TCP/UDP message format, 3 way handshaking

Lecture 37-38 (Theory)

Department of Computer Science and Engineering,
Chitkara University, Punjab

Index

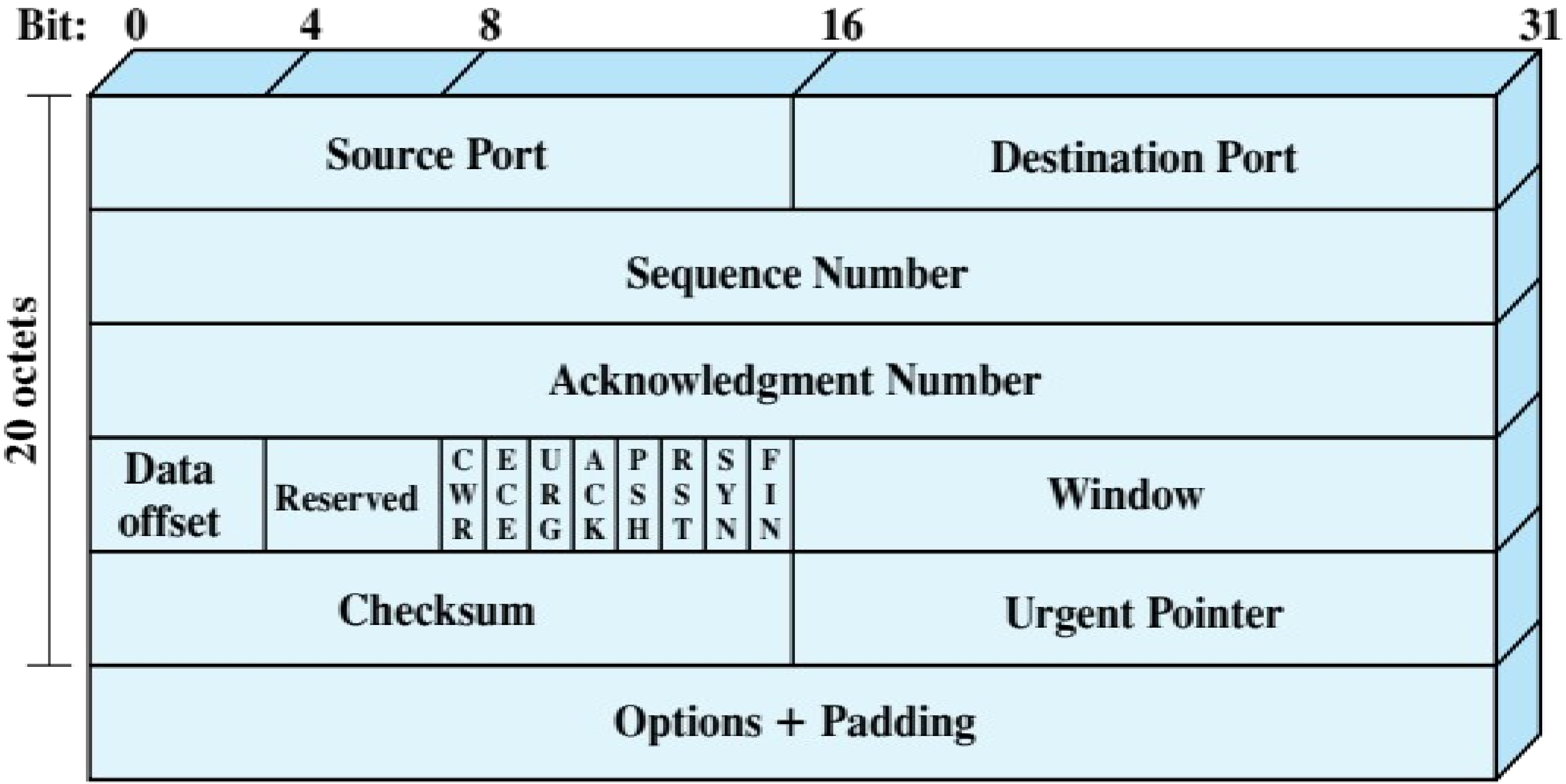
- TCP header
- TCP Message Format
- Three Way Handshaking
- UDP header
- UDP Message Format

Transmission Control Protocol (TCP)

- A TCP connection provides a full-duplex service: If there is a TCP connection between Process A on one host and Process B on another host, then application layer data can flow from Process A to Process B at the same time as application layer data flows from Process B to Process A.
- A TCP connection is also always point-to-point, that is, between a single sender and a single receiver.
- The client first sends a special TCP segment; the server responds with a second special TCP segment; and finally the client responds again with a third special segment.
- The first two segments carry no payload, that is, no application-layer data; the third of these segments may carry a payload. Because three segments are sent between the two hosts, this connection-establishment procedure is often referred to as a three-way handshake.

