

Investigación DHCP

Aldo Francisco Amaro Falcon

Juan Carlos Bermúdez Domínguez

Gregorio Castillo Jr

Sheila Lizeth Flores Acosta

Leonardo Daniel Flores Guerra

Oscar Jare García Mendo

Elías Dominick Gijón Vázquez

Perla Elizabeth Góngora Raga

Instituto Tecnológico de México

Instituto Tecnológico de Reynosa

Proyectos de innovación

Patricia Martínez Vázquez

Temario

1. Funcionamiento de DHCP.
2. Tipos de mensajes DHCP.
3. Proceso de asignación de direcciones IP.
4. Reservas DHCP.
5. Temporizadores DHCP.
6. Problemas comunes en la configuración DHCP.
7. Implementación de DHCP en Ipv6.
8. Seguridad en entornos DHCP.

**Implementación de DHCP ipv6**

## Configurar un Servidor DHCPv6 Stateless

**Paso 1. Habilitar routing IPv6.**

Se requiere el comando **ipv6 unicast-routing** para habilitar el enrutamiento IPv6. Aunque no es necesario que el router sea un servidor DHCPv6 stateless/sin estado, se requiere que el router origine mensajes RA ICMPv6.

R1(config)# ipv6 unicast-routing

R1(config)#

**Paso 2. Definir nombre pool DHCPv6.**

Crea el pool DHCPv6 mediante el comando de configuración global  **ipv6 dhcp pool** POOL-NAME. Esto entra en el modo de subconfiguración del pool DHCPv6 identificado por el mensaje **Router(config-dhcpv6)#**.

**Nota**: El nombre del pool no tiene que estar en mayúsculas. Sin embargo, el uso de un nombre en mayúsculas facilita la visualización en una configuración.

R1(config)# ipv6 dhcp pool IPV6-STATELESS

R1(config-dhcpv6)#

**Paso 3. Configurar pool DHCPv6.**

R1 se configurará para proporcionar información DHCP adicional, incluida la dirección del servidor DNS y el nombre de dominio, como se muestra en el resultado del comando.

R1(config-dhcpv6)# dns-server 2001:db8:acad:1::254

R1(config-dhcpv6)# domain-name example.com

R1(config-dhcpv6)# exit

R1(config)#

**Paso 4. Vincular pool DHCPv6 a una interfaz.**

El pool DHCPv6 debe vincularse a la interfaz mediante el comando de configuración de interfaz **ipv6 dhcp server** POOL-NAME, como se muestra en el ejemplo.

El router responde a las solicitudes de DHCPv6 stateless en esta interfaz con la información incluida en el pool. El flag O debe cambiarse manualmente de 0 a 1 utilizando el comando de interfaz **ipv6 nd other-config-flag**. Los mensajes RA enviados en esta interfaz indican que hay información adicional disponible de un servidor de DHCPv6 stateless. El flag A es 1 de forma predeterminada, indicando a los clientes que usen SLAAC para crear su propio GUA.

R1(config)# interface GigabitEthernet0/0/1

R1(config-if)# description Link to LAN

R1(config-if)# ipv6 address fe80::1 link-local

R1(config-if)# ipv6 address 2001:db8:acad:1::1/64

R1(config-if)# **ipv6 nd other-config-flag**

R1(config-if)# **ipv6 dhcp server IPV6-STATELESS**

R1(config-if)# no shut

R1(config-if)# end

R1#

**Paso 5. Verificar que hosts han recibido información de direcciones IPv6.**

Para comprobar DHCP stateless en un host de Windows, utiliza el comando **ipconfig /all**. El resultado de ejemplo muestra la configuración en PC1.

Observa en el resultado que PC1 creó su GUA IPv6 utilizando el prefijo 2001:db8:acad:1::/64. Observa también que el default gateway es la dirección link-local IPv6 de R1. Esto confirma que PC1 derivó su configuración IPv6 de RA de R1.

El resultado resaltado confirma que PC1 ha aprendido el nombre de dominio y la dirección del servidor DNS del servidor DHCPv6 stateless.

