System i

Redes
Protocolo de configuración dinámica de hosts (DHCP)

Versión 6 Release 1

System i

Redes
Protocolo de configuración dinámica de hosts (DHCP)

Versión 6 Release 1

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información que figura en el apartado “Avisos”, en la página 57.

Esta edición atañe a la versión 6, release 1, modificación 0 de IBM i5/OS (producto número 5761-SS1) y a todos los releases y modificaciones ulteriores hasta que se indique lo contrario en nuevas ediciones. Esta versión no se ejecuta en todos los modelos de sistema con conjunto reducido de instrucciones (RISC) ni tampoco se ejecutan en los modelos CISC.

Contenido

Protocolo de configuración dinámica de hosts (DHCP)

El protocolo de configuración dinámica de hosts (DHCP) es un estándar TCP/IP que utiliza un servidor central para gestionar direcciones IP y otros datos de configuración para toda una red.

Un servidor DHCP responde a las peticiones de los clientes, asignándoles propiedades de forma dinámica.

Archivo PDF de DHCP

Puede ver e imprimir un archivo PDF de esta información.

Para ver o descargar la versión PDF de este documento, seleccione DHCP (alrededor de 1399 KB).

Cómo guardar los archivos PDF

Si desea guardar un archivo PDF en su estación de trabajo para verlo o imprimirlo:

1. En el navegador, pulse el enlace del PDF con el botón derecho del ratón.
2. Pulse la opción que guarda el PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el archivo PDF.
4. Pulse **Guardar**.

Cómo descargar Adobe Reader

Para poder ver o imprimir estos archivos PDF, debe instalar Adobe en su sistema. Puede descargar una copia gratuita desde el sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html) .

Referencia relacionada

"Información relacionada con DHCP" en la página 56
Publicaciones IBM Redbooks y sitios Web que contienen información relacionada con el temario DHCP. Puede ver o imprimir cualquiera de los archivos PDF.

Conceptos de DHCP

El protocolo de configuración dinámica de hosts (DHCP) proporciona un método automatizado para la configuración dinámica de clientes. A continuación figuran algunos ejemplos relacionados con DHCP que le permitirán comprender mejor el protocolo DHCP.

Interacción cliente/servidor DHCP

La interacción entre clientes y servidores de protocolo de configuración dinámica de hosts (DHCP) permite que un cliente obtenga su dirección IP y la correspondiente información de configuración de un servidor DHCP.

Este proceso se realiza mediante una serie de pasos, ilustrados en la figura que sigue.

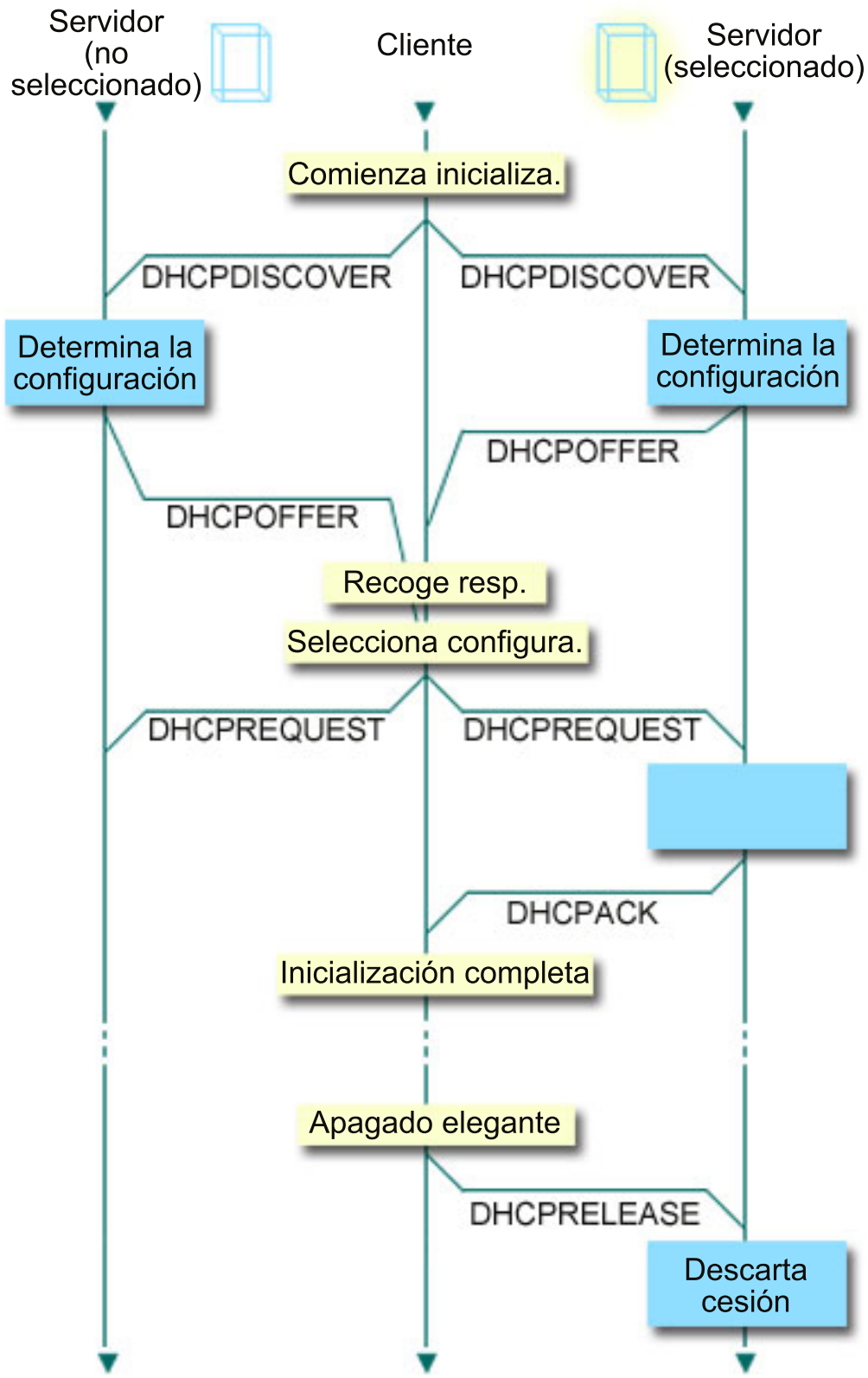


Figura 1. Interacción cliente-servidor DHCP

El cliente solicita información DHCP: DHCPDISCOVER

En primer lugar, el cliente envía un mensaje DHCPDISCOVER que solicita una dirección IP. El mensaje DHCPDISCOVER contiene un identificador exclusivo del cliente (normalmente la

dirección MAC). El mensaje también podría contener otras peticiones, tales como opciones solicitadas (por ejemplo, la máscara de subred, el servidor de nombres de dominio, el nombre de dominio o la ruta estática). El mensaje se envía en forma de difusión. Si la red contiene direccionadores, estos se pueden configurar para que reenvíen paquetes DHCPDISCOVER a los servidores DHCP de las redes conectadas.

El servidor DHCP ofrece información al cliente: DHCPOFFER

Cualquier servidor DHCP que reciba el mensaje DHCPDISCOVER podría enviar un mensaje DHCPOFFER como respuesta. El servidor DHCP podría no enviar un mensaje DHCPOFFER de nuevo al cliente por varios motivos: las causas más habituales son que todas las direcciones disponibles están actualmente cedidas, que la subred no esté configurada o que el cliente no esté soportado. Si el servidor DHCP envía un mensaje DHCPOFFER como respuesta, el DHCPOFFER contendrá una dirección IP disponible y cualquier otra información de configuración que esté definida en la configuración de DHCP.

El cliente acepta la oferta del servidor DHCP: DHCPREQUEST

El cliente recibe mensajes DHCPOFFER de los servidores DHCP que han respondido a los mensajes DHCPDISCOVER. El cliente compara las ofertas con los valores que ha solicitado y luego selecciona el servidor que desea utilizar. Envía un mensaje DHCPREQUEST para aceptar la oferta, e indica qué servidor ha seleccionado. Este mensaje se difunde por toda la red para que todos los servidores DHCP sepan cuál es el servidor que se ha seleccionado.

El servidor DHCP emite un acuse de recibo para el cliente y le cede la dirección IP: DHCPACK

Si un servidor recibe un mensaje DHCPREQUEST, el servidor marca la dirección como cedida. Los servidores que no están seleccionados devolverán las direcciones ofertadas a la agrupación de direcciones disponible. El servidor seleccionado envía al cliente un acuse de recibo (DHCPACK) que contiene información de configuración adicional.

El cliente ahora podría utilizar la dirección IP y los parámetros de configuración. Utilizará estos valores hasta que caduque la cesión o hasta que el cliente envíe un mensaje DHCPRELEASE al servidor para terminar la cesión.

El cliente intenta renovar la cesión: DHCPREQUEST, DHCPACK

El cliente empieza a renovar una cesión cuando ha transcurrido la mitad del tiempo de cesión. El cliente solicita la renovación enviando un mensaje DHCPREQUEST al servidor. Si el servidor acepta la petición, enviará un mensaje DHCPACK al cliente. Si el servidor no responde a la petición, el cliente podría seguir utilizando la dirección IP y la información de configuración hasta que caduque la cesión. Mientras la cesión está todavía activa, no es necesario que el cliente y el servidor pasen por el proceso DHCPDISCOVER y DHCPREQUEST. Cuando haya caducado la cesión, el cliente debe empezar de nuevo con el proceso DHCPDISCOVER.

El cliente finaliza la cesión: DHCPRELEASE

El cliente finaliza la cesión enviando un mensaje DHCPRELEASE al servidor DHCP. Entonces, el servidor devolverá la dirección IP del cliente a la agrupación de direcciones que esté disponible.

Conceptos relacionados

"Agentes de retransmisión y direccionadores" en la página 6
Puede utilizar agentes de retransmisión y direccionadores del protocolo de configuración dinámica de hosts (DHCP) para transferir datos por toda la red de manera eficaz y segura.

"Cesiones" en la página 4
Cuando DHCP envía información de configuración a un cliente, la información se envía con un tiempo de cesión. El tiempo de cesión especifica el tiempo que el cliente puede utilizar la dirección IP que le ha sido asignada. La duración del tiempo de cesión se puede cambiar de acuerdo con los requisitos específicos.

Cesiones

Cuando DHCP envía información de configuración a un cliente, la información se envía con un tiempo de cesión. El tiempo de cesión especifica el tiempo que el cliente puede utilizar la dirección IP que le ha sido asignada. La duración del tiempo de cesión se puede cambiar de acuerdo con los requisitos específicos.

Durante el tiempo de cesión, el servidor DHCP no puede asignar esa dirección IP a ningún otro cliente. El objetivo de una cesión es limitar el tiempo que un cliente puede utilizar una dirección IP. Una cesión impide que los clientes no utilizados ocupen direcciones IP cuando hay más clientes que direcciones. También permite que el administrador realice cambios de configuración en todos los clientes de la red durante un tiempo limitado. Cuando caduca la cesión, el cliente solicitará una nueva cesión a DHCP. Si los datos de configuración han cambiado, los nuevos datos se enviarán al cliente en ese momento.

Renovación de las cesiones

El cliente empieza a renovar una cesión cuando ha transcurrido la mitad del tiempo de cesión. Por ejemplo, en el caso de una cesión de 24 horas, el cliente intentará renovar la cesión al cabo de 12 horas. El cliente solicita la renovación enviando un mensaje DHCPREQUEST al servidor. La petición de renovación contiene la dirección IP actual y la información de configuración del cliente.

Si el servidor acepta la petición, devolverá un mensaje DHCPACK al cliente. Si el servidor no responde a la petición, el cliente puede seguir utilizando la dirección IP y la información de configuración hasta que caduque la cesión. Si la cesión está todavía activa, no es necesario que el cliente y el servidor pasen por el proceso DHCPDISCOVER y DHCPREQUEST. Cuando haya caducado la cesión, el cliente debe empezar de nuevo con el proceso DHCPDISCOVER.

Si el servidor no responde, el cliente puede seguir utilizando la dirección asignada hasta que caduque la cesión. En el ejemplo anterior, el cliente tiene 12 horas desde el momento en que intenta renovar la cesión por primera vez hasta que esta caduca. Durante una interrupción temporal del servicio de 12 horas, los usuarios nuevos no pueden obtener cesiones nuevas, pero no caducarán las cesiones de ninguna máquina que esté encendida en el momento de producirse la interrupción temporal del servicio.

Determinar la duración de la cesión

El tiempo de cesión por omisión del servidor DHCP es de 24 horas. Cuando establezca el tiempo de cesión en el servidor DHCP, considere cuáles son sus objetivos, los patrones de uso del local y los planes de servicio técnico del servidor DHCP. Las siguientes preguntas le ayudarán a determinar el tiempo de cesión pertinente.

¿Tiene más usuarios que direcciones?
Si es así, el tiempo de cesión debe ser corto para que los clientes no tengan que esperar a que caduquen las cesiones no utilizadas.

¿Tiene un tiempo mínimo que deba dar soporte?
Si su usuario típico está conectado durante una hora como mínimo, esto sugiere una cesión de una hora como mínimo.

¿Cuánto tráfico de mensajes de DHCP puede soportar su red?
Si tiene un gran número de clientes o unas líneas de comunicaciones lentas a través de las cuales pasarán los paquetes DHCP, el tráfico de la red podría causar problemas. Cuanto más corta sea la cesión, más intenso será el tráfico de carga del servidor y de la red debido a las peticiones de renovación a través de la red.

¿Qué tipo de plan de servicio técnico tiene establecido y hasta qué punto su red puede hacer frente a una interrupción temporal del servicio?
Considere las tareas de mantenimiento habituales así como el impacto potencial que puede tener una interrupción temporal del servicio. Si el tiempo de cesión es como mínimo dos veces el

tiempo de la interrupción temporal del servicio en el servidor, los clientes en ejecución que ya tengan cesiones no las perderán. Si tiene una idea clara acerca del tiempo máximo que puede durar una interrupción temporal del servicio en su servidor, puede evitar estos problemas.

¿Cuál es el tipo de entorno de red en el que se encuentra el servidor DHCP? ¿Qué suele hacer un cliente típico?

Considere lo que suelen hacer los clientes de la red en la que el servidor DHCP presta servicio. Por ejemplo, si tiene un entorno en el que los clientes son principalmente móviles, se conectan a la red a horas variables y normalmente consultan el correo electrónico una o dos veces al día, es posible que le interese un tiempo de cesión relativamente corto. En este caso, tal vez no sea necesario tener reservada una sola dirección IP para cada cliente. Al limitar el tiempo de cesión, puede utilizar menos direcciones IP para dar soporte a los clientes móviles.

Como alternativa, si tiene un entorno de oficina donde la mayoría de los empleados tienen estaciones de trabajo principales en una ubicación fija, lo más apropiado sería un tiempo de cesión de 24 horas. En este entorno, también podría ser necesario disponer de una dirección IP para cada cliente que se conecte a la red durante las horas de trabajo. En este caso, si especifica un tiempo de cesión más corto, el servidor DHCP negocia la renovación de la cesión con los clientes con mucha más frecuencia, lo que provoca un tráfico excesivo en la red.

¿Con qué frecuencia cambia la configuración de la red?

Si la topología de la red cambia bastante a menudo, quizás sea mejor desestimar las cesiones largas. Las cesiones largas pueden ser desventajosas cuando se tiene que cambiar un parámetro de la configuración. La duración de la cesión puede marcar la diferencia entre tener que ir a cada cliente afectado y reiniciarlo, o simplemente esperar un cierto tiempo a que se renueven las cesiones.

Si la topología de la red cambia muy poco y usted tiene suficientes direcciones IP en la agrupación de direcciones, puede configurar DHCP para que utilice cesiones infinitas; es decir, cesiones que no caducan nunca. Sin embargo, no se recomienda tener cesiones infinitas. Si se utiliza una cesión infinita, la dirección IP se cede al cliente indefinidamente. Estos clientes no deben pasar por ningún proceso de renovación de la cesión después de que hayan recibido la cesión infinita. Después de que se haya asignado una cesión infinita a un cliente, dicha dirección no puede asignarse a otro cliente. Por lo tanto, si desea asignar a ese cliente una nueva dirección IP o ceder más adelante la dirección IP del cliente a otro cliente, pueden producirse problemas.

Podría tener clientes en la red, como por ejemplo un servidor de archivos, que siempre recibirán la misma dirección IP. En lugar de utilizar una cesión infinita, asigne una dirección específica al cliente y déle un tiempo de cesión largo. El cliente todavía tiene la cesión durante un determinado tiempo y debe renovarla, pero el servidor DHCP reserva la dirección IP solo para ese cliente. Más adelante, si obtiene por ejemplo un nuevo servidor de archivos, basta con que cambie el identificador de cliente (dirección MAC) y el servidor DHCP dará esa misma dirección al nuevo servidor de archivos. Si le ha dado una cesión infinita, el servidor DHCP no puede volver a distribuir la dirección, a menos que la cesión se suprima explícitamente.

Conceptos relacionados

"Consideraciones sobre la topología de la red" en la página 43
Al planificar la configuración del protocolo de configuración dinámica de hosts (DHCP), debe tener presentes varios factores, como son la topología de la red, los dispositivos de la red (por ejemplo, los direccionadores) y cómo desea dar soporte a los clientes en DHCP.

Referencia relacionada

"Interacción cliente/servidor DHCP" en la página 1
La interacción entre clientes y servidores de protocolo de configuración dinámica de hosts (DHCP) permite que un cliente obtenga su dirección IP y la correspondiente información de configuración de un servidor DHCP.

Agentes de retransmisión y direccionadores

Puede utilizar agentes de retransmisión y direccionadores del protocolo de configuración dinámica de hosts (DHCP) para transferir datos por toda la red de manera eficaz y segura.

Inicialmente, los clientes DHCP difunden los paquetes DHCPDISCOVER, porque no saben a qué red están conectados. En algunas redes, el servidor DHCP podría no estar en la misma LAN que el cliente. Por lo tanto, hay que reenviar los paquetes DHCP difundidos del cliente a la LAN en la que se encuentra el servidor DHCP. Algunos direccionadores están configurados para reenviar paquetes DHCP. El direccionador, si permite reenviar paquetes DHCP, los reenvía a la LAN en la que se encuentra el servidor DHCP. Sin embargo, muchos direccionadores no permiten reenviar paquetes cuya dirección IP de destino sea la dirección de difusión (paquetes DHCP). En este caso, la LAN debe tener un agente de retransmisión de protocolo Bootstrap (BOOTP) o de protocolo DHCP para reenviar los paquetes DHCP a la LAN que tiene el servidor DHCP. Si desea ver una red de ejemplo que utiliza un agente de retransmisión y un direccionador, consulte: “Ejemplo: DHCP y perfil PPP en distintos modelos de System i” en la página 39.

En cualquiera de los dos casos, dado que el servidor DHCP está en una red distinta, los clientes deben tener la dirección IP del direccionador que conecta la red de los clientes a la red que tiene el servidor DHCP especificado en la opción de direccionador (la opción 3).

En estos casos, si no utiliza el agente de retransmisión BOOTP/DHCP, tendrá que añadir un servidor DHCP a la otra LAN para atender a esos clientes. Para ayudarle a decidir cuántos servidores DHCP debe tener en la red, consulte: “Consideraciones sobre la topología de la red” en la página 43.

Conceptos relacionados

“Consideraciones sobre la topología de la red” en la página 43
Al planificar la configuración del protocolo de configuración dinámica de hosts (DHCP), debe tener presentes varios factores, como son la topología de la red, los dispositivos de la red (por ejemplo, los direccionadores) y cómo desea dar soporte a los clientes en DHCP.

Tareas relacionadas

“Configurar el servidor DHCP y el agente de retransmisión BOOTP/DHCP” en la página 46
Utilice la información que sigue para trabajar con el servidor DHCP y el agente de retransmisión BOOTP/DHCP, haciendo tareas como las de configurar, iniciar o detener el servidor DHCP o el agente de retransmisión BOOTP/DHCP.

Referencia relacionada

“Interacción cliente/servidor DHCP” en la página 1
La interacción entre clientes y servidores de protocolo de configuración dinámica de hosts (DHCP) permite que un cliente obtenga su dirección IP y la correspondiente información de configuración de un servidor DHCP.

Soporte de cliente DHCP

Puede utilizar un servidor DHCP para gestionar individualmente cada cliente de la red, en lugar de gestionar todos los clientes como un grupo de gran tamaño (una subred).

