Frage: kann man den TCP-Handshake sehen ?

Datum: 2024-05-22

Contents

1 Antwort

Natürlich ... wenn es ihn gibt

TODO http/2 schafft ihn ab ...

2 Plan

1. Was ist der TCP-Handshake ?

3 Was ist der TCP-Handshake

Das TCP (Transmission Control Protocol) wurde ursprünglich im RFC 793 spezifiziert. (RFC) Die aktuelle Spezifikation ist RFC 9293 vom August 2022.

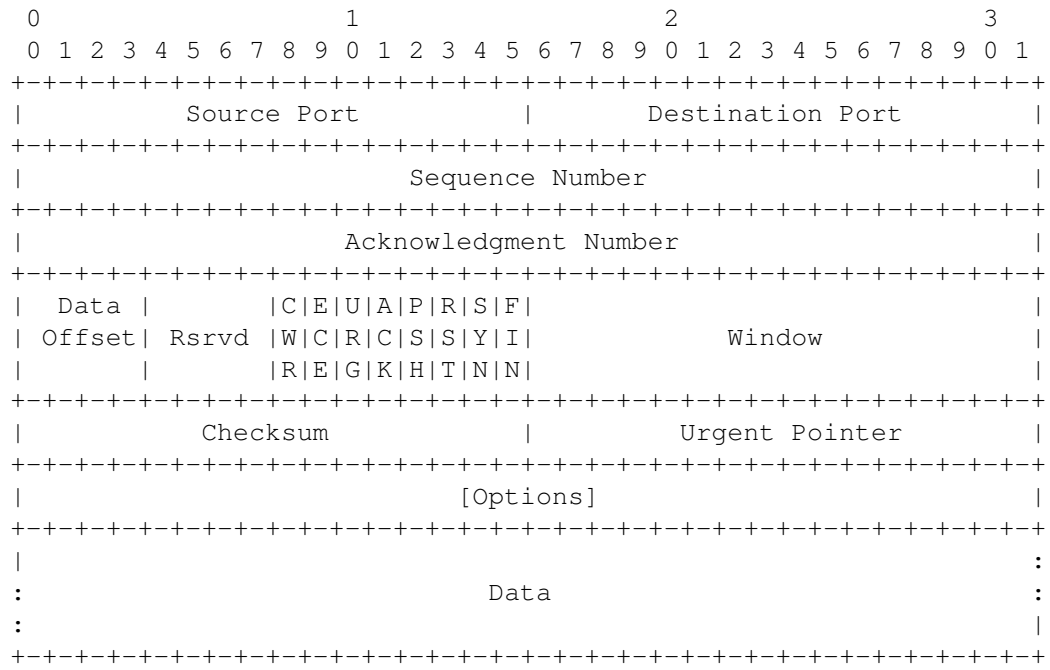
Unter *handshake* findet man folgende Zeilen:

```
For each connection there is a send sequence number and a receive sequence
number. The initial send sequence number (ISS) is chosen by the data sending
TCP peer, and the initial receive sequence number (IRS) is learned during the
connection-establishing procedure.

For a connection to be established or initialized, the two TCP peers must
synchronize on each other's initial sequence numbers. This is done in an
exchange of connection-establishing segments carrying a control bit called
"SYN" (for synchronize) and the initial sequence numbers. As a shorthand,
segments carrying the SYN bit are also called "SYNs". Hence, the solution
requires a suitable mechanism for picking an initial sequence number and a
slightly involved handshake to exchange the ISNs.

The synchronization requires each side to send its own initial sequence
number and to receive a confirmation of it in acknowledgment from the remote
TCP peer. Each side must also receive the remote peer's initial sequence
number and send a confirming acknowledgment.
```

```
  1) A --> B  SYN my sequence number is X
  2) A <-- B  ACK your sequence number is X
  3) A <-- B  SYN my sequence number is Y
  4) A --> B  ACK your sequence number is Y
```

Because steps 2 and 3 can be combined in a single message this is called the three-way (or three message) handshake (3WHS).

In der Darstellung des TCP-Headers mit Datenblock:



Note that one tick mark represents one bit position.

Figure 1: TCP Header Format

ist das SYN-Bit im 4.ten 32-Bit Block Bit 14 und ACK ist Bit 11.

4 Anschauen

Der Handshake kann nur in den übertragenen Datenpaketen passieren es gibt nicht wie bei RS232 Handshake Leitungen, also müssen die Bits sichtbar sein.

Ein Paket enthält (meist)

- den MAC-Header (Ethernet) mit Source und Destination MAC-Adressen
- den IP-Header mit Source und Destination IP-Adresse
- den TCP-Header mit Source und Destination TCP-Port *und* SYN und ACK Bits.
- danach bleibt das ACK gesetzt.

