

Conexión de sistemas mediante la configuración de redes fijas en Oracle® Solaris 11.1

Copyright © 2011, 2012, Oracle y/o sus filiales. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comunique por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera licencias en nombre del Gobierno de EE.UU. se aplicará la siguiente disposición:

U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus subsidiarias declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus subsidiarias. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden ofrecer acceso a contenidos, productos o servicios de terceros o información sobre los mismos. Ni Oracle Corporation ni sus subsidiarias serán responsables de ofrecer cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros y renuncian explícitamente a ello. Oracle Corporation y sus subsidiarias no se harán responsables de las pérdidas, los costos o los daños en los que se incurra como consecuencia del acceso o el uso de contenidos, productos o servicios de terceros.

Contenido

Prefacio	7
1 Descripción general de la configuración de red fija	11
¿Qué es la configuración de red fija?	11
Características principales de la configuración de red gestionada por perfiles	12
Herramientas de configuración de red	13
Comando dladm	15
Comando ipadm	16
2 Configuración de un sistema para la red	19
Configuración de la red (mapa de tareas)	19
▼ SPARC: Cómo asegurarse de que la dirección MAC de cada interfaz sea única	20
▼ Cómo cambiar el NCP activo en el sistema	21
▼ Cómo configurar una interfaz IP	22
Otras tareas de administración y configuración de redes	27
3 Cómo trabajar con enlaces de datos	29
Comandos dladm básicos	29
Visualización de información general sobre enlaces de datos (dladm)	29
Visualización de los enlaces de datos de un sistema (dladm show-link)	30
Visualización de atributos físicos de enlaces de datos (dladm show-phys)	30
Supresión de un enlace de datos (dladm delete-phys)	31
Cambio de nombre de un enlace de datos (dladm rename-link)	32
Personalización de propiedades de enlaces de datos	32
Descripción general de las propiedades de enlaces de datos	32
Activación de compatibilidad con tramas gigantes	33
Modificación de parámetros de la velocidad de enlace	33

Establecimiento del módulo STREAMS en enlaces de datos	35
Establecimiento del controlador e1000g para usar el enlace de acceso directo a memoria	35
Establecimiento manual de la frecuencia de interrupción	36
Obtención de información de estado de las propiedades de enlace de datos	37
Otras tareas de configuración con el comando dladm	38
▼ Cómo cambiar interfaces principales en un sistema	38
▼ Cómo sustituir una tarjeta de interfaz de red con reconfiguración dinámica	40
4 Trabajo con interfaces IP	43
Comandos ipadm básicos	43
Eliminación de una configuración de interfaz IP (ipadm delete-ip)	43
Desactivación de una configuración de interfaz IP (ipadm disable-ip)	44
Eliminación de la dirección de una interfaz (ipadm delete-addr)	44
Configuración de las propiedades de la interfaz IP	45
Activación de reenvío de paquetes	45
Configuración de las propiedades de las direcciones IP	47
Establecimiento de propiedades de protocolo TCP/IP	48
Activación del reenvío de paquetes de forma global	49
Configuración de un puerto con privilegios	49
Implementación de enrutamiento simétrico en hosts múltiples	50
Implementación del control de congestión de tráfico	52
Cambio del tamaño de la memoria intermedia de recepción de TCP	53
Supervisión de direcciones e interfaces IP	55
Obtención de información general sobre las interfaces IP	55
Obtención de información sobre interfaces IP	56
Obtención de información sobre las propiedades de la interfaz IP	57
Obtención de información sobre direcciones IP	58
Obtención de información sobre las propiedades de direcciones IP	59
5 Configuración de redes inalámbricas en equipos portátiles que ejecutan Oracle Solaris	61
Mapa de tareas de comunicaciones Wi-Fi	61
▼ Cómo conectarse a una red Wi-Fi	62
▼ Cómo supervisar el enlace Wi-Fi	65
Comunicaciones seguras mediante Wi-Fi	67

- ▼ Cómo configurar una conexión de red Wi-Fi cifrada 67

- A Mapa de comparación: comandos `ifconfig` e `ipadm` 71**

- B Mapa de comparación: comandos `ndd` y `ipadm` 75**

- Índice79**

Prefacio

Bienvenido a *Conexión de sistemas mediante la configuración de redes fijas en Oracle Solaris 11.1*. Este manual forma parte de la serie *Establecimiento de una red Oracle Solaris 11.1* que abarca procedimientos y temas básicos para configurar redes Oracle Solaris. En esta guía, se asume que ya se ha instalado Oracle Solaris. La red debe estar configurada o preparada para poder integrar cualquier software de red que se necesite.

Nota – Esta versión de Oracle Solaris es compatible con sistemas que usen arquitecturas de las familias de procesadores SPARC y x86. Los sistemas compatibles aparecen en *Listas de compatibilidad del sistema operativo Oracle Solaris*. Este documento indica las diferencias de implementación entre los tipos de plataforma.

Para conocer cuáles son los sistemas admitidos, consulte *Listas de compatibilidad del sistema operativo Oracle Solaris*.

Quién debe utilizar este manual

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

Acceso a Oracle Support

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

Convenciones tipográficas

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

TABLA P-1 Convenciones tipográficas

Tipos de letra	Descripción	Ejemplo
AaBbCc123	Los nombres de los comandos, los archivos, los directorios y los resultados que el equipo muestra en pantalla	Edite el archivo <code>.login</code> . Utilice el comando <code>ls -a</code> para mostrar todos los archivos. <code>nombre_sistema% tiene correo.</code>
AaBbCc123	Lo que se escribe, en contraposición con la salida del equipo en pantalla	<code>nombre_sistema% su</code> Contraseña:
<i>aabbcc123</i>	Marcador de posición: sustituir por un valor o nombre real	El comando necesario para eliminar un archivo es <code>rm nombre_archivo</code> .
<i>AaBbCc123</i>	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el capítulo 6 de la <i>Guía del usuario</i> . Una <i>copia en caché</i> es aquella que se almacena localmente. <i>No</i> guarde el archivo. Nota: algunos elementos destacados aparecen en negrita en línea.

Indicadores de los shells en los ejemplos de comandos

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

TABLA P-2 Indicadores de shell

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

Descripción general de la configuración de red fija

En un sistema que ejecuta Oracle Solaris 11, la configuración de red puede ser reactiva o fija según el perfil de configuración de red (NCP, Network Configuration Profile) que esté activo en el sistema. Para obtener una descripción general de la configuración de red reactiva y fija, consulte *Introducción a redes de Oracle Solaris 11*. Para obtener información detallada sobre cómo crear y configurar NCP, consulte *Conexión de sistemas mediante la configuración de redes reactivas en Oracle Solaris 11.1*.

En este capítulo se presenta una introducción general a la configuración de red fija y se tratan los siguientes temas:

- “¿Qué es la configuración de red fija?” en la página 11
- “Características principales de la configuración de red gestionada por perfiles” en la página 12
- “Herramientas de configuración de red” en la página 13

¿Qué es la configuración de red fija?

En Oracle Solaris 11, la configuración de red se gestiona mediante perfiles de configuración de red (NCP). El tipo de NCP que está funcionando en un sistema específico determina la configuración de red de ese sistema. Si el NCP es reactivo, la configuración de red de ese sistema se implementa de manera dinámica. Si el NCP es fijo, la configuración de red se implementa de manera estática.

La configuración de red fija hace referencia al modo de configuración en el que se crean instancias de una configuración de red específica en el sistema. A diferencia de lo que ocurre en un modo de configuración de red reactiva, las instancias de una configuración en un modo de configuración fijo no se modifican, independientemente de los cambios realizados en el entorno de red del sistema. Si se producen cambios en dicho entorno, como la agregación de interfaces, debe volver a establecer manualmente la configuración de red del sistema para que el sistema se adapte al nuevo entorno.

Nota – No confunda la configuración de red fija con la simple configuración de direcciones IP estáticas. En la configuración de red fija, puede asignar una dirección DHCP a una interfaz. Del mismo modo, en la configuración de red reactiva, puede crear NCP donde las interfaces estén configuradas con direcciones IP estáticas. De esta manera, la configuración de red fija tiene un ámbito más amplio y hace referencia específicamente a la capacidad de la configuración de red del sistema de cambiar según los cambios en el entorno del sistema.

En la siguiente tabla se presenta una comparación entre los dos modos de configuración de red.

Características	Configuración de red reactiva	Configuración de red fija
Se adapta automáticamente a los cambios en el entorno de red del sistema	Admitida mediante varios NCP que se pueden configurar	No admitida; se requiere volver a configurar manualmente, según sea necesario
Tipo de NCP en funcionamiento en el sistema	Reactiva (Automatic, o algún otro NCP creado por el usuario)	Fija (DefaultFixed)
Varios NCP	Admitida (pero sólo puede haber un NCP activo a la vez)	No admitida
NCP creados por el usuario	Admitida	Sólo existe un NCP fijo (DefaultFixed), que es generado por el sistema. Sin embargo, el contenido de DefaultFixed es totalmente determinado por el usuario.

En las siguientes secciones se describe de manera más detallada la configuración de red gestionada por perfiles y las herramientas que se utilizan para la configuración de red.

Características principales de la configuración de red gestionada por perfiles

En Oracle Solaris 11, la configuración de red se basa en perfiles. La configuración de red de un sistema se gestiona mediante un NCP y un perfil de ubicación correspondiente. Para obtener una introducción a la configuración de red gestionada por perfiles, consulte [“Perfiles de configuración de red” de Introducción a redes de Oracle Solaris 11](#). Para obtener información detallada sobre los NCP, consulte [Conexión de sistemas mediante la configuración de redes reactivas en Oracle Solaris 11.1](#).

Nota – Para la configuración de red, los tipos de perfil principales son NCP, perfiles de ubicación, modificadores de red externa (ENM) y redes de área local inalámbricas (WLAN). De estos tipos, el perfil principal es el NCP. En esta documentación, a menos que se especifique lo contrario, el término *perfil* hace referencia al NCP.

Las características principales de la configuración de red basada en perfil son las siguientes:

- Sólo un par de perfiles de ubicación y NCP pueden estar activos al mismo tiempo para gestionar la configuración de red de un sistema. Todos los demás NCP existentes en el sistema no son operativos.
- El NCP activo puede ser *reactivo* o *fijo*. Con un perfil reactivo, la configuración de red se supervisa para adaptarse a los cambios del entorno de red del sistema. Con un perfil fijo, la configuración de red se instancia, pero no se supervisa.
- Si el NCP activo es reactivo, la configuración de red del sistema es adaptable. Si el NCP activo es fijo, la configuración de red del sistema es constante.
- Los valores de las diferentes propiedades de un NCP constituyen una política que controla cómo el perfil gestiona la configuración de red.
- Los cambios que se realizan en las propiedades del NCP se implementan inmediatamente como nuevos valores de propiedad. Estos nuevos valores pasan a formar parte de la política del perfil que gestiona la configuración de red.

Si su sistema está configurado para redes fijas, el NCP activo que gestiona su configuración de red es `DefaultFixed`. Este perfil es generado por el sistema operativo y es el único perfil fijo del sistema. Un sistema no admite varios perfiles fijos.

Las propiedades del NCP `DefaultFixed` reflejan la configuración persistente que se crea o se modifica mientras el NCP `DefaultFixed` está activo.

Herramientas de configuración de red

En Oracle Solaris 11, hay cuatro comandos de red disponibles para configurar la red:

- Comando `netcfg`
- Comando `netadm`
- Comando `dladm`
- Comando `ipadm`

Los comandos `netcfg` y `netadm` se utilizan para administrar la configuración de red reactiva en el sistema. El comando `netcfg` se utiliza para crear y configurar perfiles que implementan la configuración de red reactiva: NCP, perfiles de ubicación, ENM y WLAN. Sin embargo, en un sistema con configuración de red fija, puede utilizar el comando `netcfg` sólo para ver el perfil

`DefaultFixed`. El comando `netadm` se utiliza para administrar todos los perfiles del sistema, especialmente para mostrar los perfiles de red del sistema y para reemplazar un NCP activo por otro.

