Seguridad de la dirección IP y de cable source-verify

Contenido

[Introducción](#)
[Antes de comenzar](#)
[Convenciones](#)
[Prerequisites](#)
[Componentes Utilizados](#)
[El entorno DOCSIS sin protección](#)
[Base de datos CMTS CPE](#)
[El comando cable source-verify](#)
[Ejemplo 1: escenario con direcciones IP duplicadas](#)
[Ejemplo 2: escenario con dirección IP duplicada – Utilización de una dirección IP que aún no se haya usado.](#)
[Ejemplo 3: uso de un número de red no suministrado por el proveedor de servicio](#)
[Cómo configurar el cable Source-Verify](#)
[Agente Relay](#)
[Conclusión](#)
[Información Relacionada](#)

Introducción

Cisco ha incorporado mejoras en los productos Cisco Cable Modem Termination System (CMTS) que inhiben ciertos tipos de ataques de negación del servicio basados en la simulación de direcciones IP y robo de direcciones IP en los sistemas de cable de Data-over-Cable Service Interface Specifications (DOCSIS). La Referencia de Comandos de Cable de Cisco CMTS describe el conjunto de comandos **cable source-verify** que forman parte de estas mejoras de seguridad de direcciones IP.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Prerequisites

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

El entorno DOCSIS sin protección

Un dominio de Control de acceso de medios (MAC) de DOCSIS es similar en su naturaleza a un segmento Ethernet. Si se deja desprotegido, los usuarios en el segmento son vulnerables a muchos tipos de ataques de Negación de servicio basados en el direccionamiento de Capa 2 y Capa 3. Además, es posible que los usuarios sufran un nivel de servicio degradado debido a la configuración incorrecta de direccionamiento en el equipo de otros usuarios. Los ejemplos de esto incluyen:

- Configuración de direcciones IP duplicadas en nodos diferentes.
- Configuración de direcciones MAC duplicadas en nodos diferentes.
- Uso no autorizado de direcciones IP estáticas en lugar de direcciones IP asignadas por el Protocolo de configuración de host dinámico (DHCP).
- El uso no autorizado de los distintos números de redes dentro de un segmento.
- Una configuración incorrecta de los nodos extremos para responder las peticiones ARP en nombre de la porción del segmento de subred IP.

Mientras estos tipos de problemas son fáciles de controlar y mitigar en un entorno Ethernet LAN por medio de la localización física y la desconexión del equipo ofensivo, tales problemas en redes DOCSIS pueden ser más difíciles de aislar, resolver y prevenir debido al tamaño potencialmente grande de la red. Además, es posible que los usuarios finales que controlan y configuran el Equipo en las instalaciones del cliente (CPE) no cuenten con un equipo local de soporte IS que les asegure que sus estaciones de trabajo y PC no estén mal configuradas, ya sea intencionalmente o no.

Base de datos CMTS CPE

La familia de productos CMTS de Cisco mantiene una base de datos interna que se completa dinámicamente con direcciones MAC e IP del CPE. La base de datos CPE también contiene detalles sobre los módems de cable correspondientes a los que pertenecen estos dispositivos CPE.

Puede obtenerse una vista parcial de la base de datos de CPE correspondiente a un cablemódem particular mediante la ejecución del comando CMTS oculto show interface cable X/Y modem Z. Aquí, X es el número de tarjeta de línea, Y es el número de puerto de flujo descendente y Z es el identificador de servicio (SID) del cable módem. Z puede configurarse en 0 para ver detalles sobre todos los cablemódems y CPE en una interfaz descendente determinada. El siguiente ejemplo muestra una salida típica generada por este comando.

```
CMTS# show interface cable 3/0 modem 0
SID   Priv bits  Type      State     IP address    method    MAC address
1     00         host      unknown   192.168.1.77  static    000C.422c.54d0
1     00         modem     up        10.1.1.30     dhcp      0001.9659.4447
2     00         host      unknown   192.168.1.90  dhcp      00a1.52c9.75ad
2     00         modem     up        10.1.1.44     dhcp      0090.9607.3831
```

Nota: Dado que este comando está oculto, está sujeto a cambios y no está garantizado que esté disponible en todas las versiones del software Cisco IOS®.

En el ejemplo anterior, la columna de método del host con la dirección IP 192.168.1.90 se enumera como dhcp. Esto significa que CMTS se enteró de este host observando las transacciones DHCP entre el host y el servidor DHCP del proveedor de servicios.