Este método de configuración de DHCP permite que solo los clientes identificados por el servidor DHCP reciban direcciones IP e información de configuración.

A menudo se piensa que DHCP sirve para distribuir direcciones IP de una agrupación de direcciones a una subred de clientes. Cuando utiliza subredes, los clientes que soliciten información DHCP desde la red podrían recibir una dirección IP de la agrupación de direcciones, a menos que el administrador de DHCP los excluya explícitamente. Sin embargo, el servidor DHCP también puede limitar el servicio DHCP a tan solo unos clientes determinados.

El servidor DHCP puede limitar el servicio a nivel de cliente individual o por tipo de cliente (protocolo Bootstrap (BOOTP) o protocolo DHCP).

Para limitar el servicio a nivel de cliente individual, se debe identificar individualmente cada cliente de la red en la configuración de DHCP. Cada cliente se identifica mediante el ID de cliente (que suele ser la dirección MAC). Solamente los clientes que están identificados en la configuración de DHCP recibirán una dirección IP e información de configuración del servidor DHCP. Si un cliente no está incluido en la configuración de DHCP, se le deniega el servicio por parte del servidor DHCP. Este método impide que los hosts desconocidos puedan obtener una dirección IP e información de configuración del servidor DHCP.

Si desea tener todavía más control sobre los clientes de la red y sobre la información de configuración que reciben, puede configurar los clientes DHCP para que reciban una dirección IP estática en lugar de recibir una dirección IP de una agrupación de direcciones. Si configura un cliente para que reciba una dirección IP definida, ese cliente debe ser el único que puede recibir esa dirección IP para evitar el solapamiento de direcciones. Si se utiliza la asignación dinámica de direcciones IP, el servidor DHCP gestionará la asignación de direcciones IP para los clientes.

A un nivel más amplio, el servidor DHCP puede limitar el servicio a un cliente basándose en el tipo de cliente (BOOTP o DHCP). El servidor DHCP puede denegar el servicio a clientes BOOTP.

Conceptos relacionados

"BOOTP"
El protocolo Bootstrap (BOOTP) es un protocolo de configuración de hosts que se utilizó antes de que se desarrollara el protocolo de configuración dinámica de hosts (DHCP). El soporte de BOOTP es un subconjunto de DHCP.

"Consideraciones sobre la topología de la red" en la página 43
Al planificar la configuración del protocolo de configuración dinámica de hosts (DHCP), debe tener presentes varios factores, como son la topología de la red, los dispositivos de la red (por ejemplo, los direccionadores) y cómo desea dar soporte a los clientes en DHCP.

BOOTP

El protocolo Bootstrap (BOOTP) es un protocolo de configuración de hosts que se utilizó antes de que se desarrollara el protocolo de configuración dinámica de hosts (DHCP). El soporte de BOOTP es un subconjunto de DHCP.

En BOOTP, los clientes se identifican mediante las correspondiente direcciones MAC y se les asigna una dirección IP específica. Básicamente, cada cliente de la red está correlacionado con una dirección IP. BOOTP no tiene asignación dinámica de direcciones: cada cliente de la red debe estar identificado en la configuración de BOOTP y los clientes solo pueden recibir una cantidad limitada de información de configuración desde el servidor BOOTP.

Dado que DHCP se basa en BOOTP, el servidor DHCP puede dar soporte a los clientes BOOTP. Si actualmente está utilizando BOOTP, puede configurar y utilizar DHCP sin que ello afecte a los clientes BOOTP. Para dar soporte satisfactorio a los clientes BOOTP, debe especificar la dirección IP del servidor bootstrap y la opción de nombre de archivo de arranque (opción 67), y debe activar el soporte de BOOTP para todo el servidor o para las diversas subredes.

Es preferible utilizar DHCP para dar soporte a los clientes BOOTP que utilizar un servidor BOOTP. Incluso cuando se utiliza DHCP para dar soporte a los clientes BOOTP, cada cliente BOOTP se correlaciona básicamente con una sola dirección IP y, por lo tanto, dicha dirección no la puede reutilizar otro cliente. Sin embargo, la ventaja de utilizar DHCP en este caso es que no es necesario configurar una correlación biunívoca entre clientes BOOTP y direcciones IP. El servidor DHCP seguirá asignando dinámicamente una dirección IP al cliente BOOTP desde la agrupación de direcciones. Después de que la dirección IP se haya asignado al cliente BOOTP, queda reservada de forma permanente para que la utilice

dicho cliente hasta que la reserva de la dirección se suprima explícitamente. Eventualmente, es posible que desee convertir los clientes BOOTP a DHCP para gestionar más fácilmente la configuración de hosts.

Conceptos relacionados

"Soporte de cliente DHCP" en la página 6
Puede utilizar un servidor DHCP para gestionar individualmente cada cliente de la red, en lugar de gestionar todos los clientes como un grupo de gran tamaño (una subred).

BOOTP

"Consideraciones sobre la topología de la red" en la página 43
Al planificar la configuración del protocolo de configuración dinámica de hosts (DHCP), debe tener presentes varios factores, como son la topología de la red, los dispositivos de la red (por ejemplo, los direccionadores) y cómo desea dar soporte a los clientes en DHCP.

Actualizaciones dinámicas

Puede configurar un servidor de protocolo de configuración dinámica de hosts (DHCP) para que funcione con un servidor de tipo sistema de nombres de dominio (DNS) para actualizar dinámicamente la información del cliente en el DNS cuando DHCP asigna una dirección IP al cliente.

El DNS es un sistema de base de datos distribuida para gestionar los nombres de hosts y las direcciones IP asociadas a ellos. Con DNS, los usuarios pueden localizar los hosts utilizando nombres simples (como www.ejemplo.com), en lugar de utilizar la dirección IP (xxx.xxx.xxx.xxx).

En el pasado, todos los datos de DNS se almacenaban en bases de datos estáticas. El administrador tenía que crear y mantener todos los registros de recursos de DNS. Ahora, los servidores DNS que ejecutan BIND 8 pueden configurarse para aceptar peticiones procedentes de otras fuentes para actualizar dinámicamente los datos de zona.

Puede configurar el servidor DHCP para enviar peticiones de actualización al servidor DNS cada vez que DHCP asigne una nueva dirección a un host. Este proceso automatizado reduce la administración del servidor DNS en redes TCP/IP que crecen o cambian rápidamente y en redes donde los hosts cambian a menudo de ubicación. Cuando un cliente que utiliza DHCP recibe una dirección IP, dichos datos se envían inmediatamente al servidor DNS. Gracias a este método, DNS puede seguir resolviendo satisfactoriamente las peticiones de hosts, incluso cuando cambian las direcciones IP.

Se puede configurar DHCP para que actualice los registros de correlación de direcciones (A), los registros de puntero de búsqueda inversa (PTR) o ambos para un cliente. El registro A correlaciona el nombre de DNS del cliente con su dirección IP. El registro PTR correlaciona la dirección IP de un host con su nombre de host. Cuando cambia la dirección de un cliente, DHCP puede enviar automáticamente una actualización al servidor DNS para que los demás hosts de la red puedan localizar el cliente mediante consultas de DNS en su nueva dirección IP. Para cada registro que se actualice dinámicamente, se escribe un registro de texto (TXT) asociado para identificar que el registro lo ha escrito DHCP.

Nota: Si configura DHCP para que actualice solamente los registros PTR, deberá configurar DNS para permitir actualizaciones de clientes de modo que cada cliente pueda actualizar su registro A.

Las zonas dinámicas se protegen creando una lista de fuentes autorizadas que pueden enviar actualizaciones. El DNS verifica que los paquetes de peticiones entrantes proceden de una fuente autorizada antes de actualizar los registros de recursos.

Se pueden realizar actualizaciones dinámicas entre el DNS y DHCP en un solo modelo de System i, en diferentes modelos de System i o en otros sistemas que tengan capacidad para las actualizaciones dinámicas.

Conceptos relacionados

Sistema de nombres de dominio (DNS)

"Consideraciones sobre la topología de la red" en la página 43
Al planificar la configuración del protocolo de configuración dinámica de hosts (DHCP), debe tener presentes varios factores, como son la topología de la red, los dispositivos de la red (por ejemplo, los direccionadores) y cómo desea dar soporte a los clientes en DHCP.

"Problema: DHCP no actualiza los registros de DNS" en la página 54
El servidor DHCP de System i es capaz de actualizar dinámicamente los registros de recursos del DNS. El servidor DHCP utiliza funciones de resolución de nombres e interfaces de programación para determinar el servidor DNS dinámico apropiado que debe actualizarse. Puede utilizar esta información al resolver errores de actualización dinámica.

Tareas relacionadas

"Configurar DHCP para que envíe actualizaciones dinámicas al DNS" en la página 50
Se puede configurar el servidor de protocolo de configuración dinámica de hosts (DHCP) para que envíe peticiones de actualización al servidor DNS cada vez que DHCP asigne una nueva dirección a un host. Este proceso automatizado reduce la administración del servidor DNS en redes TCP/IP que crecen o cambian rápidamente y en redes donde los hosts cambian a menudo de ubicación.

Configurar DNS para que reciba actualizaciones dinámicas

Referencia relacionada

Registros de recursos del sistema de nombres de dominio (DNS)

Búsqueda de opciones de DHCP

El protocolo de configuración dinámica de hosts (DHCP) tiene muchas opciones de configuración que se pueden enviar a los clientes cuando estos solicita información al servidor DHCP. Puede utilizar una herramienta de búsqueda para ver todas las opciones de DHCP.

Las opciones de DHCP definen datos de configuración adicionales que el servidor DHCP pasa a los clientes además de una dirección IP. Las opciones típicas incluyen la máscara de subred, el nombre de dominio, las direcciones IP del direccionador, las direcciones IP del servidor de nombres de dominio y las rutas estáticas.

Las opciones de DHCP estándar, que se basan en las definiciones de la RFC 2132: DHCP Options and BOOTP Vendor Extensions, se describen en la tabla siguiente. También puede configurar las opciones personalizadas utilizando la pantalla Opciones de DHCP, en: System i Navigator.

Tabla 1. Opciones de DHCP estándar

Número de opción	Opción	Descripción
1	Máscara de subred	La opción de máscara de subred especifica la máscara de subred del cliente de acuerdo con la petición de comentarios (RFC) 950. Si en una respuesta de DHCP se especifica la opción de máscara de subred y también la opción de direccionador, la opción de máscara de subred se debe especificar en primer lugar. El código para la opción de máscara de subred es 1 y su longitud es de 4 octetos. **Código Len Máscara subred** 1 | 4 | m1 | m2 | m3 | m4 RZAKG530-0

Tabla 1. Opciones de DHCP estándar (continuación)

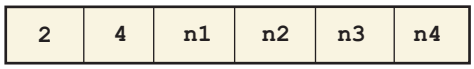
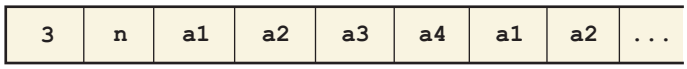
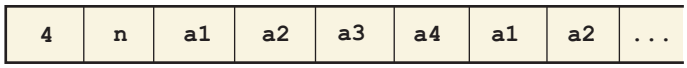
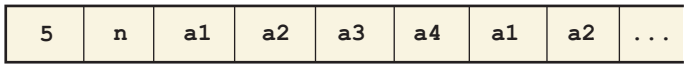
Número de opción	Opción	Descripción
2	Diferencia horaria	El campo de diferencia horaria especifica la diferencia de la subred del cliente en segundos respecto a la Hora Universal Coordinada (UTC). La diferencia se expresa como un entero de 32 bits complemento a dos. Una diferencia positiva indica una ubicación al este del meridiano cero y una diferencia negativa indica una ubicación al oeste del meridiano cero. El código para la opción de diferencia horaria es 2 y su longitud es de 4 octetos. **Código Len Diferencia horaria**  RZAKG531-0
3	Direccionador	La opción de direccionador especifica una lista de direcciones IP para los direccionadores de la subred del cliente. Los direccionadores deben listarse por orden de preferencia. El código para la opción de direccionador es 3. La longitud mínima para la opción de direccionador es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG511-0
4	Servidor de hora	La opción de servidor de hora especifica una lista de servidores de hora de RFC 868 que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor de hora es 4. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG512-0
5	Servidor de nombres	La opción de servidor de nombres especifica una lista de servidores de nombres de IEN 116 que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor de nombres es 5. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG513-0

Tabla 1. Opciones de DHCP estándar (continuación)

Número de opción	Opción	Descripción
6	Servidor de nombres de dominio	La opción de servidor de nombres de dominio especifica una lista de servidores de nombres del Sistema de nombres dominio (STD 13, RFC 1035) que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor de nombres de dominio es 6. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2** 6 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG514-0
7	Servidor de anotaciones	La opción de servidor de anotaciones especifica una lista de servidores de anotaciones de MIT-LCS UDP que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor de anotaciones es 7. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2** 7 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG515-0
8	Servidor de cookies	La opción de servidor de cookies especifica una lista de servidores de cookies de la RFC 865 que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor de cookies es 8. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2** 8 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG516-0
9	Servidor LPR	La opción de servidor LPR especifica una lista de servidores de impresora de líneas de RFC 1179 que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor LPR es 9. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2** 9 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG517-0
10	Servidor Impress	La opción de servidor Impress especifica una lista de servidores Imagen Impress que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor Impress es 10. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2** 10 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG518-0

Tabla 1. Opciones de DHCP estándar (continuación)

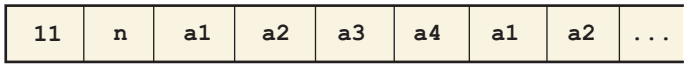
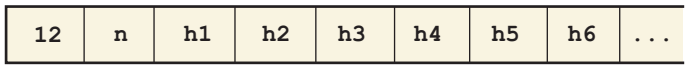
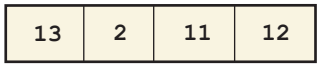
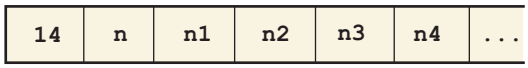
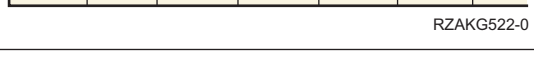
Número de opción	Opción	Descripción
11	Servidor de ubicación de recursos	Esta opción especifica una lista de servidores de ubicación de recursos RFC 887 que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para esta opción es 11. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG519-0
12	Nombre de host	Esta opción especifica el nombre del cliente. El nombre podría estar o no calificado con el nombre de dominio local (vea la sección 3.17 para saber cuál es la manera preferible de recuperar el nombre de dominio). Consulte la RFC 1035 para conocer las restricciones de juego de caracteres. El código para esta opción es 12 y su longitud mínima es 1. **Código Len Nombre de host**  RZAKG520-0
13	Tamaño del archivo de arranque	Esta opción especifica la longitud en bloques de 512 octetos de la imagen del archivo de arranque por omisión para el cliente. La longitud del archivo se especifica como un entero de 16 bits sin signo. El código para esta opción es 13 y su longitud es 2. **Código Len Tamaño de archivo**  RZAKG541-0
14	Archivo de vuelco de méritos	Esta opción especifica el nombre de vía de acceso de un archivo al que debe volcarse la imagen del núcleo del cliente en caso de que el cliente deje de funcionar. La vía de acceso se formatea como una serie de caracteres que está formada por caracteres del juego de caracteres ASCII de NVT. El código para esta opción es 14. Su longitud mínima es 1. **Código Len Nombre de vía de acceso del archivo de vuelco**  RZAKG521-0
15	Nombre de dominio	Esta opción especifica el nombre de dominio que el cliente debe utilizar al resolver nombres de host mediante el sistema de nombres de dominio (DNS). El código para esta opción es 15. Su longitud mínima es 1. **Código Len Nombre de dominio**  RZAKG522-0

Tabla 1. Opciones de DHCP estándar (continuación)

Número de opción	Opción	Descripción
16	Servidor de intercambio	Esta opción especifica la dirección IP del servidor de intercambio del cliente. El código para esta opción es 16 y su longitud es 4. **Código Len Dirección del servidor de intercamio** 16 | n | a1 | a2 | a3 | a4 RZAKG523-0
17	Vía de acceso raíz	Esta opción especifica el nombre de vía de acceso que contiene el disco raíz del cliente. La vía de acceso se formatea como una serie de caracteres que está formada por caracteres del juego de caracteres ASCII de NVT. El código para esta opción es 17. Su longitud mínima es 1. **Código Len Nombre de vía de acceso del disco raíz** 17 | n | n1 | n2 | n3 | n4 | ... RZAKG524-0
18	Vía de acceso de extensiones	Una serie que especifica un archivo, recuperable por medio de TFTP, que contiene información que puede interpretarse de la misma manera que el campo de extensiones de proveedor de 64 octetos dentro de la respuesta de BOOTP, con las siguientes excepciones: • La longitud del archivo no tiene restricciones • Se ignoran todas las referencias al Código 18 (es decir, las instancias del campo Vía de acceso de extensiones de BOOTP) del archivo. El código para esta opción es 18. Su longitud mínima es 1. **Código Len Nombre de vía de acceso de extensiones** 18 | n | n1 | n2 | n3 | n4 | ... RZAKG525-0
19	Reenvío de IP	Esta opción especifica si el cliente debe configurar su capa IP para el reenvío de paquetes. El valor 0 significa inhabilitar el reenvío de IP y el valor 1 significa habilitar el reenvío de IP. El código para esta opción es 19 y su longitud es 1. **Código Len Valor** 19 | 1 | 0/1 RZAKG544-0
20	Direccionamiento de origen no local	Esta opción especifica si el cliente debe configurar su capa IP para permitir el reenvío de datagramas con rutas de origen no locales. El valor 0 significa que no se permite el reenvío de estos datagramas y el valor 1 significa que se permite el reenvío. El código para esta opción es 20 y su longitud es 1. **Código Len Valor** 20 | 1 | 0/1 RZAKG545-0

Tabla 1. Opciones de DHCP estándar (continuación)

Número de opción	Opción	Descripción
21	Filtro de política	Esta opción especifica filtros de política para el direccionamiento de origen no local. Los filtros están formados por una lista de direcciones IP y máscaras que especifican pares de destino/máscara con los que se deben filtrar las rutas de origen entrantes. El cliente debe descartar los datagramas direccionados de origen cuya dirección de salto siguiente no coincide con uno de los filtros. El código para esta opción es 21. La longitud mínima de esta opción es 8 y la longitud debe ser un múltiplo de 8. **Código Len Dirección 1 Máscara 1** 21 | n | a1 | a2 | a3 | a4 | m1 | m2 | m3 | m4 **Dirección 2 Máscara 2** a1 | a2 | a3 | a4 | m1 | m2 | m3 | m4 | ... RZAKG510-0
22	Tamaño máximo de reensamblado de datagrama	Esta opción especifica el datagrama de tamaño máximo que el cliente debe estar preparado para reensamblar. El tamaño se especifica como un entero sin signo de 16 bits. El valor mínimo permitido es 576. El código para esta opción es 22 y su longitud es 2. **Código Len Tamaño** 22 | 2 | s1 | s2 RZAKG542-0
23	Tiempo de vida IP predeterminado	Esta opción especifica el tiempo de vida (TTL) predeterminado que el cliente debe utilizar en los datagramas de salida. El TTL se especifica como un octeto con un valor comprendido entre 1 y 255. El código para esta opción es 23 y su longitud es 1. **Código Len TTL** 23 | 1 | ttl RZAKG546-0
24	Tiempo de espera de maduración de MTU de vía de acceso	Esta opción especifica el tiempo de espera (en segundos) que debe utilizarse durante la maduración de los valores de MTU de vía de acceso descubiertos por el mecanismo definido en la RFC 1191. El tiempo de espera se especifica como un entero sin signo de 32 bits. El código para esta opción es 24 y su longitud es 4. **Código Len Tiempo de espera excedido** 24 | 4 | t1 | t2 | t3 | t4 RZAKG532-0

Tabla 1. Opciones de DHCP estándar (continuación)

