Configuración y administración de componentes de red en Oracle® Solaris 11.2

Referencia: E53785
Julio de 2014

ORACLE®

Contenido

Uso de esta documentación

- **Descripción genera**: proporciona información acerca de cómo configurar y administrar varios componentes de red en el sistema operativo (SO) Oracle Solaris, como enlaces de datos, interfaces y direcciones IP, servicios de nombres y directorios, perfiles reactivos y redes inalámbricas.
- **Destinatarios**: administradores del sistema responsables de gestionar la configuración de la red en centros de datos corporativos.
- **Conocimientos necesarios**: comprensión básica y avanzada de conceptos y prácticas de administración de redes.

Biblioteca de documentación del producto

En la biblioteca de documentación (http://www.oracle.com/pls/topic/lookup?ctx=E56339), se incluye información de última hora y problemas conocidos para este producto.

Acceso a My 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.

Comentarios

Envíenos comentarios acerca de esta documentación mediante http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Acerca de la administración de redes en Oracle Solaris

En este capítulo, se proporciona una descripción general sobre los diferentes componentes que comprende la configuración de red de un sistema cliente de host en Oracle Solaris. Las tareas y los ejemplos que se describen en esta guía, presuponen que va a realizar la configuración de red después de una instalación. Para obtener instrucciones sobre la configuración de la red durante una instalación, consulte "Instalación de sistemas Oracle Solaris 11.2 ".

Para obtener información sobre las nuevas funciones de redes, consulte "Novedades de Oracle Solaris 11.2 ".

Para conocer las tareas de planificación que se deben llevar a cabo antes de configurar un sistema cliente en la red, consulte "Planificación de la implementación de red en Oracle Solaris 11.2 ".

Para obtener un acceso directo a los comandos de administración de red más utilizados, consulte el Capítulo 3, "Hoja de referencia del comando de administración de red" de "Estrategias de administración de redes en Oracle Solaris 11.2 ".

Para obtener información sobre la administración de redes TCP/IP, consulte el Capítulo 1, "Administración de redes TCP/IP" de "Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ".

Este capítulo se divide en los siguientes apartados:

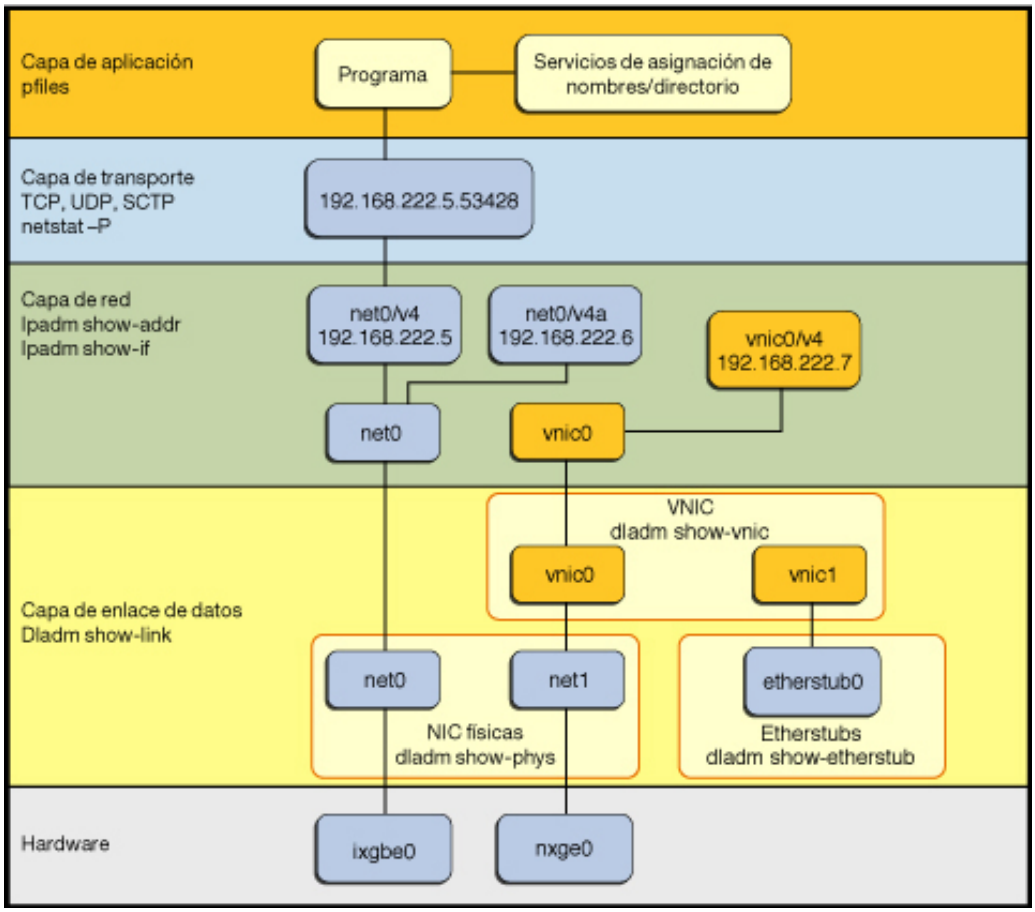
Descripción de la pila de protocolo de red de Oracle Solaris

Las interfaces de red proporcionan una conexión entre un sistema y una red. Estas interfaces se configuran mediante enlaces de datos que, a su vez, corresponden a instancias de dispositivos de hardware del sistema.

En Oracle Solaris 10, existe una relación uno a uno que enlaza el dispositivo, el enlace de datos y la interfaz, lo que significa que la configuración de red depende de la configuración del hardware y también de la topología de red. Si se implementan cambios en la capa de hardware, por ejemplo, el reemplazo de una tarjeta de interfaz de red (NIC), debe volver a configurar las interfaces en el sistema.

Sin embargo, en esta versión de Oracle Solaris, la asignación de nombres de enlaces de datos físicos ya no está enlazada al hardware subyacente asociado con el dispositivo de red. De manera predeterminada, a estos dispositivos se les asigna el nombre genérico `net` y un sufijo que refleja la ubicación física del dispositivo en el sistema, como se muestra en la Figura 1–1. Con esta separación, la configuración de red en la capa de red ya no estará vinculada al conjunto de chips ni a la topología de la red en la capa de hardware.

FIGURA 1-1 Pila de protocolo de red de Oracle Solaris 11



Esta implantación hace que la administración de red sea más flexible de las siguientes maneras:

- La configuración de red está aislada de los cambios que pueden ocurrir en la capa de hardware. Los valores de configuración de enlace e interfaz se conservan, aunque se haya eliminado el hardware subyacente. Estos mismos valores de configuración se pueden volver a aplicar a cualquier NIC de sustitución, siempre que las dos NIC sean del mismo tipo.
- La separación de la configuración de red de la configuración del hardware de red permite el uso de nombres de enlace personalizados en la capa del enlace de datos.
- Con la abstracción de la capa del enlace de datos, varias configuraciones o abstracciones de red, como las redes de área local virtuales (VLAN), las tarjetas de interfaz de red virtual

(VNIC), los dispositivos físicos, las agregaciones de enlaces y los túneles IP, se unifican en una entidad administrativa común, que es el enlace de datos.

Para comparar la pila de red de Oracle Solaris 10 con la pila de red de Oracle Solaris 11, consulte “Comparación de la pila de protocolo de red de Oracle Solaris 10 con la pila de protocolo de red de Oracle Solaris 11” de “Transición de Oracle Solaris 10 a Oracle Solaris 11.2 ”.

Capa de hardware

Los dispositivos de hardware de red también se denominan *tarjetas de interfaz de red (NIC)* o *adaptadores de red*. Las NIC pueden estar integradas y ya presentes en el sistema cuando se adquiere el sistema. También puede adquirir NIC independientes para agregar al sistema. Ciertas NIC tienen sólo una interfaz única que reside en la tarjeta. Otras marcas NIC pueden tener varias interfaces que usted puede configurar para realizar varias operaciones de red.

Capa de enlace de datos

Realice la configuración de red en la capa de enlace de datos con el comando `dladm`.

Los siguientes son algunos de los tipos de configuración de enlaces de datos que se pueden realizar en esta capa:

- Configuración de red básica de los enlaces físicos
- Configuración de VNIC (enlaces virtuales sobre enlaces físicos)

  Para configuración de VNIC, cada enlace virtual tiene su propia dirección MAC
- Configuración de agregación de enlaces

  Las agregaciones se configuran mediante enlaces físicos para ofrecer confiabilidad y rendimiento.
- Etherstubs para admitir redes de área local virtuales (VLAN)
- Puentes para compatibilidad con VLAN

Para obtener otros ejemplos, consulte “Gestión de enlaces de datos de red en Oracle Solaris 11.2 ”.

Capa de red

Realice la configuración de red en la capa de red con el comando `ipadm`.

Los siguientes son algunos de los tipos de configuración IP que puede realizar en esta capa:

- Configuración de interfaz de IP con nombres que tienen correspondencia uno a uno con nombres del enlace de datos
- Rutas múltiples de redes IP (IPMP)
- Interfaces de red virtual (VNI)
- Varias direcciones IP para una interfaz IP
- Direcciones IPv4 e IPv6 configurados en una sola interfaz IP
- Direcciones IP que se gestionan mediante sus nombres de objeto de dirección

  Un *nombre de objeto de dirección* está formado por el nombre de la interfaz seguido de una cadena única y representa una dirección IP configurada en el sistema.

Para obtener otros ejemplos, consulte las siguientes referencias:

- “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”
- “Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ”
- “Creación y uso de zonas de Oracle Solaris ”

Capa de transporte

En raras ocasiones, es necesario realizar configuración específica en la capa de transporte. Las aplicaciones que funcionan con Oracle Solaris normalmente seleccionan el protocolo de transporte apropiado y los números de puerto correspondientes de manera automática. Puede ver los puertos activos con el comando `netstat`. Consulte `netstat`(1M).

Puede ajustar algunos parámetros de protocolo de transporte con el comando `ipadm`. Consulte “Administración de servicios de capa de transporte” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ” y “Manual de referencia de parámetros ajustables de Oracle Solaris 11.2 ” para obtener más información.

Capa de aplicación

Los programas de aplicación acceden a la red mediante el las interfaces de programación de aplicaciones (API) del socket `xti` o `tli`. Estas API requieren que las aplicaciones cliente proporcionen la dirección IP del servidor y el número de puerto de transporte correspondientes al iniciar una conexión. Normalmente, el servidor sólo es conocido por un host remoto o el nombre de servicio en lugar de una dirección IP. Las aplicaciones utilizan los servicios de biblioteca estándar para convertir nombres de servicio y host en direcciones IP antes de intentar realizar conexiones de red.

Para obtener más información, consulte “Oracle Solaris 11.2 Programming Interfaces Guide ”.

Configuración de los servicios de nombres y directorio dentro de la pila de protocolo de red de Oracle Solaris

Los sistemas cliente deben tener un nombre de red y un servicio de directorio configurados para realizar búsquedas de direcciones IP. Según el entorno de red, el proceso de configuración se puede producir automáticamente durante el inicio del sistema o podría ser necesario realizarlo manualmente. Esta configuración tiene lugar en la capa de aplicación de la pila de red.

Para conocer las opciones de configuración de los servicios de nombres y directorios del lado del cliente, consulte el Capítulo 4, Administración de servicios de nombres y directorios en un cliente de Oracle Solaris.

Dispositivos de red y denominación de enlaces de datos en Oracle Solaris

Un enlace de datos representa un objeto de enlace en la segunda capa (L2) del modelo de interconexión de sistema abierto (OSI). El *enlace físico* está asociado directamente a un dispositivo y tiene un nombre de dispositivo. El nombre del dispositivo contiene el nombre del controlador y el número de instancia del dispositivo. El número de instancia puede tener un valor de 0 a *n*, según cuántas NIC utilice ese controlador en el sistema.

El nombre de la instancia del dispositivo sigue dependiendo del hardware subyacente del sistema. Sin embargo, las capas del hardware y del software están separadas, lo que significa que los enlaces de datos configurados en la parte superior de estos dispositivos ya no se vinculan de manera similar. Por lo tanto, a los enlaces de datos se les puede asignar un nombre distinto del nombre del dispositivo en el que están configurados.

De manera predeterminada, a los enlaces de datos se les asignan nombres genéricos que utilizan la convención de denominación net#, donde # es el número de instancia del dispositivo. Este número de instancia aumenta para cada dispositivo del sistema, por ejemplo `net0`, `net1`, `net2`, etc. Para obtener una descripción general más detallada, consulte “Acerca de la configuración de enlaces de datos” [23].

Acerca de los modos de configuración de red

Dos modos de configuración de red son compatibles en Oracle Solaris: fijo y reactivo.

Nota - Los términos modo fijo y reactivo hacen referencia a la capacidad del sistema para ajustarse automáticamente a los cambios en el entorno de red actual y no a si se pueden configurar direcciones IP estáticas o fijas cuando se utilizan en estos modos.

Modo fijo

Modo fijo significa que las instancias de una configuración en el sistema son persistentes, independientemente de si se producen cambios en las condiciones de red. Cuando se producen los cambios, como la agregación de interfaces, debe volver a configurar la red para que el sistema se adapte al entorno nuevo. Al utilizar un modo fijo, el sistema se configura con el mismo conjunto de comandos de configuración de red cada vez. Los servidores corporativos suelen utilizar este modo de configuración con más frecuencia, ya que tienen un entorno de red más estable. Al utilizar el modo fijo, utilice los comandos `dladm` y `ipadm` para gestionar los diferentes aspectos de la configuración de red. Consulte “Comandos de administración de red de Oracle Solaris” [18].

Modo reactivo

Por otro lado, el *modo reactivo* funciona cuando la red se configura automáticamente en respuesta a las condiciones actuales de la red. Este modo se utiliza principalmente para equipos personales portátiles y en situaciones en las que las condiciones de red pueden cambiar.

En el modo reactivo, un daemon de red (`nwamd`) supervisa el estado de las interfaces de red del sistema. Siempre que cambien las condiciones de la red, el daemon de red ajusta la configuración de red de manera dinámica. Por ejemplo, un equipo portátil podría estar conectado físicamente a la red corporativa o podría no estar conectado físicamente. Cuando está conectado físicamente, es probable que desactive la interfaz inalámbrica del equipo. Además, se suele recomendar hacer que la interfaz inalámbrica se active automáticamente al desconectar el cable Ethernet del equipo. También es posible que desee que el sistema ajuste automáticamente la configuración del filtro IP al cambiar a una red inalámbrica. El daemon de red puede realizar automáticamente estos tipos de cambios de configuración dinámica si se encuentra en el modo reactivo. Por el contrario, si está en el modo fijo, estos tipos de cambios requieren pasos de reconfiguración manual.

Acerca de la configuración de red basada en perfil

La configuración de red basada en perfil permite definir varias configuraciones alternativas, cada una identificada por un perfil único (denominado perfil de configuración de red [NCP]). Por ejemplo, puede crear un perfil llamado `office` para un equipo portátil que configura el sistema con ubicaciones de servidor DNS y direcciones IP estáticas. Un perfil alternativo

home podría usar DHCP para adquirir esta información. Un solo comando permite cambiar de un perfil a otro en cuestión de segundos. Los distintos tipos de perfiles que puede activar admiten dos posibles modos de configuración de red: fijo y reactivo. El modo predeterminado es establece mediante el perfil que se encuentre activo actualmente en el sistema.

Para obtener información sobre cómo se activan los perfiles en un sistema durante una instalación de Oracle Solaris, consulte “Configuración de la red durante una instalación” de “Transición de Oracle Solaris 10 a Oracle Solaris 11.2 ”.

Si no está seguro de qué perfil está activo actualmente en el sistema, utilice el comando `netadm list` para mostrar esta información. Para obtener información, consulte “Activación y desactivación de perfiles” [113].

Para obtener una descripción completa de los distintos tipos de perfiles compatibles en Oracle Solaris, consulte el Capítulo 5, Acerca de la administración de la configuración de red basada en perfiles en Oracle Solaris.

Comandos de administración de red de Oracle Solaris

Los siguientes comandos se utilizan para administrar la configuración de red:

- `dladm`
- `ipadm`
- `route`
- `netcfg`
- `netadm`

Comando `dladm`

Presentado en Oracle Solaris 10, `dladm` se utiliza para configurar enlaces de datos.

El comando `dladm` se utiliza para gestionar los siguientes tipos de configuración de red:

- **Interfaces físicas**: Ethernet, inalámbrica e InfiniBand
- **Funciones de redes virtuales**: Etherstubs, VNIC y túneles IP
- **Funciones de conmutador**: agregaciones de enlaces, VLAN y tecnologías de establecimiento de puentes
- **Características del dispositivo**: velocidad, función dúplex, prioridad y negociación de funciones

El comando `dladm` crea la configuración de red persistente para el perfil que está actualmente activo en el sistema. Por lo tanto, `net0` puede tener diferentes valores de MTU en diferentes perfiles. Por ejemplo, si un enlace de datos llamado `net0` está configurado con un valor de

unidad de transmisión máxima (MTU) específico de 1200, ese valor de MTU es persistente para `net0` sólo para ese perfil. Si, luego, activa otro perfil y define un valor de MTU diferente para ese perfil con el comando `dladm`, el nuevo valor de MTU se aplica sólo a ese perfil. Consulte el Capítulo 2, Administración de la configuración de enlaces de datos en Oracle Solaris.

El comando `dladm` también reemplaza el comando `ndd` que se utiliza para configurar las propiedades de protocolo en Oracle Solaris 10. Como herramienta utilizada para establecer propiedades de unidad de capa 2, el comando `dladm` ofrece las siguientes ventajas en comparación con el comando `ndd`. Consulte "Comparación del comando ndd con el comando ipadm" de "Transición de Oracle Solaris 10 a Oracle Solaris 11.2 ".

Comando `ipadm`

El comando `ipadm` reemplaza el comando `ifconfig` para configurar interfaces y direcciones IP en esta versión. El comando `ipadm` gestiona interfaces IP y direcciones IP de manera más eficaz porque el comando sólo se utiliza para la administración de la interfaz IP. Además, a diferencia del comando `ifconfig`, el comando `ipadm` implementa la configuración de red persistente. Consulte "Comparación del comando ifconfig con el comando ipadm" de "Transición de Oracle Solaris 10 a Oracle Solaris 11.2 ".

El comando `ipadm` también reemplaza el comando `ndd` que se utilizaba para configurar las propiedades de protocolo en Oracle Solaris 10. Como herramienta utilizada para establecer propiedades de protocolos, el comando `ipadm` ofrece varias ventajas en comparación con el comando `ndd`. Consulte "Comparación del comando ndd con el comando ipadm" de "Transición de Oracle Solaris 10 a Oracle Solaris 11.2 ".

Comando `route`

Dado que el archivo `/etc/defaultrouter` no se admite en Oracle Solaris 11, ya no puede gestionar las rutas (predeterminadas o no) mediante la edición de este archivo. En su lugar, utilice el comando `route` para manipular las tablas de enrutamiento del sistema manualmente. El comando `route` manipula rutas para el perfil activo *solamente*. La ruta predeterminada, así como todas las demás rutas, podrían ser reemplazadas si cambia el perfil activo. Este problema no debe generar ninguna preocupación si no cambia los perfiles del sistema.

Para obtener más información, consulte "Creación de rutas persistentes (estáticas)" [64].

Comandos `netcfg` y `netadm`

Los comandos `netcfg` y `netadm` se utilizan para gestionar diferentes tipos de perfiles. La mayoría de las funciones proporcionadas por estos dos comandos son tratadas en la gestión de

perfiles reactivos. El comando `netcfg` raramente se utiliza en servidores corporativos. Estos tipos de servidores se suelen utilizar el modo fijo.

El comando `netadm` se utiliza para activar y desactivar perfiles y mostrar información sobre los perfiles y sus estados. Consulte “Activación y desactivación de perfiles” [113] y “Administración de perfiles” [128].

Nota - Normalmente, se configuran las propiedades de perfiles reactivos mediante el comando `netcfg`. Sin embargo, también puede crear configuración persistente para un perfil reactivo con los comandos `dladm` y `ipadm`, si el perfil está activo actualmente. Sin embargo, no puede utilizar el comando `netcfg` para configurar el perfil `DefaultFixed`, que es el único perfil fijo del sistema. Para obtener más información, consulte la página del comando man `netcfg`(1M).

Comandos para volver a configurar la red del sistema

Otra opción que está disponible para volver a configurar la red del sistema es la utilidad `sysconfig`, también denominada herramienta interactiva de configuración del sistema (SCI). La herramienta SCI admite la configuración de sistemas recién instalados o no configurados, y está diseñada para proporcionar la configuración del sistema de zonas no globales recién creadas durante las instalaciones de texto. Puede utilizar la herramienta SCI de manera interactiva o no interactiva.

Puede realizar tres operaciones con la utilidad `sysconfig`: anulación de la configuración, configuración y creación de perfil. El subcomando `unconfigure` se utiliza para anular la configuración de un sistema completo. Este comando deja el sistema en estado no configurado.

El subcomando `configure` se utiliza para volver a configurar un sistema completo o parte del sistema, que incluye las siguientes seis agrupaciones funcionales:

- `network`
- `location`
- `users`
- `identity`
- `support`
- `kdb_layout`

Para obtener más información sobre los valores predeterminados para las agrupaciones, consulte “Descripción general de agrupaciones funcionales” de “Instalación de sistemas Oracle Solaris 11.2 ”.

Por ejemplo, puede volver a configurar los servicios de nombres existentes de un sistema de la siguiente manera:

```
# sysconfig configure -g network,naming_services
```

La opción -g se utiliza para especificar una agrupación funcional determinada que se debe configurar. En este ejemplo, el componente de red del sistema está configurado.

Para obtener más información, consulte la página del comando man `sysconfig`(1M) y el Capítulo 6, “Anulación de configuración o reconfiguración de una instancia de Oracle Solaris” de “Instalación de sistemas Oracle Solaris 11.2 ”.

Información necesaria para configurar sistemas cliente en la red

Puede configurar la red durante la instalación de Oracle Solaris o después. Este manual describe las tareas para configurar sistemas cliente en la red después de una instalación. Para obtener instrucciones sobre la configuración de la red durante una instalación, consulte “Instalación de sistemas Oracle Solaris 11.2 ”.

Para configurar los sistemas cliente de la red, debe proporcionar la siguiente información:

- Nombre del host
- Dirección IP
- Máscara de red

  Para obtener más información, consulte “Cómo decidir el formato de las direcciones IP para la red” de “Planificación de la implementación de red en Oracle Solaris 11.2 ” y “Cómo obtener el número de IP de la red” de “Planificación de la implementación de red en Oracle Solaris 11.2 ”.

  Si su red está dividida en subredes, debe contar con los números de subred y el esquema de direcciones IP que se aplicarán a los sistemas en cada subred, incluidas sus respectivas máscaras de red. Consulte “Uso de subredes en la red” de “Planificación de la implementación de red en Oracle Solaris 11.2 ”.
- Nombre de dominio al que pertenece el sistema

  Consulte “Uso de entidades de denominación en la red” de “Planificación de la implementación de red en Oracle Solaris 11.2 ”.
- Dirección del enrutador predeterminado

  Esta información se facilita en caso de tener una topología de red simple con un único enrutador conectado a cada red. Consulte “Planificación de enrutadores en la red” de “Planificación de la implementación de red en Oracle Solaris 11.2 ”.

  También se facilita esta información si los enrutadores no ejecutan protocolos de enrutamiento como RDISC (Router Discovery Server Protocol) o RIP (Router Information Protocol). Para obtener más información sobre los enrutadores y una lista de los protocolos de enrutamiento compatibles con Oracle Solaris, consulte “Protocolos de enrutamiento” de “Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ”.

Al configurar sistemas cliente en la red, consulte la información de "Topología de sistemas autónomos IPv4" de "Planificación de la implementación de red en Oracle Solaris 11.2 ".

Para obtener información detallada acerca de cada uno de estos componentes y las tareas relacionadas, consulte el Capítulo 1, "Planificación de la implementación de red" de "Planificación de la implementación de red en Oracle Solaris 11.2 ".

Dónde encontrar más información acerca de la administración de redes en Oracle Solaris

Además de la información de configuración básica que se describe en este manual, puede consultar las siguientes referencias para obtener información acerca de otros tipos de administración de red:

- Para personalizar protocolos de red y administrar servicios de capa de transporte, consulte el Capítulo 1, "Administración de redes TCP/IP" de "Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ".
- Para configurar un sistema como enrutador o equilibrador de carga, consulte "Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ".
- Para realizar tareas avanzadas de configuración IP y de enlaces de datos, incluida la agregación de enlaces y varios tipos de puentes, consulte "Gestión de enlaces de datos de red en Oracle Solaris 11.2 ".
- Para configurar grupos IPMP y túneles IP, consulte "Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ".
- Para establecer la seguridad de la red, consulte "Protección de la red en Oracle Solaris 11.2 ".
- Para implementar las funciones de virtualización de red, consulte "Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ".

♦ ♦ ♦ CAPÍTULO 2

Administración de la configuración de enlaces de datos en Oracle Solaris

En este capítulo, se describen los dispositivos de red y los enlaces de datos, y se incluyen las tareas para gestionar la configuración básica de los enlaces de datos con el modo fijo.

La siguiente información pertenece exclusivamente a la configuración de enlaces físicos o enlaces que representan los dispositivos de red. Para obtener más información acerca de otras entidades de la capa 2 (L2) que puede configurar, consulte "Gestión de enlaces de datos de red en Oracle Solaris 11.2 " y "Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ".

Este capítulo se divide en los siguientes apartados:

Acerca de la configuración de enlaces de datos

Los administradores crean interfaces IP sobre enlaces de datos. Cada enlace de datos representa un objeto de enlace en la segunda capa del modelo de interconexión de sistema abierto (OSI). Los enlaces de datos pueden representar varias entidades de L2 diferentes, como dispositivos de red física (llamados *enlaces físicos*), agregaciones de enlaces de datos físicos, tarjetas de interfaz de red virtual (VNIC), etc.

Los nombres de enlace se asignan cuando el objeto de enlace asociado se crea automáticamente o puede asignarlos explícitamente al crear los enlaces de datos. Los enlaces físicos (aquellos que están asociados con los dispositivos de red física) se crean automáticamente cuando se agregan dispositivos o cuando un sistema Oracle Solaris se inicia por primera vez después de una instalación. En esta versión de Oracle Solaris, la asignación de nombres de enlaces de datos físicos ya no está enlazada al hardware subyacente asociado con el dispositivo de red. De forma predeterminada, a los enlaces de datos se les asignan nombres que tienen el prefijo `net` y un número que refleja la unificación física del enlace de datos en el sistema como

sufijo. Por ejemplo, el primer dispositivo de red integrado `e1000g0` recibiría el nombre `net0`, mientras que el siguiente dispositivo `e1000g1` recibiría el nombre `net1`, y así sucesivamente. Puede asignar nombres arbitrarios a enlaces de datos que usted de forma explícita, por ejemplo, las agregaciones de enlaces. Además, si lo desea, puede cambiar explícitamente el nombre asignado de forma predeterminada `net`*N* de un enlace de datos.

Los nombres de enlace genéricos o flexibles ofrecen las siguientes ventajas para la configuración de red:

- Dentro de un único sistema, la reconfiguración dinámica (DR) resulta más fácil. La configuración de red para una NIC determinada puede ser heredada por una sustitución de NIC diferente.
- La configuración de red para la migración de zonas se hace menos complicada. La zona en el sistema migrado mantiene su configuración de red, si el enlace del sistema de destino comparte el mismo nombre que el enlace que se asignó a la zona antes de la migración. Por lo tanto, no se requiere ninguna configuración de red adicional para la zona después de la migración.
- La convención de denominación genérica hace que la configuración de red que se especifica en manifiesto de configuración del sistema (SC) utilizada durante una instalación sea menos complicada. Debido a que el enlace de datos de red principal es nombrado genéricamente `net0` para todos los sistemas, puede utilizar un manifiesto de SC genérico para varios sistemas que especifiquen una configuración para `net0`.
- La administración de enlaces de datos también se vuelve flexible. Puede personalizar aún más los nombres de los enlaces de datos, por ejemplo, para reflejar una función específica para la que sirve el enlace de datos.

  En la siguiente tabla se muestra la nueva correspondencia entre el hardware (NIC), la instancia de dispositivo, el nombre del enlace y la interfaz sobre el enlace. El sistema operativo proporciona los nombres de los enlaces de datos de manera automática.

Hardware (NIC)	Instancia de dispositivo	Nombre asignado del enlace	Interfaz IP
`e1000g`	`e1000g0`	`net0`	`net0`
`igb`	`ixgbe`	`net1`	`net1`

  Como se indica en esta tabla, mientras que el nombre de la instancia del dispositivo permanece basado en hardware, los enlaces de datos reciben otro nombre por parte del sistema operativo después de la instalación.

Para mostrar la asignación entre los enlaces de datos, sus nombres genéricos y las instancias de dispositivo correspondientes, utilice el subcomando `dladm show-phys` de la siguiente manera:

```
# dladm show-phys
LINK     MEDIA        STATE     SPEED     DUPLEX     DEVICE
net2     Ethernet     up        1000      full       bge2
net0     Ethernet     up        1000      full       e1000g0
```

```
net3     Ethernet     up        1000      full      nge3
net1     Ethernet     up        1000      full      e1000g1
```

Asignación de nombres genéricos a enlaces de datos

- Los dispositivos de red físicos se ordenan según el tipo de medio físico, donde determinados tipos tienen prioridad sobre otros. Los tipos de medio se ordenan en prioridad descendente de la siguiente manera:

  1. Ethernet
  2. Dispositivos InfiniBand
  3. Ethernet mediante IB
  4. WiFi
- Una vez que los dispositivos se agrupan y se ordenan según los tipos de medio, estos dispositivos se vuelven a ordenar en función de su ubicación física, teniendo en cuenta que se priorizan los dispositivos de la placa sobre los dispositivos periféricos.
- A los dispositivos que tienen una mayor prioridad según su tipo de medio y su ubicación se les asignan números de instancia más bajos.

En los sistemas basados en SPARC, se asignan los nombres net*N* para que coincidan con los alias de dispositivo net*N* que se utilizan en OpenBoot PROM (OBP). En sistemas basados en x86, se utilizan los datos SMBIOS (cuando están disponibles) para identificar dispositivos Ethernet integrados y asignarlos a `net0`, `net1`, etc. Además de estas fuentes de información (o ante la ausencia de ellas), los dispositivos de placa madre o placa de E/S, puente de host, complejo de raíz PCIe, bus, dispositivo y función inferiores se clasifican por encima de los demás dispositivos y reciben instancias de `net` inferiores que los que se encuentran en placas madres, puentes host, etc. superiores

Para mostrar las correspondencias entre los nombres de enlaces, los dispositivos y las ubicaciones, utilice el comando `dladm show-phys` con la opción `-L` como se indica a continuación:

```
# dladm show-phys -L
LINK         DEVICE       LOCATION
net0         e1000g0      MB
net1         e1000g1      MB
net2         e1000g2      MB
net3         e1000g3      MB
net4         ibp0         MB/RISER0/PCIE0/PORT1
net5         ibp1         MB/RISER0/PCIE0/PORT2
net6         eoib2        MB/RISER0/PCIE0/PORT1/cloud-nm2gw-2/1A-ETH-2
net7         eoib4        MB/RISER0/PCIE0/PORT2/cloud-nm2gw-2/1A-ETH-2
```

Personalización del modo en que el sistema operativo asigna nombres de enlaces genéricos

Atención - Debe personalizar el modo en que se asignan automáticamente nombres de enlaces genéricos *antes* de instalar Oracle Solaris. Después de la instalación, ya no podrá personalizar los nombres de enlace predeterminado sin eliminar las configuraciones existentes.

Oracle Solaris utiliza el prefijo `net` al asignar nombres de enlaces. Sin embargo, puede utilizar cualquier prefijo personalizado que desee, como `eth`. También puede desactivar la asignación automática de nombres de enlace genéricos.

Para desactivar la asignación automática de nombres de enlaces o para personalizar el prefijo de los nombres de enlaces, defina la siguiente propiedad en los manifiestos de configuración del sistema (SC). Los manifiestos de SC son utilizados por la función Automated Installer (AI) de Oracle Solaris.

```
<service name="network/datalink-management"
version="1" type="service">
<instance name="default enabled="true">
<property_group name='linkname-policy'
type='application'>
<propval name='phys-prefix' type='astring'
value='net'/>
</property_group>
</instance>
</service
```

De forma predeterminada, el valor para la propiedad `phys-prefix` se configura en `net`, como se muestra en negrita en la salida anterior.

- Para desactivar la asignación automática de nombres, establezca el valor para la propiedad `phys-prefix` en una cadena vacía, por ejemplo:

  ```
  <propval name='phys-prefix' type='astring' value=''/>
  ```

  Si desactiva de asignación automática de nombres, los nombres de los enlaces de datos se basan en sus controladores de hardware asociados, por ejemplo,`bge0`, `e1000g0`, etc.
- Para utilizar un prefijo distinto de `net`, especifique un nuevo prefijo como el valor de `phys-prefix`, como `eth`.

Si el valor que se proporciona para la propiedad `phys-prefix` no es válido, ese valor se ignora. Entonces, los enlaces de datos se denominan según sus controladores de hardware asociados, como `bge0`, `e1000g0`, etc. Para ver las reglas sobre los nombres de enlaces válidos, consulte “Reglas para nombres de enlaces válidos” [28].

Nombres de enlace en sistemas actualizados

En los sistemas instalados recientemente, los enlaces de datos reciben automáticamente el nombre de `net0` mediante `net`*N-1*, donde *N* representa el número total de dispositivos de red.

Por el contrario, si se actualiza desde otra versión de Oracle Solaris 11, los enlaces de datos conservan los nombres establecidos antes de la actualización. Estos nombres son nombres basados en hardware predeterminados o nombres personalizados, asignados por el administrador a los enlaces de datos antes de la actualización. Asimismo, en estos sistemas actualizados, los dispositivos de red nuevos que se agreguen posteriormente también conservarán los nombres basados en hardware predeterminados en lugar de recibir nombres genéricos. Este comportamiento para sistemas actualizados garantiza que los nombres genéricos asignados por el sistema operativo no se mezclen con otros nombres basados en hardware o nombres personalizados asignados por el administrador antes de la actualización.

Puede reemplazar los nombres basados en hardware y los nombres de enlaces proporcionados por el sistema operativo por otros nombres que usted prefiera usar. Normalmente, los nombres de enlaces predeterminados que asigna el sistema operativo bastan para crear la configuración de red del sistema. Sin embargo, tenga en cuenta la siguiente información antes de realizar cambios en los nombres de enlaces.

Reemplazo de nombres de enlaces basados en hardware

Si los enlaces de su sistema tienen nombres basados en hardware, cambie el nombre de estos enlaces, al menos, por nombres genéricos. Si conserva los nombres basados en hardware, es posible que surjan confusiones cuando se eliminen o se reemplacen estos dispositivos físicos.

Por ejemplo, se conserva el nombre de enlace `bge0` asociado con el dispositivo `bge0`. Todas las configuraciones de enlace hacen referencia al nombre de enlace. Más tarde, se reemplaza la NIC `bge` por la NIC `e1000g`. Para volver a aplicar la configuración de enlace del dispositivo anterior a la nueva NIC `e1000g0`, debería volver a asignar el nombre de enlace `bge0` a `e1000g0`. La combinación de un nombre de enlace basado en hardware `bge0` con una NIC `e1000g0` asociada diferente puede generar confusión. Si se utilizan nombres que no se basan en el hardware, se pueden distinguir mejor los enlaces de los dispositivos asociados.