El host con dirección IP 192.168.1.77 se lista con método estático. Esto significa que el CMTS no aprendió primero de este host a través de una transacción DHCP entre este dispositivo y un servidor DHCP. En su lugar, el CMTS primero detectó otros tipos de tráfico IP desde este host. Este tráfico pudo haber sido navegador de páginas de internet, correo electrónico o paquetes “ping”.

Mientras puede parecer que 192.168.77 ha sido configurado con una dirección IP estática, puede ser que este host haya adquirido un arrendamiento de DHCP pero el CMTS pudo haber sido reiniciado desde el evento y, por lo tanto, no recuerda la transacción.

La base de datos CPE normalmente está compuesta por información de recolección CMTS sobre las transacciones DHCP entre dispositivos CPE y el servidor DHCP del proveedor del servicio. Además, el CMTS es capaz de escuchar otro tráfico IP proveniente de dispositivos de CPE a fin de determinar qué direcciones MAC e IP de CPE pertenecen a los distintos cablemódems.

El comando cable source-verify

Cisco ha implementado el comando interfaz del cable: cable source-verify [dhcp]. Este comando hace que el CMTS utilice la base de datos de CPE para verificar la validez de los paquetes IP que recibe el CMTS en sus interfaces de cable y permite que el CMTS tome decisiones inteligentes respecto a reenviarlos o no.

El siguiente diagrama de flujo muestra el procesamiento extra que debe atravesar un paquete IP recibido en una interfaz de cable antes de ser admitido a través del CMTS.

