IBM

eserver

iSeries

Direccionamiento y equilibrado de la carga de trabajo TCP/IP

Versión 5 Release 3

IBM

@server

iSeries

Direccionamiento y equilibrado de la carga de trabajo TCP/IP

Versión 5 Release 3

Nota

Antes de utilizar esta información y el producto al que da soporte, asegúrese de leer la información en la sección “Avisos”, en la página 27.

Quinta edición (agosto de 2005)

Esta edición se aplica a la versión 5, release 3, modificación 0 de IBM Operating System/400 (número de producto 5722-SS1) y a todos los releases y modificaciones subsiguientes 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

Direccionamiento y equilibrado de la carga de trabajo TCP/IP

¿Está buscando una forma mejor de direccionar y equilibrar el tráfico TCP/IP del servidor iSeries? El servidor iSeries puede servir para muchas cosas, pero también conviene que sepa que sus posibilidades integradas de direccionamiento, gracias a la conexión de redes TCP/IP, pueden eliminar la necesidad de tener un direccionador externo.

Los métodos de direccionamiento y carga de trabajo, así como la información preparatoria, le ayudarán a comprender en qué consisten las opciones que podrá tener en el servidor iSeries. Los métodos están descritos por medio de una ilustración, lo que permite ver cómo se realizan las conexiones. No se han incluido las instrucciones de configuración de las técnicas de direccionamiento. Estas páginas se centran en los conceptos y principios de direccionamiento que debe conocer para que el servidor iSeries trabaje mejor para usted.

¿Por qué son importantes estos métodos?

Las técnicas de estos métodos pueden reducir el coste general de las conexiones porque pueden utilizarse menos servidores y direccionadores externos. Gracias a la utilización de estos métodos de direccionamiento, podrá dejar libres algunas direcciones IP, ya que aprenderá a gestionarlas con más efectividad. Si lee los apartados dedicados a los métodos de equilibrado de la carga de trabajo, conseguirá una mejora del rendimiento general del servidor iSeries al equilibrar la carga del trabajo de comunicaciones en el sistema.

¿Y si quiero imprimir estas páginas?

Puede imprimir este tema y leerlo como si se tratase de un solo documento. Basta con que siga las instrucciones que se dan en “Imprimir este tema” en la página 2.

Antes de empezar

Si es usted nuevo en el terreno del direccionamiento y el equilibrado de la carga de trabajo en el servidor iSeries, quizá le interese consultar las páginas siguientes antes de estudiar los métodos:

En “Funciones de direccionamiento TCP/IP por release” en la página 2 hallará información sobre las funciones de direccionamiento disponibles en cada una de las versiones y releases del servidor iSeries; así sabrá qué funciones tiene a su disposición.

En “**Proceso de paquetes**” en la página 2 se explica cómo procesa el servidor iSeries un paquete de información.

En “Reglas generales de direccionamiento” en la página 4 se dan algunas reglas básicas de direccionamiento del servidor iSeries. Tenga presentes estas reglas mientras lee los apartados dedicados a los métodos de direccionamiento.

¿Cómo sabré qué método debo utilizar?

Tiene a su disposición muchos métodos diferentes. Puede tomar las decisiones que estime oportunas y aplicar los métodos de la manera que considere mejor para la situación en la que se encuentra la red:

En “**Métodos de conectividad de direccionamiento**” en la página 4 se explica con detenimiento la manera en que el servidor iSeries puede direccionar los datos.

En “**Métodos de equilibrado de la carga de trabajo TCP/IP**” en la página 21 se explica en qué consisten las distintas técnicas TCP/IP que pueden utilizarse para equilibrar la carga del trabajo de comunicaciones en el servidor iSeries.

¿Desea más información sobre el direccionamiento TCP/IP del servidor iSeries

En “Otras fuentes de información sobre direccionamiento y equilibrado de la carga de trabajo TCP/IP” en la página 26 hallará información adicional de consulta en relación con el direccionamiento y el equilibrado de la carga TCP/IP.

Imprimir este tema

Existe una versión PDF de este documento que puede ver o bajar si desea imprimirlo. Para poder ver archivos PDF, debe tener instalado el programa Adobe(R) Acrobat(R) Reader. Puede bajar una copia del sitio Web de Adobe Acrobat. 

Para visualizar o bajar la versión PDF, seleccione Direccionamiento y equilibrado de carga de trabajo (aproximadamente 719 KB).

Para guardar un archivo PDF en la estación de trabajo para poder verlo o imprimirlo:

1. Abra el archivo PDF en el navegador (pulse en el enlace anterior).
2. En el menú del navegador, pulse **Archivo**.
3. Pulse **Guardar como**.
4. Navegue hasta el directorio en el que desea guardar el archivo PDF.
5. Pulse **Guardar**.

Funciones de direccionamiento TCP/IP por release

En la lista siguiente figuran las funciones soportadas por cada uno de los releases del servidor iSeries. Antes de planificar la utilización de una función, consulte esta lista con el fin de asegurarse de que el sistema tiene instalado el release correcto para dar soporte a dicha función. En algunos casos, no obstante, se puede utilizar un enfoque diferente para conseguir el mismo resultado.

V3R1: se introduce el reenvío de paquetes basado en rutas estáticas.

V3R7/V3R2: protocolo Internet de línea serie (SLIP), direccionamiento de protocolo de resolución de direcciones (ARP) por proxy y soporte de red de conexión no numerada.

V4R1: protocolo de información de direccionamiento (RIP) dinámico Versión 1 (RIPv1).

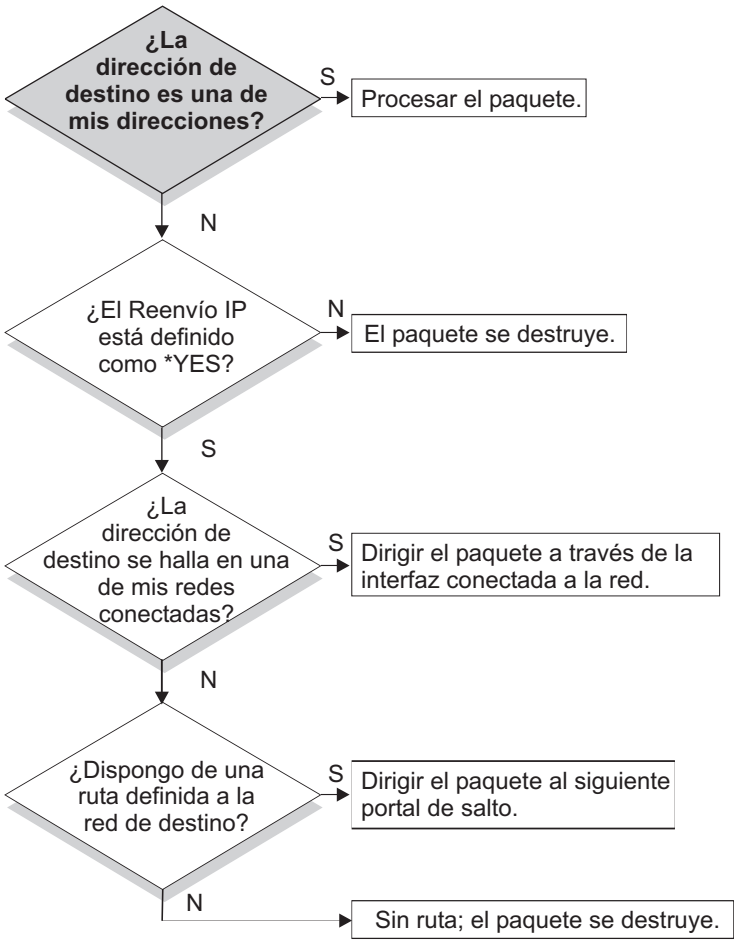
V4R2: protocolo de información de direccionamiento (RIP) dinámico Versión 2 (RIPv2), subredes transparentes y equilibrado de carga basado en rutas duplicadas.

V4R3: direcciones de IP virtual, enmascaramiento de direcciones IP, conversión de direcciones de red (NAT) y direccionamiento interdominio sin clase (CIDR).

V4R4: IP sobre OptiConnect.

Proceso de paquetes

Saber en qué consiste el proceso de paquetes sirve de ayuda a la hora de decidir la manera de implementar las funciones de direccionamiento. En el diagrama de flujo simplificado que aparece más abajo puede verse el proceso lógico que se desarrolla cuando un paquete IP (datagrama) llega al servidor iSeries. El flujo real puede ser diferente, pero el resultado final es el mismo. La lógica utilizada a continuación sirve únicamente para describir casos de proceso por omisión de paquetes. Si se emplean técnicas avanzadas de direccionamiento, el proceso de paquetes puede ser ligeramente distinto.



RZAJW523-0

En primer lugar, se compara la dirección destino que figura en la cabecera IP con todas las direcciones definidas del sistema. Si se determina que el paquete va dirigido al sistema, se pasa el paquete a un software de nivel superior dentro de la pila IP, como por ejemplo TCP, y después a la aplicación que está a la escucha en el puerto destino.

Si no se acepta el paquete localmente, la siguiente comprobación que se realiza es la del atributo de reenvío IP. Si está establecido en *YES, significa que el sistema está configurado para reenviar paquetes como si fuese un direccionador. Si está establecido en *NO dentro de los atributos TCP/IP o dentro del perfil PPP, se destruye el paquete.

Se compara la dirección destino del paquete con todas las rutas *DIRECT que conoce el sistema. Para ello, se incluye la dirección destino del paquete con la máscara de subred especificada en las entradas de direccionamiento *DIRECT de las interfaces definidas con el fin de determinar si el paquete va dirigido a una red que esté conectada directamente al sistema. La comprobación se efectúa empezando por las rutas más concretas y acabando por las menos concretas.

A continuación, si el servidor iSeries no está conectado directamente al sistema principal remoto, se lleva a cabo una búsqueda en la tabla de direccionamiento. Una vez más, esta operación se realiza empezando por la ruta de sistema principal más concreta (máscara de subred 255.255.255.255) y acabando por la ruta diferente menos concreta (máscara de subred 0.0.0.0). Si se encuentra una ruta, se reenvía el paquete a la pasarela de salto siguiente.

El último punto del diagrama de flujo muestra que si no se encuentra ninguna entrada de direccionamiento coincidente, se destruye el paquete.

Reglas generales de direccionamiento

En este apartado se presentan algunas de las reglas básicas que rigen para TCP/IP en general y para TCP/IP en el servidor iSeries. Debe tenerlas presentes cuando implemente las funciones de direccionamiento en el servidor iSeries. Le servirán de ayuda para determinar qué es lo que les ocurre a los paquetes en el sistema y adónde van a parar. Como sucede con la mayoría de las reglas, hay excepciones.

1. El sistema no tiene dirección IP; solo las interfaces tienen direcciones IP.

   La excepción a esta regla son las direcciones del protocolo Internet virtual (sin conexión), las cuales se asignan al sistema. El protocolo Internet (IP) virtual está disponible a partir de la versión V4R3 inclusive.

2. En general, si la dirección IP destino está definida en el sistema, este la procesará con independencia de a qué interfaz llegue el paquete.

   La excepción en este caso es que si la dirección está asociada con una interfaz no numerada, o si están activos el filtrado o la NAT IP, el paquete puede reenviarse o descartarse.

3. La dirección IP y la máscara definen la dirección de la red conectada.

4. La ruta de salida de un sistema se selecciona tomando como base la dirección de red que esté conectada a una interfaz. La ruta seleccionada está basada en los elementos siguientes:
   - El orden de búsqueda de grupos de rutas: las rutas directas, las rutas de subred y, por último, las rutas por omisión.
   - Dentro de un grupo, se elige la ruta que tenga la máscara de subred más concreta.
   - Si dos rutas son igual de concretas, se aplican técnicas de equilibrado de la carga o bien el orden de lista.
   - Las rutas se pueden añadir manualmente y también las puede añadir el sistema de forma dinámica.

Métodos de conectividad de direccionamiento

El direccionamiento tiene que ver con el camino que sigue el tráfico de red desde su origen hasta su destino y la manera en que dicho camino está conectado. En esta página hallará enlaces que llevan a otras páginas con información conceptual referente a los métodos de direccionamiento cuya utilización en el servidor iSeries cabe plantearse.

