17/6/2019

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 any **answers** if given.
Be aware that the exam question might be directly related to the tutorial questions

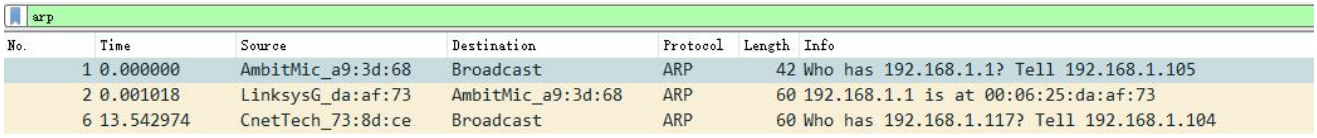
Additional Instructions: Where a **group number** is indicated, please discuss this particular question with other members of your group, prepare a short written answer and email this to your tutor before the end of the day (you may wish to verify the correctness of your answer first). This will be used to produce a set of sample answers for the class for study purposes. *Note:* You should work through all questions in the tutorials, not just ones assigned to your group. I also recommend that you complete Q4, 5 and 6 individually.

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

Answer (Group 10):

1. There are three ARP frames:



a) No.1

Frame 1 is an ARP request. The source host, which has the IP address 192.168.1.105 and the MAC address 00:d0:59:a9:3d:68, wonders the MAC address of IP 192.168.1.1. Therefore, the source host broadcasts an ARP request. The Ethernet destination MAC address is FF-FF-FF-FF-FF, which means it is a broadcast; and the target MAC address is 00-00-00-00-00-00, which means it is a unknown address. If the host with IP address 192.168.1.1 receive the frame, it will send a response to the source host.

b) No.2

Frame 2 is an ARP reply. The host with an IP address 192.168.1.1 receive frame 1 and send a reply to the source host in frame 1 to inform that required MAC address is 00:06:25:da:af:73.

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

c) No.6

Frame 6 is an ARP request. The source host, which has the IP address 192.168.1.105 and the MAC address 00:80:ad:73:8d:ce, wonders the MAC address of IP 192.168.1.117. Therefore, the source host broadcasts an ARP request. The Ethernet destination MAC address is FF-FF-FF-FF-FF, which means it is a broadcast; and the target MAC address is 00-00-00-00-00-00, which means it is a unknown address. If the host with IP address 192.168.1.117 receive the frame, it will send a response to the source host.

Unfortunately, there is no response of the broadcast according to the .pcap file.

```
> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: CnetTech_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
    Sender IP address: 192.168.1.104
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.117
```

2.

```
~  15:27:20
✔  sudo arp -d -a
Password:
169.254.31.200 (169.254.31.200) deleted
169.254.59.94 (169.254.59.94) deleted
169.254.104.31 (169.254.104.31) deleted
172.16.120.241 (172.16.120.241) deleted
172.16.120.254 (172.16.120.254) deleted
```

[...]

```
~  15:41:10
✔  arp -a
bogon (172.16.120.254) at 74:25:8a:78:e4:ec on en7 ifscope [ethernet]
```

Our own ARP request result shows as below.(figure 2)

```
    453 63.253969     Hangzhou_b5:8e:09    Broadcast           ARP          68 Who has 172.16.159.100? Tell 172.16.156.254
    456 63.578987     AmazonTe_a8:48:e6    Broadcast           ARP          50 Who has 172.16.156.254? Tell 172.16.158.52

▶ Frame 453: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
▼ Ethernet II, Src: Hangzhou_b5:8e:09 (0c:da:41:b5:8e:09), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: Hangzhou_b5:8e:09 (0c:da:41:b5:8e:09)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
    Trailer: f580738b
    Frame check sequence: 0x2264d23a [unverified]
    [FCS Status: Unverified]
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Hangzhou_b5:8e:09 (0c:da:41:b5:8e:09)
    Sender IP address: 172.16.156.254
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.159.100
```

```
0000  ff ff ff ff ff ff 0c da  41 b5 8e 09 08 06 00 01   ........ A.......
0010  08 00 06 04 00 01 0c da  41 b5 8e 09 ac 10 9c fe   ........ A.......
0020  00 00 00 00 00 00 ac 10  9f 64 00 00 00 00 00 00   ........ .d......
0030  00 00 00 00 00 00 00 00  00 00 00 00 f5 80 73 8b   ........ ......s.
0040  22 64 d2 3a                                       "d.:
```

