

Administración de Oracle® Solaris: interfaces y virtualización de redes

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 comuniqué 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 RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065

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	15
1 Descripción general de la pila de red	21
Configuración de red en esta versión de Oracle Solaris	21
La pila de red en Oracle Solaris	22
Dispositivos de red y nombres de enlaces de datos	26
Nombres de enlaces genéricos predeterminados	26
Asignación de nombres genéricos a los enlaces de datos	27
Personalización de la asignación de nombres de enlace genéricos	28
Nombres de enlace en sistemas actualizados	29
Administración de otros tipos de enlaces	31
Parte I Conexión automática a la red (NWAM, Network Auto-Magic)	35
2 Introducción a NWAM	37
¿Qué es la configuración NWAM?	38
Componentes funcionales de NWAM	39
Cuándo se utiliza NWAM	40
Cómo funciona la configuración NWAM	41
Comportamiento predeterminado de NWAM	42
Cómo funciona NWAM con otras tecnologías de red de Oracle Solaris	42
Dónde encontrar las tareas de configuración de red	44
3 Configuración y administración de NWAM (descripción general)	47
Descripción general de la configuración de NWAM	47
¿Qué son los perfiles de red?	47
Descripción de un NCP	48

Descripción de una NCU	49
Descripción de NCP automáticos y NCP definidos por el usuario	50
Descripción de un perfil de ubicación	50
Descripción de un ENM	51
Acerca de las WLAN conocidas	52
Datos de configuración de NWAM	53
Valores de propiedades de la NCU	54
Valores de propiedades de ubicaciones definidas por el sistema	56
Activación de los perfiles NWAM	58
Política de activación del NCP	59
Criterios de selección de activación de ubicación	61
Perfiles de configuración mediante el comando <code>netcfg</code>	63
Modo interactivo <code>netcfg</code>	64
Modo de línea de comandos <code>netcfg</code>	65
Modo de archivo de comandos <code>netcfg</code>	66
Subcomandos admitidos por <code>netcfg</code>	66
Administración de perfiles mediante el comando <code>netadm</code>	69
Descripción general de los daemons NWAM	71
Descripción del daemon de motor de política NWAM (<code>nwamd</code>)	71
Descripción del daemon de depósito NWAM (<code>netcfgd</code>)	72
Servicios de red SMF	72
Descripción general de la seguridad de NWAM	73
Autorizaciones y perfiles relacionados con NWAM	73
Autorizaciones necesarias para utilizar interfaces de usuario de NWAM	74
4 Configuración de perfiles de NWAM (tareas)	77
Creación de perfiles	78
Creación de perfiles en modo de línea de comandos	78
Creación de perfiles de forma interactiva	79
Creación de un NCP	80
Creación de NCU para un NCP	80
▼ Cómo crear de forma interactiva un NCP	83
Creación de un perfil de ubicación	87
Creación de un perfil de ENM	93
Creación de WLAN	95

Eliminación de perfiles	97
Configuración y cambio de valores de propiedades de un perfil	99
Consulta al sistema sobre información de perfiles	102
Enumeración de todos los perfiles en un sistema	102
Enumeración de todos los valores de propiedades de un perfil específico	103
Obtención de valores de una propiedad concreta	104
Visualización y cambio de valores de propiedades de forma interactiva mediante el subcomando <code>walkprop</code>	106
Exportación y restauración de la configuración de un perfil	107
Restauración de un perfil definido por el usuario	111
Gestión de configuración de red	111
▼ Cómo cambiar del modo de configuración de red automático al modo de configuración de red manual	111
▼ Cómo cambiar del modo de configuración de red manual al modo de configuración de red automático	112
5 Administración de perfiles de NWAM (tareas)	113
Obtención de información sobre estados de perfiles	114
Visualización del estado actual de un perfil	114
Valores de estado auxiliar	116
Activación y desactivación de perfiles	116
Realización de un análisis inalámbrico y conexión a redes inalámbricas disponibles	119
Resolución de problemas de configuración de red de NWAM	120
Supervisión del estado actual de todas las conexiones de red	120
Resolución de problemas de configuración de interfaz de red	121
6 Acerca de la interfaz gráfica de usuario de NWAM	123
Introducción a la interfaz gráfica de usuario de NWAM	124
Acceso a la GUI de NWAM desde el escritorio	124
Diferencias entre la interfaz de línea de comandos de NWAM y la interfaz gráfica de usuario de NWAM	125
Componentes funcionales de la GUI de NWAM	126
Interacción con NWAM desde el escritorio	129
Comprobación del estado de la conexión de red	129
Control de las conexiones de red desde el escritorio	131
Incorporación y gestión de redes inalámbricas favoritas	132

▼	Cómo incorporar una red inalámbrica	133
	Gestión de redes favoritas	134
Gestión de perfiles de red		135
	Acerca del cuadro de diálogo Preferencias de red	136
	Visualización de información sobre los perfiles de red	138
	Cómo cambiar de un perfil de red a otro	138
	Cómo agregar o eliminar un perfil de red	139
	Cómo editar perfiles de red	139
	Trabajo con grupos de prioridades	140
	Creación y gestión de ubicaciones	142
	Edición de ubicaciones	145
Sobre los modificadores de red externos		145
	Acerca del cuadro de diálogo Modificadores de red	146
▼	Cómo agregar un MNE de línea de comandos	147
Parte II	Configuración de interfaz y enlace de datos	149
7	Uso de comandos de configuración de interfaces y enlaces de datos en perfiles	151
	Características principales de la configuración de red basada en perfil	151
	Herramientas de configuración y perfiles	152
▼	Cómo determinar el modo de gestión de redes	152
	Pasos siguientes	154
8	Configuración y administración de enlaces de datos	155
	Configuración de enlaces de datos (tareas)	155
	El comando <code>dladm</code>	156
▼	Cómo cambiar el nombre de un enlace de datos	158
▼	Cómo visualizar información sobre atributos físicos de enlaces de datos	159
▼	Cómo visualizar información sobre enlaces de datos	160
▼	Cómo eliminar un enlace de datos	161
	Configuración de propiedades de enlaces de datos	161
	Descripción general de las propiedades de enlaces de datos	162
	Configuración de propiedades de enlaces de datos con el comando <code>dladm</code>	162
	Tareas de configuración adicionales en enlaces de datos	170

▼	Cómo sustituir una tarjeta de interfaz de red con reconfiguración dinámica	171
	Configuración de módulos STREAMS en enlaces de datos	173
9	Configuración de una interfaz IP	177
	Sobre la configuración de la interfaz IP	177
	El comando <code>ipadm</code>	177
	Configuración de la interfaz IP (tareas)	179
	▼ SPARC: Cómo asegurarse de que la dirección MAC de una interfaz sea única	179
	Configuración de interfaces IP	181
	▼ Cómo configurar una interfaz IP	181
	Configuración de las propiedades de las direcciones IP	185
	Configuración de las propiedades de la interfaz IP	187
	Administración de propiedades de protocolo	191
	Configuración de propiedades TCP/IP	191
	Supervisión de direcciones e interfaces IP	196
	▼ Cómo obtener información sobre las interfaces de red	196
	Solución de problemas de configuración de interfaces	200
	El comando <code>ipadm</code> no funciona.	200
	La dirección IP no se puede asignar con el comando <code>ipadm create-addr</code>	200
	Durante la configuración de la dirección IP, aparece el mensaje <code>cannot create address object: Invalid argument provided</code>	200
	Durante la configuración de la interfaz IP, aparece el mensaje <code>cannot create address: Persistent operation on temporary object</code>	201
	Tablas de comparación: comando <code>ipadm</code> y otros comandos de red	202
	Opciones de los comandos <code>ifconfig</code> y <code>ipadm</code>	202
	Opciones de los comandos <code>ndd</code> y <code>ipadm</code>	204
10	Configuración de las comunicaciones mediante interfaces inalámbricas en Oracle Solaris	207
	Mapa de tareas de comunicaciones Wi-Fi	207
	Comunicación mediante interfaces Wi-Fi	208
	Búsqueda de una red Wi-Fi	208
	Planificación de comunicaciones Wi-Fi	209
	Conexión y uso de Wi-Fi en los sistemas Oracle Solaris	210
	▼ Cómo conectarse a una red Wi-Fi	210
	▼ Cómo supervisar el enlace Wi-Fi	214

Comunicaciones seguras mediante Wi-Fi	216
▼ Cómo configurar una conexión de red Wi-Fi cifrada	216
11 Administración de puentes	219
Descripción general sobre puentes	219
Propiedades de enlaces	223
Daemon de STP	224
Daemon de TRILL	225
Depuración de puentes	226
Otros comportamientos de puentes	226
Ejemplos de configuración de puentes	229
Administración de puentes (mapa de tareas)	229
▼ Cómo ver información sobre puentes configurados	231
▼ Cómo ver información de configuración sobre enlaces de puentes	233
▼ Cómo crear un puente	233
▼ Cómo modificar el tipo de protección de un puente	234
▼ Cómo agregar uno o más enlaces a un puente existente	235
▼ Cómo eliminar enlaces de un puente	235
▼ Cómo eliminar un puente del sistema	236
12 Administración de agregaciones de enlaces	237
Descripción general de agregaciones de vínculos	237
Conceptos básicos de agregaciones de vínculos	238
Agregaciones de vínculos de extremo a extremo	239
Directivas y equilibrio de la carga	240
Modo de agregación y nodos	241
Requisitos para agregaciones de vínculos	241
Nombres flexibles para las agregaciones de enlaces	241
Administración de agregaciones de enlaces (mapa de tareas)	242
▼ Cómo crear una agregación de vínculos	242
▼ Cómo modificar una agregación	244
▼ Cómo agregar un enlace a una agregación	245
▼ Cómo eliminar un enlace de una agregación	246
▼ Cómo eliminar una agregación	247

13 Administración de VLAN	249
Administración de redes de área local virtuales	249
Descripción general de una configuración VLAN	250
Administración de VLAN (mapa de tareas)	252
Planificación de una red para redes VLAN	253
Configuración de redes VLAN	254
VLAN en dispositivos heredados	258
Realización de otras tareas administrativas en redes VLAN	258
Combinación de tareas de configuración de red cuando se utilizan nombres personalizados	261
14 Introducción a IPMP	265
Novedades con IPMP	265
Implementación de IPMP	266
Por qué debe utilizar IPMP	266
Cuando se debe utilizar IPMP	267
Comparación IPMP y agregación de enlaces	268
Uso de nombres de enlace flexibles en la configuración IPMP	269
Cómo funciona IPMP	270
Componentes de IPMP en Oracle Solaris	276
Tipos de configuraciones de interfaces IPMP	277
Direcciones IPMP	278
Direcciones de prueba IPv4	279
Direcciones de prueba IPv6	279
Detección de fallos y reparaciones en IPMP	279
Tipos de detección de fallos en IPMP	279
Detección de reparaciones de interfaces físicas	282
IPMP y reconfiguración dinámica	284
Conexión de nuevas NIC	284
Desconexión de NIC	285
Reemplazo de NIC	285
Terminología y conceptos de IPMP	286
15 Administración de IPMP	295
Mapas de tareas de administración de IPMP	295

Creación y configuración del grupo IPMP (mapa de tareas)	296
Mantenimiento del grupo IPMP (mapa de tareas)	296
Configuración de la detección de fallos basada en sondeos (mapa de tareas)	297
Supervisión de un grupo IPMP (mapa de tareas)	297
Configuración de grupos IPMP	298
▼ Cómo planificar un grupo IPMP	298
▼ Cómo configurar un grupo IPMP mediante el DHCP	300
▼ Cómo configurar manualmente un grupo IPMP de interfaz activa-activa	302
▼ Cómo configurar manualmente un grupo IPMP de interfaz activa-en espera	304
Mantenimiento de grupos IPMP	306
▼ Cómo agregar una interfaz a un grupo IPMP	306
▼ Cómo eliminar una interfaz de un grupo IPMP	306
▼ Cómo agregar o eliminar direcciones IP	307
▼ Cómo mover una interfaz de un grupo IPMP a otro grupo	308
▼ Cómo suprimir un grupo IPMP	309
Configuración para la detección de fallos basada en sondeos	309
▼ Cómo especificar manualmente los sistemas de destino para la detección de fallos basada en sondeos	310
▼ Cómo seleccionar qué método de detección de fallos utilizar	311
▼ Cómo configurar el comportamiento del daemon IPMP	312
Recuperación de configuración de IPMP con reconfiguración dinámica	313
▼ Cómo reemplazar una tarjeta física que ha fallado	313
Supervisión de información de IPMP	315
▼ Cómo obtener información de grupo IPMP	315
▼ Cómo obtener información de dirección de datos IPMP	316
▼ Cómo obtener información sobre interfaces IP subyacentes de un grupo	317
▼ Cómo obtener información de destino de sondeo IPMP	319
▼ Cómo observar sondeos IPMP	320
▼ Cómo personalizar la salida del comando <code>ipmpstat</code> en una secuencia de comandos	321
▼ Cómo generar salidas analizables automáticamente del comando <code>ipmpstat</code>	322
16 Intercambio de información de conectividad de red con LLDP	325
Descripción general de LLDP en Oracle Solaris	325
Componentes de una implementación LLDP	325
Funciones del agente LLDP	327

Configuración del modo de operación de los agentes LLDP	327
Configuración de la información que se anunciará	328
Gestión de las unidades de TLV	331
▼ Cómo definir los valores de TLV globales	333
Establecimiento de puentes del centro de datos	334
Supervisión de agentes LLDP	335
▼ Cómo mostrar los anuncios	335
▼ Cómo mostrar estadísticas LLDP	337
Parte III Virtualización de la red y gestión de los recursos	339
17 Introducción a la virtualización de redes y el control de recursos (descripción general)	341
La virtualización de redes y las redes virtuales	341
Partes de la red virtual interna	342
¿Quién debería ejecutar redes virtuales?	344
¿Qué es el control de recursos?	345
Funcionamiento de la gestión del ancho de banda y del control del flujo	345
Asignación de control de recursos y gestión del ancho de banda en una red	346
¿Quién debería implementar las funciones de control de recursos?	348
Funciones de observación para la virtualización de redes y el control de recursos	348
18 Planificación para la virtualización de red y el control de recursos	351
Mapa de tareas de virtualización de red y control de recursos	351
Planificación y diseño de una red virtual	352
Red virtual básica en un sistema único	352
Red privada virtual en un sistema único	354
Para obtener más información	355
Aplicación de controles en los recursos de red	356
Control de recursos basado en interfaz para una red tradicional	358
Control de flujo para la red virtual	358
▼ Cómo crear una política de uso para las aplicaciones en una red virtual	360
▼ Cómo crear un acuerdo de nivel de servicio para la red virtual	360

19 Configuración de redes virtuales (tareas)	363
Mapa de tareas de redes virtuales	363
Configuración de componentes de virtualización de red en Oracle Solaris	364
▼ Cómo crear una interfaz de red virtual	365
▼ Cómo crear etherstubs	367
Cómo trabajar con VNIC y zonas	369
Creación de zonas nuevas para utilizar con VNIC	369
Modificación de la configuración de zonas existentes para utilizar VNIC	374
Creación de una red virtual privada	378
▼ Cómo eliminar la red virtual sin eliminar las zonas	380
20 Uso de la protección de enlaces en entornos virtualizados	383
Descripción general de la protección de enlaces	383
Tipos de protección de enlaces	384
Configuración de la protección de enlaces (mapa de tareas)	385
▼ Cómo habilitar el mecanismo de protección de enlaces	386
▼ Cómo deshabilitar la protección de enlaces	386
▼ Cómo especificar las direcciones IP para la protección contra la falsificación de IP	386
▼ Cómo ver la configuración de protección de enlaces	387
21 Gestión de recursos de red	389
Descripción general de la gestión de recursos de red	389
Propiedades de enlaces de datos para el control de recursos	389
Gestión de recursos de red mediante flujos	390
Comandos para la gestión de recursos de red	391
Gestión de recursos de red (mapa de tareas)	392
Gestión de recursos en enlaces de datos	393
Anillos de transmisión y recepción	393
Agrupaciones y CPU	407
Gestión de recursos en flujos	412
Configuración de flujos en la red	412
22 Supervisión del tráfico de red y el uso de recursos	417
Descripción general del flujo del tráfico de red	417

Supervisión de tráfico y uso de recursos (mapa de tareas)	420
Recopilación de estadísticas sobre el tráfico de red en enlaces	421
▼ Cómo obtener estadísticas básicas sobre el tráfico de la red	422
▼ Cómo obtener estadísticas sobre el uso anillos	423
▼ Cómo obtener estadísticas sobre el tráfico de red en vías	425
Recopilación de estadísticas sobre tráfico de red en flujos	427
▼ Cómo obtener estadísticas de flujos	427
Configuración de la contabilidad de la red	429
▼ Cómo configurar la contabilidad de red ampliada	430
▼ Cómo obtener estadísticas históricas del tráfico de la red	431
Glosario	435
Índice	445

Prefacio

Bienvenido a Administración de Oracle Solaris: interfaces y virtualización de redes. Esta guía forma parte de un conjunto de catorce volúmenes que abarcan una parte significativa de la información acerca de la administración del sistema 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.