C:\PC1> **ipconfig /all**

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : **example.com**

Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection

Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:1dd:a2ea:66e7 Preferred)

Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21(Preferred)

IPv4 Address. . . . . . . . . . . : 169.254.102.23 (Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.0.0

Default Gateway . . . . . . . . . : fe80::1%6

DHCPv6 IAID . . . . . . . . . . . : 318768538

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A

DNS Servers . . . . . . . . . . . : **2001:db8:acad:1::1**

NetBIOS over Tcpip. . . . . . . . : Enabled

C:\PC1>

## Configurar un Cliente DHCPv6 Stateless

**Paso 1. Habilitar routing IPv6.**

El router del cliente DHCPv6 necesita tener habilitado **ipv6 unicast-routing**.

R3(config)# ipv6 unicast-routing

R3(config)#

**Paso 2. Configurar router cliente para crear LLA.**

El router del cliente necesita tener una dirección local de enlace/link-local. Una dirección link-local IPv6 se crea en la interfaz del router cuando se configura una dirección unicast global. También puede ser creada sin una GUA usando el comando de configuración de interfaz **ipv6 enable**. Cisco IOS utiliza EUI-64 para crear un ID de interfaz aleatorio.

En la salida, el comando **ipv6 enable** se configura en la interfaz Gigabit Ethernet 0/0/1 del router cliente R3.

R3(config)# interface g0/0/1

R3(config-if)# ipv6 enable

R3(config-if)#

**Paso 3. Configurar Router cliente para usar SLAAC.**

El router del cliente necesita ser configurado para usar SLAAC para crear una configuración IPv6. El comando **ipv6 address autoconfig** permite la configuración automática de la dirección IPv6 usando SLAAC.

R3(config-if)# ipv6 address autoconfig

R3(config-if)# end

R3#

**Paso 4. Verificar Router cliente tenga asignado GUA.**

Use el comando **show ipv6 interface brief** para verificar la configuración del host como se muestra. La salida confirma que a la interfaz G0/0/1 de R3 se le asignó un GUA válido.

**Nota**: la interfaz puede tardar unos segundos en completar el proceso.

R3# **show ipv6 interface brief**

GigabitEthernet0/0/0 [up/up]

unassigned

GigabitEthernet0/0/1 [up/up]

FE80::2FC:BAFF:FE94:29B1

2001:DB8:ACAD:1:2FC:BAFF:FE94:29B1

Serial0/1/0 [up/up]

unassigned

Serial0/1/1 [up/up]

unassigned

R3#

**Paso 5. Verificar Router cliente recibió otra información DHCPv6.**

El comando **show ipv6 dhcp interface g0/0/1** confirma que el DNS y los nombres de dominio también fueron aprendidos por R3.

R3# **show ipv6 dhcp interface g0/0/1**

GigabitEthernet0/0/1 is in client mode

Prefix State is IDLE (0)

Information refresh timer expires in 23:56:06

Address State is IDLE

List of known servers:

Reachable via address: FE80::1

DUID: 000300017079B3923640

Preference: 0

Configuration parameters:

**DNS server: 2001:DB8:ACAD:1::254**

**Domain name: example.com**

Information refresh time: 0

Prefix Rapid-Commit: disabled

Address Rapid-Commit: disabled

R3#

## Configurar un Servidor DHCPv6 Stateful

**Paso 1. Habilitar routing IPv6.**

El comando **ipv6 unicast-routing** es necesario para habilitar el enrutamiento IPv6.

R1(config)# ipv6 unicast-routing

R1(config)#

**Paso 2. Definir nombre pool DHCPv6.**

Cree el pool DHCPv6 mediante el comando de configuración global **ipv6 dhcp pool** POOL-NAME.

R1(config)# ipv6 dhcp pool IPV6-STATEFUL

R1(config-dhcpv6)#

**Paso 3. Configurar pool DHCPv6.**

R1 se configurará para proporcionar direccionamiento IPv6, dirección del servidor DNS y nombre de dominio, como se muestra en el resultado del comando. Con DHCPv6 stateful, todos los parámetros de direccionamiento y otros parámetros de configuración deben ser asignados por el servidor de DHCPv6. El comando **address prefix** se utiliza para indicar el conjunto/pool de direcciones que debe asignar el servidor. Otra información proporcionada por el servidor de DHCPv6 stateful suele incluir la dirección del servidor DNS y el nombre de dominio.