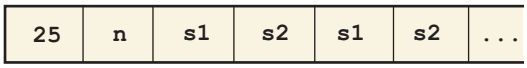
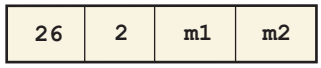
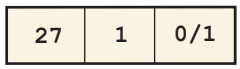
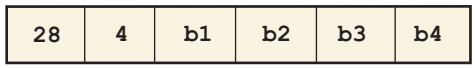
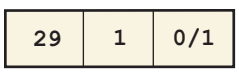
Número de opción	Opción	Descripción
25	Tabla de MTU de vía de acceso	Esta opción especifica una tabla de tamaños de MTU que debe utilizarse al realizar el descubrimiento de MTU de vía de acceso, tal como se define en la RFC 1191. La tabla se formatea como una lista de enteros sin signo de 16 bits, ordenados del más pequeño al más grande. El valor de MTU mínimo no puede ser inferior a 68. El código para esta opción es 25. Su longitud mínima es 2 y la longitud debe ser un múltiplo de 2. **Código Len Tamaño 1 Tamaño 2**  RZAKG526-0
26	MTU de interfaz	Esta opción especifica la MTU que debe utilizarse en esta interfaz. La MTU se especifica como un entero sin signo de 16 bits. El valor mínimo permitido para la MTU es 68. El código para esta opción es 26 y su longitud es 2. **Código Len MTU**  RZAKG543-0
27	Todas las subredes son locales	Esta opción especifica si el cliente puede suponer que todas las subredes de la red IP a la que está conectado el cliente utilizan la misma MTU que la subred de dicha red a la que el cliente está conectado directamente. El valor 1 indica que todas las subredes comparten la misma MTU. El valor 0 significa que el cliente debe suponer que algunas subredes de la red conectada directamente podrían tener MTU más pequeñas. El código para esta opción es 27 y su longitud es 1. **Código Len Valor**  RZAKG547-0
28	Dirección de difusión	Esta opción especifica la dirección de difusión que se utiliza en la subred del cliente. Los valores permitidos para las direcciones de difusión se especifican en la sección 3.2.1.3 de la RFC 2132. El código para esta opción es 28 y su longitud es 4. **Código Len Dirección de difusión**  RZAKG533-0
29	Realizar descubrimiento de máscara	Esta opción especifica si el cliente debe realizar el descubrimiento de máscara de subred utilizando ICMP. El valor 0 indica que el cliente no debe realizar el descubrimiento de máscara. El valor 1 significa que el cliente debe realizar el descubrimiento de máscara. El código para esta opción es 29 y su longitud es 1. **Código Len Valor**  RZAKG548-0

Tabla 1. Opciones de DHCP estándar (continuación)

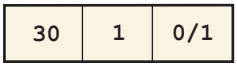
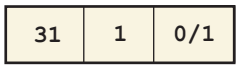
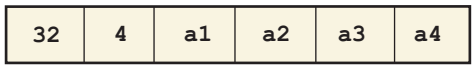
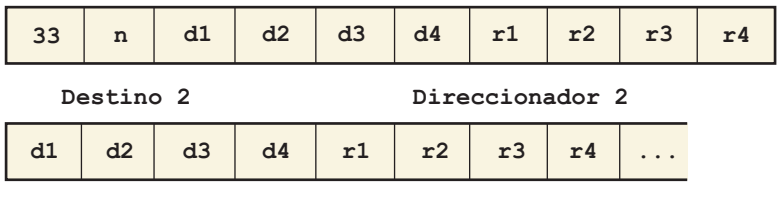
Número de opción	Opción	Descripción
30	Suministrador de máscara	Esta opción especifica si el cliente debe responder a las peticiones de máscara de subred utilizando ICMP. El valor 0 indica que el cliente no debe responder. El valor 1 significa que el cliente debe responder. El código para esta opción es 30 y su longitud es 1. **Código Len Valor**  RZAKG549-0
31	Realizar descubrimiento de direccionador	Esta opción especifica si el cliente debe solicitar direccionadores utilizando el mecanismo de descubrimiento de direccionador definido en la RFC 1256. El valor 0 indica que el cliente no debe realizar el descubrimiento de direccionador. El valor 1 significa que el cliente debe realizar el descubrimiento de direccionador. El código para esta opción es 31 y su longitud es 1. **Código Len Valor**  RZAKG550-0
32	Opción de dirección de solicitud de direccionador	Esta opción especifica la dirección a la que el cliente debe transmitir las peticiones de solicitud de direccionador. El código para esta opción es 32 y su longitud es 4. **Código Len Dirección**  RZAKG534-0
33	Ruta estática	Esta opción especifica una lista de rutas estáticas que el cliente debe instalar en su caché de direccionamiento. Si se especifican múltiples rutas en el mismo destino, las rutas se listan en orden descendente de prioridad. Las rutas constan de una lista de pares de direcciones IP. La primera dirección es la dirección de destino y la segunda dirección es el direccionador para el destino. La ruta por omisión (0.0.0.0) es un destino no permitido para una ruta estática. El código para esta opción es 33. La longitud mínima de esta opción es 8 y la longitud debe ser un múltiplo de 8. **Código Len Destino 1 Direccionador 1**  RZAKG509-0

Tabla 1. Opciones de DHCP estándar (continuación)

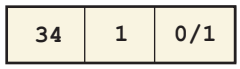
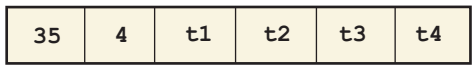
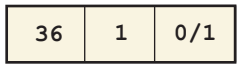
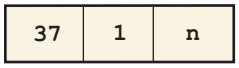
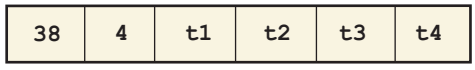
Número de opción	Opción	Descripción
34	Encapsulación de cola	Esta opción especifica si el cliente debe negociar el uso de colas (RFC 893) al utilizar el protocolo ARP. El valor 0 indica que el cliente no debe intentar utilizar colas. El valor 1 significa que el cliente debe intentar utilizar colas. El código para esta opción es 34 y su longitud es 1. **Código Len Valor**  RZAKG573-0
35	Tiempo de espera de caché de ARP	Esta opción especifica el tiempo de espera en segundos para las entradas de caché de ARP. El tiempo se especifica como un entero sin signo de 32 bits. El código para esta opción es 35 y su longitud es 4. **Código Len Tiempo**  RZAKG535-0
36	Encapsulación Ethernet	Esta opción especifica si el cliente debe utilizar la encapsulación de Ethernet Versión 2 (RFC 894) o de IEEE 802.3 (RFC 1042) si la interfaz es una Ethernet. El valor 0 indica que el cliente debe utilizar la encapsulación de RFC 894. El valor 1 significa que el cliente debe utilizar la encapsulación de RFC 1042. El código para esta opción es 36 y su longitud es 1. **Código Len Valor**  RZAKG551-0
37	Tiempo de vida predeterminado de TCP	Esta opción especifica el tiempo de vida (TTL) predeterminado que el cliente debe utilizar al enviar segmentos TCP. El valor se representa como un entero sin signo de 8 bits. El valor mínimo es 1. El código para esta opción es 37 y su longitud es 1. **Código Len TTL**  RZAKG552-0
38	Intervalo de mantener viva la conexión TCP	Esta opción especifica el intervalo (en segundos) que el cliente TCP debe esperar antes de enviar un mensaje de mantener viva la conexión TCP. El tiempo se especifica como un entero sin signo de 32 bits. El valor cero indica que el cliente no debe generar mensajes de mantener vivas las conexiones a menos que lo solicite específicamente una aplicación. El código para esta opción es 38 y su longitud es 4. **Código Len Tiempo**  RZAKG536-0

Tabla 1. Opciones de DHCP estándar (continuación)

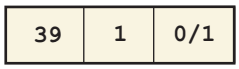
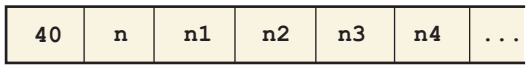
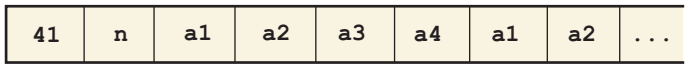
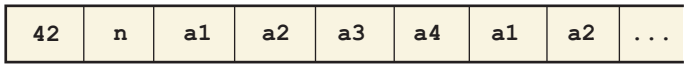
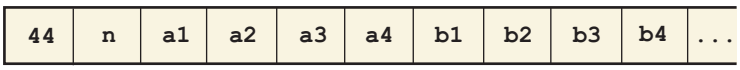
Número de opción	Opción	Descripción
39	Basura de mantener viva la conexión TCP	Esta opción especifica si el cliente debe enviar mensajes de mantener viva la conexión TCP con un octeto de basura por cuestión de compatibilidad con implementaciones más antiguas. El 0 indica que no hay que enviar un octeto de basura. El valor 1 indica que hay que enviar un octeto de basura. El código para esta opción es 39 y su longitud es 1. **Código Len Valor**  RZAKG553-0
40	Dominio de servicio de información de red	Esta opción especifica el nombre del dominio NIS del cliente. El dominio se formatea como una serie de caracteres que está formada por caracteres del juego de caracteres ASCII de NVT. El código para esta opción es 40. Su longitud mínima es 1. **Código Len Nombre de dominio NIS**  RZAKG540-0
41	Servidores de información de red	Esta opción especifica una lista de direcciones IP que indican los servidores NIS que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para esta opción es 41. Su longitud mínima es 4 y la longitud debe ser un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG556-0
42	Opción de servidores de protocolo de hora de red	Esta opción especifica una lista de direcciones IP que indican los servidores NTP que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para esta opción es 42. Su longitud mínima es 4 y la longitud debe ser un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG557-0
44	Servidor de nombres NetBIOS por TCP/IP	La opción de servidor de nombres NetBIOS (NBNS) especifica una lista de servidores de nombres NBNS de RFC 1001/1002 que se muestran por orden de preferencia. El código para esta opción es 44. La longitud mínima de la opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **CódigoLen Dirección 1 Dirección 2**  RZAKG558-0

Tabla 1. Opciones de DHCP estándar (continuación)

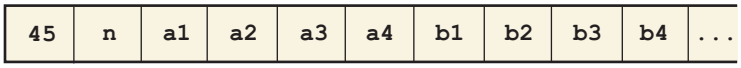
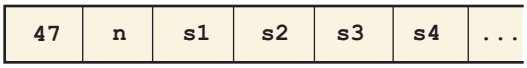
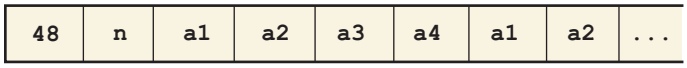
Número de opción	Opción	Descripción
45	Servidor de distribución de datagramas NetBIOS por TCP/IP	La opción de servidor de distribución de datagramas NetBIOS (NBDD) especifica una lista de servidores NBDD de RFC 1001/1002 que se muestran por orden de preferencia. El código para esta opción es 45. La longitud mínima de la opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG559-0
46	Tipo de nodo NetBIOS por TCP/IP	La opción de tipo de nodo NetBIOS permite a los clientes NetBIOS por TCP/IP que son configurables configurarse como se describe en la RFC 1001/1002. El valor se especifica como un solo octeto que identifica el tipo de cliente del siguiente modo: **Valor Tipo de nodo** **0x1 B-nodo** **0x2 P-nodo** **0x4 M-nodo** **0x8 H-nodo** RZAKG554-0 En el diagrama anterior, la notación '0x' indica un número en base 16 (hexadecimal). El código para esta opción es 46. La longitud de esta opción es siempre 1. **Código Len Tipo de nodo**  RZAKG555-0
47	Ámbito NetBIOS por TCP/IP	La opción de ámbito NetBIOS especifica el parámetro de ámbito NetBIOS por TCP/IP para el cliente, tal como se especifica en la RFC 1001/1002. El código para esta opción es 47. La longitud mínima de esta opción es 1. **Código Len Ámbito NetBIOS**  RZAKG528-0
48	Servidor de fonts de sistema X Window	Esta opción especifica una lista de servidores de fonts de sistema X Window que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para esta opción es 48. La longitud mínima de esta opción es de 4 octetos y la longitud debe ser un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG560-0

Tabla 1. Opciones de DHCP estándar (continuación)

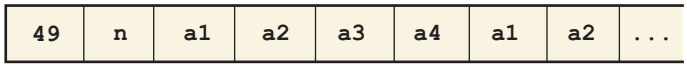
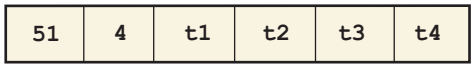
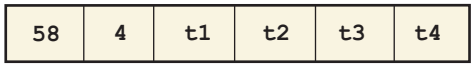
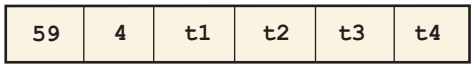
Número de opción	Opción	Descripción
49	X Window System Display Manager	Esta opción especifica una lista de direcciones IP de sistemas que ejecutan X Window System Display Manager y que están disponibles para el cliente. Las direcciones deben listarse por orden de preferencia. El código para esta opción es 49. La longitud mínima de esta opción es 4 y la longitud debe ser un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG561-0
51	Tiempo de cesión de dirección IP	Esta opción se utiliza en una petición de cliente (DHCPDISCOVER o DHCPREQUEST) para permitir que el cliente solicite un tiempo de cesión de la dirección IP. En una respuesta de servidor (DHCPOFFER), un servidor DHCP utiliza esta opción para especificar el tiempo de cesión que está dispuesto a ofrecer. El tiempo es en unidades de segundos y se especifica como un entero sin signo de 32 bits. El código para esta opción es 51 y su longitud es 4. **Código Len Tiempo de cesión**  RZAKG537-0
58	Valor de tiempo de renovación (T1)	Esta opción especifica el intervalo de tiempo desde la asignación de direcciones hasta que el cliente realiza la transición al estado de renovación (RENEWING). El valor es en unidades de segundos y se especifica como un entero sin signo de 32 bits. El código para esta opción es 58 y su longitud es 4. **Código Len Intervalo T1**  RZAKG538-0
59	Valor de tiempo de reenlace (T2)	Esta opción especifica el intervalo de tiempo desde la asignación de direcciones hasta que el cliente realiza la transición al estado de reenlace (REBINDING). El valor es en unidades de segundos y se especifica como un entero sin signo de 32 bits. El código para esta opción es 59 y su longitud es 4. **Código Len Intervalo T2**  RZAKG539-0
62	Nombre de dominio NetWare/IP	Especifica el nombre de dominio Netware/IP.
63	NetWare/IP	Especifica las subopciones de NetWare que usted desea. El rango está comprendido entre 1 y 255. Utilice la opción 62 para especificar el nombre de dominio NetWare/IP.

Tabla 1. Opciones de DHCP estándar (continuación)

Número de opción	Opción	Descripción
64	Nombre de dominio NIS	Esta opción especifica el nombre del dominio NIS+ del cliente. El dominio se formatea como una serie de caracteres que está formada por caracteres del juego de caracteres ASCII de NVT. El código para esta opción es 64. Su longitud mínima es 1. **Código Len Nombre de dominio del cliente** **64 | n | n1 | n2 | n3 | n4 | ...** RZAKG527-0
65	Servidores NIS	Esta opción especifica una lista de direcciones IP que indican los servidores NIS+ que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para esta opción es 65. Su longitud mínima es 4 y la longitud debe ser un múltiplo de 4. **Código Len Dirección 1 Dirección 2** **65 | n | a1 | a2 | a3 | a4 | a1 | a2 | ...** RZAKG562-0
66	Nombre de servidor	Esta opción se utiliza para identificar un servidor TFTP cuando se ha utilizado el campo 'sname' en la cabecera DHCP para las opciones de DHCP. El código para esta opción es 66 y su longitud mínima es 1. **Código Len Servidor TFTP** **66 | n | c1 | c2 | c3 | ...** RZAKG571-0
67	Nombre de archivo de arranque	Esta opción se utiliza para identificar un archivo de arranque cuando se ha utilizado el campo 'file' en la cabecera DHCP para las opciones de DHCP. El código para esta opción es 67 y su longitud mínima es 1. **Código Len Nombre de archivo de arranque** **67 | n | c1 | c2 | c3 | ...** RZAKG572-0
68	Dirección de inicio	Esta opción especifica una lista de direcciones IP que indican los agentes de inicio de IP móviles que están disponibles para el cliente. Los agentes deben listarse por orden de preferencia. El código para esta opción es 68. Su longitud mínima es 0 (lo que indica que no hay agentes de inicio disponibles) y la longitud debe ser un múltiplo de 4. Se espera que la longitud habitual sea de cuatro octetos y que contenga una sola dirección del agente de inicio. **Código Len Direcciones de agentes de inicio (cero o más)** **68 | n | a1 | a2 | a3 | a4 | ...** RZAKG529-0

Tabla 1. Opciones de DHCP estándar (continuación)

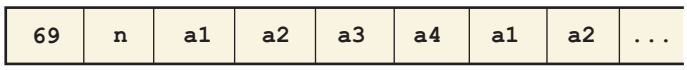
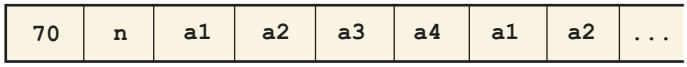
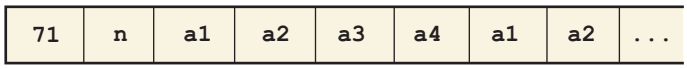
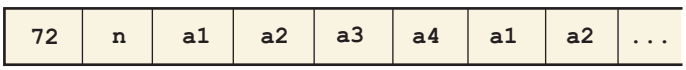
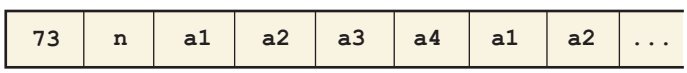
Número de opción	Opción	Descripción
69	Servidores SMTP	La opción de servidores SMTP especifica una lista de servidores SMTP que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor SMTP es 69. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG563-0
70	Servidor POP3	La opción de servidor POP3 especifica una lista de servidores POP3 que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor POP3 es 70. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG564-0
71	Servidor NNTP	La opción de servidor NNTP especifica una lista de servidores NNTP que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor NNTP es 71. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG565-0
72	Servidor WWW	La opción de servidor WWW especifica una lista de servidores WWW que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor WWW es 72. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG566-0
73	Servidor Finger	La opción de servidor Finger especifica una lista de servidores Finger que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor Finger es 73. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2**  RZAKG567-0

Tabla 1. Opciones de DHCP estándar (continuación)

Número de opción	Opción	Descripción
74	Servidor IRC	La opción de servidor IRC especifica una lista de servidores IRC que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor IRC es 74. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2** **74 n a1 a2 a3 a4 a1 a2 ...** RZAKG568-0
75	Servidor StreetTalk	La opción de servidor StreetTalk especifica una lista de servidores StreetTalk que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor StreetTalk es 75. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2** **75 n a1 a2 a3 a4 a1 a2 ...** RZAKG569-0
76	Servidor STDA	La opción de servidor STDA (StreetTalk Directory Assistance) especifica una lista de servidores STDA que están disponibles para el cliente. Los servidores deben listarse por orden de preferencia. El código para la opción de servidor STDA (StreetTalk Directory Assistance) es 76. La longitud mínima para esta opción es de 4 octetos y la longitud debe ser siempre un múltiplo de 4. **Código Len Dirección 1 Dirección 2** **76 n a1 a2 a3 a4 a1 a2 ...** RZAKG570-0
77	Clase de usuario	Especifica el nombre de clase de la que es miembro el host. Debe haber definido previamente esta clase en el servidor DHCP durante la configuración del servidor DHCP.
78	Agente de directorios	Especifica la dirección IP del agente de directorios si los clientes utilizan el Protocolo de Ubicación de Servicio (Service Location Protocol) para enviar y recibir mensajes.
79	Ámbito de servicio	Especifica el ámbito del agente de directorios que utiliza el Protocolo de Ubicación de Servicio (Service Location Protocol) para dar respuesta a los mensajes de petición de servicio.
80	Autorización de denominación	Especifica la autorización de denominación del agente de directorios si los clientes utilizan el protocolo de Ubicación de Servicio (Service Location Protocol) para enviar y recibir mensajes. La autorización de denominación especifica la sintaxis para los esquemas que se utilizan en los URL.

Información relacionada

Opciones de DHCP y extensiones de distribuidor de BOOTP

Ejemplos: DHCP

Al revisar los diagramas y ejemplos sobre cómo se configuran las diferentes redes, puede determinar cuál es la mejor elección para su instalación.

A menudo, la mejor forma de conocer una tecnología es ver cómo la han utilizado otras personas. Los ejemplos que siguen muestran cómo funciona DHCP, cómo está integrado dentro de diferentes configuraciones de red y cómo vincular algunas de las funciones de V5R1. Es un buen punto de partida tanto para los principiantes de DHCP como para los administradores de DHCP con experiencia.