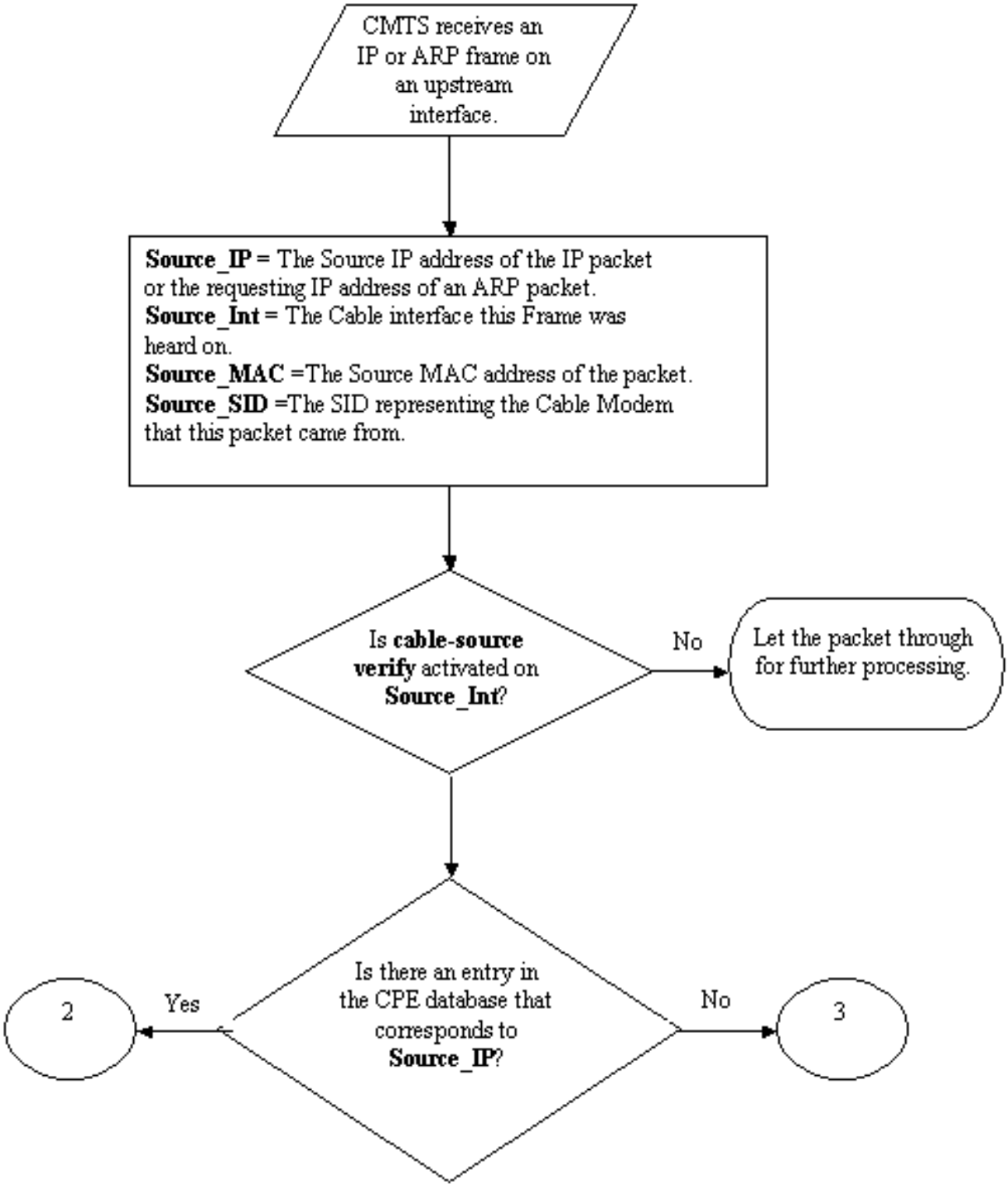

Diagrama de flujo 1

El diagrama de flujo comienza con un paquete recibido por un puerto ascendente en el CMTS y termina con el paquete ya sea habiéndosele permitido continuar para continuar el procesamiento,

o bien habiéndose perdido.

Ejemplo 1: escenario con direcciones IP duplicadas

El primer escenario de Negación de servicio que trataremos es la situación que incluye direcciones IP duplicadas. Digamos que un cliente A está conectado a su proveedor de servicios y obtuvo una licencia DHCP válida para su PC. La dirección IP que ha obtenido el cliente A se conoce como X.

Después de que A adquiere su arrendamiento DHCP, el cliente B decide configurar su PC con una dirección IP estática que es la misma que la que está usando el equipo del cliente A. La información de la base de datos CPE con respecto a la dirección IP X cambiaría dependiendo del dispositivo CPE que envió por última vez una solicitud ARP en nombre de X.

En una red DOCSIS desprotegida, es posible que el cliente B esté en condiciones de convencer al router de saltos (en la mayoría de los casos, el CMTS) que tiene derecho a usar la dirección de IP X, simplemente mediante el envío de una solicitud ARP a nombre de X al CMTS o al router de saltos siguiente. De esta manera, se detendría el reenvío del tráfico del proveedor de servicios al Cliente A.

Al habilitar el cable source-verify, el CMTS podría ver que los paquetes IP y ARP para la dirección IP X se originaban en el cablemódem equivocado y, por lo tanto, estos paquetes se descartarían, consulte Diagrama de flujo 2. Esto incluye todos los paquetes IP con las solicitudes de dirección de origen X y ARP en nombre de X. Los registros CMTS mostrarán un mensaje similar al siguiente:

%UBR7200-3-BADIPSOURCE: Interface Cable3/0, paquete IP de origen no válido. IP=192.168.1.10, MAC=0001.422c.54d0, SID esperado=10, SID real=11

