Uso de redes virtuales en Oracle® Solaris 11.1

Referencia: E36563–01
Octubre de 2012

ORACLE

130327@25097

Contenido

Prefacio

Bienvenido a *Uso de redes virtuales en Oracle Solaris 11.1*. Este manual forma parte de la serie *Establecimiento de una red Oracle Solaris 11.1* que abarca procedimientos y temas básicos para configurar redes Oracle Solaris. En esta guía, se asume que ya se ha instalado Oracle Solaris.

Quién debe utilizar este manual

Este manual está destinado a las personas encargadas de administrar sistemas que ejecutan Oracle Solaris y que están configurados en una red. Para utilizar esta guía, se debe tener, como mínimo, dos años de experiencia en la administración de sistemas UNIX. Puede resultar útil participar en cursos de formación para administración de sistemas UNIX.

Acceso a Oracle Support

Los clientes de Oracle tienen acceso a soporte electrónico por medio de My Oracle Support. Para obtener más información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o, si tiene alguna discapacidad auditiva, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`.

Convenciones tipográficas

La siguiente tabla describe las convenciones tipográficas utilizadas en este manual.

TABLA P–1 Convenciones tipográficas

Tipos de letra	Descripción	Ejemplo
`AaBbCc123`	Los nombres de los comandos, los archivos, los directorios y los resultados que el equipo muestra en pantalla	Edite el archivo `.login`. Utilice el comando `ls -a` para mostrar todos los archivos. `nombre_sistema% tiene correo.`
`AaBbCc123`	Lo que se escribe, en contraposición con la salida del equipo en pantalla	`nombre_sistema% su` `Contraseña:`

TABLA P–1 Convenciones tipográficas *(Continuación)*

Tipos de letra	Descripción	Ejemplo
aabbcc123	Marcador de posición: sustituir por un valor o nombre real	El comando para eliminar un archivo es `rm` *filename*.
AaBbCc123	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el capítulo 6 de la *Guía del usuario*.
		Una *copia en caché* es aquella que se almacena localmente.
		No guarde el archivo.
		Nota: Algunos elementos destacados aparecen en negrita en línea.

Indicadores de los shells en los ejemplos de comandos

La tabla siguiente muestra los indicadores de sistema UNIX predeterminados y el indicador de superusuario de shells que se incluyen en los sistemas operativos Oracle Solaris. Tenga en cuenta que el indicador predeterminado del sistema que se muestra en los ejemplos de comandos varía según la versión de Oracle Solaris.

TABLA P–2 Indicadores de shell

Shell	Indicador
Shell Bash, shell Korn y shell Bourne	`$`
Shell Bash, shell Korn y shell Bourne para superusuario	`#`
Shell C	`machine_name%`
Shell C para superusuario	`machine_name#`

◆ ◆ ◆ CAPÍTULO 1

Gestión de recursos y virtualización de red en Oracle Solaris

En este capítulo, se explican los conceptos básicos relacionados con la virtualización de red y el control de recursos en Oracle Solaris. Se tratan los temas siguientes:

Estas funciones sirven para gestionar el control del flujo, mejorar el rendimiento del sistema y configurar el uso de redes necesario para efectuar la virtualización del sistema operativo, la informática de utilidades y la consolidación de servidores.

Descripción general de la virtualización de red

La *virtualización de redes* es la combinación de los recursos de red del hardware con los recursos de red del software en una única unidad administrativa. El objetivo de la virtualización de redes consiste en facilitar un uso compartido de recursos de redes eficaz, controlado y seguro para los usuarios y los sistemas.

El producto final de la virtualización de redes es la *red virtual*. Las redes virtuales se clasifican en dos clases principales: externas e internas. Las *redes virtuales externas* constan de varias redes locales que el software administra como una única entidad. Las partes que componen las redes virtuales externas clásicas son el hardware de conmutación y la tecnología de software de red de área local virtual (VLAN). Entre los ejemplos de redes virtuales externas, se incluyen las grandes redes corporativas y los centros de datos.

Este manual se centra en la red virtual interna. Una *red virtual interna* consta de un sistema que usa zonas o máquinas virtuales cuyas interfaces de red están configuradas mediante, al menos, una NIC física. Estas interfaces de red se denominan *tarjetas de interfaz de red virtual o NIC virtual (VNIC)*. Estos contenedores pueden comunicarse entre sí como si estuvieran en la misma red local, por lo que se convierten en una red virtual en un único host.

Un tipo especial de red virtual interna es la *red virtual privada*. Las redes virtuales privadas son diferentes de las redes privadas virtuales (VPN). El software de VPN crea un enlace punto a

punto seguro entre dos sistemas de punto final. La red virtual privada es una red virtual en un sistema al que los sistemas externos no pueden acceder. El aislamiento de esta red interna respecto de otros sistemas externos se consigue configurando las VNIC mediante etherstubs. Los etherstubs se describen en la sección siguiente.

Puede combinar los recursos de red para configurar tanto redes virtuales internas como externas. Por ejemplo, puede configurar los sistemas individuales con redes virtuales internas en las LAN que formen parte de una gran red virtual externa.

Componentes de la virtualización de red

A continuación se muestran los componentes básicos de la virtualización de red en Oracle Solaris:

- Tarjetas de la interfaz de red virtual (VNIC)
- Conmutadores virtuales
- Etherstubs

Las *VNIC* son dispositivos de red virtual con las mismas interfaces de enlace de datos que una NIC física. Las VNIC se configuran mediante un enlace de datos subyacente. Cuando las VNIC se configuran, estas se comportan como NIC físicas. Además, los recursos del sistema tratan las VNIC como si fueran NIC físicas. Una VNIC tiene una dirección MAC que se genera automáticamente. Según la interfaz de red que esté en uso, puede asignar explícitamente a una VNIC una dirección MAC distinta de la dirección predeterminada, como se describe en la página del comando man `dladm(1M)`.

Para obtener la lista actual de interfaces físicas que admiten VNIC, consulte las preguntas más frecuentes sobre virtualización de redes y control de recursos (`http://hub.opensolaris.org/bin/view/Project+crossbow/faq`).

Cuando se crea una VNIC, automáticamente se crea un *conmutador virtual*. De acuerdo con el diseño de Ethernet, si un puerto del conmutador recibe un paquete saliente desde el host conectado a ese puerto, el paquete no puede acceder a un destino en el mismo puerto. Este diseño resulta inconveniente para los sistemas que están configurados con redes virtuales, porque las redes virtuales comparten la misma NIC. Los paquetes salientes se envían a través de un puerto del conmutador hacia la red externa. Los paquetes entrantes no pueden alcanzar su zona de destino porque los paquetes no pueden regresar por el mismo puerto por el que se enviaron. Los conmutadores virtuales proporcionan a estas zonas el medio para transferir los paquetes. El conmutador virtual abre una ruta de datos para que las redes virtuales se comuniquen entre sí.

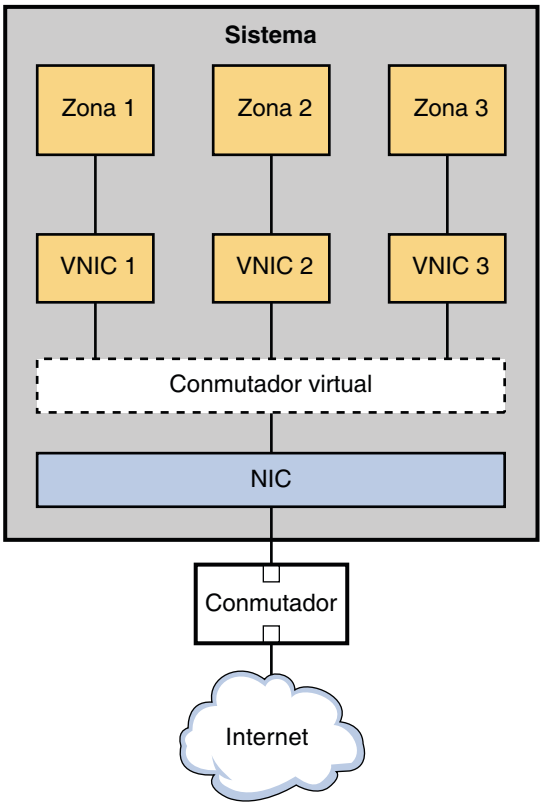
Los etherstubs son pseudo-NIC Ethernet. Puede crear VNIC sobre etherstubs en lugar de hacerlo sobre enlaces físicos. Las VNIC mediante un etherstub se independizan de las NIC físicas del sistema. Con los etherstubs, puede construir una red virtual privada que esté aislada de las demás redes virtuales del sistema y de la red externa. Por ejemplo, si desea crear un

entorno de red cuyo acceso esté limitado únicamente a los desarrolladores de su empresa y no a la red en general, los etherstubs se pueden utilizar para crear dicho entorno.

Los etherstubs y las VNIC son sólo una parte de las funciones de virtualización de Oracle Solaris. Estos componentes generalmente se utilizan con Oracle Solaris Zones. Mediante la asignación de VNIC o etherstubs para su uso en función de las zonas, puede crear una red en un único sistema. Para obtener información sobre zonas, consulte *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

Mediante la combinación de estos componentes y su implementación con zonas, puede tener redes dentro de un sistema similar al que se muestra en la siguiente figura.

FIGURA 1–1 Configuración de la VNIC para una única interfaz



En la Figura 1–1 se muestra un único sistema con una NIC. La NIC está configurada con tres VNIC. Cada VNIC admite una sola zona. Zona 1, Zona 2 y Zona 3 constituyen las redes virtuales dentro del único sistema. Las zonas se comunican entre sí y con la red externa mediante sus respectivas VNIC. A su vez, las tres VNIC se conectan a la NIC física subyacente

por medio del conmutador virtual. La función del conmutador virtual equivale a la conectividad que un conmutador externo ofrece a los sistemas conectados a los puertos del conmutador.

Cuando se configura una red virtual, una zona envía tráfico a un host externo del mismo modo que un sistema sin red virtual. El tráfico se transfiere de la zona al conmutador virtual, por medio de la VNIC, y, luego, a la interfaz física, que envía los datos a la red.

Las zonas también pueden intercambiar tráfico entre sí dentro del sistema. Por ejemplo, los paquetes se transfieren desde la Zona 1 por medio de la VNIC 1 dedicada. Luego, el tráfico fluye por el conmutador virtual hasta la VNIC 3. A continuación, VNIC 3 transfiere el tráfico a la zona 3. El tráfico nunca deja el sistema y, por lo tanto, nunca infringe las restricciones de Ethernet.

Si lo prefiere, puede crear una red virtual basada en etherstub. Los etherstubs se basan exclusivamente en software y no requieren una interfaz de red como base para la red virtual.

¿Quién debería ejecutar redes virtuales?

Si necesita consolidar los recursos en los servidores de Sun de Oracle, considere la posibilidad de implementar las VNIC y las redes virtuales. Los consolidadores de los ISP, las empresas de telecomunicaciones y las grandes instituciones financieras pueden utilizar las siguientes funciones de virtualización de redes para mejorar el rendimiento de sus servidores y sus redes.

- El hardware de NIC, incluidas las nuevas y poderosas interfaces que admiten anillos de hardware
- Varias direcciones MAC para las VNIC
- El gran ancho de banda proporcionado por las interfaces más nuevas

Es posible sustituir muchos sistemas por un único sistema que tenga varias zonas o máquinas virtuales, sin disminuir significativamente la separación, la seguridad y la flexibilidad.

Para obtener una demostración de las ventajas de la virtualización de red, consulte Consolidating the Data Center With Network Virtualization (`http://download.oracle.com/otndocs/tech/OTN_Demos/data-center-consolidation.html`).

Comandos para configurar componentes de virtualización

Para crear VNIC, utilice el comando `dladm create-vnic`.

```
# dladm create-vnic -l link [-v vid] vnic
```

`-l` *link* Hace referencia al nombre del enlace de datos mediante el que está configurada la VNIC.

`-v` *vid* Hace referencia al identificador de VLAN para la VNIC si desea crear la VNIC como una VLAN. Esta opción no es necesaria. Para configurar una VNIC con un identificador de VLAN, consulte "Cómo configurar VNIC con identificadores de VLAN" en la página 17. Para obtener más información sobre las VLAN, consulte el Capítulo 3, "Cómo trabajar con redes VLAN" de *Gestión del rendimiento de red de Oracle Solaris 11.1*.

vnic Hace referencia al nombre de la VNIC.

Nota – Puede configurar otras propiedades para una VNIC, como direcciones MAC, CPU para asociar a la VNIC, etc. Para obtener una lista de estas propiedades, consulte la página del comando man `dladm(1M)`. Ciertas modificaciones de propiedades sólo funcionan con VNIC. Por ejemplo, con el comando `dladm create-vnic` puede configurar una dirección MAC y asignar un identificador de VLAN para crear una VNIC como una VLAN. Sin embargo, no puede utilizar el comando `dladm create-vlan` para configurar una dirección MAC directamente para una VLAN.

Puede crear sólo una VNIC a la vez mediante un enlace de datos. Como los enlaces de datos, las VNIC tienen propiedades de enlace que se pueden configurar más según sea necesario. En "Propiedades de enlaces de datos para el control de recursos" en la página 11 se muestran algunas de estas propiedades para gestionar el uso de los recursos de red del sistema.

Para crear etherstubs, utilice el comando `dladm create-ether`.

```
# dladm create-ether etherstub
```

La creación de VNIC o etherstubs son sólo pasos preliminares para la configuración de redes virtuales. Para utilizar estos componentes para crear redes virtuales en su sistema, consulte el Capítulo 2, "Creación y administración de redes virtuales en Oracle Solaris".

Descripción general de la gestión de recursos de red

En esta sección se explican los distintos métodos que se pueden utilizar para gestionar el uso de los recursos de red de un sistema.

Propiedades de enlaces de datos para el control de recursos

En Oracle Solaris 11, la calidad del servicio (QoS) se obtiene de manera más fácil y dinámica, mediante la gestión de recursos de red. La gestión de recursos de red incluye la configuración de

las propiedades de enlaces de datos que pertenecen a los recursos de la red. Al establecer estas propiedades, se determina qué parte de un determinado recurso se puede utilizar para procesos de red. Por ejemplo, un enlace se puede asociar a un número específico de CPU que se reservan exclusivamente para procesos de red. O bien, a un enlace se le puede asignar un ancho de banda determinado para procesar un tipo específico de tráfico de la red.

Una vez que se define una propiedad de recurso, el nuevo valor se aplica de inmediato. Este método permite la flexibilidad de la gestión de recursos. Puede definir propiedades de recursos al crear el enlace. Como alternativa, puede definir estas propiedades más tarde, por ejemplo, después de estudiar el uso de los recursos a lo largo del tiempo y de determinar la mejor manera de asignar mejor el recurso. Los procedimientos para asignar recursos se aplican tanto al entorno de red virtual como a las redes físicas tradicionales. Por ejemplo, el comando `dladm set-linkprop` se utiliza para establecer las propiedades relacionadas con los recursos de la red. La misma sintaxis se utiliza en los enlaces de datos físicos y virtuales.

La gestión de los recursos de red se puede comparar con la creación de vías dedicadas para el tráfico. Al combinar distintos recursos para prestar servicio a tipos específicos de paquetes de red, esos recursos forman una *vía de red* para esos paquetes. Los recursos se pueden asignar de forma diferente para cada vía de red. Por ejemplo, puede asignar más recursos a una vía donde el tráfico de la red es más pesado. Al configurar las vías de red para que los recursos se distribuyan de acuerdo a las necesidades reales, se aumenta la eficiencia del sistema para procesar paquetes. Para obtener más información sobre vías de red, consulte "Descripción general del flujo del tráfico de red" en la página 51.