Los comandos `dladm` y `ipadm` se utilizan para configurar enlaces de datos e interfaces IP respectivamente. Los comandos crean configuraciones persistentes y cuando se utilizan se aplican al perfil que está activo en el sistema.

Por ejemplo, si un enlace de datos `net0` se configura con una unidad de transmisión máxima (MTU) específica de 1200 y el NCP activo es `Automatic`, este valor de MTU se convierte en el valor persistente para `net0` en el NCP `Automatic`. Luego, supongamos que ha activado un segundo NCP denominado `myncp`. Si ejecuta el comando `dladm` para establecer otro valor para la MTU, ese valor se aplicará a `myncp`. Por lo tanto, `net0` puede tener diferentes valores de MTU en diferentes perfiles. Por lo tanto, los comandos `dladm` y `ipadm` también se pueden utilizar para configurar perfiles de manera indirecta.

Al configurar enlaces de datos e interfaces IP con los comandos `dladm` o `ipadm`, tenga en cuenta los siguientes alcances de su uso:

- Los dos comandos configuran sólo los enlaces de datos y las interfaces IP del perfil activo. Para configurar otras propiedades del perfil, como el establecimiento de rutas predeterminadas, debe utilizar el comando `netcfg` para configurar la propiedad del perfil que hace referencia a rutas predeterminadas. También puede utilizar el comando `routeadm` que directamente establece las rutas predeterminadas en la tabla de enrutamiento del sistema. En el último caso, la configuración se aplica a todos los perfil que estén activos en el sistema.
- Puede utilizar los comandos `dladm` y `ipadm` en cualquier perfil reactivo, siempre que el perfil esté activo. Sin embargo, no puede utilizar el comando `netcfg` para configurar el perfil `DefaultFixed`, que es el único perfil fijo del sistema. Sólo puede utilizar los comandos `netadm` y `netcfg` para ver las propiedades del perfil `DefaultFixed`, pero no para configurarlas.

Los comandos `dladm` y `ipadm` se aplican al perfil activo, ya sea un perfil reactivo o fijo. Por lo tanto, antes de utilizar estos comandos, debe asegurarse de lo siguiente:

- Saber qué perfil está activo en el sistema para asegurarse de realizar cambios en el perfil de destino correcto.
- Saber si el perfil de destino es reactivo o fijo para evitar un comportamiento inesperado de la configuración después de utilizar los comandos. Un perfil reactivo gestiona la configuración de red de manera diferente de un perfil fijo. En consecuencia, el comportamiento de los dos perfiles también es distinto cuando se implementan los cambios.

En las siguientes secciones se describen los comandos `dladm` e `ipadm` en detalle.

Comando dladm

Utilice el comando `dladm` para configurar enlaces de datos. Las propiedades de enlaces de datos se pueden personalizar mediante el comando `dladm` siempre que el controlador de red del enlace se haya convertido a la estructura de configuración de controlador GLDv3, como `e1000g`. Para confirmar si el controlador específico admite esta función, consulte la página del comando `man` del controlador.

La implementación completa de la estructura de configuración de controlador GLDv3 ha mejorado la configuración de los controladores de tarjeta de interfaz de red (NIC) en los siguientes aspectos:

- Se necesita una sola interfaz de comando, el comando `dladm`, para configurar las propiedades del controlador de red.
- Se utiliza una sintaxis uniforme, independientemente de las propiedades: `dladm subcomando propiedades enlace de datos`.
- 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 incluso después de reiniciar el sistema.

Para aprovechar las ventajas al configurar enlaces de datos, debe utilizar `dladm` como la herramienta de configuración en lugar de las herramientas tradicionales de las versiones anteriores, como el comando `ndd`.

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

```
# dladm help
The following subcommands are supported:
Bridge      : add-bridge      create-bridge      delete-bridge
              modify-bridge  remove-bridge      show-bridge
Etherstub   : create-etherstub delete-etherstub   show-etherstub
IB          : create-part   delete-part        show-ib          show-part
IP tunnel   : create-iptun   delete-iptun       modify-iptun     show-iptun
Link Aggrgation: add-aggr      create-aggr        delete-aggr
              modify-aggr    remove-aggr        show-aggr
Link        : rename-link   reset-linkprop     set-linkprop
              show-link     show-linkprop
Secure Object : create-secobj  delete-secobj      show-secobj
VLAN        : create-vlan   delete-vlan        modify-vlan      show-vlan
VNIC        : create-vnic   delete-vnic        modify-vnic      show-vnic
Wifi        : connect-wifi  disconnect-wifi    scan-wifi        show-wifi
Miscellaneous : delete-phys  show-ether         show-phys        show-usage
For more info, run: dladm help <subcommand>.
```

Para utilizar el comando `dladm` en enlaces de datos, consulte [Capítulo 3, “Cómo trabajar con enlaces de datos”](#).

Comando `ipadm`

Los avances de Oracle Solaris han superado las capacidades de las herramientas tradicionales para administrar eficazmente distintos aspectos de la configuración de red. El comando `ifconfig`, por ejemplo, ha sido la herramienta tradicional para configurar interfaces de red. Sin embargo, este comando no implementa una configuración persistente. A lo largo del tiempo, `ifconfig` ha experimentado mejoras para abarcar más capacidades relacionadas con la administración de red. Sin embargo, como consecuencia, el comando se ha vuelto complejo y confuso.

Otro problema relacionado con la configuración y la administración de la interfaz es la ausencia de herramientas sencillas para administrar las propiedades o los valores ajustables de TCP/IP. El comando `ndd` ha sido la herramienta de personalización recomendada para este propósito. Sin embargo, al igual que el comando `ifconfig`, el comando `ndd` no implementa una configuración persistente. Anteriormente, la configuración persistente se podía simular para un escenario de red mediante la edición de las secuencias de comandos de inicio. Debido a la introducción de la utilidad de gestión de servicios (SMF) en Oracle Solaris, el uso de estas soluciones se puede volver arriesgado, debido a las complejidades de la gestión de las dependencias SMF, especialmente cuando existen actualizaciones de la instalación de Oracle Solaris.

El comando `ipadm` se introduce para reemplazar eventualmente el comando `ifconfig` para la configuración de interfaz. El comando también reemplaza el comando `ndd` para configurar propiedades de protocolo.

Como herramienta para configurar interfaces, el comando `ipadm` ofrece las ventajas siguientes:

- Gestiona interfaces IP y direcciones IP de manera más eficaz al ser una herramienta dedicada exclusivamente a la administración de interfaces IP, a diferencia del comando `ifconfig` que se utiliza para fines distintos de la configuración de interfaz.
- Implementa configuración de direcciones e interfaces persistentes.

Para obtener una lista de las opciones de `ifconfig` y sus subcomandos `ipadm` equivalentes, consulte [Apéndice A, “Mapa de comparación: comandos `ifconfig` e `ipadm`”](#).

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

- Puede establecer propiedades temporales o persistentes para IP, protocolo de resolución de direcciones (ARP), protocolo de transmisión para el control de flujo (SCTP) y protocolo de mensajes de control de Internet (ICMP), y para protocolos de capa superior, como TCP y protocolo de datagramas de usuario (UDP).

- Proporciona información sobre cada propiedad de TCP/IP, como el valor predeterminado y actual de una propiedad, y el rango de valores posibles. De esta manera, la información de depuración se obtiene con mayor facilidad.
- También sigue una sintaxis de comando coherente y, por lo tanto, es más fácil de usar.

Para obtener una lista de opciones `ndd` y sus subcomandos `ipadm` equivalentes, consulte [Apéndice B, “Mapa de comparación: comandos `ndd` y `ipadm`”](#).

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

```
# ipadm help
The following subcommands are supported:
Address          : create-addr  delete-addr  disable-addr
                  down-addr     enable-addr  refresh-addr
                  reset-addrprop set-addrprop show-addr
                  show-addrprop up-addr
Interface        : disable-if   enable-if    reset-ifprop
                  set-ifprop   show-if      show-ifprop
IP interface     : create-ip    delete-ip
IPMP interface   : add-ipmp    create-ipmp  delete-ipmp
                  remove-ipmp
Protocol property : reset-prop   set-prop     show-prop
VNI interface    : create-vni  delete-vni
For more info, run: ipadm help <subcommand>.
```


Configuración de un sistema para la red

En este capítulo se incluyen los procedimientos que debe seguir para configurar una interfaz IP en un sistema que utiliza una configuración de red fija. Se explican los siguientes temas:

- “Configuración de la red (mapa de tareas)” en la página 19
- “Otras tareas de administración y configuración de redes” en la página 27

Configuración de la red (mapa de tareas)

En esta sección se describen los procedimientos para la configuración básica de una interfaz IP. En la siguiente tabla se describen las tareas de configuración y se asignan dichas tareas a los procedimientos correspondientes.

Tarea	Descripción	Para obtener instrucciones
Configurar un sistema para que admita direcciones MAC únicas.	Configura un sistema basado en SPARC para permitir direcciones MAC únicas para las interfaces.	“SPARC: Cómo asegurarse de que la dirección MAC de cada interfaz sea única” en la página 20
Determinar qué NCP está activo en el sistema.	Muestra el NCP activo del sistema y activa <code>DefaultFixed</code> .	“Cómo cambiar el NCP activo en el sistema” en la página 21
Realizar la configuración de interfaz IP básica utilizando el comando <code>ipadm</code> .	Crea una interfaz IP y asigna direcciones IP válidas, estáticas o DHCP, a la interfaz.	“Cómo configurar una interfaz IP” en la página 22
Personalizar enlaces de datos.	Personalizar más los enlaces de datos estableciendo propiedades de enlace.	“Personalización de propiedades de enlaces de datos” en la página 32
Personalizar interfaces IP.	Personaliza más las interfaces IP mediante el establecimiento de propiedades de interfaz.	“Configuración de las propiedades de la interfaz IP” en la página 45

Tarea	Descripción	Para obtener instrucciones
Personalizar direcciones IP.	Personaliza más las direcciones IP mediante el establecimiento de propiedades de dirección.	“Configuración de las propiedades de las direcciones IP” en la página 47
Personalizar protocolos.	Personaliza más los protocolos mediante el establecimiento de propiedades de protocolo.	“Establecimiento de propiedades de protocolo TCP/IP” en la página 48
Configurar una red inalámbrica.	Conectar un equipo portátil a la red mediante redes inalámbricas.	Capítulo 5, “Configuración de redes inalámbricas en equipos portátiles que ejecutan Oracle Solaris”

▼ 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), 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. El siguiente procedimiento muestra cómo utilizar el comando `eeprom` para comprobar el valor actual de `local-mac-address?` y cambiarlo, si es preciso.

1 Conviértase en un administrador.

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

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

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

En el ejemplo, la respuesta al comando `eeprom, local-mac-address?=false`, indica que todas las interfaces utilizan la dirección MAC del sistema. El valor de `local-mac-address?=false` debe cambiarse a `local-mac-address?=true` para que las interfaces puedan pasar a ser miembros de un grupo IPMP. También debe realizar este cambio para las adiciones de enlaces.

3 Si es preciso, cambie el valor de `local-mac-address?`, tal como se indica:

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

Al reiniciar el sistema en el Paso 6, 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 las 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          DEFAULT           POSSIBLE
net0   mac-address    rw   8:0:20:0:0:1      8:0:20:0:0:1     --
net1   mac-address    rw   8:0:20:0:0:1      8:0:20:0:0:1     --
net3   mac-address    rw   0:14:4f:45:c:2d   0:14:4f:45:c:2d  --
```

Nota – Continúe con el paso siguiente sólo si hay dos o más interfaces de red con la misma dirección MAC. De lo contrario, continúe con el último paso.

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

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

En el ejemplo del paso 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
```

Consulte la página del comando `man dladm(1M)` para obtener más información sobre este comando.