Our own ARP response result shows as below.(figure 3)

```
    499 68.905047     Hangzhou_b5:8e:09    Apple_42:d1:f8      ARP          68 172.16.156.254 is at 0c:da:41:b5:8e:09
    500 69.323169     Hangzhou_b5:8e:09    Broadcast           ARP          68 Who has 172.16.159.100? Tell 172.16.156.254
    521 71.444953     HonHaiPr_0a:a4:b9    Broadcast           ARP          50 Who has 169.254.169.254? Tell 172.16.157.192

▶ Frame 499: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
▼ Ethernet II, Src: Hangzhou_b5:8e:09 (0c:da:41:b5:8e:09), Dst: Apple_42:d1:f8 (f0:18:98:42:d1:f8)
  ▶ Destination: Apple_42:d1:f8 (f0:18:98:42:d1:f8)
  ▶ Source: Hangzhou_b5:8e:09 (0c:da:41:b5:8e:09)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
    Trailer: 07c8c4e6
    Frame check sequence: 0x97ceb8c8 [unverified]
    [FCS Status: Unverified]
▼ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Hangzhou_b5:8e:09 (0c:da:41:b5:8e:09)
    Sender IP address: 172.16.156.254
    Target MAC address: Apple_42:d1:f8 (f0:18:98:42:d1:f8)
    Target IP address: 172.16.157.74
```

```
0000  f0 18 98 42 d1 f8 0c da  41 b5 8e 09 08 06 00 01   ...B.... A.......
0010  08 00 06 04 00 02 0c da  41 b5 8e 09 ac 10 9c fe   ........ A.......
0020  f0 18 98 42 d1 f8 ac 10  9d 4a 00 00 00 00 00 00   ...B.... .J......
0030  00 00 00 00 00 00 00 00  00 00 00 00 07 c8 c4 e6   ........ ........
0040  97 ce b8 c8                                       ....
```

Answer (Group 4):

(1) The working process of ARP protocol is that

a. First, according to the contents of the routing table on host A (192.168.1.105), IP determines that the forwarding IP address used to access host B is 192.168.1.1. Host A then checks hostB's matching MAC address in its local ARP cache.

b. if host A does not find B mapping in the ARP cache, it will ask for the hardware address of 192.168.1.1 and broadcast the ARP request frame to all host on the local network. Obviously, host A and host B are on the same local network, and host A doen not find host B's mapping in the cache, so host A ask for the hardware and broadcast the ARP request frame to all host on the local network , so the target MAC address in the request frame is 00:00:00:00:00:00. And the IP address (192.168.1.105) and MAC address (00:d0:59:a9:3d:68) of source host A are included

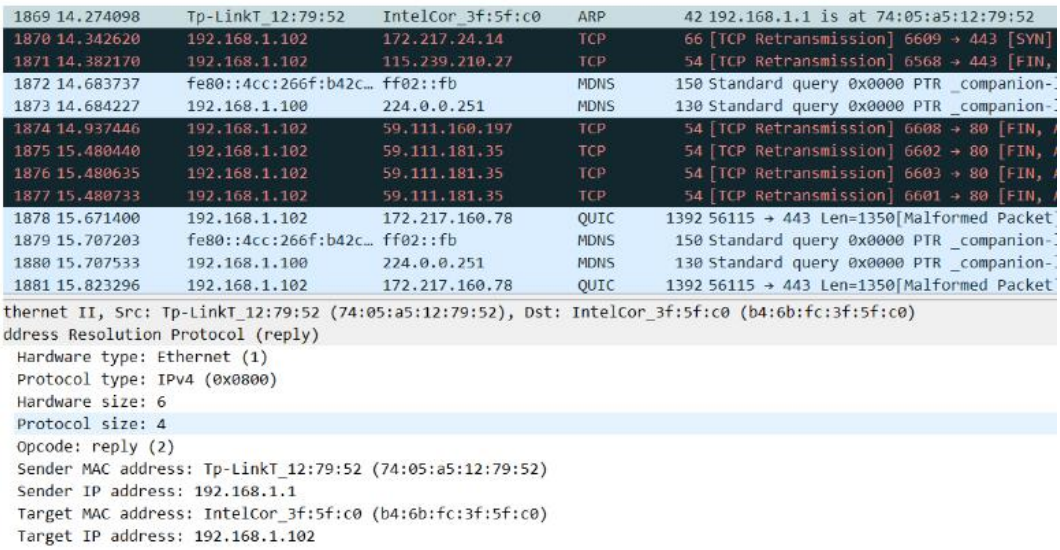
in the ARP request. Each host on the local network receives an ARP request and checks to see if it matches its IP address.