Precaución para el cambio de nombres de enlaces

Aunque el reemplazo de nombres de enlaces basados en hardware se considera una buena práctica, tendrá que planificar con cuidado antes de cambiar el nombre de los enlaces. Cuando se cambia el nombre de enlace de un dispositivo, el nuevo nombre no se propaga automáticamente a todas las configuraciones asociadas existentes. En los siguientes ejemplos se ilustran los riesgos de cambiar los nombres de enlace:

- Algunas reglas de una configuración de filtro IP se aplican a enlaces específicos. Cuando se cambia el nombre de un enlace, las reglas de filtro siguen haciendo referencia al nombre original del enlace. Por lo tanto, estas reglas ya no se comportan del modo esperado una vez que se cambia el nombre del enlace. Debe ajustar las reglas de filtro para que se apliquen al enlace mediante el nuevo nombre del enlace.
- Considere la posibilidad de exportar la información de configuración de la red. Como se explicó anteriormente, si se utilizan los nombres predeterminados `net#` proporcionados por el sistema operativo, es posible migrar zonas y exportar fácilmente la configuración de red a otro sistema. Si a los dispositivos de red del sistema de destino se les asignan nombres genéricos, como `net0`, `net1`, etc., la zona simplemente hereda la configuración de red del enlace de datos cuyo nombre coincide con el enlace de datos asignado a la zona.

Por lo tanto, como regla general, no cambie el nombre de los enlaces de datos de forma aleatoria. Cuando cambie el nombre de los enlaces de datos, asegúrese de que todas las configuraciones asociadas del enlace se sigan aplicando después de que se haya cambiado el nombre del enlace.

Algunas de las configuraciones que podrían verse afectadas por el cambio de nombre del enlace son las siguientes:

- Reglas de filtro IP
- Configuraciones IP que se especifican mediante el comando `ipadm`
- Zonas de Oracle Solaris 11
- Configuración de `autopush`

Nota - No es necesario realizar ningún cambio en la configuración de `autopush` al cambiar el nombre de los enlaces. Sin embargo, debe observar el modo en que funciona la configuración con la propiedad `autopush` por enlace una vez que se ha cambiado el nombre. Para obtener más información, consulte Establecimiento del módulo STREAMS en enlaces de datos.

Reglas para nombres de enlaces válidos

Al asignar nombres de enlaces, tenga en cuenta las siguientes reglas:

- Los nombres de enlace deben constar de una cadena y un número de *punto físico de conexión* (PPA).
- El nombre del enlace debe respetar las siguientes restricciones:
  - Los nombres idealmente deben tener entre 3 y 8 caracteres. Sin embargo, los nombres pueden tener un máximo de 16 caracteres.
  - Los caracteres válidos para los nombres son los caracteres alfanuméricos (de la "a" a la "z" y del "0" al "9") y el carácter de subrayado (_).

Atención - No utilice letras mayúsculas en los nombres de enlaces.

- Cada enlace de datos debe tener sólo un nombre de enlace al mismo tiempo.
- Cada enlace de datos debe tener un nombre de enlace único dentro del sistema.

Nota - Una restricción adicional indica que no se puede utilizar `lo0` como nombre de enlace flexible. Este nombre está reservado para identificar la interfaz de bucle de retorno IP.

La función del enlace dentro de la configuración de la red puede ser la de una referencia útil al asignar nombres de enlaces. Por ejemplo, `netmgt0` puede ser un enlace dedicado a la gestión de red. `Upstream2` puede ser el enlace que se conecta con el ISP. Como regla general, para evitar confusiones, *no* asigne nombres de dispositivos conocidos a los enlaces.

Administración de propiedades de enlaces de datos

El uso del comando `dladm` para personalizar propiedades de enlace de datos comunes proporciona las siguientes ventajas:

- El comando `dladm` es la única interfaz de comandos que se necesita para configurar las propiedades del controlador de red. Este comando reemplaza la práctica anterior de usar una combinación del comando `ndd` y las modificaciones del archivo `driver.conf` para configurar las propiedades del controlador.
- Se utiliza la siguiente sintaxis uniforme, independientemente de qué propiedades se hayan definido:

  `dladm` *subcommand properties datalink*
- El uso del comando `dladm` se aplica tanto a propiedades públicas como privadas del controlador.
- El uso del comando `dladm` en un controlador específico no interrumpe conexiones de red de otras NIC de tipos similares. Por lo tanto, puede configurar propiedades de enlaces de datos dinámicamente.
- Los valores de configuración de enlaces de datos se almacenan en un repositorio `dladm` y se mantienen después de reiniciar el sistema.

Visualización de información general acerca de los enlaces de datos

Cuando se utiliza sin ninguna opción, el comando `dladm` muestra información general acerca de los enlaces de datos del sistema, incluida la clase, el estado y los enlaces físicos subyacentes.

```
# dladm
LINK        CLASS     MTU     STATE     OVER
net0        phys      1500    unknown   --
net1        phys      1500    up        --
net2        phys      1500    unknown   --
net3        phys      1500    unknown   --
net4        phys      1500    up        --
aggr0       aggr      1500    up        net1,net4
```

Los enlaces físicos pueden ser de diferentes clases que no sean enlaces físicos, por ejemplo agregaciones de enlaces, LAN virtuales (VLAN) y NIC virtuales (VNIC). Estos otros enlaces de datos también se incluyen en la información predeterminada que muestra el comando `dladm`. Por ejemplo, en la salida anterior se configura una agregación de enlace (`aggr0`) sobre los enlaces de datos físicos `net1` y `net4`.

Para obtener información acerca de las agregaciones de enlaces y las VLAN, consulte "Gestión de enlaces de datos de red en Oracle Solaris 11.2 ". Para obtener más información acerca de las VNIC, consulte "Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ".

Visualización de los enlaces de datos de un sistema

Utilice el comando `dladm show-link` para visualizar los enlaces de datos físicos y virtuales en un sistema. Un sistema tiene la misma cantidad de enlaces de datos que de NIC instaladas. Puede utilizar diversas opciones con este comando para personalizar la información que se muestra.

Cuando se utiliza sin opciones adicionales o argumentos, el comando `dladm show-link` muestra la siguiente información:

```
# dladm show-link
LINK                CLASS     MTU    STATE    OVER
net1                phys      1500   down     --
net3                phys      1500   unknown  --
net0                phys      1500   up       --
net2                phys      1500   unknown  --
net11               phys      1500   up       --
net5                phys      1500   up       --
net6                phys      1500   up       --
```

En la salida anterior, la columna `STATE` muestra el estado actual del *enlace de datos virtual*. El estado puede ser `up`, `down` o `unknown`. Para enlaces de datos virtuales, cuando una NIC se divide en varias VNIC, se crea de manera implícita e interna un conmutador. Esta creación de un conmutador virtual permite que las VNIC y el enlace de datos principal se comuniquen entre sí, siempre que estén en la misma VLAN, incluso si el enlace de datos físico no tiene conexión con la red externa. Esta relación forma el *estado virtual* del enlace de datos.

Utilice la opción `-P` para visualizar la información de configuración persistente sobre los enlaces de datos. Según la información proporcionada por este comando, se puede seguir configurando la red. Por ejemplo, se puede determinar la cantidad de NIC del sistema, y se puede seleccionar el enlace de datos que se va a utilizar y mediante el cual se pueden configurar las interfaces IP. Cuando escribe el comando, la información que se muestra es similar a la del siguiente ejemplo:

```
# dladm show-link -P
LINK        CLASS     OVER
net0        phys      --
net1        phys      --
net2        phys      --
```

En el ejemplo anterior, se muestra que un sistema tiene tres enlaces de datos que se asocian directamente a su NIC física correspondiente. No existe ningún enlace de datos especial, como agregaciones o NIC virtual, configurado por medio de los enlaces de datos con la clase `phys`.

Visualización de los atributos físicos de enlaces de datos

Utilice el comando `dladm show-phys` para obtener información acerca de los enlaces de datos del sistema respecto de las NIC físicas a las que están asociados. Si se utiliza sin opciones, el comando muestra información similar a la del siguiente ejemplo:

```
# dladm show-phys
LINK        MEDIA          STATE     SPEED     DUPLEX     DEVICE
net0        Ethernet       up        100Mb     full       e1000g0
net1        Ethernet       down      0Mb       --         nge0
net2        Ethernet       up        100Mb     full       bge0
net3        InfiniBand     --        0Mb       --         ibd0
```

En la salida anterior, se muestran, entre otros detalles, las NIC físicas con las que están asociados los enlaces de datos con nombres de enlace genéricos. Por ejemplo, `net0` es el nombre del enlace de datos de la NIC `e1000g0`. Para ver información sobre los indicadores establecidos para los enlaces de datos, utilice la opción `-P`. Por ejemplo, un enlace de datos marcado con el indicador `r` indica que su NIC subyacente ha sido eliminada.

En la salida anterior, la columna `STATE` muestra el estado actual del *enlace de datos virtual*. El estado puede ser `up`, `down` o `unknown`. El estado del enlace físico identifica si el dispositivo

físico tiene conectividad con la red externa (el cual tiene si el cable está conectado y el estado del puerto del otro extremo del cable es `up`).

La opción `-L` es otra opción útil que puede usar. Esta opción, muestra la ubicación física de cada enlace de datos. La ubicación determina el número de instancia del enlace de datos, como `net0`, `net1`, y así sucesivamente.

```
# dladm show-phys -L
LINK     DEVICE     LOCATION
net0     bge0       MB
net2     ibp0       MB/RISER0/PCIE0/PORT1
net3     ibp1       MB/RISER0/PCIE0/PORT2
net4     eoib2      MB/RISER0/PCIE0/PORT1/cloud-nm2gw-2/1A-ETH-2
```

Utilice la opción `-m` para mostrar las direcciones MAC de los enlaces físicos de un sistema:

```
# dladm show-phys -m
LINK                SLOT     ADDRESS            INUSE CLIENT
net0                primary  0:11:22:a9:ee:66   yes   net0
```

Este comando es similar a utilizar el comando `ifconfig`.

Visualice las direcciones MAC de todos los enlaces de un sistema, físicos y no físicos, de la siguiente manera:

```
# dladm show-linkprop -p mac-address
LINK     PROPERTY        PERM VALUE        EFFECTIVE    DEFAULT   POSSIBLE
net0     mac-address     rw   0:11:22:a9:ee:66 0:11:22:a9:ee:66 0:11:22:a9:ee:66
--
```

Eliminación de un enlace de datos

Utilice el comando `dladm delete-phys` para eliminar un enlace de datos del sistema.

La eliminación de un enlace de datos está ligeramente conectada a la eliminación de una NIC física. Por ejemplo, si se elimina una NIC física del sistema, la configuración de enlace de datos que está asociada a esa NIC permanece porque la capa de software ya no está vinculada a la capa de hardware, como se describe en “Comparación de la pila de protocolo de red de Oracle Solaris 10 con la pila de protocolo de red de Oracle Solaris 11” de “Transición de Oracle Solaris 10 a Oracle Solaris 11.2 ”. De este modo, puede seguir utilizando la configuración del enlace de datos en otra NIC física subyacente mediante la asignación del nombre de ese enlace de datos al enlace asociado de otra NIC.

Si desasocia una NIC sin reemplazarla y ya no necesita su configuración de enlace de datos, puede suprimir el enlace de datos de la siguiente manera:

```
# dladm delete-phys datalink
```

Sugerencia - Para confirmar si se ha eliminado la NIC de un enlace de datos, utilice el comando `dladm show-phys -P`. La salida proporciona una columna de indicadores en la que el indicador `r` muestra si se suprimió el dispositivos físico asociado con un enlace físico.

Cambio de nombre de un enlace de datos

Utilice el comando `dladm rename-link` para cambiar el nombre de un enlace de datos. En un sistema Oracle Solaris, el sistema operativo proporciona automáticamente nombres genéricos a todos los enlaces de datos. Para obtener más información acerca de los nombres de enlace de datos genéricos, consulte “Acerca de la configuración de enlaces de datos” [23].

De manera predeterminada, estos nombres genéricos utilizan el formato de asignación de nombres `net`*n*, por ejemplo, `net0`, `net1`, `net2` y así sucesivamente. Dado que el sistema operativo gestiona estos nombres, cambiar el nombre de los enlaces de datos no formará parte de sus tareas administrativas regulares. Para un procedimiento que requiere el cambio de nombres de enlace, consulte Cómo mover la configuración IP de un dispositivo de red a otro dispositivo [39].

Obtención de estadísticas de tiempo de ejecución para enlaces de datos

Utilice el comando `dlstat` para obtener estadísticas de enlaces de datos de tiempo de ejecución para todos los tipos de enlaces de datos. Cuando se utiliza solo sin otras opciones, `dlstat` muestra información estadística acerca de todos los enlaces de datos que están en el sistema, como se muestra en la siguiente salida:

```
% dlstat
          LINK    IPKTS   RBYTES    OPKTS   OBYTES
          net0   58.00K    9.52M    5.61K    1.91M
```

Para obtener más información acerca del uso del comando `dlstat`, consulte el Capítulo 8, “Supervisión del tráfico de red y el uso de recursos” de “Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ”. Consulte también la página del comando man `dlstat`(1M).

Personalización de propiedades de enlaces de datos

Además de realizar la configuración básica de enlaces de datos, también puede utilizar el comando `dladm` para establecer propiedades de enlaces de datos y personalizarlas según los requisitos de la red.

Los siguientes tres subcomandos `dladm` se utilizan para administrar propiedades de enlace de datos:

`dladm show-linkprop -p` *propertydatalink*	Muestra las propiedades de un enlace de datos y sus valores actuales. Si no utiliza la opción `-p` *property*, se muestran todas las propiedades del enlace de datos. Si no especifica un enlace de datos, se muestran todas las propiedades de todos los enlaces de datos.
`dladm set-linkprop -p` *property=value datalink*	Asigna un valor a una propiedad del enlace de datos.
`dladm reset-linkprop -p` *property datalink*	Restablece una propiedad específica de un enlace de datos a su valor predeterminado.

Las propiedades de enlaces de datos que puede personalizar dependen de las propiedades que un determinado controlador NIC admite.

Las propiedades de enlaces de datos que se pueden configurar mediante el comando `dladm` entran en una de estas dos categorías:

- Propiedades públicas: estas propiedades se pueden aplicar a cualquier controlador de un tipo de medio determinado, como la velocidad de enlace, la negociación automática para Ethernet o el tamaño de la unidad de transmisión máxima (MTU) que se puede aplicar a todos los controladores de enlaces de datos.
- Propiedades privadas: estas propiedades son específicas para un determinado subconjunto de controladores NIC para un determinado tipo de medio. Estas propiedades pueden ser específicas para dicho subconjunto porque están estrechamente relacionadas, ya sea al hardware que está asociado con el controlador o a los detalles de la propia implementación del controlador, como los valores ajustables relacionados con la depuración.

Las propiedades de enlaces normalmente tienen valores predeterminados. Sin embargo, algunos escenarios de redes pueden requerir el cambio de valores de propiedades específicos. Por ejemplo, una NIC se podría estar comunicando con un conmutador antiguo que no realiza correctamente la negociación automática. O bien un conmutador podría haberse configurado para admitir tramas gigantes. O bien, las propiedades específicas del controlador que regulan la transmisión o recepción de paquetes podrían requerir una modificación para el controlador determinado.

Activación de compatibilidad con tramas gigantes

La MTU define el tamaño del paquete más grande que un protocolo puede transmitir desde el sistema. De manera predeterminada, la mayoría de los controladores NIC definen el tamaño de MTU en 1500. Sin embargo, si las tramas gigantes atraviesan la red, el valor predeterminado no es suficiente. Para admitir tramas gigantes el tamaño de MTU debe ser, como mínimo, 9.000.

Nota - La propiedad MTU es común para los enlaces de datos y las interfaces IP, lo que significa que puede tener un valor de MTU para un enlace de datos y otro valor de MTU para la interfaz IP configurada mediante ese enlace. El valor de MTU del enlace de datos afecta a los posibles valores que se pueden definir para el valor de MTU de una interfaz IP. Para obtener más información acerca de las implicaciones de este comportamiento al configurar la propiedad MTU para enlaces de datos e interfaces IP, consulte “Configuración de la propiedad MTU” [75].

Cambie el valor predeterminado del tamaño de MTU de la siguiente manera:

```
# dladm set-linkprop -p mtu=new-size  datalink
```

Después de cambiar el tamaño de MTU, puede volver a configurar una interfaz IP mediante el enlace de datos.

En el ejemplo siguiente, se muestra cómo activar la compatibilidad con tramas gigantes. En este ejemplo se supone que ya ha eliminado cualquier configuración de interfaz IP existente mediante el enlace de datos.

```
# dladm show-linkprop -p mtu net1
LINK     PROPERTY        PERM VALUE        EFFECTIVE    DEFAULT   POSSIBLE
net1     mtu             rw   1500         1500         1500      1500

# dladm set-linkprop -p mtu=9000 net1
# dladm show-link net1
LINK     CLASS     MTU      STATE     BRIDGE     OVER
web1     phys      9000     up        --         --
```

Modificación de parámetros de la velocidad de enlace

La mayoría de las configuraciones de red constan de una combinación de sistemas con distintas capacidades de velocidad. Cada sistema anuncia las capacidades de velocidad a otros sistemas de la red, que indica la forma en que cada sistema transmite y recibe el tráfico de red.

Los siguientes pares de propiedades de enlace de datos regulan las capacidades de velocidad que anuncia un sistema:

- adv_10gfdx_cap/en_10gfdx_cap
- adv_1000fdx_cap/en_1000fdx_cap
- adv_1000hdx_cap/en_1000hdx_cap
- adv_100fdx_cap/en_100fdx_cap
- adv_100hdx_cap/en_100hdx_cap
- adv_10fdx_cap/en_10fdx_cap
- adv_10hdx_cap/en_10hdx_cap

Un par de propiedades hace referencia a cada capacidad de velocidad de enlace: la velocidad anunciada (adv_*_cap) y la velocidad anunciada permitida (en_*_cap). Asimismo, también se proporciona información sobre la velocidad de enlace de datos para las capacidades de dúplex completo y dúplex medio, según la designación de *fdx* y *hdx* en los nombres de propiedades. La propiedad de velocidad anunciada es una propiedad de sólo lectura que indica si se anuncia la velocidad de enlace de datos. Para determinar si se anuncia una velocidad de enlace de datos determinada, se establece la propiedad en_*_cap correspondiente.

De manera predeterminada, se anuncian todas las capacidades de velocidad y dúplex de un enlace de datos. Sin embargo, puede haber casos en los que un sistema nuevo se comunica con un sistema antiguo y la negociación automática está desactivada o no está admitida. Para activar la comunicación entre estos dos sistemas, es posible que se deba cambiar el valor de la velocidad anunciada entre un sistema más antiguo y un sistema más nuevo por un valor más bajo. Es posible que se deban desactivar las capacidades gigabit del sistema, y que se anuncien solamente las capacidades de velocidad más baja. En este caso, debe escribir el siguiente comando para desactivar el anuncio de las capacidades gigabit para la capacidad de dúplex completo y la capacidad de dúplex medio:

```
# dladm set-linkprop -p en_1000fdx_cap=0 datalink
# dladm set-linkprop -p en_1000hdx_cap=0 datalink
```

Para mostrar los nuevos valores de estas propiedades, use el comando dladm show-linkprop de la siguiente manera:

```
# dladm show-linkprop -p adv_10gfdx_cap datalink
# dladm show-linkprop -p adv_1000hdx_cap datalink
```

Normalmente, los valores de una propiedad de velocidad permitida determinada y la propiedad anunciada correspondiente son idénticos. Sin embargo, si una NIC admite algunas funciones avanzadas, como la gestión de energía, esas características podrían establecer límites en los bits que son realmente anunciados entre el host y su asociado de enlace. Por ejemplo, con la gestión de energía, es posible que los valores de las propiedades adv_*_cap sólo sean un subconjunto de los valores de las propiedades en_*_cap.

Establecimiento del módulo STREAMS en enlaces de datos

Puede establecer hasta ocho módulos STREAMS para insertar en el flujo cuando se abra el enlace de datos. Estos módulos son utilizados, normalmente, por software de red de terceros, como redes privadas virtuales (VPN) y firewalls. El proveedor de software proporciona documentación acerca de dicho software de red.

La lista de módulos para insertar en un enlace de datos determinado se controla mediante la propiedad `autopush`. A su vez, el valor de la propiedad `autopush` se establece mediante el subcomando `dladm set-linkprop`.

Hay un comando `autopush` independiente que puede utilizar para insertar módulos en el flujo del enlace de datos por controlador. Este comando utiliza un archivo de configuración que se configura para cada controlador y que informa al comando los módulos que se deben insertar. Sin embargo, el controlador siempre está enlazado a la NIC. Si se elimina la NIC subyacente del enlace de datos, también se pierde la información sobre la propiedad `autopush` del enlace.

Por lo tanto, se prefiere el uso del comando `dladm` para este fin antes que el comando `autopush`. Si existe el tipo de configuración `autopush` por enlace y por controlador para un determinado enlace de datos, se utiliza la información por enlace que se establece con el comando `dladm set-linkprop` y se ignora la información por controlador.

Para insertar módulos en los módulos STREAMS cuando se abre el enlace de datos, se utiliza el mismo comando `dladm set-linkprop` para especificar módulos para la propiedad `autopush`. Por ejemplo, debería insertar los módulos `vpnmod` y `bufmod` sobre el enlace `net0` de la siguiente manera:

```
# dladm set-linkprop -p autopush=vpnmod.bufmod net0
```

Obtención de información de estado para las propiedades de enlace de datos

Para obtener información sobre las propiedades de enlaces de datos, puede utilizar uno de los siguientes comandos:

- `dladm show-linkprop -p` *property datalink*
- `dladm show-ether` *datalink*

Visualización de las propiedades del enlace de datos

Para mostrar una lista completa de las propiedades de enlace de datos, escriba el comando sin especificar una propiedad, como se muestra en el siguiente ejemplo:

```
# dladm show-linkprop net1
LINK     PROPERTY        PERM VALUE        EFFECTIVE    DEFAULT   POSSIBLE
net1     speed           r-   0            0            0         --
net1     autopush        rw   --           --           --        --
net1     zone            rw   --           --           --        --
net1     duplex          r-   unknown      unknown      unknown   half,full
net1     state           r-   up           up           up        up,down
net1     adv_autoneg_cap --   --           --           0         1,0
net1     mtu             rw   1500         1500         1500      1500
net1     flowctrl        --   --           --           no        no,tx,rx,bi,
                                                                  pfc,auto
net1     adv_10gfdx_cap  r-   --           --           0         1,0
net1     en_10gfdx_cap   --   --           --           0         1,0
net1     adv_1000fdx_cap r-   --           --           0         1,0
net1     en_1000fdx_cap  --   --           --           0         1,0
net1     adv_1000hdx_cap r-   --           --           0         1,0
net1     en_1000hdx_cap  --   --           --           0         1,0
net1     adv_100fdx_cap  r-   --           --           0         1,0
net1     en_100fdx_cap   --   --           --           0         1,0
net1     adv_100hdx_cap  r-   --           --           0         1,0
net1     en_100hdx_cap   --   --           --           0         1,0
net1     adv_10fdx_cap   r-   --           --           0         1,0
net1     en_10fdx_cap    --   --           --           0         1,0
net1     adv_10hdx_cap   r-   --           --           0         1,0
net1     en_10hdx_cap    --   --           --           0         1,0
net1     maxbw           rw   --           --           --        --
net1     cpus            rw   --           --           --        --
```

Visualización de valores de propiedad de Ethernet

Si no especifica ninguna opción con el comando `dladm show-ether`, sólo se muestran los valores de propiedad de Ethernet para el enlace de datos. Para obtener más información de la que se proporciona de manera predeterminada, utilice la opción `-x`, como se muestra en el siguiente ejemplo:

```
# dladm show-ether -x net1
LINK     PTYPE       STATE    AUTO  SPEED-DUPLEX             PAUSE
net1     current     up       yes   1G-f                     both
--       capable     --       yes   1G-fh,100M-fh,10M-fh     both
--       adv         --       yes   100M-fh,10M-fh           both
--       peeradv     --       yes   100M-f,10M-f             both
```

Con la opción `-x`, el comando también muestra las capacidades incorporadas del enlace especificado, así como las capacidades que actualmente se anuncian entre el host y el asociado de enlace.

Aparece la siguiente información en este ejemplo:

- Para el estado actual del dispositivo Ethernet, el enlace está activo y funciona a 1 Gb/s, a dúplex completo. Su capacidad de negociación automática está activada y tiene un control de flujo bidireccional, que permite que tanto el host como el asociado de enlace puedan enviar y recibir tramas de pausa. Esa información aparece en la primera fila de la salida.
- En las filas siguientes de la salida del ejemplo se muestra información sobre las capacidades de velocidad de enlace de datos, las velocidades de enlace de datos reales que se anuncian e información del sistema equivalente, como se muestra a continuación:
  - Se muestran las capacidades del dispositivo Ethernet. El tipo de negociación se puede establecer en automático. Además, el dispositivo puede admitir velocidades de 1 gigabit por segundo, 100 megabits por segundo y 10 megabits por segundo, tanto en dúplex completo como en dúplex medio. Del mismo modo, las tramas de pausa se pueden recibir o enviar en ambas direcciones entre el host y el asociado de enlace.
  - Las capacidades de `net1` se anuncian como se indica a continuación: negociación automática, velocidad y dúplex, y control de flujo de tramas de pausa.
  - De forma similar, el asociado de igual o enlace de `net1` anuncia las siguientes capacidades: negociación automática, velocidad y dúplex, y control de flujo de tramas de pausa.

Tareas de configuración adicionales de `dladm`

En esta sección, se describen los procedimientos adicionales de configuración que se simplificaron mediante el comando `dladm`, como cambiar interfaces principales o llevar a cabo una reconfiguración dinámica (DR).

▼ Cómo mover la configuración IP de un dispositivo de red a otro dispositivo

Utilice el siguiente procedimiento si debe conservar la configuración IP asociada con un dispositivo de red y, a continuación, mueva esa configuración a otro dispositivo de red. Puede realizar este procedimiento como procedimiento anterior a la eliminación de una tarjeta de red del sistema o al cambiar la conexión de un cable de red.

Por ejemplo, este procedimiento describe cómo mantener la configuración IP asociada con el dispositivo `net0` (`e1000g0`) y luego aplicarla a la configuración para el dispositivo `nge0`.

1. **Conviértase en un administrador.**
2. **Muestre el enlace físico para asignaciones de dispositivos en el sistema.**

En el siguiente ejemplo, se supone que la configuración IP para `e1000g0` dejó de funcionar por algún motivo y, por lo tanto, es necesario mover la configuración a `nge0`:

```
# dladm show-phys
LINK    MEDIA    STATE    SPEED    DUPLEX    DEVICE
net0    Ethernet down     0        unknown   e1000g0
net1    Ethernet down     0        unknown   e1000g1
net2    Ethernet up       1000     full      nge0
net3    Ethernet down     0        unknown   nge1
```

3. **Desactive la configuración IP del enlace de datos temporalmente y deje la configuración persistente intacta.**

   `# ipadm disable-if` *interface*

   Por ejemplo, puede desactivar la configuración IP en `net0` de la siguiente manera:

   ```
   # ipadm disable-if net0
   ```

   Este paso le permite cambiar el nombre del enlace de datos sin tener que volver a crear su configuración IP.

4. **Cambie el nombre del enlace de datos.**

   Por ejemplo, puede cambiar el nombre del enlace de datos `net0` de la siguiente manera:

   ```
   # dladm rename-link net0 oldnet0
   ```

5. **Asigne el nombre del enlace principal al enlace de datos designado para que se convierta en el dispositivo principal.**

   `# dladm rename-link` *new-link primary-link*

   Por ejemplo, puede volver a asignar el nombre del enlace `net0` al enlace de datos `net2` de la siguiente manera:

   ```
   # dladm rename-link net2 net0
   ```

6. **Vuelva a activar la configuración IP en el enlace de datos con nombre nuevo. Por ejemplo:**

   ```
   # ipadm enable-if -t net0
   ```

ejemplo 2-1 Eliminación de una interfaz de enlace de datos

Al realizar una nueva instalación, se asignan nombres genéricos a todos los enlaces de datos automáticamente usando la convención de denominación `net0`, `net1`, `net`*N*, etc. en función del número total de dispositivos de red en un sistema. Después de la instalación, puede asignar nombres diferentes a los enlaces de datos. El siguiente ejemplo muestra cómo cambiar de una dirección IP proporcionada inicialmente para una interfaz, que implica antes eliminar la interfaz existente:

```
# ipadm delete-ip net0
# ipadm create-ip net0
# ipadm create-addr -T addrconf net0/new-add
```

Para obtener más información, consulte el Chapter 2, Administración de la configuración de enlaces de datos en Oracle Solaris.

▼ Cómo sustituir una tarjeta de interfaz de red con reconfiguración dinámica

Este procedimiento se aplica únicamente a los sistemas que admiten la reconfiguración dinámica (DR). Hace referencia específicamente a los pasos de configuración posteriores a la finalización de la reconfiguración dinámica. Ya no es necesario volver a configurar los enlaces de red después de completar el proceso de reconfiguración dinámica. En cambio, simplemente se transfieren las configuraciones de enlaces de la NIC eliminada a la NIC de sustitución.

El procedimiento no describe los pasos para realizar la reconfiguración dinámica. Consulte la documentación del sistema para obtener esa información.

Para ver una introducción a la reconfiguración dinámica, consulte el Capítulo 2, “Configuración dinámica de dispositivos” de “Gestión de dispositivos en Oracle Solaris 11.2 ”.

Antes de empezar Asegúrese de completar los siguientes pasos primero:

- Asegúrese de que el sistema admita DR.
- Consulte el manual apropiado que describe los procedimientos de DR en el sistema.

  Para encontrar documentación actual sobre la reconfiguración dinámica en servidores Sun de Oracle, busque "reconfiguración dinámica" en http://www.oracle.com/technetwork/indexes/documentation/index.html.

  Para obtener información sobre cómo lleva a cabo la reconfiguración dinámica en el entorno de Oracle Solaris Cluster, consulte “Guía de administración del sistema de Oracle Solaris Cluster ”.

1. **Conviértase en un administrador.**
2. **(Opcional) Visualice información sobre los atributos físicos de enlaces de datos y sus ubicaciones respectivas en el sistema.**

   ```
   # dladm show-phys -L
   ```

   Para obtener más información sobre el tipo de información mostrada por el comando `dladm show-phys -L`, consulte la página del comando man `dladm`(1M).
3. **Realice el proceso de reconfiguración dinámica, como se describe en la documentación del sistema.**

4. **Después de instalar la NIC de reemplazo, continúe como se muestra a continuación, en función de la circunstancia que se aplique:**

   - **Si ha insertado la NIC de reemplazo en la misma ranura que la NIC anterior, vaya al paso 5.**

     Si la NIC nueva se coloca en la ubicación que ocupaba la NIC anterior, la NIC nueva hereda el nombre del enlace y la configuración de la NIC anterior.

   - **Si insertó la NIC de reemplazo en una ranura distinta, y la NIC nueva necesita heredar la configuración de enlace de datos de la NIC eliminada, cambie el nombre del enlace de la siguiente manera:**

     ```
     # dladm rename-link new-datalink old-datalink
     ```

     new-datalink — Hace referencia al enlace de datos de la NIC de sustitución que está en una ranura distina de la que ocupaba la NIC anterior que se ha eliminado.

     old-datalink — Hace referencia al nombre de enlace de datos asociado a la NIC anterior que se eliminó.

     Nota - En este caso, la ranura de la que se ha eliminado la NIC anterior debe permanecer vacía.

     Por ejemplo, la NIC de la ranura 1 se eliminó y la NIC nueva se inserta en la ranura 2. No se inserta ninguna NIC en la ranura 1. Suponga que el enlace de datos de la ranura 1 es `net0` y el enlace de datos de la ranura 2 es `net1`. Debe especificar que el enlace de datos de la NIC nueva hereda la configuración de enlace de datos de la NIC anterior de la siguiente manera:

     ```
     # dladm rename-link net1 net0
     ```

5. **Complete el proceso de DR mediante la activación de nuevos recursos de NIC, de manera que estén disponibles para ser utilizados.**

   Por ejemplo, puede usar el comando `cfgadm` para configurar la NIC. Para obtener más información, consulte la página del comando man `cfgadm`(1M)

6. **(Opcional) Visualice información de enlaces.**

   Puede utilizar el comando `dladm show-phys` o el comando `dladm show-link` para visualizar información sobre los enlaces de datos.

ejemplo 2-2 Reconfiguración dinámica mediante la instalación de una nueva tarjeta de red

En este ejemplo, se muestra cómo una tarjeta `bge` con nombre de enlace `net0` se reemplaza por una tarjeta `e1000g`. Una vez que se conecta `e1000g` al sistema, la configuración de enlace de `e1000g` se transfiere de `bge` a `e1000g`.

```
# dladm show-phys -L
LINK     DEVICE     LOCATION
net0     bge0       MB
net1     ibp0       MB/RISER0/PCIE0/PORT1
net2     ibp1       MB/RISER0/PCIE0/PORT2
net3     eoib2      MB/RISER0/PCIE0/PORT1/cloud-nm2gw-2/1A-ETH-2
```

Puede utilizar pasos específicos de la DR, como el uso del comando `cfgadm`, para eliminar la tarjeta `bge` e instalar la tarjeta `e1000g` en su lugar. Después de que la tarjeta se instala, el enlace de datos de `e1000g0` asume de forma automática el nombre `net0` y hereda la configuración del enlace.

```
# dladm show-phys -L
LINK     DEVICE     LOCATION
net0     e1000g0    MB
net1     ibp0       MB/RISER0/PCIE0/PORT1
net2     ibp1       MB/RISER0/PCIE0/PORT2
net3     eoib2      MB/RISER0/PCIE0/PORT1/cloud-nm2gw-2/1A-ETH-2

# dladm show-link
LINK     CLASS     MTU    STATE    OVER
net0     phys      9600   up       ---
net1     phys      1500   down     ---
net2     phys      1500   down     --
net3     phys      1500   down     ---
```

▼ SPARC: Cómo asegurarse de que la dirección MAC de cada interfaz sea única

Cada sistema basado en SPARC tiene una dirección MAC para todo el sistema, que utilizan todas las interfaces de modo predeterminado. Sin embargo, algunas aplicaciones requieren que cada interfaz de un host tenga una dirección MAC exclusiva. Determinados tipos de configuración de interfaz, como las agregaciones de enlaces y las rutas múltiples de IP (IPMP) de red, requieren que las interfaces tengan sus propias direcciones MAC.

El parámetro EEPROM `local-mac-address?` determina si todas las interfaces del sistema basado en SPARC utilizan la dirección MAC de todo el sistema o una dirección MAC exclusiva. En el siguiente procedimiento, se describe cómo utilizar el comando `eeprom` para comprobar el valor actual del parámetro `local-mac-address?` y cambiarlo, si es preciso.

1. **Conviértase en un administrador.**

2. **Determine si todas las interfaces del sistema utilizan la dirección MAC del sistema.**

```
# eeprom local-mac-address?
local-mac-address?=false
```

En la salida anterior, el valor `local-mac-address?=false` indica que todas las interfaces utilizan la dirección MAC del sistema. Debe cambiar el valor de la configuración `local-mac-address?=false` a `local-mac-address?=true` antes de que las interfaces se conviertan en miembros de un grupo IPMP, por ejemplo.

