4. Instalación del servicio DHCP en entornos GNU/Linux.

En entornos corporativos basados en GNU/Linux, el servicio DHCP se implementa habitualmente mediante soluciones como:

- **ISC DHCP Server** (isc-dhcp-server), tradicional y ampliamente desplegado.
- **Kea DHCP**, evolución moderna del proyecto ISC, orientada a entornos más escalables y API-driven.
- Servicios DHCP integrados en firewalls o appliances Linux.

En este apartado se aborda la instalación en un servidor GNU/Linux estándar, considerando un entorno empresarial con planificación previa del esquema IP.

A diferencia de Windows Server, donde el despliegue se realiza mediante asistentes gráficos, en GNU/Linux la configuración suele implicar:

- Instalación mediante gestor de paquetes.
- Edición manual de archivos de configuración.
- Gestión del servicio mediante systemd.
- Verificación mediante herramientas de red y registros del sistema.

Este enfoque ofrece mayor flexibilidad, pero exige mayor precisión técnica.

4.1. Instalación del servidor.

Antes de proceder a la instalación del servicio DHCP en GNU/Linux, deben cumplirse varios requisitos previos similares a los exigidos en entornos Windows, aunque adaptados al modelo Unix.

El servidor debe tener configurada una dirección IP fija. Esto puede establecerse mediante:

- Configuración en /etc/netplan (Ubuntu).
- Archivos en /etc/network/interfaces (Debian antiguos).
- NetworkManager.
- Configuración manual mediante nmcli.

Ejemplo

Ejemplo conceptual de configuración estática:

- IP: 10.0.1.10
- Máscara: /24
- Gateway: 10.0.1.1
- DNS: servidor interno

Un servidor DHCP no debe depender de configuración dinámica.

En entornos virtualizados (VMware, Hyper-V, Proxmox), debe verificarse que la interfaz virtual esté conectada al segmento correcto antes de iniciar la configuración. Una mala asociación de red puede provocar asignaciones en subred incorrecta.

Instalación mediante gestor de paquetes

En sistemas basados en Debian/Ubuntu:

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

En sistemas basados en Red Hat / Rocky / AlmaLinux:

```
sudo dnf install dhcp-server
```

La instalación despliega:

- Binarios del servicio.
- Archivos de configuración.
- Archivos de ejemplo.
- Servicio gestionado por systemd.

Identificación de la interfaz de red

Antes de activar el servicio, debe indicarse qué interfaz escuchará solicitudes DHCP.

En sistemas Debian/Ubuntu, suele configurarse en: `/etc/default/isc-dhcp-server`

Ejemplo: `INTERFACESv4="ens33"`

La interfaz debe corresponder exactamente al segmento donde se ofrecerán direcciones.

Puede verificarse mediante: `ip a`

Archivo principal de configuración

El archivo central del servicio suele ubicarse en: `/etc/dhcp/dhcpd.conf`

Este archivo define:

- Subredes.
- Rangos dinámicos.
- Opciones.
- Reservas.
- Parámetros globales.

Ejemplo

Un ejemplo mínimo conceptual:

```
subnet 10.0.20.0 netmask 255.255.255.0 {
  range 10.0.20.50 10.0.20.150;
  option routers 10.0.20.1;
  option domain-name-servers 10.0.20.10;
  default-lease-time 604800;
  max-lease-time 1209600;
}
```

La sintaxis debe ser rigurosamente correcta; un error impide el arranque del servicio.

Nota

En GNU/Linux, el servicio no arranca si detecta errores de sintaxis en el archivo de configuración. Esto constituye una ventaja en términos de control, pero obliga a verificar cuidadosamente cada modificación.

Comprobación de la configuración

Antes de iniciar el servicio, puede verificarse la sintaxis con:

```
sudo dhcpd -t
```

Este comando analiza el archivo de configuración sin iniciar el servidor.

Inicio y habilitación del servicio

Una vez verificada la configuración:

```
sudo systemctl start isc-dhcp-server
sudo systemctl enable isc-dhcp-server
```

Para comprobar su estado:

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

Los registros pueden consultarse mediante:

```
journalctl -u isc-dhcp-server
```

Verificación operativa

Tras iniciar el servicio, deben realizarse pruebas:

- Conectar un equipo cliente en la subred.
- Verificar obtención de IP.
- Comprobar gateway y DNS.
- Revisar tabla de concesiones.

El archivo de concesiones suele ubicarse en:

```
/var/lib/dhcp/dhcpd.leases
```

Este archivo registra todas las asignaciones activas y expiradas.

Ejemplo

Supóngase una empresa que utiliza GNU/Linux como servidor central en una sede remota.

- IP servidor: 10.1.0.2
- Subred: 10.1.0.0/24
- Gateway: 10.1.0.1
- DNS interno: 10.1.0.5
- Rango dinámico: 10.1.0.50–10.1.0.150

Se instala isc-dhcp-server.

Se configura el archivo dhcpd.conf.

Se valida sintaxis.

Se inicia servicio.

Se verifica obtención correcta desde un equipo cliente.

En menos de 10 minutos puede quedar operativo si el diseño previo está correctamente definido.

Consideraciones de seguridad inicial

Tras la instalación, es recomendable:

- Limitar acceso SSH al servidor.
- Restringir acceso al archivo dhcpd.conf.
- Implementar copias de seguridad.
- Configurar logs centralizados.
- Monitorizar uso de direcciones.

La protección del servidor DHCP incluye medidas físicas y copias de seguridad periódicas para garantizar la continuidad del servicio.

El servidor DHCP, aunque sencillo en apariencia, forma parte de la infraestructura crítica.

4.2. Configuración del archivo dhcpd.conf.

El archivo dhcpd.conf constituye el núcleo de configuración del servidor DHCP en sistemas GNU/Linux basados en ISC DHCP. A diferencia de los entornos Windows, donde la configuración se realiza principalmente mediante interfaz gráfica, en GNU/Linux la administración se basa en la edición directa de este archivo, lo que proporciona mayor flexibilidad, pero exige precisión técnica.

Su correcta estructuración es esencial para evitar errores de asignación, conflictos de red o fallos de arranque del servicio.

