

Exercici sm6ex10 - DHCP

PART 1 - Conceptes sobre DHCP

1- Quins **dispositius** haurien de tenir una **IP estàtica** i quins haurien de tenir una **IP dinàmica**?

- IP estàtica: Router, Switch, Hub, Servidors DNS i DHCP sobretot però en general qualsevol servidor no té sentit que tingui una IP dinàmica, Impressores, Firewall.
- IP dinàmica: Portàtils, estacions de treball, mòbil, TV, tauleta i en general els dispositius finals utilitzats pels usuaris

2- Quines **avantatges** ofereix el servei **DHCP**?

- Evita errors de configuració de xarxa dels equips finals de propòsit general (portàtils, mòbils, tauletes,...).
- Permet centralitzar en un únic lloc la tasca de configuració de tots els client i per tant, facilita la tasca d'administració de la xarxa.

3- Què és el **temps de concessió** o leasing DHCP?

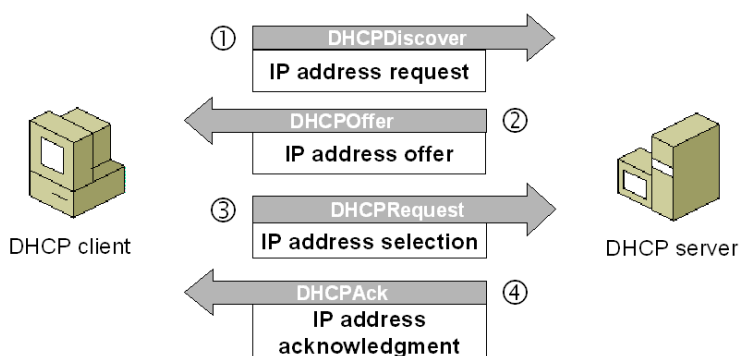
És el període de temps durant el qual el servidor DHCP assigna una configuració de xarxa a un equip client. Normalment s'assigna una IP, una màscara de subxarxa, l'adreça IP del router de la xarxa, les adreces IP dels servidors DNS. El servidor DHCP també envia al client el temps de la concessió com a part de la configuració de xarxa.

4- Escriu la llista dels principals **missatges DHCP**.

DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, DHCPRELEASE, DHCPNACK i DHCPDECLINE

5- Quina és la **seqüència típica** de missatges DHCP entre un ordinador client i el servidor quan es connecta a la xarxa?

DHCPDISCOVERY (cli) → DHCPOFFER (srv) → DHCPREQUEST (cli) → DHCPACK (srv)



6- Què passa si en comptes de rebre un **DHCPACK** es rep un **DHCPNACK**?

El Servidor està dient al client que finalment no pot assignar-li l'adreça IP que havia ofert i que per tant ha de començar la seqüència des del principi, o sigui, enviant novament un DHCPDISCOVERY.

7- Com es **renova** una concessió abans de l'expiració del temps de leasing (concessió)?

Una concessió es pot renovar, o sigui, allargar la seva durada, enviant des del client un DHCPREQUEST. Dins del DHCPREQUEST s'envia la configuració actual.

8- Què significa un **DHCPDECLINE**?. Qui ho envia?

Ho envia el client. Es per indicar al servidor que no accepta La concessió dins d'un DHCPOFFER.

9- Per quines raons s'allibera una concessió DHCP?

Alliberar una concessió consisteix en enviar un missatge DHCPRELEASE per part del client al servidor. Això es pot fer per 2 motius:

- Perquè hem arribat al temps de leasing i es genera automàticament el DHCPRELEASE.
- Perquè l'administrador ha enviat manualment un missatge DHCPRELEASE. Per exemple amb l'ordre de Windows ipconfig /release o l'ordre de Linux dhclient -r.

10- DHCP treballa sobre UDP o TCP?.

DHCP treballa sobre UDP

11- Quins ports utilitza DHCP?

El servidor DHCP utilitza el port 67/udp i el client utilitza el port 68/udp

12- Què és DHCP Relay?