En este documento, estos términos relacionados con x86 significan lo siguiente:

- x86 hace referencia a la familia más grande de productos compatibles con x86 de 32 y 64 bits.
- x64 hace referencia específicamente a CPU compatibles con x86 de 64 bits.
- "x86 de 32 bits" destaca información específica de 32 bits acerca de sistemas basados en x86.

Para conocer cuáles son los sistemas admitidos, consulte [Listas de compatibilidad del sistema operativo Oracle Solaris](#).

Usuarios a los que está destinada esta guía

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.

Organización de las guías de administración del sistema

A continuación se enumeran los temas que abarcan las guías de administración del sistema.

Título de la guía	Temas
<i>Inicio y cierre de Oracle Solaris en plataformas SPARC</i>	Inicio y cierre de un sistema, gestión de servicios de inicio, modificación de comportamiento de inicio, inicio desde ZFS, gestión de archivo de inicio y resolución de problemas de inicio en plataformas SPARC.
<i>Inicio y cierre de Oracle Solaris en plataformas x86</i>	Inicio y cierre de un sistema, gestión de servicios de inicio, modificación de comportamiento de inicio, inicio desde ZFS, gestión de archivo de inicio y resolución de problemas de inicio en plataformas x86.
<i>Administración de Oracle Solaris: tareas comunes</i>	Uso de comandos de Oracle Solaris; inicio y cierre de un sistema; gestión de cuentas de usuario y grupos; gestión de servicios, fallos de hardware, información del sistema, recursos del sistema y rendimiento del sistema; gestión de software; impresión; la consola y los terminales; y resolución de problemas del sistema y software.
<i>Administración de Oracle Solaris: dispositivos y sistemas de archivos</i>	Medios extraíbles, discos y dispositivos, sistemas de archivos y copias de seguridad y restauración de datos.
<i>Administración de Oracle Solaris: servicios IP</i>	Administración de redes TCP/IP, administración de direcciones IPv4 e IPv6, DHCP, IPsec, IKE, filtro IP e IPQoS.
<i>Oracle Solaris Administration: Naming and Directory Services</i>	Servicios de directorios y nombres DNS, NIS y LDAP, incluida la transición de NIS a LDAP.
<i>Administración de Oracle Solaris: interfaces y virtualización de redes</i>	Configuración manual y automática de interfaz IP (incluido Wi-Fi inalámbrico), administración de puentes, redes VLAN, agregaciones, LLDP, IPMP, NIC virtuales y gestión de recursos.
<i>Oracle Administración Solaris: Servicios de red</i>	Servidores de caché web, servicios relacionados con el tiempo, sistemas de archivos de red (NFS y Autofs), correo, SLP y PPP.
<i>Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos</i>	Funciones de gestión de recursos, que permiten controlar el modo en que las aplicaciones utilizan los recursos del sistema disponibles; tecnología de partición de software de zonas de Oracle Solaris, que virtualiza servicios de sistemas operativos para crear un entorno aislado para la ejecución de aplicaciones; y zonas de Oracle Solaris 10, que alojan entornos de Oracle Solaris 10 que se ejecutan en el núcleo de Oracle Solaris 11.
<i>Administración de Oracle Solaris: servicios de seguridad</i>	Auditoría, gestión de dispositivos, seguridad de archivos, BART, servicios Kerberos, PAM, estructura criptográfica, gestión de claves, privilegios, RBAC, SASL, Secure Shell y análisis de virus.

Título de la guía	Temas
<i>Oracle Solaris Administration: SMB and Windows Interoperability</i>	Servicio SMB, que permite configurar un sistema Oracle Solaris para que los recursos compartidos SMB estén disponibles para clientes SMB; cliente SMB, que permite acceder a recursos compartidos SMB; y servicios nativos de asignación de identidades, que permiten asignar identidades de usuarios y grupos entre sistemas Oracle Solaris y sistemas Windows.
<i>Administración de Oracle Solaris: sistemas de archivos ZFS</i>	Creación y gestión de sistemas de archivos y agrupaciones de almacenamiento ZFS, instantáneas, clones, copias de seguridad, uso de listas de control de acceso (ACL) para proteger archivos ZFS, uso de Solaris ZFS en un sistema Solaris con zonas instaladas, volúmenes emulados y solución de problemas y recuperación de datos.
<i>Configuración y administración de Trusted Extensions</i>	Instalación, configuración y administración de sistemas, específicas para Trusted Extensions.
<i>Directrices de seguridad de Oracle Solaris 11</i>	Protección de un sistema Oracle Solaris, así como situaciones de uso para sus funciones de seguridad, como zonas, ZFS y Trusted Extensions.
<i>Transición de Oracle Solaris 10 a Oracle Solaris 11</i>	Información sobre administración del sistema y ejemplos de transición de Oracle Solaris 10 a Oracle Solaris 11 en las áreas de instalación, dispositivo, disco y gestión del sistema de archivos; gestión de software; redes; gestión de sistemas; seguridad; virtualización; funciones de escritorio; gestión de cuentas de usuario; volúmenes emulados de entornos de usuarios; y resolución de problemas y recuperación de datos.

Referencias relacionadas con el sitio web de otras empresas

Se hace referencia a direcciones URL de terceras partes para proporcionar información adicional relacionada.

Nota – Oracle no se hace responsable de la disponibilidad de los sitios web de terceros que se mencionan en este documento. Oracle no garantiza ni se hace responsable de los contenidos, la publicidad, los productos u otros materiales que puedan estar disponibles mediante dichos sitios o recursos. Oracle no será responsable de ningún daño o pérdida ocasionados o supuestamente ocasionados debido, directa o indirectamente, al uso de los contenidos, bienes o servicios disponibles en dichas sedes o a los que se pueda acceder a través de tales sedes o recursos.

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> . <i>Una copia en antememoria es aquella que se almacena localmente.</i> <i>No guarde el archivo.</i> 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	nombre_sistema%
Shell C para superusuario	nombre_sistema#

Descripción general de la pila de red

Este capítulo brinda una introducción a la administración de redes en Oracle Solaris. También describe las interrelaciones que subyacen a las interfaces, los enlaces de datos por los que las interfaces están configuradas y los dispositivos de red, y trata detalladamente la admisión de nombres flexibles para enlaces de datos.

Configuración de red en esta versión de Oracle Solaris

Se destacan las siguientes diferencias en el modo de configurar la red en esta versión, en comparación con las versiones anteriores de Oracle Solaris:

- La configuración de red se gestiona mediante un perfil. El tipo de configuración que opera en un sistema depende del perfil de configuración de red que esté activo. Consulte la [Parte I](#).
- Los enlaces de datos de la capa 2 de la pila de red se administran mediante el comando `dladm`. Este comando reemplaza las opciones del comando `ifconfig` anteriores para configurar las propiedades de los enlaces de datos. Por lo tanto, la configuración de las agregaciones de enlaces, las VLAN y los túneles IP también se han modificado. Consulte el [Capítulo 8, “Configuración y administración de enlaces de datos”](#), el [Capítulo 12, “Administración de agregaciones de enlaces”](#) y el [Capítulo 13, “Administración de VLAN”](#). Consulte también el [Capítulo 6, “Configuración de túneles IP”](#) de *Administración de Oracle Solaris: servicios IP*.
- Los nombres de enlaces de datos ya no están vinculados con sus controladores de hardware. Por lo tanto, de manera predeterminada, se asignan a los enlaces de datos nombres de enlace genéricos, como `net0`, `net1` y así sucesivamente. Consulte [“Dispositivos de red y nombres de enlaces de datos”](#) en la [página 26](#).
- Las interfaces IP de la capa 3 de la pila en red se administran mediante el comando `ipadm`. Este comando reemplaza las opciones de comando `ifconfig` para configurar las interfaces IP. Consulte el [Capítulo 9, “Configuración de una interfaz IP”](#).

- Los grupos IPMP se implementan como interfaces IP y, por lo tanto, se configuran de manera similar con el comando `ipadm`. Además, se introduce el comando `ipmpstat`, que permite obtener estadísticas e información relacionadas con IPMP. Consulte el [Capítulo 14, “Introducción a IPMP”](#) y el [Capítulo 15, “Administración de IPMP”](#).
- La virtualización se implementa en el nivel del dispositivo de red. Por lo tanto, puede configurar las VNIC y gestionar el uso de los recursos de red para obtener una mayor eficiencia. Consulte la [Parte III](#).

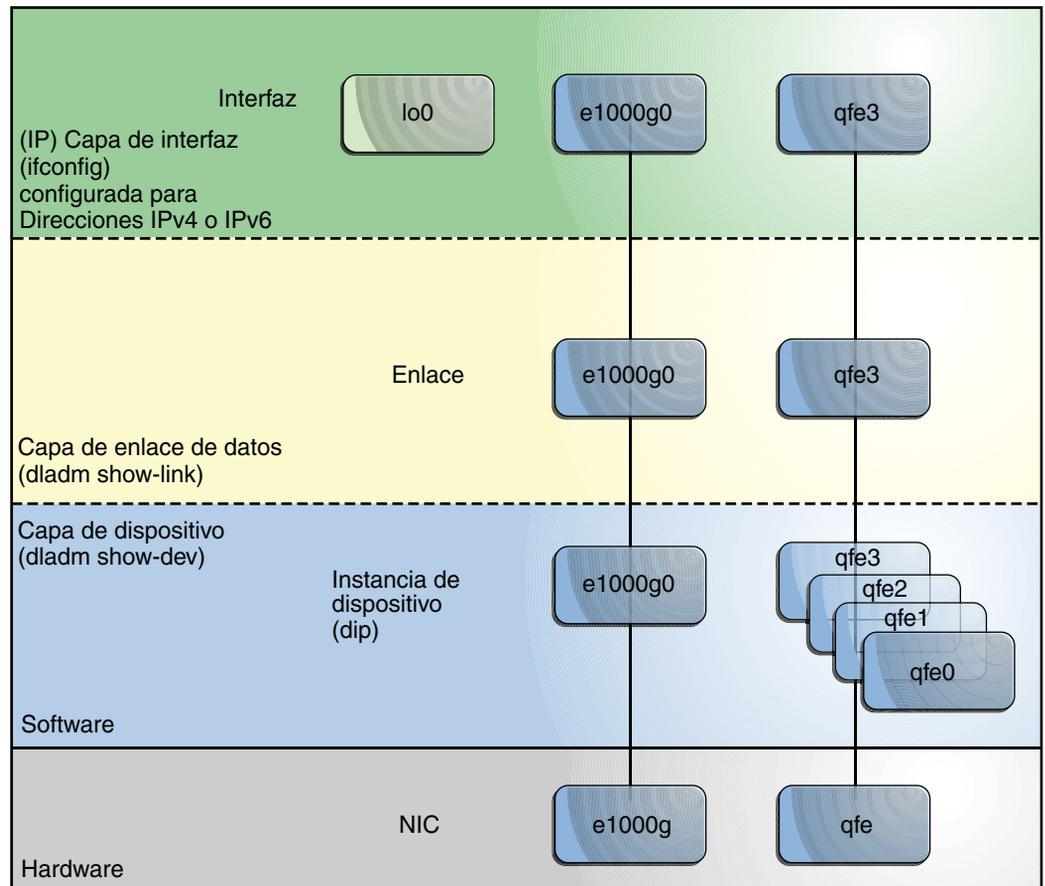
La pila de red en Oracle Solaris

Las interfaces de red proporcionan la conexión entre el sistema y la red. Estas interfaces se configuran por enlaces de datos que, a su vez, corresponden a instancias de dispositivos de hardware en el sistema. Los dispositivos de hardware de red también se denominan *tarjetas de interfaz de red (NIC, Network Interface Cards)* o *adaptadores de red*. Las tarjetas de interfaz de red se pueden integrar y vienen incluidas en el sistema que se compra. Sin embargo, también se pueden adquirir NIC por separado para agregar al sistema. Determinadas NIC tienen solamente una interfaz que reside en la tarjeta. Otras pueden tener varias interfaces que se pueden configurar para realizar las operaciones de red.

En el modelo actual de la pila de red, las interfaces y los enlaces de la capa del software se integran con los dispositivos de la capa del hardware. Específicamente, una instancia de dispositivo de hardware en la capa del hardware tiene un enlace correspondiente en la capa del enlace de datos y una interfaz configurada en la capa de la interfaz. Esta relación uno a uno entre el dispositivo de red, su enlace de datos y la interfaz IP se ilustra en la figura que aparece a continuación.

Nota – Para obtener una explicación más completa de la pila TCP/IP, consulte el [Capítulo 1, “Oracle Solaris TCP/IP Protocol Suite \(Overview\)”](#) de *System Administration Guide: IP Services*.

FIGURA 1-1 Pila de red que muestra los dispositivos de red, los enlaces y las interfaces: modelo de Oracle Solaris 10



La figura muestra dos NIC en la capa del hardware: `e1000g`, con una única instancia de dispositivo `e1000g0`, y `qfe`, con varias instancias de dispositivos, `qfe0` a `qfe3`. Los dispositivos de `qfe0` a `qfe2` no se utilizan. Se utilizan los dispositivos `e1000g` y `qfe3`, que tienen los enlaces correspondientes `e1000g0` y `qfe3` en la capa del enlace de datos. En la figura, las interfaces IP también se denominan según su respectivo hardware subyacente, `e1000g0` y `qfe3`. Estas interfaces se pueden configurar con direcciones IPv4 o IPv6 para que alojen ambos tipos de tráfico de red. Tenga en cuenta también la presencia de la interfaz de bucle de retorno `lo0` en la capa de la interfaz. Esta interfaz se utiliza para probar, por ejemplo, que la pila IP funcione correctamente.

En cada capa de la pila, se utilizan diferentes comandos administrativos. Por ejemplo, los dispositivos de hardware que están instalados en el sistema se muestran con el comando `dladm`

`show-dev`. La información sobre los enlaces de la capa del enlace de datos se muestra junto con el comando `dladm show-link`. El comando `ifconfig` muestra la configuración de la interfaz IP en la capa de interfaz.