Conceptos relacionados

"Consideraciones sobre la topología de la red" en la página 43
Al planificar la configuración del protocolo de configuración dinámica de hosts (DHCP), debe tener presentes varios factores, como son la topología de la red, los dispositivos de la red (por ejemplo, los direccionadores) y cómo desea dar soporte a los clientes en DHCP.

Ejemplo: subred DHCP simple

En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) en una LAN simple con cuatro clientes PC y una impresora basada en LAN.

En este ejemplo, el modelo de System i funciona a modo de servidor DHCP para la subred IP 10.1.1.0. El servidor está conectado a la LAN mediante su interfaz 10.1.1.1.

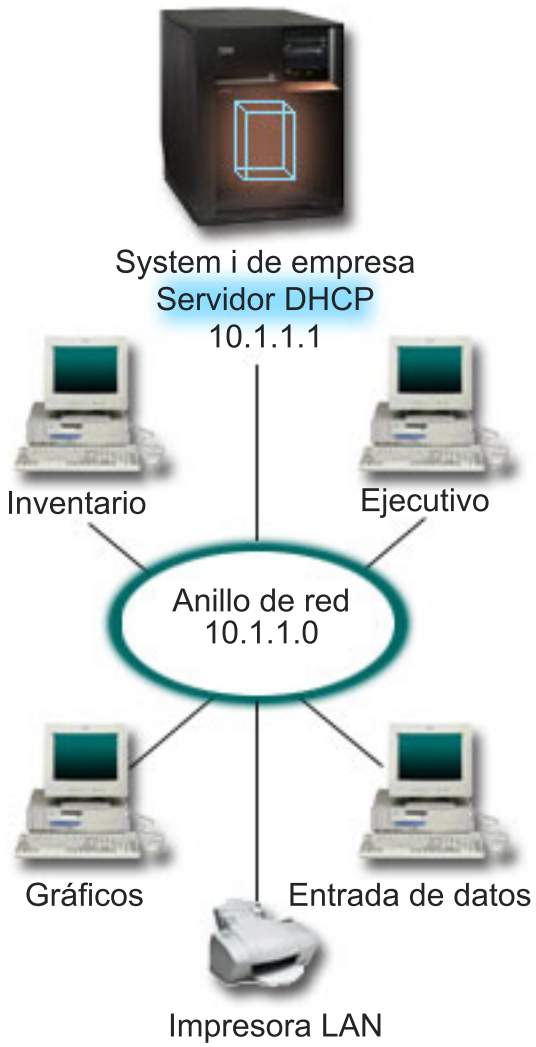


Figura 2. Configuración de LAN simple para el modelo de System i

Con tan pocos clientes PC, a los administradores les resulta fácil escribir y mantener la información relacionada con la dirección IP de cada PC. (Solo tienen que visitar cuatro PC en este caso). Ahora imagínese que los cuatro PC se convirten en 200 PC. La configuración de la información IP de cada PC sería una tarea muy larga y que además podría producir errores de exactitud. DHCP puede simplificar el proceso de asignar información IP a los clientes. Si la subred 10.1.1.0 tuviese centenares de clientes, el administrador solo tendría que crear una única política de DHCP en el sistema. Esta política distribuye la información IP a cada cliente.

Cuando los clientes PC envían las señales DHCPDISCOVER, el servidor responde con la información IP pertinente. En este ejemplo, la empresa tiene además una impresora basada en la LAN que obtiene su información IP a partir del servidor DHCP. Pero como los clientes PC dependen de que la dirección IP de la impresora siempre sea la misma, el administrador de la red debe tenerlo en cuenta en la política de DHCP. Una solución consiste en asignar una dirección IP constante a la impresora. Puede utilizar el servidor DHCP para definir un cliente (como la impresora de la LAN) en la política DHCP mediante su dirección MAC. En la definición del cliente DHCP, se pueden asignar valores específicos, como por ejemplo direcciones IP y direcciones de direccionador, al cliente deseado.

Para que un cliente se comunique con una red TCP/IP, se requiere como mínimo una dirección IP y una máscara de subred. Los clientes obtendrán la dirección IP del servidor DHCP y este pasará la información de configuración adicional (por ejemplo, la máscara de subred) utilizando las opciones de configuración.

Planificación de la configuración de DHCP para una LAN simple

Tabla 2. Opciones de configuración global (se aplica a todos los clientes atendidos por el servidor DHCP)

Objeto		**Valor**
Opciones de configuración	Opción 1: máscara de subred	255.255.255.0
	Opción 6: servidor de nombres de dominio	10.1.1.1
	Opción 15: nombre de dominio	miempresa.com
Direcciones de subred no asignadas por el sistema		10.1.1.1 (servidor de nombres de dominio)
¿Realiza el sistema actualizaciones de DNS?		No
¿Soporta el sistema clientes BOOTP?		No

Tabla 3. Subred para sistemas PC

Objeto	**Valor**
Nombre de subred	SimpleSubnet
Direcciones a gestionar	10.1.1.2 - 10.1.1.150
Tiempo de cesión	24 horas (valor predeterminado)
Opciones de configuración Opciones heredadas	 Opciones de la configuración global

Tabla 4. Cliente para impresora

Objeto	**Valor**
Nombre del cliente	LANPrinter
Dirección del cliente	10.1.1.5
Opciones de configuración Opciones heredadas	 Opciones de la configuración global

Referencia relacionada

"Ejemplo: múltiples subredes TCP/IP"
En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) con dos redes LAN conectadas por un direccionador habilitado para DHCP.

"Ejemplo: DHCP y multiubicación" en la página 29
En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) en una LAN conectada a Internet mediante un direccionador de Internet.

Ejemplo: múltiples subredes TCP/IP

En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) con dos redes LAN conectadas por un direccionador habilitado para DHCP.

Este ejemplo es similar al ejemplo de subred DHCP simple, excepto que ahora hay una subred TCP/IP adicional. Supongamos que los clientes de oficina y los clientes de entrada de datos se encuentran en distintas plantas de un edificio de oficina y que están separados con un direccionador. Si el administrador de la red desea que todos los clientes reciban la información IP a través de DHCP, esta situación presenta algunas diferencias exclusivas respecto a una subred DHCP simple. En la siguiente figura se ve el diseño de una red de ejemplo que consta de un servidor DHCP de System i conectado a dos redes LAN mediante un direccionador situado entre las redes. La figura tiene intencionadamente un número limitado de clientes por cuestión de claridad. En una empresa real suele haber un número considerablemente mayor de clientes en cada subred.

Figura 3. Múltiples redes LAN conectadas mediante un direccionador

El direccionador que conecta las dos redes debe estar habilitado para pasar paquetes DHCPDISCOVER. Si no lo está, los clientes de entrada de datos no podrán recibir la información IP ni acceder a la red. Además, se necesitan dos definiciones de subred para la política de DHCP: una para la subred de entrada de datos y otra para la subred de oficina. Como mínimo, las diferencias entre las subredes son las

subredes IP y las direcciones de direccionador. La subred de entrada de datos necesita recibir la dirección de direccionador 10.1.2.2 para comunicarse con la subred de oficina.

Planificar la configuración de DHCP para múltiples redes LAN

Tabla 5. Opciones de configuración global (atañe a todos los clientes atendidos por el servidor DHCP)

Objeto		**Valor**
Opciones de configuración	Opción 1: máscara de subred	255.255.255.0
	Opción 6: servidor de nombres de dominio	10.1.1.1
	Opción 15: nombre de dominio	miempresa.com
Direcciones de subred no asignadas por el sistema		10.1.1.1 (Servidor de nombres de dominio)
¿Realiza el sistema actualizaciones de DNS?		No
¿Soporta el sistema clientes BOOTP?		No

Tabla 6. Subred para los clientes de oficina

Objeto		**Valor**
Nombre de subred		Oficina
Direcciones que hay que gestionar		10.1.1.3 - 10.1.1.150
Tiempo de cesión		24 horas (valor predeterminado)
Opciones de configuración	Opción 3: direccionador	10.1.1.2
	Opciones heredadas	Opciones de la configuración global
Direcciones de subred no asignadas por el servidor		10.1.1.2 (Direccionador)

Tabla 7. Subred para los clientes de entrada de datos

Objeto		**Valor**
Nombre de subred		EntradaDatos
Direcciones que hay que gestionar		10.1.2.3 - 10.1.2.150
Tiempo de cesión		24 horas (valor predeterminado)
Opciones de configuración	Opción 3: direccionador	10.1.2.2
	Opciones heredadas	Opciones de la configuración global
Direcciones de subred no asignadas por el servidor		10.1.2.2 (Direccionador)

Referencia relacionada

"Ejemplo: subred DHCP simple" en la página 24
En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) en una LAN simple con cuatro clientes PC y una impresora basada en LAN.

Ejemplo: DHCP y multiubicación

En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) en una LAN conectada a Internet mediante un direccionador de Internet.

Este ejemplo es muy parecido al ejemplo de subred DHCP simple. En este ejemplo, los clientes de entrada de datos solo se comunican entre ellos y con el modelo de System i. Obtienen la información de IP dinámicamente del servidor DHCP de System i.

Sin embargo, una nueva versión de la aplicación de entrada de datos exige que la red se comunique con Internet, por lo que la empresa decide ofrecer acceso a Internet a través de un direccionador de Internet, como se ve en la siguiente figura Además del direccionador, el administrador también añade otra interfaz con una dirección IP para comunicarse con Internet. Cuando se asignan múltiples direcciones IP al mismo adaptador, el sistema es de multiubicación.

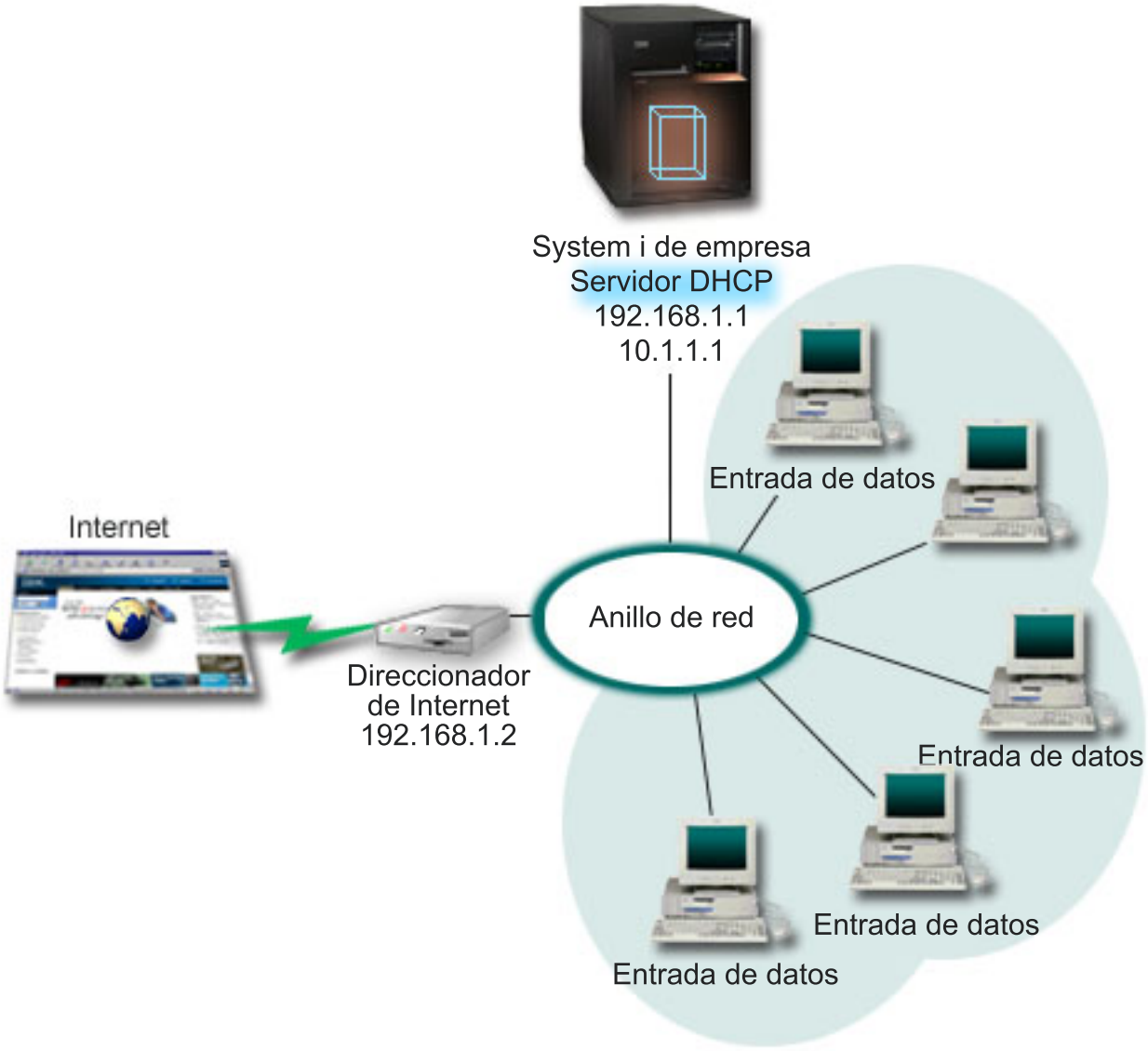


Figura 4. Utilizar DHCP con múltiples direcciones IP asignadas al mismo adaptador

Nota: Aunque esta es una forma factible de conectar la red a Internet, no es la forma más segura. Sirve a efectos de este ejemplo de DHCP, pero debe tener en cuenta las implicaciones de seguridad cuando configure su propio servidor DHCP.

Al configurar DHCP, tenga presente que el modelo de System i se conoce mediante dos direcciones IP distintas. Para entender cómo se hay que configurar DHCP correctamente en este escenario, conviene recordar lo que ocurre cuando un cliente envía un paquete DHCPDISCOVER.

Cuando un cliente envía un paquete DHCPDISCOVER, este se difunde en el anillo. Porlo tanto, el servidor DHCP de System i no puede determinar hacia qué dirección IP iba dirigido el paquete. Si este

paquete está marcado con la dirección IP de interfaz 10.1.1.1 (la utilizada para DHCP), los clientes reciben la información IP como es de esperar. Pero es posible que el paquete en realidad se marque con la dirección 192.168.1.1 (la conectada a Internet) Si el paquete se recibe en la interfaz 192.168.1.1, el cliente de entrada de datos no recibe ninguna información IP.

Para configurar DHCP en esta situación, no solo tiene que crear la subred DHCP de entrada de datos, sino también una subred para la red Internet. La política de Internet consta de una subred sin direcciones disponibles. La forma más fácil de hacerlo es definir la subred con al menos una dirección IP (por ejemplo, 192.168.1.1) y luego excluir esa misma dirección IP. Con las dos subredes definidas, combine las dos (o más) subredes para formar un grupo de subredes. Si el paquete DHCPDISCOVER se marca con la interfaz 192.168.1.1, la subred de entrada de datos seguirá emitiendo información IP válida.

Para que este escenario funcione, la subred de entrada de datos debe pasar a sus clientes la dirección de direccionador que les corresponde para acceder a Internet. En este caso, la dirección del direccionador es la interfaz 10.1.1.1 de System i. También debe activar el reenvío de datagramas IP para que las dos interfaces se direccionen los paquetes entre sí. En este ejemplo se utilizan direcciones IP reservadas para representar direcciones IP internas y externas. Si su red coincide con este escenario, también tendrá que utilizar la conversión de direcciones de red (NAT) para que los clientes de entrada de datos se comuniquen con Internet.

La utilización de grupos de subredes para eliminar este problema de marcado no se limita únicamente a los ejemplos de multiubicación. Siempre que múltiples interfaces se conectan a la misma red, se podría producir el mismo problema. En la siguiente figura se ve cómo puede el modelo de System i tener dos conexiones físicas con la red de entrada de datos. Esta configuración de red requiere una política de grupo DHCP parecida a la de la configuración de multiubicación, porque es concebible pensar que la interfaz 192.168.1.1 pueda responder a los paquetes DHCPDISCOVER.

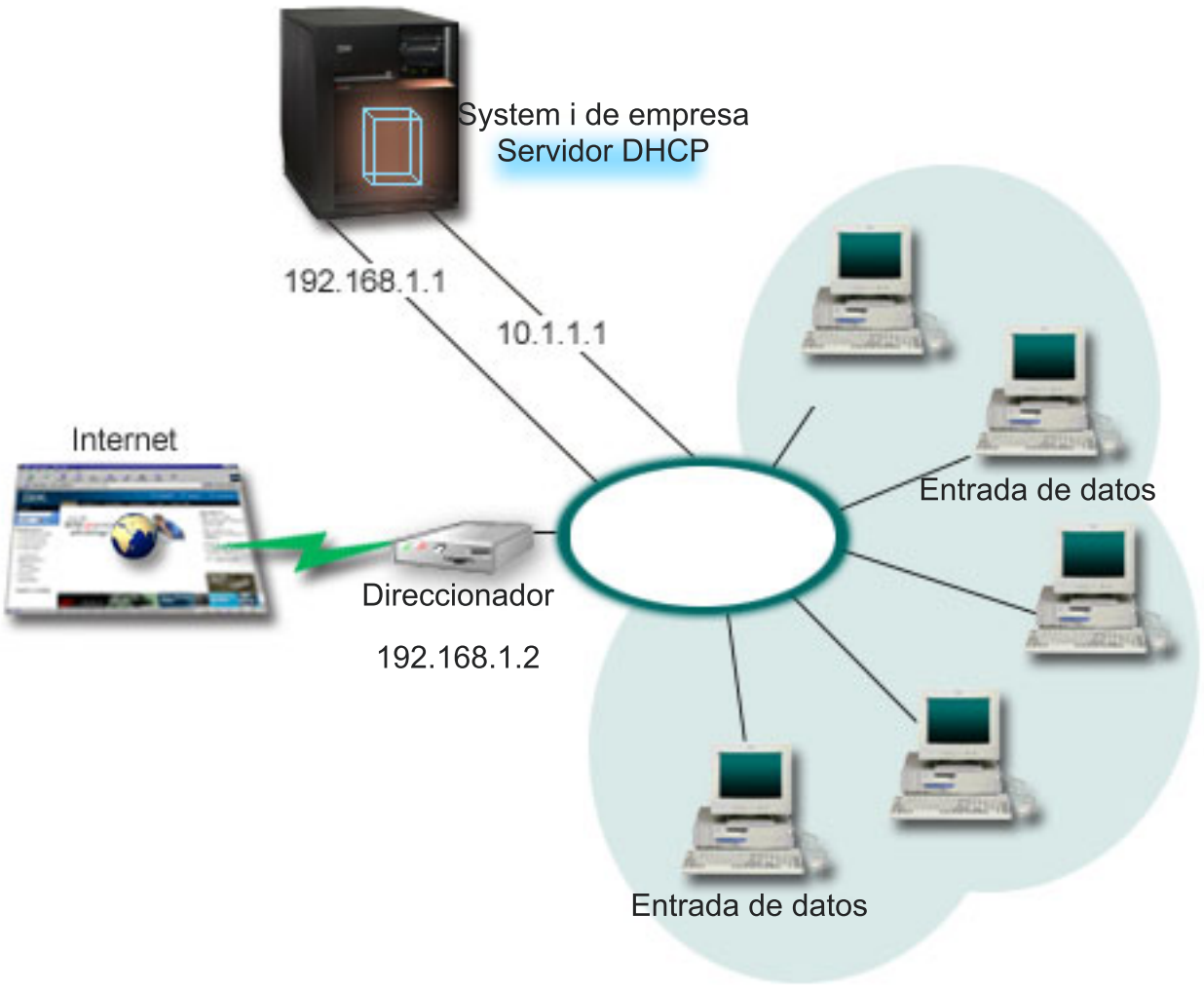


Figura 5. Utilizar DHCP con múltiples interfaces conectadas a la misma red.