Estructura general del archivo

El archivo dhcpd.conf se compone de:

- Parámetros globales.
- Definición de subredes (subnet).
- Rangos dinámicos (range).
- Opciones DHCP.
- Reservas (host).
- Parámetros de concesión.

Ejemplo

Un esquema simplificado puede representarse así:

```
# Parámetros globales
default-lease-time 604800;
max-lease-time 1209600;
authoritative;
# Definición de subred
subnet 10.0.20.0 netmask 255.255.255.0 {
   range 10.0.20.50 10.0.20.150;
   option routers 10.0.20.1;
   option domain-name-servers 10.0.20.10;
   option domain-name "empresa.local";
}
```

Cada bloque debe cerrarse correctamente con llaves y punto y coma. La ausencia de un carácter puede impedir el inicio del servicio.

Parámetros globales

Los parámetros globales se aplican a todas las subredes salvo que se sobrescriban dentro de un bloque específico. Los más habituales son:

- default-lease-time: duración estándar de la concesión.
- max-lease-time: duración máxima permitida.
- authoritative: indica que el servidor es la autoridad legítima para esa red.
- log-facility: define el sistema de registro.

Ejemplo

```
default-lease-time 86400;
max-lease-time 604800;
authoritative;
```

El parámetro authoritative es especialmente importante en redes corporativas, ya que indica al servidor que puede enviar mensajes DHCP NAK si detecta asignaciones incorrectas.

En redes donde se sustituye un servidor antiguo por uno nuevo, no declarar el servidor como "authoritative" puede generar retrasos en la reasignación de direcciones y comportamientos inesperados en clientes.

Definición de subredes

Cada subred debe declararse explícitamente mediante la directiva subnet.

Ejemplo

```
subnet 10.0.30.0 netmask 255.255.255.0 {
  range 10.0.30.50 10.0.30.180;
  option routers 10.0.30.1;
  option domain-name-servers 10.0.30.10;
}
```

Si existen múltiples VLAN, cada una requerirá su propio bloque subnet.

Es importante que:

- La dirección de red coincida con la configuración del router.
- La máscara sea coherente.
- No existan solapamientos entre bloques.

Exclusiones y diseño del rango

En ISC DHCP no se define explícitamente una exclusión como en Windows; simplemente se limita el rango dinámico para que no incluya direcciones reservadas.

Ejemplo

Infraestructura estática: 10.0.30.1–10.0.30.20

Rango dinámico: range 10.0.30.50 10.0.30.180;

Las direcciones fuera del rango nunca serán asignadas dinámicamente.

Configuración de reservas

Las reservas se definen mediante bloques host fuera o dentro de la subred correspondiente.

Ejemplo

```
host impresora_finanzas {
  hardware ethernet 00:1A:2B:3C:4D:5E;
  fixed-address 10.0.30.25;
}
```

El servidor identificará al cliente por su dirección MAC y le asignará siempre la dirección especificada.

Las reservas pueden incluir opciones personalizadas adicionales:

```
host telefono_voip {
  hardware ethernet 00:AA:BB:CC:DD:EE;
  fixed-address 10.0.30.40;
  option tftp-server-name "10.0.30.15";
}
```

Configuración avanzada: múltiples subredes

En entornos empresariales con segmentación, es habitual definir múltiples subredes en el mismo archivo:

```
subnet 10.0.10.0 netmask 255.255.255.0 {
  range 10.0.10.50 10.0.10.150;
  option routers 10.0.10.1;
}
subnet 10.0.20.0 netmask 255.255.255.0 {
  range 10.0.20.50 10.0.20.150;
  option routers 10.0.20.1;
}
```

Esto requiere que el servidor pueda recibir solicitudes de esas redes mediante DHCP Relay si no se encuentra físicamente en cada segmento.

Recuerda

Un error en la definición de subred puede provocar asignaciones fuera del segmento real, generando conflictos y pérdida de conectividad. La coherencia entre router, VLAN y archivo dhcpd.conf es crítica.

4.3. Pruebas y validación.

Una vez configurado el archivo y arrancado el servicio, la fase de pruebas es fundamental para garantizar que el servidor funciona correctamente y no genera incidencias en producción.

Validación de sintaxis

Antes de iniciar el servicio: `sudo dhcpd -t`

Este comando verifica la sintaxis del archivo sin ejecutarlo.

Si existen errores, deben corregirse antes de continuar.

Verificación del estado del servicio

`sudo systemctl status isc-dhcp-server` Debe confirmarse:

- Servicio activo (active/running).
- Ausencia de errores críticos.
- Interfaz correcta en escucha.

Prueba desde cliente

En un equipo cliente GNU/Linux: `sudo dhclient -v`

En Windows:

`ipconfig /release`

`ipconfig /renew`

Se debe comprobar:

- Dirección IP obtenida.
- Gateway correcto.
- DNS correcto.
- Tiempo de concesión.

Análisis de registros

Los registros pueden consultarse mediante: `journalctl -u isc-dhcp-server`

o en sistemas con syslog tradicional: `/var/log/syslog`

Debe verificarse:

- Recepción de mensajes Discover.
- Envío de Offer.
- Confirmación ACK.
- Ausencia de errores de asignación.

Verificación del archivo de concesiones

El archivo: /var/lib/dhcp/dhcpd.leases

Permite comprobar:

- Direcciones asignadas.
- Estado de cada lease.
- Fecha de expiración.
- Dirección MAC asociada.

Este archivo es esencial en auditorías y diagnóstico de incidencias.

Ejemplo

En una red 10.0.50.0/24:

1. Se configura ámbito dinámico 10.0.50.100–10.0.50.200.
2. Se arranca servicio.
3. Un equipo cliente obtiene 10.0.50.101.
4. Se verifica en dhcpd.leases.
5. Se comprueba conectividad a gateway y resolución DNS.

Si todos los pasos son correctos, el servidor puede considerarse operativo.

Pruebas en entorno segmentado

Si existen VLAN:

- Verificar que DHCP Relay esté configurado en router.
- Confirmar recepción de solicitudes desde cada subred.
- Probar cliente en cada segmento.
- Revisar logs para identificar posibles bloqueos de firewall.