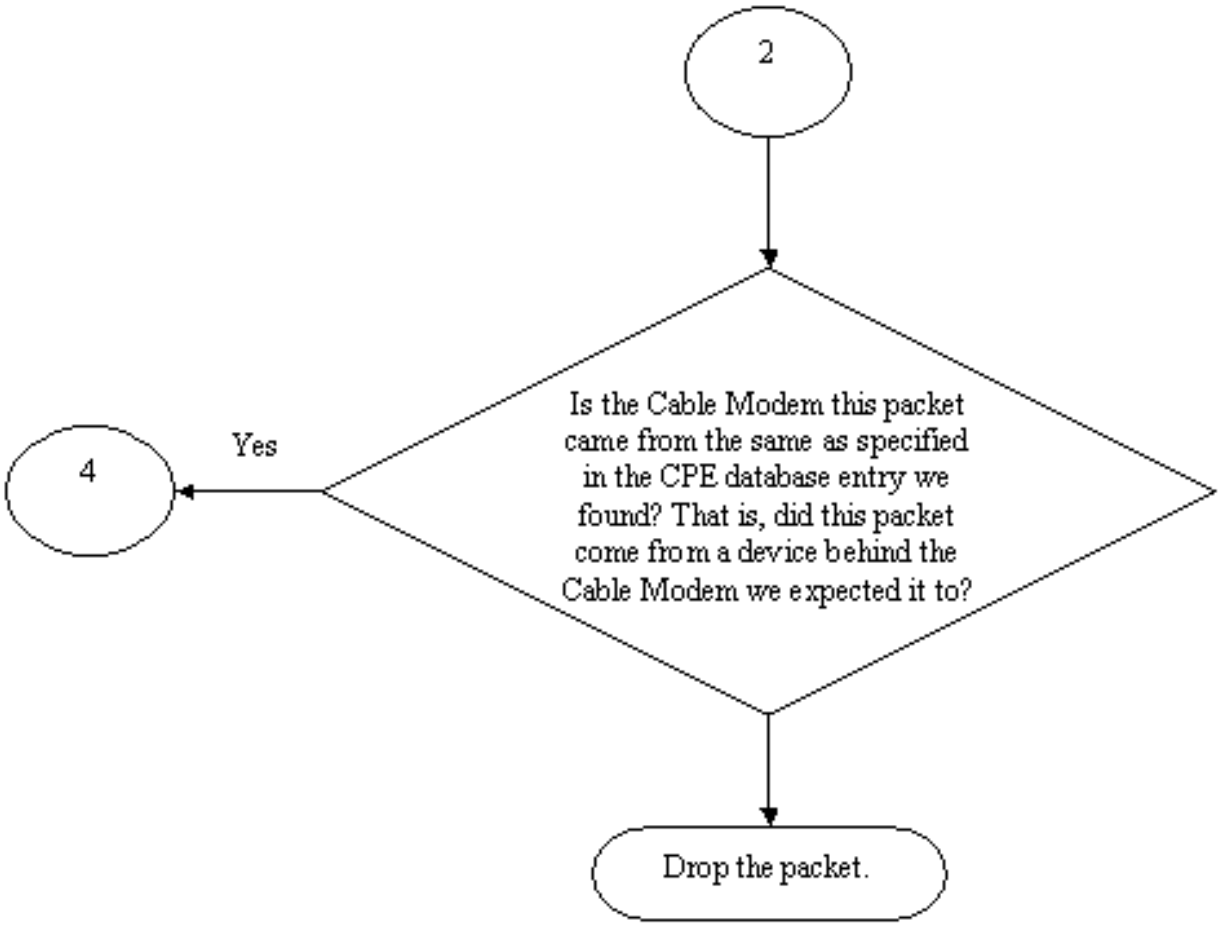

Diagrama de flujo 2

Mediante esta información se identifica a ambos clientes y se puede desactivar el cable módem con la dirección IP duplicada conectada.

Ejemplo 2: escenario con dirección IP duplicada – Utilización de una dirección IP que aún no se haya usado.

Otro escenario es que un usuario asigne estáticamente una dirección IP no utilizada hasta el momento a su PC que se encuentre dentro del rango legítimo de direcciones CPE. Este escenario no causa ninguna interrupción de servicios a nadie en la red. Digamos que el cliente B ha asignado la dirección Y para su PC.

El siguiente problema que puede surgir es que el Cliente C podría conectar su estación de trabajo a la red del proveedor de servicio y adquirir un arrendamiento DHCP para la dirección IP Y. La base de datos CPE marcaría temporalmente la dirección IP Y como perteneciente al cablemódem del cliente C. Sin embargo, puede que no pase mucho antes de que el Cliente B, el usuario no legítimo envía la secuencia adecuada de tráfico ARP para convencer al salto siguiente de que era el propietario legítimo de la dirección IP Y, por lo tanto, causó una interrupción en el servicio del Cliente C.

De manera similar, el segundo problema se puede resolver activando **cable source-verify**. Cuando

el cable de verificación de fuente está encendido, una entrada de base de datos CPE que se ha generado recogiendo detalles de una transacción DHCP no puede ser desplazada por otras clases de tráfico IP. Sólo otra transacción DHCP para esa dirección IP o la entrada ARP en el tiempo de espera CMTS para esa dirección IP puede desplazar la entrada. Esto asegura que si un usuario final adquiere exitosamente un arrendamiento DHCP para una dirección IP dada, ese cliente no tendrá que preocuparse de que el CMTS se confunda y piense que su dirección IP pertenece a otro usuario.

El primer problema de impedir que los usuarios utilicen direcciones IP aún sin utilizar se puede resolver con **cable source-verify dhcp**. Al agregar el parámetro dhcp al final de este comando, el CMTS puede verificar la validez de cada nueva dirección IP de origen de la que escucha emitiendo un tipo especial de mensaje DHCP llamado LEASEQUERY al servidor DHCP. Vea el diagrama de flujo 3.