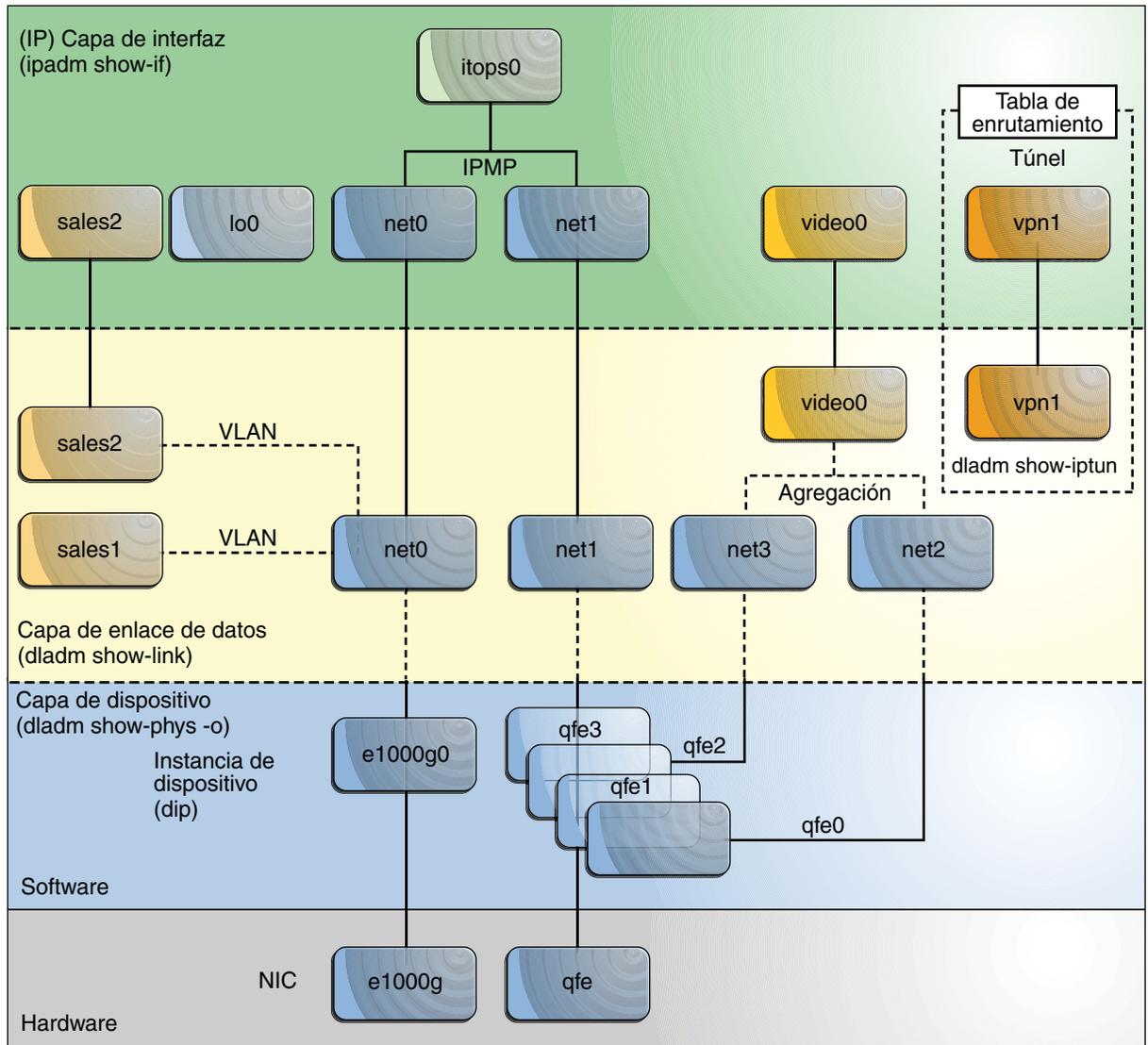
En este modelo, existe una relación de uno a uno que enlaza el dispositivo, el enlace de datos y la interfaz. Esta relación significa que la configuración de red depende de la configuración de hardware y la topología de red. Las interfaces se deben reconfigurar si los cambios se implementan en la capa del hardware, como es el caso del reemplazo de la NIC o el cambio de la topología de la red.

Oracle Solaris 11 presenta una implementación de la pila de red en la que permanece la relación básica entre el hardware, el enlace de datos y las capas de la interfaz. Sin embargo, la capa del software se separa de la capa del hardware. Con esta separación, la configuración de red en la capa del software ya no se vincula con el conjunto de chips ni la topología de red en la capa del hardware. Esta implementación hace que la administración de red sea más flexible de las siguientes maneras:

- La configuración de la red se encuentra aislada de los cambios que se puedan producir en la capa del hardware. Las configuraciones de enlaces e interfaces se conservan, incluso si el hardware subyacente se elimina. Estas mismas configuraciones pueden volver a aplicarse luego en cualquier NIC de reemplazo, siempre que las dos NIC sean del mismo tipo.
- La separación de la configuración de red de la configuración del hardware de red también permite el uso de nombres de enlace personalizados en la capa del enlace de datos.
- Con la abstracción de la capa del enlace de datos, varias configuraciones o abstracciones de red, como las VLAN, las VNIC, los dispositivos físicos, las agregaciones de enlaces y los túneles IP, se unifican en una entidad administrativa común, que es el enlace de datos.

La figura siguiente ilustra cómo estas configuraciones de red se crean en la pila de red:

FIGURA 1-2 Pila de red que muestra los dispositivos de red, enlaces e interfaces: modelo de Oracle Solaris 11



Las configuraciones que se muestran en esta ilustración se explican más adelante en [“Administración de otros tipos de enlaces” en la página 31.](#)

Dispositivos de red y nombres de enlaces de datos

Desde el punto de vista administrativo, los administradores crean interfaces IP encima de los *enlaces de datos*. El enlace de datos representa un objeto de enlace en la segunda capa del modelo de interconexión de sistemas abiertos (OSI, Open Systems Interconnection). El *enlace físico* está asociado directamente con un dispositivo y tiene un nombre de dispositivo. El nombre del dispositivo es básicamente el nombre de la instancia del dispositivo y se forma con el nombre del controlador y el número de instancia del dispositivo. El número de instancia puede tener un valor de 0 a n , según cuántas NIC utilice ese controlador en el sistema.

Pongamos por ejemplo una tarjeta Gigabit Ethernet, que se suele utilizar como NIC principal en sistemas host y en sistemas de servidor. Algunos nombres de controlador típicos para esta NIC son `bge` y `e1000g`. Cuando se utiliza como NIC principal, la interfaz de Gigabit Ethernet tiene un nombre de dispositivo como `bge0` o `e1000g0`. Otros nombres de controladores pueden ser `nge`, `nxge`, etcétera.

En esta versión de Oracle Solaris, el nombre de instancia del dispositivo sigue dependiendo del hardware subyacente. Sin embargo, los enlaces de datos que se encuentran por encima de estos dispositivos no se vinculan de manera similar y pueden tener nombres significativos. Por ejemplo, el administrador puede asignar al enlace de datos encima de la instancia del dispositivo `e1000g0` el nombre `itops0`. En esta versión de Oracle Solaris, los enlaces de datos predeterminados se proporcionan con nombres genéricos. Para mostrar la asignación entre los enlaces de datos con sus nombres genéricos y las correspondientes instancias del dispositivo, debe utilizar el subcomando `dladm sho -phys`.

Nombres de enlaces genéricos predeterminados

Cuando se instala esta versión de Oracle Solaris en un sistema por primera vez, Oracle Solaris proporciona automáticamente nombres de enlace genéricos para todos los dispositivos de red físicos del sistema. Esta asignación de nombre utiliza la convención de denominación `net #`, donde `#` es el número de instancia. Este número de instancia se incrementa para cada dispositivo, por ejemplo, `net0`, `net1`, `net2`, y así sucesivamente.

Los nombres de enlace genéricos o flexibles ofrecen ventajas en la configuración de red, como se muestra en los ejemplos siguientes:

- Dentro de un único sistema, la reconfiguración dinámica se hace más fácil. La configuración de red que se establece para una NIC determinada también puede ser heredada por un reemplazo de NIC diferente.
- La zona de migración se hace menos complicada con respecto a la configuración de red. La zona del sistema migrado conserva su configuración de red si el enlace del sistema de destino comparte el mismo nombre con el enlace que se ha asignado a la zona antes de la migración. Por lo tanto, no se requiere ninguna configuración de red adicional en la zona después de la migración.

- El esquema de denominación genérica ayuda con la configuración de red que se especifica en el manifiesto de la configuración del sistema (SC, System Configuration). Por lo general, el enlace de datos de red principal se llama `net0` en todos los sistemas. Por lo tanto, se puede usar un manifiesto SC genérico para varios sistemas que especifique una configuración para `net0`.
- La administración de enlaces de datos también se vuelve flexible. Puede personalizar aún más el nombre de los enlaces de datos, por ejemplo, para reflejar una función específica que realice el enlace de datos, como se muestra en la [Figura 1-2](#).

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

Hardware (NIC)	Instancia de dispositivo	Nombre asignado del enlace	Interfaz IP
e1000g	e1000g0	net0	net0
qfe	qfe1	net1	net1

Como la tabla lo indica, mientras que el nombre de la instancia del dispositivo permanece basado en hardware, el sistema operativo, una vez instalado, renombra los enlaces de datos.

Asignación de nombres genéricos a los enlaces de datos

En Oracle Solaris, los nombres genéricos se asignan automáticamente a todos los enlaces de datos en función de criterios específicos. Todos los dispositivos comparten el mismo prefijo `net`. Sin embargo, los números de instancia se asignan en función de lo siguiente:

- Los dispositivos de red físicos se ordenan según el tipo de medio físico, donde determinados tipos tienen prioridad sobre otros. Los tipos de medios se ordenan en prioridad descendente, como se indica a continuación:
 1. Ethernet
 2. IP sobre IB (dispositivos Infiniband)
 3. Ethernet sobre IB
 4. Wi-Fi
- Una vez que los dispositivos se agrupan y ordenan según los tipos de medios físicos, se vuelven a ordenar en función de sus ubicaciones físicas, donde los dispositivos integrados se prefieren a los dispositivos periféricos.
- A los dispositivos que tienen la mayor prioridad en función de su tipo de medio y ubicación se les asignan números de instancias inferiores.

Según los criterios, los dispositivos Ethernet en una placa base inferior o ioboard, hostbridge, complejo de raíz PCIe, bus, dispositivo y función se clasifican por delante de los demás dispositivos.

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

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

Personalización de la asignación de nombres de enlace genéricos

Oracle Solaris utiliza el prefijo `net` al asignar nombres de enlace. Sin embargo, puede usarse cualquier prefijo personalizado en su lugar; por ejemplo, `eth`. Si lo prefiere, también puede deshabilitar la asignación automática de nombres de enlace neutros.



Precaución – Debe personalizar el modo de asignación automática de nombres de enlace genéricos *antes* de instalar Oracle Solaris. Después de la instalación, no puede personalizar los nombres de enlace predeterminados sin que se modifiquen las configuraciones existentes.

Para deshabilitar la asignación de nombres de enlace automática, o para personalizar el prefijo de nombres de enlace, defina la siguiente propiedad en los manifiestos de configuración del sistema que utiliza el programa de instalación automática (AI, Automated Install).

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

De manera predeterminada, el valor para `phys-prefix` es `net`, como se ve en la parte resaltada de la salida.

- Para deshabilitar la denominación automática, elimine cualquier valor que se haya establecido para `phys-prefix`. Si deshabilita la denominación automática, los nombres de enlaces de datos se basan en sus controladores de hardware asociados, como `bge0`, `e1000g0`, etcétera.
- Para utilizar un prefijo distinto de `net`, especifique un nuevo prefijo como valor de `phys-prefix`; por ejemplo, `eth`.

Si el valor que se proporciona a `phys-prefix` no es válido, este será ignorado. A los enlaces de datos se les asigna un nombre según sus controladores de hardware asociados, como `bge0`, `e1000g0`, etcétera. Para conocer las reglas sobre nombres de enlace válidos, consulte [“Reglas para nombres de enlace válidos” en la página 31](#).

Nombres de enlace en sistemas actualizados

Automáticamente, en los sistemas en que la versión de Oracle Solaris está recién instalada, los enlaces de datos se denominan de `net0` a `netN-1`, donde `N` representa el número total de dispositivos de red.

Este caso no se cumple si se actualiza a partir de Oracle Solaris 11 Express. En estos sistemas actualizados, los enlaces de datos mantienen los nombres que tenían antes de la actualización. Estos nombres serán nombres basados en hardware predeterminados o nombres personalizados que el administrador asignó a los enlaces de datos antes de la actualización. Además, en estos sistemas modernizados, los dispositivos de red nuevos que se vayan agregando también conservarán los nombres basados en hardware predeterminados en lugar de recibir nombres neutros. Este comportamiento para sistemas actualizados garantiza que ningún nombre neutro asignado por el sistema operativo se mezcle con otros nombres basados en hardware o nombres personalizados que el administrador haya asignado antes de la actualización.

En cualquier sistema con esta versión de Oracle Solaris, tanto los nombres basados en hardware como los nombres de enlace proporcionados por el sistema operativo se pueden reemplazar por otros nombres que se prefieran. Normalmente, los nombres de enlace predeterminados que asigna el sistema operativo resultan suficientes para crear la red de configuración del sistema. Sin embargo, si elige cambiar nombres de enlace, tenga en cuenta las consideraciones importantes que se tratan en las siguientes secciones.

Reemplazo de nombres de enlace basados en hardware

Si los enlaces del sistema tienen nombres basados en hardware, cambie el nombre de estos enlaces por algún nombre genérico. Si mantiene los nombres basados en hardware de los enlaces, puede generarse confusión más adelante si los dispositivos físicos se eliminan o se reemplazan.

Por ejemplo, se mantiene el nombre de enlace `bge0` que se asocia con el dispositivo `bge0`. Todas las configuraciones de enlace se realizan estableciendo una referencia con el nombre de enlace. Más adelante, puede sustituir la NIC `bge` con la NIC `e1000g`. Para volver a aplicar la configuración de enlace del dispositivo anterior a la nueva NIC `e1000g0`, necesitaría reasignar el nombre de enlace `bge0` a `e1000g0`. La combinación de un nombre de enlace basado en hardware `bge0` con una NIC asociada diferente `e1000g0` puede crear confusión. Mediante el uso de nombres que no estén basados en hardware, puede distinguir mejor los enlaces de los dispositivos asociados.

Precaución sobre cómo cambiar los nombres de enlace

Cuando se vayan a reemplazar los nombres de enlace basados en hardware, se recomienda planificar detenidamente antes cambiar el nombre de los enlaces. El cambio del nombre de enlace del dispositivo no propaga automáticamente el nuevo nombre a todas las configuraciones asociadas. Los siguientes ejemplos ilustran los riesgos de cambiar los nombres de enlace:

- Algunas reglas de la configuración de filtros IP se aplican a enlaces específicos. Al cambiar el nombre de un enlace, las reglas de filtro siguen haciendo referencia al nombre original del enlace. Por lo tanto, estas reglas ya no se comportan según lo esperado después de cambiar el nombre del enlace. Debe ajustar las reglas de filtro para aplicarlas al enlace usando el nuevo nombre de enlace.
- Tenga en cuenta la posibilidad de exportar información de configuración de red. Como se explicó anteriormente, con el uso de los nombres predeterminados `net #` proporcionados por el sistema operativo, puede migrar las zonas y exportar la configuración de red a otro sistema fácilmente. Si los dispositivos de red del sistema de destino tienen nombres genéricos, como `net0`, `net1`, etcétera, la zona hereda implementa la configuración del enlace de datos cuyo nombre coincida con el enlace de datos asignado a la zona.

Por lo tanto, como regla general, no cambie los enlaces de datos de manera aleatoria. Cuando cambie el nombre de los enlaces de datos, asegúrese de que todas las configuraciones asociadas del enlace se sigan aplicando después de que se cambia el nombre del enlace. Algunas de las configuraciones que pueden verse afectadas por el cambio de nombre de los enlaces son las siguientes:

- Las reglas de filtro IP
- Las configuraciones IP que se especifican en los archivos de configuración, como `/etc/dhcp.*`
- Las zonas de Oracle Solaris 11
- La configuración `autopush`

Nota – No es necesario modificar la configuración autopush al cambiar el nombre de los enlaces. Sin embargo, debe saber cómo funcionaría la configuración con la propiedad autopush por enlace una vez que se haya cambiado el nombre del enlace. Para obtener más información, consulte “[Cómo establecer módulos STREAMS en enlaces de datos](#)” en la página 174.

Reglas para nombres de enlace válidos

Cuando asigne nombres de enlace, tenga en cuenta las siguientes reglas:

- Los nombres de enlace consisten de una cadena y un número de *punto físico de conexión* (PPA, *Physical Point of Attachment*).
- El nombre debe cumplir las siguientes restricciones:
 - Los nombres constan de entre 3 y 8 caracteres. Sin embargo, los nombres pueden tener un máximo de 16 caracteres.
 - Los caracteres válidos para los nombres son los caracteres alfanuméricos (a-z, 0-9) y el carácter de subrayado ('_').



Precaución – No utilice letras mayúsculas en los nombres de enlace.

