



@server

iSeries

Redes

Configuración TCP/IP

Versión 5 Release 3





@server

iSeries

Redes

Configuración TCP/IP

Versión 5 Release 3

Nota

Antes de utilizar esta información y el producto al que da soporte, asegúrese de leer la información en la sección "Avisos", en la página 59.

Séptima edición (agosto de 2005)

| Esta edición se aplica a la versión 5, release 3, modification 0 de Operating System/400 (5722-SS1) y a todos los
| releases y modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones. Esta versión no se
| ejecuta en todos los modelos de sistema con conjunto reducido de instrucciones (RISC) ni tampoco se ejecutan en
| los modelos CICS.

© Copyright International Business Machines Corporation 1998, 2005. Reservados todos los derechos.

Contenido

Parte 1. Configuración TCP/IP 1

Capítulo 1. Novedades de la V5R3 3

Capítulo 2. Imprimir este tema 5

Capítulo 3. Protocolo de Internet versión 6 (IPv6) 7

¿Qué es IPv6?	7
¿Qué funciones de IPv6 están disponibles?	8
Escenarios: IPv6	9
Crear una red de área local (LAN) IPv6	9
Enviar paquetes IPv6 a través de una red de área local (LAN) IPv4	10
Enviar paquetes IPv6 a través de una red de área amplia (WAN) IPv4	12
Conceptos: IPv6	14
Formatos de dirección de IPv6	15
Tipos de dirección IPv6	15
Túneles IPv6	16
Descubrimiento de vecinos	17
Autoconfiguración de direcciones sin estado	17
Comparación de IPv4 e IPv6.	18
Solución de problemas de IPv6	24
Información relacionada para IPv6.	25

Capítulo 4. Planificación de la configuración de TCP/IP 27

Requisitos de la configuración de TCP/IP	27
Consideraciones sobre la seguridad TCP/IP	28

Capítulo 5. Instalar TCP/IP 29

Capítulo 6. Configurar TCP/IP 31

Configurar TCP/IP por primera vez	31
Configurar TCP/IP utilizando el asistente de configuración EZ-Setup	31
Configurar TCP/IP utilizando la interfaz basada en caracteres	32
Configurar IPv6	34
Requisitos de configuración	34
Configurar IPv6 utilizando el asistente de configuración de IPv6	35
Configurar TCP/IP cuando el sistema operativo se encuentra en estado restringido.	35

Capítulo 7. Personalizar TCP/IP con el Navigator de iSeries 37

Capítulo 8. Técnicas TCP/IP para conectar Ethernet virtual a redes LAN externas 39

Método de ARP por proxy	40
Paso 1: permitir que las particiones lógicas participen en una Ethernet virtual	41
Paso 2: crear las descripciones de línea Ethernet	41
Paso 3: activar el reenvío de datagramas IP.	43
Paso 4: crear la interfaz para habilitar ARP por proxy	43
Paso 5: crear la interfaz TCP/IP virtual en la partición A	43
Paso 6: crear la interfaz TCP/IP virtual en la partición B	44
Paso 7: crear la ruta	44
Paso 8: verificar las comunicaciones de red	45
Método de conversión de direcciones de red	45
Paso 1: permitir que las particiones lógicas participen en una Ethernet virtual	46
Paso 2: crear las descripciones de línea Ethernet	46
Paso 3: activar el reenvío de datagramas IP.	48
Paso 4: crear las interfaces	48
Paso 5: verificar las comunicaciones de red	49
Paso 6: crear reglas de paquetes	49
Paso 7: verificar las comunicaciones de red	50
Método de direccionamiento TCP/IP.	50
Paso 1: permitir que las particiones lógicas participen en una Ethernet virtual	51
Paso 2: crear las descripciones de línea Ethernet	51
Paso 3: activar el reenvío de datagramas IP.	53
Paso 4: crear las interfaces	53
Consideraciones sobre Ethernet virtual	53

Capítulo 9. Información relacionada para la configuración de TCP/IP 55

Parte 2. Apéndices. 57

Apéndice. Avisos 59

Marcas registradas	60
Términos y condiciones para descargar e imprimir publicaciones.	61

Parte 1. Configuración TCP/IP

Ha llegado el servidor que adquirió recientemente y tiene ganas de ponerlo en marcha. En este tema encontrará herramientas y procedimientos para configurar TCP/IP en OS/400. Por ejemplo, puede utilizar esta información para crear una descripción de línea, una interfaz de TCP/IP y una ruta. Descubrirá cómo puede personalizar la configuración de TCP/IP mediante iSeries Navigator y aprenderá varias técnicas TCP/IP que le permitirán direccionar los datos que fluyen desde y hacia la red.

Antes de utilizar esta información para configurar TCP/IP, consulte el apartado Instalación y utilización de hardware para asegurarse de que ha instalado todos los componentes de hardware necesarios. Una vez haya completado las tareas iniciales de la configuración de TCP/IP, ya podrá ampliar las posibilidades del servidor con aplicaciones, protocolos y servicios TCP/IP para satisfacer sus necesidades concretas.

Novedades de la V5R3

Novedades y cambios en la función TCP/IP.

Imprimir este tema

Utilice este tema para imprimir o descargar una versión en PDF de la documentación referente a la configuración de TCP/IP.

Protocolo de Internet versión 6 (IPv6)

El nuevo protocolo de Internet, IPv6 juega un papel clave en el futuro de Internet, y usted puede utilizar IPv6 en el servidor iSeries. Este tema incluye información general sobre IPv6 y cómo se implementa en el servidor iSeries.

Planificación de la configuración de TCP/IP

Este tema le ayudará a preparar la instalación y configuración de TCP/IP en el servidor iSeries. Aquí encontrará los requisitos básicos para la instalación y configuración, para que tenga a mano toda la información necesaria cuando empiece a configurar TCP/IP. También se ofrecen referencias a términos y conceptos relacionados.

Instalar TCP/IP

Este tema le ayudará en la instalación de aquellos productos que preparan al servidor iSeries para el funcionamiento.

Configurar TCP/IP

Este tema le muestra cómo poner en marcha el sistema iSeries y configurar TCP/IP. Vea también las instrucciones referentes a la configuración de IPv6.

Personalizar TCP/IP con iSeries Navigator.

Este tema proporciona opciones de personalización utilizando iSeries Navigator.

Técnicas TCP/IP para conectar Ethernet virtual a redes LAN

Descubra cómo puede aprovechar Ethernet virtual en OS/400.

Solución de problemas de TCP/IP

Para la solución de problemas relacionados con el tráfico o las conexiones TCP/IP, consulte Solución de problemas de TCP/IP. Esta guía para la solución de problemas le ayudará a resolver problemas relacionados con IPv4 e IPv6.

Información relacionada para la configuración de TCP/IP

En este tema se da respuesta a la pregunta "¿qué más puedo hacer?". Encontrará referencias a servicios y aplicaciones que aumentan el rendimiento del servidor.

Capítulo 1. Novedades de la V5R3



Mejoras en la configuración de TCP/IP

Si utiliza una red Ethernet virtual para que las distintas particiones puedan comunicarse entre sí, quizás deba extender esa comunicación a una LAN física externa. Consulte el tema Técnicas TCP/IP para conectar Ethernet virtual a redes LAN externas para conocer cómo conectar la red Ethernet virtual a una LAN externa. Utilice esta información para revisar ejemplos que ilustran tres métodos distintos para conectar el tráfico de red de la red Ethernet virtual con una LAN externa.

Para obtener más información sobre las novedades o los cambios de este release, consulte el Memorándum para los usuarios.

Cómo ver la información nueva o cambiada

Para ayudarle a ver los lugares donde se han efectuado cambios técnicos, esta información utiliza los siguientes elementos gráficos:

- La imagen  marca el lugar en que empieza la información nueva o modificada.
- La imagen  marca el lugar en el que acaba la información nueva o modificada.



Capítulo 2. Imprimir este tema

Para ver o bajar la versión PDF de este documento, seleccione Configuración de TCP/IP (aproximadamente 362 KB).



Más información

También puede ver o imprimir los siguientes documentos PDF:

- Manuales:

- **TCP/IP Configuration and Reference**  (592 KB)
Este libro proporciona información sobre la configuración del Protocolo de control de la transmisión/Protocolo de Internet (TCP/IP) y sobre el funcionamiento y la administración de la red.
- **Consejos y herramientas para proteger el iSeries**  (1 MB)
Este libro proporciona recomendaciones básicas para utilizar las opciones de seguridad del iSeries para proteger el servidor y sus operaciones asociadas.

- Redbooks:


- **TCP/IP Tutorial and Technical Overview**  (7 MB)
Este redbook proporciona información sobre los conceptos básicos de TCP/IP.
- **TCP/IP for AS/400: More Cool Things Than Ever**  (9 MB)
Este redbook incluye una amplia lista de servicios y aplicaciones de TCP/IP habituales.

Cómo guardar los archivos PDF

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

1. Pulse el botón derecho sobre el PDF en su navegador (pulse el botón derecho del ratón sobre el enlace anterior).
2. Pulse **Guardar destino como...** si utiliza Internet Explorer. Pulse **Guardar enlace como...** si utiliza Netscape Communicator.
3. Diríjase al directorio donde desea guardar el archivo PDF.
4. Pulse **Guardar**.

Descargar Adobe Acrobat Reader

Se necesita Adobe Acrobat Reader para ver o imprimir estos documentos PDF. Puede bajar una copia del sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html) .

Capítulo 3. Protocolo de Internet versión 6 (IPv6)

El protocolo de Internet versión 6 (IPv6) es la versión actualizada del Protocolo de Internet versión 4 (IPv4) y está sustituyendo gradualmente a IPv4 como el estándar de Internet.

Quizás se pregunte cómo puede utilizar IPv6 para mejorar el negocio electrónico de su empresa, o quizás sea un programador que desee crear aplicaciones IPv6 para que su empresa puede beneficiarse de este protocolo de Internet mejorado. En estos temas encontrará información básica sobre IPv6 y sobre cómo utilizar IPv6 en el servidor iSeries:

¿Qué es IPv6?

Averigüe porqué IPv6 está sustituyendo a IPv4 como el estándar de Internet y cómo sacarle provecho.

¿Qué funciones de IPv6 están disponibles?

Conozca cómo se está implementando actualmente IPv6 en el servidor iSeries.

Escenarios de IPv6

Vea ejemplos que le ayudarán a entender las situaciones en las que utilizaría IPv6 para su empresa.

Conceptos de IPv6

Conozca los conceptos básicos de IPv6. Si no está seguro de cuáles son las diferencias entre IPv4 e IPv6, consulte comparaciones detalladas en las que se comparan, por ejemplo, las direcciones de IPv4 y IPv6, o se explican las diferencias entre las cabeceras de los paquetes de IPv4 y IPv6.

Configurar IPv6

Consulte los requisitos de hardware y de software y las instrucciones para configurar IPv6 en el servidor.

Solución de problemas de IPv6

Encuentre soluciones para los problemas de IPv6.

Información relacionada para IPv6

Acceda a enlaces que le remitirán a recursos que le ayudarán a entender IPv6.

¿Qué es IPv6?

El protocolo de Internet versión 6 (IPv6) es la versión actualizada del protocolo de Internet. En gran parte de Internet se utiliza IPv4, un protocolo elástico y digno de crédito durante más de 20 años. Sin embargo, IPv4 tiene graves limitaciones que causan más problemas a medida que Internet crece.

En concreto, hay un déficit cada vez más importante de direcciones IPv4, necesarias para todos los dispositivos nuevos que se incorporan a Internet. La clave para la mejora de IPv6 es la expansión del espacio de direcciones IP de 32 a 128 bits, habilitando direcciones IP únicas virtualmente sin límite. El nuevo formato de texto para las direcciones en IPv6 es:

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
```

donde cada x es un dígito hexadecimal que representa 4 bits.

La mayor capacidad del espacio para direcciones de IPv6 proporciona una solución para el problema de escasez de direcciones. Se trata de algo especialmente importante a medida que más personas utilizan sistemas móviles, como teléfonos móviles y agendas personales. La creciente demanda de usuarios que

utilizan dispositivos sin cable contribuye al agotamiento de direcciones IPv4. La mayor capacidad para direcciones IP de IPv6 resuelve este problema proporcionando suficientes direcciones IP para el número creciente de dispositivos sin cable.

Además de este mayor espacio para direcciones, IPv6 proporciona funciones nuevas que simplifican las tareas de configurar y gestionar las direcciones en la red. La configuración y el mantenimiento de redes es una actividad laboriosa. IPv6 reduce parcialmente el volumen de trabajo automatizando algunas de las tareas del administrador de red.

Si utiliza IPv6, no tendrá que volver a numerar las direcciones de su dispositivo cuando cambie de proveedor de servicios de Internet (ISP). Podrá conservar las siguientes direcciones porque son direcciones únicas globalmente.

La función de auto-configuración de IPv6 configura automáticamente las direcciones del direccionador y la interfaz. En una autoconfiguración sin información sobre el estado, IPv6 asume la dirección MAC del sistema y un prefijo de red que proporciona un nodo local, y combina estas dos direcciones para crear una nueva dirección IPv6 única. Con esta función ya no es necesario disponer de un servidor DHCP, con lo cual se agiliza la tarea del administrador y la empresa ahorra dinero.

Puede acceder a otras fuentes de información sobre IPv6 en Información relacionada para IPv6

Consulte ¿Qué funciones de IPv6 están disponibles? donde encontrará información del IPv6 relacionada específicamente con el servidor iSeries.

¿Qué funciones de IPv6 están disponibles?

IBM implementa IPv6 para el servidor iSeries en varios releases de software. IPv6 se implementa actualmente en una plataforma de desarrollo de aplicaciones para desarrollar y evaluar las aplicaciones de IPv6. Las funciones de IPv6 son transparentes para las aplicaciones TCP/IP existentes y coexisten con las funciones de IPv4.

Estas son las principales funciones del servidor iSeries asumidas por IPv6:

- **Configuración**

Tenga en cuenta que el proceso de configuración de IPv6 es diferente del proceso de IPv4. Para utilizar la función de IPv6, debe cambiar la configuración TCP/IP del servidor configurando una línea para IPv6. Puede configurar IPv6 en una línea Ethernet o en una línea de túnel.

Si configura una línea de Ethernet para el tráfico de IPv6, enviará paquetes IPv6 a través de una red IPv6. En Crear una red de área local (LAN) IPv6 encontrará un escenario que describe una situación en la que configuraría una línea de Ethernet para IPv6.

Si configura líneas de túnel, enviará paquetes IPv6 a través de una red IPv4 existente. Consulte Enviar paquetes IPv6 a través de una red de área local (LAN) IPv4 y Enviar paquetes IPv6 a través de una red de área amplia (WAN) IPv4 donde encontrará escenarios que describen dos situaciones en las que se crearía una línea de túnel configurada para IPv6.

Consulte Configurar IPv6 para configurar su red para IPv6.

- **Sockets**

Desarrollar y evaluar las aplicaciones de sockets utilizando las API y herramientas de IPv6. IPv6 mejora los sockets de forma que las aplicaciones pueden utilizar IPv6 utilizando una familia de direcciones nueva: AF_INET6. Estas mejoras no afectan a las aplicaciones IPv4 existentes. Puede crear aplicaciones que den soporte al tráfico IPv4 e IPv6 concurrente o sólo al tráfico IPv6. Véase Utilizar la familia de direcciones AF_INET6 para más información sobre IPv6 para sockets.

- **DNS**

DNS (Domain Name System) da soporte a direcciones AAAA y a un dominio nuevo para búsquedas inversas: IP6.ARPA. Aunque es cierto que DNS recupera información de IPv6, el servidor debe utilizar IPv4 para comunicarse con el DNS.

- **Solución de problemas de TCP/IP**

Utilice herramientas estándar para la solución de problemas como PING, netstat, rastrear ruta y rastreo de comunicaciones para las redes y túneles de IPv6. Ahora, estas herramientas dan soporte al formato de direcciones de IPv6. Consulte Solución de problemas de TCP/IP para resolver problemas relacionados con las redes IPv4 e IPv6.

Consulte Información relacionada para IPv6 donde encontrará recursos de IPv6.

Escenarios: IPv6

Consulte los escenarios siguientes para entender porqué implementaría IPv6 y cómo configuraría su red en cada una de estas situaciones:

- Crear una red de área local (LAN) IPv6
- Enviar paquetes IPv6 a través de una red de área local (LAN) IPv4
- Enviar paquetes IPv6 a través de una red de área amplia (WAN) IPv4

Nota: en los escenarios, las direcciones IP 10.x.x.x representan direcciones IP públicas. Todas las direcciones que se utilizan en estos escenarios se incluyen sólo a modo de ejemplo.

Consulte Configurar IPv6 para configurar su servidor para IPv6.

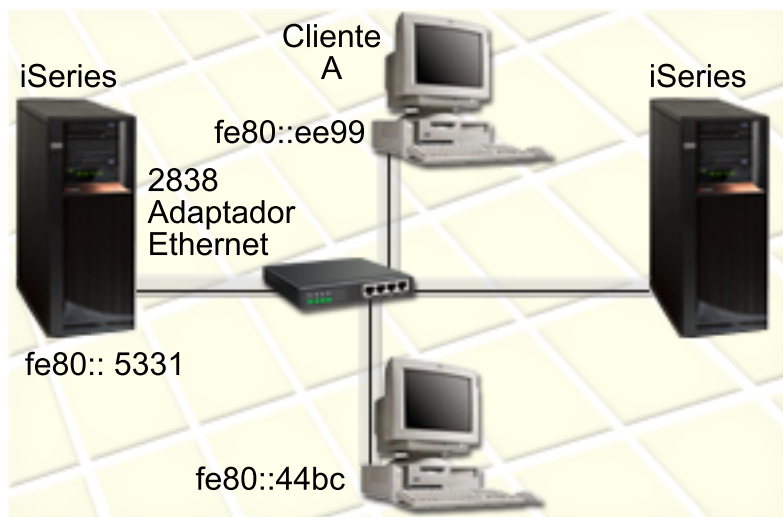
Consulte Conceptos de IPv6 para obtener definiciones de los conceptos básicos de IPv6.

Crear una red de área local (LAN) IPv6

Situación

A la larga, IPv6 sustituirá a IPv4 como estándar de Internet. Por lo tanto, su empresa decide implementar IPv6 para sus operaciones financieras y adquiere una nueva aplicación de contabilidad que utiliza IPv6 para la conectividad. La aplicación necesita conectarse con otra instancia de la aplicación situada en un servidor diferente conectado a la red de área local (LAN) Ethernet de la ubicación. Su tarea consiste en configurar su servidor para IPv6, de forma que su empresa pueda empezar a utilizar la aplicación de contabilidad. La imagen siguiente ilustra la configuración de la red en este escenario.

Departamento de contabilidad Red IPv6



Solución

Para crear una LAN IPv6, debe configurar una descripción de línea Ethernet para IPv6. Los paquetes de IPv6 viajan entre los servidores iSeries y los clientes de la red, a medida que los empleados utilizan la aplicación de contabilidad.

Los requisitos para la configuración incluyen:

- OS/400 Versión 5 Release 2 o posterior.
- Adaptadores de Ethernet 2838 o 2849, pues estos son los únicos tipos de recursos de hardware a los que actualmente da soporte IPv6.
- iSeries Access para Windows e iSeries Navigator (componente de red de iSeries Navigator)
- En el servidor debe haberse configurado una interfaz física IPv4 separada antes de configurar la línea Ethernet para IPv6, pues es preciso que se esté ejecutando TCP/IP en el servidor. Si no ha configurado el servidor para IPv4, consulte Configurar TCP/IP por primera vez antes de configurar la línea para IPv6.

Configuración

Para configurar una descripción de línea Ethernet para IPv6, debe utilizar el asistente de **Configuración de IPv6** en iSeries Navigator. IPv6 sólo puede configurarse desde iSeries Navigator, y no es posible configurarlo desde la interfaz basada en caracteres.

El asistente necesita el nombre del recurso de comunicaciones de hardware en el servidor en que se configurará IPv6; por ejemplo, CMN01. Debe ser un adaptador de Ethernet 2838 o 2849 que no esté configurado actualmente para IPv4.

Para utilizar el asistente de **Configuración de IPv6**, siga estos pasos:

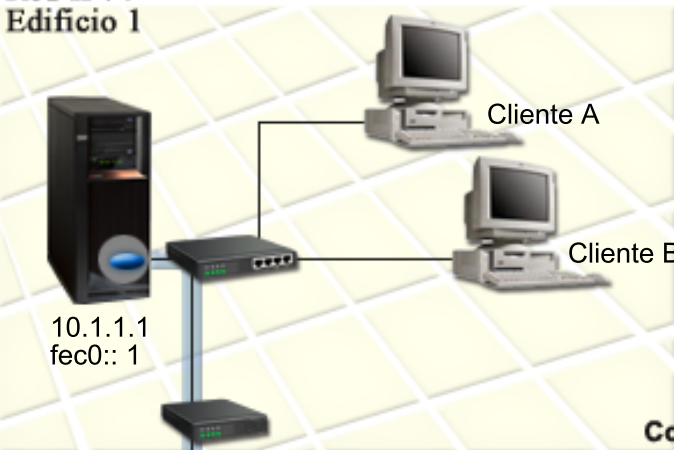
1. En iSeries Navigator, seleccione el **servidor** —> **Red** —> **Configuración TCP/IP**.
2. Pulse el botón derecho en **IPv6**, seleccione **Configuración IPv6**, y siga las instrucciones del asistente para configurar una línea de Ethernet para IPv6.

Enviar paquetes IPv6 a través de una red de área local (LAN) IPv4

Situación

Su empresa ha escrito una nueva aplicación de contabilidad de IPv6. Se trata de una aplicación servidor/cliente que se utilizará localmente. La aplicación se comunica con otras instancias de la propia aplicación situadas en la misma ubicación, pero en otros edificios y LAN. Aunque su empresa desea utilizar IPv6 para esta aplicación, no está preparada para cambiar toda su infraestructura de IPv4 a IPv6. Su tarea consiste en configurar líneas de túnel IPv6 que permitan la ejecución de paquetes IPv6 a través de las redes IPv4 locales. La imagen siguiente ilustra la configuración de la red en este escenario.

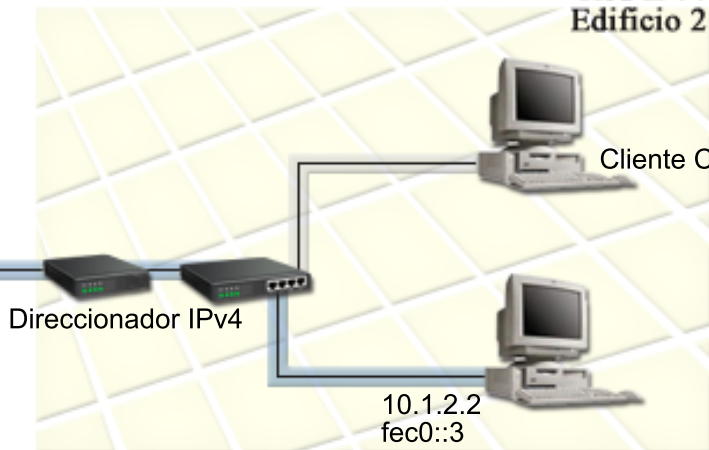
Contabilidad de deudores
Red IPv4
Edificio 1



Túnel configurado rojo
Punto final local = 10.1.1.1
Punto final remoto = 10.1.2.1
Dirección IPv6 local = fec0::1

Túnel configurado azul
Punto final local = 10.1.1.1
Punto final remoto = 10.1.2.2
Dirección IPv6 local = fec0::1

Contabilidad de acreedores
Red IPv4
Edificio 2



Solución

Para utilizar IPv6 en estas redes locales IPv4, debe crear dos túneles configurados y varias rutas asociadas. Un túnel se representa en rojo y el otro en azul, a modo de ejemplo.

En primer lugar, consideremos el túnel de color rojo:

- El túnel de color rojo empieza en el iSeries A (punto extremo local 10.1.1.1) en el Edificio 1 y finaliza en el Cliente C (punto extremo remoto 10.1.2.1) en el Edificio 2.
- iSeries A encapsula un paquete IPv6 dentro de un paquete IPv4 y envía el paquete IPv4 a través del túnel al Cliente C, que desencapsula el paquete IPv6 para poder conectarse con otra instancia de la aplicación IPv6.

A continuación, consideremos el túnel azul:

- El túnel azul empieza en iSeries A (punto extremo local 10.1.1.1) en el Edificio 1, como el túnel de color rojo; sin embargo, el túnel azul finaliza en el Cliente D (punto extremo remoto 10.1.2.2) del Edificio 2.
- iSeries A encapsula un paquete IPv6 dentro de un paquete IPv4 y envía el paquete IPv4 a través del túnel al Cliente D, que desencapsula el paquete IPv6 para poder conectarse con otra instancia de la aplicación IPv6.

Todas las conexiones de túnel son conexiones de punto a punto, por lo tanto debe definirse un punto extremo remoto para cada túnel. Para ello se crean dos rutas. Las dos rutas están asociadas con la misma línea de túnel, pero definen puntos finales remotos diferentes como el salto siguiente. Es decir, al crear las rutas se definen los puntos finales remotos de cada túnel.

Además de crear las rutas iniciales que definen los puntos finales del túnel y permiten que los paquetes lleguen a los clientes del Edificio 2, debe crear otras dos rutas para que los paquetes puedan volver al servidor situado en el Edificio 1.

Los requisitos para la configuración incluyen:

- OS/400 Versión 5 Release 2 o posterior.
- iSeries Access para Windows e iSeries Navigator (componente de red de iSeries Navigator)
- Para poder crear la línea de túnel configurada, antes debe configurarse TCP/IP (con IPv4) en el servidor. Si no ha configurado el servidor para IPv4, consulte Configurar TCP/IP por primera vez antes de configurar la línea de túnel para IPv6.

Configuración

Para crear una línea de túnel configurada, debe utilizar el asistente de **Configuración IPv6** y el asistente **Nueva ruta IPv6** de iSeries Navigator. IPv6 sólo puede configurarse desde iSeries Navigator, y no es posible configurarlo desde la interfaz basada en caracteres.

Para utilizar el asistente de **Configuración de IPv6** para crear la línea del túnel rojo, siga estos pasos:

1. En iSeries Navigator, seleccione el **servidor** —> **Red** —> **Configuración TCP/IP**.
2. Pulse el botón derecho en **IPv6**, seleccione el asistente de **Configuración de IPv6**, y siga las instrucciones del asistente para configurar una línea de túnel para IPv6. Tras completar el asistente de **Configuración de IPv6**, éste le solicitará que cree una ruta nueva para la línea de túnel configurada, aparecerá el diálogo del asistente **Nueva ruta IPv6**. Debe crear una ruta nueva para que los paquetes IPv6 puedan viajar a través del túnel de color rojo.
3. Desde el asistente **Nueva ruta IPv6**, cree una ruta para el túnel de color rojo. Especifique el punto extremo remoto 10.1.2.1 como el salto siguiente y especifique fec0::2 como la dirección de destino.

Utilice de nuevo el asistente **Nueva ruta IPv6** para crear una ruta para el túnel azul. Observe que no es necesario crear el túnel azul con el asistente de **Configuración de IPv6**. El túnel azul se crea al definir su punto extremo remoto mediante el asistente **Nueva ruta IPv6**. Para utilizar el asistente **Nueva ruta IPv6**, siga estos pasos:

1. En iSeries Navigator, seleccione el **servidor** —> **Red** —> **Configuración TCP/IP**—> **IPv6**.
2. Pulse el botón derecho en **Rutas**, seleccione **Nueva ruta**, y siga las instrucciones del asistente para configurar una ruta IPv6 para el túnel azul. Especifique el punto extremo remoto 10.1.2.2 como el salto siguiente y especifique fec0::3 como la dirección de destino.

Tras crear las líneas de túnel configuradas y las rutas que definen los puntos finales de túnel, deberá crear una ruta en el Cliente C y una ruta en el Cliente D que permita que los paquetes vuelvan al servidor del Edificio 1. Para cada una de estas rutas, debe especificarse 10.1.1.1 como el salto siguiente y fec0::1 como la dirección de destino.

Enviar paquetes IPv6 a través de una red de área amplia (WAN) IPv4

Situación

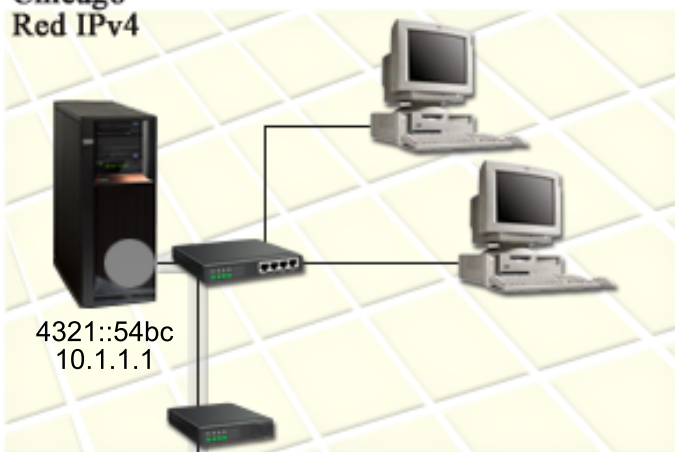
Su empresa utiliza una aplicación para la contabilidad de deudores que se encuentra en el servidor de su oficina en Chicago. Usted debe conectar la aplicación a un servidor de la oficina de Dallas. Esta

aplicación utiliza el direccionamiento IPv6 en los servidores de ambas ciudades. Puesto que su ISP no puede facilitarle direccionadores IPv6 entre estas dos ubicaciones, se ve obligado a configurar un túnel entre los dos servidores. Los paquetes de la aplicación viajan por el túnel, a través de la red de área amplia IPv4 entre los dos servidores. La imagen siguiente ilustra la configuración de la red en este escenario.

Nota: en este escenario, las direcciones IP 10.x.x.x representan direcciones IP públicas que pueden direccionarse globalmente. Todas las direcciones utilizadas se incluyen sólo a modo de ejemplo.

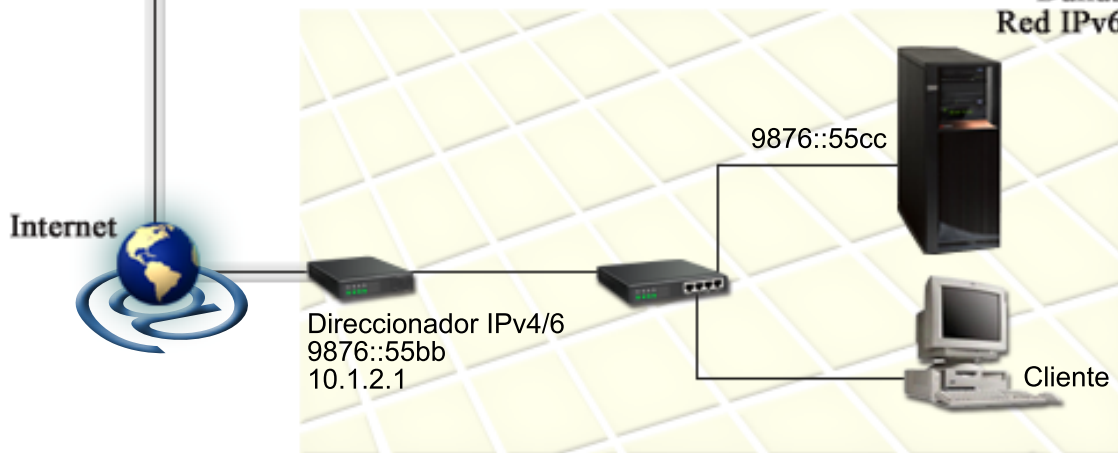
Contabilidad de deudores

Chicago
Red IPv4



Túnel configurado verde
Punto final local = 10.1.1.1
Punto final remoto = 10.1.2.1
Dirección IPv6 local = 4321::54bc

Contabilidad de acreedores
Dallas
Red IPv6



Solución

Para utilizar IPv6 a través de una red de área amplia consistente en una infraestructura de IPv4, debe crear una línea de túnel configurada y varias rutas asociadas. Funciona del siguiente modo:

- El túnel empieza en iSeries A (punto extremo local 10.1.1.1) de Chicago y acaba en el direccionador IPv4/6 (punto extremo remoto) de Dallas.
- La aplicación que reside en el iSeries A debe conectarse a la aplicación que reside en el iSeries B. El iSeries A encapsula el paquete IPv6 dentro del paquete IPv4 y lo envía a través del túnel al direccionador IPv4/6, que desencapsula el paquete IPv6 y lo reenvía al iSeries B.
- El paquete vuelve a Chicago por la ruta inversa.

La conexión de túnel es una conexión de punto a punto, por lo tanto debe definir el punto extremo remoto del túnel. Para ello se crea una ruta que se asocia a esta línea de túnel. La ruta define el punto extremo remoto (10.1.2.1) como el salto siguiente. es decir, al crear la ruta se define el punto extremo remoto. Además, la ruta define la dirección de destino como 9876::55cc (la dirección IPv6 asociada con el iSeries B).

Además de crear la ruta inicial que define el punto extremo del túnel y permite al paquete llegar hasta el iSeries B de Dallas, debe crear otras dos rutas para que el paquete pueda volver al iSeries A de Chicago.

Los requisitos para la configuración incluyen:

- OS/400 Versión 5 Release 2 o posterior.
- iSeries Access para Windows e iSeries Navigator (componente de red de iSeries Navigator)
- Para poder crear la línea de túnel configurada, antes debe configurarse TCP/IP (con IPv4) en el servidor. Si no ha configurado el servidor para IPv4, consulte Configurar TCP/IP por primera vez antes de configurar la línea de túnel para IPv6.

Configuración

Para crear una línea de túnel configurada, debe utilizar el asistente de **Configuración IPv6** y el asistente **Nueva ruta IPv6** de iSeries Navigator. Los túneles configurados sólo pueden configurarse desde iSeries Navigator, y no es posible configurarlo desde la interfaz basada en caracteres.

Para utilizar el asistente de **Configuración de IPv6** para crear la línea de túnel, siga estos pasos:

1. En iSeries Navigator, seleccione el **servidor** —> **Red** —> **Configuración TCP/IP**.
2. Pulse el botón derecho sobre **IPv6**, seleccione **Configuración de IPv6**, y siga las instrucciones del asistente para configurar una línea de túnel para IPv6. Tras completar el asistente de **Configuración de IPv6**, éste le solicitará que cree una ruta nueva para la línea de túnel configurada, aparecerá el diálogo del asistente **Nueva ruta IPv6**. Debe crear una ruta nueva para que los paquetes IPv6 puedan viajar a través del túnel de color.
3. Desde el asistente **Nueva ruta IPv6**, cree una ruta de sistema principal para el túnel. Especifique el punto extremo remoto 10.1.2.1 como el salto siguiente y 9876::55cc como la dirección de destino.

Tras crear la línea de túnel configurado y la ruta que define el punto extremo del túnel, debe crear rutas en el iSeries B y en el direccionador IPv4/6 que permitan a los paquetes volver a Chicago. Para la ruta del iSeries B, debe especificar 9876::55bb como el salto siguiente y 4321::54bc como la dirección de destino. Para la ruta del direccionador IPv4/6, debe especificar 10.1.1.1 como el salto siguiente y 4321::54bc como la dirección de destino.

Nota: el direccionador IPv4/6 de Dallas debe disponer de una ruta directa a 9876::55cc, pero puesto que esta ruta se crea automáticamente, no es necesario ningún tipo de configuración manual.

Conceptos: IPv6

Lea las descripciones de estos conceptos de IPv6 para entender mejor cómo funciona IPv6:

Comparación entre IPv4 y IPv6

Comparación entre los atributos de IPv4 e IPv6. Esta tabla le permite buscar rápidamente funciones específicas y compara su utilización en cada protocolo de Internet.

Formatos de dirección de IPv6

Obtenga más información sobre el tamaño y el formato de la dirección IPv6.

Tipos de dirección IPv6

Obtenga más información sobre los tipos nuevos de direcciones en IPv6.

Creación de túneles de IPv6

Averigüe cómo la creación de túneles de IPv6 permite que los paquetes IPv6 viajen a través de una red IPv4.

Descubrimiento de vecinos

Averigüe cómo el descubrimiento de vecinos permite a los sistemas principales y a los direccionadores comunicarse entre sí.

Configuración automática de direcciones sin información de estado

Averigüe cómo la configuración automática de direcciones sin información de estado automatiza algunas de las tareas del administrador de red.

Formatos de dirección de IPv6

El tamaño de las direcciones de IPv6 es de 128 bits. La representación preferente de direcciones de IPv6 es: `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx` donde cada `x` es un dígito hexadecimal que representa 4 bits. Las direcciones IPv6 abarcan desde `0000:0000:0000:0000:0000:0000:0000:0000` a `ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`.

Además de este formato preferente, las direcciones IPv6 pueden especificarse en otros dos formatos abreviados:

- **Omitir ceros iniciales**

Especifique las direcciones IPv6 omitiendo los ceros iniciales. Por ejemplo, la dirección IPv6 `1050:0000:0000:0000:0005:0600:300c:326b` puede escribirse como `1050:0:0:0:5:600:300c:326b`.

- **Dos signos de dos puntos**

Especifique las direcciones IPv6 con dos signos de dos puntos (`::`) en lugar de una serie de ceros. Por ejemplo, la dirección IPv6 `ff06:0:0:0:0:0:c3` puede escribirse como `ff06::c3`. Los dos signos de dos puntos sólo pueden utilizarse una vez en una dirección IP.

