Preparation Lab 2: EITF45 - André Frisk

ARP

1. What is the purpose of an ARP request? To find MAC-address for a host-computer if you know the IP-address

2. Does ARP use IP headers? No

3. What MAC destination address is an ARP request ALWAYS sent to? To the Ethernet broadcast address FF:FF:FF:FF:FF:FF

4. What MAC destination address is an ARP reply sent to? To the host MAC-address that sent away the request

5. Exactly what information does an ARP request contain? The packet contains the source MAC address, the source IP address and the destination IP address

6. Exactly what information does an ARP reply contain? Two MAC-addresses, one from the replying host and one from the host that sent the request

DNS

7. What is the purpose of a DNS request? To ask for the IP address associated with the domain name typed in on the internet. The DNS request is sent from the user's computer (DNS client) to a DNS server which will give the IP address for the domain name

8. When a DNS request is sent to a DNS server on another subnet, what IP destination address will be used in the IP header?

The IP address wont change, the IP address is to the requested DNS server

9. When a DNS reply is sent by a DNS server to host on another subnet, what IP destination address will be used in the IP header?

The IP address is to the one who sent the DNS request

10. When a DNS reply is sent by a DNS server to a host on another subnet, what MAC destination address will be used in the MAC header?

The MAC address goes to the router who sent over the packet to the subnet and therefore to the destination who sent the DNS request

Networking

11. When an IP packet is transmitted to a host on another subnet, what IP address will be used in the destination field of the IP header?

The destination IP address used in the beginning

12. When an IP packet is transmitted to a host on another subnet, what MAC address will be used in the destination field of the MAC header?

The MAC address will change whenever it reaches a new destination, so the MAC address will be the next hop to get to the destination, will most likely get the destination MAC address after being transported to the router

13. When a switch forwards a packet, how will the destination MAC address be affected? It will not be affected because the switch works at layer 2, the switch only works with MAC-addresses

14. When a switch forwards a packet, how will the destination IP address be affected? The IP-address is irrelevant because the switch doesn't take care of IP-addresses.

15. When a router forwards a packet, how will the destination MAC address be affected? The MAC-address will change when we go from our router, to the destination router and to the destination.

16. When a router forwards a packet, how will the destination IP address be affected? The IP-address will be changed to the destination IP-address of the destination on the other net as we change router.

17. Describe the classful addressing method. A classful network is a network addressing architecture used in the Internet, the method divides the IP address space for Internet Protocol version 4 (IPv4) into five address classes based on the leading four address bits. Classes A, B, and C provide unicast addresses for networks of three different network sizes. Class D is for multicast networking and the class E address range is reserved for future or experimental purposes.

18. Describe the classless addressing method. Classless Addressing is an improved IP Addressing system. It makes the allocation of IP Addresses more efficient. It replaces the older classful addressing system based on classes. It is also known as Classless Inter Domain Routing (CIDR). To know which bits that form host-id respectively net-id a bit-mask belongs to a IP-address.

ARP – Address Resolution Protocol

Why are previous mappings cached in the first place?
To simplify, instead of sending ARP-Requests all the time the computer can save the MAC-address to access the destination easier and more frequently (if the MAC-address isn't switched or the timer is out).

Describe your network environment. That is, where are you, and what type of Internet access do you have?
Im at home in Tomelilla. We use Fiber with 100/100 MBit/s.

What is your computer's current IPv4 address?
192.168.1.36

Is this a private or public IPv4 address?
Private

What is your public IPv4 address?
85.30.178.52

Explain how NAT mapping from private to public IP addresses works!
NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

What MAC addresses do your computer have (specify which address belongs to which network interface)?
B2-68-E6-F0-07-61 (Wireless LAN adapter Local Area Connection* 1, Microsoft Wi-Fi Direct Virtual Adapter)
F2-68-E6-F0-07-61 (Wireless LAN adapter Local Area Connection* 2, Microsoft Wi-Fi Direct Virtual Adapter #2)
B0-68-E6-F0-07-61 (Wireless LAN adapter WiFi, Realtek RTL8822BE 802.11ac PCIe Adapter)
B0-68-E6-F0-07-62 (Ethernet adapter Bluetooth Network Connection, Bluetooth Device (Personal Area Network))

How many address pairs are cached (if any)? Give an example of an address pair that is cached.
13 pairs.

```
Internet Address      Physical Address      Type
```

```
192.168.1.1          e8-37-7a-7c-52-ae     dynamic
```

Router

What is the relationship between the ping program and ICMP echo packets?
Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply.

