IBM

System i

Redes - Direccionamiento y equilibrado de la carga de trabajo TCP/IP

Versión 6 Release 1

System i

Redes - Direccionamiento y equilibrado de la carga de trabajo TCP/IP

Versión 6 Release 1

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información de la sección “Avisos”, en la página 35.

Esta edición se aplica a la versión 6, release 1, modificación 0 de IBM i5/OS (número de producto 5761-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

Puede direccionar y equilibrar el tráfico TCP/IP del sistema utilizando las funciones de direccionamiento integradas para eliminar la necesidad de un direccionador externo.

Los métodos de direccionamiento y de equilibrado de la carga de trabajo, así como la información preparatoria, le ayudarán a comprender en qué consisten las opciones que podrá tener en el sistema. Los métodos están descritos por medio de una ilustración, lo que permite ver cómo se realizan las conexiones. En estos métodos no se incluyen las instrucciones de configuración de las técnicas de direccionamiento. Este tema se centra en los conceptos y principios de direccionamiento que debe conocer para que el sistema funcione mejor para usted.

Porqué estos métodos son importantes para usted

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 sistema al equilibrar la carga del trabajo de comunicaciones en el sistema.

Novedades de V6R1

Lea sobre la información nueva o modificada considerablemente para el tema de equilibrado de la carga de trabajo y direccionamiento TCP/IP.

Nuevo protocolo de direccionamiento soportado

El sistema operativo i5/OS se ha ampliado para dar soporte al protocolo de direccionamiento OSPF (Open Shortest Path First). *Open Shortest Path First* (OSPF) es un protocolo de direccionamiento de estado de enlace en el que los direccionadores o sistemas dentro de la misma área mantienen una base de datos de estado de enlace idéntica que describe la topología del área.

Mejoras de IP virtual

Las mejoras de IP virtual que afectan al tema de equilibrado de la carga de trabajo y direccionamiento TCP/IP son las siguientes:

- El soporte de dirección IP virtual se ha ampliado para incluir direcciones IPv6.
- Una interfaz de protocolo punto a punto (PPP) o una interfaz L2TP (Layer Two Tunneling Protocol) pueden utilizar una dirección IP virtual como la dirección IP local para proporcionar tolerancia a errores para conexiones remotas.
- Puede configurar ARP por proxy de IP virtual mientras la interfaz de IP virtual está activa.

Puede encontrar estas mejoras de IPv6 en los temas “Direccionamiento con IP virtual” en la página 17 y “Tolerancia a errores” en la página 18.

Nuevo método de equilibrado de carga documentado

Aunque la utilización de IP virtual y ARP por proxy como método de equilibrado de carga no es nuevo para V6R1, este método de equilibrado de carga no estaba documentado anteriormente en este documento. Se ha añadido un tema “Equilibrado de la carga mediante IP virtual y ARP por proxy” en la página 27 para presentar este método de equilibrado de carga.

Cómo visualizar las novedades o cambios

Para facilitar la visualización de los cambios técnicos, el Information center utiliza:
- La imagen » para marcar el inicio de información nueva o cambiada.
- La imagen « para marcar el final de la información nueva o cambiada.

En archivos PDF, puede ver barras de revisión (|) en el margen izquierdo de la información nueva y modificada.

Para obtener otra información acerca de los cambios y novedades de este release, consulte el Memorándum para los usuarios.

Archivo PDF para el direccionamiento y equilibrado de la carga de trabajo TCP/IP

Puede visualizar e imprimir un archivo PDF de esta información.

Para visualizar o bajar la versión PDF de este documento, seleccione Direccionamiento y equilibrado de carga de trabajo TCP/IP (aproximadamente 1,40 MB).

Guardar archivos PDF

Para guardar un archivo PDF en la estación de trabajo para poder verlo o imprimirlo:
1. Pulse con el botón derecho del ratón en el enlace del PDF del navegador.
2. Pulse la opción destinada a guardar el PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el archivo PDF.
4. Pulse **Guardar**.

Bajar Adobe Reader

Necesita tener instalado Adobe Reader en el sistema para ver o imprimir estos PDF. Puede bajar una copia libre del sitio web de Adobe (www.adobe.com/products/acrobat/readstep.html) .

Referencia relacionada

"Información relacionada con el direccionamiento y equilibrado de la carga de trabajo TCP/IP" en la página 33
Otros documentos del information center contienen información relacionada con el direccionamiento y equilibrado de la carga de trabajo TCP/IP.

Funciones de direccionamiento TCP/IP por release

Antes de planificar la utilización de una función de direccionamiento, asegúrese de que el sistema tiene instalado el release correcto para dar soporte a dicha función.

V3R1: 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

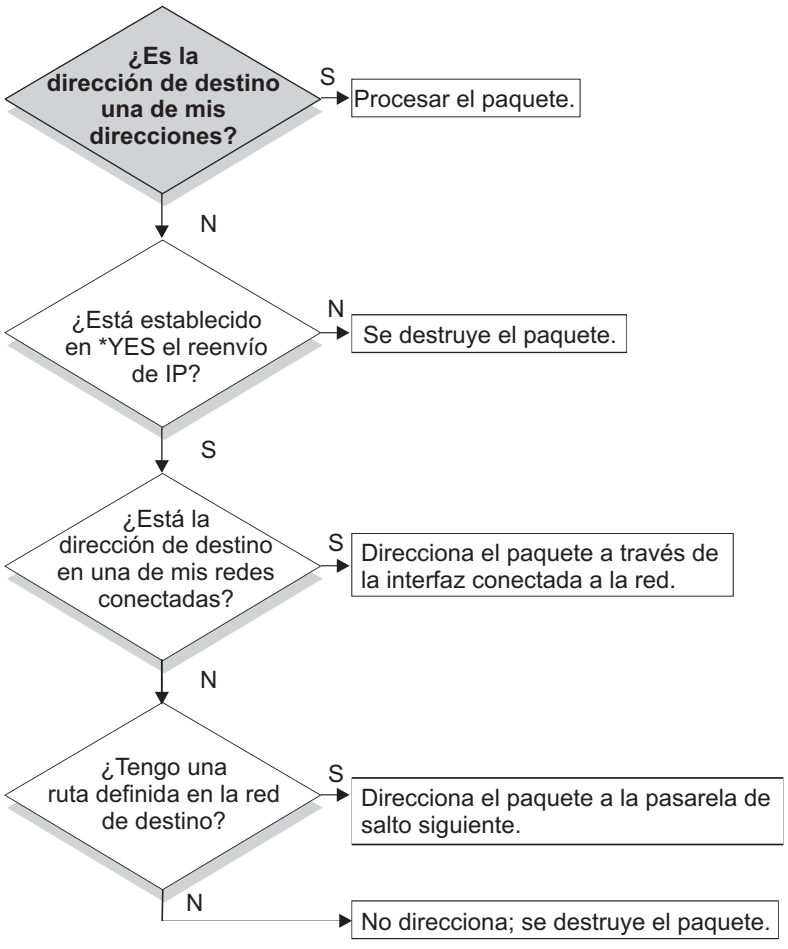
V5R4: Lista de interfaces favoritas

V6R1: protocolo de direccionamiento OSPF (Open Shortest Path First) y soporte de dirección IP virtual para direcciones IPv6

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 sistema operativo i5/OS. El flujo real puede ser diferente, pero el resultado final debe ser 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 i5/OS no está conectado directamente al sistema principal remoto, se lleva a cabo una búsqueda en la tabla de direccionamiento. 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 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

Estas reglas se aplican a TCP/IP en general y a TCP/IP en el sistema operativo i5/OS.

Para gestionar paquetes en el sistema, debe tener presentes estas reglas cuando implemente las funciones de direccionamiento en el sistema. Estas reglas 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.

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

  Nota: Las direcciones del protocolo Internet virtual (sin conexión) se asignan al sistema.
- 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.
- La dirección IP y la máscara definen la dirección de la red conectada.
- 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.

Direccionamiento con conexiones punto a punto

Por medio de conexiones punto a punto, los datos se pueden enviar del sistema local a un sistema remoto o bien de una red local a una red remota.

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. Consulte el tema Conexiones PPP para encontrar más información sobre cómo configurar y gestionar las conexiones PPP.

Las conexiones punto a punto pueden utilizarse en líneas de acceso telefónico, líneas no conmutadas 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

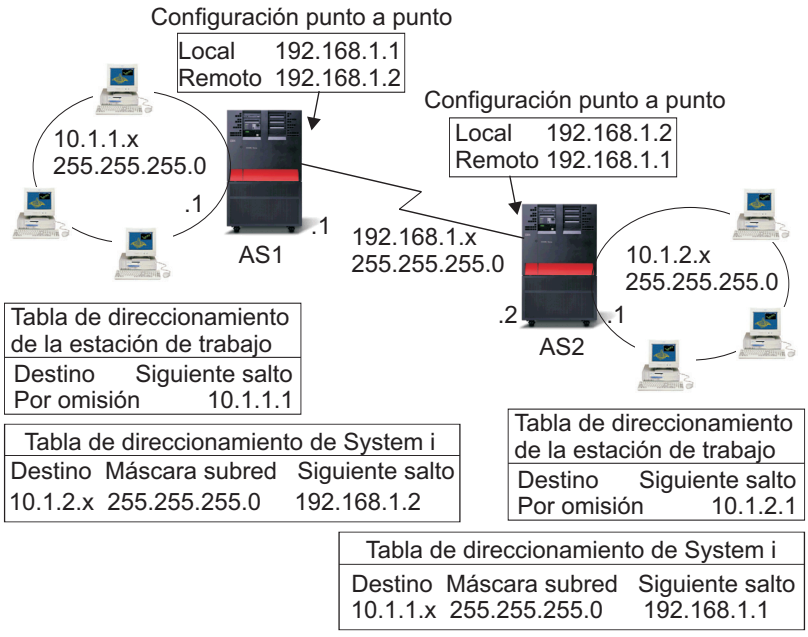
A simple vista, la forma más sencilla de configurar una conexión punto a punto es utilizar una conexión numerada. Una conexión numerada es una definición punto a punto que tiene una dirección IP exclusiva definida para cada uno de los extremos de la conexión.

