Transport Layer (IV)

TCP (Transport Control Protocol)

- Design parameters and objectives
  - used by most popular applications, majority of Internet traffic is transported over TCP
  - significant impact on congestion behavior of the Internet
  - must operate over networks with widely-varying characteristics
  - must be robust and (relatively) simple to implement

- TCP Header
  - Typically 20 bytes. More than 20 byte if the Options field is used.

<table>
<thead>
<tr>
<th>Offsets Octet</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octet</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Bit</td>
<td>0</td>
<td>32</td>
<td>64</td>
<td>96</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Source port</td>
<td>Destination port</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>32</td>
<td>Sequence number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>64</td>
<td>Acknowledgment number (if ACK set)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>96</td>
<td>Data offset</td>
<td>Reserved</td>
<td>NS</td>
</tr>
<tr>
<td>16</td>
<td>128</td>
<td>Window Size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>160</td>
<td>Checksum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>Options (if Data Offset &gt; 5, padded at the end with &quot;0&quot; bytes if necessary)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>Urgent pointer (if URG set)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Sequence number** and **Acknowledgment number**: reliable data transfer service
- **Window size** (receive window): flow control
- **Data offset** (header length): 4-bit, specifies the length of the TCP header in 32-bit words.
- **Options**: optional, variable-length, used when a sender and receiver negotiate the maximum segment size (MSS) or as a window scaling factor for use in high-speed networks.
  - MSS is used by TCP to specify the largest amount of data a computer or communication device can receive in a single TCP segment.
  - MTU (Maximum Transmission Unit) is used by the IP layer to specify the largest packet size that can be sent over this path without suffering fragmentation.
- Flag fields:
  - **ACK**: indicate that the value carried in the acknowledgement field is valid; that is, the segment contains an acknowledgement for a segment that has been successfully received.
  - **RST, SYN, and FIN**: for connection setup and teardown
  - **CWR** and **ECE**: used in explicit congestion notification
- **PSH**: indicate that the receiver should pass the data to the upper layer immediately
- **URG**: indicate that there is data in this segment that the sending-size upper-layer entity has marked as “urgent”.

How does TCP establish and terminate a connection? How does TCP leverage those header fields to provide reliable transmission (E.g., sequence number, acknowledgment number, etc)? Let’s use an example to illustrate.

The following **http.pcapng** was a trace captured when opening [http://cs.colby.edu/courses/F19/cs333/homework/h3.html](http://cs.colby.edu/courses/F19/cs333/homework/h3.html). Filter: (ip.src == 137.146.102.176 & & ip.dst == 137.146.213.6) || (ip.src == 137.146.213.6 & & ip.dst == 137.146.102.176)

The initial sequence/ACK numbers (2347378559/2347378560) are absolute sequence numbers randomly picked from $0 \sim 2^{32}$ (wrapped around) to avoid duplication.
Go to “Preference”, find “TCP” under “Protocols,” and check the option “Relative sequence numbers.” Then, Wireshark can display relative sequence numbers instead of absolute sequence numbers (shown in the screenshot above).

As shown in the screenshot below, the sequence number of packet 29 becomes 0, and the ACK number of packet 30 becomes 1.

To build a connection, TCP uses 3-way handshake. as shown in the screenshot above.

TCP 3-way handshake

To start, the client sends a packet with SYN field in the header set to 1 and Sequence Number set to X.

After received the initial packet, the server sends an acknowledge packet with SYN set to 1, ACK field set to 1, Sequence Number set to Y, and ACK Number set to X + 1.

Once the client received the response packet, it sends an acknowledgement packet to the server, with SYN set to 0, ACK set to 1, Sequence number set to X + 1, and ACK number.

After the TCP connection is set up, both ends can transmit data (shown in the screenshot below).
- The client sends a HTTP GET request to the server.
- The server sends an acknowledgement to the client, followed by a response to the GET request that includes the file the client request.
- The client sends an acknowledgment to the server after received the response.

- The next step is to close the TCP connection (shown in the screenshot below).
- To start the closing, either the server or the client can initialize the closing. In the above trace, the server sends a packet with FIN field in the header set to 1 and ACK set to 1.
- Once the close process starts, both ends cannot send data anymore.
- The client sends an acknowledge after received this close message with ACK set to 1.
- Then, the server also sends a close message to the client with FIN set to 1.
- The client sends an acknowledge packet to the server after received the server’s close message.

- The diagram gives a more detailed illustration including the state transition. Please note that the client initialize the closing in this diagram.
- We can draw a sequence diagram for the HTTP trace shown above to better understand the process.

- Please note that TCP uses sequence and acknowledgement numbers to provide reliability.

_Disclaimer: Notes adapted from the textbook and online resources._