Web Application Security

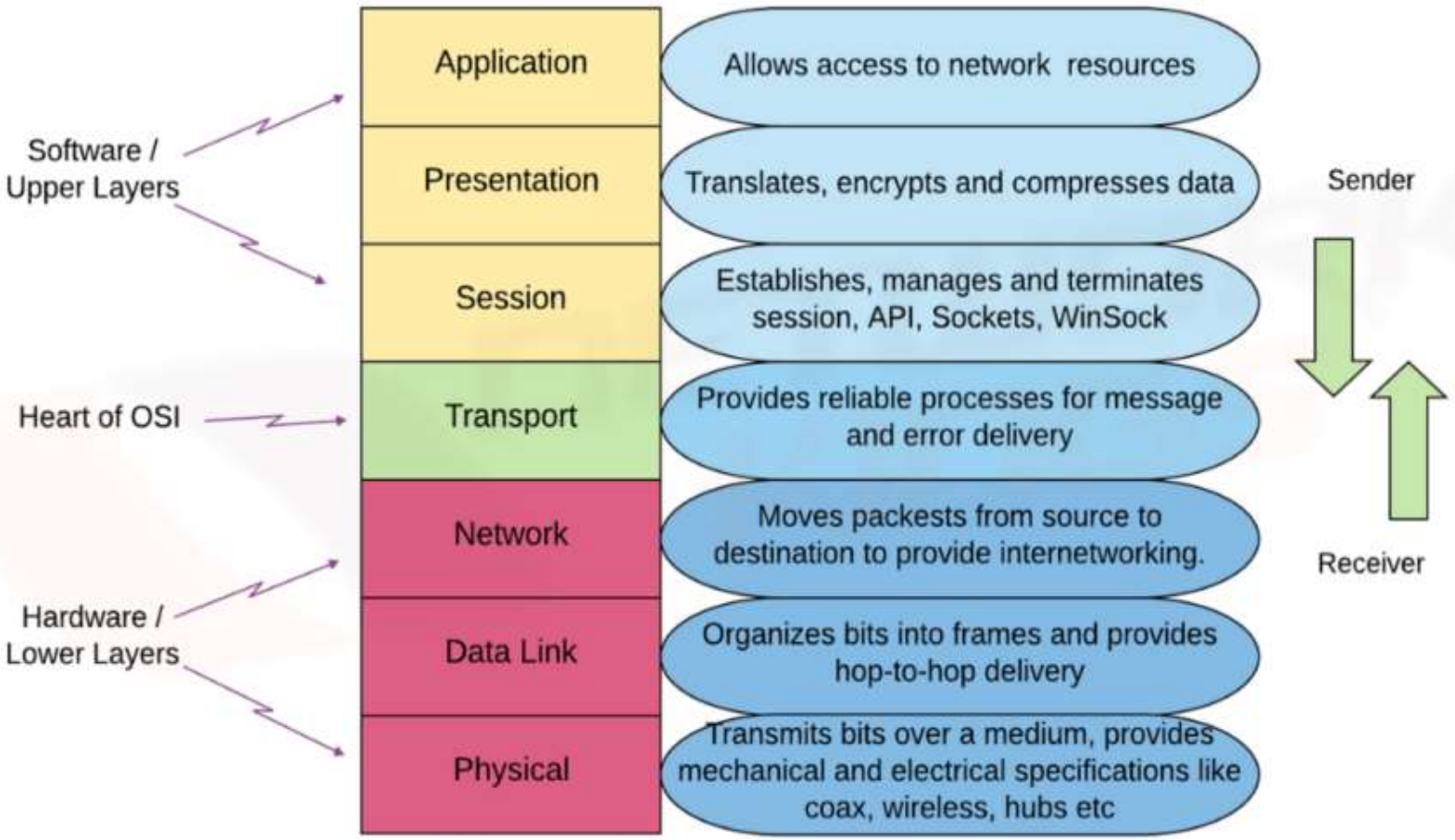
Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in

TCP
(Transmission Control Protocol)

Ref: https://www.geeksforgeeks.org/tcp-3-way-handshake-process/

OSI Model


Application
Presentation
Session
Transport
Network
Data Link
Physical
Allows access to network resources
Translates, encrypts and compresses data
Establishes, manages and terminates session, API, Sockets, WinSock
Provides reliable processes for message and error delivery
Moves packests from source to destination to provide internetworking.
Organizes bits into frames and provides hop-to-hop delivery
Transmits bits over a medium, provides mechanical and electrical specifications like coax, wireless, hubs etc
Software / Upper Layers
Heart of OSI
Hardware / Lower Layers
Sender
Receiver