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 sistema, 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 sistema 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 siguiente puede verse una conexión de red numerada entre dos plataformas System i. 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

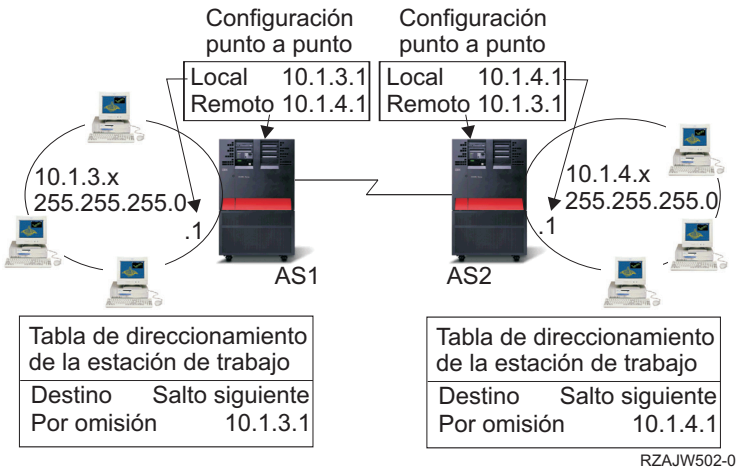
Una conexión no numerada es un método más complejo de definir una conexión punto a punto que una conexión numerada. Sin embargo, las conexiones no numeradas pueden constituir una manera mejor y más sencilla de gestionar la red.

El proceso de selección de rutas de i5/OS depende de que haya una dirección IP para cada interfaz. En una conexión no numerada, la interfaz punto a punto no necesita tener una dirección exclusiva. La dirección IP de la interfaz del sistema 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.

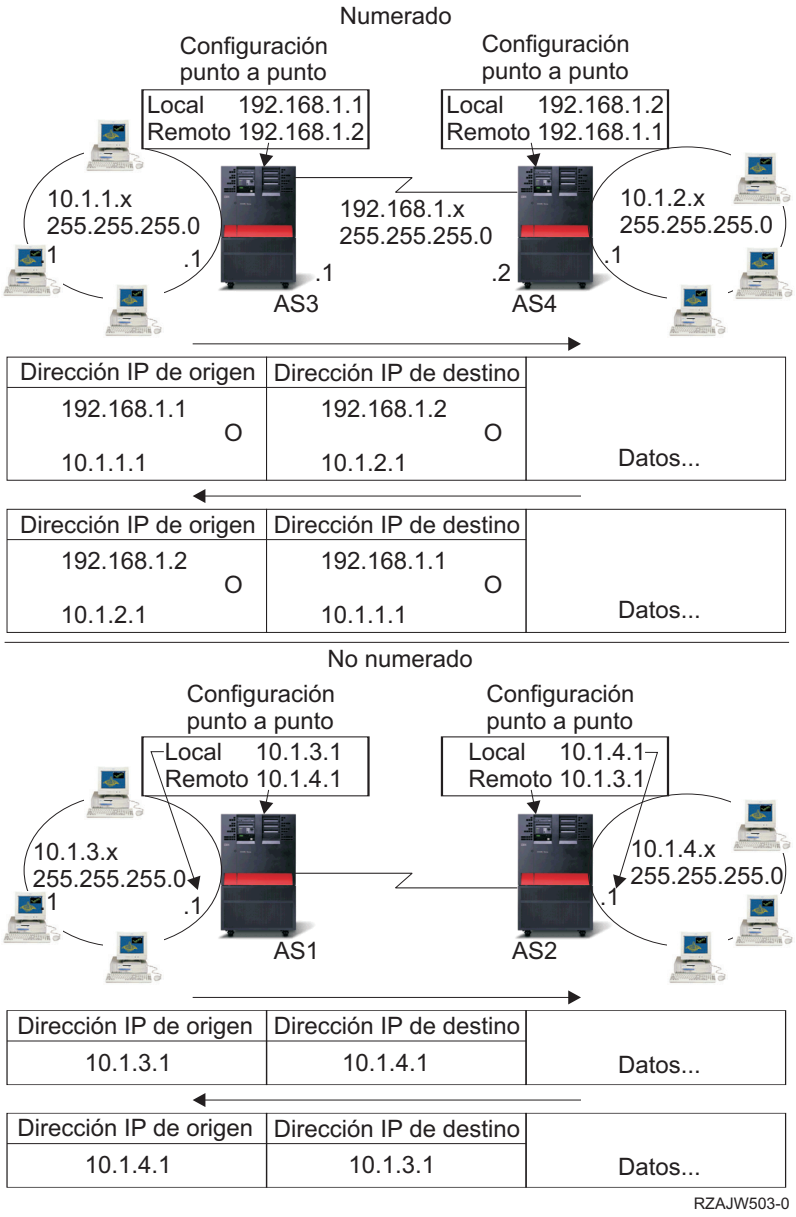


En el ejemplo también interviene AS2. AS2 está conectado a la red LAN 10.1.4.x por medio de la dirección 10.1.4.1. Esto permite a AS2 comunicarse directamente con cualquier sistema de la red 10.1.4.x. Cada uno de estos dos sistemas (AS1 y AS2) añade la dirección remota a su respectiva tabla de direccionamiento 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 estos dos sistemas se encontrasen en la misma sala, basta 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 utilizaran adaptadores de LAN sin añadir ninguna entrada de direccionamiento al sistema. Para ello, cada sistema toma prestada la dirección IP del sistema remoto con el propósito de utilizarla en la resolución de ruta.

Flujo de datos de las conexiones numeradas frente al de las no numeradas

En la figura siguiente se muestran las direcciones que se utilizarán 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.



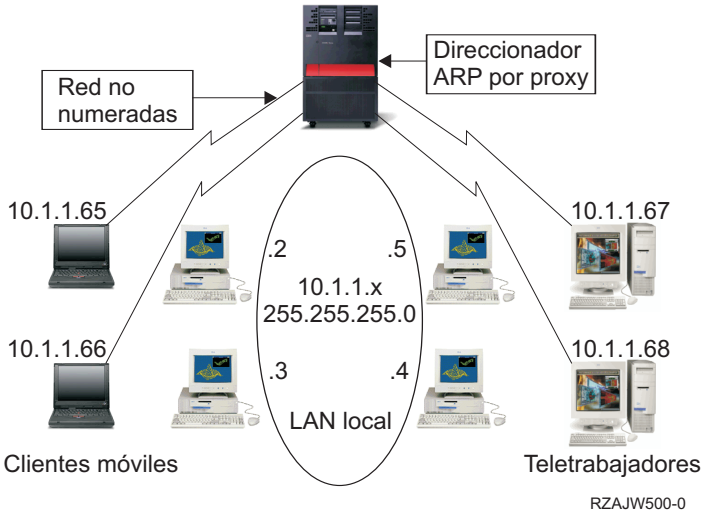
Conceptos relacionados

Conexiones PPP

Direccionamiento de protocolo de resolución de direcciones (ARP) por proxy

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. Este tema contiene también una descripción de las subredes transparentes, que es una ampliación de la técnica de direccionamiento ARP por proxy.

El direccionamiento ARP permite que redes separadas y físicamente distintas den la impresión de formar una sola red lógica. Permite que sistemas que no están conectados directamente a una red de área local (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.

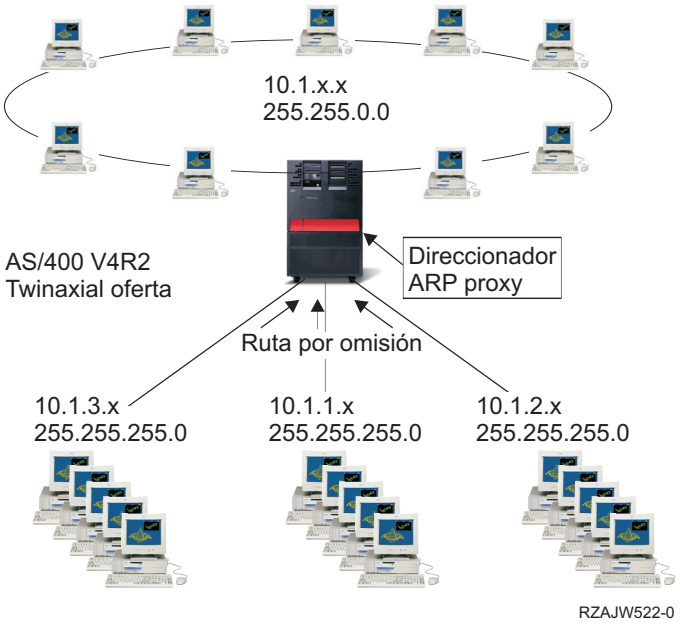


Cuando un sistema de la LAN local (10.1.1.x) desea enviar datos a uno de los sistemas remotos, primero realizará una petición ARP. Esta es una difusión que se manda a todos los sistemas conectados al segmento de LAN para solicitar la dirección del sistema destino. Los sistemas conectados remotamente no verán la difusión. Pero con ARP por proxy, el sistema sabe qué sistemas están conectados remotamente. Si el sistema observa una petición ARP dirigida a uno de los sistemas conectados remotamente, el sistema responderá a la petición ARP con su dirección. El sistema, 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 sistema no responderá a la petición ARP y el sistema peticionario no enviará los datos.

Subredes transparentes

Podrá utilizar las subredes transparentes como una manera de ampliar el concepto de ARP por proxy. 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.

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 siguiente 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).



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 a través de 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 de la plataforma System i. 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. Esta acción hace que el tráfico dirigido a la red local se direccione de manera automática al sistema de la red local. Este sistema, a su vez, direcciona los datos al sistema remoto correcto. El sistema 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 sistema 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 es un método de bajo mantenimiento que reconfigura automáticamente las tablas de direccionamiento a medida que cambia la red.

El direccionamiento dinámico lo proporcionan los protocolos de pasarela interior (IGP). El protocolo de información de direccionamiento (RIP) y el protocolo Abrir primero vía de acceso más corta (OSPF) son los dos IGP a los que da soporte el sistema operativo i5/OS.

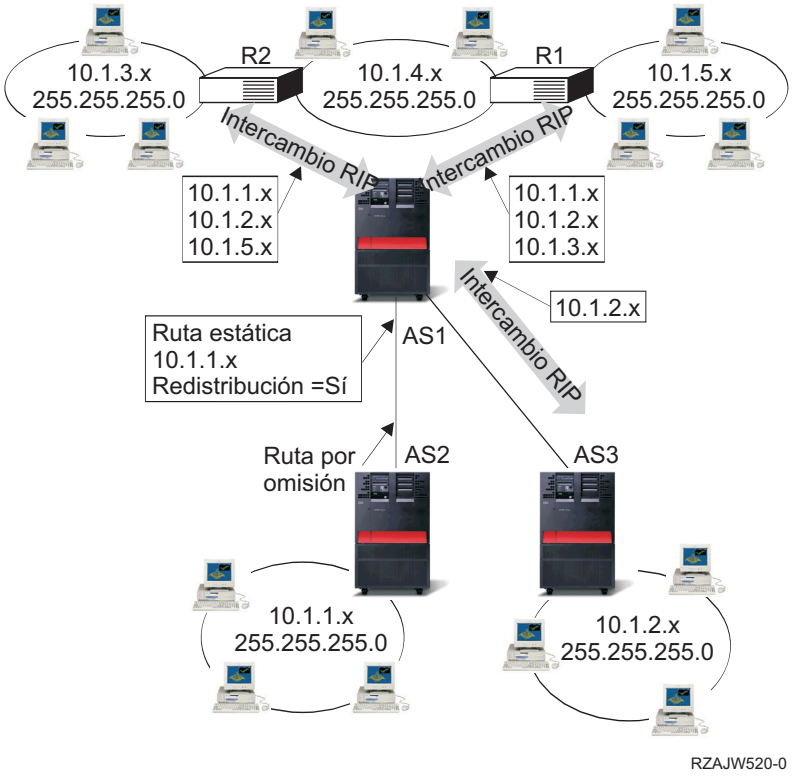
Protocolo de información de direccionamiento

Protocolo de información de direccionamiento (RIP) es un protocolo de direccionamiento de vectores de distancia. Los direccionadores que ejecutan el protocolo de vectores de distancia envían toda o una parte de sus tablas de direccionamiento en mensajes de actualización de direccionamiento a sus vecinos.