**Note**: Este ejemplo está configurando el servidor DNS en el servidor DNS público de Google.

R1(config-dhcpv6)# address prefix 2001:db8:acad:1::/64

R1(config-dhcpv6)# dns-server 2001:4860:4860::8888

R1(config-dhcpv6)# domain-name example.com

R1(config-dhcpv6)#

**Paso 4. Vincular pool DHCPv6 a una interfaz.**

El ejemplo muestra la configuración completa de la interfaz GigabitEthernet 0/0/1 en R1.

El pool de DHCPv6 tiene que estar unido a la interfaz usando el comando de configuración de interfaz **ipv6 dhcp server** POOL-NAME.

* La bandera/flag M se cambia manualmente de 0 a 1 usando el comando de interfaz **ipv6 nd managed-config-flag**.
* La bandera/flag A se cambia manualmente de 1 a 0 usando el comando de interfaz **ipv6 nd prefix default** **no-autoconfig**. La bandera A puede dejarse en 1, pero algunos sistemas operativos clientes como Windows crearán una GUA usando SLAAC y obtendrán una GUA del servidor DHCPv6 stateful/con estado. Colocar la bandera A a 0 le dice al cliente que no use SLAAC para crear una GUA.
* El comando **ipv6 dhcp server** une el pool DHCPv6 a la interfaz. R1 responderá ahora con la información contenida en el pool cuando reciba solicitudes de DHCPv6 stateful/con estado en esta interfaz.

**Nota**: Puede usar el comando **no ipv6 nd managed-config-flag** para devolver la bandera M a su valor predeterminado de 0. El comando **no** **ipv6 nd prefix default no-autoconfig** devuelve la bandera A a su valor predeterminado de 1.

R1(config)# interface GigabitEthernet0/0/1

R1(config-if)# description Link to LAN

R1(config-if)# ipv6 address fe80::1 link-local

R1(config-if)# ipv6 address 2001:db8:acad:1::1/64

R1(config-if)# ipv6 nd managed-config-flag

R1(config-if)# ipv6 nd prefix default no-autoconfig

R1(config-if)# ipv6 dhcp server IPV6-STATEFUL

R1(config-if)# no shut

R1(config-if)# end

R1#

**Paso 5. Verificar que hosts han recibido información de direcciones IPv6.**

Para verificar en un host Windows, usa el comando **ipconfig /all** para verificar el método de configuración de DHCP con estado. La salida muestra la configuración en PC1. La salida resaltada muestra que PC1 ha recibido su GUA IPv6 de un servidor DHCPv6 stateful/con estado.

C:\PC1> **ipconfig /all**

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : example.com

Description . . . . . . . . . . . : IntelI 82574L Gigabit Network Connection

Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1a43c:fd28:9d79:9e42 (Preferred)

Lease Obtained. . . . . . . . . . : Saturday, September 27, 2019, 10:45:30 AM

Lease Expires . . . . . . . . . . : Monday, September 29, 2019 10:05:04 AM

Link-local IPv6 Address . . . . . : fe80::192f:6fbc:9db:b749%6(Preferred)

Autoconfiguration IPv4 Address. . : 169.254.102.73 (Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.0.0

Default Gateway . . . . . . . . . : fe80::1%6

DHCPv6 IAID . . . . . . . . . . . : 318768538

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A

DNS Servers . . . . . . . . . . . : 2001:4860:4860::8888

NetBIOS over Tcpip. . . . . . . . : Enabled

C:\PC1>

## Configurar un Cliente DHCPv6 Stateful

**Paso 1. Habilitar routing IPv6.**

El router cliente DHCPv6 necesita tener habilitado **ipv6 unicast-routing**.

R3(config)# ipv6 unicast-routing

R3(config)#

**Paso 2. Configurar router cliente para crear LLA.**

En la salida, el comando **ipv6 enable** está configurado en la interfaz R3 Gigabit Ethernet 0/0/1. Esto permite al router crear un LLA IPv6 sin necesidad de un GUA.

R3(config)# interface g0/0/1

R3(config-if)# ipv6 enable

R3(config-if)#

**Paso 3. Configurar Router cliente para usar SLAAC.**

El comando **ipv6 address dhcp** configura R3 para solicitar su información de dirección IPv6 de un servidor DHCPv6.