Consider an organization with 4000 hosts. Divide the hosts into two subnets containing 1000 and 3000 hosts. Choose network IDs and define the subnet masks so that the organization's requirements are fulfilled and the address space is as small as possible.
To be able to host for 4000 hosts more than 4000 IP-addresses is needed, which will require 12 bits which will be 2^12 = 4096-2 = 4094 addresses which is bigger than 4000, so that's confirmed working. So, the whole organisation got a subnet mask of 255.255.240.0 (using the Host's formula, 2^12 – 2 = 4094 which means there will be 12 zeros starting from the right to the left, 11111111.11111111.11110000.00000000).

In case of 3000 hosts, it requires still 12 bits and the subnet mask will be 255.255.240.0. However, on 100 hosts it requires 10 bits which will give using Host's formula 2^10 -2 = 1022 addresses which is enough and hence the subnet mask will be 11111111.11111111.11111100.00000000 which is 255.255.252.0

ANSWER: 3000 hosts – 255.255.240.0 and 1000 hosts – 255.255.252.0

Use the table in Lab2-instructions:
What is this computer's limited broadcast IP address?
The one using a destination IP of 255.255.255.255 which is Gateway 10.0.12.10

What is this computer's directed broadcast IP address?
The one using a destination IP of 10.255.255.255 which is Gateway 10.0.12.10

Which of the rows apply if you are sending a packet to IP address 10.0.12.100? Why?
As this address is outside of the subnet it must be sent to the router that is connected to the rest of the network, the row applied to this is the last one, as the default gateway is the router and it must be sent to this one if the packet shall be sent to another subnet. Also, the third (directed broadcast) as the IP is not in the same subnet it must be broadcasted to the specified subnet which a directed broadcast does, it sends the packet to a subnet.

Which of the rows apply if you are sending a packet to IP address 10.1.12.100? Why?
This one is outside of the router as the net-id is not the same, so it must go through the default gateway (last one) to send it away to the destination which is not within the subnet.

What is the IP address of the computer containing the routing table? Explain how you found your answer!
10.0.12.1, if a route has been made the default gateway which is the IP address of the computer containing the routing table is the option where the net mask and destination is 0.0.0.0 which is in this case

Route table on own computer:
What is the IPv4 address of your computer's default gateway?
192.168.1.1 (route print)

Is your computer connected to a subnet?
Yes, 192.168.1.0/24

DNS

Use nslookup to find out the domain name of your computer!
host-85-30-178-52.sydskane.nu

Find the IP address of the domain lu.se
130.235.52.5 (using tracert)

What transport layer protocol is used? Why?
UDP. With DNS the thought is that the packets are very small which means that they rarely cause errors/wrong and thus are more suitable to use UDP over the more reliable TCP, to use TCP would cause a lot more of extra traffic because a connection set up and shut down all the time + ACK-packets. ICMP was also used but it was used by traceroute

Which destination port is used?
Port 53

Applications

What is your current Internet access capacity?
Up: 84,36 Mbit/s. Down: 29,01 Mbit/s (WiFi)

What video streaming site have you chosen, and what video are you watching?
Youtube. What Happends if You Enter the Yiga Clan Hideout Early in Zela Breath of the Wild (Non Voiced). https://www.youtube.com/watch?v=urDSe2Mf7sI&ab_channel=GamingReinvented

What is the average transmission rate uplink and downlink?
Down: 11,92 Mbit/s. Up: 0,24 Mbit/s

Is there a difference compared to the result from Bredbandskollen? Explain why!
Yes, a very big difference. This is because of throughput and bandwidth. Throughput is an actual measure of how much data is successfully transferred from source to destination, and bandwidth is a theoretical measure of how much data could be transferred from source to destination. It is not possible to transfer the full internet access capacity during this.

