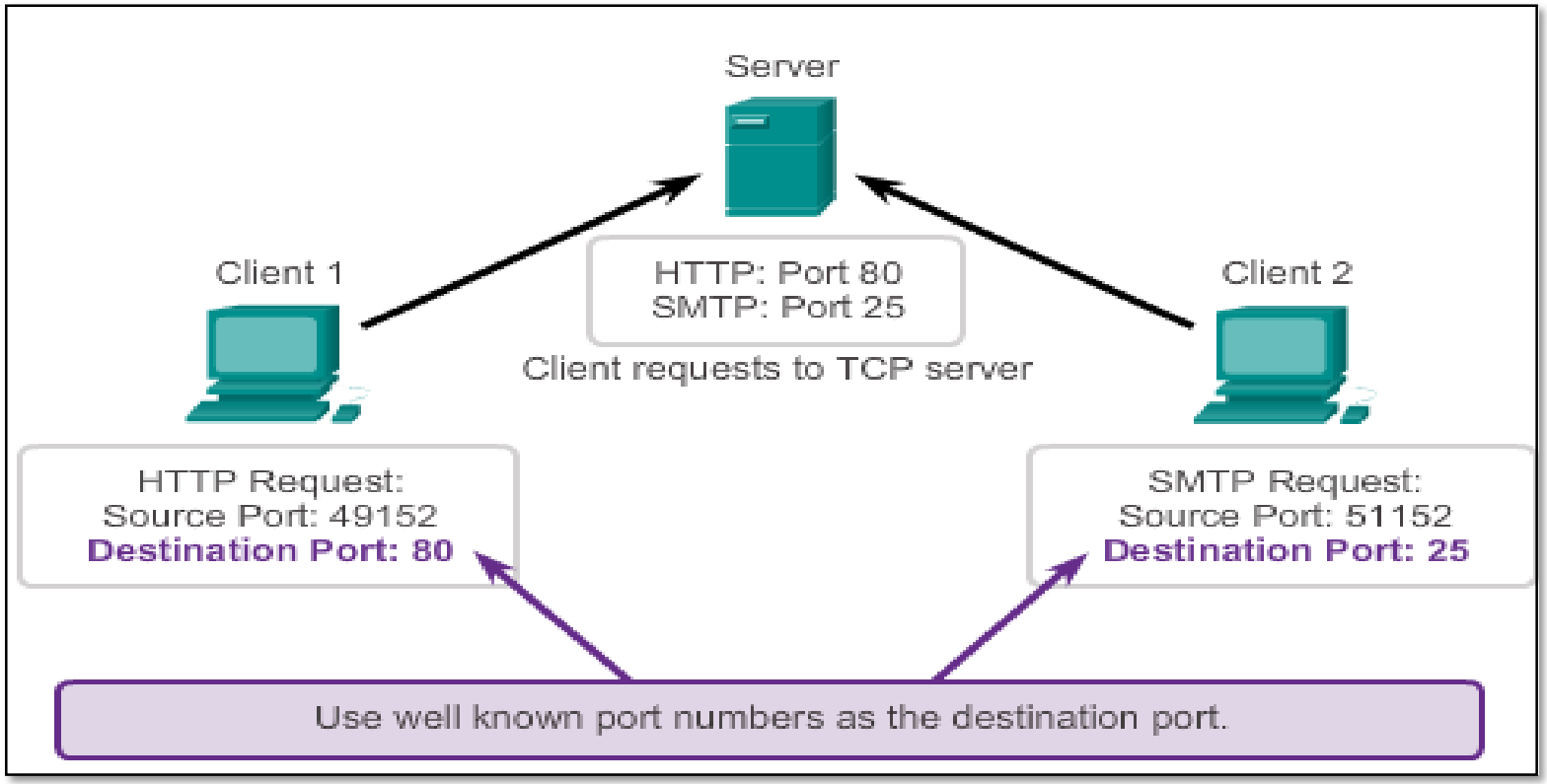
TCP and UDP Segmentation

The transport layer divides the data into pieces and adds a header for delivery over the network



