Pràctica 3
Sessió 4 - Implementar un servei DNS
Alumnes:
Mariona Farré Tapias,
Marc Pérez Guerrero

CARPETA VMS SESSIÓ 4:
https://drive.google.com/drive/folders/1CLkkZxqUsj-0WdNOyltyFykCa08K0jI2?usp=sharing

---

ÍNDEX:

Enunciat

1- Configurar un servidor DHCP.

- Cal que doni servei a 2 xarxes.
  + Agafeu com a referència les 2 xarxes (DMZ i clients) de l'escenari de les sessions 1 i 2 i situeu el servidor al router intern
  + A la xarxes (DMZ) les màquines definides estan sempre enceses, però n'hi poden haver d'altres que apareguin puntualment
  + A la xarxa clients les màquines no estan enceses mai més de 8h i hi ha rotació d'equips (portàtils).
- Cal raonar prèviament quins equips utilitzaran una assignació d'adreces dinàmica, i per aquestos
  + La durada del prèstec
  + Si sempre han de tenir la mateixa IP

- Cal utilitzar rangs d'IPs diferents en funció de la xarxa on està connectat el client.
- Cal assignar qualsevol altre paràmetre necessari per a tenir accés a Internet
  + Agafeu com a referència el definit i a l'escenari de les sessions 1 i 2
- Cal assignar el mateix domini a tots els clients
  + Utilitzeu el domini "seax.edu" de la sessió 3.
- Cal permetre un pool d'adreces d'assignació dinàmica i així com la reserva d'algunes adreces.
- Raonar com es podria utilitzar aquest servei per millorar la seguretat d'una xarxa.
  + Hi ha hosts coneguts i d'altres que no ho són (potencials atacants)

+ El trànsit de la xarxa passa per un tallafocs

- (Opcional) Configurar correctament el DDNS.

2- Protecció del servidor de DHCP

- Apliqueu les directrius de seguretat específiques pels servidors definides a la sessió 1 i 2

3- Verificar el seu bon funcionament.

- Implementar un escenari de treball amb 2 xarxes servides pel mateix servidor.
- Comprovar que els clients reben tots els paràmetres definits d'acord amb la xarxa a la que estan connectats.

- Comprovar el funcionament de les assignacions dinàmiques d'un pool d'adreces, de les reserves i del temps que duren.
- Realitzar captures de xarxa adients o utilitzar el propi client DHCP per mostrar i comentar les transasccions clients-servidor.

4- Lliurar els resultats.

Mitjançant Atenea (2 fitxers).

- Redactar l'informe de la pràctica p3_s4_cognom1_nom.txt.
- Realitzar les proves necessàries per justificar els resultats i encapsular els fitxers necessaris en el fitxer p3_s4_cognom1_nom.zip.

Mitjançant Google Drive (màquines virtuals)

- Compartir amb rafael.vidal@upc.edu una carpeta a Google Drive (UPC) amb la VM del servidor DHCP.

Important:

- L'informe de la pràctica ha de contenir l'enllaç a la carpeta amb la VM.
- Les VM ha de contenir una còpia de l'informe al directori /root.

5- A títol orientatiu el resultat de la pràctica cal que doni resposta a les següents qüestions:

- Quins criteris podem fer servir per determinar que una interfície de xarxa d'una màquina s'ha de configurar amb un assignació dinàmica amb o sense reserva d'adreça IP?
- Quin escenari (VMs, adaptadors de xarxa i configuració) es necessita?
- Quin software es necessita per donar el servei de servidor DHCP? Com s'instal·la?
- Com es comprova l'estat d'un servidor DHCP?
- Com es configura el servidor DHCP (paràmetres)?
  + Com s'assigna un domini?
  + Com s'assigna una adreça dinàmicament?
  + Com es reserven adreces?
  + Com s'indica durant quant de temps s'assigna una adreça?
  + Quins altres paràmetres d'interès es poden assignar per a disposar de connexió a Internet?
  + Com es s'assignen rangs d'adreces diferents en funció de la xarxa?
- Com es valida la configuració del servidor DHCP?

- Relacionat amb l'anterior pregunta, com s'ha d'utilitzar el client DHCP (per consola i via fitxer /etc/network/interfaces) per validar el servidor?
- Com es pot veure quin servidor està proporcionant la configuració a un client DHCP?
- Com es podria fer servir DHCP per millorar la seguretat d'una xarxa? Penseu si qualsevol màquina pel fet d'estar connectada a la xarxa ha de rebre configuració independentment de si és coneguda o no i a partir d'aquí, feu alguna proposta.

- (Opcional) Com es configura el DDNS (paràmetres)?