- Cada enlace de datos debe tener solamente un nombre de enlace por vez.
- Cada enlace de datos debe tener un nombre de enlace único dentro del sistema.

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

La función de los enlaces dentro de la configuración de red puede servir como referencia útil al asignar nombres de enlace. Por ejemplo, `netmg0` puede ser un enlace que esté dedicado a la gestión de red. `upstream2` puede ser el enlace que se conecta al ISP. Como regla general, para evitar confusiones, *no* asigne nombres de dispositivos conocidos a sus enlaces.

Administración de otros tipos de enlaces

La separación entre la configuración de red y la configuración del hardware de red introduce la misma flexibilidad a otros tipos de configuraciones de enlaces. Por ejemplo, a las redes de área local virtuales (VLAN), las agregaciones de enlaces y los túneles IP se les pueden asignar nombres elegidos administrativamente, pero luego se les debe asignar una configuración que haga referencia a esos nombres. Otras tareas relacionadas, como efectuar la reconfiguración

dinámica (DR) para reemplazar dispositivos de hardware, también resultan más fáciles de realizar porque no es necesario reconfigurar más la red, siempre que la configuración de red no se haya suprimido.

La siguiente figura muestra la interrelación entre los dispositivos, los tipos de enlace y sus correspondientes interfaces.

Nota – En la figura, los enlaces de datos se nombran según las funciones específicas que realizan en el sistema, como `video0` o `sales2`. La figura tiene por objeto resaltar la flexibilidad con la que se puede asignar un nombre a los enlaces de datos. Sin embargo, se prefiere el uso de los nombres neutros predeterminados, como `net0`, según lo que proporciona el sistema operativo, que resultan suficientes.

La figura también proporciona un ejemplo de cómo se pueden usar los nombres seleccionados administrativamente en la configuración de red:

- VLAN configuradas en el enlace `net0`. A estas VLAN, a su vez, también se les asignan nombres personalizados, como `sales1` y `sales2`. La interfaz IP de la VLAN `sales2` está conectada y se encuentra en funcionamiento.
- Las instancias de dispositivos `qfe0` y `qfe2` se utilizan para dar el servicio de tráfico de video. En consecuencia, a los enlaces correspondientes de la capa del enlace de datos se les asignan los nombres `subvideo0` y `subvideo1`. Estos dos enlaces se agregan a la alimentación de video host. La agregación de enlaces también tiene su propio nombre personalizado: `video0`.
- Dos interfaces (`net0` y `net1`) con distinto hardware subyacente (`e1000g` y `qfe`) forman un grupo IPMP (`itops0`) con el tráfico de correo electrónico host.

Nota – Aunque las interfaces IPMP no son enlaces en la capa de enlace de datos, al igual que los enlaces, puede tener nombres personalizados. Para obtener más información sobre los grupos IPMP, consulte el [Capítulo 14, “Introducción a IPMP”](#).

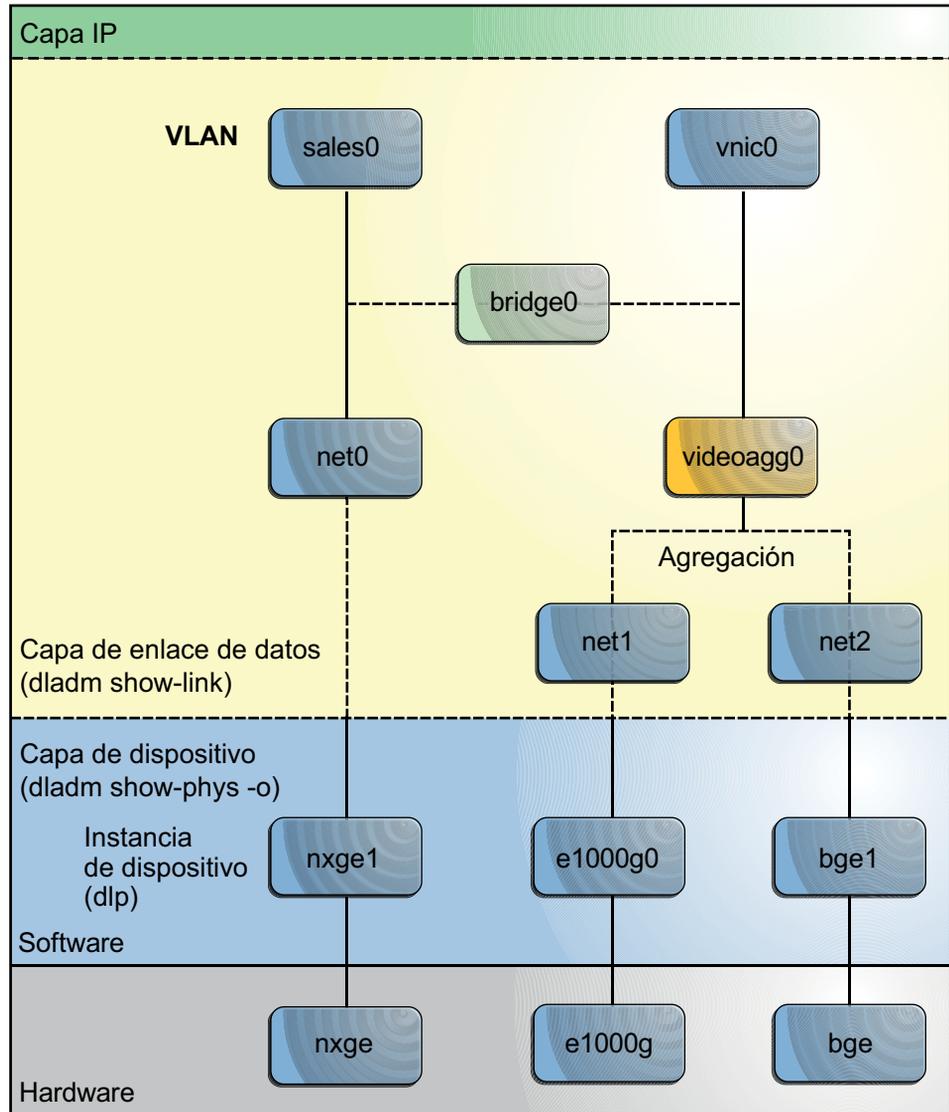
- Hay dos interfaces que no tienen dispositivos subyacentes: el túnel `vpn1`, que está configurado para conexiones VPN, y `lo0`, destinado para operaciones en bucle de retorno IP.

Todas las configuraciones de enlaces e interfaces que se muestran en esta figura son independientes de las configuraciones del hardware subyacente. Por ejemplo, si la tarjeta `qfe` se reemplaza, la configuración de interfaz `video0` para tráfico de video se mantiene y, más adelante, se puede aplicar a una NIC de reemplazo.

La siguiente figura muestra una configuración de puente. Hay dos interfaces (`net0` y `videoagg0`) que están configuradas como puente (`bridge0`). Los paquetes que se reciben en una

se envían a la otra. Después de efectuar la configuración de puente, ambas interfaces se siguen pudiendo utilizar para configurar las VLAN y las interfaces IP.

FIGURA 1-3 Puentes en la pila de red



P A R T E I

Conexión automática a la red (NWAM, Network Auto-Magic)

La conexión automática a la red es una función de Oracle Solaris que automatiza la configuración de red básica del sistema. En los temas que se tratan en estos capítulos, se describen los componentes de la arquitectura NWAM y el modo en que estos componentes funcionan juntos para llevar a cabo la configuración de red automatizada en el sistema Oracle Solaris.

Esta documentación se centra principalmente en cómo gestionar la configuración de red con las utilidades de la línea de comandos de NWAM. También se incluye información básica sobre cómo utilizar la interfaz gráfica de usuario de NWAM para ver y supervisar el estado de la red e interactuar con NWAM desde el escritorio. En la ayuda en pantalla, encontrará instrucciones detalladas sobre la supervisión y la gestión de la configuración de red con la interfaz gráfica de usuario de NWAM.

Introducción a NWAM

La función de conexión automática a la red (NWAM, Network Auto-Magic) simplifica la configuración de red básica mediante la ejecución automática de las configuraciones básicas de Ethernet y Wi-Fi, como la conexión a la red (con o sin cable) en el inicio y la visualización de notificaciones acerca del estado de la conexión de red activa desde el escritorio. Además, NWAM está diseñada para simplificar algunas de las tareas de red más complejas, como la creación y la gestión de perfiles de red en todo el sistema; por ejemplo, la configuración de los servicios de nombres, el filtro IP y la seguridad IP (IPsec), que son todas funciones de Oracle Solaris.

En este capítulo, se tratan los siguientes temas:

- “¿Qué es la configuración NWAM?” en la página 38
- “Cuándo se utiliza NWAM” en la página 40
- “Cómo funciona la configuración NWAM” en la página 41
- “Cómo funciona NWAM con otras tecnologías de red de Oracle Solaris” en la página 42
- “Dónde encontrar las tareas de configuración de red” en la página 44

Este capítulo está dirigido a los usuarios y administradores de sistemas que tengan conocimientos básicos sobre conceptos de red y algo de experiencia en la gestión de configuración de red con comandos y herramientas de red tradicionales. Si está preparado para usar NWAM para gestionar su configuración de red, vaya al [Capítulo 4](#), “Configuración de perfiles de NWAM (tareas)”.

Para obtener información básica sobre la administración de interfaces de red en Oracle Solaris, consulte la [Parte II](#).

¿Qué es la configuración NWAM?

La configuración NWAM consta de varios componentes que trabajan conjuntamente para efectuar la configuración de red de un sistema de la manera más automatizada posible. Con la movilidad como objetivo principal, NWAM es capaz de cambiar dinámicamente la configuración del sistema en respuesta a diferentes eventos de red o ante la solicitud de un usuario. NWAM incluye capacidades dinámicas que se encargan de los cambios en las condiciones de red; por ejemplo, si la interfaz de red con cables se convierte en una interfaz inalámbrica o si una nueva red inalámbrica se pone disponible.

La configuración de red mediante NWAM consta de propiedades con sus valores asociados a diferentes tipos de perfiles, que a veces son denominados *objetos de configuración*.

Estos perfiles y objetos de configuración incluyen lo siguiente:

- **Perfiles de configuración de red (NCP, Network Configuration Profiles)**

Un NCP especifica la configuración de los enlaces de red y las interfaces. Este perfil es uno de los principales tipos de perfil que componen la configuración NWAM. El segundo tipo de perfil principal es el perfil de ubicación.

El sistema siempre define un NCP denominado NCP automático. Este NCP se activa cuando no hay entradas del usuario. El sistema crea y mantiene el NCP automático, que no se puede modificar ni eliminar.

También se pueden crear NCP definidos por el usuario según sea necesario. Para obtener una descripción completa de los NCP automáticos y los definidos por el usuario, consulte [“Descripción de NCP automáticos y NCP definidos por el usuario” en la página 50](#).

- **Unidades de configuración de red (NCU, Network Configuration Units)**

Las NCU son objetos de configuración individual que contienen todas las propiedades que conforman un NCP. El NCP es, básicamente, un contenedor que almacena las NCU que lo definen. Cada NCU se correlaciona con una interfaz o un enlace individual en el sistema. Para obtener una descripción completa de las NCU, consulte [“Descripción de una NCU” en la página 49](#).

- **Ubicaciones**

El perfil de ubicación es uno de los dos principales tipos de perfil que conforman la configuración NWAM. La ubicación especifica la configuración de red de todo el sistema; por ejemplo, los servicios de nombres, el dominio, el filtro IP y la configuración de IPsec. Esta información tiene un conjunto de propiedades que se aplican a la configuración de red de todo el sistema. Hay ubicaciones definidas por el sistema y ubicaciones definidas por el usuario. Para obtener una descripción completa del perfil de ubicación, consulte [“Descripción de un perfil de ubicación” en la página 50](#).

- **Modificadores de red externos (ENM, External Network Modifiers)**

Los ENM son perfiles que se utilizan para gestionar aplicaciones que sean ajenas a NWAM; por ejemplo la aplicación VPN. Estas aplicaciones pueden modificar y crear configuraciones de red. El daemon `nwamd` activa y desactiva un ENM dependiendo de las condiciones que se especifican como parte del ENM. Para obtener una descripción completa de un ENM, consulte [“Descripción de un ENM” en la página 51](#).

- **Redes de área local inalámbricas (WLAN, Wireless Local Area Networks) conocidas**

Las WLAN conocidas son objetos de configuración que NWAM utiliza para supervisar y almacenar información sobre las redes inalámbricas que son conocidas para el sistema. NWAM lleva una lista de todas estas redes inalámbricas y, luego, hace referencia a esta lista para determinar el orden en el que se intenta establecer las conexiones a redes inalámbricas disponibles. Para obtener una descripción completa de las WLAN conocidas, consulte [“Acerca de las WLAN conocidas” en la página 52](#).

Componentes funcionales de NWAM

NWAM consta de los siguientes componentes funcionales:

- **Depósito de perfiles NWAM:** el depósito de perfiles es donde se almacenan los datos de configuración de NWAM. El acceso al depósito de perfiles se gestiona con el daemon del depósito, `netcfgd`.
El depósito de perfiles NWAM incluye una instantánea de la configuración de red con NWAM habilitada. Estos datos se preservan por si es necesario volver a usar la configuración manual de la red. Para obtener más información, consulte [“Datos de configuración de NWAM” en la página 53](#).
- **Programas de configuración de perfiles (interfaces de usuario):** la arquitectura de NWAM incluye tanto una interfaz de línea de comandos (CLI) como una interfaz gráfica de usuario (GUI). Estas interfaces se pueden utilizar para realizar tareas similares, como crear y modificar perfiles, activar perfiles, y consultar en el sistema la información sobre los perfiles.

La CLI de NWAM consta de dos comandos administrativos: `netcfg` y `netadm`. El comando `netcfg` permite crear y modificar perfiles. Este comando funciona en modo interactivo, en modo de línea de comandos y en modo de archivo de comandos. El comando `netadm` permite realizar algunas acciones, como la habilitación o la deshabilitación de un perfil o el listado de información sobre los estados del perfil. Para obtener más información, consulte las páginas del comando `man netcfg(1M)` y `netadm(1M)`.

Para obtener instrucciones paso a paso sobre la creación y la gestión de perfiles con la CLI de NWAM, consulte el [Capítulo 4, “Configuración de perfiles de NWAM \(tareas\)”](#) y el [Capítulo 5, “Administración de perfiles de NWAM \(tareas\)”](#).

La GUI de NWAM también se puede utilizar para crear y gestionar los perfiles de red. La GUI tiene funciones adicionales que permiten visualizar y supervisar rápidamente el estado de las conexiones de red desde el escritorio. La GUI también tiene una función de notificación que alerta sobre los cambios realizados en el estado actual de la red. La función de notificación está disponible solamente en la GUI. Para obtener más información sobre el

uso de la GUI de NWAM, consulte el [Capítulo 6, “Acerca de la interfaz gráfica de usuario de NWAM”](#) o la ayuda en pantalla. También puede consultar las páginas del comando `man nwammgr(1M)` y `nwammgr-properties(1M)`.

- **Daemon de motor de políticas:** el daemon `nwamd` es el componente de política de NWAM. Este daemon funciona en varios roles y gestiona la configuración de red basada en los perfiles que se almacenan en el depósito de perfiles. El daemon determina qué perfil debe activarse según las condiciones de red actuales y lo activa. Para realizar esta tarea, el daemon integra información de varias fuentes. Los distintos roles que cumple el daemon `nwamd` se describen en detalle, en la sección [“Descripción general de los daemons NWAM” en la página 71](#).
- **Daemon de depósito:** el daemon `netcfgd` controla el depósito de perfiles común que almacena todos los datos de configuración de los perfiles y otros objetos de configuración. El comando `netcfg`, la GUI de NWAM y el daemon `nwamd` interactúan con el daemon `netcfgd` mediante el envío de solicitudes para acceder al depósito de perfiles. El trabajo del daemon de depósito consiste en comprobar si los distintos procesos que intentan acceder a los datos del depósito tienen las autorizaciones correctas. El daemon prohíbe (hace fallar) cualquier intento de acceso de procesos no autorizados. Para obtener más información, consulte [“Descripción del daemon de depósito NWAM \(netcfgd\)” en la página 72](#).
- **Interfaz de biblioteca de NWAM:** la biblioteca `libnwam` proporciona una interfaz funcional para interactuar con el depósito de perfiles, habilitando así la información sobre los perfiles que NWAM debe leer y modificar.
- **Servicios de red de la utilidad de gestión de servicios (SMF):** varios de los servicios de red que usa NWAM ya forman parte de Oracle Solaris. Sin embargo, algunos de estos servicios existentes se han modificado, y se han introducido nuevos servicios que son específicos de NWAM. Para obtener más información, consulte [“Servicios de red SMF” en la página 72](#).