Transmission Control Protocol(TCP)

TCP Header



Bit: 0 4 8 16 31

20 octets

Source Port | Destination Port

Sequence Number

Acknowledgment Number

Data offset | Reserved | CWR | ECE | URG | ACK | PSH | RST | SYN | FIN | Window

Checksum | Urgent Pointer

Options + Padding

Figure 1: TCP header

Transmission Control Protocol(TCP)

- **Source Port (16 bits)**: Source TCP user. Example values are Telnet 23;
- TFTP = 69; HTTP = 80
- **Destination Port (16 bits)**: Destination TCP user.
- **Sequence Number (32 bits)**: Sequence number of the first data octet in this segment except when the SYN flag is set. If SYN is set, this field contains the initial sequence number (ISN) and the first data octet in this segment has sequence number ISN + 1
- **Acknowledgment Number (32 bits)**: Contains the sequence number of the next data octet that the TCP entity expects to receive.
- **Data Offset (4 bits)**: Number of 32-bit words in the header.
- **Reserved (4 bits)**: Reserved for future use.

Transmission Control Protocol (TCP)

- **Flags (6 bits):** For each flag, if set to 1, the meaning is
  - CWR: congestion window reduced.
  - ECE: ECN-Echo; the CWR and ECE bits, are used for the explicit congestion notification function
  - URG: urgent pointer field significant.
  - ACK: acknowledgment field significant.
  - PSH: push function.
  - RST: reset the connection.
  - SYN: synchronize the sequence numbers.
  - FIN: no more data from sender

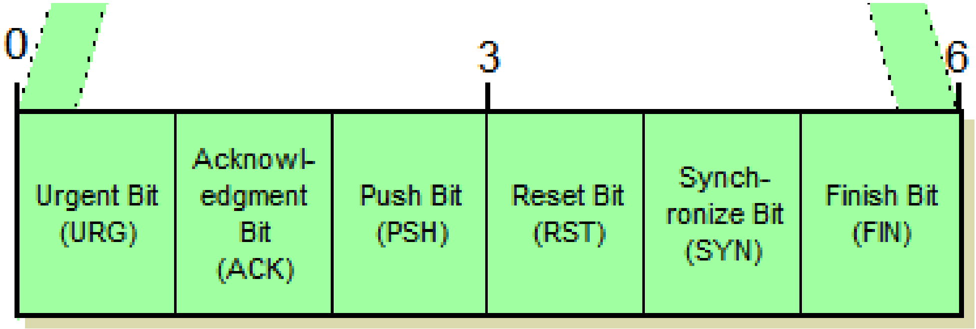


Figure 2: TCP Segment Format

Transmission Control Protocol(TCP)

- **Window (16 bits):** Flow control credit allocation, in octets. Contains the number of data octets, beginning with the sequence number indicated in the acknowledgment field that the sender is willing to accept.
- **Checksum (16 bits):** The ones complement of the ones complement sum of all the 16-bit words in the segment plus a pseudoheader, described subsequently.
- **Urgent Pointer (16 bits):** This value, when added to the segment sequence number, contains the sequence number of the last octet in a sequence of urgent data. This allows the receiver to know how much urgent data is coming.
- **Options (Variable):** An example is the option that specifies the maximum segment size that will be accepted.

What is TCP Three-Way HandShake?

Three-Way HandShake or a TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.

Three-way handshake process is designed in such a way that both ends help you to initiate, negotiate, and separate TCP socket connections at the same time. It allows you to transfer multiple TCP socket connections in both directions at the same time.

TCP message type

Message	**Description**
Syn	Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.
ACK	Helps to confirm to the other side that it has received the SYN.
SYN-ACK	SYN message from local device and ACK of the earlier packet.
FIN	Used to terminate a connection.