6 Reinicie el sistema.

▼ Cómo cambiar el NCP activo en el sistema

El tipo de NCP activado en el sistema determina si la configuración de red del sistema es reactiva o fija. Un sistema con configuración reactiva no se comporta de la misma manera que un sistema con configuración de red fija. Todos los procedimientos de este manual crean configuraciones persistentes que se aplican al NCP activo. Por lo tanto, antes de realizar cualquier procedimiento, debe saber qué NCP está activo para aplicar la configuración al perfil correcto. De esta manera, la configuración de red del sistema se comporta de la forma esperada una vez completados los procedimientos.

1 Visualice los perfiles del sistema.

```
# netadm list
TYPE          PROFILE      STATE
ncp           DefaultFixed online
ncp           Automatic    disabled
loc           Automatic    offline
loc           NoNet        offline
loc           User         offline
loc           DefaultFixed online
```

El perfil cuyo estado aparece como en línea (online) es el NCP activo del sistema.

Para obtener información más detallada sobre el NCP en el sistema, utilice la opción `-x` con el comando `netadm`.

```
netadm list -x
TYPE          PROFILE      STATE          AUXILIARY STATE
ncp           DefaultFixed online          active
ncp           Automatic    disabled       disabled by administrator
loc           Automatic    offline        conditions for activation are unmet
loc           NoNet        offline        conditions for activation are unmet
loc           User         offline        conditions for activation are unmet
loc           DefaultFixed online          active
```

2 Para cambiar entre los tipos de perfiles, por ejemplo, de un perfil reactivo a un perfil fijo, escriba el siguiente comando:

```
# netadm enable -p ncp NCP-name
```

donde *NCP-name* es el nombre de un tipo de NCP.

Por ejemplo, suponga que la configuración de red del sistema es reactiva. Si desea que las configuraciones creadas mediante los procedimientos descritos en este manual se apliquen al NCP `DefaultFixed`, debe escribir lo siguiente:

```
# netadm enable -p ncp defaultfixed
```



Precaución – Al alternar perfiles activos, la configuración de red existente se elimina y una nueva configuración se crea. Cualquier configuración persistente que se haya implementado en un NCP que haya estado activo anteriormente se excluye del nuevo NCP activo.

▼ Cómo configurar una interfaz IP

El procedimiento siguiente brinda los pasos básicos que debe utilizar para configurar la interfaz IP de un sistema.

Antes de empezar

Compruebe qué NCP está activo en el sistema para asegurarse de estar aplicando la configuración al perfil correcto.

1 Conviértase en un administrador.

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

2 Cree la 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 más común que podrá crear al efectuar la configuración de red. Para crear esta clase de interfaz, utilice el subcomando `create-ip`.
- Controlador de interfaz de red virtual (VNI, Virtual Network Interface) STREAMS. Para crear esta clase de interfaz, utilice el subcomando `create-vni`. Para obtener más información sobre dispositivos o interfaces VNI, consulte la página del comando `man vni(7d)`.
- Interfaz IPMP. Esta interfaz se utiliza cuando se configuran los grupos IPMP. Para crear esta clase de interfaz, utilice el subcomando `create-ipmp`. Para obtener más información sobre los grupos IPMP, consulte el [Capítulo 5, “Introducción a IPMP” de Gestión del rendimiento de red de Oracle Solaris 11.1](#).

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 conocer los enlaces de datos del sistema, utilice el comando `dladm show-link`.

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

- Para configurar una dirección estática, escriba lo siguiente:

```
# 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 sobre las direcciones local y remota, y sobre la configuración de túneles, consulte el [Capítulo 6, “Configuración de túneles IP” de Configuración y administración de redes Oracle Solaris 11.1](#).

Para una dirección IP numérica, utilice la notación CIDR. Si no utiliza la notación CIDR, la máscara de red se calcula según la

secuencia que se muestra para netmask en el servicio name-service/switch o mediante el uso de semántica de direcciones con clase.

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, la creación de direcciones IP precede a los servicios de nombres que se ponen 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 está identificada por el objeto de dirección correspondiente y está representada en el comando por *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 crear el nombre de objeto de dirección automáticamente, especifique el nombre de interfaz para *interface*. De lo contrario, proporcione el nombre de 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. Varias direcciones de la misma interfaz tienen letras del alfabeto anexadas a los nombres de objeto de dirección, como, `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 como `net0/static`, `net0/static1`, `net1/private`, etc.

- Para configurar una dirección no estática, escriba lo siguiente:

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

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

Para obtener una explicación más completa de *[interface | addrobj]*, consulte la descripción anterior para crear direcciones estáticas.

4 (Opcional) Visualice la información de la interfaz IP recientemente configurada.

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

```
# ipadm [interface]
```

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

Para obtener más información sobre la salida del subcomando `ipadm show - *`, consulte [“Supervisión de direcciones e interfaces IP” en la página 55](#).

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 Definen 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 las páginas del comando `man route(1M)` y `routeadm(1M)`. Consulte también [“Tablas y tipos de enrutamiento” de Configuración y administración de redes Oracle Solaris 11.1](#).

Ejemplo 2-1 Configuración de una interfaz de red con una dirección IP estática

En este ejemplo se explica cómo configurar una interfaz con una dirección IP estática. El ejemplo comienza con la activación del NCP `DefaultFixed` en el sistema para poder utilizar los comandos `dladm` y `ipadm` para la configuración de red fija.

```
# 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      BRIDGE      OVER
net3      phys       1500    up         --         --

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

# ipadm
NAME      CLASS/TYPE  STATE    UNDER    ADDR
lo0       loopback   ok       --        --
  lo0/v4   static     ok       --        127.0.0.1/8
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   campus01

# route -p add default 192.168.84.1
# netstat -r
Routing Table: IPv4
  Destination          Gateway             Flags Ref    Use    Interface
-----
default                some.machine.com   UG      2     10466
192.168.84.0          192.168.84.3      U        3     1810 net3
localhost             localhost          UH      2      12    lo0

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

```

Tenga en cuenta que si `campus01` ya está definido en el archivo `/etc/hosts`, puede usar ese nombre de host al asignar la siguiente dirección:

```

# ipadm create-addr -a campus01 net3
ipadm: net3/v4

```

Ejemplo 2-2 Configuración automática de una interfaz de red con una dirección IP

En este ejemplo, la interfaz IP se ha configurado para recibir su dirección de un servidor DHCP.

```

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

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

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

```

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

Otras tareas de administración y configuración de redes

En este manual se describe la configuración de red básica que permite conectar su sistema a la red. Concretamente, la información se centra en la configuración de los enlaces de datos y las interfaces del sistema. Se puedan realizar otras tareas de administración y configuración que se describen en otros manuales de redes. Suponiendo que su sistema está configurado para una configuración de red fija, puede consultar los siguientes manuales para estas otras tareas:

- Para configurar los sistemas como enrutadores, los servidores de configuración de red, etc., consulte [Configuración y administración de redes Oracle Solaris 11.1](#).
- Para realizar la configuración avanzada de enlace de datos e interfaz IP, consulte [Gestión del rendimiento de red de Oracle Solaris 11.1](#).
- Para aprovechar la configuración básica y mejorar el rendimiento de la red, por ejemplo, mediante la configuración de agregaciones de enlaces, grupos IPMP, etc., consulte [Gestión del rendimiento de red de Oracle Solaris 11.1](#).
- Para establecer la seguridad de la red, consulte [Protección de la red en Oracle Solaris 11.1](#).
- Para implementar la virtualización de redes, consulte [Uso de redes virtuales en Oracle Solaris 11.1](#).

Otros manuales especializados en áreas de red específicas, como DHCP, servicios de nombres, etc., también están disponibles en la biblioteca.

Cómo trabajar con enlaces de datos

En este capítulo se trata el comando `dladm` y se explica cómo utilizarlo en enlaces de datos para mostrar su configuración actual, cambiar los valores predeterminados de sus propiedades o suprimir enlaces de datos del sistema. Se explican los siguientes temas:

- “Comandos `dladm` básicos” en la página 29
- “Personalización de propiedades de enlaces de datos” en la página 32
- “Otras tareas de configuración con el comando `dladm`” en la página 38

Comandos `dladm` básicos

En esta sección se describen los comandos `dladm` básicos que puede usar con regularidad en enlaces de datos del sistema. Se admiten otros subcomandos `dladm` aparte de los mencionados en esta sección. Para obtener información sobre otros subcomandos, consulte la página del comando `man dladm(1M)`.

Nota – Excepto los subcomandos `dladm` que muestran información de enlace de datos, todos los demás subcomandos requieren la eliminación previa de cualquier configuración de interfaz existente por medio del enlace de datos. Para eliminar la configuración de la interfaz IP, consulte “Eliminación de una configuración de interfaz IP (`ipadm delete-ip`)” en la página 43.

Visualización de información general sobre enlaces de datos (`dladm`)

Si se usa solo, el comando `dladm` muestra información general sobre los enlaces de datos del sistema, incluidos 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 de datos pueden ser de distintas clases aparte de enlaces físicos, como agregaciones de enlaces, LAN virtuales (VLAN) o NIC virtual (VNIC). Estos otros enlaces de datos también se incluyen en la información predeterminada que muestra el comando `dladm`. Por ejemplo, en la salida se muestra una agregación de enlace `aggr0` configurada mediante los enlaces de datos físicos `net1` y `net4`.

Para obtener información sobre las agregaciones de enlaces y las VLAN, consulte [Gestión del rendimiento de red de Oracle Solaris 11.1](#). Para obtener información sobre las VNIC, consulte [Uso de redes virtuales en Oracle Solaris 11.1](#).

Visualización de los enlaces de datos de un sistema (`dladm show-link`)

Utilice el comando `dladm show-link` para visualizar los enlaces de datos de un sistema. Un sistema tiene la misma cantidad de enlaces de datos que de NIC instaladas. Se pueden utilizar opciones con este comando para personalizar la información que se obtiene. Por ejemplo, si se utiliza la opción `-P`, se incluye 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 se ejecuta el comando, se visualiza información similar a la siguiente:

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

En este ejemplo 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 atributos físicos de enlaces de datos (`dladm show-phys`)

Utilice el comando `dladm show-phys` para obtener información 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 siguiente:

```
# 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 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.

Otra opción útil para el comando es `-L`, que 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
```

Supresión de un enlace de datos (`dladm delete-phys`)

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, se elimina una NIC física del sistema. La configuración del enlace de datos asociada a esa NIC permanece porque la capa de software ya no estará vinculada a la capa de hardware, como se describe en [“Pila de red en Oracle Solaris” de Introducción a redes de Oracle Solaris 11](#). 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
```

Consejo – Para confirmar si se ha eliminado la NIC de un enlace de datos, utilice el comando `dladm show-phys -P`.

Cambio de nombre de un enlace de datos (`dladm rename-link`)

Utilice el comando `dladm rename-link` para cambiar el nombre de un enlace de datos. En un sistema Oracle Solaris 11, el sistema operativo asigna automáticamente nombres genéricos a todos los enlaces de datos. Los nombres de enlace de datos genéricos se describen en “[Nombres de enlaces genéricos predeterminados](#)” de *Introducción a redes de Oracle Solaris 11*.

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 los nombres, cambiar el nombre de los enlaces de datos no formará parte de sus tareas administrativas regulares. Para obtener información sobre el procedimiento para cambiar nombres de enlace, consulte “[Cómo cambiar interfaces principales en un sistema](#)” en la [página 38](#).

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.

Para las propiedades de enlaces de datos se utilizan tres subcomandos `dladm`:

- `dladm show-linkprop [-p property] [datalink]` muestra las propiedades de un enlace de datos y sus valores actuales. Si no utiliza la opción `-p property`, se muestran todas las propiedades de un 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 la propiedad del enlace de datos.
- `dladm reset-linkprop -p property datalink` restablece el valor predeterminado de la propiedad en cuestión.

