TP2:

DHCPV6

[https://learningnetwork.cisco.com/s/article/Analizando-DHCPv6-con-estado-y-sin-estado#:~:text=\*DHCPv6%20con%20estado%20(Solo%20mensajes%20del%20servidor%20DHCPv6)&text=En%20el%20cliente%2C%20la%20direcci%C3%B3n,en%20el%20sistema%20operativo%20Windows](https://learningnetwork.cisco.com/s/article/Analizando-DHCPv6-con-estado-y-sin-estado#:~:text=*DHCPv6%20con%20estado%20(Solo%20mensajes%20del%20servidor%20DHCPv6)&text=En%20el%20cliente%2C%20la%20direcci%C3%B3n,en%20el%20sistema%20operativo%20Windows).

<https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/networksetup/ipv6_dhcp_server_c.html#:~:text=DHCPv6%20es%20un%20m%C3%A9todo%20para,a%20clientes%20que%20se%20conectan>.

El Protocolo de Configuración Dinámica de Hosts para IPv6 (DHCPv6) es un protocolo cliente-servidor, definido en la RFC 3315 de la IETF, que proporciona una configuración administrada de dispositivos sobre IPv6 La especificación inicial de DHCPv6 fue publicada en julio de 2003 como RFC 3315 por el Internet Engineering Task Force (IETF), una organización internacional que desarrolla y promueve estándares de Internet. La principal motivación para crear DHCPv6 fue la necesidad de un mecanismo de configuración automática de red para el protocolo IPv6, que es la versión más reciente del Protocolo de Internet (IP).

¿Por qué fue creado?

Escasez de Direcciones IPv4: El agotamiento de las direcciones IPv4 llevó a la creación de IPv6, que tiene un espacio de direcciones mucho más grande. Con IPv6, se necesitaba un nuevo protocolo de configuración automática para manejar estas nuevas direcciones.

Necesidades de Configuración: Así como con IPv4, los dispositivos en una red IPv6 también necesitan configurarse automáticamente para simplificar la administración de la red, especialmente en redes grandes.

Características Avanzadas de IPv6: IPv6 introdujo nuevas características y mejoras que requerían un protocolo de configuración que pudiera manejar estas nuevas capacidades de manera eficiente.

Asignación Automática de Direcciones: DHCPv6 permite a los dispositivos en una red IPv6 obtener direcciones IP automáticamente sin intervención manual.

Configuración de Parámetros de Red: Además de las direcciones IP, DHCPv6 puede proporcionar a los dispositivos información adicional necesaria para la comunicación en la red, como servidores DNS, dominios de búsqueda, y otros parámetros de configuración de red.

Soporte para Configuraciones Complejas: En redes grandes y complejas, DHCPv6 facilita la gestión centralizada de la configuración de la red, reduciendo el esfuerzo administrativo y minimizando errores.

Compatibilidad con IPv6: Proporciona un método estandarizado y confiable para la configuración de dispositivos en redes IPv6, asegurando una transición más suave desde IPv4.

Aunque [IPv6](https://es.wikipedia.org/wiki/IPv6) resuelve la auto configuración de direcciones, lo cual es la principal motivación de [DHCP](https://es.wikipedia.org/wiki/DHCP) en [IPv4](https://es.wikipedia.org/wiki/IPv4). DHCPv6,le brinda más control al administrador de la red sobre las asignaciones, así como mayor amplitud en la configuración de servicios de red.

DHCPv6 puede trabajar de forma conjunta con el mecanismo “stateless”. El administrador de red determina qué procesos se van a emplear a través de los mensajes “RA” de [ICMPv6](https://es.wikipedia.org/wiki/ICMPv6). También permite a los clientes la solicitud de múltiples [direcciones IPv6](https://es.wikipedia.org/wiki/Direcci%C3%B3n_IPv6), que no era posible en IPv4 ni a través del mecanismo “stateless”.

DHCPv6 funciona sobre el protocolo de transporte UDP. El cliente utiliza una dirección link-local u otra determinada a través de otros mecanismos para transmitir y recibir los mensajes DHCPv6.

Los servidores DHCPv6 reciben mensajes de los clientes utilizando una dirección reservada multicast. Un cliente DHCPv6 transmite la mayoría de los mensajes a la dirección anteriormente mencionada por lo que no es necesario que el cliente sea configurado con dirección unicast del servidor DHCPv6.