Cuándo se utiliza NWAM

Por lo general, si cambia los entornos de trabajo y los métodos de conexión con frecuencia (con cables o inalámbrico), querrá beneficiarse con las capacidades de configuración de red automática de NWAM. Puede utilizar NWAM para configurar los perfiles definidos por el usuario que le permiten conectarse a las redes en distintas situaciones, por ejemplo, en la oficina, en su hogar o cuando esté de viaje. NWAM es una herramienta valiosa para los usuarios de sistemas y modelos de equipos portátiles que requieran cambios frecuentes en los entornos de red. Además, la GUI de NWAM hace que sea mucho más fácil establecer las configuraciones y las conexiones de IP estática con redes Wi-Fi que con los comandos y las herramientas de red tradicionales.

NWAM se pueden configurar para adaptarse a los cambios en el entorno de red, por ejemplo, en el caso de pérdida de conectividad Ethernet o adición o eliminación de una tarjeta de interfaz de red (NIC).

Nota – Puede optar por configurar su red manualmente, por ejemplo, si está utilizando funciones de red avanzadas que NWAM no admite. Para obtener más información, consulte [“Gestión de configuración de red” en la página 111](#).

Cómo funciona la configuración NWAM

El comportamiento predeterminado de NWAM sirve para realizar operaciones básicas de configuración de una red con cables o inalámbrica "automáticamente", sin ningún tipo de interacción con el usuario. El usuario debe interactuar con NWAM únicamente si el sistema le pide más información, por ejemplo, para proporcionar una clave o contraseña de seguridad para una red inalámbrica.

La configuración NWAM automatizada se inicia con los siguientes eventos y actividades:

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

Los componentes NWAM interactúan entre sí de la siguiente manera:

- En todo momento, un NCP y un perfil de ubicación deben estar activos en el sistema.
- Durante el inicio del sistema, el daemon de motor de políticas, `nwamd`, realiza las siguientes acciones:
 1. Consulta la propiedad de servicio para el NCP que se encuentra activo
 2. Continúa en ejecución hasta que una o más direcciones IP se hayan configurado
 3. Comprueba las condiciones de los perfiles de ubicación
 4. Activa el perfil de ubicación especificado por el motor de políticas
 5. Configura la red, o las redes, según corresponda
- A medida que suceden los eventos que podrían generar un cambio en la configuración de red, el daemon de NWAM, `nwamd`, funciona en distintos roles y realiza las siguientes operaciones:
 1. Como manejador de eventos, `nwamd` detecta cada evento que ocurre.
 2. Como daemon de perfil, `nwamd` consulta el perfil activo.
 3. Según el cambio, `nwamd` puede volver a configurar la red, o las redes, según corresponda.

Comportamiento predeterminado de NWAM

Si no hay perfiles de red definidos por el usuario, `nwamd` gestiona la configuración de red en función de los siguientes tres perfiles definidos por el sistema:

- NCP automático
- Ubicación Automatic
- Ubicación NoNet

El NCP automático implementa la siguiente política básica:

- Se configuran todas las interfaces Ethernet disponibles (conectadas) mediante DHCP.
- Si no hay interfaces Ethernet conectadas, o si ninguna puede obtener una dirección IP, se activa una interfaz inalámbrica que automáticamente establece una conexión con las mejores WLAN disponibles de la *lista de WLAN conocidas*. Si no, se espera a que el usuario seleccione una red inalámbrica para conectarse.
- Se obtiene al menos una dirección IPv4. La ubicación NoNet permanece activa. Este perfil de ubicación proporciona un conjunto estricto de las reglas de filtro IP que sólo transfieren datos que sean relevantes para la adquisición de direcciones IP (mensajes `autoconf` DHCP e IPv6). Todas las propiedades de la ubicación NoNet, a excepción de las condiciones de activación, se pueden modificar.
- Cuando se haya asignado al menos una dirección IPv4 a una de las interfaces del sistema, la ubicación Automatic estará activada. Este perfil de ubicación no tiene Filtro IP ni reglas de IPsec. El perfil de ubicación aplica datos de configuración de DNS que se obtienen del servidor DHCP. Al igual que con la ubicación NoNet, todas las propiedades de la ubicación Automatic, con la excepción de sus condiciones de activación, pueden modificarse.
- La ubicación NoNet siempre se aplica cuando el sistema no tiene direcciones IPv4 asignadas para ella. Cuando hay al menos una dirección IPv4 asignada, el sistema selecciona el perfil de ubicación con las reglas de activación que mejor coincidan con las condiciones de red actuales. Si no hay una coincidencia adecuada, el sistema vuelve a la ubicación Automatic. Para obtener más información, consulte [“Activación de los perfiles NWAM” en la página 58](#).

Cómo funciona NWAM con otras tecnologías de red de Oracle Solaris

NWAM funciona con las siguientes tecnologías de red de Oracle Solaris:

- **Virtualización de redes**

NWAM funciona con las distintas tecnologías de virtualización de redes de Oracle Solaris, como se indica a continuación:

- **Máquinas virtuales: Oracle VM Server para SPARC (anteriormente, Logical Domains) y Oracle VM VirtualBox**

NWAM se admite en hosts y clientes de Oracle Solaris. NWAM gestiona solamente las interfaces que pertenecen a las máquinas virtuales especificadas y no interfieren con otras máquinas virtuales.

- **Instancias de pila y zonas de Oracle Solaris**

NWAM funciona en las zonas globales o una zona no global de pila exclusiva.

Nota – NWAM no funciona en zonas de pila compartidas.

- **VNIC**

Aunque la implementación actual de NWAM no gestiona VNIC, las VNIC creadas manualmente persisten tras los reinicios y se pueden crear, por ejemplo, para la asignación a una zona de pila exclusiva.

- **Tecnología de establecimiento de puentes**

La tecnología de establecimiento de puentes es un método para conectar segmentos de red independientes a fin de habilitar las comunicaciones entre los nodos conectados, como si se estuviera usando solamente un único segmento. Aunque la implementación actual de NWAM no admite activamente las configuraciones de red que utilizan la tecnología de establecimiento de puentes, no es necesario deshabilitar la gestión de configuración NWAM antes de utilizar esta tecnología en el sistema.

- **Reconfiguración dinámica y perfiles de configuración de red**

En los sistemas que admiten la reconfiguración dinámica (DR, Dynamic Reconfiguration) y las capacidades de conexión en caliente, estas funciones se utilizan directamente sólo si el NCP activo en los sistemas es `DefaultFixed`.

Si el NCP habilitado en estos sistemas es `Automatic` o cualquier otro NCP creado por el usuario, antes de realizar cualquier operación de DR, primero debe realizar uno de los siguientes pasos:

- Detenga el servicio de red. Esta acción desactiva todas las interfaces de red del sistema. Por lo tanto, debe utilizar la consola del sistema para detener el servicio. Después de haber eliminado o reemplazado el dispositivo, reinicie el servicio.
- Elimine la interfaz IP de la configuración de ese NCP activo con el comando `netcfg`. A continuación, puede reemplazar o retirar físicamente el dispositivo de hardware subyacente de esa interfaz IP. Si corresponde, vuelva a configurar la interfaz IP una vez finalizada la DR.

- **Utilidades y comandos de red tradicionales**

En cualquier momento, el sistema utiliza la configuración de red tradicional o la configuración de red NWAM. Si se habilita el NCP `DefaultFixed`, el sistema utiliza la configuración de red tradicional. El sistema aplica la configuración persistente que se almacena en los archivos `/etc/ipadm/ipadm.conf` y `/etc/dladm/datalink.conf` cuando este NCP está habilitado. Además, puede utilizar los comandos `ipadm` y `dladm` para ver y modificar la configuración de red. Si un NCP de NWAM está habilitado, el sistema ignora la configuración `/etc/ipadm/ipadm.conf`, y NWAM gestiona la configuración de red de acuerdo con la política especificada en el NCP activo.

Cuando NWAM gestiona la configuración de red, igual puede emplear las utilidades de red de la línea de comandos, `dladm` y `ipadm`, para ver los componentes de la configuración de redes actual.

Nota – No se admite la realización de cambios a la configuración de red con herramientas de la línea de comando, ya que esos cambios pueden entrar en conflicto con la política que aplica NWAM.

- **Rutas múltiples de redes IP (IPMP, IP Network Multipathing)**

Actualmente, NWAM no admite el uso de las IPMP. Antes de configurar la red para utilizar IPMP, asegúrese de que el NCP `DefaultFixed` se encuentre habilitado.

Dónde encontrar las tareas de configuración de red

La siguiente tabla lista los temas de configuración de red y dice dónde se puede obtener más información.

Tarea de redes	Para obtener más información
Buscar información general detallada sobre NWAM.	Capítulo 3, “Configuración y administración de NWAM (descripción general)”
Crear, modificar y eliminar perfiles y objetos de configuración mediante la CLI de NWAM.	Capítulo 4, “Configuración de perfiles de NWAM (tareas)”
Ver información sobre los perfiles y los objetos de configuración, y administrarlos mediante la CLI de NWAM.	Capítulo 5, “Administración de perfiles de NWAM (tareas)”
Ver información sobre el estado de la red, cambiar las conexiones de red y crear y modificar perfiles y objetos de configuración mediante la GUI de NWAM desde el escritorio.	Capítulo 6, “Acerca de la interfaz gráfica de usuario de NWAM” y la ayuda en pantalla

Tarea de redes	Para obtener más información
Cambiar entre el modo de configuración de red de NWAM y el modo de configuración de red tradicional.	“Gestión de configuración de red” en la página 111
Gestionar la configuración de red utilizando comandos y herramientas de red tradicionales.	Capítulo 8, “Configuración y administración de enlaces de datos” y Capítulo 9, “Configuración de una interfaz IP”
Configurar y gestionar redes virtuales.	Capítulo 17, “Introducción a la virtualización de redes y el control de recursos (descripción general)”

Configuración y administración de NWAM (descripción general)

En este capítulo se proporciona información de contexto e información general sobre el proceso de configuración y administración de NWAM. También se proporciona una descripción detallada de la implementación de perfiles que utiliza NWAM para simplificar y automatizar la configuración de red.

En este capítulo, se tratan los siguientes temas:

- “Descripción general de la configuración de NWAM” en la página 47
- “Datos de configuración de NWAM” en la página 53
- “Activación de los perfiles NWAM” en la página 58
- “Perfiles de configuración mediante el comando `netcfg`” en la página 63
- “Administración de perfiles mediante el comando `netadm`” en la página 69
- “Descripción general de los daemons NWAM” en la página 71
- “Servicios de red SMF” en la página 72
- “Descripción general de la seguridad de NWAM” en la página 73

Descripción general de la configuración de NWAM

NWAM gestiona la configuración de red mediante el almacenamiento de valores de propiedad preferidos como perfiles en el sistema. Entonces NWAM determina qué perfil se debe activar, según las condiciones actuales de la red y, posteriormente, lo activa. La implementación de perfiles NWAM es un componente principal de NWAM.

¿Qué son los perfiles de red?

Los perfiles de red son recopilaciones de propiedades que determinan el modo en que se configura y funciona la red según las condiciones actuales de la red.

Los siguientes son los tipos de perfil y los objetos de configuración que componen la configuración de NWAM:

- Perfiles de configuración de red (NCP)
- Perfiles de ubicación
- Modificadores de red externos (ENM)
- Redes de área local inalámbricas (WLAN) conocidas

Los dos tipos principales de perfiles de red son NCP y el perfil de ubicación. Para efectuar la configuración automática de la red a través de NWAM, debe haber exactamente un NCP y un perfil de ubicación activos en el sistema en todo momento.

El NCP especifica la configuración de la red local, incluida la configuración de los componentes individuales, como los enlaces físicos y las interfaces IP. Cada NCP consta de objetos de configuración individuales que se denominan *unidades de configuración de red* (NCU). Cada NCU representa un enlace físico o una interfaz y está compuesto por propiedades que definen la configuración de ese enlace o interfaz. El proceso de configuración de un NCP definido por el usuario implica la creación de NCU para ese NCP. Para obtener más información, consulte [“Descripción de una NCU” en la página 49](#).

Un perfil de ubicación contiene información de configuración de red de todo el sistema, como la siguiente:

- Condiciones en las cuales se activa el perfil de ubicación
- Qué servicio de nombres se debe utilizar
- Nombre de dominio
- Conjunto de reglas de filtro IP
- Política IPsec

Para obtener más información, consulte [“Descripción de un perfil de ubicación” en la página 50](#).

Los ENM son perfiles NWAM para las aplicaciones externas que son capaces de crear y modificar la configuración de la red. Se puede configurar NWAM para activar y desactivar estas aplicaciones externas en las condiciones que haya especificado al crear el ENM.

Las WLAN conocidas son perfiles NWAM que se utilizan para mantener una lista de redes inalámbricas conocidas a las que se ha conectado anteriormente. Para obtener más información, consulte [“Descripción de un ENM” en la página 51](#) y [“Acerca de las WLAN conocidas” en la página 52](#).

Descripción de un NCP

Un NCP define la configuración de red de un sistema. Las NCU que conforman un NCP especifican cómo configurar los distintos enlaces e interfaces de red, por ejemplo, qué interfaz o interfaces se deben traer adelante y en qué condiciones, así como la manera en que se obtiene la

dirección IP para la interfaz. Hay dos tipos de NCP: automático y definido por el usuario. Un NCP automático es un perfil definido por el sistema creado automáticamente por NWAM. Este perfil no se puede crear, modificar ni eliminar. Los NCP definidos por el usuario son perfiles que el usuario puede crear para satisfacer las necesidades de su configuración de red particular. Un NCP definido por el usuario puede ser modificado y eliminado por el usuario.

El NCP automático es una representación de todos los enlaces y las interfaces que se encuentran actualmente en el sistema. El contenido del NCP automático cambia si se agregan o eliminan dispositivos de red. Sin embargo, las preferencias de configuración que están asociadas con el NCP automático no se pueden editar. El NCP automático se crea para proporcionar acceso a un perfil que utiliza DHCP y configuración automática de direcciones que hacen posible la obtención de direcciones IP para el sistema. Este perfil también implementa una política de selección de enlaces que favorece los enlaces con cables por sobre los enlaces inalámbricos. Si se requiere que se especifique una política de configuración de IP alternativa, o una política de selección de enlace alternativa, se crearían NCP adicionales definidos por el usuario en el sistema.

Descripción de una NCU

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

Hay dos tipos de NCU:

- **NCU de enlace**

Las NCU de enlace, por ejemplo, los dispositivos físicos, son entidades de capa 2 en el modelo OSI (de interconexión de sistemas abiertos).

- **NCU de interfaz**

Las NCU de interfaz, en concreto las interfaces IP, son entidades de capa 3 en el modelo OSI.

Las NCU de enlace representan enlaces de datos. Existen diferentes clases de enlaces de datos:

- Enlaces físicos (Ethernet o Wi-Fi)
- Túneles
- Agregaciones
- Redes de área local virtual (VLAN)
- Tarjetas de la interfaz de red virtual (VNIC)

Nota – La implementación actual de NWAM incluye *solamente* compatibilidad para la configuración básica de red de los enlaces físicos (Ethernet y Wi-Fi). Varias tecnologías de red avanzadas, como las VNIC y el establecimiento de puentes, se pueden configurar en la red sin tener que deshabilitar la gestión de configuración de NWAM, aunque no sean activamente compatibles con NWAM.

Sin embargo, si configura el sistema para utilizar rutas múltiples de red IP (IPMP), no puede utilizar la gestión de configuración de NWAM. Debe utilizar la configuración de red tradicional. Para obtener instrucciones, consulte [“Cómo cambiar del modo de configuración de red automático al modo de configuración de red manual” en la página 111](#).