What transport protocol is used?
QUIC

On average, how large is a data packet from the server to your computer?
1392 bytes

What data is sent from your computer while downloading?
A "handshake" to check if the connection is still up on the server, also it is some kind of buffering for the video, YouTube buffers around 30 seconds of a video at the same time and if the person is watching longer it will buffer even more which causes bursts in the data sent and that is when the video buffers.

How many packets are sent from your computer for each packet received by your computer? How many bytes does a typical return packet contain?

Of estimated 30 received 4 are sent back. 80 bytes.

What site have you chosen, and what channel/program are you watching?

Twitch.tv. Warframe. https://www.twitch.tv/warframe

What is the average transmission uplink and downlink?

Down: 3,81 Mbit/s. Up: 0,20 Mbit/s

Is there a difference compared to the result from Bredbandskollen? Explain why!

Yes, a very big difference. This is because of throughput and bandwidth. Throughput is an actual measure of how much data is successfully transferred from source to destination, and bandwidth is a theoretical measure of how much data could be transferred from source to destination. It is not possible to transfer the full internet access capacity during this.

What transport protocol is used?

TCP and TLSv1.2

On average, how large is a data packet from the server to your computer?

1514 bytes

What data is sent from your computer while downloading?

A "handshake" to check if the connection is still up on the server, as it is a Livestream this handshake is needed more often because it is not a video on internet but a live. Here it also "buffers" but it checks if a stable connection is up, if the connection is lowered the stream will stop or decrease the quality of the video which causes lower traffic of packets.

How many packets are sent from your computer for each packet received by your computer? How many bytes does a typical return packet contain?

Of Estimated 3 received 1 is sent back. 54 bytes.

Compare your results with the results from the stored video streaming! What conclusion can you make?

The difference with stored video streaming and livestream is that my computer must send back to Twitch server and check if my connection is still there more often at it's a live video and need more data just because it is live. The download is estimated the same but the upload is way bigger on stored video streaming, this could be because of automated quality settings on the video as I'm pretty sure the YouTube video was shown in HD 60 fps and Twitch had lower video settings.

What game are you playing?

As I'm using my laptop which not is that powerful I have been approved by William to use whatever program I want (none of my other gamer friends want to fix with WireShark and it's a lot more difficult to help with it during COVID-19, plus my gaming PC is unavailable at the moment). I have chosen to use Minecraft while being connected to an online server.

What is the average transmission rate uplink and downlink?

Down: 0,20 Mbit/s (there was a spike with 5,72 Mbit/s that happened while rendering the whole world). Up: 0,09 Mbit/s

Is there a difference compared to the result from Bredbandskollen? Explain why!

Yes, a very big difference. This is because of throughput and bandwidth. Throughput is an actual measure of how much data is successfully transferred from source to destination, and bandwidth is a theoretical measure of how much data could be transferred from source to destination. It is not possible to transfer the full internet access capacity during this.

What transport protocol is used?
TCP

On average, how large is a packet from the server?
202 bytes

What data is sent from your computer while playing?
A “handshake” to check if the connection is still up on the server, the game checks the connection very frequently as it’s an online game a stable connection need to be up at all time to be able use the game.

How many packets are sent from your computer for each packet received by your computer? How many bytes does a typical return packet contain?
Almost for every 2 packet 1 is sent back. 54 bytes

Compare with the result from the video streaming. What conclusion can you make?
Minecraft and Twitch uses the same protocol and does not have the same kind of uplink or downlink, that might be because Minecraft isn’t that kind of powerful game, it would be different if it was for example in a Raid in World of Warcraft. The number of packets received and sent back is almost the same however the packets differ, Twitch packets are way bigger and got more data. Testing with a bigger more powerful game would probably give a result more similar to Twitch or even higher.