Un formato alternativo para las direcciones IPv6 combina la notación de dos puntos y un punto, de forma que la dirección IPv4 puede incrustarse en la dirección IPv6. Se especifican valores hexadecimales para los 96 bits de más a la izquierda, y valores decimales para los 32 bits de más a la derecha que indican la dirección IPv4 incrustada. Este formato garantiza la compatibilidad entre los nodos IPv6 y los nodos IPv4 cuando se está trabajando en un entorno de red mixto.

Estos dos tipos de direcciones IPv6 utilizan este formato alternativo:

- **Dirección IPv6 correlacionada con IPv4**

Este tipo de dirección se utiliza para representar los nodos IPv4 como direcciones IPv6. Permite que las aplicaciones de IPv6 se comuniquen directamente con las aplicaciones de IPv4. Por ejemplo, `0:0:0:0:0:ffff:192.1.56.10` y `::ffff:192.1.56.10/96` (formato abreviado).

- **Dirección IPv6 compatible con IPv4**

Este tipo de dirección se utiliza para túneles. Permite a los nodos IPv6 comunicarse a través de una infraestructura IPv4. Por ejemplo, `0:0:0:0:0:0:192.1.56.10` y `::192.1.56.10/96` (formato abreviado).

Todos estos formatos son formatos de dirección IPv6 válidos. Especifique cualquiera de estos formatos de dirección IPv6 en iSeries Navigator.

Tipos de dirección IPv6

Las direcciones IPv6 se agrupan en tres tipos básicos de categorías:

Dirección de difusión simple

La dirección de difusión simple especifica una interfaz única. Un paquete enviado a un destino de dirección de difusión simple viaja de un sistema principal al sistema principal de destino.

Existen tres tipos de dirección de difusión simple:

Dirección de enlace local

Las direcciones de enlace local han sido diseñadas para su uso en un solo enlace local (red local). Las direcciones de enlace local se configuran automáticamente en todas las interfaces. El prefijo que se utiliza para una dirección de enlace local es fe80::/10. Los direccionadores no reenvían paquetes cuya dirección de destino o de origen contenga una dirección de enlace local.

Dirección de ubicación local

Las direcciones de ubicación local han sido diseñadas para su uso en una ubicación específica. El prefijo que se utiliza para una dirección de enlace local es fec0::/10. Los direccionadores no reenvían paquetes con una dirección de origen que contenga una dirección de ubicación local fuera de una ubicación específica.

Dirección global

Las direcciones globales están diseñadas para su uso en cualquier red. El prefijo que se utiliza para una dirección global empieza por un 001 binario.

Existen dos tipos especiales de direcciones de difusión simple:

Dirección sin especificar

La dirección sin especificar es 0:0:0:0:0:0:0 o puede abreviarse con dos signos de dos puntos (::). La dirección sin especificar indica la ausencia de una dirección, y nunca puede asignarse a un sistema principal. Puede utilizarse por un sistema principal IPv6 al que todavía no se le haya asignado una dirección. Por ejemplo, cuando el sistema principal envía un paquete para descubrir una dirección de otro nodo, el sistema principal utiliza la dirección sin especificar como su dirección de origen.

Dirección de bucle de retorno

La dirección de bucle de retorno es 0:0:0:0:0:0:0:1 o puede abreviarse como ::1. Un nodo utiliza una dirección de bucle de retorno para enviarse a sí mismo un paquete.

Dirección de difusión indiferente

La dirección de difusión indiferente especifica un conjunto de interfaces, posiblemente en ubicaciones diferentes, que comparten una única dirección. Un paquete enviado a una dirección de difusión indiferente se transmite sólo al miembro más próximo del grupo. Actualmente, el servidor iSeries no da soporte a las direcciones de difusión indiferente.

Dirección de difusión múltiple

La dirección de difusión múltiple especifica un conjunto de interfaces, posiblemente en ubicaciones múltiples. El prefijo que se utiliza para una dirección de difusión múltiple es ff. Cuando se envía un paquete a una dirección de difusión múltiple, se envía una copia del paquete a cada miembro del grupo. El servidor iSeries actualmente da soporte básico a las direcciones de difusión múltiple. Actualmente no se secunda el soporte de aplicaciones y la creación de interfaces de difusión múltiple.

Túneles IPv6

Los túneles IPv6 permiten al servidor iSeries conectarse a nodos IPv6 (sistemas principales y direccionadores) a través de dominios IPv4. Los túneles permiten que redes o nodos IPv6 aislados se comuniquen sin modificar la infraestructura IPv4 subyacente. Los túneles permiten la cooperación entre los protocolos IPv4 e IPv6, y de este modo proporcionan un método transitorio de implementar IPv6 al mismo tiempo que se retiene la conectividad de IPv4.

Un túnel consiste en dos nodos de pila dual (IPv4 e IPv6) en una red IPv4. Estos nodos de pila dual pueden procesar las comunicaciones IPv4 e IPv6. Uno de los nodos de pila dual en el margen de la infraestructura IPv6 introduce (encapsula) una cabecera IPv4 delante de cada paquete IPv6 que llega, y lo

envía como si fuera tráfico IPv4 normal, a través de enlaces existentes. Los direccionadores IPv4 siguen reenviando este tráfico. En el otro lado del túnel, otro nodo de pila dual elimina la cabecera IP extra del paquete IPv6 (desencapsula) y la direcciona al destino final mediante IPv6 estándar.

Los túneles IPv6 para el servidor iSeries se ejecutan a través de líneas de túnel configurado, que son líneas virtuales. Las líneas de túnel configurado proporcionan comunicaciones IPv6 a cualquier nodo con una dirección IPv4 direccionable que de soporte a los túneles IPv6. Estos nodos pueden existir en cualquier lugar, es decir, dentro del dominio IPv4 local o dentro de un dominio remoto.

Las conexiones de túnel configurado son conexiones de punto a punto. Para configurar este tipo de línea de túnel, debe especificar el punto extremo de túnel local (dirección IPv4), como 124.10.10.150, y la dirección IPv6 local, como 1080:0:0:0:8:800:200c:417a. También debe crear una ruta IPv6 para que el tráfico pueda viajar a través del túnel. Cuando se cree la ruta, se definirá uno de los puntos finales remotos del túnel (dirección IPv4) como el salto siguiente de la ruta. Puede configurar un número ilimitado de puntos finales para un número ilimitado de túneles.

Consulte Enviar paquetes IPv6 a través de una red de área local (LAN) IPv4 y Enviar paquetes IPv6 a través de una red de área amplia (WAN) IPv4 donde encontrará escenarios e imágenes que ejemplifican los túneles IPv6.

Descubrimiento de vecinos

Los nodos IPv6 (sistemas principales o direccionadores) utilizan funciones de descubrimiento de vecinos para descubrir la presencia de otros nodos IPv6, para determinar las direcciones de capa de enlace de los nodos, buscar direccionadores que puedan reenviar paquetes IPv6, y mantener una antememoria de vecinos IPv6 activos. Los nodos IPv6 utilizan estos cinco mensajes ICMPv6 (Internet Control Message Protocol version 6) para comunicarse con otros nodos:

Solicitud de direccionador

Los sistemas principales envían estos mensajes para solicitar a los direccionadores que generen anuncios de direccionador. Un sistema principal envía una solicitud de direccionador inicial cuando un sistema principal está disponible por primera vez.

Anuncio de direccionador

Los direccionadores envían estos mensajes periódicamente o como respuesta a una solicitud de direccionador. Los sistemas principales utilizan la información facilitada por anuncios de direccionador para crear automáticamente interfaces locales y globales, y rutas asociadas. Los anuncios de direccionador también contienen más información de configuración utilizada por un sistema principal, como la unidad de transmisión máxima y el límite de saltos.

Solicitud de vecino

Los nodos envían estos mensajes para determinar la dirección de capa de enlace de un vecino o para verificar que todavía es posible alcanzar a un vecino.

Anuncio de vecino

Los nodos envían estos mensajes como respuesta a una solicitud de vecino o como un mensaje no solicitado para anunciar un cambio de dirección.

Redirección

Los direccionadores utilizan estos mensajes para informar a los sistemas principales de un primer salto mejor para un destino.

Consulte el documento RFC 2461 para obtener más información acerca del descubrimiento de vecino y el descubrimiento de direccionador. Para ver el documento RFC 2461, acceda al Editor de RFC

(<http://www.rfc-editor.org/rfcsearch.html>) .

Autoconfiguración de direcciones sin estado

La autoconfiguración de direcciones sin estado es el proceso que utilizan los nodos IPv6 (sistemas principales o direccionadores) para configurar automáticamente las direcciones IPv6 para las interfaces. El

nodo genera varias direcciones IPv6 combinando un prefijo de dirección con la dirección MAC del nodo o con un identificador de interfaz especificado por el usuario. El prefijo incluye el prefijo de enlace local (fe80::/10) y prefijos de longitud 64 anunciados por direccionadores IPv6 locales (si existen). La autoconfiguración de direcciones sin estado también crea interfaces apropiadas de difusión múltiple cuando el tipo de enlace admite la difusión múltiple.

El nodo efectúa una detección de direcciones duplicadas para verificar la exclusividad de la dirección antes de asignarla a una interfaz. El nodo envía una consulta de solicitud de vecino a la nueva dirección y espera una respuesta. Si el nodo no recibe una respuesta, se asume que la dirección es única. Si el nodo recibe una respuesta en forma de anuncio de vecino, significa que la dirección ya se está utilizando. Si un nodo determina que la dirección IPv6 intentada no es exclusiva, la autoconfiguración se detiene y es necesario configurar manualmente la interfaz.

Comparación de IPv4 e IPv6

IBM implementa IPv6 para el servidor iSeries en varios releases de software. IPv6 se implementa actualmente en una plataforma de desarrollo de aplicaciones para desarrollar y evaluar las aplicaciones de IPv6.

Quizás se pregunte en qué difieren los detalles de IPv6 e IPv4. La siguiente tabla le ofrece un resumen de los atributos comunes que se asocian a IPv4 y los compara con atributos similares de IPv6. Seleccione un atributo de esta lista para enlazarlo con la comparación de la tabla.

- “dirección” en la página 19
- “asignación de direcciones” en la página 19
- “tiempo de vida máximo de la dirección” en la página 19
- “máscara de dirección” en la página 20
- “prefijo de dirección” en la página 20
- “ARP (protocolo de resolución de dirección)” en la página 20
- “ámbito de la dirección” en la página 20
- “tipos de dirección” en la página 20
- “rastreo de comunicaciones” en la página 20
- “configuración” en la página 20
- “DNS (sistema de nombres de dominio)” en la página 20
- “DHCP (Dynamic Host Configuration Protocol)” en la página 20
- “FTP (Protocolo de transferencia de archivos)” en la página 20
- “fragmentos” en la página 20
- “tabla de sistemas principales” en la página 21
- “interfaz” en la página 21
- “ICMP (Internet Control Message Protocol)” en la página 21
- “IGMP (Internet Group Management Protocol)” en la página 21
- “cabecera IP” en la página 21
- “opciones de cabecera IP” en la página 21
- “byte de protocolo de cabecera IP” en la página 21
- “byte TOS (tipo de servicio) de cabecera IP” en la página 21
- “soporte de iSeries Navigator” en la página 21
- “conexión de LAN” en la página 21
- “L2TP (Layer 2 Tunnel Protocol)” en la página 21
- “dirección de bucle de retorno” en la página 22
- “MTU (unidad máxima de transmisión)” en la página 22
- “netstat” en la página 22
- “NAT (traducción de dirección de red)” en la página 22
- “tabla de red” en la página 22
- “petición de información de nodo” en la página 22
- “filtro de paquetes” en la página 22
- “reenvío de paquetes” en la página 22
- “túneles de paquetes” en la página 22

- “PING” en la página 22
- “PPP (protocolo de punto a punto)” en la página 22
- “restricciones de puerto” en la página 22
- “puertos” en la página 22
- “direcciones privadas y públicas” en la página 23
- “tabla de protocolos” en la página 23
- “QoS (calidad de servicio)” en la página 23
- “cambio de numeración” en la página 23
- “ruta” en la página 23
- “RIP (protocolo de información de direccionamiento)” en la página 23
- “tabla de servicios” en la página 23
- “SNMP (protocolo simple de gestión de red)” en la página 23
- “API de sockets” en la página 24
- “selección de dirección de origen” en la página 24
- “inicio y detención” en la página 24
- “Telnet” en la página 24
- “rastrear ruta” en la página 24
- “capas de transporte” en la página 24
- “dirección no especificada” en la página 24
- “VPN (red privada virtual)” en la página 24

	IPv4	IPv6
dirección	<p>32 bits de longitud (4 bytes). La dirección se compone de una red y una parte de sistema principal, que dependen de la clase de dirección. Existen varias clases de dirección: A, B, C, D o E, según los bits iniciales. El número total de direcciones IPv4 es 4 294 967 296.</p> <p>El formato de texto de las direcciones IPv4 es nnn.nnn.nnn.nnn, donde $0 \leq nnn \leq 255$, y cada n es un dígito decimal. Los ceros iniciales pueden omitirse. El número máximo de caracteres de impresión es 15, sin contar una máscara.</p>	<p>128 bits de longitud (16 bytes). La arquitectura básica es 64 bits para el número de red y 64 bits para el número de sistema principal. Con frecuencia, la parte de sistema principal de una dirección IPv6 (o parte de la misma) será una dirección MAC u otro identificador de interfaz.</p> <p>Según el prefijo de subred, IPv6 tiene una arquitectura más complicada que IPv4.</p> <p>El número de direcciones IPv6 es de 10^{28} (79 228 162 514 264 337 593 543 950 336) veces <u>mayor</u> que el número de direcciones IPv4. El formato de texto de la dirección IPv6 es xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, donde cada x es un dígito hexadecimal que representa 4 bits. Los ceros iniciales pueden omitirse. Pueden utilizarse dos signos de dos puntos (::) una vez en el formato de texto de una dirección para designar cualquier número de 0 bits. Por ejemplo, ::ffff:10.120.78.40 es una dirección IPv6 correlacionada con IPv4. (Consulte el documento RFC 2373 para obtener más detalles. Para ver este documento RFC, acceda al Editor de RFC (http://www.rfc-editor.org/rfcsearch.html).</p>
asignación de direcciones	<p>Originariamente, las direcciones se asignaban por clase de red. A medida que se agota el espacio de direcciones, se efectúan asignaciones más pequeñas mediante CIDR (direccionamiento interdominio sin clase). La asignación no está equilibrada entre instituciones y naciones.</p>	<p>La asignación está en las primeras fases. El grupo IETF (Internet Engineering Task Force) y el grupo IAB (Internet Architecture Board) han recomendado asignar una longitud de prefijo de subred /48 a prácticamente cada organización, domicilio privado o entidad. Ello dejaría 16 bits para división en subredes para la organización. El espacio de direcciones es suficientemente extenso para asignar a cada persona del mundo su propia longitud de prefijo de subred /48.</p>
tiempo de vida máximo de la dirección	<p>Por regla general, no se trata de un concepto pertinente, excepto en las direcciones asignadas mediante DHCP.</p>	<p>Las direcciones IPv6 tienen dos tiempos de vida: el preferido y el válido. El tiempo de vida preferido siempre es \leq válido.</p> <p>Si ha expirado el tiempo de vida preferido, la dirección no debe utilizarse como dirección IP de origen. Si ha expirado el tiempo de vida válido, la dirección no se utilizará (reconocerá) como dirección IP de destino válida para paquetes entrantes.</p> <p>Algunas direcciones IPv6 tienen, por definición, tiempos de vida preferidos y válidos infinitos, como la de enlace local (véase “ámbito de la dirección” en la página 20).</p>

	IPv4	IPv6
máscara de dirección	Se utiliza para designar la red desde la parte del sistema principal.	No se utiliza (véase “prefijo de dirección”).
prefijo de dirección	Algunas veces se utiliza para designar la red desde la parte del sistema principal. Puede escribirse como sufijo /nn en el formato de presentación de la dirección.	Se utiliza para designar el prefijo de subred en una dirección. Se escribe como sufijo /nnn (hasta 3 dígitos decimales, 0 <= nnn <= 128) tras el formato de impresión. Por ejemplo: fe80::982:2a5c/10, donde los primeros 10 bits engloban el prefijo de subred.
ARP (protocolo de resolución de dirección)	IPv4 utiliza el protocolo de resolución de dirección para encontrar una dirección física, como la dirección MAC o de enlace, asociada con una dirección IPv4.	IPv6 incrusta estas funciones dentro del propio IP como parte de los algoritmos para autoconfiguración sin estado y descubrimiento de vecino, utilizando ICMPv6 (Internet Control Message Protocol version 6). Por lo tanto, <u>no</u> hay nada igual a ARP6.
ámbito de la dirección	Este concepto no es válido para las direcciones de difusión simple. Existen rangos de direcciones privadas designados y bucles de retorno. Por lo demás, se asume que las direcciones son globales.	En IPv6, el ámbito de la dirección forma parte de la arquitectura. Las direcciones de difusión simple tienen tres ámbitos definidos (de enlace local, de ubicación local y global), mientras que las direcciones de difusión múltiple tienen 14 ámbitos. La selección de direcciones por omisión para el origen y para el destino tiene en cuenta el ámbito. Una zona de ámbito es una instancia de un ámbito en una red específica. Como consecuencia, las direcciones IPv6 a veces deben entrarse o asociarse con un ID de zona. La sintaxis es %zid donde zid es un número (normalmente pequeño) o un nombre. El ID de zona se escribe después de la dirección y antes del prefijo. Por ejemplo, 2ba::1:2:14e:9a9b:c%3/48.
tipos de dirección	Difusión simple, difusión múltiple y difusión general.	Difusión simple, difusión múltiple y difusión indiferente. Consulte Tipos de dirección IPv6 para obtener más descripciones.
rastreo de comunicaciones	Una herramienta para recoger un rastreo detallado de los paquetes TCP/IP (y otros) que entran y salen de un servidor iSeries.	Igual para IPv6, y se da soporte a IPv6, inclusive ICMPv6 y paquetes IPv6 transmitidos por túneles en IPv4.
configuración	La configuración debe efectuarse en un sistema recién instalado antes de poder establecer una comunicación; es decir, deben asignarse rutas y direcciones IP.	La configuración es opcional, según las funciones requeridas. Debe designarse una Ethernet o interfaz de túnel apropiada como interfaz IPv6, utilizando iSeries Navigator. Tras finalizar esta tarea, las interfaces IPv6 se configuran automáticamente. Por lo tanto, el sistema podrá comunicarse con otros sistemas IPv6 locales y remotos, según el tipo de red o según si existe un direccionador IPv6.
DNS (sistema de nombres de dominio)	Las aplicaciones aceptan nombres de sistema principal y utilizan DNS para obtener una dirección IP, utilizando la API de socket gethostbyname(). Las aplicaciones también aceptan direcciones IP y luego utilizan DNS para obtener nombres de sistema principal con gethostbyaddr(). Para IPv4, el dominio para búsquedas inversas es in-addr.arpa.	Igual para IPv6. Se da soporte a IPv6 con el tipo de registro AAAA (A cuádruple) y la búsqueda inversa (IP-a-nombre). Una aplicación puede aceptar (o no) direcciones IPv6 de DNS y seguidamente utilizar (o no) IPv6 para la comunicación. La API de socket gethostbyname() no cambia para IPv6 y la API getaddrinfo() puede utilizarse para obtener (a elección de la aplicación) sólo IPv6, o direcciones IPv4 e IPv6. Para IPv6, el dominio que se utiliza para las búsquedas inversas de elementos es ip6.arpa y, si no se encuentra, ip6.int (consulte la API getnameinfo()).