Nota

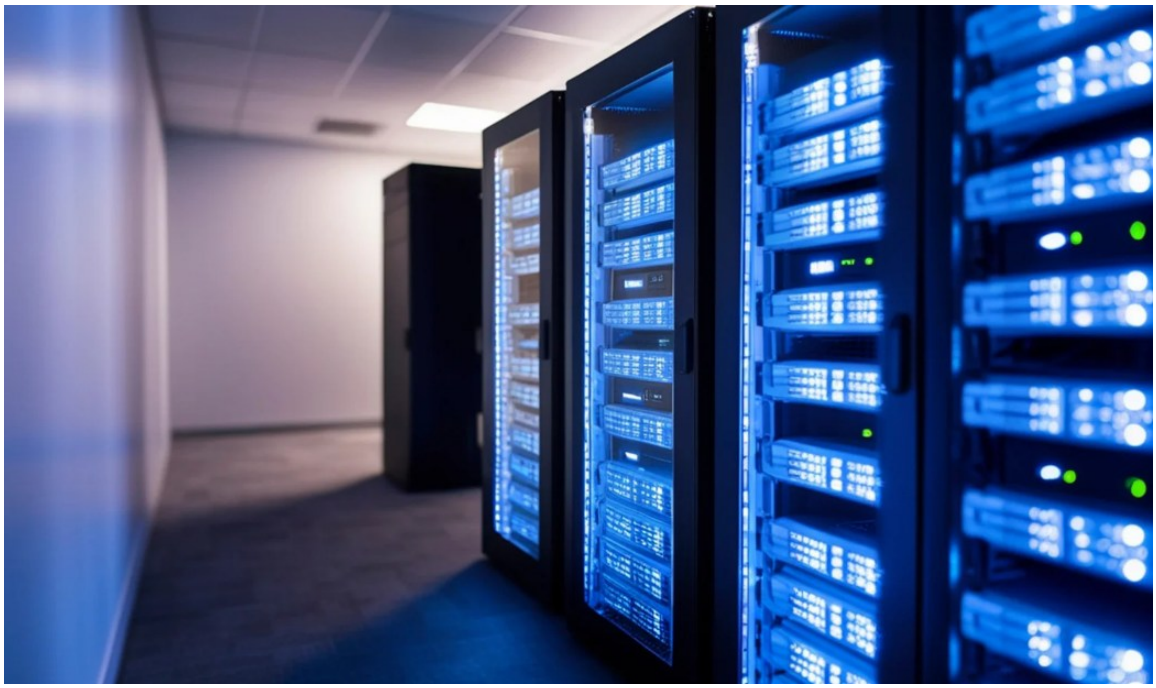
Antes de desplegar en producción, es recomendable realizar pruebas en un entorno controlado o fuera del horario laboral. Un error en la configuración DHCP puede afectar simultáneamente a toda la red.

5. Alta disponibilidad y redundancia.

El servicio DHCP es un componente crítico de la infraestructura de red. Aunque técnicamente los equipos pueden seguir funcionando durante el tiempo que dure su concesión activa, la caída prolongada del servidor DHCP provoca:

- Imposibilidad de que nuevos dispositivos obtengan dirección IP.
- Pérdida de conectividad tras expiración de leases.
- Interrupción de servicios dependientes.
- Incidencias masivas en redes WiFi o entornos con alta rotación.

Por este motivo, en entornos corporativos medianos y grandes, el despliegue del servicio DHCP debe contemplar mecanismos de **alta disponibilidad (HA)** y redundancia.



Infraestructura de centro de datos diseñada para garantizar alta disponibilidad y continuidad de los servicios de red corporativos.

La alta disponibilidad busca garantizar continuidad operativa ante fallos de hardware, sistema operativo o red.

5.1. Failover DHCP.

El failover DHCP permite que dos servidores trabajen conjuntamente compartiendo información sobre concesiones, estados y disponibilidad de direcciones. Si uno de los servidores falla, el otro puede continuar ofreciendo servicio sin pérdida significativa de funcionalidad.

Concepto de failover

En un esquema de failover:

- Existen al menos dos servidores DHCP.

- Ambos comparten información de concesiones.
- Se comunican constantemente para sincronizar estados.
- Gestionan conjuntamente el mismo ámbito o conjunto de ámbitos.

Si uno queda fuera de servicio, el otro asume la responsabilidad.

Failover en Windows Server

Windows Server incorpora soporte nativo de failover DHCP desde versiones modernas.

Existen dos modos principales:

- **Load Balance (Balanceo de carga activo-activo)**
- **Hot Standby (Activo-pasivo)**

En modo Load Balance:

- Ambos servidores atienden solicitudes simultáneamente.
- El porcentaje habitual de reparto es 50/50.
- Ambos mantienen sincronizadas las concesiones.

En modo Hot Standby:

- Un servidor actúa como principal.
- El segundo permanece en espera.
- Solo entra en funcionamiento si el principal falla.

El proceso conceptual de configuración consiste en:

1. Instalar rol DHCP en ambos servidores.
2. Crear ámbito en servidor principal.
3. Configurar asociación de failover.
4. Definir modo operativo.
5. Establecer secreto compartido.
6. Iniciar sincronización.

Una vez configurado, ambos servidores mantienen comunicación constante para actualizar estados de concesión.


Nota

En modo Load Balance, cada servidor gestiona un porcentaje del pool. Sin embargo, ambos conocen el estado completo de las concesiones. Esto evita asignaciones duplicadas incluso en caso de fallo parcial.

Failover en GNU/Linux (ISC DHCP)

En ISC DHCP, el failover se configura manualmente dentro del archivo dhcpd.conf, declarando un bloque failover peer.

Ejemplo

Ejemplo conceptual:

```
failover peer "dhcp-failover" {
   primary;
   address 10.0.1.10;
   port 647;
   peer address 10.0.1.11;
   peer port 647;
   max-response-delay 60;
   max-unacked-updates 10;
   load balance max seconds 3;
}
```

Cada servidor debe configurarse como primary o secondary según corresponda.

Este método requiere:

- Sincronización adecuada.
- Configuración idéntica de ámbitos.
- Comunicación estable entre servidores.