Se puede utilizar RIP para 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 la comunicación de red se detiene. Se ha añadido RIPv2 al producto System i con el fin de que se puedan enviar y recibir paquetes RIP para actualizar las rutas en toda la red.

En la figura siguiente, 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 a la plataforma System i central (AS1). AS2 hace que se inicie el sistema 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.



RZAJW520-0

El proceso siguiente describe el direccionamiento de tráfico en la figura anterior.

- 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.

OSPF (Open Shortest Path First)

Open Shortest Path First (OSPF) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP).

En una red OSPF, los direccionadores o sistemas de la misma área mantienen una base de datos de enlace-estado idéntica que describe la topología del área. Cada direccionador o sistema del área genera su propia base de datos de enlace-estado a partir de los anuncios de enlace-estado (LSA) que recibe de los demás direccionadores o sistemas de la misma área y de los LSA que él mismo genera. El LSA es un

paquete que contiene información sobre los vecinos y los costes de cada vía. Basándose en la base de datos de enlace-estado, cada direccionador o sistema calcula un árbol de extensión de vía más corta, siendo él mismo la raíz, utilizando el algoritmo SPF.

Las ventajas principales de OSPF son las siguientes:

- En comparación con los protocolos de direccionamiento de distancia-vector como el protocolo de información de direccionamiento (RIP), OSPF es más adecuado para servir entre redes heterogéneas de gran tamaño. OSPF puede recalcular las rutas en muy poco tiempo cuando cambia la topología de la red.
- Con OSPF, puede dividir un sistema autónomo (AS) en áreas y mantenerlas separadas para disminuir el tráfico de direccionamiento de OSPF y el tamaño de la base de datos de enlace-estado de cada área.
- OSPF proporciona un direccionamiento multivía de coste equivalente. Se pueden añadir rutas duplicadas a la pila TCP utilizando saltos siguientes distintos.

Protocolo OSPF Hello e intercambio de base de datos de enlace-estado

Los direccionadores o sistemas de una red OSPF, después de haberse asegurado de que sus interfaces son funcionales, envían en primer lugar paquetes Hello, utilizando el protocolo Hello por sus interfaces OSPF, para descubrir vecinos. Vecinos son los direccionadores o sistemas que tienen interfaces con la red común. Después, los direccionadores o sistemas vecinos intercambian sus bases de datos de enlace-estado para establecer adyacencias.

La siguiente figura ilustra el proceso de descubrir vecinos y establecer adyacencias en el caso de dos sistemas de la subred 9.7.85.0. Cada sistema tiene una interfaz OSPF con la subred común 9.7.85.0 (interfaz 9.7.85.1 para el sistema A e interfaz 9.7.85.2 para el sistema B). La subred 9.7.85.0 pertenece al área 1.1.1.1.

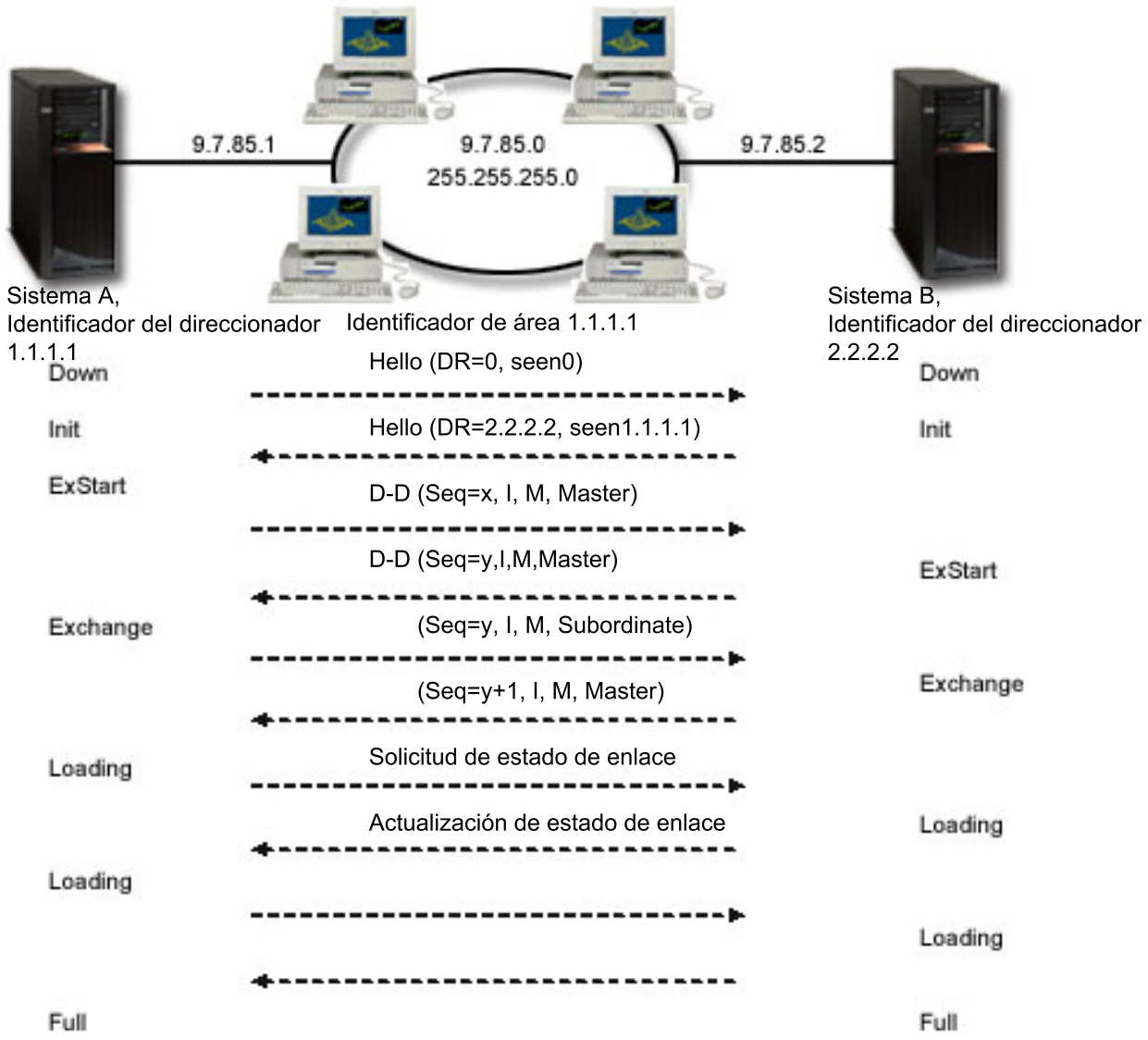


Figura 1. Protocolo OSPF Hello e intercambio de base de datos

Fase EXSTART
Es el primero paso del intercambio de bases de datos de enlace-estado. Los dos sistemas negocian quién hace de maestro y quién hace de subordinado.

Fase EXCHANGE
Los dos sistemas intercambian paquetes de descripción de base de datos para averiguar qué anuncios de enlace-estado (LSA) no están en la base de datos de enlace-estado de cada sistema. Cada sistema almacena los LSA que no están en la base de datos de enlace-estado en la lista de retransmisiones.

Fase LOADING
Cada sistema envía paquetes de petición de enlace estado para pedir al vecino (en este ejemplo, sería el otros sistema) que envíe los LSA completos que se almacenaron en la lista de retransmisiones durante la fase EXCHANGE. El vecino responde a la petición con los LSA en paquetes de actualización de enlace estado.

Fase FULL
Cuando dos sistemas terminan de intercambiarse los LSA, y sus bases de datos de enlace-estado ya están sincronizadas, se establece la adyacencia entre los dos sistemas.

Cuando ya se han establecido adyacencias entre todos los direccionadores o sistemas de un área, cada direccionador o sistema del área envía periódicamente un LSA para compartir sus adyacencias o para informar de su cambio de estado. Comparando las adyacencias establecidas con los LSA, los direccionadores o sistemas del área pueden descubrir los cambios de topología del área y actualizar debidamente sus bases de datos de enlace-estado.

Direccionador designado y direccionador designado de reserva

En una red OSPF multiacceso que tenga como mínimo dos direccionadores conectados, los direccionadores eligen un direccionador designado y un direccionador designado de reserva utilizando el protocolo Hello. (Red multiacceso es aquella en la que múltiples dispositivos se pueden conectar y comunicar simultáneamente).

El direccionador designado genera anuncios de enlace-estado (LSA) para toda la red multiacceso, envía los LSA a los otros direccionadores de la red y determina qué direccionadores deben ser los adyacentes. Los demás direccionadores de la red son adyacentes al direccionador designado. El direccionador designado disminuye el tráfico de la red y el tamaño de la base de datos de enlace-estado correspondiente a esta red.

El direccionador designado de reserva no presenta diferencias con los otros direccionadores, salvo que necesita establecer adyacencias con todos los direccionadores de la red (incluido el direccionador designado). El direccionador designado de reserva queda promocionado a ser el direccionador designado cuando falla el direccionador designado actual.

En la Figura 1, la subred 9.7.85.0 es una red de difusión. Por lo tanto, los direccionadores de la subred 9.7.85.0 eligen un direccionador designado y un direccionador designado de reserva utilizando el protocolo Hello. En este ejemplo, el sistema A es elegido como direccionador designado y el sistema B, como direccionador designado de reserva.

Dividir un AS OSPF en áreas

A diferencia de RIP, el protocolo OSPF puede funcionar dentro de una jerarquía. La entidad más grande de la jerarquía es el sistema autónomo (AS). El AS es un grupo de redes bajo una administración común que comparten una estrategia de direccionamiento común. El AS se puede dividir en áreas, conectadas entre sí por direccionadores. El área consta de grupos de redes contiguas y de hosts conectados. La topología de un área es invisible para las entidades situadas fuera del área. Los direccionadores de una misma área tienen una base de datos de enlace-estado idéntica. Las topologías de áreas separadas permiten disminuir el tráfico de direccionamiento y reducir el tamaño de la base de datos de enlace-estado para cada área.