3-way handshake process: Connection establishment

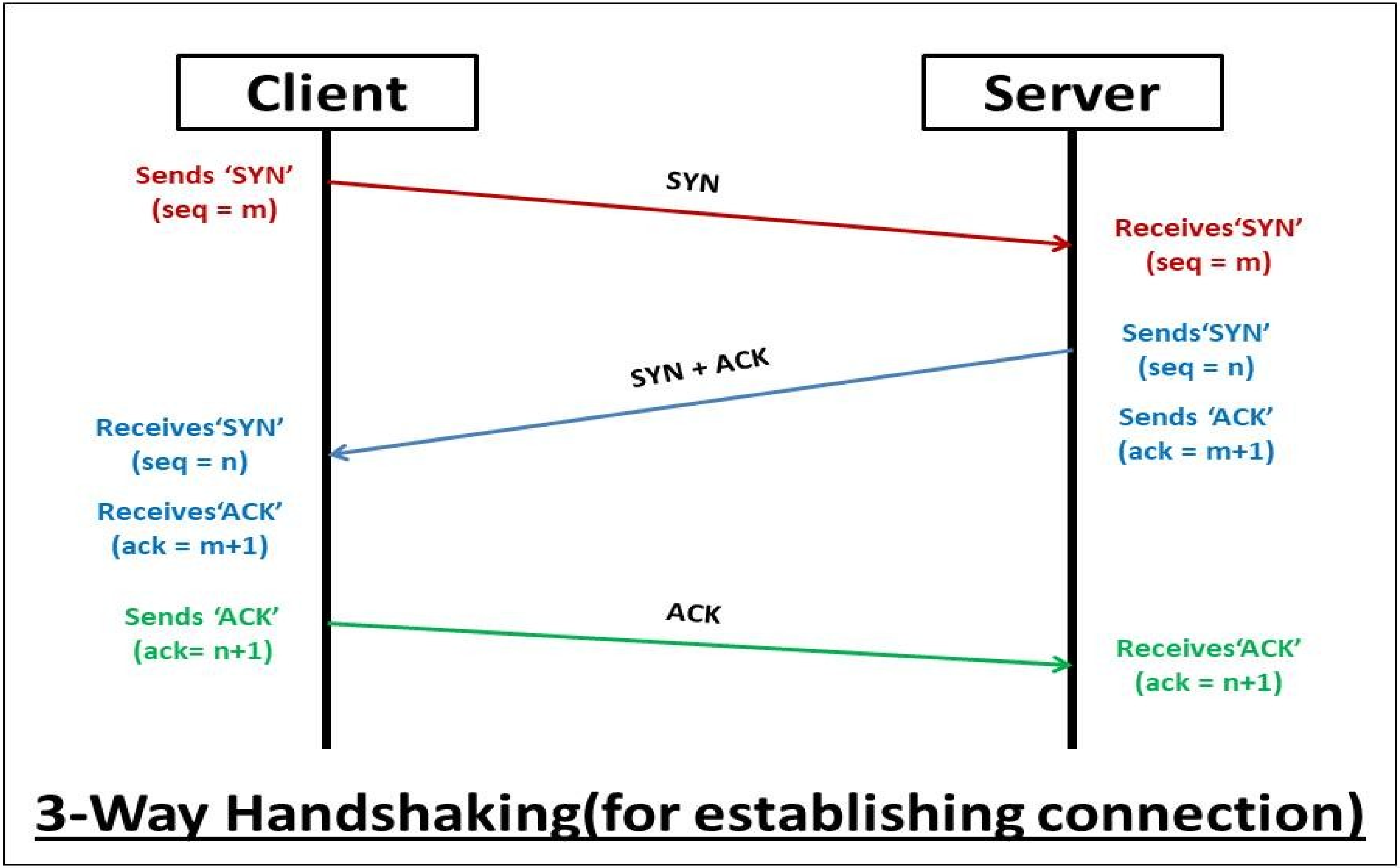


Figure 3: 3-way handshake process for connection establishment .

3-way handshake process: Connection establishment

- **The client sends the SYN to the server:** When the client wants to connect to the server. It sets the 'SYN' flag as 1 and sends the message to the server. The message has also some additional information like the sequence number(any random 32 bits number), the ACK is set here to 0, the window size, and the maximum segment size. For Example, if the window size is 2000 bits, and the maximum segment size is 200 bits then a maximum of 10 data segments (2000/200 = 10) can be transmitted in the connection.