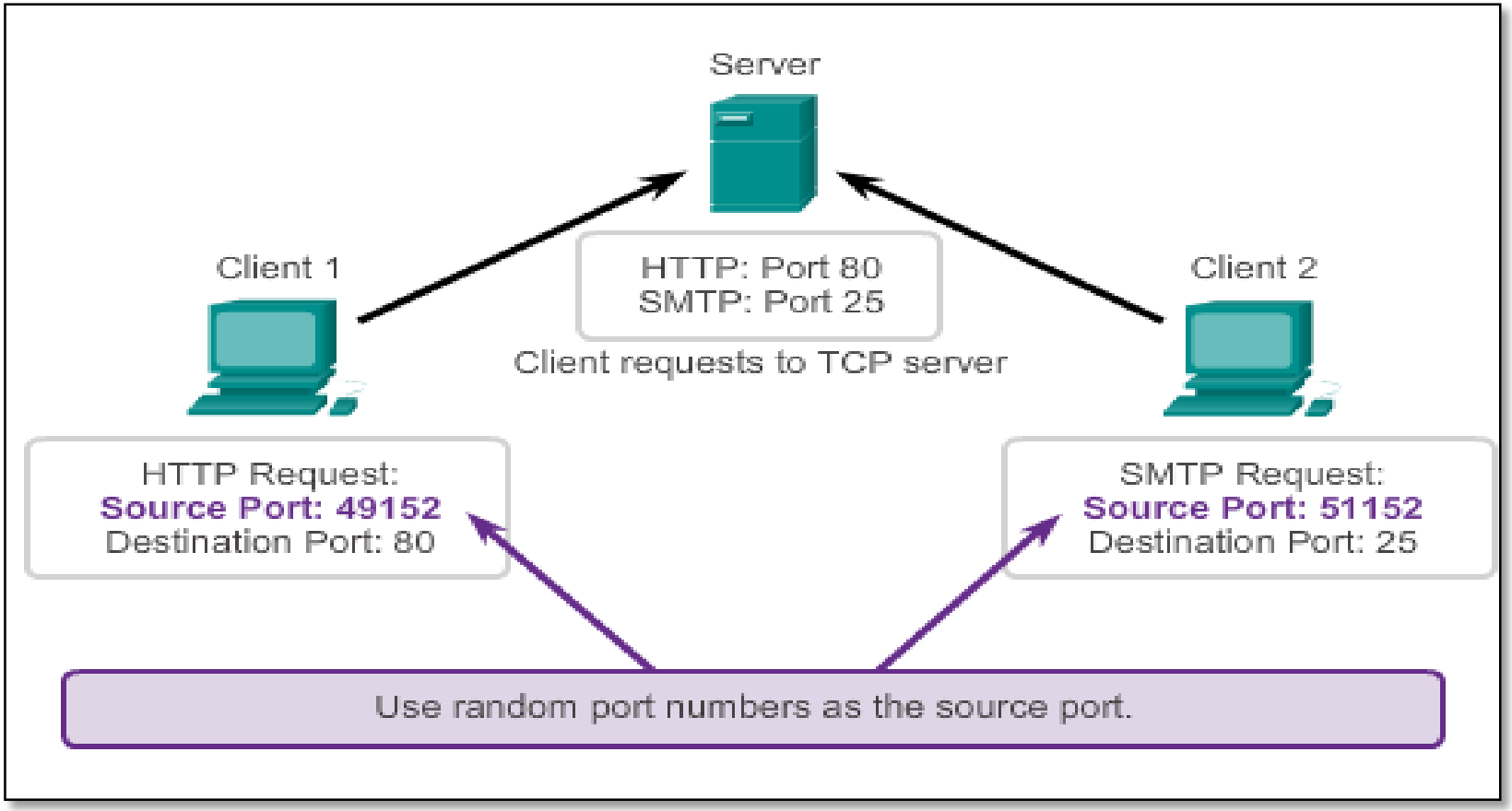
TCP Server Processes

Well-known ports are used as destinations, such as 80 (SMTP) and 25 (HTTP).



