Lab#3B: DHCP

Please read Kurose 4.4.2.

Exercises of this lab are prepared to do in Windows.

1. Intro

DHCP is a protocol to provide an IP address to a computer remotely through the network. DHCP uses UDP traffic to achieve its goal. One or more DHCP servers can sit in the same network for providing IP addresses to requesting computers. Addresses may be assigned from a common pool on a FCFS-basis or based on a table provided by network admin.

DHCP process consists of four different exchanges: DISCOVER, OFFER, REQUEST and CONFIRMATION. A fifth step may happen once a system no longer needs the IP it obtained in the past: RELEASE.

2. Traffic analysis

Exercise#1: Check how is your computer obtaining its IP address looking at the control panel in Windows, or you may use ipconfig /all. Write down the parameters related to the DHCP protocol (when the IP address is assigned, lease time, expire time,…)

Exercise#2:

a) Start capturing UDP traffic on port 67 with Wireshark
b) Issue ipconfig /release to release your current IP address (Linux command: sudo dhclient -r)
c) Issue ipconfig /renew to start a new DHCP request (Linux command: sudo dhclient)
d) Observe the traffic created due to the above process
e) What transport protocol does DHCP, TCP or UDP use?
f) Looking at the source and destination IP addresses of the datagram of this first DHCP message that appears, could you justify choosing DHCP for that kind of service (transport protocol)?
g) Look for DHCPDISCOVER message and provide the following values: type of message, source IP, destination IP, source port, destination port, transaction ID, your IP & server IP.

With the aim that we all work with the same captures, we have left two captures in Poliformat: Captura1Practica3.pcap that includes the process of obtaining the IP configuration and Captura2Practica3.pcap that includes the process of releasing the IP configuration. These captures have been made on a computer in the Network Laboratory and, therefore, they will allow us to know a little about the IP configuration of Computer Networks' Lab.

Exercise#3:

a) Download the Captura1Practica3.pcap capture from the PoliformaT and open it with the Wireshark program
b) Focus in the 1st DHCP message: DHCPDISCOVER and answer the following questions:
   a. What transport protocol does DHCP, TCP or UDP use?
   b. Looking at the source and destination IP addresses of the datagram of this first DHCP message that appears, could you justify choosing DHCP for that kind of service

(transport protocol)?

c) Look for DHCPDISCOVER message and provide the following values:
- type of message,
- source IP,
- destination IP,
- source port,
- destination port,
- transaction ID,
- your IP & server IP

d) In this message the computer is asking for an specific IP address: where is that done?

e) List the first four options the client is requesting.

Exercise#4: Now focus on DHCPOFFER responses.

a) How many are there?

b) Provide the following values:

- type of message,
- source IP,
- destination IP,
- source port,
- destination port,
- transaction ID,
- your IP & server IP

c) What is the value for DHCP server identifier on each of the answers?

d) Search and write down in any of the DHCPOFFER messages the following IP information that the DHCP servers are offering to the computer that has requested the IP configuration: offered IP address, subnet mask, assigned router and domain name.

e) Where are these DHCP servers located in the campus networks? Is that your same network? (you may want to use ipconfig /all to see that).

f) Compare the values of the "DHCP Server Identifier" field of the remaining DHCPOffer messages that appear in the capture. How many different DHCP servers are answering?

Exercise#5: Now focus on DHCPREQUEST:

a) Provide the following values: type of message, source IP, destination IP, source port, destination port, transaction ID, your IP & server IP.

b) What is the server the client is replying to?

Exercise#6 Now focus on DHCPACK of which you've got more than one.

a) How many answers have you got?

b) What are the IP addresses of these servers?

Finally, we are going to analyse a new capture with Wireshark in order to study the DHCP traffic that is generated when a node releases its IP address. To do this we open the capture captura2Practica3.pcap (we have obtained it by executing the command: ipconfig / release).

Exercise#7: Now focus on what happens when an address is released.

a) What DHCP messages are transmitted? Who does intervene in the dialog? Is there any response?