c. Host B determines that the IP address in the ARP request matches its own IP address, and adds host A's IP address (192.168.1.105) and MAC address (00:d0:59:a9:3d:68) mapping to the local ARP caches. Host B sends the ARP response message containing its MAC address (00:06:25:da:af:73) directly back to Host A.

d. When Host A receives an ARP reply from Host B, it updates the ARP cache with Host B's IP and MAC address mappings. The native cache is alive, and at the end of the lifetime, the process is repeated again. Once the MAC address of Host B is determined, Host A can send IP communication to Host B.

(2)

ARP response



Question 1.

What is an ARP and what is it used for?

Answer (Group 1):

ARP: Address Resolution protocol. The Address Resolution Protocol (ARP) is a telecommunication protocol used for resolution of network layer addresses into link layer addresses. The ARP table maintains mapping between the Physical and IP addresses.

Answer (Group 5):

What is ARP?

Address Resolution Protocol

What ARP used for?

When the host sends the information, it broadcasts the ARP request containing the target IP address to all hosts on the network and receives the return message to determine the physical address of the target;After receiving the return message, the IP address and physical address are stored in the native ARP cache for a certain period of time, and the next time the request is made, the ARP cache is directly inquired to save

resources.

Question 2.
A host A would like to send a packet to another host B or C. How can the host A can know if the receiver is in the same subnet? Consider the following example with the subnet mask \26 or 255.255.255.192.

```
IP-A          134.105.44.193
IP-B          134.105.44.224
IP-C          134.105.44.191
```

Answer (Group 2):
192 = 128 + 64 = 1100 0000 (binary form)
---
193 = 128 + 65 = 1100 0001 (binary form)
224 = 128 + 64 + 32 = 1110 0000 (binary form)
191 = 128 + 63 = 1011 1111 (binary form)
ipA AND subnet mask = ipB AND subnet mask = 134.105.44.192
ipC AND subnet mask = 134.105.44.128
SO ipA and ipB in the same subnet and ipc is not in the same subnet

Answer (Group 5):
The mask and IP binaries perform the and operation
In this example, IPA, IPB, IPC perform the and operation with 255.255.255.192, the
ResultA: 255.255.255.192
ResultB: 255.255.255.192
ResultC: 255.255.255.128
As a result, the IP-A and IP-B are in the same subnet but the IP-C