Una tècnica que permet a servidors i clients DHCP enviar missatges DHCP a una xarxa remota a través dels routers. Això permet a un servidor donar servei DHCP dins de la seva xarxa local i també a xarxes remotes.

13- Quin són els camps més importants de la capçalera d'un missatge DHCP?

a) Camps d'un missatge DHCP:

Table 3-2 Fields in a DHCP message

Field	Length	Description
op	1 byte	Operation Code: indicates the general type of message. The values are: • 1: DHCP Discover message • 2: DHCP Offer message
htype	1 byte	Hardware Type: indicates the type of hardware used for the local network. The values of this field differ for different hardware types. The most common value is 1, which indicates Ethernet (10 Mb).
hlen	1 byte	Hardware Address Length: indicates the length of a hardware address. For Ethernet, the value is 6.
hops	1 byte	Hops: indicates the number of DHCP relay agents through which a DHCP message passes. This value is set to 0 by a client and is incremented by 1 each time the message passes through a DHCP relay agent. A DHCP message passes through a maximum of 16 DHCP relay agents when being transmitted between a server and a client. That is, the number of hops between the server and client cannot exceed 16. Otherwise, the DHCP message is discarded.
xid	4 bytes	Transaction Identifier: indicates a random number chosen by a client for exchanging messages with a DHCP server.
secs	2 bytes	Seconds: indicates the number of seconds elapsed since a client obtained or renewed an IP address.
flags	2 bytes	Flags: indicates the Flags field. Only the leftmost bit in this field is used, and the other bits are set to 0. The leftmost bit specifies the mode a DHCP server uses to transmit a DHCP Offer message. The values are: • 0: The DHCP server unicasts a DHCP Offer message. • 1: The DHCP server broadcasts a DHCP Offer message.
ciaddr	4 bytes	Client IP Address: indicates the IP address of a DHCP client. The IP address is either the existing IP address of the client or an IP address allocated by a DHCP server to the client. During the process of a client acquiring an IP address, the value of this field is 0.0.0.0. 0.0.0.0 is an invalid destination address and is used by a DHCP-enabled device to communicate only temporarily with other devices during startup.
yiaddr	4 bytes	Your IP Address: indicates the IP address that a DHCP server allocates to a client.
siaddr	4 bytes	Server IP Address: indicates the server IP address from which a DHCP client obtains its startup configuration file.
giaddr	4 bytes	Gateway Address: indicates the IP address of the first DHCP relay agent. When a client sends a DHCP Request message and is on a different network segment from its DHCP server, the first DHCP relay agent forwards the message to the DHCP server and fills its IP address in the giaddr field. The DHCP server determines the network segment address of the client based on this field, selects an appropriate address pool, and assigns an IP address on this network segment to the client. The server also returns a DHCP reply message to the first DHCP relay agent, which then forwards the message to the client. If the DHCP Request message passes through multiple DHCP relay agents before reaching the DHCP server, the giaddr field value is still the IP address of the first DHCP relay agent, and the hops field value is incremented by 1 each time the message passes through a DHCP relay agent.
chaddr	16 bytes	Client Hardware Address: indicates the Layer 2 address of a client. For Ethernet, this field must contain a 6-byte Ethernet MAC address if the hardware type and hardware length fields are set to 1 and 6 respectively.
sname	64 bytes	Server Hostname: indicates the name of the server from which a client obtains configuration information. This field is optional, is filled in by the DHCP server, and must be a character string that ends with 0.
file	128 bytes	Boot File: indicates the name of the startup configuration file to be obtained by a client. This field is filled in by a DHCP server and delivered to the client when a DHCP address is allocated to the client. The field is optional and must be a character string that ends with 0.
options	Variable	Options: indicates the DHCP Options field. This field is a maximum of 1200 bytes in length and contains the DHCP message type and configuration parameters allocated by a DHCP server to a client. The configuration parameters include the gateway IP address, DNS server IP address, and IP address lease. For details about the Options field, see DHCP Options .