- **The server replies with the SYN and the ACK to the client:** After receiving the client's synchronization request, the server sends an acknowledge to the client by setting the ACK flag to '1'. The acknowledgement number of the ACK is one more than the received sequence number. For Example, if the client has sent the SYN with sequence number = 1000, then the server will send the ACK with acknowledgement number = 10001. Also, the server sets the SYN flag to '1' and sends it to the client, if the server also wants to establish the connection. The sequence number used here for the SYN will be different from the client's SYN. The server also advertises its window size and maximum segment size to the client. After completion of this step, the connection is established from the client to the server-side.

- **The client sends the ACK to the server:** After receiving the SYN from the server, the client sets the ACK flag to '1' and sends it with an acknowledgement number 1 greater than the server's SYN sequence number to the client. Here, the SYN flag is kept '0'. After completion of this step, the connection is now established from the server to the client-side also. After the connection is being established, the minimum of the sender's and receiver's maximum segment size is taken under consideration for data transmission.

3-way handshake process: Connection termination

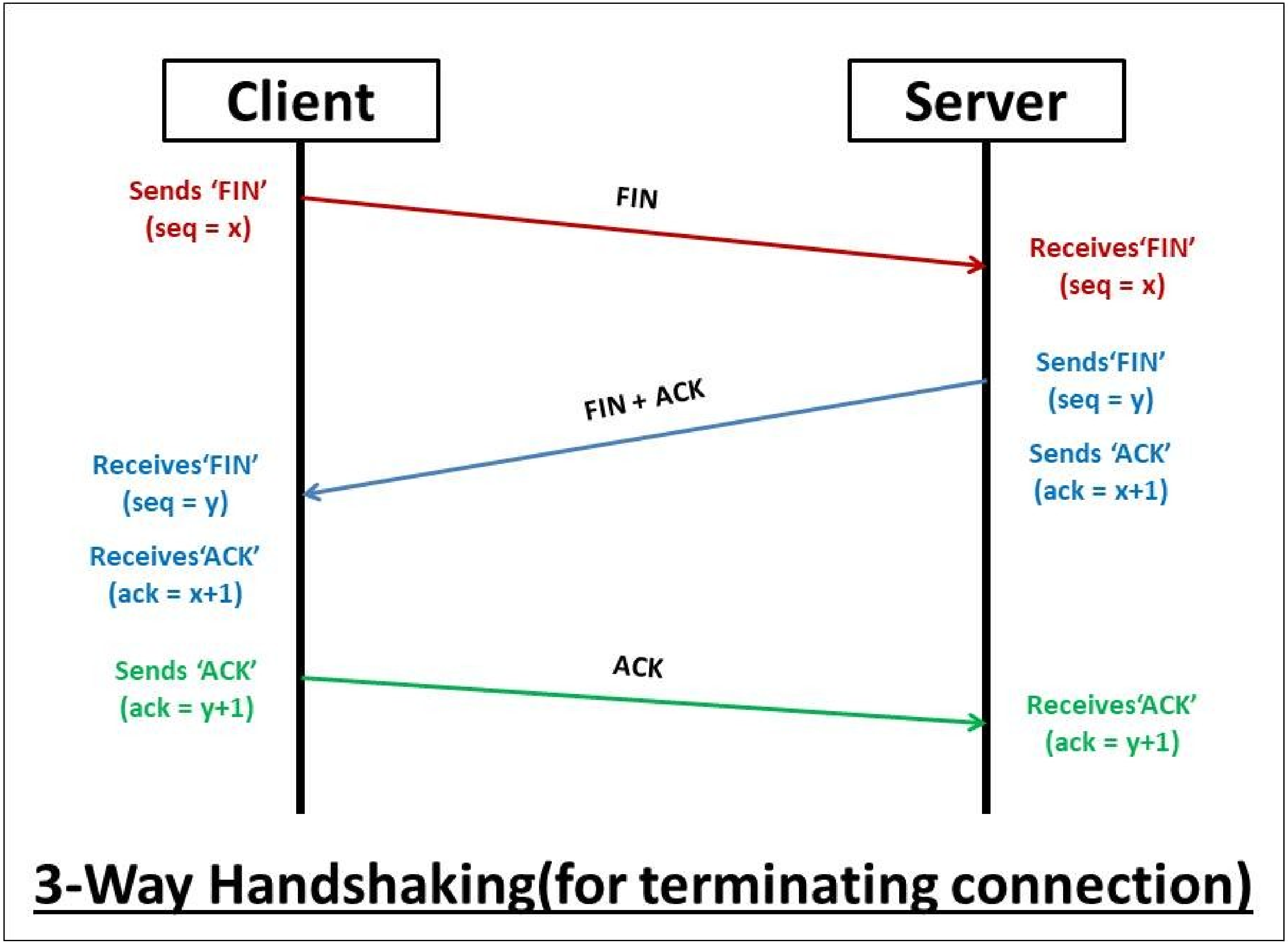


Figure 4: 3-way handshake process for connection termination.

3-way handshake process: Connection termination

1. **The client sends the FIN to the server:** When the client wants to terminate the connection. It sets the FIN flag as '1' and sends the message to the server with a random sequence number. Here, the ACK is set to 0.

2. **The server replies with the FIN and the ACK to the client:** After receiving the client's termination request, the server sends an acknowledge to the client by setting the ACK flag to '1'. The acknowledgement number of the ACK is one more than the received sequence number. For Example, if the client has sent the FIN with sequence number = 1000, then the server will send the ACK with acknowledgement number = 10001. Also, the server sets the FIN flag to '1' and sends it to the client, if the server also wants to terminate the connection. The sequence number used here for the FIN will be different from the client's FIN. After completion of this step, the connection is terminated from the client to the server-side.

3. **The client sends the ACK to the server:** After receiving the FIN from the server, the client sets the ACK flag to '1' and sends it with an acknowledgement number 1 greater than the server's FIN sequence number to the client. Here, the FIN flag is kept '0'. After completion of this step, the connection is now terminated from the server to the client-side also.