R3(config-if)# ipv6 address dhcp

R3(config-if)# end

R3#

**Paso 4. Verificar Router cliente tenga asignado GUA.**

Usa el comando **show ipv6 interface brief** para verificar la configuración del host como se muestra.

R3# **show ipv6 interface brief**

GigabitEthernet0/0/0 [up/up]

unassigned

GigabitEthernet0/0/1 [up/up]

FE80::2FC:BAFF:FE94:29B1

2001:DB8:ACAD:1:B4CB:25FA:3C9:747C

Serial0/1/0 [up/up]

unassigned

Serial0/1/1 [up/up]

**Paso 5. Verificar Router cliente recibió otra información DHCPv6.**

El comando show **show ipv6 dhcp interface g0/0/1** confirma que el DNS y los nombres de dominio fueron aprendidos por R3.

R3# **show ipv6 dhcp interface g0/0/1**

GigabitEthernet0/0/1 is in client mode

Prefix State is IDLE

Address State is OPEN

Renew for address will be sent in 11:56:33

List of known servers:

Reachable via address: FE80::1

DUID: 000300017079B3923640

Preference: 0

Configuration parameters:

IA NA: IA ID 0x00060001, T1 43200, T2 69120

Address: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C/128

preferred lifetime 86400, valid lifetime 172800

expires at Sep 29 2019 11:52 AM (172593 seconds)

**DNS server: 2001:4860:4860::8888**

**Domain name: example.com**

Information refresh time: 0

Prefix Rapid-Commit: disabled

Address Rapid-Commit: disabled

R3#

## Comandos de Verificación Servidor DHCPv6

El comando **show ipv6 dhcp pool**verifica el nombre del pool de DHCPv6 y sus parámetros. El comando también identifica el número de clientes activos. En este ejemplo, el pool IPV6-STATEFUL tiene actualmente 2 clientes, lo que refleja PC1 y R3 que reciben su dirección de unidifusión global IPv6 de este servidor.

Cuando un router proporciona servicios DHCPv6 stateful, también mantiene una base de datos de direcciones IPv6 asignadas.

R1# **show ipv6 dhcp pool**

DHCPv6 pool: IPV6-STATEFUL

Address allocation prefix: 2001:DB8:ACAD:1::/64 valid 172800 preferred 86400 (2 in use, 0 conflicts)

DNS server: 2001:4860:4860::8888

Domain name: example.com

Active clients: 2

R1#

Utiliza la salida del comand **show ipv6 dhcp binding** para mostrar la dirección link-local IPv6 del cliente y la dirección de unidifusión global asignada por el servidor.

El resultado muestra el enlace con estado actual en R1. El primer cliente en el resultado es PC1 y el segundo cliente es R3.

Esta información la mantiene un servidor de DHCPv6 stateful. Un servidor DHCPv6 stateless no mantendría esta información.

R1# **show ipv6 dhcp binding**

Client: FE80::192F:6FBC:9DB:B749

DUID: 0001000125148183005056B327D6

Username : unassigned

VRF : default

IA NA: IA ID 0x03000C29, T1 43200, T2 69120

Address: 2001:DB8:ACAD:1:A43C:FD28:9D79:9E42

preferred lifetime 86400, valid lifetime 172800

expires at Sep 27 2019 09:10 AM (171192 seconds)

Client: FE80::2FC:BAFF:FE94:29B1

DUID: 0003000100FCBA9429B0

Username : unassigned

VRF : default

IA NA: IA ID 0x00060001, T1 43200, T2 69120

Address: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C

preferred lifetime 86400, valid lifetime 172800

expires at Sep 27 2019 09:29 AM (172339 seconds)

R1#

**Reservas DHCP**

La red incluye servidores, enrutadores, conmutadores, impresoras y otros dispositivos que pueden requerir direcciones IP reservadas (estáticas). Es una buena idea hacer una lista de estos dispositivos, que incluya direcciones de marcador de posición adicionales para que pueda utilizarlas a medida que aumenten sus necesidades. Una reserva DHCP es una dirección IP preestablecida que proporciona el servidor DHCP y que se asigna a una tarjeta de interfaz de red (NIC) cuando esta solicita una dirección IP al servidor DHCP. Tenga en cuenta que un dispositivo debe admitir DHCP para usar reservas.