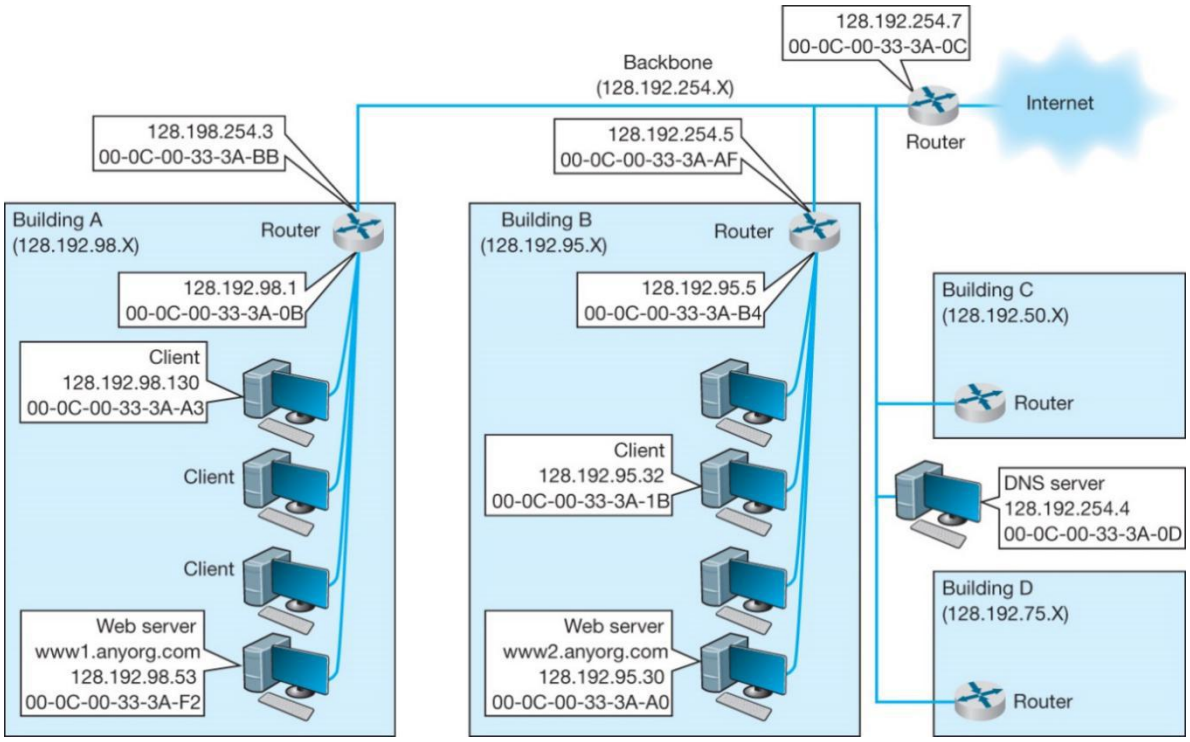
Question 3.
Why is an ARP query sent within a broadcast frame? Why is an ARP response sent within a frame with a specific destination MAC address?

Answer (Group 3):
Because we do not know the MAC address of the destination when send ARP query and can only broadcast the query.
The MAC address of the source is contained in the ARP query, so the destination can specify MAC address in ARP response.

Answer (Group 5):
The query does not know the MAC address of the destination, so it wishes the destination with the same IP address in the ARP query frame response to it only.
The ARP response frame tells the source the MAC address to itself, so that the source can then communicates with it.

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?



Answer (Group 4):
a) The router in Building A: 9 IP and Mac addresses.
The router in Building B: 9 IP and Mac addresses.
The router in Building C: 5 IP and Mac addresses.
The router in Building D: 5 IP and Mac addresses.
The router in Backbone: 5 IP and Mac addresses.
b) 5 subnets, they are 128.192.254.0, 128.192.98.0, 128.192.95.0, 128.192.50.0 and 128.192.75.0.
c) They are both 255.255.255.0 and 255.255.128.0.

Answer (Group 5):
a. The number equals to the interfaces of each router
b. 5
c. 128.192.98.0/24,
128.192.254.0/24,
128.192.95.0/24,
128.192.50.0/24,
128.192.75.0/24

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.

Answer (Group 5):

a. List/sketch all data link layer packets encapsulating IP packets exchanged between the client computer, routers and web server during the **request of the Web page.**

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 Request

Step 2: Router in B to Router in A

-3A-BB	**-3A-AF**	**.95.32**	**.98.53**	**TCP**	**HTTP Request**

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

-3A-F2	**-3A-0B**	**.95.32**	**.98.53**	**TCP**	**HTTP Request**

b. 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**	**.95.53**	**.98.32**	**TCP**	**HTTP Request**

Step 3: From Router in B to Client in B

-3A-1B	**-3A-B4**	**.95.53**	**.98.32**	**TCP**	**HTTP Request**

c. It will take multiple Ethernet frames to deliver the full HTTP response (size 2.5KB). As discussed in previous lectures, the maximum size of data (or payload) that an Ethernet frame can carry is 1500 bytes. How many frames are required to completely deliver the HTTP response?