La gestión de recursos de red es útil para las siguientes tareas:

- Suministro de red
- Establecimiento de acuerdos de nivel de servicio
- Facturación a los clientes
- Diagnóstico de problemas de seguridad

Puede aislar, priorizar y controlar el tráfico de datos de un sistema individual, y realizar un seguimiento de él, sin las complejas definiciones de reglas de calidad de servicio.

Gestión de recursos de red mediante flujos

Un *flujo* es una forma personalizada de categorizar los paquetes para controlar aún más la manera en que se utilizan los recursos para procesar estos paquetes. Los paquetes de red se pueden categorizar de acuerdo con un *atributo*. Los paquetes que comparten un atributo constituyen un flujo y están etiquetados con un nombre de flujo específico. Al flujo se le pueden asignar recursos específicos.

Los atributos que sirven como base para crear flujos se obtienen de la información del encabezado de un paquete. El tráfico de paquetes se puede organizar en flujos según uno de los siguientes atributos:

- Dirección IP
- Nombre de protocolo de transporte (UDP, TCP o SCTP)
- Número de puerto de aplicación (por ejemplo, el puerto 21 para FTP)
- Atributo de campo DS, que se utiliza para QoS en paquetes IPv6 únicamente. Para obtener más información sobre el campo DS, consulte *Gestión de calidad de servicio IP en Oracle Solaris 11.1*.

Un flujo se puede basar sólo en uno de los atributos de la lista. Por ejemplo, puede crear un flujo según el puerto que se esté utilizando, como el puerto 21 para FTP, o según las direcciones IP, como los paquetes de una dirección IP de origen específica. Sin embargo, no puede crear un flujo para los paquetes de una dirección IP especificada que se reciban en el puerto número 21. Del mismo modo, no puede crear un flujo para todo el tráfico de la dirección IP `192.168.1.10` y, luego, crear un flujo para el tráfico de la capa de transporte en `192.168.1.10`. Por lo tanto, puede configurar varios flujos en un sistema y hacer que cada flujo se base en un atributo diferente.

Comandos para la gestión de recursos de red

Los comandos que se deben usar para asignar recursos de red dependen de si se está trabajando directamente en enlaces de datos o en flujos.

- En el caso de los enlaces de datos, el uso del subcomando `dladm` adecuado depende de si se está estableciendo la propiedad mientras se crea el enlace o mientras se establece la propiedad de un enlace existente. Para crear un enlace y asignarle recursos simultáneamente, utilice la siguiente sintaxis:

  ```
  # dladm create-vnic -l link -p property=value[,property=value] vnic
  ```

  Donde *link* puede ser un enlace físico o un enlace virtual.

  Para establecer la propiedad de un enlace existente, utilice la siguiente sintaxis:

  ```
  # dladm set-linkprop -p property=value[,property=value] link
  ```

  Las siguientes son propiedades de enlace que puede definir para la asignación de recursos:

  - **Ancho de banda**: puede limitar el ancho de banda de un dispositivo de hardware para el uso de un enlace determinado.

- **Anillos de NIC**: si una NIC admite la asignación de anillos, sus anillos de transmisión y recepción pueden ser asignados de manera exclusiva para su uso por parte de los enlaces de datos. Los anillos de NIC se tratan en "Trabajo con clientes, transmisión de anillos y recepción de anillos " en la página 31.
- **Agrupaciones de CPU**: las agrupaciones de CPU generalmente se crean y asocian con zonas específicas. Estas agrupaciones se pueden asignar a enlaces de datos para reservar los conjuntos de CPU para gestionar los procesos de red de las zonas asociadas. Las CPU y las agrupaciones se tratan en "Trabajo con agrupaciones y CPU" en la página 40.
- **CPU**: en un sistema con varias CPU, puede dedicar un número determinado de CPU para un procesamiento de red específico.

- Para flujos, utilice los subcomandos de `flowadm`. La gestión de recursos en los flujos se asemeja a los métodos para la gestión de recursos en enlaces de datos. Para crear un flujo y agregarle recursos simultáneamente, utilice la siguiente sintaxis:

  ```
  # flowadm add-flow -l link -a attribute=value[,attribute=value] \
  -p property=value[,property=value] flow
  ```

  El conjunto de atributos definidos que caracteriza los flujos constituye la *política de control de flujo* del sistema.

  Para establecer la propiedad de un flujo existente, utilice la sintaxis siguiente:

  ```
  # flowadm set-flowprop -p property=value[,property=value] flow
  ```

  Las propiedades de asignación de recursos que se pueden asignar a un flujo son las mismas que las propiedades que se asignan directamente a un enlace. Sin embargo, actualmente, sólo las propiedades de ancho de banda se pueden asociar a los flujos. Aunque los comandos para establecer propiedades para los enlaces de datos y para los flujos son diferentes, la sintaxis es similar. Para configurar las propiedades de ancho de banda, consulte los ejemplos que aparecen en "Cómo configurar flujos" en la página 46

  Para obtener más información sobre el comando `flowadm`, consulte la página del comando man `flowadm(1M)`. Para obtener una lista de los subcomandos que se pueden utilizar con el comando `flowadm`, escriba lo siguiente:

  ```
  # flowadm help
  The following subcommands are supported:
  Flow    : add-flow       remove-flow     reset-flowprop
            set-flowprop   show-flow       show-flowprop
  For more info, run: flowadm help <subcommand>.
  ```

◆ ◆ ◆ CAPÍTULO 2

Creación y administración de redes virtuales en Oracle Solaris

En este capítulo se incluyen tareas para la configuración de redes virtuales en un solo sistema.

Se tratan los temas siguientes:

- "Configuración de los componentes de la virtualización de redes" en la página 15
- "Creación de redes virtuales" en la página 18
- "Otras tareas administrativas para VNIC" en la página 25

Para obtener una introducción a redes virtuales, consulte el Capítulo 1, "Gestión de recursos y virtualización de red en Oracle Solaris".

Configuración de los componentes de la virtualización de redes

En Oracle Solaris 11, los etherstubs y las VNIC son los componentes básicos de la virtualización de redes. En esta sección se describen los pasos para configurar estos componentes antes de la creación de una red virtual. Para obtener una descripción de estos componentes, consulte "Componentes de la virtualización de red" en la página 8.

Se describen los siguientes procedimientos:

- "Cómo configurar VNIC y etherstubs" en la página 15
- "Cómo configurar VNIC con identificadores de VLAN" en la página 17

▼ Cómo configurar VNIC y etherstubs

La VNIC conecta la red virtual a la red externa. La VNIC también permite que las zonas se comuniquen entre sí por medio del conmutador virtual que se crea automáticamente con la VNIC. Para que una red virtual aloje el tráfico de forma interna entre las zonas y con la LAN externa e Internet, cada zona debe tener su propia interfaz. Por lo tanto, deberá repetir este procedimiento para cada zona que pertenecerá a la red virtual.

1 Conviértase en un administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 (Opcional) Cree el etherstub.

```
# dladm create-etherstub etherstub
```

Realice este paso sólo si va a crear una red virtual privada en la que desea restringir el acceso de sistemas externos. Para obtener una descripción de una red virtual privada, consulte "Descripción general de la virtualización de red" en la página 7.

Como cualquier enlace de datos, puede asignar al etherstub cualquier nombre que tenga sentido para su configuración de red. Para obtener instrucciones sobre la creación de nombres personalizados, consulte "Reglas para nombres de enlaces válidos" de *Introducción a redes de Oracle Solaris 11*.

3 Cree la VNIC.

```
# dladm create-vnic -l datalink [-v vid] vnic
```

Si va a crear la VNIC para una red virtual privada, especifique un etherstub para `datalink`. Incluya la opción `-v` *vid* en la sintaxis del comando sólo si va a crear la VNIC como una VLAN, donde *vid* hace referencia al ID de VLAN de la NIC. De lo contrario, omita esta opción.

Si va a crear una VNIC como una VLAN, consulte "Cómo configurar VNIC con identificadores de VLAN" en la página 17 para obtener los pasos adicionales que son específicos para VNIC como VLAN.

Puede asignar cualquier nombre a la VNIC. Para asignar nombres personalizados a las VNIC, consulte "Reglas para nombres de enlaces válidos" de *Introducción a redes de Oracle Solaris 11*.

4 Cree una interfaz IP mediante la VNIC.

```
# ipadm create-ip interface
```

5 Asigne una dirección IP estática a la interfaz VNIC.

```
# ipadm create-addr -a address interface
```

`-a` *address* Especifica la dirección IP, que pueden estar en la notación CIDR.

interface Especifica VNIC que ha creado en el paso anterior.

La dirección IP estática puede ser una dirección IPv4 o una dirección IPv6. Para obtener más información sobre la configuración de direcciones IP, consulte "Cómo configurar una interfaz IP" de *Conexión de sistemas mediante la configuración de redes fijas en Oracle Solaris 11.1*.

Para obtener más información sobre la configuración de direcciones IP, consulte "Cómo configurar una interfaz IP" de *Conexión de sistemas mediante la configuración de redes fijas en Oracle Solaris 11.1*.

6 **Agregue la información de dirección al archivo `/etc/hosts`.**

▼ Cómo configurar VNIC con identificadores de VLAN

En la red virtual, puede configurar VNIC con identificadores de VLAN para alojar el tráfico de VLAN. También puede establecer la propiedad de enlace `vlan-announce` para propagar la configuración de VLAN de cada VNIC a la red.

A diferencia de enlace VLAN regular, la VNIC configurada como una VLAN tiene su propia dirección MAC. Para obtener información sobre las VLAN no relacionadas con VNIC, consulte el Capítulo 3, "Cómo trabajar con redes VLAN" de *Gestión del rendimiento de red de Oracle Solaris 11.1*.

Nota – El siguiente procedimiento sólo incluye los pasos para crear la VNIC con un ID de VLAN y para establecer las propiedades adecuadas que permiten que la VNIC sea adecuada para el tráfico de VLAN. Aunque los conmutadores y los puertos intermediarios se actualizan automáticamente al activar la propiedad, los puntos finales se debe configurar por separado para definir redes VLAN en estos puntos.

---

1 **Conviértase en un administrador.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Cree una VNIC con un ID de VLAN.**

```
# dladm create-vnic -l link -v vid vnic
```

3 **Transmita la configuración de VLAN de la VNIC a la red.**

```
# dladm set-linkprop -p vlan-announce=gvrp link
```

Mediante este paso se puede activar un sistema cliente de protocolo de registro VLAN GARP (GVRP) que registra automáticamente los identificadores de VLAN con conmutadores conectados. De manera predeterminada, la propiedad `vlan-announce` está establecida en `off` y no se envían mensajes transmitidos de por VLAN a la red. Después de establecer la propiedad en `gvrp`, la configuración de VLAN para ese enlace se propaga para activar la configuración automática de puerto de VLAN de los dispositivos de red. De esta manera, estos dispositivos pueden aceptar y reenviar el tráfico de VLAN.

4 **(Opcional) Para configurar el tiempo de espera entre transmisiones VLAN, establezca la propiedad `gvrp-timeout`.**

```
# dladm set-linkprop -p gvrp-timeout=time link
```

Donde *time* se expresa en milisegundos. El valor predeterminado es de 250 milisegundos. Un sistema con una carga importante puede requerir un intervalo más corto para la retransmisión de información VLAN. Esta propiedad permite ajustar el intervalo.

5 **(Opcional) Para mostrar los valores de las propiedades `vlan-announce` y `gvrp-timeout`, utilice el siguiente comando:**

```
# dladm show-linkprop -p vlan-announce,gvrp-timeout
```

Ejemplo 2–1 Configuración de una VNIC como una VLAN

En este ejemplo se crea una VNIC con un ID de VLAN y se permite el anuncio de la configuración VLAN a la red.

```
# dladm create-vnic -l net0 -v 123 vnic0
# dladm set-linkprop -p vlan-announce=gvrp net0
# dladm show-linkprop -p vlan-announce,gvrp-timeout net0
LINK    PROPERTY        PERM   VALUE   DEFAULT   POSSIBLE
net0    vlan-announce   rw     gvrp    off       gvrp,off
net0    gvrp-timeout    rw     250     250       --
```

Creación de redes virtuales

Una red virtual combina las zonas y componentes de virtualización. Se crea la cantidad de zonas que sean necesarias y que admita el sistema. Cada zona tiene su propia interfaz virtual. Las zonas del sistema se puedan comunicar entre sí. La red virtual en su totalidad se conecta a los destinos de la red externa más grande.

La creación de una red virtual consta de uno o varios pasos para configurar etherstubs o VNIC y de pasos para configurar zonas. Aunque estos son conjuntos de procedimientos independientes, ambos deben llevarse a cabo para finalizar la construcción de la red virtual.

Los procedimientos de esta sección se basan en las siguientes suposiciones:

- La red virtual del sistema consta de tres zonas. Las zonas están en diferentes etapas de configuración: la primera zona se crea como una zona nueva, la segunda ya existe en el sistema y se debe volver a configurar para utilizar una VNIC y la tercera está designada como red virtual privada. Por lo tanto, los procedimientos demuestran las diversas maneras para preparar las zonas para la red virtual.
- La interfaz física del sistema está configurada con la dirección IP `192.168.3.70`.
- La dirección IP del enrutador es `192.168.3.25`.

En cada procedimiento de esta sección, se agregan más detalles al escenario para proporcionar un contexto más concreto para los pasos.

Cuando se crea la red virtual, se realizan algunos pasos en la zona global y algunos pasos en una zona no global. Para mayor claridad, en los indicadores de los ejemplos que aparecen después de cada procedimiento se indica en qué zona se ejecuta cada comando específico. Sin embargo, la ruta real que muestran los indicadores puede variar según los indicadores especificados para su sistema.

En esta sección, se describen los siguientes procedimientos:

- "Cómo configurar una zona para la red virtual" en la página 19
- "Cómo volver a configurar una zona para que utilice una VNIC" en la página 21
- "Cómo crear una red virtual privada" en la página 23

▼ Cómo configurar una zona para la red virtual

Este procedimiento explica cómo configurar una zona nueva a una VNIC nueva. Observe que en el procedimiento.sólo se incluyen los pasos relacionados con la virtualización de redes. Para obtener instrucciones detalladas sobre la configuración de zonas, consulte el Capítulo 17, "Planificación y configuración de zonas no globales (tareas)" de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

En el procedimiento se supone que la primera zona para la red virtual se crea como una zona nueva.

1 Conviértase en un administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Configure la VNIC.

Consulte "Cómo configurar VNIC y etherstubs" en la página 15. Sin embargo, para este procedimiento específico, omita el paso para crear un etherstub.

3 Cree la zona.

```
global# zonecfg -z zone
```

Cuando cree la zona, asegúrese de establecer el parámetro `ip-type` en `exclusive` y de asignar la VNIC que acaba de crear a la interfaz física de la zona.

4 Para salir del modo de configuración de zona, compruebe la configuración y, luego, confírmela.

5 Instale la zona.

```
global# zoneadm -z zone install
```

Nota – El proceso de instalación puede tardar.

6 Inicie la zona.

```
global# zoneadm -z zone boot
```

7 Una vez que la zona se haya iniciado por completo, inicie sesión en la zona.

```
# zlogin -C zone
```

8 Proporcione la información que se le solicita.

La mayor parte de la información se proporciona mediante la selección de una lista de opciones. En general, las opciones predeterminadas son suficientes. Para configurar la red virtual, debe proporcionar o verifique la siguiente información:

- El nombre de host de la zona, por ejemplo `zone1`.
- La dirección IP de la zona que se basa en la dirección IP de la VNIC de la zona.
- Si IPv6 se debe activar.
- Si el sistema con la red virtual forma parte de una subred.
- La máscara de red de la dirección IP.
- La ruta predeterminada, que puede ser la dirección IP de la interfaz física en la que se crea la red virtual.

Una vez que haya proporcionado la información necesaria, la zona se reiniciará.