Nota - También debe realizar este cambio para configurar agregaciones de enlaces.

3. **Cambie el valor de la configuración `local-mac-address?` de la siguiente manera:**

```
# eeprom local-mac-address?=true
```

Al reiniciar el sistema, las interfaces con las direcciones MAC de fábrica utilizarán esta configuración de fábrica, en lugar de la dirección MAC de todo el sistema. Las interfaces sin direcciones MAC de fábrica seguirán utilizando la dirección MAC de todo el sistema.

4. **Compruebe las direcciones MAC de todas las interfaces del sistema.**

Busque los casos en que varias interfaces tengan la misma dirección MAC. En este ejemplo, dos interfaces utilizan la dirección MAC de todo el sistema, `8:0:20:0:0:1`.

```
# dladm show-linkprop -p mac-address
LINK     PROPERTY        PERM VALUE        EFFECTIVE    DEFAULT   POSSIBLE
net0     mac-address     rw   0:14:4f:f9:b1:a9 0:14:4f:f9:b1:a9 0:14:4f:f9:b1:a9 --
net3     mac-address     rw   0:14:4f:fb:9a:d4 0:14:4f:fb:9a:d4 0:14:4f:fb:9a:d4 --
net2     mac-address     rw   0:14:4f:f9:c:d 0:14:4f:f9:c:d 0:14:4f:f9:c:d --
net1     mac-address     rw   0:14:4f:fa:ea:42 0:14:4f:fa:ea:42 0:14:4f:fa:ea:42 --
```

5. **(Opcional) Si es preciso, configure manualmente las interfaces restantes para que todas tengan direcciones MAC exclusivas.**

```
# dladm set-linkprop -p mac-address=mac-address  interface
```

Nota - Este paso sólo es necesario si dos o más interfaces de red tienen la misma dirección MAC.

En el ejemplo anterior, debe configurar `net0` y `net1` con direcciones MAC administradas localmente. Por ejemplo, para volver a configurar `net0` con la dirección MAC administrada localmente `06:05:04:03:02`, debe escribir el siguiente comando:

```
# dladm set-linkprop -p mac-address=06:05:04:03:02 net0
```

6. **Reinicie el sistema.**

♦ ♦ ♦ CAPÍTULO 3

Configuración y administración de direcciones e interfaces IP en Oracle Solaris

En este capítulo, se describe cómo configurar una red que implementa direcciones IPv4 e IPv6. Muchas de las tareas de este capítulo se aplican a redes activadas tanto para IPv4 como para IPv6. Los procedimientos que pertenecen sólo a IPv4 o IPv6 se indican especialmente.

Antes de configurar la red, revise las tareas de planificación relacionadas con IP que se describen en "Planificación de la implementación de red en Oracle Solaris 11.2 ".

Para obtener información acerca de la administración de otras propiedades de TCP/IP, como el envío de paquetes globales y los servicios de capa de transporte, consulte "Administración de servicios de capa de transporte" de "Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ".

Este capítulo se divide en los siguientes apartados:

Administración de configuración de red con el comando `ipadm`

El comando `ipadm` se introduce para reemplazar eventualmente el comando `ifconfig` como medio principal para configurar interfaces IP.

El comando `ipadm` también reemplaza el comando `ndd` para configurar propiedades de los siguientes TCP/IP protocolos:

- IP
- Protocolo de resolución de direcciones (ARP)
- Protocolo de transmisión para el control de flujo (SCTP)
- Protocolo de mensajes de control de Internet (ICMP)
- Protocolos de capas superiores, como TCP y protocolo de datagramas de usuario (UDP)

Como herramienta para configurar interfaces, el comando `ipadm` ofrece las siguientes ventajas en comparación con el comando `ifconfig`:

- Proporciona una estructura de subcomando orientada al objeto que es superior a la estructura que proporciona el comando `ifconfig`. Este cambio debería, a fin de cuentas, hacer que los procedimientos de configuración resulten más fáciles de comprender.
- Puede realizar cambios en la configuración de la red persistente, a diferencia del comando `ifconfig`.
- Admite una opción de salida analizable que puede ser útil para secuencias de comandos.

Como herramienta utilizada para establecer propiedades de protocolos, el comando `ipadm` ofrece las siguientes ventajas en comparación con el comando `ndd`:

- Proporciona más información acerca de la propiedad que el comando `ndd`, por ejemplo, el valor predeterminado y actual de una propiedad, y el rango de valores posibles.
- Define valores de propiedad de manera persistente (o temporal). El comando `ndd` sólo define valores de propiedad temporalmente.
- Admite una opción de salida analizable que puede ser útil para secuencias de comandos.

Para comparar el comando `ipadm` con los comandos `ifconfig` y `ndd`, consulte “Cambios de comandos de administración de red” de “Transición de Oracle Solaris 10 a Oracle Solaris 11.2 ”.

Para obtener más información sobre el comando `ipadm`, consulte la página del comando man `ipadm`(1M).

Configuración de las interfaces IPv4

El siguiente procedimiento y los siguientes ejemplos describen cómo configurar una red que utiliza direcciones IPv4.

▼ Cómo configurar una interfaz IPv4

Antes de empezar Compruebe qué NCP está activo en el sistema para asegurarse de estar aplicando la configuración al perfil correcto. Consulte el Ejemplo 6-6, “Cambio entre los modos fijo y reactivo”.

1. **Conviértase en un administrador.**

2. **Cree la interfaz.**

   `# ipadm create-`*interface-class interface*

   interface-class Se refiere a una de las tres clases de interfaces que se pueden crear:

   - Interfaz IP

     Esta clase de interfaz es la clase más común que puede crear al realizar la configuración de red. Para crear esta clase de interfaz, utilice el subcomando `create-ip`.
   - Interfaz de red virtual STREAMS (interfaz VNI)

     Para crear esta clase de interfaz, utilice el subcomando `create-vni`.

     A partir de Oracle Solaris 11.2, puede nombrar las interfaces de VNI de manera arbitraria. Anteriormente, el nombre de la interfaz VNI debe incluir "vni" en el prefijo, por ejemplo `vni0`. Este requisito ya no se aplica. Para obtener más información acerca de los dispositivos y las interfaces de VNI, consulte las páginas del comando man `vni`(7d) y `ipadm`(1M).
   - Interfaz IPMP

     Esta clase de interfaz se utiliza cuando se configuran los grupos IPMP. Para crear esta clase de interfaz, utilice el subcomando `create-ipmp`. Para obtener información sobre grupos IPMP, consulte el Capítulo 2, “Acerca de la administración de IPMP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.

   interface Se refiere al nombre de la interfaz. Este nombre es idéntico al nombre del enlace de datos mediante el que se crea la interfaz. Para mostrar los enlaces de datos que se encuentran en un sistema, utilice el comando `dladm show-link`.

3. **Configure la interfaz IP con una dirección IP válida mediante uno de los siguientes comandos:**

   - Configure una dirección IP estática:

     `# ipadm create-addr -a` *address* `[`*interface* `|` *addrobj*`]`

`-a` *address*
: Especifica la dirección IP que se debe configurar en la interfaz.

Nota - La configuración de túnel generalmente requiere dos direcciones para la interfaz de túnel: una dirección local y una dirección remota. Para obtener información acerca de las direcciones locales y remotas y la configuración del túnel, consulte el Capítulo 5, “Administración de túneles IP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.

Para las direcciones IP numéricas, utilice la notación enrutamiento entre dominios sin clase (CIDR). Si no utiliza la notación CIDR, la máscara de red es determinada mediante el uso de la búsqueda de la base de datos de la máscara de red `svc:/system/name-service/switch:default` o mediante *classful address semantics*.

También puede especificar un nombre de host en lugar de una dirección IP numérica. El uso de un nombre de host es válido si una dirección IP numérica correspondiente está definida para ese nombre de host en el archivo `/etc/hosts`. Si no hay ninguna dirección IP numérica definida en el archivo, el valor numérico se obtiene únicamente utilizando el orden de resolución especificado para `host` en el servicio `name-service/switch`. Si hay varias entradas para un determinado nombre de host, se genera un error.

Nota - Durante el proceso de inicio, se configuran las direcciones de IP antes de que los servicios de nombres se pongan en línea. Por lo tanto, debe asegurarse de que cualquier nombre de host que se utilice en la configuración de red esté definido en el archivo `/etc/hosts`.

[*interface* | *addrobj*]
: En Oracle Solaris, cada dirección es identificada mediante un objeto de dirección correspondiente y representada en el comando mediante *addrobj*. Para cualquier configuración posterior de la dirección, deberá hacer referencia al objeto de dirección en lugar de hacer referencia a la dirección IP real. Por ejemplo, deberá escribir `ipadm show-addr` *addrobj* o `ipadm delete-addr` *addrobj*. Para que el nombre de objeto de dirección se genere automáticamente, especifique solamente el nombre de interfaz para *interface*. Para asignar manualmente el objeto de dirección, proporcione el nombre del objeto de dirección directamente.

  - Si especifica el nombre de la interfaz, se asigna automáticamente un nombre a un objeto de dirección con el formato *interface*/*address-family*. *Address family* es `v4` para una dirección IPv4 o `v6` para una dirección IPv6. Si se configuran varias

direcciones en una interfaz mediante nombres de objeto de dirección generados automáticamente, las letras alfabéticas se anexan a los nombres de objetos de dirección para que sean únicos. Por ejemplo, `net0/v4`, `net0/v4a`, `net0/v4b`, `net0/v6`, `net0/v6a`, etc.

- Si asigna manualmente un nombre al objeto de dirección para *addrobj*, debe utilizar el formato *interface*/*user-specified-string*. *User-specified-string* hace referencia a una cadena de caracteres alfanuméricos que empieza por un carácter alfabético y tiene una longitud máxima de 32 caracteres. Por ejemplo, puede asignar a los objetos de dirección nombres `net0/static`, `net0/static1`, `net1/private`, etc.

- Configure una dirección no estática.

  ```
  # ipadm create-addr -T address-type [interface | addrobj]
  ```

  donde *address-type* es `dhcp` o `addrconf`. El argumento `addrconf` hace referencia a direcciones IPv6 generadas automáticamente.

  Para obtener una explicación más detallada de las opciones *interface* y *addrobj* consulte la descripción previa para crear direcciones estáticas.

4. **(Opcional) Muestre información acerca de la interfaz IP recién configurada.**

   Puede utilizar los siguientes comandos, dependiendo de la información que desea comprobar:

   ```
   # ipadm interface
   ```

   Si no especifica un subcomando, se muestra información para todas las interfaces del sistema.

   ```
   # ipadm show-if interface
   ```

   Si no especifica *interface*, se visualiza la información de todas las interfaces del sistema.

   ```
   # ipadm show-addr interface|addrobj
   ```

   Si no especifica *interface* o *addrobj*, se muestra información para todos los objetos de dirección.

   Para obtener más información sobre la salida del subcomando `ipadm show-*`, consulte “Supervisión de direcciones e interfaces IP” [80].

5. **Si está configurando una dirección IP estática que utiliza un nombre de host, agregue entradas para la dirección IP en el archivo `/etc/hosts`.**

   Las entradas de este archivo constan de direcciones IP y sus nombres de host correspondientes.

   Nota - Si está configurando una dirección DHCP, no necesita actualizar el archivo `/etc/hosts`.

6. **Defina la ruta predeterminada.**

```
# route -p add default address
```

Puede verificar el contenido de la tabla de enrutamiento con el comando `netstat -r`.

Para obtener más información sobre la gestión de rutas, consulte `route`(1M) y “Creación de rutas persistentes (estáticas)” [64].

ejemplo 3-1 Configuración de una interfaz IPv4 con una dirección IP estática

El siguiente ejemplo muestra cómo configurar una interfaz con una dirección IP estática. El ejemplo comienza con la activación del NCP `DefaultFixed` en el sistema para asegurarse de que los comandos `dladm` y `ipadm` no modifique un NCP reactivo, lo que podría negar cualquier configuración manual de red que realice, según su entorno.

```
# netadm enable -p ncp DefaultFixed

# dladm show-phys
LINK     MEDIA        STATE     SPEED     DUPLEX     DEVICE
net3     Ethernet     up        100Mb     full       bge3

# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net3     phys      1500    up        --        --

# ipadm create-ip net3
# ipadm create-addr -a 192.168.84.3/24 net3
net3/v4

# ipadm
NAME      CLASS/TYPE     STATE     UNDER     ADDR
lo0       loopback       ok        --        --
lo0/v4     static        ok        --     127.0.0.1/8
lo0/v6     static        ok        --     ::1/128
net3      ip             ok        --        --
net3/v4   static         ok        --     192.168.84.3/24

# vi /etc/hosts
# Internet host table
# 127.0.0.1     localhost
10.0.0.14       myhost
192.168.84.3    sales1

# route -p add default 192.168.84.1
# netstat -r
Routing Table: IPv4
Destination          Gateway              Flags Ref   Use        Interface
-------------------- -------------------- ----- ----- ---------- ---------
default              192.168.84.1         UG    2     10466
192.168.84.0         192.168.84.3         U     3     1810       net0
localhost            localhost            UH    2     12         lo0
```

```
Routing Table: IPv6
Destination/Mask            Gateway                 Flags Ref   Use    If
--------------------------- ----------------------- ----- --- ------- -----
solaris                       solaris                 UH      2     156  lo0
```

Si `sales1` ya está definido en el archivo `/etc/hosts`, puede usar el nombre de host cuando asigna las siguientes direcciones:

```
# ipadm create-addr -a sales1 net3
net3/v4
```

ejemplo 3-2 Configuración de una interfaz de red para recibir una dirección IP de un servidor DHCP

En el siguiente ejemplo, la interfaz IP se ha configurado para recibir su dirección de un servidor DHCP. DHCP normalmente también instala una ruta predeterminada. Por lo tanto, en este ejemplo, se incluye un paso para agregar de manera manual una ruta predeterminada.

```
# dladm show-phys
LINK     MEDIA        STATE     SPEED     DUPLEX     DEVICE
net3     Ethernet     up        100Mb     full       bge3

# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net3     phys      1500    up        --       --

# ipadm create-ip net3
# ipadm create-addr -T dhcp net3
net3v4

# ipadm
NAME      CLASS/TYPE     STATE     UNDER     ADDR
lo0       loopback       ok        --        --
l0/v4     static         ok        --        127.0.0.1/8
net3      ip             ok        --        --
net3/v4   dhcp           ok        --        10.0.1.13/24
```

Configuración de interfaces IPv6

Como paso inicial para usar direcciones IPv6 en una red, debe configurar IPv6 en la interfaz IP del sistema. En el proceso de instalación, IPv6 se puede activar en una o varias interfaces del sistema.

Si activó la compatibilidad con IPv6 durante la instalación, una vez que se completa la instalación, se crean los siguientes archivos y tablas relacionados con IPv6:

- El servicio SMF `name-service/switch` se modifica para permitir búsquedas mediante direcciones IPv6.

- Se crea la tabla de directrices de selección de direcciones IPv6. En esta tabla se da prioridad al formato de direcciones IP que debe utilizarse en las transmisiones a través de una interfaz activada para IPv6.

▼ Cómo configurar un sistema para IPv6

En el procedimiento siguiente se explica cómo activar IPv6 para una interfaz agregada después de instalar Oracle Solaris. Comience el proceso de configuración de IPv6. Para ello, active IPv6 en las interfaces de todos los sistemas que se convertirán en nodos de IPv6. Las implementaciones típicas de IPv6 utilizan la configuración automática para configurar interfaces IP. Una dirección IP `autoconf` asigna una dirección de enlace local y detecta los prefijos y enrutadores que están en uso en la subred. Posteriormente, puede adaptar a su conveniencia la configuración del nodo a partir de su función en la red IPv6 como host, servidor o enrutador. Las interfaces configuradas para `autoconf` también solicitarán automáticamente la información de dirección DHCPv6. Para activar sólo las direcciones IPv6 estáticas, sin configuración automática o DHCPv6, utilice el comando `ipadm` con las opciones adecuadas para crear una dirección de enlace local en la interfaz sin agregar ninguna otra dirección asignada dinámicamente. Para ver un ejemplo, consulte “Migración de una red IPv4 a una red IPv6” [62].

Nota - Si la interfaz se ubica en el mismo enlace como enrutador que anuncia un prefijo de IPv6, la interfaz obtiene el prefijo de sitio como parte de sus direcciones configuradas automáticamente. Para obtener más información, consulte “Cómo configurar un enrutador activado para IPv6” de “Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ”.

---

1. **(Opcional) Configure la interfaz IP mediante el comando `ipadm create-ip` con las opciones adecuadas.**

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

   Por ejemplo, configure una interfaz IP para `net0` de la siguiente manera:

   ```
   # ipadm create-ip net0
   ```

   Si la interfaz ya se configuró para utilizar con IPv4, no es necesario realizar este paso. Consulte Cómo configurar una interfaz IPv4 para obtener instrucciones generales acerca de la configuración de una interfaz IP.

2. **Asigne la dirección o direcciones IP.**

Nota - Al asignar la dirección IP, asegúrese de utilizar la opción correcta para asignar una dirección IPv6:

```
# ipadm create-addr -T addrconf interface
```

Para agregar más direcciones, utilice la sintaxis siguiente:

```
# ipadm create-addr -a ipv6-address  interface
```

3. **(Opcional) Cree una ruta IPv6 estática predeterminada.**

```
# /usr/sbin/route -p add -inet6 default ipv6-address
```

Nota - Como parte de la configuración automática, `in.ndpd` agrega las rutas predeterminadas a medida que se detectan, lo que puede causar que varias rutas predeterminadas aparezcan como disponibles, incluidas las rutas predeterminadas configuradas manualmente. El sistema automáticamente realiza una selección de rutas predeterminadas en función de todas las rutas disponibles, lo que significa que es posible que no siempre se utilice una ruta predeterminada configurada de manera manual.

4. **(Opcional) Cree un archivo `/etc/inet/ndpd.conf` que defina los parámetros para las variables de interfaz que están en el nodo.**

   Si tiene que crear direcciones temporales para la interfaz del host, consulte “Uso de direcciones temporales para una interfaz IPv6” [56]. Para obtener más información sobre `/etc/inet/ndpd.conf`, consulte la página de comando man `ndpd.conf`(4).

5. **(Opcional) Muestre el estado de las interfaces IP con sus configuraciones IPv6 de la siguiente manera:**

```
# ipadm show-addr
```

ejemplo 3-3 Activación de una interfaz para IPv6 tras la instalación

En el siguiente ejemplo, se muestra cómo activar IPv6 en la interfaz `net0`. Antes de comenzar, compruebe el estado de todas las interfaces configuradas en el sistema.

```
# ipadm show-addr
ADDROBJ   TYPE     STATE   ADDR
lo0/v4    static   ok      127.0.0.1/8
net0/v4   static   ok      172.16.27.74/24
```

Como se muestra en la salida anterior, actualmente, sólo está configurada la interfaz `net0` para este sistema. Si aún no se configuró la interfaz `net0`, utilice el comando `ipadm create-ip net0` para mostrar la interfaz.

A continuación, se activa IPv6 en esta interfaz de la siguiente manera:

```
# ipadm create-addr -T addrconf net0
# ipadm create-addr -a 2001:db8:3c4d:15::203/64 net0

# ipadm show-addr
ADDROBJ      TYPE       STATE   ADDR
lo0/v4       static     ok      127.0.0.1/8
net0/v4      static     ok      172.16.27.74/24
net0/v6      addrconf   ok      fe80::203:baff:fe13:14e1/10
lo0/v6       static     ok      ::1/128
net0/v6a     static     ok      2001:db8:3c4d:15::203/64

# route -p add -inet6 default fe80::203:baff:fe13:14e1
```

Pasos siguientes

- Para obtener información sobre cómo configurar el nodo de IPv6 como enrutador, consulte "Configuración de un enrutador IPv6" de "Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ".
- Para obtener información sobre cómo adaptar el nodo como servidor, consulte "Configuración de interfaces activadas para IPv6 en servidores" [61].

Uso de direcciones temporales para una interfaz IPv6

Una *dirección temporal IPv6* incluye un número de 64 bits generado aleatoriamente como ID de interfaz, en lugar de la dirección MAC de la interfaz. Puede utilizar direcciones temporales para las interfaces de un nodo IPv6 que desee mantener anónimas. Por ejemplo, puede utilizar direcciones temporales para las interfaces de un host que deba acceder a servidores web públicos. Las direcciones temporales implementan mejoras de privacidad de IPv6. Estas mejoras se describen en RFC 3041, que está disponible en "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" (http://www.rfc-editor.org/rfc/rfc3041.txt).

Las direcciones temporales se activan en el archivo `/etc/inet/ndpd.conf` para una o varias interfaces, si es necesario. Sin embargo, a diferencia de las direcciones IPv6 estándar configuradas automáticamente, una dirección temporal consta del prefijo de subred de 64 bits y un número de 64 bits generado aleatoriamente. Ese número aleatorio constituye el segmento de ID de interfaz de la dirección IPv6. Una dirección local de enlace no se genera con la dirección temporal como ID de interfaz.

Las direcciones temporales tienen un *período de vida preferente* predeterminado de un día. Al activar la generación de direcciones temporales, también puede configurar las variables siguientes en el archivo `/etc/inet/ndpd.conf`:

valid lifetime TmpValidLifetime — Lapso durante el cual existe la dirección temporal; una vez transcurrido, la dirección se suprime del host.

preferred lifetime TmpPreferredLifetime	Tiempo transcurrido antes de prescindir de la dirección temporal. Ese lapso de tiempo debe ser más breve que el período de vida válido.
address regeneration	Intervalo de tiempo antes de la conclusión del período de vida preferente durante el cual el host debe generar otra dirección temporal.

La duración de las direcciones temporales se especifica de la manera siguiente:

n	*n* cantidad de segundos, que es el valor predeterminado
n `h`	*n* cantidad de horas (`h`)
n `d`	*n* cantidad de días (`d`)

▼ Cómo configurar una dirección temporal IPv6

1. **Si es necesario, active IPv6 en las interfaces del host.**
   Consulte Cómo configurar un sistema para IPv6 [54].

2. **Edite el archivo `/etc/inet/ndpd.conf` para activar la generación de direcciones temporales.**

   - Para configurar direcciones temporales en todas las interfaces de un host, agregue la siguiente línea al archivo `/etc/inet/ndpd.conf`:

     `ifdefault TmpAddrsEnabled true`
   - Para configurar una dirección temporal para una determinada interfaz, agregue siguiente la línea al archivo `/etc/inet/ndpd.conf`:

     `if` *interface* **`TmpAddrsEnabled true`**

3. **(Opcional) Especifique el período de vida válido de la dirección temporal.**

   `ifdefault TmpValidLifetime` *duration*

   Esta sintaxis especifica el período de vida válido de todas las interfaces en un host. El valor de *duración* debe especificarse en segundos, horas o días. El período de vida válido predeterminado es 7 días. `TmpValidLifetime` también puede usarse con las palabras clave `if` *interface* para especificar el período de vida válido de una dirección temporal relativa a una determinada interfaz.

4. **(Opcional) Especifique un período de vida preferente para la dirección temporal; una vez transcurrido, se prescinde de la dirección.**

   `if` *interface* **`TmpPreferredLifetime`** *duration*

Esta sintaxis especifica el período de vida preferente de la dirección temporal de una determinada interfaz. El período de vida preferente predeterminado es un día. `TmpPreferredLifetime` también se puede utilizar con la palabra clave `ifdefault` para indicar el período de vida preferente de las direcciones temporales relativas a todas las interfaces de un host.

Nota - La selección de direcciones predeterminadas otorga una prioridad inferior a las direcciones IPv6 que se han descartado. Si se prescinde de una dirección IPv6 temporal, la selección de direcciones predeterminadas elige una dirección no descartada como dirección de origen de un paquete. Una dirección no descartada podría ser la dirección IPv6 generada de manera automática o, posiblemente, la dirección IPv4 de la interfaz. Para obtener más información sobre la selección de direcciones predeterminadas, consulte "Administración de selección de direcciones predeterminadas" de "Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ".

---

5. **(Opcional) Especifique el tiempo de generación antes del descarte de direcciones durante el cual el host debe generar otra dirección temporal.**

   `ifdefault TmpRegenAdvance` *duration*

   Esta sintaxis indica el tiempo de generación antes del descarte de dirección de las direcciones temporales relativas a todas las interfaces de un host. El valor predeterminado es 5 segundos.

6. **Cambie la configuración el daemon `in.ndpd` de la siguiente manera:**

   ```
   # pkill -HUP in.ndpd
   # /usr/lib/inet/in.ndpd
   ```

7. **Verifique que las direcciones temporales se hayan creado con el comando `ipadm show-addr`, como se muestra en el Ejemplo 3-4, "Visualización de la salida del comando `ipadm show-addr` con direcciones temporales activadas".**

   La salida del comando muestra el indicador `t` en el campo `CURRENT` de las direcciones temporales.

ejemplo 3-4 Visualización de la salida del comando `ipadm show-addr` con direcciones temporales activadas

En este ejemplo, se muestra la salida del comando `ipadm show-addr` después de crear direcciones temporales. Tenga en cuenta que en la salida de ejemplo únicamente se incluye información relacionada con IPv6.

```
# ipadm show-addr -o all
ADDROBJ   TYPE     STATE CURRENT PERSISTENT ADDR
lo0/v6    static   ok    U----   ---        ::1/128
net0/v6   addrconf ok    U----   ---        fe80::a00:20ff:feb9:4c54/10
net0/v6a  static   ok    U----   ---        2001:db8:3c4d:15:a00:20ff:feb9:4c54/64
net0/?    addrconf ok    U--t-   ---        2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64
```

Tenga en cuenta que para el objeto de dirección `net0/?`, el indicador `t` se configura en el campo `CURRENT`, lo que indica que la dirección correspondiente tiene un ID de interfaz temporal.

Véase también

- Para configurar la compatibilidad con el servicio de nombres para las direcciones IPv6, consulte el Capítulo 4, Administración de servicios de nombres y directorios en un cliente de Oracle Solaris.
- Para configurar direcciones IPv6 para un servidor, consulte Cómo configurar un token IPv6 especificado por el usuario [59].
- Para supervisar actividades en nodos IPv6, consulte el Capítulo 1, “Administración de redes TCP/IP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.

Configuración de un token IPv6

El ID de interfaz de 64 bits de una dirección IPv6 también se denomina *token*. Durante la configuración automática de direcciones, el token se asocia con la dirección MAC de la interfaz. En la mayoría de los casos, los nodos sin enrutadores (hosts y servidores IPv6) deben utilizar sus tokens configurados automáticamente.

No obstante, el uso de tokens configurados automáticamente puede resultar en problemas en servidores cuyas interfaces se intercambien de manera rutinaria como parte de la administración de sistemas. Si se cambia la tarjeta de interfaz, también se cambia la dirección MAC. Como consecuencia, los servidores que necesiten direcciones IP estables pueden tener problemas. Distintas partes de la infraestructura de red, como el sistema de nombres de dominio (DNS) o el sistema de información de red (NIS), pueden tener almacenadas direcciones IPv6 específicas para las interfaces del servidor.

Para prevenir los problemas de cambio de dirección, puede configurar manualmente un token para emplearse como ID de interfaz en una dirección IPv6. Para crear el token, especifique un número hexadecimal de 64 bits o menos para ocupar la parte del ID de interfaz de la dirección IPv6. En la subsiguiente configuración automática de direcciones, el descubrimiento de vecinos no crea un ID de interfaz que se base en la dirección MAC de la interfaz. En lugar de ello, el token creado manualmente se convierte en el ID de interfaz. Este token queda asignado a la interfaz, incluso si se sustituye una tarjeta.

Nota - La diferencia entre los tokens especificados por el usuario y las direcciones temporales es que estas segundas se generan aleatoriamente, no las crea el usuario.

▼ Cómo configurar un token IPv6 especificado por el usuario

El siguiente procedimiento es especialmente útil para los servidores con interfaces que se reemplazan de manera rutinaria. También puede seguir estos pasos para configurar los tokens específicos para el usuario en cualquier nodo IPv6.

1. **Verifique que la interfaz que desea configurar con un token exista y que no haya direcciones IPv6 configuradas en esa interfaz.**

```
# ipadm show-if
IFNAME   CLASS      STATE   ACTIVE   OVER
lo0      loopback   ok       yes     ---
net0     ip         ok       yes     ---

# ipadm show-addr
ADDROBJ      TYPE       STATE   ADDR
lo0/v4       static     ok      127.0.0.1/8
```

   En la salida anterior, se muestra que la interfaz de red `net0` existe y no que tiene configurada ninguna dirección IPv6.

2. **Cree uno o varios números hexadecimales de 64 bits para utilizar como tokens para las interfaces del nodo que aparece a continuación, en el siguiente formato:** *xxxx*:*xxxx*:*xxxx*:*xxxx*

3. **Configure cada interfaz que tendrá un ID de interfaz especificado por el usuario (token).**

   # ipadm create-addr -T addrconf -i *interface-ID interface*

   Por ejemplo, puede configurar la interfaz `net0` con un token de la siguiente manera:

```
# ipadm create-addr -T addrconf -i ::1a:2b:3c:4d/64 net0
```

   Nota - Después de crear el objeto de dirección con el token, no se puede modificar el token.

4. **Actualice el daemon de IPv6 con los cambios.**

```
# pkill -HUP in.ndpd
```

ejemplo 3-5 Configuración de un token especificado por el usuario en una interfaz de IPv6

En el ejemplo siguiente, se muestra cómo configurar `net0` con una dirección IPv6 y un token.

```
# ipadm show-if
IFNAME   CLASS      STATE    ACTIVE     OVER
lo0      loopback   ok       yes        ---
net0     ip         ok       yes        ---

# ipadm show-addr
ADDROBJ      TYPE       STATE   ADDR
lo0/v4       static     ok      127.0.0.1/8

# ipadm create-addr -T addrconf -i ::1a:2b:3c:4d/64 net0
# pkill -HUP in.ndpd
# ipadm show-addr
ADDROBJ      TYPE       STATE   ADDR
```

```
lo0/v6       static     ok      ::1/128
net0/v6      addrconf   ok      fe80::1a:2b:3c:4d/10
net0/v6a     addrconf   ok      2002:a08:39f0:1:1a:2b:3c:4d/64
```

Después de configurar el token, el objeto de dirección `net0/v6` tiene una dirección de enlace local y una dirección con `1a:2b:3c:4d` configurado para este ID de interfaz. Tenga en cuenta que este token no puede ser modificado para esta interfaz después de la creación de `net0/v6`.

Véase también

- Para actualizar los servicios de nombres con las direcciones IPv6 del servidor, consulte el Capítulo 4, Administración de servicios de nombres y directorios en un cliente de Oracle Solaris.
- Para supervisar el rendimiento del servidor, consulte el Capítulo 1, “Administración de redes TCP/IP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.

Configuración de interfaces activadas para IPv6 en servidores

Cuando planea implementar direcciones IPv6 en un servidor, debe tomar algunas decisiones al activar IPv6 en las interfaces de un servidor. Las decisiones repercuten en la estrategia que se aplica en la configuración de los ID de interfaz (tokens), de una dirección IPv6 de interfaz.

▼ Cómo activar IPv6 en las interfaces de un servidor

El siguiente procedimiento describe cómo activar IPv6 en los servidores de la red. Algunos de los pasos pueden variar según cómo desea implementar IPv6.

1. **Active IPv6 en las interfaces IP del servidor.**
   Para obtener instrucciones paso a paso, consulte “Configuración de interfaces IPv6” [53].

2. **Compruebe que el prefijo de subred IPv6 esté configurado en un enrutador en el mismo enlace que el servidor.**
   Para obtener más información, consulte “Configuración de un enrutador IPv6” de “Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ”.

3. **Seleccione una de las siguientes estrategias para la asignación de un ID de interfaz para las interfaces activadas para IPv6 del servidor.**
   De forma predeterminada, la configuración automática de direcciones IPv6 utiliza la dirección MAC de una interfaz al crear la parte del ID de interfaz de la dirección IPv6. Si se conoce bien la dirección IPv6 de la interfaz, el intercambio de interfaces puede resultar problemático. La dirección MAC de la nueva interfaz será distinta. En el proceso de configuración automática de direcciones, se genera un nuevo ID de interfaz.

- **Para una interfaz activada para IPv6 que no desea reemplazar, utilice la dirección IPv6 configurada automáticamente.**
- **En el caso de interfaces activadas para IPv6 que deben figurar como anónimas fuera de la red local, plantee la posibilidad de utilizar para el ID de interfaz un token generado aleatoriamente.**

  Para obtener más información, consulte Cómo configurar una dirección temporal IPv6 [57].
- **Para las interfaces activadas para IPv6 que tenga previsto intercambiar con regularidad, puede utilizar la configuración estática o puede crear tokens para los ID de interfaz.**

  Para obtener más información, consulte Cómo configurar un token IPv6 especificado por el usuario [59].

Migración de una red IPv4 a una red IPv6

Nota - Antes de migrar de una red IPv4 a una red ipv6, tenga en cuenta que la mayoría de los planes de migración implican ejecutar IPv4 e IPv6 juntos por un largo período de tiempo, tal vez indefinidamente.

Antes de migrar de una red IPv4 a una red IPv6, revise la información del Capítulo 2, “Planificación para el uso de direcciones IPv6” de “Planificación de la implementación de red en Oracle Solaris 11.2 ” para determinar si necesita realizar alguna tarea adicional.

Los pasos básicos para migrar de una red IPv4 a una red IPv6 implican primero eliminar todas las DHCP IPv4 existentes y direcciones IP estáticas y, luego, volver a configurar todas las nuevas direcciones IPv6 que sean necesarias. Si la nueva interfaz de IPv6 está en el mismo enlace que el enrutador que actualmente anuncia un prefijo de IPv6, la interfaz obtiene el prefijo del enlace. Para obtener más información, consulte “Configuración de un enrutador IPv6” de “Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ”.

EJEMPLO 3-6 Migración de direcciones IPv4 a direcciones IPv6

Los siguientes ejemplos muestran cómo migrar sus direcciones IPv4 existentes a direcciones IPv6. El proceso comienza con la supresión de todas las DHCP IPv4 y direcciones IP estáticas existentes.

```
# ipadm show-addr net0/
ADDROBJ   TYPE     STATE   ADDR
lo0/v4    static   ok      127.0.0.1/8
net0/v4   static   ok      172.16.27.74/24
```

```
# ipadm delete-addr net0/v4
```

Para obtener instrucciones, consulte “Eliminación o modificación de la configuración de una interfaz IP” [79].

A continuación, la nueva dirección IPv6 se crea mediante el comando `ipadm create addr` con las opciones y los argumentos adecuados.

Por ejemplo, puede crear una dirección IPv6 de enlace local y `addrconf` de la siguiente manera:

```
# ipadm create-addr -T addrconf -p stateless=yes,stateful=yes net0/v6a
```

Cree una dirección IPv6 estática sin DHCPv6 y una dirección `addrconf` de la siguiente manera:

```
# ipadm create-addr -T addrconf -p stateless=no,stateful=no net0/v6a
# ipadm create-addr -T static -a a::b/64 net0/v6b
```

Cree una dirección IPv6 estática de la siguiente manera:

```
# ipadm create-addr -T static -a a::b/64 net0/v6b
```

Muestre la nueva configuración de IPv6 mediante el comando `ipadm show-addr`.

Para obtener pasos de configuración IPv6 adicionales (necesarios y opcionales) que no se incluyen en este ejemplo, consulte “Configuración de interfaces IPv6” [53].

