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?

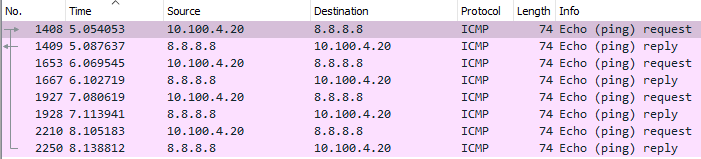
Answer 12:



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: Nnnn

Answer 1: Nnnn

Question 2: Nnnn

Answer 2: Nnnn

Question 3: Nnnn

Answer 3: Nnnn

Question 4: Nnnn

Answer 4: Nnnn

…

# 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

…