Descripción de NCP automáticos y NCP definidos por el usuario

Un NCP automático es un perfil definido por el sistema que está formado por una NCU de enlace y una NCU de interfaz por cada enlace físico presente en el sistema. La política de activación de NCU en este NCP es preferir los enlaces conectados con cable por sobre los enlaces inalámbricos, y conectar IPv4 e IPv6 en cada enlace habilitado. DHCP se utiliza para obtener las direcciones IPv4. Para obtener las direcciones IPv6, se utiliza configuración automática y DHCP sin estado. El NCP automático cambia de forma dinámica cuando se insertan o se eliminan nuevos enlaces en el sistema. Todas las NCU que corresponden al enlace insertado o eliminado también se agregan o eliminan al mismo tiempo. El daemon `nwamd` actualiza automáticamente el perfil.

Los NCP definidos por el usuario son creados y gestionados por el usuario. Debe agregar o eliminar de forma explícita las NCU desde el perfil especificado. Puede crear NCU que no tengan una correlación con ningún enlace que esté actualmente presente en el sistema. También puede eliminar NCU que no tengan ninguna correlación con ningún enlace presente en el sistema. Asimismo, puede determinar la política para el NCP definido por el usuario. Por ejemplo, puede permitir la habilitación de varios enlaces e interfaces en el sistema en un momento determinado, así como especificar diferentes relaciones de dependencia entre las NCU y las direcciones IP estáticas.

Para obtener instrucciones paso a paso sobre la creación de NCP definidos por el usuario y la adición y eliminación de NCU en este NCP, consulte [“Creación de un NCP” en la página 80](#).

Descripción de un perfil de ubicación

Un perfil de ubicación proporciona detalles de red adicionales después de establecer la conectividad IP básica. Las ubicaciones contienen información de configuración de red que se compone de un conjunto de propiedades que se relacionan con la configuración de red en el nivel del sistema.

Un perfil de ubicación se compone de determinada información de configuración de red, por ejemplo, servicio de nombres y configuración de cortafuegos, que se aplican en conjunto cuando es necesario. También, como una ubicación no necesariamente se corresponde a una ubicación física, puede configurar varios perfiles de ubicación para que satisfagan diferentes necesidades de redes. Por ejemplo, se puede usar una ubicación cuando está conectado a la intranet de la empresa. Se puede usar otra ubicación cuando está conectado a la red pública de Internet mediante un punto de acceso inalámbrico situado en la oficina.

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

- **NoNet**

La ubicación NoNet tiene condiciones de activación muy específicas. NWAM aplica este perfil para un sistema independiente cuando ninguna interfaz local tiene una dirección IP asignada. Puede modificar la ubicación NoNet después de activarla en el sistema por primera vez. En el sistema se almacena una copia de sólo lectura de la ubicación NoNet original en caso de que desee restaurar los valores predeterminados de esta ubicación.

- **Automatic**

La ubicación Automatic se activa si hay redes disponibles, pero ningún otro perfil de ubicación la reemplaza. Puede modificar la ubicación Automatic después de haberla activado en su sistema por primera vez. En el sistema se almacena una copia de sólo lectura de la ubicación Automatic original en caso de que desee restaurar los valores predeterminados de esta ubicación.

Nota – La ubicación Automatic no se debe confundir con el NCP automático. La ubicación Automatic es un tipo de perfil de ubicación que define propiedades de red de todo el sistema después de la configuración de red inicial de un sistema. El NCP automático especifica la configuración de enlace e interfaz en un sistema.

Las ubicaciones definidas por el usuario son perfiles que crea con valores que especifica para la configuración de red de todo el sistema. Las ubicaciones definidas por el usuario son idénticas a las ubicaciones definidas por el sistema, con excepción de que una ubicación definida por el usuario se configura con los valores que establece, mientras que las ubicaciones definidas por el sistema tiene valores preestablecidos.

Para obtener más información sobre la creación de ubicaciones definidas por el usuario, consulte [“Creación de un perfil de ubicación” en la página 87](#).

Descripción de un ENM

Los ENM son perfiles que pertenecen a las aplicaciones externas a NWAM. Estas aplicaciones pueden crear y modificar la configuración de red. Los ENM se incluyen en el diseño NWAM como una forma de crear y eliminar una configuración de red personalizada que no es un NCP

o un perfil de ubicación. Un ENM también se puede definir como un servicio o aplicación que modifica directamente la configuración de red cuando está habilitada o deshabilitada. Puede configurar NWAM para activar y desactivar ENM en las condiciones que especifique. A diferencia de un NCP o un perfil de ubicación, en los que sólo puede haber un tipo de perfil activo en el sistema en un momento determinado, pueden llegar a estar activos varios ENM en el sistema al mismo tiempo. Los ENM que están activos en un sistema en un momento determinado no dependen necesariamente del NCP o el perfil de ubicación habilitado en el sistema al mismo tiempo.

Aunque hay varias aplicaciones y servicios externos para los que puede crear un ENM, el ejemplo obvio es la aplicación VPN. Después de instalar y configurar una VPN en el sistema, puede crear un ENM que active y desactive automáticamente la aplicación en las condiciones que especifique.

Nota – Es importante comprender que NWAM no tienen la capacidad de obtener información automáticamente sobre las aplicaciones externas que son capaces de modificar directamente la configuración de red en un sistema. Para gestionar la activación o desactivación de una aplicación VPN, o de cualquier aplicación o servicio externos, primero debe instalar la aplicación y, luego, puede crear un ENM para ella mediante la interfaz de línea de comandos o la interfaz gráfica de usuario de NWAM.

NWAM no almacena ni realiza seguimiento de la información persistente sobre cualquier configuración de red que se lleva a cabo por medio de un ENM exactamente de la misma forma en que almacena la información sobre un NCP o un perfil de ubicación. Sin embargo, NWAM es capaz de notar una configuración de red iniciada de forma externa y, luego, en función de los cambios de configuración realizados al sistema por un ENM, volver a evaluar qué perfil de ubicación debe estar activo y, posteriormente, activar esa ubicación. Un ejemplo sería pasar a una ubicación activada condicionalmente cuando cierta dirección IP está en uso. Si el servicio `svc:/network/physical:default` se reinicia en cualquier momento, se restablece la configuración de red especificada por el NCP activo. Los ENM también se reinician, y posiblemente anulan y recrean la configuración de red en el proceso.

Para obtener información sobre la creación y modificación de las propiedades de un ENM, consulte [“Creación de un perfil de ENM” en la página 93](#).

Acerca de las WLAN conocidas

Las WLAN conocidas son los objetos de configuración que utiliza NWAM para gestionar las redes inalámbricas conocidas en el sistema. NWAM mantiene una lista global de estas redes inalámbricas conocidas. Esta información se utiliza entonces para determinar el orden en el que NWAM intenta conectarse a las redes inalámbricas disponibles. Si una red inalámbrica que existe en la *lista de WLAN conocidas* está disponible, NWAM automáticamente se conecta a esa red. Si hay dos o más redes inalámbricas conocidas disponibles, NWAM intenta conectarse a la

red inalámbrica con la prioridad más alta (número menor). Cualquier red inalámbrica nueva a la que NWAM se conecte se agrega automáticamente a la parte superior de la lista de WLAN conocidas y se convierte en la red inalámbrica con la prioridad más alta.

Las WLAN conocidas se seleccionan en orden de prioridad; la prioridad es asignada por un número entero no firmado. Un número inferior indica una prioridad mayor en la lista de WLAN conocidas. La primera vez que se conecta a una red inalámbrica, NWAM automáticamente agrega esa WLAN a la lista. Cuando se agrega una WLAN nueva, asume la prioridad más alta en esta lista. El comportamiento predeterminado de NWAM es preferir las WLAN a las que se haya conectado más recientemente por sobre las WLAN anteriores. En ningún momento más de una WLAN conocida pueden compartir la misma prioridad. Si se agrega una nueva WLAN a la lista con el mismo valor de prioridad que una WLAN ya existente, la entrada existente se desplaza hacia una prioridad de valor inferior. Después, el valor de prioridad de cada otra WLAN de la lista se cambia dinámicamente a una prioridad de valor inferior.

También es posible asociar uno o más nombres de clave con una WLAN conocida. Los *nombres de clave* le permiten crear sus propias claves mediante el comando `dladm create -secobj`. Puede asociar estas claves con las WLAN si agrega los nombres de objeto seguro a la propiedad `keyname` de las WLAN conocidas. Para obtener más información, consulte la página del comando `man dladm(1M)`.

Para obtener más información sobre el uso de las utilidades de línea de comando de NWAM para gestionar las WLAN, consulte [“Realización de un análisis inalámbrico y conexión a redes inalámbricas disponibles” en la página 119.](#)

Datos de configuración de NWAM

Hay efectivamente dos depósitos de configuración en el sistema: el depósito de perfiles NWAM, que se almacena en el directorio `/etc/nwam` y el depósito de configuración tradicional, que incluye los archivos `/etc/ipadm/ipadm.conf` y `/etc/dladm/datalink.conf`, así como otros archivos de configuración que están asociados con los servicios de red.

Cuando NWAM gestiona la configuración de la red, funciona principalmente desde su propio depósito. La configuración de la interfaz que se almacena en el archivo `/etc/ipadm/ipadm.conf` se ignora. NWAM configura enlaces físicos e interfaces directamente según los datos del NCP.

Los datos del perfil de ubicación se leen desde el depósito del perfil NWAM. Cuando una ubicación está activada, esta configuración se aplica al sistema en ejecución en la mayoría de los casos mediante la fijación de las propiedades de servicio SMF apropiadas y el reinicio de los servicios pertinentes a fin de aplicar los cambios de configuración. Esta acción sobrescribe los valores existentes para esas propiedades del servicio.

Debido a que NWAM sobrescribe los datos de configuración heredados en el proceso de aplicación de perfiles de ubicación, al inicio, se guarda cualquier configuración que pueda llegar a sobrescribirse. Al cerrar, NWAM restaura dicha configuración. Aunque no es una ubicación que pueda aplicarse como parte de la operación de NWAM, estos datos se denominan *datos de ubicación heredada*.

Los valores de propiedad para los siguientes perfiles de red definidos por el sistema y por el usuario se almacenan en el depósito de NWAM:

- NCP: contiene los valores para el NCP automático, así como cualquier NCP definido por el usuario.
- NCU: contiene valores para las NCU de enlace y de interfaz.
- Ubicaciones: contiene valores para los tres tipos de ubicaciones definidas por el sistema, además de valores para cualquier ubicación definida por el usuario.
- ENM: contiene información acerca de las aplicaciones.
- WLAN conocidas: contiene información sobre las redes inalámbricas a las que puede conectarse automáticamente.

Los datos de configuración para cada NCP se almacenan de manera persistente como un archivo en el directorio `/etc/nwam`, con el formato, `ncp-nombre`. Hay un archivo por NCP, con las entradas que representan a cada NCU. Por ejemplo, el archivo para el NCP automático se denomina `ncp-Automatic.conf`. Todos los archivos del NCP se almacenan en el directorio `/etc/nwam`.

Las propiedades de ubicación se almacenan en el archivo `/etc/nwam/loc.conf`.

Las propiedades del ENM se almacenan en el archivo `/etc/nwam/enm.conf`. Las WLAN conocidas se almacenan en el archivo `/etc/nwam/known-wlan.conf`. Este formato de archivo es similar al formato del archivo `/etc/dladm/datalink.conf`.

Nota – Si bien es posible modificar los perfiles de red mediante la edición directa de los archivos en el depósito del perfil NWAM, la forma apropiada de modificar un perfil es utilizar el comando `netcfg` o los paneles de configuración de la interfaz gráfica de NWAM. El formato de archivo y el uso de los archivos puede cambiar en futuras versiones. Consulte [“Configuración y cambio de valores de propiedades de un perfil” en la página 99](#).

Valores de propiedades de la NCU

Las NCU, los objetos de configuración individual de un NCP, representan enlaces e interfaces individuales en un sistema. Las propiedades generales para ambos tipos de NCU (de enlace y de interfaz), así como las propiedades que son específicas de cada tipo de NCU, se almacenan en el depósito de perfiles de NWAM. Las propiedades `type`, `class` y `parent` se establecen cuando se crea la NCU y no se pueden cambiar más adelante. Además, no puede cambiar directamente

una propiedad `enabled`. La propiedad se cambia indirectamente mediante la activación o desactivación de una NCU con el comando `netadm`.

El NCP automático consta de una NCU de enlace para cada enlace físico detectado en el sistema y una NCU de interfaz conectada en cada enlace. El NCP automático cambia dinámicamente cuando se insertan otros enlaces físicos. A medida que se insertan nuevos enlaces, se crean una NCU de enlace y una NCU de interfaz correspondiente para cada enlace nuevo. Las siguientes tablas definen los valores que se asignan a cada NCU que compone el NCP automático.

Nota – Las propiedades de esta tabla se muestran en el orden en el que aparecen al visualizar las propiedades de la NCU del NCP automático. Determinados valores se aplican a cada tipo de NCU.

TABLA 3-1 Propiedades de la NCU de enlace para el NCP automático

Propiedad	Valor de la NCU de enlace
<code>type</code>	<code>link</code>
<code>class</code>	<code>phys</code>
<code>parent</code>	<code>Automatic</code>
<code>enabled</code>	<code>true</code>
<code>activation-mode</code>	<code>prioritized</code>
<code>priority-group</code>	<code>0</code> (para enlaces 802.3) o <code>1</code> (para enlaces 802.11)
<code>priority-group-mode</code>	<code>shared</code> (para enlaces 802.3) o <code>exclusive</code> (para enlaces 802.11)
<code>mac-address</code>	Asignado por hardware
<code>autopush</code>	N/D
<code>MTU</code>	N/D

TABLA 3-2 Propiedades de la NCU de interfaz para el NCP automático

Propiedad	Valor de la NCU de interfaz
<code>type</code>	<code>interface</code>
<code>class</code>	<code>IP</code>
<code>parent</code>	<code>Automatic</code>
<code>enabled</code>	<code>true</code>
<code>ip-version</code>	<code>ipv4, ipv6</code>
<code>ipv4-addrsrc</code>	<code>dhcp</code>

TABLA 3-2 Propiedades de la NCU de interfaz para el NCP automático *(Continuación)*

Propiedad	Valor de la NCU de interfaz
ipv4-static-addr	N/D
ipv6-addrsrc	dhcp, autoconf
ipv6-static-addr	N/D

Valores de propiedades de ubicaciones definidas por el sistema

La siguiente tabla proporciona los valores de propiedad predeterminados para la ubicación Automatic, que es un perfil definido por el sistema. Puede modificar estos valores, con la excepción de las propiedades `activation-mode` y `enabled`. El sistema siempre activa la ubicación Automatic cuando al menos una interfaz está activa y ningún otro perfil de ubicación la reemplaza.

TABLA 3-3 Propiedades de ubicaciones definidas por el sistema

Propiedad	Valor
<code>name</code>	Automatic
<code>activation-mode</code>	system
<code>enabled</code>	modificado por system, según sea necesario
<code>conditions</code>	N/D
<code>default-domain</code>	N/D
<code>nameservices</code>	dns
<code>nameservices-config-file</code>	/etc/nsswitch.dns
<code>dns-nameservice-configsrc</code>	dhcp
<code>dns-nameservice-domain</code>	N/D
<code>dns-nameservice-servers</code>	N/D
<code>dns-nameservice-search</code>	N/D
<code>nis-nameservice-configsrc</code>	N/D
<code>nis-nameservice-servers</code>	N/D
<code>ldap-nameservice-configsrc</code>	N/D
<code>ldap-nameservice-servers</code>	N/A

TABLA 3-3 Propiedades de ubicaciones definidas por el sistema *(Continuación)*

Propiedad	Valor
nfsv4-domain	N/A
ipfilter-config-file	N/D
ipfilter-v6-config-file	N/D
ipnat-config-file	N/D
ippool-config-file	N/D
ike-config-file	N/D
ipsecpolicy-config-file	N/D

La siguiente tabla proporciona las propiedades predefinidas para la ubicación NoNet. Tenga en cuenta que puede modificar estos valores, con la excepción de las propiedades `activation-mode` y `enabled`. El sistema siempre habilita la ubicación NoNet cuando no hay interfaces activas.