Ejemplo 2–2 Configuración de una zona para la red virtual

En este ejemplo se incluyen pasos detallados para crear `zone1`. Sin embargo, sólo se muestran los parámetros de zona que son relevantes para la creación de una red virtual.

```
global # zonecfg -z zone1
zonecfg:zone1> create
zonecfg:zone1> set zonepath=/export/home/zone1
zonecfg:zone1> set autoboot=true
zonecfg:zone1> set ip-type=exclusive
zonecfg:zone1> add net
zonecfg:zone1:net> set physical=vnic1
zonecfg:zone1:net> end
zonecfg:zone1> verify
zonecfg:zone1> commit
zonecfg:zone1> exit

global# zoneadm -z zone1 install
Preparing to install zone <zone1>
Creating list of files to copy from the global zone.
.
.
```

```
Zone <zone1> is initialized.

global# zoneadm -z zone1 boot

zlogin -C zone1
What type of terminal are you using?
.
.
.
8) Sun Workstation
9) Televideo 910
10) Televideo 925
11) Wyse Model 50
12) X Terminal Emulator (xterms)
13) CDE Terminal Emulator (dtterm)
14) Other
Type the number of your choice and press Return: 13
.
(More prompts)
..
```

Se proporciona la siguiente información de red:

```
Hostname: zone1
IP address: 192.168.3.80
System part of a subnet: Yes
Netmask: 255.255.255.0
Enable IPv6: No
Default route: 192.168.3.70
Router IP address: 192.168.3.25
```

▼ Cómo volver a configurar una zona para que utilice una VNIC

Este procedimiento hace referencia a la segunda zona de la red virtual. La zona ya existe, pero su configuración actual impide que forme parte de la red virtual. En concreto, el tipo de IP de zona es un tipo compartido y su interfaz actual es `net0`. Ambas configuraciones se debe cambiar.

1 Conviértase en un administrador.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Cree la VNIC.

```
global# dladm create-vnic [-v vid] -l datalink vnic
```

Donde *vid* hace referencia al identificador de VLAN que se asigna a la VNIC. Especifique el identificador de VLAN sólo si desea crear la VNIC como una VLAN.

Todavía no configure la interfaz de VNIC. Realizará este paso más adelante en este procedimiento.

3 Cambie el tipo de IP de la zona de compartido a exclusivo.

```
global# zonecfg -z zone
zonecfg:zone1> set ip-type=exclusive
zonecfg:zone1>
```

4 Cambie la interfaz de la zona para usar una VNIC.

```
zonecfg:zone1> remove net physical=NIC
zonecfg:zone1> add net
zonecfg:zone1:net> set physical=vnic
zonecfg:zone1:net> end
zonecfg:zone1>
```

5 Verifique y confirme los cambios que ha implementado y, a continuación, salga de la zona.

```
zonecfg:zone1 verify
zonecfg:zone1> commit
zonecfg:zone1> exit
global#
```

6 Reinicie la zona.

```
global# zoneadm -z zone reboot
```

7 Inicie sesión en la zona.

```
global# zlogin zone
```

8 Configure la VNIC con una dirección IP válida.

Si asigna una dirección estática a la VNIC, debe escribir lo siguiente:

zone`# ipadm create-addr -a` *address interface*

Donde *address* puede utilizar la notación CIDR.

9 Desde la zona global, agregue la información de dirección al archivo `/etc/hosts`.

Ejemplo 2–3 Reconfiguración de una configuración de zona para utilizar una VNIC

En este ejemplo, `zone2` ya existe como zona compartida. La zona también utiliza la interfaz principal del sistema en lugar de un enlace virtual. Debe modificar `zone2` para utilizar `vnic2`. Para utilizar `vnic2`, primero, se debe cambiar el tipo de IP de `zone2` a exclusivo. Tenga en cuenta que parte de la salida está truncada para centrar la atención en la información pertinente relacionada con redes virtuales.

```
global# dladm create-vnic -l net0 vnic2

global# zonecfg -z zone2
zonecfg:zone1> set ip-type=exclusive
zonecfg:zone1> remove net physical=net0
zonecfg:zone1> add net
zonecfg:zone1:net> set physical=vnic2
zonecfg:zone1:net> end
```

```
zonecfg:zone1> verify
zonecfg:zone1> commit
zonecfg:zone1> exit
global# zoneadm -z zone2 reboot

global# zlogin zone2
zone2# ipadm create-ip vnic2
zone2# ipadm create-addr -a 192.168.3.85/24 vnic2
ipadm: vnic2/v4

zone2# exit

global# vi /etc/hosts
#
::1             localhost
127.0.0.1       localhost
192.168.3.70    loghost   #For net0
192.168.3.80    zone1   #using vnic1
192.168.3.85    zone2   #using vnic2
```

▼ Cómo crear una red virtual privada

En el procedimiento siguiente se explica cómo configurar la tercera zona de la red virtual. Aunque la zona forma parte de la red virtual, no se podrá acceder a ella desde sistemas externos. Para permitir que la zona aislada envíe tráfico de red fuera del sistema, deberá utilizar la traducción de direcciones de red (NAT). NAT traduce las direcciones IP privadas de la VNIC en direcciones IP enrutables de la interfaz de red física. Sin embargo, las direcciones IP privadas no se pueden ver desde la red externa. Para obtener más información sobre NAT, consulte "Uso de la función NAT del filtro IP" de *Protección de la red en Oracle Solaris 11.1*.

El uso de etherstubs constituye la diferencia principal entre una red virtual normal y una red virtual privada. En una red virtual privada, las VNIC que se asignan a las zonas se configuran mediante un etherstub. Por lo tanto, quedan aisladas del tráfico de red que fluye por el sistema.

En este procedimiento se supone que la zona ya existe, pero en la actualidad no tiene ninguna interfaz asociada.

1. **Conviértase en un administrador.**

   Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2. **Cree el etherstub.**

   ```
   global# dladm create-etherstub etherstub
   ```

3. **Cree una VNIC mediante el etherstub.**

   ```
   global# dladm create-vnic -l etherstub vnic
   ```

Todavía no configure la interfaz de VNIC. Realizará este paso más adelante en este procedimiento.

4 Asigne la VNIC a la zona.

```
global# zonecfg -z zone
 zone# set physical=vnic
```

5 Verifique y confirme los cambios que ha implementado y, a continuación, salga de la zona.

```
zonecfg:zone1 verify
zonecfg:zone1> commit
zonecfg:zone1> exit
global#
```

6 Inicie sesión en la zona.

```
# zlogin zone
```

7 En la zona, cree una interfaz IP mediante la VNIC que en este momento está asignada a la zona.

```
# ipadm create-ip interface
```

8 Configure la VNIC con una dirección IP válida.

Si asigna una dirección estática a la VNIC, debe escribir lo siguiente:

```
zone# ipadm create-addr -a address interface
```

Donde *address* puede utilizar la notación CIDR.

9 Desde la zona global, agregue la información de dirección al archivo `/etc/hosts`.

10 Desde la zona global, establezca la interfaz principal para realizar el reenvío de IP.

```
# ipadm set-ifprop -p forwarding=on -m ipv4 primary-interface
```

Nota – En general, en Oracle Solaris 11, la interfaz principal utiliza el nombre `net0`.

---

11 Desde la zona global, configure la traducción de direcciones de red (NAT) en el archivo `/etc/ipnat.conf` para la interfaz principal.

12 Inicie el servicio de filtro IP para activar NAT.

```
# svcadm enable network/ipfilter
```

13 Reinicie la zona.

```
# zoneadm -z zone reboot
```

Ejemplo 2–4 Creación de la configuración de una red virtual privada

En este ejemplo, zone3 está configurada para ser aislada como una red privada. Las opciones de NAT y reenvío de IP también se configuran para permitir que la red privada virtual envíe paquetes fuera del host y, al mismo tiempo, oculte su dirección privada a la red externa. La zona ya está configurada con un tipo de IP exclusiva. Sin embargo, no se le ha asignado ninguna interfaz IP.

```
global# dladm create-etherstub ether0
global# dladm create-vnic -l ether0 vnic3
global# zonecfg -z zone3
zonecfg:zone3> add net
zonecfg:zone3:net> set physical=vnic3
zonecfg:zone3:net> end
zonecfg:zone3> verify
zonecfg:zone3> commit
zonecfg:zone3> exit
global#

global# zlogin zone3
zone3# ipadm create-ip vnic3
zone3# ipadm create-addr -a 192.168.0.10/24 vnic3
ipadm: vnic3/v4
zone3# exit

global# cat /etc/hosts
::1             localhost
127.0.0.1       localhost
192.168.3.70    loghost   #For net0
192.168.3.80    zone1   #using vnic1
192.168.3.85    zone2   #using vnic2
192.168.0.10    zone3   #using vnic3

global# ipadm set-ifprop -p forwarding=on -m ipv4 vnic3

global# vi /etc/ipf/ipnat.conf
map vnic3 192.168.0.0/24 -> 0/32  portmap tcp/udp auto
map vnic3 192.168.0.0/24 -> 0/32

global# svcadm enable network/ipfilter
global# zoneadm -z zone3 boot
```

Otras tareas administrativas para VNIC

En esta sección, se describen las tareas que puede realizar en las VNIC después de realizar la configuración básica. En esta sección, se tratan los siguientes temas:

- "Cómo suprimir una VNIC" en la página 30

Nota – Las VNIC se pueden configurar como VLAN. Un subcomando paralelo, `dladm modify-vlan`, le permite modificar las VLAN directas que se han creado con el comando `dladm create-vlan`. Debe utilizar el subcomando correcto en función de si se está modificando las VLAN o VNIC configuradas como VLAN. Utilice el subcomando `modify-vlan` en las VLAN que muestra el subcomando `dladm show-vlan`. Utilice el subcomando `modify-vnic` en las VNIC, incluidas las que tienen identificadores de VLAN, que muestra el subcomando `dladm show-vnic`. Para modificar las VLAN directas, consulte "Modificación de las VLAN" de *Gestión del rendimiento de red de Oracle Solaris 11.1*.

Hay dos tipos de modificación de VNIC disponibles:

- La modificación global cambia un atributo de todas las VNIC de un enlace de datos específico a la vez. La opción `-L` se utiliza para identificar el enlace de datos subyacente cuya VNIC desea modificar.
- La modificación selectiva modifica un atributo de las VNIC seleccionadas. En lugar de utilizar la opción `-L` para identificar el enlace de datos subyacente, se especifican las VNIC cuyo atributo se desea cambiar.

Se pueden modificar los siguientes atributos: el identificador de VLAN, la dirección MAC y el enlace subyacente. Modificar el enlace subyacente significa mover una VNIC a otro enlace de datos. En las siguientes secciones se describen estas modificaciones en detalle.

Modificación del identificador de VLAN de una VNIC

Para cambiar el identificador de VLAN de una VNIC, utilice uno de los siguientes comandos:

- `dladm modify-vnic -v` *vid* `-L` *datalink*

  En este comando, *vid* especifica el nuevo identificador de VLAN que se asigna a la VNIC. *datalink* hace referencia al enlace subyacente mediante el que se configura la VNIC. Puede utilizar esta sintaxis de comando si sólo existe una VNIC única en el enlace de datos. Se produce un error de comando en los enlaces de datos que tienen varias VNIC configuradas, porque estas VNIC deben tener identificadores de VLAN exclusivos.
- `dladm modify-vnic -v` *vid vnic*

  Utilice este comando para cambiar los identificadores de VLAN exclusivos de varias VNIC mediante un solo enlace de datos. Dado que cada identificador de VLAN es exclusivo para las VNIC del mismo enlace de datos, debe cambiar un identificador de VLAN por vez. Suponga que desea cambiar los identificadores de VLAN de `vnica0`, `vnicb0` y `vnicc0`, que están configuradas mediante `net0`. Deberá proceder de esta manera:

```
# dladm modify-vnic -v 123 vnica0
# dladm modify-vnic -v 456 vnicb0
# dladm modify-vnic -v 789 vnicc0
```

- `dladm modify-vnic -v` *vid vnic*`,`*vnic*`,[...]`

  Utilice este comando para cambiar el identificador de VLAN de las VNIC como un grupo, siempre y cuando cada VNIC esté en un enlace de datos distinto. Suponga que desea cambiar los identificadores de VLAN de `vnic0`, `vnic1` y `vnic2`. Estas VNIC están configuradas mediante `net0`, `net1` y `net2` respectivamente. Debe utilizar el comando siguiente:

  ```
  # dladm modify-vnic -v 123 vnic0,vnic1,vnic2
  ```

Modificación de las direcciones MAC de las VNIC

Las VNIC tienen direcciones MAC únicas. Para modificar estas direcciones, utilice uno de los siguientes comandos según corresponda a las circunstancias específicas:

- `dladm modif-vnic -m` *mac-address vnic*

  Utilice este comando para asignar una dirección MAC específica a una VNIC específica.

- `dladm modif-vnic -m random -L` *datalink*

  Este comando realiza una modificación global, mediante la cual se cambia la dirección MAC de todas las VNIC del enlace de datos. El sistema asigna automáticamente direcciones MAC únicas a las VNIC. En este comando, la opción `-m random` es equivalente a la opción `-m auto`.

- `dladm modif-vnic -m random` *vnic, vnic*`,[...]`

  Este comando realiza una modificación selectiva de VNIC. Tenga en cuenta que tanto para las modificaciones globales como para las selectivas, se especifica `random` para la opción `-m`.

Puede modificar la dirección MAC y el identificador de VLAN de una VNIC con un solo comando. Sin embargo, tenga cuidado al utilizar comandos para modificar varios atributos de VNIC de manera global, ya que esto puede provocar un comportamiento inesperado. Es preferible cambiar varios atributos de a una VNIC por vez antes que cambiar varios atributos de un grupo de VNIC al mismo tiempo.

En el ejemplo siguiente se muestra la salida antes y después de modificar la dirección MAC y el identificador de VLAN de una VNIC.

```
# dladm show-vnic vnic0
LINK      OVER     SPEED  MACADDRESS        MACADDRTYPE    VID
vnic0     net0     1000   2:8:20:ec:c4:1d   random         0
# dladm modify-vnic -m random -v 123 vnic0
# dladm show-vnic vnic0
LINK      OVER     SPEED  MACADDRESS        MACADDRTYPE    VID
vnic0     net0     1000   2:8:20:0:1:2      random         123
```

Migración de VNIC

Puede mover una o varias VNIC de un enlace de datos subyacente a otro sin suprimir ni volver a configurar la VNIC. El enlace subyacente puede ser un enlace físico, una agregación de enlaces o un etherstub.

Para lograr la migración correcta de las VNIC, el enlace de datos subyacente al que se mueven las VNIC debe poder admitir las propiedades de enlace de datos de las VNIC. Si estas propiedades no son admitidas, la migración fallará y el usuario será notificado. Después de una migración correcta, todas las aplicaciones que utilizan las VNIC continúan funcionando normalmente, siempre y cuando las VNIC permanezcan conectadas a la red.

Es posible que después de una migración de VNIC algunas propiedades que dependen del hardware cambien, como el estado del enlace de datos, velocidad de enlace, el tamaño de MTU, etc. Los valores de estas propiedades se heredan del enlace de datos al que se migran las VNIC.

También puede migrar VNIC de manera global o selectiva. La migración global significa que se migran todas las VNIC de un enlace de datos a otro. Para realizar una migración global, sólo tiene que especificar el enlace de datos de origen y el de destino. En el siguiente ejemplo, se mueven todas las VNIC de `ether0` a `net1`:

```
# dladm modify-vnic -l net1 -L ether0
```

Donde

- `-l` *datalink* hace referencia al enlace de datos de destino al que se migran las VNIC.
- `-L` *datalink* hace referencia al enlace de datos de origen mediante el que se configuran las VNIC.

Nota – Debe especificar el enlace de datos de destino antes que el enlace de datos de origen.

Para realizar la migración selectiva de VNIC, debe especificar las VNIC que desea mover. En el ejemplo siguiente se mueven las VNIC seleccionadas de `net0` a `net1`:

```
# dladm modify-vnic -l net1 vnic0,vnic1,vnic2
```

Nota – La opción `-L` se limita sólo a la modificación global.

