

Computer Networks

Exercise Session 14

Prof. Dr. Oliver Hahm

Frankfurt University of Applied Sciences
Faculty 2: Computer Science and Engineering
oliver.hahm@fb2.fra-uas.de
<https://teaching.dahahm.de>

February 09, 2024

General Schedule

All exercises will follow this general schedule

- Identify potential understanding problems
 - Ask your questions
 - Recap of the lecture
- Address the understanding problems
 - Answer your questions
 - Repeat certain topics
- Walk through the exercises/solutions → Some hints and guidance
 - Work time or presentation of results

TCP

You have seen . . .

- what **congestion control** is
- which **enhancements** for TCP exist
- how a TCP connection is implemented with **sockets**
- what **SYN Flood DOS attack** is

UDP

You have seen . . .

- the **functioning** and **segment structure** of UDP
- that UDP is much **simpler** compared to TCP and allows for **best-effort** communication
- how a UDP server and client is implemented with **sockets**

Other Protocols

You have seen . . .

- **SCTP** as another **connection-oriented** transport layer protocol
- **DCCP** to be used for real-time applications
- **QUIC** as the newest relevant transport layer protocol to deal with shortcomings of TCP for web traffic

Domain Name System

You have seen . . .

- DNS as an essential protocol to translate between IP addresses and domain names
- the hierarchical namespace for domain names
- that every FQDN is part of a tree
- that this tree is composed below the root servers
- what a resource record is and which type it can have

Remote Shells

You have seen . . .

- **Telnet** and **rlogin/rsh** as simple examples for remote access to a host over the Internet
- that the **Telnet** client may serve as a debugging tool
- how **SSH** represents very popular and **secure** alternative for remote access
- that SSH can be used to **tunnel** traffic through

Exercise 1: TCP Congestion Control

- 1 Describe what the slow-start phase is.

Exercise 1: TCP Congestion Control

- 1 Describe what the slow-start phase is.
The (initial) exponential growth phase.

Exercise 1: TCP Congestion Control

1 Describe what the slow-start phase is.

The (initial) exponential growth phase.

2 Describe what the congestion avoidance phase is.

Exercise 1: TCP Congestion Control

1 Describe what the slow-start phase is.

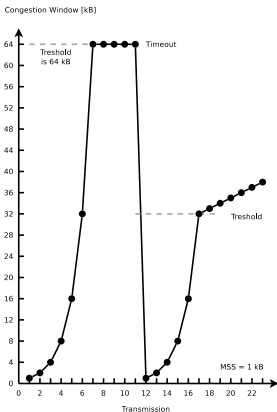
The (initial) exponential growth phase.

2 Describe what the congestion avoidance phase is.

The linear growth phase after a configured threshold has exceeded.

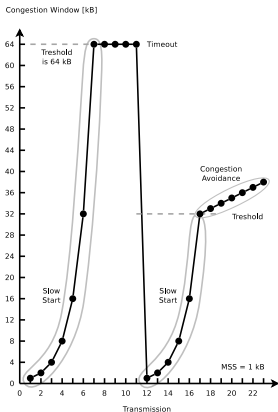
Exercise 1: TCP Congestion Control

- 4 Mark in the figure both the slow-start phase and the congestion avoidance phase.



Exercise 1: TCP Congestion Control

- 4 Mark in the figure both the slow-start phase and the congestion avoidance phase.



Exercise 1: TCP Congestion Control

6 Describe what fast retransmit is.

Exercise 1: TCP Congestion Control

6 Describe what fast retransmit is.

After three duplicate ACKs arrived, the lost segment is sent again.

Exercise 1: TCP Congestion Control

6 Describe what fast retransmit is.

After three duplicate ACKs arrived, the lost segment is sent again.

7 Describe what fast recovery is.

Exercise 1: TCP Congestion Control

6 Describe what fast retransmit is.

After three duplicate ACKs arrived, the lost segment is sent again.