Planificar la configuración de DHCP para multiubicación

Tabla 8. Opciones de configuración global (atañe a todos los clientes atendidos por el servidor DHCP)

Objeto	Valor
¿Realiza el sistema actualizaciones de DNS?	No
¿Soporta el sistema clientes BOOTP?	No

Tabla 9. Subred para clientes de entrada de datos

Objeto	Valor
Nombre de subred	Entrada de datos
Direcciones que hay que gestionar	10.1.1.2 - 10.1.1.150
Tiempo de cesión	24 horas (valor predeterminado)

Tabla 9. Subred para clientes de entrada de datos (continuación)

Objeto		Valor
Opciones de configuración	Opción 1: máscara de subred	255.255.255.0
	Opción 3: direccionador	10.1.1.1
	Opción 6: servidor de nombres de dominio	10.1.1.1
	Opción 15: nombre de dominio	miempresa.com
Direcciones de subred no asignadas por el servidor		10.1.1.1 (Direccionador, servidor DNS)

Tabla 10. Subred para clientes de Internet (subred vacía)

Objeto	Valor
Nombre de subred	Internet
Direcciones que hay que gestionar	192.168.1.1 - 192.168.1.1
Direcciones de subred no asignadas por el servidor	192.168.1.1 (Todas las direcciones IP disponibles)

Tabla 11. Grupo de subredes para todos los paquetes DHCPDISCOVER entrantes

Objeto	Valor
Nombre del grupo de subredes	Multiubicación
Subredes incluidas en el grupo	Subred Internet Subred EntradaDatos

Otras configuraciones

- Activar el reenvío de datagramas IP para las dos interfaces
- Configurar NAT para los clientes de entrada de datos

Referencia relacionada

"Ejemplo: subred DHCP simple" en la página 24
En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) en una LAN simple con cuatro clientes PC y una impresora basada en LAN.

Ejemplo: DNS y DHCP en el mismo System i

En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) con actualizaciones dinámica del sistema de nombres de dominio (DNS) en una LAN simple.

En la siguiente figura se ve cómo puede el modelo de System i funcionar como servidor DHCP y DNS para una subred simple. En este entorno de trabajo, supongamos que los clientes ejecutivos, de inventario y de entrada de datos crean documentos con gráficos a partir del servidor de archivos gráficos. Los clientes se conectan al servidor de archivos gráficos correlacionando una unidad de red con el nombre de host que les corresponde.

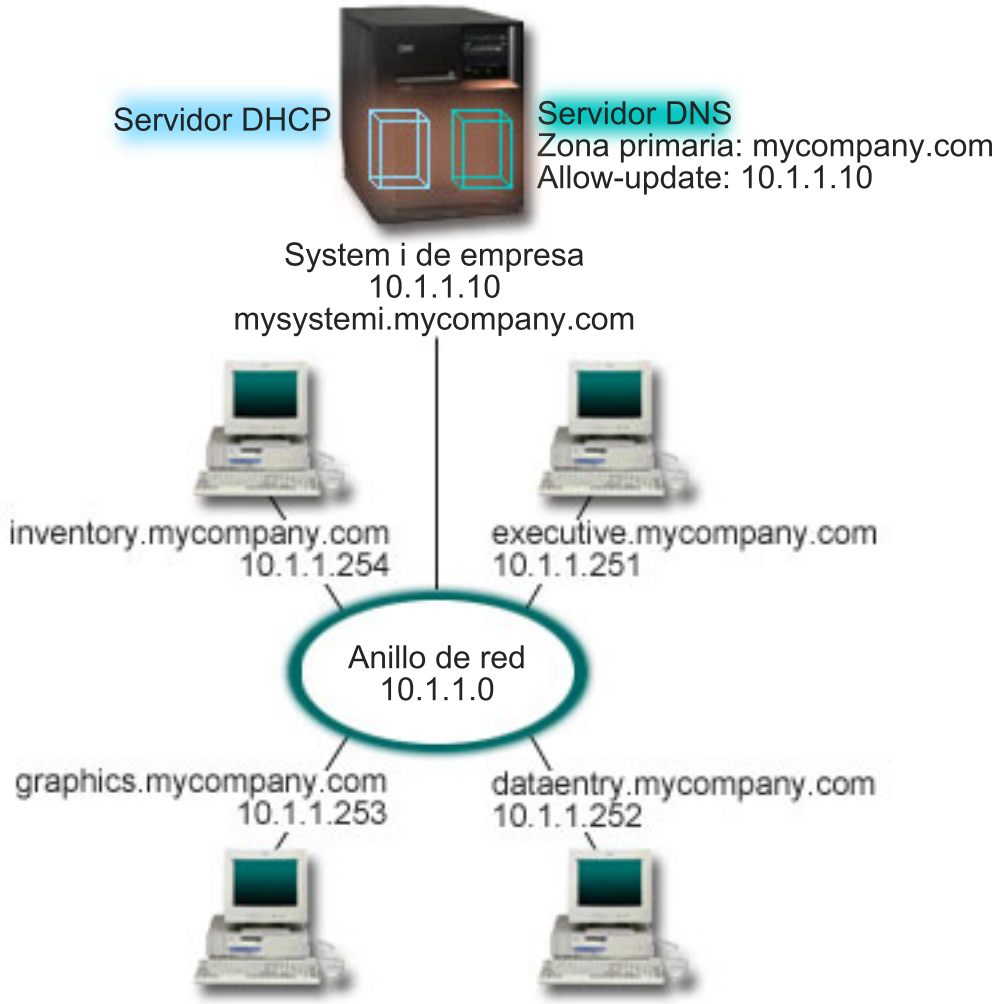


Figura 6. DNS dinámico y DHCP

Las versiones anteriores de DHCP y DNS eran independientes entre sí. Si DHCP asignaba una nueva dirección IP a un cliente, el administrador tenía que actualizar manualmente los registros de DNS. En este ejemplo, si cambia la dirección IP del servidor de archivos gráficos porque está asignada por DHCP, entonces los clientes dependientes no pueden correlacionar una unidad de red con el nombre de host ya que los registros de DNS contienen la dirección IP anterior del servidor de archivos.

Con el servidor DNS actual, los registros de DNS se pueden actualizar dinámicamente junto con cambios de dirección intermitentes a través de DHCP. Por ejemplo, cuando el servidor de archivos gráficos renueva la cesión y el servidor DHCP le asigna la dirección IP 10.1.1.250, los registros de DNS asociados se actualizan dinámicamente. Esto permite a los otros clientes buscar en el servidor DNS el servidor de archivos gráficos mediante el nombre de host sin interrupción.

Puede configurar DHCP para que actualice los registros de recursos en los registros de correlación de direcciones (A) y en los registros de puntero de búsqueda inversa (PTR) en nombre de un cliente. El registro A correlaciona el nombre de host de un cliente con su dirección IP. El registro PTR correlaciona la dirección IP de un cliente con su nombre de host. Para cada registro que se actualice dinámicamente, se escribe un registro de texto (TXT) asociado para identificar que el registro lo ha escrito DHCP. Puede optar por dejar que DHCP actualice los registros A y PTR o tan solo los registros PTR. Para obtener más información sobre cómo configurar el DNS para que acepte actualizaciones dinámicas, consulte el Ejemplo: DNS y DHCP en el mismo System i, en el temario DNS.

Nota: Si configura DHCP para que solo actualice los registros PTR, deberá configurar el DNS para que permita actualizaciones de los clientes, de modo que cada cliente pueda actualizar su registro A. No todos los clientes DHCP tiene soporte para realizar sus propias peticiones de actualización de los registros A. Consulte la documentación de la plataforma del cliente antes de elegir este método.

Para habilitar las actualizaciones de DNS, debe crear una clave de DNS para el servidor DHCP. La clave de DNS autoriza al servidor DHCP a actualizar los registros de DNS de acuerdo con las direcciones IP que ha distribuido. A continuación, en la configuración de DHCP, elija el ámbito donde desea que se realicen las actualizaciones de DNS. Por ejemplo, si desea que todas las subredes realicen actualizaciones de DNS, establezca las actualizaciones a nivel global. Si desea que una sola subred realice actualizaciones, defina únicamente esa subred para que realice actualizaciones.

Planificar la configuración de DHCP cuando se utiliza DNS dinámico

Tabla 12. Opciones de configuración global (atañe a todos los clientes atendidos por el servidor DHCP)

Objeto		**Valor**
Opciones de configuración	Opción 1: máscara de subred	255.255.255.0
	Opción 6: servidor de nombres de dominio	10.1.1.10
	Opción 15: nombre de dominio	miempresa.com
¿Realiza el sistema actualizaciones de DNS?		Sí -- Registros A y registros PTR
¿Soporta el sistema clientes BOOTP?		No

Tabla 13. Subred para anillo de red

Objeto		**Valor**
Nombre de subred		NetworkSubnet
Direcciones para gestionar		10.1.1.250 - 10.1.1.254
Tiempo de cesión		24 horas (valor predeterminado)
Opciones de configuración	Opciones heredadas	Opciones de la configuración global

Otras configuraciones:

Autorice a DHCP para que envíe actualizaciones al DNS. Consulte el Ejemlo: DNS y DHCP en el mismo System i, en el temario DNS.

Ejemplo: DNS y DHCP en distintos modelos de System i

En este ejemplo se explica cómo configurar el protocolo de configuración dinámica de hosts (DHCP) y el sistema de nombres de dominio (DNS) en dos modelos distintos de System i para realizar actualizaciones dinámicas por una LAN simple.

En la siguiente figura se ve una pequeñas red de subredes en la que DNS y DHCP se ejecutan en modelos de System i separados. El sistema que ejecuta DNS se configura de la misma manera que cuando DNS y DHCP están en el mismo modelo de System i. Sin embargo, se deben realizar algunos pasos adicionales para configurar el servidor DHCP para que envíe actualizaciones dinámicas.

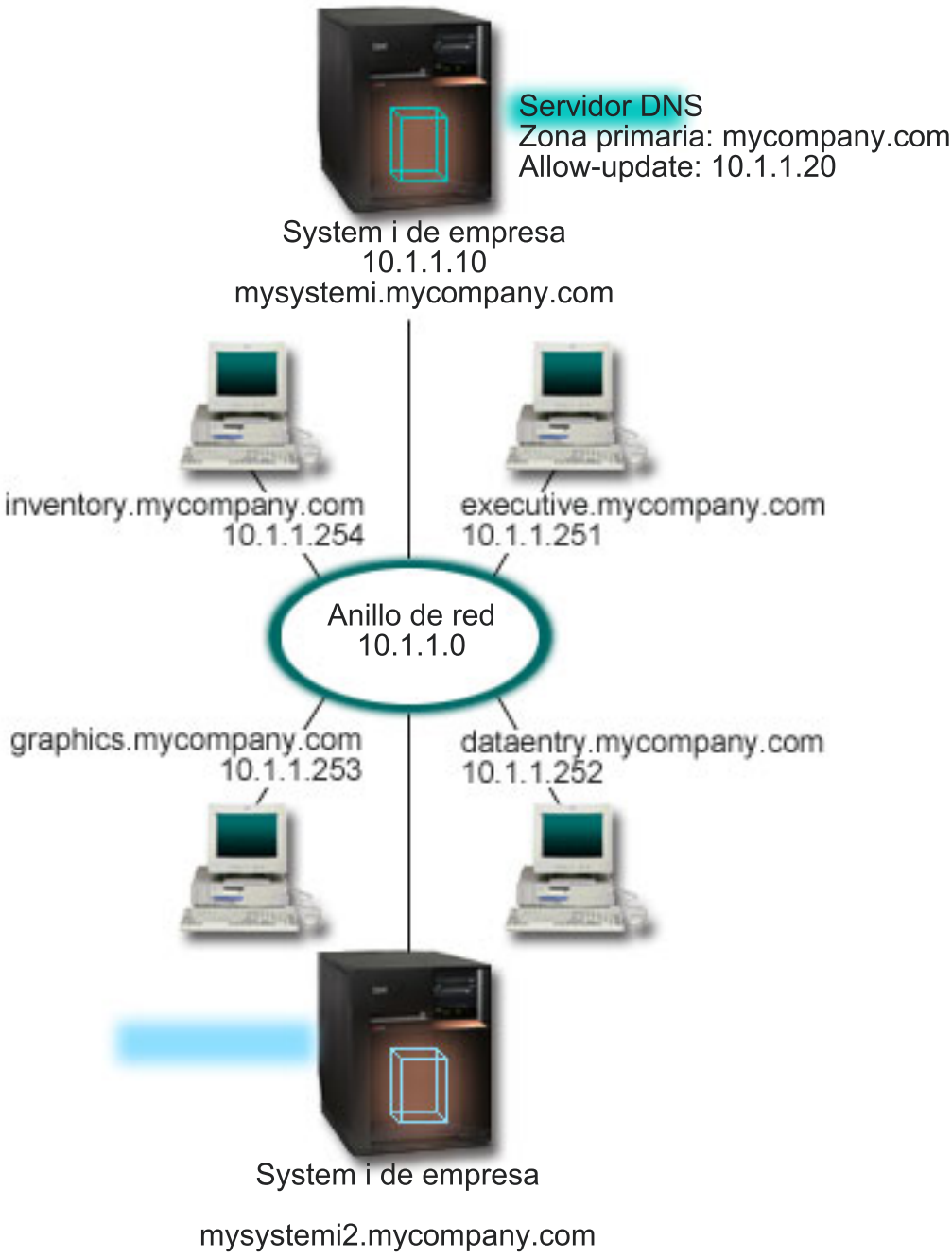


Figura 7. DNS y DHCP en distintos modelos de System i

Planificar la configuración de DHCP cuando se utiliza un DNS dinámico

Consulte el "Ejemplo: DNS y DHCP en el mismo System i" en la página 33 para ver ejemplos de opciones de configuración global y valores de subred.

Otras configuraciones:

Instalar el sistema de nombres de dominio (DNS) de i5/OS (Opción 31).

Instalar el sistema de nombres de dominio (DNS) de i5/OS (Opción 31) en el modelo de System i que ejecutará DHCP, que en este caso es mysystemi2. Esta opción contiene la API de actualización dinámica que gestiona el proceso de actualización de registros de recursos. Las instrucciones de instalación están en los requisitos del sistema DNS.

Autorizar a DHCP para que envíe actualizaciones al DNS

Debe autorizar al servidor DHCP para que envíe actualizaciones al servidor DNS. Puede repetir el proceso de definir la clave de actualización dinámica, o bien enviar el archivo y colocarlo en la vía de acceso del directorio pertinente.

Para crear una clave de actualización dinámica en ambos modelos de System i, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **DNS**.
2. En el panel de la izquierda, pulse **DNS** con el botón derecho del ratón y seleccione **Gestionar claves de actualización dinámica**.
3. En la página Gestionar claves de actualización dinámica, seleccine **Añadir**.
4. En la página Añadir claves de actualización dinámica, cumplimente estos campos:
   - **Nombre de clave**: especifique el nombre de la clave, por ejemplo `miempresa.key.` El nombre de la clave debe terminar con un punto.
   - **Zonas de actualización dinámica**: especifique los nombres de las zonas para las que será válida esta clave. Puede especificar más de una zona.
   - **Generar clave**: seleccione el método que desea utilizar para generar una clave secreta.
5. Repita los pasos anteriores para que la misma clave esté definida en ambos modelos, el modelo de System i que ejecuta el DNS y el modelo de System i que ejecuta DHCP.

Conceptos relacionados

Requisitos del sistema de nombres de dominio (DNS)

Información relacionada

API de DNS de actualización

Ejemplo: PPP y DHCP en un solo System i

En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) para una LAN y un cliente de acceso telefónico remoto.

Los clientes remotos, como los de acceso telefónico, necesitan acceder a menudo a la red de una empresa. Los clientes de acceso telefónico obtienen acceso a un modelo de System i con un protocolo punto a punto (PPP). Para acceder a la red, el cliente de acceso telefónico necesita información IP exactamente igual que cualquier cliente conectado directamente a la red. Un servidor DHCP de System i puede distribuir la información de direcciones IP al cliente de acceso telefónico PPP exactamente igual que lo hace cualquier otro cliente conectado directamente. En la siguiente figura se ve un cliente remoto que debe acceder telefónicamente a la red de la empresa para realizar un trabajo.

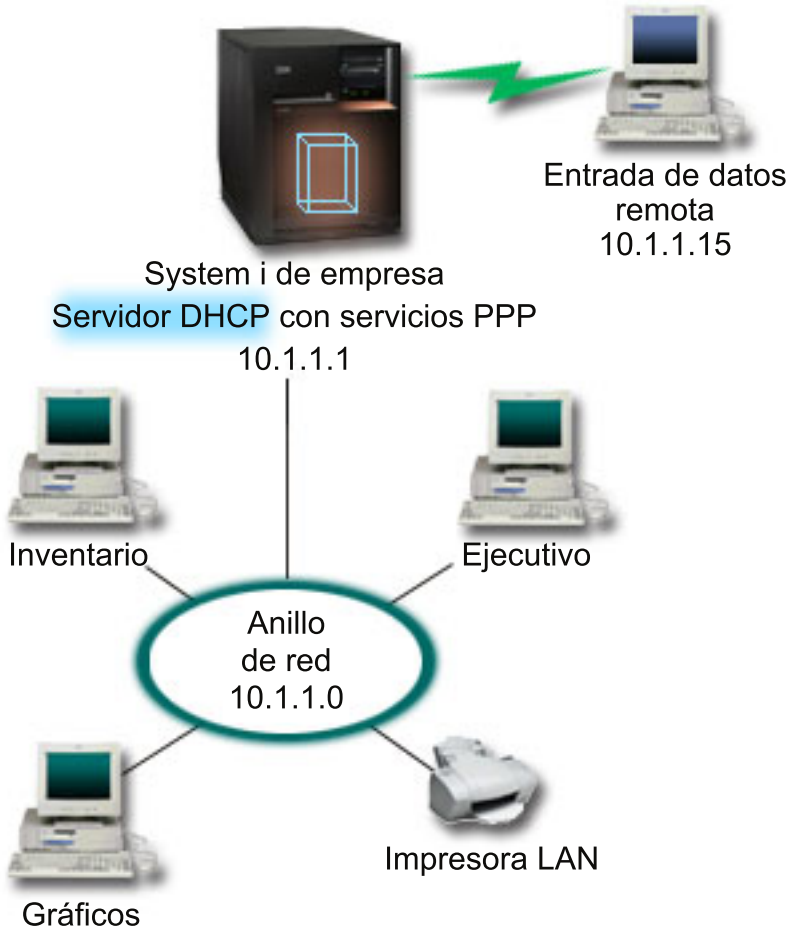


Figura 8. PPP y DHCP en un solo modelo de System i

Para que el empleado remoto entre satisfactoriamente a formar parte de la red de la empresa, el modelo de System i debe utilizar una combinación de servicios de acceso remoto(RAS) y DHCP. La función de servicios de acceso remoto crea la prestación de acceso telefónico para el modelo de System i. Si está debidamente configurado, después de que el cliente establezca la conexión de acceso telefónico, el servidor PPP indica al servidor DHCP que distribuya la información TCP/IP al cliente.

En este ejemplo, una sola política de subred DHCP abarca tanto a los clientes locales de la red como a los clientes de acceso telefónico.

Si desea que el perfil PPP se adecue al DHCP para la distribución IP, debe hacerlo en el perfil PPP. En los valores TCP/IP del perfil de conexión del receptor, establezca que el método de asignación de direcciones IP remotas pase de ser Fijo a ser DHCP. Para que los clientes de acceso telefónico se puedan comunicar con otros clientes de la red (por ejemplo, con la impresora de la LAN), también debe activar el reenvío de IP en los valores TCP/IP del perfil y en las propiedades de la configuración (pila) de TCP/IP. Si solo ha activado el reenvío de IP en el perfil PPP, el modelo de System i no pasará los paquetes IP. Debe activar el reenvío de IP tanto en el perfil como en la pila.

Además, la dirección IP de la interfaz local del perfil PPP debe ser una dirección IP que esté dentro de la definición de subred del servidor DHCP. En este ejemplo, la dirección de la interfaz local del perfil PPP debe ser 10.1.1.1. Esta dirección también se debe excluir de la agrupación de direcciones del servidor DHCP para que no se asigne a un cliente DHCP.

Planificar la configuración de DHCP para clientes in situ y PPP

Tabla 14. Opciones de configuración global (atañe a todos los clientes atendidos por el servidor DHCP)

Objeto		**Valor**
Opciones de configuración	Opción 1: máscara de subred	255.255.255.0
	Opción 6: servidor de nombres de dominio	10.1.1.1
	Opción 15: nombre de dominio	miempresa.com
¿Realiza el sistema actualizaciones de DNS?		No
¿Soporta el sistema clientes BOOTP?		No

Tabla 15. Subred para clientes in situ y clientes de acceso telefónico

Objeto		**Valor**
Nombre de subred		RedPrincipal
Direcciones que hay que gestionar		10.1.1.3 - 10.1.1.150
Tiempo de cesión		24 horas (valor predeterminado)
Opciones de configuración	Opciones heredadas	Opciones de la configuración global
Direcciones de subred no asignadas por el servidor		10.1.1.1 (Dirección de la interfaz local especificada en las propiedades de Valores TCP/IP del Perfil de conexión de receptor en System i Navigator)

Otras configuraciones

- Establezca el método de asignación de direcciones IP remotas en DHCP en el perfil de conexión de receptor PPP.
  1. Habilite la conexión de cliente WAN de DHCP con un servidor DHCP o una conexión de retransmisión utilizando el elemento de menú **Servicios**, para los servicios de acceso remoto (RAS) de System i Navigator.
  2. Seleccione que hay que utilizar DHCP para el método de asignación de direcciones IP en las propiedades de Valores TCP/IP del Perfil de conexión de receptor en System i Navigator.
- Permita que el sistema remoto acceda a otras redes (reenvío de IP) en las propiedades de Valores TCP/IP del Perfil de conexión de receptor en System i Navigator.
- Habilite el reenvío de datagramas IP en las propiedades de los valores de Configuración de TCP/IP en System i Navigator.