DHCP (Dynamic Host Configuration Protocol)	Se utiliza para obtener dinámicamente una dirección IP y más información de configuración.	Actualmente, DHCP no da soporte a IPv6.
FTP (Protocolo de transferencia de archivos)	El protocolo de transferencia de archivos le permite enviar y recibir archivos a través de redes.	Actualmente, FTP no da soporte a IPv6.
fragmentos	Cuando un paquete es demasiado grande para el siguiente enlace por el que debe viajar, puede ser fragmentado por el remitente (sistema principal o direccionador).	Para IPv6, la fragmentación sólo puede producirse en el nodo de origen y el reensamblado sólo se efectúa en el nodo de destino. Actualmente, no se da soporte a la cabecera de extensión de fragmentación.

	IPv4	IPv6
tabla de sistemas principales	En iSeries Navigator, una tabla configurable que asocia una dirección de Internet con un nombre de sistema principal; por ejemplo, 127.0.0.1, bucle inverso. El resolvidor de nombres de sockets utiliza esta tabla, bien sea antes de una búsqueda de DNS o cuando ha fallado una búsqueda de DNS (según la prioridad de búsqueda del nombre de sistema principal).	Actualmente, esta tabla no da soporte a IPv6. Los clientes deben configurar un registro AAAA en un DNS para la resolución de dominios IPv6. Puede ejecutar el DNS localmente en el mismo sistema que el resolvidor, o puede ejecutarlo en un sistema diferente.
interfaz	La entidad conceptual o lógica que utiliza TCP/IP para enviar y recibir paquetes y siempre asociada íntimamente con una dirección IPv4, si no denominada con una dirección IPv4. También se denomina interfaz lógica. Pueden iniciarse y detenerse independientemente entre sí e independientemente de TCP/IP utilizando los mandatos STRTCPIFC y ENDTCPIFC y utilizando iSeries Navigator.	El mismo concepto que en IPv4. Pueden iniciarse y detenerse independientemente entre sí e independientemente de TCP/IP utilizando los mandatos STRTCPIFC y ENDTCPIFC y utilizando iSeries Navigator.
ICMP (Internet Control Message Protocol)	IPv4 utiliza ICMP para comunicar información de red.	Para IPv6, se utiliza de un modo similar; sin embargo, ICMPv6 (Protocolo de mensajes de control de Internet, versión 6) proporciona algunos atributos nuevos. Siguen existiendo los tipos de error básicos, como "no puede alcanzarse el destino", "petición y respuesta de eco". Se añaden tipos y códigos nuevos para dar soporte al descubrimiento de vecino y funciones relacionadas.
IGMP (Internet Group Management Protocol)	Los direccionadores IPv4 utilizan IGMP para buscar sistemas principales que aceptan tráfico para un determinado grupo de difusión múltiple, y los sistemas principales IPv4 utilizan IGMP para informar a los direccionadores IPv4 sobre la existencia de escuchadores de grupo de difusión múltiple (en el sistema principal).	Sustituido por el protocolo MLD (descubrimiento de escuchador de difusión múltiple) para IPv6. Esencialmente, es similar a IGMP para IPv4, pero utiliza ICMPv6 añadiendo unos valores de tipo ICMPv6 específicos de MLD.
cabecera IP	Longitud variable de 20-60 bytes, según las opciones IP existentes.	Longitud fija de 40 bytes. No existen opciones de cabecera IP. En general, la cabecera IPv6 es más sencilla que la cabecera IPv4.
opciones de cabecera IP	Varias opciones que pueden acompañar a una cabecera IP (antes de cualquier cabecera de transporte).	La cabecera IPv6 no tiene opciones. Por el contrario, IPv6 añade cabeceras adicionales de extensión (opcionales). Las cabeceras de extensión son AH y ESP (inalteradas desde IPv4), salto-a-salto, direccionamiento, fragmento y destino. Actualmente, IPv6 no da soporte a ninguna cabecera de extensión.
byte de protocolo de cabecera IP	El código de protocolo de la capa de transporte o carga de paquete; por ejemplo, ICMP.	El tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo de protocolo IPv4. Aunque el efecto arquitectónico es permitir un rango definido actualmente de cabeceras siguientes, y se amplía fácilmente. La cabecera siguiente será una cabecera de transporte, una cabecera de extensión o ICMPv6.
byte TOS (tipo de servicio) de cabecera IP	Utilizado por QoS y servicios diferenciados para designar una clase de tráfico.	Designa la clase de tráfico IPv6, de un modo similar a IPv4. Utiliza códigos diferentes. Actualmente, IPv6 no da soporte a TOS.
soporte de iSeries Navigator	iSeries Navigator proporciona una función de configuración completa para TCP/IP.	La configuración opcional para IPv6 viene proporcionada en su totalidad por iSeries Navigator, inclusive el asistente de Configuración IPv6 .
conexión de LAN	La interfaz IP utiliza la conexión de LAN para acceder a la red física. Existen muchos tipos diferentes, por ejemplo: token ring, Ethernet y PPP. También se conoce como la interfaz, enlace o línea física.	IPv6 tiene el mismo concepto. Actualmente, sólo se da soporte a las tarjetas Ethernet 2838 y 2849, y a las líneas de túnel.
L2TP (Layer 2 Tunnel Protocol)	L2TP puede considerarse una PPP virtual, y funciona a través de todos los tipos de línea a los que se da soporte.	Actualmente, L2TP no da soporte a IPv6.

	IPv4	IPv6
dirección de bucle de retorno	Una interfaz con la dirección 127.*.*.* (normalmente 127.0.0.1) que un nodo sólo puede utilizar para enviarse paquetes a sí mismo. La interfaz física (descripción de línea) se denomina *LOOPBACK.	El concepto es el mismo que en IPv4, y la dirección de bucle de retorno individual es 0000:0000:0000:0000:0000:0000:0000:0001 o ::1 (versión abreviada). La interfaz física virtual se denomina *LOOPBACK6.
MTU (unidad máxima de transmisión)	La unidad máxima de transmisión de un enlace es el número máximo de bytes que soporta un tipo de enlace determinado, como una Ethernet o un módem. Para IPv4, 576 es el mínimo habitual.	IPv6 tiene un enlace inferior estructurado en MTU de 1280 bytes. Es decir, IPv6 no fragmentará los paquetes por debajo de este límite. Para enviar IPv6 a través de un enlace con menos de 1280 MTU, la capa de enlace debe fragmentar y desfragmentar con transparencia los paquetes IPv6.
netstat	Una herramienta para ver el estado de las conexiones, interfaces o rutas TCP/IP. Disponible utilizando iSeries Navigator y 5250.	Igual para IPv6, además IPv6 da soporte a 5250 e iSeries Navigator.
NAT (traducción de dirección de red)	Funciones básicas de cortafuegos integradas en TCP/IP, configuradas con iSeries Navigator.	Actualmente, NAT no da soporte a IPv6. Por regla general, IPv6 no requiere NAT. El mayor espacio de direcciones de IPv6 soluciona el problema de escasez de direcciones y permite una reenumeración más sencilla.
tabla de red	En iSeries Navigator, una tabla configurable que asocia un nombre de red con una dirección IP sin máscara. Por ejemplo, la red de sistema principal 14 y la dirección IP 1.2.3.4.	Actualmente, no se efectúan cambios en esta tabla para IPv6.
petición de información de nodo	No existe.	Una herramienta de red simple y cómoda que debe funcionar como ping, pero con contenido: un nodo IPv6 puede consultar a otro nodo el nombre DNS del destino, la dirección de difusión simple IPv6, o la dirección IPv4. Actualmente, no se soporta.
filtro de paquetes	Funciones básicas de cortafuegos integradas en TCP/IP, configuradas con iSeries Navigator.	Actualmente, el filtro de paquetes no da soporte a IPv6. Sin embargo, el filtro IPv4 puede aplicarse al tráfico IPv6 transmitido por túnel.
reenvío de paquetes	El servidor iSeries puede configurarse para reenviar los paquetes IP que recibe para direcciones IP no locales. Normalmente, la interfaz de entrada y la interfaz de salida se conectan a LAN diferentes.	Actualmente, los paquetes IPv6 no se reenvían.
túneles de paquetes	En IPv4, la transmisión por túneles se da en VPN para conexiones VPN en modo túnel (IPv4 transmitido en túnel en IPv4) y en L2TP.	Para IPv6, se espera que la transmisión por túneles en paquetes IPv4 sea una parte destacada de su evolución. Actualmente, el grupo IETF define como mínimo 5 tipos diferentes de túneles 6 en 4, cada uno de ellos con atributos y ventajas diferentes. Se da soporte a un tipo básico y flexible de transmisión por túneles de IPv6 en IPv4, para permitir que los nodos IPv6 puedan utilizar la existente Internet IPv4 para la comunicación. Este servicio se conoce como túneles configurados , y proporciona un enlace virtual de punto a punto entre dos nodos IPv6 y utiliza un tipo nuevo de línea de túnel llamada *TNLCFG64.
PING	Herramienta básica de TCP/IP para comprobar si puede accederse a un elemento. Disponible utilizando iSeries Navigator y 5250.	Igual para IPv6, además IPv6 da soporte a 5250 e iSeries Navigator.
PPP (Protocolo de punto a punto)	PPP da soporte a interfaces de marcación a través de varios tipos de líneas y módem.	Actualmente, PPP no da soporte a IPv6.
restricciones de puerto	Estos paneles de iSeries permiten a un cliente configurar el número de puerto o los rangos de números de puerto seleccionados para TCP o UDP, de forma que sólo están disponibles para un perfil específico.	No se soporta para IPv6. Las restricciones configuradas sólo son válidas para IPv4.
puertos	TCP y UDP tienen espacios de puerto separados, identificados mediante números de puerto en el rango 1-65535.	Para IPv6, los puertos funcionan igual que para IPv4. Puesto que se encuentran en una nueva familia de direcciones, ahora existen cuatro espacios de puerto separados. Por ejemplo, existen dos espacios de puerto TCP 80 a los que puede enlazarse una aplicación, uno en AF_INET y uno en AF_INET6.

	IPv4	IPv6
direcciones privadas y públicas	Todas las direcciones IPv4 son públicas, excepto tres intervalos de direcciones que IETF RFC 1918 ha designado como privados: 10.*.* (10/8), 172.16.0.0 a 172.31.255.255 (172.16/12), y 192.168.*.* (192.168/16). Los dominios de direcciones privados normalmente se utilizan en organizaciones. Las direcciones privadas no pueden direccionarse a través de Internet.	IPv6 tiene un concepto similar, pero con diferencias importantes. Las direcciones son públicas o temporales (anteriormente denominadas anónimas). Véase RFC 3041. A diferencia de las direcciones privadas de IPv4, las direcciones temporales pueden direccionarse globalmente. La motivación también es diferente; las direcciones temporales de IPv6 pretenden proteger la identidad de un cliente cuando establece una comunicación (asuntos de privacidad). Las direcciones temporales tienen un tiempo de vida limitado, y no contienen un identificador de interfaz que sea una dirección de enlace (MAC). Generalmente no pueden distinguirse de las direcciones públicas. IPv6 tiene el concepto de ámbito de direcciones limitado utilizando sus designaciones de ámbito estructurado (véase "ámbito de la dirección" en la página 20).
tabla de protocolos	En iSeries Navigator, una tabla configurable que asocia un nombre de protocolo con su número de protocolo asignado; por ejemplo, UDP, 17. El sistema se envía con un número pequeño de entradas: IP, TCP, UDP, ICMP.	La tabla da soporte a IPv6 sin cambios.
QoS (calidad de servicio)	La calidad de servicio le permite solicitar la prioridad de paquetes y la anchura de banda para las aplicaciones TCP/IP.	Actualmente, QoS no da soporte a IPv6. Sin embargo, cuando IPv6 se envía en túneles dentro de IPv4, pueden aplicarse los recursos de QoS de iSeries existentes al tráfico IPv4, que entonces manejará de forma transparente las cargas útiles de IPv6.
cambio de numeración	Efectuado mediante una nueva configuración manual, con la posible excepción de DHCP. Generalmente, para una ubicación u organización, un proceso difícil y problemático que debe evitarse siempre que sea posible.	Es un elemento arquitectónico importante de IPv6, y se supone que es en gran parte automático especialmente en el prefijo /48.
ruta	Lógicamente, una correlación de un conjunto de direcciones IP (puede contener sólo 1) a una interfaz física y una sola dirección IP de salto siguiente. Los paquetes IP cuya dirección de destino se define como parte del conjunto se reenvían al salto siguiente utilizando la línea. Las rutas IPv4 se asocian con una interfaz IPv4, por consiguiente, una dirección IPv4. La ruta por omisión es *DFROUTE.	Conceptualmente, igual que IPv4. Una diferencia importante: las rutas IPv6 se asocian (vinculan) con una interfaz física (un enlace como *TNLCFG64 o ETH03), y no con una interfaz. Existen varios motivos. Uno de ellos es que la selección de la dirección de origen funciona de un modo distinto para IPv6 y para IPv4. Véase "selección de dirección de origen" en la página 24. Se permiten rutas duplicadas para mejorar la solidez, pero éstas se ignoran durante la búsqueda de rutas.
RIP (protocolo de información de direccionamiento)	RIP es un protocolo de direccionamiento al que da soporte el daemon direccionado.	Actualmente, RIP no da soporte a IPv6. El direccionamiento de IPv6 utiliza rutas estáticas.
tabla de servicios	En el servidor iSeries, una tabla configurable que asocia un nombre de servicio con un puerto y protocolo; por ejemplo, control FTP de nombre de servicio, puerto 21, TCP y UDP. En la tabla de servicios aparece un número elevado de servicios muy conocidos. Muchas aplicaciones utilizan esta tabla para determinar qué puerto utilizar.	Para IPv6, no se efectúa ningún cambio en esta tabla.
SNMP (protocolo simple de gestión de red)	SNMP es un protocolo para la administración de sistemas.	Actualmente, SNMP no da soporte a IPv6. El direccionamiento de IPv6 utiliza rutas estáticas.

	IPv4	IPv6
API de sockets	Estas API son la forma en que las aplicaciones utilizan TCP/IP. Las aplicaciones que no necesitan IPv6 no se ven afectadas por los cambios de sockets para dar soporte a IPv6.	IPv6 mejora los sockets de forma que ahora las aplicaciones pueden utilizar IPv6, con una familia de direcciones nueva: AF_INET6. Las mejoras han sido diseñadas de forma que las aplicaciones IPv4 existentes no se ven afectadas de ningún modo por IPv6 y los cambios de API. Se da cabida a las aplicaciones que quieren dar soporte al tráfico IPv4 e IPv6 concurrente, o sólo al tráfico IPv6, utilizando direcciones IPv6 correlacionadas con IPv4 con el formato <code>::ffff:a.b.c.d</code> , donde a.b.c.d es la dirección IPv4 del cliente. Las nuevas API también incluyen soporte para la conversión de direcciones IPv6 de texto a binario y de binario a texto. Véase Utilización de la familia de direcciones AF_INET6 para más información sobre las mejoras de sockets para IPv6.
selección de dirección de origen	Una aplicación puede designar un IP de origen (normalmente, mediante sockets <code>bind()</code>). Si se enlaza con <code>INADDR_ANY</code> , se selecciona un IP de origen basándose en la ruta.	Al igual que con IPv4, una aplicación puede designar una dirección IPv6 de origen utilizando <code>bind()</code> . Del mismo modo, puede dejar que el sistema seleccione una dirección de origen IPv6 utilizando <code>in6addr_any</code> . Sin embargo, puesto que las líneas IPv6 tienen muchas direcciones IPv6, el método interno de selección de un IP de origen es diferente.
inicio y detención	Utilice <code>STRTCP</code> y <code>ENDTCP</code> para iniciar o detener TCP/IP.	Igual que para IPv4. IPv4 e IPv6 no se inician o detienen independientemente entre sí o independientemente de TCP/IP. Es decir, se inicia o detiene todo el TCP/IP, no sólo IPv4 o IPv6. Las interfaces IPv6 se inician automáticamente cuando el parámetro <code>AUTOSTART = *YES</code> (el valor por omisión). IPv6 no puede utilizarse o configurarse sin IPv4, e IPv6 debe tener el bucle de retorno IPv6 configurado (<code>::1</code>).
Telnet	Telnet le permite iniciar la sesión y utilizar un ordenador remoto como si estuviera conectado al mismo directamente.	Actualmente, Telnet no da soporte a IPv6.
rastrear ruta	Herramienta básica de TCP/IP para efectuar determinaciones de ruta. Disponible utilizando <code>iSeries Navigator</code> y <code>5250</code> .	Igual para IPv6, además IPv6 da soporte a <code>5250</code> e <code>iSeries Navigator</code> .
capas de transporte	TCP, UDP, RAW. Un transporte nuevo, SCTP (protocolo de transmisión de control de flujo) pretende ofrecer las mejores funciones de TCP y UDP, es decir, comunicación garantizada sin conexión. SCTP se utiliza desde hace muy poco, y todavía no se soporta en el <code>iSeries</code> .	Para IPv6, existen los mismos tres transportes, sin cambios funcionales.
dirección no especificada	Aparentemente, no definida como tal. La programación de sockets utiliza <code>0.0.0.0</code> como <code>INADDR_ANY</code> .	Se define como <code>::/128</code> (128 0 bits). Se utiliza como el IP de origen en algunos paquetes de descubrimiento de vecino, y otros contextos diferentes, como sockets. La programación de sockets utiliza <code>::/128</code> como <code>in6addr_any</code> .
VPN (red privada virtual)	La red privada virtual (con IPsec) le permite extender una red privada segura a lo largo de una red pública existente.	Actualmente, VPN no da soporte a IPv6. Sin embargo, cuando IPv6 se envía en túneles dentro de IPv4, pueden aplicarse los recursos VPN de <code>iSeries</code> existentes al tráfico IPv4, que entonces manejará con transparencia las cargas útiles de IPv6.


Solución de problemas de IPv6


Si ha configurado IPv6 en el servidor, puede utilizar muchas de las herramientas para la solución de problemas que se utilizan para IPv4. Por ejemplo, herramientas como rastrear ruta y PING aceptan los dos formatos de direcciones IPv4 e IPv6, y pueden utilizarse para verificar las conexiones y rutas para ambos tipos de redes. Además, puede utilizar la función rastreo de comunicaciones para rastrear datos en líneas de comunicaciones IPv4 e IPv6.


Véase Solución de problemas de TCP/IP donde encontrará una guía general con técnicas para la solución de problemas relacionados con IPv4 e IPv6.

Información relacionada para IPv6

Para obtener más información sobre IPv6, consulte estas fuentes de información:

The Internet Engineering Task Force (IETF) (<http://www.ietf.cnri.reston.va.us/>) 
Información sobre el grupo de personas que desarrollan el protocolo de Internet, inclusive IPv6.

IP Version 6 (IPv6) (<http://playground.sun.com/pub/ipng/html/ipng-main.html>) 
Contiene especificaciones actuales de IPv6 y referencias a varias fuentes sobre IPv6.

IPv6 Forum (<http://www.ipv6forum.com/>) 
Incluye artículos y eventos nuevos relacionados con los últimos desarrollos de IPv6.

Capítulo 4. Planificación de la configuración de TCP/IP

Antes de empezar a instalar y configurar su servidor iSeries, tómese unos minutos para planificar la operación. Consulte los temas que se indican a continuación para conocer las directrices de la planificación. Estas directrices de planificación se refieren a la configuración básica de TCP/IP utilizando IPv4. Si pretende configurar IPv6, consulte Configurar IPv6 donde encontrará los requisitos para la instalación e instrucciones para la configuración.

Requisitos de configuración de TCP/IP

Recopile y anote información básica de configuración, necesaria para la configuración de TCP/IP.

Consideraciones sobre la seguridad TCP/IP

Considere las necesidades de seguridad como nuevo miembro de una red.

Requisitos de la configuración de TCP/IP

Imprima esta página y anote la información de configuración acerca del servidor y de la red TCP/IP a la que va a conectarse. Más tarde deberá consultar esta información cuando configure TCP/IP. Utilice las instrucciones que encontrará después de la tabla para determinar los valores de las primeras dos filas. Si no está familiarizado con ninguno de estos conceptos, consulte el libro rojo de IBM TCP/IP for AS/400:

More Cool Things Than Ever  y consulte el Capítulo 2, "TCP/IP: Basic Installation and Configuration".

Información necesaria	Para el sistema	Ejemplo
Tipo de adaptador de comunicaciones instalado en el sistema (ver más abajo las instrucciones)		Ethernet