7 Describe what fast recovery is.

The slow-start phase after three duplicate ACKs arrived is avoided. If three duplicate ACKs arrive, the congestion window is set directly on the threshold value.

Exercise 1: TCP Congestion Control

- 8 The concept of TCP congestion control is called **AIMD** (= Additive Increase / Multiplicative Decrease). **Describe the reason** for the aggressive reduction and conservative increase of the congestion window.

Exercise 1: TCP Congestion Control

- 8 The concept of TCP congestion control is called **AIMD** (= Additive Increase / Multiplicative Decrease). **Describe the reason** for the aggressive reduction and conservative increase of the congestion window.

The consequences of a congestion window which is too large in size are worse than for a window which is too small. If the window is too small in size, available bandwidth remains unused. If the window is too large in size, segments will get lost and must be transmitted again. This increases the congestion of the network even more! The congestion state must be left as fast as possible. Therefore, the size of the congestion window is reduced significantly.

Exercise 1: TCP Congestion Control

- 9 Describe the functioning of a Denial-of-Service attack via **SYN flood**.

Exercise 1: TCP Congestion Control

9 Describe the functioning of a Denial-of-Service attack via **SYN flood**.

A client sends many connection requests (*SYN*), but does not respond to the acknowledgments (*SYN ACK*) of the server via *ACK*. The server waits some time for the acknowledgment of the clients because the delay of the confirmation could be caused by a network issue. During this period, the address of the client and the status of incomplete connection are stored in the memory of the network stack. By flooding the server with connection requests, the table which stores the TCP connections in the network stack is completely filled. This causes the server to become unable to establish new connections. The memory consumption at the server may become this large that the main memory gets completely filled and the server crashes.

Exercise 2: Transmission Control Protocol

- 1 Consider the effect of using slow start on a line with a RTT of 10 ms. The maximum segment size is 2 kB and the receive window has a size of 24 kB. How long does it take before the first full window can be sent if no congestion occurs?

Exercise 2: Transmission Control Protocol

- 1 Consider the effect of using slow start on a line with a RTT of 10 ms. The maximum segment size is 2 kB and the receive window has a size of 24 kB. How long does it take before the first full window can be sent if no congestion occurs?

The first bursts contain 2 kB, 4 kB, 8 kB, and 16 kB bytes, respectively. The next one is 24 kB and occurs after 40 ms.

Exercise 2: Transmission Control Protocol

- 1 Consider the effect of using slow start on a line with a RTT of 10 ms. The maximum segment size is 2 kB and the receive window has a size of 24 kB. How long does it take before the first full window can be sent if no congestion occurs?

The first bursts contain 2 kB, 4 kB, 8 kB, and 16 kB bytes, respectively. The next one is 24 kB and occurs after 40 ms.

- 2 Given a maximum segment size of 1 kB: Assume that the congestion window is set to 18 kB just before a timeout occurs. How big will the window be after four consecutive successful transmissions if fast recovery is **not** used?

Exercise 2: Transmission Control Protocol

- 1 Consider the effect of using slow start on a line with a RTT of 10 ms. The maximum segment size is 2 kB and the receive window has a size of 24 kB. How long does it take before the first full window can be sent if no congestion occurs?

The first bursts contain 2 kB, 4 kB, 8 kB, and 16 kB bytes, respectively. The next one is 24 kB and occurs after 40 ms.

- 2 Given a maximum segment size of 1 kB: Assume that the congestion window is set to 18 kB just before a timeout occurs. How big will the window be after four consecutive successful transmissions if fast recovery is **not** used?

The next transmission will be 1 MSS. Then 2, 4, and 8. So after four successes, it will be 8 kB.

Exercise 2: Transmission Control Protocol

- 3 A TCP machine is sending full windows of 65,535 bytes over a 1 Gb/s channel. The channel provides a one-way delay of 10 ms. What is the maximum throughput that can be achieved? What does this mean for the efficiency of the channel usage?