- (Opcional) Com es comprovar que el DDNS està ben configurat?

Informe pràctica 3 sessió 4:

***** Introducció de l'escenari:**

En aquesta pràctica, es configurarà un servidor DHCP que ha de proporcionar serveis a dues xarxes diferents: la DMZ i la xarxa de clients. Aquest servidor estarà situat en el router intern, segons l'escenari de les sessions 1 i 2. A continuació es detallen les característiques i requisits de les xarxes, així com els criteris per a la configuració del servidor DHCP.

- Xarxa DMZ (Demilitarized Zone):
Les màquines en aquesta xarxa estan sempre enceses.
Poden aparèixer dispositius puntuals que necessitin accés temporal a la xarxa.
És important garantir que les màquines crítiques tinguin sempre la mateixa IP.

- Xarxa de Clients:
Les màquines en aquesta xarxa no estan enceses més de 8 hores al dia.
Hi ha una rotació constant d'equips, especialment portàtils.
Els dispositius aquí no necessiten tenir la mateixa IP cada vegada que es connecten.

Requisits de Configuració DHCP

- Assignació d'Adreces Dinàmica:
Les adreces IP han de ser assignades dinàmicament en funció de la xarxa on està connectat el client.
La durada del préstec (lease time) serà diferent per a cada xarxa, tenint en compte el temps d'ús dels dispositius.

- Rangs d'IPs:
S'utilitzaran rangs d'IPs diferents per a cada xarxa.
Per a la DMZ, es definiran IPs fixes per a màquines crítiques.
La resta d'adreces en la DMZ i totes les de la xarxa de clients es distribuiran dinàmicament.
Paràmetres Necessaris per a Accés a Internet:

Configuració de la porta d'enllaç (gateway), servidors DNS i altres paràmetres de xarxa necessaris per garantir la connectivitat a Internet.
Domini:

Tots els clients de les dues xarxes tindran el domini "seax.edu".

Quins serien els possibles criteris per determinar que una interfície de xarxa d'una màquina s'ha de configurar amb una assignació dinàmica amb o sense reserva d'adreça IP:

Assignació Dinàmica Sense Reserva:
Dispositius Temporals: Equips que es connecten a la xarxa durant períodes curts de temps, com portàtils en la xarxa de clients.
Màquines Amb Alta Rotació: Dispositius que canvien sovint, sense necessitat de mantenir la mateixa adreça IP.

Exemples: Portàtils d'usuaris, telèfons mòbils, tablets.

Assignació Dinàmica Amb Reserva:
Dispositius Crítics: Equips que necessiten sempre la mateixa adreça IP per funcionar correctament, com servidors o dispositius de xarxa.
Màquines Amb Funcions Específiques: Equips que proporcionen serveis essencials i han de ser accessibles sempre a la mateixa adreça IP.
Exemples: Servidors de bases de dades, impressores de xarxa, equips de seguretat com càmeres IP.

Per l'escenari actual, es necessitem els dos routers existents de router d'accés i intern, amb les xarxes troncals amb accés a internet, la següent sent una xarxa interna anomenada dmz entre els dos routers i la última xarxa que sigui del router intern per tenir donar funcionalitat a clients.
Per la creació del servidor dhcp, l'instalarem en el router intern per donar servei a les xarxes dmz i la dels clients.

Els adaptadors de Xarxa haurien de ser els específics pel router intern, amb dos adaptadors de xarxa connectat a les dues xarxes per poder-hi accedir.
I pels diferent clients i monitors del servei dhcp, amb els adaptadors de xarxa configurats per accedir a les respectives xarxes.

En aquest escenari, tenim dues subxarxes principals:

Subxarxa DMZ: 10.1.10.0/28 (amb les primeres 10 adreces reservades)
Subxarxa de Clients: 10.1.20.0/24 (amb les primeres 10 adreces reservades)

Les configuracions específiques per aquestes subxarxes seran les següents:
Subxarxa DMZ (10.1.10.0/28)
Rang d'IP: 10.1.10.10 - 10.1.10.14
IPs Reservades: Les primeres 10 adreces (10.1.10.0 - 10.1.10.9)
Assignació: Estàtica per a dispositius crítics que estan sempre encesos (servidors DNS, monitors, etc.)

Subxarxa de Clients (10.1.20.0/24)
Rang d'IP: 10.1.20.10 - 10.1.20.254
IPs Reservades: Les primeres 10 adreces (10.1.20.0 - 10.1.20.9)
Assignació: Dinàmica per a dispositius temporals (portàtils, dispositius mòbils)
Durada del prèstec: 8 hores
Requisit de la mateixa IP: No, no és necessari que els dispositius temporals mantinguin la mateixa IP després de la renovació del prèstec.