Un direccionador que esté situado en la frontera de las áreas OSPF y conecte esas áreas con la red troncal se llama direccionador de áreas fronterizo. El direccionador de áreas fronterizo tiene múltiples interfaces con múltiples áreas y mantiene bases de datos de enlace-estado separadas para cada área.

En la siguiente figura se han configurado dos áreas (el área 1.1.1.1 y el área 2.2.2.2). El Sistema B es un direccionador de áreas fronterizo, con la interfaz 9.7.85.2 conectada al área 1.1.1.1 y la interfaz 9.5.104.241 conectada al área 2.2.2.2. El Sistema B tiene dos bases de datos de enlace-estado, una para cada área. El sistema B establece adyacencias con el sistema A y el direccionador C en el área 1.1.1.1 a través de la interfaz 9.7.85.2, y establece adyacencia con el sistema D en el área 2.2.2.2 a través de la interfaz 9.5.104.241.

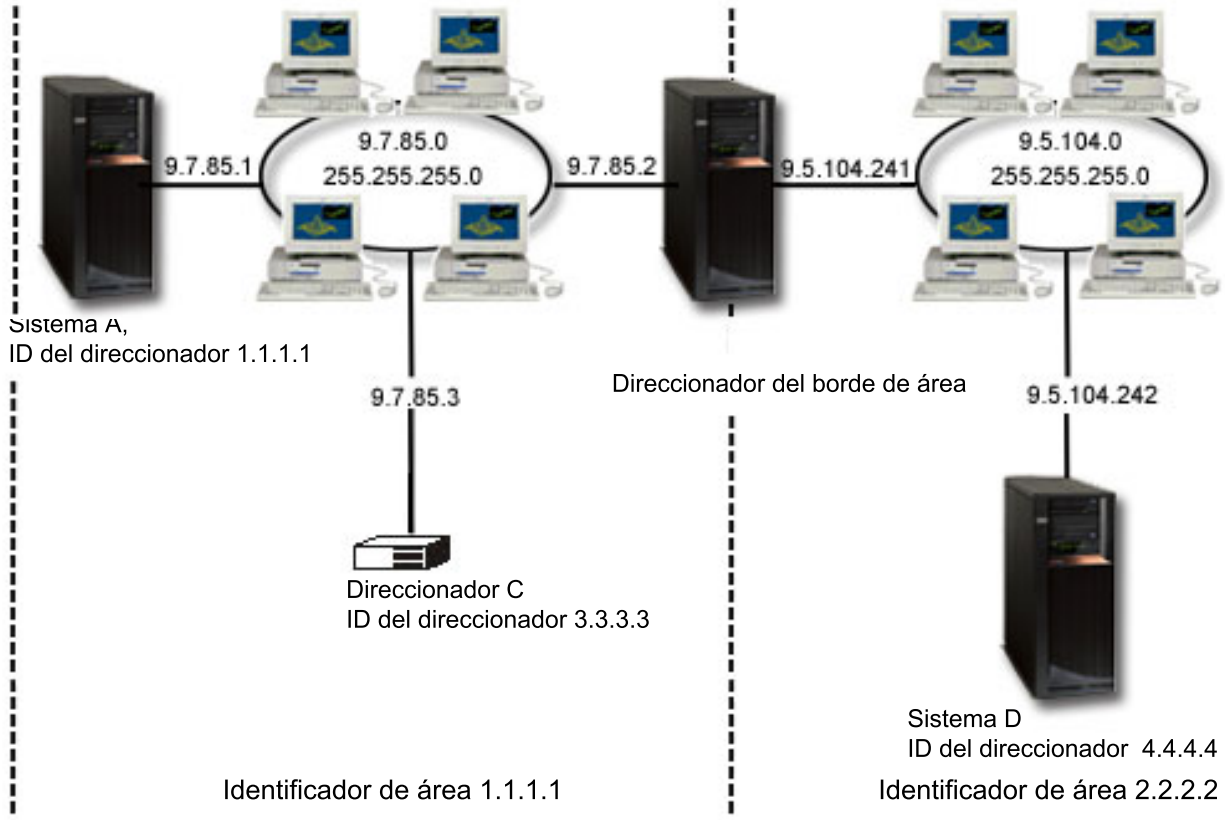


Figura 2. Dividir un AS OSPF en áreas

Conceptos relacionados

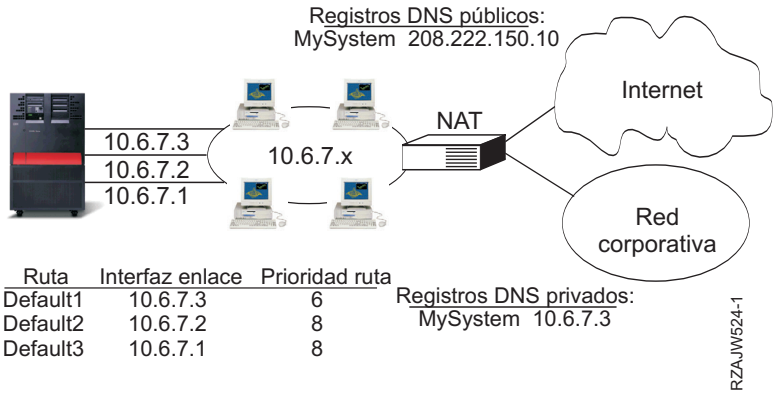
OSPF (Open Shortest Path First)

Enlace de ruta

El enlace de ruta le permite tener control sobre cuál es la interfaz utilizada para enviar paquetes de información de respuesta.

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 siguiente 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, se debe añadir las rutas duplicadas a cada interfaz. En este ejemplo se han 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.



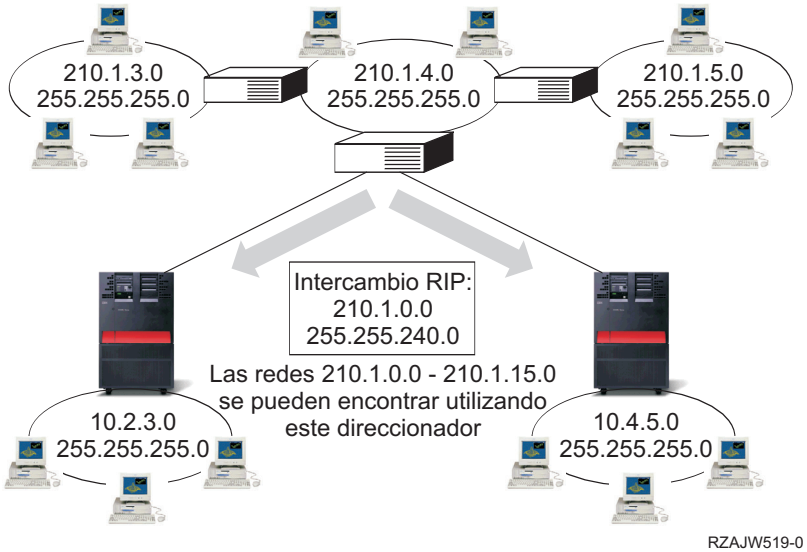
Direccionamiento interdominio sin clase

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.

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), puede pedir al ISP que las convierta 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.

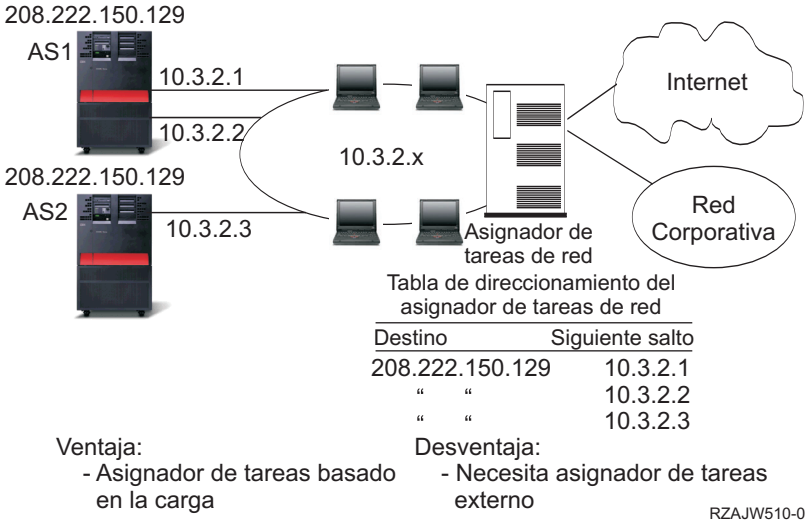


En este ejemplo, el direccionador está configurado para enviar un mensaje RIP con la dirección de red 210.1.0.0 y la máscara de subred 255.255.240.0. Esto indica a los sistemas que han de recibir los mensajes RIP dirigidos a las redes de la 210.1.0.0 a la 210.1.15.0 por medio de este direccionador. Este 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

IP virtual, denominado también interfaz sin circuito o de bucle de retorno, es una potente función que proporciona una manera de asignar una o varias direcciones al sistema sin la necesidad de enlazar la dirección con una interfaz física.

Puede utilizar esta función cuando interesa ejecutar múltiples instancias de un sistema 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 la plataforma System i, 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 sistema, tal como se muestra en la figura siguiente.



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 sistema. Lo ideal sería que los clientes remotos percibiesen el sistema como una única dirección IP. El modo en que el paquete entrante cruza la pasarela, recorre la red local y llega hasta el sistema debe resultar imperceptible para un cliente remoto. La manera de conseguirlo es utilizar IP virtual. Los clientes locales se comunicarán con el sistema 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 sistema 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 sistema 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 sistema no responderá nunca a una petición de protocolo de resolución de direcciones (ARP) enviada a la dirección de IP virtual, a menos que habilite ARP por proxy para la dirección IP virtual. En otras palabras, si se habilita ARP por proxy, una interfaz local puede responder a las peticiones ARP en nombre de la dirección IP virtual. De lo

contrario, los sistemas remotos deben tener definida una ruta para llegar a la dirección. Ahora puede configurar ARP por proxy de IP virtual para una interfaz de IP virtual mientras está activa.

En el ejemplo anterior, todas las estaciones de trabajo señalan hacia una de las interfaces 10.3.2, del sistema como pasarela de salto siguiente. Cuando un paquete llega al sistema, 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.

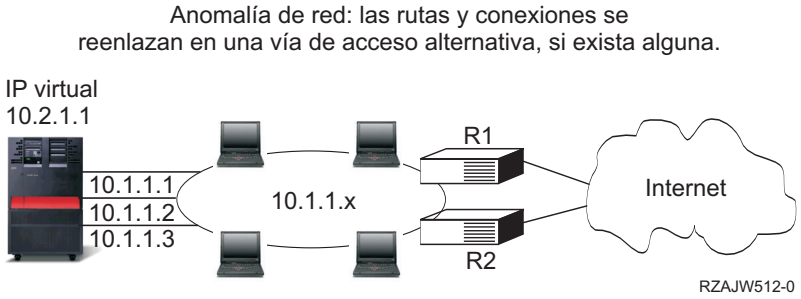
Los servidores de DNS (Sistemas de nombres de dominio) utilizan las direcciones del sistema solicitado. En este caso, todas las direcciones representan al mismo sistema. La función de IP virtual se puede utilizar cuando se unifican múltiples sistemas en uno de mayor tamaño.