Configuración de rutas

Esta sección incluye los siguientes temas:

- “Tablas y tipos de enrutamiento” [63]
- “Creación de rutas persistentes (estáticas)” [64]
- “Activación del enrutamiento para sistemas de interfaz única” [67]

Tablas y tipos de enrutamiento

Los enrutadores y los hosts mantienen una *tabla de enrutamiento*. Por ejemplo, la siguiente tabla de enrutamiento enumera las direcciones IP de las redes que conoce el sistema, incluida la red local predeterminada del sistema. La tabla también enumera la dirección IP de un sistema de portal para cada red conocida. Una *puerta de enlace* es un sistema que puede recibir paquetes de salida y reenviarlos un salto más allá de la red local.

```
Routing Table: IPv4
Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
default              172.20.1.10          UG       1    532   net0
224.0.0.0            10.0.5.100           U        1      0   net1
10.0.0.0             10.0.5.100           U        1      0   net1
```

```
127.0.0.1          127.0.0.1          UH       1     57   lo0
```

En un sistema Oracle Solaris, puede configurar dos tipos de enrutamiento: estático y dinámico. Puede configurar uno o ambos tipos de enrutamiento en un único sistema. Un sistema que implementa el *enrutamiento dinámico* se basa en protocolos de enrutamiento, como el protocolo de información de enrutamiento (RIP) para redes IPv4 y RIPng (RIP de próxima generación) para redes IPv6, para enrutar el tráfico de red y actualizar información enrutamiento en la tabla. Con el *enrutamiento estático*, la información de enrutamiento se mantiene de manera manual con el comando `route`. Para obtener más información, consulte la página del comando man `route`(1M).

Al configurar el enrutamiento para la red local o el sistema autónomo (SA), considere el tipo de enrutamiento que desea para los hosts y enrutadores específicos. La siguiente tabla muestra los diversos tipos de enrutamiento y las redes para las que es adecuado cada tipo.

Tipo de encaminamiento	Uso recomendado
Estática	Hosts y redes de tamaño reducido que obtienen las rutas de un enrutador predeterminado, y enrutadores predeterminados que sólo necesitan conocer uno o dos enrutadores en los siguientes saltos.
Dinámica	Interredes de mayor tamaño, enrutadores en redes locales con múltiples hosts y hosts de sistemas autónomos de gran tamaño. El enrutamiento dinámico es la mejor opción para los sistemas en la mayoría de las redes.
Estático y dinámico combinados	Enrutadores que conectan una red con enrutamiento estático y una red con enrutamiento dinámico, y enrutadores de límite que conectan un sistema autónomo interior con redes externas. La combinación del enrutamiento estático y dinámico en un sistema es una práctica habitual.

La topología que se describe en“Topología de sistemas autónomos IPv4” de “Planificación de la implementación de red en Oracle Solaris 11.2 ” combina el enrutamiento dinámico y estático.

Nota - Dos rutas hacia el mismo destino no hacen que el sistema ejecute automáticamente la función de equilibrio de carga o failover. Si necesita estas capacidades, use IPMP. Para obtener más información, consulte el Capítulo 2, “Acerca de la administración de IPMP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.

Creación de rutas persistentes (estáticas)

Utilice el comando `route` para manipular las tablas de enrutamiento del sistema manualmente. Para que los cambios sean persistentes después de los reinicios, utilice la opción `-p`. Dado que el archivo `/etc/defaultrouter` no se admite en Oracle Solaris 11, ya no puede gestionar las rutas (predeterminadas o no) mediante la edición de este archivo. El uso del comando `route` es la única manera de configurar manualmente las rutas para que sean persistentes a través de los reinicios del sistema.

Nota - El comando `route` manipula rutas para el perfil activo *solamente*. La ruta predeterminada, así como todas las demás rutas, podrían ser reemplazadas si cambia el perfil activo. Sin embargo, esto no es una preocupación si siempre utiliza el mismo perfil en el sistema.

Al agregar las rutas de manera persistente se debe tener cuidado para asegurarse de que las rutas que agrega no existan en la configuración persistente. Si estas rutas ya existen en la configuración persistente, las tablas de enrutamiento de la red podrían cambiar sin actualizar la ruta persistente. Un ejemplo sería una situación en la que la ruta predeterminada del sistema se asigna a la interfaz principal del sistema (que es con frecuencia el caso después de una instalación Oracle Solaris). Si cambia posteriormente la interfaz principal del sistema a otra interfaz, la ruta predeterminada del sistema también debe actualizarse de manera persistente. Un uso recomendado es suprimir la configuración de la ruta persistente antes de agregar la nueva ruta. Para obtener más información, consulte “Resolución de problemas al agregar una ruta persistente” de “Resolución de problemas de administración de redes en Oracle Solaris 11.2 ”.

Tenga en cuenta la siguiente información adicional sobre la creación y visualización de rutas persistentes:

- Utilice el comando `route` con la opción `-p` para agregar una ruta de manera persistente:

  ```
  # route -p add default ip-address
  ```

  Para las rutas creadas mediante este método, utilice el comando `route -p show` para mostrar todas las rutas estáticas persistentes:

  ```
  # route -p show
  ```

- Muestre las rutas activas actualmente en un sistema mediante el comando `netstat` con las siguientes opciones:

  ```
  # netstat -rn
  ```

  Consulte las páginas del comando man `netstat`(1M) y `route`(1M).

Para obtener más información, consulte las páginas del comando man `netstat`(1M) y `route`(1M).

Para obtener información sobre la creación y visualización de las rutas predeterminadas cuando se utiliza el modo reactivo, consulte el Capítulo 5, Acerca de la administración de la configuración de red basada en perfiles en Oracle Solaris.

▼ Cómo agregar una ruta estática a la tabla de enrutamiento

1. **Visualice el estado actual de la tabla de enrutamiento mediante la cuenta de usuario normal.**

```
% netstat -rn
```

La salida sería similar a la siguiente:

```
Routing Table: IPv4
  Destination           Gateway           Flags  Ref     Use     Interface
-------------------- -------------------- ----- ----- ---------- ---------
192.168.5.125        192.168.5.10         U     1     5879       net0
224.0.0.0            198.168.5.10         U     1     0          net0
default              192.168.5.10         UG    1     91908
127.0.0.1            127.0.0.1            UH    1     811302     lo0

Routing Table: IPv6
  Destination/Mask            Gateway                   Flags Ref   Use    If
--------------------------- --------------------------- ----- --- ------- -----
::1                         ::1                         UH      2       0 lo0
```

2. **Conviértase en un administrador.**

3. **(Opcional) Vacíe las entradas existentes en la tabla de enrutamiento.**

```
# route flush
```

4. **Agregue una ruta persistente.**

```
# route -p add -net network-address -gateway gateway-address
```

`-p`	Crea una ruta que permanece tras el reinicio del sistema. Si desea que la ruta sea válida sólo para la sesión actual, no utilice la opción `-p`.
`-net` *network-address*	Especifica que la ruta se dirige a la red con la dirección especificada en *network-address*.
`-gateway` *gateway-address*	Indica que el sistema de portal para la ruta especificada tiene la dirección IP *dirección_portal*.

ejemplo 3-7 Cómo agregar una ruta estática a la tabla de enrutamiento

El siguiente ejemplo muestra cómo agregar una ruta estática a un enrutador (enrutador 2). La ruta estática es necesaria para el enrutador de límite del SA: `10.0.5.150`. Consulte la Figura 3-1, “Sistema autónomo con varios enrutadores IPv4” para obtener una ilustración de esta configuración en particular.

Debería ver la tabla de enrutamiento en el enrutador 2 de la siguiente manera:

```
# netstat -rn
Routing Table: IPv4
Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
```

```
default              172.20.1.10          UG        1    249 ce0
224.0.0.0            172.20.1.10          U         1      0 ce0
10.0.5.0             10.0.5.20            U         1     78 bge0
127.0.0.1            127.0.0.1            UH        1     57 lo0

Routing Table: IPv6
  Destination/Mask            Gateway                   Flags Ref   Use    If
--------------------------- --------------------------- ----- --- ------- -----
::1                         ::1                         UH      2       0 lo0
```

La tabla de enrutamiento indica que hay dos rutas que conoce el enrutador 2. La ruta predeterminada utiliza la interfaz `172.20.1.10` del enrutador 2 como portal. El segundo enrutador, `10.0.5.0`, fue detectado por el daemon `in.routed` que se ejecuta en el enrutador 2. La puerta de enlace de esta ruta es el enrutador 1, con la dirección IP `10.0.5.20`.

Para agregar una segunda ruta a la red `10.0.5.0`, que tiene su puerta de enlace como enrutador de límite, de la siguiente manera:

```
# route -p add -net 10.0.5.0/24 -gateway 10.0.5.150
add net 10.0.5.0: gateway 10.0.5.150
```

Ahora la tabla de enrutamiento cuenta con una ruta para el enrutador de límite, que tiene la dirección IP `10.0.5.150`.

```
# netstat -rn
Routing Table: IPv4
Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
default              172.20.1.10          UG        1    249 ce0
224.0.0.0            172.20.1.10          U         1      0 ce0
10.0.5.0             10.0.5.20            U         1     78 bge0
10.0.5.0             10.0.5.150           U         1    375 bge0
127.0.0.1            127.0.0.1            UH        1     57 lo0

Routing Table: IPv6
  Destination/Mask            Gateway                   Flags Ref   Use    If
--------------------------- --------------------------- ----- --- ------- -----
::1                         ::1                         UH      2       0 lo0
```

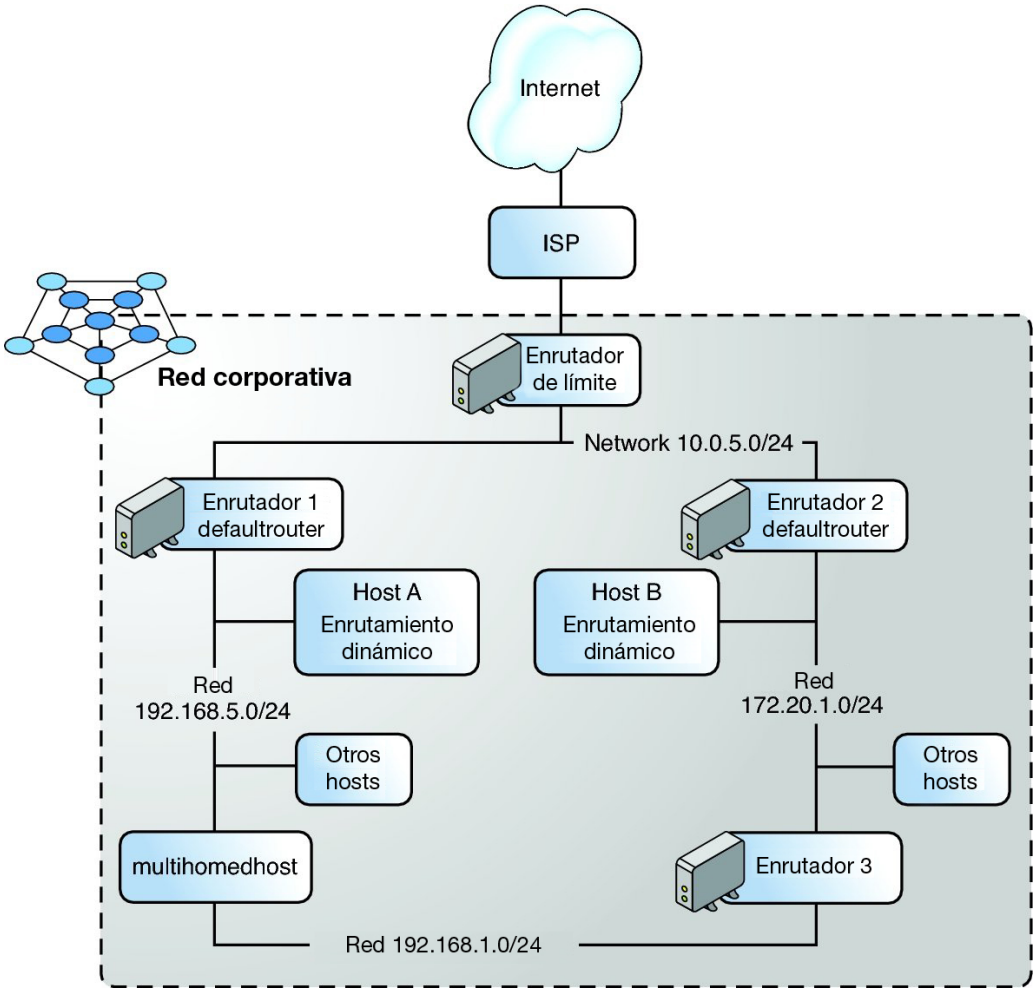
Activación del enrutamiento para sistemas de interfaz única

Puede configurar sistemas de interfaz única con enrutamiento estático o dinámico. Con el enrutamiento estático, el host debe confiar en los servicios de un enrutador predeterminado para obtener información de enrutamiento. La activación del enrutamiento dinámico que utiliza un protocolo de enrutamiento es la manera más sencilla de gestionar el enrutamiento en un sistema.

Los sitios con varios enrutadores y redes generalmente administran su topología de red como dominio de enrutamiento único o *sistema autónomo* (SA). Los procedimientos y ejemplos de

esta sección están basados en la siguiente figura. En esta figura, un SA está dividido en tres redes locales `10.0.5.0`, `172.20.1.0` y `192.168.5.0`. La red se compone de los enrutadores y sistemas cliente, incluidos los siguientes tipos de enrutadores: enrutadores de límite, enrutadores predeterminados y enrutadores de reenvío de paquetes. Los sistemas cliente incluyen sistemas de host múltiple y sistemas de interfaz única. Para obtener más detalles sobre cada uno de estos componentes, consulte “Topología de sistemas autónomos IPv4” de “Planificación de la implementación de red en Oracle Solaris 11.2 ”.

FIGURA 3-1 Sistema autónomo con varios enrutadores IPv4



▼ Cómo activar el enrutamiento dinámico en un sistema de interfaz única

El siguiente ejemplo supone que ya se configuró la interfaz IP del sistema. Para obtener más información acerca de la planificación de enrutadores en una red, consulte “Topología de sistemas autónomos IPv4” de “Planificación de la implementación de red en Oracle Solaris 11.2 ”.

1. **Conviértase en un administrador.**

2. **Configure una de las interfaces IP del sistema con una dirección IP para la red a la que pertenece el sistema.**

   Para obtener instrucciones, consulte Cómo configurar una interfaz IPv4 [49].

3. **Suprima todas las rutas definidas de manera persistente del sistema.**

   Realice este paso, ya que la presencia de cualquier ruta predeterminada definida estáticamente impide que el sistema active el enrutamiento dinámico durante un inicio del sistema.

   a. **Determine todas las rutas predeterminadas definidas de manera persistente de la siguiente forma:**

      ```
      # route -p show
      ```

   b. **Suprima cada una de las rutas definidas de manera persistente. Por ejemplo:**

   ```
   # route -p delete -net default -gateway 172.20.1.10
   ```

4. **Asegúrese de que el reenvío de paquetes esté desactivado.**

   ```
   # routeadm -d ipv4-forwarding -u
   ```

5. **Active el enrutamiento de IPv4 en el sistema.**

   ```
   # routeadm -e ipv4-routing -u
   ```

ejemplo 3-8 Ejecución del enrutamiento dinámico en un sistema de interfaz única

En el ejemplo siguiente, se muestra cómo configurar el enrutamiento dinámico para `hosta`, un sistema de interfaz única en la red `192.168.5.0`, que se muestra en la Figura 3-1, “Sistema autónomo con varios enrutadores IPv4”. El sistema utiliza el enrutador 1 como enrutador predeterminado. El ejemplo supone que ya se configuró la interfaz IP del sistema.

Primero, debe iniciar sesión en `hosta` con derechos de administrador. Luego, debe eliminar todas las rutas definidas de manera persistente del sistema.

```
# route -p show
persistent: route add default 172.20.1.10

# route -p delete default 172.20.1.10
delete net default: gateway 172.20.1.10
delete persistent net default: gateway 172.20.1.10

# routeadm
              Configuration   Current             Current
                     Option   Configuration       System State
---------------------------------------------------------------
               IPv4 routing   disabled            disabled
               IPv6 routing   disabled            disabled
             IPv4 forwarding  disabled            disabled
             IPv6 forwarding  disabled            disabled

           Routing services   "route:default ripng:default"

Routing daemons:

                      STATE   FMRI
                   disabled   svc:/network/routing/ripng:default
                     online   svc:/network/routing/ndp:default
                   disabled   svc:/network/routing/rdisc:default
                   disabled   svc:/network/routing/legacy-routing:ipv4
                   disabled   svc:/network/routing/legacy-routing:ipv6
                   disabled   svc:/network/routing/route:default

# routeadm -d ipv4-forwarding -u
# routeadm -e ipv4-routing -u
# routeadm
              Configuration   Current             Current
                     Option   Configuration       System State
---------------------------------------------------------------
               IPv4 routing   enabled             enabled
               IPv6 routing   disabled            disabled
             IPv4 forwarding  disabled            disabled
             IPv6 forwarding  disabled            disabled

           Routing services   "route:default ripng:default"

Routing daemons:

                      STATE   FMRI
                   disabled   svc:/network/routing/ripng:default
                     online   svc:/network/routing/ndp:default
                   disabled   svc:/network/routing/rdisc:default
                   disabled   svc:/network/routing/legacy-routing:ipv4
                   disabled   svc:/network/routing/legacy-routing:ipv6
                     online   svc:/network/routing/route:default
```

Acerca del enrutamiento de IPv6

El enrutamiento IPv6 es casi idéntico al enrutamiento IPv4 en CIDR. La única diferencia estriba en que las direcciones son IPv6 de 128 bits, en lugar de IPv4 de 32 bits. Con extensiones sumamente sencillas, todos los algoritmos de enrutamiento de IPv4, como abrir la ruta de acceso más corta primero (OSPF), RIP, el protocolo de enrutamiento entre dominios (IDRP) y el sistema intermedio a sistema intermedio (IS-IS) se pueden usar para enrutar IPv6.

Asimismo, IPv6 incluye extensiones sencillas de enrutamiento que admiten las siguientes posibilidades de enrutamiento nuevas y potentes.

- La selección del proveedor se basa en las directrices, el rendimiento, los costes, etcétera
- Movilidad de los hosts, enrutamiento a la ubicación actual
- Redireccionamiento automático, enrutamiento a la dirección nueva

Para acceder a las nuevas funciones de enrutamiento, debe crear secuencias de direcciones IPv6 que utilicen la opción de enrutamiento de IPv6. Un origen de IPv6 utiliza la opción de enrutamiento para obtener uno o varios nodos intermedios, o un grupo topológico, que debe visitarse en dirección al destino del paquete. Esta función es muy parecida a las opciones de ruta de registro y ruta holgada fija en origen de IPv4.

Para que las secuencias de direcciones sean una función general, los hosts de IPv6 deben (en la mayoría de los casos) invertir las rutas de un paquete que reciba un host. El paquete se debe autenticar correctamente mediante el encabezado de autenticación de IPv6. El paquete debe contener secuencias de direcciones para devolver el paquete al emisor. Esta técnica obliga a que las implementaciones de hosts de IPv6 admitan el control y la inversión de las rutas de origen. El control y la inversión de las rutas de origen permite a los proveedores trabajar con los hosts que implementan las nuevas funciones de IPv6 como la selección de proveedor y las direcciones extendidas.

Configuración de hosts múltiples

En Oracle Solaris, un sistema con más de una interfaz es considerado *host múltiple*. Las interfaces de un host múltiple se conectan a distintas subredes, ya sea en redes físicas diferentes o en la misma red física. Para obtener instrucciones paso a paso sobre la creación de un host múltiple, consulte Cómo crear un host múltiple [72].

En un sistema con interfaces múltiples que se conectan a la misma subred, es necesario configurar primero las interfaces en un grupo IPMP. De lo contrario, el sistema no puede ser un host múltiple. Para obtener más información acerca de IPMP, consulte el Capítulo 2, “Acerca de la administración de IPMP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.

Un host múltiple no reenvía paquetes IP, pero puede configurar para ejecutar que un host múltiple ejecute protocolos de enrutamiento. Normalmente se configuran los siguientes tipos de sistemas como hosts múltiples:

- Los servidores NFS, especialmente los que funcionan como grandes centros de datos, se pueden conectar a más de una red para compartir archivos entre una agrupación de usuarios de gran tamaño. No es necesario que estos servidores mantengan tablas de enrutamiento.
- Los servidores de bases de datos pueden tener varias interfaces de red que proporcionan recursos a una agrupación de usuarios de gran tamaño, como los servidores NFS.
- Los portales de firewall son sistemas que proporcionan conexión entre la red de una compañía y las redes públicas como Internet. Los administradores configuran los firewalls como una medida de seguridad. Cuando se configura el host como un firewall, no transfiere paquetes entre las redes conectadas a las interfaces del host. Sin embargo, el host puede seguir ofreciendo los servicios TCP/IP estándar, como `ssh`, a los usuarios autorizados.

Nota - Cuando los hosts múltiples tienen distintos tipos de firewall en cualquiera de sus interfaces, procure evitar la interrupción involuntaria de los paquetes del host. Este problema sucede especialmente con los firewalls con estado. Una solución podría ser configurar los firewalls sin estado. Para obtener más información acerca de los firewalls, consulte “Sistemas de firewall” de “Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ” o la documentación del firewall si es de un tercero.

▼ Cómo crear un host múltiple

1. **Conviértase en un administrador.**
2. **Configure cada interfaz de red adicional que no se configuró como parte del proceso de instalación.**
   Consulte Cómo configurar una interfaz IPv4 [49].
3. **Si el reenvío de paquetes está activado, desactive este servicio.**

```
# routeadm -p ipv4-forwarding
persistent=enabled default=disabled current=enabled
# routeadm -d ipv4-forwarding -u
# routeadm -p ipv4-forwarding
persistent=disabled default=disabled current=disabled
```

4. **(Opcional) Active el enrutamiento dinámico para el host múltiple.**

```
# routeadm -e ipv4-routing -u
# routeadm -p ipv4-routing
persistent=enabled default=enabled current=enabled
```

ejemplo 3-9 Configuración de un host múltiple

En el siguiente ejemplo, se muestra cómo configurar un host múltiple, como se ilustra en la figura de “Topología de sistemas autónomos IPv4” de “Planificación de la implementación de

red en Oracle Solaris 11.2 ". En este ejemplo, el sistema tiene el nombre de host `hostc`. Este host cuenta con dos interfaces, que están conectadas a la red `192.168.5.0`.

Para empezar, debe mostrar el estado de las interfaces del sistema.

```
# dladm show-link
LINK     CLASS     MTU     STATE   BRIDGE   OVER
net0     phys      1500    up      --       --
net1     phys      1500    up      --       --

# ipadm show-addr
ADDROBJ        TYPE     STATE        ADDR
lo0/v4         static   ok           127.0.0.1/8
net0/v4        static   ok           192.168.5.82/24
```

El comando `dladm show-link` informa que `hostc` tiene dos enlaces de datos. Sin embargo, únicamente `net0` se configuró con una dirección IP. Para configurar `hostc` como host múltiple, debe configurar `net1` con una dirección IP en la misma red `192.168.5.0`. Asegúrese de que la NIC física subyacente de `net1` esté conectada físicamente a la red.

```
# ipadm create-ip net1
# ipadm create-addr static -a 192.168.5.85/24 net1
# ipadm show-addr
ADDROBJ        TYPE     STATE        ADDR
lo0/v4         static   ok           127.0.0.1/8
net0/v4        static   ok           192.168.5.82/24
net1/v4        static   ok           192.168.5.85/24
```

A continuación, debe agregar la interfaz `net1` al archivo `/etc/hosts`de la siguiente manera:

```
# vi /etc/inet/hosts
127.0.0.1           localhost
192.168.5.82        hostc    #primary network interface for host3
192.168.5.85         hostc-2  #second interface
```

Luego, debe desactivar el reenvío de paquetes si este servicio se está ejecutando en `hostc` de la siguiente manera:

```
# routeadm -p ipv4-forwarding
persistent=enabled default=disabled current=enabled

# routeadm
              Configuration   Current             Current
                     Option   Configuration       System State
---------------------------------------------------------------
               IPv4 routing   enabled             enabled
               IPv6 routing   disabled            disabled
             IPv4 forwarding  disabled            disabled
             IPv6 forwarding  disabled            disabled

           Routing services   "route:default ripng:default"

Routing daemons:
```

```
   STATE   FMRI
disabled   svc:/network/routing/ripng:default
  online   svc:/network/routing/ndp:default
disabled   svc:/network/routing/rdisc:default
disabled   svc:/network/routing/legacy-routing:ipv4
disabled   svc:/network/routing/legacy-routing:ipv6
  online   svc:/network/routing/route:default
```

El comando `routeadm` informa que el enrutamiento dinámico a través del daemon `in.routed` está actualmente desactivado.

Implementación de enrutamiento simétrico en hosts múltiples

De manera predeterminada, un sistema con varias interfaces (denominado *host múltiple*) enruta su tráfico de red en función de la ruta coincidente de mayor distancia hasta el destino del tráfico en la tabla de enrutamiento. Cuando existen varias rutas de igual distancia hasta el destino, Oracle Solaris aplica los algoritmos ECMP (Equal-Cost Multi-Path) para repartir el tráfico por esas rutas.

No siempre es ideal repartir el tráfico de este modo. Por ejemplo, es posible que un paquete IP se envíe por medio de una interfaz de un host múltiple que no está en la misma subred que la dirección IP de origen del paquete. Además, si el paquete saliente es en respuesta a una solicitud entrante determinada, como una solicitud de eco ICMP, la solicitud y la respuesta podrían no atravesar la misma interfaz. Este tipo de configuración de enrutamiento de tráfico se denomina *enrutamiento asimétrico*. Si su proveedor de servicios de Internet (ISP) está implementando *el filtrado de entrada*, como se describe en RFC 3704 (http://www.rfc-editor.org/rfc/bcp/bcp84.txt), una configuración de enrutamiento asimétrica podría hacer que el ISP pierda un paquete saliente.

RFC 3704 tiene el propósito de limitar ataques de denegación de servicio (DoS) en Internet. Para cumplir con este propósito, su red debe configurarse para el enrutamiento simétrico. La propiedad `hostmodel` le permite cumplir este requisito. Esta propiedad controla el comportamiento de los paquetes IP que se reciben o se transmiten por medio de un host múltiple.

La propiedad `hostmodel` puede tener uno de los tres valores siguientes:

`strong` (fuerte)	Corresponde al modelo de sistema final (ES, End System) fuerte, como se define en RFC 1122. Este valor implementa el enrutamiento simétrico.
`weak` (débil)	Corresponde al modelo de ES débil, como se define en RFC 1122. Con este valor, un host múltiple utiliza el enrutamiento asimétrico.

`src-priority` Configura el enrutamiento de paquetes usando rutas preferidas. Si existen varias rutas de destino en la tabla de enrutamiento, las rutas preferidas son las que usan interfaces en las que está configurada la dirección IP de origen de un paquete saliente. Si no hay ninguna ruta de esa clase, el paquete saliente utiliza la ruta coincidente de mayor distancia hasta el destino IP del paquete.

Por ejemplo, debe implementar el enrutamiento simétrico de paquetes IP en un host múltiple de la siguiente manera:

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY   PERM  CURRENT  PERSISTENT  DEFAULT   POSSIBLE
ipv6   hostmodel  rw    strong   --          weak      strong,
src-priority,
weak
ipv4   hostmodel  rw    strong   --          weak      strong,
src-priority,
weak
```

Personalización de las propiedades y direcciones de la interfaz IP

Existen tres subcomandos `ipadm` que se utilizan para gestionar las propiedades de la interfaz IP:

- `show-ifprop -p` *property interface*: muestra las propiedades de una interfaz IP y sus valores actuales. Si no utiliza la opción `-p` *property*, se muestran todas las propiedades de la interfaz IP. Si no especifica una interfaz IP, se muestran todas las propiedades de todas las interfaces IP.
- `set-ifprop -p` *property=value interface*: asigna un valor a la propiedad de la interfaz IP.
- `reset-ifprop -p` *property interface*: restablece la propiedad específica a sus valores predeterminados.

Los enlaces de datos, al igual que las interfaces IP, tienen propiedades que se pueden personalizar para el entorno de red específico. Para cada interfaz, existen dos conjuntos de propiedades, uno para el protocolo IPv4 y otro para el protocolo IPv6.

Configuración de la propiedad MTU

Algunas propiedades, incluida la propiedad MTU, son iguales para los enlaces de datos y las interfaces IP. Por lo tanto, puede tener un valor de MTU para un enlace de datos y otro valor de MTU diferente para la interfaz configurada mediante ese enlace. Además, puede tener valores de MTU diferentes que se apliquen a los paquetes de IPv4 e IPv6 que atraviesan esa interfaz IP.

Al definir las propiedades de MTU para una interfaz IP, tenga en cuenta los siguientes puntos clave:

- El valor de la configuración de MTU de una interfaz IP no puede ser mayor que el valor de la configuración de MTU de un enlace de datos. En tales casos, el comando `ipadm` muestra un mensaje de error.
- Si un valor de MTU de una interfaz IP es distinto de un valor de MTU de un enlace de datos, los paquetes IP están limitados al valor MTU de la interfaz IP. Por ejemplo, si un enlace de datos tiene un valor de MTU de 9000 bytes y una interfaz IP tiene un valor de MTU de 1500 bytes, los paquetes IP se limitan a 1500 bytes. Sin embargo, otros protocolos de capa 3 que utilizan el protocolo de capa 2 subyacente pueden enviar paquetes de hasta 9000.

  Para obtener instrucciones sobre la personalización de las propiedades de enlaces de datos, incluida la información sobre la forma en que la configuración de MTU de un enlace de datos afecta a la configuración de MTU de una interfaz IP, consulte “Personalización de propiedades de enlaces de datos” [34].

Activación de reenvío de paquetes

En una red, un host puede recibir paquetes de datos que estén destinados a otro sistema host. Mediante la activación del reenvío de paquetes en el sistema local de recepción, dicho sistema puede reenviar el paquete de datos al host de destino. Este proceso se conoce como *reenvío IP* y está desactivado de manera predeterminada en Oracle Solaris.

El reenvío de paquetes se gestiona mediante una propiedad que se puede establecer en interfaces IP y en el protocolo TCP/IP. Si desea elegir el modo en que se reenvían los paquetes, puede activar el reenvío de paquetes en la interfaz IP. Por ejemplo, puede tener un sistema con varias NIC, donde algunas NIC están conectadas a la red externa, mientras que otras están conectadas a una red privada. En ese caso, se debe activar el reenvío de paquetes solamente en algunas de las interfaces, no en todas.

También puede activar el reenvío de paquetes de forma global en el sistema estableciendo la propiedad del protocolo TCP/IP. Consulte “Activación del reenvío de paquetes de forma global” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ” para obtener más información.

Nota - La propiedad `forwarding` de protocolos o interfaces IP no se excluye mutuamente. Puede establecer la propiedad para la interfaz y el protocolo al mismo tiempo. Por ejemplo, puede activar el reenvío de paquetes de forma global en el protocolo y, a continuación, personalizar el reenvío de paquetes de cada interfaz IP del sistema. De esta manera, aunque esté activado globalmente, el reenvío de paquetes puede ser selectivo para el sistema.

Por ejemplo, debe activar el reenvío de paquetes en la interfaz IP de la siguiente manera:

```
# ipadm set-ifprop -p forwarding=on -m protocol-version interface
```

donde *protocol-version* es IPv4 o IPv6. Debe ejecutar el comando por separado para los paquetes IPv4 e IPv6.

El siguiente ejemplo muestra cómo activar solamente el reenvío de paquetes IPv4 en el sistema:

```
# ipadm show-ifprop -p forwarding net0
IFNAME   PROPERTY     PROTO   PERM   CURRENT   PERSISTENT   DEFAULT   POSSIBLE
net0     forwarding   ipv4    rw     off       off          off       on,off
net0     forwarding   ipv6    rw     off       --           off       on,off

# ipadm set-ifprop -p forwarding=on -m ipv4 net0
# ipadm show-ifprop net0
IFNAME   PROPERTY         PROTO  PERM  CURRENT  PERSISTENT  DEFAULT   POSSIBLE
...
net0     forwarding       ipv4   rw    on       on          off       on,off
...
```

Personalización de las propiedades de dirección IP

El comando `ipadm` le permite gestionar propiedades específicas de la dirección IP.

Puede personalizar las propiedades de direcciones IP para gestionar los siguientes parámetros de configuración de red:

- Longitud de la máscara de red
- Si una dirección IP puede utilizarse como una dirección de origen para los paquetes salientes
- Si la dirección pertenece a una zona global o no global
- Si la dirección es una dirección privada

Cuando trabaja con las propiedades de direcciones IP, utiliza los siguientes subcomandos `ipadm`:

- `show-addrprop -p` *property addrobj*: muestra las propiedades de dirección, según las opciones que utiliza.

  Para mostrar las propiedades de todas las direcciones IP, no especifique una propiedad ni un objeto de dirección. Para mostrar los valores de una sola propiedad para todas las direcciones IP, especifique sólo esa propiedad. Para mostrar todas las propiedades de un objeto de dirección determinado, especifique sólo el objeto de dirección.
- `set-addrprop -p` *property*=*value addrobj*: asigna valores a las propiedades de dirección. Tenga en cuenta que sólo puede establecer una propiedad de dirección por vez.
- `reset-addrprop -p` *property addrobj*: restaura los valores predeterminados a la propiedad de dirección.

Nota - Si desea cambiar la dirección IP de una interfaz específica, no utilice el subcomando `set-addressprop`. En cambio, suprima el objeto de dirección y cree uno nuevo con la nueva dirección IP. Consulte “Eliminación o modificación de la configuración de una interfaz IP” [79].

Por ejemplo, suponga que desea cambiar la máscara de red de una dirección IP. La dirección IP está configurada en la interfaz IP `net3`y se identifica mediante el nombre de objeto de dirección `net3/v4`. Los siguientes ejemplos muestran cómo revisar la máscara de red:

```
# ipadm show-addr
ADDROBJ     TYPE       STATE     ADDR
lo0/?       static     ok        127.0.0.1/8
net3/v4     static     ok        192.168.84.3/24

# ipadm show-addrprop -p prefixlen net3/v4
ADDROBJ  PROPERTY   PERM  CURRENT  PERSISTENT  DEFAULT   POSSIBLE
net3/v4  prefixlen  rw    24       24          24        1-30,32

# ipadm set-addrprop -p prefixlen=8 net3/v4
# ipadm show-addrprop -p prefixlen net3/v4
ADDROBJ  PROPERTY   PERM  CURRENT  PERSISTENT  DEFAULT   POSSIBLE
net3/v4  prefixlen  rw    8        24          24        1-30,32
```

Desactivación, eliminación y modificación de la configuración de la interfaz IP

Esta sección incluye los siguientes temas:

- “Eliminación de una configuración de interfaz IP” [78]
- “Desactivación de la configuración de una interfaz IP” [79]
- “Eliminación o modificación de la configuración de una interfaz IP” [79]

Eliminación de una configuración de interfaz IP

Utilice el subcomando `delete-ip` para eliminar una interfaz IP configurada. Este comando es especialmente importante para llevar a cabo ciertas tareas de configuración de enlace de datos. Por ejemplo, el cambio de nombre de un enlace de datos falla si se configuran interfaces IP mediante dicho enlace de datos. Antes de intentar cambiar el nombre del enlace de datos, deberá utilizar el comando `ipadm delete-ip` para eliminar la configuración IP existente. El siguiente ejemplo muestra los comandos que debe utilizar para realizar esta tarea:

```
# ipadm delete-ip interface
```

```
# dladm rename-link old-name new-name
# ipadm create-ip interface
# ipadm create-address parameters
```

Consulte también “Cambio de nombre de un enlace de datos” [33] para obtener más información. Para volver a configurar una interfaz IP después de haber cambiado el nombre del enlace de datos, consulte Cómo configurar una interfaz IPv4 [49].

Desactivación de la configuración de una interfaz IP

De manera predeterminada, una interfaz IP es sondeada y se vuelve parte de la configuración activa al crear la interfaz mediante el uso del comando `ipadm create-ip`. La interfaz se marca como `UP` cuando se crea la primera dirección en la interfaz.

Para eliminar una interfaz de la configuración activa sin destruir la configuración, utilice el subcomando `disable-if` como se indica a continuación. Este subcomando desasocia la interfaz del núcleo.