***** Configuració del router intern:**

Per proporcionar el servei de servidor DHCP, necessitareu instal·lar i configurar un programari de servidor DHCP. Un dels servidors DHCP més utilitzats és isc-dhcp-server, desenvolupat per l'Internet Systems Consortium (ISC).

Per instal·lar isc-dhcp-server a un sistema basat en Debian s'ha d'utilitzar el següent comandament:

```
sudo apt-get update
sudo apt-get install isc-dhcp-server
```

Un cop instal·lat, es necessita configurar el servidor DHCP editant el fitxer de configuració principal /etc/dhcp/dhcpd.conf.
Ja que una vegada instal·lat pot sortir un error de que no hi hagui aquest fitxer de configuració creat.

Per mirar l'estat del servidor, podem fer servir la comanda:

```
systemctl status isc-dhcp-server
```

Aquesta inicialment donarà un error en el servei, però una vegada haguem configurat el fitxer de configuració ens retornarà un estat actiu i correcte.

Un servidor DHCP (Dynamic Host Configuration Protocol) assigna automàticament adreces IP i altres paràmetres de configuració de xarxa als dispositius clients de la xarxa. La configuració del servidor DHCP inclou diversos paràmetres clau que permeten la gestió eficient de les adreces IP i altres opcions de configuració de la xarxa.

En el fitxer de configuració s'ha de pensar en:
Assignació de Domini: El paràmetre option domain-name s'utilitza per assignar un nom de domini als clients DHCP.

Assignació Dinàmica d'Adreces: Les adreces IP es poden assignar dinàmicament utilitzant el paràmetre range, que especifica el rang d'adreces IP que el servidor pot assignar als clients.

Reserva d'Adreces: Les adreces IP es poden reservar per a dispositius específics utilitzant les adreces MAC dels dispositius. Això es fa amb la directiva host.

Durada del Prèstec d'Adreces: Els paràmetres default-lease-time i max-lease-time especifiquen la durada del prèstec d'adreces IP en segons.

Altres Paràmetres d'Interès: A més de les adreces IP, el servidor DHCP pot assignar altres paràmetres de configuració com servidors DNS (option domain-name-servers), passarel·les predeterminades (option routers), adreces de broadcast (option broadcast-address), i màscares de subxarxa (option subnet-mask).

Assignació de Rangs Diferents segons la Xarxa: Les subxarxes es configuren utilitzant la directiva subnet, que permet definir rangs d'adreces IP i altres paràmetres per a cada subxarxa.

Per això el fitxer de configuració del servei dhcp el router intern l'hem configurat com: /etc/dhcp/dhcpd.conf

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
option domain-name "seax.edu";
option domain-name-servers 10.1.10.3, 10.1.10.4;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Subxarxa DMZ
subnet 10.1.10.0 netmask 255.255.255.240 {
   range 10.1.10.12 10.1.10.14;  # Rang per a màquines puntuals
   option routers 10.1.10.1;
   option subnet-mask 255.255.255.240;

   # Adreces IP estàtiques per a dispositius crítics
   host dns1 {
      hardware ethernet 08:00:27:01:10:03;
      fixed-address 10.1.10.3;
   }

   host dns2 {
      hardware ethernet 08:00:27:01:10:04;
      fixed-address 10.1.10.4;
   }

   host nagios {
      hardware ethernet 08:00:27:01:10:05;
      fixed-address 10.1.10.5;
   }

   host monitor {
      hardware ethernet 08:00:27:01:10:11;
      fixed-address 10.1.10.11;
   }
}

# Subxarxa de Clients
subnet 10.1.20.0 netmask 255.255.255.0 {
   range 10.1.20.10 10.1.20.254;
   option routers 10.1.20.1;
```

```
    option subnet-mask 255.255.255.0;

