Overview (Visión general)

El Dynamic Host Configuration Protocol es utilizado por las computadoras para la solicitud de parámetros de protocolo de Internet , como por ejemplo una dirección IP de un servidor de red . El protocolo opera basado en el modelo cliente- servidor. DHCP es muy común en todas las redes modernas que van desde redes domésticas hasta grandes redes de campus y redes regionales de proveedores de servicios de Internet. La mayoría de los routers de la red de viviendas reciben una dirección IP única a nivel mundial dentro de la red de proveedores. Dentro de una red local, el DHCP le asigna una dirección IP local a los dispositivos conectados a la red local.

Cuando un ordenador u otro dispositivo de red se conecta a una red, el software de cliente DHCP en el sistema operativo envía una consulta broadcast solicitando la información necesaria. Cualquier servidor DHCP en la red puede atender la solicitud . El servidor DHCP gestiona un conjunto de direcciones IP y la información acerca de los parámetros de configuración del cliente (como puerta de enlace predeterminada , el nombre de dominio, los servidores de nombres , y los servidores de tiempo) . Al recibir una petición , el servidor puede responder con información específica para cada cliente, como se ha configurado previamente por un administrador, o con una dirección específica y cualquier otra información válida para toda la red , y el período de tiempo durante el cual la asignación (arrendamiento) es válida . Un host normalmente consulta esta información inmediatamente después del arranque , y después periódicamente antes de la expiración de la información . Cuando una tarea se refresca con el equipo cliente , solicita inicialmente los mismos valores de los parámetros , pero se le puede asignar una nueva dirección desde el servidor, basado en las políticas de asignación establecidos por los administradores.

En redes grandes que constan de múltiples enlaces , un único servidor DHCP puede dar servicio a toda la red , cuando la ayuda de agentes de retransmisión de DHCP ubicadas en los routers de interconexión. Tales agentes transmiten mensajes entre los clientes DHCP y los servidores DHCP ubicados en distintas subredes .

Dependiendo de la aplicación , el servidor DHCP puede tener tres métodos de asignación de direcciones IP :

• Asignación dinámica: Un administrador de red reserva un rango de direcciones IP de DHCP y cada ordenador cliente de la LAN está configurado para solicitar una dirección IP desde el servidor DHCP durante la inicialización de la red . El proceso de peticiones y donación utiliza un concepto de arrendamiento con un período de tiempo controlable , lo que permite que el servidor DHCP para recuperar (y luego reasignar) direcciones IP que no se renuevan .

• Asignación automática : El servidor DHCP asigna permanentemente una dirección IP a un cliente solicitante del rango definido por el administrador. Esto es como la asignación dinámica , pero el servidor de DHCP mantiene una tabla de asignaciones de direcciones IP anteriores , de modo que pueda asignar preferentemente a un cliente de la misma dirección IP que el cliente tenía previamente .

• Asignación estática : El servidor DHCP asigna una dirección IP basándose en una correlación preconfigurado para la dirección MAC de cada cliente. Esta característica se llama indistintamente asignación DHCP estática DD- WRT , dirección fijada por la documentación dhcp, reserva de dirección por Netgear , reserva DHCP o DHCP estático por Cisco y Linksys, y reserva de dirección IP o direcciones MAC / IP vinculante por varios otro router fabricantes .

DHCP se utiliza para Protocolo de Internet versión 4 (IPv4) , así como de IPv6 . Mientras que ambas versiones tienen el mismo propósito , los detalles del protocolo para IPv4 e IPv6 son lo suficientemente diferentes para que puedan ser considerados protocolos separados . Para el funcionamiento de IPv6 , los dispositivos pueden utilizar alternativamente la autoconfiguración de direcciones sin estado . Hosts IPv4 también pueden utilizar - direccionamiento local para lograr un funcionamiento restringido al enlace de la red local.

Historia

DHCP se definió por primera vez como un protocolo de seguimiento de las normas en el RFC 1531 en octubre de 1993, como una extensión del protocolo Bootstrap (BOOTP). La motivación para extender BOOTP era porque BOOTP requería intervención manual para completar la información de configuración en cada cliente, y no proporcionan un mecanismo para la recuperación de las direcciones IP en desuso.