- “Direccionamiento con conexiones punto a punto” en la página 5
  Por medio de conexiones punto a punto, los datos pueden ir del sistema local a un sistema remoto o bien de una red local a una red remota. En esta página se explican dos conceptos utilizados en la configuración de direcciones IP para una conexión punto a punto.
- “Direccionamiento de protocolo de resolución de direcciones por proxy” en la página 8
  El protocolo de resolución de direcciones (ARP) por proxy proporciona conectividad entre redes separadas físicamente sin crear ninguna red lógica nueva y sin actualizar ninguna tabla de direccionamiento. Esta página contiene también una descripción de las subredes transparentes, que es una ampliación de la técnica de direccionamiento ARP por proxy.
- “Direccionamiento dinámico” en la página 10
  El direccionamiento dinámico es un método de bajo mantenimiento que reconfigura automáticamente las tablas de direccionamiento a medida que cambia la red.
- “Enlace de ruta” en la página 11
  El enlace de ruta le permite tener control sobre cuál es la interfaz utilizada para enviar paquetes de información de respuesta.

- “Direccionamiento interdominio sin clase” en la página 12
  El direccionamiento interdominio sin clase puede reducir el tamaño de las tablas de direccionamiento y hacer que haya más direcciones IP disponibles en la empresa.
- “Direccionamiento con IP virtual” en la página 13
  IP virtual constituye una manera de asignar una o varias direcciones al sistema sin la necesidad de enlazar la dirección con una interfaz física. Puede utilizarse cuando interesa ejecutar varias instancias de un servidor Domino Web enlazadas con diferentes direcciones o bien otros servicios que necesitan enlazarse con puertos por omisión.
- “Tolerancia a errores” en la página 14
  En esta página se presentan varias formas diferentes de recuperar una ruta después de producirse un corte del suministro eléctrico.
- “**Direccionamiento con conversión de direcciones de red (NAT)**” en la página 14
  El direccionamiento con NAT permite acceder a redes remotas, como Internet, al tiempo que protege la red privada enmascarando las direcciones IP utilizadas en ella. En esta página se explican los tipos de NAT soportados por el servidor iSeries y por qué conviene utilizarlos.
- “Direccionamiento con OptiConnect y particiones lógicas” en la página 18
  OptiConnect puede conectar múltiples servidores iSeries mediante un bus de fibra óptica y alta velocidad. La información facilitada en esta página trata sobre la utilización de OptiConnect con particiones lógicas y las ventajas que esto conlleva.

Direccionamiento con conexiones punto a punto

Las conexiones punto a punto se utilizan normalmente para conectar entre sí dos sistemas dentro de una red de área amplia (WAN). Una conexión punto a punto sirve para llevar los datos del sistema local a un sistema remoto o bien de una red local a una red remota. No confunda las conexiones punto a punto con las de protocolo punto a punto (PPP). Este es un tipo de conexión punto a punto que se utiliza habitualmente para conectar una máquina a Internet. En Conexiones PPP hallará más información sobre cómo configurar y gestionar las conexiones PPP.

Las conexiones punto a punto pueden utilizarse en líneas de acceso telefónico, líneas alquiladas y otros tipos de redes, como las de Frame Relay. Existen dos maneras de configurar las direcciones IP de una conexión punto a punto: como conexión numerada y como conexión no numerada. Como su nombre indica, una conexión numerada tiene una dirección IP exclusiva definida para cada una de las interfaces. En una conexión no numerada no se utilizan direcciones IP adicionales para la conexión.

Conexiones de red numeradas:

A simple vista, la forma más sencilla de configurar una conexión punto a punto es utilizar una conexión numerada. Una conexión numerada es una definición punto a punto que tiene una dirección IP exclusiva definida para cada uno de los extremos de la conexión.

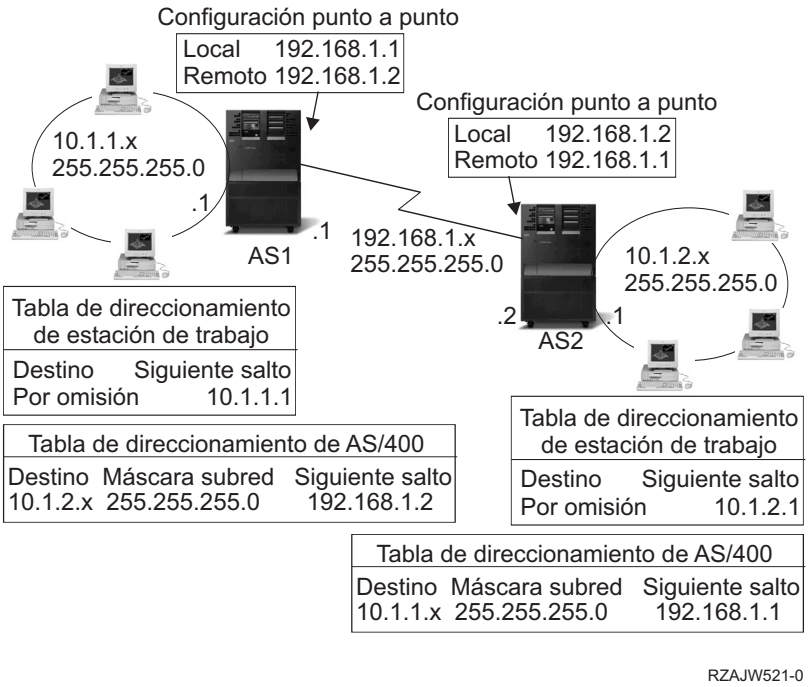
He aquí algunos aspectos que conviene tener presentes ante la posibilidad de utilizar una conexión punto a punto numerada:

- Cada uno de los extremos de la conexión tiene una dirección IP exclusiva.
- Se deben añadir sentencias de direccionamiento al sistema para que el tráfico circule hasta el sistema remoto.
- Las direcciones del enlace punto a punto debe gestionarlas el administrador de la red.
- Se consumen las direcciones que hagan falta para conectar dos sistemas.

Cuando se define una conexión punto a punto en el servidor iSeries, debe crearse una entrada de direccionamiento en cada extremo con el fin de describir cómo llegar hasta cualquier red que haya en el otro extremo de la conexión. El proceso de selección de rutas del servidor iSeries depende de que haya una dirección IP para cada interfaz. Las direcciones y las rutas debe gestionarlas el administrador de la red. Si la red es pequeña, resulta fácil estar al tanto de las direcciones, y no se utilizan muchas

direcciones adicionales. En una red grande, sin embargo, puede suceder que, solo para definir una interfaz en cada extremo, se necesite toda una subred de direcciones.

En la figura que aparece más abajo puede verse una conexión de red numerada entre dos servidores iSeries. No es necesario crear una entrada de direccionamiento si lo único que interesa es poner en comunicación AS1 con AS2. Si lo que interesa es comunicarse con los sistemas de la red remota (10.1.2.x), deberá añadirse a cada sistema la entrada de direccionamiento mostrada en la figura. El motivo es que la red remota, 10.1.2.x, forma parte de la conexión 192.168.1.x.



Conexiones de red no numeradas:

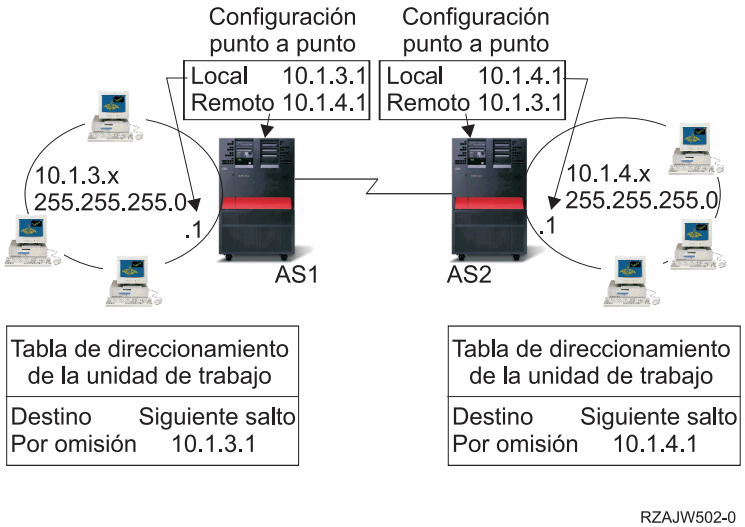
Una conexión no numerada es un método más complejo de definir una conexión punto a punto que una conexión numerada. Sin embargo, las conexiones no numeradas pueden constituir una manera mejor y más sencilla de gestionar la red.

El proceso de selección de rutas del servidor iSeries depende de que haya direcciones IP para las interfaces. En una conexión no numerada, la interfaz punto a punto no necesita tener una dirección exclusiva. En realidad, la dirección IP de la interfaz del servidor iSeries para una conexión no numerada es la dirección IP del sistema remoto.

Aspectos que conviene tener presentes ante la posibilidad de utilizar una conexión no numerada:

- La interfaz punto a punto tiene una dirección que en apariencia está en la red remota.
- No es necesario que haya sentencias de direccionamiento en el sistema.
- La administración de la red se simplifica porque el enlace no consume todas las direcciones IP.

En el ejemplo siguiente, AS1 tiene aparentemente una interfaz en la red 10.1.4.x y AS2 tiene también aparentemente una interfaz en la red 10.1.3.x. AS1 está conectado a la red LAN 10.1.3.x por medio de la dirección 10.1.3.1. Esto permite a AS1 comunicarse directamente con cualquier sistema de la red 10.1.3.x.



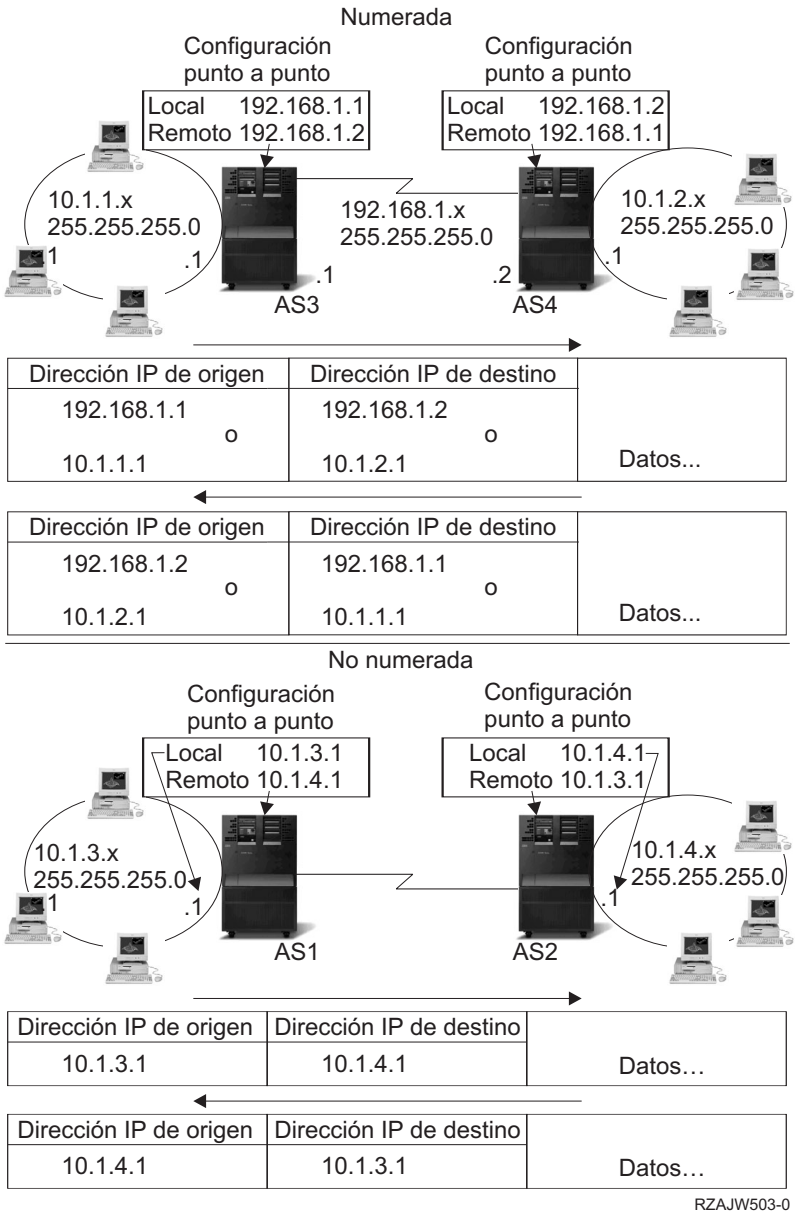
RZAJW502-0

En el ejemplo también interviene AS2. AS2 está conectado a la red LAN 10.1.4.x por medio de la dirección 10.1.4.1. Esto permite a AS2 comunicarse directamente con cualquier sistema de la red 10.1.4.x. Cada uno de estos dos sistemas (AS1 y AS2) añade la dirección remota a su respectiva tabla de direccionamiento como interfaz local. La dirección recibe un tratamiento especial para que, así, los paquetes dirigidos a dicha dirección no se procesen localmente. Los paquetes dirigidos a la dirección remota quedan colocados en la interfaz y son transportados hasta el otro extremo de la conexión. Cuando llegan al otro extremo de la conexión, se utiliza el proceso normal de paquetes.