Para permitir que un cliente DHCPv6 pueda enviar un mensaje a un servidor DHCPv6 al que no está unido por el mismo enlace deberá haber un agente DHCPv6 de retransmisión que se encargará de transmitir los mensajes entre cliente y servidor en ambos sentidos de la comunicación.

Una vez que el cliente ha determinado la dirección de un servidor, se podrá, bajo algunas circunstancias enviar mensaje directamente al servidor utilizando su dirección unicast.

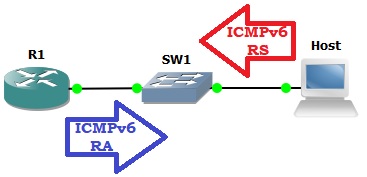
Para solicitar la asignación de una o más direcciones IPv6 así como información de configuración , un cliente primero tiene que localizar al servidor DHCPv6 y luego hacer la petición al servidor para la asignación de dirección y otra información de configuración.

\*Protocolo de configuración dinámica de host para IPv6 (DHCPv6)

(SLAAC: método mediante el cual un host puede obtener una dirección de unidifusión global IPv6 sin los servicios de un servidor DHCPv6)

a) Mensaje de solicitud del router (RS: Router Solicitation); Cuando un cliente se configura para obtener su información de direccionamiento IPv6 automáticamente mediante SLAAC, éste envía un mensaje RS al enrutador. El mensaje RS se envía a la dirección multicast de todos los routers IPv6 FF02::2. Es un mensaje ICMPv6 tipo 133.

b) Mensaje de anuncio del enrutador (RA: Router Advertisement); Los routers envían mensajes RA para proporcionar información de direccionamiento IPv6 a los clientes. El mensaje RA incluye el prefijo y la longitud del prefijo del segmento local. Un enrutador envía un mensaje RA periódicamente (configurable entre 4 y 1800 segundos) o en respuesta a un mensaje RS. Por defecto, los routers Cisco envían mensajes RA cada 200 segundos. Los mensajes RA siempre se envían a la dirección multicast de todos los nodos IPv6 FF02::1. Es un mensaje ICMPv6 tipo 134.



SLAAC no tiene estado, significa que no hay ningún servidor que mantenga la información de la dirección de red, asimismo no se conoce qué direcciones IPv6 se están utilizando o cuáles están disponibles y también otra información como el DNS. Por esto, DHCPv6 es necesario.

Con el protocolo IPv6, un cliente (PC, laptop, celular, etc) puede obtener su dirección IPv6 automáticamente usando SLAAC, solo con un servidor DHCPv6 o una combinación de ambos. Esto dependerá de la configuración que estará presente en el mensaje RA de un enrutador. Para esto tenemos dos banderas: Bandera de configuración de dirección administrada (M flag) y Bandera de otra configuración (O flag) .

Los mensajes RA tienen una de las tres opciones de direccionamiento para el dispositivo IPv6:

\*SLAAC (Solo mensajes RA del enrutador)

\*DHCPv6 sin estado (Mensajes RA y mensajes del servidor DHCPv6)

\*DHCPv6 con estado (Solo mensajes del servidor DHCPv6)

Aunque el mensaje RA define la forma en que el cliente puede obtener una dirección IPv6 de forma dinámica, el sistema operativo del Cliente puede elegir ignorar el mensaje RA y usar solo los servicios de un servidor DHCPv6.

SLAAC es la opción predeterminada en los routers Cisco. Tanto la bandera M como la bandera O están establecidas en "0" en el mensaje RA. En el cliente, la dirección IPv6 unicast global se crea combinando el prefijo brindando en el mensaje RA y una ID de interfaz utilizando EUI-64 o un valor generado aleatoriamente como ocurre en el sistema operativo Windows.

Si ya hubo modificaciones previas de las banderas M y O, podremos restablecer la interfaz específica para operar solo con SLAAC.

DHCPv6 sin estado (DHCP Stateless)

La opción DHCPv6 sin estado informa al cliente que utiliza la información del mensaje RA para la obtención de direccionamiento IPv6, pero los parámetros de configuración adicionales están disponibles desde un servidor DHCPv6. Se le conoce así porque el servidor DHCPv6 no mantiene ninguna información de estado del cliente.

Para el DHCPv6 sin estado, la bandera O se establece en “1” y la bandera M se deja en la configuración predeterminada de “0”. El valor de la bandera O de “1” se utiliza para informar al cliente que hay información de configuración adicional disponible desde un servidor DHCPv6 sin estado.

