Student name: Joel Mäenpää

Email address (prefer your @students.oamk.fi email if you have such address): t8majo03@students.oamk.fi

Save the final version of this document as PDF and submit it for peer reviews via Moodle’s workshop tool before the deadline. Last course week is for peer reviews.

# Week 1

Question 1: What is MAC address (or "physical address")?

Answer 1: A MAC, media access control, address [1] is an identifier assigned to a network interface controller to communicate on the physical network segment. MAC addresses are usually assigned by the manufacturer of the network interface controller.

[1] <https://www.guru99.com/what-is-mac-address.html>

Question 2: What is the purpose of 48-bit ethernet MAC address where all bits are just 1s (or typical hex presentation: FF:FF:FF:FF:FF:FF)?

Answer 2: It is a special reserved MAC address used for broadcast. A broadcast address [1] is a network address used to transmit to all devices connected to a communications network.

[1] <https://www.omnisecu.com/tcpip/broadcast-mac-address.php>

Question 3: What is the purpose of ARP in computer networks?

Answer 3: ARP [1] is a protocol used to map dynamic IP addresses to the hardware addresses in a local area network.

[1] <https://erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>

[1] <https://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP>

Question 4: What is "broadcast domain"?

Answer 4: A broadcast domain [1] is a collection of network devices that reach each other with Ethernet broadcasts.

[1] <https://geek-university.com/ccna/broadcast-domain-explained/>

[1] <https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/broadcast-domain>

Question 5: Define "bridging" in computer networks. What is the difference to routing?

Answer 5: Bridging [1] basically means just plugging a device into another device that has access to a larger network; allowing the bridged device to use the network device’s connection. Some key differences [2] between a bridge and a router are:

* that a bridge functions at a data link layer while a router operates at the network layer
* a router can work on more than one broadcast domain where as a bridge can work on only one

[1] <https://wiki.debian.org/BridgeNetworkConnections>

[2] <https://techdifferences.com/difference-between-bridge-and-router.html>

Question 6: What is the difference between physical and logical topology?

Answer 6: Difference between physical and logical topology [1] [2] is that physical topology is the placement and the layout of various components in a network. Logical topology refers to the data flow transmitted within a network.

[1] <https://blogs.arubanetworks.com/solutions/network-topologies-logical-vs-physical/>

[2] <https://techdifferences.com/difference-between-physical-and-logical-topology.html#KeyDifferences>

Question 7: What is the difference between public and private IPs?

Answer 7: A public IP [1] can be accessed over the Internet but private IPs [2] are not routed to the Internet and are reserved for internal use.

[1] <https://www.iplocation.net/public-vs-private-ip-address>

[2] <https://www.lifewire.com/what-is-a-private-ip-address-2625970>

Question 8: What are RFC documents?

Answer 8: RFC documents [1] are publications describing various practices written by engineers and computer scientists relevant to the Internet.

[1] <https://ietf.org/standards/rfcs/>

[1] <https://flaviocopes.com/rfc/>

[1] <http://jkorpela.fi/rfcs.html>

Question 9: What is "plain text protocol"?

Answer 9: Plain text protocol is a human readable communications protocol.

Question 10: What is "protocol overhead" (and computing overhead)? Search examples when programmers should/must take it into account.

Answer 10: Overhead [1] refers to the resources required (which don’t directly contribute to the end result) to set up an operation.

[1] <https://stackoverflow.com/questions/24879959/what-is-overhead-payload-and-header>

Question 11: Install Wireshark protocol analyzer and inspect your IP traffic (DNS requests, web browsing and such)

Answer 11: Inspected.

Question 12: With Wireshark: Capture some web browsing traffic and related DNS requests. What are those A (and maybe AAAA requests)? What protocols are used for DNS requests?

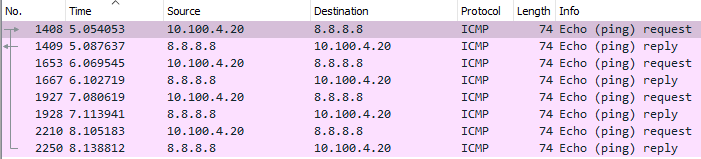
Answer 12:



DNS primarily uses the User Datagram Protocol.