Exercise 2: Transmission Control Protocol

- 3 A TCP machine is sending full windows of 65,535 bytes over a 1 Gb/s channel. The channel provides a one-way delay of 10 ms. What is the maximum throughput that can be achieved? What does this mean for the efficiency of the channel usage?

One window can be sent every 20 ms. This gives 50 windows/s, for a maximum data rate of about 3.3 million B/s. The line efficiency is then $\frac{26.4}{1000}$ Mb/s or 2.6 percent.

Exercise 2: Transmission Control Protocol

- 3 A TCP machine is sending full windows of 65,535 bytes over a 1 Gb/s channel. The channel provides a one-way delay of 10 ms. What is the maximum throughput that can be achieved? What does this mean for the efficiency of the channel usage?

One window can be sent every 20 ms. This gives 50 windows/s, for a maximum data rate of about 3.3 million B/s. The line efficiency is then $\frac{26.4}{1000}$ Mb/s or 2.6 percent.

- 4 What is the impact of the bandwidth-delay product on flow control?

Exercise 2: Transmission Control Protocol

- 3 A TCP machine is sending full windows of 65,535 bytes over a 1 Gb/s channel. The channel provides a one-way delay of 10 ms. What is the maximum throughput that can be achieved? What does this mean for the efficiency of the channel usage?

One window can be sent every 20 ms. This gives 50 windows/s, for a maximum data rate of about 3.3 million B/s. The line efficiency is then $\frac{26.4}{1000}$ Mb/s or 2.6 percent.

- 4 What is the impact of the bandwidth-delay product on flow control?

The higher the bandwidth-delay product, the more data is *stored* in the line. The more data is stored in the line, the longer a sender has to wait for an acknowledgement. The longer a sender has to wait for an ACK, the lower the efficiency.

Exercise 3: Domain Name System

- 1** DNS uses UDP instead of TCP. In case of packet loss on the network layer, there is no automatic recovery. Does this cause a problem, and if so, how is it solved?

Exercise 3: Domain Name System

- 1** DNS uses UDP instead of TCP. In case of packet loss on the network layer, there is no automatic recovery. Does this cause a problem, and if so, how is it solved?

DNS is idempotent. Operations can be repeated without harm. When a process makes a DNS request, it starts a timer. If the timer expires, it just makes the request again. No harm is done.

Exercise 3: Domain Name System

- 1** DNS uses UDP instead of TCP. In case of packet loss on the network layer, there is no automatic recovery. Does this cause a problem, and if so, how is it solved?

DNS is idempotent. Operations can be repeated without harm. When a process makes a DNS request, it starts a timer. If the timer expires, it just makes the request again. No harm is done.

- 2** In addition to being subject to loss, UDP packets have a maximum length, potentially as low as 576 bytes. What happens when a DNS name to be looked up exceeds this length? Can it be sent in two packets?

Exercise 3: Domain Name System

- 1** DNS uses UDP instead of TCP. In case of packet loss on the network layer, there is no automatic recovery. Does this cause a problem, and if so, how is it solved?

DNS is idempotent. Operations can be repeated without harm. When a process makes a DNS request, it starts a timer. If the timer expires, it just makes the request again. No harm is done.

- 2** In addition to being subject to loss, UDP packets have a maximum length, potentially as low as 576 bytes. What happens when a DNS name to be looked up exceeds this length? Can it be sent in two packets?

The problem usually does not occur. DNS names must be shorter than 256 bytes. The standard requires this. Thus, all DNS names fit in a single minimum-length packet. In other cases (for other RR types) TCP can be used.

Exercise 3: Domain Name System

- 3** The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

Exercise 3: Domain Name System

- 3** The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

Exercise 3: Domain Name System

- 3 The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

- 4 Which of the following specifies a valid domain name:
- mail.frankfurt-university.de.

Exercise 3: Domain Name System

- 3 The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

- 4 Which of the following specifies a valid domain name:
- mail.frankfurt-university.de. → valid
 - www.frankfurt/university.de.