    default-lease-time 28800;  # 8 hores en segons
    max-lease-time 28800;      # 8 hores en segons
}
```

Les configuracions comentades anteriorment les podem veure en el fitxer com:
Assignació d'un domini:
El domini es defineix amb el paràmetre option domain-name.
Exemple: option domain-name "seax.edu";

Assignació d'una adreça IP dinàmica:
Les adreces IP es poden assignar dinàmicament utilitzant el paràmetre range dins de la definició de la subxarxa.
Exemple: range 10.1.10.12 10.1.10.14;

Reserva d'adreces IP:
Les adreces IP es poden reservar per a dispositius específics utilitzant la directiva host, on es defineix la MAC address del dispositiu i l'adreça IP fixa.
Exemple:
```
host dns1 {
    hardware ethernet 08:00:27:01:10:03;
    fixed-address 10.1.10.3;
}
```

Durada del prèstec d'adreces:
La durada del prèstec es defineix amb els paràmetres default-lease-time i max-lease-time en segons.
Exemple:
```
default-lease-time 28800;  # 8 hores en segons
max-lease-time 28800;      # 8 hores en segons
```

Els paràmetres com el option routers per definir la passarel·la predeterminada i option domain-name-servers per definir els servidors DNS.
Exemple:
```
option routers 10.1.10.1;
option domain-name-servers 10.1.10.3, 10.1.10.4;
```

Assignació de rangs d'adreces diferents en funció de la xarxa:
Les subxarxes es defineixen utilitzant la directiva subnet, i cada subxarxa pot tenir configuracions pròpies, com ara el rang d'adreces IP i la durada del prèstec.
Exemple:
```
subnet 10.1.10.0 netmask 255.255.255.240 {
    range 10.1.10.12 10.1.10.14;
    option routers 10.1.10.1;
    option subnet-mask 255.255.255.240;
}

subnet 10.1.20.0 netmask 255.255.255.0 {
```

```
    range 10.1.20.10 10.1.20.254;
    option routers 10.1.20.1;
    option subnet-mask 255.255.255.0;
}
```

També s'ha de configurar per quina interfície de xarxa s'utilitza el servidor dhcp, això es configura en el següent fitxer on l'hi haurem de configurar les interfaces de versio4 posant:
/etc/default/isc-dhcp-server

```
…
INTERFACESv4="eth-dmz eth-clients"
…
```

Després de fer els canvis, reiniciar el servidor dhcp i mirar el seu estat:

```
systemctl restart isc-dhcp-server
```

Assegurar que el servei està funcionant correctament:

```
systemctl status isc-dhcp-server
```

Ara si podem veure que l'estat és actiu i funciona correctament

Fitxers d'evidència:

configuració del router intern : 1-1-routerintern.txt

Fitxers involucrats:

-/etc/dhcp/dhcpd.conf
Configuració del servei dhcp
- /etc/default/isc-dhcp-server
Per especificar la interfície de xarxa del servei dhcp

***** Verificacions de màquines**

Per verificar la sintaxi podem utilitzar el comandament dhcp per verificar la sintaxi del fitxer de configuració:

```
dhcpd -t -cf /etc/dhcp/dhcpd.conf
```

Aquest comandament comprova el fitxer de configuració per assegurar-se que no hi ha errors de sintaxi.

Ara hem de verificar les diferents màquines en les diferents xarxes que dhcp dona servei:

Per configurar les màquines hem de posar en el fitxer de interfícies la configuració de l'adaptador d'aquella xarxa que utilitzi el servei dhcp, hauria de ser com:

/etc/network/interfaces
…