Algunas consideraciones técnicas en failover son:

- Ambos servidores deben tener relojes sincronizados.
- La conectividad entre ellos debe ser estable.
- Debe evitarse que ambos operen aislados durante tiempo prolongado.
- Se recomienda monitorización activa.

Ejemplo

Una empresa con 600 dispositivos en red cableada y WiFi corporativa:

- Implementa dos servidores DHCP virtualizados.
- Configura modo Load Balance.
- Si uno falla por mantenimiento o error, el otro continúa operando.
- Los usuarios no perciben interrupción.

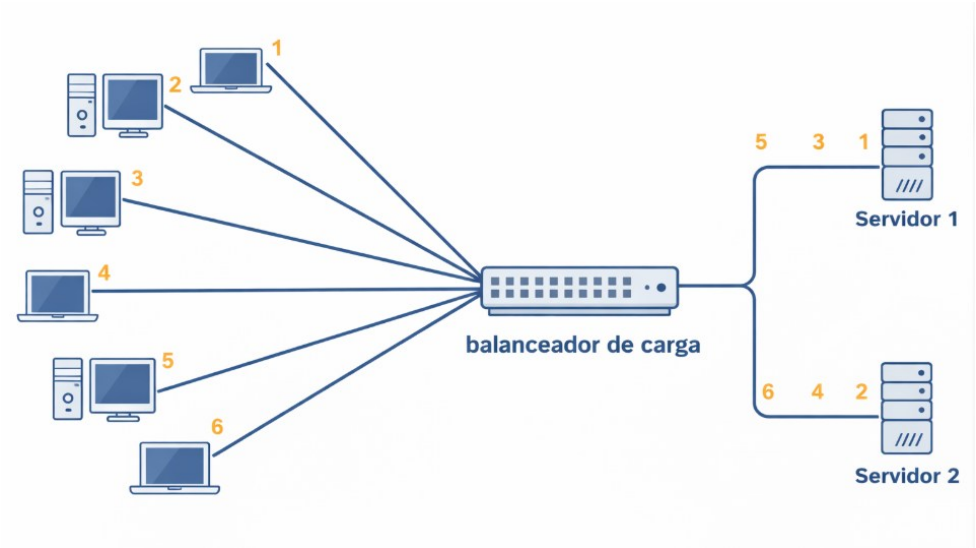
Este modelo elimina punto único de fallo.

5.2. Balanceo y replicación.

El balanceo y la replicación son conceptos relacionados con la distribución de carga y la sincronización de información entre servidores DHCP. Aunque a veces se utilizan como sinónimos, técnicamente representan aspectos distintos.

Balanceo de carga

El balanceo distribuye solicitudes DHCP entre dos o más servidores activos.



Representación conceptual del reparto de solicitudes DHCP entre servidores en modo activo-activo, mecanismo utilizado para garantizar alta disponibilidad y resiliencia en entornos corporativos.

Sus objetivos son:

- Repartir carga de trabajo.
- Mejorar rendimiento.
- Reducir latencia.
- Incrementar resiliencia.

En modo activo-activo:

- Ambos servidores responden a solicitudes.
- El reparto puede ser 50/50 o ajustable.
- Las concesiones se sincronizan constantemente.

Este modelo es recomendable en:

- Redes con alta densidad de dispositivos.
- Entornos educativos.
- Oficinas con elevada movilidad.
- Infraestructuras WiFi intensivas.

Replicación de concesiones

La replicación garantiza que ambos servidores conozcan:

- Direcciones asignadas.
- Estado de cada lease.
- Tiempos de expiración.
- Información de cliente.

Sin replicación, dos servidores podrían asignar la misma dirección a clientes distintos, generando conflicto IP.

En entornos modernos:

- Windows Server realiza replicación automática en failover.
- ISC DHCP sincroniza mediante protocolo de failover.
- Kea DHCP utiliza base de datos centralizada o mecanismos avanzados de backend.

La siguiente tabla resume diferencias entre modelos habituales:

Modelo	Servidores activos	Sincronización	Uso recomendado
Único servidor	1	No aplica	Redes pequeñas
Hot Standby	1 activo + 1 espera	Sí	Redes medianas
Load Balance	2 activos	Sí	Redes grandes
Independientes sin replicación	2	No	No recomendado

El último modelo no es adecuado para entornos corporativos, ya que puede provocar conflictos graves.

Diseño 80/20 tradicional

Antes del soporte nativo de failover, era habitual dividir el rango DHCP en proporción 80/20 entre dos servidores independientes.

Por ejemplo:

- Servidor A → 80% del rango.
- Servidor B → 20% del rango.

Si A fallaba, B aún podía asignar direcciones, aunque limitadamente.

Este método:

- No sincroniza concesiones.
- Es menos eficiente.
- Se considera solución heredada.

Actualmente se recomienda failover real con replicación.

Recuerda

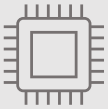
En entornos críticos (hospitales, industria, finanzas), el servidor DHCP debe desplegarse en infraestructura virtualizada con alta disponibilidad del propio hipervisor, además de failover a nivel de servicio. La redundancia debe contemplarse en múltiples capas.

Monitorización en entornos redundantes

Una infraestructura redundante requiere supervisión constante:

- Estado de sincronización.
- Latencia entre servidores.
- Uso de pool disponible.
- Eventos de failover.
- Alertas ante desconexión de peers.

La ausencia de monitorización puede ocultar fallos hasta que se produce una incidencia real.



Actividad 3

Una organización sanitaria con 900 dispositivos conectados (equipos clínicos, estaciones de trabajo, WiFi médica y terminales móviles) quiere eliminar el punto único de fallo de su servidor DHCP actual.

El equipo técnico plantea tres opciones:

A) Instalar un segundo servidor DHCP independiente sin sincronización.

B) Configurar dos servidores en modo 80/20 tradicional.

C) Implementar failover en modo Load Balance con replicación de concesiones.

Debes:

Indicar cuál es la opción técnicamente correcta para este entorno.

Explicar por qué las otras dos opciones no son adecuadas.

Señalar qué aspectos deben monitorizarse una vez implantada la solución.

6. Seguridad en DHCP.

Aunque DHCP es un protocolo esencial para la automatización de la configuración de red, su diseño original no incorporaba mecanismos de autenticación robusta. Esto implica que, si no se aplican medidas adicionales, puede convertirse en un vector de ataque dentro de la red corporativa.