Exercise 3: Domain Name System

- 3 The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

- 4 Which of the following specifies a valid domain name:
- mail.frankfurt-university.de. → valid
 - www.frankfurt/university.de. → invalid, only the hyphen as special character is allowed
 - sea-01.cit.frankfurt-university.de.

Exercise 3: Domain Name System

- 3 The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

- 4 Which of the following specifies a valid domain name:
- mail.frankfurt-university.de. → valid
 - www.frankfurt/university.de. → invalid, only the hyphen as special character is allowed
 - sea-01.cit.frankfurt-university.de. → valid
 - university.berlin.

Exercise 3: Domain Name System

- 3 The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

- 4 Which of the following specifies a valid domain name:
- mail.frankfurt-university.de. → valid
 - www.frankfurt/university.de. → invalid, only the hyphen as special character is allowed
 - sea-01.cit.frankfurt-university.de. → valid
 - university.berlin. → valid
 - www1.frankfurt-university.de.

Exercise 3: Domain Name System

- 3 The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

- 4 Which of the following specifies a valid domain name:
- mail.frankfurt-university.de. → valid
 - www.frankfurt/university.de. → invalid, only the hyphen as special character is allowed
 - sea-01.cit.frankfurt-university.de. → valid
 - university.berlin. → valid
 - www1.frankfurt-university.de. → valid
 - 1www.frankfurt-university.de.

Exercise 3: Domain Name System

- 3 The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

- 4 Which of the following specifies a valid domain name:
- mail.frankfurt-university.de. → valid
 - www.frankfurt/university.de. → invalid, only the hyphen as special character is allowed
 - sea-01.cit.frankfurt-university.de. → valid
 - university.berlin. → valid
 - www1.frankfurt-university.de. → valid
 - 1www.frankfurt-university.de. → valid
 - www.frankfurt.-university.de.

Exercise 3: Domain Name System

- 3 The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

- 4 Which of the following specifies a valid domain name:
- mail.frankfurt-university.de. → valid
 - www.frankfurt/university.de. → invalid, only the hyphen as special character is allowed
 - sea-01.cit.frankfurt-university.de. → valid
 - university.berlin. → valid
 - www1.frankfurt-university.de. → valid
 - 1www.frankfurt-university.de. → valid
 - www.frankfurt.-university.de. → invalid, a label must not start with a hyphen
 - myhost.local.domain.

Exercise 3: Domain Name System

- 3 The TTL of resource record may cause a delay of various hours or even days until the change of an IP address for a given name is updated for every host. Hence, would it be a good idea to use only very small values for the TTL? Explain why or why not.

The shorter the TTL, the shorter an entry might be cached. Hence, more requests are required, putting more load on the network.

- 4 Which of the following specifies a valid domain name:
- mail.frankfurt-university.de. → valid
 - www.frankfurt/university.de. → invalid, only the hyphen as special character is allowed
 - sea-01.cit.frankfurt-university.de. → valid
 - university.berlin. → valid
 - www1.frankfurt-university.de. → valid
 - 1www.frankfurt-university.de. → valid
 - www.frankfurt.-university.de. → invalid, a label must not start with a hyphen
 - myhost.local.domain. → valid, but won't resolve in the Internet

Exercise 4: Networking Applications

- 1 Describe which protocols are involved when you boot up your computer, open a web browser, go to the `https://webmail.frankfurt-university.de`, login, and send an email to `oliver.hahm@fb2.fra-uas.de`.

Exercise 4: Networking Applications

- 1 Describe which protocols are involved when you boot up your computer, open a web browser, go to the `https://webmail.frankfurt-university.de`, login, and send an email to `oliver.hahm@fb2.fra-uas.de`.

At boot time DHCP (over UDP, IPv4, and Ethernet/WLAN) or SLAAC (over IPv6) may be used to obtain an IP address

Accessing the webmail page Uses HTTP over TCP, IP and layer 2

Login to the mailserver Uses HTTP POST and IMAP (again over TCP/IP and layer 2)

Send a mail Uses HTTP POST (and maybe PUT) plus SMTP (again over TCP/IP and layer 2)

Exercise 4: Networking Applications

- 2 Explain the purpose for each of the protocols from the previous question.

