***FASE 1:***

1. Instalación de dnsmasq

- Actualizar lista de paquetes:

*sudo apt update*

- Instalar dnsmasq:

*sudo apt install -y dnsmasq*

2. Copia de seguridad del fichero de configuración

- Hacer copia de dnsmasq.conf:

*sudo cp /etc/dnsmasq.conf /etc/dnsmasq.conf.bak*

3. Configurar escucha solo en LAN

- Editar /etc/dnsmasq.conf:

*sudo nano /etc/dnsmasq.conf*

- Añadir al principio:

*interface=enp0s3*

*bind-interfaces*

4. Definición de rangos DHCP por grupo

- Al final del fichero, añadir:

*dhcp-range=192.168.1.100,192.168.1.149,12h* # Desarrollo

*dhcp-range=192.168.1.150,192.168.1.199,12h*  # Diseño

*dhcp-range=192.168.1.200,192.168.1.249,12h* # Administración

5. Reservas estáticas por MAC

- Añadir después de los rangos:

*dhcp-host=AA:BB:CC:11:22:33,192.168.1.10*  # PC Jesús

*dhcp-host=DD:EE:FF:44:55:66,192.168.1.20* # Impresora Sala

6. Reiniciar y verificar funcionamiento

- Reiniciar dnsmasq:

*sudo systemctl restart dnsmasq*

- Comprobar estado del servicio:

*sudo systemctl status dnsmasq*

- Probar en cliente con DHCP:

*sudo netplan apply*

*ip a show enp0s3 | grep inet*

-> IP dentro del rango configurado

***FASE 2:***

1. Lista blanca de dispositivos en dnsmasq

- Editar /etc/dnsmasq.conf:

*sudo nano /etc/dnsmasq.conf*

- Añadir al principio:

*interface=enp0s3*

*bind-interfaces*

*dhcp-host=AA:BB:CC:11:22:33,set:authorized,pc-jesus,192.168.1.101*

*dhcp-host=DD:EE:FF:44:55:66,set:authorized,impresora-sala,192.168.1.102*

*dhcp-range=tag:authorized,192.168.1.100,192.168.1.150,12h*

- Reiniciar dnsmasq:

*sudo systemctl restart dnsmasq*

2. Validar DHCP y DNS local

- En cliente autorizado, solicitar IP:

*sudo netplan apply # o dhclient*

*ip a | grep inet*

- Ver hostname por DNS:

*nslookup pc-jesus 192.168.1.201*

3. Reglas de cortafuegos (iptables)

- *Políticas por defecto: rechazar todo:*

*sudo iptables -P INPUT DROP*

*sudo iptables -P FORWARD DROP*

- Permitir estado establecido:

*sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j* *ACCEPT*

- Abrir puertos DHCP y DNS:

*sudo iptables -A INPUT -p udp --dport 67:68 -j ACCEPT*

*sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT*

- Lista blanca de IPs:

*sudo iptables -A INPUT -s 192.168.1.101 -j ACCEPT*

*sudo iptables -A INPUT -s 192.168.1.102 -j ACCEPT*

- Permitir SSH (opcional):

*sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT*

4. Persistencia de reglas

- Instalar paquete:

*sudo apt install -y iptables-persistent*

- Guardar reglas actuales:

*sudo netfilter-persistent save*

5. Verificación

- Desde cliente autorizado:

*ping -c 3 192.168.1.201 # OK*

*ssh daviniase@192.168.1.201 # OK si SSH habilitado*

***FASE 3 :***

1. Preparar el cliente (dev1)

1. Duplicamos la máquina base y ponemos nombre dev1.

2. Aseguramos de que el equipo realmente se llame dev1:

*sudo hostnamectl set-hostname dev1*

3. Revisamos /etc/hosts y dejamos solo:

*127.0.0.1 localhost*

(Eliminamos otras á­neas para evitar errores con sudo.)

2. Pedimos IP al servidor (DHCP)

En el cliente abrimos */etc/netplan/00-installer-config.yaml* y comprobamos que ponga:

*dhcp4: true*

Luego aplicamos:

*sudo netplan apply*

El cliente debe recibir una IP dentro de 192.168.1.100-149.

3. Configurar el servidor DNS/DHCP

En el servidor editamos */etc/dnsmasq.conf* y añadimos al final:

*dhcp-range=192.168.1.100,192.168.1.149,12h*

*host-record=dev1,192.168.1.155*

*host-record=cliente-ntp2,192.168.1.151*

*host-record=srv-base-daviniaSierra,192.168.1.201*

*dhcp-option=option:dns-server,192.168.1.201*

Guardamos y reiniciamos:

*sudo systemctl restart dnsmasq*

4. Abrimos puertos necesarios

En el servidor:

*sudo iptables -I INPUT -p udp --dport 53 -j ACCEPT*

*sudo iptables -I INPUT -p icmp -j ACCEPT*

*sudo netfilter-persistent save*

5. Forzamos uso de DNS interno en el cliente

En dev1:

*sudo dhclient -r enp0s3*

*sudo dhclient enp0s3*

Comprobamos */etc/resolv.conf* que solo tenga:

nameserver 192.168.1.201

6. Comprobamos todo

1. Resolución de nombres:

*nslookup dev1 # debe devolver 192.168.1.155*

*nslookup cliente-ntp2*

*nslookup srv-base-daviniaSierra*

2. Ping:

*ping -4 -c2 dev1*

*ping -4 -c2 cliente-ntp2*

*ping -4 -c2 srv-base-daviniaSierra*

Errores corregidos

- Eliminamos la línea 127.0.1.1 dev1 de /etc/hosts, que impedía usar sudo.

- Añadimos host-record en dnsmasq para que el DNS conozca cada máquina.

- Abiertos puertos DNS (UDP 53) y Ping (ICMP) en el firewall.

***FASE 4:***

Capturar tráfico DHCP y DNS con tcpdump

**1.** Instalamos tcpdump:

*sudo apt update*

*sudo apt install -y tcpdump*

**2.** Capturamos 20 paquetes en la interfaz enp0s3 filtrando DHCP y DNS:

*sudo tcpdump -i enp0s3 'port 67 or port 68 or port 53' -n -c 20*

Vemos líneas como:

10:05:23.123456 IP 192.168.1.151.68 > 192.168.1.201.67: UDP, length 300

10:05:23.123789 IP 192.168.1.201.53 > 192.168.1.151.56789: UDP, length 100

que confirman peticiones DHCP y consultas DNS.

2. Revisamos logs de dnsmasq y syslog

1. Ver las últimas 20 líneas de DHCP en syslog:

*sudo grep dhcp /var/log/syslog | tail -n 20*

2. Ver las últimas 20 líneas de peticiones DNS de dnsmasq:

*sudo grep dnsmasq /var/log/syslog | tail -n 20*

No existe /var/log/dnsmasq.log por defecto, todo va al syslog.

**3.** Listar dispositivos con arp-scan

1. Instalamos arp-scan:

*sudo apt install -y arp-scan ieee-data*

2. Escaneamos la LAN:

*sudo arp-scan --interface=enp0s3 --localnet*

Vemos una tabla con IP y MAC, por ejemplo:

*192.168.1.155 08:00:27:52:88:43 dev1*

*192.168.1.201 AA:BB:CC:DD:EE:FF srv-base-daviniaSierra*

Los warnings de "Permission denied" al abrir los ficheros OUI no afectan al escaneo básico.