Muchos trabajaron para mejorar el protocolo, ya que ganó popularidad y en 1997 se publicó el RFC 2131, y al 2011 se mantiene como el estándar para redes IPv4. DHCPv6 está documentado en el RFC 3315. El RFC 3633 añadió un mecanismo de delegación de prefijo para DHCPv6. DHCPv6 se amplió aun más para proporcionar información de configuración a los clientes configurados con la configuración automática de direcciones sin estado en el RFC 3736.

El protocolo BOOTP a su vez fue definido por primera vez en el RFC 951 como un reemplazo para el protocolo RARP (del inglés Reverse Address Resolution Protocol), o resolución de direcciones inversa. La principal motivación para la sustitución de RARP con BOOTP fue que RARP era un protocolo de la capa de enlace de datos. Esto hizo más difícil su aplicación en muchas plataformas de servidores, y requería un servidor presente en cada enlace de red individual. BOOTP introdujo la innovación de un agente de retransmisión, lo que permitió el envío de paquetes BOOTP fuera de la red local utilizando enrutamiento IP estándar, por lo que un servidor central de BOOTP podría servir de anfitriones en muchas subredes IP.

Anatomía del protocolo

DHCP Discovery

DHCP Discovery es una solicitud DHCP realizada por un cliente de este protocolo para que el servidor DHCP de dicha red de computadoras le asigne una Dirección IP y otros Parámetros DHCP como la máscara de red o el nombre DNS.2

DHCP Offer

DHCP Offer es el paquete de respuesta del Servidor DHCP a un cliente DHCP ante su petición de la asignación de los Parámetros DHCP. Para ello involucra su dirección MAC (Media Access Control).

DHCP Request

El cliente selecciona la configuración de los paquetes recibidos de *DHCP Offer*. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor

DHCP Acknowledge (Reconocimiento DHCP)

Cuando el servidor DHCP recibe el mensaje DHCPREQUEST del cliente, se inicia la fase final del proceso de configuración. Esta fase implica el reconocimiento DHCPACK el envío de un paquete al cliente. Este paquete incluye el arrendamiento de duración y cualquier otra información de configuración que el cliente pueda tener solicitada. En este punto, la configuración TCP / IP proceso se ha completado. El servidor reconoce la solicitud y la envía acuse de recibo al cliente. El sistema en su conjunto espera que el cliente para configurar su interfaz de red con las opciones suministradas. El servidor DHCP responde a la DHCPREQUEST con un DHCPACK, completando así el ciclo de iniciación. La dirección origen es la dirección IP del servidor de DHCP y la dirección de destino es todavía 255.255.255.255. El campo YIADDR contiene la dirección del cliente, y los campos CHADDR y DHCP: Client Identifier campos son la dirección física de la tarjeta de red en el cliente. La sección de opciones del DHCP identifica el paquete como un ACK.

Client configuration parameters(Parámetros de configuración del cliente)

Un servidor DHCP puede proporcionar parámetros de configuración opcionales para el cliente . RFC 2132 describe las opciones de DHCP disponibles definidos por Internet Assigned Numbers Authority (IANA) - . DHCP y BOOTP parámetros.

Un cliente DHCP puede seleccionar, manipular y sobrescribir los parámetros proporcionados por un servidor DHCP.

DHCP relaying(Retransmisión DHCP)

En redes pequeñas, donde se está manejando solo una subred IP , los clientes DHCP se comunican directamente con los servidores DHCP . Sin embargo , los servidores DHCP también pueden proporcionar direcciones IP de varias subredes . En este caso , un cliente DHCP que aún no ha adquirido una dirección IP no puede comunicarse directamente con el servidor DHCP utilizando el enrutamiento IP , ya que no tiene una dirección IP enrutable , ni saber la dirección IP de un router. Con el fin de permitir a los clientes DHCP en subredes que no estén directamente atendidos por los servidores DHCP para comunicarse con los servidores DHCP , agentes de retransmisión DHCP se pueden instalar en estas subredes . Las difusiones de cliente DHCP en el vínculo local ; el agente de retransmisión recibe la emisión y la transmite a uno o más servidores DHCP usando unicast. El agente de retransmisión almacena su propia dirección IP en el campo GIADDR del paquete DHCP . El servidor DHCP utiliza el GIADDR para determinar la subred en la que el agente de retransmisión recibe la emisión , y asigna una dirección IP en la subred. Cuando el servidor DHCP responde al cliente , envía la respuesta a la dirección de GIADDR , otra vez usando unicast. El agente de retransmisión retransmite la respuesta en la red local .