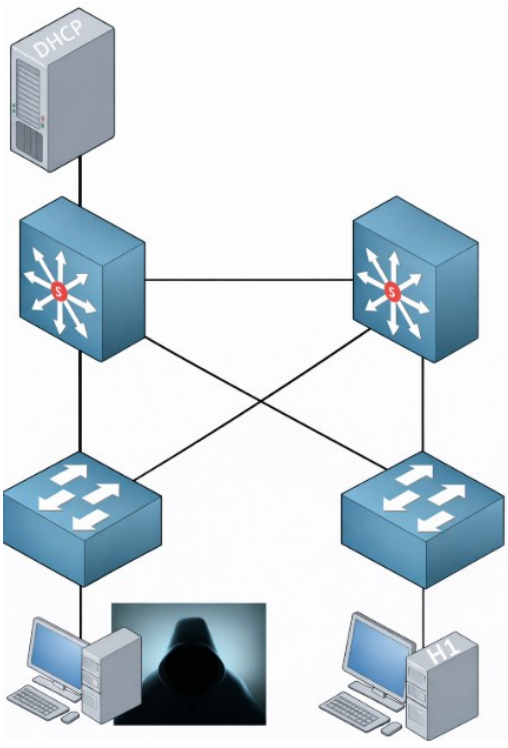
Las principales amenazas asociadas a DHCP son:

- Servidores DHCP no autorizados (rogue DHCP).
- Asignación de parámetros maliciosos.
- Redirección de tráfico hacia gateways fraudulentos.
- Ataques de denegación de servicio por agotamiento del pool.
- Suplantación de identidad mediante MAC spoofing.

Por tanto, en entornos profesionales es imprescindible complementar la instalación del servicio con mecanismos de protección a nivel de infraestructura de red.

6.1. DHCP Snooping.

DHCP Snooping es un mecanismo de seguridad implementado en switches gestionables (normalmente de capa 2 o capa 3) que permite controlar qué puertos pueden enviar respuestas DHCP. Su objetivo principal es evitar que un dispositivo no autorizado actúe como servidor DHCP dentro de la red.



Topología de red con servidor DHCP autorizado y equipo potencialmente malicioso. DHCP Snooping habilitado en el switch impide que dispositivos conectados a puertos no confiables envíen respuestas DHCP a los clientes.

En un entorno con DHCP Snooping habilitado:

- Se definen puertos **confiables (trusted)**.
- Se definen puertos **no confiables (untrusted)**.
- Solo los puertos confiables pueden enviar mensajes DHCP Offer y ACK.
- Los mensajes DHCP Discover y Request pueden originarse desde cualquier puerto.

Normalmente:

- El puerto conectado al servidor DHCP se marca como confiable.
- El puerto conectado al router (si actúa como relay) también.
- Los puertos de usuario final se marcan como no confiables.

Si un equipo conectado a un puerto no confiable intenta enviar una oferta DHCP, el switch la bloquea automáticamente.

DHCP Snooping genera una tabla interna denominada **binding table**, que asocia:

- Dirección IP asignada.
- Dirección MAC.
- Puerto físico.
- VLAN.
- Tiempo de concesión.

Esta tabla puede utilizarse posteriormente para reforzar otros mecanismos de seguridad como:

- IP Source Guard.
- Dynamic ARP Inspection (DAI).

La existencia de esta tabla permite verificar coherencia entre IP, MAC y puerto físico.

 Nota

En redes donde DHCP Snooping está habilitado, si el servidor DHCP cambia de puerto físico y no se actualiza la configuración de puertos confiables, la red puede quedar sin servicio DHCP aunque el servidor esté funcionando correctamente.

Protección frente a ataques de agotamiento (DHCP Starvation)

Un atacante puede generar múltiples solicitudes DHCP con direcciones MAC falsas para agotar el pool disponible. Este ataque se conoce como **DHCP Starvation**.

DHCP Snooping puede configurarse para:

- Limitar número de solicitudes por puerto.
- Detectar comportamiento anómalo.
- Bloquear tráfico excesivo.

Esto protege la disponibilidad del servicio.

 Ejemplo

En una red universitaria con cientos de estudiantes conectados:

- Se habilita DHCP Snooping en todos los switches.
- Se marca como trusted únicamente el puerto hacia el servidor central.
- Se limita a 10 solicitudes DHCP por segundo en puertos de usuario.
- Se habilita registro de eventos sospechosos.

Esto evita que un estudiante configure un servidor DHCP personal para redirigir tráfico.

6.2. Prevención de servidores no autorizados.

Un servidor DHCP no autorizado (rogue DHCP) es un dispositivo que responde a solicitudes DHCP sin estar oficialmente configurado por el departamento técnico.

Este tipo de servidor puede asignar:

- Gateway malicioso.
- DNS fraudulento.
- IP incorrecta.
- Parámetros que redirigen tráfico hacia un atacante.

El impacto puede incluir:

- Interceptación de credenciales.
- Ataques Man-in-the-Middle.
- Pérdida de conectividad.
- Exfiltración de datos.

Medidas preventivas a nivel de infraestructura

Las principales medidas para evitar servidores no autorizados son:

1. Implementación de DHCP Snooping.
2. Segmentación adecuada por VLAN.

3. Control de acceso a red (802.1X).
4. Monitorización continua del tráfico DHCP.
5. Restricción física de acceso a switches.

Los mecanismos de seguridad como DHCP Snooping y la segmentación por VLAN se configuran en switches gestionables dentro de la infraestructura de red.

Autorización en Active Directory (entornos Windows)

En redes basadas en dominio:

- El servidor DHCP debe autorizarse explícitamente en Active Directory.
- Un servidor no autorizado no podrá iniciar el servicio.
- El directorio mantiene registro de servidores legítimos.

Este mecanismo reduce significativamente el riesgo dentro de redes corporativas basadas en Windows.

Monitorización y detección

Es recomendable implementar:

- Herramientas de escaneo de red.
- Sistemas IDS/IPS.
- Alertas ante aparición de nuevas respuestas DHCP.
- Registro centralizado de eventos.