Nombre de recurso		CMN01
Dirección IP para su servidor iSeries		199.5.83.158
Máscara de subred para su servidor iSeries		255.255.255.0
Dirección de la pasarela		199.5.83.129
Nombre de sistema principal y nombre de dominio del sistema		sys400.xyz.empresa.com
Dirección IP del servidor de nombres de dominio		199.4.191.76

Para averiguar la información del adaptador de comunicaciones, siga estos pasos:

1. En la línea de mandatos del servidor, escriba `go hardware y`, a continuación, **Intro**.
2. Para seleccionar la opción Trabajar con recursos de comunicaciones (Opción 1), escriba `1`, y pulse **Intro**.


Los recursos de comunicaciones se listarán ordenados por nombre de recurso. Siga las instrucciones de la pantalla si desea trabajar con los recursos o ver más detalles.

Qué hacer a continuación:

Instalar TCP/IP

Consideraciones sobre la seguridad TCP/IP

Cuando planifique la configuración TCP/IP, debe considerar las necesidades de seguridad. Las siguientes estrategias pueden ayudarle a limitar el riesgo en TCP/IP:

- **Arranque sólo aquellas aplicaciones TCP/IP que necesite.**
Cada aplicación TCP/IP tiene sus propios riesgos de seguridad exclusivos. No depende de un direccionador para rechazar peticiones para una aplicación determinada. Como defensa secundaria, establezca en NO los valores de inicio automático de las aplicaciones que no sean necesarias.
- **Limite las horas durante las que se ejecutan las aplicaciones TCP/IP.**
Limite el riesgo reduciendo las horas de ejecución de los servidores. Si es posible, detenga los servidores TCP/IP, como por ejemplo FTP y Telnet, fuera de la jornada laboral.
- **Controle las personas que pueden arrancar y cambiar las aplicaciones TCP/IP.**
Por omisión, se necesita la autorización *IOSYSCFG para modificar los valores de la configuración de TCP/IP. Un usuario sin autorización *IOSYSCFG necesitará la autorización *ALLOBJ o una autorización explícita para los mandatos de arranque de TCP/IP. El hecho de otorgar autorizaciones especiales a usuarios representa un riesgo de seguridad. Evalúe la necesidad de otorgar autorizaciones especiales a cada uno de los usuarios y otorgue el mínimo de ellas. Realice un seguimiento de los usuarios que tienen autorizaciones especiales y revise periódicamente su necesidad. De este modo también se limita la posibilidad de que se acceda al servidor fuera de la jornada laboral.
- **Controle el direccionamiento TCP/IP:**
 - No permita el reenvío IP; de este modo los piratas informáticos no podrán utilizar su servidor Web para atacar otros sistemas de confianza.
 - Defina sólo una ruta en el servidor Web público: la ruta por omisión al Proveedor de Servicios de Internet.
 - No configure nombres ni direcciones IP de sistemas principales protegidos internos en la tabla de sistemas principales TCP/IP del servidor Web. Coloque en ella sólo el nombre de los demás servidores públicos que necesite alcanzar.
- **Controle los servidores TCP/IP diseñados para los inicios de sesión remotos e interactivos.**
Las aplicaciones tales como FTP y Telnet son más vulnerables a los ataques externos. Si desea obtener detalles sobre cómo controlar el riesgo, puede leer el capítulo dedicado a ofrecer consejos sobre el control de los inicios de sesión interactivos en el apartado Consejos y herramientas para proteger el iSeries  .

Si desea obtener más información acerca de la seguridad y de las opciones disponibles, consulte la sección iSeries y la seguridad en Internet.

Capítulo 5. Instalar TCP/IP

El soporte TCP/IP base viene con OS/400 y le permite conectar un servidor iSeries a una red. No obstante, si desea utilizar aplicaciones TCP/IP, como por ejemplo Telnet, FTP y SMTP, también deberá instalar TCP/IP Connectivity Utilities, que es un producto bajo licencia instalable por separado que se incluye con el sistema operativo.

Para instalar TCP/IP Connectivity Utilities en el servidor iSeries, siga los pasos siguientes:

1. Inserte el soporte de instalación de TCP/IP en el servidor. Si el soporte de instalación es un CD-ROM, insértelo en el dispositivo óptico. Si el soporte de instalación es una cinta, insértela en la unidad de cintas.
2. En la línea de mandatos, escriba G0 LICPGM y pulse **Intro** para acceder a la pantalla Trabajar con programas bajo licencia.
3. Seleccione la opción **11** (Instalar programas bajo licencia) en la pantalla Trabajar con Programas bajo Licencia, para ver una lista de los programas bajo licencia y sus componentes opcionales.
4. Introduzca **1** (Instalar) en la columna Opción junto a la entrada 57xxTC1 (TCP/IP Connectivity Utilities para iSeries). Pulse **Intro**. La pantalla Confirmar Instalación de Programas Bajo Licencia muestra el programa bajo licencia que se ha seleccionado para su instalación. Pulse **Intro** para confirmar la acción.
5. Cumplimente las siguientes opciones en la pantalla Opciones de Instalación:

Dispositivo de instalación	Escriba Q0PT si efectúa la instalación desde un dispositivo CD-ROM. Escriba TAP01 si efectúa la instalación desde una unidad de cinta.
Objetos a instalar	Esta opción le permite instalar tanto programas como objetos de idioma, sólo programas o sólo objetos de idioma.
Reinicio automático	Esta opción determina si el sistema se arrancará automáticamente cuando haya finalizado satisfactoriamente el proceso de instalación.

Cuando se instala satisfactoriamente TCP/IP Connectivity Utilities, aparece el menú Trabajar con Programas bajo Licencia o la pantalla de Inicio de Sesión.

6. Seleccione la opción **50** (Visualizar anotaciones para mensajes) para verificar que se haya instalado satisfactoriamente el programa bajo licencia.

Si se produce un error, verá el mensaje No se ha completado la función de Trabajar con Programas bajo Licencia en la parte inferior de la pantalla Trabajar con Programas bajo Licencia. Si se produce un error, intente de nuevo la instalación de TCP/IP Connectivity Utilities. Si el problema no se resuelve, puede ponerse en contacto con el servicio técnico.

Nota:

Otros programas bajo licencia que puede instalar son los siguientes:

- iSeries Access para Windows 95/NT (5769–XD1 V3R1M3 o posterior) proporciona soporte para iSeries Navigator que se utiliza para configurar algunos de los componentes de TCP/IP.
- IBM HTTP Server para iSeries (57xx–DG1) proporciona soporte de servidor Web.
- Algunas aplicaciones TCP/IP requieren la instalación de programas bajo licencia adicionales. Para conocer qué programas son necesarios, repase las instrucciones de instalación de la aplicación concreta que desea instalar.

Capítulo 6. Configurar TCP/IP

Quizás configure TCP/IP por primera vez, o puede que esté modificando una configuración existente para utilizar la función IPv6. Este tema facilita instrucciones para configurar TCP/IP en cada una de estas situaciones. En las siguientes opciones encontrará instrucciones sobre cómo configurar TCP/IP en su servidor:

Configurar TCP/IP por primera vez

Utilice estas instrucciones si está configurando un servidor nuevo. Establecerá una conexión y configurará TCP/IP por primera vez.

Configurar IPv6

Utilice estas instrucciones para configurar su servidor para IPv6. Se beneficiará de prestaciones de direccionamiento mejoradas y las sólidas opciones de este protocolo de Internet. Si no está familiarizado con IPv6, consulte Protocolo de Internet versión 6 (IPv6) donde encontrará un resumen descriptivo. Debe tener TCP/IP configurado en el servidor antes de poder configurar IPv6.

Configurar TCP/IP cuando el sistema se encuentra en estado restringido

Utilice este método si necesita ejecutar TCP/IP mientras el sistema operativo se encuentra en estado restringido.

Configurar TCP/IP por primera vez

Seleccione uno de los métodos siguientes para configurar TCP/IP en su nuevo servidor:

Configurar TCP/IP utilizando el asistente de configuración EZ-Setup

Utilice este método preferente si su sistema está equipado para utilizar el asistente de configuración EZ-Setup. El asistente de configuración EZ-Setup se incluye con el servidor iSeries.

Configurar TCP/IP utilizando la interfaz basada en caracteres

Utilice este método si no puede utilizar el asistente de configuración EZ-Setup. Por ejemplo, si quiere utilizar iSeries Navigator desde un sistema que requiere una configuración TCP/IP básica antes de la ejecución de iSeries Navigator, debe utilizar este método.

Configurar TCP/IP utilizando el asistente de configuración EZ-Setup

iSeries Navigator es una interfaz de usuario gráfica que proporciona cuadros de diálogo y asistentes concisos para configurar TCP/IP. Para la configuración inicial, utilice el asistente EZ-Setup de iSeries Navigator para establecer una conexión y configurar TCP/IP por primera vez. Este es el método preferente para trabajar con el servidor, pues la interfaz es fácil de utilizar. El CD-ROM que contiene el asistente de configuración EZ-Setup se incluye con el servidor iSeries.


Para configurar el servidor, siga estos pasos:

1. Utilice el asistente de configuración EZ-Setup. Acceda al asistente desde el CD-ROM incluido con el servidor. Siga las instrucciones del asistente para configurar TCP/IP.
2. Arrancar TCP/IP
 - a. En iSeries Navigator, expanda **servidor** -> **Red**.
 - b. Pulse el botón derecho del ratón en **Configuración TCP/IP** y seleccione **Arrancar**. Todas las interfaces y todos los servidores que se han establecido para iniciarse automáticamente cuando se iniciara TCP/IP se arrancarán en este momento.

Ya ha finalizado la configuración de TCP/IP en el servidor. Utilice iSeries Navigator para modificar la configuración cuando varíen sus necesidades de trabajo en red. Consulte Personalizar TCP/IP con iSeries Navigator para añadir rutas e interfaces o Configurar IPv6 para utilizar el protocolo de Internet versión 6 en su red.

Configurar TCP/IP utilizando la interfaz basada en caracteres

Si no puede utilizar el asistente de configuración EZ-Setup de iSeries Navigator, utilice en su lugar la interfaz basada en caracteres. Por ejemplo, si desea utilizar iSeries Navigator desde un sistema que requiera una configuración básica de TCP/IP antes de la ejecución de iSeries Navigator, deberá utilizar la interfaz basada en caracteres para llevar a cabo la configuración básica.

Para realizar los pasos de configuración de esta sección, necesita la autorización especial *IOSYSCFG en su perfil de usuario. Para obtener más información sobre este tipo de autorización, consulte el capítulo sobre perfiles de usuario en Referencia de seguridad del iSeries .

Para configurar TCP/IP utilizando la interfaz basada en caracteres, siga los pasos siguientes:

1. En la línea de mandatos, introduzca GO TCPADM para visualizar el menú Administración TCP/IP, y pulse Intro.
2. Especifique la opción 1 (Configurar TCP/IP) para visualizar el menú Configurar TCP/IP (CFGTCP), y pulse Intro. Utilice este menú para seleccionar tareas de configuración. Antes de empezar a configurar el servidor, repase las opciones del menú durante unos instantes.

Para configurar TCP/IP en su servidor, siga estos pasos:

1. Configurar una descripción de línea
2. Activar el reenvío de datagramas
3. Configurar una interfaz
4. Configurar una ruta
5. Definir nombres de sistema principal y dominio local
6. Definir una tabla de sistemas principales
7. Arrancar TCP/IP

Configurar una descripción de línea (Ethernet)

Con estas instrucciones puede configurar TCP/IP a través de un adaptador de comunicaciones Ethernet. Sin embargo, si está utilizando un tipo de adaptador diferente, por ejemplo un token-ring, consulte Configuración de TCP/IP y Referencias, *Apéndice A*, y busque un mandato específico para su adaptador.

Para configurar una descripción de línea, siga estos pasos:

1. En la línea de mandatos, entre CRTLINETH para acceder al menú Crear desc línea (Ethernet)(CRTLINETH), y pulse Intro.
2. Especifique el nombre de la línea y pulse Intro. (Utilice cualquier nombre).
3. Especifique el nombre del recurso y pulse Intro.

Qué hacer a continuación:

Activar el reenvío de datagramas

Activar el reenvío de datagramas

Active el reenvío de datagramas IP para que los paquetes se puedan reenviar a diferentes subredes.

Para activar el reenvío de datagramas IP, siga estos pasos:

1. En la línea de mandatos, escriba CHGTCPA y pulse F4.
2. En la solicitud *Reenvío de datagramas IP*, escriba *YES.

Qué hacer a continuación:

Configurar una interfaz

Configurar una interfaz

Para configurar una interfaz, siga estos pasos:

1. En la línea de mandatos, entre CFGTCP para acceder al menú Configurar TCP/IP, y pulse Intro.
2. Seleccione la opción 1 (Trabajar con interfaces TCP/IP) del menú Configurar TCP/IP, y pulse Intro.
3. Especifique la opción 1 (Añadir) para ver la pantalla Añadir interfaz TCP/IP, y pulse Intro.
4. Especifique el valor de la dirección que desea que represente a su servidor iSeries, la dirección de máscara de subred, y el nombre de descripción de línea previamente definido, y pulse Intro.

Para iniciar la interfaz, especifique la opción 9 (Arrancar) para la interfaz configurada, y pulse Intro.

Qué hacer a continuación:

Configurar una ruta

Configurar una ruta

Para acceder a redes remotas, se requiere como mínimo una entrada de direccionamiento. Si no se añaden manualmente entradas de direccionamiento, el servidor no podrá acceder a los sistemas que no estén en la misma red a la que pertenece el servidor. También deberá añadir entradas de direccionamiento para permitir el funcionamiento correcto de los clientes TCP/IP que intentan acceder a su servidor desde una red remota.

Debe proyectar tener la tabla de direccionamientos definida de forma que siempre exista una entrada para, como mínimo, una ruta por omisión (*DFTRROUTE). Si no existe ninguna coincidencia en ninguna otra entrada de la tabla de direccionamientos, los datos se envían al direccionador IP que especifica la primera entrada de dirección por omisión disponible.

Para configurar una ruta por omisión, siga estos pasos:

1. Seleccione la opción 2 (Trabajar con rutas TCP/IP) en el menú Configurar TCP/IP, y pulse Intro.
2. Especifique la opción 1(Añadir) para pasar a la pantalla Añadir ruta TCP/IP (ADDTCPRTE), y pulse Intro.
3. Especifique *DFTRROUTE en el destino de la ruta y *NONE para la máscara de subred; especifique la dirección IP para el salto siguiente y pulse Intro.

Qué hacer a continuación:

Definir nombres de sistema principal y dominio local

Definir nombres de sistema principal y dominio local

Siga estos pasos para definir nombres de sistema principal y dominio local:

1. Seleccione la opción 12 (Modificar dominio TCP/IP) del menú Configurar TCP/IP y pulse Intro.
2. Especifique los nombres seleccionados como nombre de sistema principal local y nombre de dominio local, respetando los valores por omisión del resto de parámetros, y pulse Intro.

Qué hacer a continuación:

Definir una tabla de sistemas principales

Definir una tabla de sistemas principales

Para definir una tabla de sistemas principales, siga estos pasos:

1. Seleccione la opción 10 (Trabajar con las entradas de la tabla de sistemas principales TCP/IP) del menú Configurar TCP/IP, y pulse Intro.
2. Especifique la opción 1 (Añadir) para acceder a la pantalla Añadir entrada a la tabla de sistemas principales TCP/IP y pulse Intro.

3. Especifique la dirección IP, el nombre de sistema principal local asociado y el nombre de sistema principal totalmente calificado, y pulse Intro.
4. Especifique un signo de más (+) para dejar espacio para más de un nombre de sistema principal, si es necesario.
5. Repita estos pasos para cada uno de los sistemas principales de la red con los que desea comunicarse por el nombre, y añada una entrada para cada uno.

Qué hacer a continuación:

Arrancar TCP/IP

Arrancar TCP/IP

Los servicios TCP/IP no están disponibles hasta que no se arranca TCP/IP.

Para arrancar TCP/IP, entre STRTCP en la línea de mandatos.

El mandato Arrancar TCP/IP (STRTCP) inicializa y activa el proceso de TCP/IP, arranca las interfaces TCP/IP, e inicia los trabajos del servidor. Con el mandato STRTCP sólo se arrancan los servidores y las interfaces TCP/IP con AUTOSTART *YES.

Ya ha finalizado la configuración de TCP/IP en el servidor. Utilice iSeries Navigator para modificar la configuración cuando varíen sus necesidades de trabajo en red. Consulte Personalizar TCP/IP con iSeries Navigator para añadir rutas e interfaces o Configurar IPv6 para utilizar el protocolo de Internet versión 6 en su red.

Configurar IPv6

Ahora ya puede aprovechar las ventajas que le ofrece la Internet de próxima generación utilizando IPv6 en la red. Para utilizar la función IPv6, debe cambiar la configuración de TCP/IP configurando una línea específica para IPv6. Debe configurar una línea en un adaptador de Ethernet 2838 o 2849 o en una línea de túnel configurada (línea virtual). En estos temas encontrará instrucciones referentes a la configuración de IPv6:

Requisitos de configuración

Este tema muestra los requisitos de hardware y de software para la configuración del servidor para IPv6.

Configurar IPv6 utilizando el asistente de Configuración de IPv6

Consulte las instrucciones para utilizar el asistente de **Configuración de IPv6** para configurar IPv6 en el servidor.

Requisitos de configuración

Determine cuál de estos dos tipos de configuraciones IPv6 es apropiado en su caso. Si no está seguro de qué tipo seleccionar, consulte Escenarios de IPv6 para obtener ejemplos.

Para que IPv6 funcione en su servidor, debe cumplir estos requisitos:

Para configurar una línea Ethernet para IPv6:

- OS/400 Versión 5 Release 2 o posterior.
- iSeries Access para Windows e iSeries Navigator
 - Componente de red de iSeries Navigator
- Adaptador de Ethernet 2838 o 2849 que debe dedicarse a IPv6.
- Sólo se requiere un direccionador que admita IPv6 si desea enviar tráfico IPv6 más allá de la LAN inmediata.

- Debe configurarse TCP/IP (con IPv4) en un adaptador físico separado porque TCP/IP debe ejecutarse en el servidor. Si no ha configurado el servidor para IPv4, consulte Configurar TCP/IP por primera vez antes de configurar la línea para IPv4.

Para crear una línea de túnel configurada (TNLCFG64):

- OS/400 Versión 5 Release 2 o posterior.
- iSeries Access para Windows e iSeries Navigator
 - Componente de red de iSeries Navigator
- Debe configurarse TCP/IP (con IPv4) en el servidor, antes de configurar la línea de túnel para IPv6. Si no ha configurado su servidor para IPv4, consulte Configurar TCP/IP por primera vez.

Acceda a Configurar IPv6 con el asistente de Configuración de IPv6 donde encontrará instrucciones para acceder al asistente.

Configurar IPv6 utilizando el asistente de configuración de IPv6

Para configurar IPv6 en el servidor, debe cambiar la configuración del servidor utilizando el asistente de **Configuración de IPv6** en iSeries Navigator. IPv6 sólo puede configurarse desde iSeries Navigator, y no es posible configurarlo desde la interfaz basada en caracteres.

Nota: puede configurar la descripción de la línea de Ethernet IPv6 utilizando el mandato Crear desc línea (Ethernet) CRTLINETH en la interfaz basada en caracteres; sin embargo, debe especificar la dirección de grupo de difusión múltiple hexadecimal 333300000001. A continuación, debe utilizar el asistente de **Configuración de IPv6** para acabar la configuración de IPv6.

El asistente necesita la siguiente información:

Para configurar una línea Ethernet para IPv6:

esta configuración le permite enviar paquetes IPv6 a través de una red de área local (LAN) IPv6. El asistente necesita el nombre del recurso de comunicaciones de hardware en el servidor en que se configurará IPv6; por ejemplo, CMN01. Debe ser un adaptador de Ethernet 2838 o 2849 que no esté configurado actualmente para IPv4. Véase Crear una red de área local (LAN) IPv6 donde encontrará un escenario que describe una situación en la que se configuraría una línea Ethernet para IPv6.