TCP Server Processes (Cont.)

Random ports are used sources.



TCP Connection, Establishment and Termination

Three-Way Handshake

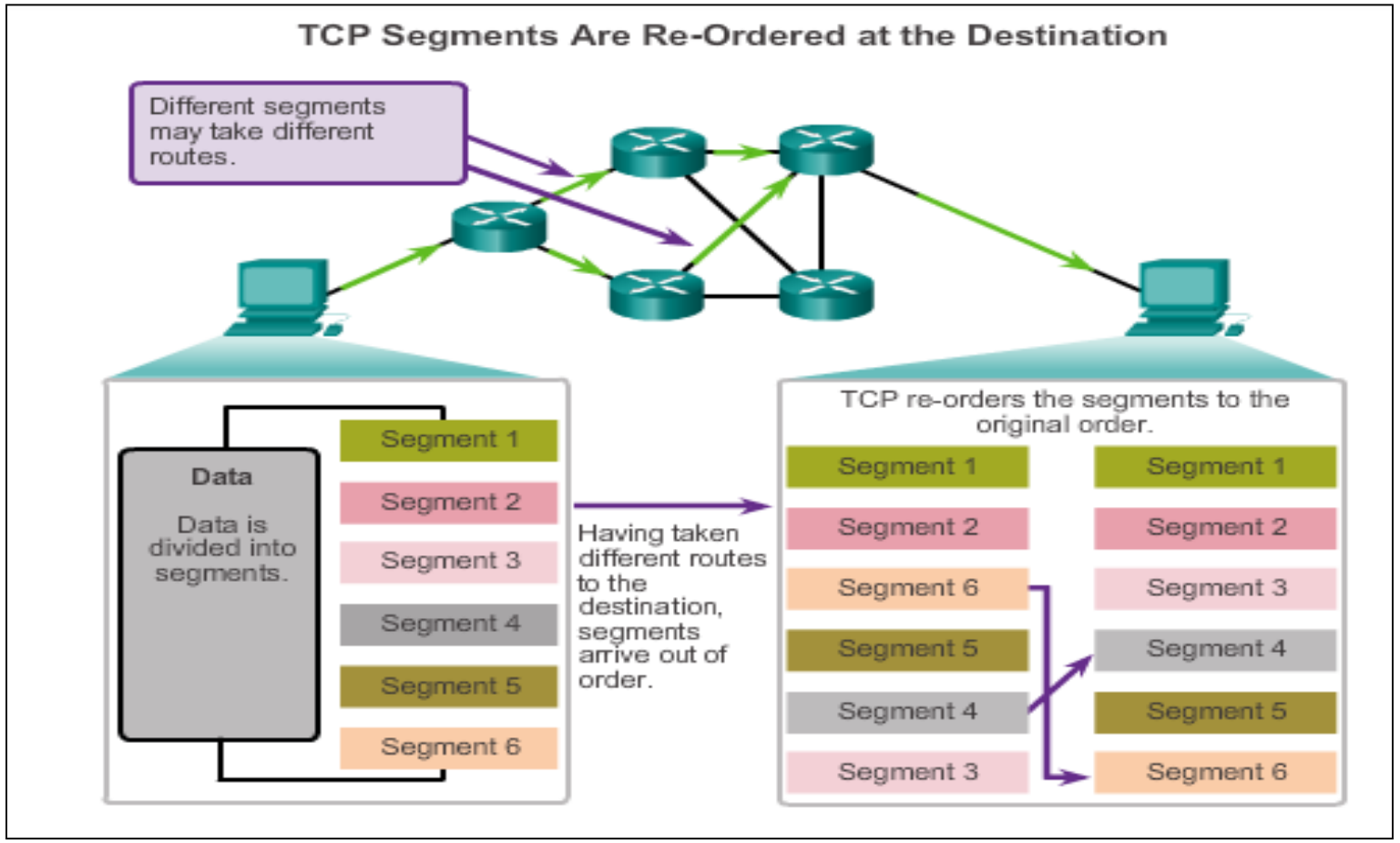
- Three-way Handshake is the method used by TCP set up a TCP/IP connection over an Internet Protocol based network.
- It first establishes that the destination device is present on the network
- It then verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use for the session
- It 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