```
# The primary network interface
auto enp0s3
 iface enp0s3 inet dhcp
```

Ara al fer un reboot la màquina per veure quina adreça se li ha assignat mirant amb: ip a

**** Verificacions de màquines de dns:**

Configuració del Servidor DNS1
La interfície de xarxa eth-dmz ara està configurada per obtenir una adreça IP mitjançant DHCP.
Es reinicia la configuració de la xarxa per aplicar els canvis.
I el servidor DNS1 rep l'adreça IP 10.1.10.3 de manera dinàmica, tal com està configurat al servidor DHCP.

Configuració del Servidor DNS2
La interfície de xarxa eth-dmz ara està configurada per obtenir una adreça IP mitjançant DHCP.
Es reinicia la configuració de la xarxa per aplicar els canvis.
I el servidor DNS2 rep l'adreça IP 10.1.10.4 de manera dinàmica, tal com està configurat al servidor DHCP.

Els servidors DNS1 i DNS2 estan configurats per obtenir adreces IP mitjançant DHCP. Tot i que les adreces IP estan especificades com a dinàmiques, el servidor DHCP està configurat per assignar adreces fixes a aquests servidors basades en les seves adreces MAC, i el servidor DHCP assigna correctament les adreces IP 10.1.10.3 i 10.1.10.4 als servidors DNS1 i DNS2 respectivament, ja que coincideixen amb les adreces MAC configurades al fitxer dhcpd.conf.

**** Verificacions de màquines en xarxa clients:**

Les següents verificacions que hem fet és per uns clients en la xarxa clients:

CLIENT 1:
fitxer: 1-2-verificacio-client1.txt

- cat /etc/network/interfaces: Aquesta comanda mostra la configuració de la interfície de xarxa. La interfície enp0s3 està configurada per obtenir una adreça IP mitjançant DHCP.

- cat /etc/resolv.conf: Aquesta comanda mostra la configuració dels servidors DNS. Els servidors configurats són 10.1.10.3 i 10.1.10.4, amb el domini seax.edu.

- ip a: Aquesta comanda mostra les adreces IP assignades a les interfícies de xarxa. El client ha rebut l'adreça IP 10.1.20.11, dins del rang configurat per a la xarxa de clients.

- ping -c 1 10.1.10.1: Aquesta comanda envia un paquet ICMP de ping a la passarel·la de la xarxa DMZ (10.1.10.1). El client pot fer ping a la passarel·la.

- ping -c 1 10.1.10.3: Aquesta comanda envia un paquet ICMP de ping al servidor DNS1 (10.1.10.3). El client pot fer ping al servidor DNS1.

- ping -c 1 10.1.10.4: Aquesta comanda envia un paquet ICMP de ping al servidor DNS2 (10.1.10.4). El client pot fer ping al servidor DNS2.

- ping -c 1 10.1.20.1: Aquesta comanda envia un paquet ICMP de ping a la passarel·la de la xarxa de clients (10.1.20.1). El client pot fer ping a la passarel·la.

- ping -c 1 google.com: Aquesta comanda envia un paquet ICMP de ping a un domini extern (google.com). El client pot fer ping a un domini extern, confirmant la configuració correcta de DNS i la connectivitat a Internet.

- dig @10.1.10.3 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el nom de domini google.com. El servidor DNS1 resol correctament el domini google.com.

- dig @10.1.10.4 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el nom de domini google.com. El servidor DNS2 resol correctament el domini google.com.

CLIENT 2:
Ara mirarem d'utilitzar un altre client 2 per veure si s'assigna correctament noves ips.
fitxer: 1-2-verificacio-client1.txt

- dhclient -v: Aquesta comanda s'executa per obtenir una adreça IP mitjançant DHCP. El client rep l'adreça IP 10.1.20.12 del servidor DHCP.

- cat /etc/network/interfaces: Aquesta comanda mostra la configuració de la interfície de xarxa. La interfície enp0s3 està configurada per obtenir una adreça IP mitjançant DHCP.

- cat /etc/resolv.conf: Aquesta comanda mostra la configuració dels servidors DNS. Els servidors configurats són 10.1.10.3 i 10.1.10.4, amb el domini seax.edu.

- ip a: Aquesta comanda mostra les adreces IP assignades a les interfícies de xarxa. El client ha rebut l'adreça IP 10.1.20.12, dins del rang configurat per a la xarxa de clients.

- ping -c 1 10.1.10.1: Aquesta comanda envia un paquet ICMP de ping a la passarel·la de la xarxa DMZ (10.1.10.1). El client pot fer ping a la passarel·la.

- ping -c 1 10.1.10.3: Aquesta comanda envia un paquet ICMP de ping al servidor DNS1 (10.1.10.3). El client pot fer ping al servidor DNS1.

- ping -c 1 10.1.10.4: Aquesta comanda envia un paquet ICMP de ping al servidor DNS2 (10.1.10.4). El client pot fer ping al servidor DNS2.

- ping -c 1 10.1.20.1: Aquesta comanda envia un paquet ICMP de ping a la passarel·la de la xarxa de clients (10.1.20.1). El client pot fer ping a la passarel·la.

