Computer Networks: Assignment 4

20 March 2017

Solving and submitting your assignment

Requirements about the delivery of this assignment:

- Submit via Blackboard (`http://blackboard.ru.nl`);
- Upload one pdf file for written answers and all supplemental files in a single zip file;
- The file should take the name of your student number, for example student *s0123456* should submit a file named *s0123456.pdf*.
- Write both your name and student number into the document (and only your student number in the filename).

Deadline: April 12, 20:00 sharp!

Goals: After completing these exercises successfully you should be able to:

- interpret DHCP traces to uncover relevant information from them;
- discuss and apply the way an address is resolved via ARP;
- simulate a practical ARP scenario in Netkit;
- explain how switches do self-learning to support plug and play;
- interpret what is actually happening at all networking layers when one accesses a web page.

Marks: You will be graded with marks from 0 to 3 where 0 means not serious, 1 means serious but insufficient, 2 means sufficient and 3 means good. You can have at most 1 assignment graded 0. To get 1 or more, you MUST attempt to solve ALL exercises, even if the provided solution is not correct/complete. In other words, leaving an exercise out automatically turns your grade to 0. In your solution, please explain all answers clearly and concisely.

1 DHCP Wireshark

Capture Wireshark traces of DHCP while performing the following operations.

1. Release the current IP address;
2. Request a new IP address;
3. Release the IP address;

4. Request a new IP address.

Add a print-out of the capture to the assignment. For Linux/MacOs, use the commands `sudo dhclient -r` to release a lease (IP address), respectively `sudo dhclient -1` to obtain a new lease. For Windows, use `ipconfig /release`, respectively `ipconfig /renew`. To minimize the print-out, ensure you filter out all irrelevant traffic; basically, only DHCP- and ARP-related packets are relevant.

Answer the following questions using the captured data by providing adequate annotations on print-outs.

a) What is the link-layer (e.g., Ethernet) address of your host?

b) What values in the DHCP discover message differentiate this message from the DHCP request message?

c) What is the IP address of your DHCP server?

d) What is the lease time obtained by a Request?

e) What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set of DHCP messages? What is the purpose of the Transaction-ID field?

f) What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt for this message? What happens if the client's DHCP release message is lost?

2 Address Resolution Protocol

Consider three LANs interconnected by two routers, as shown in Figure 1.

1. Assign IP addresses to all of the interfaces. For Subnet 1 use addresses of the form 192.168.1/24; for Subnet 2 uses addresses of the form 192.168.2/24; and for Subnet 3 use addresses of the form 192.168.3/24.
2. In the rest of this problem, use the capital letters in the figure (A through F) also as MAC addresses. Consider sending an IP datagram from Host E to Host B. Suppose all of the ARP tables are up to date. Enumerate all the steps, as done for the single-router example at Figure 5.19 of the book.[1]
3. Repeat the last point, now assuming that the ARP table in the sending host is empty (and the other tables are up to date).

3 Self-learning

Let's consider the operation of a learning switch in the context of a network in which 6 nodes labeled A through F are star connected into an link-layer switch. Suppose that (i) B sends a frame to E, (ii) E replies with a frame to B, (iii) A sends a frame to B, (iv) B replies with a frame to A. The switch table is initially empty. Show the state of the switch table before and after each of these events. For each of these events, identify the link(s) on which the transmitted frame will be forwarded, and briefly justify your answers.

[1] The same figure in the seventh edition is numbered as 6.19.

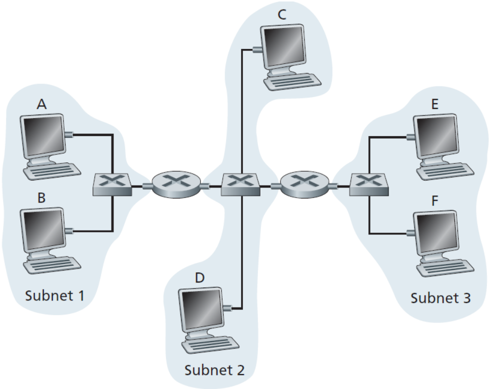
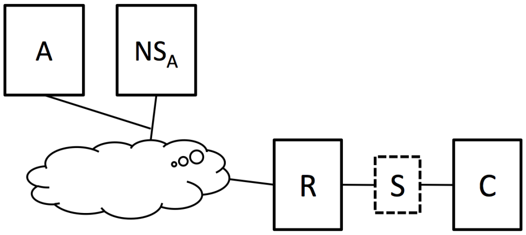


Figure 1: Three connected subnets

4 All in problem

Before you start solving this problem, make sure that you have read the following book section: *'5.7 Retrospective: A Day in the Life of a Web Page Request'*.