2.5*1024=2560 B
2560/1500=1.7
So, it need 2 frames

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.

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

Answer (Group 6):
• Client B knows the IP address of its gateway/router but does not know its MAC address. Needs to broadcast an ARP request (who has 128.192.95.5 ?) inside its subnet:

brdcast	**-3A-1B**	**.95.32**	**.95.5**	**ARP**	

• The router B replies with the ARP response frame

-3A-1B	**-3A-B4**	**.95.5**	**.95.32**	**ARP**	

• Client B can now issue its DNS request (what is the IP address of www1.anyorg.com) to its DNS server through its gateway/router

-3A-B4	**-3A-1B**	**.95.32**	**.254.4**	**DNS**	**www1.anyorg.com**

• Assuming that the Gateway B knows MAC addresses in the backbone subnet, it passes the DNS request to the DNS server:

-3A-0D	**-3A-AF**	**.95.32**	**.254.4**	**DNS**	**www1.anyorg.com**

• The DNS server replies with the IP address to the Gateway B

-3A-AF	**-3A-0D**	**.254.4**	**.95.32**	**www1.anyorg.com**	**…98.53**

• The Gateway B passes the DNS response to the Client B:

-3A-1B	**-3A-B4**	**.254.4**	**.95.32**	**www1.anyorg.com**	**…98.53**

• Once the Client A knows the IP address of the web server, it follows the steps as in

– Case 2: Known Address, Different Subnet

– It requests the web page through its Gateway/router B**.**

• Prepares the Frame 1 and sends it to the subnet gateway/router B.

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

Answer (Group 5):

1. Client broadcast an ARP request.
Broadcast -3A-1B .95.32 .95.5 ARP
2. The router B replies with the ARP response frame
-3A-1B -3A-B4 95.5 95.32 ARP
3. Client now issue its DNS request (what the ip address of www1.anyorg.com) to its DNS server through its gateway/router
4. Gateway knows the MAC addresses in the backbone and it passes the DNS request to the DNS server
5. The DNS server replies with the IP address to the Gateway
6. The Gateway passes the DNS response to the client
7. Client sent http request to Bgate router
8. Bgate router to Agate router
9. Agate router to server www1.anyorg.com

Answer (Group 7):

Client B doesn't find the IP address for www1.anyorg.com in the DNS list, so it has to send DNS request to get the IP address. However, the IP for DNS server is not in the same subnet, so Client B has to sends the packet to the gateway. But it doesn't know the MAC address of the gateway, so it has to broadcast an ARP request with the IP of the gateway. (How does it know the IP of the gateway?)

Step 1: Client B broadcasts an ARP request within the subnet.

Broadcast	-3A-1B	.95.32	.95.5	ARP	

Step 2: Router B responses the ARP request.

-3A-1B	-3A-B4	.95.5	.95.32	ARP	

Step 3: Client B sends a DNS request to the gateway(Router B).

-3A-B4	-3A-1B	.95.32	.95.5	DNS	www1.

Step 4: Router B pass the DNS request to DNS server. (What if the DNS server is not directly connected to the backbones?)

-3A-0D	-3A-AF	.254.5	.254.4	DNS	www1.

Step 5: The DNS server replies with the IP address to Router B.

-3A-AF	-3A-0D	.254.4	.254.5	www1	.98.53

Step 6: Router B passes the DNS response to Client B.

-3A-1B	-3A-B4	.95.5	.95.32	www1	.98.53

Step 7: Client B finds the destination is not in the same subnet, so it sends the web request to Router B.

-3A-B4	-3A-1B	.95.32	.95.5	TCP	HTTP

Step 8: Router B passes the request to Router A. (How can Router B find the matched subnet?)

-3A-BB	-3A-AF	.254.5	.254.3	TCP	HTTP

Step 9: Router A passes the request to the destination server. (Assume the MAC address can be found in the ARP list in Router A.)