Mientras se migra un grupo de VNIC, también se pueden modificar sus identificadores de VLAN al mismo tiempo. Sin embargo, para asignar identificadores de VLAN nuevos, debe migrar las VNIC una por vez, como se muestra en el siguiente ejemplo:

```
# dladm modify-vnic -l net1 -v 123 vnic0
# dladm modify-vnic -l net1 -v 456 vnic1
# dladm modify-vnic -l net1 -v 789 vnic2
```

Los efectos de la migración en la dirección MAC dependen de si la VNIC utiliza una dirección MAC de fábrica del de enlace de datos de origen.

- Si no especifica la opción `-m` durante la migración, después de la migración, la dirección MAC de fábrica se sustituye por una dirección asignada de manera aleatoria del enlace de datos de destino.
- Si utiliza la opción `-m` *address* durante la migración, esa dirección se asigna a la VNIC después de la migración.

Las direcciones MAC asignadas de manera aleatoria no se ven afectadas y son retenidas por sus respectivas VNIC después de la migración.

En el ejemplo siguiente se muestra cómo migrar varias VNIC. Tenga en cuenta que las VNIC están utilizando direcciones MAC asignadas de manera aleatoria. Por lo tanto, estas direcciones no se modificarán después de la migración.

```
# dladm show-vnic
LINK      OVER     SPEED  MACADDRESS        MACADDRTYPE    VID
vnic1     net0     1000   2:8:20:c2:39:38   random         0
vnic2     net0     1000   2:8:20:5f:84:ff   random         0

# dladm modify-vnic -l net1 -L net0
# dladm show-vnic vnic0
LINK      OVER     SPEED  MACADDRESS        MACADDRTYPE    VID
vnic1     net1     1000   2:8:20:c2:39:38   random         0
vnic2     net1     1000   2:8:20:5f:84:ff   random         0
```

Visualización de la información de VNIC

Para obtener información sobre las VNIC del sistema, utilice el comando `dladm show-vnic`.

```
# dladm show-vnic
LINK      OVER     SPEED         MACADDRESS          MACADDRTYPE
vnic1     net0     1000 Mbps     2:8:20:c2:39:38     random
vnic2     net0     1000 Mbps     2:8:20:5f:84:ff     random
```

Las VNIC también son enlaces de datos. Por lo tanto, también es posible utilizar cualquier comando dladm que muestre información sobre enlaces de datos para incluir información sobre las VNIC, si estas existen en el sistema. Por ejemplo, `dladm show-link` incluye las VNIC en la lista. También puede usar el comando `dladm show-linkprop` para comprobar las propiedades de las VNIC. Para obtener información de las propiedades de una sola VNIC, especifique la VNIC al mostrar las propiedades de enlace:

```
# dladm show-linkprop [-p property] vnic
```

▼ Cómo suprimir una VNIC

En este procedimiento se explica cómo suprimir una configuración de VNIC del sistema. En los pasos se supone que la VNIC está conectada a una zona. Debe encontrarse en la zona global para poder realizar este procedimiento.

1 Como la VNIC está conectada a una zona, detenga la zona.

```
global# zoneadm -z zone halt
```

Nota – Para determinar los enlaces utilizados por una zona, use el comando `dladm show-link`.

2 Elimine o desconecte la VNIC de la zona.

```
global# zonecfg -z zone remove net physical=vnic
```

3 Suprima la VNIC del sistema.

```
global# dladm delete-vnic vnic
```

4 Reinicie la zona.

```
global# zonecfg -z zone boot
```

Ejemplo 2–5 Supresión de una VNIC del sistema

En este ejemplo, se elimina `vnic1` de `zoneB` y del sistema.

```
Global# dladm show-link
LINK            CLASS   MTU    STATE   OVER
net0            phys    1500   up      --
net2            phys    1500   up      --
net1            phys    1500   up      --
net3            phys    1500   up      --
zoneA/net0      vnic    1500   up      net0
zoneB/net0      vnic    1500   up      net0
vnic0           vnic    1500   up      net1
zoneA/vnic0     vnic    1500   up      net1
vnic1           vnic    1500   up      net1
zoneB/vnic1     vnic    1500   up      net1

Global# zoneadm -z zoneB halt
Global# zonecfg -z zoneB remove net physical=vnic1
Global# dladm delete-vnic vnic1
Global# zonecfg -z zoneB reboot
```

◆ ◆ ◆ CAPÍTULO 3

Gestión de recursos de red en Oracle Solaris

En este capítulo se explica cómo gestionar recursos en enlaces de datos, incluidos los enlaces virtuales, como las VNIC. La gestión de recursos de red implementa la calidad de servicio (QoS) IP para mejorar el rendimiento, especialmente en la red virtual.

Se tratan los temas siguientes:

Trabajo con clientes, transmisión de anillos y recepción de anillos

En las NIC, los anillos de recepción (Rx)y los anillos de transmisión (Tx) son recursos de hardware mediante los que el sistema recibe y envía paquetes de red, respectivamente. En las secciones siguientes, se proporciona una descripción general de los anillos y de los procedimientos que se utilizan para asignar anillos a procesos de red. También se proporcionan ejemplos para mostrar cómo funciona el mecanismo al ejecutar comandos para asignar anillos.

Clientes MAC y asignación de anillos

Los clientes MAC, como las VNIC y otros enlaces de datos, se configuran mediante una NIC para permitir la comunicación entre un sistema y otros nodos de red. Una vez que un cliente se configura, éste utiliza los anillos Rx y Tx para recibir o transmitir paquetes de red respectivamente. Un cliente MAC puede estar basado en hardware o en software. Un cliente basado en hardware debe cumplir con alguna de las siguientes condiciones:

- Tiene el uso dedicado de uno o varios anillos de Rx.
- Tiene el uso dedicado de uno o varios anillos de Tx.

- Tiene el uso dedicado de uno o varios anillos de Rx y de uno o varios anillos Tx.

Los clientes que no cumplen con ninguna de estas condiciones son clientes MAC basados en software.

A los clientes basados en hardware se les puede asignar anillos para uso exclusivo según la NIC. Las NIC como `nxge` admiten la *asignación dinámica de anillos*. En estas NIC, puede configurar no sólo clientes basados en hardware. También tiene la flexibilidad para determinar el número de anillos para asignar a dichos clientes, suponiendo que los anillos siguen estando disponibles para la asignación. El uso de anillos siempre se optimiza para la interfaz principal, por ejemplo, `net0`. La interfaz principal también se conoce como el *cliente principal*. Los anillos disponibles que no se han asignado para el uso exclusivo de otros clientes, se asignan automáticamente a la interfaz principal.

Otras NIC como `ixge` sólo admiten la *asignación estática de anillos*. En estas NIC, sólo puede crear clientes basados en hardware. Los clientes se configuran automáticamente con un conjunto fijo de anillos por cliente. El conjunto fijo se determina durante la configuración inicial del controlador de la NIC. Para obtener más información sobre la configuración inicial de un controlador para la asignación estática de anillos, consulte *Manual de referencia de parámetros ajustables de Oracle Solaris 11.1*.

Los clientes basados en software no tienen uso exclusivo de anillos. En cambio, comparten anillos con otros clientes basados en software existentes o con el cliente principal. Los anillos que utilizan los clientes basados en software dependen del número de clientes basados en hardware que tienen prioridad en la asignación de anillos.

Es importante entender la diferencia entre el *cliente principal* y otros *clientes secundarios*. El cliente principal es el enlace de datos físico de la NIC. Según los nombres genéricos proporcionados por Oracle Solaris durante la instalación, el cliente principal se denominará `net`*N*, donde *N* es un número de instancia. Para obtener una explicación de nombres genéricos para enlaces de datos, consulte "Nombres de enlaces de datos y dispositivos de red" de *Introducción a redes de Oracle Solaris 11*. Las VNIC son *clientes secundarios* que se crean mediante el enlace de datos físico. Si estos clientes son clientes basados en hardware, pueden tener el uso exclusivo de anillos. De lo contrario, los clientes se basan en software.

Asignación de anillos en VLAN

En el caso de las VLAN, la asignación de anillos se lleva a cabo de manera diferente según cómo se crea la VLAN. Las VLAN se crean de una de estas dos maneras:

- Mediante el uso del subcomando `dladm create-vlan`:

  ```
  # dladm create-vlan -l link -v vid vlan
  ```

- Mediante el uso del subcomando `dladm create-vnic`:

  ```
  # dladm create-vnic -l link -v vid vnic
  ```

Una VLAN que se crea mediante el subcomando `dladm create-vlan` comparte la misma dirección MAC que la interfaz subyacente. Por lo tanto, esa VLAN también comparte los anillos de Rx y Tx de la interfaz subyacente. Una VLAN que se crea como una VNIC mediante el comando `dladm create-vnic` tiene una dirección MAC distinta de la de su interfaz subyacente. La asignación de anillos para esta VLAN es independiente de la asignación para el enlace subyacente. Por lo tanto, a esa VLAN se le pueden asignar sus propios anillos dedicados, suponiendo que la NIC admite clientes basados en hardware.

Propiedades de enlace de datos para la asignación de anillos

Para administrar anillos, se pueden definir dos propiedades de anillos mediante el comando `dladm`:

- `rxrings` se refiere al número de anillos de Rx asignados a un enlace especificado.
- `txrings` se refiere al número de anillos de Tx asignados a un enlace especificado.

Puede establecer cada propiedad en uno de los tres valores posibles:

- `sw` indica que está configurando un cliente basado en software. El cliente no tiene el uso exclusivo de los anillos. En cambio, el cliente comparte los anillos con cualquier otro cliente existente que esté configurado de manera similar.
- *n* > *0* (número mayor que cero) se aplica a la configuración de un cliente basado en hardware únicamente. El número hace referencia a la cantidad de anillos que asigna al cliente para su uso exclusivo. Puede especificar un número sólo si la NIC subyacente admite la asignación dinámica de anillos.
- `hw` también se aplica a la configuración de un cliente basado en hardware. Sin embargo, para dicho cliente, no puede especificar el número real de anillos dedicados. En su lugar, ya está establecido el número fijo de anillos por cliente según la configuración inicial del controlador de la NIC. Debe establecer las propiedades `*rings` en `hw` únicamente si la NIC subyacente admite la asignación estática de anillos.

Para proporcionar información sobre las asignaciones y el uso actuales de los anillos, están disponibles las siguientes propiedades de anillo de sólo lectura adicionales:

- `rxrings-available` y `txrings-available` indican el número de anillos de Rx y Tx que están disponibles para la asignación.
- `rxhwclnt-available` y `txhwclnt-available` indican el número clientes basados en hardware de Rx y Tx que se pueden configurar mediante una NIC.

Comandos para trabajar con la recepción y transmisión de anillos

Para gestionar el uso de la recepción y transmisión de anillos de enlaces de datos, debe utilizar los siguientes subcomandos `dladm` principales:

- `dladm show-linkprop`: muestra los valores actuales de las propiedades de enlace de datos, incluidos los anillos de Rx y de TX. La salida proporciona la siguiente información sobre las capacidades de admisión de anillos de un enlace de datos. Necesita la información para determinar qué tipo de cliente puede configurar para utilizar anillos de Rx y de TX.
  - Los clientes disponibles que puede crear
  - Los anillos disponibles que puede asignar a los clientes disponibles
  - La capacidad de admitir la asignación dinámica o estática de anillos
  - Si sólo se admite de asignación estática de anillos, la distribución actual de anillos a los clientes existentes

  En "Propiedades de enlace de datos para la asignación de anillos" en la página 33 se describe más detalladamente cómo interpretar la salida de este comando.
- `dladm show-phys -H` *datalink*: muestra el modo en que los anillos de un enlace de datos físico están siendo utilizados actualmente por los clientes existentes.
- `dladm create-vnic -p` *ring-properties vnic*: crea un cliente con un número específico de anillos de Tx o de Rx para usar para el tráfico.
- `dladm set-linkprop -p` *ring-properties datalink*: asigna anillos a un cliente específico, siempre que haya anillos disponibles y se admita la asignación de anillos.

Obtención e interpretación de información de anillos

En esta sección, se describe la salida de `dladm show-linkprop` que muestra las propiedades relacionadas con los anillos de un enlace de datos.

Visualización de las capacidades de asignación anillos de un enlace de datos

En esta sección se proporcionan ejemplos de salidas de comandos de propiedades relacionadas con anillos y se explica qué tipo de información se puede obtener. En los ejemplos se utilizan las siguientes NIC:

- `net0` (mediante `nxge`)
- `net1` (mediante `ixgbe`)
- `net2` (mediante `e1000g`)

EJEMPLO 3–1 Información de anillos de nxge

En el siguiente ejemplo, se muestra la información de anillos de `nxge`:

```
# dladm show-linkprop net0
LINK    PROPERTY            PERM  VALUE  DEFAULT  POSSIBLE
...
net0    rxrings             rw    --     --       sw,<1-7>
...
net0    txrings             rw    --     --       sw,<1-7>
...
net0    rxrings-available   r-    5      --       --
net0    txrings-available   r-    5      --       --
net0    rxhwclnt-available  r-    2      --       --
net0    txhwclnt-available  r-    2      --       --
...
```

Con `net0`, los valores del campo `POSSIBLE` son `sw` y `<1-7>` para `rxrings` y `txrings`. Estos valores indican que `nxge` admite clientes basados en hardware y clientes basados en software. El rango `<1-7>` indica los límites del número de anillos de Rx o de Tx que se pueden establecer para los clientes. El rango también indica que la NIC admite la asignación dinámica de anillos tanto para la recepción y como para la transmisión.

Además, las propiedades `*rings-available` indican que cinco anillos de Rx y cinco anillos de Tx están disponibles para ser asignados a clientes basados en hardware.

Sin embargo, las propiedades `*clnt-available` muestran que sólo puede configurar dos clientes para que tengan el uso exclusivo de los anillos de Rx disponibles. Del mismo modo, sólo puede configurar dos clientes que pueden tener el uso exclusivo de los anillos de Tx disponibles.

EJEMPLO 3–2 Información de anillos de ixgbe

En el siguiente ejemplo, se muestra la información de anillos de `ixgbe`:

```
# dladm show-linkprop net1
LINK   PROPERTY            PERM  VALUE  DEFAULT  POSSIBLE
...
net1   rxrings             rw    --     --       sw,hw
...
net1   txrings             rw    --     --       sw,hw,<1-7>
...
net1   rxrings-available   r-    0      --       --
net1   txrings-available   r-    5      --       --
net1   rxhwclnt-available  r-    0      --       --
net1   txhwclnt-available  r-    7      --       --
...
```

Con `net1`, los valores `sw` y `hw` del campo `POSSIBLE` para `rxrings` y `txrings` indican que `ixgbe` admite clientes basados en hardware y clientes basados en software. Para los anillos de Rx sólo se admite la asignación estática de anillos, en la que el hardware asigna un conjunto fijo de anillos de Rx a cada cliente basado en hardware. No obstante, en el caso de los anillos de TX, el rango `<1–7>` indica que se admite la asignación dinámica. Puede determinar que el número de anillos de Tx para asignar a un cliente basado en hardware, en este ejemplo, sea de hasta siete anillos.

EJEMPLO 3–2 Información de anillos de ixgbe *(Continuación)*

Además, las propiedades `*rings-available` indican que hay cinco anillos de Tx disponibles para asignar a clientes basados en hardware, pero no se pueden asignar anillos de Rx.

Por último, en función de las propiedades `*hwclnt-available`, puede configurar siete clientes de Tx basados en hardware para utilizar anillos de Tx exclusivamente. Sin embargo, no puede crear clientes basados en hardware con uso exclusivo de anillos de Rx porque no se admite la asignación dinámica de anillos de Rx.