Consider the network topology below where client C is connecting to an Ethernet network with gateway router R via the switch S, as shown in the figure below. The router runs both a DHCP server and a DNS resolver and is used as such by connecting clients. As soon as it is connected, client C requests *once* the web page `http://A.com/index.html`. Client C's browser implements an *internal web cache*. Web server A is located in a different network. This server handles HTTP requests for `A.com`. The authoritative name server NS_A for domain `A.com` is located in the same network as A. This network is separated *by more than one router* from R.



The table on the next page lists possible packets between the participants when C connects to the network and subsequently accesses the mentioned webpage. We assume that any HTTP connection established is persistent, hence only one TCP connection is used.

In this problem, you will need to arrange the various packets exchanged in chronological order. Note that *not all sent packets are listed* and *some of the packets listed are not sent.* In the latter case, please put a "–" sign in the respective entry cell of the table. The first empty cell has already been filled up with the correct ordering.

1. Consider first the case when all caches (ARP, DNS, Web) are empty. Complete the column of *Scenario 1* with the right ordering. Give an ordered list of packet identifiers. (That is, the numbers you would write in the table column vertically.)

2. There are at least two packets that are not (supposed to be) indicated in the ordering in (a). Choose any two of them and explain why they are never sent.

3. The switch S maintains a switch table with mappings from MAC addresses to links. Assuming that the switch table is empty at connection time, after which packet is the table updated with the MAC

Id	Source	Destination	Protocol	Content	Scenario 1 (a)	Scenario 2 (d)
1	C	broadcast	DHCP	DHCP discover	1	
2	R	broadcast	ARP	who is NS_A		
3	A	C	HTTP	index.html		
4	C	broadcast	ARP	who is R		
5	R	NS_A	DNS	query for A.com		
6	C	A	TCP	SYN+ACK		
7	C	A	HTTP	GET index.html		
8	A	C	HTTP	Not Modified		
9	C	R	DNS	query for A.com		
10	R	broadcast	DHCP	DHCP offer		

address for client C? How about the MAC address R?

4. Give two packets in the table that do not contain a transport layer header. Specify these packets by giving their identifiers. Moreover, specify the layer at which the protocols which sent these packets operate.

5. Assume now that C's browser has the web page cached, and the page hasn't changed since the last access nor has the cache expired. Also that router R has an A DNS record entry for the name `A.com` cached in its DNS cache and the record is still valid. All other assumptions are the same as *before* the first scenario. Complete then the column for *Scenario 2* with the right ordering. Similarly to 1., give an ordered list of packet identifiers; that is, give the numbers you would write in the table column vertically.

5 ARP tables and ARP spoofing

In this assignment you will observe and explain the ARP process across three netkit virtual machines. Begin by starting three virtual machines which all share the same Ethernet domain using

```
vstart pcX --eth0=A
```

This will result in a simple, bus-topology network that looks like Figure 2

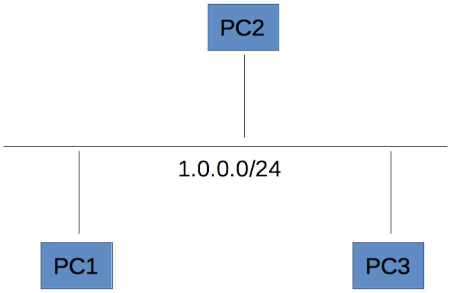


Figure 2: Three connected nodes on one network

a) Assign each virtual machine a unique IP address on the 1.0.0.0/24 network and issue the command `arp`. ARP will print the current known hosts for the given machine and you since no traffic has been generated the resulting table should be empty. From pc1 ping pc2 and then run `arp`.

b) Using your understanding of ARP, explain what happened.

c) Now with the third host issue

```
arpspoof -i eth0 pc2-ip-address
```

After pinging pc2 from pc1 again, observe the change in the ARP table. Explain what happened?

Please turn in screen shots of your populated ARP tables and text for answering the questions.