TABLA 3-4 Propiedades de la ubicación NoNet

Propiedad	Valor
name	NoNet
activation-mode	system
enabled	modificado por system, según sea necesario
conditions	N/D
default-domain	N/D
nameservices	files
nameservices-config-file	/etc/nsswitch.files
dns-nameservice-configsrc	N/D
dns-nameservice-domain	N/D
dns-nameservice-servers	N/D
dns-nameservice-search	N/D
nis-nameservice-configsrc	N/D
nis-nameservice-servers	N/D
ldap-nameservice-configsrc	N/D
ldap-nameservice-servers	N/A

TABLA 3-4 Propiedades de la ubicación NoNet (Continuación)

Propiedad	Valor
<code>nfsv4-domain</code>	N/A
<code>ipfilter-config-file</code>	<code>/etc/nwam/loc/NoNet/ipf.conf</code> , que consta de reglas de filtro IP que bloquean todo el tráfico sin bucle de retorno, con la excepción de una cantidad mínima de tráfico de red requerido por NWAM para realizar la configuración de red, como la asignación de dirección DHCP.
<code>ipfilter-v6-config-file</code>	<code>/etc/nwam/loc/NoNet/ipf6.conf</code> , que consta de las reglas de filtro IP, como se describe para el <code>ipfilter-config-file</code> .
<code>ipnat-config-file</code>	N/D
<code>ippool-config-file</code>	N/D
<code>ike-config-file</code>	N/D
<code>ipsecpolicy-config-file</code>	N/D

Para obtener más información sobre las propiedades de ubicación, incluidas las propiedades que conforman las ubicaciones definidas por el usuario, consulte la página del comando `man netcfg(1M)`.

Activación de los perfiles NWAM

Los NCP, los perfiles de ubicación y los ENM tienen propiedades `activation-mode`. Los valores permitidos para cada tipo de perfil son distintos. Además, la forma en la que se valida la propiedad `activation-mode` varía para cada tipo de perfil, así como las condiciones bajo las cuales se activa cada perfil.

Para ubicaciones definidas por el sistema (Automatic y NoNet), el valor de la propiedad `activation-mode` se configura como `system`, lo que significa que la ubicación sólo puede ser activada por el sistema, en las condiciones que según haya predeterminado el sistema sean adecuadas para la ubicación predeterminada.

Para las ubicaciones definidas por el usuario, puede definir las propiedades `activation-mode` y `conditions` en `manual`, `conditional-any` o `conditional-all`. Para obtener más información, consulte “Criterios de selección de activación de ubicación” en la página 61.

Una ubicación de perfil se puede habilitar de forma manual mediante el comando `netadm` o mediante la interfaz gráfica de usuario de NWAM. Si no habilita explícitamente una ubicación, el daemon de NWAM, `nwamd`, comprueba las reglas de activación de todos los perfiles de ubicación activados condicionalmente y activados por el sistema y, a continuación, elige la ubicación que mejor se ajuste al actual entorno de red.

NWAM utiliza un algoritmo para determinar la “mejor coincidencia” para una elección de ubicación. Si no hay ninguna coincidencia adecuada para una ubicación, se activa la ubicación Automatic. Los cambios en el entorno de red hacen que el daemon `nwamd` reevalúe continuamente la selección de ubicación para determinar la mejor coincidencia. Sin embargo, si habilita explícitamente un perfil de ubicación mediante el comando `netadm` (ya sea una ubicación que se active manualmente o una ubicación activa condicionalmente), esa ubicación permanecerá activa hasta que la deshabilite explícitamente o habilite una ubicación diferente. En esta situación, los cambios realizados en el entorno de red no tiene como resultado un cambio en los perfiles de ubicación, independientemente de si podría haber una coincidencia mejor disponible. El hecho de que haya especificado explícitamente la ubicación actual la convierte, en efecto, en la mejor coincidencia posible. Para obtener instrucciones sobre la activación y desactivación de perfiles, consulte [“Activación y desactivación de perfiles” en la página 116](#).

Política de activación del NCP

NWAM le permite especificar la política del NCP, en términos de cuándo se activan las NCU. La política del NCP se aplica mediante el uso de propiedades y condiciones que se pueden especificar para cada NCU. Entre las políticas que puede especificar se incluyen, por ejemplo: “preferir conexiones con cables antes que conexiones inalámbricas” o “activar una interfaz a la vez”. Cómo y cuándo se activan los NCP se define en las propiedades configuradas para cada tipo de NCU.

Nota – Una NCU de interfaz siempre debe estar asociada con una NCU de enlace subyacente. Cada NCU de interfaz se activa cuando la NCU de enlace asociada se activa. Puede reemplazar el comportamiento predeterminado de una NCU mediante el comando `netadm`. Sin embargo, la dependencia en la NCU de enlace subyacente nunca se puede eliminar. Por ejemplo, si habilita una NCU de interfaz sin activar su NCU de enlace correspondiente, la interfaz en realidad no se activará hasta que la NCU subyacente para esa interfaz se active.

Ejemplo de una política de NCP

En el siguiente ejemplo, se establecen las propiedades de la NCU cuando la política del NCP necesita especificar que todos los enlaces con cables disponibles están activados, y que sólo se debe usar una conexión inalámbrica si no hay ninguna conexión con cables disponible.

Para todos los enlaces físicos:

- Tipo de NCU: `link`
- Clase de NCU: `phys`
- `activation-mode: prioritized`
- `priority-group: 0` para con cables; `1` para inalámbrica
- `priority-mode: shared` para con cables; `exclusive` para inalámbrica

En el siguiente ejemplo, se definen las propiedades de la NCU según una política del NCP que especifica que sólo debe haber un enlace activo en el sistema en un momento dado, y que se prefiere una conexión con cables a una conexión inalámbrica.

Para todos los enlaces físicos:

- Tipo de NCU: `link`
- Clase de NCU: `phys`
- `activation-mode: prioritized`
- `priority-group: 0` para con cables; 1 para inalámbrica
- `priority-mode: exclusivo`

Propiedades de activación de la NCU

En las propiedades de la NCU de enlace, se establece la manera en que se activan las conexiones de red. Las siguientes propiedades se utilizan para definir la política de activación del NCP:

- Propiedad `activation-mode`

Esta propiedad se puede establecer en `manual` o `prioritized`.

- `manual`: la activación de la NCU es gestionada por el administrador. Puede utilizar la interfaz de línea de comandos o la interfaz gráfica de NWAM para activar o desactivar la NCU. Si el `activation-mode` de una NCU se configura en `manual`, se ignoran los valores que se configuran para las propiedades NCU de `priority-group` y `priority-mode`.
- `prioritized`: la NCU se activa en función de los valores que se establecen en las propiedades `priority-group` y `priority-mode` para la NCU especificada. La propiedad habilitada siempre es verdadera para las NCU prioritarias.

La activación prioritaria permite la activación simultánea de grupos de enlaces. Este modo de activación también permite que uno o más enlaces se prefieran con respecto a otros enlaces. La propiedad `priority-group` asigna un nivel de prioridad numérica a un enlace determinado. Todos los enlaces que compartan el mismo nivel de prioridad se examinan como un grupo. La propiedad `priority-mode` define cuántos de los miembros del grupo pueden o deben estar disponibles para que se active el grupo.

- Propiedad `enabled` (`activation-mode` establecido como `manual`)

El valor de esta propiedad puede ser `true` o `false`. No puede establecer el valor de esta propiedad. En su lugar, este valor refleja el estado actual de una NCU habilitada de forma manual, que se puede cambiar con el comando `netadm` o mediante la interfaz gráfica de NWAM.

- Propiedad `priority-group` (`activation-mode` establecido como `prioritized`)

El valor es numérico. Un cero (0) indica la prioridad más alta. Los valores negativos no son válidos.

Entre todos los `priority-groups` disponibles, sólo se activan las NCU con el mayor `priority-group` disponible. Cuando hay más de una NCU con la misma prioridad disponible, el comportamiento de activación es definido por la propiedad `priority-mode`. El número de prioridad no es un valor absoluto. Puede cambiar a medida que se actualiza el depósito del NCP.

Nota – El orden de prioridad se aplica estrictamente.

- Propiedad `priority-mode` (`activation-mode` establecido como `prioritized`)

La propiedad se establece cuando se ha especificado un valor para la propiedad `priority-group`.

Los valores de esta propiedad son los siguientes:

- `exclusive`: especifica que sólo se puede activar una NCU en el `priority-group` en un momento determinado. NWAM activa la primera NCU disponible dentro del grupo de prioridades e ignora las otras NCU.
- `shared`: especifica que varias NCU en el grupo de prioridades pueden estar activas al mismo tiempo. Se activa cualquier NCU disponible en el grupo de prioridades.
- `all`: especifica que todas las NCU en el grupo de prioridades deben estar disponibles para que el grupo de prioridades se considere disponible y, por lo tanto, esté activo.

Criterios de selección de activación de ubicación

Cada perfil de ubicación contiene las propiedades que definen los criterios de activación. Estas propiedades especifican información sobre las condiciones en las que se activa una ubicación. NWAM continuamente vuelve a evaluar los criterios de selección para todas las ubicaciones configuradas, y cada vez determina qué ubicación tiene los criterios con la mejor coincidencia para el entorno de red actual. Si en el entorno actual de red ocurren cambios que dan lugar a mejores criterios de coincidencia, NWAM desactiva el perfil de ubicación actual y activa el perfil de ubicación con la mejor coincidencia para el entorno nuevo.

Los criterios de selección para cuándo y cómo se activa una ubicación se especifican según las siguientes propiedades:

- `activation-mode`
- `conditions`

La propiedad `activation-mode` se establece en uno de los siguientes valores posibles:

- `manual`
- `conditional-any`
- `conditional-all`

- system

Nota – El valor `system` de la propiedad `activation-mode` sólo se puede asignar a ubicaciones proporcionadas por el sistema: las ubicaciones `Automatic` y `NoNet`. El valor `system` indica que el sistema determina cuánto activar estas ubicaciones.

Si la propiedad `activation-mode` se establece en `conditional-any` o `conditional-all`, la propiedad `conditions` contiene una expresión condicional (o varias expresiones condicionales) que define el usuario. Cada expresión contiene una condición a la que se puede asignar un valor booleano, por ejemplo, “`ncu ip:net0 is-not active`”.

Si la propiedad `activation-mode` se establece en `conditional-any`, la condición se satisface si cualquiera de las condiciones es verdadera.

Si la propiedad `activation-mode` se establece en `conditional-all`, se satisfacen todas las condiciones sólo si *todas* las condiciones son verdaderas. En la siguiente tabla, se definen los criterios y operaciones que se pueden utilizar para generar las cadenas de condición.

TABLA 3-5 Criterios y operaciones para la generación de cadenas de condición

Tipo de objeto/atributo	Condición	Objeto
<code>ncu, enm, loc</code>	<code>is/is-not active</code>	nombre
<code>ssid</code>	<code>is/is-not contains/does-not-contain</code>	cadena de nombre
<code>bssid</code>	<code>is/is-not</code>	cadena bssid
<code>ip-address</code>	<code>is/is-not</code>	direcciones IPv4 o IPv6
<code>ip-address</code>	<code>is-in-range/is-not-in-range</code>	Dirección IPv4 o IPv6 más máscara de red/prefixlen
<code>advertised-domain</code>	<code>is/is-not contains/does-not-contain</code>	cadena de nombre
<code>system-domain</code>	<code>is/is-not contains/does-not-contain</code>	cadena de nombre

Nota – La propiedad `ssid` representa un Extended Service Set Identifier (ESSID), que es el nombre de red de una LAN inalámbrica (WLAN). La propiedad `bssid` representa un Basic Service Set Identifier (BSSID), que es la dirección MAC de un punto de acceso inalámbrico específico (WAP) o de cualquier punto de acceso (AP).

Tenga en cuenta la diferencia entre los atributos `advertised-domain` y `system-domain`. El dominio anunciado se descubre mediante comunicaciones externas, por ejemplo, los nombres `DNSdomain` o `NISdomain`, que son anunciados por el servidor DHCP. Este atributo es útil para la activación condicional de ubicaciones, por ejemplo, si el dominio anunciado es `mycompany.com`, se activa la ubicación `work`. El atributo `system-domain` es el dominio actualmente asignado al sistema. Se trata del valor devuelto por el comando `domainname`. Este atributo es útil para la activación condicional de ENM, ya que sólo se convierte en verdadero después de que una ubicación se ha activado y el sistema se ha configurado para ese dominio concreto. Para obtener más información, consulte la página del comando `man domainname(1M)`.

Para obtener más información sobre propiedades de ubicación, consulte [“Descripción de un perfil de ubicación” en la página 50](#).

Perfiles de configuración mediante el comando netcfg

El comando `netcfg`, que se describe en la página del comando `man netcfg(1M)`, se usa para configurar propiedades y los valores de los perfiles de red.

Puede usar el comando `netcfg` para realizar las siguientes tareas:

- Crear o destruir un perfil definido por el usuario.

Nota – No es posible crear ni destruir un perfil definido por el sistema.

- Mostrar todos los perfiles que existen en un sistema y sus valores de propiedad.
- Mostrar todos los valores de la propiedad y recursos para un perfil especificado.
- Mostrar cada propiedad que está asociada a un perfil.
- Definir o modificar una o todas las propiedades de un perfil especificado.
- Exportar la configuración actual de un perfil definido por el usuario en la salida estándar o en un archivo.

Nota – No es posible exportar un perfil definido por el sistema.

- Suprimir cualquier cambio que se haya realizado en un perfil y volver a la configuración anterior para dicho perfil.
- Verificar que un perfil tenga una configuración válida.

Puede utilizar la interfaz de usuario de netcfg en el modo interactivo, el modo de línea de comandos o el modo de archivo de comandos. Como el comando netcfg es jerárquico, se entiende más fácilmente cuando se utiliza en el modo interactivo.

Para el comando netcfg, se utiliza el concepto de un *ámbito*. Cuando utiliza el comando de forma interactiva, el ámbito en el que se encuentra en cualquier momento dado depende del tipo de perfil y la tarea que está realizando. Cuando escribe el comando netcfg en una ventana del terminal, aparece un indicador en el *ámbito global*.

Desde aquí, puede utilizar los subcomandos select o create para ver, modificar o crear los siguientes perfiles de nivel superior:

- NCP
- Ubicaciones
- ENM
- WLAN conocidas

Antes de crear o seleccionar un perfil, el indicador interactivo netcfg se muestra en el siguiente formato:

```
netcfg>
```

Después de haber creado o seleccionado un perfil, el indicador interactivo netcfg se muestra de la siguiente manera:

```
netcfg:profile-type:profile-name>
```

Nota – En el modo de línea de comandos, debe escribir el comando completo en una sola línea. Los cambios que realice a un perfil seleccionado mediante el comando netcfg en el modo de línea de comandos se asignan al depósito persistente apenas termine de escribir el comando.

Para obtener instrucciones paso a paso sobre el uso del comando netcfg, consulte el [Capítulo 4, “Configuración de perfiles de NWAM \(tareas\)”](#). Para obtener más información sobre el uso del comando netcfg, consulte la página del comando man [netcfg\(1M\)](#).

