Lecture 06 tutorial: Network Layer. Part 2.

During tutorials prepare a short report of your activities and show it to your tutor.
Study the following **questions** and verify the correctness of the **answers** if given.
Be aware that the exam question might be directly related to the tutorial questions

Wireshark: ARP Experiment

1. Inspect the file **ethernet-ARP-trace -1.pcap** and comment on the ARP request and response.
2. Record your own ARP request response Wireshark file. To do it you might either need to clear the ARP table/cache with **arp –d** (you need to be an administrator) or reboot your PC to have the ARP table/cache

(I suggest you start with Q4, 5, 6)

Question 1.
What is an ARP and what is it used for?

A
ARP is the Address Resolution Protocol that is used to translate the IP addresses of the computers/hosts in a **subnet** into the MAC addresses of corresponding Network Interface Cards (NICs). Since the computers/hosts in the subnet must route packets to other computers in the same subnets themselves, they must know the related MAC addresses.

Question 2.
The host A would like to send a packet to host B. How the host A can know if the host B is in the same subnet? Give an example with the subnet mask \26.

A
The host A use its own IP address, the subnet mask and the IP address of the host B to check the IP addresses are identical at the positions indicated by ones in the subnet mask.

```
IP-A         134.105.44.193  last byte:  1100 0001
IP-B         134.105.44.224  last byte:  1110 0000
IP-C         134.105.44.191  last byte:  1011 1111
Subnet mask: 255.255.255.192 last byte:  1100 0000
```

The result is: Host A and B are in the same subnet. The host C is in a different subnet.

Question 3.
Why is an ARP query sent within a broadcast frame? Why is an ARP response sent within a frame with a specific destination MAC address?

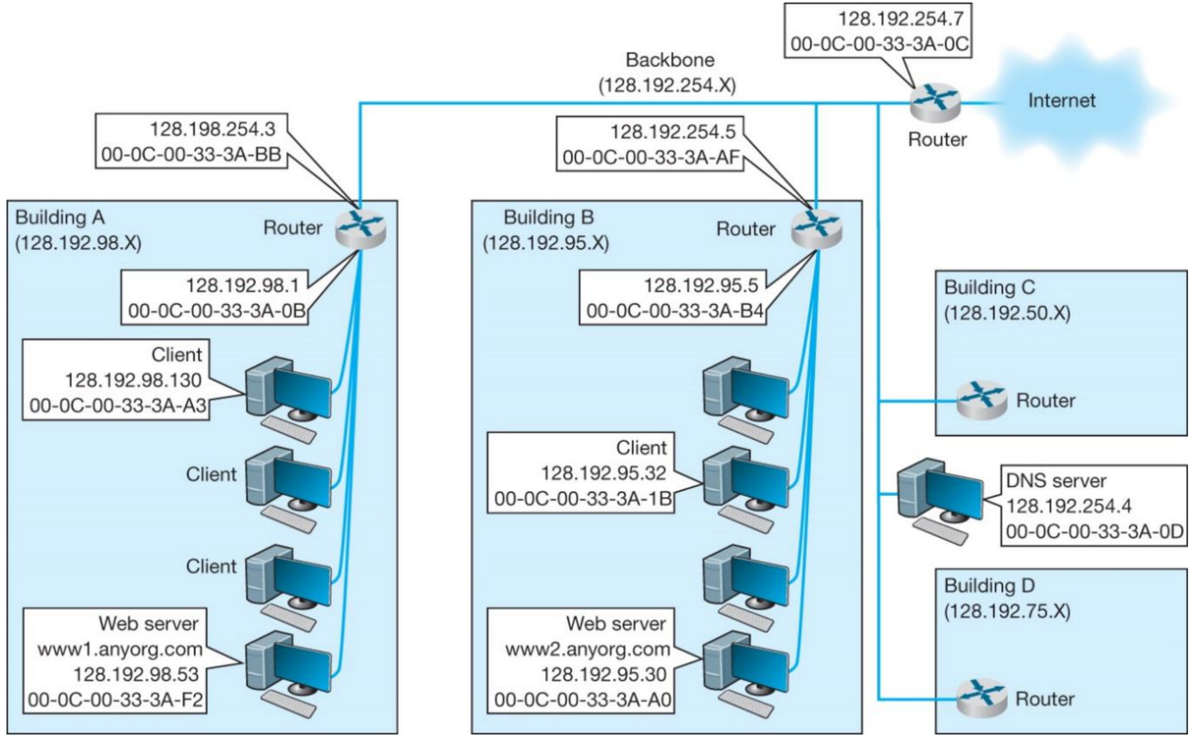
A

An ARP query is sent in a broadcast frame because the querying host does not which adapter address corresponds to the IP address in question. For the response, the sending node knows the adapter address to which the response should be sent, so there is no need to send a broadcast frame (which would have to be processed by all the other nodes on the LAN).