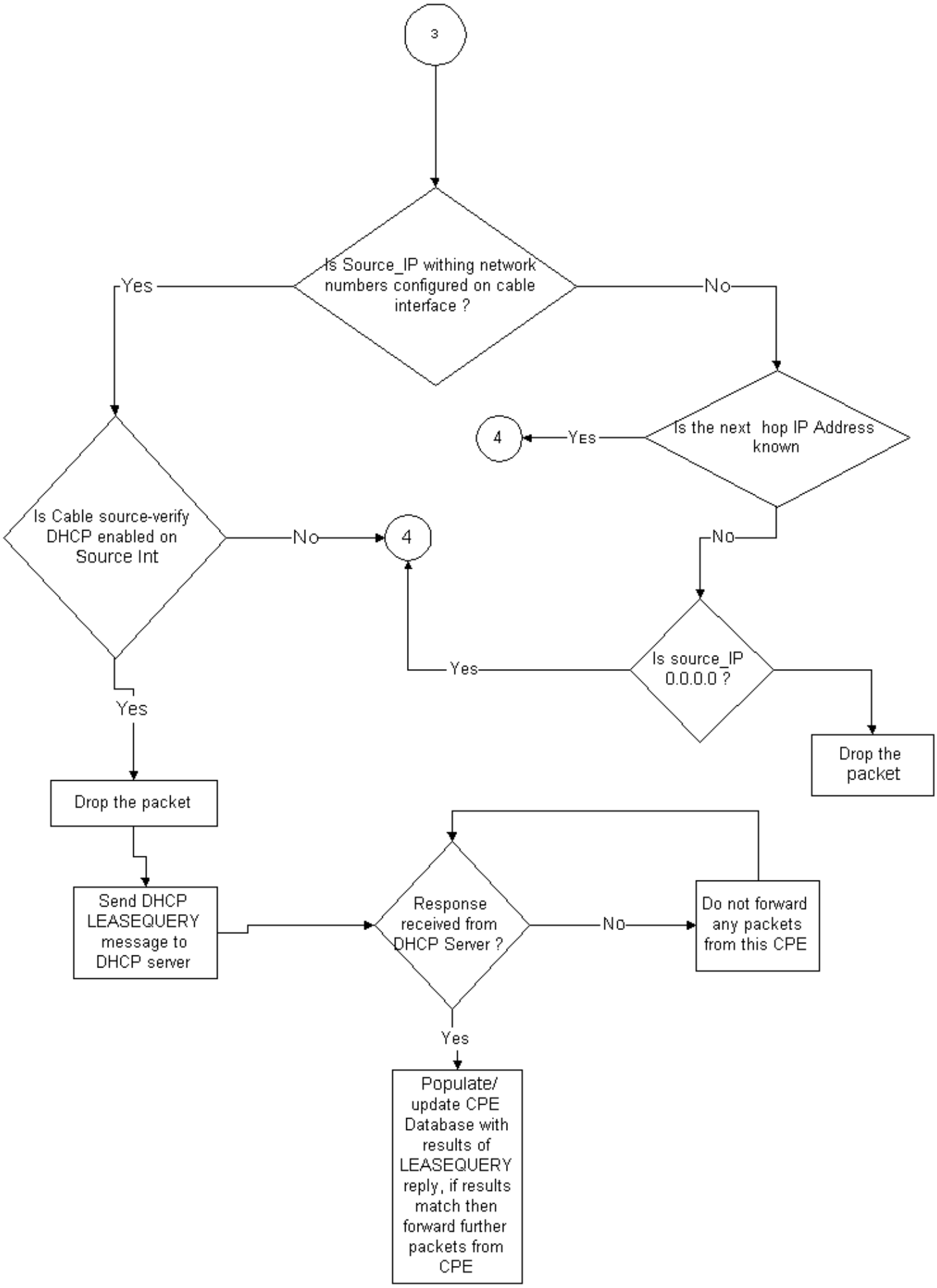

Diagrama de flujo 3

Para una dirección IP de CPE determinada, el mensaje LEASEQUERY consulta cuáles son las direcciones MAC y de Cable Módem correspondientes.

En esta situación, si el cliente B conecta su estación de trabajo a la red de cables con la dirección estática Y, el CMTS enviará una LEASEQUERY (consulta sobre arrendamiento) al servidor DHCP para verificar si la dirección Y ha sido arrendada a la PC del cliente B. El servidor DHCP puede informarle al CMTS que no se ha otorgado ningún arrendamiento a la dirección IP Y y que, por lo tanto, se le denegará el acceso al cliente B.