```
# ipadm disable-if -t interface
```

Debería hacer que la interfaz IP esté operativa y que el indicador aparezca como `UP`, de la siguiente manera:

```
# ipadm enable-if -t interface
```

Sugerencia - Para mostrar el estado actual de las interfaces IP, consulte “Obtención de información sobre interfaces IP” [82].

Eliminación o modificación de la configuración de una interfaz IP

El comando `ipadm delete-addr` suprime una configuración de dirección específica de una interfaz IP. Este comando resulta útil cuando simplemente desea eliminar una dirección IP del sistema o como parte del cambio de una dirección IP configurada en una interfaz. Si desea cambiar la dirección Ip que está configurado en una interfaz, primero debe eliminar la configuración de dirección IP original antes de asignar una nueva configuración de dirección. Consulte Cómo modificar una dirección IP existente [80].

Para obtener instrucciones sobre cómo crear una dirección IP para una interfaz, consulte Cómo configurar una interfaz IPv4 [49].

Nota - Una interfaz puede tener varias direcciones IP. Cada dirección se identifica mediante un objeto de dirección. Para asegurarse de eliminar la dirección correcta, debe conocer el objeto de dirección. Utilice el comando `ipadm show-addr` para mostrar las direcciones IP que están configuradas en una interfaz. Para obtener una explicación del objeto de dirección, consulte Cómo configurar una interfaz IPv4 [49]. Para obtener más información sobre la visualización de direcciones IP, consulte "Obtención de información sobre direcciones IP" [84].

▼ Cómo modificar una dirección IP existente

El siguiente procedimiento describe los pasos para volver a configurar una dirección IP existente del sistema.

1. **Conviértase en administrador**
2. **Suprima el objeto de dirección que representa la dirección IP que desea volver a configurar.**

   ```
   # ipadm delete-addr addrobj
   ```

3. **Asigne una nueva dirección IP mediante el mismo nombre de objeto de dirección.**

   ```
   # ipadm create-addr -a IP-address addrobj
   ```

   Para agregar otra interfaz al sistema, consulte Cómo configurar una interfaz IPv4.

4. **(Opcional) Si es necesario, modifique el nombre de host del sistema de la siguiente manera:**

   ```
   # hostname new-hostname
   ```

5. **(Opcional) Si la máscara de subred cambió, modifique las entradas de subred.**
6. **(Opcional) Si la dirección de subred cambió, cambie la dirección IP del enrutador predeterminado.**
   Consulte "Creación de rutas persistentes (estáticas)" [64] para obtener instrucciones.
7. **Reinicie el sistema para que los cambios surtan efecto.**

Supervisión de direcciones e interfaces IP

Utilice el comando `ipadm` para supervisar las interfaces IP y sus propiedades, y obtener información sobre ellas. Si se utiliza solo, el comando muestra información general sobre

las interfaces IP del sistema. Sin embargo, también puede utilizar varios subcomandos para restringir la información que desea mostrar mediante la siguiente sintaxis de comando:

ipadm show-* *other-arguments interface*

- Para obtener información de la interfaz únicamente, use el subcomando `show-if`.
- Para obtener información de la dirección únicamente, use el subcomando `show-addr`.
- Para obtener información sobre las propiedades de interfaz, use el subcomando `show-ifprop`.
- Para obtener información sobre las propiedades de dirección, use el subcomando `show-addrprop`.

Para obtener una explicación de todos los campos que muestran los comandos `ipadm show-*`, consulte la página del comando man `ipadm`(1M).

Obtención de información general sobre las interfaces IP

El comando `ipadm` proporciona una imagen completa de las interfaces del sistema. Si se utiliza el comando sin subcomandos, se muestra la información predeterminada sobre todas las interfaces IP del sistema. Por ejemplo:

```
# ipadm
NAME         CLASS/TYPE STATE     UNDER  ADDR
lo0          loopback   ok        --     --
lo0/v4       static     ok        --     127.0.0.1/8
lo0/v6       static     ok        --     ::1/128
net0         ip         ok        --     --
net0/v4      static     ok        --     10.132.146.233/23
net0/v4      dhcp       ok        --     10.132.146.234/23
ipmp0        ipmp       degraded  --     --
ipmp0/v6     static     ok        --     2001:db8:1:2::4c08/128
net1         ip         failed    ipmp0  --
net1/v6      addrconf   ok        --     fe80::124:4fff:fe58:1831/10
net2         ip         ok        ipmp0  --
net2/v6      addrconf   ok        --     fe80::214:4fff:fe58:1832/10
iptun0       ip         ok        --     --
iptun0/v4    static     ok        --     172.16.111.5->172.16.223.75
iptun0/v6    static     ok        --     fe80::10:5->fe80::223:75
iptun0/v6a   static     ok        --     2001:db8:1a0:7::10:5->2001:db8:7a82:64::223:75
```

La salida anterior muestra la siguiente información:

- Interfaces IP.
- Clase de cada interfaz.
- Estado de cada interfaz.

- Estado de la interfaz: ya sea una interfaz IP “independiente” o una interfaz subyacente para otro tipo de configuración de interfaz. En el ejemplo, `net1` y `net2` son interfaces subyacentes de `ipmp0`, como se indica en la columna `UNDER`.
- Los objetos de dirección que están asociados con la interfaz. Los objetos de dirección identifican una dirección IP específica. Estos objetos de dirección aparecen con sangrado debajo del encabezado `NAME` para distinguirlos de los nombres de interfaz.
- Tipo de dirección IP, que aparece con sangrado debajo del encabezado `CLASS/TYPE` y que pueda ser `static`, `dhcp`, etc.
- Las direcciones reales que aparecen en la columna `ADDRESS`.

Obtención de información sobre interfaces IP

Para obtener información sobre interfaces IP, utilice el subcomando `ipadm show-if` *interface*. Si no especifica una interfaz, la información incluye todas las interfaces del sistema.

Los campos de la salida del comando hacen referencia a la siguiente información:

`IFNAME` Hace referencia a la interfaz cuya información se muestra.

`CLASS` Hace referencia a la clase de interfaz, que puede ser una de cuatro:

- `ip` hace referencia a una interfaz IP.
- `ipmp` hace referencia a una interfaz IPMP.
- `vni` hace referencia a una interfaz virtual.
- `loopback` hace referencia a una interfaz de bucle de retorno, que se crea automáticamente. Excepto la interfaz de bucle de retorno, puede crear manualmente las 3 clases de interfaz restantes.

`STATE` Hace referencia al estado de la interfaz, que puede ser uno de los siguientes: `ok`, `offline`, `failed` , `down` o `disabled`.

El estado `failed` se aplica a los grupos IPMP y puede hacer referencia a un enlace de datos o a una interfaz IP que no está en funcionamiento y no puede alojar tráfico. Si la interfaz IP pertenece a un grupo IPMP, la interfaz IPMP puede seguir recibiendo y enviando tráfico mediante otras interfaces IP activas del grupo.

El estado `down` hace referencia a una interfaz IP desconectada por el administrador.

El estado `disable` hace referencia a la interfaz IP que se desconecta mediante el comando `ipadm disable-if`.

`ACTIVE` Indica si la interfaz se está utilizando para alojar tráfico, y se establece en `yes` o `no`.

`OVER` Se aplica sólo a la clase de interfaz IPMP y hace referencia a las interfaces subyacentes que constituyen la interfaz o el grupo IPMP.

A continuación se muestra un ejemplo de la información que muestra el comando:

```
# ipadm show-if
IFNAME       CLASS        STATE     ACTIVE     OVER
lo0          loopback     ok        yes        --
net0         ip           ok        yes        --
net1         ip           ok        yes        --
tun0         ip           ok        yes        --
```

Obtención de información sobre las propiedades de la interfaz IP

Utilice el comando `ipadm show-ifprop` *interface* para obtener información sobre las propiedades de las interfaces IP. Si no especifica una propiedad ni una interfaz, se muestra información de todas las propiedades de todas las interfaces IP del sistema.

Los campos de la salida del comando hacen referencia a lo siguiente:

`IFNAME` Hace referencia a la interfaz IP cuya información se muestra.

`PROPERTY` Hace referencia a la propiedad de la interfaz. Una interfaz puede tener varias propiedades.

`PROTO` Hace referencia al protocolo al que se aplica la propiedad, que puede ser IPv4 o IPv6.

`PERM` Se refiere a los permisos posibles de una propiedad determinada, que pueden ser de sólo lectura, sólo escritura, o ambos.

`CURRENT` Indica el valor actual de la propiedad en la configuración activa.

`PERSISTENT` Hace referencia al valor de la propiedad que se volverá a aplicar cuando se reinicie el sistema.

`DEFAULT` Indica el valor predeterminado de la propiedad especificada.

`POSSIBLE` Se refiere a una lista de valores que se pueden asignar a la propiedad especificada. Para valores numéricos, se muestra un rango de valores aceptables.

Nota - Si un valor de campo es desconocido, como cuando una interfaz no admite la propiedad cuya información se solicita, el valor aparece como un signo de interrogación (`?`).

El ejemplo siguiente muestra el tipo de información que el subcomando `show-ifprop` muestra:

```
# ipadm show-ifprop -p mtu net1
IFNAME  PROPERTY  PROTO  PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
net1    mtu       ipv4   rw    1500      --         1500     68-1500
net1    mtu       ipv6   rw    1500      --         1500     1280-1500
```

Obtención de información sobre direcciones IP

Para obtener información sobre direcciones IP, utilice el comando `ipadm show-addr` *interface*. Si no especifica una interfaz, se muestra la información sobre todas las direcciones IP del sistema.

Los campos de la salida del comando hacen referencia a lo siguiente:

`ADDROBJ` — Especifica el objeto de dirección cuya dirección IP se está mostrando.

`TYPE` — Indica si la dirección IP es `static`, `dhcp` o `addrconf`. El valor `addrconf` indica que la dirección se obtuvo mediante la configuración de dirección sin estado o con estado.

`STATE` — Describe el estado del objeto de dirección en la configuración activa. Para obtener una lista completa de estos valores, consulte la página del comando man `ipadm`(1M).

`ADDR` — Especifica la dirección IP que se configurada mediante la interfaz. La dirección puede ser IPv4 o IPv6. Una interfaz de túnel muestra las direcciones locales y remotas.

Para obtener información acerca de los túneles, consulte el Capítulo 5, “Administración de túneles IP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.

A continuación se muestra un ejemplo de la información que proporciona el subcomando `show-addr`:

```
# ipadm show-addr
ADDROBJ           TYPE       STATE     ADDR
lo0/v4            static     ok        127.0.0.1/8
net0/v4           static     ok        192.168.84.3/24
tun0/v4           static     ok        172.16.134.1-->172.16.134.2
```

Si especifica una interfaz con el comando y la interfaz tiene varias direcciones, se mostrará información similar a la siguiente:

```
# ipadm show-addr net0
ADDROBJ           TYPE       STATE     ADDR
```

```
net0/v4          static     ok        192.168.84.3/24
net0/v4a         static     ok        10.0.1.1/24
net0/v4bc        static     ok        172.16.10.1
```

Un objeto de dirección que aparece como *interface*/*?* indica que la dirección fue configurada en la interfaz por una aplicación que no utilizó las API `libipadm`. Estas aplicaciones no están bajo el control del comando `ipadm`, por lo que se necesita que el nombre del objeto de dirección use el formato *interface*/*user-defined-string*. Para ver ejemplos de la asignación de direcciones IP, consulte Cómo configurar una interfaz IPv4 [49].

Obtención de información sobre las propiedades de direcciones IP

Para obtener información sobre propiedades de direcciones IP, utilice el comando `ipadm show-addrprop` *addrobj*. Para mostrar todas las propiedades, omita la opción *addrobj*. Para mostrar una sola propiedad para todas las direcciones IP, especifique sólo esa propiedad. Para mostrar todas las propiedades de una dirección específica, especifique sólo la opción *addrobj*.

Los campos de la salida del comando hacen referencia a lo siguiente:

`ADDROBJ`	Se refiere al objeto de dirección cuyas propiedades se muestran.
`PROPERTY`	Hace referencia a una propiedad del objeto de dirección. Un objeto de dirección puede tener varias propiedades.
`PERM`	Se refiere a los permisos posibles de una propiedad determinada, que pueden ser de sólo lectura, sólo escritura, o ambos.
`CURRENT`	Hace referencia al valor real de la propiedad en la configuración actual.
`PERSISTENT`	Hace referencia al valor de la propiedad que se volverá a aplicar cuando se reinicie el sistema.
`DEFAULT`	Indica el valor predeterminado de la propiedad especificada.
`POSSIBLE`	Se refiere a una lista de valores que se pueden asignar a la propiedad especificada. Para valores numéricos, se muestra un rango de valores aceptables.

A continuación, se muestra un ejemplo del tipo de información que muestra el subcomando `show-addrprop`:

```
# ipadm show-addrprop net1/v4
ADDROBJ   PROPERTY     PERM   CURRENT         PERSISTENT  DEFAULT          POSSIBLE
```

```
net1/v4   broadcast    r-     192.168.84.255  --          192.168.84.255   --
net1/v4   deprecated   rw     off             --          off              on,off
net1/v4   prefixlen    rw     24              24          24               1-30,32
net1/v4   private      rw     off             --          off              on,off
net1/v4   transmit     rw     on              --          on               on,off
net1/v4   zone         rw     global          --          global           --
```

♦ ♦ ♦ CAPÍTULO 4

Administración de servicios de nombres y directorios en un cliente de Oracle Solaris

En este capítulo, se describe cómo configurar los servicios de nombres para un sistema cliente de host de Oracle Solaris. Para obtener una descripción general completa de los servicios de nombres y directorios, y de la administración por parte del servidor, consulte "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ".

Para obtener información sobre la resolución de problemas de configuración de los servicios de nombres y directorios, consulte el Capítulo 3, "Resolución de problemas de servicios de nombres" de "Resolución de problemas de administración de redes en Oracle Solaris 11.2 ".

Este capítulo se divide en los siguientes apartados:

Nota - Las tareas que se describen en este capítulo se aplican a redes IPv4 e IPv6, a menos que se indique lo contrario.

Novedades en la configuración del servicio de nombres

Las siguientes funciones son nuevas o cambiaron:

- **Migración de configuración del sistema y los servicios de nombres a SMF**: en esta versión, los servicios de nombres se gestionan mediante la utilidad de gestión de servicios (SMF). El comportamiento anterior, donde podía modificar un determinado archivo para configurar servicios de nombres, por ejemplo `/etc/nsswitch.conf` y `/etc/resolv.conf` ya no funciona. Los archivos de configuración heredados se mantienen en esta versión de Oracle Solaris sólo para tener compatibilidad con versiones anteriores de Oracle Solaris. El

contenido de estos archivos se genera mediante el servicio SMF que pertenece al servicio de nombres específico.

Si no existe ninguna configuración de red, los servicios de nombres quedan predeterminados para el comportamiento `files only`, en lugar de `nis files`. El servicio SMF `svc:/system/name-service/cache` debe estar activado en todo momento. Tenga en cuenta también que si realiza cambios de configuración en estos servicios mediante comandos SMF, los servicios deben estar activados, actualizados o ambos para que se apliquen los cambios. Consulte las páginas del comando man `svccfg`(1M) y `svcadm`(1M).

- **Capacidades de comprobación de errores** `resolv.conf`: antes de la migración de los servicios de nombres a SMF, los errores del archivo `resolv.conf` de configuración se procesaban en silencio y no producían advertencias. Como resultado, el archivo `resolv.conf` no se comportó según el modo en que se había configurado. Oracle Solaris 11 presenta comprobación de errores básica a través de plantillas SMF para que las condiciones de error ahora se informen correctamente. Consulte la página del comando man `resolv.conf`(4).
- **Configuración del servidor Sistema de nombre de dominio (DNS)**: el proceso para configurar un servidor DNS cambió. Para obtener más instrucciones, consulte "Administración de DNS (tareas)" de "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ".

Descripción general de la configuración de los servicios de nombres y directorios

Un servicio de nombres realizan búsquedas de información almacenada, como nombres de host y direcciones, nombres de usuario, contraseñas, permisos de acceso, etc. Esta información está disponible para que los usuarios puedan iniciar una sesión en su host, tener acceso a los recursos y se les concedan los permisos. La información del servicio de nombres se puede almacenar en archivos, mapas o diferentes formatos de archivos de base de datos. Estos repositorios de información pueden ser locales en el sistema o estar alojados en una base de datos o un repositorio basado en red de manera central. Sin un servicio de nombres central, cada host tendría que conservar su propia copia de esta información. Si centraliza todos los datos, la administración resulta más fácil. Los servicios de nombres son fundamentales para cualquier red informática.

Los siguientes servicios de nombres y directorios son compatibles:

- **Sistema de nombres de dominios (DNS)**

  DNS es una base de datos distribuida y jerárquica que se implementa en una red TCP/IP. Principalmente se utiliza para buscar direcciones IP para los nombres de host de Internet y los nombres de host para direcciones IP. Los datos se distribuyen a través de la red y se ubican mediante el uso de nombres separados por puntos que se leen de derecha a

izquierda. DNS también se utiliza para almacenar otra información de host relacionada con Internet, como información de enrutamiento de intercambio de correo, datos de ubicación y servicios disponibles. La estructura jerárquica de la naturaleza del servicio permite la administración local de dominios locales, a la vez que proporciona cobertura internacional de otros dominios que están conectados a a Internet, a una intranet o ambas. Para obtener más información, consulte “Descripción del servicio de nombres DNS” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

Dos extensiones para el protocolo DNS son gestionadas por el servicio `svc:network/dns/multicast`. DNS de multidifusión (mDNS) implementa DNS en una red pequeña donde ningún servidor DNS convencional se ha instalado. La detección de servicios DNS (DNS-SD) amplía el DNS de multidifusión para que también proporcione una detección de servicios simple (exploración de red). Consulte “Descripción de DNS de multidifusión y detección de servicios” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

- **Sistema de información de redes (NIS)**

  NIS (que se pronuncia "niss" en esta guía) se desarrolló independientemente de DNS. NIS se centra en facilitar la administración de la red al proporcionar un control centralizado sobre una variedad de información de red. NIS almacena información acerca de la red, nombres y direcciones de equipo, usuarios y servicios de red. Esta recopilación de información de red se conoce como *espacio de nombres NIS*. Para obtener más información, consulte “Descripción del servicio de nombres NIS” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

- **Protocolo ligero de acceso a directorios (LDAP)**

  LDAP es el protocolo de red seguro de que se utiliza para acceder a los servidores de directorios para servicios de nombres distribuidos y otros servicios de directorio. Este protocolo basado en estándares admite una estructura de base de datos jerárquica. Se puede utilizar el mismo protocolo para proporcionar servicios de nombres que estén en UNIX y en entornos de varias plataformas. Oracle Solaris es compatible con LDAP junto con Oracle Directory Server Enterprise Edition (anteriormente Sun Java System Directory Server), además de otros servidores de directorio LDAP. Para obtener más información, consulte “Descripción de los servicios de nombres LDAP” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

Para obtener una descripción general completa de los servicios de nombres (del lado del servidor y del lado del cliente) compatibles en Oracle Solaris, consulte el Capítulo 1, “Acerca de los servicios de nombres y directorios” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ” y “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ”.

Acerca del servicio SMF name-service/switch

El servicio SMF name-service/switch es un servicio de selección configurable que permite especificar qué servicio de información de nombres u origen se va a utilizar para cada tipo de información de red.

El conmutador de servicios de nombres es utilizado por aplicaciones cliente que llaman a cualquiera de las siguientes interfaces:

- gethostbyname
- getpwuid
- getpwnam
- getaddrinfo

El servicio SMF name-service/switch define qué servicio de nombres o servicios se deben utilizar para cada base de datos de red. Esta información se almacenaba anteriormente en el archivo /etc/nsswitch.conf. Aunque este archivo todavía existe, los valores de configuración que contiene el archivo deben ser modificados por el cambio de las propiedades adecuadas en este servicio SMF.

Puede mostrar estas propiedades de la siguiente manera:

```
$ svccfg -s name-service/switch listprop config
  config                      application
  config/default              astring     files
  config/value_authorization astring     solaris.smf.value.name-service.switch
  config/password             astring     "files ldap"
  config/group                astring     "files ldap"
  config/host                 astring     "files dns"
  config/automount            astring     "files ldap"
```

La propiedad config/default especifica qué origen u orígenes predeterminados se deben buscar. Si una base de datos determinada no tiene su propio conjunto de propiedades, se utiliza el origen o los orígenes predeterminados. En el ejemplo anterior, todas las bases de datos, a excepción de password, group, host y automount, usaban archivos locales como origen. Si se requiere un origen u orígenes diferentes a los predeterminados, se crea una propiedad de la base de datos específica. En este ejemplo, se busca password, groups y automount en archivos locales primero y luego en LDAP. Las búsquedas de host se realizan primero en archivos locales y luego en DNS.

Si cambia los servicios de nombres que están activos en el sistema, debe actualizar las propiedades adecuadas del servicio SMF name-service/switch para utilizar el servicio de nombres correcto. Por ejemplo, imagine que name-service/switch se configuró de forma similar al ejemplo anterior, y luego desactivó LDAP y activó NIS en su lugar.

- En este caso, debe definir las siguientes propiedades del servicio name-service/switch para utilizar archivos y NIS:

- `config/password`
- `config/group`
- `config/automount`

Debería escribir los siguientes comandos para configurar estas propiedades correctamente:

```
# svccfg -s name-serivce/switch setprop config/password = astring: "'files nis'"
# svccfg -s name-serivce/switch setprop config/group = astring: "'files nis'"
# svccfg -s name-serivce/switch setprop config/automountconfig/password = astring:
 "'files nis'"
# svccfg -s name-service/switch:default refresh
```

Para obtener más información, consulte el Capítulo 2, “Acerca del cambio de servicio de nombres” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ” y “Configuración del conmutador de servicio de nombres” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

Configuración de un sistema para el modo de archivos locales

Al ejecutar el sistema en modo de archivos locales, el sistema obtiene toda la información de configuración TCP/IP de los archivos que se encuentran en un directorio local. En el modo de cliente de red, la información de configuración se proporciona para todos los sistemas de la red mediante un servidor de configuración de red remota.

Normalmente, los siguientes servidores de la red se ejecutan en modo de archivos locales:

- Servidores de configuración de red
- Servidores NFS
- Servidores de nombres que proporcionan servicios NIS, LDAP o DNS
- Servidores de correo
- Enrutadores

Debido a que los clientes pueden ejecutar en modo de cliente de red o en modo de archivos locales, puede tener cualquier combinación de estos modos con los que se configuran los diferentes sistemas.

▼ Cómo configurar un sistema para el modo de archivos locales

1. **Conviértase en un administrador.**
2. **Configure las interfaces IP del sistema con las direcciones IP asignadas.**

Consulte Cómo configurar una interfaz IPv4.

3. **Verifique que el nombre de host se haya definido correctamente.**

```
# hostname
```

Para obtener más información, consulte la página del comando man `hostname`(1).

4. **Compruebe que las entradas de `/etc/inet/hosts` sean actuales.**

Oracle Solaris crea entradas para la interfaz de red principal, la dirección en bucle de retorno y cualquier interfaz adicional que se haya configurado durante la instalación. Si las entradas no son actuales, agregue las direcciones IP y los nombres correspondientes para las interfaces de red que se hayan agregado al sistema tras la instalación.

5. **Especifique el dominio completo del sistema como una propiedad del servicio SMF `nis/domain`.**

Por ejemplo, especifique `deserts.worldwide.com` como el valor para la propiedad `domainname` del servicio SMF `nis/domain` de la siguiente manera:

```
# domainname domainname
```

Este paso hace que el cambio sea persistente.

6. **Agregue la información de enrutamiento.**

Nota - Si está usando servicios DHCP, puede omitir este paso.

Para obtener instrucciones, consulte “Configuración de rutas” [63].

7. **Agregue la información de la máscara de red, si corresponde.**

Nota - Si está usando servicios DHCP, puede omitir este paso.

a. **Escriba el número de red y la máscara de red en el archivo `/etc/inet/netmasks`.**

Para crear entradas, utilice el formato *número_red*, *máscara_red*. Por ejemplo, para especificar el número de red de clase C `192.168.83`, debería escribir la siguiente información:

```
192.168.83.0    255.255.255.0
```

Para las direcciones CIDR, convierta el prefijo de red en la representación decimal con punto equivalente. Por ejemplo, escriba la siguiente información para expresar el prefijo de red CIDR `192.168.3.0/22`.

```
192.168.3.0     255.255.252.0
```

b. **Cambie el origen de consulta para la máscara de red en la propiedad `name-service/switch`, de manera que se busquen sólo los archivos locales; a continuación, actualice la instancia.**

```
# svccfg -s name-service/switch setprop config/netmask = astring: "files"
# svccfg -s name-service/switch:default refresh
```

8. **Reinicie el sistema.**

Configuración de un cliente DNS

DNS tiene dos partes: un servicio que proporciona respuestas y un cliente que consulta el servicio. En Oracle Solaris, el servicio DNS predeterminado es proporcionado por Berkeley Internet Name Domain (BIND) desde Internet Systems Consortium (ISC) y su daemon de servidor `named` asociado. El cliente DNS consta de una recopilación de utilidades y bibliotecas.

Para obtener más información relacionada con la tarea, consulte “Administración de DNS (tareas)” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

▼ Cómo activar un cliente DNS

1. **Conviértase en un administrador.**

2. **Enumere los dominios para buscar y las direcciones IP para los servidores de nombres DNS, luego actualice el repositorio SMF. Por ejemplo:**

```
# svccfg -s network/dns/client
   svc:/network/dns/client> setprop config/search = astring: ("example.com"
 "sales.example.com")
   svc:/network/dns/client> setprop config/nameserver = net_address: (192.168.1.10
 192.168.1.11)
   svc:/network/dns/client> select network/dns/client:default
   svc:/network/dns/client:default> refresh
   svc:/network/dns/client:default> quit
```

Asegúrese de actualizar el servicio para que se apliquen los cambios.

3. **Actualice la información del conmutador de servicios de nombres para utilizar el DNS.**

El primer comando actualiza la información de configuración del DNS en el repositorio SMF.

```
# svccfg -s system/name-service/switch
```

```
svc:/system/name-service/switch> setprop config/host = astring: "files dns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

4. **Inicie los servicios necesarios para ejecutar el cliente DNS.**

```
# svcadm enable network/dns/client
# svcadm enable system/name-service/switch
```

5. **Verifique que el cliente DNS esté activado mediante uno de los siguientes comandos (o ambos):**

```
# dig knownserver.example.com
```

```
# getent hosts knownserver.example.com
```

El comando `dig` cuando se lo utiliza solo, comprueba que el cliente DNS esté activado. El comando `getent hosts` comprueba que el cliente DNS utilice el archivo `/etc/nsswitch.conf`.

ejemplo 4-1 Configuración de varias opciones de DNS para un cliente de manera simultánea

En el siguiente ejemplo, se muestra cómo debería definir múltiples opciones de `/etc/resolv.conf`.

```
# svccg
svc:> select /network/dns/client
svc:/network/dns/client> setprop config/options = "ndots:2 retrans:3 retry:1"
svc:/network/dns/client> listprop config/options
config/options astring     ndots:2 retrans:3 retry:1
svc:/network/dns/client> exit
# svcadm refresh dns/client
# grep options /etc/resolv.conf
options ndots:2 retrans:3 retry:1
```

Activación de DNS de multidifusión

Para que DNS de multidifusión (mDNS) y la detección de servicios DNS funcione, mDNS se debe estar implementado en todos los sistemas que participarán en mDNS. El servicio mDNS se utiliza para anunciar la disponibilidad de los servicios que se proporcionan en el sistema.

Antes de activar mDNS, asegúrese de que el paquete de software está instalado en el sistema. Si es necesario, instale el paquete de la siguiente manera:

```
# pkg install pkg:/service/network/dns/mdns
```

Parte del proceso de activación de mDNS es primero actualizar la información del conmutador del servicio de nombres. Para poder resolver hosts locales, debe cambiar la propiedad `config/`

host del servicio SMF name-service/switch para que incluya mdns como origen, de la siguiente manera:

```
#  /usr/sbin/svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns mdns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch> quit
```

Active el servicio SMF de mDNS de la siguiente manera:

```
# svcadm enable svc:/network/dns/multicast:default
```

Al activar el mDNS mediante este método, los cambios permanecen a través de actualizaciones y los reinicios. Para obtener más información, consulte la página del comando man svcadm(1M).

Anuncio de recursos para DNS

Puede utilizar el comando dns-sd para explorar y detectar servicios de forma similar a la forma en que se pueden utilizar los comandos ping o traceroute. El comando dns-sd es, más que nada, utilizado de manera interactiva, principalmente porque sus argumentos de línea de comandos y su formato de salida pueden cambiar con el paso del tiempo, lo que hace que invocarlo desde una secuencia de comandos de shell sea imprevisible y riesgoso. Además, la naturaleza asíncrona de la detección de servicios DNS (DNS-SD) no se presta a sí misma con facilidad a la programación orientada a la secuencia de comandos.

Para ver ejemplos, consulte "Anuncio de recursos para DNS" de "Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ". Consulte también la página del comando man dns-sd(1M).

Configuración de un cliente NIS

NIS es un servicio de nombres distribuido que se utiliza para identificar y ubicar objetos y recursos de red. NIS proporciona un método de almacenamiento y recuperación uniforme para la información de toda la red en forma de protocolo de transporte e independiente de los medios. NIS se desarrolló independientemente de DNS y tiene un enfoque levemente distinto. Mientras que DNS trata de facilitar la comunicación con el uso de nombres de equipos en lugar de direcciones IP numéricas, NIS se centra en facilitar la administración de la red al proporcionar control centralizado sobre distintos tipos de información de red.

Mediante la ejecución de NIS, puede distribuir bases de datos administrativas (mapas) entre una variedad de servidores (maestros y esclavos). Puede actualizar las bases de datos desde una

ubicación centralizada de manera automática y confiable, lo que garantiza que todos los clientes comparten la misma información del servicio de nombres en forma coherente y en toda la red. Para obtener información detallada, consulte el Capítulo 5, “Acerca del servicio de información de red” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

Hay dos servicios SMF que proporcionan servicio de cliente NIS en un sistema. Utilice el comando `svcadm` para activar, desactivar, reiniciar y actualizar estos servicios. Muestre el estado de los servicios NIS en un sistema como se indica a continuación:

```
# svcs \*nis\*
STATE          STIME    FMRI
online         Oct_09   svc:/network/nis/domain:default
online         Oct_09   svc:/network/nis/client:default
```

Para obtener información adicional relacionada con la tarea, consulte el Capítulo 6, “Instalación y configuración del servicio de información de red” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

▼ Cómo configurar un cliente NIS en modo de difusión

El modo de difusión es el método más sencillo para establecer un cliente NIS. Al iniciar el servicio SMF `nis/client`, el servicio ejecuta el comando `ypbind`, que busca un servidor NIS en la subred local. Si se encuentra una subred, el comando `ypbind` se enlaza a ella. Esta búsqueda se denomina difusión. Si no hay ningún servidor NIS en la subred local del cliente, el comando `ypbind` no puede realizar el enlace, y la máquina cliente no puede obtener datos de espacios de nombres del servicio NIS. Consulte Cómo configurar un cliente NIS mediante servidores NIS específicos [97].

1. **Conviértase en un administrador.**

2. **Establezca el nombre de dominio NIS.**

   ```
   # domainname example.com
   ```

3. **Si es necesario, realice cambios en el conmutador de servicios de nombres.**

   Consulte “Configuración del conmutador de servicio de nombres” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

4. **Inicie los servicios de clientes NIS.**

   ```
   # svcadm enable network/nis/domain
   # svcadm enable network/nis/client
   ```

▼ Cómo configurar un cliente NIS mediante servidores NIS específicos

Antes de empezar En el siguiente procedimiento, se requiere que los nombres de hosts (servidores) que se especifican en el paso 3 puedan ser resueltos por el DNS. Si no utiliza un DNS o escribe un nombre de host en lugar de una dirección IP, asegúrese de agregar una entrada apropiada para cada servidor NIS en el archivo `/etc/hosts` del cliente. Para obtener más información, consulte la página del comando man `ypinit`(1M).

1. **Conviértase en un administrador.**
2. **Defina el dominio NIS.**

   ```
   # domainname example.com
   # svcadm enable network/nis/domain
   ```

3. **Ejecute la secuencia de comandos de configuración de cliente.**

   ```
   # ypinit -c
   ```

   Se le solicita que nombre los servidores NIS desde donde el cliente obtiene la información del servicio de nombres. Puede enumerar el servidor maestro y todos los servidores esclavos que desee. Los servidores que enumera se pueden ubicar en cualquier lugar del dominio. Se recomienda primero enumerar los servidores más cercanos (con respecto a la red) a la máquina que los que están más distantes de la red.

4. **Active el cliente NIS.**

   ```
   # svcadm enable network/nis/client
   ```

▼ Cómo desactivar los servicios de cliente NIS

1. **Conviértase en un administrador.**
2. **Detenga los servicios de clientes NIS de la siguiente manera:**

   ```
   # svcadm disable network/nis/domain
   # svcadm disable network/nis/client
   ```

Configuración de un cliente LDAP

Para que un cliente de Oracle Solaris utilice LDAP como servicio de nombres, se deben cumplir los siguientes requisitos:

- El nombre de dominio del cliente debe tener servicio del servidor LDAP.
- El conmutador de servicios de nombres debe apuntar a LDAP para los servicios necesarios.
- El cliente debe estar configurado con todos los parámetros establecidos que definen su comportamiento.
- `ldap_cachemgr` se debe estar ejecutando en el cliente.
- Al menos un servidor para el que se configura un cliente debe estar activo y en ejecución.

El comando `ldapclient` es la clave para configurar un cliente LDAP, ya que realiza todas las tareas anteriores, excepto iniciar el servidor.

Al utilizar el modo fijo para la configuración de red, la forma más sencilla de configurar LDAP en un sistema cliente es activar el perfil `DefaultFixed` y realizar una configuración de red persistente. Luego, puede utilizar el comando `ldapclient` para completar la configuración de LDAP, mediante un perfil o mediante la configuración manual. Consulte la página del comando man `ldapclient`(1M) para obtener más información.

Para obtener información detallada sobre LDAP, consulte “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: LDAP ”.

Importación de la configuración de servicios de nombres

El comando `nscfg` transfiere la configuración de archivos heredados para los componentes del conmutador `name-service` al depósito SMF. Al actualizar a Oracle Solaris 11, la configuración del servicio de nombres del sistema se migra automáticamente a SMF. Sin embargo, si es necesario, puede migrar manualmente esta configuración a SMF con el comando `nscfg`.