DHCPv6 con estado (DHCPv6 con estado)

El mensaje RA informa al cliente que no debe usar la información de su mensaje y toda la información de direccionamiento IPv6 y los parámetros de configuración adicionales deben obtenerse de un servidor DHCPv6 con estado. Se define con este nombre porque el servidor DHCPv6 mantiene la información de estado de IPv6.

La bandera M indica si se debe usar o no DHCPv6 con estado. La bandera O no está involucrada y puede ser ignorada.

Ventajas de DHCPv6

Control Centralizado: DHCPv6 permite a los administradores de red tener un control centralizado sobre la asignación de direcciones, lo que facilita la administración y la organización de la red.

Registro y Auditoría: Los servidores DHCPv6 mantienen registros detallados de las asignaciones de direcciones, lo que es útil para la resolución de problemas y auditorías​​.

Compatibilidad con DNS: DHCPv6 puede configurar automáticamente servidores DNS, lo que simplifica la configuración de redes y mejora la accesibilidad mediante nombres de dominio legibles por humanos en lugar de direcciones IP​​.

Asignación de Prefijos: Es posible delegar prefijos completos en lugar de direcciones individuales, lo que es beneficioso para la configuración de subredes más grandes.

Flexibilidad en la Configuración: DHCPv6 permite la transmisión de información de configuración adicional, como servidores NTP y parámetros de VoIP​​.

Desventajas de DHCPv6

Complejidad de Implementación: Configurar DHCPv6 puede ser más complejo en comparación con otras opciones de configuración de IPv6, lo que puede aumentar la carga de mantenimiento.

Dependencia del Servidor: La funcionalidad de la red depende de la disponibilidad y el buen funcionamiento del servidor DHCPv6, lo que introduce un punto único de fallo.

Compatibilidad Limitada: Algunos sistemas operativos, como ciertas versiones de Android, no son compatibles con DHCPv6, lo que puede limitar su adopción en entornos mixtos de dispositivos.

Inmadurez del Protocolo: En algunos casos, DHCPv6 puede ser menos fiable y más inmaduro en su implementación en comparación con las configuraciones más establecidas, como SLAAC.

Vulnerabilidades:

Desbordamiento de búfer en Microsoft DHCPv6 Server (CVE-2023-28231): Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario mediante el envío de mensajes DHCPv6 Relay-forward especialmente diseñados. La explotación exitosa podría permitir la ejecución de código con privilegios elevados​.

Desbordamiento de búfer en el código de análisis de paquetes DHCPv6 (CVE-2022-0324): Un atacante remoto podría explotar esta vulnerabilidad para crear un paquete que cause un desbordamiento de búfer en una llamada memcpy, lo que resultaría en una escritura fuera de los límites de la memoria y potencialmente en la caída del servicio DHCPv6 Relay. Esta vulnerabilidad es crítica y puede causar interrupciones significativas en los servicios de red​

Denegación de servicio en Cisco IOS y IOS XE Software: Una vulnerabilidad en la función de relé y servidor DHCPv6 puede ser explotada para causar una denegación de servicio (DoS). Los dispositivos que no tienen configurado el procesamiento de tráfico IPv6 o una dirección IPv6 no se ven afectados por esta vulnerabilidad. Cisco ha publicado actualizaciones de software para mitigar esta vulnerabilidad​.

Múltiples vulnerabilidades en Junos OS: Estas vulnerabilidades en el procesamiento de paquetes DHCPv6 pueden causar que el proceso jdhcpd se bloquee y se reinicie, lo cual puede ser aprovechado para interrumpir los servicios de red. Juniper ha emitido boletines de seguridad y parches para abordar estas vulnerabilidades​ (Juniper Support Portal)​.

Proceso de Adquisición de Dirección:

Solicitud de Router (Router Solicitation): Un cliente DHCPv6 envía un mensaje de solicitud de router para descubrir los routers en el enlace local.

Anuncio de Router (Router Advertisement): Un router responde con un mensaje de anuncio de router que indica cómo el cliente debe obtener su dirección IP, ya sea mediante DHCPv6 stateful o SLAAC (Stateless Address Autoconfiguration).

Configuración de Puerta de Enlace: Una vez que el cliente recibe el anuncio de router, establece su puerta de enlace predeterminada y puede crear una dirección temporal utilizando SLAAC.