4.1 tcpdump

tcpdump ist ein Konsolenprogramm am Linux.

Wir machen einen Zugriff auf einen Webserver (Ping ist kein TCP)

```
nslookup cloud.htlinn.ac.at

Name:   cloud.htlinn.ac.at
Address: 192.168.227.112
```

Wir starten tcpdump und beschränken die Ausgabe auf Pakete von und zu 192.168.227.112:

```
tcpdump host 192.168.227.112
```

im Browser eine Verbindung zum moodle herstellen.

Der Anfang des tcp-Verkehrs:

```
09:27:14.357205 IP host1.44202 > 192.168.227.112.https: Flags [S], ...
09:27:14.359750 IP 192.168.227.112.https > host1.44202: Flags [S.], ...
09:27:14.359774 IP host1.44202 > 192.168.227.112.https: Flags [.], ...
09:27:14.362983 IP host1.44202 > 192.168.227.112.https: Flags [P.], ...
```

Der *host1* sendet

- ein Paket mit dem *S*-Flag und
- bekommt eins mit "S" und ".", das ACK-Bit wird als Punkt angezeigt, zurück und
- sendet dann ein Paket mit ACK zurück

Der *host1* sendet von einem TCP-Port (44202) an das https (443) Port.

Detailierter mit http (Port 80):

1. Aufbau SYN, keine Daten:

   ```
   09:39:08.747268 IP host1.44556 > 192.168.227.112.http: Flags [S],
     seq 991250217, win 32120, options [mss 1460,sackOK,
     TS val 966964480 ecr 0,nop,wscale 7],
     length 0
   ```

2. Antwort SYN und ACK, keine Daten:

   ```
   09:39:08.754445 IP 192.168.227.112.http > host1.44556: Flags [S.],
     seq 3394459794, ack 991250218, win 65160,
     options [mss 1250,sackOK,TS val 102147784 ecr 966964480,nop,wscale 7],
     length 0
   ```

3. Antwort von host1 an Server, ACK ohne Daten:

   ```
   09:39:08.754494 IP host1.44556 > 192.168.227.112.http: Flags [.],
     ack 1, win 251, options [nop,nop,TS val 966964487 ecr 102147784],
     length 0
   ```

4. Anfrage an Server, 191 Bytes: `GET / HTTP/1.0`:

   ```
   09:39:08.755332 IP host1.44556 > 192.168.227.112.http: Flags [P.],
     seq 1:192, ack 1, win 251, options [nop,nop,TS val 966964488
     ecr 102147784],
     length 191: HTTP: GET / HTTP/1.0
   ```

5. Antwort vom Server, nur ACK keine Daten:

   ```
   09:39:08.759613 IP 192.168.227.112.http > host1.44556: Flags [.],
     ack 192, win 508, options [nop,nop,TS val 102147789 ecr 966964488],
     length 0
   ```

6. Antwort vom Server, "Page moved permanently":

   ```
   09:39:08.760251 IP 192.168.227.112.http > host1.44556: Flags [P.],
     seq 1:544, ack 192, win 508, options [nop,nop,TS val 102147790
     ecr 966964488],
     length 543: HTTP: HTTP/1.1 301 Moved Permanently
   ```

Der erste Block in hex mit MAC-Header (tcpdump -xx)

```
0x0000:  0008 e3ff fd8c 7412 b385 4f27 0800 4500
0x0010:  003c fe47 4000 4006 ab94 0a0a e2bc c0a8
0x0020:  e370 ed7c 0050 86c7 eeef 0000 0000 a002
0x0030:  7d78 adcf 0000 0204 05b4 0402 080a 39ad
0x0040:  eea6 0000 0000 0103 0307
```

Im MAC-Header:

- Gateway MAC-Adresse: 00:08:e3:ff:fd:8c
- Host MAC-Adresse: 74:12:b3:85:4f:27

Der IP-Header beginnt bei `4500`

- `0a0a e2bc` ist hexadezimal 10.10.226.188 host1
- `c0a8 e370` ist hexadezimal 192.168.227.112 moodle

sieht man eh.

Das `0050` ist dann Dezimal Port 80.

Nach dem Destination Port ist im Header 4 Byte Sequence Number 4 Byte Acknowledgment Number und ein Byte Offset. Dann ist im `a002` das 02 das SYN-Flag.