Descripción general de las propiedades de enlaces de datos

Las propiedades de enlaces de datos que se pueden 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* que 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* que 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.

En general, las propiedades de enlaces 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. En las siguientes secciones se describen las propiedades seleccionadas y se explica cómo cambiar sus valores para que funcionen correctamente en su entorno de red.

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.

Para cambiar el valor predeterminado del tamaño de MTU, escriba el siguiente comando:

```
# 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 muestran los pasos para activar la admisión de 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  VALUE    DEFAULT  POSSIBLE
net1      mtu       1500    1500    --
# dladm set-linkprop -p mtu=9000 net1
# dladm show-link web1
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, debería escribir lo siguiente 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
```

El comando desactiva el anuncio de las capacidades gigabit del sistema para la capacidad de dúplex completo y la capacidad de dúplex medio.

Para mostrar los nuevos valores de estas propiedades, use el comando `dladm show-linkprop`.

```
# 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`.

También se puede utilizar otro comando `autopush` para insertar módulos en el flujo del enlace de datos por controlador. El 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, para este fin es preferible el comando `dladm` 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 `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, para insertar los módulos `vpnmod` y `bufmod` sobre el enlace `net0`, debería escribir:

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

Establecimiento del controlador e1000g para usar el enlace de acceso directo a memoria

En esta sección y la siguiente se muestra cómo configurar las propiedades privadas. Las dos secciones se aplican a propiedades específicas del controlador `e1000g`. Sin embargo, la información general de estas secciones se aplica al configurar las propiedades privadas de otros controladores NIC.

El tráfico en masa, como las transferencias de archivos, normalmente implica una negociación de grandes paquetes en la red. En tales casos, puede obtener un mejor rendimiento del controlador `e1000g` configurándolo para que use automáticamente el enlace DMA, donde se define un umbral para tamaños de fragmentos de paquetes. Si un tamaño de fragmento supera el umbral, el enlace DMA se usa para transmitir los paquetes. Si un tamaño de fragmento está dentro del umbral, se usa el modo `bcopy`, donde los datos del fragmento se copian en la memoria intermedia de transmisión preasignada.

```
# dladm set-linkprop -p _tx_bcopy_threshold=value datalink
```

Para esta propiedad, los valores válidos para el umbral van de 60 a 2.048.

Nota – A todos los enlaces de datos se les asigna automáticamente un nombre genérico. Debe asegurarse de que esta propiedad privada esté configurada en el enlace de datos cuya NIC subyacente es e1000g. Utilice el comando `dladm show-phys` para verificar esto antes de establecer la propiedad.

De la misma manera que para la configuración de las propiedades públicas, para modificar los valores de las propiedades privadas también se debe suprimir la interfaz IP.

Es posible que deba realizar un procedimiento como el siguiente:

```
# dladm show-phys
LINK  MEDIA      STATE  SPEED  DUPLEX  DEVICE
net0  Ethernet   up     100Mb  full    nge0
net1  Ethernet   up     100Mb  full    e1000g0

# dladm set-linkprop -p _tx_bcopy_threshold=1024 net1
```

Establecimiento manual de la frecuencia de interrupción

Las propiedades que regulan la frecuencia con la que el controlador e1000g genera interrupciones también afectan el rendimiento del sistema y la red. Normalmente, los paquetes de red se envían a la capa superior de la pila mediante la generación de una interrupción para cada paquete. A su vez, la frecuencia de interrupción, de manera predeterminada, es ajustada automáticamente por la capa GLD en el núcleo. Sin embargo, es posible que este modo no se desee en todas las condiciones de tráfico de red. Para ver una explicación de este problema, consulte este documento (<http://www.stanford.edu/class/cs240/readings/mogul.pdf>), que fue presentado en la conferencia técnica USENIX, en 1996. Por lo tanto, en determinadas circunstancias, la configuración manual de la frecuencia de interrupciones se vuelve necesaria para obtener un mejor rendimiento.

Para definir la frecuencia de interrupciones, establezca las siguientes propiedades:

- `_intr_throttling_rate` determina el retraso entre aserciones de interrupciones, independientemente de las condiciones de tráfico de red.
- `_intr_adaptive` determina si el ajuste automático de la frecuencia de límite de interrupciones está activado. De manera predeterminada, esta propiedad está activada.

Primero, debe desactivar el ajuste automático de la frecuencia de límite de interrupciones. A continuación, debe establecer manualmente la propiedad de frecuencia de límite de interrupciones.

Supongamos que tiene un sistema basado en x86 y una NIC e1000g cuya frecuencia de límite de interrupciones se debe modificar. Supongamos, además, que el nombre de enlace de datos de e1000g0 es net1. Debería escribir los comandos siguientes:

```
# dladm set-linkprop -p _intr_adaptive=0 net1
# dladm set-linkprop -p _intr-throttling_rate=1024 net1
```

Obtención de información de estado de 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 propiedades de enlaces de datos (dladm show-linkprop)

Este método se explica en “[Personalización de propiedades de enlaces de datos](#)” en la página 32. Para mostrar una lista completa de las propiedades de enlaces de datos, escriba el comando sin especificar una propiedad. Por ejemplo:

```
# dladm show-linkprop net1
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net1      speed         1000      --           --
net1      autopush     --        --           --
net1      zone         --        --           --
net1      duplex       half      --           half,full
net1      state        unknown   up           up,down
net1      adv_autoneg_cap 1         1           1,0
net1      mtu          1500     1500        --
net1      flowctrl     no        bi           no,tx,rx,bi
net1      adv_1000fdx_cap 1         1           1,0
net1      en_1000fdx_cap 1         1           1,0
net1      adv_1000hdx_cap 1         1           1,0
net1      en_1000hdx_cap 1         1           1,0
net1      adv_100fdx_cap 0         0           1,0
net1      en_100fdx_cap 0         0           1,0
net1      adv_100hdx_cap 0         0           1,0
net1      en_100hdx_cap 0         0           1,0
net1      adv_10fdx_cap 0         0           1,0
net1      en_10fdx_cap 0         0           1,0
net1      adv_10hdx_cap 0         0           1,0
net1      en_10hdx_cap 0         0           1,0
```

Visualización de valores de propiedad de Ethernet (dladm show-ether)

Si no se utilizan opciones con el comando `dladm show-ether`, solamente se muestran los valores de propiedad de Ethernet actuales del enlace de datos. Para obtener más información

aparte de lo que se ofrece de manera predeterminada, utilice la opción `-x`. A continuación se muestra un ejemplo de cómo se utiliza el comando:

```
# 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. A continuación se explica la información que se muestra en el ejemplo anterior:

- 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 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.

Otras tareas de configuración con el comando dladm

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

▼ Cómo cambiar interfaces principales en un sistema

El cambio de la interfaz principal de un sistema consiste en cambiar el nombre de los enlaces de datos. El siguiente procedimiento se basa en la siguiente configuración del sistema:

- El sistema tiene dos enlaces de datos: `net0` y `net1`.

- Las NIC subyacentes son e1000g0 y nge0, respectivamente.
- Se configura una interfaz IP mediante net0. La interfaz IP siempre toma el nombre del enlace de datos subyacente.

La interfaz principal del sistema es net0 según su número de instancia cero (0). La interfaz principal se configura mediante e1000g0. Los siguientes pasos guiarán al usuario para convertir la configuración de enlace de datos mediante nge0 en la configuración de la interfaz principal.

1 Conviértase en un administrador.

Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” de Administración de Oracle Solaris 11.1: servicios de seguridad](#).

2 Muestre los atributos físicos de los enlaces de datos del sistema.

```
# dladm show-phys
```

3 Suprima la interfaz IP principal.

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

Nota – Para obtener más información sobre el comando ipadm, consulte [Capítulo 4, “Trabajo con interfaces IP”](#) y la página del comando man [ipadm\(1M\)](#).

4 Reemplace el nombre del enlace principal por un nombre que no esté utilizado por otros enlaces de datos del sistema.

```
# dladm rename-link primary-link unused-name
```

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
```

Ejemplo 3-1 Cambio de la interfaz principal

En el siguiente ejemplo se combinan todos los pasos del procedimiento para cambiar la interfaz principal del sistema. Al final del ejemplo, la interfaz principal configurada mediante e1000g0 se reemplaza por la interfaz configurada mediante nge0. Una vez que haya cambiado el enlace principal a otra NIC, podrá configurar una interfaz mediante el enlace de datos de la NIC nueva.

```
# dladm show-phys
LINK  MEDIA   STATE  SPEED  DUPLEX  DEVICE
net0  Ethernet up     100Mb  full   e1000g0
net1  Ethernet up     100Mb  full   nge0

# ipadm delete-ip net0
# dladm rename-link net0 oldnet0
# dladm rename-link net1 net0
```

```
# ipadm create-ip net0
# ipadm create-addr -a 192.168.10.10/24 net0
ipadm: net0/v4

# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX     DEVICE
oldnet0   Ethernet   up         1000      full      e1000g0
net0      Ethernet   up         1000      full      nge0
```

▼ 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. En Oracle Solaris 11 ya no es necesario volver a configurar los enlaces de red una vez finalizada la reconfiguración dinámica. En cambio, simplemente se transfieren las configuraciones de enlaces de la NIC eliminada a la NIC de sustitución.

El procedimiento no detalla los pasos para realizar la reconfiguración dinámica. Consulte la documentación del sistema para ver estos pasos.

Para ver una introducción a la reconfiguración dinámica, consulte el [Capítulo 4, “Configuración dinámica de dispositivos \(tareas\)”](#) de *Administración de Oracle Solaris 11.1: dispositivos y sistemas de archivos*.

Antes de empezar Los procedimientos para realizar la DR varían con el tipo de sistema. Asegúrese de completar primero lo siguiente:

- 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.

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

2 (Opcional) Visualice información sobre 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 `dladm show-phys -L`, consulte la página del comando `man dladm(1M)`.

3 Lleve a cabo la reconfiguración dinámica como se describe en la documentación del sistema.

Consulte la documentación sobre la DR del sistema para realizar este paso.

Después de instalar la NIC de sustitución, continúe con el siguiente paso.

4 Realice uno de los pasos siguientes en función de la circunstancia que se aplique:

- Si ha insertado la NIC de sustitución en la misma ranura que la NIC anterior, vaya al paso 5. Si la NIC nueva se coloca en la misma ubicación que ocupaba la NIC anterior, la NIC nueva hereda el nombre del enlace y la configuración de la NIC anterior.
- Si ha insertado la NIC de sustitución en una ranura distinta, y la NIC nueva necesita heredar la configuración de enlace de datos de la NIC eliminada, escriba:

```
# 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 distinta 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 ha eliminado.

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 ha eliminado 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`. Para que el enlace de datos de la NIC nueva herede la configuración de enlace de datos de la NIC anterior, escriba:

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

5 Complete el proceso de DR mediante la activación de los recursos de la nueva NIC para que Oracle Solaris la pueda utilizar.

Por ejemplo, puede utilizar 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 `dladm show-phys` o `dladm show-link` para visualizar información sobre los enlaces de datos.

Ejemplo 3-2 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 sustituye por una tarjeta e1000g. Una vez que se conecta e1000g al sistema, la configuración de enlace de net0 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
```

El administrador realiza los pasos específicos de reconfiguración dinámica, como usar c f gadm para eliminar bge y, después, instalar 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 las configuraciones de enlaces.

