* + 1. Which layers are included in the TCP/IP model?

Application, Transport, Internet, Link

* + 1. What are the advantages and disadvantages of using a layer model?

Advantages:

1. It makes communication between different applications and types of computers easy.
2. Changes in one of the layers does not affect the layers

Disadvantages:

1. Overhead, layered models make no distinction between sending data across a network with two clients and across one with two million clients.
2. The higher layers cannot access the lower layers in any way.

Ports

* 1. What is the purpose of using ports?

Differentiates connections between different services or processes

* 1. In total there are 65536 ports and one usually divide them into three areas. What are these areas called and which port range belong to which area?

Well-known ports(or system ports); 1-1023, registered ports 1024-49151, Dynamic/Private/ephemeral ports 49152-65535

* 1. What is the default port for HTTP?

Port 80

* 1. Which is the standard port for SMTP?

Port 25

HTTP

* 1. What is the purpose of the HTTP protocol?

To transfer data across the internet

* 1. What response code is received from a web server if everything has gone well?

200 OK

* 1. What response code is obtained if the web server cannot find resource that is in demand?

1. Not found
   1. Which two response codes, you can get if you do not have the rights to a requested resource?
2. Unauthorized, 403 Forbidden
   1. What are the different requests can be done using HTTP?

OPTIONS, GET, HEAD, POST, PUT, DELTE, TRACE, CONNECT, PATCH.

SMTP

* 1. What is the purpose of the SMTP protocol?

To transmit email over internet.

* 1. How the command appears to indicate the sender’s address to SMTP?

“MAIL” usage: “MAIL from:<source email address>”

* 1. How the command appears to enter the destination address under SMTP?

“RCPT” usage: “RCPT to:<destination email address>

* 1. How the command appears to indicate the actual text of an e-mail to SMTP?

“DATA” usage: “DATA” -> “<Data stream>”

* 1. Which command asks an SMTP server on which extensions it supports?

The client starts by sending EHLO and if the server does not respond it falls back to HELO

* 1. An e-mail message consists of two parts: Header and Body. Which two fields must always be in the header?

From(The sender), Date(Time and date the message was written)

DNS

* 1. What is the purpose of DNS?

To be able to use human-readable addresses which are then mapped to IP addresses so as to make it

* 1. What type of DNS resource record should you ask for if you want to know the IPv4 address for a domain?

Type: A id: 1

* 1. What DNS record should you ask for if you want to know the IPv6 address for a domain?

Type: AAAA id: 28

Wireshark

* + 1. How can you define a filter in Wireshark to only see the traffic that contains the HTTP?

Set capture filter to “port 80”

* + 1. How follow a specific TCP stream in wireshark?

Right click a packet in the stream and go follow -> tcp stream or filter the stream by “tcp.stream eq ‘X’”

2.1.3 Ask for the resource /art.txt

2.1.4 Ask for resource /layers.html

2.1.5 Ask for resource /grades.txt

/art

1. How did your conversation with the Web server look like?

Request -> response

1. What response code you got?

200 OK

1. What are response codes?

Standard responses to the clients requests

1. What type of content is in the response from the web server?

Text/plain

/layers.html

1. How did your conversation with the Web server look like?

Request -> response

1. What response code you got?

200 OK

1. What are response codes?

Standard responses to the clients requests

1. What type of content is in the response from the web server?

Text/html

/grades.txt

1. How did your conversation with the Web server look like?

Request -> response

1. What response code you got?

200 OK

1. What are response codes?

Standard responses to the clients requests

1. What type of content is in the response from the web server?

Text/plain containing html

* + 1. What are the IP addresses of both sender & receiver?

Sender: 10.100.16.211 Receiver: 130.237.177.253

* + 1. Between which ports the packet was sent?

Source:65059 Destination: 80

* + 1. Which transport protocol used?

TCP

* + 1. How large is the package in bytes?

Request: 56 bytes. Response: 407 bytes

* + 1. Between which MAC addresses the packet was send?

Source: 40:e2:30:cf:d8:47 Destination: 00:09:0f:09:00:18

3.1 Which transport protocol was used by DNS?

UDP

3.2 Between which ports packets were sent?

Source:53 Destination: 49775