4.3. The Transmission Control Protocol

The Transmission Control Protocol (TCP) was initially defined in RFC 793. Several parts of the protocol have been improved since the publication of the original protocol specification [10]. However, the basics of the protocol remain and an implementation that only supports RFC 793 should interoperate with today’s implementation.

TCP provides a reliable bytestream, connection-oriented transport service on top of the unreliable connectionless network service provided by IP. TCP is used by a large number of applications, including:

- Email (SMTP, POP, IMAP)
- World wide web (HTTP, ...)
- Most file transfer protocols (ftp, peer-to-peer file sharing applications, ...)
- remote computer access: telnet, ssh, X11, VNC, ...
- non-interactive multimedia applications: flash

On the global Internet, most of the applications used in the wide area rely on TCP. Many studies [11] have reported that TCP was responsible for more than 90% of the data exchanged in the global Internet.

To provide this service, TCP relies on a simple segment format that is shown in the figure below. Each TCP segment contains a header described below and, optionally, a payload. The default length of the TCP header is twenty bytes, but some TCP headers contain options.
A TCP header contains the following fields:

- Source and destination ports. The source and destination ports play an important role in TCP, as they allow the identification of the connection to which a TCP segment belongs. When a client opens a TCP connection, it typically selects an ephemeral TCP port number as its source port and contacts the server by using the server’s port number. All the segments that are sent by the client on this connection have the same source and destination ports. The server sends segments that contain as source (resp. destination port, the destination (resp. source) port of the segments sent by the client (see figure Utilization of the TCP source and destination ports). A TCP connection is always identified by five pieces of information:
  - the IP address of the client
  - the IP address of the server
  - the port chosen by the client
  - the port chosen by the server
  - TCP

- the sequence number (32 bits), acknowledgement number (32 bits) and window (16 bits) fields are used to provide a reliable data transfer, using a window-based protocol. In a TCP bytestream, each byte of the stream consumes one sequence number. Their utilisation will be described in more detail in section TCP reliable data transfer

- the Urgent pointer is used to indicate that some data should be considered as urgent in a TCP bytestream. However, it is rarely used in practice and
will not be described here. Additional details about the utilisation of this pointer may be found in [RFC 793, RFC 1122] or [Stevens1994]

- the flags field contains a set of bit flags that indicate how a segment should be interpreted by the TCP entity receiving it:
  - the SYN flag is used during connection establishment
  - the FIN flag is used during connection release
  - the RST is used in case of problems or when an invalid segment has been received
  - when the ACK flag is set, it indicates that the acknowledgment field contains a valid number. Otherwise, the content of the acknowledgment field must be ignored by the receiver
  - the URG flag is used together with the Urgent pointer
  - the PSH flag is used as a notification from the sender to indicate to the receiver that it should pass all the data it has received to the receiving process. However, in practice TCP implementations do not allow TCP users to indicate when the PSH flag should be set and thus there are few real utilizations of this flag.

- the checksum field contains the value of the Internet checksum computed over the entire TCP segment and a pseudo-header as with UDP
- the Reserved field was initially reserved for future utilization. It is now used by [RFC 3168].
- the TCP Header Length (THL) or Data Offset field is a four bits field that indicates the size of the TCP header in 32 bit words. The maximum size of the TCP header is thus 64 bytes.
- the Optional header extension is used to add optional information to the TCP header. Thanks to this header extension, it is possible to add new fields to the TCP header that were not planned in the original specification. This allowed TCP to evolve since the early eighties. The details of the TCP header extension are explained in sections TCP connection establishment and TCP reliable data transfer.
Utilization of the TCP source and destination ports

The rest of this section is organised as follows. We first explain the establishment and the release of a TCP connection, then we discuss the mechanisms that are used by TCP to provide a reliable bytestream service. We end the section with a discussion of network congestion and explain the mechanisms that TCP uses to avoid congestion collapse.