```
# 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    ---
```

◆ ◆ ◆ 4

CAPÍTULO 4

Trabajo con interfaces IP

En este capítulo se trata el comando `ipadm` y se explica cómo se utiliza este comando en interfaces IP. Para obtener una descripción general del comando `ipadm` y sus beneficios, consulte “Comando `ipadm`” en la página 16.

Se explican los siguientes temas:

- “Comandos `ipadm` básicos” en la página 43
- “Configuración de las propiedades de la interfaz IP” en la página 45
- “Configuración de las propiedades de las direcciones IP” en la página 47
- “Establecimiento de propiedades de protocolo TCP/IP” en la página 48
- “Supervisión de direcciones e interfaces IP” en la página 55

Comandos `ipadm` básicos

En “Cómo configurar una interfaz IP” en la página 22, se presentaron los tres subcomandos `ipadm` principales:

- `ipadm`
- `ipadm create-ip`
- `ipadm create-addr`

En esta sección se describen otros usos seleccionados del comando `ipadm` en las interfaces IP. La lista no es exhaustiva. Para obtener una descripción completa del comando `ipadm` y todos los posibles subcomandos y opciones, consulte la página del comando `man ipadm(1M)`.

Eliminación de una configuración de interfaz IP (`ipadm delete-ip`)

Utilice este comando para eliminar una interfaz IP configurada mediante un enlace de datos. Este comando es especialmente importante para llevar a cabo ciertas configuraciones 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 cambiar el nombre del enlace de datos, debe ejecutar el comando `ipadm delete-ip`.

En general, este comando se utiliza junto con otros subcomandos `ipadm` y `dladm`, por ejemplo, para cambiar la interfaz principal del sistema. Para realizar esta tarea, sería necesario suprimir la interfaz, cambiar el nombre del enlace y, a continuación, volver a configurar la interfaz mediante el enlace de datos con nuevo nombre. La secuencia es la siguiente:

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

Consulte el ejemplo para cambiar la interfaz principal en “[Cambio de nombre de un enlace de datos \(dladm rename-link\)](#)” en la [página 32](#). Para volver a configurar una interfaz IP después de haber cambiado el nombre del enlace de datos, consulte “[Cómo configurar una interfaz IP](#)” en la [página 22](#).

Desactivación de una configuración de interfaz IP (`ipadm disable-ip`)

De manera predeterminada, una interfaz IP se marca con el indicador UP y se convierte en parte de la configuración activa cuando la interfaz se crea con `ipadm create-ip`. Puede eliminar la interfaz de la configuración activa sin destruir la configuración mediante el subcomando `ipadm disable-ip`. Este comando marca la interfaz específica con el indicador DOWN.

```
# ipadm disable-ip interface
```

Para que la interfaz IP funcione y su indicador sea UP, escriba:

```
# ipadm enable-ip interface
```

Consejo – Para visualizar el estado de las interfaces, utilice `ipadm`. Consulte “[Obtención de información sobre interfaces IP](#)” en la [página 56](#).”

Eliminación de la dirección de una interfaz (`ipadm delete-addr`)

Este comando suprime una configuración de dirección específica de una interfaz IP. Este comando es útil cuando se desea cambiar la dirección IP de una interfaz específica. Antes de asignar una configuración de dirección nueva, debe eliminar la configuración de dirección original. Debe realizar los siguientes pasos generales:

```
# ipadm delete-addr addrobj
# ipadm create-addr parameters
```

Para obtener un ejemplo de cómo crear una dirección IP para una interfaz, consulte [“Cómo configurar una interfaz IP” en la página 22](#).

Nota – Una interfaz puede tener varias direcciones. Cada dirección se identifica mediante un objeto de dirección. Para asegurarse de eliminar la dirección correcta, debe conocer el objeto de dirección. Utilice el subcomando `ipadm show-addr` para mostrar las direcciones de interfaz del sistema. Para obtener una explicación del objeto de dirección, consulte [“Cómo configurar una interfaz IP” en la página 22](#). Para obtener más información sobre la visualización de direcciones, consulte [“Obtención de información sobre direcciones IP” en la página 58](#).

Configuración de las propiedades de la interfaz IP

En esta sección se explica cómo utilizar el comando `ipadm` para establecer propiedades de la interfaz IP seleccionada.

Las interfaces IP, al igual que los enlaces de datos, 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. Algunas propiedades, como 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.

Para establecer propiedades de interfaz IP se utilizan tres subcomandos `ipadm`:

- El subcomando `ipadm 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.
- El subcomando `ipadm set-ifprop -p property =value interface` asigna un valor a la propiedad de la interfaz IP.
- El subcomando `ipadm reset-ifprop -p property interface` restablece los valores predeterminados de la propiedad específica.

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. De manera predeterminada, el reenvío de IP está desactivado.

El reenvío de paquetes se gestiona mediante una propiedad que se puede establecer en ambas interfaces IP y en el protocolo TCP/IP. Si desea elegir el modo en que se reenvían los paquetes, active el reenvío de paquetes en la interfaz IP. Por ejemplo, puede tener un sistema con varias NIC. Algunas NIC pueden estar conectadas a la red externa, mientras que otras NIC pueden estar conectadas a la 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” en la página 49](#).

Nota – La propiedad `forwarding` de protocolos o interfaces IP no es exclusiva. 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.

Para activar el reenvío de paquetes en la interfaz IP, utilice el siguiente comando:

```
# ipadm set-ifprop 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.

A continuación se muestra un ejemplo de 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
...
```

Configuración de las propiedades de las direcciones IP

El comando `ipadm` le permite establecer propiedades específicas de direcciones IP una vez que estas direcciones se asignan a interfaces. Para configurar estas propiedades, puede determinar lo siguiente:

- La 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 se trabaja con las propiedades de direcciones IP, se utilizan los siguientes subcomandos `ipadm`:

- El subcomando `ipadm show-addrprop [-p property] [addrobj]` muestra las propiedades de las direcciones en función de las opciones que se utilizan.

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.

- El subcomando `ipadm set-addrprop -p property =value addrobj` asigna valores a propiedades de direcciones. Tenga en cuenta que sólo puede establecer una propiedad de dirección por vez.
- El subcomando `ipadm reset-addrprop -p property addrobj` restaura los valores predeterminados de 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 de la dirección de una interfaz \(`ipadm delete-addr`\)” en la página 44.](#)

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 comandos siguientes muestran cómo modificar 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
```

Establecimiento de propiedades de protocolo TCP/IP

Utilice el comando `ipadm` para configurar las propiedades de protocolo, también conocidas como *valores ajustables*. El comando `ipadm` reemplaza el comando `ndd`, que en las versiones anteriores generalmente se utilizaba para establecer valores ajustables.

Las propiedades TCP/IP pueden ser basadas en interfaz o globales. Las propiedades se pueden aplicar a una interfaz específica o globalmente a todas las interfaces de una zona. Las propiedades globales pueden tener diferentes valores en diferentes zonas no globales. Para obtener una lista con las propiedades de protocolo admitidas, consulte la página del comando `man ipadm(1M)`.

Normalmente, los valores predeterminados del protocolo de Internet TCP/IP son suficientes para que la red funcione. Sin embargo, si los valores predeterminados son insuficientes para su topología de red, puede personalizar estas propiedades según sea necesario.

Para establecer propiedades de interfaz TCP/IP se utilizan tres subcomandos `ipadm`:

- El comando `ipadm show-prop -p property protocol` muestra las propiedades de un protocolo y sus valores actuales. Si no utiliza la opción `-p property`, se muestran todas las propiedades del protocolo. Si no especifica un protocolo, se muestran todas las propiedades de todos los protocolos.
- El subcomando `ipadm set-prop -p property=value protocol` asigna un valor a la propiedad de la interfaz IP.
- El subcomando `ipadm reset-prop -p property protocol` restablece los valores predeterminados de la propiedad de protocolo específica.

Nota – Si una propiedad puede admitir varios valores, debe asignar varios valores a la propiedad con el cualificador `+=` de la siguiente manera:

```
ipadm set-prop -p property+=value1 [value2 value3 ...].
```

Para eliminar un valor de un conjunto de valores de una propiedad, utilice el cualificador `==` de la siguiente forma:

```
ipadm set-prop -p property==value2
```

Activación del reenvío de paquetes de forma global

En “[Activación de reenvío de paquetes](#)” en la [página 45](#) se muestra cómo activar el reenvío de paquetes en la interfaz. El establecimiento del reenvío de paquetes en la propiedad de interfaz IP le permite implementar esta función de manera selectiva. Puede activar esta propiedad sólo en interfaces específicas del sistema.

Si desea activar el reenvío de paquetes en todo el sistema independientemente del número de interfaces IP, debe utilizar la propiedad de protocolo: En los protocolos el nombre de propiedad es el mismo que en las interfaces IP: `forwarding`. Debe ejecutar el comando por separado para activar el reenvío de paquetes en los protocolos IPv4 e IPv6.

En el siguiente ejemplo se muestra cómo activar el reenvío de paquetes para todo el tráfico IPv4 e IPv6 del sistema:

```
# ipadm show-prop -p forwarding ip
PROTO  PROPERTY      PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4   forwarding    rw    off      --           off      on,off
ipv6   forwarding    rw    off      --           off      on,off
#
# ipadm set-prop -p forwarding=on ipv4
# ipadm set-prop -p forwarding=on ipv6
#
# ipadm show-prop ip
PROTO  PROPERTY      PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4   forwarding    rw    on       on          off      on,off
ipv4   ttl           rw    255     --          255     1-255
ipv6   forwarding    rw    on       on          off      on,off
ipv6   hoplimit     rw    255     --          255     1-255#
```

Nota – La propiedad `forwarding` de protocolos o interfaces IP no es exclusiva. 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.

Configuración de un puerto con privilegios

En los protocolos de transporte como TCP, UDP y SCTP, los puertos 1–1023 son puertos con privilegios predeterminados a los que sólo se pueden vincular los procesos que se ejecutan con permisos de usuario `root`. Mediante el uso del comando `ipadm`, puede reservar un puerto fuera de este rango predeterminado de modo que se convierta en un puerto con privilegios. Por lo tanto, sólo los procesos `root` pueden vincularse a ese puerto. Para configurar un puerto con privilegios, debe personalizar las siguientes propiedades de protocolo de transporte:

- `smallest_nonpriv_port`: la propiedad cuyo valor indica el rango de números de puerto a los que los usuarios comunes se pueden vincular. Si el puerto designado está dentro de este rango, entonces puede configurarse como un puerto con privilegios. Utilice el comando `ipadm show-prop` para mostrar los valores de la propiedad.
- `extra_priv_ports`: la propiedad que especifica qué puertos tienen privilegios. Utilice el subcomando `ipadm set-prop` para especificar los puertos que desee restringir. A esta propiedad se le pueden asignar varios valores.

Por ejemplo, suponga que desea establecer los puertos TCP 3001 y 3050 como puertos con privilegios con acceso restringido sólo al usuario root. La propiedad `smallest_nonpriv_port` indica que 1024 es el número de puerto más bajo para un puerto sin privilegios. Por lo tanto, los puertos designados 3001 y 3050 se pueden cambiar para convertirse en puertos con privilegios. A continuación, deberá ejecutar comandos similares a los siguientes:

```
# ipadm show-prop -p smallest_nonpriv_port tcp
PROTO PROPERTY          PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp  smallest_nonpriv_port  rw    1024    --         1024    1024-32768

# ipadm show-prop -p extra_priv_ports tcp
PROTO PROPERTY          PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp  extra_priv_ports      rw    2049,4045  --         2049,4045  1-65535

# ipadm set-prop -p extra_priv_ports+=3001 tcp
# ipadm set-prop -p extra_priv_ports+=3050 tcp
# ipadm show-prop -p extra_priv_ports tcp
PROTO PROPERTY          PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp  extra_priv_ports      rw    2049,4045  3001,3050  2049,4045  1-65535
                                     3001,3050
```

Para que uno de los puertos, por ejemplo, 4045, deje de ser un puerto con privilegios, debe escribir los siguientes comandos:

```
# ipadm set-prop -p extra_priv_ports-=4045 tcp
# ipadm show-prop -p extra_priv_ports tcp
PROTO PROPERTY          PERM  CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp  extra_priv_ports      rw    2049,3001  3001,3050  2049,4045  1-65535
                                     3050
```

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.