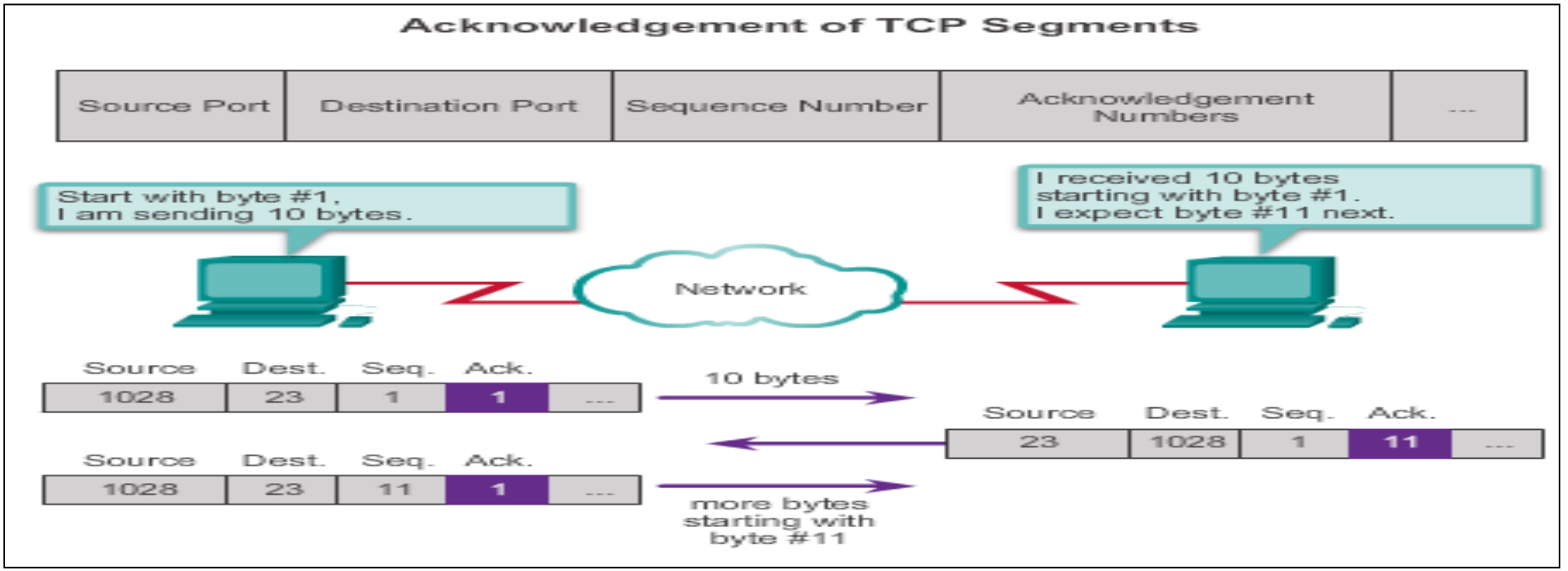
TCP Reliability – Ordered Delivery

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