Para crear una línea de túnel configurada (TNLCFG64):

este tipo de configuración le permite enviar paquetes IPv6 a través de redes IPv4. El asistente requiere la dirección IPv4 para el punto extremo local y la dirección IPv6 para la interfaz local asociada con el túnel. Consulte Enviar paquetes IPv6 a través de una red de área local (LAN) IPv4 y Enviar paquetes IPv6 a través de una red de área amplia (WAN) IPv4 donde encontrará escenarios que describen dos situaciones en las que se crearían las líneas de túnel configuradas para IPv6.

Para utilizar el asistente de **Configuración de IPv6**, siga estos pasos:

1. En el Navigator de iSeries, expanda **servidor** —> **Red** —> **Configuración TCP/IP**.
2. Pulse el botón derecho sobre **IPv6** y seleccione **Configuración de IPv6**.
3. Siga las instrucciones del asistente para configurar IPv6 en el servidor.

Configurar TCP/IP cuando el sistema operativo se encuentra en estado restringido

Situación

Como administrador de red, necesita obtener informes del estado de las copias de seguridad del servidor. Al ejecutar los procedimientos de copia de seguridad, el sistema operativo debe estar en un estado restringido para impedir que los usuarios puedan cambiar la configuración. Ya que se encuentra en una ubicación remota, accede a los informes de estado mediante un dispositivo PDA (asistente digital personal) o cualquier dispositivo de red TCP/IP. El PDA utiliza una aplicación habilitada para sockets

que requiere una interfaz TCP/IP activa para comunicarse con el servidor. Para permitir esta comunicación, primero debe iniciar TCP/IP utilizando unos parámetros especiales. Una vez haya iniciado TCP/IP, deberá iniciar una interfaz TCP/IP específica para permitir el acceso al sistema. A continuación encontrará información más detallada.

Prerrequisitos

El servidor iSeries debe ejecutar OS/400(R) V5R2 o posterior.

Restricciones

Son aplicables las siguientes restricciones cuando el sistema operativo se ejecuta en estado restringido:

- No se pueden iniciar servidores TCP/IP (mandato CL STRTCPSRV), ya que requieren subsistemas activos.
- Sólo puede iniciarse una interfaz para un tipo de línea determinado (Ethernet, Token Ring o DDI) que no esté conectado a una descripción de servidor de red (NWSD) o una descripción de interfaz de red (NWID).

Pasos de la configuración

1. Iniciar TCP/IP utilizando parámetros especiales

Cuando el sistema iSeries se encuentre en estado restringido, procese el siguiente mandato desde la interfaz de línea de mandatos: STRTCP STRSVR(*NO) STRIFC(*NO). Estos son los únicos parámetros que se aceptan cuando el sistema operativo se encuentra en estado restringido. El mandato anterior iniciará TCP/IP; no obstante, no iniciará ni puede iniciar servidores de aplicaciones TCP/IP ni interfaces IP.

2. Iniciar una interfaz TCP/IP determinada

Una vez haya iniciado TCP/IP en estado restringido, puede iniciar la interfaz concreta necesaria para la aplicación habilitada para sockets.

- a. Verificar que la interfaz que desea iniciar utiliza una descripción de línea de *ELAN, *TRLAN o *DDI.

Para ver el tipo de línea de la interfaz, en una interfaz de línea de mandatos entre CFGTCP y seleccione la opción 1 - Trabajar con interfaces TCP/IP.

- b. Verificar que la interfaz no está conectada a una NWID o NWSD. Cualquier otro intento provocará un mensaje de error.

Para verificar que la interfaz no está conectada a una NWID o NWSD, desde una interfaz de línea de mandatos entre DSPLIND abc (donde abc es el nombre de la descripción de línea). Verifique que el nombre de recurso no es *NWID o *NWSD.

Nota: Si la interfaz está conectada a una NWID o una NWSD, se recomienda seleccionar una interfaz diferente.

- c. Por último, iniciar la interfaz. En una interfaz de línea de mandatos, entre el siguiente mandato: STRTCPIFC INTNETADR('a.b.c.d'). Sustituya a.b.c.d por la dirección IP de la interfaz.

Nota: Verifique que no se ha especificado STRTCPIFC INTNETADR(*AUTOSTART).

3. Verificar que la interfaz está activa.

Efectúe un PING con la interfaz de la aplicación. Existen muy pocos programas de utilidad relacionados con TCP/IP que funcionarán en estado restringido. No obstante, Ping y Netstat sí se pueden utilizar. Hallará más información acerca de la utilización de los mandatos ping y netstat en el apartado Herramientas para verificar la estructura de la red del tema de resolución de problemas TCP/IP.

Capítulo 7. Personalizar TCP/IP con el Navigator de iSeries

Una vez haya configurado TCP/IP, puede personalizar la configuración. A medida que la red vaya creciendo, quizás sea necesario modificar propiedades, añadir interfaces, o añadir rutas al servidor. Quizás deba configurar el servidor para IPv6 (protocolo de Internet versión 6) para utilizar aplicaciones IPv6. Utilice los asistentes del Navigator de iSeries para realizar muchas de estas tareas rápidamente.

Seleccione uno de los temas siguientes para personalizar la configuración utilizando el Navigator de iSeries. Estos temas proporcionan un punto de partida para gestionar su configuración TCP/IP con el Navigator de iSeries.

- Cambiar valores de TCP/IP
- Configurar IPv6
- Añadir interfaces IPv4
- Añadir interfaces IPv6
- Añadir rutas IPv4
- Añadir rutas IPv6

Cambiar valores de TCP/IP

Puede ver y modificar los valores de TCP/IP utilizando el Navigator de iSeries. Por ejemplo, puede cambiar las propiedades para los nombres de sistema principal o dominio, el servidor de nombres, las entradas de la tabla de sistemas principales, los atributos del sistema, las restricciones de puertos, los servidores o las conexiones de clientes. Puede modificar propiedades generales o propiedades específicas de IPv4 o IPv6, como los transportes.

Para acceder las páginas de propiedades de TCP/IP generales, siga estos pasos:

1. En el Navigator de iSeries, seleccione **servidor** —> **Red** .
2. Pulse el botón derecho del ratón en **Configuración TCP/IP** y seleccione **Propiedades** para abrir el diálogo **Propiedades de TCP/IP**.
3. Seleccione las pestañas situadas en la parte superior del diálogo para ver y editar la información de TCP/IP.

Para añadir y cambiar las entradas de la tabla de sistemas principales, siga estos pasos:

1. En el Navigator de iSeries, seleccione **servidor** —> **Red** .
2. Pulse el botón derecho en **Configuración TCP/IP** y seleccione **Tabla de sistemas principales** para abrir el diálogo de la **Tabla de sistemas principales**.
3. Utilice el diálogo de la **Tabla de sistemas principales** para añadir, editar o eliminar entradas de la tabla de sistemas principales.

Para acceder a páginas de propiedades específicas para IPv4, siga estos pasos:

1. En el Navigator de iSeries, seleccione **servidor** —> **Red** .
2. Pulse el botón derecho del ratón en **IPv4** y seleccione **Propiedades** para abrir el diálogo **Propiedades IPv4**.
3. Seleccione las pestañas situadas en la parte superior del diálogo para ver y editar las propiedades de IPv4.

Para acceder a las páginas con las propiedades específicas de IPv6, siga estos pasos:

1. En el Navigator de iSeries, seleccione **servidor** —> **Red** .
2. Pulse el botón derecho en **IPv6** y seleccione **Propiedades** para abrir el diálogo **Propiedades IPv6**.

3. Seleccione las pestañas situadas en la parte superior del diálogo para ver y editar las propiedades de IPv6.

Configurar IPv6

Si no está familiarizado con IPv6, consulte Protocolo de Internet versión 6 (IPv6) donde encontrará un resumen descriptivo.

Para configurar IPv6, debe cambiar la configuración del servidor utilizando el asistente de **Configuración de IPv6**. Antes de utilizar el asistente, consulte Configurar IPv6 donde encontrará las instrucciones y los requisitos especiales.

Añadir interfaces IPv4

Para crear una nueva interfaz IPv4, siga estos pasos:

1. En el Navigator de iSeries, seleccione **servidor** → **Red** → **Configuración TCP/IP** → **IPv4**.
2. Pulse el botón derecho en **Interfaces**, seleccione **Interfaz nueva**, y **Red de área local**, **Red de área amplia**, o **IP virtual** para crear el tipo apropiado de interfaz IPv4.
3. Siga las instrucciones del asistente para crear una nueva interfaz IPv4.

Añadir interfaces IPv6

Para crear una interfaz IPv6 nueva, siga estos pasos:

1. En el Navigator de iSeries, seleccione **servidor** → **Red** → **Configuración TCP/IP** → **IPv6**.
2. Pulse el botón derecho del ratón en **Interfaces** y seleccione **Interfaz nueva**.
3. Siga las instrucciones del asistente para crear una interfaz IPv6 nueva.

Añadir rutas IPv4

Todo cambio que efectúe en la información de direccionamiento surte efecto inmediatamente.

Para configurar una ruta IPv4 nueva, siga estos pasos:

1. En el Navigator de iSeries, seleccione **servidor** → **Red** → **Configuración TCP/IP** → **IPv4**.
2. Pulse el botón derecho en **Rutas**, y seleccione **Ruta nueva**.
3. Siga las instrucciones del asistente para configurar una ruta IPv4 nueva.

Añadir rutas IPv6

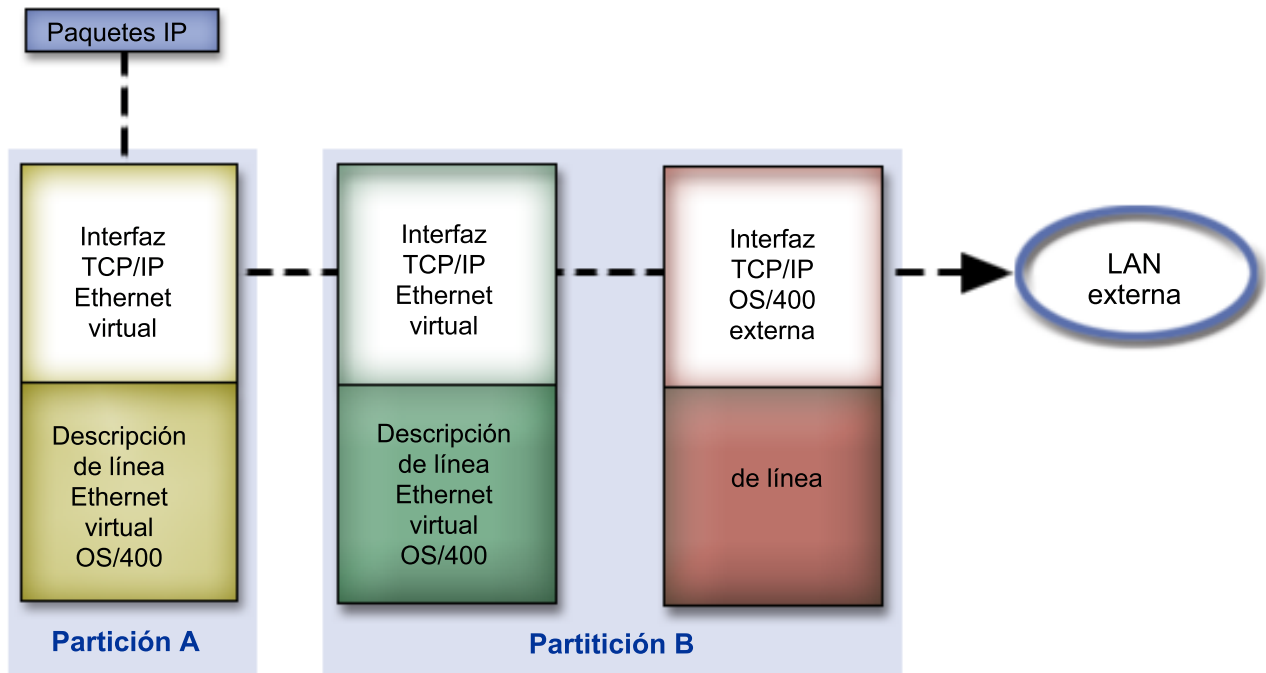
Todo cambio que efectúe en la información de direccionamiento surte efecto inmediatamente.

Para configurar una ruta IPv6 nueva, siga estos pasos:

1. En el Navigator de iSeries, seleccione **servidor** → **Red** → **Configuración TCP/IP** → **IPv6**.
2. Pulse el botón derecho en **Rutas**, y seleccione **Ruta nueva**.
3. Siga las instrucciones del asistente para configurar una ruta IPv6 nueva.

Capítulo 8. Técnicas TCP/IP para conectar Ethernet virtual a redes LAN externas

Si utiliza una red Ethernet virtual para las comunicaciones entre particiones, quizás deba permitir que estas particiones se comuniquen con una LAN física externa. Existen varias formas de conectar la red Ethernet virtual a una red LAN externa mediante distintas técnicas TCP/IP. Deberá habilitar que el tráfico TCP/IP fluya entre la red Ethernet virtual y la LAN externa. En la siguiente figura se muestra un flujo lógico de los paquetes IP.



El tráfico IP que se inicia en la Partición A va de su interfaz Ethernet virtual a la interfaz Ethernet virtual de la partición B. Mediante la implementación de alguna de las tres técnicas TCP/IP que se describen a continuación, puede permitir que los paquetes IP lleguen hasta la interfaz externa y vayan hacia sus destinos.

Existen tres métodos para conectar la Ethernet virtual y la LAN externa. Cada método tiene sus matices que los hacen más adecuados, en función de los conocimientos que se tengan de TCP/IP y del entorno. Elija uno de los siguientes métodos:

- **ARP por proxy**

Este método utiliza la creación de subredes transparentes para asociar la interfaz virtual de una partición a una interfaz externa. La función de ARP por proxy viene incorporada en la pila TCP/IP. Si tiene las direcciones IP necesarias, este enfoque es el más recomendado.

- **Conversión de direcciones de red**


Se puede utilizar el filtrado de paquetes de OS/400 para direccionar el tráfico entre una partición y la red externa.

- **Direccionamiento TCP/IP**

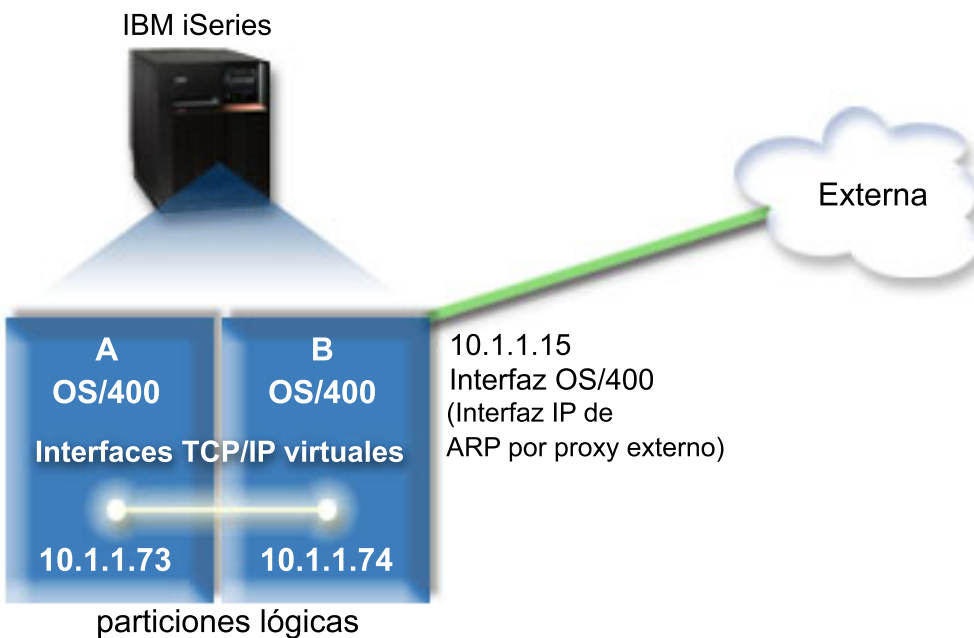
El direccionamiento TCP/IP estándar se utiliza para direccionar el tráfico a la red Ethernet virtual del mismo modo en que se define el direccionamiento en cualquier otra LAN. Para ello es necesario actualizar la información de direccionamiento en toda la red.

Método de ARP por proxy

El método de ARP por proxy utiliza una técnica conocida habitualmente como *creación de subredes transparentes*. Encontrará más información sobre las subredes transparentes en las siguientes fuentes de información:

- V4 TCP/IP for AS/400: More Cool Things Than Ever 
Este libro rojo proporciona ejemplos de casos prácticos que demuestran soluciones comunes con ejemplos de configuración. También le ayuda a planificar, instalar, adaptar, configurar y resolver problemas de TCP/IP en el servidor iSeries.
- Direccionamiento TCP/IP y equilibrado de carga de trabajo
En este tema se ofrecen técnicas e instrucciones para el direccionamiento y el equilibrado de carga de trabajo.

Si opta por utilizar el método de ARP por proxy, debe tener un profundo conocimiento de la creación de subredes y TCP/IP. Deberá obtener un bloque contiguo de direcciones IP que la red pueda direccionar. En este bloque de direcciones IP se crea una subred. En este ejemplo, se utiliza un bloque contiguo de cuatro direcciones IP (de la 10.1.1.72 a la 10.1.1.75). Ya que se trata de un bloque de cuatro direcciones IP, la máscara de subred de estas direcciones es 255.255.255.252. Se asigna una a cada interfaz TCP/IP virtual de las particiones, como se muestra en la siguiente figura.



En este ejemplo, el tráfico TCP/IP de la partición A circula por la Ethernet virtual hasta la interfaz 10.1.1.74 de la partición B. Dado que la dirección 10.1.1.74 está asociada a la dirección 10.1.1.15 de la interfaz de ARP por proxy externa, los paquetes salen de la Ethernet virtual a través de la interfaz de ARP por proxy.

Para configurar una Ethernet virtual de manera que utilice el método de conexión de ARP por proxy, realice las siguientes tareas de configuración.

1. Permitir que las particiones lógicas participen en una Ethernet virtual
2. Crear las descripciones de línea Ethernet
3. Activar el reenvío de datagramas
4. Crear la interfaz para habilitar ARP por proxy
5. Crear la interfaz TCP/IP virtual en la partición A
6. Crear la interfaz TCP/IP virtual en la partición B

- | 7. Crear la ruta
- | 8. Verificar las comunicaciones de red

| **Paso 1: permitir que las particiones lógicas participen en una Ethernet virtual**

| **Nota:** Si utiliza algún servidor distinto a los servidores modelo 270 y 8xx, deberá realizar este paso utilizando la Consola de gestión de hardware de eServer (HMC) en lugar de la partición primaria. Encontrará los detalles en el tema Ethernet virtual.

| Para habilitar Ethernet virtual, siga estos pasos:

- | 1. En la línea de mandatos de la partición primaria (partición A), escriba STRSST y pulse Intro.
- | 2. Escriba el ID de usuario y contraseña de las herramientas de servicio.
- | 3. En la pantalla Herramientas de servicio del sistema (SST), seleccione la opción 5 (Trabajar con particiones del sistema).
- | 4. En la pantalla Trabajar con particiones del sistema, seleccione la opción 3 (Trabajar con configuración de partición).
- | 5. Pulse F10 (Trabajar con Ethernet virtual).
- | 6. Escriba 1 en las correspondientes columnas de la partición A y la partición B para permitir que las particiones se comuniquen entre sí a través de Ethernet virtual.
- | 7. Salga de las herramientas de servicio del sistema (SST) para regresar a la línea de mandatos.

| **Qué hacer a continuación**

| Crear las descripciones de línea Ethernet

| **Paso 2: crear las descripciones de línea Ethernet**

| Puede llevar a cabo este paso de dos modos, en función del modelo de servidor que utilice. Elija uno de los siguientes métodos para crear las descripciones de línea, en función del modelo de servidor concreto que tenga.

- | • Crear las descripciones de línea Ethernet en servidores modelo 270 y 8xx
- | • Crear las descripciones de línea Ethernet en servidores distintos a los modelos 270 y 8xx

| **Crear las descripciones de línea Ethernet en servidores modelo 270 y 8xx**

| Para configurar las descripciones de línea Ethernet con el fin de dar soporte a Ethernet virtual, siga estos pasos:

- | 1. En la línea de mandatos de la partición A, escriba WRKHDWRSC *CMN y pulse Intro.
- | 2. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 7 (Visualizar detalles del recurso) junto al correspondiente puerto Ethernet virtual.
| El puerto Ethernet identificado como 268C es el recurso Ethernet virtual. Habrá uno por cada Ethernet virtual conectada a la partición lógica.
- | 3. En la pantalla Visualizar detalle del recurso, desplace la pantalla hasta encontrar la dirección del puerto. La dirección del puerto corresponde a la Ethernet virtual que ha seleccionado durante la configuración de la partición lógica.
- | 4. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 5 (Trabajar con descripciones de configuración) junto al correspondiente puerto Ethernet virtual y pulse Intro.
- | 5. En la pantalla Trabajar con descripciones de configuración, seleccione la opción 1 (Crear) y pulse Intro para ver la pantalla Crear descripción de línea Ethernet (CRTLINETH).
 - | a. En la solicitud *Descripción de línea*, escriba VETH0 . El nombre VETH0, aunque arbitrario, corresponde a la columna numerada de la página Ethernet virtual en la que ha habilitado la

comunicación entre particiones lógicas. Si utiliza los mismos nombres para las descripciones de línea y sus Ethernet virtuales asociadas, puede hacer un seguimiento fácilmente de las configuraciones Ethernet virtuales.

- b. En la solicitud *Velocidad de línea*, escriba 1G.
- c. En la solicitud *Dúplex*, escriba *FULL y pulse Intro.
- d. En la solicitud *Tamaño máximo de trama*, escriba 8996 y pulse Intro. Al cambiar el tamaño de trama a 8996, la transferencia de datos a través de la Ethernet virtual se ve mejorada.

Verá un mensaje indicando que la descripción de línea se ha creado.

6. Active la descripción de línea. Escriba WRKCFGSTS *LIN y seleccione la opción 1 (Activar) para VETH0.
7. Repita los pasos del 1 al 6, pero esta vez realice los pasos desde la línea de mandatos de la partición B para crear una descripción de línea Ethernet para la partición B.

Aunque los nombres de las descripciones de línea son arbitrarios, resulta útil utilizar los mismos nombres para todas las descripciones de línea asociadas a la Ethernet virtual. En este caso práctico, todas las descripciones de línea tienen el nombre VETH0.

Qué hacer a continuación

Activar el reenvío de datagramas

Crear las descripciones de línea Ethernet en servidores distintos a los modelos 270 y 8xx

Para configurar las descripciones de línea Ethernet con el fin de dar soporte a Ethernet virtual, siga estos pasos:

1. En la línea de mandatos de la partición A, escriba WRKHDWRSC *CMN y pulse Intro.
2. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 7 (Visualizar detalles del recurso) junto al correspondiente puerto Ethernet virtual.
Los puertos Ethernet identificados como 268C son los recursos de Ethernet virtual. Habrá uno por cada adaptador de Ethernet virtual. Cada puerto identificado como 268C tiene un código de ubicación asociado que se crea al crear el adaptador Ethernet virtual utilizando la HMC (Paso 1).
3. En la pantalla Visualizar detalle del recurso, desplace la pantalla hasta encontrar el recurso 268C asociado al código de ubicación específico creado para esta Ethernet virtual.
4. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 5 (Trabajar con descripciones de configuración) junto al correspondiente recurso Ethernet virtual y pulse Intro.
5. En la pantalla Trabajar con descripciones de configuración, seleccione la opción 1 (Crear) y pulse Intro para ver la pantalla Crear descripción de línea Ethernet (CRTLINETH).
 - a. En la solicitud *Descripción de línea*, escriba VETH0 . Si utiliza los mismos nombres para las descripciones de línea y sus Ethernet virtuales asociadas, como por ejemplo VETH0, puede hacer un seguimiento fácilmente de las configuraciones Ethernet virtuales.
 - b. En la solicitud *Velocidad de línea*, escriba 1G.
 - c. En la solicitud *Dúplex*, escriba *FULL y pulse Intro.
 - d. En la solicitud *Tamaño máximo de trama*, escriba 8996 y pulse Intro. Al cambiar el tamaño de trama a 8996, la transferencia de datos a través de la Ethernet virtual se ve mejorada.
Verá un mensaje indicando que la descripción de línea se ha creado.
6. Active la descripción de línea. Escriba WRKCFGSTS *LIN y seleccione la opción 1 (Activar) para VETH0.
7. Repita los pasos del 1 al 6, pero esta vez realice los pasos desde la línea de mandatos de la partición B para crear una descripción de línea Ethernet para la partición B.