Un cero (`0`) en el campo `VALUE` de cualquiera de las propiedades `*rings-available` puede significar una de las siguientes opciones:

- No hay más anillos disponibles para asignar a los clientes.
- No se admite asignación dinámica de anillos.

Puede verificar el significado del cero mediante la comparación del campo `POSSIBLE` para `rxrings` y `txrings`, y del campo `VALUE` para `rxrings-available` y `txrings-available`.

Por ejemplo, suponga que `txrings-available` es `0`, como se muestra a continuación:

```
# dladm show-linkprop net1
LINK   PROPERTY            PERM  VALUE  DEFAULT  POSSIBLE
...
net1   rxrings             rw    --     --       sw,hw
net1   txrings             rw    --     --       sw,hw,<1-7>
net1   rxrings-available   r-    0      --       --
net1   txrings-available   r-    0      --       --
...
```

En esta salida, el campo `VALUE` para `rxrings-available` es `0`, mientras que el campo `POSSIBLE` para `rxrings` es `sw,hw`. La información combinada significa que no hay anillos de Rx disponibles, porque la NIC no admite la asignación dinámica de anillos. En la transmisión, el campo `VALUE` para `txrings-available` es `0`, mientras que el campo `POSSIBLE` para `txrings` es `sw,hw,<1-7>`. La información combinada indica que no hay anillos de Tx disponibles, porque todos los anillos de Tx ya se han asignado. Sin embargo, como indica el campo `POSSIBLE` para `txrings`, se admite la asignación dinámica de anillos. Por lo tanto, puede asignar anillos de Tx a medida que estos anillos estén disponibles.

EJEMPLO 3–3 Información de anillos de e1000g

En el siguiente ejemplo, se muestra la información de anillos de `e1000g`:

```
# dladm show-linkprop net2
LINK   PROPERTY             PERM  VALUE  DEFAULT  POSSIBLE
...
net2   rxrings              rw    --      --      --
...
net2   txrings              rw    --      --      --
...
```

EJEMPLO 3–3 Información de anillos de e1000g *(Continuación)*

```
net2   rxrings-available   r-     0       --     --
net2   txrings-available   r-     0       --     --
net2   rxhwclnt-available  r-     0       --     --
net2   txhwclnt-available  r-     0       --     --
...
```

La salida indica que no se pueden configurar anillos ni clientes basados en hardware, porque no se admite la asignación de anillos en `e1000g`.

Visualización del uso y las asignaciones de anillos en un enlace de datos

Dos propiedades de enlace de datos de sólo lectura proporcionan información sobre cómo están siendo utilizados actualmente los anillos por los clientes existentes en el enlace de datos:

- `rxrings-effective`
- `txrings-effective`

Para obtener información sobre el uso de los anillos y sobre qué anillos están distribuidos a los clientes, use los subcomandos `dladm show-linkprop` y `dladm show-phys -H`.

En los ejemplos siguientes se muestran los diferentes tipos de salida generados por los dos comandos en relación con el uso de los anillos de Rx y de Tx, y con la manera en que estos anillos están distribuidos entre los clientes.

EJEMPLO 3–4 Uso de los anillos del cliente principal

El cliente principal es la interfaz que se configura mediante el enlace de datos físico de la NIC. En este ejemplo, la NIC es una tarjeta `ixgbe`. De manera predeterminada, su enlace de datos es `net0`. La interfaz IP mediante `net0` es el cliente principal.

```
# dladm show-linkprop net0
LINK   PROPERTY              PERM  VALUE  DEFAULT  POSSIBLE
...
net0   rxrings               rw    --     --       sw,hw
net0   rxrings-effective     r     2      --       --
net0   txrings               rw    --     --       sw,hw,<1-7>
net0   txrings-effective     r     8      --       --
net0   txrings-available     r-    7      --       --
net0   rxrings-available     r-    0      --       --
net0   rxhwclnt-available    r-    3      --       --
net0   txhwclnt-available    r-    7      --       --
...
# dladm show-phys -H net0
LINK   RINGTYPE   RINGS   CLIENTS
net0   RX         0-1     <default,mcast>
net0   TX         0-7     <default>net0
net0   RX         2-3     net0
net0   RX         4-5     --
net0   RX         6-7     --
```

La salida proporciona la siguiente información sobre el uso y la distribución de anillos para el cliente principal `net0`:

EJEMPLO 3–4 Uso de los anillos del cliente principal *(Continuación)*

- `rxrings-effective` muestra que `net0` automáticamente recibe dos anillos de Rx. `txrings-effective` muestra que `net0` tiene el uso de ocho anillos de Tx. De manera predeterminada, todos los anillos no utilizados se asignan automáticamente al cliente principal.
- De acuerdo con la salida del comando `dladm show-phys -H`, los dos anillos de Rx asignados a `net0` son los anillos `2` y `3`. Para los anillos de Tx, `net0` utiliza los anillos `0` a `7`.

EJEMPLO 3–5 Uso de los anillos de un cliente secundario

En este ejemplo se supone la configuración de un cliente VNIC `vnic1` mediante `net0`, el enlace de datos físico de la tarjeta `ixgbe`.

```
# dladm show-linkprop vnic1
LINK    PROPERTY            PERM  VALUE  DEFAULT  POSSIBLE
...
vnic1   rxrings             rw    hw     --       sw,hw
vnic1   rxrings-effective   r-    2      --       --
vnic1   txrings             rw    hw     --       sw,hw,<1-7>
vnic1   txrings-effective   r-    1      --       --
...
# dladm show-linkprop net0
LINK    PROPERTY            PERM  VALUE  DEFAULT  POSSIBLE
...
net0  rxrings             rw     --    --       sw,hw
net0  rxrings-effective   r-     2     --       --
net0  txrings             rw     --    --       sw,hw,<1-7>
net0  txrings-effective   r-     --    --       --
net0  txrings-available   r-     6     --       --
net0  rxrings-available   r-     0     --       --
net0  rxhwclnt-available  r-     3     --       --
net0  txhwclnt-available  r-     6     --       --
...
# dladm show-phys -H net0
LINK     RINGTYPE   RINGS     CLIENTS
net0   RX         0-1       <default,mcast>
net0   TX         0,2-7     <default>net0
net0   RX         2-3       net0
net0   RX         4-5       vnic1
net0   RX         6-7       --
net0   TX         1         vnic1
```

La salida combinada de los tres comandos proporciona la siguiente información:

- `rxrings-effective` para `vnic1` muestra que esta VNIC recibe automáticamente dos anillos de Rx. `txrings-effective` muestra que `vnic1` tiene el uso de un anillo de Tx. Estos anillos están asignados de manera estática, como lo indica el valor `hw` establecido para las propiedades `*ring`.
- De acuerdo con la salida del comando `dladm show-phys -H`, los dos anillos de Rx asignados a `net0` son los anillos `2` y `3`. Para los anillos de Tx, `net0` utiliza el anillo `0` y los anillos `2` a `7`. `vnic1` utiliza el anillo `1` para un anillo de Tx, y los anillos `4` y `5` para los anillos de Rx.

EJEMPLO 3–5 Uso de los anillos de un cliente secundario *(Continuación)*

Tenga en cuenta que `vnic1` está configurado como un cliente basado en hardware con asignación estática de anillos. Por lo tanto, el número de clientes de hardware de Tx disponibles `txhwclnt-available`) que se pueden crear mediante `net0` se reduce a seis.

▼ Cómo configurar clientes y asignar anillos

En este procedimiento se explica cómo configurar clientes en un enlace de datos en función del tipo de compatibilidad con la asignación de anillos. Asegúrese de poder interpretar la salida de los comandos `dladm` que muestran las propiedades de anillos de enlace de datos, como se explica en "Visualización de las capacidades de asignación anillos de un enlace de datos" en la página 34 y "Visualización del uso y las asignaciones de anillos en un enlace de datos" en la página 37. La información lo guiará para la configuración de los clientes.

1 Visualice las propiedades de anillo del enlace de datos.

```
# dladm show-linkprop datalink
```

En función de la salida, determine lo siguiente:

- Si la NIC admite clientes basados en hardware
- El tipo de asignación de anillos que admite la NIC
- La disponibilidad de anillos para asignar a los clientes basados en hardware
- La disponibilidad de clientes basados en hardware que puede configurar en el enlace

2 En función de la información obtenida en el paso anterior, realice una de las siguientes acciones:

- Si la NIC admite la asignación dinámica de anillos, cree el cliente basado en hardware con la siguiente sintaxis:

  ```
  # dladm create-vnic -p rxrings=number[,txrings=number] -l link vnic
  ```

  Si el cliente ya estaba creado, utilice la siguiente sintaxis:

  ```
  # dladm set-linkprop -p rxrings=number[,txrings=number] vnic
  ```

  Nota – Algunas NIC admiten la asignación dinámica de anillos en anillos de Rx o en anillos de Tx, pero no en ambos tipos. Debe especificar *number* en el tipo de anillo para el que se admite la asignación dinámica de anillos.

- Si la NIC admite la asignación estática de anillos, cree el cliente basado en hardware con la siguiente sintaxis:

  ```
  # dladm create-vnic -p rxrings=hw[,txrings=hw] -l link vnic
  ```

  Si el cliente ya estaba creado, utilice la siguiente sintaxis:

```
# dladm set-linkprop -p rxrings=hw[,txrings=hw] vnic
```

Nota – Algunas NIC admiten la asignación estática de anillos en anillos de Rx o en anillos de Tx, pero no en ambos tipos. Debe especificar el `hw` en el tipo de anillo para el que se admite la asignación estática de anillos.

- Si la NIC sólo admite clientes basados en software, cree el cliente con la siguiente sintaxis:

  ```
  # dladm create-vnic -p rxrings=sw[,txrings=sw] -l link vnic
  ```

  Si el cliente ya estaba creado, utilice la siguiente sintaxis:

  ```
  # dladm set-linkprop -p rxrings=sw[,txrings=sw] vnic
  ```

3. **(Opcional) Compruebe la información de anillo del cliente recién creado.**

   ```
   # dladm show-linkprop vnic
   ```

4. **(Opcional) Compruebe cómo están distribuidos los anillos del enlace de datos entre los distintos clientes.**

   ```
   # dladm show-phys -H datalink
   ```

Véase también Si desea ver un ejemplo en el que se muestre cómo utilizar los flujos y cómo asignar recursos del sistema, incluidos los anillos de Rx y de Tx, para procesar el tráfico de red en una red virtual, consulte el Ejemplo 3–8.

Trabajo con agrupaciones y CPU

La propiedad de enlace `pool` le permite vincular el procesamiento de red a una agrupación de CPU. Con esta propiedad, puede integrar mejor la gestión de recursos de red con la vinculación y la administración de las CPU en zonas. En Oracle Solaris, la administración de zonas incluye la vinculación de procesos no relacionados con redes a una agrupación de recursos de CPU mediante el comando `zonecfg` o `poolcfg`. Para que esa misma agrupación de recursos también gestione los procesos de red, utilice el comando `dladm set-linkprop` para configurar la propiedad `pool` de un enlace. A continuación, asigne dicho enlace a la zona.

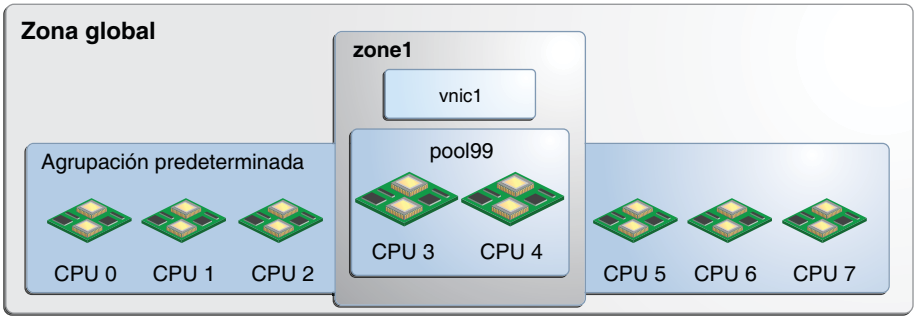
Al establecer la propiedad `pool` para un enlace y asignar el enlace como la interfaz de red de la zona, ese enlace también se vincula a la agrupación de una zona. Si dicha zona se establece como exclusiva, los recursos de CPU de la agrupación ya no podrán ser utilizados por otros enlaces de datos que no estén asignados a dicha zona.

Nota – Otra propiedad, `cpu`, se puede establecer para asignar CPU específicas a un enlace de datos. Las dos propiedades, `cpu` y `pool`, son mutuamente excluyentes. No puede definir ambas propiedades para un enlace de datos determinado. Para asignar recursos de CPU a un enlace de datos mediante la propiedad `cpu`, consulte "Cómo asignar las CPU a un enlace" en la página 44.

Para obtener más información sobre agrupaciones dentro de una zona, consulte el Capítulo 13, "Creación y administración de agrupaciones de recursos (tareas)" de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*. Para obtener más información sobre cómo crear agrupaciones y asignar conjuntos de CPU a las agrupaciones, consulte la página del comando man `poolcfg`(1M).

La siguiente figura muestra cómo funcionan las agrupaciones cuando se asigna la propiedad `pool` a un enlace de datos.

FIGURA 3–1 Propiedad pool de una VNIC asignada a una zona

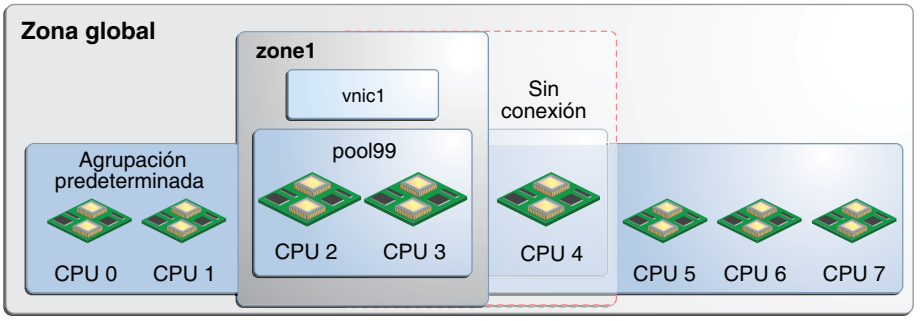


En la figura, el sistema tiene ocho CPU. Cuando no se configuran agrupaciones en el sistema, todas las CPU pertenecen a la *agrupación predeterminada* y son utilizadas por la zona global. Sin embargo, en este ejemplo, se creó la agrupación `pool99`, que está compuesta por `CPU 3` y `CPU 4`. Esta agrupación está asociada a `zone1`, que es una zona exclusiva. Si `pool99` se establece como una propiedad de `vnic1`, `pool99` se dedica a gestionar también los procesos de red de `vnic1`. Una vez que `vnic1` se asigna como la interfaz de red de `zone1`, las CPU de `pool99` se reservan para gestionar procesos relacionados y no relacionados con redes de `zone1`.

La propiedad `pool` es dinámica por naturaleza. Las agrupaciones de zona se pueden configurar con un rango de CPU, y el núcleo determina qué CPU se asignan al conjunto de CPU de la agrupación. Los cambios realizados en la agrupación se implementan de manera automática en el enlace de datos, lo que simplifica la administración de las agrupaciones de ese enlace. Por el contrario, para asignar CPU específicas al enlace mediante la propiedad `cpu`, debe especificar la CPU que se asignará. Debe establecer la propiedad `cpu` cada vez que desea cambiar los componentes de la CPU de la agrupación.

Por ejemplo, suponga que se desconecta el sistema `CPU 4` de la Figura 3–1. Como la propiedad `pool` es dinámica, el software automáticamente asocia una CPU adicional a la agrupación. Por lo tanto, se conserva la configuración original de dos CPU de la agrupación. Para `vnic1`, el cambio es transparente. En la siguiente figura, se muestra la configuración ajustada.