Ahora, hace falta conectar AS1 con la red 10.1.4.x y AS2 con la red 10.1.3.x. Si ambos sistemas se encontrasen en la misma sala, bastaría con añadir un adaptador de LAN a cada uno de ellos y con enchufar la nueva interfaz en la LAN correcta. Si se hiciera así, no sería necesario añadir ninguna entrada de direccionamiento a AS1 ni a AS2. En este ejemplo, sin embargo, los sistemas se hallan en diferentes ciudades, por lo que debe utilizarse una conexión punto a punto. De todas formas, interesa evitar el paso de añadir entradas de direccionamiento. Si se define la conexión del protocolo punto a punto (PPP) como conexión no numerada, se consigue el mismo resultado que se obtendría si se pudiesen utilizar adaptadores de LAN sin añadir ninguna entrada de direccionamiento al servidor iSeries. Para ello, cada sistema toma prestada la dirección IP del sistema remoto con el propósito de utilizarla en la resolución de ruta.

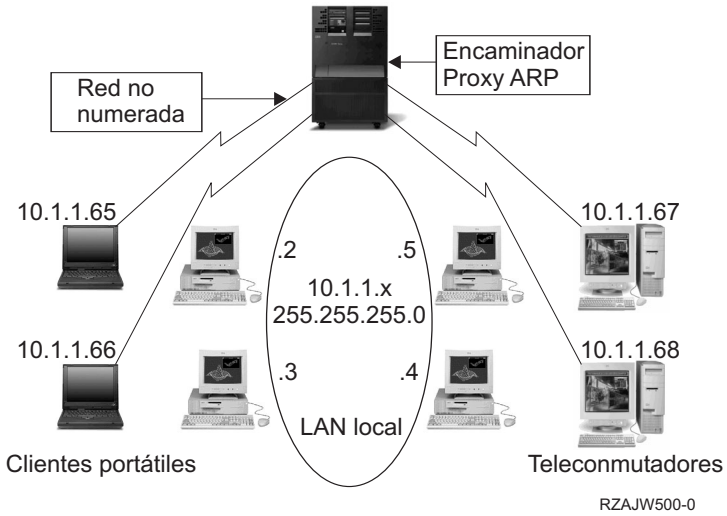
El flujo de datos de las conexiones numeradas frente al de las no numeradas:

En la figura que aparece más abajo pueden verse las direcciones que se utilizarían en una conexión punto a punto numerada y en una no numerada. De la mitad superior se desprende que, con una conexión numerada, se podría utilizar la dirección de sistema remoto 192.168.1.2 ó 10.1.2.1 para llegar hasta el sistema remoto. El motivo es que en AS3 existe una entrada de direccionamiento que manda los paquetes dirigidos a 10.1.2.1 a 192.168.1.2 como salto siguiente. Las direcciones utilizadas en el paquete de retorno están basadas en el paquete recibido. La mitad inferior de la figura muestra las direcciones utilizadas en el caso de una conexión no numerada. La dirección origen del paquete de salida es 10.1.3.1 y la destino es 10.1.4.1. No es necesario crear ninguna entrada de direccionamiento en ninguno de los dos sistemas porque ambos tienen una interfaz directa con la red remota gracias a la dirección de sistema remoto de la conexión punto a punto.



Direccionamiento de protocolo de resolución de direcciones por proxy

El direccionamiento de protocolo de resolución de direcciones (ARP) por proxy permite que redes separadas y físicamente distintas den la impresión de formar una sola red lógica. Proporciona conectividad entre redes separadas físicamente sin crear ninguna red lógica nueva y sin actualizar ninguna tabla de direccionamiento. ARP por proxy permite que sistemas que no están conectados directamente a una LAN den la impresión, de cara a los demás sistemas de la LAN, de que sí están conectados. Esto resulta útil en los casos de acceso por línea telefónica para proporcionar conexiones a toda la red desde una interfaz que acceda telefónicamente. En la figura que aparece más abajo puede verse un caso posible. 10.1.1.x es la LAN local, y de 10.1.1.65 a 10.1.1.68 son los sistemas remotos.

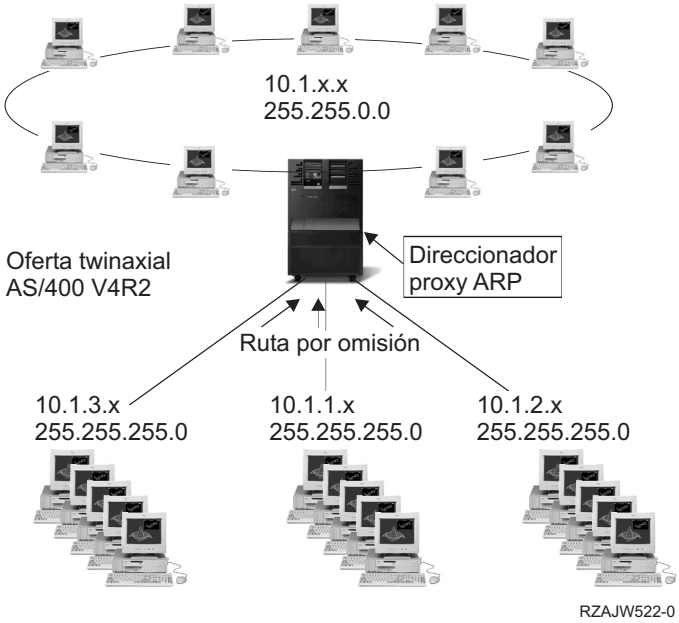


Cuando un sistema de la LAN local (10.1.1.x) desea enviar datos a uno de los sistemas remotos, primero realizará una petición ARP. Esta es una difusión que se manda a todos los sistemas conectados al segmento de LAN para solicitar la dirección del sistema destino. Sin embargo, los sistemas conectados remotamente no verán la difusión. Aquí es donde interviene ARP por proxy. El servidor iSeries sabe qué sistemas están conectados remotamente. El servidor iSeries, si ve una petición ARP dirigida a una de las máquinas conectadas remotamente, responderá a la petición ARP con su dirección (la del servidor iSeries). El servidor iSeries, a su vez, recibirá los datos y los reenviará al sistema remoto. Para que el reenvío tenga lugar, el valor de reenvío IP debe ser *yes. Si el sistema remoto no está conectado, el servidor iSeries no responderá a la petición ARP y el sistema peticionario no enviará los datos.

Puede usar “Subredes transparentes” a modo de proxy para toda una subred o para un rango de sistemas principales. El empleo de subredes transparentes permite asignar a las redes aisladas direcciones que no estén dentro del espacio de direcciones de red primaria.

Subredes transparentes

Podrá utilizar las subredes transparentes como una manera de ampliar el concepto de ARP por proxy. Estas subredes, al trabajar para un solo sistema principal, permiten conectarse a la totalidad de una subred o bien a un rango de sistemas principales. En la figura que aparece más abajo puede verse que a las redes aisladas (de 10.1.1.x a 10.1.3.x) se les asignan direcciones que no se hallan en el espacio de direcciones de red primaria (10.1.x.x).



Las LAN twinaxiales están definidas dentro de rangos de direcciones comprendidos en el rango de direcciones de LAN real. En las versiones anteriores a la V4R2, los campos de edición de Añadir ruta TCP/IP y Añadir interfaz TCP/IP no permitían que esto fuese así. En la V4R2, los campos de edición se hicieron más flexibles. Con esto se consigue que dos interfaces situadas en dos segmentos distintos tengan direcciones que en apariencia están en el mismo segmento. Cuando el servidor iSeries ve que esto sucede, automáticamente emplea ARP por proxy en los sistemas que haya conectados detrás del controlador twinaxial. Esto permite a todos los sistemas de la red 10.1.x.x comunicarse con todos los sistemas de subred sin realizar cambios en los sistemas de la red 10.1.x.x.

Subredes transparentes en redes WAN:

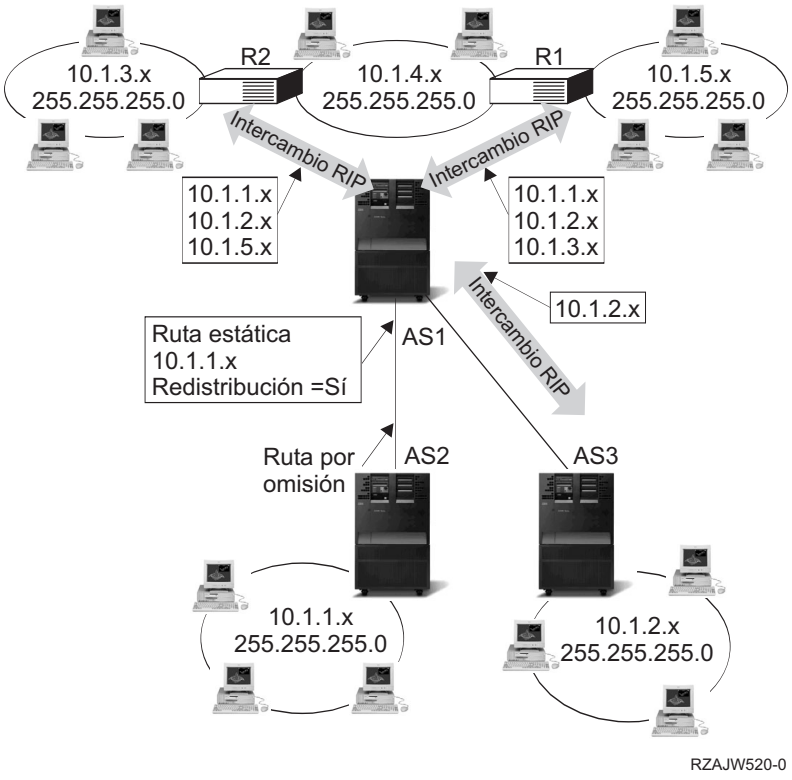
La función de subredes transparentes puede ampliarse todavía más para que puedan manejar las LAN reales situadas en ubicaciones remotas. El uso de subredes transparentes en redes WAN hace posible que las redes remotas estén en apariencia conectadas con la red local. En la figura anterior, las tres redes están conectadas a la red 10.1.x.x local por medio del servidor iSeries. Estas redes están definidas mediante una máscara de subred que las convierte en transparentes desde el punto de vista de la red local. ARP por proxy responde a cualquier petición ARP de la red local dirigida a los sistemas de las subredes 10.1.1.x, 10.1.2.x y 10.1.3.x. Con esto se consigue que el tráfico dirigido a la red local se direccione de manera automática al servidor iSeries de la red local. Este, a su vez, direcciona los datos al debido servidor iSeries remoto. El servidor iSeries remoto procesa los datos o bien los reenvía al sistema correcto dentro de la LAN remota. Las estaciones de trabajo de la LAN remota deben tener una ruta por omisión que señale hacia el servidor iSeries remoto de la red como pasarela del primer salto. Las estaciones de trabajo de la LAN local no necesitan entradas de direccionamiento adicionales porque no se ha creado ninguna red lógica nueva.

Direccionamiento dinámico

El direccionamiento dinámico lo proporcionan los protocolos de pasarela interior (IGP), como puede ser el protocolo Internet de direccionamiento (RIP). El protocolo RIP permite configurar los sistemas principales como parte de una red RIP. Este tipo de direccionamiento no requiere apenas mantenimiento y, además, reconfigura automáticamente las tablas de direccionamiento cuando la red cambia o sufre una anomalía general. Se ha añadido RIPv2 al servidor iSeries con el fin de que se puedan enviar y recibir paquetes RIP para actualizar las rutas en toda la red.

En la figura que aparece más abajo, se añade una ruta estática al sistema central (AS1) que describe la conexión con la red 10.1.1.x a través de AS2. Esta es una ruta estática (añadida por el administrador de

la red) cuyo valor de redistribución de ruta es sí. Este valor hace que la ruta se comparta con otros direccionadores y sistemas, de manera que cuando estos tienen tráfico para 10.1.1.x, lo direccionan al servidor iSeries central (AS1). AS2 hace que se inicie el servidor direccionado, de manera que envíe y reciba información RIP. En este ejemplo, AS1 envía un mensaje en el que se informa que AS2 tiene una conexión directa con 10.1.2.x.