Question 13: With Wireshark: Try to ping 8.8.8.8 from command line and capture the traffic. What protocols ping was using? What is the total header length of your ping request (all used protocols combined)?

Answer 13:



It uses ethernet, IPv4, and ICMP. Total header length of a ping request is 82.

Question 14: What is the MAC address of host 192.168.80.32?

Answer 14: 08:00:27:f1:90:ad

Question 15: What is the MAC address of host 192.168.80.1? Which vendor has build the ethernet chipset of host 192.168.80.1 (use Wireshark or IEEE OUI data)?

Answer 15: fc:ec:da:4a:84:d3, Ubiquiti

Question 16: Which IP address sent ICMP echo requests to this (192.168.80.32) host? Also, there is a repeating short message inside ICMP datagrams the host sent as payload. What is the repeated message?

Answer 16: 192.168.80.58, Hi there Oamk!

Question 17: What was the web page the host 192.168.0.32 visited first (full web address, not just the host)? What was the web browser or HTTP user agent used to access that web server?

Answer 17: <http://www.oamk.fi/~tkorpela/>, cURL

Question 18: What is most likely the default DNS server (IP address) used by the host 192.168.80.32?

Answer 18: 8.8.8.8

Question 19: What is the exact web address in the web server 192.168.0.88 which was visited by 192.168.80.32 via HTTP protocol? What is the hostname in "Host:" -field of HTTP GET request sent by 192.168.0.32?

Answer 19: <http://www.oamk.fi/~tkorpela/autumn.zip>, www.oamk.fi

Question 20: What is the HTTP user agent which was used to access the 192.168.0.88? What is the operating system of 192.168.0.32?

Answer 20: wget, GNU Linux

Question 21: Use Wireshark's file/export objects/HTTP to extract the ZIP file which was downloaded from the web server 193.168.100.88. What is inside the ZIP file?

Answer 21:



Question 22: Host 192.168.80.32 sent DNS requests to host 9.9.9.9. What are the requests?

Answer 22: Standard query to [www.teemukorpela.fi](http://www.teemukorpela.fi), standard query to nokia.com, and standard query to [www.youtube.com](http://www.youtube.com).

# Week 2

Question 1: What is TCP SYN bit?

Answer 1: SYN bit [1] is the synchronization flag and is used as the first step when initiating a TCP connection.

[1] <https://www.keycdn.com/support/tcp-flags>

Question 2: Explain shortly what are TCP acknowledgment and sequence numbers

Answer 2: A sequence number [1] is the byte number of the first byte of data in the TCP packet. Acknowledgement number [1] is the sequence number of the next byte the receiver expects to receive.

[1] <https://www.cs.miami.edu/home/burt/learning/Csc524.032/notes/tcp_nutshell.html>

Question 3: Explain TCP connection states: What is LISTENING? What is ESTABLISHED?

Answer 3: LISTENING [1] means that the listener will listen to connections on a specific port. ESTABLISHED [1] means that the connection has been successful and has been in fact established.

[1] <https://blog.confirm.ch/tcp-connection-states/>

Question 4: What is the purpose of TCP (or UDP) source port?

Answer 4: It [1] is a number assigned to a machine by the TCP/IP, which determines where to send responses back to.

[1] <https://www.pcmag.com/encyclopedia/term/tcpip-port>

Question 5: What is the purpose of TCP (or UDP) destination port?

Answer 5: Destination ports [1] are ports used by major Internet applications.