Question 4.

Consider the following network and write the answers to the following questions:

a. How many IP and MAC addresses does each router have?
b. How many subnets are in the network?
c. What are expected subnets masks in each subnet?



Question 5.

For the network as above, list/sketch all data link layer packets that encapsulate IP packets exchanged between the client computer, gateways and the Web server in response to the Web page request until the page is delivered to the client.

- Suppose a client computer in Building B (128.192.95.32) requests a Web page from the server in building A (www1.anyorg.com).
- The size of the Web page is approximately 2.5kB.
- Assume that the client computer, all gateways and Web servers involved **know all network layer and data link layer addresses.**
- Show only last pair of bytes of Ethernet and IP addresses.

A

Step 1: Client in B to Router in B:

E-Dst	E-Src	IP-Src	IP-Dst		
-3A-B4	-3A-1B	.95.32	.98.53	TCP	HTTP Rq

Step 2: Router in B to Router in A

-3A-BB	-3A-AF	.95.32	.98.53	TCP	HTTP Rq

Step 3: Router in A to the Web server in A:

-3A-F2	-3A-0B	.95.32	.98.53	TCP	HTTP Rq

Fill in in a similar way the steps related to the web server response

Here we are assuming that all IP and Ethernet addresses are known to all hosts. The HTTP response from server in A to client in B will travel via routers A and B.

A single Ethernet frame **carrying the HTTP response** will take the path as below

Step 1: From Server in A to Router in A

-3A-0B	-3A-F2	.98.53	.95.32	TCP	HTTP Resp

Step 2: From Router in A to Router in B

-3A-AF	-3A-BB	.98.53	.95.32	TCP	HTTP Resp

Step 3: From Router in B to Client in B

-3A-1B	-3A-B4	.98.53	.95.32	TCP	HTTP Resp

However, it will take multiple Ethernet frames to deliver the full HTTP response (size 2.5KB). As discussed in previous weeks, the maximum size of data (or payload) that an Ethernet frame can carry is 1500 bytes. Thus, we need two frames to completely deliver the HTTP response

Question 6.

For the same network consider the Client in building B requests the web page from the www1.anyorg.com server which is located in different subnet. Assume that the Client B knows only addresses as in the **configuration file** and needs to use ARP and DNS to get required IP addresses.

List/sketch all data link layer packets that encapsulate IP packets exchanged between the client computer, gateways and the Web server **in response** to the Web page request until the page is delivered to the client.

A

Follow the steps describe in slides 15, 16, 14, … (Case 3: Different Subnets, Unknown Addresses)

Question 7.

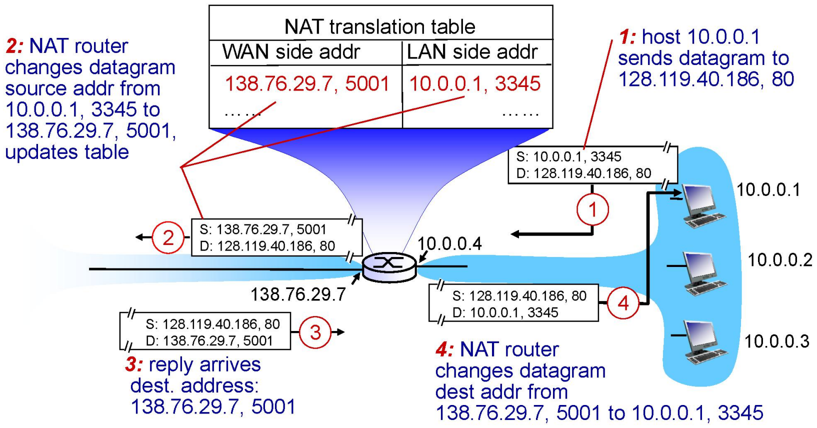
What is the Network Address Translation and why do we use it?

A

Compile an answer from slides 18 – 20

Question 8.

Consider the NAT problem as in the following figure (slide ?)



2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

1: host 10.0.0.1 sends datagram to 128.119.40.186, 80

3: reply arrives dest. address: 138.76.29.7, 5001

4: NAT router changes datagram dest addr from 138.76.29.7, 5001 to 10.0.0.1, 3345

A

Describe step-by-step how the addresses are translated. Itemize your answer.

Question 9.

Consider the Internet Control Message Protocol (ICMP)

a. What is it used for?
b. What is the format of the ICMP message?
c. What two popular commands use the ICMP?

A

a. ICMP is used by hosts and routers to communicate network-level information, e.g
   - error reporting: unreachable host, network, port, protocol

   echo request/reply (used by ping)
b. ICMP message consists of the type, code, header plus first 8 bytes of IP datagram causing error
c. The **ping** and **tracert** commands use the ICMP