Una respuesta DHCP proveniente de dirección no documentada debe investigarse inmediatamente.

Recuerda

En redes corporativas grandes, la prevención no debe limitarse al control técnico. Deben establecerse políticas internas que prohíban la conexión de dispositivos de red no autorizados, incluyendo routers domésticos o puntos de acceso personales.

Integración con 802.1X y NAC

Los sistemas de autenticación de acceso a red permiten que un dispositivo:

- Se autentique antes de obtener dirección IP.
- Sea asignado a VLAN específica según perfil.
- Sea bloqueado si no cumple políticas de seguridad.

La combinación de:

- DHCP Snooping
- 802.1X
- NAC
- Monitorización centralizada

proporciona un modelo de defensa en profundidad.

Ejemplo

Una empresa con maquinaria conectada a red implementa:

- VLAN separadas para IoT.
- DHCP Snooping en switches industriales.
- Reservas DHCP para dispositivos críticos.
- Monitorización continua.

Cuando un empleado conecta un router personal para mejorar cobertura WiFi, el switch bloquea inmediatamente sus respuestas DHCP.

Buenas prácticas en seguridad DHCP

Se recomienda:

- Documentar servidores autorizados.
- Limitar físicamente el acceso a racks.
- Implementar failover seguro.
- Monitorizar logs periódicamente.
- Auditar tabla de concesiones.
- Revisar periódicamente configuración de switches.

Supervisión técnica de infraestructura en rack: el control físico y la monitorización periódica forman parte de las buenas prácticas en seguridad de servicios DHCP.

El servicio DHCP, aunque aparentemente simple, puede convertirse en un punto crítico de vulnerabilidad si no se protege adecuadamente.

7. Monitorización y resolución de incidencias.

La correcta configuración del servicio DHCP no garantiza por sí sola su funcionamiento continuo. En entornos corporativos, donde cientos o miles de dispositivos dependen de este servicio, la **monitorización constante** y la **capacidad de diagnóstico estructurado** son elementos esenciales para garantizar la disponibilidad.

Una incidencia DHCP puede manifestarse de múltiples formas:

- Equipos que no obtienen dirección IP.
- Asignaciones duplicadas.
- Lentitud en la obtención de configuración.
- Concesiones que no se renuevan.
- Fallos de resolución DNS tras asignación correcta.

La resolución eficaz exige comprender tanto el funcionamiento interno del protocolo como la arquitectura de red subyacente.

Monitorización del servicio DHCP

La monitorización debe realizarse en varios niveles:

- Estado del servicio.
- Uso del pool de direcciones.
- Registro de eventos.
- Comunicación con servidores secundarios.
- Integridad de la base de datos de concesiones.

Supervisión del estado del servicio

En Windows Server:

- Verificación desde el Administrador del servidor.
- Consulta del Visor de eventos.
- Supervisión mediante herramientas de monitorización (SCOM, Zabbix, PRTG).

En GNU/Linux:

```
systemctl status isc-dhcp-server
journalctl -u isc-dhcp-server
```

Debe confirmarse que:

- El servicio esté activo.
- No existan errores recurrentes.
- No se registren reinicios inesperados.

Control de utilización del ámbito

Un problema frecuente en redes corporativas es el **agotamiento del pool DHCP**.

El administrador debe monitorizar:

- Número total de direcciones disponibles.
- Número de concesiones activas.
- Tendencia de crecimiento.
- Existencia de leases expirados no liberados.

En Windows Server, la consola DHCP muestra estadísticas por ámbito.

En GNU/Linux, debe analizarse el archivo dhcpd.leases.

Nota

El agotamiento del pool suele producirse en redes WiFi con lease prolongado o en casos de ataque DHCP Starvation. Una supervisión periódica evita que la incidencia se detecte únicamente cuando los usuarios ya no obtienen IP.

Monitorización en entornos con failover

En configuraciones redundantes es imprescindible supervisar:

- Estado de sincronización.
- Conectividad entre servidores.
- Eventos de failover.
- Latencia de replicación.

La pérdida de sincronización puede no generar fallo inmediato, pero sí inconsistencias futuras.

Resolución estructurada de incidencias

El diagnóstico debe realizarse siguiendo un procedimiento metódico. Las incidencias DHCP no siempre tienen origen en el servidor; pueden estar relacionadas con:

- Segmentación de red.
- Configuración de VLAN.
- DHCP Relay.
- Firewalls.
- Problemas físicos de conexión.

Equipos que no obtienen dirección IP

Cuando un equipo no obtiene IP, el procedimiento recomendado es:

1. Verificar conectividad física.
2. Comprobar estado de la interfaz.
3. Forzar renovación de IP.
4. Revisar si obtiene dirección APIPA (169.254.x.x).
5. Analizar registros del servidor DHCP.
6. Verificar configuración de DHCP Relay.

Si el cliente recibe dirección APIPA, significa que no ha recibido respuesta del servidor.

Conflictos de dirección IP

Un conflicto IP puede producirse cuando:

- Existe un dispositivo con IP estática dentro del rango dinámico.
- Falló la sincronización en un entorno redundante.
- Un servidor rogue asigna direcciones duplicadas.

El diagnóstico debe incluir:

- Análisis de tabla ARP.
- Revisión de reservas.
- Verificación de exclusiones.
- Comprobación de existencia de servidores no autorizados.

Ejemplo

En una oficina se detecta que varios equipos pierden conectividad intermitente. Se observa que dos dispositivos tienen la misma IP.

El análisis revela que:

- Un equipo antiguo fue configurado manualmente con IP dentro del rango dinámico.
- El servidor DHCP asignó esa misma IP a otro cliente.
- Se corrige excluyendo esa dirección del ámbito.

Este tipo de error es común en redes con documentación incompleta.

Lentitud en asignación

La asignación lenta puede deberse a:

- Saturación del servidor.
- Problemas de red.
- Retransmisiones DHCP Relay.
- Latencia entre servidores en failover.
- Configuración incorrecta de puertos confiables en switches.

El análisis debe incluir:

- Captura de tráfico mediante herramientas como Wireshark.
- Medición de tiempo entre Discover y ACK.
- Revisión de carga del servidor.