El siguiente comando importa el archivo heredado y, a continuación, convierte y envía la configuración a SMF:

```
# /usr/sbin/nscfg import -f FMRI
```

Usar el comando `nscfg` es la manera más simple de completar la configuración de DNS son información de un archivo `resolv.conf` que ya existe. En el siguiente ejemplo, el comando `nscfg` lee la información del archivo `/etc/resolv.conf`, la convierte y, a continuación, la almacena en el servicio SMF `svc:/network/dns/client`.

```
# cp resolv.conf /etc/resolv.conf
# /usr/sbin/nscfg import -f dns/client
# svcadm enable dns/client
```

Al cambiar un servicio de nombres del sistema, también debe modificar la información del conmutador de servicios de nombres según corresponda y, posiblemente, deba eliminar la información obsoleta de la caché del servicio de nombres, como se muestra en el siguiente ejemplo:

```
# cp /etc/nsswitch.dns /etc/nsswitch.conf
# /usr/sbin/nscfg import -f name-service/switch
# svcadm refresh name-service/switch
# svcadm refresh name-service/cache
```

Para obtener más información, consulte la página del comando man `nscfg`(1M).

Restablecimiento de la configuración de servicios de nombres SMF

Puede restablecer las propiedades de configuración de un servicio de nombres SMF al modo `files only` como se indica a continuación:

```
# /usr/sbin/nscfg unconfig FMRI
# svcadm refresh name-service/switch
```

Por ejemplo, debe revertir los cambios realizados en la configuración de SMF en “Importación de la configuración de servicios de nombres” [98] de la siguiente manera:

```
# svcadm disable dns/client
# /usr/sbin/nscfg unconfig dns/client
# /usr/sbin/nscfg unconfig name-service/switch
# svcadm refresh name-service/switch
# svcadm refresh name-service/cache
```

♦ ♦ ♦ CAPÍTULO 5

Acerca de la administración de la configuración de red basada en perfiles en Oracle Solaris

En este capítulo se proporciona una descripción general de la configuración de red basada en perfiles, que se utiliza principalmente cuando el sistema usa el modo reactivo. El modo reactivo es compatible con varios tipos de perfiles para la gestión de la configuración de red en el sistema Oracle Solaris. Este modo se suele utilizar en equipos personales portátiles y en situaciones en las que cambian las condiciones de la red con frecuencia. En el modo reactivo, un daemon de red (`nwamd`) supervisa el estado del sistema y ajusta dinámicamente la configuración de la red si cambian las condiciones.

Para obtener información sobre el uso del modo fijo, el modelo de administración de red que se utiliza con más frecuencia en entornos corporativos, consulte el Capítulo 2, Administración de la configuración de enlaces de datos en Oracle Solaris y el Capítulo 3, Configuración y administración de direcciones e interfaces IP en Oracle Solaris.

Para obtener instrucciones paso a paso sobre la configuración y administración de perfiles de red, consulte el Capítulo 6, Administración de la configuración de red basada en perfiles en Oracle Solaris.

Este capítulo se divide en los siguientes apartados:

Acerca del modo reactivo

El modo reactivo significa que el sistema se adapta automáticamente a cualquier cambio en las condiciones de red y luego ajusta la configuración de la red actual sin necesidad de realizar

ninguna configuración manual. Por ejemplo, si la interfaz de red con cables se desconecta, si hay una nueva red inalámbrica disponible o si cambian las ubicaciones físicas, el sistema adapta su configuración de red en consecuencia.

Con la movilidad como objetivo principal, la política de configuración de red reactiva en Oracle Solaris permite que la configuración de red del sistema cambie de manera dinámica en respuesta a diferentes eventos de red o según usted lo solicite. Este tipo de configuración de red funciona mejor para equipos personales portátiles y en situaciones en las que cambian las condiciones de la red con frecuencia. Cuando se utiliza el modo reactivo, la configuración básica de Ethernet y Wi-Fi de un sistema se realizan automáticamente. El sistema se conecta de manera automática a una red con cables o inalámbrica durante el inicio y muestra notificaciones en el escritorio acerca del estado de la conexión de la red activa actualmente. Puede configurar perfiles reactivos con propiedades que determinan las condiciones bajo las que un perfil determinado está activado. Estas propiedades permiten que la configuración del perfil se aplique de manera dinámica en el sistema mediante el daemon de gestión de redes, `nwamd`, según sea necesario.

Los cambios de configuración de red reactiva normalmente se inician con los siguientes eventos y actividades:

- Conexión o desconexión de un cable Ethernet
- Conexión o desconexión de una tarjeta de red de área local inalámbrica (WLAN)
- Inicio de un sistema cuando una interfaz con cables o una interfaz inalámbrica están disponibles
- Reanudación luego de una suspensión cuando una interfaz con cables o una interfaz inalámbrica están disponibles (si esto se admite)
- Adquisición o pérdida de un permiso de DHCP

Puede utilizar dos comandos para administrar la configuración de red en el modo de reactivo: el comando `netcfg` para realizar cambios en la configuración de red a perfiles y el comando `netadm` para mostrar información acerca de perfiles y activar y desactivar perfiles. Para obtener más información, consulte las páginas del comando man `netcfg`(1M) y `netadm`(1M). Para obtener información relacionada con las tareas, consulte el Capítulo 6, Administración de la configuración de red basada en perfiles en Oracle Solaris.

El modo fijo, por otro lado, es lo opuesto al modo reactivo. Cuando se utiliza el modo fijo, el daemon de red crea una instancia de una configuración de red específica en el sistema, pero no ajusta automáticamente dicha configuración ante las diferentes condiciones de la red. Para obtener más información sobre el modo fijo, consulte “Acerca de los modos de configuración de red” [16].

Para obtener más información sobre todos los comandos de administración de red admitidos y cuándo usarlos, consulte “Comandos de administración de red de Oracle Solaris” [18].

Acerca de la configuración de red basada en perfil

Oracle Solaris proporciona un conjunto predeterminado de perfiles definidos por el sistema y la capacidad para crear varios tipos de perfiles reactivos definidos por el usuario con las propiedades y condiciones de activación que usted especifique para satisfacer sus necesidades concretas de red. Los perfiles definidos por el usuario se pueden utilizar para simplificar la configuración básica de enlaces de datos y direcciones IP del sistema, y para definir la configuración de la red más compleja en todo el sistema, por ejemplo, configuraciones de servicios de nombres, filtros IP y seguridad IP (IPsec)

Se admiten los siguientes tipos de perfiles:

- **Perfiles de configuración de red (NCP)**: un NCP es el tipo de perfil principal que se utiliza para especificar la configuración de enlaces de datos de red e interfaces IP. Los NCP se configuran con los valores de propiedad que especifican cómo se configura la red cuando se activa ese NCP determinado en el sistema. Los NCP pueden ser reactivos o fijos. Puede tener varios NCP reactivos configurados, pero Oracle Solaris sólo admite un NCP fijo denominado `DefaultFixed`.
- **Unidades de configuración de red (NCU)**: la información de configuración individual (propiedades) que define un NCP se especifican dentro de las NCU. Una NCU puede representar un enlace físico o una interfaz y contiene propiedades que especifican la configuración de ese enlace o interfaz.
- **Perfiles de ubicación**: un perfil de ubicación (también conocido como ubicación) especifica la configuración de red de todo el sistema, por ejemplo, servicios de nombres, dominio, configuración de filtro IP y configuración IPsec.
- **Modificadores de red externa (ENM)**: un ENM es un perfil que gestiona las aplicaciones responsables de crear la configuración de red que es externa a la configuración de red principal del sistema, por ejemplo, una aplicación VPN.
- **WLAN conocidas**: una WLAN es un perfil que almacena información acerca de redes inalámbricas que son detectadas por el sistema.

Descripciones de tipo de perfil

A continuación, se muestra una descripción detallada de cada uno de los tipos de perfil que se admiten en la versión de Oracle Solaris.

Descripción de un NCP

Un NCP define la configuración de red específica del sistema, por ejemplo, los enlaces de datos y las interfaces y direcciones IP. Las diferentes NCU (unidades de configuración de red) que conforman cada NCP especifican cómo configurar los distintos enlaces e interfaces de red, por ejemplo, qué interfaz o interfaces se deben traer adelante y en qué condiciones, así como la manera en que se obtiene la dirección IP para la interfaz.

El NCP `Automatic` representa todos los enlaces de red y las interfaces que están actualmente en el sistema. El contenido del NCP `Automatic` cambia si se agregan o eliminan dispositivos de red. El NCP `Automatic` proporciona acceso a un perfil que utiliza configuración automática de DHCP, que hace posible la obtención de direcciones IP para el sistema. Este NCP también implementa una política de selección de enlaces que favorece los enlaces con cables por sobre los enlaces inalámbricos. Si se requiere que se especifique una política de configuración de IP alternativa, o una política de selección de enlace alternativa, sería necesario crear otro NCP en el sistema. No puede suprimir el NCP `Automatic`. Puede copiar este NCP y realizar cambios en la copia. Consulte el Ejemplo 6-7, “Creación de un NCP mediante la clonación del NCP `Automatic`”.

Descripción de una NCU

Las NCU contienen los valores de propiedad que definen un NCP. Esas NCU representan los enlaces físicos y las interfaces individuales en un sistema. El proceso de configuración de un NCP definido por el usuario incluye la creación de NCU que especifiquen cómo y en qué condiciones se debe configurar cada enlace e interfaz.

Hay dos tipos de NCU:

- NCU de enlace: representan los dispositivos físicos (entidades de capa 2 en el modelo OSI [de interconexión de sistemas abiertos]).
- NCU de interfaz: representan interfaces IP (entidades de capa 3).

Las NCU de enlace representan las siguientes clases de capa de enlace de datos:

- Agregaciones
- Puentes
- Etherstubs
- Ethernet mediante IB (EoIB)
- Enlaces físicos (Ethernet o Wi-Fi)
- Túneles
- Redes de área local virtual extensible (VXLAN)
- Redes de área local virtual (VLAN)
- Tarjetas de la interfaz de red virtual (VNIC)

Las NCU de interfaz representan las siguientes clases de capa IP:

- Interfaces IP
- Interfaces IPMP
- Interfaces de VNI

Para obtener información sobre las propiedades que puede definir para los distintos tipos de objeto, consulte la página del comando man `netcfg`(1M)

Descripción de un perfil de ubicación

Un perfil de ubicación (también denominado simplemente *ubicación*) consta de información de configuración de red, como configuración de los servicios de nombres y del firewall que se aplican en conjunto para especificar la configuración de red de todo el sistema cuando dicha ubicación está activa. Debido a que una ubicación no necesariamente se corresponde a una ubicación física, puede configurar varios perfiles de ubicación para que satisfagan diferentes necesidades de redes. Por ejemplo, se puede usar una ubicación cuando está conectado a la intranet de la empresa. Se puede usar otra ubicación cuando está conectado a la red pública de Internet mediante un punto de acceso inalámbrico situado en la oficina.

De manera predeterminada, hay tres perfiles de ubicación predefinidos por el sistema:

- **DefaultFixed**

  La ubicación `DefaultFixed` se activa siempre que el NCP `DefaultFixed` está activo. La ubicación `DefaultFixed` no puede ser modificada directamente con el comando `netcfg`. Cuando esta ubicación está activada (como parte de la activación del NCP `DefaultFixed`), la, propiedades de la utilidad de gestión de servicios (SMF) pertinentes se actualizan para reflejar la configuración de la ubicación. Cuando se cierra el sistema o se activa otra ubicación, la configuración de las propiedades de SMF pertinentes se guarda como parte de la configuración de la ubicación `DefaultFixed`.

- **Automatic**

  La ubicación `Automatic` se activa si hay redes disponibles, pero ninguna otra ubicación la sustituye. Puede modificar la ubicación `Automatic` mediante el comando `netcfg`.

Nota - La ubicación `Automatic` no se debe confundir con el NCP `Automatic`. La ubicación `Automatic` define las propiedades de red de todo el sistema después de la configuración de red inicial de un sistema. El NCP `Automatic` especifica la configuración de red de enlaces e interfaces en un sistema.

- **NoNet**

  La ubicación `NoNet` tiene condiciones de activación muy específicas. El sistema aplica esta ubicación a un sistema independiente cuando ninguna interfaz local tiene una dirección IP asignada. Puede modificar la ubicación `NoNet` mediante el comando `netcfg`.

Las ubicaciones definidas por el usuario son idénticas a las ubicaciones definidas por el sistema, con excepción de que una ubicación definida por el usuario se configura con los valores que usted establece, mientras que las ubicaciones definidas por el sistema tienen valores preestablecidos.

Descripción de un ENM

Los ENM permiten especificar cuándo las aplicaciones o las secuencias de comandos deben realizar la configuración de red que es externa a la configuración especificada en los perfiles de ubicación y NCP. Los ENM también se pueden definir como servicios o aplicaciones que modifican directamente la configuración de red cuando se activan o se desactivan. Puede especificar las condiciones en las que se debe activar o desactivar un ENM. También puede activar o desactivar un ENM manualmente. A diferencia de un NCP o un perfil de ubicación, en los que sólo puede haber un tipo de perfil activo en el sistema en un momento determinado, pueden llegar a estar activos varios ENM en el sistema al mismo tiempo. Los ENM que están activos en un sistema en un momento determinado no dependen necesariamente del NCP o el perfil de ubicación activado en el sistema al mismo tiempo.

Aunque hay varias aplicaciones y servicios externos para los que puede crear un ENM, el ejemplo obvio es la aplicación VPN. Después de instalar y configurar una VPN en el sistema, puede crear un ENM que active y desactive automáticamente la VPN en las condiciones que especifique.

Nota - El modo de configuración de red reactiva no puede detectar automáticamente las aplicaciones externas que pueden modificar directamente la configuración de red de un sistema. Para gestionar la activación o desactivación de una aplicación VPN, o cualquier aplicación o servicio externo, primero debe instalar la aplicación y, a continuación, debe crear un ENM para ella mediante la interfaz de línea de comandos (CLI) o la GUI de administración de redes.

No se almacena ni se realiza seguimiento de la información persistente sobre cualquier configuración de red que se lleva a cabo por medio de un ENM exactamente de la misma forma en que almacena la información sobre un NCP o un perfil de ubicación. Sin embargo, el sistema es capaz de notar una configuración de red iniciada de manera externa y, luego, en función de los cambios de configuración realizados al sistema por un ENM, volver a evaluar qué ubicación debe estar activa y, posteriormente, activar esa ubicación. Un ejemplo sería pasar a una ubicación activada condicionalmente cuando cierta dirección IP está en uso. Si el servicio `svc:/network/physical:default` se reinicia en cualquier momento, se restablece la configuración de red especificada por el NCP activo. Los ENM también se reinician, y posiblemente anulan y recrean la configuración de red en el proceso.

Descripción de una WLAN conocida

Las WLAN conocidas son perfiles que se utilizan para gestionar redes inalámbricas conocidas para el sistema. Por lo tanto, el sistema mantiene una lista global de estas redes inalámbricas conocidas. Esta información se utiliza para determinar el orden en que se intenta conectar a redes inalámbricas disponibles. Si una red inalámbrica de la lista de WLAN conocidas está disponible, el sistema se conecta automáticamente a esa red. Si hay dos o más redes inalámbricas conocidas disponibles, el sistema intenta conectarse a la red inalámbrica con la prioridad más alta (número menor). Cualquier red inalámbrica nueva a la que se conecte se

agrega automáticamente a la parte superior de la lista de WLAN conocidas y se convierte en la red inalámbrica con la prioridad más alta.

El comportamiento predeterminado es preferir las WLAN a las que se haya conectado más recientemente por sobre las WLAN anteriores. En ningún momento más de una WLAN conocida puede compartir la misma prioridad. Si se agrega una nueva WLAN a la lista con el mismo valor de prioridad que una WLAN ya existente, la entrada existente se desplaza hacia una prioridad de valor inferior. Después, el valor de prioridad de cada otra WLAN de la lista se cambia dinámicamente a una prioridad de valor inferior.

También es posible asociar un nombre de clave con una WLAN conocida. Un *nombre de clave* le permite crear sus propias claves mediante el comando `dladm create-secobj`. Puede asociar esta clave con las WLAN si agrega los nombres de objeto seguro a la propiedad `keyname` de las WLAN. Para obtener información, consulte la página del comando man `dladm`(1M).

Para obtener más información sobre la gestión de WLAN desde la línea de comandos, consulte “Administración de WLAN conocidas en modo reactivo” [153].

Perfiles definidos por el usuario y por el sistema

Un NCP `Automatic` es un perfil definido por el sistema que está formado por una NCU de enlace y una NCU de interfaz por cada enlace físico presente en el sistema. La política de activación de NCU en este NCP es preferir los enlaces conectados con cable por sobre los enlaces inalámbricos, y conectar IPv4 e IPv6 en cada enlace activado. DHCP se utiliza para obtener las direcciones IPv4. Para obtener las direcciones IPv6, se utiliza configuración automática y DHCP sin estado. El NCP `Automatic` cambia de manera dinámica cuando se insertan o se eliminan nuevos enlaces en el sistema. Todas las NCU que corresponden al enlace insertado o eliminado también se agregan o eliminan al mismo tiempo. El daemon `nwamd` actualiza automáticamente el perfil.

Cuando está activo, el NCP `Automatic` implementa la siguiente política básica:

- Se configuran todas las interfaces Ethernet disponibles (conectadas) mediante DHCP.
- Si no hay interfaces Ethernet conectadas, o si ninguna puede obtener una dirección IP, se activa una interfaz inalámbrica que automáticamente establece una conexión con la mejor WLAN disponible de la lista de WLAN conocidas. Consulte “Descripción de una WLAN conocida” [106].
- Mantenga activa la ubicación `NoNet` activa hasta obtener al menos una dirección IPv4. Consulte “Descripción de un perfil de ubicación” [105]. Esta ubicación proporciona un conjunto estricto de las reglas de filtro IP que sólo transfieren datos que sean relevantes para la adquisición de direcciones IP (mensajes autoconf DHCP e IPv6). Se pueden modificar todas las propiedades de la ubicación `NoNet`, a excepción de las condiciones de activación.
- Cuando se haya asignado al menos una dirección IP a una de las interfaces del sistema, active la ubicación `Automatic`. Esta ubicación no tiene Filtro IP ni reglas de IPsec. La

ubicación aplica datos de configuración de sistema de nombre de dominio (DNS, Domain Name System) que se obtienen del servidor DHCP. Al igual que con la ubicación `NoNet`, se pueden modificar todas las propiedades de la ubicación `Automatic`, con la excepción de sus condiciones de activación.

De manera opcional, puede configurar los NCP definidos por el usuario. Debe agregar o eliminar de manera explícita las NCU desde el NCP especificado. También puede crear NCU que no tengan una correlación con ningún enlace que esté actualmente presente en el sistema. Asimismo, puede determinar la política para el NCP definido por el usuario. Por ejemplo, puede permitir la activación de varios enlaces e interfaces en el sistema en un momento determinado, así como especificar diferentes relaciones de dependencia entre las NCU y las direcciones IP estáticas.

Directrices para utilizar la configuración de red basada en perfiles

La configuración de red basada en el perfil se adhiere a las siguientes directrices:

- Sólo un perfil de configuración de red (NCP) y un perfil de ubicación pueden estar activos en cualquier momento en un sistema. Todos los demás NCP existentes en el sistema no son operativos.
- El NCP activo puede ser reactivo o fijo (`DefaultFixed`). Con un NCP reactivo, el sistema supervisa la configuración de red para adaptarse a los cambios en el entorno de red del sistema. Con el NCP `DefaultFixed` (el único perfil fijo del sistema), la configuración de red se instancia, pero no se supervisa.
- Los valores de las diferentes propiedades de un NCP constituyen una política que controla cómo el perfil gestiona la configuración de red del sistema.
- Cualquier cambio en las propiedades del NCP se implementan inmediatamente como nuevos valores de propiedades, que luego pasan a formar parte de la política del perfil para gestionar la configuración de red cada vez que un perfil está activo.
- Si el sistema utiliza el modo reactivo, el NCP activo que gestiona su configuración de red es el NCP `Automatic` o un NCP reactivo definidos por el usuario que usted creó. Cuando un NCP reactivo está activo, puede administrar la configuración de red con los comandos `netcfg` y `netadm`.

Si el sistema se utiliza en el modo fijo, el NCP activo que gestiona la configuración de red siempre es `DefaultFixed`. Cuando este NCP está activo, puede administrar la configuración de red mediante los comandos `dladm` y `ipadm`. Consulte el Capítulo 2, Administración de la configuración de enlaces de datos en Oracle Solaris y el Capítulo 3, Configuración y administración de direcciones e interfaces IP en Oracle Solaris para obtener más información.

Política de activación de perfil

Los modos de activación para los perfiles son manual, automático o condicional. Cuando un perfil reactivo está activo, los cambios en el entorno de la red hacen que el sistema vuelva a evaluar la configuración de red y, a continuación, realice la "estimación óptima" sobre qué NCP reactivo y ubicación activar, según las condiciones actuales. Entre los cambios en las condiciones de la red se incluyen la conexión y desconexión del cable Ethernet, la obtención o pérdida de un permiso DHCP y la detección de una nueva red inalámbrica. En todo momento, debe haber en una ubicación y un NCP activo en el sistema.

El modo de configuración de red reactiva permite le especificar la política de activación de los NCP reactivos. Esta política determina cuándo se activan las NCU. Cada perfil de ubicación contiene además propiedades que definen los criterios de activación.

Las NCU, las ubicaciones y los ENM tienen la propiedad `activation-mode`. Los valores permitidos para cada uno de los tipos de perfil son distintos. Además, la forma en que se valida la propiedad `activation-mode` varía para cada tipo de perfil, así como las condiciones en las que se activa cada perfil.

Nota - La propiedad `activation-mode` para la NCU se puede establecer en `manual` o `prioritized`. La propiedad `activation-mode` del perfil de ubicación se puede definir en `manual`, `conditional-any`, `conditional-all` o `system`.

La política de activación de NCP se aplica mediante el uso de propiedades y condiciones que se pueden especificar para cada NCU. Entre los ejemplos de las políticas que puede especificar, se incluyen: “preferir conexiones con cables antes que conexiones inalámbricas” o “activar una interfaz a la vez”. En las propiedades configuradas para cada tipo de NCU, se define cómo y cuándo se activan los NCP. Para obtener más información sobre las condiciones de activación, consulte la página del comando man `netcfg`(1M).

Nota - Una NCU de interfaz está asociada con una NCU de enlace subyacente. Cada NCU de interfaz se activa cuando la NCU de enlace asociada se activa. La dependencia en la NCU de enlace subyacente nunca se puede eliminar. Si activa una NCU de interfaz sin activar su NCU de enlace asociada, la NCU de interfaz en realidad no se activará hasta que la NCU subyacente para esa interfaz se active.

Modos de activación de perfil

Las NCU definidas por el usuario, los perfiles de ubicación y los ENM tienen propiedades `activation-mode`. La propiedad `activation-mode` se define al crear o modificar un perfil mediante el comando `netcfg`. Los NCP no tienen ninguna propiedad `activation-mode`. Todos los NCP se activan de forma manual.

En la siguiente tabla, se describen los valores posibles para la propiedad `activation-mode` para los diferentes tipos de perfil.

TABLA 5-1 Valores de propiedad `activation-mode`

Tipo de perfil	Valor de `activation-mode`
NCU	`manual` o `prioritized`
Ubicación	`manual`, `conditional-any`, `conditional-all` o `system`
ENM	`manual`, `conditional-any` o `conditional-all`

Para obtener más información sobre cómo activar y desactivar perfiles, consulte “Activación y desactivación de perfiles” [113].

Requisitos de seguridad para el uso de la configuración de red basada en perfiles

El daemon `netcfgd` controla el repositorio donde se almacena toda la información de configuración de red. El comando `netcfg`, la GUI de administración de redes y el daemon `nwamd` envían solicitudes al daemon `netcfgd` para acceder al repositorio.

La implementación actual de la configuración de red utiliza las siguientes autorizaciones para realizar tareas específicas:

- `solaris.network.autoconf.read`: permite la lectura de datos de perfiles de red, que verifica el daemon `netcfgd`.
- `solaris.network.autoconf.write`: permite la escritura de datos de perfiles de red, que verifica el daemon `netcfgd`.
- `solaris.network.autoconf.select`: permite que se apliquen nuevos datos de configuración, que verifica el daemon `nwamd`.
- `solaris.network.autconf.wlan`: permite la escritura de datos de configuración de WLAN conocidas.

Estas autorizaciones se registran en la base de datos `auth_attr`. Consulte la página del comando man `auth_attr`(4).

La autorización `solaris.network.autoconf.read` se incluye en el perfil de derechos de usuario de Solaris básico, que se asigna a todos los usuarios de manera predeterminada. Cualquier usuario con esta autorización puede, por lo tanto, ver el estado actual de la red y el contenido de todos los perfiles de red.

Se proporcionan dos perfiles de derechos adicionales: Network Autoconf User y Network Autoconf Admin. El perfil Network Autoconf User tiene las autorizaciones `read`, `select` y `wlan`. El perfil Network Autoconf Admin agrega la autorización `write`. El perfil Network Autoconf User está asignado al perfil Console User . De manera predeterminada, cualquier usuario que ha iniciado sesión en la consola puede ver, activar y desactivar perfiles. Como el perfil Console User no tiene asignada la autorización `solaris.network.autoconf.write`, un usuario que tenga esta autorización no puede crear ni modificar NCP, NCU, ubicaciones ni ENM. Sin embargo, el perfil Console User tiene permiso para ver, crear y modificar las WLAN.

Los comandos `netcfg` y `netadm` se pueden usar para ver los perfiles de red de cualquiera que tenga el perfil de derechos Basic Solaris User. Este perfil se asigna a todos los usuarios de manera predeterminada.

El comando `netadm` también se puede utilizar para activar los perfiles de cualquier usuario que tenga el perfil Network Autoconf User o Console User. El perfil Console User se asigna automáticamente al usuario que ha iniciado sesión en el sistema desde `/dev/console`.

Para modificar perfiles de red con el comando `netcfg`, necesita la autorización `solaris.network.autoconf.write` o el perfil Network Autoconf Admin.

Por ejemplo, debe determinar los privilegios que están asociados con el perfil de derechos Console User de la siguiente manera:

```
$ profiles -p "Console User" info
 name=Console User
 desc=Manage System as the Console User
 auths=solaris.system.shutdown,solaris.device.cdrw,solaris.devinde.mount.removable,
 solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
 profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU
 Power Management,Network Autoconf User,Desktop Removable Media User
 help=RtConsUser.html
```

Cómo funciona la configuración de red basada en perfiles con otras funciones de Oracle Solaris

El modo de configuración de red reactiva funciona con otras tecnologías de Oracle Solaris de la siguiente manera:

- Máquinas virtuales: Oracle VM Server para SPARC (anteriormente, Logical Domains) y Oracle VM VirtualBox

  Los perfiles reactivos funcionan con hosts e invitados de Oracle Solaris. Sin embargo, el modo de configuración de red reactivo gestiona solamente las interfaces que pertenecen a las máquinas virtuales especificadas sin interferir con otras máquinas virtuales del sistema.
- Zonas de Oracle Solaris e instancias de pila

Los perfiles reactivos funcionan en zonas globales o en zonas no globales de pila exclusivas. Sin embargo, no puede configurar perfiles reactivos para una zona de pila compartida, ya que la configuración de red para las zonas de pila compartida siempre se gestiona en la zona global.

- Reconfiguración dinámica (DR)

  La configuración de red del sistema admite las funciones de reconfiguración dinámica (DR) y conexión en marcha para los sistemas que tienen estas características. Puede utilizar estas funciones para agregar o eliminar un dispositivo, independientemente de qué NCP está activo actualmente (un NCP reactivo o el NCP `DefaultFixed`). Sin embargo, el comportamiento del sistema varía según el tipo de NCP actualmente activo.

  Cuando el perfil `Automatic` u otro NCP reactivo está activo y hay un dispositivo conectado, el NCP crea automáticamente la configuración IP del dispositivo recién agregado. Si se elimina el dispositivo del sistema mientras un perfil reactivo está activo, la interfaz IP para el dispositivo se desconfigura. Cuando el NCP `DefaultFixed` está activo en el sistema, debe configurar explícitamente la interfaz IP después de agregar el dispositivo. También debe eliminar explícitamente la configuración IP antes de eliminar el dispositivo.

  Para obtener más información sobre la configuración dinámica de dispositivos, consulte "Gestión de dispositivos en Oracle Solaris 11.2 ". Para obtener más información sobre la reconfiguración dinámica cuando se utiliza un perfil fijo, consulte Cómo sustituir una tarjeta de interfaz de red con reconfiguración dinámica.

♦ ♦ ♦ CAPÍTULO 6

Administración de la configuración de red basada en perfiles en Oracle Solaris

En este capítulo, se describe cómo administrar la configuración de red con varios tipos de perfiles. Para obtener una descripción general de la configuración de red basada en perfiles y del modo reactivo, consulte el Capítulo 5, Acerca de la administración de la configuración de red basada en perfiles en Oracle Solaris.

Para obtener información sobre la configuración de enlaces de datos e interfaces IP cuando se utiliza el modo fijo, consulte el Capítulo 2, Administración de la configuración de enlaces de datos en Oracle Solaris y el Capítulo 3, Configuración y administración de direcciones e interfaces IP en Oracle Solaris.

Este capítulo se divide en los siguientes apartados:

Activación y desactivación de perfiles

Utilice el comando `netadm` para activar y desactivar todos los perfiles, independientemente del tipo de perfil o si el perfil es fijo para reactivo. La sintaxis básica del comando es la siguiente:

```
# netadm enable [ -p profile-type ] [ -c ncu-class ] profile-name
```

Por ejemplo, debe activar el NCP automático definido por el sistema de la siguiente manera:

```
# netadm enable -p ncp Automatic
```

Para obtener información básica sobre la activación y desactivación de perfiles, consulte "Directrices para utilizar la configuración de red basada en perfiles" [108].

Consulte las siguientes directrices adicionales para activar y desactivar los distintos tipos de perfiles:

- **NCP**: en un momento dado, *debe* haber un NCP activo y un perfil de ubicación activo en el sistema. El NCP activo permanece activo hasta que se activa otro NCP explícitamente.

Al activar otro NCP, se desactiva implícitamente el NCP activo en ese momento. No puede desactivar explícitamente el NCP activo en un sistema. “Descripción de un NCP” [103].

Al cambiar al modo fijo mediante la activación del NCP `DefaultFixed`, la ubicación `DefaultFixed` también se activa automáticamente y no se puede cambiar.

Al activar el NCP `Automatic`, la política de activación selecciona la ubicación correspondiente según las condiciones actuales de la red y activa esa ubicación.

- **NCU**: puede activar y desactivar manualmente NCU individuales que son parte del NCP activo actualmente, si el modo de activación del NCU está configurado en `manual`. Si el enlace o la clase de NCU no se especifica, se activan o desactivan ambas NCU. Consulte “Descripción de una NCU” [104].
- **Ubicaciones**: de manera predeterminada, el sistema selecciona el mejor perfil de ubicación para activar. El sistema selecciona una ubicación del conjunto de ubicaciones con el modo de activación `system` o `conditional`. Sin embargo, el usuario puede sustituir en cualquier momento la selección del sistema mediante la activación manual de cualquier ubicación, sin importar su modo de activación. Cuando activa una ubicación manualmente, el sistema no modifica la ubicación activa automáticamente. La selección automática de una ubicación está desactivada. Debe desactivar de manera explícita la ubicación activada manualmente para restaurar la selección de la ubicación condicional realizada por el sistema. Consulte “Descripción de un perfil de ubicación” [105].
- **ENM**: estos perfiles pueden tener un modo de activación `manual` o `conditional`. Si establece la propiedad `activation-mode` en `conditional`, el sistema activa o desactiva el ENM en función de las condiciones especificadas. Si establece el modo de activación en `manual`, puede activar o desactivar el EMN mediante el comando `netadm`. No hay restricciones en cuanto a la activación de ENM. Ningún ENM o muchos ENM pueden estar activos en un sistema en un momento dado. La activación o desactivación de un ENM no tiene ningún efecto sobre otros ENM activos. Consulte “Modos de activación de perfil” [109].

EJEMPLO 6-1 Activación de un NCP

En el ejemplo siguiente, se activa un NCP definido por el usuario denominado `myncp`.

```
$ netadm enable -p ncp myncp
Enabling ncp 'myncp'
```

EJEMPLO 6-2 Activación de un perfil de ubicación

En el siguiente ejemplo, una ubicación denominada `office` está activada.

```
$ netadm enable -p loc office
Enabling loc 'office'
```

Tenga en cuenta que al especificar nombres de perfil, el comando `netadm` distingue entre mayúsculas y minúsculas.

EJEMPLO 6-3 Desactivación de una NCU de enlace

En el ejemplo siguiente, se desactiva una NCU de enlace denominada `net1`.

```
$ netadm disable -p ncu -c phys net1
```

EJEMPLO 6-4 Desactivación de una ubicación

En el siguiente ejemplo, se desactiva una ubicación llamada office.

```
$ netadm disable -p loc office
Disabling loc 'office'
```

EJEMPLO 6-5 Activación y desactivación de ENM

En el siguiente ejemplo, un ENM `test-enm1` está activado y otro ENM `test-enm2` está desactivado.

```
$ netadm enable -p enm test-enm1
Enabling enm 'test-enm1'
$ netadm disable -p enm test-enm2
Disabling enm 'test-enm2'
```

EJEMPLO 6-6 Cambio entre los modos fijo y reactivo

En el ejemplo siguiente, se muestra cómo cambiar al modo fijo mediante la activación el NCP `DefaultFixed` definido por el sistema.

```
$ netadm enable -p ncp DefaultFixed
Enabling ncp 'DefaultFixed'
```

Configuración de perfiles

Puede configurar perfiles reactivos mediante el comando `netcfg` de las siguientes maneras:

- Interactivamente
- Modo de línea de comandos
- Modo de archivo de comandos

Uso del modo interactivo `netcfg`

Cuando se usa de manera interactiva, el concepto de un *ámbito* se utiliza para el comando `netcfg`. Cuando utiliza el comando de manera interactiva, el ámbito en el que se encuentra en

cualquier momento dado depende del tipo de perfil y la tarea en particular que está realizando. Cuando escribe el comando `netcfg` solo en una ventana de terminal, como se muestra en el ejemplo siguiente, aparece un indicador en el *ámbito global*:

```
$ netcfg
netcfg>
```

Para crear o seleccionar un perfil, primero debe iniciar la sesión interactiva `netcfg`.

Desde el indicador de ámbito global, puede utilizar los subcomandos `select` o `create` para ver, modificar o crear los siguientes tipos de perfil, que son los perfiles de nivel superior:

- NCP
- Ubicaciones
- ENM
- WLAN conocidas

Después de haber creado o seleccionado un perfil, la sintaxis del indicador interactivo `netcfg` es similar a la del siguiente ejemplo:

`netcfg:`*object-type*`:`*object-name*`>`

Utilice el comando `netcfg` en modo interactivo para realizar las siguientes tareas:

- Crear un perfil.
- Seleccionar y modificar un perfil.
- Verificar que toda la información necesaria sobre un perfil esté configurada y sea válida.
- Confirmar los cambios de un nuevo perfil.
- Cancelar la configuración actual del perfil sin confirmar los cambios en el almacenamiento persistente.
- Revertir los cambios realizados en un perfil.