Mensaje de Solicitud DHCPv6 (DHCPv6 Solicit): El cliente envía un mensaje de solicitud DHCPv6 para obtener la información de direccionamiento.

Mensaje de Anuncio DHCPv6 (DHCPv6 Advertise): El servidor DHCPv6 responde con un mensaje de anuncio indicando que está disponible para el servicio.

Mensaje de Petición DHCPv6 (DHCPv6 Request): El cliente envía una petición formal solicitando los parámetros de configuración.

Mensaje de Respuesta DHCPv6 (DHCPv6 Reply): El servidor responde con un mensaje de respuesta que contiene la dirección global unicast y otros detalles de configuración.

Tipos de Configuración DHCPv6:

Stateful DHCPv6: Similar a DHCPv4, asigna direcciones IP específicas a los clientes y mantiene el estado de las asignaciones. Esto requiere que el router envíe anuncios de router con la bandera "M" (Managed) activada.

Stateless DHCPv6: Proporciona solo información adicional, como servidores DNS, sin asignar direcciones IP. Esto se usa típicamente junto con SLAAC, donde las direcciones IP se autoconfiguran y el DHCPv6 proporciona otros detalles de configuración. Aquí, el anuncio de router incluye la bandera "O" (Other) activada.

Configuración del Servidor DHCPv6:

Para configurar un servidor DHCPv6, se crean pools de direcciones y se asignan a interfaces específicas en el router. Dependiendo de si es stateful o stateless, se configuran los flags apropiados en los anuncios de router y se define el pool con las direcciones y otros parámetros necesarios.

RFCs relevantes para DHCPv6

DHCPv6 está definido en varios RFCs que detallan su funcionamiento, mensajes y opciones. Los más importantes son:

RFC 3315: Este es el documento principal que define el protocolo DHCPv6. Publicado en julio de 2003, describe los mecanismos para asignar direcciones IPv6 y otros parámetros de configuración a los dispositivos en una red.

RFC 3633: Define la delegación de prefijos DHCPv6, que permite a los clientes DHCPv6 recibir bloques de direcciones IPv6 más grandes para subredes locales. Publicado en diciembre de 2003.

RFC 3736: Descripción de un modelo de DHCPv6 sin estado (stateless), que proporciona parámetros de configuración sin asignar direcciones IP. Publicado en abril de 2004.

RFC 5007: Introduce las extensiones de reconfiguración para DHCPv6, permitiendo que los servidores actualicen la configuración de los clientes en tiempo real. Publicado en septiembre de 2007.

RFC 8415: Una actualización significativa que reemplaza a RFC 3315, incluyendo nuevas características y mejorando la funcionalidad general del protocolo DHCPv6. Publicado en noviembre de 2018.

Funcionamiento de DHCPv6 según los RFCs

Proceso de Adquisición de Dirección:

Solicitud de Router (Router Solicitation): Un cliente envía un mensaje RS para descubrir routers en el enlace local.

Anuncio de Router (Router Advertisement): Un router responde con un mensaje RA indicando cómo debe el cliente obtener su dirección IP (SLAAC o DHCPv6).

Solicitud DHCPv6 (DHCPv6 Solicit): El cliente envía un mensaje de solicitud para obtener configuración del servidor DHCPv6.

Anuncio DHCPv6 (DHCPv6 Advertise): El servidor responde con un mensaje anunciando su disponibilidad.

Petición DHCPv6 (DHCPv6 Request): El cliente solicita formalmente la configuración.

Respuesta DHCPv6 (DHCPv6 Reply): El servidor responde con la configuración solicitada.

Tipos de Configuración:

Stateful DHCPv6: Asigna direcciones IP y mantiene el estado de las asignaciones.

Stateless DHCPv6: Proporciona solo información adicional, como servidores DNS, sin asignar direcciones IP.

RFC 3315, RFC 3633, RFC 3736, RFC 5007, RFC 8415

Navigating IPv6 Address Configuration​ (This Bridge is the Root)​

Choosing Static, SLAAC or DHCPv6​ (Infoblox Blog)​

ISC DHCP and IPv6 – the DHCPv6 Story​ (ISC)​

IPv6 configuration approaches for servers​ (APNIC Blog)​.

NVD - CVE-2023-28231, NVD - CVE-2022-0324

Cisco Security Advisory, Juniper Security Bulletin

ICTShore, RapidSeedbox, NetworkAcademy

(National Vulnerability Database (NVD))​.

(Zero Day Initiative)​.