- ping -c 1 google.com: Aquesta comanda envia un paquet ICMP de ping a un domini extern (google.com). El client pot fer ping a un domini extern, confirmant la configuració correcta de DNS i la connectivitat a Internet.

- dig @10.1.10.3 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el nom de domini google.com. El servidor DNS1 resol correctament el domini google.com.

- dig @10.1.10.4 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el nom de domini google.com. El servidor DNS2 resol correctament el domini google.com.

**** Verificacions de màquines en xarxa dmz:**

Les següents verificacions que hem fet és per unes màquines en la xarxa dmz:

MÀQUINA1:

- cat /etc/network/interfaces: Aquesta comanda mostra la configuració de la interfície de xarxa. La interfície enp0s3 està configurada per obtenir una adreça IP mitjançant DHCP.

- ip a: Aquesta comanda mostra les adreces IP assignades a les interfícies de xarxa. El client ha rebut l'adreça IP 10.1.10.7, dins del rang configurat per a la xarxa DMZ.

- ping -c 1 10.1.10.1: Aquesta comanda envia un paquet ICMP de ping a la passarel·la de la xarxa DMZ (10.1.10.1). El client pot fer ping a la passarel·la.

- ping -c 1 10.1.10.2: Aquesta comanda envia un paquet ICMP de ping a un dispositiu a la xarxa DMZ (10.1.10.2). El client pot fer ping a aquest dispositiu.

- ping -c 1 10.1.10.3: Aquesta comanda envia un paquet ICMP de ping al servidor DNS1 (10.1.10.3). El client pot fer ping al servidor DNS1.

- ping -c 1 10.1.10.4: Aquesta comanda envia un paquet ICMP de ping al servidor DNS2 (10.1.10.4). El client pot fer ping al servidor DNS2.

- ping -c 1 10.1.20.1: Aquesta comanda envia un paquet ICMP de ping a la passarel·la de la xarxa de clients (10.1.20.1). El client pot fer ping a la passarel·la.

- ping -c 1 google.com: Aquesta comanda envia un paquet ICMP de ping a un domini extern (google.com). El client pot fer ping a un domini extern, confirmant la configuració correcta de DNS i la connectivitat a Internet.

- dig @10.1.10.3 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el nom de domini google.com. El servidor DNS1 resol correctament el domini google.com.

- dig @10.1.10.4 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el nom de domini google.com. El servidor DNS2 resol correctament el domini google.com.

MONITOR:

El monitor de la xarxa DMZ està confgurat per la interfície de xarxa dmz que sigui activada, i aquesta tingui una ip assignada pel servei dhcp:

cat /etc/network/interfaces: Aquesta comanda mostra la configuració de la interfície de xarxa. Les interfícies enp0s3, enp0s8 i enp0s9 estan configurades amb DHCP per a la xarxa troncal i la xarxa DMZ, i amb una adreça IP estàtica per a la xarxa de clients respectivament.

systemctl restart networking: Aquesta comanda reinicia la configuració de la xarxa per aplicar els canvis.

ip a: Aquesta comanda mostra les adreces IP assignades a les interfícies de xarxa. El monitor ha rebut l'adreça IP 10.1.10.11 per la interfície enp0s8 (xarxa DMZ) i 10.1.20.11 per la interfície enp0s9 (xarxa de clients).

ping -c 1 10.1.10.1: Aquesta comanda envia un paquet ICMP de ping a la passarel·la de la xarxa DMZ (10.1.10.1). El monitor pot fer ping a la passarel·la.

ping -c 1 10.1.10.3: Aquesta comanda envia un paquet ICMP de ping al servidor DNS1 (10.1.10.3). El monitor pot fer ping al servidor DNS1.

ping -c 1 10.1.10.4: Aquesta comanda envia un paquet ICMP de ping al servidor DNS2 (10.1.10.4). El monitor pot fer ping al servidor DNS2.

ping -c 1 10.1.20.1: Aquesta comanda envia un paquet ICMP de ping a la passarel·la de la xarxa de clients (10.1.20.1). El monitor pot fer ping a la passarel·la.

ping -c 1 google.com: Aquesta comanda envia un paquet ICMP de ping a un domini extern (google.com). El monitor pot fer ping a un domini extern, confirmant la configuració correcta de DNS i la connectivitat a Internet.

dig @10.1.10.3 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el nom de domini google.com. El servidor DNS1 resol correctament el domini google.com.

dig @10.1.10.4 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el nom de domini google.com. El servidor DNS2 resol correctament el domini google.com.

Fitxers involucrats:

-/etc/network/interfaces
Configuració de les màquines per utilitzar el servidor dhcp

Fitxers d'evidència:

verificació dns:	1-2-config-dns1dns2.txt
verificació màquines:	1-2-verificacio-client1.txt
	1-2-verificacio-client2.txt