Real-world example

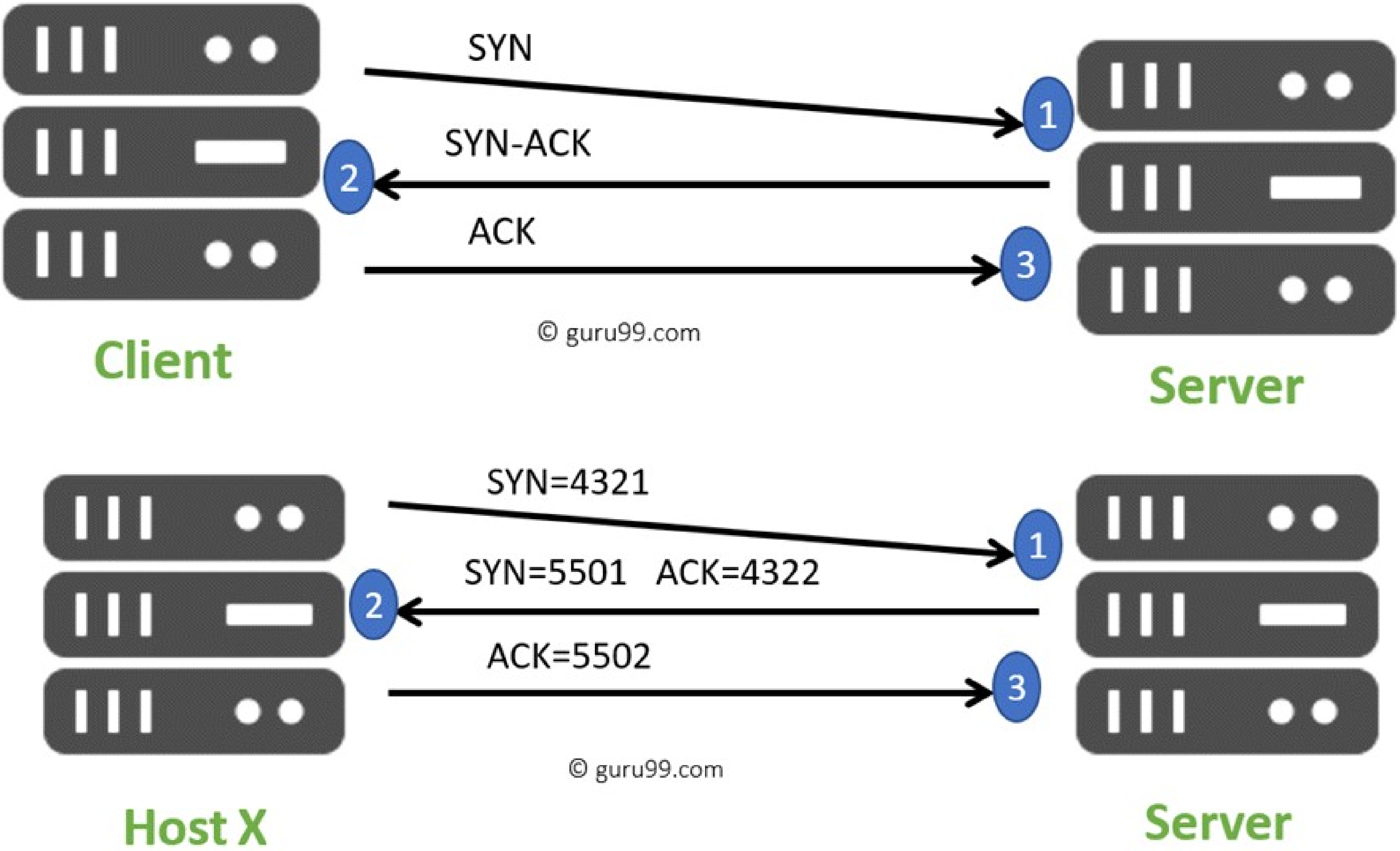


Figure 5: Real world example of 3-way handshake process .

Summary for TCP 3-way handshake

- TCP 3-way handshake or three-way handshake or TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between server and client.
- Syn use to initiate and establish a connection
- ACK helps to confirm to the other side that it has received the SYN.
- SYN-ACK is a SYN message from local device and ACK of the earlier packet.
- FIN is used for terminating a connection.
- TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server
- In the first step, the client establishes a connection with a server
- In this second step, the server responds to the client request with SYN-ACK signal set