Exercise 4: Networking Applications

- 2 Explain the purpose for each of the protocols from the previous question.

DHCP For address autoconfiguration

HTTP To communicate with the webserver hosting the webmail frontend

IMAP To retrieve (read) the emails

SMTP To send an email

UDP As transport layer for DHCP

TCP As reliable transport layer for all other application layer protocols

IP To address the web server or mailserver and find the best path

Ethernet/WLAN To connect your computer to your local router/gateway

Exercise 4: Networking Applications

- 2** Explain the purpose for each of the protocols from the previous question.

DHCP For address autoconfiguration

HTTP To communicate with the webserver hosting the webmail frontend

IMAP To retrieve (read) the emails

SMTP To send an email

UDP As transport layer for DHCP

TCP As reliable transport layer for all other application layer protocols

IP To address the web server or mailserver and find the best path

Ethernet/WLAN To connect your computer to your local router/gateway

- 3** Which of these protocols act on the application layer?

Exercise 4: Networking Applications

- 2** Explain the purpose for each of the protocols from the previous question.

DHCP For address autoconfiguration

HTTP To communicate with the webserver hosting the webmail frontend

IMAP To retrieve (read) the emails

SMTP To send an email

UDP As transport layer for DHCP

TCP As reliable transport layer for all other application layer protocols

IP To address the web server or mailserver and find the best path

Ethernet/WLAN To connect your computer to your local router/gateway

- 3** Which of these protocols act on the application layer?

DHCP, HTTP, SMTP, IMAP

Exercise 4: Networking Applications

- 4 The DNS *A record* for `teaching.dahahm.de` resolves to `176.9.70.110`. An alternative way to enter the URL into the browser's address field is: `https://176.9.70.110/index.html` How does the browser know whether the given name is a DNS name or an IP address?

Exercise 4: Networking Applications

- 4 The DNS *A record* for `teaching.dahahm.de` resolves to `176.9.70.110`. An alternative way to enter the URL into the browser's address field is: `https://176.9.70.110/index.html` How does the browser know whether the given name is a DNS name or an IP address?

A label in a DNS name may not be alnumeric.

Exercise 4: Networking Applications

- 4 The DNS *A record* for `teaching.dahahm.de` resolves to `176.9.70.110`. An alternative way to enter the URL into the browser's address field is: `https://176.9.70.110/index.html` How does the browser know whether the given name is a DNS name or an IP address?

A label in a DNS name may not be alphanumeric.

- 5 When you try to access my personal web page via `https://176.9.70.110/index.html` you will get an HTTP status code 404. When you access it via `https://teaching.dahahm.de/index.html` you will get HTTP status code 200. Explain the meaning of both status codes. Can you imagine why the result is different?

Exercise 4: Networking Applications

- 4 The DNS *A record* for `teaching.dahahm.de` resolves to `176.9.70.110`. An alternative way to enter the URL into the browser's address field is: `https://176.9.70.110/index.html` How does the browser know whether the given name is a DNS name or an IP address?

A label in a DNS name may not be alnumeric.

- 5 When you try to access my personal web page via `https://176.9.70.110/index.html` you will get an HTTP status code 404. When you access it via `https://teaching.dahahm.de/index.html` you will get HTTP status code 200. Explain the meaning of both status codes. Can you imagine why the result is different?

The webserver manages multiple *vhosts*. If no hostname is given, a default configuration may be used (or not).

Exercise 4: Networking Applications

- 4 The DNS *A record* for `teaching.dahahm.de` resolves to `176.9.70.110`. An alternative way to enter the URL into the browser's address field is: `https://176.9.70.110/index.html` How does the browser know whether the given name is a DNS name or an IP address?

A label in a DNS name may not be alphanumeric.