	1-2-verificacio-dmz1.txt
	1-2-verificacio-monitordmz.txt

Es poden veure els resultats de l'execució de les explicacions anteriors

***** Verificacions de xarxa**

2 CLIENTS ALHORA:

Els dos clients (10.1.20.11 i 10.1.20.10) estan negociant amb el servidor DHCP per obtenir les seves adreces IP i altres configuracions de xarxa necessàries. El procés inclou peticions i respostes que finalitzen amb l'assignació d'adreces IP i altres paràmetres de configuració de xarxa, assegurant que els clients puguin comunicar-se correctament a la xarxa eth-clients.

1. Petició DHCP del Primer Client (08:00:27:01:20:10)

El client amb MAC 08:00:27:01:20:10 envia una petició DHCP (DHCP Request).
Sol·licita l'adreça IP 10.1.20.11 amb el nom de host seax1. Paràmetres sol·licitats inclouen la màscara de subxarxa, la passarel·la per defecte, el nom de domini, i els servidors DNS.

El servidor DHCP (10.1.20.1) respon amb un ACK, confirmant que el client pot utilitzar l'adreça IP 10.1.20.11. Especifica la màscara de subxarxa, la passarel·la per defecte (10.1.20.1), el nom de domini (seax.edu), i els servidors DNS (10.1.10.3, 10.1.10.4).

2. Petició DHCP del Segon Client (08:00:27:01:20:11)
El client amb MAC 08:00:27:01:20:11 envia una petició DHCP (DHCP Discover). Sol·licita l'adreça IP 10.1.20.10 amb el nom de host seax1. Paràmetres sol·licitats inclouen la màscara de subxarxa, la passarel·la per defecte, el nom de domini, i els servidors DNS.

El servidor DHCP (10.1.20.1) respon amb una oferta DHCP (DHCP Offer), oferint l'adreça IP 10.1.20.10. Especifica la màscara de subxarxa, la passarel·la per defecte (10.1.20.1), el nom de domini (seax.edu), i els servidors DNS (10.1.10.3, 10.1.10.4).

El client respon amb una sol·licitud DHCP (DHCP Request), confirmant que vol utilitzar l'adreça IP 10.1.20.10. Paràmetres sol·licitats inclouen la màscara de subxarxa, la passarel·la per defecte, el nom de domini, i els servidors DNS.

El servidor DHCP respon amb un ACK, confirmant que el client pot utilitzar l'adreça IP 10.1.20.10. Especifica la màscara de subxarxa, la passarel·la per defecte (10.1.20.1), el nom de domini (seax.edu), i els servidors DNS (10.1.10.3, 10.1.10.4).

MÀQUINA EN DMZ:
Els clients de la xarxa DMZ estan negociant amb els servidors DHCP per obtenir adreces IP. Els clients fan sol·licituds d'adreça i reben respostes NACK quan les adreces no estan disponibles. Posteriorment, els clients fan noves sol·licituds de descobriment, reben ofertes de noves adreces IP, i finalment reben confirmació d'aquestes adreces juntament amb la configuració de xarxa necessària. Els servidors DHCP responen adequadament, oferint adreces IP disponibles i confirmant la configuració correcta de la xarxa.

1. Petició DHCP del Primer Client (08:00:27:01:10:11):

El client amb MAC 08:00:27:01:10:11 envia una petició DHCP sol·licitant l'adreça IP 10.1.20.11 amb el nom de host seax1. Sol·licita paràmetres com la màscara de subxarxa, la passarel·la per defecte, el nom de domini, i els servidors DNS.

El servidor DHCP (10.1.10.2) respon amb un missatge NACK indicant que l'adreça sol·licitada no està disponible.

2. Repetició de la Petició DHCP del Primer Client (08:00:27:01:10:11):

El client envia una nova petició DHCP Discover.

El servidor DHCP (10.1.10.2) respon oferint l'adreça IP 10.1.10.11. Especifica la màscara de subxarxa, la passarel·la per defecte, el nom de domini (seax.edu), i els servidors DNS (10.1.10.3, 10.1.10.4).

El client confirma que vol utilitzar l'adreça IP 10.1.10.11.

El servidor DHCP respon amb un ACK confirmant que el client pot utilitzar l'adreça IP 10.1.10.11. Especifica la màscara de subxarxa, la passarel·la per defecte, el nom de domini (seax.edu), i els servidors DNS (10.1.10.3, 10.1.10.4).

3. Petició DHCP del Segon Client (08:00:27:01:10:12):

El client amb MAC 08:00:27:01:10:12 envia una petició DHCP sol·licitant l'adreça IP 10.1.20.10 amb el nom de host seax1. Sol·licita paràmetres com la màscara de subxarxa, la passarel·la per defecte, el nom de domini, i els servidors DNS.

El servidor DHCP (10.1.10.2) respon amb un missatge NACK indicant que l'adreça sol·licitada no està disponible.

MÀQUINA DNS2:
En aquesta situació, el client amb MAC 08:00:27:01:10:04, identificat com dns2, està sol·licitant una adreça IP mitjançant DHCP. El servidor DHCP principal (10.1.10.2) respon oferint l'adreça 10.1.10.4 amb els paràmetres de configuració adequats. Tot i que hi ha un altre servidor DHCP (10.0.10.3) que ofereix adreces IP alternatives, el client acaba acceptant l'oferta del servidor principal i obté l'adreça IP 10.1.10.4. Aquest procés es repeteix per assegurar que el client tingui la configuració correcta.