[1] <https://www.pcmag.com/encyclopedia/term/tcpip-port>

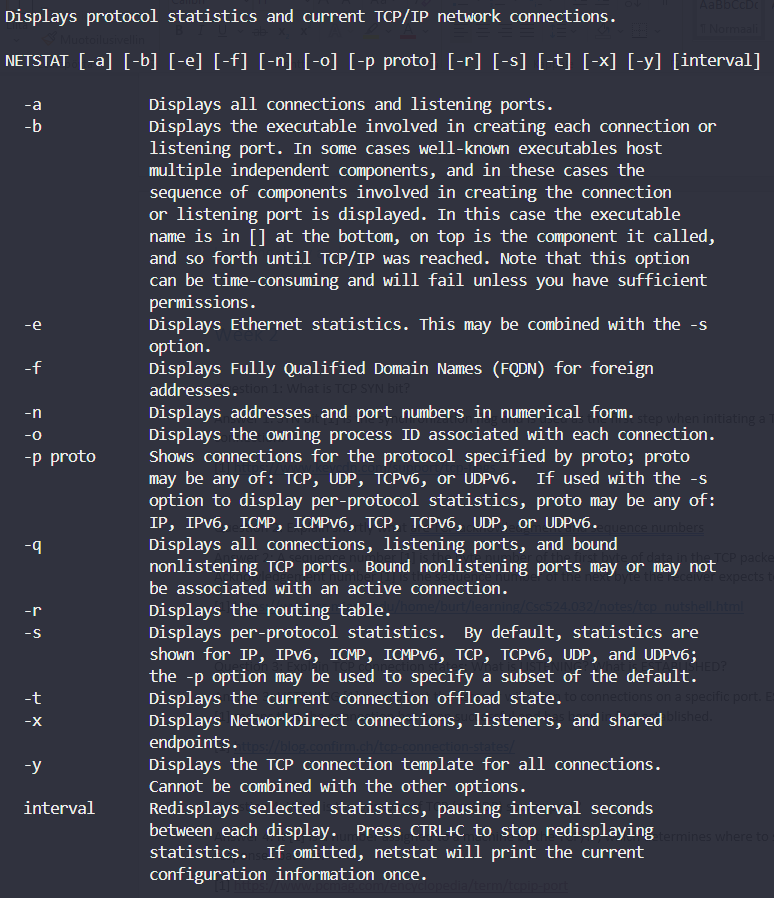
Question 6: What are the common services for TCP ports: 22, 23, 25, 80, 443, 445, 3309?

Answer 6:

* 22 — SSH
* 23 — Telnet protocol
* 25 — Simple Mail Transfer Protocol
* 80 — HTTP
* 443 — HTTP
* 445 — Microsoft-DS
* 3309 — TNS ADV

Question 7: Study available options with command line command "netstat /?" (windows) or netstat --help (linux). What different things you can see with netstat?

Answer 7:



Question 8: Why UDP is "connectionless" protocol?

Answer 8: UDP is a connectionless [1] protocol because not all network applications require the overhead of TCP. It is needed when sending continuously is important.

[1] <https://www.quora.com/In-TCP-IP-UDP-is-connection-less-why>

Question 9: Why UDP lacks flow-control features?

Answer 9: Because UDP needs to be faster than TCP.

Question 10: Why most services using UDP prefer max 512 byte UDP datagrams?

Answer 10: 512 byte payload [1] guarantees that DNS packets can be reassembled if they get fragmented when sent. Also the chance for smaller packets getting randomly dropped is lower.

[1] <https://serverfault.com/questions/587625/why-dns-through-udp-has-a-512-bytes-limit>

Question 11: When it is more reasonable to use UDP instead of TCP?

Answer 11: Basically when you just want to get an answer to a server quickly. One case is also when you’re delivering data that can be lost because new data is coming to replace the previous.

<https://stackoverflow.com/questions/1099672/when-is-it-appropriate-to-use-udp-instead-of-tcp>

Question 12: What is the length of TCP header without extra options? What about UDP header?

Answer 12: 20 bytes. 8 bytes.

Question 13: What is TCP Nagle's algorithm? As a programmer, when you don't want to use it?

Answer 13: It is an algorithm [1] to automatically concatenate a number of small buffer messages. You wouldn’t want to use it [2] in realtime and high interactive applications.

[1] <https://searchnetworking.techtarget.com/definition/Nagles-algorithm>

[2] <http://www.davidromerotrejo.com/2016/09/nagles-algorithm.html?m=1>

Question 14: Why some applications are using "keepalive" mechanisms over TCP or UDP to maintain established connection?

Answer 14: Some applications need to check for dead peers and/or prevent disconnection due to inactivity.