- 5 When you try to access my personal web page via `https://176.9.70.110/index.html` you will get an HTTP status code 404. When you access it via `https://teaching.dahahm.de/index.html` you will get HTTP status code 200. Explain the meaning of both status codes. Can you imagine why the result is different?

The webserver manages multiple *virtual hosts*. If no hostname is given, a default configuration may be used (or not).

- 6 For the exchange of emails more than one protocol is used. Name at least two of them and explain the provided service for each of them.

Exercise 4: Networking Applications

- 4 The DNS *A record* for `teaching.dahahm.de` resolves to `176.9.70.110`. An alternative way to enter the URL into the browser's address field is: `https://176.9.70.110/index.html` How does the browser know whether the given name is a DNS name or an IP address?

A label in a DNS name may not be alphanumeric.

- 5 When you try to access my personal web page via `https://176.9.70.110/index.html` you will get an HTTP status code 404. When you access it via `https://teaching.dahahm.de/index.html` you will get HTTP status code 200. Explain the meaning of both status codes. Can you imagine why the result is different?

The webserver manages multiple *vhosts*. If no hostname is given, a default configuration may be used (or not).

- 6 For the exchange of emails more than one protocol is used. Name at least two of them and explain the provided service for each of them.

SMTP is used to between MTAs and for sending mails from the MUA. IMAP and POP can be used to retrieve mails from the server.

Exercise 5: Do some research

- 1 The FTP protocol specification requires two ports. Why?

Exercise 5: Do some research

1 The FTP protocol specification requires two ports. Why?

FTP needs two ports (one for sending and one for receiving) because it was originally designed to operate on Network Control Program (NCP), which was a simplex protocol that utilized two port addresses, establishing two connections, for two-way communications.

Exercise 5: Do some research

- 1 The FTP protocol specification requires two ports. Why?

FTP needs two ports (one for sending and one for receiving) because it was originally designed to operate on Network Control Program (NCP), which was a simplex protocol that utilized two port addresses, establishing two connections, for two-way communications.

- 2 Explain the term *Open Relay*.

Exercise 5: Do some research

1 The FTP protocol specification requires two ports. Why?

FTP needs two ports (one for sending and one for receiving) because it was originally designed to operate on Network Control Program (NCP), which was a simplex protocol that utilized two port addresses, establishing two connections, for two-way communications.

2 Explain the term *Open Relay*.

A SMTP should only accept mails that it can deliver locally or forward (*relay*) mails from an authenticated and authorized user. If a mail server relays all mails of any user it its called an *open relay* and can be exploited to send spam mails.

Exercise 5: Do some research

- 3 Basically all relevant protocols on the layers above 2 and below 7 have been specified by the IETF. Name two protocols on the Application Layer which has also been specified by the IETF and two protocols which have **not**.

Exercise 5: Do some research

- 3** Basically all relevant protocols on the layers above 2 and below 7 have been specified by the IETF. Name two protocols on the Application Layer which has also been specified by the IETF and two protocols which have **not**.

HTTP or SMTP Are specified by the IETF, MQTT is specified by OASIS and the Signal Protocol by the Signal Technology Foundation.

Exercise 5: Do some research

- 3** Basically all relevant protocols on the layers above 2 and below 7 have been specified by the IETF. Name two protocols on the Application Layer which has also been specified by the IETF and two protocols which have **not**.

HTTP or SMTP Are specified by the IETF, MQTT is specified by OASIS and the Signal Protocol by the Signal Technology Foundation.

- 4** Name two popular software projects that implement the HTTP protocol.

Exercise 5: Do some research

- 3** Basically all relevant protocols on the layers above 2 and below 7 have been specified by the IETF. Name two protocols on the Application Layer which has also been specified by the IETF and two protocols which have **not**.

HTTP or SMTP Are specified by the IETF, MQTT is specified by OASIS and the Signal Protocol by the Signal Technology Foundation.

- 4** Name two popular software projects that implement the HTTP protocol.

Mozilla Firefox, Chromium, Microsoft Edge, Apache Webserver, lighttpd, nginx ...