Nota

Una diferencia excesiva entre el envío de DHCP Discover y la recepción del DHCP Offer suele indicar problemas de retransmisión o filtrado en dispositivos intermedios.

Problemas tras renovación de concesión

Si un cliente pierde conectividad tras renovar su lease, puede deberse a:

- Cambio en configuración de opciones.
- Error en DNS distribuido.
- Fallo de sincronización en entorno redundante.
- Inconsistencia en archivo de concesiones.

En estos casos, es recomendable:

- Liberar manualmente la concesión.
- Reiniciar interfaz del cliente.
- Verificar coherencia en el servidor.

Herramientas de diagnóstico

Un administrador debe dominar herramientas específicas para análisis de incidencias DHCP.

En Windows:

```
ipconfig /all
ipconfig /release
ipconfig /renew
```

En GNU/Linux:

```
ip a
dhclient -v
```

Estas herramientas permiten verificar:

- IP asignada.
- Servidores DNS.
- Gateway.
- Tiempo restante de concesión.

Análisis de tráfico

Wireshark permite observar directamente el proceso DORA:

- DHCP Discover.
- DHCP Offer.
- DHCP Request.
- DHCP ACK.

El análisis del tráfico puede revelar:

- Retrasos.
- Respuestas múltiples.
- Respuestas de servidor no autorizado.
- Errores en opciones enviadas.

Revisión de logs

Los registros del servidor proporcionan información clave:

- Concesiones otorgadas.
- Errores de asignación.
- Conflictos detectados.
- Eventos de failover.

La centralización de logs en un sistema SIEM mejora la capacidad de análisis histórico.

Buenas prácticas operativas

Para minimizar incidencias:

- Mantener documentación actualizada del esquema IP.
- Supervisar periódicamente uso del pool.
- Implementar alertas automáticas.

- Probar failover regularmente.
- Realizar auditorías de reservas.
- Limitar cambios en producción sin validación previa.

Recuerda

El servicio DHCP suele considerarse un componente “transparente” hasta que falla. Sin embargo, en entornos empresariales modernos constituye uno de los servicios más críticos. La combinación de diseño adecuado, seguridad activa, redundancia y monitorización constante es lo que diferencia una red doméstica de una infraestructura profesional robusta.

8. Resumen.

La instalación de servicios de configuración dinámica constituye un elemento esencial en la administración moderna de infraestructuras de red corporativas. La automatización en la asignación de parámetros IP permite garantizar coherencia, reducir errores humanos y optimizar la gestión de entornos con alta densidad de dispositivos. En redes empresariales, donde la movilidad, la virtualización y la segmentación son constantes, el uso del protocolo DHCP resulta imprescindible para asegurar la continuidad operativa.

El direccionamiento IP constituye la base lógica de cualquier arquitectura de red. Una planificación adecuada debe contemplar la segmentación por departamentos, niveles de seguridad, VLAN y zonas diferenciadas (como DMZ o redes de invitados). La estructura jerárquica de red, subred y host permite organizar la infraestructura de forma coherente y escalable. La evolución desde el modelo clásico por clases hacia el uso de CIDR ha permitido optimizar el espacio de direcciones y adaptar los prefijos a necesidades reales, reduciendo desperdicio y mejorando la eficiencia del enrutamiento.

La coexistencia entre IPv4 e IPv6 marca el diseño actual de redes corporativas. Mientras IPv4 continúa siendo predominante por compatibilidad y madurez tecnológica, IPv6 aporta un espacio de direccionamiento prácticamente ilimitado, autoconfiguración nativa y mejoras estructurales en seguridad y movilidad. En la práctica, muchas organizaciones operan en modo dual stack, exigiendo planificación en ámbitos DHCP, reglas de firewall y servicios de resolución de nombres.

El direccionamiento puede asignarse de forma estática o dinámica. El modelo estático aporta estabilidad para servidores y dispositivos críticos, pero incrementa la carga administrativa y el riesgo de errores manuales. El modelo dinámico, gestionado por DHCP, automatiza la entrega de dirección IP, máscara, puerta de enlace y servidores DNS, mejorando la escalabilidad y reduciendo incidencias. En entornos profesionales es habitual emplear reservas DHCP como solución híbrida, combinando estabilidad con gestión centralizada.

El funcionamiento interno del protocolo DHCP se basa en el modelo cliente-servidor y en el proceso DORA (Discover, Offer, Request, Acknowledge), mediante el cual el cliente obtiene su configuración automáticamente. Este proceso utiliza difusión (broadcast) y requiere mecanismos como DHCP Relay en redes segmentadas por VLAN. Además de la dirección IP, DHCP puede distribuir múltiples opciones adicionales: servidores DNS, dominio corporativo, NTP, parámetros de arranque PXE o configuraciones específicas para VoIP, lo que lo convierte en una herramienta de estandarización de configuraciones en toda la organización.

La instalación del servicio puede realizarse tanto en entornos Windows Server como en sistemas GNU/Linux. En Windows, el despliegue se realiza mediante el rol DHCP, con autorización en Active Directory y configuración de ámbitos, exclusiones y reservas desde consola administrativa. En GNU/Linux, la instalación mediante gestor de paquetes y la edición del archivo dhcpd.conf permiten un control granular del servicio, requiriendo verificación de sintaxis y pruebas operativas rigurosas. En ambos casos, la planificación previa del esquema IP es condición indispensable para evitar conflictos o solapamientos.

La gestión profesional del servicio incluye la definición de ámbitos por subred, la delimitación de rangos dinámicos, la creación de reservas para dispositivos críticos y la configuración adecuada del tiempo de concesión (lease). Una mala definición del rango puede provocar agotamiento de direcciones o conflictos que afecten simultáneamente a múltiples usuarios.

Dado su carácter crítico, el servicio DHCP debe contemplar mecanismos de alta disponibilidad. El failover, tanto en entornos Windows como GNU/Linux, permite sincronizar concesiones entre servidores y evitar puntos únicos de fallo. Los modelos activo-activo o activo-pasivo garantizan continuidad ante incidencias, especialmente en redes con gran volumen de dispositivos o fuerte dependencia de conectividad inalámbrica.