FIGURA 3–2 Reconfiguración automática de la propiedad pool



Las propiedades adicionales relacionadas con la agrupación muestran información sobre el uso de un enlace de datos de las CPU o de una agrupación de CPU. Estas propiedades son de sólo lectura y no pueden ser configuradas por el administrador.

- `pool-effective` muestra la agrupación que se está utilizando para procesos de red.
- `cpus-effective` muestra la lista de las CPU que se están utilizando para procesos de red.

Para gestionar los recursos de CPU de una zona, la configuración de la propiedad `pool` de un enlace de datos no se suele llevar a cabo como paso inicial. Con mayor frecuencia, se utilizan comandos, como `zonecfg` y `poolcfg`, para configurar una zona con el fin de usar una agrupación de recursos. Las propiedades de enlace `cpu` y `pool` en sí mismas no se establecen. En tales casos, las propiedades `pool-effective` y `cpus-effective` de estos enlaces de datos se definen de manera automática según las configuraciones de zona cuando se inicia la zona. La agrupación predeterminada aparece en `pool-effective` y el valor de `cpus-effective` es seleccionado por el sistema. Por lo tanto, si utiliza el comando `dladm show-linkprop`, las propiedades `pool` y `cpu` estarán vacías, pero las propiedades `pool-effective` y `cpus-effective` contendrán valores.

Configurar directamente las propiedades `pool` y `cpu` de un enlace de datos es un paso alternativo que puede utilizar para vincular la agrupación de CUP de una zona para procesos de red. Una vez que se hayan configurado estas propiedades, sus valores también se reflejarán en las propiedades `pool-effective` y `cpus-effective`. Sin embargo, tenga en cuenta que este paso alternativo se usa con menos frecuencia para gestionar los recursos de red de una zona.

▼ Cómo configurar una agrupación de CPU para un enlace de datos

Como sucede con otras propiedades de enlace, la propiedad `pool` se puede configurar para un enlace de datos en el momento en que se crea el enlace o más adelante, cuando el enlace requiere configuración adicional.

Para establecer la propiedad `pool` mientras crea la VNIC, utilice la sintaxis siguiente:

```
# dladm create-vnic -p pool=pool-name -l link vnic
```

Para establecer la propiedad `pool` de una VNIC existente, utilice la sintaxis siguiente:

```
# dladm setlinkprop -p pool=pool-name vnic
```

El siguiente procedimiento muestra cómo configurar una agrupación de CPU para una VNIC.

Antes de empezar Primero, debe realizar lo siguiente:

- Crear un conjunto de procesadores con su número asignado de CPU
- Crear la agrupación con la que se asociará el conjunto de procesadores
- Asociar la agrupación con el conjunto de procesadores

Nota – Para ver las instrucciones para completar estos requisitos previos, consulte "Cómo modificar una configuración" de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

---

1. **Establezca la propiedad `pool` del enlace en la agrupación de CPU que creó para la zona. Realice uno de los pasos siguientes, según si la VNIC existe o no:**

   - Si la VNIC todavía no se creó, utilice la sintaxis siguiente:

     ```
     # dladm create-vnic -l link -p pool=pool vnic
     ```

     Donde *pool* hace referencia al nombre de la agrupación que se creó para la zona.

   - Si la VNIC existe, utilice la sintaxis siguiente:

     ```
     # dladm setlinkprop -p pool=pool vnic
     ```

2. **Establezca una zona para utilizar la VNIC.**

   ```
   zonecfg>zoneid:net> set physical=vnic
   ```

Nota – Para ver las instrucciones sobre cómo asignar una interfaz de red a una zona, consulte "Configuración, verificación y confirmación de una zona" de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

Ejemplo 3–6 Asignación de una agrupación de CPU de un enlace a una zona con un tipo de IP exclusiva

En este ejemplo se muestra cómo se asigna una agrupación al enlace de datos de una zona. El escenario se basa en la configuración en la Figura 3–1. En el ejemplo, se presupone que una agrupación de CPU denominada `pool99` ya fue configurada para la zona. La agrupación se asigna a una VNIC. Por último, la zona no global `zone1` se configura para usar la VNIC como la interfaz de red.

```
# dladm create-vnic -l net1 -p pool99 vnic1

# zonecfg -c zone1
zonecfg:zone1> set ip-type=exclusive
zonecfg:zone1> add net
zonecfg:zone1>net> set physical=vnic1
zonecfg:zone1>net> end
zonecfg:zone1> exit
```

▼ Cómo asignar las CPU a un enlace

El procedimiento siguiente explica cómo asignar CPU específicas para procesar el tráfico que atraviesa un enlace de datos mediante la configuración de la propiedad `cpu`.

1 Compruebe las asignaciones de CPU para la interfaz.

```
# dladm show-linkprop -p cpus link
```

De manera predeterminada, no se asigna ninguna CPU a ninguna interfaz específica. Por lo tanto, el parámetro `VALUE` de la salida del comando no contendrá ninguna entrada.

2 Muestre las interrupciones y las CPU con las que están asociadas las interrupciones.

```
# echo ::interrupts | mdb -k
```

La salida muestra los parámetros de cada enlace del sistema, incluido el número de CPU.

3 Asigne las CPU al enlace.

Las CPU pueden incluir aquellas con las que están asociadas las interrupciones del enlace.

```
# dladm set-linkprop -p cpus=cpu1,cpu2,... link
```

Donde *cpu1* es el número de CPU que se va a asignar al enlace. Puede dedicar varias CPU al enlace.

4. **Compruebe la interrupción del enlace para verificar las nuevas asignaciones de CPU.**

   ```
   # echo ::interrupts | mdb -k
   ```

5. **(Opcional) Muestre las CPU que están asociadas al enlace.**

   ```
   # dladm show-linkprop -p cpus link
   ```

Ejemplo 3–7 Asignación de las CPU a un enlace

En este ejemplo se muestra cómo dedicar CPU específicas al enlace de datos `net0`.

Tenga en cuenta la siguiente información de la salida generada por los diferentes comandos. Para mayor claridad, la información significativa se destaca en la salida.

- De manera predeterminada, `net0` no tiene CPU dedicada. Por lo tanto, `VALUE` es `--`.
- La interrupción de `net0` está asociada con la CPU `18`.
- Después de que se asignan las CPU, `net0` muestra una nueva lista de CPU en `VALUE`.

```
# dladm show-linkprop -p cpus net0
LINK          PROPERTY     PERM     VALUE     DEFAULT     POSSIBLE
net0     cpus          rw       --        --          --

# echo ::interrupts | mdb -k
Device  Shared   Type   MSG #   State   INO    Mondo   Pil   CPU
net#0   no       MSI    2       enbl    0x1a   0x1a    6     18

# dladm set-linkprop -p cpus=14,18,19,20 net0

# dladm show-linkprop -p cpus net0
LINK   PROPERTY   PERM   VALUE        DEFAULT   POSSIBLE
net0   cpus       rw     14,18,19,20  --        --
```

Todos los subprocesos auxiliares, incluida la interrupción, ahora se limitan al conjunto de CUP recientemente asignado.

Véase también Si desea ver un ejemplo en el que se muestre cómo utilizar los flujos y cómo asignar recursos del sistema, incluidas las CPU y las agrupaciones de CPU, para procesar el tráfico de red en una red virtual, consulte el Ejemplo 3–8.

Gestión de recursos en flujos

Los flujos están compuestos por paquetes de red que se organizan según un atributo. Los flujos permiten asignar más recursos de red. Para obtener una descripción general de los flujos, consulte "Gestión de recursos de red mediante flujos" en la página 12.

El uso de flujos para la gestión de recursos implica los siguientes pasos generales:

1. Crear el flujo sobre la base de un atributo específico como se muestra en "Gestión de recursos de red mediante flujos" en la página 12.

2. Personalizar el uso de recursos del flujo mediante el establecimiento de las propiedades que pertenecen a los recursos de la red. Actualmente, sólo se puede configurar el ancho de banda para el procesamiento de los paquetes.

▼ Cómo configurar flujos

1 Si es necesario, muestre los enlaces disponibles para determinar el enlace en el que configurará los flujos.

```
# dladm show-link
```

2 Verifique que las interfaces IP mediante el enlace seleccionado estén correctamente configuradas con direcciones IP.

```
# ipadm show-addr
```

3 Cree los flujos según el atributo que ha determinado para cada flujo.

```
# flowadm add-flow -l link -a attribute=value[,attribute=value] flow
```

link Se refiere al enlace en el que se va a configurar el flujo.

attribute Se refiere a una de las siguientes clasificaciones según las que puede organizar los paquetes de red en un flujo:

- Dirección IP
- Protocolo de transporte (UDP, TCP o SCTP)
- Número de puerto para una aplicación (por ejemplo, puerto 21 para FTP)
- Atributo de campo DS, que se utiliza para la calidad de servicio en paquetes IPv6 únicamente. Para obtener más información sobre el campo DS, consulte "Punto de código DS" de *Gestión de calidad de servicio IP en Oracle Solaris 11.1*.

flow Se refiere al nombre que le asigna al flujo en particular.

Para obtener más información sobre los flujos y sus atributos, consulte la página del comando man `flowadm(1M)`.

4 (Opcional) Visualice el rango de valores posible para el ancho de banda del enlace de datos.

```
# dladm show-linkprop -p maxbw link
```

Donde *link* es el enlace de datos en el que está configurado el flujo.

El rango de valores se muestra en el campo `POSSIBLE`.

5 Asigne una parte de ancho de banda al flujo.

```
# flowadm set-flowprop -p maxbw=value flow
```

El valor que se define debe estar dentro del rango de valores permitido para el ancho de banda del enlace.

Nota – Actualmente, sólo se puede personalizar el ancho de banda de un flujo.

---

6 (Opcional) Visualice los flujos que ha creado mediante el enlace.

```
# flowadm
```

Nota – El comando `flowadm`, si se utiliza sin subcomandos, proporciona la misma información que el comando `flowadm show-flow`.

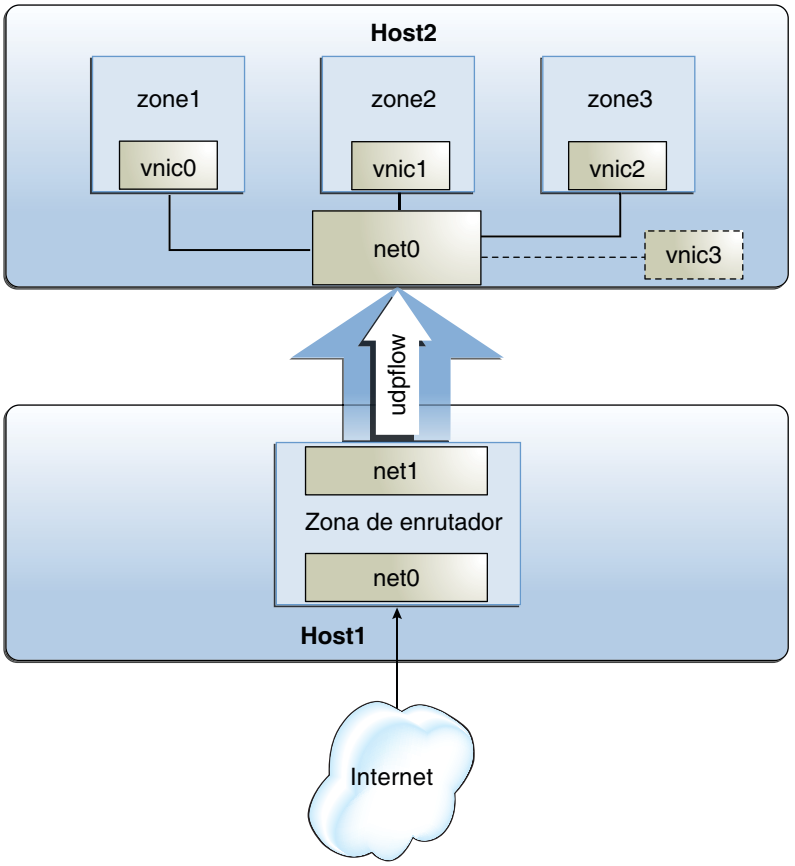
---

7 (Opcional) Visualice los valores de propiedad para un flujo especificado.

```
# flowadm show-flowprop flow
```

Ejemplo 3–8 Gestión de recursos mediante la configuración de propiedades de flujos y enlaces

En este ejemplo se combinan los pasos para asignar recursos de red a enlaces de datos y flujos. El ejemplo se basa en la configuración que se muestra en la figura siguiente.



La figura muestra dos hosts físicos que están conectados entre sí.

- `Host1` tiene la siguiente configuración:
  - Tiene una zona no global que actúa como una zona enrutadora. Se asignan dos interfaces a la zona: `net0` se conecta a Internet y `net1` se conecta a la red interna, incluido el segundo host.
  - `udpflow` es un flujo que se configura mediante `net0` para aislar el tráfico UDP e implementar el control sobre el modo en que los paquetes UDP utilizan los recursos. Para obtener información sobre la configuración de flujos, consulte "Gestión de recursos en flujos" en la página 45.
- `Host2` tiene la siguiente configuración:
  - Tiene tres zonas no globales y sus respectivas VNIC. Las VNIC se configuran mediante `net0` cuya tarjeta admite la asignación dinámica de anillos. Para obtener más información sobre la asignación de anillos, consulte "Trabajo con clientes, transmisión de anillos y recepción de anillos " en la página 31.

- La carga de procesamiento de red de cada zona es diferente. Para este ejemplo, la carga para `zone1` es pesada, la carga para `zone2` es moderada y la carga para `zone3` el liviana. Los recursos se asignan a estas zonas según sus cargas.
- Se configura una VNIC aparte como un cliente basado en software. Para obtener una descripción general de clientes MAC, consulte "Clientes MAC y asignación de anillos" en la página 31.

Las tareas de este ejemplo incluyen lo siguiente:

- Crear un flujo y configurar controles de flujo: se crea un flujo mediante `net1` para crear controles de recursos independientes respecto de los paquetes UDP recibidos por `Host2`.
- Configurar propiedades de recursos de red para las VNIC en `Host2`: según la carga de procesamiento de cada zona, se configura la VNIC de cada zona con un conjunto de anillos dedicados. También se configura una VNIC independiente sin anillos dedicados como un ejemplo de un cliente basado en software.