Petició DHCP del Client dns2 (08:00:27:01:10:04):

El client amb MAC 08:00:27:01:10:04 envia una petició DHCP Discover sol·licitant una adreça IP. El nom del host és dns2 i sol·licita paràmetres com la màscara de subxarxa, la passarel·la per defecte, el nom de domini, i els servidors DNS.

El servidor DHCP (10.1.10.2) respon oferint l'adreça IP 10.1.10.4. Especifica la màscara de subxarxa, la passarel·la per defecte (10.1.10.1), el nom de domini (seax.edu), i els servidors DNS (10.1.10.3, 10.1.10.4).

Un altre servidor DHCP (10.0.10.3) respon oferint una adreça IP alternativa 10.0.10.9, però no és rellevant en aquest context.

2. Confirmació de la Petició DHCP del Client dns2 (08:00:27:01:10:04):

El client respon amb una sol·licitud DHCP (DHCP Request) confirmant que vol utilitzar l'adreça IP 10.1.10.4.

El servidor DHCP (10.1.10.2) respon amb un ACK confirmant que el client pot utilitzar l'adreça IP 10.1.10.4. Especifica la màscara de subxarxa, la passarel·la per defecte (10.1.10.1), el nom de domini (seax.edu), i els servidors DNS (10.1.10.3, 10.1.10.4).

3. Repetició de la Petició DHCP del Client dns2 (08:00:27:01:10:04):

El client envia una nova petició DHCP Discover. El nom del host segueix sent dns2 i sol·licita els mateixos paràmetres.

El servidor DHCP (10.1.10.2) torna a oferir l'adreça IP 10.1.10.4 amb els mateixos paràmetres.

Un altre servidor DHCP (10.0.10.3) torna a oferir una adreça IP alternativa 10.0.10.10.

El client confirma que vol utilitzar l'adreça IP 10.1.10.4 de nou.

El servidor DHCP (10.1.10.2) torna a confirmar amb un ACK que el client pot utilitzar l'adreça IP 10.1.10.4.

Fitxers d'evidència:

verificació tcpdumps:	1-3-tcpdump-dosclients.txt
	1-3-tcpdump-dmz.txt
	1-3-tcpdump-dns2.txt

Es poden veure els resultats de l'execució de les explicacions anteriors

Per millorar la seguretat d'una xarxa utilitzant DHCP, es poden aplicar diverses mesures que ajuden a controlar quines màquines poden rebre configuració IP i accedir a la xarxa. Aquestes son alguna de les propostes que hem trobat:

Llistes de Control d'Accés (ACL) basades en DHCP:

Podem configurar el servidor DHCP perquè només assigni adreces IP a dispositius coneguts mitjançant llistes de control d'accés basades en les adreces MAC. Només les adreces MAC registrades prèviament podran obtenir una IP.
Això es pot fer configurant reserves DHCP per a dispositius coneguts i assegurant-nos que cap altra adreça MAC pugui obtenir una IP.

Segregació de Subxarxes:
Utilitzarem múltiples subxarxes o VLANs per a diferents tipus de dispositius (per exemple, una subxarxa per a dispositius coneguts i confiables i una altra per a convidats o dispositius no confiables).
Els dispositius a la xarxa de convidats poden tenir accés limitat a recursos específics de la xarxa interna.

Registre i Monitoratge DHCP:
Configurarem el servidor DHCP per registrar tots els dispositius que sol·liciten adreces IP i monitoritzarem aquests registres regularment.
Això ens permetrà identificar i respondre ràpidament a dispositius no autoritzats que intentin connectar-se a la xarxa.

Assignació d'Adreces IP Temporals:
Assignarem adreces IP amb un període de lloguer curt per a dispositius desconeguts. Això limitarà el temps durant el qual un dispositiu no conegut pot romandre a la xarxa.
Això es pot complementar amb polítiques que requereixin una re-autenticació freqüent.

Totes aquestes mesures es podrien executar fent:
Una configuració de Reserves DHCP per a Dispositius Confiables:
Registrarem totes les adreces MAC dels dispositius coneguts i confiables.
Configurarem reserves DHCP per a aquestes adreces MAC al servidor DHCP.

Subxarxes Separades per a Convidats:
Crearem una subxarxa separada per a dispositius no registrats o convidats amb polítiques d'accés limitades.
Ens assegurarem que aquesta subxarxa tingui accés restringit als recursos crítics de la xarxa interna.

Fonts d'informació:

dhcp server debian:
https://wiki.debian.org/DHCP_Server?highlight=(/bCategoryNetworkApplication/b)|(CategoryNetwork)
dhcp client debian:
https://wiki.debian.org/DHCP_Client?highlight=(/bCategoryNetworkApplication/b)|(CategoryNetwork)

configurar server dhcp en linux:
https://www.linuxtechi.com/how-to-configure-dhcp-server-on-ubuntu/