Ejemplo 3: uso de un número de red no suministrado por el proveedor de servicio

Los usuarios pueden tener estaciones de trabajo configuradas detrás de sus cable módems con direcciones IP estáticas que no pueden entrar en conflicto con ninguno de los números de red actuales del proveedor de servicio, pero pueden ocasionar problemas en un futuro. Por lo tanto, al utilizar el cable de verificación de fuente, un CMTS puede filtrar paquetes que vienen de direcciones IP de origen que no pertenecen al rango configurado en la interfaz del cable CMTS.

Nota: Para que esto funcione correctamente, también necesita configurar el comando **ip verify unicast reverse-path** para evitar direcciones IP de origen simuladas. Consulte Comandos de Cable: cable s para obtener más información.

Algunos clientes pueden tener un router como un dispositivo CPE y acordar que el proveedor del servicio enrute el tráfico a este router. Si el CMTS recibe tráfico IP del router CPE con una dirección IP de origen de Z, entonces cable source-verify dejará pasar este paquete siempre y cuando el CMTS posea una ruta que hacia la red a la que pertenezca Z vía ese dispositivo CPE. Consulte el Diagrama de flujo 3.

Ahora considere el siguiente ejemplo:

Aparece la siguiente configuración en CMTS:

```
interface cable 3/0
 ip verify unicast reverse-path
 ip address 10.1.1.1 255.255.255.0
 ip address 24.1.1.1 255.255.255.0 secondary
 cable source-verify
!
ip route 24.2.2.0 255.255.255.0 24.1.1.2

Note: This configuration shows only what is
relevant for this example
```

Suponiendo que un paquete con la dirección IP de origen 172.16.1.10 llegó al CMTS del cablemódem 24.2.2.10, el CMTS vería que 24.2.2.10 no reside en la base de datos CPE, **show int cable x/y modem 0**, sin embargo **ip verify unicast reverse-path habilita** Unicast Reverse Path Forwarding (RPF unidifusión), que verifica cada paquete recibido en una interfaz para verificar que la dirección IP de origen del paquete aparece en las tablas de ruteo que pertenecen a esa interfaz. El **cable source-verify** verifica para ver cuál es el siguiente salto para 24.2.2.10. En la configuración anterior tenemos una ruta ip 24.2.2.0 255.255.255.0 24.1.1.2 lo que significa que el siguiente salto es 24.1.1.2. Ahora al asumir que 24.1.1.2 es una entrada válida en la base de datos CPE, el CMTS determina que el paquete está bien y entonces lo procesará de acuerdo con el diagrama de flujo 4.