Aunque los nombres de las descripciones de línea son arbitrarios, resulta útil utilizar los mismos nombres para todas las descripciones de línea asociadas a la Ethernet virtual. En este caso práctico, todas las descripciones de línea tienen el nombre VETH0.

| Qué hacer a continuación

| Activar el reenvío de datagramas

| Paso 3: activar el reenvío de datagramas IP

| Active el reenvío de datagramas IP para que los paquetes se puedan reenviar a diferentes subredes.

| Para activar el reenvío de datagramas IP, siga estos pasos:

- | 1. En la línea de mandatos de la partición A, escriba CHGTCPA y pulse F4.
- | 2. En la solicitud *Reenvío de datagramas IP*, escriba *YES.

| Qué hacer a continuación

| Crear la interfaz para habilitar ARP por proxy

| Paso 4: crear la interfaz para habilitar ARP por proxy

| Para crear la interfaz TCP/IP que permita habilitar ARP por proxy, realice estos pasos:

- | 1. Obtenga un bloque contiguo de direcciones IP que la red pueda direccionar.
| Dado que tiene dos particiones en esta Ethernet virtual, necesitará un bloque de cuatro direcciones. El cuarto segmento de la primera dirección IP del bloque debe ser divisible por cuatro. La primera y la última dirección IP de este bloque son las direcciones IP de subred y difusión, y no se pueden utilizar. La segunda y la tercera dirección IP se pueden utilizar para las interfaces TCP/IP de la Ethernet virtual en la partición A y en la partición B. Para este procedimiento, el bloque de direcciones IP es de la 10.1.1.72 a la 10.1.1.75, con una máscara de subred de 255.255.255.252.
| También necesitará una dirección IP para la dirección TCP/IP externa. Esta dirección IP no debe pertenecer al bloque de direcciones contiguas, pero debe estar dentro de la misma máscara de subred original de 255.255.255.0. En este procedimiento, la dirección IP externa es 10.1.1.15.
- | 2. Cree una interfaz TCP/IP OS/400 para la partición B. Esta interfaz es conocida como la interfaz IP externa de ARP por proxy. Para crear la interfaz, siga estos pasos:
 - | a. En la línea de mandatos de la partición B, escriba CFGTCP y pulse Intro para ver la pantalla Configurar TCP/IP.
 - | b. Seleccione la opción 1 (Trabajar con interfaces TCP/IP) y pulse Intro.
 - | c. Seleccione la opción (Añadir) y pulse Intro para ver la pantalla Añadir interfaz TCP/IP (ADDTCPIFC).
 - | d. En la solicitud *Dirección Internet*, escriba '10.1.1.15'.
 - | e. En la solicitud *Descripción de línea*, escriba el nombre de la descripción de línea, como por ejemplo ETHLINE.
 - | f. En la solicitud *Máscara de subred*, escriba '255.255.255.0'.
- | 3. Inicie la interfaz. En la pantalla Trabajar con interfaces TCP/IP, seleccione la opción 9 (Iniciar) para la interfaz.

| Qué hacer a continuación

| Crear la interfaz TCP/IP virtual en la partición A

| Paso 5: crear la interfaz TCP/IP virtual en la partición A

| Para crear la interfaz virtual, siga estos pasos:

- | 1. En la línea de mandatos de la partición A, escriba CFGTCP y pulse Intro para ver la pantalla Configurar TCP/IP.
- | 2. Seleccione la opción 1 (Trabajar con interfaces TCP/IP) y pulse Intro.

- | 3. Seleccione la opción (Añadir) y pulse Intro para ver la pantalla Añadir interfaz TCP/IP (ADDTCPIFC).
- | 4. En la solicitud *Dirección Internet*, escriba '10.1.1.73'.
- | 5. En la solicitud *Descripción de línea*, escriba el nombre de la descripción de línea, como por ejemplo ETHLINE.
- | 6. En la solicitud *Máscara de subred*, escriba '255.255.255.252'.
- | 7. Inicie la interfaz. En la pantalla Trabajar con interfaces TCP/IP, seleccione la opción 9 (Iniciar) para la interfaz.

| Qué hacer a continuación

- | Crear la interfaz TCP/IP virtual en la partición B

| Paso 6: crear la interfaz TCP/IP virtual en la partición B

| Para crear la interfaz virtual, siga estos pasos:

- | 1. En la línea de mandatos de la partición B, escriba CFGTCP y pulse Intro para ver la pantalla Configurar TCP/IP.
- | 2. Seleccione la opción 1 (Trabajar con interfaces TCP/IP) y pulse Intro.
- | 3. Seleccione la opción (Añadir) y pulse Intro para ver la pantalla Añadir interfaz TCP/IP (ADDTCPIFC).
- | 4. En la solicitud *Dirección Internet*, escriba '10.1.1.74'.
- | 5. En la solicitud *Descripción de línea*, escriba el nombre de la descripción de línea, como por ejemplo ETHLINE.
- | 6. En la solicitud *Máscara de subred*, escriba '255.255.255.252'.
- | 7. En la solicitud *Interfaz local asociada*, escriba '10.1.1.15'. De este modo se asocia la interfaz virtual a la interfaz externa y permite a ARP por proxy reenviar paquetes entre la interfaz virtual 10.1.1.74 y la interfaz externa 10.1.1.15.
- | 8. Inicie la interfaz. En la pantalla Trabajar con interfaces TCP/IP, seleccione la opción 9 (Iniciar) para la interfaz.

| Qué hacer a continuación

- | Crear la ruta

| Paso 7: crear la ruta

| Para crear la ruta por omisión que permita a los paquetes salir de la red Ethernet virtual, siga estos pasos:

- | 1. En la línea de mandatos de la partición A, escriba CFGTCP y pulse Intro.
- | 2. Seleccione la opción 2 (Trabajar con rutas de TCP/IP) y pulse Intro.
- | 3. Seleccione la opción 1 (Añadir) y pulse Intro.
- | 4. En la solicitud *Destino de la ruta*, escriba *DFTRROUTE.
- | 5. En la solicitud *Máscara de subred*, escriba *NONE.
- | 6. En la solicitud *Salto siguiente*, escriba '10.1.1.74'.
| Los paquetes de la partición A viajarán por la Ethernet virtual hasta la interfaz 10.1.1.74 utilizando esta ruta por omisión. Dado que la dirección 10.1.1.74 está asociada a la interfaz 10.1.1.15 de ARP por proxy externa, los paquetes salen de la Ethernet virtual a través de la interfaz de ARP por proxy.

| Qué hacer a continuación

- | Verificar las comunicaciones de red

Paso 8: verificar las comunicaciones de red

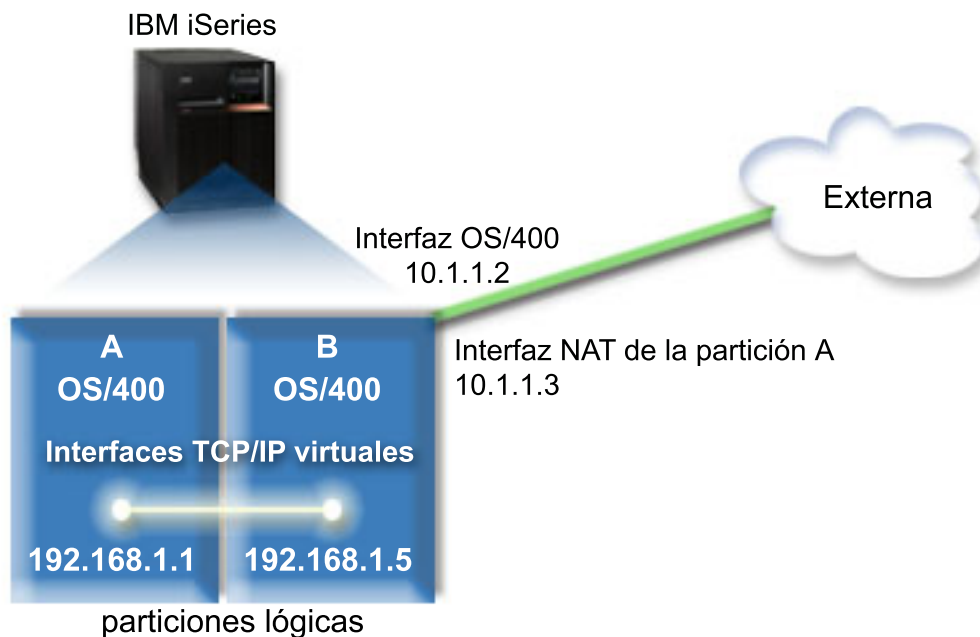
Verifique las comunicaciones de la red mediante el siguiente mandato ping:

- En la partición A, efectúe un ping a la interfaz Ethernet externa 10.1.1.74 y a un sistema principal externo.
- En un sistema principal OS/400 externo, efectúe un ping a las interfaces 10.1.1.73 y 10.1.1.74 de la Ethernet virtual.

Método de conversión de direcciones de red

La conversión de direcciones de red (NAT) puede direccionar el tráfico entre la red Ethernet virtual y la red externa. Esta forma particular de NAT se llama NAT estática y permitirá el tráfico IP entrante y saliente desde y hacia la red Ethernet virtual. Otras formas de NAT, como por ejemplo la NAT enmascarada, también serían adecuadas si la red Ethernet virtual no necesitara recibir tráfico iniciado por clientes externos. Al igual que los métodos de direccionamiento TCP/IP y ARP por proxy, puede aprovechar la conexión de red OS/400 existente. Dado que utilizará reglas de paquetes IP, deberá utilizar iSeries Navigator para crear y aplicar esas reglas.

En la siguiente figura se muestra un ejemplo de utilización de NAT para conectar la red Ethernet virtual a una red externa. La red 10.1.1.x representa una red externa, mientras que la red 192.168.1.x representa la red Ethernet virtual.



En este ejemplo, todo el tráfico TCP/IP existente para el servidor viaja por la interfaz 10.1.1.2. Dado que se trata de un caso práctico de correlación estática, el tráfico sufre la conversión de la interfaz 10.1.1.3 a la interfaz 192.168.1.5. El tráfico saliente sufre la conversión de la interfaz 192.168.1.5 a la interfaz 10.1.1.3 externa. La partición A y la partición A utilizan sus interfaces virtuales 192.168.1.1 y 192.168.1.5 respectivamente para comunicarse entre sí.

Para que la NAT estática pueda funcionar, primero debe configurar las comunicaciones TCP/IP y OS/400. A continuación, creará y aplicará algunas reglas de paquetes IP. Para configurar Ethernet virtual de manera que utilice el método NAT, realice las siguientes tareas de configuración:

1. Permitir que las particiones lógicas participen en una Ethernet virtual
2. Crear las descripciones de línea Ethernet
3. Activar el reenvío de datagramas
4. Crear las interfaces

- | 5. Verificar las comunicaciones de red
- | 6. Crear reglas de paquetes
- | 7. Verificar las comunicaciones de red

| **Paso 1: permitir que las particiones lógicas participen en una Ethernet virtual**

| **Nota:** Si utiliza algún servidor distinto a los servidores modelo 270 y 8xx, deberá realizar este paso utilizando la Consola de gestión de hardware de eServer (HMC) en lugar de la partición primaria. Encontrará los detalles en el tema Ethernet virtual.

| Para habilitar Ethernet virtual, siga estos pasos:

- | 1. En la línea de mandatos de la partición primaria (partición A), escriba STRSST y pulse Intro.
- | 2. Escriba el ID de usuario y contraseña de las herramientas de servicio.
- | 3. En la pantalla Herramientas de servicio del sistema (SST), seleccione la opción 5 (Trabajar con particiones del sistema).
- | 4. En la pantalla Trabajar con particiones del sistema, seleccione la opción 3 (Trabajar con configuración de partición).
- | 5. Pulse F10 (Trabajar con Ethernet virtual).
- | 6. Escriba 1 en las correspondientes columnas de la partición A y la partición B para permitir que las particiones se comuniquen entre sí a través de Ethernet virtual.
- | 7. Salga de las herramientas de servicio del sistema (SST) para regresar a la línea de mandatos.

| **Qué hacer a continuación**

| Crear las descripciones de línea Ethernet

| **Paso 2: crear las descripciones de línea Ethernet**

| Puede llevar a cabo este paso de dos modos, en función del modelo de servidor que utilice. Elija uno de los siguientes métodos para crear las descripciones de línea, en función del modelo de servidor concreto que tenga.

- | • Crear las descripciones de línea Ethernet en servidores modelo 270 y 8xx
- | • Crear las descripciones de línea Ethernet en servidores distintos a los modelos 270 y 8xx

| **Crear las descripciones de línea Ethernet en servidores modelo 270 y 8xx**

| Para configurar las descripciones de línea Ethernet con el fin de dar soporte a Ethernet virtual, siga estos pasos:

- | 1. En la línea de mandatos de la partición A, escriba WRKHDWRSC *CMN y pulse Intro.
- | 2. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 7 (Visualizar detalles del recurso) junto al correspondiente puerto Ethernet virtual.
El puerto Ethernet identificado como 268C es el recurso Ethernet virtual. Habrá uno por cada Ethernet virtual conectada a la partición lógica.
- | 3. En la pantalla Visualizar detalle del recurso, desplace la pantalla hasta encontrar la dirección del puerto. La dirección del puerto corresponde a la Ethernet virtual que ha seleccionado durante la configuración de la partición lógica.
- | 4. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 5 (Trabajar con descripciones de configuración) junto al correspondiente puerto Ethernet virtual y pulse Intro.
- | 5. En la pantalla Trabajar con descripciones de configuración, seleccione la opción 1 (Crear) y pulse Intro para ver la pantalla Crear descripción de línea Ethernet (CRTLINETH).

- a. En la solicitud *Descripción de línea*, escriba VETH0 . El nombre VETH0, aunque arbitrario, corresponde a la columna numerada de la página Ethernet virtual en la que ha habilitado la comunicación entre particiones lógicas. Si utiliza los mismos nombres para las descripciones de línea y sus Ethernet virtuales asociadas, puede hacer un seguimiento fácilmente de las configuraciones Ethernet virtuales.
 - b. En la solicitud *Velocidad de línea*, escriba 1G.
 - c. En la solicitud *Dúplex*, escriba *FULL y pulse Intro.
 - d. En la solicitud *Tamaño máximo de trama*, escriba 8996 y pulse Intro. Al cambiar el tamaño de trama a 8996, la transferencia de datos a través de la Ethernet virtual se ve mejorada.
Verá un mensaje indicando que la descripción de línea se ha creado.
6. Active la descripción de línea. Escriba WRKCFGSTS *LIN y seleccione la opción 1 (Activar) para VETH0.
 7. Repita los pasos del 1 al 6, pero esta vez realice los pasos desde la línea de mandatos de la partición B para crear una descripción de línea Ethernet para la partición B.
Aunque los nombres de las descripciones de línea son arbitrarios, resulta útil utilizar los mismos nombres para todas las descripciones de línea asociadas a la Ethernet virtual. En este caso práctico, todas las descripciones de línea tienen el nombre VETH0.

Qué hacer a continuación

Activar el reenvío de datagramas

Crear las descripciones de línea Ethernet en servidores distintos a los modelos 270 y 8xx

Para configurar las descripciones de línea Ethernet con el fin de dar soporte a Ethernet virtual, siga estos pasos:

1. En la línea de mandatos de la partición A, escriba WRKHDWRSC *CMN y pulse Intro.
2. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 7 (Visualizar detalles del recurso) junto al correspondiente puerto Ethernet virtual.
Los puertos Ethernet identificados como 268C son los recursos de Ethernet virtual. Habrá uno por cada adaptador de Ethernet virtual. Cada puerto identificado como 268C tiene un código de ubicación asociado que se crea al crear el adaptador Ethernet virtual utilizando la HMC (Paso 1).
3. En la pantalla Visualizar detalle del recurso, desplace la pantalla hasta encontrar el recurso 268C asociado al código de ubicación específico creado para esta Ethernet virtual.
4. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 5 (Trabajar con descripciones de configuración) junto al correspondiente recurso Ethernet virtual y pulse Intro.
5. En la pantalla Trabajar con descripciones de configuración, seleccione la opción 1 (Crear) y pulse Intro para ver la pantalla Crear descripción de línea Ethernet (CRTLINETH).
 - a. En la solicitud *Descripción de línea*, escriba VETH0 . Si utiliza los mismos nombres para las descripciones de línea y sus Ethernet virtuales asociadas, como por ejemplo VETH0, puede hacer un seguimiento fácilmente de las configuraciones Ethernet virtuales.
 - b. En la solicitud *Velocidad de línea*, escriba 1G.
 - c. En la solicitud *Dúplex*, escriba *FULL y pulse Intro.
 - d. En la solicitud *Tamaño máximo de trama*, escriba 8996 y pulse Intro. Al cambiar el tamaño de trama a 8996, la transferencia de datos a través de la Ethernet virtual se ve mejorada.
Verá un mensaje indicando que la descripción de línea se ha creado.
6. Active la descripción de línea. Escriba WRKCFGSTS *LIN y seleccione la opción 1 (Activar) para VETH0.
7. Repita los pasos del 1 al 6, pero esta vez realice los pasos desde la línea de mandatos de la partición B para crear una descripción de línea Ethernet para la partición B.
Aunque los nombres de las descripciones de línea son arbitrarios, resulta útil utilizar los mismos nombres para todas las descripciones de línea asociadas a la Ethernet virtual. En este caso práctico, todas las descripciones de línea tienen el nombre VETH0.

| Qué hacer a continuación

| Activar el reenvío de datagramas

| Paso 3: activar el reenvío de datagramas IP

| Active el reenvío de datagramas IP para que los paquetes se puedan reenviar a diferentes subredes.

| Para activar el reenvío de datagramas IP, siga estos pasos:

- | 1. En la línea de mandatos de la partición A, escriba CHGTCPA y pulse F4.
- | 2. En la solicitud *Reenvío de datagramas IP*, escriba *YES.

| Qué hacer a continuación

| Crear las interfaces

| Paso 4: crear las interfaces

| Para crear las interfaces TCP/IP, siga estos pasos:

- | 1. Cree e inicie una interfaz TCP/IP OS/400 en la partición B para las comunicaciones generales con el servidor. Para crear la interfaz, siga estos pasos:
 - | a. En la línea de mandatos de la partición B, escriba CFGTCP y pulse Intro para ver la pantalla Configurar TCP/IP.
 - | b. Seleccione la opción 1 (Trabajar con interfaces TCP/IP) y pulse Intro.
 - | c. Seleccione la opción (Añadir) y pulse Intro para ver la pantalla Añadir interfaz TCP/IP (ADDTCPIFC).
 - | d. En la solicitud *Dirección Internet*, escriba '10.1.1.2'.
 - | e. En la solicitud *Descripción de línea*, escriba ETHLINE .
 - | f. En la solicitud *Máscara de subred*, escriba '255.255.255.0'.
 - | g. Inicie la interfaz. En la pantalla Trabajar con interfaces TCP/IP, seleccione la opción 9 (Iniciar) para la interfaz.
- | 2. Cree e inicie otra interfaz TCP/IP conectada a la red externa. Debe utilizar la misma descripción de línea que la interfaz TCP/IP externa existente. Esta interfaz realizará la conversión de direcciones de la partición. Para crear la interfaz, siga estos pasos:
 - | a. En la línea de mandatos de la partición B, escriba CFGTCP y pulse Intro para ver la pantalla Configurar TCP/IP.
 - | b. Seleccione la opción 1 (Trabajar con interfaces TCP/IP) y pulse Intro.
 - | c. Seleccione la opción (Añadir) y pulse Intro para ver la pantalla Añadir interfaz TCP/IP (ADDTCPIFC).
 - | d. En la solicitud *Dirección Internet*, escriba '10.1.1.3'.
 - | e. En la solicitud *Descripción de línea*, escriba ETHLINE .
 - | f. En la solicitud *Máscara de subred*, escriba '255.255.255.0'.
 - | g. Inicie la interfaz. En la pantalla Trabajar con interfaces TCP/IP, seleccione la opción 9 (Iniciar) para la interfaz.
- | 3. Cree e inicie la interfaz TCP/IP OS/400 en la partición A para Ethernet virtual. Para crear la interfaz, siga estos pasos:
 - | a. En la línea de mandatos de la partición A, escriba CFGTCP y pulse Intro para ver la pantalla Configurar TCP/IP.
 - | b. Seleccione la opción 1 (Trabajar con interfaces TCP/IP) y pulse Intro.
 - | c. Seleccione la opción (Añadir) y pulse Intro para ver la pantalla Añadir interfaz TCP/IP (ADDTCPIFC).

- d. En la solicitud *Dirección Internet*, escriba '192.168.1.1'.
 - e. En la solicitud *Descripción de línea*, escriba VETH0 .
 - f. En la solicitud *Máscara de subred*, escriba '255.255.255.0'.
 - g. Inicie la interfaz. En la pantalla Trabajar con interfaces TCP/IP, seleccione la opción 9 (Iniciar) para la interfaz.
4. Cree e inicie la interfaz TCP/IP OS/400 en la partición B para Ethernet virtual. Para crear la interfaz, siga estos pasos:
- a. En la línea de mandatos de la partición B, escriba CFGTCP y pulse Intro para ver la pantalla Configurar TCP/IP.
 - b. Seleccione la opción 1 (Trabajar con interfaces TCP/IP) y pulse Intro.
 - c. Seleccione la opción (Añadir) y pulse Intro para ver la pantalla Añadir interfaz TCP/IP (ADDTCPIFC).
 - d. En la solicitud *Dirección Internet*, escriba '192.168.1.5'.
 - e. En la solicitud *Descripción de línea*, escriba VETH0 .
 - f. En la solicitud *Máscara de subred*, escriba '255.255.255.0'.
 - g. Inicie la interfaz. En la pantalla Trabajar con interfaces TCP/IP, seleccione la opción 9 (Iniciar) para la interfaz.

Qué hacer a continuación

Verificar las comunicaciones de red

Paso 5: verificar las comunicaciones de red

Verifique las comunicaciones de la red mediante el siguiente mandato ping:

- En la partición A, efectúe un ping a la interfaz Ethernet externa 192.168.1.5 y a un sistema principal externo.
- En un sistema principal OS/400 externo, efectúe un ping a cada una de las interfaces Ethernet virtuales 192.168.1.1 y 192.168.1.5.

Qué hacer a continuación

Crear reglas de paquetes

Paso 6: crear reglas de paquetes

Utilice el asistente Conversión de direcciones de iSeries Navigator para crear las reglas de paquetes que correlacionan la dirección privada de la partición A con la dirección pública de la partición B.

Para crear las reglas de paquetes, siga estos pasos:

1. En iSeries Navigator, expanda el servidor **iSeries** -> **Red**-> **Políticas IP**.
2. Pulse con el botón derecho del ratón en **Reglas de paquete** y seleccione **Editor de reglas**.
3. Seleccione **Conversión de direcciones** en el menú **Asistente**.
4. Siga las instrucciones del asistente para crear las reglas de paquetes. Este procedimiento utiliza las siguientes selecciones:
 - Seleccione **Correlacionar conversión de direcciones**
 - Especifique la dirección IP privada 192.168.1.1
 - Especifique la dirección IP pública 10.1.1.3