En algunos casos, no resulta ideal repartir el tráfico de este modo. 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 una respuesta a una solicitud entrante determinada, como una solicitud de eco ICMP, la solicitud y la respuesta podrían no atravesar la misma interfaz. Esta configuración de enrutamiento de tráfico se denomina *enrutamiento asimétrico*. Si su proveedor de servicios de Internet está efectuando un filtrado de entrada como se describe en RFC 3704 (<http://rfc-editor.org/rfc/bcp/bcp84.txt>), la configuración de enrutamiento asimétrico puede hacer que el proveedor pierda un paquete saliente.

RFC 3704 tiene el propósito de limitar ataques de denegación de servicio en Internet. Para cumplir con este propósito, su red debe configurarse para el enrutamiento simétrico. En Oracle Solaris, la propiedad IP `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:

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

En el ejemplo siguiente se muestra cómo implementar el enrutamiento simétrico de paquetes IP en un host múltiple.

```
# ipadm set-prop -p hostmodel=strong ip
# 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
```

Implementación del control de congestión de tráfico

La congestión de la red generalmente se produce cuando hay desbordamientos de la memoria intermedia del enrutador, cuando los nodos envían más paquetes de los que la red puede recibir. Existen diversos algoritmos que evitan la congestión del tráfico mediante el establecimiento de controles en los sistemas de envío. Estos algoritmos se pueden usar en Oracle Solaris y se pueden agregar de forma sencilla o conectar directamente al sistema operativo.

En la siguiente tabla se muestran y describen los algoritmos admitidos.

Algoritmo	Nombre de Oracle Solaris	Descripción
NewReno	newreno	Algoritmo predeterminado en Oracle Solaris. El mecanismo de control incluye la elusión de la congestión, el retardo en el inicio y el intervalo de congestión del remitente.
HighSpeed	highspeed	Una de las modificaciones más sencillas y más conocidas de NewReno para redes de alta velocidad.
CUBIC	cubic	Actualmente, el algoritmo predeterminado en Linux 2.6. Cambia la fase de elusión de congestión del aumento de intervalo lineal a una función cúbica.
Vegas	vegas	Un algoritmo basado en retraso clásico que intenta predecir la congestión sin desencadenar la pérdida real de paquetes.

El control de congestión se activa mediante el establecimiento de las siguientes propiedades TCP relacionadas con el control. Aunque estas propiedades se muestran para TCP, el mecanismo de control que se activa mediante estas propiedades también se aplica al tráfico SCTP.

- `cong_enabled`: contiene una lista de algoritmos, separados por comas, que funcionan actualmente en el sistema. Puede agregar o eliminar algoritmos para activar sólo los algoritmos que desea utilizar. Esta propiedad puede tener varios valores. Por lo tanto, debe usar el cualificador `+=` o `-=`, según el cambio que desee realizar.
- `cong_default`: el algoritmo utilizado de manera predeterminada cuando las aplicaciones no especifican los algoritmos explícitamente en las opciones de socket. Actualmente, el valor de la propiedad `cong_default` se aplica a zonas globales y no globales.

Para agregar un algoritmo para el control de congestión al protocolo, ejecute el siguiente comando:

```
# ipadm set-prop -p cong_enabled+=algorithm tcp
```

Para eliminar un algoritmo, ejecute el siguiente comando:

```
# ipadm set-prop -p cong_enabled-=algorithm tcp
```

Para reemplazar el algoritmo predeterminado, ejecute el siguiente comando:

```
# ipadm set-prop -p cong_default=algorithm tcp
```

Nota – No se siguen reglas de secuencia para agregar o eliminar algoritmos. Puede eliminar un algoritmo antes de agregar otros algoritmos para una propiedad. Sin embargo, la propiedad `cong_default` siempre debe tener un algoritmo definido.

En el siguiente ejemplo se muestran los pasos que se pueden seguir para implementar el control de congestión. En el ejemplo, el algoritmo predeterminado para el protocolo TCP se cambia de `newreno` a `cubic`. A continuación, el algoritmo `vegas` se elimina de la lista de algoritmos activados.

```
# ipadm show-prop -p cong_default,cong_enabled tcp
```

PROTO	PROPERTY	PERM	CURRENT	PERSISTENT	DEFAULT	POSSIBLE
tcp	cong_default	rw	newreno	--	newreno	-
tcp	cong_enabled	rw	newreno,cubic, highspeed, vegas	--	newreno	newreno,cubic, highspeed,vegas

```
# ipadm set-prop -p cong_enabled-=vegas tcp
```

```
# ipadm set-prop -p cong_default=cubic tcp
```

```
# ipadm show-prop -p cong_default,cong_enabled tcp
```

PROTO	PROPERTY	PERM	CURRENT	PERSISTENT	DEFAULT	POSSIBLE
tcp	cong_default	rw	cubic	--	newreno	-
tcp	cong_enabled	rw	newreno,cubic, highspeed	--	newreno	newreno,cubic, highspeed,vegas

Cambio del tamaño de la memoria intermedia de recepción de TCP

El tamaño de la memoria intermedia de recepción TCP se establece mediante la propiedad `TCP recv_buf`, que de manera predeterminada es de 128 KB. Sin embargo, las aplicaciones que no utilizan los anchos de banda de manera uniforme. Por lo tanto, es posible que la latencia de conexión requiera el cambio del tamaño predeterminado. Por ejemplo, si se utiliza la función Secure Shell de Oracle Solaris se genera una sobrecarga en el uso del ancho de banda debido a los procesos de cifrado y suma de comprobación adicionales que se realizan en la secuencia de datos. Por lo tanto, es posible que sea necesario aumentar el tamaño de la memoria intermedia.

Del mismo modo, para que las aplicaciones que realizan retenciones de transferencia masiva usen el ancho de banda eficientemente, también es necesario el mismo ajuste de tamaño de memoria intermedia.

Puede calcular el tamaño de memoria intermedia de recepción correcto que se debe utilizar mediante el cálculo del *producto de retraso de ancho de banda* (BDP) de la siguiente manera:

$$BDP = available_bandwidth * connection-latency$$

Utilice `ping -s host` para obtener el valor de latencia de conexión. Utilice las herramientas `uperf` y `iperf` para calcular el uso del ancho de banda.

El tamaño de memoria intermedia de recepción adecuado se aproxima al valor del producto de retraso de ancho de banda. Sin embargo, tenga en cuenta que el uso del ancho de banda también depende de una serie de condiciones. Una infraestructura compartida o el número de aplicaciones y usuarios que compiten por el uso del ancho de banda pueden cambiar ese cálculo.

Para cambiar el valor del tamaño de la memoria intermedia, utilice la siguiente sintaxis:

```
# ipadm set-prop -p recv_buf=value tcp
```

En el siguiente ejemplo se muestra cómo aumentar el tamaño de la memoria intermedia a 164 KB.

```
# ipadm show-prop -p recv_buf tcp
PROTO PROPERTY  PERM CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp  recv_buf    rw  128000     --          128000    2048-1048576
```

```
# ipadm set-prop -p recv_buf=164000 tcp
```

```
# ipadm show-prop -p recv_buf tcp
PROTO PROPERTY  PERM CURRENT  PERSISTENT  DEFAULT  POSSIBLE
tcp  recv_buf    rw  164000     --          164000    2048-1048576
```

No se prefiere ningún valor establecido para el tamaño de la memoria intermedia, porque el tamaño preferido varía según las circunstancias. Tenga en cuenta los siguientes casos que muestran distintos valores para el BDP para cada red con sus propias condiciones específicas:

LAN típica de 1 Gbps, donde 128 KB es el valor predeterminado del tamaño de la memoria intermedia:

$$BDP = 128 \text{ MBps} * 0.001 \text{ s} = 128 \text{ kB}$$

WAN teórica de 1 Gbps con latencia de 100 ms:

$$BDP = 128 \text{ MBps} * 0.1 \text{ s} = 12.8 \text{ MB}$$

Enlace de Europa a Estados Unidos (ancho de banda medido por `uperf`):

$$BDP = 2.6 \text{ MBps} * 0.175 = 470 \text{ kB}$$

Si no puede calcular el BDP, utilice las siguientes observaciones como directrices:

- Para transferencias masivas mediante una LAN, el valor predeterminado del tamaño de la memoria intermedia, 128 KB, es suficiente.
- Para la mayoría de las implementaciones de WAN, el tamaño de la memoria intermedia de recepción debe estar dentro del rango de 2 MB.



Precaución – Aumentar el tamaño de la memoria intermedia de recepción de TCP aumenta el espacio de memoria de muchas aplicaciones de red.

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 subcomandos para restringir la información que desea mostrar mediante la siguiente sintaxis:

`ipadm show-* [other-arguments] [interface]`

- Para obtener sólo información de las interfaces, use `ipadm show-if`.
- Para obtener sólo información de las direcciones, use `ipadm show-addr`.
- Para obtener información sobre las propiedades de interfaz, use `ipadm show-ifprop`.
- Para obtener información sobre las propiedades de dirección, use `ipadm show-addrprop`.

En esta sección se proporcionan varios ejemplos de cómo utilizar los subcomandos `ipadm` para obtener la información de las interfaces. 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

Si se utiliza el comando `ipadm` sin subcomandos, se proporciona 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 de ejemplo proporciona la siguiente información:

- Las interfaces IP.
- La clase de cada interfaz.
- El estado de cada interfaz.
- El 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 asociados a 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.
- El 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`.

De esta manera, el comando `ipadm` proporciona una imagen completa de las interfaces del sistema.

Obtención de información sobre interfaces IP

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

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

<code>IFNAME</code>	Hace referencia a la interfaz cuya información se muestra.
<code>CLASS</code>	Hace referencia a la clase de interfaz, que puede ser una de cuatro: <ul style="list-style-type: none"> ▪ <code>ip</code> hace referencia a una interfaz IP. ▪ <code>ipmp</code> hace referencia a una interfaz IPMP. ▪ <code>vni</code> hace referencia a una interfaz virtual. ▪ <code>loopback</code> 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.
<code>STATE</code>	Hace referencia al estado de la interfaz, que puede ser uno de los siguientes: <code>ok</code> , <code>offline</code> , <code>failed</code> , <code>down</code> o <code>disabled</code> .

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 <code>yes</code> o <code>no</code> .
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 proporciona 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 proporciona 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 (?).

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

```
# 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 subcomando `ipadm show-addr` [*interface*]. Si no especifica una interfaz, se proporciona 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.
TIPO	Indica si la dirección IP es <code>static</code> , <code>dhcp</code> o <code>addrconf</code> . El valor <code>addrconf</code> 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 <code>man ipadm(1M)</code> .
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 más información sobre túneles, consulte el [Capítulo 6, “Configuración de túneles IP”](#) de *Configuración y administración de redes Oracle Solaris 11.1*.

A continuación se muestra un ejemplo de la información que proporciona el subcomando `ipadm 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 IP](#)” en la [página 22](#).

Obtención de información sobre las propiedades de direcciones IP

Para obtener información sobre propiedades de direcciones IP, utilice el subcomando `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 la 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 de la información que proporciona el subcomando `ipadm 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         --
```

Configuración de redes inalámbricas en equipos portátiles que ejecutan Oracle Solaris

Las especificaciones IEEE 802.11 definen las comunicaciones inalámbricas para las 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 incluye funciones para configurar servidores o puntos de acceso Wi-Fi.