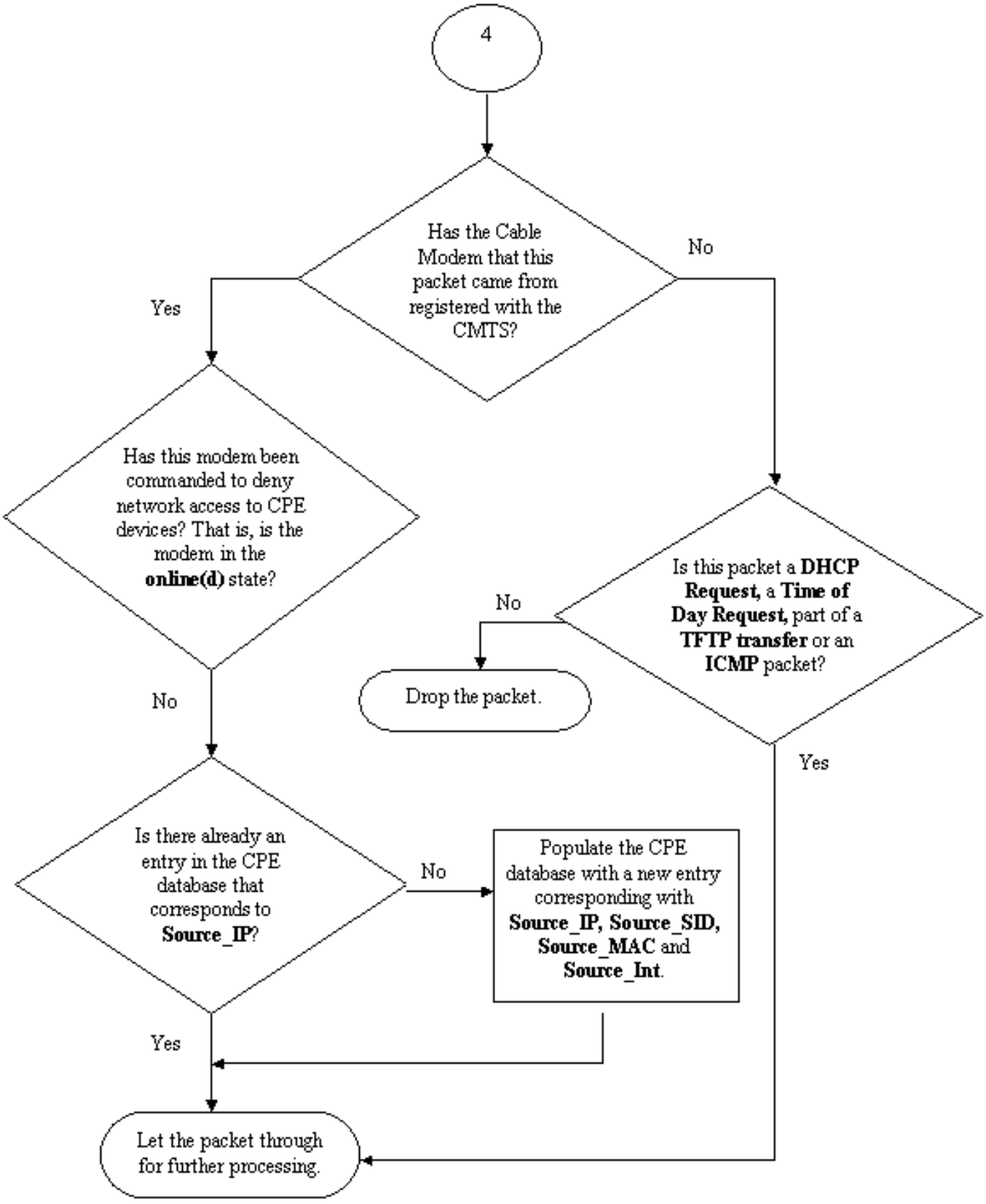

Diagrama de flujo 4

Cómo configurar el cable Source-Verify

La configuración de **cable source-verify** simplemente implica agregar el comando **cable source-verify** a la interfaz de cable en la que desea activar la función. Si está utilizando el agrupamiento de la interfaz de cable, debe agregar **cable source-verify** a la configuración de la interfaz primaria.

Cómo configurar `cable source-verify dhcp`

Nota: cable source-verify se introdujo por primera vez en Cisco IOS Software Release 12.0(7)T y es compatible con Cisco IOS Software Releases 12.0SC, 12.1EC y 12.1T.

La configuración de cable source-verify dhcp requiere algunos pasos.

Asegúrese de que su servidor DHCP admita el mensaje DHCP LEASEQUERY especial.

Para hacer uso de la funcionalidad **cable source-verify dhcp**, su servidor DHCP debe responder a los mensajes según lo especificado por draft-ietf-dhcp-leasequery-XX.txt. Cisco Network Registrar versiones 3.5 y posteriores pueden responder a este mensaje.

Asegúrese de que su servidor DHCP admite el procesamiento de Opción de información del agente de retransmisión . Consulte la **sección Agente Relay****.**

Otra función que su servidor DHCP debe admitir es el procesamiento con Opción de información de relé DHCP. Esto también se conoce como procesamiento de la opción 82. Esta opción se describe en Opción de información de relé DHCP (RFC 3046). Las versión de Cisco Network Registrar 3.5 y posteriores soportan el procesamiento de Opción de información del agente de relevo, sin embargo debe ser activado mediante la utilidad de línea de comandos nrcmd de Cisco Network Registrar con la siguiente secuencia de comandos:

nrcmd -U admin -P changeme -C 127.0.0.1 dhcp enable save-relay-agent-data

nrcmd -U admin -P changeme -C 127.0.0.1 save

nrcmd -U admin -P changeme -C 127.0.0.1 dhcp reload

Es posible que deba sustituir el nombre del usuario, la contraseña y la dirección IP correspondientes del servidor, anteriormente se muestran los valores predeterminados. Alternativamente, si está en la indicación nrcmd, >nrcmd, simplemente escriba lo siguiente:

dhcp enable save-relay-agent-data

guardar

dhcp reload

Active el procesamiento de la opción de información de relé DHCP en el CMTS.