Referencia relacionada

"Ejemplo: DHCP y perfil PPP en distintos modelos de System i"
En este ejemplo se explica cómo configurar dos modelos de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) y como agente de retransmisión BOOTP/DHCP para dos redes LAN y clientes remotos de acceso telefónico.

Ejemplo: DHCP y perfil PPP en distintos modelos de System i

En este ejemplo se explica cómo configurar dos modelos de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) y como agente de retransmisión BOOTP/DHCP para dos redes LAN y clientes remotos de acceso telefónico.

En el ejemplo sobre PPP y DHCP en un solo modelo de System i se enseña a utilizar PPP y DHCP en un solo sistema para permitir que los clientes de acceso telefónico accedan a un red. Si le preocupa el diseño físico de la red o su seguridad, podría ser mejor tener separados los servidores PPP y DHCP o bien tener un servidor PPP dedicado sin servicios DHCP. En la siguiente figura se ve una red que tiene clientes de

acceso telefónico con las políticas de PPP y DHCP en distintos servidores.

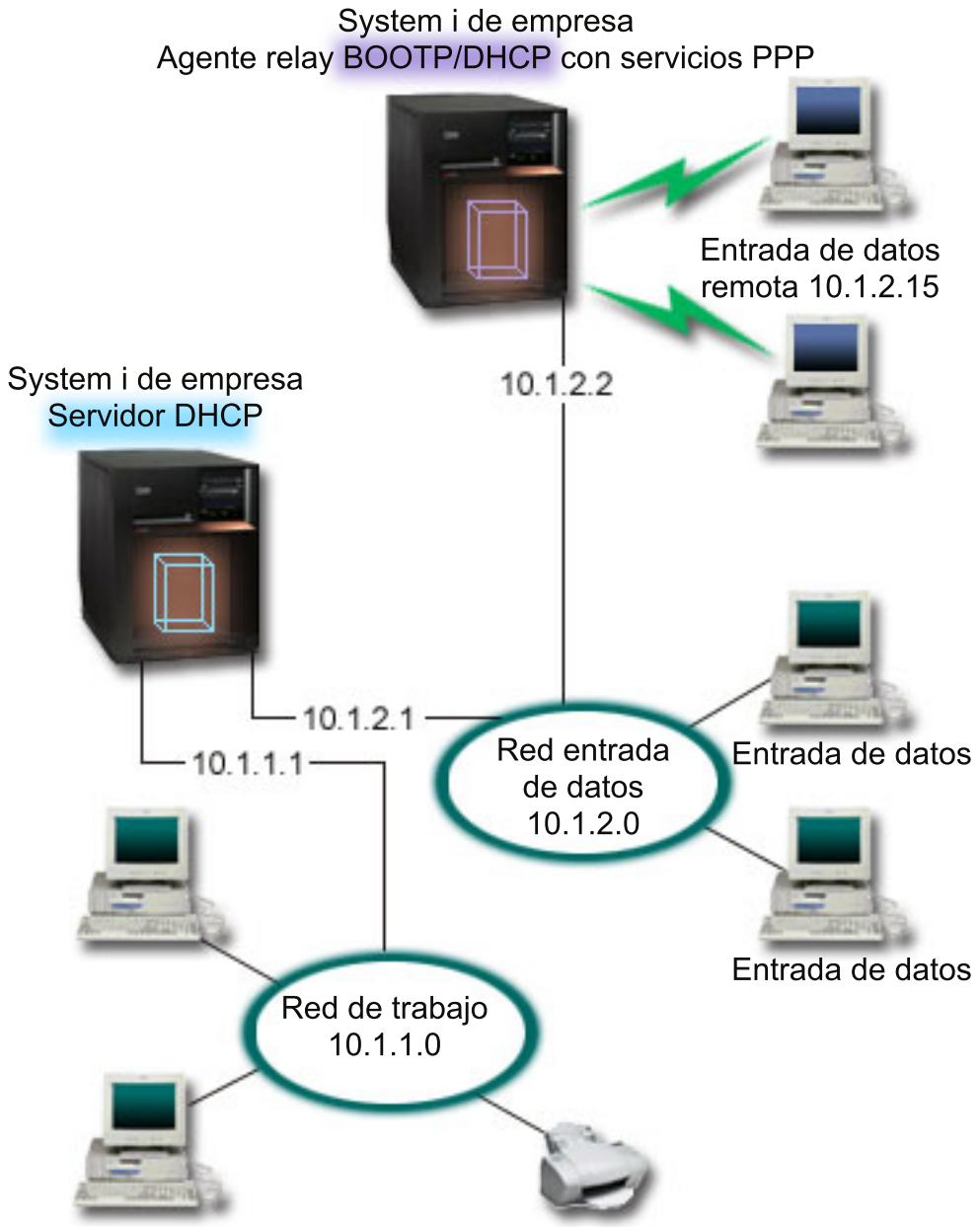


Figura 9. DHCP y perfil PPP en distintos modelos de System i

Los clientes de entrada de datos remotos acceden telefónicamente al servidor PPP de System i. El perfil PPP de dicho servidor debe tener un método de asignación de direcciones IP remotas igual a DHCP, como el que se emplea en el ejemplo de PPP y DHCP en un solo modelo de System i. El perfil PPP y las propiedades de la pila de TCP/IP del servidor PPP deben tener reenvío de IP. Además, como este servidor actúa como agente de retransmisión DHCP, este debe estar activado. Ello permite que el servidor de acceso remoto de System i pase paquetes DHCPDISCOVER al servidor DHCP. Entonces, el servidor DHCP responde y distribuye información TCP/IP a los clientes de acceso telefónico mediante el servidor PPP.

El servidor DHCP es responsable de distribuir direcciones IP tanto a la red 10.1.1.0 como a la red 10.1.2.0. En la red de entrada de datos, el servidor DHCP distribuye direcciones IP comprendidas entre 10.1.2.10 y 10.1.2.40 a los clientes de acceso telefónico o a los clientes conectados directamente a la red. Los clientes de entrada de datos también necesitan una dirección de direccionador (opción 3) igual a 10.1.2.1 para comunicarse con la red de trabajo, y el servidor DHCP de System i también debe tener habilitado el reenvío de IP.

Además, la dirección IP de la interfaz local del perfil PPP debe ser una dirección IP que esté dentro de la definición de subred del servidor DHCP. En este ejemplo, la dirección de la interfaz local del perfil PPP debe ser 10.1.2.2. Esta dirección también se debe excluir de la agrupación de direcciones del servidor DHCP para que no se asigne a un cliente DHCP. La dirección IP de la interfaz local debe ser una dirección a la que el servidor pueda enviar paquetes de respuesta.

Planificar la configuración de DHCP para DHCP con un agente de retransmisión DHCP

Tabla 16. Opciones de configuración global (atañe a todos los clientes atendidos por el servidor DHCP)

Objeto		**Valor**
Opciones de configuración	Opción 1: máscara de subred	255.255.255.0
	Opción 6: servidor de nombres de dominio	10.1.1.1
	Opción 15: nombre de dominio	miempresa.com
¿Realiza el sistema actualizaciones de DNS?		No
¿Soporta el sistema clientes BOOTP?		No

Tabla 17. Subred para la red de trabajo

Objeto		**Valor**
Nombre de subred		RedTrabajo
Direcciones que hay que gestionar		10.1.1.3 - 10.1.1.150
Tiempo de cesión		24 horas (valor predeterminado)
Opciones de configuración	Opciones heredadas	Opciones de la configuración global
Direcciones de subred no asignadas por el servidor		ninguna

Tabla 18. Subred para la red de entrada de datos

Objeto		**Valor**
Nombre de subred		EntradaDatos
Direcciones que hay que gestionar		10.1.2.10 - 10.1.2.40
Tiempo de cesión		24 horas (valor predeterminado)
Opciones de configuración	Opción 3: direccionador	10.1.2.1
	Opciones heredadas	Opciones de la configuración global
Direcciones de subred no asignadas por el servidor		10.1.2.1 (Direccionador) 10.1.2.15 (Dirección IP de la interfaz local del cliente de entrada de datos remotos) 10.1.2.14 (Dirección IP de la interfaz local del cliente de entrada de datos remotos)

Otras configuraciones en una plataforma System i que ejecute PPP

- Configure el servidor TCP/IP del agente de retransmisión BOOTP/DHCP

Objeto	Valor
Dirección de interfaz	10.1.2.2
Retransmitir paquetes a la dirección IP del servidor	10.1.2.1

- Establezca que el método de asignación de direcciones IP remotas sea DHCP en el perfil de conexión de receptor PPP
  1. Habilite la conexión de cliente WAN de DHCP con un servidor DHCP o una conexión de retransmisión utilizando el elemento de menú Servicios para los servicios de acceso remoto (RAS) de System i Navigator
  2. Seleccione que hay que utilizar DHCP para el método de asignación de direcciones IP en las propiedades de Valores TCP/IP del Perfil de conexión de receptor en System i Navigator
- Permita que el sistema remoto acceda a otras redes (reenvío de IP) en las propiedades de Valores TCP/IP del Perfil de conexión de receptor en System i Navigator (para permitir que clientes remotos se comuniquen con la red de entrada de datos)
- Habilite el reenvío de datagramas IP en las propiedades de los valores de Configuración de TCP/IP en Configuration in System i Navigator (para permitir que clientes remotos se comuniquen con la red de entrada de datos)

Referencia relacionada

"Ejemplo: PPP y DHCP en un solo System i" en la página 37
En este ejemplo se explica cómo configurar un modelo de System i como servidor del protocolo de configuración dinámica de hosts (DHCP) para una LAN y un cliente de acceso telefónico remoto.

Elaborar un plan para DHCP

La configuración del protocolo de configuración dinámica de hosts (DHCP) puede ser un proceso lento y propenso a errores si no dedica un cierto tiempo a planificar cómo hay que configurar el servidor DHCP. Para configurar el servidor DHCP de manera más eficaz, tenga en cuenta de antemano algunas cuestiones problemáticas que plantean la configuración y la seguridad de la red.

Referencia relacionada

"Configurar DHCP" en la página 46
Aquí encontrará instrucciones para configurar el servidor y los clientes DHCP, así como para configurar DHCP para que envíe actualizaciones dinámicas al sistema de nombres de dominio (DNS).

Consideraciones sobre la seguridad

El protocolo DHCP no es capaz de verificar si los clientes que solicitan direcciones IP están autorizados para hacerlo.

Debido a la naturaleza de la interacción del servidor DHCP con la red, es importante que proteja el modelo de System i ante los clientes externos. Si el servidor DHCP está en un modelo de System i que que forma parte de una red interna de confianza, es posible que pueda utilizar el filtrado IP y la conversión de direcciones de red (NAT) para proteger aún más contra terceros no autorizados. Su el servidor DHCP está en un modelo de System i conectado a una red que no sea de confianza, como Internet, consulte el tema System i y la seguridad en Internet.

Conceptos relacionados

Filtrado IP y conversión de direcciones de red (NAT)

Seguridad

Consideraciones sobre la topología de la red

Al planificar la configuración del protocolo de configuración dinámica de hosts (DHCP), debe tener presentes varios factores, como son la topología de la red, los dispositivos de la red (por ejemplo, los direccionadores) y cómo desea dar soporte a los clientes en DHCP.

Qué es la topología de la red

Uno de los aspectos más importantes a la hora de planificar una implementación DHCP es entender el diseño o topología de la red. Una vez que haya entendido la topología de la red, podrá identificar rápidamente los rangos de direcciones IP para DHCP, la información de configuración que necesita cada cliente, los dispositivos que deben configurarse para reenviar mensajes de DHCP y si DHCP puede trabajar con los servidores DNS o PPP. En función de la complejidad de la red, podría incluso esbozar la topología de la red en un trozo de papel. Debe incluir todas las LAN, los dispositivos que conectan las LAN, y las direcciones IP de los dispositivos y clientes (por ejemplo, una impresora) que deban tener definida una dirección IP. Es posible que le interese examinar algunos de los ejemplos de DHCP que le ayudarán a esbozar la topología de su red.

Determinar el número de servidores DHCP

Incluso con una red compleja, todavía puede gestionar todos los clientes de la red utilizando un solo servidor DHCP. Dependiendo de la topología de la red, es posible que necesite configurar algunos agentes de retransmisión DHCP/BOOTP o habilitar direccionadores para reenviar paquetes DHCP para que funcione la configuración.

La utilización de un solo servidor DHCP para toda la red centralizará la gestión de la configuración de hosts para todos los clientes. Sin embargo, hay casos en los que quizás le interese utilizar varios servidores DHCP de la red.

Para mayor seguridad en caso de anomalía, puede configurar dos o más servidores DHCP que den servicio a la misma subred. Si un servidor falla, los otros pueden seguir dando servicio a la subred. Cada uno de los servidores DHCP debe poder ser accesible mediante una conexión directa a la subred o bien utilizando un agente de retransmisión DHCP/BOOTP.

Dado que dos servidores DHCP no pueden dar servicio a las mismas direcciones, las agrupaciones de direcciones definidas para una subred deben ser exclusivas entre los servidores DHCP. Por tanto, cuando se utilizan dos o más servidores DHCP para dar servicio a una determinada subred, la lista completa de direcciones de dicha subred debe dividirse entre los servidores. Por ejemplo, puede configurar un servidor con una agrupación de direcciones formada por el 70% de las direcciones disponibles de la subred y el otro servidor con una agrupación de direcciones formada por el restante 30% de las direcciones disponibles.

La utilización de varios servidores DHCP disminuye la probabilidad de tener una anomalía de acceso a la red relacionada con DHCP, pero no garantiza que no se vaya a producir. Si falla un servidor DHCP de una determinada subred, puede ocurrir que el otro servidor DHCP no pueda atender todas las peticiones de clientes nuevos que pueden, por ejemplo, agotar la limitada agrupación de direcciones disponibles del servidor.

Si está considerando la posibilidad de utilizar varios servidores DHCP, recuerde que varios servidores DHCP no pueden compartir las mismas direcciones. Si utiliza más de un servidor DHCP en la red, cada servidor debe configurarse con sus rangos propios de direcciones IP exclusivas.

Identificar las direcciones IP que el servidor DHCP debe gestionar

Mediante la topología de la red, puede documentar qué rangos de direcciones de la red desea que gestione el servidor DHCP. Debe identificar los dispositivos que tienen una dirección IP configurada manualmente (por ejemplo, la dirección IP del direccionador) que desea excluir de la agrupación de direcciones del servidor DHCP.

Además, le interesará considerar si estas direcciones las debe asignar dinámicamente el servidor DHCP o si quiere asignar direcciones IP específicas a determinados clientes. Es posible que le interese reservar una dirección específica y los parámetros de configuración para un cliente concreto de una determinada subred, como puede ser un servidor de archivos. O bien, podría correlacionar todos los clientes con una dirección IP concreta. Consulte el apartado Soporte de cliente DHCP para obtener más información sobre cómo asignar direcciones IP ya sea de forma dinámica o estática.

Determinar el tiempo de cesión de las direcciones IP

El tiempo de cesión por omisión del servidor DHCP es de 24 horas. La duración para la que se establece el tiempo de cesión en el servidor DHCP depende de varios factores. Deberá considerar cuáles son sus objetivos, los patrones de uso del centro de trabajo y los planes de servicio técnico del servidor DHCP. Si desea más información que le ayude a determinar el tiempo de cesión para los clientes DHCP, consulte el apartado Cesiones.

Dar soporte a clientes BOOTP

Si actualmente utiliza un servidor BOOTP, piense que el servidor DHCP puede sustituir al servidor BOOTP de la red con poco o ningún efecto sobre los clientes BOOTP. Dispone de tres opciones si actualmente tiene clientes BOOTP en la red.

La opción más fácil es configurar el servidor DHCP para que dé soporte a los clientes BOOTP. Cuando se utiliza DHCP para dar soporte a clientes BOOTP, cada cliente BOOTP se correlaciona básicamente con una sola dirección IP y, por tanto, dicha dirección no puede ser reutilizada por otro cliente. Sin embargo, la ventaja de utilizar DHCP en este caso es que no es necesario configurar una correlación unívoca entre clientes BOOTP y direcciones IP. El servidor DHCP seguirá asignando dinámicamente direcciones IP a los clientes BOOTP desde la agrupación de direcciones. Después de que la dirección IP se haya asignado al cliente BOOTP, queda reservada de forma permanente para que la utilice dicho cliente hasta que la reserva de la dirección se suprima explícitamente. Esta es una buena opción en caso de tener un gran número de clientes BOOTP en la red.

Otra opción consiste en migrar la configuración del servidor BOOTP al servidor DHCP. Se creará un cliente DHCP para cada cliente BOOTP incluido en la configuración del servidor BOOTP. En esta opción, se recomienda volver a configurar los clientes para que sean clientes DHCP. Sin embargo, cuando se migra la configuración de BOOTP a DHCP, las asignaciones de direcciones de DHCP funcionarán tanto para un cliente BOOTP como para un cliente DHCP. Esta podría ser una buena opción para hacer la transición de los clientes BOOTP a DHCP. Los clientes BOOTP todavía tendrán soporte durante el proceso de reconfiguración a DHCP.

En último término, podría optar por la tercera opción: cambiar cada cliente BOOTP a DHCP y configurar DHCP para que les asigne direcciones dinámicamente. En esencia, esta opción elimina totalmente BOOTP de la red.

Identificar la información de configuración para los clientes de la red

Utilizando el diseño de la topología de la red, se pueden ver claramente los dispositivos (por ejemplo, direccionadores) que deben identificarse en la configuración de DHCP. Además, debe identificar otros servidores de la red (como el servidor del sistema de nombres de dominio o DNS) de cuya existencia

tendrían que estar enterados los clientes. Puede especificar esta información para toda la red, para una subred específica o para un cliente determinado, sea cual sea la subred.

Si tiene dispositivos que afectan a muchos clientes, seguramente querrá especificarlos al nivel más alto posible (por ejemplo, a nivel global para toda la red o a nivel de subred para una determinada subred). De este modo se minimizarán los cambios que se deban realizar en la configuración de DHCP cuando cambie el dispositivo. Si, por ejemplo, ha especificado el mismo direccionador para cada cliente de la red, debe cambiar la configuración de cada cliente cuando cambie el direccionador. Sin embargo, si ha especificado el direccionador a nivel global (todos los clientes heredarán esta información de configuración), solamente necesita cambiar la información una vez y la información se cambia para todos los clientes.

Algunos de los clientes podrían tener una configuración de TCP/IP exclusiva que requiera que la información se configure a nivel de cliente. DHCP puede reconocer a dichos clientes y proporcionarles los datos de configuración exclusiva. Esto no solamente es aplicable para las opciones de configuración sino también para el tiempo de cesión y la dirección IP. Por ejemplo, un cliente podría necesitar un tiempo de cesión más largo que los demás clientes. O bien, quizás solo un cliente, como por ejemplo un servidor de archivos, necesite una dirección IP dedicada. La identificación temprana de dichos clientes y de la información exclusiva que necesitan le ayudará a la hora de empezar a configurar el servidor DHCP.

Para una consulta rápida de todas las opciones de configuración, vea el apartado “Búsqueda de opciones de DHCP” en la página 9.

Utilizar DNS dinámico con el servidor DHCP

Si actualmente utiliza un servidor DNS para gestionar todos los nombres de host y direcciones IP del cliente, sin duda deseará volver a configurar el servidor DNS para que acepte actualizaciones dinámicas de DHCP. Si utiliza DNS dinámico, los clientes no apreciarán ninguna interrupción ni ningún cambio en el servicio DNS cuando pase a DHCP. Para obtener más información sobre cómo utilizar DHCP con el servidor DNS, consulte el apartado Actualizaciones dinámicas.