- In this final step, the client acknowledges the response of the Server
- TCP automatically terminates the connection between two separate endpoints.

Note

User datagram protocol (UDP) operates on top of the Internet Protocol (IP) to transmit datagrams over a network. **UDP does not require the source and destination to establish a three-way handshake before transmission takes place**. Additionally, there is no need for an end-to-end connection.

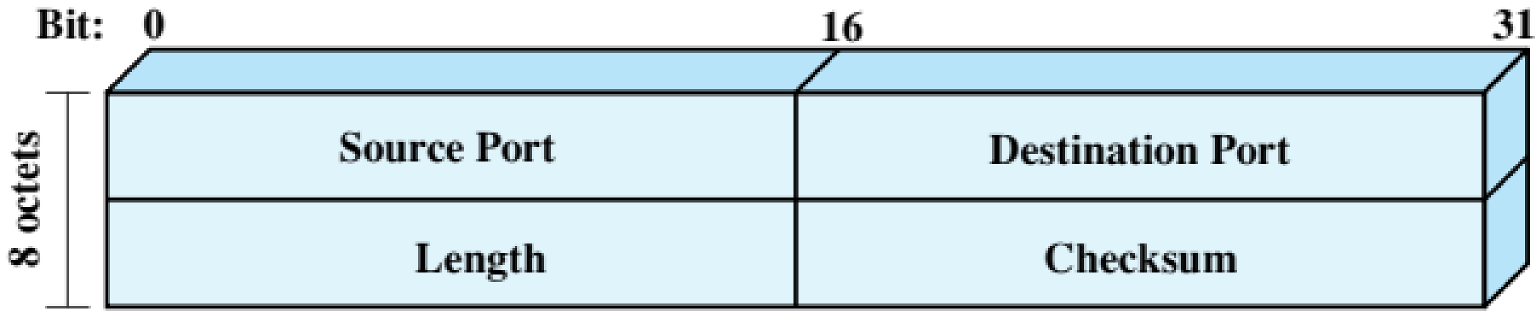
User Datagram Protocol (UDP)

- UDP provides a connectionless service for application-level procedures.
- Thus, UDP is basically an unreliable service; delivery and duplicate protection are not guaranteed.
- However, this does reduce the overhead of the protocol and may be adequate in many cases.