TCP IP Model

#	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc..	Messages	n/a
4	Transport	TCP/UDP	Segment	Port #'s
3	Network	IP	Datagram	IP address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

3 – Way Hanshaking

- ✓ This could also be seen as a way of how TCP connection is established. Before getting into the details, let us look at some basics.
- ✓ TCP stands for **Transmission Control Protocol** which indicates that it does something to control the transmission of the data in a reliable way.

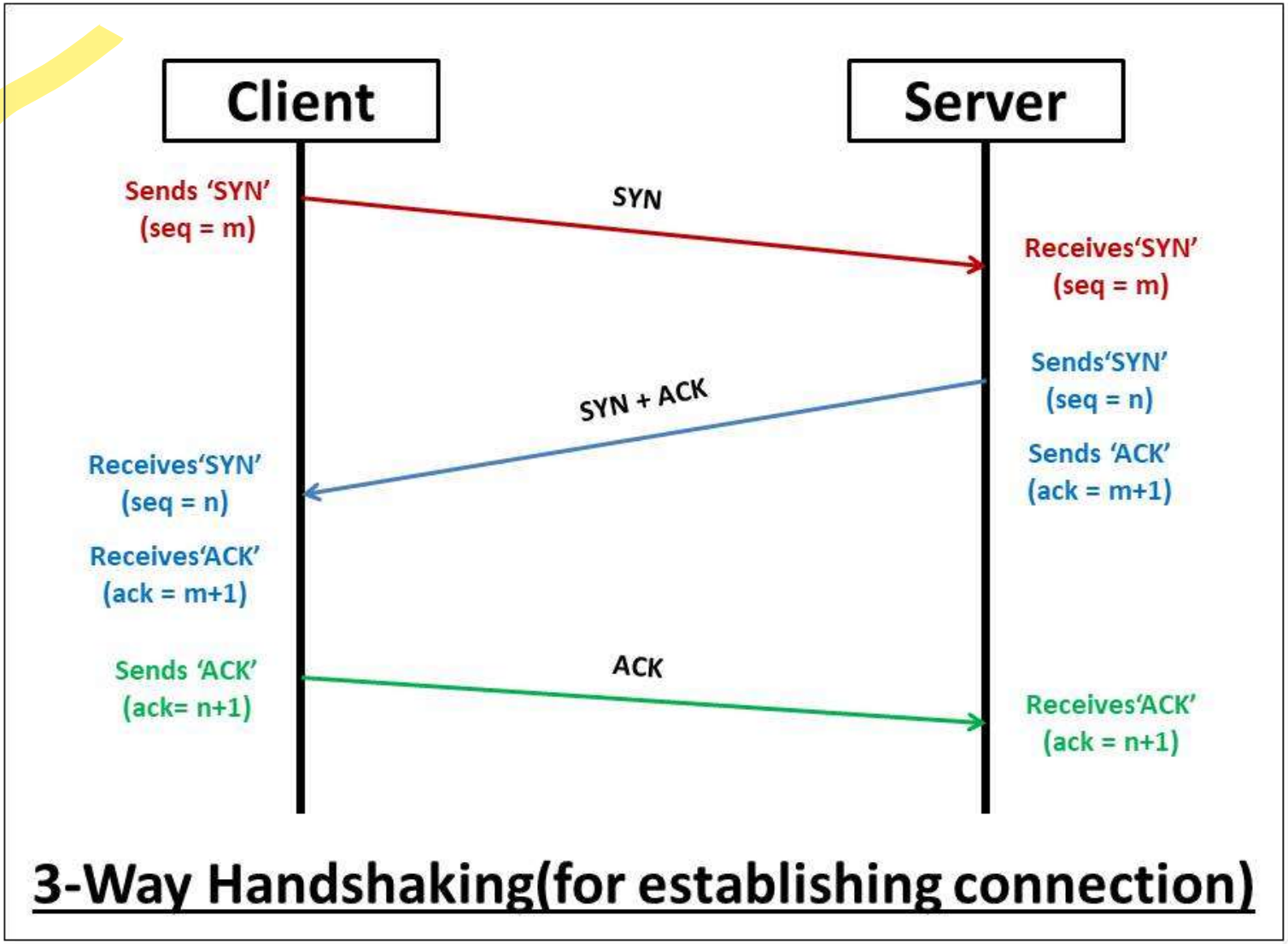
3 – Way Hanshaking

- ✓ The process of communication between devices over the internet happens according to the current **TCP/IP** suite model(stripped out version of OSI reference model).
- ✓ The Application layer is a top pile of a stack of TCP/IP models from where network referenced applications like web browsers on the client-side establish a connection with the server. From the application layer, the information is transferred to the transport layer where our topic comes into the picture.