Se tratan los temas siguientes:

- “Mapa de tareas de comunicaciones Wi-Fi” en la página 61
- “Comunicaciones seguras mediante Wi-Fi” en la página 67

Mapa de tareas de comunicaciones Wi-Fi

Tarea	Descripción	Para obtener instrucciones
Conectarse a una red Wi-Fi.	Configurar y establecer comunicaciones con una red Wi-Fi local.	“Cómo conectarse a una red Wi-Fi” en la página 62
Supervisar las comunicaciones en el enlace Wi-Fi.	Utilizar las herramientas de red estándar de Oracle Solaris para revisar el estado del enlace Wi-Fi.	“Cómo supervisar el enlace Wi-Fi” en la página 65

Tarea	Descripción	Para obtener instrucciones
Establecer comunicaciones Wi-Fi seguras.	Crear una clave de privacidad equivalente a cable (WEP, Wired Equivalent Privacy) y utilizarla para establecer conexiones con una red Wi-Fi segura.	“Cómo configurar una conexión de red Wi-Fi cifrada” en la página 67

▼ Cómo conectarse a una red Wi-Fi

Antes de empezar

Realice los siguientes pasos para conectar el equipo portátil a una red Wi-Fi.

1 Conviértase en un administrador.

Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” de Administración de Oracle Solaris 11.1: servicios de seguridad.](#)

2 Visualice los atributos físicos de enlaces de datos.

```
# dladm show-phys
LINK          MEDIA          STATE  SPEED  DUPLEX  DEVICE
net0          Ethernet      up     1500   full    ath0
net1          Ethernet      up     1500   full    e1000g0
```

En este ejemplo, la salida indica que hay dos enlaces disponibles. Net0 mediante el enlace ath0 de dispositivo admite comunicaciones Wi-Fi. El enlace e1000g0 sirve para conectar el sistema a una red inalámbrica.

3 Configure la interfaz Wi-Fi.

Efectúe los pasos siguientes para configurar la interfaz:

a. Cree una interfaz que admita Wi-Fi:

```
# 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 Verifique las 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
```

La salida de ejemplo del comando scan-wi-fi muestra información sobre las redes Wi-Fi disponibles en la ubicación actual. La información de la salida incluye lo 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, el identificador único para un ESSID determinado. 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. Los valores son none o WEP. Para obtener más información sobre WEP, consulte “Comunicaciones seguras mediante Wi-Fi” en la página 67.
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 pueden ser a, b o g, por separado o combinados.
SPEED	Hace referencia a la velocidad en megabits por segundo de la red específica.

5 Conéctese a una red Wi-Fi.

Realice una de las acciones siguientes:

- Conéctese a la 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
```

El subcomando `connect-wifi` de `dladm` tiene varias opciones más para conectarse a una red Wi-Fi. Para obtener información detallada, consulte la página del comando `man dladm(1M)`.

6 Configure la dirección IP para la interfaz.

Realice una de las siguientes acciones:

- Obtenga una dirección IP de un servidor DHCP.

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

Si la red Wi-Fi no admite DHCP, recibirá el siguiente mensaje:

```
ipadm: interface: interface does not exist or cannot be managed using DHCP
```

- Configure una dirección de IP estática:

Utilice esta opción si tiene una dirección IP dedicada para el sistema.

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

7 Compruebe el estado de la red Wi-Fi a la que está conectado el sistema.

```
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
net0      connected   ofc        none    very good g      36Mb
```

En este ejemplo, la salida indica que el sistema actualmente está conectado a la red ofc. La salida `scan-wifi` anterior del Paso 4 indicaba que ofc tenía la señal más fuerte entre las redes disponibles. El comando `dladm connect-wifi` selecciona de manera automática la red Wi-Fi con mejor señal, a menos que el usuario especifique directamente una red distinta.

8 Acceda a Internet mediante la red Wi-Fi.

Realice una de las siguientes tareas, según la red a la que el sistema está conectado:

- Si el punto de acceso ofrece servicio gratuito, ahora 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 actual. Por lo general, deberá ejecutar un explorador, introducir una clave y proporcionar información de su tarjeta de crédito al proveedor de redes.

9 Termine la sesión.

Realice una de las siguientes acciones:

- Termine la sesión Wi-Fi, pero deje el sistema en ejecución.
- Termine una sesión Wi-Fi en particular cuando se esté ejecutando más de una sesión.

```
# dladm disconnect-wifi
```

```
# 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 desactivar el sistema con el comando `shutdown`.

Ejemplo 5-1 Conexión con una red Wi-Fi determinada

En el ejemplo siguiente se combinan los diferentes pasos que debe realizar para conectar su equipo portátil con 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 este ejemplo se

supone que el usuario tiene la dirección IP estática 10.192.16.3/24 configurada en el equipo portátil. El ejemplo empieza con la determinación de la disponibilidad de un enlace Wi-Fi.

```
# 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
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

# 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

# dladm show-wifi
LINK      STATUS      ESSID          SEC    STRENGTH  MODE  SPEED
net0     connected   citinet        none   good      g     11Mb
```

Ejecute un explorador en otra aplicación para comenzar a trabajar en la red Wi-Fi.

```
# firefox
```

Aparece la página de inicio del explorador Firefox.

Termine la sesión, pero deje el equipo portátil 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

Este procedimiento muestra cómo supervisar el estado de un enlace Wi-Fi mediante herramientas de red estándar y cómo cambiar las propiedades del enlace seleccionado mediante el subcomando `linkprop`.

1 Conviértase en un administrador.

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

2 Conéctese a la red Wi-Fi, como se describe en “Cómo conectarse a una red Wi-Fi” en la página 62.

3 Vea las propiedades del enlace.

Use la sintaxis siguiente:

```
# dladm show-linkprop link
```

Por ejemplo, debe utilizar la siguiente sintaxis para mostrar el estado de la conexión establecida mediante el enlace inalámbrico net0:

```
# dladm show-linkprop net0
...
PROPERTY          VALUE          DEFAULT        POSSIBLE
channel            5              --             --
powermode          off            off            off,fast,max
radio              ?              on             on,off
speed              36            --             1,2,5.5,6,9,11,12,18,24,36,48,54
...
```

4 Defina una velocidad fija para el enlace.



Precaución – Oracle Solaris elige automáticamente la velocidad óptima para la conexión Wi-Fi. La modificación de la velocidad inicial del enlace puede generar una disminución del rendimiento o evitar que se establezcan determinadas conexiones Wi-Fi.

Puede modificar la velocidad del enlace con uno de los posibles valores de velocidad que aparece en la salida show-linkprop.

```
# dladm set-linkprop -p speed=value link
```

5 Compruebe el flujo de paquetes mediante el 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 5-2 Establecimiento de la velocidad de un enlace

Este ejemplo muestra cómo establecer la velocidad de un enlace después de establecer una conexión con una red Wi-Fi.

```
# dladm show-linkprop -p speed net0
PROPERTY      VALUE      DEFAULT      POSSIBLE
speed         24        --          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
PROPERTY      VALUE      DEFAULT      POSSIBLE
speed         36        --          1,2,5,6,9,11,12,18,24,36,48,54
```

Comunicaciones seguras mediante Wi-Fi

La tecnología de ondas de radio hace que las redes Wi-Fi estén disponibles fácilmente, y a menudo libremente, para los usuarios en muchos lugares. Por lo tanto, establecer la conexión con una red Wi-Fi puede resultar inseguro. Sin embargo, determinados tipos de conexiones Wi-Fi son más seguros, por ejemplo:

- La conexión a una red Wi-Fi privada de acceso restringido
 - Las redes privadas, como las redes internas, creadas por las empresas o las universidades, restringen el acceso a sus 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 VPN segura.
- El cifrado de la conexión con 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, Wired Equivalent Privacy) para cifrar conexiones mediante el punto de acceso. El protocolo WEP se define en las especificaciones IEEE 802.11 para conexiones inalámbricas. Para obtener los detalles completos de las opciones relacionadas con WEP del comando `dladm`, consulte la página del comando `man dladm(1M)`.

▼ Cómo configurar una conexión de red Wi-Fi cifrada

El siguiente procedimiento muestra 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 permite 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.

Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” de Administración de Oracle Solaris 11.1: servicios de seguridad](#).

2 Cree un objeto seguro que contenga la clave WEP.

Abra una ventana de terminal en el sistema y escriba lo siguiente:

```
# 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.

A continuación, el subcomando `create-secobj` ejecuta una secuencia de comandos que solicita el valor de 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 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
```

El valor `wep` del encabezado `SEC` indica que el cifrado WEP está ubicado para la conexión.

Ejemplo 5-3 Configuración de comunicaciones Wi-Fi cifradas

Para llevar a cabo lo que se muestra en este ejemplo, primero debe realizar lo siguiente:

- Conectar el sistema a un enrutador para el hogar que puede crear una clave WEP.
- 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.

Cree un objeto seguro.

```
# 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.

```
# dladm show-secobj
OBJECT          CLASS
mykey           wep
# dladm connect-wifi -e citinet -k mykey net0
```

El comando anterior establece una conexión cifrada a la red Wi-Fi `citinet` mediante el objeto seguro `mykey`.