User Datagram Protocol (UDP)

UDP Header

- The header includes a source port and destination port.
- The Length field contains the length of the entire UDP segment, including header and data.
- The checksum is the same algorithm used for TCP and IP.
- For UDP, the checksum applies to the entire UDP segment plus a pseudoheader prefixed to the UDP header at the time of calculation and which is the same pseudoheader used for TCP.
- If an error is detected, the segment is discarded and no further action is taken.
- The Checksum field in UDP is optional. If it is not used, it is set to zero.



Source Port	Destination Port
Length	Checksum

Figure 6: UDP header.

UDP Message Format

Field Name	Size (bytes)	Description
Source Port	2	**Source Port:** The 16-bit port number of the process that originated the UDP message on the source device. This will normally be an ephemeral (client) port number for a request sent by a client to a server, or a well-known/registered (server) port number for a reply sent by a server to a client.
Destination Port	2	**Destination Port:** The 16-bit port number of the process that is the ultimate intended recipient of the message on the destination device. This will usually be a well-known/registered (server) port number for a client request, or an ephemeral (client) port number for a server reply.
Length	2	**Length:** The length of the entire UDP datagram, including both header and Data fields.
Checksum	2	**Checksum:** An optional 16-bit checksum computed over the entire UDP datagram plus a special "pseudo header" of fields. See below for more information.
Data	Variable	**Data:** The encapsulated higher-layer message to be sent.

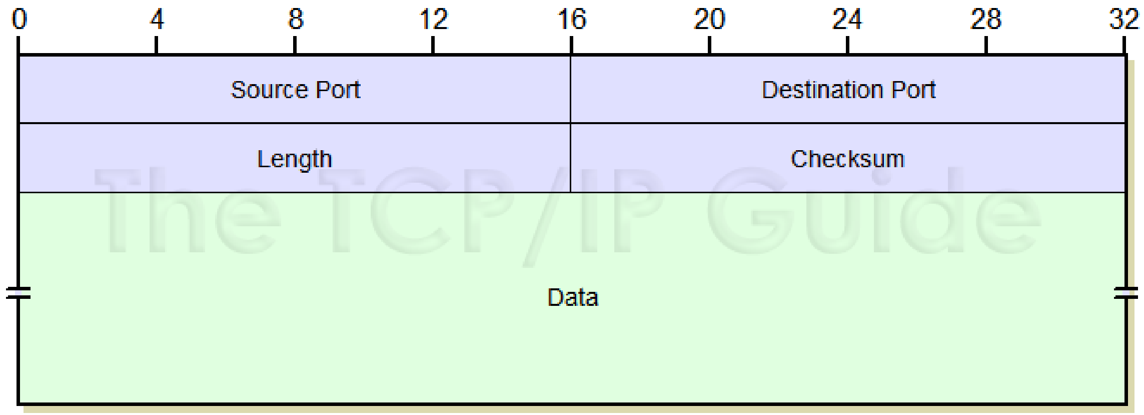


Figure 7: UDP Message Format.

References

- **Data Communications and Networking** by Forouzan, 5th edition, 2013.
- **Computer Networks** By Andrew S. Tanenbaum 5th edition, Pearson Education,2013.
- **Data and computer Communications** by William Stallings, 8th edition, Pearson,2007.
- **CCNA Cisco Certified Network Associate Study Guide**, by Todd Lammle, Wiley, 7th edition,2011.
- **Computer Networking: A Top-Down Approach**, by Kurose and Ross, Pearson Education, 6th edition,2013.

Practice Questions

Q1 Explain TCP Three-Way Handshake process

Q2 What is the importance of Sequence Number and Acknowledgement Number?

Q3 Three way handshake technique in TCP is used _________.

a) To indicate the problems.

b) To solve the problem of delayed duplicate packet.

c) For data transmission

d) All of above

Q4 The difference between TCP and UDP protocols?

Q5 Write down the name of services provided by TCP?

Q6 UDP does not ad anything to the services of IP except for providing ________communication

a) node-to-node

b) Process-to-process

c) Host-to-host

d) None of the above

Q7 In the sending computer, UDP receives a data unit from the ____________ layer.

a) Application

b) Transport

c) IP

d) None of the above

Thank you