Para los perfiles de ubicación y ENM, la selección o creación de un perfil de nivel superior mientras se está en el modo interactivo `netcfg` resulta en un símbolo del sistema que aparece en el *ámbito del perfil*, como se muestra en el siguiente ejemplo:

```
netcfg> select loc test-loc
netcfg:loc:test-loc>
```

Cuando selecciona un NCP, el símbolo del sistema están en el *ámbito de NCP*. Las NCU están seleccionadas y creadas en este ámbito. La selección o creación de una NCU desplaza la sesión al *ámbito de perfil* para el NCP seleccionado. En este ámbito, se pueden ver y establecer todas las propiedades asociadas al perfil seleccionado actualmente.

En el siguiente ejemplo, el NCP `office` está seleccionado, lo que mueve la sesión interactiva al ámbito de NCP para el NCO, desde donde se selecciona la NCU luego. Esta acción genera el ámbito de perfil para la NCU seleccionada. En este ámbito, se pueden ver o establecer las propiedades de la NCU.

```
$ netcfg
netcfg> select ncp office
netcfg:ncp:office> select ncu phys net2
netcfg:ncp:office:ncu:net2>
```

En cualquier ámbito determinado, el indicador de comandos muestra el perfil seleccionado actualmente. Todos los cambios realizados al perfil en este ámbito pueden ser *confirmados*, lo que quiere decir que los cambios se guardan en el almacenamiento persistente. Los cambios se confirman implícitamente al salir el ámbito. Si no desea confirmar los cambios que haya realizado, puede volver al estado comprometido anterior para ese perfil. Al hacerlo, revierte los cambios realizados en el perfil de ese nivel. Los subcomandos `revert` y `cancel` funcionan de manera similar.

Para obtener instrucciones, consulte “Creación de NCP” [118].

Nota - El subcomando `walkprop` se utiliza para mostrar cada propiedad que está asociada a un perfil de manera individual. Este comando es significativo sólo cuando se utiliza en el modo interactivo.

Uso del modo de línea de comandos `netcfg`

En el modo de línea de comandos, cualquier subcomando `netcfg` que afecta un perfil o propiedad seleccionados se debe ejecutar en el ámbito particular en el que existe el perfil o la propiedad seleccionados. Seleccionar un perfil en el modo de línea de comandos es lo mismo que seleccionarlo en el modo interactivo. La única diferencia es que en el modo de línea de comandos todos los subcomandos se escriben en la línea de comandos. Por ejemplo, para mostrar el contenido de un NCP, primero debe seleccionar el NCP y, a continuación, utilizar el subcomando `list` para mostrar las NCU para ese NCP, como se muestra en el siguiente ejemplo:

```
$ netcfg "select ncp myncp; list"
ncp:myncp
 management-type reactive
NCUs:
 phys net0
 phys net1
 ip   net0
 ip   net1
```

Consulte las siguientes directrices cuando utilice el comando `netcfg` en este modo:

- Separe cada subcomando con un punto y coma.
- Especifique el subcomando `select` del ámbito global para mover al ámbito del NCP.
- Especifique el subcomando `list` desde el ámbito del NCP para mostrar las propiedades que están en ese ámbito.
- Use comillas rectas para evitar que el shell interprete que son punto y coma.

Nota - En el modo de línea de comandos, debe escribir el comando completo en una sola línea. Los cambios que realice a un perfil seleccionado mediante el comando `netcfg` en el modo de línea de comandos se envían al almacenamiento persistente cuando se ejecuta el comando.

Puede usar cualquiera de los subcomandos `netcfg` en el modo de línea de comandos, salvo el subcomando `walkprop`.

Uso del modo de archivo de comandos `netcfg`

En el modo de línea de comandos, la información de configuración del perfil y los comandos se obtienen de un archivo. Los comandos del archivo son iguales que los que se usan en el modo interactivo o los proporcionados por el subcomando `export`. El subcomando export con la opción `-f` se utiliza para producir el archivo. Por ejemplo, el siguiente comando exporta la configuración actual del perfil a un archivo:

```
$ netcfg export -f /tmp/nwam.config
```

Para importar la configuración del perfil desde un archivo, escriba el siguiente comando:

```
$ netcfg -f /tmp/nwam.config
```

El subcomando `export` también se puede usar de manera interactiva. Para obtener más información, consulte “Exportación de la configuración de un perfil” [139].

Creación de NCP

Un NCP define la configuración de red de un sistema. Sólo puede crear NCP reactivos, no NCP fijos.

Para crear un NCP en el modo interactivo, debe empezar con el inicio de la sesión interactiva. A continuación, use el subcomando `create` para crear el nuevo NCP, como se muestra en el siguiente ejemplo:

```
$ netcfg
netcfg> create ncp myncp
netcfg:ncp:myncp>
```

EJEMPLO 6-7 Creación de un NCP mediante la clonación del NCP `Automatic`

Puede crear un NCP mediante la clonación de cualquier NCP existente que no sea el NCP `DefaultFixed`. Puede modificar las propiedades del NCP para especificar parámetros de configuración nuevos. En el ejemplo siguiente, se crea un nuevo NCP denominado `newncp` mediante la clonación del NCP `Automatic` definido por el sistema.

```
$ netcfg
netcfg> create -t Automatic ncp newncp
netcfg:ncp:newncp> list
ncp:newncp
 management-type reactive
NCUs:
 phys net0
 phys net1
 ip   net0
 ip   net1
```

La propiedad `management-type` es una propiedad de sólo lectura que siempre está definida en `reactive`. En el ejemplo anterior, el subcomando `list` se utiliza para mostrar el contenido del NCP que se acaba de copiar (`newncp`).

También puede clonar el NCP `Automatic` directamente mediante el modo de línea de comandos `netcfg`, como se muestra en el siguiente ejemplo. Tanto el método interactivo como el método de línea de comandos copian las NCU existentes del NCP `Automatic` al NCP creado recientemente.

```
$ netcfg create -t Automatic ncp newncp
$ netcfg list ncp newncp
ncp:newncp
 management-type reactive
NCUs:
 phys net0
 phys net1
 ip   net0
 ip   net1
```

Creación de NCU para un NCP

El NCP es básicamente un contenedor que consta de un conjunto de NCU que están configuradas con propiedades que definen la configuración de red para el NCP. Todos los NCP contienen NCU de enlace e interfaz.

Las NCU de enlace especifican la configuración de enlaces y la política de selección de enlaces para el NCP. Las NCU de interfaz especifican la política de configuración de interfaces para el NCP. Si se requiere conectividad IP, se requieren tanto un enlace como una NCU de interfaz. Las NCU se deben agregar o eliminar explícitamente con el comando `netcfg` o mediante la GUI de administración de redes. Para obtener más información sobre cómo agregar y eliminar NCU mediante la GUI de administración de redes, consulte “Administración de la configuración de red desde el escritorio” [142].

Puede crear NCU mediante el comando `netcfg` en modo interactivo o modo de línea de comandos. Como la creación de una NCU implica varias operaciones, es más fácil y más eficaz crear NCU de manera interactiva, en lugar de intentar construir un comando de una sola línea que crea la NCU y todas sus propiedades. Las NCU se pueden crear al crear por primera

vez un NCP o posteriormente. El proceso de creación o modificación de una NCU implica la configuración de propiedades generales de la NCU, así como la configuración de propiedades que se aplican específicamente a cada tipo de NCU.

Al crear una NCU de manera interactiva, el comando `netcfg` recorre cada propiedad relevante para la NCU y muestra el valor predeterminado, si existe uno, y los posibles valores. Por ejemplo, si especifica `dhcp` para la propiedad `ipv4-addrsrc` de una NCU de interfaz, no se le pide que especifique un valor para la propiedad `ipv4-addr` porque esta propiedad se utiliza para la configuración de una dirección IP estática. Puede especificar otros valores para cada propiedad en el indicador interactivo. Si presiona la tecla de retorno sin especificar un valor, se vuelve a aplicar el valor predeterminado, o se deja la propiedad vacía si no hay ningún valor predeterminado.

Existen varias propiedades de NCU que puede especificar al crear o modificar una NCU. Algunas propiedades se aplican a ambos tipos de NCU, mientras que otras se aplican a una NCU de enlace o una NCU de interfaz. Para obtener una descripción completa de todas las propiedades de NCU, incluidas las reglas y condiciones que se pueden aplicar al especificar estas propiedades, consulte la página del comando man `netcfg`(1M).

▼ Cómo crear NCU para un NCP de manera interactiva

El siguiente procedimiento describe cómo seleccionar un NCP existente y luego crear NCU para el NCP de manera interactiva.

Nota - El proceso de "recorrido" que se realiza durante la creación del perfil inicial garantiza que al modificar el NCP sólo se soliciten las propiedades pertinentes, de acuerdo con las selecciones realizadas durante su creación.

---

1. **Inicie la sesión interactiva `netcfg`.**

```
$ netcfg
netcfg>
```

2. **Seleccione un NCP existente.**

En el ejemplo siguiente, el NCP `myncp` está seleccionado:

```
netcfg> select ncp myncp
netcfg:ncp:myncp>
```

La selección del NCP lo lleva automáticamente al ámbito del NCP. Para una ubicación, un ENM o un objeto WLAN, el símbolo del sistema lo llevará al ámbito del perfil de ese perfil.

3. **Cree NCU de enlace e interfaz para el NCP.**

En el ejemplo siguiente, se crea una NCU de enlace:

```
netcfg:ncp:myncp> create ncu phys net0
```

```
Created ncu `net0'. Walking properties ...
activation-mode (manual) [manual|prioritized]>
mac-address>
autopush>
mtu> 1600
```

donde `ncu` es el tipo de objeto, `phys` es la clase de NCU y `net0` es el nombre del objeto.

La creación de una NCU lo lleva al ámbito de ese objeto y lo guía por las propiedades predeterminadas para el objeto.

En este ejemplo, se especifican las siguientes propiedades:

- La propiedad `activation-mode`, cuyo valor predeterminado es `manual`, se acepta pulsando la tecla de retorno.
- Las propiedades `mac-address` y `autopush` se dejan vacías.
- La propiedad `mtu` se configura en un valor de `1600`.

El siguiente ejemplo muestra cómo crear una NCU de interfaz:

```
netcfg:ncp:myncp> create ncu ip net0
Created ncu `net0'. Walking properties ...
ip-version (ipv4,ipv6) [ipv4|ipv6]> ipv4
ipv4-addrsrc (dhcp) [dhcp|static]> dhcp
ipv4-default-route>
```

donde `ncu` es el tipo de objeto, `ip` es la clase de objeto y `net0` es el nombre del objeto.

La creación de una NCU lo lleva al ámbito de ese objeto y lo guía por las propiedades predeterminadas para el objeto.

En este ejemplo, se especifican las siguientes propiedades:

- La propiedad `ip-version` está configurada en `ipv4`.
- La propiedad `ipv4-addrsrc` está configurada en `dhcp`.

Durante la creación de una NCU, la opción `class` se utiliza para diferenciar entre los dos tipos de NCU.

4. **(Opcional) Verifique que la configuración sea correcta de la siguiente manera:**

```
netcfg:ncp:myncp:ncu:net0> verify
All properties verified
```

El subcomando `verify` verifica la configuración y notifica si falta alguno de los valores necesarios.

5. **Guarde cada NCU que cree.**

   - **Utilice el subcomando `commit`:**

     ```
     netcfg:ncp:myncp:ncu:net0> commit
     ```

```
Committed changes
netcfg:ncp:myncp:ncu:net0>
```

El subcomando `commit` verifica implícitamente las propiedades.

- **Utilice el subcomando `end`:**

```
netcfg:ncp:myncp:ncu:net0> end
Committed changes
netcfg:ncp:myncp>
```

El subcomando `end` implícitamente confirma los cambios.

En esta instancia, si ha terminado de agregar las NCU a los NCP, el subcomando `end` mueve la sesión al ámbito del NCP.

En el modo interactivo, los cambios no se guardan en el almacenamiento persistente hasta que los confirma. Al utilizar el subcomando `commit`, se confirma el perfil entero. Para mantener la coherencia del almacenamiento persistente, la operación `commit` también incluye un paso de verificación. Si la verificación falla, la operación `commit` también falla. Si una confirmación implícita falla, se le da la opción de finalizar la sesión interactiva sin confirmar los cambios actuales o de salir de ella de la misma manera. También puede permanecer en el ámbito actual y continuar realizando cambios en el perfil.

Nota - Para cancelar los cambios realizados, utilice el subcomando `cancel` o `revert`.

El subcomando `cancel` finaliza la configuración del perfil actual sin confirmar los cambios actuales en el almacenamiento persistente y, a continuación, pasa la sesión interactiva al siguiente nivel del ámbito. El subcomando `revert` deshace los cambios realizados y relee la configuración anterior. Al utilizar el subcomando `revert`, la sesión interactiva permanece en el mismo ámbito.

---

6. **Cuando termine, salga de la sesión interactiva.**

```
netcfg:ncp:myncp> exit
```

El subcomando `exit` es similar al subcomando `end` pero también sale de la sesión interactiva.

Creación de ubicaciones

Un perfil de ubicación contiene propiedades que definen los valores de configuración de red que no están relacionados directamente con la conectividad básica de enlace e IP. Algunos ejemplos incluyen los valores de filtros IP y servicios de nombres que se aplican juntos, cuando es necesario. Exactamente un perfil de ubicación y un NCP deben estar activos en el sistema en todo momento.

Puede crear perfiles de ubicación mediante el comando `netcfg` en modo interactivo o modo de línea de comandos. Al crear un perfil de ubicación, debe definir las propiedades para la ubicación especificando valores que definen los parámetros de configuración concretos cuando esa ubicación está activada. Las propiedades de ubicación están clasificadas por grupo, donde el grupo denota una clase concreta de preferencias de configuración.

Las propiedades de ubicación también se almacenan en un repositorio. Cuando se activa una ubicación determinada, sus propiedades se aplican automáticamente al sistema en ejecución. La creación y modificación de perfiles de ubicación también implica la configuración de las propiedades que definen cuando una ubicación determinada está activada. Las propiedades que se le presentan durante el proceso de configuración se basan en los valores de propiedades que ya definió anteriormente.

Para obtener una descripción completa de todas las propiedades del perfil de ubicación, incluidas las reglas, las condiciones y las dependencias que se pueden aplicar al especificar cualquiera de estas propiedades, consulte la página del comando man `netcfg`(1M).

▼ Cómo crear un perfil de ubicación de manera interactiva

El siguiente procedimiento describe cómo crear un perfil de ubicación. El proceso de "recorrido" que se realiza durante la creación del perfil inicial sólo solicita las propiedades pertinentes, de acuerdo con los valores especificados anteriormente.

1. Inicie la sesión interactiva `netcfg`.

```
$ netcfg
netcfg>
```

2. Cree el perfil de ubicación.

En el siguiente ejemplo, se crea una ubicación denominada `office`:

```
netcfg> create loc office
Created loc 'office'. Walking properties ...
activation-mode (manual) [manual|conditional-any|conditional-all]> conditional-any
conditions> ncu ip:net0 is active
nameservices (dns) [dns|files|nis|ldap]>
nameservices-config-file ("/etc/nsswitch.dns")>
dns-nameservice-configsrc (dhcp) [manual|dhcp]>
nfsv4-domain>
ipfilter-config-file> /export/home/test/wifi.ipf.conf
ipfilter-v6-config-file>
ipnat-config-file>
ippool-config-file>
ike-config-file> /etc/inet/ike/ikev1.config
ikev2-config-file>
ipsecpolicy-config-file>
```

La creación de la ubicación lo pasa automáticamente al ámbito del perfil de esta ubicación.

En este ejemplo, se definieron las siguientes propiedades:

- La propiedad `activation-mode` se definió en `conditional-any`, lo que resultó en un símbolo del sistema que permitió la especificación de las condiciones de activación.
- La condición de activación de la ubicación se especificó como `ncu ip:net0 is active`.
- Para la propiedad `ipfilter-config-file`, se especificó el archivo `/export/home/test/wifi.ipf.conf`.
- Para la propiedad `ike-config-file`, se especificó `/etc/inet/ike/ikev1.config`.
- Para el resto de propiedades, los valores predeterminados se aceptaron presionando la tecla de retorno.

3. (Opcional) Muestre la configuración de perfil mediante el subcomando `list` de la siguiente manera:

```
netcfg:loc:office> list
loc:office
        activation-mode                 conditional-any
        conditions                      "ncu ip:net0 is active"
        enabled                         false
        nameservices                    dns
        nameservices-config-file        "/etc/nsswitch.dns"
        dns-nameservice-configsrc       dhcp
        ipfilter-config-file            "/export/home/test/wifi.ipf.conf"
        ike-config-file                 "/etc/inet/ike/ikev1.config"
```

4. Verifique que la configuración del perfil sea correcta.

```
netcfg:loc:office> verify
All properties verified
```

El subcomando `verify` verifica la configuración y notifica si falta alguno de los valores necesarios.

5. Cuando haya verificado la configuración, guarde la ubicación.

```
netcfg:loc:office> commit
Committed changes
```

Como alternativa, puede utilizar el subcomando `end` para terminar la sesión, lo que también guarda la configuración del perfil y mueve la sesión al ámbito global.

```
netcfg:loc:office> end
Committed changes
netcfg>
```

6. Salga de la sesión interactiva.

```
netcfg> exit
```

Creación de ENM

Los ENM permiten especificar cuándo las aplicaciones o las secuencias de comandos, como una aplicación VPN, deben realizar la configuración de red, que es independiente (externa) de la configuración que se especifica en los perfiles de ubicación y NCP. Para obtener más información sobre los ENM, consulte “Descripción de un ENM” [106].

Nota - El sistema no reconoce automáticamente una aplicación para la que pueda crear un ENM. Estas aplicaciones deben instalarse primero y luego ser configuradas en el sistema antes de crear un ENM para ellas mediante el comando `netcfg`.

Para obtener más información sobre las propiedades que puede especificar al crear un ENM, consulte la página del comando man `netcfg`(1M).

▼ Cómo crear un ENM de manera interactiva

1. Inicie la sesión interactiva `netcfg`.

```
$ netcfg
netcfg>
```

2. Cree el ENM.

```
netcfg> create enm test-enm
Created enm 'test-enm'.  Walking properties ...
activation-mode (manual) [manual|conditional-any|conditional-all]>
fmri> svc:/application/test-enm:default
start>
stop>
netcfg:enm:test-enm>
```

La creación automática de ENM lo mueve al ámbito de perfil para el ENM y recorre cada una de sus propiedades.

En este ejemplo, se especifican las siguientes propiedades para el ENM `test-enm`:

- La propiedad `activation-mode`, que se establece en manual, se acepta pulsando la tecla de retorno. Debido a que este valor se define en `manual`, la propiedad `conditions` no está disponible para configuración.
- La propiedad `fmri` se define en `svc:/application/test-enm:default`.
- Las propiedades `start` y `stop` no se configuran para este ENM.

3. (Opcional) Visualice la configuración del perfil.

```
netcfg:enm:test-enm> list
```

```
enm:test-enm
 activation-mode manual
 enabled   false
 fmri      "svc:/application/test-enm:default"
```

4. **Verifique que la configuración del perfil sea correcta.**

```
netcfg:enm:test-enm> verify
All properties verified
```

El subcomando `verify` verifica la configuración y notifica si falta alguno de los valores necesarios.

5. **Guarde el ENM.**

```
netcfg:enm:test-enm> commit
Committed changes
netcfg>
```

El subcomando `commit` verifica y guarda la configuración.

Como alternativa, puede utilizar el subcomando `end` para terminar la sesión, que también guarda la configuración del perfil.

```
netcfg:enm:test-enm> end
Committed changes
```

6. **Salga de la sesión interactiva.**

```
netcfg> exit
```

Creación de WLAN conocidas

Las WLAN conocidas son perfiles que almacenan información sobre las redes inalámbricas que conoce el sistema. Los NCP pueden configurar automáticamente interfaces inalámbricas en función de la información de configuración proporcionada por cada una de las redes inalámbricas a las que está conectado el sistema. Para obtener más información, consulte “Descripción de una WLAN conocida” [106].

Para obtener más información sobre las propiedades que puede especificar al crear o modificar WLAN, consulte la página del comando man `netcfg`(1M).

▼ Cómo crear una WLAN conocida de manera de interactiva

1. **Inicie la sesión interactiva `netcfg`.**

```
$ netcfg
```

```
netcfg>
```

2. **Cree la WLAN conocida.**

   El siguiente ejemplo crea una WLAN conocida que se conecta a una red inalámbrica denominada ESSID. La WLAN conocida debe tener el mismo nombre que la red inalámbrica o su ESSID:

```
netcfg> create wlan mywifi
Created wlan 'mywifi'.  Walking properties ...
priority (0)> 100
bssids>
keyname> mywifi-key
keyslot>
security-mode [none|wep|wpa]> wpa
netcfg:wlan:mywifi>
```

   La creación automática de WLAN lo mueve al ámbito de perfil para la WLAN y lo guía a través de cada una de sus propiedades.

   En este ejemplo, se especificaron las siguientes propiedades para la WLAN conocida `mywifi`:

   - El valor de la propiedad `priority` se cambia de un valor predeterminado de `0` a `100`.
   - La propiedad `keyname` se configura en `mywifi-key` y especifica el nombre del objeto seguro para esta red inalámbrica. Consulte “Definición de comunicaciones seguras mediante Wi-Fi” [151] para obtener más información.
   - La propiedad `security-mode` se configura en `wpa`. Esta propiedad especifica el tipo de cifrado que utiliza esta red inalámbrica.
   - Los valores de la propiedad `keyslot` y `bssid` se dejan vacíos.

3. **(Opcional) Visualice la configuración del perfil.**

```
netcfg:wlan:mywifi> list
known wlan:mywifi
 priority   100
 keyname "mywifi-key"
 security-mode    wpa
netcfg:wlan:mywifi>
```

4. **Verifique que la configuración del perfil sea correcta.**

```
netcfg:wlan:mywifi> verify
All properties verified
```

   El subcomando `verify` verifica la configuración y notifica si falta alguno de los valores necesarios.

5. **Guarde la WLAN conocida.**

```
netcfg:wlan:mywifi> commit
Committed changes
```

El subcomando `commit` verifica y guarda la configuración.

Como alternativa, puede utilizar el subcomando `end` para terminar la sesión, lo que también guarda la configuración del perfil y mueve la sesión al ámbito global.

```
netcfg:wlan:mywifi> end
Committed changes
netcfg>
```

6. **Salga de la sesión interactiva.**

```
netcfg> exit
```

Administración de perfiles

Esta sección incluye los siguientes temas:

Configuración de valores de propiedades para perfiles

Los valores de propiedad de perfiles reactivos se establecen o modifican mediante el subcomando `set`. Este subcomando se puede utilizar de manera interactiva o en modo de línea de comandos. Si un valor de propiedad se establece o se cambia en modo de línea de comandos, el cambio se confirma de inmediato en el almacenamiento persistente.

Nota - No puede modificar el NCP `DefaultFixed`ni el perfil de ubicación `DefaultFixed` mediante el subcomando `set`. Siempre que el NCP `DefaultFixed` esté activo, utilice los comandos `dladm` y `ipadm` para realizar cambios de configuración. Cuando la ubicación `DefaultFixed` está activa, realice los cambios directamente a las propiedades SMF pertinentes mediante los comandos `svccfg` y `svcadm`. Consulte las páginas del comando man `svccfg`(1M) y `svcadm`(1M).

La sintaxis del subcomando `set` es la siguiente:

```
netcfg> set prop-name=value1[,value2,...]
```

▼ Cómo configurar los valores de propiedades de perfil de manera interactiva

El siguiente procedimiento describe cómo configurar los valores de propiedad para un perfil de ubicación de manera interactiva. Cuando se establecen valores de propiedades de manera interactiva, primero, debe seleccionar un perfil en el ámbito actual, lo que mueve la sesión interactiva al ámbito de dicho perfil. El perfil seleccionado se carga en la memoria del almacenamiento persistente. En este ámbito, puede modificar las propiedades del perfil.

A modo de ejemplo únicamente, el siguiente procedimiento muestra cómo definir la propiedad `ipfilter-config-file` de la ubicación `test-loc` de manera interactiva.

1. **Inicie la sesión interactiva `netcfg`.**

```
$ netcfg
netcfg>
```

2. **Seleccione el objeto de configuración o perfil que desea modificar.**

```
netcfg> select loc test-loc
netcfg:loc:test-loc>
```

3. **Establezca el valor de la propiedad.**

   En el siguiente ejemplo, se establece la propiedad `ipfilter-config-file`:

```
netcfg:loc:test-loc> set ipfilter-config-file = /path/to/ipf-file
```

4. **(Opcional) Muestre la información de configuración.**

```
netcfg:loc:test-loc> list
loc:test-loc
 activation-mode   manual
 enabled        false
 nameservices        dns
 dns-nameservice-configsrc  dhcp
 nameservices-config-file  "/etc/nsswitch.dns"
 ipfilter-config-file   "/path/to/ipf-file"
```

5. **Cierre la sesión.**

```
netcfg:loc:test-loc> end
Committed changes
netcfg>
```

El subcomando `end` guarda y mueve la sesión al ámbito global.

6. **Salga de la sesión interactiva.**

```
netcfg> exit
```

ejemplo 6-8 Configuración de los valores de propiedades para un perfil en el modo de línea de comandos

El ejemplo anterior que muestra cómo definir de manera interactiva la propiedad `ipfilter-config-file` también se puede realizar en el modo de línea de comandos, de la siguiente manera:

```
$ netcfg "select loc test-loc; set ipfilter-config-file = /path/to/ipf-file"
```

El modo de línea de comandos es ideal para cuando sólo necesita realizar una acción simple. Sin embargo, también puede utilizar el modo de línea de comandos para realizar acciones más complejas especificando, con cuidado, los subcomandos correspondientes en la línea de comandos. Como con el ejemplo interactivo, en el modo de línea de comandos también debe primero seleccionar la ubicación para moverla al ámbito del perfil. Puede especificar el subcomando `set` para configurar valores de propiedad individuales.

Cuando utiliza el modo de línea de comandos, se pueden definir varios valores para una propiedad determinada al mismo tiempo. Al definir varios valores de esta manera, cada valor debe estar separado por una coma (`,`). Si los valores individuales de una propiedad especificada también contienen una coma, la coma que forma parte del valor de la propiedad debe estar precedida por una barra diagonal inversa (`\`). Las comas dentro de propiedades que sólo tienen un valor único no se interpretan como delimitadores y, por lo tanto, no necesitan estar precedidas por una barra diagonal inversa.

Por ejemplo, puede configurar la propiedad `ip-version` para utilizar IPv4 e IPv6 para la NCU `net0` en el NCP `myncp`, de la siguiente manera:

```
$ netcfg "select ncp myncp; select ncu ip net0; set ip-version=ipv4,ipv6"
```

Obtención de información acerca de la configuración de perfiles

Utilice el subcomando `list` para mostrar todos los perfiles, los pares propiedad-valor y los recursos que existen en el ámbito actual o especificado, de manera interactiva o en el modo de línea de comandos.

En el ámbito global, el subcomando `list` muestra todos los perfiles definidos por el sistema y definidos por el usuario del sistema, como se muestra en el siguiente ejemplo:

```
$ netcfg list
netcfg list
NCPs:
 DefaultFixed
 Automatic
 myncp
Locations:
 Automatic
 NoNet
 DefaultFixed
 office
ENMs:
 test-enm
WLANs:
 mywifi
```

Nota - En el modo interactivo, el uso del subcomando `list` en el ámbito global muestra la misma información.

Tenga en cuenta que el subcomando `list` no muestra el estado de cada perfil. Para mostrar información sobre los perfiles y sus estados, utilice el comando `netadm` con el subcomando `list`. Para obtener más información, consulte “Visualización del estado actual de un perfil” [137].

Visualización de valores de propiedad para un perfil individual

El subcomando `list` en el ámbito de perfil muestra todos los valores de propiedades de un perfil especificado. La sintaxis es la siguiente:

```
netcfg> list [ object-type [ class ] object-name ]
```

▼ Cómo visualizar todos los valores de propiedades para un perfil de manera interactiva

El siguiente procedimiento describe cómo visualizar todos los valores de propiedades para un perfil mediante el subcomando `list` de manera interactiva. El ejemplo en el siguiente procedimiento muestra cómo visualizar la información de configuración para un nombre NCP IP `net0` Los valores que se muestran para cada perfil varían en función de el perfil.

1. **Inicie la sesión interactiva `netcfg`.**

```
$ netcfg
netcfg>
```

2. **Seleccione el NCP.**

```
netcfg> select ncp myncp
netcfg:ncp:myncp>
```

3. **Muestre la configuración de la NCU IP mediante uno de los siguientes métodos:**

   - **Muestre la configuración desde el ámbito global:**

     ```
     netcfg:ncp:myncp> list ncu ip net0
     ncu:net0
             type                    interface
             class                   ip
             parent                  "myncp"
             enabled                 false
             ip-version              ipv4,ipv6
             ipv4-addrsrc            dhcp
             ipv6-addrsrc            dhcp,autoconf
     netcfg:ncp:myncp>
     ```

   - **Muestre la configuración desde el ámbito del perfil:**

     ```
     netcfg:ncp:myncp> select ncu ip net0
     netcfg:ncp:myncp:ncu:net0> list
     ncu:net0
             type                    interface
             class                   ip
             parent                  "myncp"
             enabled                 false
             ip-version              ipv4,ipv6
             ipv4-addrsrc            dhcp
             ipv6-addrsrc            dhcp,autoconf
     netcfg:ncp:myncp:ncu:net0>
     ```

4. **Salga de la sesión interactiva.**

   ```
   netcfg:ncp:myncp:ncu:net0> exit
   ```

ejemplo 6-9 Visualización de valores de propiedades en el modo de línea de comandos

El ejemplo anterior que muestra cómo visualizar valores de propiedad de manera interactiva se puede realizar en el modo de línea de comandos. La salida es idéntica, independientemente del modo que utilice.

Por ejemplo, debe visualizar las propiedades de la NCU IP `net0` desde el ámbito de NCP de la siguiente manera:

```
$ netcfg "select ncp myncp; list ncu ip net0"
```

Para mostrar las propiedades de la NCU IP `net0` desde el ámbito de perfil, debe utilizar el comando siguiente:

```
$ netcfg "select ncp myncp; select ncu ip net0; list"
```

Obtención un valor de la propiedad específico para un perfil

Utilice el subcomando `get` para obtener un valor de propiedad determinado para un perfil. Este subcomando se puede utilizar de manera interactiva o en modo de línea de comandos. La sintaxis del comando es la siguiente:

```
netcfg> get [ -V ] prop-name
```

▼ Cómo obtener un valor de la propiedad específico para un perfil

El siguiente procedimiento describe cómo obtener un valor de propiedad específico para un perfil mediante el subcomando `get` de manera interactiva. El ejemplo del siguiente procedimiento muestra cómo obtener la propiedad `ip-version` de una NCU IP.

1. **Inicie la sesión interactiva `netcfg`.**

```
$ netcfg
netcfg>
```

2. **Seleccione el NCP y, a continuación, seleccione la NCU IP. Por ejemplo:**

```
netcfg> select ncp myncp
netcfg:ncp:myncp> select ncu ip net0
netcfg:ncp:myncp:ncu:net0>
```

3. **Obtenga el valor de la propiedad específica mediante uno de los siguientes comandos:**

   - **Utilice el subcomando `get` para mostrar el nombre de la propiedad y el valor de la propiedad de la siguiente manera:**

```
netcfg:ncp:myncp:ncu:net0> get ip-version
 ip-version ipv4,ipv6
```

   - **Si sólo desea obtener el valor de la propiedad, sin mostrar el nombre de la propiedad, utilice la opción `-V` con el subcomando `get`, de la siguiente manera:**

```
netcfg:ncp:myncp:ncu:net0> get -V ip-version
ipv4,ipv6
```

4. **Salga de la sesión interactiva.**

```
netcfg:ncp:myncp:ncu:net0> exit
```

ejemplo 6-10 Obtención de un valor de propiedad específico para un perfil en el modo de línea de comandos

El ejemplo interactivo anterior también se pueden realizar en el modo de línea de comandos. La salida es idéntica, independientemente del modo que utilice.

Por ejemplo, debe obtener el valor de la propiedad `ip-version` para una NCU IP en el modo de línea de comandos, de la siguiente manera:

```
$ netcfg "select ncp myncp; select ncu ip net0; get ip-version"
 ip-version ipv4,ipv6
```

El siguiente ejemplo muestra cómo utilizar el subcomando `get` con la opción `-V` para obtener un determinado valor de propiedad. Este método es útil para las secuencias de comandos, donde el nombre de la propiedad no debe ser analizado.

```
$ netcfg "select ncp myncp; select ncu ip net0; get -V ip-version"
ipv4,ipv6
```

Configuración de valores de propiedad para un perfil mediante el subcomando `walkprop`

Utilice el subcomando `walkprop` para ver y cambiar de manera interactiva los valores de propiedades individuales de un perfil. Después de iniciar la sesión interactiva, escribir el subcomando `walkprop` le permite mostrar el nombre y el valor actual de cada una de las propiedades del perfil, una propiedad a la vez. A medida que ve las diferentes propiedades, puede configurar o cambiar el valor actual o predeterminado, según lo desee.

Nota - El subcomando `walkprop` sólo se puede utilizar en el modo interactivo.

▼ Cómo "recorrer" y definir los valores de propiedad para un perfil determinado

El siguiente procedimiento describe cómo utilizar el subcomando `walkprop` para ver y cambiar de manera interactiva los valores de propiedad para un perfil determinado. Como se muestra en los siguientes ejemplos, al utilizar el subcomando `walkprop` para establecer las propiedades de un perfil, no tiene que usar el subcomando `set`.

1. **Inicie la sesión interactiva `netcfg`.**

   ```
   $ netcfg
   netcfg>
   ```

2. **Seleccione el perfil cuyas propiedades desea ver y cambiar.**
   En el siguiente ejemplo, una ubicación denominada `test-loc` está seleccionada:

```
netcfg> select loc test-loc
netcfg:loc:test-loc>
```

3. **Escriba el subcomando `walkprop` para iniciar el recorrido.**

   En el ejemplo siguiente, una vez emitido el subcomando `walkprop`, la primera propiedad que se muestra es la propiedad `activatation-mode`. Observe que el valor predeterminado de la propiedad, actualmente definido en `manual` (entre paréntesis).

   ```
   netcfg:loc:test-loc> walkprop
   activation-mode (manual) [manual|conditional-any|conditional-all]>
   ```

4. **Para modificar un valor de propiedad, escriba el nuevo valor en el indicador interactivo y pulse la tecla de retorno.**

   Por ejemplo, puede cambiar la propiedad `activation-mode` para la ubicación de `manual` a `conditional-all`, de la siguiente manera:

   ```
   netcfg:loc:test-loc> walkprop
   activation-mode (manual) [manual|conditional-any|conditional-all]> conditional-all
   ```

   Al pulsar Retorno se guarda la configuración actual y se recorre la siguiente propiedad.

5. **Repita el proceso de recorrido hasta que se hayan mostrado todas las propiedades del perfil, realice las modificaciones necesarias según las instrucciones del Paso 4.**

   ```
   netcfg:loc:test-loc> walkprop
   activation-mode (manual) [manual|conditional-any|conditional-all]> conditional-all
   conditions> advertised-domain is example.com
   nameservices (dns) [dns|files|nis|ldap]>
   nameservices-config-file ("/etc/nsswitch.dns")>
   dns-nameservice-configsrc (dhcp) [manual|dhcp]>
   nfsv4-domain>
   ipfilter-config-file>
   ipfilter-v6-config-file>
   ipnat-config-file>
   ippool-config-file>
   ike-config-file>
   ikev2-confg-file>
   ipsecpolicy-config-file>
   ```

   Si pulsa la tecla de retorno sin realizar ningún cambio en una propiedad, se conserva el valor predeterminado existente y avanza el recorrido a la siguiente propiedad.