Tenga en cuenta que el ejemplo no incluye ningún procedimiento para la configuración de zonas. Para configurar zonas, consulte el Capítulo 17, "Planificación y configuración de zonas no globales (tareas)" de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

En primer lugar, vea la información sobre enlaces e interfaces IP en `Host1`.

```
# ipadm
NAME              CLASS/TYPE STATE     UNDER      ADDR
lo0               loopback   ok        --         --
    lo0/v4         static     ok        --         127.0.0.1/8
net0              ip         ok        --         --
    net0/v4        static     ok        --         10.10.6.5/24
net1              ip         failed    ipmp0      --
    net1/v4        static     ok        --         10.10.12.42/24
```

A continuación, cree un flujo mediante `net1` para aislar el tráfico UDP a `Host2`. A continuación, implemente los controles de recursos en el flujo.

```
# flowadm add-flow -l net1 -a transport=udp udpflow
# flowadm set-flowprop -p maxbw=80 udpflow
```

Luego, compruebe la información sobre el flujo creado.

```
flowadm
FLOW         LINK    IPADDR    PROTO    LPORT    RPORT    DFSLD
udpflow      net1    --        udp      --       --       --

# flowadm show-flowprop
FLOW          PROPERTY        VALUE          DEFAULT        POSSIBLE
udpflow       maxbw             80           --             --
```

En Host2, configure las VNIC mediante net0 para cada zona. Implemente los controles de recursos en cada VNIC. A continuación, asigne las VNIC a las zonas respectivas.

```
# dladm create-vnic -l net0 vnic0
# dladm create-vnic -l net0 vnic1
# dladm create-vnic -l net0 vnic2

# dladm set-prop -p rxrings=4,txrings=4 vnic0
# dladm set-prop -p rxrings=2,txrings=2 vnic1
# dladm set-prop -p rxrings=1,txrings=1 vnic2


# zonecfg -z zone1
# zonecfg:zone1> add net
# zonecfg:zone1:net> set physical=vnic0
# zonecfg:zone1:net> end
# zonecfg:zone1> commit
# zonecfg:zone1> exit
# zoneadm -z zone1 reboot

# zonecfg -z zone2
# zonecfg:zone2> add net
# zonecfg:zone2:net> set physical=vnic1
# zonecfg:zone2:net> end
# zonecfg:zone2> commit
# zonecfg:zone2> exit
# zoneadm -z zone2 reboot
#

# zonecfg -z zone3
# zonecfg:zone3> add net
# zonecfg:zone3:net> set physical=vnic2
# zonecfg:zone3:net> end
# zonecfg:zone3> commit
# zonecfg:zone3> exit
# zoneadm -z zone3 reboot
#
```

Suponga que pool1, un conjunto de CPU de Host2, previamente se configuró para ser utilizado por zone1. Vincule esa agrupación de CPU para gestionar también los procesos de red de zone1 como se indica a continuación:

```
# dladm set-prop -p pool=pool1 vnic0
```

Por último, cree un cliente basado en software que comparta los anillos con net0, la interfaz principal.

```
# dladm create-vnic -p rxrings=sw,txrings=sw -l net0 vnic3
```

◆ ◆ ◆ CAPÍTULO 4

Supervisión del tráfico de red y el uso de recursos en Oracle Solaris

En este capítulo se describen las tareas para la supervisión y la recopilación de estadísticas sobre el uso de los recursos de red en entornos de redes físicas y virtuales de Oracle Solaris 11. Esta información puede ser útil para analizar la asignación de recursos para fines de provisión, consolidación y facturación. En este capítulo se introducen los dos comandos que se utilizan para mostrar las estadísticas: `dlstat` y `flowstat`.

Se analizan los siguientes temas:

Descripción general del flujo del tráfico de red

Los paquetes recorren una ruta para ingresar a un sistema y para salir de él. En un nivel granular, los paquetes se reciben y se transmiten mediante los anillos de recepción (Rx) y de transmisión (Tx) de una NIC. Desde estos anillos, los paquetes recibidos se transfieren a la pila de red para su posterior procesamiento mientras los paquetes salientes se envían a la red.

En esta sección se presenta el concepto de vías de red. Una *vía de red* es una combinación de los recursos del sistema que se asignan para gestionar el tráfico de red. Por lo tanto, las vías de red son rutas personalizadas para determinados tipos de tráfico de red. Cada vía puede ser una *vía de hardware* o una *vía de software*. Además, cada tipo de vía puede ser una vía de *recepción* o una vía de *transmisión*.

La distinción entre vías de hardware y software se basa en la capacidad de una NIC para admitir anillos y asignación de anillos como se describe en "Trabajo con clientes, transmisión de anillos y recepción de anillos " en la página 31. Este capítulo se centra principalmente en el tráfico de entrada que se recibe mediante las vías de recepción.

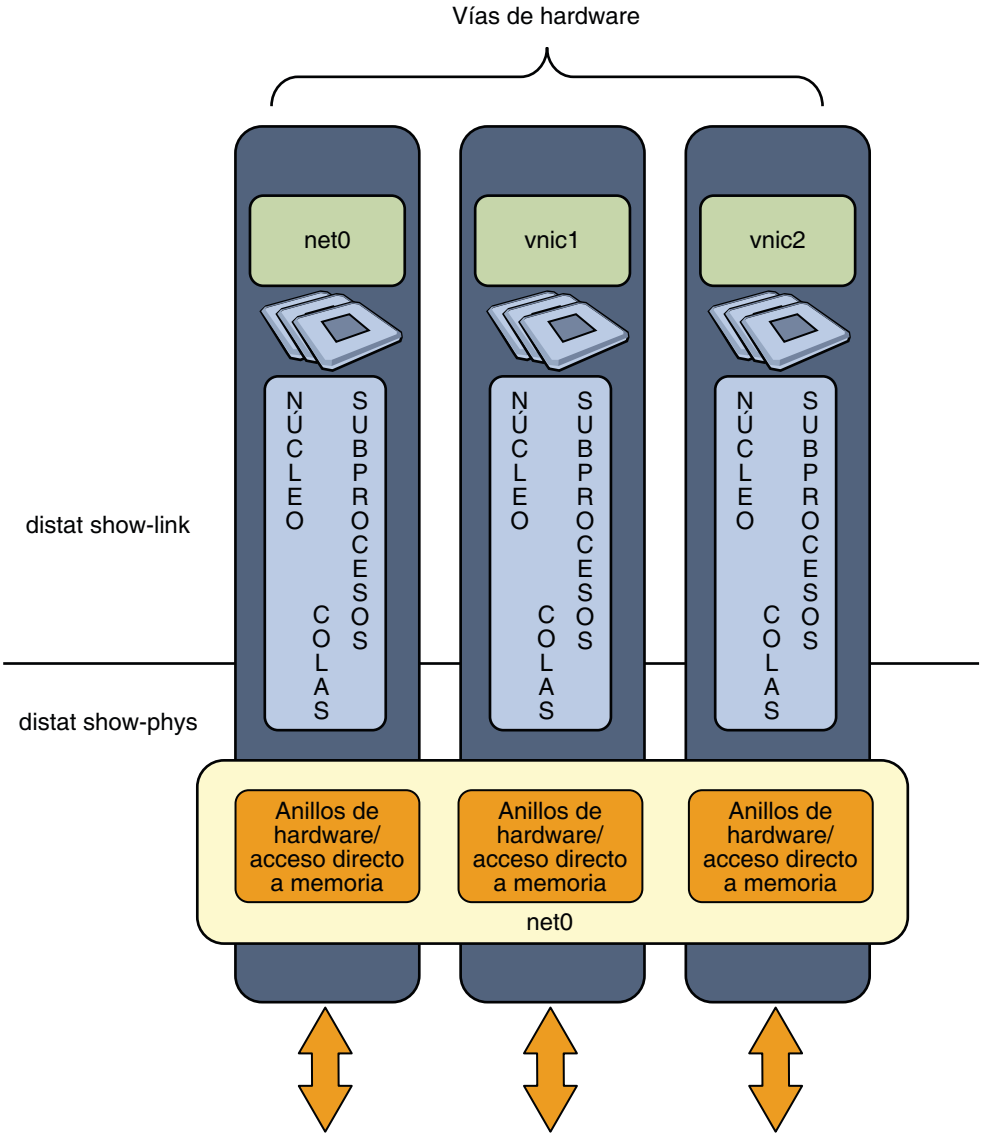
Nota – Los anillos de Rx y de Tx, y otros recursos de la red, se asignan mediante la configuración de las propiedades de enlaces de datos. Por lo tanto, los enlaces de datos son las vías de red de un sistema.

En las vías de hardware, los paquetes tienen el uso exclusivo de los anillos que se asignan a esas vías. Por el contrario, los anillos de las vías de software están compartidos por todos los paquetes de red en esas vías. Los enlaces de datos se configuran para compartir anillos por los siguientes motivos:

- Objetivo administrativo. Es posible que el enlace de datos no esté realizando procesos intensivos que requieran anillos dedicados.
- La NIC no admite la asignación de anillos.
- A pesar de la compatibilidad con la asignación de anillos, los anillos ya no están disponibles para ser asignados para uso exclusivo.

En la siguiente figura se muestran diferentes vías de hardware.

FIGURA 4–1 Vías de hardware



En la Figura 4–1 se muestra la siguiente configuración:

- Se configuran dos VNIC mediante `net0`: `vnic1` y `vnic2`. Como el cliente principal, `net0` también es la vía principal. Las VNIC como clientes secundarios también son vías de red.
- Se asignan conjuntos de anillos de hardware a los clientes secundarios. Cada cliente, incluido el cliente principal, funciona como una vía de hardware.

- Se asigna un conjunto de CPU a cada vía.

El en las secciones siguientes se describe cómo supervisar el tráfico que fluye por estas vías.

Comandos para supervisar las estadísticas de tráfico

Los comandos `dlstat` y `flowstat` permiten supervisar y obtener estadísticas sobre el tráfico de red en enlaces de datos y flujos, respectivamente. Estos comandos son equivalentes a los comandos `dladm` y `flowadm`. En la siguiente tabla se comparan las funciones del par de comandos `*adm` con las del par de comandos `*stat`.

Comandos administrativos		Comandos de supervisión	
Comando	**Función**	**Comando**	**Función**
Opciones del comando `dladm`	Interfaz de usuario y herramienta para configurar y administrar enlaces de datos	Opciones del comando `dlstat`	Interfaz de usuario y herramienta para obtener estadísticas sobre el tráfico en enlaces de datos
Opciones del comando `flowadm`	Interfaz de usuario y herramienta para configurar y administrar flujos	Opciones del comando `flowstat`	Interfaz de usuario y herramienta para obtener estadísticas sobre el tráfico en los flujos

En las secciones siguientes se describe cada comando de supervisión más detalladamente.

Recopilación de estadísticas sobre el tráfico de red en enlaces

Puede utilizar las siguientes variantes del comando `dlstat` para recopilar información sobre el tráfico de red.

Comando	Información proporcionada
`dlstat` [*link*] `dlstat -rt` [*link*] `dlstat show-link` [*link*]	Estadísticas de tráfico entrante y saliente por vía
`dlstat show-link -rt` [*link*]	Estadísticas de tráfico entrante y saliente por anillo por pista
`dlstat show-phys` [*link*]	Estadísticas de tráfico entrante y saliente por dispositivo físico de red

Comando	Información proporcionada
`dlstat show-phys -rt` [*link*]	Estadísticas de tráfico entrante y saliente por anillo por dispositivo físico de red
`dlstat show-aggr` [*link*] `dlstat show-aggr -rt` [*link*]	Estadísticas de tráfico entrante y saliente por puerto por agregación

Puede utilizar la opción `-r` o la opción `-t` del comando `dlstat` para restringir la información de las estadísticas a la recepción o a la transmisión, respectivamente. Asimismo, puede utilizar otras opciones con el comando `dlstat`. Para obtener más información, consulte la página del comando man `dlstat(1M)`.

Obtención de estadísticas de tráfico de red en dispositivos de red

El subcomando `dlstat show-phys` proporciona estadísticas que hacen referencia al dispositivo físico de red. Como se muestra en la Figura 4–1, el subcomando funciona en los anillos de hardware, que están en la capa de dispositivo de la pila de red. El subcomando equivalente `dladm show-phys` también funciona en el mismo nivel de la pila. Compare la Figura 4–1 con la pila de red que se muestra en "Implementación de Oracle Solaris 11" de *Introducción a redes de Oracle Solaris 11*.

En el ejemplo siguiente se muestran las estadísticas de todos los enlaces físicos del sistema:

```
# dlstat show-phys
 LINK    IPKTS     RBYTES    OPKTS     OBYTES
net0     2.14M   257.48M     3.19M    210.88M
net1     1.15M   120.32M     1.00M     98.70M
net2     1.10M   110.10M     1.28     183.00M
...
```

En la salida se muestran las estadísticas de tráfico entrante y saliente de cada enlace del sistema. Se muestra el número de paquetes y sus tamaños en bytes.

En el siguiente ejemplo, se muestran las estadísticas de recepción de todos los anillos de hardware de `net0`:

```
# dlstat show-phys -r net0
 LINK    TYPE       ID    INDEX     IPKTS      RBYTES
net0       rx    local       --         0           0
net0       rx       hw        1         0           0
net0       rx       hw        2     1.73M       2.61G
net0       rx       hw        3         0           0
net0       rx       hw        4     8.44M      12.71G
net0       rx       hw        5     5.68M       8.56G
net0       rx       hw        6     4.99M       7.38G
net0       rx       hw        7         0           0
```

En la segunda salida, el dispositivo `net0` tiene ocho anillos de recepción, que se identifican en el campo `INDEX`. Una distribución uniforme de paquetes por anillo constituye una configuración ideal que indica que los anillos están asignados correctamente a los enlaces según la carga de los enlaces. Una distribución desigual puede indicar una distribución desproporcionada de los anillos por enlace. La resolución de la distribución desigual depende de si la NIC admite la asignación dinámica de anillos. Si es así, puede redistribuir los anillos por enlace para procesar paquetes de manera más uniforme. Para obtener más información sobre la asignación dinámica de anillos, consulte "Trabajo con clientes, transmisión de anillos y recepción de anillos " en la página 31.

En el ejemplo siguiente se muestra información sobre el tráfico que se recibe en los dispositivos cada segundo. El intervalo se especifica mediante la opción `-i`. Para detener el refrescamiento de la visualización, presione Control-C.

```
# dlstat show-phys -r -i 1
LINK  TYPE   INDEX     IPKTS    RBYTES
net0    rx       0   101.91K    32.86M
net1    rx       0     9.61M    14.47G
net2    rx       8      336K         0
net0    rx       0         0         0
net1    rx       0    82.13K   123.69M
net2    rx       0         0         0
...
^C
```

En este ejemplo se muestra el uso de los anillos de transmisión para `net1` como un dispositivo de red.

```
# dlstat show-phys -t net1
LINK TYPE INDEX   OPKTS   OBYTES
net1   tx     0      44    3.96K
net1   tx     1       0        0
net1   tx     2   1.48M  121.68M
net1   tx     3   2.45M  201.11M
net1   tx     4   1.47M  120.82M
net1   tx     5       0        0
net1   tx     6   1.97M  161.57M
net1   tx     7   4.59M  376.21M
net1   tx     8   2.43M  199.24M
net1   tx     9       0        0
net1   tx     10  3.23M  264.69M
net1   tx     11  1.88M  153.96M
```

Obtención de estadísticas de tráfico de red en vías

El subcomando `dlstat show-link` proporciona estadísticas que hacen referencia a las vías configuradas mediante el enlace físico. Las vías están constituidas por los enlaces de datos. Como se muestra en la Figura 4–1, el subcomando funciona en la capa de enlace de datos de la pila de red. El subcomando equivalente `dladm show-link` también funciona en el mismo nivel de la pila. Compare la Figura 4–1 con la pila de red que se muestra en "Implementación de Oracle Solaris 11" de *Introducción a redes de Oracle Solaris 11*.

En el siguiente ejemplo, se muestran las estadísticas de tráfico de recepción de `vnic0`.

```
# dlstat show-link -r vnic0
 LINK  TYPE    ID  INDEX    IPKTS   RBYTES    INTRS    POLLS  IDROPS
vnic0    rx    hw      2    1.73M    2.61G    1.33M  400.22K       0
vnic0    rx    hw      4    8.44M   12.71G    4.35M    4.09M       0
```

En la salida anterior se muestran las estadísticas de tráfico para la vía `vnic0`. A esta vía se le han asignado dos anillos de recepción (anillo `2` y anillo `4`) para uso exclusivo. En la salida se muestra cómo se utilizan estos dos anillos para el tráfico de red entrante. Sin embargo, es posible que los datos también reflejen la implementación de otras asignaciones de recursos, como límites de ancho de banda y procesamiento de prioridades.

Suponga que se muestra la siguiente información para `net0`, la vía principal:

```
# dlstat show-link -r net0
LINK TYPE    ID INDEX   IPKTS  RBYTES    INTRS  POLLS  IDROPS
net0   rx local    --       0       0        0      0       0
net0   rx    sw    -- 794.28K   1.19G  794.28K      0       0
...
```

Según la salida, uno de los anillos de Rx, el anillo `0`, está compartido con otro cliente. Los anillos se comparten si los clientes secundarios se configuran sin ningún anillo asignado. Es posible que no se asigne un anillo por los siguientes motivos:

- Los clientes de hardware ya no están disponibles para ser creados mediante el enlace.
- Los anillos de hardware ya no están disponibles para su asignación.
- El administrador intencionadamente configura un cliente de software.