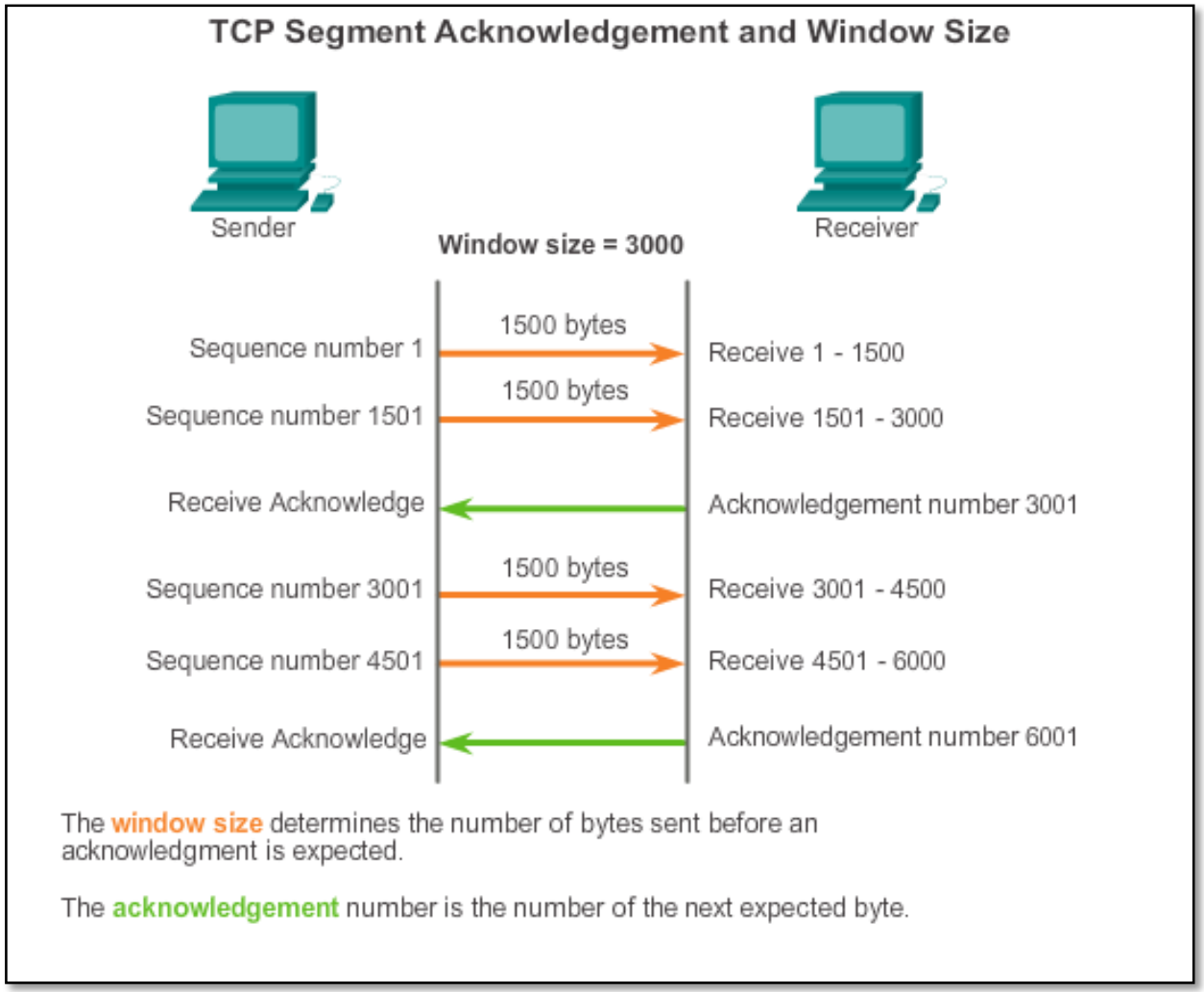
Acknowledgement and Window Size

The sequence number and acknowledgement number are used together to confirm receipt.