 - Seleccione la línea en la que se ha configurado las interfaces, por ejemplo ETHLINE
5. Seleccione **Activar reglas** en el menú **Archivo**.

| Qué hacer a continuación

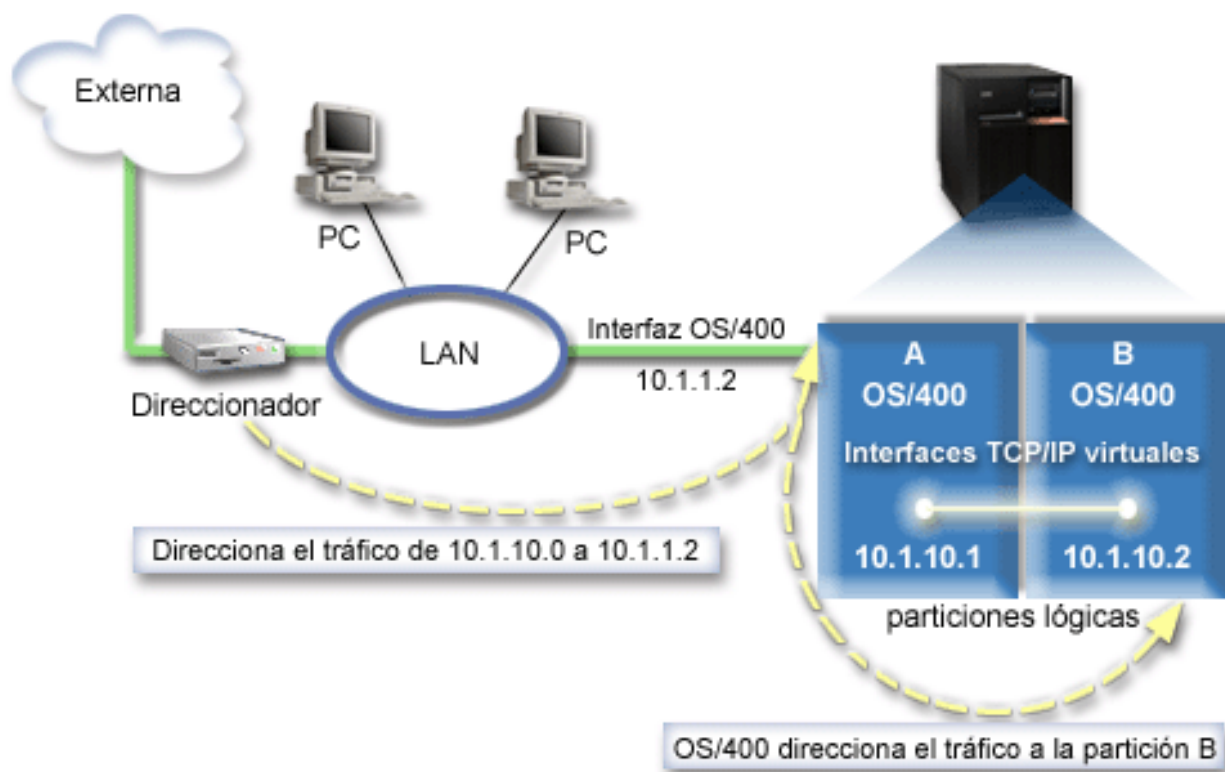
| Verificar las comunicaciones de red

| Paso 7: verificar las comunicaciones de red

| Una vez haya creado las reglas de paquetes, deberá verificar las comunicaciones de red. Para probar las comunicaciones salientes, efectúe un ping a un sistema principal externo desde la partición A. A continuación, desde dicho sistema principal externo, efectúe un ping a la partición A para probar las comunicaciones entrantes.

| Método de direccionamiento TCP/IP

| También puede direccionar el tráfico a las particiones a través del servidor iSeries con varias técnicas de direccionamiento. Esta solución no es difícil de configurar en el servidor, pero, en función de la topología de la red, su implementación puede no ser muy práctica. Considere la siguiente figura.



| La interfaz TCP/IP existente (10.1.1.2) se conecta a la LAN. La LAN se conecta a las redes remotas con un direccionador. La interfaz TCP/IP virtual de la partición B tiene la dirección 10.1.10.2 y la interfaz TCP/IP virtual de la partición A tiene la dirección 10.1.10.1. En OS/400, si activa el reenvío de datagramas IP, OS/400 direccionará los paquetes IP hacia y desde la partición B. Al definir la conexión TCP/IP de la partición B, la dirección del direccionador debe ser 10.1.10.1.

| La dificultad de este tipo de direccionamiento reside en lograr que los paquetes IP lleguen al iSeries. En este caso práctico, podría definir una ruta en el direccionador de manera que pase los paquetes cuyo destino es la red 10.1.10.0 a la interfaz 10.1.1.2. Esto sirve para los clientes de redes remotas. También sirve para los clientes LAN locales (clientes conectados a la misma LAN que el iSeries) si reconocen el mismo direccionador como su salto siguiente. En caso contrario, cada cliente debe tener una ruta que dirija el tráfico de 10.1.10.0 a la interfaz 10.1.1.2 de OS/400; aquí empieza la impracticabilidad de este método. Si se tienen muchos clientes LAN, es necesario definir muchas rutas.

| Para configurar Ethernet virtual de manera que utilice el método de direccionamiento TCP/IP, utilice las siguientes instrucciones:

- | 1. Permitir que las particiones lógicas participen en una Ethernet virtual
- | 2. Crear las descripciones de línea Ethernet
- | 3. Activar el reenvío de datagramas
- | 4. Crear las interfaces

| **Paso 1: permitir que las particiones lógicas participen en una Ethernet virtual**

| **Nota:** Si utiliza algún servidor distinto a los servidores modelo 270 y 8xx, deberá realizar este paso utilizando la Consola de gestión de hardware de eServer (HMC) en lugar de la partición primaria. Encontrará los detalles en el tema Ethernet virtual.

| Para habilitar Ethernet virtual, siga estos pasos:

- | 1. En la línea de mandatos de la partición primaria (partición A), escriba STRSST y pulse Intro.
- | 2. Escriba el ID de usuario y contraseña de las herramientas de servicio.
- | 3. En la pantalla Herramientas de servicio del sistema (SST), seleccione la opción 5 (Trabajar con particiones del sistema).
- | 4. En la pantalla Trabajar con particiones del sistema, seleccione la opción 3 (Trabajar con configuración de partición).
- | 5. Pulse F10 (Trabajar con Ethernet virtual).
- | 6. Escriba 1 en las correspondientes columnas de la partición A y la partición B para permitir que las particiones se comuniquen entre sí a través de Ethernet virtual.
- | 7. Salga de las herramientas de servicio del sistema (SST) para regresar a la línea de mandatos.

| **Qué hacer a continuación**

| Crear las descripciones de línea Ethernet

| **Paso 2: crear las descripciones de línea Ethernet**

| Puede llevar a cabo este paso de dos modos, en función del modelo de servidor que utilice. Elija uno de los siguientes métodos para crear las descripciones de línea, en función del modelo de servidor concreto que tenga.

- | • Crear las descripciones de línea Ethernet en servidores modelo 270 y 8xx
- | • Crear las descripciones de línea Ethernet en servidores distintos a los modelos 270 y 8xx

| **Crear las descripciones de línea Ethernet en servidores modelo 270 y 8xx**

| Para configurar las descripciones de línea Ethernet con el fin de dar soporte a Ethernet virtual, siga estos pasos:

- | 1. En la línea de mandatos de la partición A, escriba WRKHDWRSC *CMN y pulse Intro.
- | 2. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 7 (Visualizar detalles del recurso) junto al correspondiente puerto Ethernet virtual.
| El puerto Ethernet identificado como 268C es el recurso Ethernet virtual. Habrá uno por cada Ethernet virtual conectada a la partición lógica.
- | 3. En la pantalla Visualizar detalle del recurso, desplace la pantalla hasta encontrar la dirección del puerto. La dirección del puerto corresponde a la Ethernet virtual que ha seleccionado durante la configuración de la partición lógica.
- | 4. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 5 (Trabajar con descripciones de configuración) junto al correspondiente puerto Ethernet virtual y pulse Intro.

5. En la pantalla Trabajar con descripciones de configuración, seleccione la opción 1 (Crear) y pulse Intro para ver la pantalla Crear descripción de línea Ethernet (CRTLINETH).
 - a. En la solicitud *Descripción de línea*, escriba VETH0 . El nombre VETH0, aunque arbitrario, corresponde a la columna numerada de la página Ethernet virtual en la que ha habilitado la comunicación entre particiones lógicas. Si utiliza los mismos nombres para las descripciones de línea y sus Ethernet virtuales asociadas, puede hacer un seguimiento fácilmente de las configuraciones Ethernet virtuales.
 - b. En la solicitud *Velocidad de línea*, escriba 1G.
 - c. En la solicitud *Dúplex*, escriba *FULL y pulse Intro.
 - d. En la solicitud *Tamaño máximo de trama*, escriba 8996 y pulse Intro. Al cambiar el tamaño de trama a 8996, la transferencia de datos a través de la Ethernet virtual se ve mejorada.
Verá un mensaje indicando que la descripción de línea se ha creado.
6. Active la descripción de línea. Escriba WRKCFGSTS *LIN y seleccione la opción 1 (Activar) para VETH0.
7. Repita los pasos del 1 al 6, pero esta vez realice los pasos desde la línea de mandatos de la partición B para crear una descripción de línea Ethernet para la partición B.
Aunque los nombres de las descripciones de línea son arbitrarios, resulta útil utilizar los mismos nombres para todas las descripciones de línea asociadas a la Ethernet virtual. En este caso práctico, todas las descripciones de línea tienen el nombre VETH0.

Qué hacer a continuación

Activar el reenvío de datagramas

Crear las descripciones de línea Ethernet en servidores distintos a los modelos 270 y 8xx

Para configurar las descripciones de línea Ethernet con el fin de dar soporte a Ethernet virtual, siga estos pasos:

1. En la línea de mandatos de la partición A, escriba WRKHDWRSC *CMN y pulse Intro.
2. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 7 (Visualizar detalles del recurso) junto al correspondiente puerto Ethernet virtual.
Los puertos Ethernet identificados como 268C son los recursos de Ethernet virtual. Habrá uno por cada adaptador de Ethernet virtual. Cada puerto identificado como 268C tiene un código de ubicación asociado que se crea al crear el adaptador Ethernet virtual utilizando la HMC (Paso 1).
3. En la pantalla Visualizar detalle del recurso, desplace la pantalla hasta encontrar el recurso 268C asociado al código de ubicación específico creado para esta Ethernet virtual.
4. En la pantalla Trabajar con recursos de comunicaciones, seleccione la opción 5 (Trabajar con descripciones de configuración) junto al correspondiente recurso Ethernet virtual y pulse Intro.
5. En la pantalla Trabajar con descripciones de configuración, seleccione la opción 1 (Crear) y pulse Intro para ver la pantalla Crear descripción de línea Ethernet (CRTLINETH).
 - a. En la solicitud *Descripción de línea*, escriba VETH0 . Si utiliza los mismos nombres para las descripciones de línea y sus Ethernet virtuales asociadas, como por ejemplo VETH0, puede hacer un seguimiento fácilmente de las configuraciones Ethernet virtuales.
 - b. En la solicitud *Velocidad de línea*, escriba 1G.
 - c. En la solicitud *Dúplex*, escriba *FULL y pulse Intro.
 - d. En la solicitud *Tamaño máximo de trama*, escriba 8996 y pulse Intro. Al cambiar el tamaño de trama a 8996, la transferencia de datos a través de la Ethernet virtual se ve mejorada.
Verá un mensaje indicando que la descripción de línea se ha creado.
6. Active la descripción de línea. Escriba WRKCFGSTS *LIN y seleccione la opción 1 (Activar) para VETH0.
7. Repita los pasos del 1 al 6, pero esta vez realice los pasos desde la línea de mandatos de la partición B para crear una descripción de línea Ethernet para la partición B.

Aunque los nombres de las descripciones de línea son arbitrarios, resulta útil utilizar los mismos nombres para todas las descripciones de línea asociadas a la Ethernet virtual. En este caso práctico, todas las descripciones de línea tienen el nombre VETH0.

Qué hacer a continuación

Activar el reenvío de datagramas

Paso 3: activar el reenvío de datagramas IP

Active el reenvío de datagramas IP para que los paquetes se puedan reenviar a diferentes subredes.

Para activar el reenvío de datagramas IP, siga estos pasos:

1. En la línea de mandatos de la partición A, escriba CHGTCPA y pulse F4.
2. En la solicitud *Reenvío de datagramas IP*, escriba *YES.

Qué hacer a continuación

Crear las interfaces

Paso 4: crear las interfaces

Para crear las interfaces TCP/IP, siga estos pasos:

1. Cree una interfaz TCP/IP OS/400 en la partición A. Para crear la interfaz, siga estos pasos:
 - a. En la línea de mandatos de la partición A, escriba CFGTCP y pulse Intro para ver la pantalla Configurar TCP/IP.
 - b. Seleccione la opción 1 (Trabajar con interfaces TCP/IP) y pulse Intro.
 - c. Seleccione la opción (Añadir) y pulse Intro para ver la pantalla Añadir interfaz TCP/IP (ADDTCPIFC).
 - d. En la solicitud *Dirección Internet*, escriba '10.1.1.2'.
 - e. En la solicitud *Descripción de línea*, escriba el nombre de la descripción de línea, como por ejemplo ETHLINE.
 - f. En la solicitud *Máscara de subred*, escriba '255.255.255.0'.
2. Inicie la interfaz. En la pantalla Trabajar con interfaces TCP/IP, seleccione la opción 9 (Iniciar) para la interfaz.
3. Repita los pasos 2 y 3 para crear e iniciar las interfaces TCP/IP de las particiones A y B.
Estas interfaces se utilizan para la Ethernet virtual. Utilice las direcciones IP 10.1.10.1 y 10.1.10.2 para esas interfaces, y la máscara de subred 255.255.255.0.

Consideraciones sobre Ethernet virtual

Puede utilizar Ethernet virtual como una alternativa al uso de una tarjeta de red en las comunicaciones entre particiones. Permite establecer una comunicación de alta velocidad entre particiones lógicas sin tener que adquirir hardware adicional. Para cada uno de los 16 puertos habilitados, el sistema crea un puerto de comunicaciones Ethernet virtual, como por ejemplo CMNxx, en un tipo de recurso de 268C. Las particiones lógicas asignadas a la misma red de área local (LAN) pasan a estar disponibles para la comunicación a través de dicho enlace. Un sistema físico permite configurar un máximo de 16 redes de área local virtuales distintas. Ethernet virtual proporciona la misma funcionalidad que el uso de un adaptador Ethernet de 1 Gb. Ethernet virtual no soporta redes de área local Token Ring o Ethernet 10 Mbps y 100 Mbps.

Ethernet virtual es una solución de red económica que proporciona importantes ventajas:



- Económico: potencialmente no se necesita hardware de red adicional. Se pueden añadir particiones al servidor y comunicarse con una LAN externa sin tener que instalar tarjetas LAN físicas adicionales. Si

- | el servidor actual tiene una disponibilidad limitada de ranuras de tarjetas en las que instalar tarjetas LAN adicionales, el uso de Ethernet virtual ofrece la posibilidad de operar particiones conectadas a la LAN sin la necesidad de actualizar el servidor.
- | • Flexible: es posible configurar un máximo de 16 conexiones distintas, lo que permite la configuración de rutas de comunicación selectivas entre las particiones. Si se desea una mayor flexibilidad, el modelo de configuración permite que las particiones lógicas implementen una conexión Ethernet tanto virtual como física. Es una característica muy atractiva en aquellos casos en que se utiliza la partición Linux para hospedar una aplicación de cortafuegos.
 - | • Rápido: Ethernet virtual emula una conexión Ethernet de 1 GB y proporciona un método de comunicación rápido y cómodo entre las particiones. Esto aumenta la oportunidad de integrar aplicaciones separadas que se ejecutan en particiones lógicas distintas.
 - | • Versátil: independientemente de si las particiones ejecutan OS/400 o Linux, pueden conectarse a la misma Ethernet virtual.
 - | • Menor congestión: al utilizar Ethernet virtual para las comunicaciones entre particiones, el tráfico se reduce en la LAN externa. En el caso de Ethernet, que es un estándar basado en la detección de colisiones, esto ciertamente ayudará a evitar la degradación del servicio a los demás usuarios de la LAN.
- | <<



Capítulo 9. Información relacionada para la configuración de TCP/IP

Ahora que el servidor ya está en marcha, quizá se pregunte qué más puede hacer con su servidor. A continuación encontrará un listado con los manuales e IBM Redbooks (en formato PDF) y el tema del Information Center referente al tema de configuración de TCP/IP. Puede visualizar o imprimir los PDF. Utilice las referencias siguientes para sacar el máximo provecho de TCP/IP en el servidor iSeries:




Manuales

- **TCP/IP Configuration and Reference**  (592 KB)
Este libro proporciona información sobre la configuración del Protocolo de control de la transmisión/Protocolo de Internet (TCP/IP) y sobre el funcionamiento y la administración de la red.
- **Consejos y herramientas para proteger el iSeries**  (1 MB)
Este libro proporciona recomendaciones básicas para utilizar las opciones de seguridad del iSeries para proteger el servidor y sus operaciones asociadas.

Redbooks

- **TCP/IP Tutorial and Technical Overview**  (7 MB)
Este redbook proporciona información sobre los conceptos básicos de TCP/IP.
- **TCP/IP for AS/400: More Cool Things Than Ever**  (9 MB)
Este redbook incluye una amplia lista de servicios y aplicaciones de TCP/IP habituales.

IPv6


- **The Internet Engineering Task Force (IETF)**(<http://www.ietf.cnri.reston.va.us/>) 
Información sobre el grupo de personas que desarrollan el protocolo de Internet, inclusive IPv6.
- **IP Version 6 (IPv6)** (<http://playground.sun.com/pub/ipng/html/ipng-main.html>) 
Contiene especificaciones actuales de IPv6 y referencias a varias fuentes sobre IPv6.
- **IPv6 Forum**(<http://www.ipv6forum.com/>) 
Incluye artículos y eventos nuevos relacionados con los últimos desarrollos de IPv6.

Más información

- **TCP/IP**
Este tema contiene información acerca de aplicaciones y servicios TCP/IP que van más allá del ámbito de la configuración.

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

1. Pulse el botón derecho sobre el PDF en su navegador (pulse el botón derecho del ratón sobre el enlace anterior).
2. Pulse **Guardar destino como...**
3. Diríjase al directorio donde desea guardar el archivo PDF.
4. Pulse **Guardar**.

Si necesita Adobe Acrobat Reader para ver o imprimir estos archivos PDF, puede bajar una copia del sitio Web de Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Parte 2. Apéndices

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 pretenden 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, Japón

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 licenciarios de este programa que deseen obtener información acerca del mismo con el fin de: (i) intercambiar la información entre programas creados independientemente y otros programas (incluyendo éste) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

- | IBM Corporation
- | Software Interoperability Coordinator, Department 49XA
- | 3605 Highway 52 N
- | Rochester, MN 55901
- | Estados Unidos

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

- | El programa bajo licencia descrito en esta información y todo el material bajo licencia a su disposición los proporciona IBM bajo los términos de los acuerdos IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code o de cualquier acuerdo equivalente entre nosotros.

Los datos de rendimiento incluidos aquí se determinaron en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Puede que se hayan tomado algunas medidas en los sistemas a nivel de desarrollo y no existe ninguna garantía de que estas medidas serán las mismas en sistemas disponibles generalmente. Además, puede que se haya estimado alguna medida mediante la 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 suministradores de esos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha comprobado los productos y no puede afirmar la exactitud en cuanto a rendimiento, compatibilidad u otras características relativas a productos no IBM. Las consultas acerca de las posibilidades de productos no IBM deben dirigirse a los suministradores de los mismos.

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

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

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

Marcas registradas

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

AS/400
e(logo)server
eServer
IBM
iSeries
OS/400
Redbooks

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los 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 para descargar e imprimir publicaciones

- | Los permisos para la utilización de la información cuya descarga ha seleccionado, se otorgan en base a los siguientes términos y condiciones, y la indicación por la presente de su aceptación.
- | **Uso personal:** puede reproducir esta información para su uso personal y no comercial, siempre que se conserven todos los avisos de propiedad. No puede distribuir, visualizar o realizar trabajos derivados de esta información, o parte de ella, sin el consentimiento explícito de IBM.
- | **Uso comercial:** puede reproducir, distribuir y visualizar esta información únicamente en su empresa, siempre que se conserven todos los avisos de propiedad. No puede realizar trabajos derivados de esta información, ni reproducir, distribuir o visualizar esta información o parte de ella fuera de su empresa, sin el consentimiento explícito de IBM.
- | Excepto los permisos explícitamente otorgados por la presente, no se otorga ningún permiso, licencia o derecho, implícita o explícitamente, sobre la información o los datos, software o demás propiedad intelectual aquí contenida.
- | IBM se reserva el derecho de retirar los permisos aquí otorgados siempre que, a su discreción, el uso de la información se realice en detrimento de sus intereses o, a decisión de IBM, no se cumplan correctamente las instrucciones anteriores.
- | No puede descargar, exportar o reexportar esta información si no es en total conformidad con todas las legislaciones y regulaciones aplicables, incluyendo todas las legislaciones y regulaciones de exportación de Estados Unidos. IBM NO EFECTÚA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTA INFORMACIÓN. LA INFORMACIÓN SE PROPORCIONA "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUYENDO, PERO NO LIMITÁNDOSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO INFRACCIÓN Y ADECUACIÓN A UN PROPÓSITO DETERMINADO.

Todos los materiales son copyright de IBM Corporation.

- | Al descargar o imprimir información desde este sitio, indica su aceptación de estos términos y condiciones.



Impreso en España