¿Qué ocurre en este ejemplo?

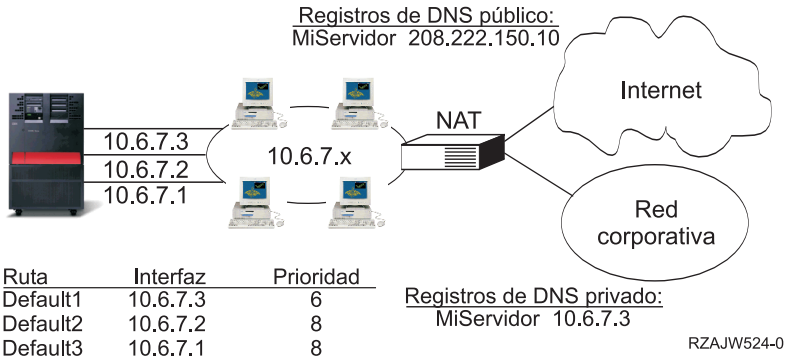
- AS1 recibe el paquete RIP de AS2 y lo procesa. Si AS1 no tiene una ruta a 10.1.2.x, almacenará esta ruta. Si tiene una vía de acceso a 10.1.2.x con el mismo número de saltos o menos, descartará la nueva información de ruta. En este ejemplo, AS1 conserva los datos de ruta.
- AS1 recibe información de R1 con información de ruta hasta 10.1.5.x. AS1 conserva esta información de ruta.
- AS1 recibe información de R2 con información de ruta hasta 10.1.3.x. AS1 conserva esta información de ruta.
- La próxima vez que AS1 envíe mensajes RIP, enviará información a R1 en la que se describirán todas las conexiones de las que AS1 tiene conocimiento y de las que R1 puede que no. AS1 envía información de ruta sobre 10.1.1.x, 10.1.2.x y 10.1.3.x. En cambio, no envía información sobre 10.1.4.x a R1 porque sabe que R1 está conectado a 10.1.4.x y no necesita ninguna ruta. Se envía información de la misma naturaleza a R2 y a AS3.

Enlace de ruta

Antes de que hiciese su aparición el enlace de ruta preferido, no se tenía control sobre cuál era la interfaz utilizada para enviar paquetes de información de respuesta. La interfaz de enlace de ruta preferida, añadida a la función de añadir ruta, da un mayor grado de control sobre cuál es la interfaz que se utiliza para enviar los paquetes, ya que permite enlazar de manera explícita rutas con interfaces.

En la figura que aparece más abajo hay tres interfaces conectadas a la misma red. Para garantizar que, independientemente de cuál sea la interfaz que recibe la petición de entrada, se puede enviar la respuesta de vuelta a la misma interfaz. Para ello, tendrá que añadir las rutas ″duplicadas″ a cada una de

las interfaces. En este ejemplo, hemos añadido tres rutas por omisión, cada una de las cuales está enlazada de manera explícita con una interfaz diferente. Este enlazado no cambia sea cual sea el orden en que se inicien o finalicen las interfaces.



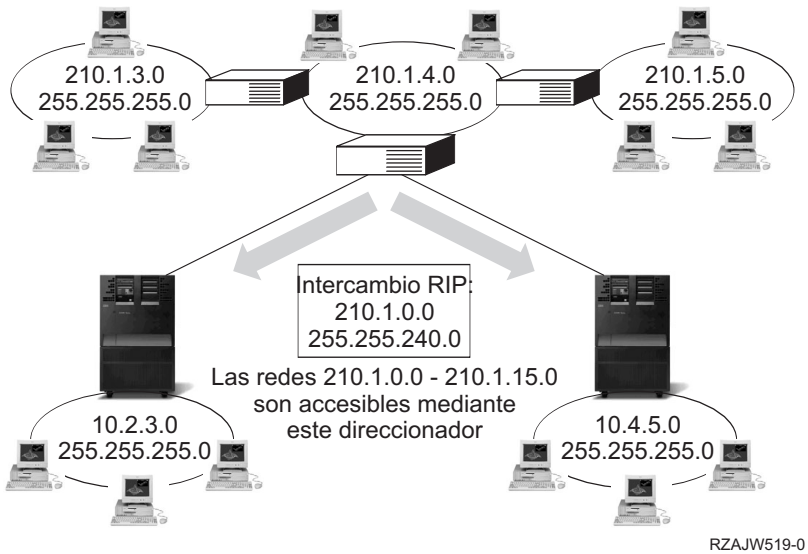
Ruta	Interfaz	Prioridad
Default1	10.6.7.3	6
Default2	10.6.7.2	8
Default3	10.6.7.1	8

Direccionamiento interdominio sin clase

El direccionamiento interdominio sin clase (CIDR o superred) es una manera de combinar varios rangos de direcciones de clase C y formar una única red o ruta. Este método de direccionamiento añade direcciones IP de clase C. Estas direcciones las reparten los proveedores de servicios de Internet (ISP) a sus clientes para que estos las utilicen. Las direcciones CIDR pueden reducir el tamaño de las tablas de direccionamiento y hacer que haya más direcciones IP disponibles en la empresa.

Antes, era necesario entrar una máscara de subred que fuese igual o mayor que la máscara necesaria para la clase de red. En el caso de las direcciones de clase C, esto significaba que la subred 255.255.255.0 era la de mayor tamaño (253 sistemas principales) que se podía especificar. Para conservar las direcciones IP, cuando las empresas necesitaban más de 253 sistemas principales en una red, Internet emitía varias direcciones de clase C. Esto complicaba la configuración de las rutas, entre otras cuestiones.

Ahora, CIDR permite que estas direcciones de clase C contiguas se combinen y formen un único rango de direcciones de red gracias a la utilización de la máscara de subred. Por ejemplo, si se reparten cuatro direcciones de red de clase C (208.222.148.0, 208.222.149.0, 208.222.150.0 y 208.222.151.0 con la máscara de subred 255.255.255.0), se podría pedir al ISP que las convirtiese en una superred por medio de la máscara de subred 255.255.252.0. Esta máscara combina las cuatro redes en una sola a efectos de direccionamiento. CIDR es provechoso porque reduce el número de direcciones IP asignadas pero innecesarias.

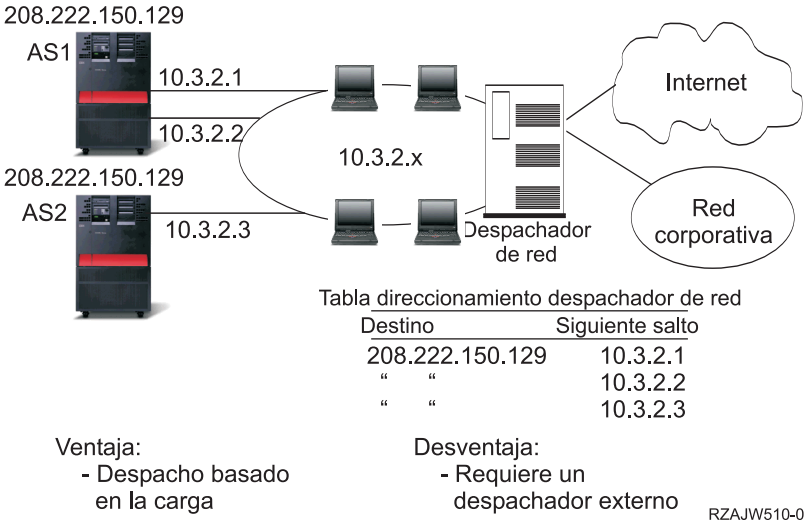


En este ejemplo, el direccionador está configurado para enviar un mensaje RIP con la dirección de red 210.1.0.0 y la máscara de subred 255.255.240.0. Esto indica a los sistemas que han de recibir los mensajes RIP dirigidos a las redes de la 210.1.0.0 a la 210.1.15.0 por medio de este direccionador. Este envía un mensaje en lugar de los 16 que necesitaría para comunicar la misma información si no se dispusiese de CIDR.

Direccionamiento con IP virtual

El protocolo Internet (IP) virtual, denominado también interfaz sin circuito o de bucle de retorno, es una potente función que sirve para muchas y muy diversas cosas. Constituye una manera de asignar una o varias direcciones al sistema sin necesidad de enlazar la dirección con una interfaz física. Puede utilizarse cuando interesa ejecutar múltiples instancias de un servidor Web Domino enlazadas con diferentes direcciones o si interesa ejecutar otros servicios que se tienen que enlazar con puertos por omisión.

La mayoría de los entornos en los que puede ser conveniente utilizar IP virtual son casos en los que interesa proporcionar múltiples vías de acceso entre la pasarela local y el servidor iSeries; por ejemplo, el equilibrado de la carga y la tolerancia a errores. En este contexto, cada ″vía de acceso″ conlleva la existencia de una interfaz adicional y, en consecuencia, la de una dirección adicional no virtual en el servidor iSeries. La presencia de estas interfaces solo debe percibirse en la red local. No interesa que los clientes remotos tengan que estar enterados de la existencia de múltiples direcciones IP para el servidor iSeries. Lo ideal sería que los clientes remotos percibiesen el servidor iSeries como una única dirección IP. El modo en que el paquete entrante cruza la pasarela, recorre la red local y llega hasta el servidor iSeries debe resultar imperceptible para un cliente remoto. La manera de conseguirlo es utilizar IP virtual. Los clientes locales se comunicarán con el servidor iSeries por medio de las direcciones IP físicas, mientras que los clientes remotos solo verán la interfaz IP virtual.



El entorno IP virtual está dirigido al servidor iSeries que actúa a modo de servidor de los clientes conectados remotamente. Lo más importante es que la dirección de IP virtual se halla en una subred distinta a aquella en la que se encuentran las interfaces físicas. Además, la dirección de IP virtual hace que el servidor iSeries sea en apariencia un único sistema principal y no necesariamente uno que esté conectado a una subred o una red de mayor tamaño. Por lo tanto, la máscara de subred de la interfaz IP virtual debe estar normalmente establecida en 255.255.255.255.

Dado que la dirección de IP virtual no está enlazada con una sola interfaz física, el servidor iSeries no responderá nunca a una petición de protocolo de resolución de direcciones (ARP) enviada a la dirección de IP virtual. Dicho de otra manera, no se puede efectuar un direccionamiento de forma directa a una dirección de IP virtual. Para que otros sistemas puedan llegar hasta la dirección de IP virtual, deben tener definida una ruta a tal efecto. Este es el motivo por el que IP virtual está diseñado principalmente para clientes conectados remotamente. En el ejemplo que figura más abajo, todas las estaciones de trabajo

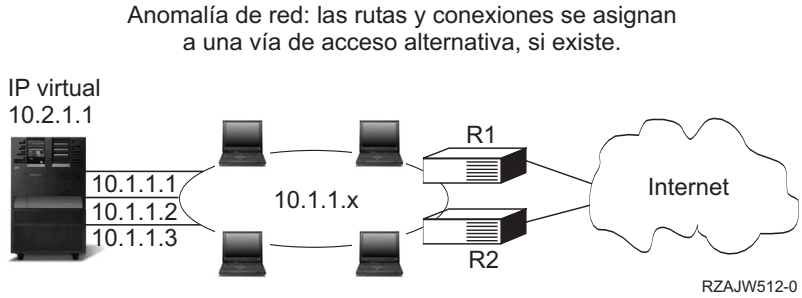
señalan hacia una de las interfaces 10.3.2, del servidor iSeries, como pasarela de salto siguiente. Cuando un paquete llega al servidor iSeries, pasa por el proceso de paquetes. Si la dirección destino coincide con alguna de las direcciones definidas en el sistema (incluidas las direcciones de IP virtual), el sistema procesa el paquete.

Los servidores de DNS utilizan las direcciones del servidor solicitado. En este caso, todas las direcciones representan el mismo sistema. La función de IP virtual se puede utilizar cuando se consolidan múltiples sistemas en uno de mayor tamaño.

Tolerancia a errores

Otro uso que se puede dar a las direcciones de IP virtual es la protección contra errores de ruta.

En este ejemplo se presentan varias formas diferentes de recuperar una ruta después de producirse un corte del suministro eléctrico. La conexión más fiable se da cuando hay definida una dirección de IP virtual en el sistema. Con el soporte de IP virtual, aunque falle una interfaz, la sesión podrá igualmente comunicarse por medio de otras interfaces.



¿Qué sucede si falla el direccionador R1?