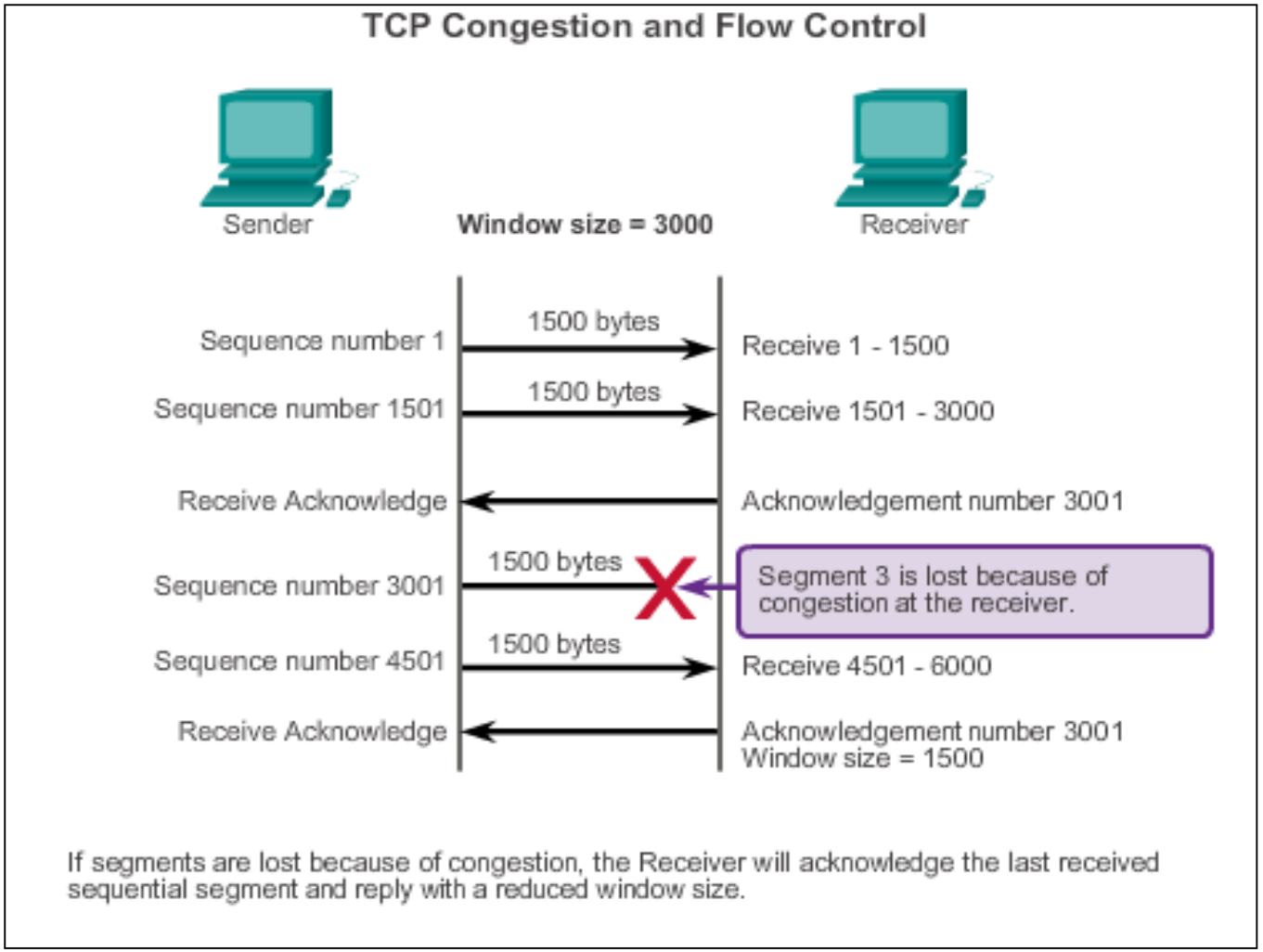


The window size is the amount of data that a source can transmit before an acknowledgement must be received.