   Nota - Sólo se muestran las propiedades relevantes de un perfil determinado, como se describe en Cómo crear un perfil de ubicación de manera interactiva [123].

6. **Muestre los valores de propiedad actuales predeterminados para el perfil. Por ejemplo:**

```
netcfg:loc:test-loc> list
loc:test-loc
 activation-mode    conditional-all
 conditions      "advertised-domain is example.com"
 enabled      false
 nameservices       dns
 nameservices-config-file    "/etc/nsswitch.dns"
 dns-nameservice-configsrc   dhcp
```

Observe que la propiedad `activation-mode` de la salida anterior ahora está configurada en `conditional-all`.

7. **Salga de la sesión interactiva para confirmar los cambios.**

```
netcfg:loc:test-loc> exit
Committed changes
```

Visualización de la información sobre perfiles

Utilice el comando `netadm` con el subcomando `list` para mostrar información sobre alguno de los perfiles que están en el sistema, o todos, incluido el estado actual de cada perfil.

La sintaxis del subcomando `list` es la siguiente:

```
$ netadm list [ -p object-type ] [ -c ncu-class ] [ object-name ]
```

Puede mostrar todos los perfiles de un sistema y el estado actual de cada perfil de la siguiente manera:

```
$ netadm list
TYPE   PROFILE    STATE
ncp    DefaultFixed  disabled
ncp    Automatic  online
ncu:phys  net0    online
ncu:phys  net1    offline
ncu:ip    net0    online
ncu:ip    net1    offline
loc    Automatic  online
loc    NoNet   offline
loc    DefaultFixed  offline
enm    test-enm   disabled
```

Tenga en cuenta que el subcomando `list` muestra el NCP activado y todas las NCU que componen ese NCP concreto.

Visualización del estado actual de un perfil

El tipo de perfil y la clase de NCU se pueden incluir con el subcomando `list` para identificar un perfil específico. Si se proporciona sólo un tipo de perfil, se muestran todos los perfiles que son de ese tipo. Si un perfil es especificado por su nombre, se muestra el estado actual de ese perfil. Si el nombre de perfil no es único, se muestran todos los perfiles con ese nombre.

EJEMPLO 6-11 Visualización del estado actual de un perfil especificado

El siguiente ejemplo muestra el estado actual de todos los perfiles que están en el sistema con el nombre `Automatic`.

```
$ netadm list Automatic
TYPE         PROFILE        STATE
ncp          Automatic      online
ncu:ip       net1           offline
ncu:phys     net1           offline
ncu:ip       net0           online
ncu:phys     net0           online
loc          Automatic      online
```

En el ejemplo siguiente, el subcomando `list` se utiliza con la opción `-p` para mostrar todas las ubicaciones que se encuentran actualmente en el sistema. En el ejemplo concreto, la ubicación **`Automatic`** está en línea (activada).

```
$ netadm list -p loc
TYPE  PROFILE   STATE
loc  DefaultFixed  offline
loc  NoNet   offline
loc  Automatic  online
```

En el ejemplo siguiente, se utiliza el subcomando `list` con la opción `-c` para mostrar todas las NCU de interfaz del NCP activo.

```
$ netadm list -c ip
TYPE         PROFILE         STATE
ncu:ip       net0            online
ncu:ip       net1            offline
```

Visualización de valores del estado auxiliar de perfiles

El estado auxiliar de un perfil proporciona una explicación sobre el motivo por el que un perfil determinado está en línea o fuera de línea (activado o desactivado). Para mostrar los valores del estado auxiliar, utilice la opción `-x` con el subcomando `list`, como se muestra a continuación.

```
$ netadm list -x
TYPE        PROFILE        STATE          AUXILIARY STATE
```

```
ncp         DefaultFixed   disabled       disabled by administrator
ncp         Automatic      online         active
ncu:phys    net0           online         interface/link is up
ncu:phys    net1           offline        interface/link is down
ncu:ip      net0           online         interface/link is up
ncu:ip      net1           offline        conditions for activation are unmet
loc         Automatic      offline        conditions for activation are unmet
loc         NoNet          offline        conditions for activation are unmet
enm   test-enm    disabled    disabled by administrator
loc         DefaultFixed   offline        conditions for activation are unmet
```

Los valores de estado auxiliar varían en función del tipo de perfil. Para obtener información detallada sobre estados auxiliares, consulte la página del comando man nwamd(1M).

Eliminación de perfiles

Utilice el subcomando `destroy` para eliminar los perfiles definidos por el usuario y los objetos de configuración, como NCU. *No puede* eliminar perfiles definidos por el sistema, incluidos los siguientes: NCP `Automatic` y `DefaultFixed` y las ubicaciones `Automatic`, `NoNet` y `DefaultFixed`. Tenga en cuenta que tampoco puede eliminar un perfil que está activo actualmente. Primero debe desactivar el perfil y, a continuación, eliminarlo.

La sintaxis del subcomando `destroy` es la siguiente:

```
netcfg> destroy [ -a | object-type [ class ] object-name]
```

La opción `-a` elimina todos los perfiles definidos por el usuario del sistema, salvo los perfiles definidos por el usuario actualmente activos.

▼ Cómo eliminar un perfil de manera interactiva

El siguiente procedimiento describe cómo eliminar un perfil definido por el usuario de manera interactiva. A modo de ejemplo únicamente, este procedimiento muestra cómo eliminar una NCU IP del NCP definido por el usuario `myncp`.

1. Inicie la sesión interactiva `netcfg`.

```
$ netcfg
netcfg>
```

2. Seleccione el perfil.

Por ejemplo, para seleccionar el NCP `myncp`, debe escribir el siguiente comando:

```
netcfg> select ncp myncp
```

```
netcfg:ncp:myncp>
```

3. **Elimine el objeto de configuración o el perfil.**

   En el siguiente ejemplo, se elimina la NCU IP `net1` del NCP `myncp`:

```
netcfg:ncp:myncp> destroy ncu ip net1
netcfg:ncp:myncp>
```

4. **Salga de la sesión interactiva. Por ejemplo:**

```
netcfg:ncp:myncp> exit
```

ejemplo 6-12 Eliminación de un perfil en el modo de línea de comandos

El ejemplo anterior que muestra cómo eliminar un perfil de manera interactiva también se puede realizar en el modo de línea de comandos de la siguiente manera:

```
$ netcfg "select ncp myncp; destroy ncu ip net1"
```

Exportación de la configuración de un perfil

Utilice el subcomando `export` para guardar la configuración de un perfil. La exportación de un perfil puede ser útil si usted es responsable del mantenimiento de múltiples servidores que requieren configuraciones de red idénticas. El subcomando `export` se puede utilizar en modo interactivo o en el modo de línea de comandos. Cuando se exporta un perfil, la salida se muestra como una serie de subcomandos que el comando `netcfg` puede interpretar. Estos subcomandos son similares a los comandos que escribe en el modo interactivo o de línea de comandos.

Nota - El uso de la función `export` está limitado a algunas configuraciones. Sólo puede exportar o restaurar objetos de configuración que se crearon inicialmente mediante el comando `netcfg`. No puede exportar objetos de configuración que se crearon mediante el comando `dladm` o el comando `ipadm`, por ejemplo, las agregaciones de enlaces o los grupos IPMP. Tampoco puede exportar el NCP `DefaultFixed` y las ubicaciones `DefaultFixed`.

La sintaxis del subcomando `export` es la siguiente:

```
netcfg> export [ -d ] [ -f output-file ] [ object-type [ class ] object-name ]
```

Nota - Las opciones `-d` y `-f` del subcomando `export` se pueden utilizar de manera independiente de las demás. La opción `-f` imprime la configuración actual en el ámbito actual o en el especificado para un archivo determinado. La opción `-d` agrega el comando `destroy -a` como la primera línea de la salida.

EJEMPLO 6-13 Exportación de la configuración de un perfil de manera interactiva

El siguiente ejemplo muestra cómo visualizar la configuración de un perfil en pantalla mediante el subcomando `export` de manera interactiva.

```
$ netcfg
netcfg> export
create ncp "myncp"
create ncu ip "net0"
set ip-version=ipv4
set ipv4-addrsrc=dhcp
set ipv6-addrsrc=dhcp,autoconf
end
create ncu phys "net0"
set activation-mode=manual
set mtu=5000
end
end
create loc "test-loc"
set activation-mode=conditional-all
set conditions="system-domain is example.com"
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
end
create enm "test-enm"
set activation-mode=conditional-all
set conditions="ip-address is-not-in-range 10.2.3.4"
set fmri="svc:/application/test-enm:default"
end
create wlan "mywifi"
set priority=100
set keyname="mywifi-key"
set security-mode=wpa
end
```

En el modo de línea de comandos, escriba el siguiente comando:

```
$ netcfg export
```

Puede utilizar la opción `-d` con el subcomando `export` para agregar el comando `destroy -a` como la primera línea de la salida `netcfg export`, como se muestra en el siguiente ejemplo, que aparece truncado para que sea más breve:

```
$ netcfg
netcfg> export -d
destroy -a
create ncp "myncp"
create ncu ip "net0"
set ip-version=ipv4
set ipv4-addrsrc=dhcp
.
```

.
.

En el modo de línea de comandos, escriba el siguiente comando:

```
$ netcfg export -d
```

EJEMPLO 6-14 Exportación de una configuración de perfil a un archivo

En los siguientes ejemplos, la información de configuración del NCP `myncp` se escribe en un archivo mediante el subcomando `export` con la opción `-f`. En el siguiente ejemplo, la opción `-f` escribe la salida en un nuevo archivo denominado `myncp2`. La opción `-d` se utiliza para agregar el comando `destroy -a` como la primera línea de la salida de `netcfg export`.

Puede exportar la configuración del perfil a un archivo de manera interactiva como se describe a continuación:

```
$ netcfg
netcfg> export -d -f myncp2
```

Puede realizar la misma tarea en el modo de línea de comandos de la siguiente manera:

```
$ netcfg export -d -f myncp2
```

El siguiente ejemplo truncado muestra cómo se vería la configuración del perfil:

```
$ cat myncp2
destroy -a
create ncp "myncp"
create ncu ip "net0"
.
.
.
```

Restauración de la configuración de un perfil exportado

Puede importar una configuración de perfil que se generó con el subcomando `export` de vuelta al sistema. El archivo exportado tiene una serie de subcomandos que el comando `netcfg` es capaz de interpretar. El subcomando `export` es útil si necesita restaurar la configuración de un perfil o copiar la configuración de un perfil a otro sistema. Tenga en cuenta que sólo puede restaurar una configuración de perfil con el modo de línea de comandos `netcfg`.

Utilice el siguiente comando para restaurar una configuración exportada:

```
$ netcfg -f file
```

Por ejemplo, debe restaurar el archivo que se exportó en el Ejemplo 6-14, “Exportación de una configuración de perfil a un archivo”, de la siguiente manera:

```
$ netcfg -f myncp2
Configuration read.
```

Administración de la configuración de red desde el escritorio

Puede gestionar la configuración de red desde el escritorio mediante la GUI de administración de redes (anteriormente NWAM). La herramienta es similar al uso de los comandos `netcfg` y `netadm`. Con la GUI, puede conectarse a redes con cables o redes inalámbricas, configurar una nueva conexión con cables o inalámbrica, crear perfiles de ubicación, y activar o desactivar perfiles. La gestión de la configuración de red desde el escritorio funciona mejor para los usuarios de equipos portátiles y en situaciones en las que las condiciones de red cambian a menudo, por ejemplo, cuando se pasa de una oficina doméstica a la red inalámbrica del trabajo, o cuando se está de viaje.

Para obtener información acerca de la gestión de redes inalámbricas desde el escritorio, consulte “Administración de redes inalámbricas desde el escritorio” [153].

Cuando gestione la configuración de red desde el escritorio, siga estas pautas generales y las prácticas recomendadas:

- En el momento de gestionar la configuración de red desde el escritorio, la solución más fácil es activar el NCP `Automatic` definido por el sistema. En casa, puede utilizar este NCP para conectarse a la red inalámbrica.
- Si decide que desea utilizar una conexión con cable, conecte el cable Ethernet. No cambie del NCP `Automatic` predeterminado a otro NCP. La conexión de red se adaptará automáticamente de una conexión de red inalámbrica a una conexión de red con cable, sin tener que realizar ningún otro cambio en la configuración de red existente.
- En la oficina, se aplican las mismas reglas. Si no hay ningún cable Ethernet conectado a la red, y el NCP `Automatic` está activado, se utiliza la red reactiva y se establece automáticamente una conexión de red inalámbrica.
- Si el NCP `DefaultFixed` está activado actualmente, *sólo* puede ver su estado. Para configurar la red cuando este NCP está activo, debe utilizar los comandos `dladm` y `ipadm`. Consulte el Capítulo 2, Administración de la configuración de enlaces de datos en Oracle Solaris y el Capítulo 3, Configuración y administración de direcciones e interfaces IP en Oracle Solaris.
- Tenga en cuenta que, tanto en su casa como en la oficina, primero, deberá elegir una red inalámbrica y guardarla en su lista de redes inalámbricas favoritas, si todavía no lo ha hecho.

Elija una red inalámbrica mediante la GUI de administración de redes o mediante la ejecución del comando `netadm select-wifi`. Consulte “Administración de WLAN conocidas en modo reactivo” [153].

- Para ver el estado de la conexión de red actual, pase el mouse sobre el icono de notificación de estado de red ubicado en el escritorio, o simplemente haga clic en el ícono. El ícono de notificación de estado de red también incluye un menú contextual para crear y gestionar la configuración de red mediante la GUI.

  Si el ícono de notificación de estado de red no está visible en el escritorio, inícielo mediante la selección de Sistema -> Administración -> Red. Para iniciar la GUI desde la línea de comandos, ejecute el comando `nwam-manager`. Consulte la página del comando man `nwam-manager`(1M) en la recopilación de páginas del comando man JDS/GNOME para obtener más información.
- La configuración relacionada con IP se gestiona en la sección Perfil de red del cuadro de diálogo Preferencias de red. Para acceder al cuadro de diálogo Preferencias de red, haga clic en el ícono de notificación de estado de red ubicado en el escritorio, o elija la opción Preferencias de red del menú contextual del ícono de notificación de estado de red.

♦ ♦ ♦ CAPÍTULO 7

Administración de redes inalámbricas en Oracle Solaris

Este capítulo incluye tareas para administrar las redes inalámbricas en la versión Oracle Solaris.

Las especificaciones de IEEE 802.11 definen las comunicaciones inalámbricas para redes de área local. Estas especificaciones y las redes que describen se denominan colectivamente *Wi-Fi*, un término que es una marca comercial registrada por el grupo de comercio Wi-Fi Alliance. Las redes Wi-Fi son razonablemente fáciles de configurar para los proveedores y los posibles clientes. Por lo tanto, son cada vez más populares y más utilizadas en todo el mundo. Las redes Wi-Fi utilizan la misma tecnología de onda de radio que los teléfonos móviles, las televisiones y las radios.

Nota - Oracle Solaris no contiene funciones para configurar servidores o puntos de acceso Wi-Fi.

Este capítulo se divide en los siguientes apartados:

Administración de redes inalámbricas mediante la línea de comandos

En esta sección, se describen las siguientes tareas:

▼ Cómo conectarse a una red Wi-Fi

Antes de empezar Realice los siguientes pasos para conectar su equipo personal portátil a una red Wi-Fi.

1. **Conviértase en un administrador.**

2. **Visualice los atributos físicos de los enlaces de datos que se encuentran en el sistema.**

```
# dladm show-phys
LINK            MEDIA               STATE    SPEED  DUPLEX    DEVICE
net0            Ethernet            up       1500   full      ath0
net1            Ethernet            up       1500   full      e1000g0
```

En el ejemplo anterior, la salida indica que hay dos enlaces disponibles. `net0` en el enlace `ath0` del dispositivo admite comunicaciones Wi-Fi. El enlace `e1000g0` le permite conectar el sistema a una red con cables.

3. **Configure la interfaz Wi-Fi.**

   a. **Cree una interfaz que admita Wi-Fi. Por ejemplo:**

```
# ipadm create-ip net0
```

   b. **Compruebe que el enlace esté conectado.**

```
# ipadm show-if
IFNAME      CLASS        STATE     ACTIVE     OVER
lo0         loopback     ok        yes        --
net0        ip           ok        yes        --
```

4. **Compruebe si hay redes disponibles.**

```
# dladm scan-wifi
LINK       ESSID        BSSID/IBSSID       SEC     STRENGTH   MODE   SPEED
net0       ofc          00:0e:38:49:01:d0  none     good       g      54Mb
net0       home         00:0e:38:49:02:f0  none     very weak  g      54Mb
net0       linksys      00:0d:ed:a5:47:e0  none     very good  g      54Mb
```

El comando `scan-wifi` muestra información sobre las redes Wi-Fi disponibles en la ubicación actual. Este capítulo incluye la información siguiente:

`LINK` Hace referencia al nombre del enlace que se utilizará en la conexión Wi-Fi.

`ESSID` Hace referencia al identificador de conjunto de servicios extendidos. El `ESSID` es el nombre de la red Wi-Fi, a la que el administrador de la red inalámbrica específica le puede asignar un nombre de manera aleatoria.

`BSSID/IBSSID`	Hace referencia al identificador de conjunto de servicios básicos, que es un identificador único para un ESSID determinado. El BSSID es la dirección MAC de 48 bits del punto de acceso cercano que brinda a la red un determinado ESSID.
`SEC`	Hace referencia al tipo de seguridad necesaria para acceder a la red inalámbrica. Los valores son `none`, `WEP` y `WPA`. Para obtener más información, consulte "Definición de comunicaciones seguras mediante Wi-Fi" [151].
`STRENGTH`	Hace referencia a la fuerza de la señales de radio de las redes Wi-Fi que están disponibles en la ubicación.
`MODE`	Hace referencia a la versión del protocolo 802.11 que ejecuta la red. Los modos son a, b y g, o cualquier combinación de estos modos.
`SPEED`	Hace referencia a la velocidad (en megabits por segundo) de la red específica.

5. **Conéctese a una red Wi-Fi con cualquiera de los siguientes métodos:**

   - **Conéctese a una red Wi-Fi no segura que tenga la señal más fuerte.**

     ```
     # dladm connect-wifi
     ```

   - **Conéctese a una red no segura especificando su ESSID.**

     ```
     # dladm connect-wifi -e ESSID
     ```

     Para obtener más información sobre cómo utilizar el comando `dladm connect-wifi`, consulte "Definición de comunicaciones seguras mediante Wi-Fi" [151] y la página del comando man `dladm`(1M).

6. **Verifique el estado de la red Wi-Fi a la que está conectada el sistema de la siguiente manera:**

```
# dladm show-wifi
LINK       STATUS       ESSID       SEC     STRENGTH   MODE   SPEED
net0       connected    ofc         none    very good   g      36Mb
```

La salida anterior indica que el sistema está conectado a la red `ofc`. La salida `scan-wifi` del Paso 4 de este procedimiento indicaba que `ofc` tenía la señal más fuerte de las otras redes disponibles. El comando `dladm connect-wifi` selecciona de manera automática la red Wi-Fi con mejor señal, a menos que especifique directamente una red distinta.

7. **Configure una dirección IP para la interfaz con cualquiera de los siguientes métodos:**

- **Obtenga una dirección IP de un servidor DHCP.**

  ```
  # ipadm create-addr -T dhcp interface
  ```

  Si la red Wi-Fi no admite DHCP, aparece el siguiente mensaje:

  ```
  ipadm: interface: interface does not exist or cannot be managed using DHCP
  ```

- **Configure una dirección IP estática.**

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

  Utilice esta opción si tiene una dirección IP dedicada para el sistema.

8. **Acceda a Internet a través de la red Wi-Fi de una de las siguientes maneras:**

   - **Si el punto de acceso ofrece servicio gratuito, puede ejecutar un explorador o una aplicación de su elección.**

   - **Si el punto de acceso está en una red Wi-Fi comercial que requiere el pago de un arancel, siga las instrucciones que se proporcionan en la ubicación.**

     Normalmente, debe proporcionar una clave y un método de pago para esta opción.

9. **Termine la sesión de una de las siguientes maneras:**

   - **Termine la sesión Wi-Fi, pero deje el sistema en ejecución.**

     ```
     # dladm disconnect-wifi
     ```

   - **Termine una sesión Wi-Fi en particular cuando se esté ejecutando más de una sesión.**

     ```
     # dladm disconnect-wifi link
     ```

     donde *link* representa la interfaz que se está utilizando para la sesión.

   - **Cierre el sistema sin errores mientras la sesión Wi-Fi se está ejecutando.**

     ```
     # shutdown -g0 -i5
     ```

     No es necesario desconectar explícitamente la sesión Wi-Fi antes de cerrar el sistema.

ejemplo 7-1 Conexión con una red Wi-Fi determinada

El siguiente ejemplo combina los diferentes pasos que debe realizar para conectar el sistema Oracle Solaris a una red inalámbrica. También se muestra cómo se puede forzar la conexión del sistema a una red inalámbrica preferida y específica, en lugar de permitir que el sistema

operativo seleccione aleatoriamente la red inalámbrica. En el siguiente ejemplo, se supone que tiene la dirección IP estática 10.192.16.3/24 asignada para usarla en su equipo personal portátil.

```
# dladm show-phys
LINK            MEDIA               STATE    SPEED  DUPLEX    DEVICE
net0            Ethernet            up       1500   full      ath0
net1            Ethernet            up       1500   full      e1000g0

# ipadm create-ip net0
# ipadm show-if net0
IFNAME      CLASS        STATE     ACTIVE     OVER
lo0         loopback     ok        yes        --
net0        ip           ok        yes        --

# dladm scan-wifi
LINK       ESSID        BSSID/IBSSID       SEC     STRENGTH   MODE   SPEED
net0       wifi-a       00:0e:38:49:01:d0  none     weak       g      54Mb
net0       wifi-b       00:0e:38:49:02:f0  none     very weak  g      54Mb
net0       ofc-net      00:0d:ed:a5:47:e0  wep      very good  g      54Mb
net0       citinet      00:40:96:2a:56:b5  none     good       b      11Mb

# dladm connect-wifi -e citinet
# dladm show-wifi
LINK       STATUS        ESSID         SEC     STRENGTH   MODE   SPEED
net0       connected     citinet       none    good       g      11Mb

# ipadm create-addr -a 10.192.16.3/24 net0
ipadm: net0/v4
# ipadm show-addr net0
ADDROBJ           TYPE     STATE        ADDR
net0/v4           static   ok           10.192.16.3/24
```

Inicie un explorador u otra aplicación para comenzar a trabajar en la red Wi-Fi.

```
# firefox
```

Termine la sesión, pero deje el equipo en ejecución.

```
# dladm disconnect-wifi
# dladm show-wifi
LINK       STATUS        ESSID         SEC     STRENGTH   MODE   SPEED
net0       disconnected   --            --       --       --       --
```

La salida de `show-wifi` verifica que se haya desconectado el enlace `net0` de la red Wi-Fi.

▼ Cómo supervisar el enlace Wi-Fi

El siguiente procedimiento describe cómo supervisar el estado del enlace Wi-Fi mediante herramientas de red estándar y también cómo cambiar la propiedad del enlace seleccionado.

1. **Conviértase en un administrador.**

2. **Conéctese a la red Wi-Fi, como se describe en Cómo conectarse a una red Wi-Fi [146].**

3. **Vea las propiedades de los enlaces de datos del sistema.**

   ```
   # dladm show-linkprop link
   ```

4. **Defina una velocidad fija para el enlace.**

   Atención - Oracle Solaris selecciona automáticamente la velocidad óptima para una conexión Wi-Fi. La modificación de la velocidad inicial del enlace puede disminuir del rendimiento o evitar que se establezcan determinadas conexiones Wi-Fi.

   Puede modificar la velocidad del enlace a uno de los posibles valores que se muestra en la salida del subcomando `show-linkprop`, como se muestra en el siguiente ejemplo:

   ```
   # dladm set-linkprop -p speed=value link
   ```

5. **Compruebe el flujo el paquete mediante un enlace.**

   ```
   # netstat -I net0 -i 5
   input   net0      output       input  (Total)    output
   packets errs  packets errs  colls  packets errs  packets errs  colls
   317     0     106     0     0      2905    0     571     0     0
   14      0     0       0     0      20      0     0       0     0
   7       0     0       0     0      16      0     1       0     0
   5       0     0       0     0      9       0     0       0     0
   304     0     10      0     0      631     0     316     0     0
   338     0     9       0     0      722     0     381     0     0
   294     0     7       0     0      670     0     371     0     0
   306     0     5       0     0      649     0     338     0     0
   289     0     5       0     0      597     0     301     0     0
   ```

ejemplo 7-2 Establecimiento de la velocidad de un enlace

El siguiente ejemplo muestra cómo configurar la velocidad de un enlace después de haberse conectado a una red Wi-Fi.

```
# dladm show-linkprop -p speed net0
LINK     PROPERTY        PERM VALUE        EFFECTIVE    DEFAULT   POSSIBLE
net0     speed           r-   25           0            0
 1,2,5,6,9,11,12,18,24,36,48,54
# dladm set-linkprop -p speed=36 net0

# dladm show-linkprop -p speed net0
LINK     PROPERTY        PERM VALUE        EFFECTIVE    DEFAULT   POSSIBLE
net0     speed           r-   36           0            0
 1,2,5,6,9,11,12,18,24,36,48,54
```

Definición de comunicaciones seguras mediante Wi-Fi

La tecnología de onda de radio hace que las redes Wi-Fi estén disponibles y tengan acceso libre para los usuarios. Por lo tanto, establecer la conexión con una red Wi-Fi puede resultar inseguro.

Los siguientes tipos de conexiones Wi-Fi son más seguros:

- Conexión a una red Wi-Fi privada de acceso restringido.

  Las redes privadas, como las redes internas, establecidas por las empresas o las universidades, restringen el acceso a las redes para los usuarios que puedan cumplir con el desafío de seguridad planteado. Los usuarios potenciales deben proporcionar una clave durante la secuencia de conexión o iniciar una sesión en la red mediante una red privada virtual (VPN) segura.
- Cifrado de la conexión a la red Wi-Fi

  Puede cifrar las comunicaciones entre el sistema y la red Wi-Fi utilizando claves seguras. El punto de acceso a la red Wi-Fi debe ser un enrutador ubicado en su hogar u oficina que tenga la función para generar claves seguras. El sistema y el enrutador se establecen y, a continuación, se puede compartir la clave antes de crear la conexión segura.

El comando `dladm` puede utilizar una clave de privacidad equivalente a cable (WEP) o un acceso protegido Wi-Fi (WPA) para cifrar conexiones mediante un punto de acceso. El protocolo WEP se define en las especificaciones IEEE 802.11 para conexiones inalámbricas. El protocolo WPA se define en las especificaciones IEEE 802.11i para conexiones inalámbricas. Oracle Solaris admite las versiones 1 y 2 del estándar de WPA. Para obtener más información sobre las opciones del comando `dladm` relacionadas con WEP y WPA, consulte la página del comando man `dladm`(1M).

▼ Cómo configurar una conexión de red Wi-Fi cifrada mediante la especificación de una clave WEP

El siguiente procedimiento describe cómo configurar comunicaciones seguras entre un sistema y un enrutador en el hogar. Muchos enrutadores inalámbricos o con cables para el hogar cuentan con una función de cifrado que puede generar claves seguras.

Antes de empezar Si se va a conectar a la red inalámbrica de su hogar, asegúrese de haber configurado el enrutador y de haber generado la clave WEP. Siga la documentación del fabricante del enrutador para generar y guardar la configuración de clave.

1. **Conviértase en un administrador.**
2. **Cree un objeto seguro que contenga la clave WEP de la siguiente manera:**

```
# dladm create-secobj -c wep keyname
```

donde *keyname* representa el nombre que desea dar a la clave.

3. **Proporcione el valor de la clave WEP al objeto seguro.**

   Luego, el subcomando `create-secobj` ejecuta una secuencia de comandos que solicita un valor para la clave.

   ```
   provide value for keyname: 5-or-13-byte key
   confirm value for keyname: Retype key
   ```

   Este valor es la clave generada por el enrutador. La secuencia de comandos acepta una cadena de 5 o 13 bytes, en formato ASCII o en hexadecimal, como valor de la clave.

4. **Vea el contenido de la clave que acaba de crear.**

   ```
   # dladm show-secobj
   OBJECT              CLASS
   keyname               wep
   ```

   donde *keyname* es el nombre del objeto seguro.

5. **Establezca una conexión cifrada para la red Wi-Fi.**

   ```
   # dladm connect-wifi -e network -k keyname interface
   ```

6. **Compruebe que la conexión sea segura.**

   ```
   # dladm show-wifi
   LINK       STATUS        ESSID         SEC     STRENGTH   MODE   SPEED
   net0       connected     wifi-1        wep     good       g      11Mb
   ```

   En la salida anterior, el valor `wep` que se encuentra en la columna `SEC` indica que el cifrado WEP para la conexión está en su lugar.

ejemplo 7-3 Configuración de comunicaciones Wi-Fi cifradas mediante una clave WEP

El siguiente ejemplo supone que ya realizó lo siguiente:

- Seguir la documentación del fabricante del enrutador y crear la clave WEP.
- Guardar la clave a fin de utilizarla para crear el objeto seguro en el sistema.

Un objeto seguro se crea de la siguiente manera:

```
# dladm create-secobj -c wep mykey
provide value for mykey: *****
confirm value for mkey: *****
```

Cuando introduzca la clave WEP generada por el enrutador, el valor que escriba se verá como asteriscos en la pantalla.

El siguiente comando establece una conexión cifrada a la red Wi-Fi `citinet` mediante el objeto seguro `mykey`.

```
# dladm show-secobj
OBJECT              CLASS
mykey               wep
# dladm connect-wifi -e citinet -k mykey net0
```

El siguiente comando verifica que está conectado a la red inalámbrica `citinet` mediante un cifrado WEP.

```
# dladm show-wifi
LINK       STATUS        ESSID         SEC     STRENGTH   MODE   SPEED
net0       connected     citinet       wep     good       g      36Mb
```

Administración de WLAN conocidas en modo reactivo

Si utiliza un perfil reactivo, es posible que también desee aprovechar la capacidad del sistema para conectarse automáticamente a las *WLAN conocidas*. Cuando se conecta a una WLAN, se guarda la información acerca de esa WLAN en un perfil de red de tipo `known-wlan`. También puede crear manualmente los perfiles `known-wlan` de mediante el comando `netcfg`. Para obtener información general sobre las WLAN conocidas, consulte “Descripción de una WLAN conocida” [106] For task-related information, see “Creación de WLAN conocidas” [126].

Administración de redes inalámbricas desde el escritorio

De manera predeterminada, cuando se activan conexiones de red inalámbrica, el daemon de red reactivo (`nwamd`) intenta conectarse a cualquier red disponible de la lista de favoritos, sin preguntar, en el orden de prioridad en el que se muestran las conexiones. Si no hay redes favoritas disponibles, se abre el cuadro del selector de redes inalámbricas. En este cuadro, puede elegir una red inalámbrica para incorporarse.

También puede modificar la manera en la que se intentan las conexiones inalámbricas en la ficha Inalámbrico de la vista Propiedades de conexión del cuadro de Preferencias de red en la GUI de administración de redes. Si es necesario, también puede conectarse manualmente a una red inalámbrica diferente haciendo clic con el botón derecho en el ícono de notificación de estado de red que se encuentra en el escritorio.

Sugerencia - Puede acceder a la vista de Propiedades de conexión para una red seleccionada mediante el cuadro de diálogo de Preferencias de red. Este cuadro de diálogo contiene una lista desplegable con la etiqueta Mostrar. Esta lista le permite alternar entre las vistas para una red determinada. En cada vista, hay diferentes tareas que puede realizar, así como información sobre la red seleccionada que es específica para esa vista.

Las siguientes vistas existen para cada conexión de red en cada perfil de red que está en el sistema:

- Estado de conexión
- Perfil de red
- Propiedades de conexión

Para obtener más información sobre la configuración de red basada en perfiles, consulte el Capítulo 5, Acerca de la administración de la configuración de red basada en perfiles en Oracle Solaris y la ayuda en pantalla de la GUI.

▼ Cómo incorporar una red inalámbrica

Las redes inalámbricas se incorporan mediante la selección de la opción Incorporarse a red inalámbrica a la que puede accederse haciendo clic con el botón derecho en el ícono de notificación de estado de red. El cuadro del selector de redes inalámbricas es donde se muestra una lista de redes inalámbricas disponibles para conectarse.

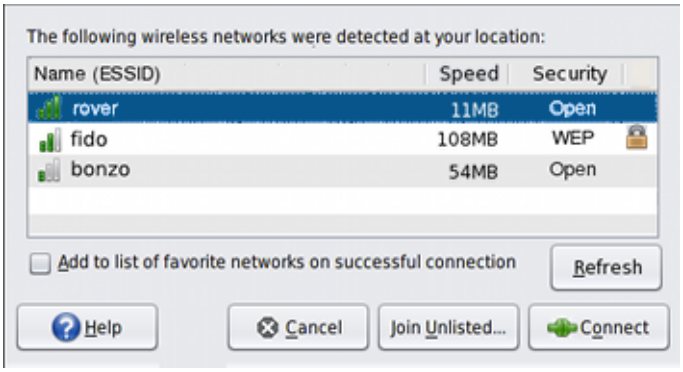
1. **Para conectarse manualmente a una red inalámbrica diferente, realice una de las siguientes acciones:**

   - **Seleccione una red inalámbrica disponible desde el icono de notificación de estado de red del menú que aparece al hacer clic con el botón derecho.**

   - **Seleccione la opción Incorporarse a red inalámbrica que no está en la lista del menú del icono de notificación de estado de red.**

     Una red inalámbrica que no está en la lista es una red que ha sido configurada de modo que no se difunda su nombre de red pero que está disponible para incorporarse a ella.

   - **Seleccione una red inalámbrica disponible desde el cuadro de diálogo del selector de redes inalámbricas. Este cuadro de diálogo se muestra automáticamente siempre que haya una elección de redes inalámbricas disponible para a las que pueda incorporarse.**



2. **Si se abre el cuadro de diálogo Incorporarse a red inalámbrica, proporcione toda la información necesaria para la red inalámbrica que haya escogido.**

Gestión de redes inalámbricas favoritas desde el escritorio

De manera predeterminada, cuando se une a una red inalámbrica por primera vez, aparece la casilla de selección Agregar a lista de redes favoritas cuando la conexión sea satisfactoria en el cuadro de diálogo Incorporarse a red inalámbrica.

Para agregar la red inalámbrica a su lista de favoritas (si la conexión es satisfactoria) active esta casilla. Si no desea que se agregue la red a su lista de favoritas, desactive esta casilla. La casilla está activada de manera predeterminada.

Para agregar una red inalámbrica que no está disponible actualmente o que no informa actualmente su nombre de red a su lista de favoritas, vaya a la ficha Inalámbrico de la vista Propiedades de conexión y haga clic en el botón Agregar. Para agregar una red, debe conocer su nombre de red, su tipo de seguridad y su clave de seguridad.

índice

D

E

G

H

I

M

N

O

P

R

S

T

U

V

W