- Las conexiones realizadas por medio de R1 se redireccionan a partir de ese momento a través de R2.
- La pasarela fallida detectará la recuperación de R1, pero las conexiones activas seguirán ejecutándose a través de R2.

¿Qué sucede si falla la interfaz 10.1.1.1?

- Las conexiones activas con 10.1.1.1 se pierden, pero no así las demás conexiones con 10.1.1.2, 10.1.1.3 y 10.2.1.1.
- Reenlace de ruta:
  - Versiones anteriores a la V4R2: las rutas indirectas pasan a estar enlazadas con 10.1.1.2 ó 10.1.1.3.
  - V4R2: las rutas se reenlazan solo si el valor de interfaz de enlace preferida es NONE.
  - V4R3 y versiones posteriores: es necesario definir 10.2.1.1 como dirección de IP virtual y dirección primaria del sistema.
    - La dirección IP primaria del sistema permanece activa.
    - El sistema sigue siendo accesible siempre y cuando permanezca activa una interfaz física como mínimo.

Direccionamiento con conversión de direcciones de red (NAT)

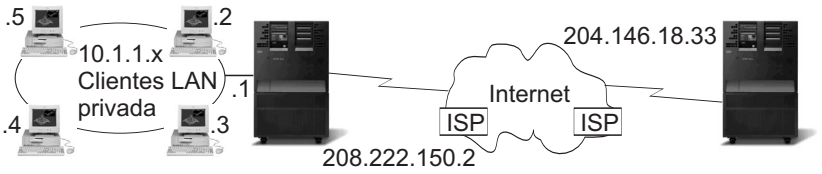
La conversión de direcciones de red (NAT) da acceso a una red remota, que suele ser Internet, al tiempo que protege la red privada enmascarando las direcciones IP utilizadas dentro del cortafuegos. Los tipos de NAT que se pueden utilizar para el direccionamiento del servidor iSeries son los siguientes:

- “NAT de enmascaramiento”
  Permite a la red privada ocultarse detrás de (y estar representada por) la dirección enlazada con la interfaz pública.
- “NAT dinámica” en la página 17
  Establece una conexión que va desde el interior de una red privada hasta una red pública. La diferencia es que, cuando se realiza una conexión de salida, se mantiene y utiliza una agrupación de direcciones públicas.
- “NAT estática” en la página 18
  Da soporte a las conexiones de entrada que van desde una red pública hasta una red privada.

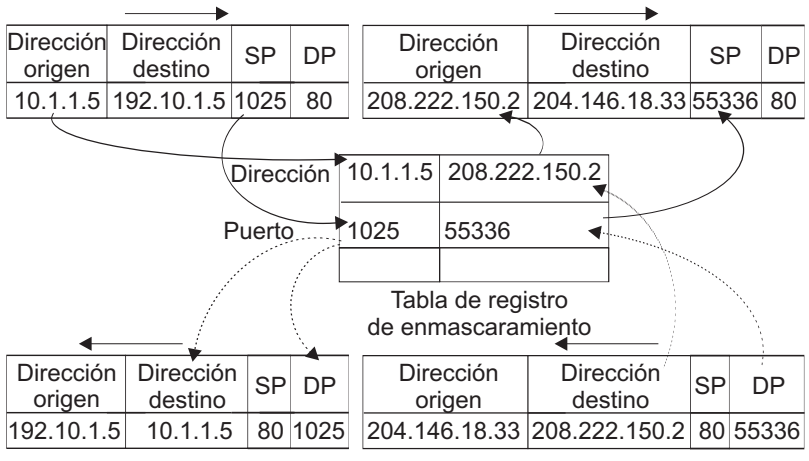
NAT de enmascaramiento

La conversión de direcciones de red (NAT) de enmascaramiento sirve para permitir a la red privada ocultarse detrás de (así como estar representada por) la dirección enlazada con la interfaz pública. En muchas ocasiones, se trata de la dirección que ha sido asignada por un proveedor de servicios de Internet (ISP) y puede ser una dirección dinámica en el caso de las conexiones PPP. Este tipo de conversión solo se puede utilizar para conexiones cuyo origen esté en el interior de la red privada y cuyo destino se halle en la red pública exterior. Cada conexión de salida se mantiene utilizando un número de puerto IP origen diferente.

La NAT de enmascaramiento permite a las estaciones de trabajo que tengan direcciones IP privadas comunicarse con los sistemas principales de Internet mediante el servidor iSeries. Este servidor tiene una dirección IP, asignada por el ISP local, como pasarela Internet. Se emplea el término máquina conectada localmente para hacer referencia a todas las máquinas de una red interna, sea cual sea el método de conexión (LAN o WAN) y la distancia que cubre la conexión. Se utiliza el término máquinas externas para designar las máquinas situadas en Internet. La figura siguiente ilustra cómo funciona la NAT de enmascaramiento.



Función de NAT de enmascaramiento



RZAJW507-0

Desde la perspectiva de Internet, todas las estaciones de trabajo están en apariencia contenidas en el servidor iSeries; es decir, solo hay una dirección IP asociada al servidor iSeries y a las estaciones de trabajo. Un direccionador, cuando recibe un paquete dirigido a la estación de trabajo, intenta determinar cuál es la dirección de la LAN interna que debe recibirlo y se lo envía.

Cada estación de trabajo debe estar configurada de manera que el servidor iSeries sea su pasarela y, a la vez, su destino por omisión. La correspondencia entre una determinada conexión de comunicaciones (puerto) y una estación de trabajo se configura cuando una de las estaciones de trabajo envía un paquete al servidor iSeries para que se envíe a Internet. La NAT de enmascaramiento guarda el número de puerto, de manera que, cuando recibe a través de la conexión la respuesta al paquete de la estación de trabajo, puede enviarla a la estación de trabajo correcta.

La NAT de enmascaramiento crea y mantiene un registro de las conexiones de puerto activas y de la hora del último acceso por parte de cualquiera de los dos extremos de la conexión. De este registro se eliminan de forma periódica todas las conexiones que han estado desocupadas durante un tiempo predeterminado tomando como base la suposición de que una conexión desocupada ha dejado de utilizarse.

Toda comunicación entre la estación de trabajo e Internet debe ser iniciada por las máquinas conectadas localmente. Se trata de un cortafuegos de seguridad efectivo; Internet desconoce por completo la existencia de las estaciones de trabajo y no puede difundir sus direcciones por Internet.

Un factor clave en la implementación de la NAT de enmascaramiento es la utilización de puertos lógicos, emitidos por la NAT de enmascaramiento con el fin de distinguir las diversas corrientes de comunicación. TCP contiene un número de puerto origen y otro destino. A estas designaciones, la NAT añade un número de puerto lógico.

Proceso de NAT de enmascaramiento de salida:

El mensaje de salida de la figura anterior es un paquete procedente de la LAN privada que va hacia Internet. Los mensajes de salida (de una ubicación local a una externa) contienen el puerto origen utilizado por la estación de trabajo de la que son originarios. La NAT guarda este número y lo sustituye en la cabecera de transporte por un número exclusivo de puerto lógico. En el caso de los datagramas de salida, el número de puerto origen es el número de puerto local.

1. El proceso de NAT de enmascaramiento de salida presupone que todos los paquetes IP que recibe van con rumbo a direcciones IP externas y, por lo tanto, no realiza ninguna comprobación para determinar si los paquetes deben direccionarse localmente.

2. El conjunto de números de puerto lógico busca una coincidencia en la capa de transporte, así como la dirección IP origen y el puerto origen. Si la encuentra, se sustituye el puerto origen por el número de puerto lógico correspondiente. Si no se encuentra ningún número de puerto coincidente, se crea uno nuevo, se selecciona un nuevo número de puerto lógico y se sustituye el puerto origen por él.

3. Se convierte la dirección IP origen.

4. A continuación, IP procesa el paquete de la forma habitual y el paquete se envía al sistema externo correcto.

Proceso de NAT de enmascaramiento de entrada (respuesta y otros):

El mensaje de entrada de la figura anterior es un paquete procedente de Internet que va hacia la LAN privada. En el caso de los datagramas de entrada, el número de puerto destino es el número de puerto local. (En el caso de los mensajes de entrada, el número de puerto origen es el número de puerto externo. En el caso de los mensajes de salida, el número de puerto destino es el número de puerto externo).

Los mensajes de respuesta devueltos desde Internet con rumbo a una máquina conectada localmente tienen un número de puerto lógico asignado por enmascaramiento como número de puerto destino en la cabecera de la capa de transporte. Los pasos del proceso de entrada de NAT de enmascaramiento son:

1. La NAT de enmascaramiento busca en su base de datos el número de puerto lógico (puerto origen). Si no lo encuentra, se supone que el paquete es un paquete no solicitado y se devuelve al llamador sin efectuar cambio alguno. A continuación, se maneja como si se tratase de un destino desconocido normal.

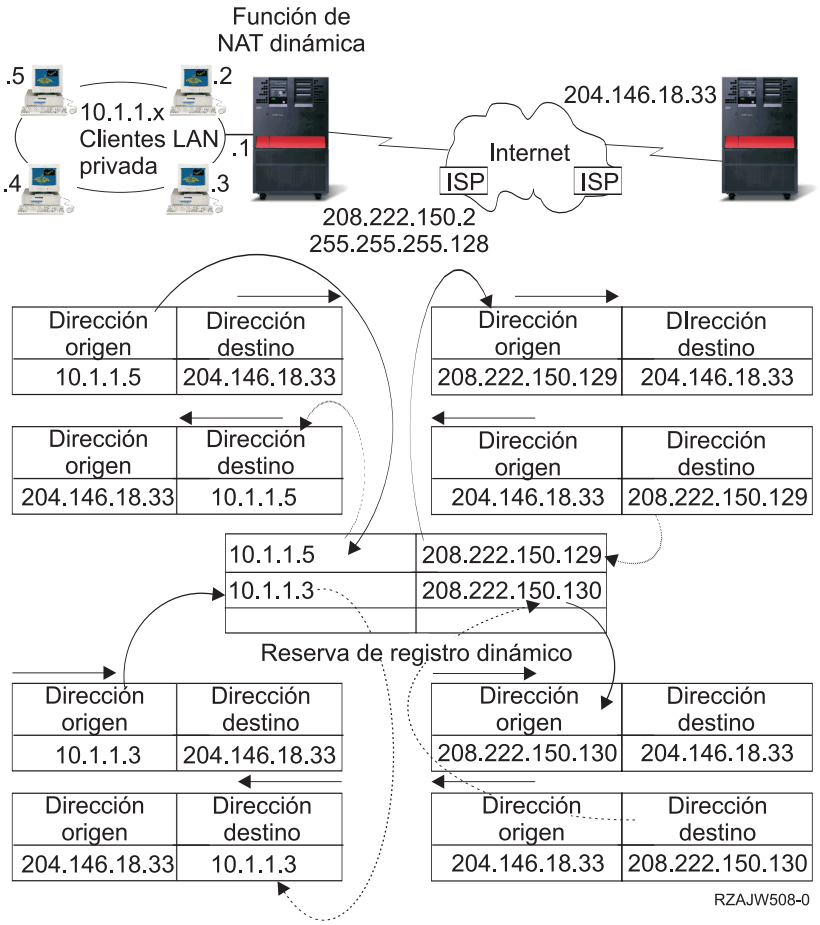
2. Si se encuentra un número de puerto lógico coincidente, se realiza una comprobación más con objeto de determinar que la dirección IP origen coincide con la dirección IP destino de la entrada existente en la tabla de números de puerto lógico. Si coincide, se sustituye el puerto origen que figura en la cabecera IP por el número de puerto de la máquina local original. Si la comprobación falla, se devuelve el paquete sin efectuar cambio alguno.

3. Se colocan las direcciones IP coincidentes locales en el destino IP del paquete.

4. A continuación, IP o TCP procesa el paquete de la forma habitual y el paquete va a parar a la debida máquina conectada localmente. Dado que la NAT de enmascaramiento necesita un número de puerto lógico para determinar cuáles son las direcciones correctas de los puertos origen y destino, no puede manejar los datagramas no solicitados procedentes de Internet.