Security(Seguridad)

El protocolo DHCP base no incluye ningún mecanismo para la autenticación . Debido a esto , es vulnerable a una variedad de ataques . Estos ataques se dividen en tres categorías principales :

• Los servidores DHCP no autorizados que proporcionen información falsa a los clientes.
• Los clientes no autorizados tengan acceso a los recursos.
• ataques de agotamiento de recursos de clientes DHCP maliciosos .
Debido a que el cliente no tiene ninguna forma de validar la identidad de un servidor DHCP , los servidores DHCP no autorizados (comúnmente llamados "DHCP rogue ") pueden funcionar en las redes , proporcionando información incorrecta a los clientes DHCP . Esto puede servir ya sea como una negación - ataque de servicio , evitando que el cliente tenga acceso a la conectividad de red , o como un ataque man-in- the-middle . Debido a que el servidor DHCP proporciona al cliente DHCP con direcciones IP del servidor , como la IP dirección de uno o más servidores DNS , un atacante puede convencer a un cliente DHCP para hacer sus búsquedas de DNS a través de su propio servidor DNS, y por lo tanto puede proporcionar a sus propias respuestas a las consultas de DNS por parte del cliente . Esto a su vez permite el atacante para redirigir el tráfico de red a través de sí mismo, lo que le permite escuchar a escondidas en las conexiones entre el cliente y los servidores de red que entra en contacto , o simplemente para reemplazar los servidores de red con su propia .
Debido a que el servidor DHCP no tiene un mecanismo seguro para la autenticación del cliente , los clientes pueden obtener acceso no autorizado a las direcciones IP por las credenciales que presentan , como identificadores de cliente , que pertenecen a otros clientes DHCP. Esto también permite que los clientes DHCP para agotar el servidor de DHCP tienda de direcciones IP - mediante la presentación de nuevas credenciales cada vez que pregunta por una dirección , el cliente puede consumir todas las direcciones IP disponibles en un enlace de red en particular , la prevención de otros clientes DHCP de conseguir el servicio.
DHCP proporciona algunos mecanismos para mitigar estos problemas. El agente de Información de extensión del protocolo Opción (RFC 3046 , generalmente se hace referencia en la industria por su número real como opción 82) permite a los operadores de red para sujetar etiquetas a los mensajes de DHCP , ya que estos mensajes lleguen a la red de confianza del operador de red . Esta etiqueta se utiliza entonces como una señal de autorización para controlar el acceso del cliente a los recursos de red . Debido a que el cliente no tiene acceso a la red aguas arriba del agente de retransmisión , la falta de autenticación no impedir que el operador del servidor DHCP de confiar en el token de autorización .
Otra de las posibilidades , Autenticación de DHCP Mensajes (RFC 3118) , proporciona un mecanismo para la autenticación de mensajes DHCP . Desafortunadamente RFC 3118 no ha visto (a partir de 2002) la adopción generalizada a causa de los problemas de gestión de claves para un gran número de clientes DHCP. Un libro de 2007 sobre las tecnologías DSL remarcó que " hubo numerosas vulnerabilidades de seguridad identificadas en contra de las medidas de seguridad propuestas por el RFC 3118 . Este hecho, combinado con la introducción de 802.1x, se desaceleró el despliegue y la adopción tasa de DHCP autenticado, y nunca ha sido ampliamente desplegado . " Un libro 2010 señala que" no se han muy pocas implementaciones de autenticación de DHCP . El desafió de los retrasos de gestión y procesamiento de clave debido a hash de cálculo se han considerado un precio demasiado alto a pagar por los beneficios percibidos " .
Más recientes (2008) las propuestas arquitectónicas implican autenticar las peticiones DHCP utilizando 802.1x o PANA (ambos de los cuales el transporte EAP) Una propuesta IETF se hizo para incluir EAP en sí DHCP, el llamado EAP o DHCP ; esto hace no parecen haber progresado más allá de proyecto de nivel IETF , el último de los cuales data de 2010 .

IETF standards documents (IETF documentos estandar)

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions
- RFC 3046, DHCP Relay Agent Information Option
- RFC 3942, Reclassifying Dynamic Host Configuration Protocol Version Four (DHCPv4) Options

- RFC 4242, Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6
- RFC 4361, Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
- RFC 4436, Detecting Network Attachment in IPv4 (DNAv4)