b) Format del missatge DHCP

Figure 3-2 DHCP message format

0	7	15	23	31
op(1)	htype (1)		hlen (1)	hops (1)
xid (4)				
secs (2)		flags (2)		
ciaddr (4)				
yiaddr (4)				
siaddr (4)				
giaddr (4)				
chaddr (16)				
sname (64)				
file (128)				
options (variable)				

c) Fonts:

- <https://support.huawei.com/enterprise/en/doc/EDOC1100034071/225eec10/dhcp-messages>
- <https://datatracker.ietf.org/doc/html/rfc2131> (Pàgines 9 a 11)

PART 2 - Wireshark

Descarrega el fitxer de wireshark <https://www.collados.org/asix2/sm6/sm6ex10/dhcp.pcapng>. Posa en marxa wireshark i obre el fitxer **dhcp.pcapng**. Crea el següent filtre: **dhcp** (o **bootp** segons la versió de Wireshark). Respon a les següents preguntes:

a) A la primera captura: Quin són els camps utilitzats per saber el tipus de missatge DHCP enviat?

- Camp **Options** → Option **53 (0x35)** → Enviament d'un missatge tipus DHCP o **DHCP Message Type**.
- El missatge de tipus DHCP enviat és de tipus **DHCPRELEASE** perquè el valor del registre DHCP és **0x07** o **7** en hexadecimal. Per tant, el client està alliberant la seva concessió de.

b) Les captures 2 a 5 formen part d'una mateixa seqüència de missatges DHCP. Com ho sabem?

Els 4 missatges tenen el mateix valor dins del camp **Transaction ID**, que en aquest cas és **0xd046514b**.

c) A quina adreça IP s'envia el missatge DHCPDISCOVER?.

Si mirem l'adreça IP de destinació del paquet IP dins del qual es troba el missatge DHCP veurem que l'adreça IP destinació les **255.255.255.255** que és l'adreça IP especial de Broadcast per qualsevol xarxa, també anomenada **IP de Broadcast limitada** perquè els routers mai permeten que passi per ells i sempre és descartada.

d) Quina és l'adreça IP del servidor DHCP?. Com ho sabem?

Si mirem el missatge de tipus **DHCPOFFER** podem trobar l'adreça IP del servidor DHCP dins del camp **Options**. Concretament dins de l'opció **54 (0x36) DHCP Server Identifier** trobem el registre **DHCP Server Identifier** que té l'adreça **IP del servidor DHCP**. En aquest cas és el **192.168.1.1**.

e) Quina és l'adreça que rep el client?. I la màscara?. Com ho sabem?

- Si mirem el missatge de tipus **DHCPOFFER** o el **DHCPACK** podem trobar l'adreça del client. Dins del camp **Your (client) IP address**. En aquest cas és l'adreça IP que s'ofereix i finalment s'accepta és **192.168.1.33**. Així doncs, el client es configurarà amb aquests adreça IP.

- Si mirem el missatge de tipus **DHCPOFFER** o el **DHCPACK** podem trobar la màscara assignada al client. Concretament dins de l'opció **1 (0x01) Subnet Mask** trobem el registre **Subnet Mask** que té l'adreça la **màscara** assignada a l'equip client. En aquest cas és el **255.255.255.0**.

f) Quina és l'adreça IP dels servidors DNS assignats al client?. Com ho sabem?

Si mirem el missatge de tipus **DHCPOFFER** o **DHCPACK** podem trobar les adreces IP dels servidors **DNS**. Concretament dins de l'opció **6 (0x06) Domain Name Server** trobem **dos** registres de nom **Domain Name Server** que tenen les adreces **IP dels servidors DNS**. En aquest cas són **80.58.61.250** i **80.58.61.254**.

g) El procés ha finalitzar amb èxit?. Com ho sabem?

Sí, perquè hem rebut des del servidor un **DHCPACK**.

h) Quin és el temps de leasing?. Com ho sabem?

Si mirem el **DHCPOFFER** o el **DHCPACK** podem trobar el temps de leasing dins del camp **Options**. Concretament dins de l'opció **51 (0x33) IP Address Lease Time** trobem el registre **IP Address Lease Time** que té el valor del temps de concessió. En aquest cas és **43200** segons que correspon a **12 hores**.