Im nächsten Block steht dort `a012`:

```
0x0000:  7412 b385 4f27 0008 e3ff fd8c 0800 4500
0x0010:  003c 0000 4000 3f06 aadc c0a8 e370 0a0a
0x0020:  e2bc 0050 ed7c 386c c4f5 86c7 eef0 a012
0x0030:  fe88 490b 0000 0204 04e2 0402 080a 0621
0x0040:  e0f1 39ad eea6 0103 0307
```

0x12 ist ACK und SYN.

4.2 wireshark

In der GUI geht das auch.

5 Anhang

Das Dokument enthält ein schönes Diagramm der Zustandsmaschine

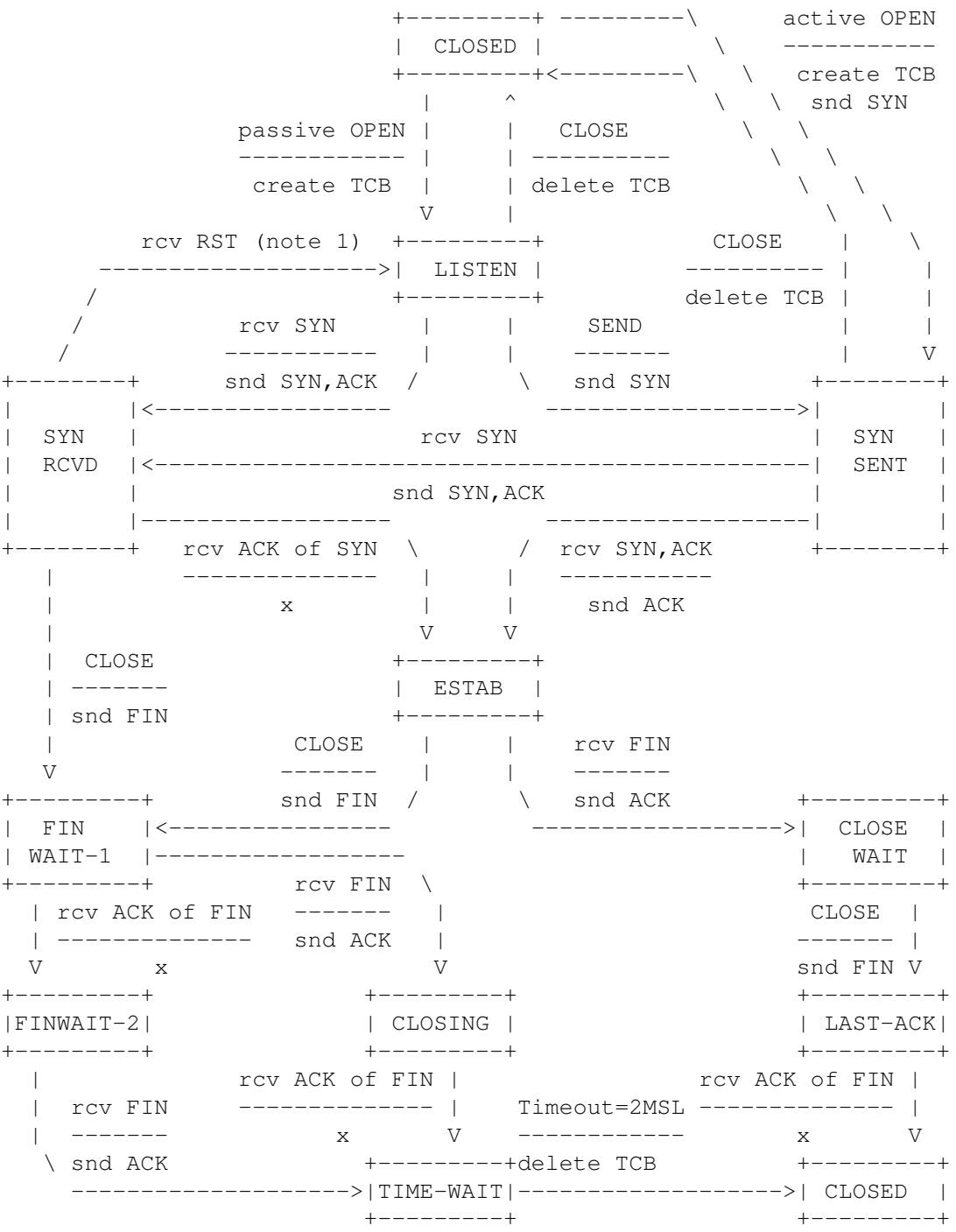


Figure 5: TCP Connection State Diagram

5.1 RFC

Request For Comment

Das Internet ist in großen Teilen eine offene Entwicklung. Jemand hatte eine Idee, schreibt einen offenen Brief mit der Aufforderung um Kommentar ... Request For Comment.