<https://tldp.org/HOWTO/TCP-Keepalive-HOWTO/overview.html>

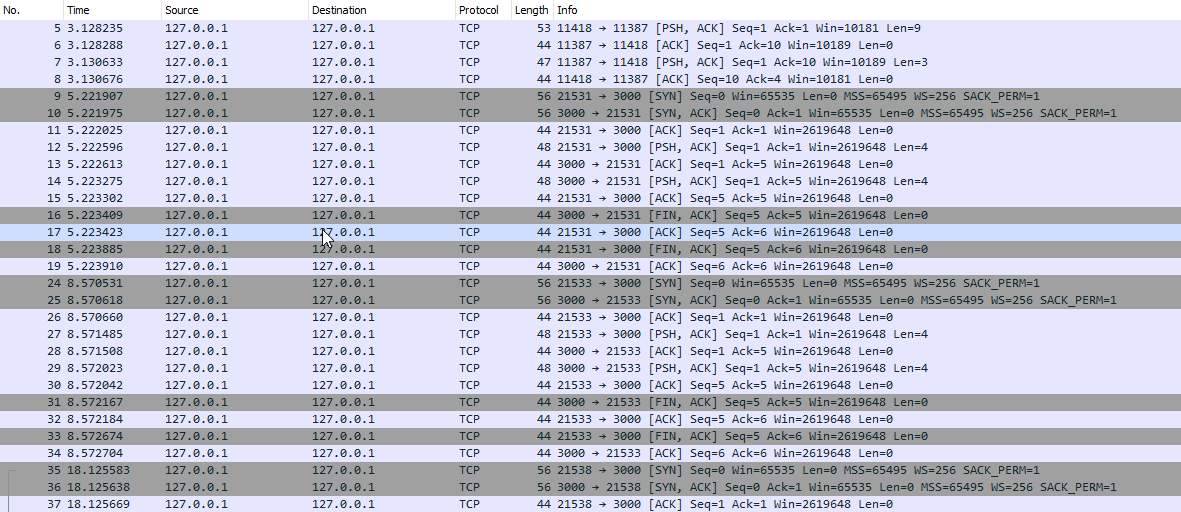
Question 15: What is a raw socket?

Answer 15: A socket [1] that allows access to the underlying transport provider.

[1] <https://docs.microsoft.com/en-us/windows/win32/winsock/tcp-ip-raw-sockets-2>

Question 16: TCP Application

Answer 16: My code can be found in: <https://github.com/Makeliiii/eldritch-iot-course/tree/master/Internet_ov_Things/TCP_application>



# Week 3

Question 1: Nnnn

Answer 1: Nnnn

Question 2: Nnnn

Answer 2: Nnnn

Question 3: Nnnn

Answer 3: Nnnn

Question 4: Nnnn

Answer 4: Nnnn

…

# Week 4

Question 1: Nnnn

Answer 1: Nnnn

Question 2: Nnnn

Answer 2: Nnnn

Question 3: Nnnn

Answer 3: Nnnn

Question 4: Nnnn

Answer 4: Nnnn

…

# Week 5

Question 1: Nnnn

Answer 1: Nnnn

Question 2: Nnnn

Answer 2: Nnnn

Question 3: Nnnn

Answer 3: Nnnn

Question 4: Nnnn

Answer 4: Nnnn

…

# Week 6

Question 1: Nnnn

Answer 1: Nnnn

Question 2: Nnnn

Answer 2: Nnnn

Question 3: Nnnn

Answer 3: Nnnn

Question 4: Nnnn

Answer 4: Nnnn

…

# Week 7

Question 1: Nnnn

Answer 1: Nnnn

Question 2: Nnnn

Answer 2: Nnnn

Question 3: Nnnn

Answer 3: Nnnn

Question 4: Nnnn

Answer 4: Nnnn

…

# Week 8

Question 1: Nnnn

Answer 1: Nnnn

Question 2: Nnnn

Answer 2: Nnnn

Question 3: Nnnn

Answer 3: Nnnn

Question 4: Nnnn

Answer 4: Nnnn

…