Lab work answers (The Mandatory Part):

ARP

Now, do you see any cached address pairs in the ARP cache? Which?
All the addresses that was there in the beginning still have the (incomplete) state, 192.168.3.40 192.168.3.51 192.168.3.50 192.168.3.30 192.168.3.4 192.168.3.49

What is the destination MAC address of the ARP request? What does this address represent? Which host or hosts is the ARP request aimed for?
Broadcast (ff:ff:ff:ff:ff:ff:), its tries to send out to other computers to ask if the MAC-address for the one searched for is available. The host aimed for is the one searched from within the same subnet.

The Ethernet frame's length/type field differs for frames containing ARP datagrams and frames containing ICMP datagrams! Check the difference and describe it with corresponding value's.
ARP contained 42 bytes and ICMP contained 98 bytes.

What is the source MAC address of the ARP reply?
50:e5:49:35:26:81 ← The one requested

What is the destination MAC address of the ARP reply?
1c:6f:65:d8:38:c7 ← My computer

Describe the data contents of the frame! What information is found in the payload?
The payload of the packet consists of four addresses, the hardware and protocol address of the sender and receiver hosts.
The destination and source IP-address and MAC-address

Use your findings and describe (why not a simple sketch?) how the address resolution process works! What is the function of ARP? Why is ARP needed? Why is the ARP request broadcasted? Why is the ARP reply not broadcasted?
I cant paint here so im trying to describe as good as I can. The function of ARP is to find the MAC-address to a specific IP-address so that it can send packets to it. First the host IP-address sends an ARP-request with a Broadcast to check if someone knows the MAC-address to this destination in the subnet. If a computer knows the address it sends an ARP-reply which contains the MAC-address of the destination searched for and it sends it back to the host, it is not Broadcasted because only the host who sent the request want this MAC-address at the point and thus its unnecessary to send a Broadcast.

Routing

What is the IP address of your computer's default gateway?
192.168.3.30

What is the IP address of your computer?
192.168.3.52

Is your computer connected to a subnet? If so, which?
A computer is always connected to a subnet, in this case its 192.168.3.0/24

What is the MAC address of the destination in this frame?
00:04:96:1c:3f:30

Is this the MAC address of the IP destination? Which host has this MAC address? Explain!
No, the host is my default gateway which is within my subnet. That is because the default gateway is the one who will send a packet away if something must be accessed outside of the subnet

Which network path do you think your ICMP packets took?
First it goes to the repeater which sends it to the router and then to the switch which have the address to the server.

Trace route – Explain the results!
Traceroute is a function used to see how many hops and how long it will take to reach a destination of choice, as here it was the server containing our network, the traceroute took 2,5 ms because the network is so close to us. The traceroute goes from my computer and goes up in the network drawing to the server. It does 2 hops.

Compare with your findings using the network drawing! What do you see?
That the traceroute goes through my subnet into the server directly through the network drawing.

Which path do you think it will take? Compare with the output of traceroute.
If a ping is used on a host on the same subnet the signal will just go from my computer to the other host directly. And with traceroute we see that it takes one hop less than if we did it to the server, that is because it is inside the subnet and does not have to do more hops than that.

What is the routing table entry regarding the subnet your computer is connected to?
Destination: 192.168.3.0
Gateway: *
Genmask: 255.255.255.0
Interface: eth0

Which host owns the MAC address of the destination of the first ICMP echo request? Explain!
The default gateway. That is because we don't have the MAC-address of the host (and the IP-address) we are trying to search for, so the ping program sends us to the default gateway to ask for the MAC-address to the host to be searched for so the ping program can check the ping to the host. This is because my computer doesn't recognise anything inside the subnet as it have been removed.

Compare with your notes above. What do you see?
Again if ping is trying to access the host to be searched it does not have to ask the default gateway for the address to it because the routing table is restored which means the subnet is back and it can locate anything inside the subnet.

DNS

Use nslookup to find the domain name of your computer!
lina52.three.local.lab

Explain the difference in capture output between the two connection attempts!
While doing the domain name in the terminal does one DNS request and one reply, while doing it in Firefox it does two requests and two replys, which could mean that it must first get to the server and get the address to this domain localy

Explain what will happen if you use the IP address instead of the domain name in the previous exercise.
Nothing, as the domain name is already known