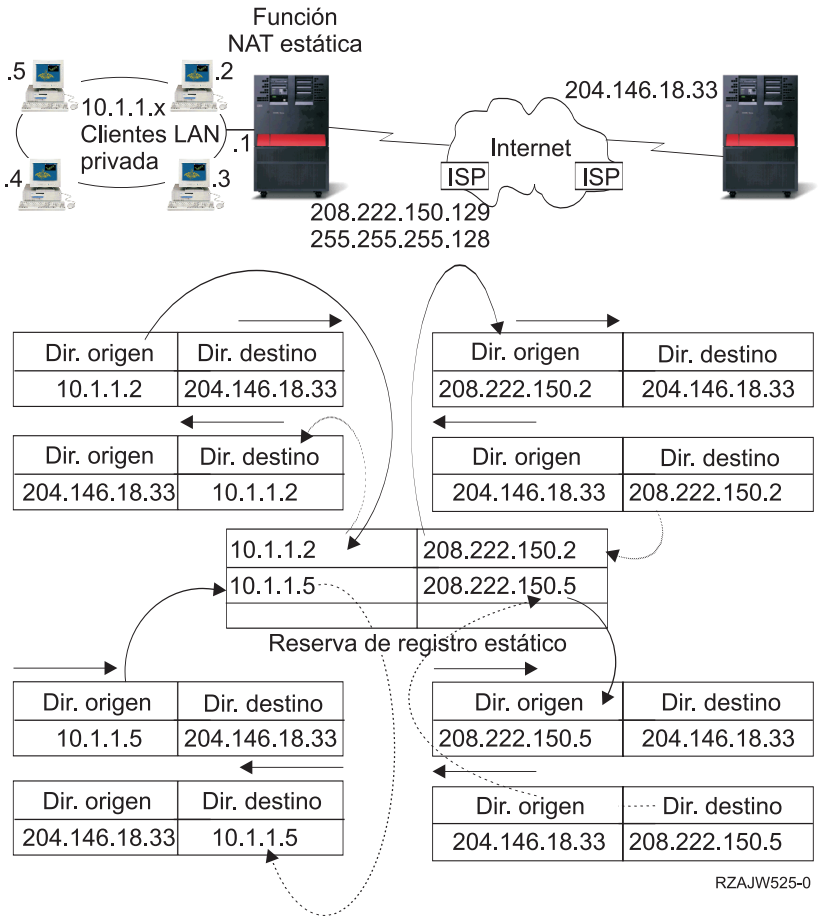
NAT dinámica

La NAT dinámica solo se puede utilizar para establecer conexiones que vayan desde el interior de la red privada hasta la red pública. Cuando se realiza una conexión de salida, se mantiene y utiliza una agrupación de direcciones de red. A cada conexión se le asigna una dirección pública exclusiva. El número máximo de conexiones simultáneas es igual al número de direcciones públicas que hay en la agrupación. Es similar a una correspondencia biunívoca entre direcciones. La NAT dinámica le permite comunicarse con Internet a través de una dirección de NAT dinámica. La figura que aparece a continuación ilustra el concepto de NAT dinámica.



NAT estática

La NAT estática es una simple correlación biunívoca de direcciones privadas y públicas. Es necesaria para dar soporte a conexiones de entrada que van desde la red pública hasta la red privada. Para cada dirección local definida, tiene que haber asociada una dirección exclusiva globalmente.



Direccionamiento con OptiConnect y particiones lógicas

OptiConnect y las particiones lógicas constituyen otros entornos en los que utilizar los componentes básicos de direccionamiento, que son ARP por proxy, las conexiones punto a punto y las interfaces de IP virtual. He aquí algunos métodos diferentes de estos componentes básicos.

- “TCP/IP y OptiConnect”
  OptiConnect ofrece la posibilidad de definir conexiones TCP/IP sobre un bus OptiConnect. En esta página se describe esta función y la manera en que puede utilizarse.
- “Direccionamiento con OptiConnect virtual y particiones lógicas” en la página 19
  Las interfaces de TCP/IP OptiConnect Virtual se emplean como vías de comunicación entre particiones. Un servidor iSeries individual está particionado lógicamente en múltiples máquinas virtuales. Cada partición cuenta con un espacio de direcciones propio. Para TCP/IP, cada partición es en apariencia un servidor iSeries distinto. En esta página se explica el modo de utilizar esta función en beneficio propio.

TCP/IP y OptiConnect

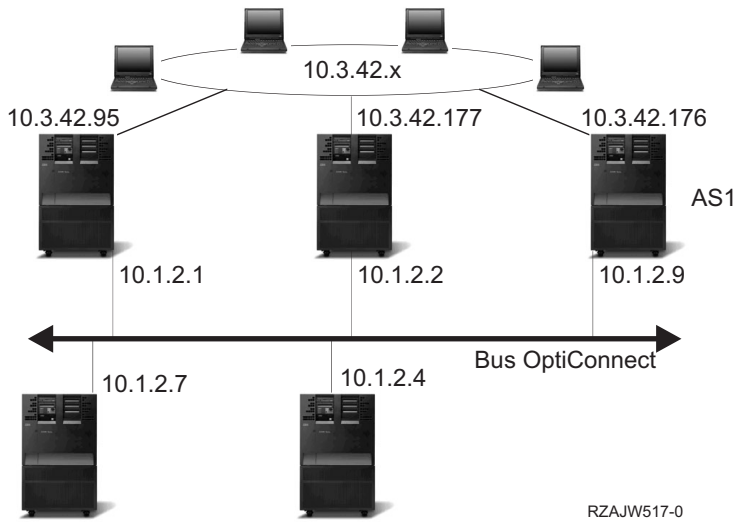
OptiConnect ofrece la posibilidad de definir conexiones TCP/IP sobre un bus OptiConnect. TCP/IP sobre OptiConnect constituye otro método para los elementos esenciales de direccionamiento, como son ARP por proxy, las redes punto a punto no numeradas y las interfaces de IP virtual. Se puede configurar empleando una configuración de LAN emulada por OptiConnect y una configuración punto a punto OptiConnect.

Con una **configuración de LAN emulada por OptiConnect**, el bus OptiConnect es en apariencia una LAN para TCP/IP. Esto es sencillo de configurar, pero la conectividad OptiConnect de LAN no es automática porque se necesita el protocolo de información de direccionamiento (RIP) o bien rutas estáticas.

La **configuración punto a punto OptiConnect** utiliza interfaces no numeradas punto a punto configuradas para cada par de sistemas principales OptiConnect. No se crea ninguna red nueva y, por ello, la conectividad OptiConnect de LAN es automática. Una de las ventajas de esta configuración es que no se necesita ninguna definición de ruta adicional. La conectividad entre un sistema principal de una red con los de la otra es automática. Otra de las ventajas es que, si ambas redes están inactivas, los datos enviados entre servidores iSeries circulan por el bus OptiConnect porque estas rutas tienen la máscara de subred más concreta. Si por algún motivo falla el bus OptiConnect, el tráfico se transfiere de forma automática a la LAN Token Ring.

La configuración punto a punto OptiConnect mediante IP virtual es una variante de la configuración punto a punto no numerada. Recuerde que, siempre que utilice interfaces punto a punto no numeradas, cada interfaz ha de tener especificada una interfaz local asociada. Es la dirección IP mediante la que el sistema situado en el extremo remoto del enlace punto a punto conocerá el servidor iSeries local. La interfaz local asociada puede ser la interfaz de LAN primaria del servidor iSeries, como se indica más abajo. La interfaz local asociada también puede ser una interfaz IP virtual. En esta configuración, se utiliza el bus OptiConnect a modo de colección de conexiones punto a punto. Se define una conexión no numerada para cada par de sistemas principales. Al igual que ocurre en la configuración anterior, no se necesita ninguna definición de ruta adicional, y la conectividad entre un sistema principal de una red con los de la otra es automática. Una de las ventajas de esta configuración es que, si está activa una de las dos redes, existe una vía de acceso para llegar hasta cualquier servidor iSeries.

Configuración de LAN con OptiConnect emulada

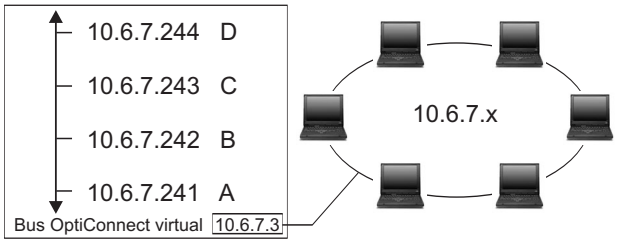


Direccionamiento con OptiConnect virtual y particiones lógicas

Cuando hay particiones lógicas, un servidor iSeries individual está particionado lógicamente en múltiples máquinas virtuales. Las interfaces de TCP/IP OptiConnect Virtual se emplean como vías de comunicación entre particiones. Cada partición cuenta con un espacio de direcciones propio, con una instancia de TCP/IP propia y, quizás, con adaptadores de E/S dedicados propios. Para TCP/IP, cada partición es en apariencia un servidor iSeries distinto. La comunicación TCP/IP entre las diferentes particiones se efectúa mediante un bus OptiConnect virtual. El código de direccionamiento TCP/IP utiliza la vía de acceso a otra partición de modo no diferente a como utiliza la vía de acceso a otro sistema conectado por medio de un bus OptiConnect físico.

Particiones lógicas: las interfaces TCP/IP OptiConnect virtual se utilizan como vías de comunicación entre particiones.

Red OptiConnect virtual = 10.6.7.241 - 10.6.7.254
Proporciona direcciones hasta para 14 particiones



Partición	Interfaz	Línea	Máscara de subred	MTU
D	10.6.7.244	*OPC	255.255.255.240	4096
C	10.6.7.243	*OPC	255.255.255.240	4096
B	10.6.7.242	*OPC	255.255.255.240	4096
A	10.6.7.241	*OPC	255.255.255.240	4096 (Interfaz local
A	10.6.7.3	TRNLINE	255.255.255.0	4096 asociada = 10.6.7.3)

RZAJW515-0

En estos ejemplos, solo hay un adaptador de LAN instalado en el sistema. Se le ha asignado la partición A. Los clientes de la LAN necesitan comunicarse con las demás particiones definidas en el sistema. Para ello, se define una subred transparente en el bus OptiConnect virtual. La dirección de red de la LAN es 10.6.7.x. Está previsto crear particiones adicionales, por lo que se necesitan direcciones IP. Para obtener 12 direcciones, se debe utilizar la máscara de subred 255.255.255.240. Con ello se consiguen las direcciones de la 10.6.7.241 a la 10.6.7.254, lo que hace un total de 14 direcciones útiles. Hay que asegurarse de que en la LAN no se utilicen ya estas direcciones. Una vez obtenidas las direcciones, se asigna una a cada partición. Se añade una interfaz a cada partición y se define la dirección en el bus OptiConnect virtual.

OPC	Partición	IP virtual	Partición	Interfaz	Línea	Máscara de subred	MTU	Interfaz local asociada
10.6.7.3	D	10.6.7.4	D	10.6.7.4	VIRTUALIP	255.255.255.255	4096	NINGUNA
10.6.7.2			D	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.4
10.6.7.1			D	10.6.7.2	OPC	255.255.255.255	4096	10.6.7.4
			D	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.4
10.6.7.4	C	10.6.7.3	C	10.6.7.3	VIRTUALIP	255.255.255.255	4096	NINGUNA
10.6.7.2			C	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.3
10.6.7.1			C	10.6.7.2	OPC	255.255.255.255	4096	10.6.7.3
			C	10.6.7.4	OPC	255.255.255.255	4096	10.6.7.3
10.6.7.4	B	10.6.7.2	B	10.6.7.2	VIRTUALIP	255.255.255.255	4096	NINGUNA
10.6.7.3			B	10.6.7.1	OPC	255.255.255.255	4096	10.6.7.2
10.6.7.1			B	10.6.7.3	OPC	255.255.255.255	4096	10.6.7.2
			B	10.6.7.4	OPC	255.255.255.255	4096	10.6.7.2
10.6.7.3	A	10.6.7.1	A	10.6.7.1	TRNLINE	255.255.255.0	4096	NINGUNA
10.6.7.3			A	10.6.7.2	OPC	255.255.255.255	4096	10.6.7.1
10.6.7.2			A	10.6.7.3	OPC	255.255.255.255	4096	10.6.7.1
Bus OC virtual			A	10.6.7.4	OPC	255.255.255.255	4096	10.6.7.1

A LAN externa 10.6.7.x

rzajw516-0

La subred transparente queda habilitada de forma automática cuando las dos afirmaciones siguientes son ciertas: primero, el bus OptiConnect virtual es menor o igual que el tamaño de la MTU de la interfaz de LAN real; y segundo, la subred del bus OptiConnect es una subred de la dirección de red de la LAN. Si ambas afirmaciones son ciertas, la subred transparente queda automáticamente habilitada. La interfaz 10.6.7.3 actúa a modo de proxy para todas las interfaces definidas en las particiones. Esto permite a los clientes de la LAN conectarse con las particiones.