Si actualmente no utiliza un servidor DNS, quizás le interese añadir un servidor DNS cuando añada el servidor DHCP. Puede leer el tema DNS de Information Center para averiguar más información sobre las ventajas y los requisitos del DNS.

Utilizar DHCP para los clientes remotos

Si tiene clientes remotos que se conectan a la red mediante PPP, puede configurar DHCP para que les asigne dinámicamente una dirección IP cuando esos clientes remotos se conecten a la red. Si desea ver algunos ejemplos donde esto podría ser de utilidad, consulte: “Ejemplo: PPP y DHCP en un solo System i” en la página 37 o “Ejemplo: DHCP y perfil PPP en distintos modelos de System i” en la página 39. Estos ejemplos también explican cómo configurar la red para la utilización conjunta de PPP y DHCP para los clientes remotos.

Conceptos relacionados

“Ejemplos: DHCP” en la página 24
Al revisar los diagramas y ejemplos sobre cómo se configuran las diferentes redes, puede determinar cuál es la mejor elección para su instalación.

“Agentes de retransmisión y direccionadores” en la página 6
Puede utilizar agentes de retransmisión y direccionadores del protocolo de configuración dinámica de hosts (DHCP) para transferir datos por toda la red de manera eficaz y segura.

“Soporte de cliente DHCP” en la página 6
Puede utilizar un servidor DHCP para gestionar individualmente cada cliente de la red, en lugar de gestionar todos los clientes como un grupo de gran tamaño (una subred).

“Cesiones” en la página 4
Cuando DHCP envía información de configuración a un cliente, la información se envía con un

tiempo de cesión. El tiempo de cesión especifica el tiempo que el cliente puede utilizar la dirección IP que le ha sido asignada. La duración del tiempo de cesión se puede cambiar de acuerdo con los requisitos específicos.

"BOOTP" en la página 7
El protocolo Bootstrap (BOOTP) es un protocolo de configuración de hosts que se utilizó antes de que se desarrollara el protocolo de configuración dinámica de hosts (DHCP). El soporte de BOOTP es un subconjunto de DHCP.

"Actualizaciones dinámicas" en la página 8
Puede configurar un servidor de protocolo de configuración dinámica de hosts (DHCP) para que funcione con un servidor de tipo sistema de nombres de dominio (DNS) para actualizar dinámicamente la información del cliente en el DNS cuando DHCP asigna una dirección IP al cliente.

Sistema de nombres de dominio (DNS)

Configurar DHCP

Aquí encontrará instrucciones para configurar el servidor y los clientes DHCP, así como para configurar DHCP para que envíe actualizaciones dinámicas al sistema de nombres de dominio (DNS).

Referencia relacionada

"Elaborar un plan para DHCP" en la página 42
La configuración del protocolo de configuración dinámica de hosts (DHCP) puede ser un proceso lento y propenso a errores si no dedica un cierto tiempo a planificar cómo hay que configurar el servidor DHCP. Para configurar el servidor DHCP de manera más eficaz, tenga en cuenta de antemano algunas cuestiones problemáticas que plantean la configuración y la seguridad de la red.

Configurar el servidor DHCP y el agente de retransmisión BOOTP/DHCP

Utilice la información que sigue para trabajar con el servidor DHCP y el agente de retransmisión BOOTP/DHCP, haciendo tareas como las de configurar, iniciar o detener el servidor DHCP o el agente de retransmisión BOOTP/DHCP.

Conceptos relacionados

"Agentes de retransmisión y direccionadores" en la página 6
Puede utilizar agentes de retransmisión y direccionadores del protocolo de configuración dinámica de hosts (DHCP) para transferir datos por toda la red de manera eficaz y segura.

Configurar o ver el servidor DHCP

Puede utilizar la función de configuración del servidor DHCP para crear una nueva configuración de DHCP o para ver la configuración de DHCP existente.

Para acceder a la configuración del servidor DHCP, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP** → **DHCP**.
2. Pulse **DHCP** con el botón derecho del ratón y luego seleccione **Configuración**.

Si está creando una nueva configuración de DHCP, un asistente le ayudará a configurar el servidor DHCP. Este asistente le hará unas preguntas básicas sobre la configuración y le guiará en el proceso de creación de una subred. Una vez que haya completado el asistente, podrá cambiar y mejorar la configuración según las necesidades de la red.

Si el servidor DHCP ya está configurado, la función de configuración del servidor DHCP mostrará la configuración actual, incluidas todas las subredes y los clientes que pueden gestionarse desde el servidor DHCP y la información de configuración que se enviará a los clientes.

Crear un acceso directo a la ventana de configuración de DHCP

Siga estos pasos si consulta a menudo la configuración de DHCP y desea crear un acceso directo a la ventana de configuración de DHCP en el escritorio.

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP** → **DHCP**.
2. Pulse **DHCP** con el botón derecho del ratón y luego seleccione **Crear acceso directo**.

Iniciar o detener el servidor DHCP

Una vez que el servidor DHCP esté configurado, siga estos pasos para iniciarlo o detenerlo.

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP** → **DHCP**.
2. Pulse **DHCP** con el botón derecho del ratón y luego seleccione **Iniciar** o **Detener**.

Configurar el servidor DHCP para que se inicie automáticamente

Si desea configurar el servidor DHCP para que se inicie automáticamente, siga estos pasos.

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP** → **DHCP**.
2. Pulse **DHCP** con el botón derecho del ratón y luego seleccione **Configuración**.
3. Pulse **Servidor DHCP** con el botón derecho del ratón y seleccione **Propiedades**.
4. Marque el recuadro de selección **Iniciar cuando se inicia TCP/IP**.
5. Pulse **Aceptar**.

Acceder al supervisor del servidor DHCP

El supervisor del servidor de protocolo de configuración dinámica de hosts (DHCP) sirve para supervisar la información de las cesiones activas de un servidor DHCP IBM System i. Esta interfaz gráfica le permite ver qué direcciones IP están cedidas, cuánto tiempo llevan cedidas y cuándo volverán a estar disponibles para ser cedidas de nuevo.

Para acceder al supervisor del servidor DHCP, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP** → **DHCP**.
2. Pulse **DHCP** con el botón derecho del ratón y luego seleccione **Supervisar**.

Configurar el agente de retransmisión BOOTP/DHCP

i5/OS proporciona un agente de retransmisión DHCP/BOOTP que sirve para reenviar paquetes DHCP a un servidor DHCP de una red distinta.

Para configurar el agente de retransmisión DHCP/BOOTP, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP** → **Agente de retransmisión BOOTP/DHCP**.
2. Pulse **Agente de retransmisión BOOTP/DHCP** con el botón derecho del ratón y luego seleccione **Configuración**.
3. Especifique la interfaz desde la que el agente de retransmisión recibirá los paquetes DHCP y el destino al que deben reenviarse los paquetes, y pulse **Aceptar**.

Iniciar o detener el agente de retransmisión BOOTP/DHCP

Una vez que el agente de retransmisión DHCP/BOOTP esté configurado, podrá iniciarlo o detenerlo, siguiendo estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP** → **Agente de retransmisión BOOTP/DHCP**.
2. Pulse **Agente de retransmisión BOOTP/DHCP** con el botón derecho del ratón y seleccione **Iniciar** o **Detener**.

Configurar el agente de retransmisión BOOTP/DHCP para que se inicie automáticamente

Si desea configurar el agente de retransmisión BOOTP/DHCP para que se inicie automáticamente cuando se inicia TCP/IP, siga estos pasos.

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP** → **Agente de retransmisión BOOTP/DHCP**.
2. Pulse **Agente de retransmisión BOOTP/DHCP** con el botón derecho del ratón y luego seleccione **Propiedades**.
3. Marque el recuadro de selección **Iniciar cuando se inicia TCP/IP** y pulse **Aceptar**.

Configurar los clientes para que utilicen DHCP

Tras configurar el servidor de protocolo de configuración dinámica de hosts (DHCP), también hay que configurar los clientes para que soliciten la información de preguntar que les corresponde al servidor DHCP.

La siguiente información describe los pasos que hay que seguir para configurar los clientes Windows para que soliciten información de configuración que les corresponde al servidor DHCP. Además, describe cómo pueden ver los clientes su propia información de cesión DHCP.

Habilitar DHCP para los clientes Windows Me

La función Protocolo de configuración dinámica de hosts (DHCP) de los clientes Windows Me se puede habilitar o inhabilitar desde una interfaz gráfica proporcionada por el sistema operativo Windows Me.

Para habilitar DHCP, siga estos pasos:

1. En el menú **Inicio**, pulse **Configuración** → **Panel de control**.
2. Pulse dos veces en **Red** y luego seleccione la pestaña **Protocolos**.
3. Seleccione **Protocolo TCP/IP** y después pulse **Propiedades**.
4. En la pestaña **Dirección IP**, pulse **Obtener una dirección IP de un servidor DHCP** y, después, **Aceptar**.

Comprobar la cesión DHCP para los clientes Windows Me:

Los clientes Windows Me tienen un programa de utilidad que muestra la información de cesión DHCP y la dirección MAC del cliente. También le permite liberar y renovar las cesiones DHCP.

Para comprobar la cesión DHCP del cliente, siga estos pasos:

1. Abra un *Indicador de mandatos de MS-DOS*.
2. Ejecute **WINIPCFG**.

Nota: Este programa de utilidad no actualiza dinámicamente la información visualizada y, por tanto, es necesario volver a ejecutar el programa de utilidad para ver el estado actualizado.

Habilitar DHCP para los clientes Windows 2000

La función Protocolo de configuración dinámica de hosts (DHCP) de los clientes Windows 2000 se puede habilitar o inhabilitar desde una interfaz gráfica proporcionada por el sistema operativo Windows 2000.

Para habilitar DHCP, siga estos pasos:

1. En el menú **Inicio**, seleccione **Configuración** → **Conexiones de red y de acceso telefónico**.
2. Pulse el nombre de la conexión pertinente con el botón derecho del ratón y seleccione **Propiedades**.
3. Seleccione **Protocolo TCP/IP** y luego seleccione **Propiedades**.
4. En la pestaña **General**, seleccione **Obtener una dirección IP de un servidor DHCP**.
5. Pulse **Aceptar**.

Comprobar la cesión DHCP y la dirección MAC:

Los clientes Windows 2000 y Windows XP tienen un programa de utilidad que muestra la información de cesión DHCP y la dirección MAC del cliente. Este programa de utilidad también le permite liberar y renovar las cesiones DHCP.

Para comprobar la cesión DHCP de un cliente Windows 2000 o Windows XP, siga estos pasos:

1. Abra una ventana Indicador de mandatos.
2. Ejecute **IPCONFIG /ALL**.

Nota: Este programa de utilidad no actualiza dinámicamente la información visualizada y, por tanto, será necesario volver a ejecutar el programa de utilidad para ver el estado actualizado. Puede utilizar el mismo programa de utilidad con distintos parámetros para liberar y renovar una cesión (IPCONFIG /RELEASE e IPCONFIG /RENEW). Ejecute IPCONFIG /? desde un indicador de mandatos de MS-DOS para ver todos los parámetros posibles del mandato.

Si desea que el servidor DHCP actualice los registros A de DNS en nombre del cliente, configure los clientes DHCP de Microsoft Windows 2000 y Windows XP. Esta configuración puede simplificar la administración de DNS, porque entonces las actualizaciones de DNS se emitirán desde el servidor DHCP para todos los clientes, en lugar de que algunos clientes actualicen sus propios registros.

Actualizar registros A de DNS:

Puede seguir estos pasos para permitir que Windows 2000 o Windows XP utilice el servidor DHCP para actualizar los registros A del DNS en nombre del cliente.

1. En el menú **Inicio**, siga una de estas series de pasos en función del entorno Windows que tenga.
   - Windows XP: seleccione **Panel de control** → **Conexiones de red**.
   - Windows 2000: seleccione **Configuración** → **Conexiones de red y de acceso telefónico**.
2. Pulse el nombre de la conexión pertinente con el botón derecho del ratón y seleccione **Propiedades**.
3. Seleccione **Protocolo TCP/IP** y, después, **Propiedades**.
4. Pulse **Valores avanzados**. En la pestaña **DNS**, no debe haber una marca de selección en el recuadro **Registrar las direcciones de esta conexión en DNS**.
5. Pulse **Aceptar** en el panel Valores avanzados de TCP/IP.
6. Pulse **Aceptar** en el panel Propiedades de protocolo de Internet (TCP/IP).
7. Pulse **Aceptar**.

Habilitar DHCP para los clientes Windows XP

Puede habilitar o inhabilitar la función Protocolo de configuración dinámica de hosts (DHCP) de los clientes Windows XP desde una interfaz gráfica proporcionada por el sistema operativo Windows XP.

Para habilitar DHCP, siga estos pasos:

1. En el menú **Inicio**, seleccione **Panel de control** → **Conexiones de red**.
2. Pulse el nombre de la conexión pertinente con el botón derecho del ratón y seleccione **Propiedades**.
3. Seleccione **Protocolo TCP/IP** y luego seleccione **Propiedades**.
4. En la pestaña **General**, seleccione **Obtener una dirección IP automáticamente**.
5. Pulse **Aceptar**.

Comprobar la cesión DHCP y la dirección MAC:

Los clientes Windows 2000 y Windows XP tienen un programa de utilidad que muestra la información de cesión DHCP y la dirección MAC del cliente. Este programa de utilidad también le permite liberar y renovar las cesiones DHCP.

Para comprobar la cesión DHCP de un cliente Windows 2000 o Windows XP, siga estos pasos:

1. Abra una ventana Indicador de mandatos.
2. Ejecute **IPCONFIG /ALL**.

Nota: Este programa de utilidad no actualiza dinámicamente la información visualizada y, por tanto, será necesario volver a ejecutar el programa de utilidad para ver el estado actualizado. Puede utilizar el mismo programa de utilidad con distintos parámetros para liberar y renovar una cesión (IPCONFIG /RELEASE e IPCONFIG /RENEW). Ejecute IPCONFIG /? desde un indicador de mandatos de MS-DOS para ver todos los parámetros posibles del mandato.

Si desea que el servidor DHCP actualice los registros A de DNS en nombre del cliente, configure los clientes DHCP de Microsoft Windows 2000 y Windows XP. Esta configuración puede simplificar la administración de DNS, porque entonces las actualizaciones de DNS se emitirán desde el servidor DHCP para todos los clientes, en lugar de que algunos clientes actualicen sus propios registros.

Actualizar registros A de DNS:

Puede seguir estos pasos para permitir que Windows 2000 o Windows XP utilice el servidor DHCP para actualizar los registros A del DNS en nombre del cliente.

1. En el menú **Inicio**, siga una de estas series de pasos en función del entorno Windows que tenga.
   - Windows XP: seleccione **Panel de control** → **Conexiones de red**.
   - Windows 2000: seleccione **Configuración** → **Conexiones de red y de acceso telefónico**.
2. Pulse el nombre de la conexión pertinente con el botón derecho del ratón y seleccione **Propiedades**.
3. Seleccione **Protocolo TCP/IP** y, después, **Propiedades**.
4. Pulse **Valores avanzados**. En la pestaña **DNS**, no debe haber una marca de selección en el recuadro **Registrar las direcciones de esta conexión en DNS**.
5. Pulse **Aceptar** en el panel Valores avanzados de TCP/IP.
6. Pulse **Aceptar** en el panel Propiedades de protocolo de Internet (TCP/IP).
7. Pulse **Aceptar**.

Configurar DHCP para que envíe actualizaciones dinámicas al DNS

Se puede configurar el servidor de protocolo de configuración dinámica de hosts (DHCP) para que envíe peticiones de actualización al servidor DNS cada vez que DHCP asigne una nueva dirección a un host. Este proceso automatizado reduce la administración del servidor DNS en redes TCP/IP que crecen o cambian rápidamente y en redes donde los hosts cambian a menudo de ubicación.

Cuando un cliente que utiliza DHCP recibe una dirección IP, dichos datos se envían inmediatamente al servidor DNS. Gracias a este método, el DNS puede seguir resolviendo satisfactoriamente las peticiones de hosts, incluso cuando cambian las direcciones IP.

Para que se produzcan las actualizaciones de registros, el sistema de nombres de dominio (opción 31 de i5/OS) debe estar instalado en este servidor. El servidor DHCP utiliza interfaces de programación que proporciona la Opción 31 para realizar actualizaciones dinámicas. El servidor DNS se puede ejecutar en un modelo de System i aparte que sea capaz de realizar actualizaciones dinámicas. Si desea información sobre cómo verificar que la opción 31 está instalada, consulte: Requisitos del sistema DNS.

Para configurar las propiedades de DHCP que permiten al servidor DHCP realizar actualizaciones de DNS dinámicas, siga estos pasos:

1. Expanda **Red** → **Servidores** → **TCP/IP**.
2. En el panel derecho, pulse **DHCP** con el botón derecho del ratón y seleccione **Configuración**.
3. En el panel izquierdo de la ventana Configuración del servidor DHCP, pulse **Global** con el botón derecho del ratón y seleccione **Propiedades**.
4. Seleccione la pestaña **Opciones**.

5. Seleccione **opción 15: Nombre de dominio** en la lista **Opciones seleccionadas**. Si la opción 15 no aparece en la lista **Opciones seleccionadas**, seleccione 15: Nombre de dominio en la lista **Opciones disponibles** y pulse **Añadir**.
6. En el campo **Nombre de dominio**, especifique el nombre de dominio que el cliente utiliza para resolver nombres de host mediante el DNS.
7. Seleccione la pestaña **DNS dinámico**.
8. Seleccione **El servidor DHCP actualiza los registros A y los registros PTR** o bien **El servidor DHCP actualiza solamente los registros PTR**.
9. Establezca que **Añadir nombre de dominio a nombre de host** sea igual a **Sí**.
10. Pulse **Aceptar** para cerrar la página de propiedades globales.

Conceptos relacionados

"Actualizaciones dinámicas" en la página 8
Puede configurar un servidor de protocolo de configuración dinámica de hosts (DHCP) para que funcione con un servidor de tipo sistema de nombres de dominio (DNS) para actualizar dinámicamente la información del cliente en el DNS cuando DHCP asigna una dirección IP al cliente.

Inhabilitar las actualizaciones dinámicas del DNS

Si inhabilita la función de actualizaciones dinámicas del sistema de nombres de dominio (DNS), la responsabilidad de gestionar el servidor DNS recae en el administrador. Puede ser conveniente inhabilitar las actualizaciones dinámicas de DNS en aquellas redes en las que los hosts cambian de ubicación en contadas ocasiones, en las que el crecimiento y el cambio son poco frecuentes, y en las que se necesita una administración más estricta del servidor DNS.

Para inhabilitar las actualizaciones dinámicas de DNS desde el cliente, siga estos pasos:

1. En el menú **Inicio**, seleccione **Configuración → Conexiones de red y de acceso telefónico**.
2. Pulse el nombre de la conexión pertinente con el botón derecho del ratón y seleccione **Propiedades**.
3. Seleccione **Protocolo TCP/IP** y luego seleccione **Propiedades**.
4. Seleccione **Avanzadas**.
5. En la pestaña **DNS**, deseleccione las opciones ″Registrar las direcciones de esta conexión en DNS″ y ″Utilizar el sufijo DNS de esta conexión al registrar DNS″.
6. Pulse **Aceptar**.

Siga estos pasos para todas las conexiones en las que desee delegar la actualización de los registros de DNS al servidor DHCP.

Gestionar direcciones IP cedidas

Puede utilizar la herramienta de configuración de DHCP para especificar la agrupación de direcciones IP que gestiona DHCP y los tiempos de cesión de dichas agrupaciones de direcciones. Puede utilizar el supervisor del servidor DHCP para ver qué direcciones IP están cedidas en este momento.

El supervisor del servidor DHCP sirva para supervisar la información de las cesiones activas de un servidor DHCP de System i. Esta interfaz gráfica le permite ver qué direcciones IP están cedidas, cuánto tiempo llevan cedidas y cuándo volverán a estar disponibles para ser cedidas de nuevo.

También puede utilizar el supervisor del servidor DHCP para reclamar las direcciones IP que ya no se utilizan. Si la agrupación de direcciones DHCP se ha agotado, puede examinar la información de las cesiones activas. Utilice la información de cesiones activas para determinar si puede suprimir cesiones para que las direcciones IP estén disponibles para otros clientes. Por ejemplo, podría haber un cliente que ya no esté en la red pero que todavía tiene una cesión de dirección IP activa. Puede suprimir la cesión de dirección IP activa de dicho cliente. Solo puede realizar esta operación si tiene la seguridad de que el cliente ya no intentará utilizar la dirección. El servidor DHCP no notifica a los clientes cuando se suprime

la cesión de dirección IP activa. Si suprime una cesión activa de un cliente que todavía esté en la red sin liberar la dirección IP del cliente, podría acabar teniendo asignaciones de direcciones IP duplicadas en la red.