Window Size and Acknowledgements



TCP Flow Control – Congestion



UDP Low Overhead vs. Reliability

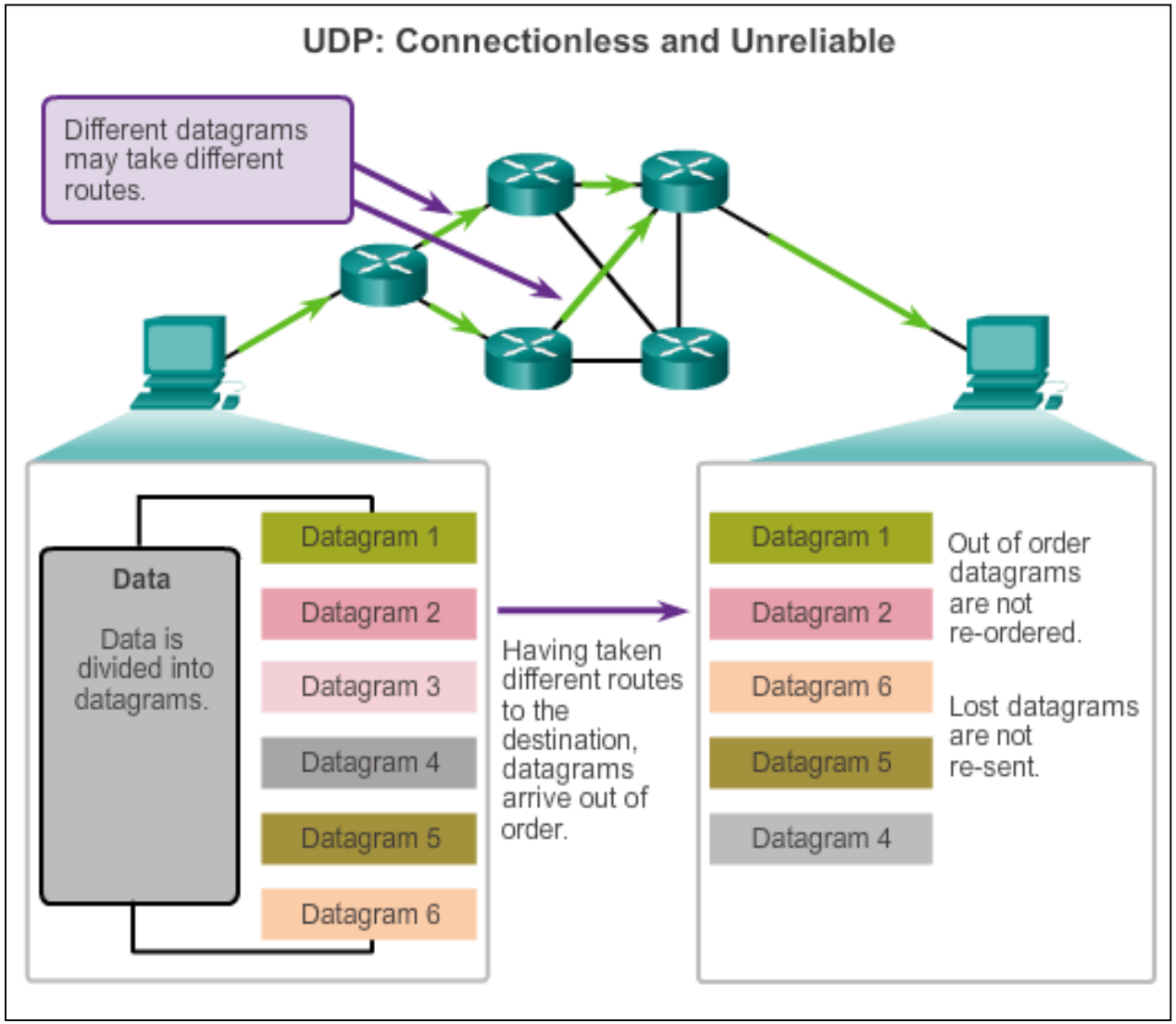
UDP

- 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

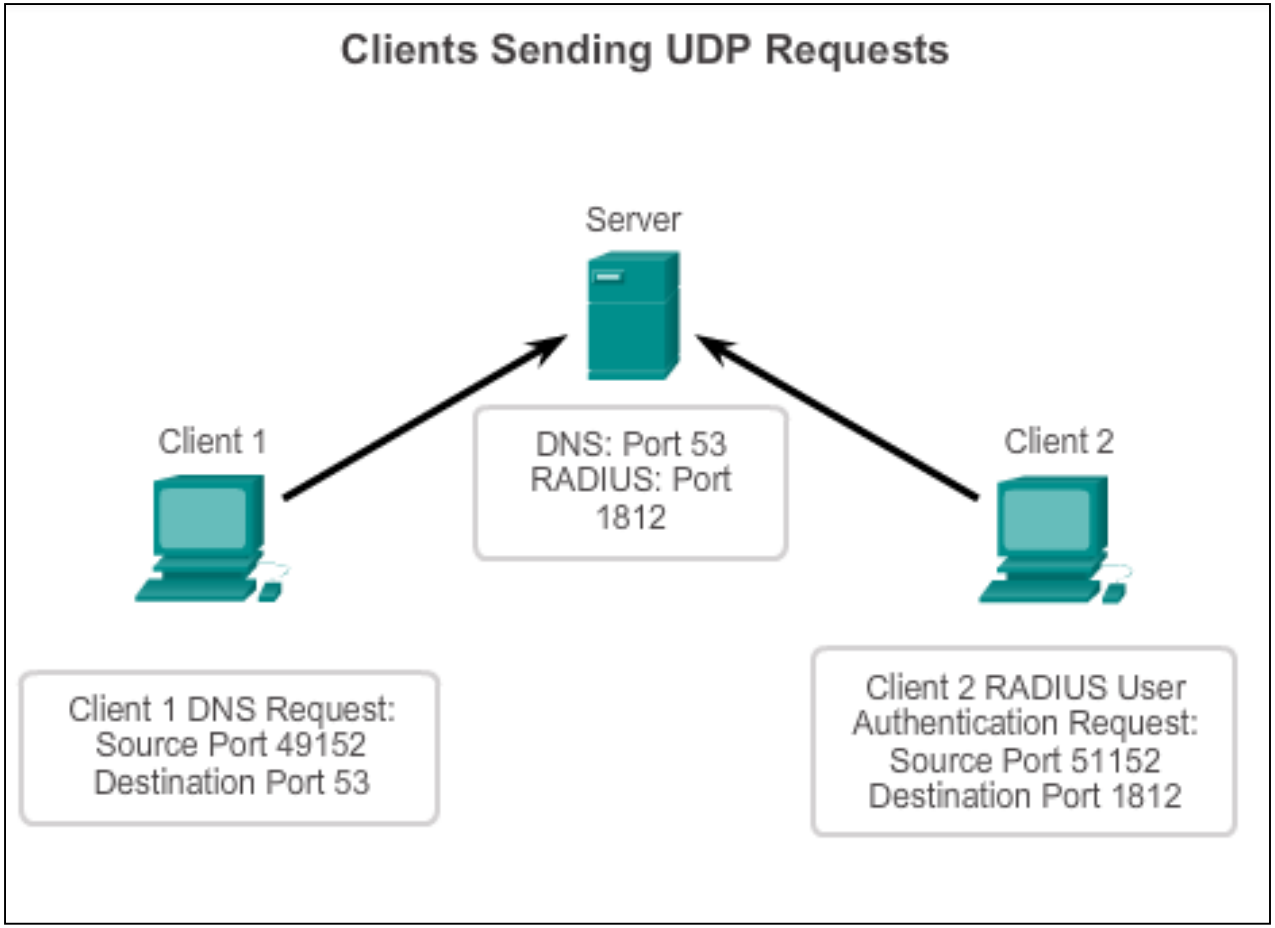
- DNS
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- IP telephony or VoIP
- Online games

Datagram Reassembly



UDP Server and Client Processes

- UDP-based server applications are assigned well-known or registered port numbers.
- UDP client process randomly selects port number from range of dynamic port numbers as the source port.



END