Agente Relay

El CMTS debe etiquetar las solicitudes DHCP de cablemódems y CPE con la Opción de información del agente de retransmisión para que **cable source-verify dhcp** sea efectivo. Los siguientes comandos se deben ingresar en el modo de configuración global en un CMTS que ejecute las versiones 12.1EC, 12.1T o posteriores del IOS de Cisco.

Opción ip dhcp relay information

Si su CMTS ejecuta la versión 12.0SC de software del IOS de Cisco capacite al IOS de Cisco y ejecute el comando cable relay-agent-option cable interface en su lugar.

Tenga cuidado de utilizar los comandos apropiados, dependiendo de la versión de Cisco IOS que esté ejecutando. Asegúrese de actualizar su configuración si cambia los trenes de Cisco IOS.

Los comandos relay information option agregan una opción especial llamada Opción 82, o la opción de información de relé, al paquete DHCP transmitido cuando CMTS transmite paquetes DHCP.

La opción 82 contiene una subopción, la ID del circuito del agente, que hace referencia a la interfaz física en el CMTS en el cual se oyó el pedido de DHCP. Además de esto, otra subopción, el ID remoto del agente, se completa con la dirección MAC de 6 bytes del cable módem del que se recibió o por el que pasó la petición DHCP.

Por ejemplo, si un PC con dirección MAC 99:88:77:66:55:44 que está detrás del cable módem aa:bb:cc:dd:ee:ff envía una solicitud DHCP, el CMTS reenviará la solicitud DHCP configurando la subopción de ID remoto del agente de la opción 82 a la dirección MAC del cable módem, aa:bb:cc:dd:ee:ff.

Al tener la opción de información de relé incluida dentro de la solicitud DHCP de un dispositivo CPE, el servidor DHCP puede almacenar información acerca de cuál CPE debe ubicarse detrás de cuál cablemódem. Es especialmente útil cuando el comando cable source-verify dhcp está configurado en el CMTS, dado que el servidor DHCP puede enviar información en forma confiable al CMTS sobre qué dirección MAC tiene un cliente en particular y a qué cliente de cablemódem debería estar conectado.

Habilitar el comando cable source-verify dhcp bajo la interfaz de cable apropiada.

El paso final es ingresar el comando cable source-verify dhcp en la interfaz del cable en la cual se desea activar la función. Si el CMTS está utilizando el agrupamiento de la interfaz de cable, debe ingresar el comando bajo la interfaz principal del agrupamiento.

Conclusión

El cable source-verify suites de los comandos permite que un proveedor servicio proteja la red del cable contra usuarios con direcciones IP no autorizadas para usar la red.

El comando cable source-verify en sí mismo constituye una forma eficaz y simple de implementar la seguridad de la dirección IP. Si bien no cubre todos los escenarios, al menos garantiza que los clientes que tienen derecho a utilizar direcciones de IP asignadas no detecten ninguna interrupción cuando otras personas utilizan sus direcciones de IP.

En su forma más simple, como se describe en este documento, un dispositivo CPE no configurado a través de DHCP no puede obtener acceso a la red. Esta es la mejor manera de asegurar el espacio de direcciones IP y aumentar la estabilidad y fiabilidad de un servicio de datos sobre cable. Sin embargo, varios operadores de servicio (MSO) que tienen servicios comerciales que les obligaban a utilizar direcciones estáticas querían implementar una seguridad estricta del comando **cable source-verify dhcp**.

Cisco Network Registrar versión 5.5 tiene una nueva capacidad para responder a la consulta de arrendamiento de direcciones "reservadas", aunque la dirección IP no se obtuvo a través de DHCP. El servidor DHCP incluye los datos de reserva de arrendamiento en las respuestas DHCPLEASEQUERY. En las versiones anteriores de Network Registrar, las respuestas DHCPLEASEQUERY eran posibles sólo para clientes alquilados o previamente alquilados para

los cuales se almacenó la dirección MAC. Los agentes de relé uBR de Cisco, por ejemplo, descartan los datagramas DHCPLEASEQUERY que no tienen una dirección MAC y tiempo de concesión (opción dhcp-lease-time).

Network Registrar vuelve al tiempo de validez predeterminado de un año (31536000 segundos) para arriendos reservados en una respuesta DHCPLEASEQUERY. Si la dirección se alquila realmente, Network Registrar devuelve el tiempo de arrendamiento restante.

Información Relacionada

- Opción de información de relé DHCP (RFC 3046)
- Soporte Técnico y Documentación - Cisco Systems