Puede usar reservas para asignar una dirección IP a un dispositivo cliente específico (NIC) en función de su dirección MAC. El dispositivo siempre recibe la misma dirección IP y la dirección nunca cambia. El dispositivo depende del servidor DHCP después de configurar la reserva. Si el servidor DHCP experimenta problemas y se apaga, el dispositivo de reserva DHCP también deja de estar disponible.

Las reservas ofrecen la posibilidad de cambiar las direcciones IP fácilmente sin tener que iniciar sesión en un dispositivo. También puede administrar direcciones IP para dispositivos de terceros si se establecen en DHCP.

**IMPORTANTE:** La dirección IP tiene que estar dentro del rango DHCP Reservation. Esto se debe a que no se puede establecer una reserva de IP fuera del rango DHCP.

**SUGERENCIA:** El servidor DHCP debe estar habilitado porque si lo deshabilita hará que su router trabaje como un switch, permitiendo a sólo una (1) computadora tener acceso a Internet. En los casos en que el servidor DHCP está desactivado, pero las direcciones IP se asignan todavía, es la traducción de direcciones de red del router (NAT) que traduce estas direcciones que provienen de su módem.

En la reserva DHCP se realiza lo siquiente:

1. Identificación del dispositivo: Primero, se debe identificar el dispositivo para el cual se desea reservar una dirección IP. Esto se hace mediante su dirección MAC (Media Access Control), que es un identificador único para cada dispositivo de red.
2. Configuración de la reserva: En el servidor DHCP, se crea una entrada de reserva que asocia la dirección MAC del dispositivo con una dirección IP específica que se desea asignar de manera permanente. Esto se hace en la configuración del servidor DHCP.
3. Asignación de la dirección IP: Cuando el dispositivo con la dirección MAC específica solicita una dirección IP al servidor DHCP, este servidor le asignará la dirección IP reservada, en lugar de asignar una dirección IP de manera dinámica.

Ventajas de la reserva DHCP

La reserva DHCP es útil para dispositivos que necesitan tener siempre la misma dirección IP, como impresoras de red, servidores, dispositivos de seguridad, cámaras IP, etc. Esto facilita la administración y el acceso a estos dispositivos en una red, ya que su dirección IP es constante y predecible.

Evita conflictos de direcciones

La reserva DHCP también evita conflictos de direcciones IP, ya que garantiza que el dispositivo asociado a la dirección MAC recibirá siempre la misma dirección IP, incluso si otros dispositivos están conectados a la red y solicitan direcciones IP dinámicas.

**Problemas comunes en la configuración DHCP.**

Para que los dispositivos funcionen en una red, es necesario asignarles una dirección IP. Esta asignación puede realizarse manualmente o de manera automática. La automatización de la asignación es controlada a través del Protocolo de Configuración Dinámica de Host (DHCP).

DHCP es un protocolo estándar establecido en el RFC 1541 (que posteriormente fue reemplazado por el RFC 2131). Su función principal es permitir que un servidor distribuya información de configuración y direcciones IP de manera dinámica a los clientes. Por lo general, el servidor DHCP proporciona al cliente al menos la siguiente información esencial:

* Dirección IP
* Máscara de subred
* Puerta de enlace predeterminada
* Otra información, como las direcciones de los servidores DNS (Sistema de Nombres de Dominio) y las direcciones de los servidores WINS (Sistema de Nombres de Internet de Windows). El administrador del sistema configura el servidor DHCP utilizando las opciones que se detallan en el cliente.

**Resolución de problemas en servidores DHCP**

Cuando se trata de resolver problemas en servidores DHCP, es importante verificar los siguientes dispositivos y configuraciones:

1. Asegúrese de que el servicio del servidor DHCP esté iniciado y en ejecución. Puede hacerlo ejecutando el comando 'net start' y buscando el servidor DHCP.
2. Verifique que el servidor DHCP esté autorizado. Consulte la autorización del servidor DHCP de Windows en el escenario donde se encuentra unido a un dominio.
3. Confirme que las concesiones de direcciones IP estén disponibles en el ámbito del servidor DHCP correspondiente a la subred del cliente DHCP. Para esto, consulte las estadísticas del ámbito adecuado en la consola de administración del servidor DHCP.
4. Revise si hay alguna lista de direcciones 'BAD\_ADDRESS' en la sección de concesiones de direcciones.
5. Asegúrese de que los dispositivos de la red no tengan direcciones IP estáticas que no hayan sido excluidas del ámbito DHCP.
6. Verifique que la dirección IP a la que está enlazado el servidor DHCP esté dentro de la subred de los ámbitos desde los cuales deben concederse direcciones IP, en caso de que no haya ningún agente de retransmisión disponible. Esto se puede hacer ejecutando el comando 'Get-DhcpServerv4Binding' o 'Get-DhcpServerv6Binding'.
7. Compruebe que solamente el servidor DHCP esté escuchando en los puertos UDP 67 y 68. Ningún otro proceso ni servicio (como WDS o PXE) debe ocupar estos puertos. Esto se verifica con el comando 'netstat -anb'.
8. Si está trabajando en un entorno configurado con IPsec, verifique que se haya añadido una excepción de IPsec para el servidor DHCP.
9. Confirme que puede hacer ping a la dirección IP del agente de retransmisión desde el servidor DHCP.
10. Enumere y revise los filtros y políticas de DHCP configurados.

**Resolución de problemas en clientes DHCP**

* Cuando se trata de resolver problemas en clientes DHCP, es fundamental verificar los siguientes elementos y configuraciones:
* Asegúrese de que los cables estén conectados y en funcionamiento.
* Compruebe si el filtrado MAC está activado en los conmutadores a los que el cliente está conectado.
* Verifique que el adaptador de red esté habilitado y en funcionamiento.
* Asegúrese de que se haya instalado y actualizado el controlador de adaptador de red correcto.
* Confirme que el servicio del cliente DHCP esté iniciado y en ejecución. Para hacerlo, ejecute el comando 'net start' y busque el cliente DHCP.
* Verifique que no haya un firewall bloqueando los puertos 67 y 68 UDP en el equipo cliente.

**Problemas más comunes y sus resoluciones**

Asignación de direcciones IP incorrectas o no asignación:

Posible causa: Configuración incorrecta del rango de direcciones IP en el servidor DHCP.

Solución: Asegúrate de que el rango de direcciones IP en el servidor DHCP esté configurado correctamente y que haya suficientes direcciones disponibles en el rango.

Conflictos de direcciones IP:

Posible causa: Cuando dos dispositivos en la red tienen la misma dirección IP asignada.

Solución: Configura el servidor DHCP para evitar asignar direcciones duplicadas y verifica que los dispositivos en la red no tengan direcciones IP estáticas duplicadas.

Servidor DHCP no responde:

Posible causa: El servidor DHCP puede estar apagado o mal configurado.

Solución: Asegúrate de que el servidor DHCP esté encendido y funcionando correctamente. Verifica su configuración para asegurarte de que esté distribuyendo direcciones IP correctamente.

Problemas de conectividad de red:

Posible causa: Los dispositivos no pueden comunicarse con el servidor DHCP.

Solución: Asegúrate de que los dispositivos estén conectados correctamente a la red y que el servidor DHCP esté accesible.

Tiempo de arrendamiento (lease time) demasiado corto:

Posible causa: Las direcciones IP asignadas por DHCP caducan rápidamente.

Solución: Aumenta el tiempo de arrendamiento en el servidor DHCP para que las direcciones IP se mantengan válidas durante más tiempo.

Problemas de seguridad:

Posible causa: Acceso no autorizado a la red debido a una configuración de DHCP no segura.

Solución: Implementa medidas de seguridad, como autenticación de clientes DHCP, para evitar que dispositivos no autorizados obtengan direcciones IP de tu servidor DHCP.

Conflictos de subred:

Posible causa: El servidor DHCP y los dispositivos están en subredes diferentes.

Solución: Asegúrate de que el servidor DHCP y los dispositivos estén en la misma subred y que estén configurados correctamente para esa subred.

Problemas de DNS o puerta de enlace:

Posible causa: Configuración incorrecta de servidores DNS o puertas de enlace.

Solución: Verifica la configuración de los servidores DNS y las puertas de enlace en la configuración del servidor DHCP para asegurarte de que sean correctas.