Métodos de equilibrado de la carga de trabajo TCP/IP

El proceso de equilibrar la carga de trabajo consiste en redistribuir entre varios procesadores, varios adaptadores de interfaz o varios servidores de sistema principal el tráfico de la red y la carga de trabajo de las máquinas a las que se accede con asiduidad. Si desea conseguir el mejor rendimiento posible del servidor iSeries, debe repartir la carga de las comunicaciones entre múltiples componentes del servidor.

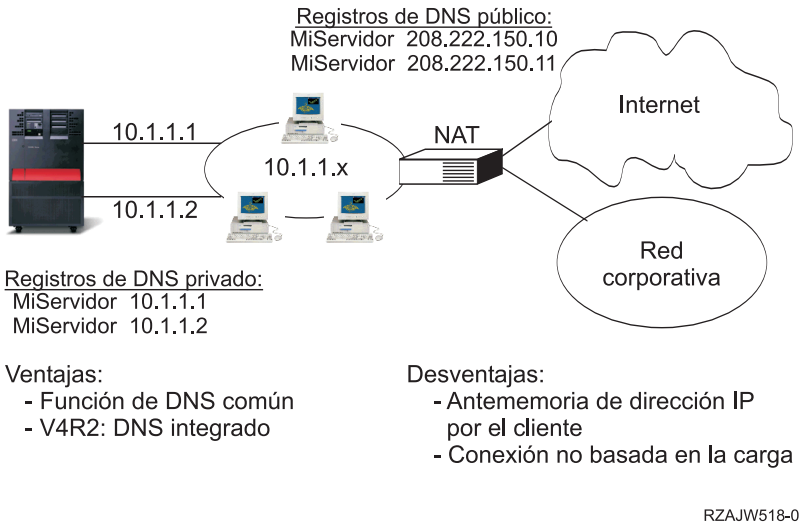
Para equilibrar la carga de trabajo del servidor iSeries, se pueden utilizar varios métodos de direccionamiento TCP/IP:

- "Equilibrado de la carga basado en DNS"
  Sirve para la carga de trabajo de entrada y debe utilizarse si es necesario equilibrar la carga de los clientes locales.
- "Equilibrado de la carga basado en rutas duplicadas" en la página 22
  En esta página se habla sobre el equilibrado de la carga de trabajo de salida entre varias interfaces. Esta es una solución basada en conexiones que tiene un mayor grado de flexibilidad que el equilibrado de la carga basado en DNS, pero no está activa para clientes locales.
- "Conmutación por anomalía de adaptador utilizando IP virtual y ARP por proxy" en la página 23
  Para esta solución hay que tener una máquina externa de equilibrado de la carga, como puede ser IBM eNetwork Dispatcher. Las direcciones de IP virtual permiten asignar una dirección al sistema en lugar de a una interfaz concreta. Se puede definir la misma dirección en múltiples servidores, lo que permite muchas opciones nuevas de equilibrado de la carga.

Equilibrado de la carga basado en DNS

El equilibrado de la carga basado en DNS sirve para equilibrar la carga de entrada. En el DNS, se configuran múltiples direcciones IP de sistema principal para un solo nombre de servidor de sistema principal. El DNS va alternando la dirección IP de sistema principal que se devuelve a las sucesivas peticiones de resolución de nombre de sistema principal efectuadas por los clientes. Una de las ventajas de este tipo de equilibrado de la carga es que esta es una función de DNS común. Los inconvenientes de esta solución es que un cliente puede guardar las direcciones IP en la antememoria y que es una solución basada en la conexión y no en la carga.

El primer modo de conseguir el equilibrado de la carga es utilizar una función del DNS para pasar múltiples direcciones para un mismo nombre de sistema. El DNS servirá una dirección IP diferente cada vez que se realice una petición solicitando el registro de dirección del nombre de sistema. En el ejemplo que aparece más abajo, cada dirección se corresponde con un sistema distinto. Esto permite equilibrar la carga entre dos sistemas aparte. En el caso de los clientes de las redes privadas, estos reciben una dirección diferente para cada petición. Esta es una función de DNS común. Observe que también hay dos entradas de direcciones para el DNS público. Estas direcciones se convierten mediante la "NAT estática" en la página 18 para que, si usted está en Internet, pueda llegar hasta ambos sistemas.

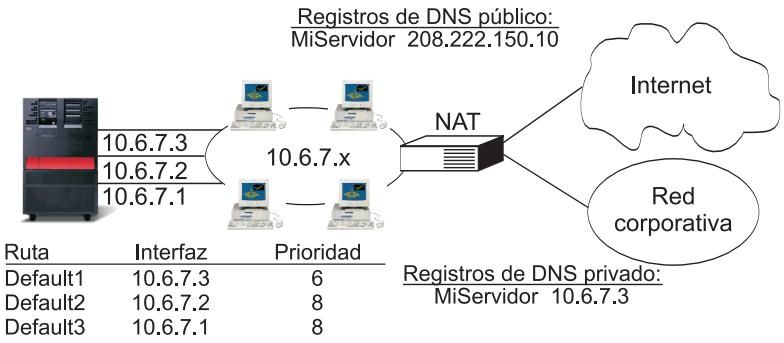


Si los programas dependen del hecho de llegar hasta un sistema concreto o de regresar al mismo sistema tras la conexión inicial, el sitio y las páginas Web deben estar codificados para que se envíe un nombre de sistema diferente una vez establecido el primer contacto. Se podrían añadir entradas de DNS adicionales para MiServidor1 208.222.150.10 y MiServidor2 208.222.150.11. Con ello, el sitio Web podría, por ejemplo, señalar hacia MiServidor2 tras el primer contacto. Este tipo de equilibrado de la carga realiza el equilibrado en función de la petición de conexión. En la mayoría de los casos, una vez resuelta la dirección, el cliente la guardará en la antememoria y no volverá a preguntar. Este tipo de equilibrado de la carga no toma en consideración el volumen del tráfico que llega a cada uno de los sistemas. Observará que solo toma en consideración el tráfico de entrada y que, además, se pueden tener dos adaptadores en un solo sistema en lugar de un adaptador en dos sistemas.

Equilibrado de la carga basado en rutas duplicadas

El equilibrado de la carga basado en rutas duplicadas sirve para equilibrar la carga de trabajo de salida entre varias interfaces. Esta es una solución basada en conexiones que tiene un mayor grado de flexibilidad que el equilibrado de la carga basado en DNS, pero no está activa para clientes locales. Las ventajas de utilizar este tipo de equilibrado de la carga son que se trata de una solución de servidor iSeries total, que tiene un grado de flexibilidad mayor que el DNS y que va bien para aquellas aplicaciones cuyo tráfico es mayoritariamente de salida, como HTTP y Telnet. Los inconvenientes son que se trata de una solución basada en la conexión (y no en la carga), que no está activa para los clientes locales y que no tiene efecto alguno sobre las peticiones de entrada.

En el ejemplo que aparece más abajo, los tres adaptadores del sistema están conectados al mismo segmento de LAN. Se ha configurado uno de los adaptadores como línea de entrada únicamente y los otros dos adaptadores como líneas de salida. Los clientes locales siguen trabajando de la misma manera que antes. Es decir, la interfaz de salida es la misma que la de entrada. Recuerde que un cliente local es cualquier sistema al que se puede llegar sin necesidad de un direccionador. Esta red podría tener un tamaño inmenso si se utilizasen conmutadores en lugar de direccionadores.



En las rutas indirectas duplicadas con prioridad >(5), se seleccionará el valor por omisión según la prioridad de la ruta

Ventajas:
- Solución total AS/400
- Más flexibilidad que un DNS
- Bueno para HTTP, Telnet

Desventajas:
- Basado en la conexión, no en la carga
- Inactivo para clientes locales
- Sin efecto en solicitudes de entrada

RZAJW511-0

¿Dónde hay que configurarlo?

Esto se puede configurar en la línea de mandatos de la pantalla Añadir ruta TCP/IP y también en la interfaz gráfica, que es iSeries Navigator. El primer parámetro es la prioridad de ruta duplicada y el segundo, la interfaz de enlace preferida. Si se deja el valor por omisión de prioridad de ruta duplicada, que es 5, no sucede nada. Si se establece un valor mayor que 5, las conexiones se distribuirán entre las rutas que tengan la misma prioridad. La interfaz de enlace preferida se utiliza para enlazar una ruta con una interfaz concreta por dirección IP en lugar de la primera que vea el sistema.

En el ejemplo anterior, hay un adaptador ″de entrada″ (10.6.7.3) cuya prioridad de ruta duplicada es 6. La de los otros dos adaptadores es 8. Dado que la prioridad de ruta duplicada de uno de los adaptadores es 6, este no se seleccionará para una conexión de salida a menos que fallen todas las interfaces cuya prioridad de ruta individual es 8.

Conviene que todas las interfaces de salida tengan la misma prioridad. Si algunas interfaces tienen un valor determinado y el resto de ellas otro, solo se utilizarán aquellas cuyo valor sea el más alto.

Observará que el DNS señala hacia la interfaz 10.6.7.3, lo que la convierte en la interfaz de entrada. Aunque se decida no utilizar la prioridad de ruta duplicada, se ha de definir siempre una ruta por omisión fuera del sistema en cada interfaz, utilizando para ello el parámetro de interfaz de enlace preferida.

Conmutación por anomalía de adaptador utilizando IP virtual y ARP por proxy

Situación

Su iSeries de producción maneja la entrada de datos por parte de clientes remotos y de clientes de LAN. En él está situada una aplicación crítica de la empresa. A medida que la empresa ha ido creciendo, cada vez se exige más del iSeries y de la red. Debido al crecimiento, se ha hecho imprescindible que el iSeries esté funcionando en la red de forma continuada, sin que se den tiempos de indisponibilidad. Si, por

cualquier razón, un adaptador de la red quedara temporalmente fuera de servicio, el iSeries debería tener otros adaptadores que tomasen el control y así los clientes de la red ni se enterarían de las anomalías producidas.

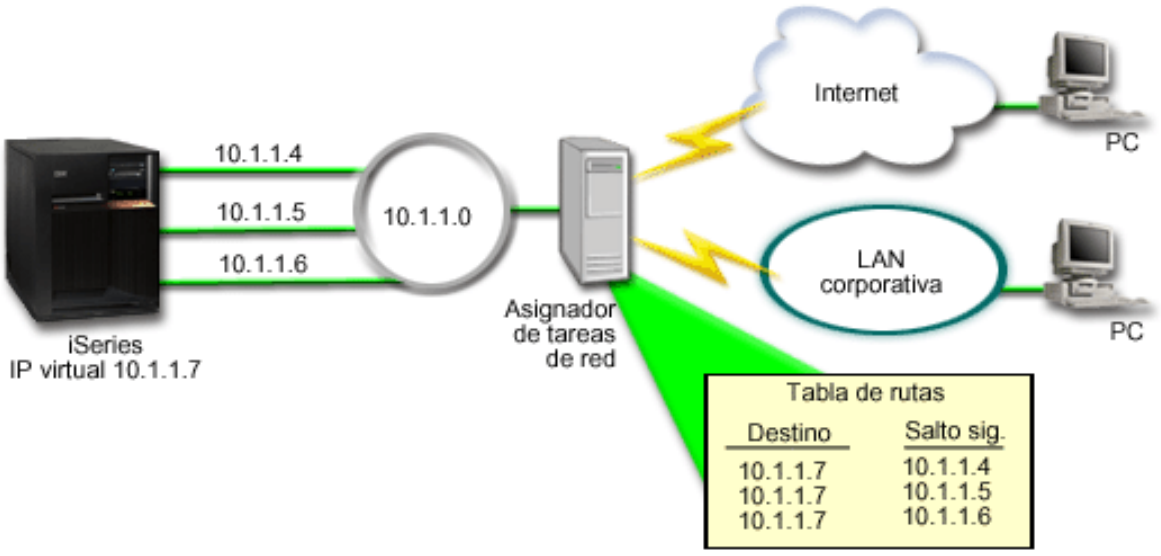
Objetivos

En el concepto de disponibilidad intervienen numerosos aspectos distintos, como son la existencia de componentes redundantes y de reserva que reemplacen a los componentes averiados. En este escenario, nos proponemos como objetivo mantener la disponibilidad de la red para los clientes del iSeries en el caso de que se produzca una anomalía de adaptador.