Conceptos relacionados

"Problema: asignaciones de direcciones IP duplicadas en la misma red" en la página 53
La dirección IP debe ser exclusiva en toda la red. El servidor de protocolo de configuración dinámica de hosts (DHCP) no puede asignar una misma dirección IP a más de un cliente.

Resolución de problemas relacionados con DHCP

Siga estas directrices cuando resuelva problemas relacionados con DHCP.

Si su problema no aparece aquí, consulte el tema "Elaborar un plan para DHCP" en la página 42 para verificar que ha tenido en cuenta todos los aspectos a la hora de configurar DHCP.

Seleccione la descripción de un problema en la lista siguiente, o bien lea el tema Reunir información de error detallada de DHCP para ver las instrucciones sobre cómo acceder a los datos de las anotaciones del servidor y a la información de rastreo.

Referencia relacionada

Utilizar el rastreo de comunicaciones para resolver problemas de comunicación

Reunir información de error detallada de DHCP

Existen dos formas de averiguar los detalles de error del problema que ha encontrado.

En primer lugar, mire en las anotaciones de trabajo del servidor DHCP, siguiendo estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP** → **DHCP**.
2. Pulse **DHCP** con el botón derecho del ratón y luego seleccione **Trabajos servidores**.

Si no hay ningún mensaje en las anotaciones de trabajo del servidor DHCP, podría ser necesario recoger la información a partir del rastreo de comunicaciones de System i o a partir del rastreo interno del programa del servidor DHCP. El rastreo de comunicaciones ayuda a determinar si las peticiones de cliente llegan al servidor DHCP y si el servidor DHCP responde al cliente. Si las peticiones de cliente llegan al servidor DHCP, pero el servidor no responde, utilice la función de rastreo interno del programa del servidor DHCP.

Rastrear el servidor DHCP

El archivo de anotaciones de DHCP sirve para registrar la información de anotaciones del servidor DHCP. Conviene que consulte el archivo de anotaciones de DHCP para poder localizar el problema y conocer las razones que lo provocaron.

Para rastrear el servidor DHCP, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP** → **DHCP**.
2. Pulse **DHCP** con el botón derecho del ratón y luego seleccione **Configuración**.
3. Pulse **Servidor DHCP** con el botón derecho del ratón y seleccione **Propiedades**.
4. Seleccione la pestaña de propiedades **Anotaciones**.
5. Marque el recuadro de selección **Habilitar anotaciones**.
6. Verifique que el **Nombre de archivo de anotaciones** es **dhcpsd.log**.
7. Seleccione todas las categorías de **Anotaciones** excepto Rastreo y Estadísticas (las anotaciones de rastreo y estadísticas solo las utiliza la línea de soporte).
8. Pulse **Aceptar**.
9. Pulse **Servidor DHCP** con el botón derecho del ratón y seleccione **Actualizar servidor** para reiniciar el servidor DHCP si el servidor ya está iniciado.

10. Reproduzca el problema.
11. Pulse **Servidor DHCP** con el botón derecho del ratón y luego seleccione **Propiedades** → **Anotaciones**.
12. Deseleccione **Habilitar anotaciones** para desactivar las anotaciones.
13. Pulse **Aceptar**.
14. Pulse **Servidor DHCP** con el botón derecho del ratón y luego seleccione **Actualizar servidor** para reiniciar el servidor DHCP.
15. Vea el archivo de anotaciones de DHCP, que está en QIBM/UserData/OS400/DHCP/dhcpsd.log. Realice uno de estos pasos:
    - En System i Navigator, expanda ***su sistema*** → **Sistemas de archivos** → **Sistema de archivos integrado** → **Root** → ***el directorio del archivo***.
    - En una interfaz basada en caracteres, utilice el mandato Trabajar con enlaces de objeto (WRKLNK) y seleccione la opción 5 (Visualizar).

Problema: los clientes no reciben una dirección IP ni la información de configuración

Podrían producirse problemas si los clientes no pueden recibir una dirección IP ni la información de configuración. La dirección IP se cede a un cliente mediante un proceso de cuatro pasos entre el cliente y el servidor de protocolo de configuración dinámica de hosts (DHCP).

Los cuatro pasos deben realizarse antes de que el cliente reciba una dirección IP. Los detalles del proceso de cuatro pasos están en el tema: "Interacción cliente/servidor DHCP" en la página 1.

Las causas más habituales de este problema son:

El cliente está conectado a una subred que no está configurada en el servidor DHCP.
Compruebe la configuración de DHCP y verifique que todas las subredes que gestiona el servidor DHCP están incluidas en la configuración. Si no está seguro acerca de qué subredes debe gestionar el servidor DHCP, consulte: "Consideraciones sobre la topología de la red" en la página 43.

El mensaje DHCPDISCOVER del cliente no llega al servidor DHCP.
Si el servidor DHCP no tiene una dirección IP en la subred del cliente, debe haber un direccionador o agente de retransmisión DHCP/BOOTP que pueda reenviar el mensaje DHCPDISCOVER del cliente al servidor DHCP. Hallará más información en: "Agentes de retransmisión y direccionadores" en la página 6. Además de recibir el mensaje de difusión, el servidor debe poder enviar paquetes de respuesta a la subred del cliente.

Si el modelo de System i es de multiubicación, tal vez deba añadir un grupo de subred a la configuración de DHCP. Si desea más detalles sobre cómo configurar DHCP para un sistema multiubicación, vea: "Ejemplo: DHCP y multiubicación" en la página 29. En este ejemplo describe lo que se debe hacer en la configuración de DHCP para que el sistema reciba el mensaje de difusión del cliente.

El servidor DHCP no tiene direcciones disponibles para el cliente en la agrupación de direcciones.
Puede utilizar el supervisor del servidor DHCP para ver qué direcciones utiliza actualmente el servidor DHCP. "Gestionar direcciones IP cedidas" en la página 51 proporciona más detalles sobre cómo utilizar el supervisor del servidor DHCP. Si el servidor DHCP ha agotado las direcciones disponibles, deberá añadir más direcciones IP a la agrupación de agrupaciones, acortar el tiempo de cesión o suprimir las cesiones permanentes que ya no se necesitan.

Problema: asignaciones de direcciones IP duplicadas en la misma red

La dirección IP debe ser exclusiva en toda la red. El servidor de protocolo de configuración dinámica de hosts (DHCP) no puede asignar una misma dirección IP a más de un cliente.

En determinados casos, el servidor DHCP intentará verificar que una dirección actualmente no está en uso antes de asignarla a un cliente. Cuando el servidor DHCP detecta que una dirección está siendo utilizada y no debería ser así, marca temporalmente esa dirección como utilizada y no la asigna a ningún cliente. Puede utilizar el supervisor del servidor DHCP para ver las direcciones IP que el servidor ha detectado que están en uso, pero que no han sido asignadas por el servidor DHCP. Estas direcciones tendrán el estado USED y el identificador de cliente UNKNOWN_TO_IBMDHCP.

Las causas más habituales de este problema son:

Varios servidores DHCP están configurados para asignar la misma dirección IP.
Si dos servidores DHCP están configurados para asignar la misma dirección IP a clientes, entonces es posible que dos clientes distintos reciban la misma dirección IP. Uno de los clientes recibe la dirección IP de uno de los servidores DHCP y el otro cliente recibe la misma dirección IP del otro servidor DHCP. Puede haber múltiples servidores DHCP que sirvan la misma subred o la misma red, pero no deben estar configurados con la misma agrupación de direcciones o con agrupaciones de direcciones solapadas.

Un cliente se ha configurado manualmente con una dirección IP que está gestionada por DHCP.
El servidor DHCP normalmente intenta verificar si una dirección IP está actualmente en uso antes de asignarla a un cliente. Sin embargo, no hay ninguna garantía de que el cliente configurado manualmente esté actualmente conectado a la red o pueda responder cuando el servidor DHCP verifique la dirección IP. Por tanto, el servidor DHCP podría asignar la dirección IP a un cliente DHCP. Cuando el cliente configurado manualmente se conecta a la red, habrá direcciones IP duplicadas en la red. Las direcciones IP que están gestionadas por DHCP no deben utilizarse para configurar manualmente un cliente de la red. Si un cliente debe configurarse manualmente con una dirección IP, esa dirección IP debe excluirse de la agrupación de direcciones del servidor DHCP.

Conceptos relacionados

"Gestionar direcciones IP cedidas" en la página 51
Puede utilizar la herramienta de configuración de DHCP para especificar la agrupación de direcciones IP que gestiona DHCP y los tiempos de cesión de dichas agrupaciones de direcciones. Puede utilizar el supervisor del servidor DHCP para ver qué direcciones IP están cedidas en este momento.

Problema: DHCP no actualiza los registros de DNS

El servidor DHCP de System i es capaz de actualizar dinámicamente los registros de recursos del DNS. El servidor DHCP utiliza funciones de resolución de nombres e interfaces de programación para determinar el servidor DNS dinámico apropiado que debe actualizarse. Puede utilizar esta información al resolver errores de actualización dinámica.

Verifique los puntos siguientes cuando los registros del DNS no se actualizan dinámicamente.

Verifique qué subredes y qué tipo de registros de recursos (registros A y/o PTR) se están actualizando.
Compruebe la configuración de DHCP y verifique que la subred del cliente está configurada para actualizar dinámicamente registros de recursos y qué tipo de registro se está actualizando.

Verifique que el sistema de nombres de dominio (DNS) de i5/OS (Opción 31) está instalado en el modelo de System i que ejecuta DHCP.
El servidor DHCP utiliza interfaces de programación proporcionadas por el dispositivo Sistema de nombres de dominio (DNS) de i5/OS, Opción 31. No es necesario que el DNS que se actualiza dinámicamente resida en el mismo sistema que el servidor DHCP.

Verifique que el servidor DHCP está autorizado para enviar actualizaciones al servidor DNS.
Compruebe la configuración del DNS para verificar que la zona del DNS está configurada para permitir actualizaciones dinámicas y que el servidor DHCP está incluido en la Lista de control de accesos.

Verifique que los servidores DNS pueden resolver el dominio del cliente.
Visualice la lista de servidores DNS del modelo de System i en el que reside DHCP, utilizando

para ello el mandato Cambiar dominio de TCP/IP (CHGTCPDMN). Verifique que estos servidores DNS pueden resolver el dominio que se está actualizando. Para ello, ejecute la herramienta Búsqueda de servidor de nombres (NSLOOKUP) desde el modelo de System i en el que se ejecuta DHCP para resolver un nombre (o una dirección IP) del dominio que no se puede actualizar El servidor DHCP debe poder obtener el nombre de dominio totalmente calificado (FQDN) del cliente para actualizar su registro del DNS. El servidor DHCP no intentará actualizar un DNS dinámico sin un FQDN (el nombre de host y nombre de dominio del cliente). El servidor DHCP obtiene el FQDN del cliente utilizando la siguiente secuencia:

1. Opción 81 (FQDN del cliente) en el mensaje DHCPREQUEST del cliente.
2. Opción 12 (Nombre de host) y/o la Opción 15 (Nombre de dominio) en el mensaje DHCPREQUEST del cliente.
3. Opción 12 (Nombre de host) en el mensaje DHCPREQUEST del cliente y/o la Opción 15 (Nombre de dominio) configurada en el servidor DHCP. En este caso, para obtener el FQDN, el servidor DHCP debe estar configurado para añadir el nombre de dominio al nombre de host (especificado en la pestaña **Propiedades → DNS dinámico** para el nivel global, subred, clase o cliente).

El registro TXT podría no coincidir con el correspondiente registro de DNS.

El servidor DHCP puede configurarse para comprobar los registros de recursos de DNS existentes y determinar a qué cliente DHCP están asociados. El servidor DHCP lo lleva a cabo escribiendo un registro TXT para cada registro A y PTR que actualiza en el DNS. Si el sistema está configurado para verificar el ID de cliente antes de llevar a cabo la actualización de DNS, entonces los datos del registro TXT deben coincidir con el ID del cliente que ha recibido la dirección del servidor DHCP. Si no coinciden, el servidor DHCP no actualiza el registro de recursos A de DNS. Así se impide que se puedan sobrescribir registros existentes. Sin embargo, el servidor DHCP se puede configurar para que ignore los registros existentes y realice actualizaciones de DNS independientemente de los datos del registro TXT (especificados en la pestaña **Propiedades → DNS dinámico** para el nivel, subred, clase o cliente global).

Conceptos relacionados

"Actualizaciones dinámicas" en la página 8
Puede configurar un servidor de protocolo de configuración dinámica de hosts (DHCP) para que funcione con un servidor de tipo sistema de nombres de dominio (DNS) para actualizar dinámicamente la información del cliente en el DNS cuando DHCP asigna una dirección IP al cliente.

Problema: las anotaciones de trabajo de DHCP tienen mensajes DNS030B cuyo código de error es 3447

El código de error 3447 significa que el servidor de protocolo de configuración dinámica de hosts (DHCP) ha agotado el tiempo de espera para una respuesta del servidor del sistema de nombres de dominio (DNS). Esto podría deberse a problemas de red o de conexión entre el servidor DHCP de System i y el servidor DNS.

Este mensaje irá acompañado de un mensaje TCP5763 que contiene el tipo de registro de recurso de DNS y los datos detallados del registro de recurso que el servidor DHCP intentaba actualizar.

Dado que el servidor DHCP intenta actualizar los registros de recursos de DNS cada vez que se renueva una cesión, es posible que los registros de recursos ya estén presentes en el archivo de configuración de zona desde la cesión inicial de la dirección IP o una renovación anterior de la cesión. Compruebe los datos de configuración de zona de DNS utilizando una herramienta como, por ejemplo, NSLOOKUP. Podría ocurrir que el registro de recurso ya esté presente con los datos correctos y no sea necesario realizar ninguna acción.

Si el registro de recurso no está presente en el DNS, hay varias formas de actualizar el registro de recurso. El servidor DHCP intenta actualizar el registro de recurso durante la siguiente petición de renovación de la cesión. Por tanto, puede esperar hasta que esto ocurra. O bien, muchos clientes intentan

renovar o readquirir una dirección IP cuando se encienden. Podría intentar reiniciar el cliente para que el servidor DHCP intente actualizar de nuevo los registros de recursos de DNS.

Si ninguna de estas opciones funciona, puede actualizar manualmente los registros de recursos de DNS. No se recomienda utilizar este método porque la zona dinámica no debe estar en ejecución cuando se realizan actualizaciones manuales. Por tanto, se pierden otras actualizaciones dinámicas del servidor DHCP durante este tiempo de inactividad. Sin embargo, puede utilizar las utilidades de actualización dinámica proporcionadas por algunas implementaciones de servidor DNS BIND y de cliente para actualizar el registro de recurso. Aunque tienen un proceso similar a la actualización manual de la zona (un administrador debe entrar los datos del registro de recurso que se debe actualizar), las utilidades de actualización dinámica permiten actualizar la zona mientras esta está activa.

Información relacionada con DHCP

Publicaciones IBM Redbooks y sitios Web que contienen información relacionada con el temario DHCP. Puede ver o imprimir cualquiera de los archivos PDF.

IBM Redbooks

AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support  (5181 KB)

Esta publicación IBM Redbooks describe el soporte para el servidor de sistema de nombres de dominio (DNS) y para el servidor de protocolo de configuración dinámica de hosts (DHCP) que está incluido en i5/OS. La información de esta publicación Redbooks le ayudará a instalar, adaptar, configurar y resolver problemas relacionados con el soporte de DNS y DHCP mediante ejemplos.

Peticiones RFC de DHCP

Las peticiones de comentarios (RFC) son definiciones escritas de los estándares de protocolos y estándares propuestos que se utilizan para Internet. Las siguientes RFC pueden ayudarle a entender DHCP y las funciones relacionadas:

- RFC 2131: Dynamic Host Configuration Protocol (reemplaza a la RFC 1541)
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 951: The Bootstrap Protocol (BOOTP)
- RFC 1534: Interoperation Between DHCP and BOOTP
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC 2136: Dynamic Updates in the Domain Name System (DNS UPDATE)

Referencia relacionada

"Archivo PDF de DHCP" en la página 1
Puede ver e imprimir un archivo PDF de esta información.

Apéndice. Avisos

Esta información se ha escrito para productos y servicios ofrecidos en los EE.UU.

Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte al representante de IBM local acerca de los productos y servicios disponibles actualmente en su zona. Las referencias a productos, programas o servicios IBM no pretender afirmar ni implican que únicamente puedan utilizarse dichos productos, programas o servicios IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran los temas descritos en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Para consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe las consultas, por escrito, a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106-0032, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país en que dichas disposiciones entren en contradicción con las leyes locales: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUYENDO, PERO NO LIMITÁNDOSE, A LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícitas ni explícitas, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información incluida en este documento; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en el producto(s) y/o el programa(s) descritos en esta publicación en cualquier momento y sin previo aviso.

Cualquier referencia hecha en esta información a sitios Web no de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno como promoción de esos sitios Web. Los materiales de estos sitios Web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios Web es de la entera responsabilidad del usuario.

IBM puede utilizar o distribuir la información que proporcione de la manera que crea más oportuna sin incurrir en ningún tipo de obligación hacia usted.

Los licenciatarios de este programa que deseen obtener información acerca de él para: (i) intercambiar la información entre programas creados independientemente y otros programas (incluido este) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
Estados Unidos

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluyendo en algunos casos el pago de una tarifa.

El programa bajo licencia descrito en este documento, así como todo el material bajo licencia disponible para él, lo proporciona IBM según los términos del Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programas bajo Licencia de IBM, el Acuerdo de Licencia para Código de Máquina de IBM o cualquier otro acuerdo equivalente entre ambas partes.

Los datos de rendimiento contenidos en esta documentación se han determinado en un entorno controlado. Por tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Algunas de las mediciones pueden haberse efectuado en sistemas a nivel de desarrollo, y no existe garantía alguna de que dichas mediciones sean las mismas en sistemas disponibles a nivel general. Además, algunas mediciones pueden haberse estimado por extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado estos productos y no puede confirmar la exactitud del rendimiento, de la compatibilidad ni de ninguna otra afirmación relacionada con productos no IBM. Las cuestiones relativas a las capacidades de productos no IBM deben dirigirse a los proveedores de dichos productos.

Todas las declaraciones relativas a la dirección o intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de muestra en el lenguaje fuente, que ilustran técnicas de programación en varias plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin pagar nada a IBM, bajo el propósito de desarrollo, uso, márketing o distribución de programas de aplicación de acuerdo con la interfaz de programación de la aplicación para la plataforma operativa para la cual se han escrito los programas de ejemplo. Estos ejemplos no se han verificado a fondo bajo todas las condiciones. IBM, por lo tanto, no puede garantizar ni dar por supuesta la fiabilidad, la posibilidad de servicio, ni el funcionamiento de estos programas.

Cada copia o cada parte de los programas de ejemplo o de los trabajos que se deriven de ellos debe incluir un aviso de copyright como se indica a continuación:

© (nombre de empresa) (año). Algunas partes de este código proceden de los programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o los años_. Reservados todos los derechos.

Si está visualizando esta copia software de información, es posible que las fotografías y las ilustraciones en color no aparezcan.

Información de la interfaz de programación

Esta publicación de DHCP facilita información sobre las interfaces de programación previstas que permiten al cliente escribir programas para obtener los servicios de IBM i5/OS.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:

AS/400
i5/OS
IBM
IBM (logotipo)
Redbooks
System i

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Los demás nombres de compañías, productos o servicios pueden ser marcas registradas o de servicio de terceros.

Términos y condiciones

Los permisos para utilizar estas publicaciones están sujetos a los siguientes términos y condiciones.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Aparte de la autorización que se concede explícitamente en este permiso, no se otorga ningún otro permiso, licencia ni derecho, ya sea explícito o implícito, sobre las publicaciones, la información, los datos, el software o cualquier otra propiedad intelectual contenida en ellas.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer de IBM, las publicaciones se utilicen en detrimento de sus intereses o cuando, también según el parecer de IBM, no se sigan debidamente las instrucciones anteriores.

No puede descargar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍA DE

NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.

Impreso en España