El soporte de dirección IP virtual ahora incluye direcciones IPv6.

Tolerancia a errores

Otro uso que se puede dar a las direcciones de IP virtual es la protección contra anomalías de direccionador. La tolerancia a errores muestra varias formas diferentes de recuperar una ruta después de producirse un corte del suministro eléctrico.

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.

Una interfaz de protocolo punto a punto (PPP) o una interfaz de protocolo L2TP (Layer Two Tunneling Protocol) ahora puede utilizar una dirección IP local para proporcionar la tolerancia a errores para conexiones remotas.

Direccionamiento con conversión de direcciones de red (NAT)

El direccionamiento con NAT (conversión de direcciones de red) permite acceder a redes remotas, como Internet, al tiempo que protege la red privada enmascarando las direcciones IP utilizadas en ella.

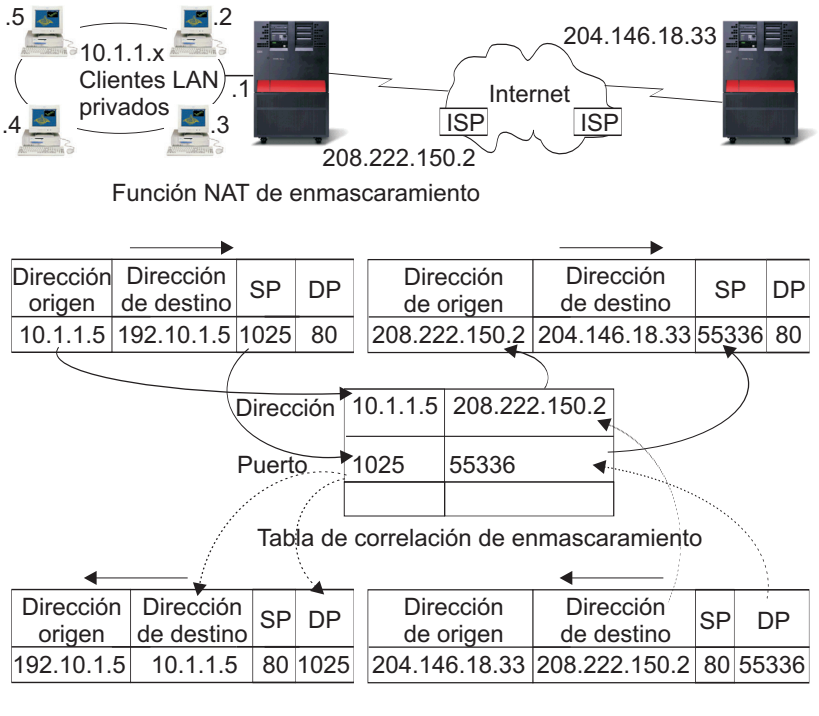
NAT da acceso a una red remota, que suele ser Internet, al tiempo que protege la red privada enmascarando las direcciones IP utilizadas dentro del cortafuegos.

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, la dirección enlazada con la interfaz pública es 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 (Protocolo punto a punto). 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 sistema operativo i5/OS. i5/OS tiene una dirección IP, asignada por el ISP local, como pasarela Internet. Se emplea el término *sistema conectado localmente* para hacer referencia a todos los sistemas de una red interna, sea cual sea el método de conexión (red de área local o red de área amplia) y la distancia que cubre la conexión. El término *sistemas externos* hace referencia a sistemas ubicados en Internet. La figura siguiente ilustra cómo funciona la NAT de enmascaramiento.



Desde la perspectiva de Internet, todas las estaciones de trabajo están en apariencia contenidas en el sistema; es decir, solo hay una dirección IP asociada al sistema y 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 i5/OS 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 a i5/OS

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 los sistemas conectados 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 entrada (respuesta y otros):

Este proceso, que es la contraparte del proceso de NAT de enmascaramiento de salida, desdobla el mensaje de salida correspondiente para obtener la información de estación de trabajo origen correcta.

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 un sistema conectado 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 del sistema 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 al sistema correcto conectado 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.

Proceso de NAT de enmascaramiento de salida:

Este proceso sustituye el puerto origen de un mensaje de salida por un número de puerto lógico exclusivo cuando el mensaje se envía desde la LAN privada a Internet.

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

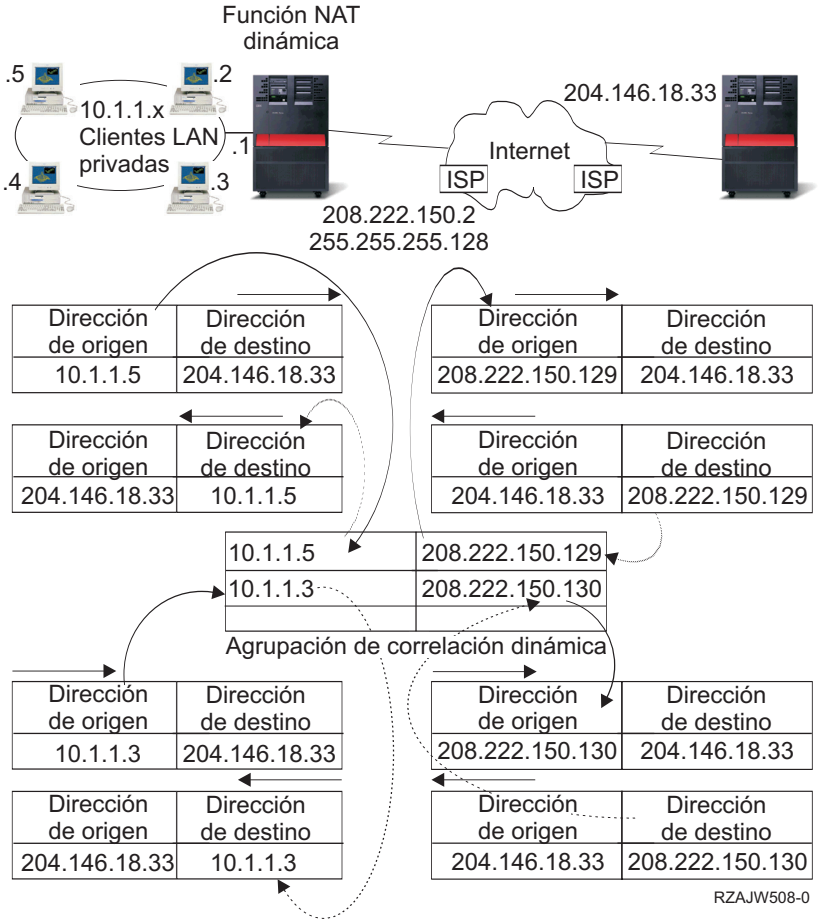
en la cabecera de transporte por un número exclusivo de puerto lógico. En el caso de los datagramas de salida, el número de puerto origen es el número de puerto local. Los pasos del proceso de salida de NAT de enmascaramiento son:

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.

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.

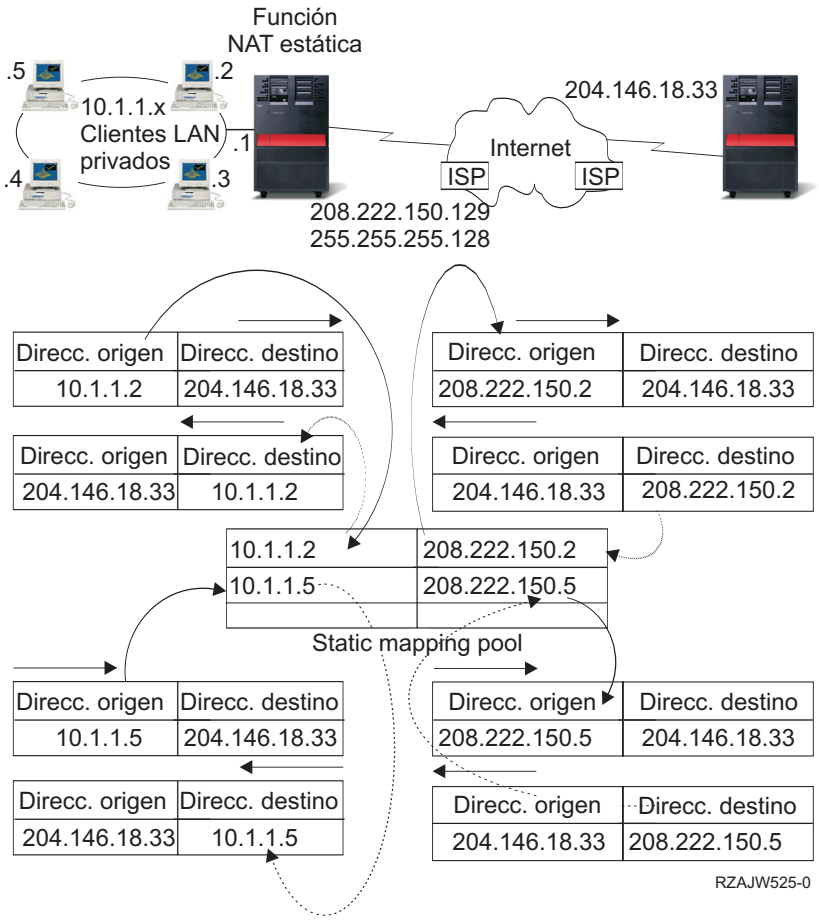
Cuando se realiza una conexión de salida, se mantiene y utiliza una agrupación de direcciones de red. A cada conexión se le asigna una dirección pública exclusiva. El número máximo de conexiones simultáneas es igual al número de direcciones públicas que hay en la agrupación. Es similar a una correspondencia biunívoca entre direcciones. La NAT dinámica le permite comunicarse con Internet a través de una dirección de NAT dinámica. La figura que sigue ilustra la NAT dinámica.



NAT estática

La NAT estática puede utilizar conexiones de entrada que van desde una red pública hasta una red privada.

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.



Conceptos relacionados

"Equilibrado de la carga basado en DNS" en la página 25
Puede utilizar el equilibrado de carga basado en DNS para la carga de trabajo de entrada. Si es necesario equilibrar la carga de los clientes locales, utilice el equilibrado de carga DNS.