-3A-F2	-3A-0B	.98.1	.98.53	TCP	HTTP

Step 10: Server A sends response back to Router A.

-3A-0B	-3A-F2	.98.53	.98.1	TCP	HTTP

Step 11: Router A passes the response to Router B.

-3A-AF	-3A-BB	.254.3	.254.5	TCP	HTTP

Step 12: Router B passes the response to Client B.

-3A-1B	-3A-B4	.95.5	.95.32	TCP	HTTP

Question 7.

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

Answer (Group 7):

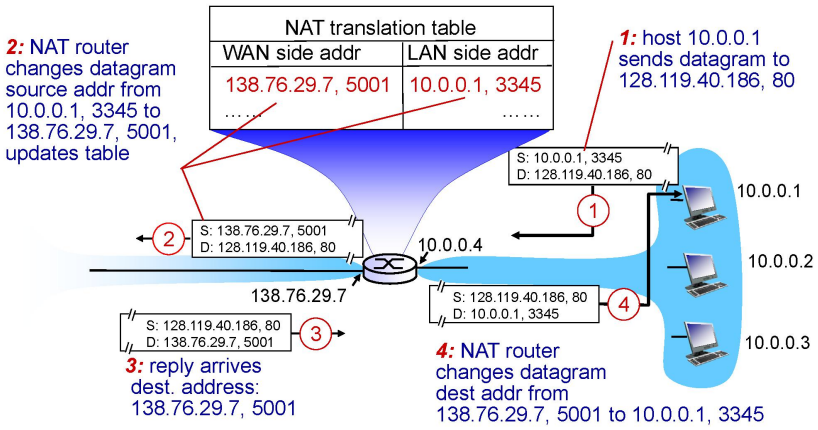
Network address translation (NAT) is a method of remapping one IP is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
motivation: local network uses just one IP address as far as outside world is concerned:
– just one IP address for all devices is needed from the ISP (internet Service Provider)
– can change addresses of devices in local network without notifying outside world
– can change ISP without changing addresses of devices in local network
– devices inside local net not explicitly addressable, visible by outside world (a security plus)

Answer (Group 5):

What is NAT?
Network Address Translation
What is it used for?
NAT can not only solve the problem of insufficient IP addresses, but also effectively avoid attacks from outside the network, hiding and protecting the computers inside the network

Question 8.

Consider the NAT problem as in the following figure:



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

Answer (Group 8):
1. The host of the local network sends a datagram to remote machine, the NAT router will record the host IP with specific port of LAN, meanwhile, it will store a WAN IP address with a port number. These two IP addresses will stores in the NAT translation table. Source IP address, port number <=> NAT IP address, new port number
2. The datagram will send to the remote machine with a WAN IP address.
3. The remote host replies with a new datagram. The datagram will arrive to the NAT router, the router will search corresponding IP address according to the NAT translation table.
4. NAT router change the IP address of the datagram with the concrete host IP address with port, then the host get the datagram.

Answer (Group 5):
a. Client's packet sent to NAT server
b. NAT server change the port and IP address
c. Reply packet received by NAT server
d. NAT server change the port and IP address to the original one
e. Sent the datagram to client

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?

Answer (Group 9):

a) used by hosts & routers to communicate network-level information,

b) type, code, header plus first 8 bytes of IP datagram causing error

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

c) use ping to echo request/reply

use Traceroute to print out all the routers before reach the destination

Answer (Group 5):

a. Used to pass control messages between IP hosts and routers.Control message refers to the message of network itself, such as whether the network is not accessible, whether the host is accessible, and whether the route is available.Although these control messages do not transmit user data, they play an important role in the transmission of user data.

b. ICMP message contained in the IP datagram, belongs to a user IP, IP head is in front of the ICMP message, so an ICMP message including the IP header, ICMP head and ICMP packets, IP header Protocol value of 1 means that this is an ICMP packet, ICMP head Type (Type) of the domain is used to illustrate the ICMP message function and format, and a Code (Code) domain is used to elaborate some ICMP message Type, all data in ICMP header.

c. Ping and traceroute