```
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
net0     connected  citinet    wep      good      g     36Mb
```

Esta salida verifica que esté conectado a `citinet` mediante cifrado WEP.

Mapa de comparación: comandos `ifconfig` e `ipadm`

El comando `ipadm` ha reemplazado el comando `ifconfig` para la configuración de las interfaces de red. Aunque el comando `ifconfig` aún funciona en Oracle Solaris 11, el comando `ipadm` es la herramienta preferida para la configuración de red. Sin embargo, algunas opciones de `ifconfig` no tienen equivalente en los subcomandos `ipadm`. En la siguiente tabla se muestran las opciones de comando seleccionadas del comando `ifconfig` y sus equivalentes en el comando `ipadm`.

Nota – En esta tabla no se ofrece una lista completa de las opciones de `ipadm`. Para obtener una lista completa, consulte la página del comando `man ipadm(1M)`.

TABLA A-1 Asignación de sintaxis entre los comandos `ifconfig` y `ipadm`

Comando <code>ifconfig</code>	Comando <code>ipadm</code>
<code>plumb/unplumb</code>	<code>ipadm create-ip</code> <code>ipadm create-vni</code> <code>ipadm create-ipmp</code> <code>ipadm enable-addr</code> <code>ipadm delete-ip</code> <code>ipadm delete-vni</code> <code>ipadm delete-ipmp</code> <code>ipadm disable-addr</code>

TABLA A-1 Asignación de sintaxis entre los comandos ifconfig y ipadm (Continuación)

Comando ifconfig	Comando ipadm
[address[/prefix-length] [dest-address]] [addif address[/prefix-length]] [removeif address[/prefix-length]][netmask mask][destination dest-address]{auto-dhcp dhcp}[primary][wait seconds]extend release start	ipadm create-addr ipadm create-addr -T dhcp ipadm create-addr -T addrconf ipadm delete-addr ipadm refresh-addr
[deprecated -deprecated] [preferred -preferred] [private -private] [zone zonename -zones -all-zones][xmit -xmit]	ipadm set-addprop ipadm reset-addprop ipadm show-addprop
up	ipadm up-addr
down	ipadm down-addr
[metric n] [mtu n] [nud -nud] [arp -arp] [usesrc [name none] [router -router]	ipadm set-ifprop ipadm show-ifprop ipadm reset-ifprop
[ipmp] [group [name ""]] standby -standby] [failover -failover]	ipadm create-ipmp ipadm delete-ipmp ipadm add-ipmp ipadm remove-ipmp ipadm set-ifprop -p [standby] [group]
[interface] [-a]	ipadm ipadm show-if ipadm show-addr
[tdst tunnel-dest-addr] [tsrc tunnel-srcs-addr] [encaplimit n -encaplimit] [thoplimit n]	Conjunto de comandos dladm *-iptun. Para obtener más información, consulte la página del comando man dladm(1M) y “Configuración y administración de túneles con el comando dladm” de <i>Configuración y administración de redes Oracle Solaris 11.1</i> .
[auth_algs authentication algorithm] [encr_algs encryption algorithm] [encr_auth_algs encryption authentication algorithm]	ipseconf Para obtener información, consulte la página del comando man ipseconf(1M) y el Capítulo 7, “Configuración de IPsec (tareas)” de <i>Protección de la red en Oracle Solaris 11.1</i> .

TABLA A-1 Asignación de sintaxis entre los comandos ifconfig y ipadm (Continuación)

Comando ifconfig	Comando ipadm
[auth_revarp] [ether <i>address</i>] [index <i>if-index</i>] [subnet <i>subnet-address</i>] [broadcast <i>broadcast-address</i>] [token <i>address/prefix-length</i>] Opciones de DHCP: inform, ping, release, status, drop	Subcomandos equivalentes que no se encuentran disponibles en este momento.
modlist] [modinsert <i>mod_name@pos</i>] [modremove <i>mod_name@pos</i>]	Subcomandos equivalentes que no se encuentran disponibles en este momento.

Mapa de comparación: comandos `ndd` y `ipadm`

El comando `ipadm` ha reemplazado el comando `ndd` para la personalización de los valores ajustables o parámetros de red. Aunque el comando `ndd` aún funciona en Oracle Solaris 11, el comando `ipadm` es la herramienta preferida para la personalización de los parámetros de red. Sin embargo, algunas opciones de `ndd` no tienen subcomandos `ipadm` equivalentes. En la siguiente tabla se muestran las opciones de comando seleccionadas del comando `ndd` y sus equivalentes en el comando `ipadm`.

Nota – En esta tabla no se ofrece una lista completa de las opciones de `ipadm`. Para obtener una lista completa, consulte la página del comando `man ipadm(1M)`.

TABLA B-1 Asignación de sintaxis entre los comandos ndd e ipadm: recuperación de propiedades

Comando ndd	Comando ipadm
<pre>bash-3.2# ndd -get /dev/ip ? ip_def_ttl (read and write) ip6_def_hops (read and write) ip_forward_directed_broadcasts (read and write) ip_forwarding (read and write)</pre>	<pre>bash-3.2# ipadm show-prop ip PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE ipv4 forwarding rw off -- off on,off ipv4 ttl rw 255 -- 255 1-255 ipv6 forwarding rw off -- off on,off ipv6 hoplimit rw 255 -- 255 1-255 ...</pre>
<pre>bash-3.2# ndd -get /dev/ip \ ip_def_ttl 100 bash-3.2# ndd -get /dev/ip \ ip6_def_hops 255</pre>	<pre>bash-3.2# ipadm show-prop -p ttl,hoplimit ip PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE ipv4 ttl rw 255 -- 255 1-255 ipv6 hoplimit rw 255 -- 255 1-255</pre>
<pre>bash-3.2# ndd -get /dev/tcp ? tcp_cwnd_max (read and write) tcp_strong_iss (read and write) tcp_time_wait_interval (read and write) tcp_tstamp_always (read and write) tcp_tstamp_if_wscale (read and write)</pre>	<pre>bash-3.2# ipadm show-prop tcp PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE tcp ecn rw passive -- passive never,passive, active tcp extra_priv_ports rw 2049 2049,4045 2049,4045 1-65535 tcp largest_anon_port rw 65535 -- 65535 1024-65535 tcp recv_maxbuf rw 128000 -- 128000 2048-1073741824 tcp sack rw active -- active never,passive, active tcp send_maxbuf rw 49152 -- 49152 4096-1073741824 tcp smallest_anon_port rw 32768 -- 32768 1024-65535 tcp smallest_nonpriv_port rw 1024 -- 1024 1024-32768 bash-3.2# ipadm show-prop -p ecn,sack tcp PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE tcp ecn rw passive -- passive never,passive,active tcp sack rw active -- active never,passive,active</pre>

TABLA B-2 Asignación de sintaxis entre los comandos ndd e ipadm: establecimiento de propiedades

Comando ndd	Comando ipadm
<pre>bash-3.2# ndd -set /dev/ip \ ip_def_ttl 64 bash-3.2# ndd -get /dev/ip \ ip_def_ttl 64</pre>	<pre>bash-3.2# ipadm set-prop -p ttl=64 ipv4 bash-3.2# ipadm show-prop -p ttl ip PROTO PROPERTY FAMILY PERM VALUE DEFAULT POSSIBLE ip ttl inet rw 64 255 1-255 PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE ipv4 ttl rw 64 64 255 1-255 bash-3.2# ipadm reset-prop -p ttl ip bash-3.2# ipadm show-prop -p ttl ip PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE ipv4 ttl rw 255 255 255 1-255</pre>

Índice

A

acceso directo a la memoria (DMA), 35–36
agregaciones de enlaces, 29–30
archivo /etc/hosts, 23

B

BSSID, 63

C

comando `cfgadm`, 41
comando `dladm`, 13–17, 29–32
 `connect-wifi`, 63
 `delete-phys`, 31–32
 `help`, 15–16
 `rename-link`, 32
 `reset-linkprop`, 32–38
 `scan-wifi`, 62
 `set-linkprop`, 32–38
 `show-ether`, 37–38
 `show-link`, 30
 `show-linkprop`, 37–38, 65
 `show-phys`, 30–31
 `show-wifi`, 64
comando `ifconfig`, 16
 y comando `ipadm`, 71–73
comando `ipadm`, 13–17, 43–60
 comparación de comando `ifconfig`, 71–73
 comparación de comando `ndd`, 75–77

comando `ipadm` (*Continuación*)

`create-addr`, 23
 `create-ip`, 22–27
 `delete-addr`, 44–45
 `delete-ip`, 43–44
 `disable-ip`, 44
 `help`, 16, 17
 `set-addrprop`, 47
 `set-ifprop`, 45
 `set-prop`, 48–55
 `show-addr`, 58–59
 `show-addrprop`, 47, 59–60
 `show-if`, 56–57
 `show-ifprop`, 45, 57–58
 `show-prop`, 48–55
comando `ndd`, 17
 y comando `ipadm`, 75–77
comando `netadm`, 13–17, 21–22
comando `netcfg`, 13–17
comando `netstat`, comprobación de flujo de paquetes
 mediante un enlace Wi-Fi, 66
comando `route`, 25
configuración de red fija, 11–17
 direcciones IP estáticas, 12
configuración de red gestionada por perfiles, 11–12
configuración de red reactiva, 11–17
 ENM, 13
 perfiles de ubicación, 13
 WLAN, 13
consideraciones de seguridad, Wi-Fi, 67
control de congestión, 52–53
controladores NIC, 32–33

D

DHCP, 25
dirección IP
 DHCP, 25
 eliminación, 44–45
 estática, 23
 IPv4 e IPv6, 23
 local y remota, 23
 propiedades, 47, 59–60
 reenvío de paquetes, 45–46, 49
 supervisión, 55–60
dirección local, 23
dirección MAC, comprobación de exclusividad, 20–21
dirección remota, 23
dúplex completo, 34
dúplex medio, 34

E

ECMP, 50–51
enlaces de datos
 agregaciones de enlaces, 29–30
 cambio de nombre, 32
 cambio MTU tamaño, 33
 configuración de una interfaz IP mediante un enlace, 22–27
 eliminación, 31–32
 enlace DMA, 35–36
 enlaces físicos, 30
 establecimiento de propiedades, 32–38
 frecuencia de interrupción, 36–37
 módulos STREAMS, 35
 negociación automática, 33
 nombres genéricos, 32
 propiedad autopush, 35
 propiedades públicas y privadas, 32–33
 valores de parámetros de Ethernet, 37–38
 velocidad anunciada y permitida, 33–34
 velocidad de enlace, 33–34
 visualización
 atributos físicos, 30–31
 enlaces, 30
 información general, 29–30
 propiedades de controlador de red, 37–38

enlaces de datos, visualización (*Continuación*)
 propiedades de enlace, 37–38
 ubicaciones físicas del sistema, 31
 VLAN, 29–30
 VNIC, 29–30
enrutamiento simétrico, 50–51
ESSID, 63

F

frecuencia de interrupción, 36–37

G

Generic LAN Driver (GLD), 36–37
gestión de energía, 34
GLDv3, 15–16

H

herramientas de configuración de red, 13–17
 comando `dladm`, 15–16
 comando `ipadm`, 16
 comando `netadm`, 13
 comando `netcfg`, 13
host múltiple, 50–51

I

ICMP, 16
interfases inalámbricas, 61
interfaz de red virtual (VNI), 22–27
interfaz de rutas múltiples de red IP (IPMP), 22–27
interfaz IP
 activación de reenvío de paquetes, 45–46, 49
 asignación de direcciones IP, 23
 cambio de interfaz principal, 43–44
 cambio de una dirección IP, 44–45
 comprobación de exclusividad de dirección MAC, 20–21
 configuración, 25

interfaz IP (Continuación)

- creación y asociación, 22–27
- dirección IP, 58–59, 59–60
- desactivación y activación, 44
- eliminación de una dirección IP, 44–45
- establecimiento de propiedades de interfaz, 45
- interfaz IPMP, 22–27
- interfaz VNI, 22–27
- propiedades de dirección, 47
- propiedades de interfaz, 57–58
- propiedades de protocolo TCP/IP, 48–55
- puertos con privilegios, 49
- supervisión, 55–60
- supresión de configuración de interfaz, 43–44
- visualización
 - direcciones IP, 58–59
 - información general, 25, 55–56
 - interfaces, 56–57
 - propiedades de dirección, 59–60
 - propiedades de interfaz, 57–58
 - propiedades de protocolo, 48
 - visualización de propiedades de interfaz, 45
 - Wi-Fi, 62
- interfaz principal, cambio, 32, 38–42, 43–44

M

- memorias intermedias, 35–36
- modificadores de red externa (ENM), 13
- módulos STREAMS, y enlaces de datos, 35
- MTU, 33

N

- NCP, Ver perfil de configuración de red
- NCP DefaultFixed, 13
- negociación automática, 33
- nombres de enlace, 32
- notación CIDR, 23

O

- objeto de dirección, 24

P

- parámetros de Ethernet, 37–38
- perfil de configuración de red (NCP), 11–17
 - cambio de NCP activos, 21–22
 - NCP activo, 11–17
 - visualización de NCP, 21–22
- perfil de configuración de red (NCP, Network Configuration Profile), 12–13
 - cambio de NCP activos, 13
 - DefaultFixed, 12, 13
 - fijo, 12–13
 - reactive, 12–13
- perfiles de ubicación, 13
- producto de retraso de ancho de banda (BDP), 53–55
- propiedad autopush, 35
- protocolo de resolución de direcciones (ARP), 16
- protocolos, propiedades de, 48–55
- puertos con privilegios, 49

R

- reconfiguración dinámica (DR), reemplazo de NIC, 40
- redes de área local virtuales (VLAN), 29–30
- redes privadas virtuales (VPN), 35
- reenvío de paquetes
 - en interfaces, 45–46
 - en protocolos, 49

S

- SCTP, 16
- servicio name-service/switch, 23

T

- tamaño de memoria intermedia de recepción de TCP, 53–55

tarjeta de interfaz de red (NIC), sustitución, con
DR, 40
tarjetas de red virtual (VNIC), 29–30
tramas gigantes, activación de la admisión de, 33
túneles IP, 23
direcciones local y remota, 23

U

UDP, 16
USENIX, 36–37
utilidad de gestión de servicios (SMF), 16

V

velocidad de enlace, 33–34

W

Wi-Fi

cifrado de una conexión, 67
comprobación de flujo de paquetes, 66
conexión a una red Wi-Fi, 62, 63
conexión con una red Wi-Fi, 64
definición, 61
ejemplo, configuración de la velocidad de un
enlace, 67
ejemplo de comunicaciones cifradas, 68
ejemplo de configuración Wi-Fi, 64
enlaces Wi-Fi seguros, 67
especificación IEEE 802.11, 61
ID de conjunto de servicios básicos (BSSID, Basic
Service Set ID), 63
ID de conjunto de servicios extendidos (ESSID,
Extended Service Set ID), 63
supervisión de un enlace, 65

WLAN, 13