Direccionamiento con OptiConnect y particiones lógicas

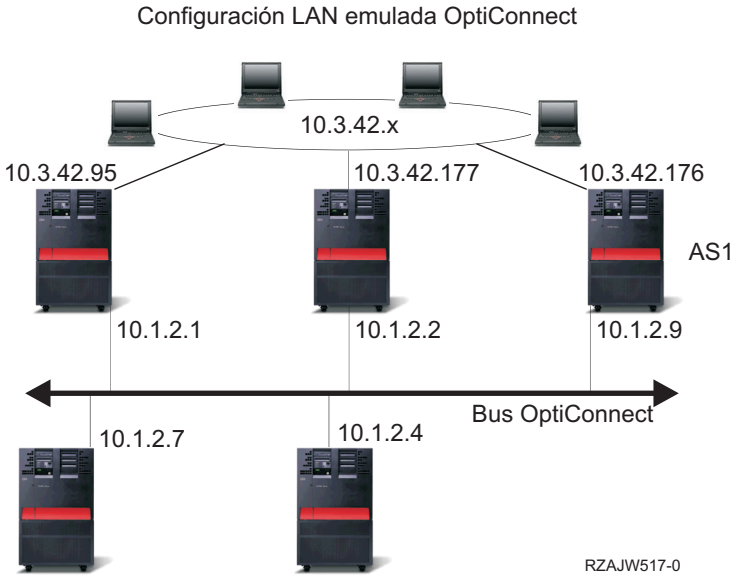
OptiConnect puede conectar varias plataformas System i mediante un bus de fibra óptica y alta velocidad. OptiConnect y las particiones lógicas constituyen otros entornos en los que utilizar los componentes básicos de direccionamiento, que son ARP por proxy, las conexiones punto a punto y las interfaces de IP virtual.

TCP/IP y OptiConnect

Puede 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 TCP/IP sobre OptiConnect 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, tal como se muestra en la figura siguiente. 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 sistemas 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. 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 sistema local. La interfaz local asociada puede ser la interfaz de LAN primaria del sistema, como se indica en la figura siguiente. La interfaz local asociada también puede ser una interfaz IP virtual.

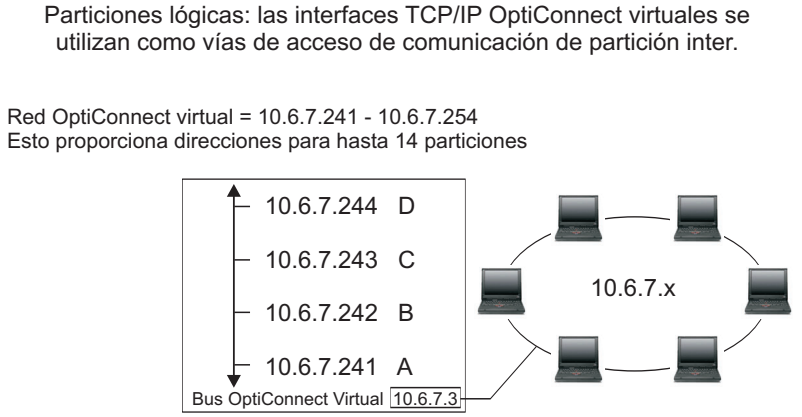
En la configuración punto a punto OptiConnect que utiliza IP virtual, se utiliza el bus OptiConnect a modo de colección de conexiones punto a punto. Se define una conexión no numerada para cada par de sistemas principales. Al igual que ocurre en la configuración punto a punto OptiConnect, no se necesita 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 sistema operativo i5/OS.

Direccionamiento con OptiConnect virtual y particiones lógicas

Cuando hay particiones lógicas, un sistema 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 sistema 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.



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 subred	MTU	Interfaz local asociada
10.6.7.3		10.6.7.4	D	10.6.7.4	VIRTUALIP	255.255.255.255	4096	NONE
10.6.7.2	D		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		10.6.7.3	C	10.6.7.3	VIRTUALIP	255.255.255.255	4096	NONE
10.6.7.2	C		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		10.6.7.2	B	10.6.7.2	VIRTUALIP	255.255.255.255	4096	NONE
10.6.7.3	B		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		10.6.7.1	A	10.6.7.1	TRNLINE	255.255.255.0	4096	NONE
10.6.7.3	A		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
Virtual OC Bus			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 *equilibrado de la carga de trabajo* consiste en redistribuir entre varios procesadores, varios adaptadores de interfaz o varios sistemas principales el tráfico de la red y la carga de trabajo de los sistemas a los que se accede con asiduidad.

Si desea conseguir el mejor rendimiento posible del sistema operativo i5/OS, debe repartir la carga de las comunicaciones entre múltiples componentes del sistema.

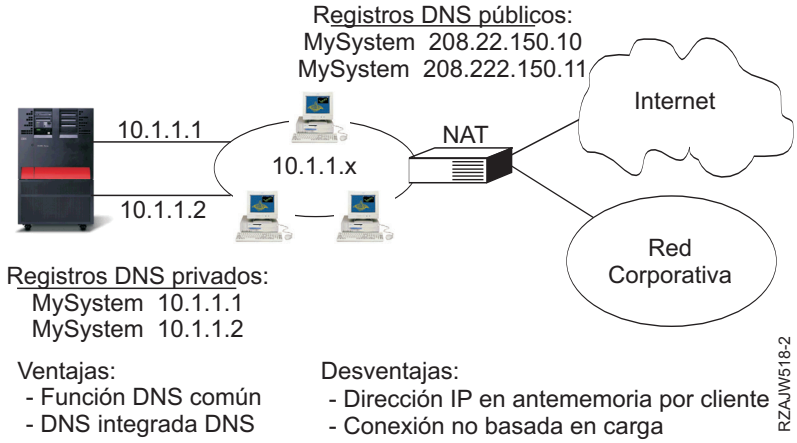
Para equilibrar la carga de trabajo del sistema se pueden utilizar varios métodos de direccionamiento TCP/IP.

Equilibrado de la carga basado en DNS

Puede utilizar el equilibrado de carga basado en DNS para la carga de trabajo de entrada. Si es necesario equilibrar la carga de los clientes locales, utilice el equilibrado de carga 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 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 son 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 siguiente, 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 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, los sitios y las páginas Web deben estar codificados para que se envíe un nombre de sistema diferente una vez establecido el primer contacto. Se pueden añadir entradas de DNS adicionales para MiServidor1 208.222.150.10 y MiServidor2 208.222.150.11. Con ello, los sitios Web pueden, 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.

Conceptos relacionados

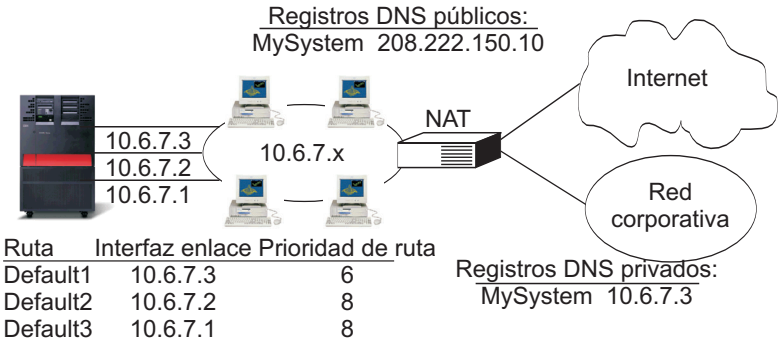
"NAT estática" en la página 22
La NAT estática puede utilizar conexiones de entrada que van desde una red pública hasta una red privada.

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 i5/OS 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 siguiente, 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.



Rutas indirectas, duplicadas, con prioridad predeterminada >(5) se seleccionarán de acuerdo con la prioridad de ruta

Ventajas:
- Mayor flexibilidad que DNS
- Bueno para HTTP, Telnet

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

RZAJW511-2

Puede configurar el equilibrado de la carga basado en rutas publicadas con el mandato Añadir ruta TCP/IP (ADDTCPRTE) o con la interfaz System i Navigator. Se realiza estableciendo la prioridad de ruta duplicada o la interfaz de enlace favorito. 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 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.

Observe 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.

Equilibrado de la carga mediante IP virtual y ARP por proxy

Puede utilizar IP virtual y ARP por proxy para conseguir equilibrado de la carga entre varias interfaces. Este método de equilibrado de la carga de trabajo da soporte tanto a carga de trabajo entrante como saliente.

Las siguientes son las ventanas de la utilización de IP virtual y ARP por proxy como el método de equilibrado de la carga de trabajo:

- Da soporte tanto a carga de trabajo entrante como saliente.
- Da soporte a clientes locales.
- Proporciona más flexibilidad que los métodos de equilibrado de la carga basados en rutas duplicadas y en DNS.

El inconveniente de este método de equilibrado de la carga de trabajo es que se trata de una solución basada en la conexión y no en la carga. No se tiene en cuenta la carga en cada interfaz. Se presupone que la carga de tráfico es similar para todas las conexiones.

El ejemplo siguiente se beneficia completamente de la utilización de direcciones IP virtuales. Además de enlazar una dirección IP virtual exclusiva con cada aplicación, este ejemplo proporciona equilibrado de conexión entrante y saliente y cierto nivel de tolerancia a errores.