Detalles

Una manera de manejar el escenario anterior consiste en tener múltiples conexiones físicas entre el iSeries y la LAN. Fíjese en la siguiente figura:

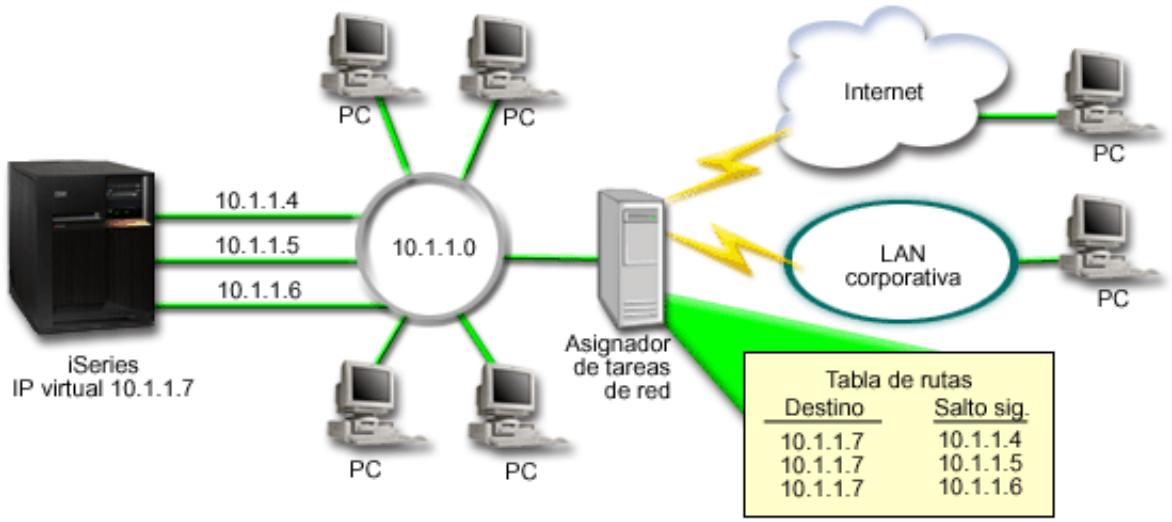
Figura 1. Conmutación por anomalía de adaptador sin clientes locales



Cada una de las conexiones físicas tendría una dirección IP distinta. Luego se podría asignar una dirección de IP virtual al sistema. Esta sería la dirección mediante la que todos los clientes reconocerían el sistema. Todos los clientes remotos (clientes que no están físicamente conectados a la misma LAN que el iSeries) se comunicarían con el iSeries por medio de un servidor de equilibrado de carga externo como puede ser un asignador de tareas de red. Cuando las peticiones IP procedentes de los clientes remotos pasasen por el asignador de tareas de red, este direccionaría las direcciones de IP virtual a uno de los adaptadores de red situados en el iSeries.

Si la LAN a la que está conectado el iSeries tuviera clientes, estos no emplearían el asignador de tareas de red para dirigir su tráfico enlazado localmente, porque ello supondría una sobrecarga innecesaria para el asignador de tareas. Usted podría crear en cada cliente entradas de ruta similares a las tablas de rutas situadas en el asignador de tareas de red; pero, cuando el número de clientes fuese muy elevado, esta solución sería muy difícil de llevar a la práctica. Esta situación es la que se ilustra en la siguiente figura.

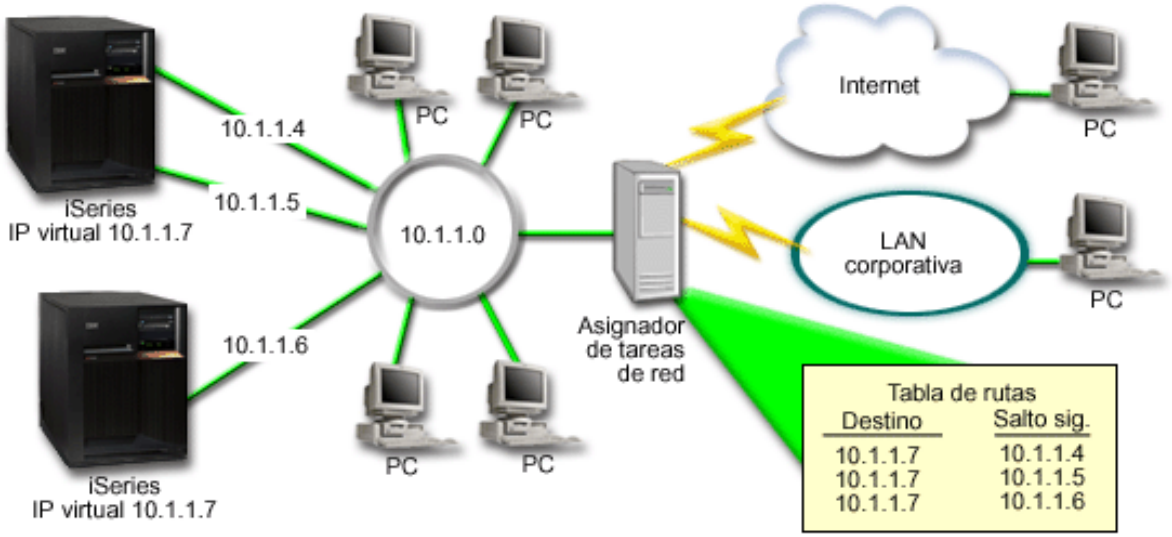
Figura 2. Conmutación por anomalía de adaptador con clientes locales



En OS/400 V5R2, ahora los clientes locales (clientes que están conectados a la misma LAN que el iSeries) se pueden conectar a la dirección de IP virtual del iSeries por medio de ARP. Esto permite asimismo que los clientes locales tengan una solución de conmutación por anomalía de adaptador.

La solución también puede implicar que se utilicen dos o más servidores iSeries para darse soporte mutuo. Si uno de los sistemas iSeries queda temporalmente fuera de servicio, el control puede pasar al segundo sistema (conmutación por anomalía). La siguiente figura muestra la misma configuración empleando dos servidores iSeries:

Figura 3. Conmutación por anomalía de adaptador con múltiples iSeries y clientes locales



El direccionamiento de paquetes equivale al direccionamiento de un solo iSeries y sus clientes remotos; sin embargo, hay una diferencia en el caso de los clientes locales. Si tiene múltiples iSeries que utilicen la misma dirección de IP virtual, solo podrá usar como proxy uno de los iSeries. En este caso, el iSeries que tiene las dos conexiones de LAN funcionaría como proxy.

Pasos de configuración

La configuración del equilibrado de la carga de trabajo utilizando IP virtual y ARP por proxy es muy parecida a las configuraciones de TCP/IP estándar con la adición de una interfaz de TCP/IP virtual. En el caso anterior de conmutación por anomalía de adaptador con clientes locales, los pasos de configuración general serían:

1. **Configurar una interfaz de TCP/IP virtual.**

   Utilizando iSeries Navigator, cree una interfaz de TCP/IP virtual. Para acceder al asistente Interfaz nueva de IP Virtual, pulse:
   Red—>**Configuración de TCP/IP**->**IPv4**->**Interfaces**. Luego, pulse **Interfaces** con el botón derecho del ratón y elija **Interfaz nueva**->**IP virtual**.

   En nuestro ejemplo, entraríamos la dirección IP 10.1.1.7 con una máscara de subred igual a 255.255.255.255. Una vez creada la interfaz virtual, púlsela con el botón derecho del ratón y seleccione **Propiedades**. Pulse la pestaña **Avanzadas** y ponga una marca de selección en el recuadro **Habilitar ARP por proxy**.

2. **Crear interfaces TCP/IP para todas las conexiones LAN físicas.**

   Utilice el asistente Crear interfaz TCP/IP para crear sus interfaces TCP/IP. El asistente está en iSeries Navigator; para acceder a él, pulse:
   Red—>**Configuración de TCP/IP**->**IPv4**->**Interfaces**. Luego, pulse **Interfaces** con el botón derecho del ratón y elija **Interfaz nueva**->**Red de área local**. Siga las instrucciones del asistente para cada una de las conexiones de LAN.

   En nuestro ejemplo, ejecute el asistente tres veces, entrando las direcciones IP 10.1.1.4, 10.1.1.5 y 10.1.1.6 con una máscara de subred igual a 255.255.255.0. Cuando haya terminado con cada una de las interfaces, pulse cada una de ellas con el botón derecho del ratón y elija **Propiedades**. En la pestaña **Avanzadas**, asocie la interfaz a la interfaz de IP virtual que creó en el paso 1. Puede asociar las interfaces con el recuadro de selección **Interfaz local asociada**.

Otras fuentes de información sobre direccionamiento y equilibrado de la carga de trabajo TCP/IP

El DNS es un sistema avanzado para gestionar los nombres de sistema principal asociados a las direcciones de protocolo Internet (IP) en las redes TCP/IP. En esta página hallará los procedimientos y conceptos básicos necesarios para configurar y administrar el DNS.

En la página Particiones lógicas hallará más información detallada y de preparación.

La página NAT y la administración de filtro IP le ayudará a gestionar las reglas de filtrado. Entre otras funciones, se incluye la adición de comentarios, la edición y la visualización.

En el tema OptiConnect  , hallará información sobre el direccionamiento OptiConnect. Es un manual en línea del servidor iSeries titulado *OptiConnect for OS/400*.

El protocolo punto a punto se utiliza habitualmente para conectar una máquina a Internet. Es un estándar Internet y el protocolo más utilizado por los proveedores de servicios de Internet (ISP).

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
500 Columbus Avenue
Thornwood, NY 10594-1785
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
Tokyo 106, 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 del mismo con el fin de: (i) intercambiar la información entre programas creados independientemente y otros programas (incluyendo éste) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
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 esta información y todo el material bajo licencia disponible para el mismo, los proporciona IBM bajo los términos del Acuerdo de Cliente IBM, el Acuerdo de Licencia de Programa IBM o cualquier otro acuerdo equivalente entre ambas partes.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:
e (logotipo)
IBM
iSeries
Operating System/400
OS/400

Los demás nombres de compañías, productos y servicios pueden ser marcas registradas o de servicio de otras empresas.

Términos y condiciones para descargar e imprimir publicaciones

Los permisos para la utilización de las publicaciones cuya descarga ha seleccionado, se otorgan en base a los siguientes términos y condiciones, y la indicación por la presente de su aceptación.

Uso personal: puede reproducir estas publicaciones para su uso personal y no comercial, siempre que se conserven todos los avisos de propiedad. No puede distribuir, visualizar o realizar trabajos derivados de estas publicaciones, o parte de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente en su empresa, siempre que se conserven todos los avisos de propiedad. No puede realizar trabajos derivados de estas publicaciones, ni reproducir, distribuir o visualizar estas publicaciones o parte de ellas fuera de su empresa, sin el consentimiento explícito de IBM.

Excepto los permisos explícitamente otorgados por la presente, no se otorga ningún permiso, licencia o derecho, implícita o explícitamente, sobre las publicaciones o la información, datos, software o demás propiedad intelectual aquí contenida.

IBM se reserva el derecho de retirar los permisos aquí otorgados siempre que, a su discreción, el uso de las publicaciones se realice en detrimento de sus intereses o, a decisión de IBM, no se cumplan correctamente las instrucciones anteriores.

No puede descargar, exportar o reexportar esta información si no es en total conformidad con todas las legislaciones y regulaciones aplicables, incluyendo todas las legislaciones y regulaciones de exportación de Estados Unidos. IBM NO EFECTÚA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN ″TAL CUAL″ SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUYENDO, PERO NO LIMITÁNDOSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN Y ADECUACIÓN A UN PROPÓSITO DETERMINADO.

Todos los materiales son copyright de IBM Corporation.

Al descargar o imprimir una publicación desde este sitio, indica su aceptación de estos términos y condiciones.

Declaración de limitación de responsabilidad

Este documento contiene ejemplos de programación.

IBM le otorga una licencia de copyright no exclusiva para utilizar todos los ejemplos de código de programación a partir de los cuales pueda generar una función similar adaptada a sus necesidades concretas.

IBM ofrece todos los ejemplos de código sólo a efectos ilustrativos. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones posibles. IBM, por lo tanto, no puede garantizar o implicar la fiabilidad, la facilidad de mantenimiento o la función de dichos programas.

Todos los programas aquí contenidos se proporcionan ″TAL CUAL″ sin ninguna garantía de ningún tipo. Las garantías implícitas de no vulneración, de comerciabilidad e idoneidad para un propósito particular se excluyen expresamente.

Impreso en España