3 – Way Hanshaking

- ✓ The two important protocols of this layer are – TCP, **UDP(User Datagram Protocol)** out of which TCP is prevalent(since it provides reliability for the connection established).
- ✓ However, you can find an application of UDP in querying the DNS server to get the binary equivalent of the Domain Name used for the website.

3 – Way Hanshaking



3-Way Handshaking(for establishing connection)

- ✓ Step 1 (SYN): In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with.

- ✓ Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with

- ✓ Step 3 (ACK): In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

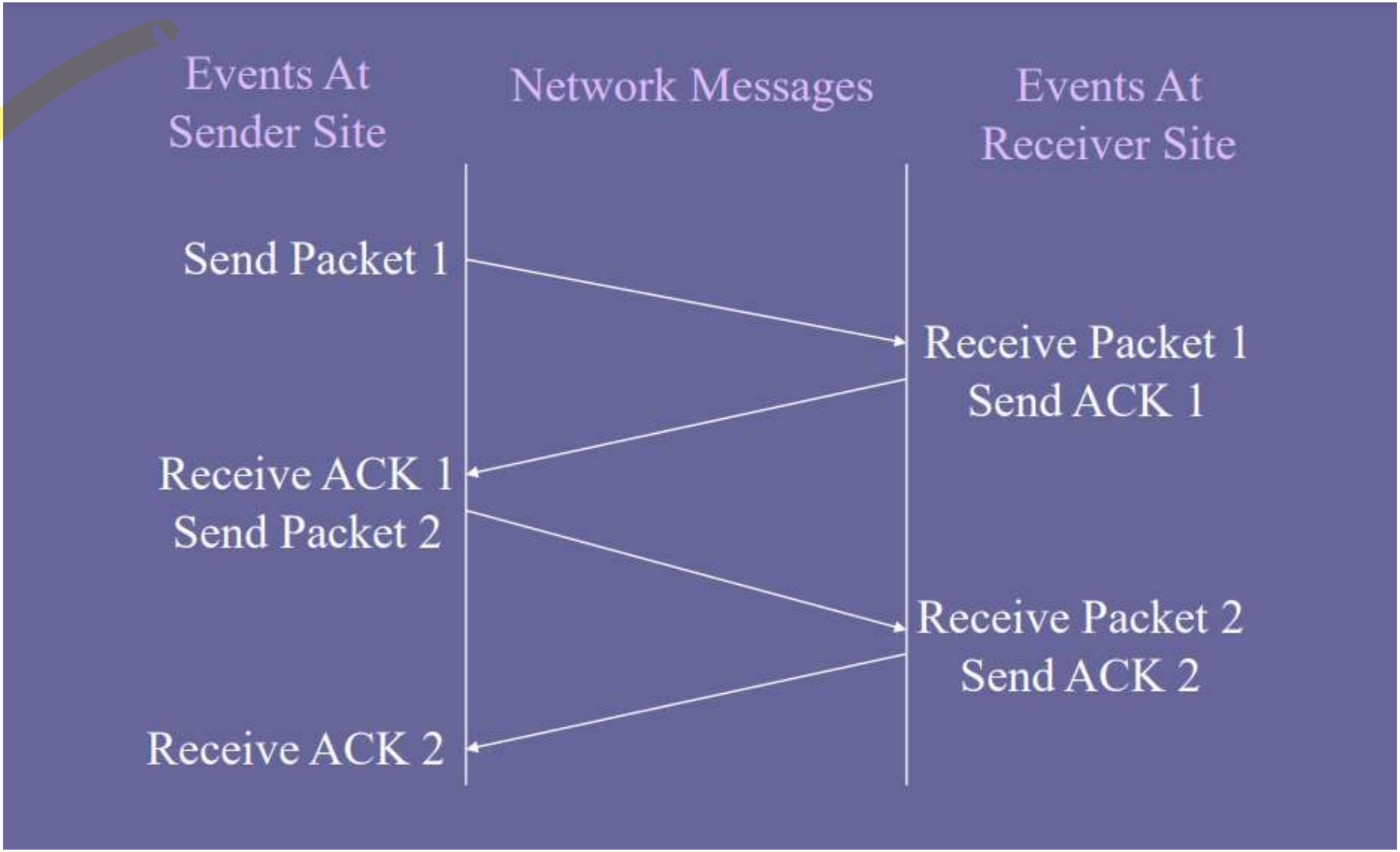
Reliable Delivery Service:

- ✓ Features of the interface between application programs and the TCP/IP reliable delivery service include:
- ✓ Stream Orientation - data is considered as a bitstream divided into bytes.
- ✓ Buffered Transfer - transport mechanisms buffer application data until it can fill a reasonably large datagram, using PUSH for immediate transfer.

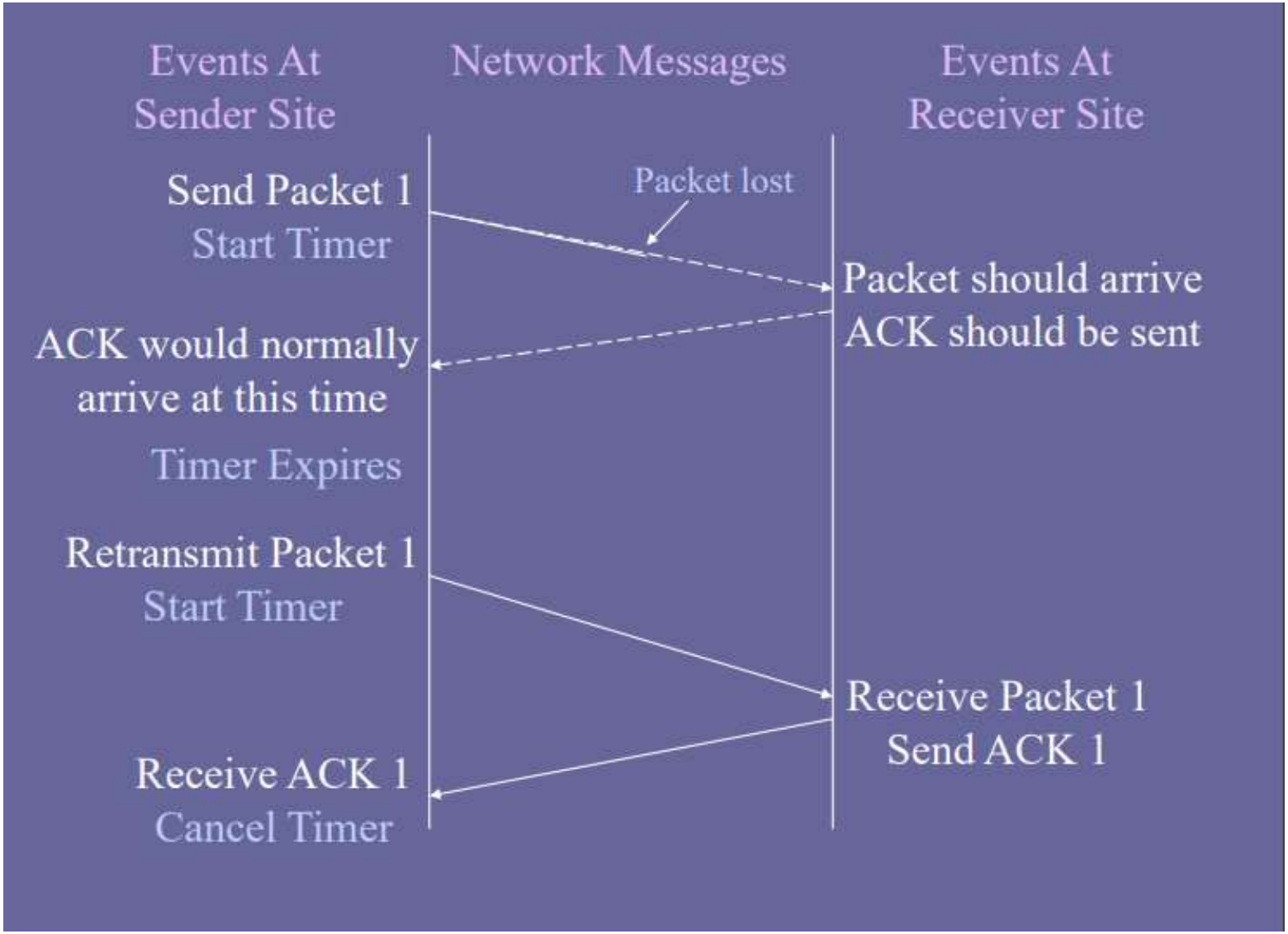
Providing Reliability:

- ✓ Sending positive acknowledgments (ACKs) with retransmission is a fundamental technique used to provide reliable transfer.
- ✓ A timer is started during each transmission and if it expires, the message is then retransmitted.
- ✓ A combination of several timers are all used to provide a reliable delivery system.

Providing Reliability:

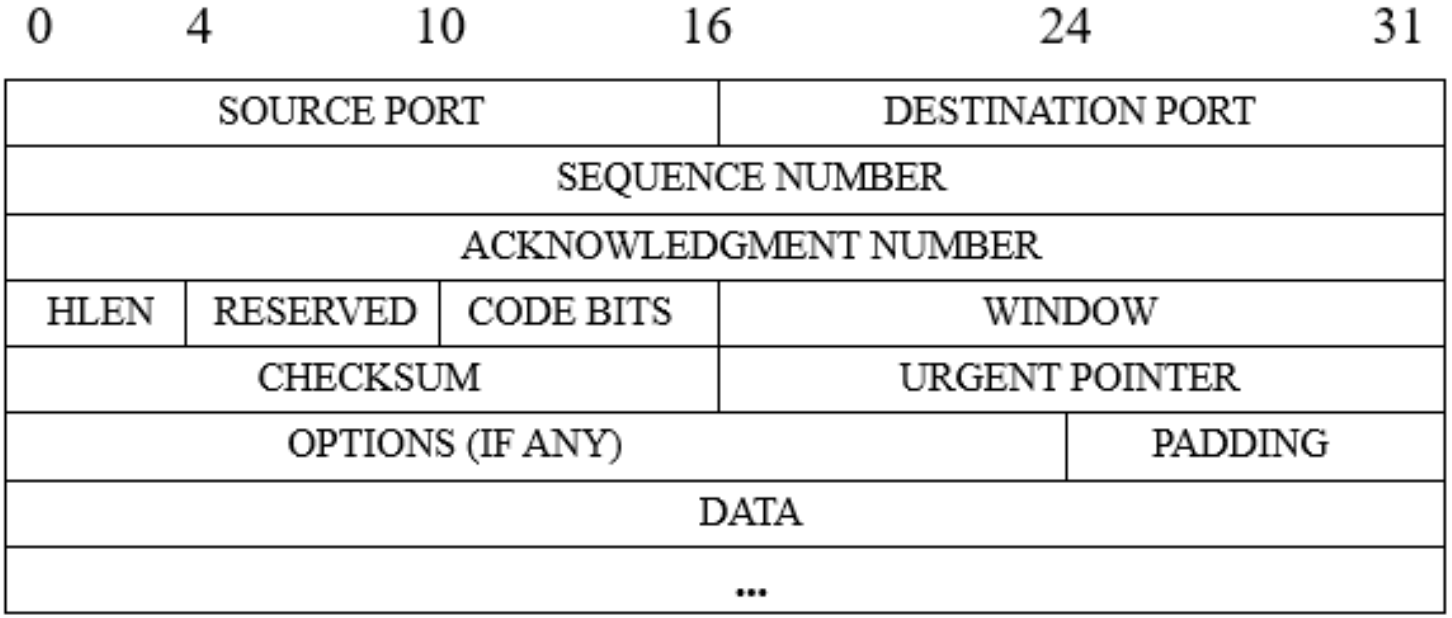


Providing Reliability:



TCP Segment Format

- TCP divides the data stream into *segments* for transmission:



TCP Segment Header Fields

Code bits - identify the contents of the segment:

Bit (left to right)	Meaning if bit is set to 1
URG	Urgent pointer field is valid
ACK	Acknowledgment field is valid
PSH	This segment requests a push
RST	Reset the connection
SYN	Synchronize sequence numbers
FIN	Sender has reached end of its byte stream

Window - how much data the sender is willing to accept (flow control)

Urgent pointer - specifies the position in the segment where urgent data ends

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in