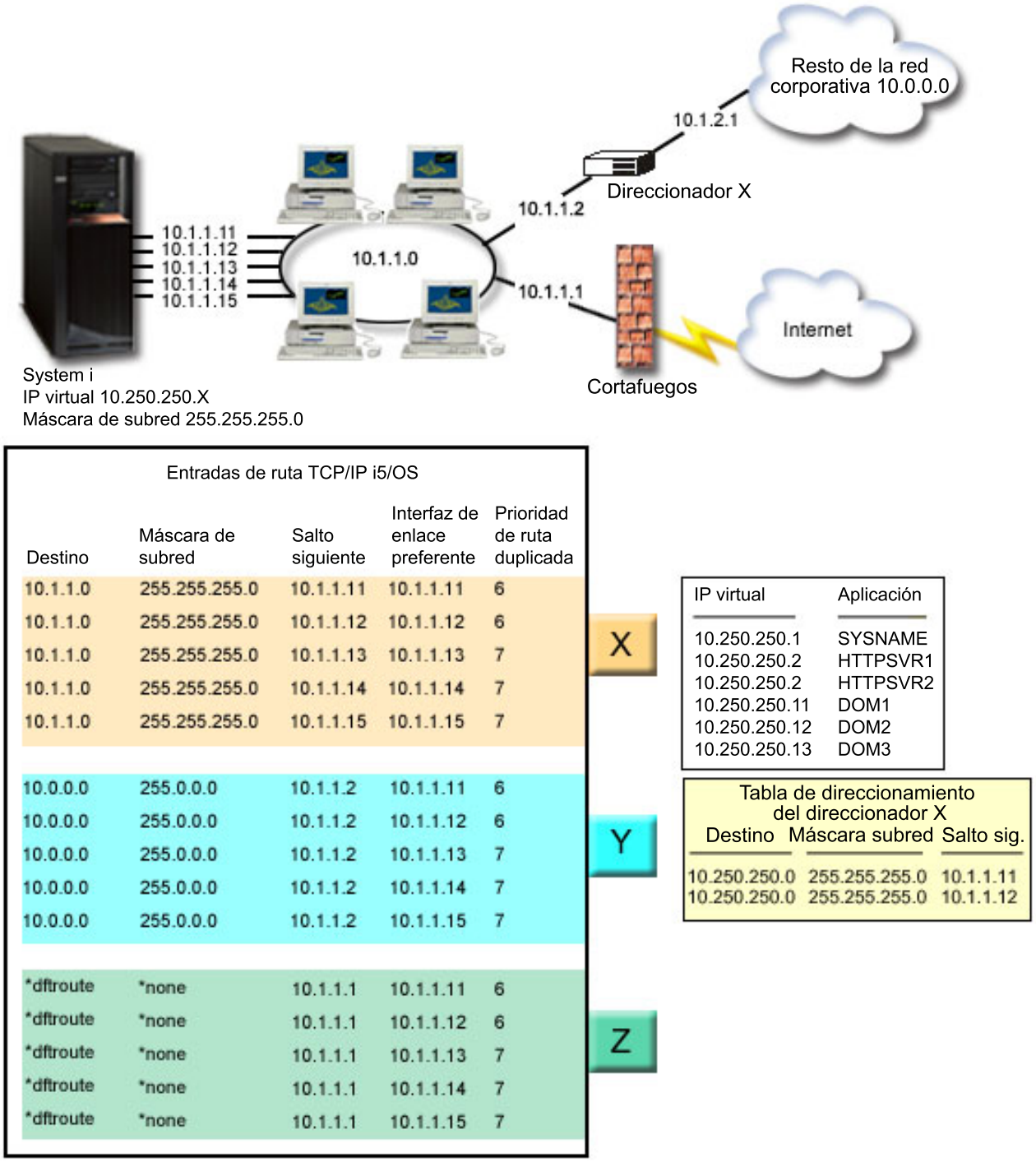


Figura 3. Equilibrado de la carga mediante IP virtual y ARP por proxy

En este ejemplo, el equilibrado de conexión entrante se consigue mediante la utilización de direcciones IP virtuales definidas en el sistema y del direccionador externo, cortafuegos y conmutador que pueden realizar direccionamiento de capa tres (capa de red). El equilibrado de conexión saliente se consigue

mediante la utilización de los parámetros de prioridad de ruta duplicada y de interfaz de enlace favorita en las entradas de la ruta TCP/IP de i5/OS. Las conexiones salientes se distribuyen de forma rotativa turnos entre todas las interfaces con la misma prioridad de ruta duplicada cuando el valor de la prioridad de ruta duplicada está establecido en un valor superior al valor por omisión de 5. Si todas las interfaces con un valor pasan a estar disponibles, el sistema conmuta a las interfaces con el siguiente nivel más bajo.

Según las directivas de ruta que están configuradas en el direccionador X, las interfaces 10.1.1.11 y 10.1.1.12 están configuradas como las interfaces salientes principales. Las conexiones entrantes se distribuyen de forma rotativa entre las interfaces 10.1.1.11 y 10.1.1.12, que es una función que proporcionan la mayoría de direccionadores.

Según las entradas de ruta TCP/IP de i5/OS, las interfaces 10.1.1.13, 10.1.1.14 y 10.1.1.15 con una prioridad de ruta duplicada de 7 están configuradas como las interfaces salientes principales. Las conexiones salientes se distribuyen de forma rotativa entre las interfaces 10.1.1.13, 10.1.1.14 y 10.1.1.15. Si estas tres interfaces están inactivas, se utilizan las interfaces 10.1.1.11 y 10.1.1.12 con una prioridad de ruta duplicada de 6 tanto para conexiones entrantes como salientes.

En este ejemplo, las entradas de ruta TCP/IP de i5/OS constan de tres grupos. El Grupo X proporciona equilibrado de conexión saliente al segmento local de la red corporativa (10.1.1.0). El Grupo Y proporciona equilibrado de conexión saliente al resto de la red corporativa (10.0.0.0) mediante el direccionador. El Grupo Z proporciona equilibrado de conexión saliente a Internet mediante el cortafuegos.

Conceptos relacionados

"Caso práctico: Conmutación por anomalía de adaptador utilizando IP virtual y ARP por proxy"
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 sistemas, lo que permite muchas opciones nuevas de equilibrado de la carga.

Caso práctico: Conmutación por anomalía de adaptador utilizando IP virtual y ARP por proxy

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 sistemas, lo que permite muchas opciones nuevas de equilibrado de la carga.

Nota: Este caso práctico hace referencia a un único adaptador de LAN en lugar de a un tipo de interrupción de servicio del sistema importante como sería la agrupación en clúster. Esta solución requiere un sistema externo de equilibrado de la carga.

Situación

El sistema 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 hardware System i y de la red. Debido al crecimiento, se ha hecho imprescindible que este sistema esté funcionando en la red de forma continuada, sin que se den tiempos de indisponibilidad no planificados. Si, por cualquier razón, un adaptador de la red quedara temporalmente fuera de servicio, el sistema debería tener otros adaptadores de red que tomasen el control y así los clientes de la red ni se enterarían de las anomalías.

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 caso práctico, nos proponemos como objetivo mantener la disponibilidad de la red para los clientes del

sistema en el caso de que se produzca una anomalía de adaptador.

Detalles

Una manera de manejar la situación anterior consiste en tener múltiples conexiones físicas entre la plataforma System i y la LAN. Observe la siguiente figura:

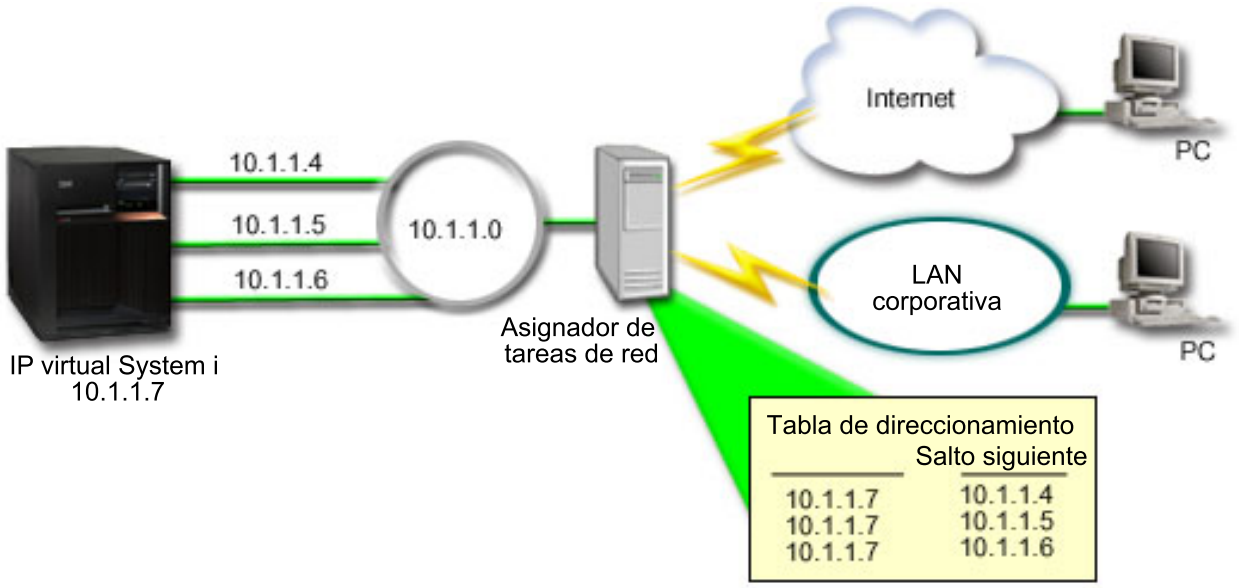


Figura 4. Conmutación por anomalía de adaptador sin clientes locales

Cada conexión física tiene una dirección IP diferente. Luego se puede asignar una dirección IP virtual al sistema. Esta es la dirección IP mediante la que todos los clientes reconocerán el sistema. Todos los clientes remotos (clientes que no están físicamente conectados a la misma LAN que la plataforma System i) se comunicarán con el sistema 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 pasen por el asignador de tareas de red, éste direccionará las direcciones IP virtuales a uno de los adaptadores de red situados en el sistema.

Si la LAN a la que está conectado el sistema tiene clientes, estos no emplearán el asignador de tareas de red para dirigir su tráfico enlazado localmente, porque ello supondría una sobrecarga innecesaria para el asignador de tareas de red. Puede crear en cada cliente entradas de ruta similares a las tablas de rutas situadas en el asignador de tareas de red. Sin embargo, si la LAN tiene un número de clientes locales muy elevado, esta solución no sería práctica. Esta situación es la que se ilustra en la siguiente figura.

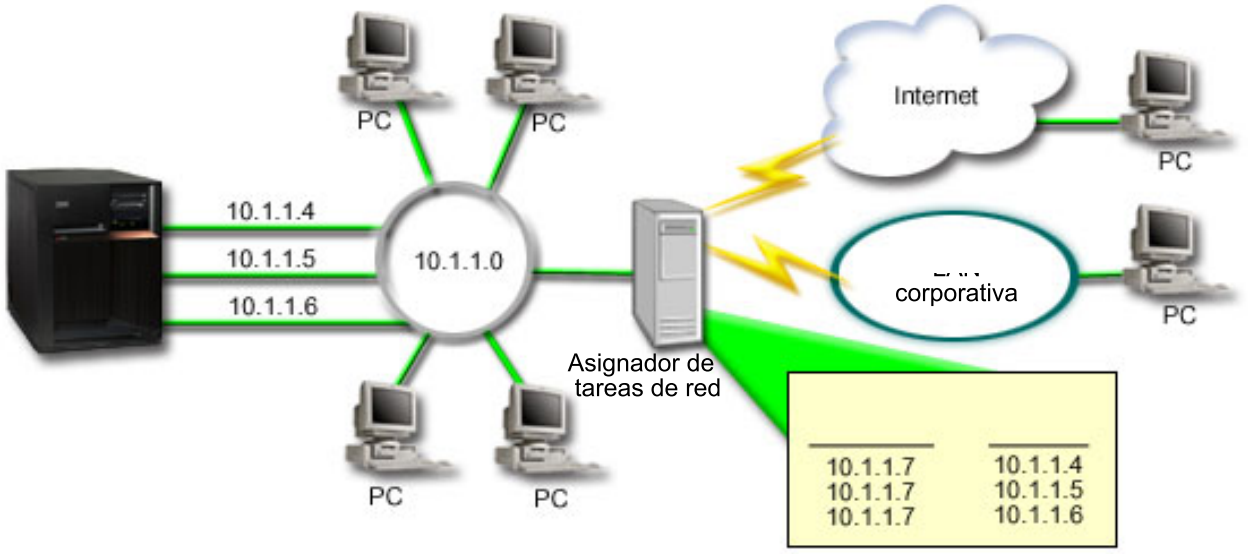


Figura 5. Conmutación por anomalía de adaptador con clientes locales

Los clientes locales (clientes que están conectados a la misma LAN que el sistema) se pueden conectar a la dirección de IP virtual del sistema por medio de ARP. Esto permite asimismo que los clientes locales tengan una solución de conmutación por anomalía de adaptador.