Finalmente, la seguridad del servicio resulta prioritaria. DHCP carece de autenticación robusta en su diseño original, lo que lo expone a amenazas como servidores no autorizados (rogue DHCP) o ataques de agotamiento del pool. Por ello, deben implementarse mecanismos complementarios como DHCP Snooping en switches gestionables, control de puertos confiables, limitación de solicitudes por interfaz y monitorización constante de concesiones.

La instalación de servicios de configuración dinámica no se limita a desplegar un software, sino que implica diseñar una arquitectura coherente de direccionamiento, segmentación, seguridad y disponibilidad. Una implementación profesional garantiza escalabilidad, trazabilidad y continuidad operativa en entornos corporativos modernos.

9. Prueba de autoevaluación.

1. ¿Cuál es la función principal del protocolo DHCP en una red corporativa?

a) Traducir nombres de dominio en direcciones IP

b) Asignar automáticamente direcciones IP y otros parámetros de red

c) Filtrar el tráfico entrante según reglas definidas

d) Cifrar las comunicaciones entre cliente y servidor

2. ¿Qué característica diferencia a una dirección IP de una dirección MAC?

a) La IP es física y la MAC es lógica

b) Ambas son siempre estáticas

c) La IP es lógica y puede cambiar según la red

d) La MAC depende del servidor DHCP

3. ¿Cuál es una limitación estructural importante de IPv4?

a) No permite segmentación en subredes

b) No admite máscaras de subred

c) Carece de compatibilidad con routers

d) El espacio de direccionamiento está agotado a nivel global

4. ¿Qué indica el número "/24" en la notación CIDR 192.168.1.0/24?

a) Que existen 24 subredes disponibles

b) Que 24 bits corresponden a la parte de red

c) Que hay 24 dispositivos conectados

d) Que la red es de Clase C obligatoriamente

5. ¿Cuál es una ventaja principal del direccionamiento dinámico frente al estático?

a) Mayor estabilidad de dirección

b) Eliminación de la necesidad de documentación

c) Automatización y reducción de errores humanos

d) Garantiza siempre la misma dirección IP

6. En el proceso DORA del protocolo DHCP, ¿qué mensaje envía el servidor tras recibir un Discover?

a) DHCP Release

b) DHCP Offer

c) DHCP Inform

d) DHCP NAK

7. ¿Cuál es el puerto UDP utilizado por el servidor DHCP?

a) 53

b) 68

c) 443

d) 67

8. ¿Qué tipo de asignación DHCP garantiza siempre la misma dirección IP sin configurar manualmente el cliente?

a) Asignación dinámica

b) Asignación automática

c) Asignación manual mediante reserva

d) Asignación por broadcast

9. ¿Qué requisito es obligatorio antes de instalar el rol DHCP en Windows Server?

a) Configurar el servidor como cliente DHCP

b) Asignar dirección IP estática al servidor

c) Instalar previamente DNS externo

d) Activar NAT en el servidor

10. ¿Cuál es el propósito principal del mecanismo DHCP Snooping?

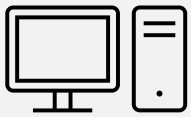
a) Reducir el tiempo de concesión

b) Optimizar el rendimiento del servidor

c) Traducir direcciones privadas a públicas

d) Bloquear servidores DHCP no autorizados en la red

Unidad 2



Instalación de servicios de resolución de nombres

El sistema de resolución de nombres es un componente esencial para el funcionamiento de redes y servicios en Internet. La traducción de nombres de dominio en direcciones IP permite que los usuarios accedan a recursos de manera intuitiva sin necesidad de memorizar direcciones numéricas.

El **DNS (Domain Name System)** constituye la base de esta funcionalidad, organizándose de forma jerárquica y distribuida. Su correcta configuración impacta directamente en la disponibilidad de servicios web, correo electrónico, aplicaciones internas y sistemas corporativos.

En esta unidad se estudian los fundamentos de la arquitectura DNS, los distintos tipos de registros, la instalación y configuración del servicio en entornos Windows y GNU/Linux, así como los mecanismos de seguridad que protegen frente a ataques como la suplantación o la manipulación de respuestas. Se incluye también el análisis de herramientas de diagnóstico y resolución de incidencias.

1. Fundamentos del sistema DNS.

El **Domain Name System (DNS)** es uno de los pilares fundamentales de cualquier infraestructura de red moderna. Su función principal es traducir nombres legibles por humanos en direcciones IP comprensibles por los sistemas de red. Sin DNS, los usuarios deberían acceder a los servicios mediante direcciones numéricas, lo que resultaría inviable en entornos corporativos complejos.

En redes empresariales, el DNS no solo resuelve nombres públicos en Internet, sino que desempeña un papel crítico en:

- Localización de servidores internos.
- Funcionamiento de Active Directory.
- Resolución de aplicaciones corporativas.
- Distribución de servicios.
- Integración con sistemas de correo electrónico.
- Gestión de certificados y seguridad.

El DNS está diseñado como un sistema **distribuido, jerárquico y escalable**, lo que permite su funcionamiento global sin un único punto central de control.

1.1. Jerarquía y estructura.

El sistema DNS se organiza en una estructura jerárquica en forma de árbol invertido. Esta jerarquía permite delegar responsabilidades y distribuir la gestión de nombres de manera eficiente.

En la parte superior se encuentra la raíz del sistema, seguida de los dominios de nivel superior (TLD), los dominios secundarios y los subdominios.

Nivel raíz (Root)

En la parte superior se encuentra el dominio raíz, representado por un punto (.). Aunque normalmente no se escribe explícitamente, toda consulta DNS termina en el dominio raíz.

Los servidores raíz:

- No almacenan todos los dominios del mundo.
- Indican qué servidores gestionan cada dominio de nivel superior.
- Constituyen el primer paso en la resolución recursiva global.

Existen múltiples servidores raíz distribuidos globalmente mediante técnicas de anycast para garantizar alta disponibilidad.

Dominios de nivel superior (TLD)

Por debajo del dominio raíz se encuentran los **Top-Level Domains (TLD)**:

- Genéricos (gTLD): .com, .org, .net
- Geográficos (ccTLD): .es, .fr, .de
- Nuevos TLD: .tech, .cloud, .empresa