Las estadísticas de las interrupciones (`INTRS`) y los descartes (`*DROPS`) también son importantes. Un número bajo de interrupciones y cero descarte de paquetes indican una mayor eficacia en el rendimiento. Si los números de interrupciones o de descarte de paquetes son altos, es posible que deba agregar más recursos a la vía.

En el siguiente ejemplo se muestran las estadísticas de paquetes salientes en los anillos utilizados por `net1`, la vía principal. En la salida se muestra que `net1` utiliza todos los anillos de transmisión.

```
# dlstat show-link -t net1
LINK   TYPE   ID  INDEX    OPKTS    OBYTES   ODROPS
net1     tx   hw      0       32     1.44K        0
net1     tx   hw      1        0         0        0
net1     tx   hw      2    1.48M    97.95M        0
net1     tx   hw      3    2.45M   161.87M        0
net1     tx   hw      4    1.47M    97.25M        0
net1     tx   hw      5        0       276        0
net1     tx   hw      6    1.97M   130.25M        0
net1     tx   hw      7    4.59M   302.80M        0
net1     tx   hw      8    2.43M   302.80M        0
net1     tx   hw      9        0         0        0
net1     tx   hw      10   3.23M   213.05M        0
net1     tx   hw      11   1.88M   123.93M        0
```

El siguiente comando muestra el uso de estadísticas de recepción para el enlace `net1`. Además, con el uso de la opción `-F` en el comando, la salida también proporciona información de distribución. Específicamente, el recuento de distribuciones es de dos (`0` y `1`). El tráfico de red que se recibe en la vía de hardware que utiliza el anillo `0` se divide y se transmite mediante las dos distribuciones. Del mismo modo, el tráfico de red que se recibe en la vía de hardware que utiliza el anillo `1` también se divide y se reparte entre las dos distribuciones.

```
# dlstat show-link -r -F net1
LINK     ID   INDEX   FOUT   IPKTS
net1  local      --      0       0
net1     hw       0      0  382.47K
net1     hw       0      1       0
net1     hw       1      0  367.50K
net1     hw       1      1  433.24K
```

Obtención de estadísticas de tráfico de red en agregaciones de enlaces

El comando `dlstat show-aggr` muestra estadísticas de paquetes de red para cada puerto de agregación cuando el tráfico atraviesa la agregación en el sistema.

```
# dlstat show-aggr
 LINK            PORT    IPKTS   RBYTES    OPKTS   OBYTES
aggr1              --        0        0        0        0
aggr1            net0        0        0        0        0
aggr1            net1        0        0        0        0
```

La salida indica la configuración de una agregación de enlace `aggr1` con dos enlaces subyacentes, `net0` y `net1`. Como el tráfico de red es recibido o enviado por el sistema mediante la agregación, la información sobre los paquetes entrantes y salientes, y sus respectivos tamaños se indica para cada puerto. Los puertos son identificados por los enlaces subyacentes de la agregación.

Recopilación de estadísticas sobre tráfico de red en flujos

Las estadísticas de flujo ayudan a evaluar tráfico de paquetes en cualquier flujo definido del sistema. Para obtener información de flujo, utilice el comando `flowstat`. Para obtener más información sobre este comando, consulte la página del comando man `flowstat(1M)`.

A continuación se indica la sintaxis más utilizada del comando `flowstat`:

`# flowstat [-r|-t] [-i` *interval*`] [-l`** *link*`] [`*flow*`]`

`[-r|-t]` Muestra sólo las estadísticas de recepción (opción `-r`) o sólo las estadísticas de transmisión (opción `-t`). Para mostrar las estadísticas de la recepción y la transmisión, omita la opción.

`-i` *interval* — Especifica cada cuantos segundos desea que se refresquen las estadísticas mostradas. Si no utiliza esta opción, se muestra una salida estática.

`-l` *link* — Indica que desea supervisar las estadísticas de todos los flujos del enlace de datos especificado. Si no utiliza esta opción, se muestra la información sobre todos los flujos de todos los enlaces de datos.

flow — Indica que desea supervisar sólo las estadísticas del flujo especificado. Si no utiliza esta opción, según si ha especificado un enlace o no, se muestran todas las estadísticas de flujo.

En los ejemplos siguientes, se muestran distintas maneras de visualizar información sobre los flujos configurados en el sistema.

EJEMPLO 4–1 Visualización de estadísticas de tráfico de todos los flujos cada intervalos de un segundo

En este ejemplo se muestra información cada un segundo sobre el tráfico entrante y saliente en todos los flujos configurados en el sistema.

```
# flowstat -i 1
FLOW     IPKTS   RBYTES  IERRS    OPKTS  OBYTES  OERRS
flow1  528.45K  787.39M      0  179.39K  11.85M      0
flow2  742.81K    1.10G      0        0       0      0
flow3        0        0      0        0       0      0
flow1   67.73K  101.02M      0   21.04K    1.39M     0
flow2        0        0      0        0       0      0
flow3        0        0      0        0       0      0
...
^C
```

En este ejemplo, se muestran las estadísticas del tráfico saliente de todos los flujos configurados.

EJEMPLO 4–2 Visualización de las estadísticas de transmisión de todos los flujos

```
# flowstat -t
 FLOW    OPKTS   OBYTES   OERRS
flow1   24.37M    1.61G       0
flow2        0        0       0
flow1        4      216       0
```

EJEMPLO 4–3 Visualización de estadísticas de recepción de todos los flujos en un enlace especificado

En este ejemplo se muestra el tráfico entrante en las vías de hardware de todos los flujos que se crearon mediante el enlace de datos `net0`.

```
# flowstat -r -i 2 -l net0
    FLOW    IPKTS   RBYTES    IERRS
tcp-flow  183.11K  270.24M        0
udp-flow        0        0        0
tcp-flow  373.83K  551.52M        0
udp-flow        0        0        0
```

EJEMPLO 4–3 Visualización de estadísticas de recepción de todos los flujos en un enlace especificado *(Continuación)*

```
tcp-flow  372.35K  549.04M        0
udp-flow        0        0        0
tcp-flow  372.87K  549.61M        0
udp-flow        0        0        0
tcp-flow  371.57K  547.89M        0
udp-flow        0        0        0
tcp-flow  191.92K  282.95M        0
udp-flow  206.51K  310.70M        0
tcp-flow        0        0        0
udp-flow  222.75K  335.15M        0
tcp-flow        0        0        0
udp-flow  223.00K  335.52M        0
tcp-flow        0        0        0
udp-flow  160.22K  241.07M        0
tcp-flow        0        0        0
udp-flow  167.89K  252.61M        0
tcp-flow        0        0        0
udp-flow    9.52K   14.32M        0
^C
```

Configuración de contabilidad de red para el tráfico de red

Puede utilizar la utilidad de contabilidad ampliada para configurar la contabilidad de red en el sistema. La contabilidad de red implica capturar estadísticas sobre el tráfico de red en un archivo de registro. De esta forma, puede mantener registros de tráfico con fines de seguimiento, provisión, consolidación y facturación. Posteriormente, puede consultar el archivo de registro para obtener información histórica sobre el uso de la red durante un período determinado.

Para configurar la contabilidad de red, utilice el comando `acctadm` de la utilidad de contabilidad ampliada. Una vez que haya finalizado la configuración de la contabilidad de red, utilice el comando `flowstat` para registrar las estadísticas de tráfico.

En esta sección, se describen los siguientes procedimientos:

- "Cómo configurar la contabilidad de red" en la página 61
- "Cómo obtener estadísticas históricas del tráfico de la red" en la página 62

▼ Cómo configurar la contabilidad de red

1 **Conviértase en un administrador, en el sistema con las interfaces cuyo uso de red desea controlar.**

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 **Vea el estado de los tipos de contabilidad que se pueden activar mediante la utilidad de contabilidad ampliada.**

```
# acctadm [process | task | flow | net]
```

La utilidad de contabilidad ampliada puede activar cuatro tipos de contabilidad. Los operandos opcionales del comando `acctadm` corresponden a estos tipos de contabilidad. Para configurar un tipo de contabilidad específico, se utiliza un operando junto con el comando.

- Contabilidad de proceso
- Contabilidad de tarea
- Contabilidad de flujo para IPQoS
- Contabilidad de red para enlaces y flujos

Nota – La contabilidad de red también se aplica a los flujos que se gestionan mediante los comandos `flowadm` y `flowstat`, como se explicó en "Gestión de recursos en flujos" en la página 45. Por lo tanto, para configurar la contabilidad de estos flujos, utilice la opción `net` con el comando `acctadm`. *No* utilice la opción `flow`, que activa la contabilidad de flujo para configuraciones de IPQoS.

Si se especifica `net`, se muestra el estado de contabilidad de red. Si no se utiliza `net`, se muestra el estado de los cuatro tipos de contabilidad.

---

3 **Active la contabilidad ampliada para el tráfico de red.**

```
# acctadm -e extended -f filename net
```

Donde *nombre_archivo* incluye la ruta completa del archivo de registro que va a capturar las estadísticas del tráfico de red. El archivo de registro se puede crear en cualquier directorio que especifique.

4 **Verifique que la contabilidad de red ampliada esté activada.**

```
# acctadm net
```

Ejemplo 4–4 Configuración de la contabilidad de red en el sistema

En este ejemplo se muestra cómo configurar la contabilidad de red para capturar y visualizar la información histórica sobre el tráfico del sistema.

En primer lugar, vea el estado de todos los tipos de contabilidad de la siguiente manera:

```
# acctadm
            Task accounting: inactive
       Task accounting file: none
     Tracked task resources: none
   Untracked task resources: extended
         Process accounting: inactive
    Process accounting file: none
  Tracked process resources: none
Untracked process resources: extended,host
            Flow accounting: inactive
       Flow accounting file: none
     Tracked flow resources: none
   Untracked flow resources: extended
            Network accounting: inactive
       Network accounting file: none
     Tracked Network resources: none
   Untracked Network resources: extended
```

La salida muestra que la contabilidad de red no está activa.

A continuación, active la contabilidad de red ampliada.

```
# acctadm -e extended -f /var/log/net.log net
# acctadm net
            Net accounting: active
       Net accounting file: /var/log/net.log
     Tracked net resources: extended
   Untracked net resources: none
```

▼ Cómo obtener estadísticas históricas del tráfico de la red

Después de activar la contabilidad de red, puede utilizar los comandos `dlstat` y `flowstat` para extraer información del archivo de registro. En este procedimiento se describen los pasos.

Antes de empezar Para poder visualizar los datos históricos de la red, debe activar la contabilidad ampliada para la red. Además, para visualizar los datos históricos del tráfico en los flujos, primero, debe configurar los flujos del sistema como se explica en "Gestión de recursos en flujos" en la página 45.

1 Conviértase en un administrador, en el sistema con las interfaces cuyo uso de red desea controlar.

Para obtener más información, consulte "Cómo usar los derechos administrativos que tiene asignados" de *Administración de Oracle Solaris 11.1: servicios de seguridad*.

2 Para extraer y visualizar información histórica sobre el uso de los recursos en los enlaces de datos, utilice el siguiente comando:

```
# dlstat show-link -h [-a] -f filename [-d date] [-F format] [-s start-time] [-e end-time] [link]
```

`-h`	Muestra un resumen de la información histórica sobre el uso de los recursos por parte de los paquetes entrantes y salientes en los enlaces de datos.
`-a`	Muestra el uso de los recursos en todos los enlaces de datos, incluidos los que ya se suprimieron después de la captura de los datos.
`-f` *filename*	Especifica el archivo de registro que se definió al activar la contabilidad red con el comando `acctadm`.
`-d` *date*	Muestra la información registrada para la fecha especificada.
`-F` *format*	Muestra los datos en un formato específico que se puede trazar para el análisis. Actualmente, `gnuplot` es el único formato admitido.
`-s` *start-time*, `-e` *end-time*	Muestra la información registrada disponible para un rango de fecha y hora especificado. Utilice el formato `MM/DD/YYY,hh:mm:ss`. La `hora` (`hh`) debe utilizar la notación de reloj de 24 horas. Si no incluye la fecha, se muestran los datos del rango de tiempo especificado para la fecha actual.
link	Muestra los datos históricos para un enlace de datos determinado. Si no utiliza esta opción, se muestran los datos de red históricos para todos los enlaces de datos configurados.

3 Para extraer y visualizar información histórica sobre el tráfico de red en los flujos configurados, utilice el siguiente comando:

```
# flowstat -h [-a] -f filename [-d date] [-F format] [-s start-time] [-e end-time] [flow]
```

`-h`	Muestra un resumen de la información histórica sobre el uso de los recursos por parte de los paquetes entrantes y salientes en los flujos configurados.
`-a`	Muestra el uso de los recursos en todos los flujos configurados, incluidos los que ya se suprimieron después de la captura de los datos.
`-f` *filename*	Especifica el archivo de registro que se definió al activar la contabilidad red con el comando `acctadm`.
`-d`	Muestra la información registrada para la fecha especificada.
`-F` *format*	Muestra los datos en un formato específico. Actualmente, `gnuplot` es el único formato admitido.
`-s` *start-time*, `-e` *end-time*	Muestra la información registrada disponible para un rango de fecha y hora especificado. Utilice el formato `MM/DD/YYY,hh:mm:ss`. La `hora` (`hh`) debe

utilizar la notación de reloj de 24 horas. Si no incluye la fecha, se muestran los datos del rango de tiempo especificado para la fecha actual.

flow Muestra los datos históricos para un flujo especificado. Si no utiliza esta opción, se muestran los datos de red históricos para todos los flujos configurados.

Ejemplo 4–5 Visualización de información histórica sobre el uso de los recursos en enlaces de datos

En el siguiente ejemplo se muestran las estadísticas históricas del tráfico de red y el uso de los recursos por parte del tráfico de red en un enlace de datos especificado:

```
# dlstat show-link -h -f /var/log/net.log net0
 LINK  DURATION  IPACKETS RBYTES      OPACKETS OBYTES      BANDWIDTH
net0   80        1031     546908      0        0           2.44 Kbps
```

Ejemplo 4–6 Visualización de información histórica sobre el uso de los recursos en flujos

En los siguientes ejemplos se muestran diferentes maneras de visualizar estadísticas históricas sobre el tráfico de red en un flujo y su uso de recursos.

En el siguiente ejemplo se muestran las estadísticas históricas del uso de recursos por parte del tráfico en un flujo:

```
# flowstat -h -f /var/log/net.log
FLOW      DURATION  IPACKETS RBYTES      OPACKETS OBYTES      BANDWIDTH
flowtcp   100       1031     546908      0        0            43.76Kbps
flowudp   0         0        0           0        0            0.00Mbps
```

En el siguiente ejemplo se muestran las estadísticas históricas del uso de recursos por parte del tráfico en un flujo durante un determinado rango de fechas y horas:

```
# flowstat -h -s 02/19/2008,10:39:06 -e 02/19/2008,10:40:06 \
-f /var/log/net.log flowtcp

FLOW      START       END         RBYTES   OBYTES     BANDWIDTH
flowtcp   10:39:06    10:39:26    1546     6539        3.23 Kbps
flowtcp   10:39:26    10:39:46    3586     9922        5.40 Kbps
flowtcp   10:39:46    10:40:06    240      216       182.40 bps
flowtcp   10:40:06    10:40:26    0        0           0.00 bps
```

En el siguiente ejemplo se muestran las estadísticas históricas del uso de recursos por parte del tráfico en un flujo durante un determinado rango de fechas y horas. La información se muestra con el formato `gnuplot`.

```
# flowstat -h -s 02/19/2008,10:39:06 -e 02/19/2008,10:40:06 \
-F gnuplot -f /var/log/net.log flowtcp
# Time tcp-flow
```

```
10:39:06 3.23
10:39:26 5.40
10:39:46 0.18
10:40:06 0.00
```

Índice