En cualquier caso, ni los clientes locales ni los remotos tiene conocimiento de la conmutación por anomalía cuando se produce. El sistema elige los adaptadores y las direcciones IP que forman la interfaz preferida para la selección del agente ARP (Protocolo de resolución de direcciones) de proxy VIPA (dirección IP virtual).

Puede seleccionar manualmente los adaptadores y direcciones IP que deben formar la interfaz preferida para la selección del agente ARP de proxy VIPA. Puede seleccionar la interfaz que debe utilizarse creando una lista de interfaces favoritas si se produce una anomalía del adaptador. Una lista de interfaces favoritas es una lista ordenada de las direcciones de interfaz que toman el control en lugar de los adaptadores anómalos. Puede utilizar System i Navigator o la interfaz de programación de aplicaciones (API) Cambiar interfaz TCP/IP IPv4 (QTOCC4IF) para configurar una lista de interfaces favoritas. La lista de interfaces favoritas también puede configurarse para Ethernet virtual y para interfaces de dirección IP virtual.

Utilizando la Figura 2 como ejemplo, los clientes remotos se comunican con el sistema local mediante la dirección IP virtual 10.1.1.7. Supongamos que 10.1.1.4 es el adaptador local inicial utilizado para esta comunicación, y desea que 10.1.1.5 tome el control si 10.1.1.4 falla. También desea que la interfaz 10.1.1.6 tome el control si los dos adaptadores, el de 10.1.1.4 y el de 10.1.1.5, fallan. Para controlar el orden de utilización de estas interfaces en una situación de conmutación por anomalía, puede definir una lista de interfaces favoritas para la dirección IP virtual 10.1.1.7. En este caso, será una lista ordenada de direcciones de interfaz que constará de las direcciones 10.1.1.4, 10.1.1.5 y 10.1.1.6.

La solución también puede implicar la utilización de dos o más plataformas System i para darse soporte mutuo. Si uno de los sistemas queda temporalmente fuera de servicio, el control puede pasar al segundo sistema como migración tras error. La siguiente figura muestra la misma configuración empleando dos sistemas.

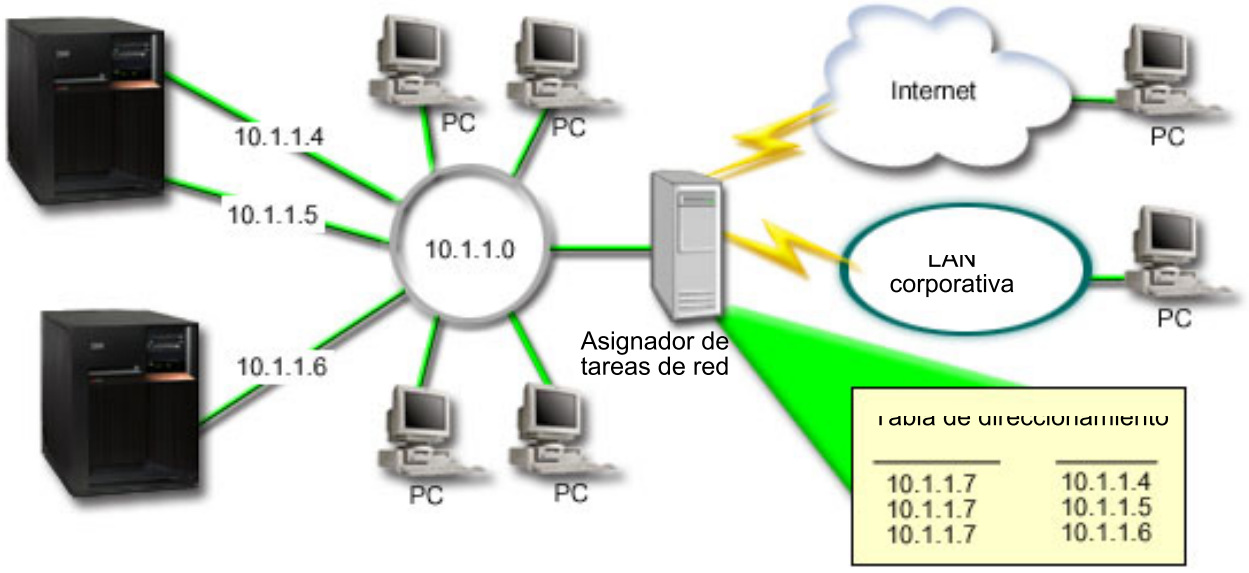


Figura 6. Migración tras error con varias plataformas System i y clientes locales

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

Pasos de configuración

La configuración del equilibrado de la carga 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.

Conceptos relacionados

"Equilibrado de la carga mediante IP virtual y ARP por proxy" en la página 27
Puede utilizar IP virtual y ARP por proxy para conseguir equilibrado de la carga entre varias interfaces. Este método de equilibrado de la carga de trabajo da soporte tanto a carga de trabajo entrante como saliente.

Migración tras error utilizando selección automática de interfaz

Utilice estos pasos para configurar IP virtual y ARP por proxy para situaciones de migración tras error del adaptador en este caso práctico.

Utilizando la Figura 2 como ejemplo, los pasos generales de configuración son los siguientes:

1. Configurar una interfaz de TCP/IP virtual.

   Utilizando System i Navigator, cree una interfaz de TCP/IP virtual. El asistente Interfaz IP virtual nueva se encuentra en: **Red** → **Configuración TCP/IP** → **IPv4** → **Interfaces**. A continuación, pulse **Interfaces** con el botón derecho del ratón y elija **Interfaz nueva** → **IP virtual**.

   En nuestro ejemplo, especificará 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 marque el recuadro de selección **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 System i Navigator y puede encontrarse en: **Network** → **Configuración TCP/IP** → **IPv4** → **Interfaces**. A

continuación, 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 este ejemplo, ejecutará 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 seleccione **Propiedades**. Pulse la pestaña **Avanzadas** y marque el recuadro de selección **Interfaz local asociada** para asociar la interfaz con la interfaz de IP virtual que ha creado en el paso 1.

Migración tras error utilizando una lista de interfaces favoritas

Puede crear una lista de interfaces favoritas para controlar el orden en que se utilizan las interfaces locales cuando se produce una anomalía de adaptador.

Para crear una lista de interfaces favoritas, siga estos pasos:

1. En System i Navigator, expanda **Network → Configuración TCP/IP → IPv4**.
2. Pulse **Interfaces**.
3. En las listas de interfaces que se visualizan, seleccione una interfaz para la dirección IP virtual o Ethernet virtual para la que desee crear la lista de interfaces favoritas.

   Utilizando la Figura 2 como ejemplo, seleccionará la dirección IP virtual 10.1.1.7.
4. Pulse la interfaz con el botón derecho del ratón y seleccione **Propiedades**.
5. Pulse la pestaña **Avanzadas**.
6. En el panel, seleccione las direcciones de interfaz en la lista Interfaces disponibles y pulse **Añadir**.

   Utilizando la Figura 2 como ejemplo, seleccionará las interfaces 10.1.1.4, 10.1.1.5 y 10.1.1.6 y las añadirá a la lista de interfaces favoritas una por una.

   También puede eliminar una interfaz de la lista de interfaces favoritas en el panel derecho mediante el botón **Eliminar**, o subir o bajar una interfaz en la lista para cambiar el orden mediante los botones **Subir** y **Bajar**.
7. Marque el recuadro de selección **habilitar ARP proxy** situado sobre la lista Interfaces disponibles para habilitar la lista.
8. Pulse **Aceptar** para salvar la lista de interfaces favoritas que acaba de crear.

Nota: Sólo puede incluir 10 interfaces en la lista de interfaces favoritas. Si configura más de 10, la lista de truncará al llegar a la décima.

Información relacionada con el direccionamiento y equilibrado de la carga de trabajo TCP/IP

Otros documentos del information center contienen información relacionada con el direccionamiento y equilibrado de la carga de trabajo TCP/IP.

Otra información

- El Servidor de nombres de dominio

  (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.
- Particiones lógicas

  Este tema ofrece más información detallada y contextual.
- Filtrado de IP y conversión de direcciones de red

  La información de este tema facilita la gestión de las normas de filtrado. Entre otras funciones, se incluye la adición de comentarios, la edición y la visualización.
- OptiConnect

Este tema proporciona información acerca del direccionamiento de OptiConnect.

- Servicios de acceso remoto: conexiones PPP

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

Referencia relacionada

"Archivo PDF para el direccionamiento y equilibrado de la carga de trabajo TCP/IP" en la página 2
Puede visualizar 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
Tokyo 106-0032, Japan

El párrafo siguiente no puede aplicarse en el Reino Unido ni en cualquier otro país en el que tales disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGUNA CLASE, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O IDONEIDAD PARA 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 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 y todo el material bajo licencia a su disposición los proporciona IBM bajo los términos del Acuerdo de cliente de IBM, el Acuerdo de licencia de programa internacional de IBM, el Acuerdo de licencia de IBM para el código de máquina o de cualquier acuerdo equivalente entre las 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 mediciones pueden haberse efectuado en sistemas a nivel de desarrollo y no existe garantía de que dichas mediciones sean las mismas en sistemas disponibles de modo genérico. Además, algunas mediciones pueden haberse estimado mediante 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 distribuidores 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, compatibilidad ni ninguna otra afirmación relacionada con productos no IBM. Las preguntas relativas a las capacidades de los productos no IBM deben dirigirse a los distribuidores de los mismos.

Todas las afirmaciones relativas a planes o intenciones futuras de IBM están sujetas a cambio o retirada sin previo aviso, y representan sólo metas y objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones diarias de gestión. Para ilustrarlos del modo más completo posible, incluyen los nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones utilizados por empresas reales es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que ilustran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin pago a IBM, con el propósito de desarrollar, utilizar, comercializar o distribuir programas de aplicación compatibles con la interfaz de programación de aplicaciones correspondiente a la plataforma operativa para la que se han escrito los programas de ejemplo. 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.

Cada copia o parte de estos programas de ejemplo o cualquier trabajo derivado debe incluir un aviso de copyright como el siguiente:

© (nombre de la 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 viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Información acerca de las interfaces de programación

Esta publicación relativa al direccionamiento y el equilibrado de la carga de trabajo TCP/IP documenta interfaces de programación 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:

i5/OS
IBM
IBM (logotipo)
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.

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

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 del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer del fabricante, no se sigan debidamente las instrucciones anteriores.

No puede bajar, 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