**Seguridad en entornos DHCP**

La seguridad en entornos de DHCP (Protocolo de Configuración Dinámica de Host) es importante para proteger una red contra posibles amenazas y ataques. DHCP es un protocolo utilizado para asignar direcciones IP y otros parámetros de configuración de red de manera automática a dispositivos en una red.

Consideraciones clave para asegurar entornos de DHCP:

* **Filtrado de MAC Address**: Puedes configurar tu servidor DHCP para que solo asigne direcciones IP a dispositivos cuyas direcciones MAC estén autorizadas. Esto limita la capacidad de dispositivos no autorizados para obtener direcciones IP.
* **Asignación de direcciones IP estáticas**: Reserva direcciones IP específicas para dispositivos críticos y asigna estas direcciones de manera estática en lugar de a través de DHCP. Esto garantiza que ciertos dispositivos siempre tengan la misma dirección IP.
* **Tiempo de arrendamiento (lease time) adecuado**: Configura tiempos de arrendamiento cortos para evitar que las direcciones IP queden bloqueadas durante mucho tiempo, lo que podría permitir que dispositivos no autorizados las utilicen.
* **Redundancia del servidor DHCP**: Utiliza múltiples servidores DHCP en la red para garantizar la disponibilidad y la resistencia a fallos.
* **Seguridad de red física**: Asegura físicamente los servidores DHCP para evitar el acceso no autorizado.
* **Segmentación de redes**: Utiliza VLANs y segmentación de redes para limitar el alcance del DHCP a segmentos específicos de la red, lo que reduce el riesgo de que dispositivos no autorizados accedan al servidor DHCP.
* **Autenticación DHCP**: Algunos sistemas de autenticación, como 802.1X, pueden integrarse con DHCP para autenticar dispositivos antes de que se les asigne una dirección IP.
* **Monitoreo y registro**: Supervisa el tráfico DHCP y registra las asignaciones de direcciones IP para detectar cualquier actividad inusual.
* **Actualización y parcheo**: Mantén actualizado el software del servidor DHCP para protegerlo contra vulnerabilidades conocidas.
* **Firewalls y filtrado de tráfico**: Utiliza firewalls y reglas de filtrado de tráfico para controlar qué dispositivos pueden acceder al servidor DHCP y limitar el acceso solo a las direcciones MAC autorizadas.
* **Control de acceso basado en políticas (NAC)**: Implementa soluciones de control de acceso basado en políticas que permitan o denieguen el acceso a la red en función de la conformidad con políticas de seguridad establecidas.
* **Auditorías regulares de seguridad**: Realiza auditorías regulares de seguridad para identificar posibles vulnerabilidades y debilidades en la configuración de DHCP y corregirlas de manera proactiva.

Al seguir estas prácticas de seguridad, puedes ayudar a proteger tu red contra amenazas y ataques en entornos de DHCP y garantizar una operación segura y confiable de tu infraestructura de red.

**Bibliografía**

Cómo configurar la reserva de DHCP con su cuenta de Linksys en la nube. (s. f.). [https://www.linksys.com/bz/support-article/?articleNum=135673#:~:text=La%20DHCP%20Reservation%20(Dynamic%20Host,otros%20dispositivos%20de%20la%20red](https://www.linksys.com/bz/support-article/?articleNum=135673#:~:text=La DHCP Reservation (Dynamic Host,otros dispositivos de la red).

Robinharwood. (2023, 5 octubre). Ámbitos DHCP en Windows Server. Microsoft Learn. <https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-scopes>

Deland-Han. (s/f). Instrucciones para solucionar problemas de DHCP - Windows Server. Microsoft.com. Recuperado el 16 de octubre de 2023, de https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/troubleshoot-dhcp-guidance

Errores de asignación de dirección IP en DHCP (Guía de administración del sistema: servicios IP). (s/f). Oracle.com. Recuperado el 16 de octubre de 2023, de <https://docs.oracle.com/cd/E19957-01/820-2981/dhcp-trouble-35/index.html>

De Luz, S. (2023, 8 septiembre). Qué es el DHCP, funcionamiento y ejemplos de configuración. RedesZone. <https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/#474990-ataques-que-existen-al-dhcp>