Modo interactivo netcfg

La selección o creación de un perfil de nivel superior mientras trabaja en el modo interactivo netcfg da como resultado un indicador de comandos que aparece en el *ámbito de perfil* para los perfiles de ubicación y ENM. Por ejemplo:

```
netcfg> select loc foo
netcfg:loc:foo>
```

Si se selecciona un NCP, el indicador de comandos se muestra en el *ámbito del NCP*. Desde el ámbito del NCP, se puede seleccionar o crear una NCU. La selección o creación de una NCU produce un indicador de ámbito de perfil para la NCU seleccionada. En este ámbito, todas las propiedades asociadas con el perfil seleccionado actualmente se pueden ver y definir, como se muestra en el siguiente ejemplo donde el User NCP se ha seleccionado en primer lugar y, luego, se ha creado una NCU en el ámbito del NCP. Esta acción ha producido el ámbito de perfil para la NCU creada recientemente. En este ámbito, se pueden ver o establecer las propiedades de la NCU:

```
netcfg> select ncp User
netcfg:ncp:User> create ncu phys net2
Created ncu 'net2'. Walking properties ...
activation-mode (manual) [manual|prioritized]>
```

En cualquier ámbito determinado, el indicador de comandos muestra el perfil seleccionado actualmente. Todos los cambios realizados al perfil en este ámbito puede ser *confirmados*, lo que quiere decir que los cambios se guardan en el depósito persistente. Los cambios se confirman implícitamente al salir el ámbito. Si no desea confirmar los cambios que haya realizado en el perfil seleccionado, puede volver a los último cambios confirmados para dicho perfil. Si realiza esta acción, revierte los cambios realizados en el perfil de ese nivel. Los subcomandos `revert` y `cancel` funcionan de forma parecida.

Modo de línea de comandos netcfg

En el modo de línea de comandos, cualquier subcomando que afecte un perfil o propiedad seleccionados se debe ejecutar en el ámbito particular en el que existe el perfil o la propiedad seleccionados. Por ejemplo, para obtener el valor de una propiedad de una NCU, se utilizaría el subcomando `get` en el ámbito de esa NCU particular. Cuando está en el modo interactivo `netcfg`, es bastante fácil comprender la sintaxis que debe utilizarse para este comando. Sin embargo, en el modo de línea de comandos, la sintaxis puede ser menos obvia.

Por ejemplo, para obtener el valor de una propiedad “foo”, que es un atributo de una NCU denominada `myncu` en el NCP `User`, debe utilizar la siguiente sintaxis:

```
$ netcfg "select ncp User; select ncu ip myncu; get foo"
```

En este ejemplo, tenga en cuenta la siguiente información:

- Cada ámbito se separa con un punto y coma.
- El subcomando `select` se emite en cada ámbito, una vez en el ámbito global y una vez en el ámbito de perfil.
- El subcomando `get` se usa dentro del ámbito en el que existe la propiedad “foo”.
- Se requieren comillas rectas para evitar que el shell las interprete como punto y coma.

Modo de archivo de comandos netcfg

En el modo de archivo de comandos, la información de configuración se obtiene de un archivo. Para producir este archivo, se utiliza el subcomando `export`. La configuración puede imprimirse en una salida estándar, o bien puede utilizarse la opción `-f` para especificar un archivo de salida. El subcomando `export` también se puede usar de modo interactivo. Para obtener más información, consulte “Subcomandos admitidos por netcfg” en la página 66.

Subcomandos admitidos por netcfg

Los siguientes subcomandos netcfg se admiten en el modo interactivo y el modo de línea de comandos. Tenga en cuenta que determinados subcomandos tienen semánticas diferentes dentro de cada ámbito. Si un subcomando no se puede utilizar en cierto modo, esto se observa en la descripción del subcomando.

- `cancel`
Finaliza la especificación del perfil actual sin conformar los cambios actuales en el almacenamiento persistente y, a continuación, continúa con el ámbito anterior, que está en un nivel superior.
- `clear nombre_prop`
Borra el valor de la propiedad especificada.
- `commit`
Confirma el perfil actual en el almacenamiento persistente. Para que pueda confirmarse, una configuración debe ser correcta. Por lo tanto, esta operación también realiza automáticamente una verificación en el perfil o el objeto. La operación `commit` se intenta automáticamente al salir del ámbito actual, utilizando el subcomando `end` o `exit`.
- `create [-t plantilla] tipo_objeto [clase] nombre_objeto`
Crea un perfil en memoria con el tipo y el nombre especificados. La opción `-t plantilla` especifica que el nuevo perfil es idéntico a *plantilla*, donde *plantilla* es el nombre de un perfil existente del mismo tipo. Si no se usa la opción `-t`, el nuevo perfil se crea con los valores predeterminados.
- `destroy -a`
Elimina todos los perfiles definidos por el usuario de la memoria y el almacenamiento persistente.
- `destroy tipo_objeto [clase] nombre_objeto`
Elimina el perfil definido por el usuario especificado de la memoria y el almacenamiento persistente.



Precaución – Esta operación es inmediata y no es necesario confirmarla. Un perfil destruido no se puede revertir.

- **end**
Finaliza la especificación del perfil actual y continúa con el ámbito anterior, que está en un nivel superior. El perfil actual se verifica y confirma antes de finalizar la operación de edición. En caso de que ocurra un fallo en la operación `verify` o `commit`, se mostrará un mensaje de error. Tendrá la oportunidad de finalizar la operación sin confirmar los cambios actuales. O bien, puede permanecer en el ámbito actual y continuar editando el perfil.
- **exit**
Sale de la sesión interactiva `netcfg`. El perfil actual se verifica y confirma antes de que finalice la sesión actual. En caso de que ocurra un fallo en la operación `verify` o `commit`, se mostrará un mensaje de error. Tendrá la oportunidad de finalizar la sesión sin confirmar los cambios actuales. O bien, puede permanecer en el ámbito actual y continuar editando el perfil.
- **export [-d] [-f *archivo_salida*] [*tipo_objeto* [*clase*] *nombre_objeto*]**
Imprime la configuración actual en el ámbito actual o especificado en la salida estándar o en un archivo que se especifica con la opción `-f`. La opción `-d` genera el subcomando `destroy -a` como la primera línea de la salida. Este subcomando genera una salida en una forma que es adecuada para usar en un archivo de comandos.

Nota – Los perfiles definidos por el sistema, incluidos el NCP automático y las ubicaciones Automatic, NoNet y heredadas, no se pueden exportar.

- **get [-V] *nombre_prop***
Obtiene el valor actual en memoria de la propiedad especificada. De manera predeterminada, se imprimen el nombre y el valor de la propiedad. Si se especifica la opción `-V`, sólo se imprime el valor de la propiedad.
- **help [*subcomando*]**
Muestra ayuda general o ayuda sobre un asunto específico.
- **list [-a] [*tipo_objeto* [*clase*] *nombre_objeto*]**
Muestra todos los perfiles, los pares de valor-propiedad y los recursos que se utilizarán en el ámbito actual o el especificado. Si se especifica la opción `-a`, se muestran todas las propiedades, incluidas aquellas que se ignorarán, en función de los ajustes actuales.
- **revert**
Suprime los cambios actuales que se realizaron en un perfil y, luego, vuelve a los valores del almacenamiento persistente.

- `select tipo_objeto [clase] nombre_objeto`

Selecciona el objeto especificado.

- `set nombre_prop= valor`

Establece el valor actual en memoria de la propiedad especificada.

Si se realiza en el modo de línea de comandos, el cambio también se confirma inmediatamente en el almacenamiento persistente.

Para delimitar propiedades de varios valores se utiliza una coma (,). Si un valor individual de una propiedad especificada contiene una coma, debe estar precedido con una barra diagonal inversa (\). Las comas dentro de las propiedades que sólo incluyen un valor único no se interpretan como delimitadores y no es necesario que estén precedidas por una barra diagonal inversa.

- `verify`

Verifica que el objeto o perfil en memoria actual tengan una configuración válida.

- `walkprop [-a]`

“Guía” a cada propiedad que está asociada al perfil actual. Para cada propiedad, se muestran el nombre y el valor actual. Se proporciona un indicador para permitirle cambiar el valor actual. Si una propiedad no se utiliza, según los valores especificados anteriormente, no se muestra la propiedad. Por ejemplo, si la propiedad `ipv4-addrsrc` se establece en `static`, no se usa la propiedad `ipv4-addr`, y no se guía ni muestra, al menos que especifique la opción `-a`.

Cuando se utiliza, la opción `-a` repite todas las propiedades disponibles para el objeto o perfil especificado.

Para delimitar propiedades de varios valores se utiliza una coma (,). Si un valor individual de una propiedad especificada contiene una coma, debe ir precedido por una barra oblicua inversa (\). Las comas dentro de las propiedades que sólo incluyen un valor único no se interpreten como delimitadores y no es necesario que estén precedidas por una barra diagonal inversa.

Nota – Este subcomando es significativo sólo cuando se utiliza en el modo interactivo.

Para obtener información relacionada con la tarea, consulte el [Capítulo 4, “Configuración de perfiles de NWAM \(tareas\)”](#).

Administración de perfiles mediante el comando netadm

El comando `netadm` se usa para administrar y obtener el estado de los perfiles (NCP, ubicaciones, ENM y WLAN) y las NCU, los objetos de configuración individuales que componen un NCP. Además, puede usar el comando `netadm` para interactuar con el daemon NWAM (`nwamd`) en la ausencia de una interfaz de gráfica. Para obtener más información sobre `netadm`, consulte la página del comando `man netadm(1M)`.

Se admiten los siguientes subcomandos `netadm`:

- `enable [-p tipo_perfil] [-c clase_ncu] nombre_perfil`

Habilita el perfil especificado. Si el nombre de perfil no es único, se debe especificar el tipo de perfil. Si el tipo de perfil es `ncu` y el nombre no es único, por ejemplo, si existen tanto una `ncu` de enlace como una de interfaz con el mismo nombre, se habilitan ambas NCU, a menos que se use la opción `-c` para especificar la clase de NCU.

El tipo de perfil debe ser uno de los siguientes:

- `ncp`
- `ncu`
- `loc`
- `enm`
- `wlan`

La clase de NCU debe estar especificada como `phys` o `ip`.

- `disable [-p tipo_perfil] [-c clase_ncu] nombre_perfil`

Desactiva el perfil especificado. Si el nombre de perfil no es único, se debe especificar el tipo de perfil para identificar el perfil que se va a deshabilitar. Si el tipo de perfil es `ncu` y el nombre no es único, por ejemplo, si existen tanto una `ncu` de enlace como una de interfaz con el mismo nombre, se deshabilitarán ambas NCU, a menos que se use la opción `-c` para especificar la clase de NCU.

El tipo de perfil debe ser uno de los siguientes:

- `ncp`
- `ncu`
- `loc`
- `enm`
- `wlan`

La clase de NCU debe estar especificada como `phys` o `ip`.

- `list [-x] [-p tipo_perfil] [-c clase_ncu] [nombre_perfil]`

Muestra todos los perfiles disponibles y su estado actual. Los posibles valores de estado se muestran en la sección siguiente. Si un perfil es especificado por nombre, entonces, sólo se muestra el estado actual de ese perfil. Si el nombre de perfil no es único, se muestran todos

los perfiles con ese nombre determinado. O bien, el tipo de perfil, la clase de NCU o ambos pueden incluirse para identificar un perfil específico. Si sólo se especifica el tipo de perfil, se muestran todos los perfiles de ese tipo.

Cuando se muestran las NCP habilitadas, se incluyen todas las NCU que componen ese NCP.

Si se especifica la opción -x, también se incluye en la salida una descripción expandida del estado de cada perfil que se muestra.

Entre los valores de estado de perfil posibles se incluyen los siguientes:

- `disabled`
Indica un perfil activado manualmente que no ha sido habilitado.
- `offline`
Indica un perfil activado condicionalmente o activado por el sistema que no ha sido habilitado. Es posible que el perfil no esté activo porque no se cumplen sus condiciones. O es posible que el perfil no esté activo porque en su lugar se activó otro perfil con condiciones más específicas que sí se cumplen. Esta condición se aplica a los tipos de perfil que deben estar activados de a uno por vez, por ejemplo, el perfil de ubicación.
- `online`
Indica un perfil activado condicionalmente o activado por el sistema cuyas condiciones se cumplieron y fue habilitado de manera satisfactoria. O bien puede indicar un perfil activado manualmente que se ha habilitado correctamente a petición del usuario.
- `maintenance`
Indica que se intentó la activación del perfil, pero que se produjo un fallo.
- `initialized`
Indica que el perfil representa un objeto de configuración válida para el que no se realizó ninguna acción todavía.
- `uninitialized`
Indica que el perfil representa un objeto de configuración que no está presente en el sistema. Por ejemplo, este estado puede indicar una NCU que corresponde a un enlace físico que se haya eliminado del sistema.
- `show-events`
Recibe un flujo de eventos desde el daemon de NWAM y los muestra.
- `scan-wifi nombre_enlace`
Inicia una exploración inalámbrica en el enlace que se especifica como *nombre_enlace*.
- `select-wifi nombre_enlace`
Selecciona una red inalámbrica a la cual conectarse desde los resultados de análisis en el enlace especificado como *nombre_enlace*.
- `help`

Muestra un mensaje de uso con una breve descripción de cada subcomando.

Para obtener información relacionada con la tarea, consulte [Capítulo 5, “Administración de perfiles de NWAM \(tareas\)”](#).

Descripción general de los daemons NWAM

Hay dos daemons que utiliza NWAM: el daemon `nwamd` y el daemon `netcfgd`. El daemon de motor de política, `nwamd`, controla la configuración automática de la red mediante el funcionamiento en roles múltiples. El daemon de depósito, `netcfgd`, controla el acceso al depósito de configuración de red.

Descripción del daemon de motor de política NWAM (`nwamd`)

El daemon `nwamd` controla la configuración automática de red al asumir los siguientes roles:

- **Recopilador de eventos**

Este rol implica la recopilación de eventos relacionados con enlaces que se deben detectar mediante el socket de enrutamiento y el registro `sysevent`. Un ejemplo de cómo `nwamd` realiza esta tarea es que el daemon obtiene un `EC_DEV_ADD` `sysevent`, que significa que la NIC se conectó en el sistema mientras estaba en funcionamiento. Todos estos eventos se empaquetan en la estructura de eventos `nwamd` y luego se envían al thread de manejo de eventos, que es responsable de la tarea.

- **Controlador de eventos**

Este rol implica la ejecución de un thread de bucle de evento para responder a eventos de interés. El controlador de eventos opera en los equipos de estado que están asociados con los diferentes objetos gestionados por el servicio NWAM. En el transcurso del manejo de eventos, el daemon `nwamd` detecta cambios en el entorno de red, lo que podría desencadenar como resultado cambios en un perfil o en varios perfiles.

- **Distribuidor de eventos**

Este rol implica el envío de eventos a consumidores externos que hayan registrado un interés en dichos eventos. Entre los ejemplos de distribución de eventos se incluyen los eventos de análisis inalámbricos que contienen información sobre las WLAN disponibles, lo que es útil para la interfaz gráfica de NWAM. La interfaz gráfica puede, a su vez, mostrar las opciones disponibles para el usuario.

- **Gestor de perfiles**

La gestión de estos perfiles mediante el daemon `nwamd` implica aplicar la configuración de red en función de la siguiente información:

- Qué enlaces e interfaces se activan
- Las características de las redes conectadas
- Las contingencias y dependencias integradas en los perfiles activados
- Los eventos externos que se han recibido

Descripción del daemon de depósito NWAM (`netcfgd`)

El daemon de perfil, `netcfgd`, controla y gestiona el acceso a un depósito de configuración de red. El daemon es iniciado automáticamente por el servicio SMF

`svc:/network/netcfg:default`. El daemon se asegura de que cualquier aplicación que intente leer la información o escribir información en el depósito tenga las siguientes autorizaciones:

- `solaris.network.autoconf.read`
- `solaris.network.autoconf.write`

Para obtener más información sobre autorizaciones, consulte la página del comando `man auth_attr(4)`. Para obtener más información sobre los perfiles de seguridad, consulte la página del comando `man prof_attr(4)`.

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

Servicios de red SMF

En Oracle Solaris, la configuración de red es implementada por múltiples servicios SMF:

- `svc:/network/loopback:default`: crea las interfaces de bucle de retorno IPv4 e IPv6.
- `svc:/network/netcfg:default`: es un requisito para el servicio `svc:/network/physical:default`. El servicio gestiona el depósito de configuración de red y su principal función es iniciar el daemon `netcfgd`.
- `svc:/network/physical:default`: brinda enlaces y conecta interfaces IP. Este servicio determina si NWAM o la configuración de red tradicional están en uso, en función del NCP actualmente activo. Si NWAM está en uso, el servicio inicia el daemon de política, `nwamd`. Si el NCP `DefaultFixed` está activo, el servicio detiene `nwamd` y aplica la configuración persistente `ipadm`.
- `svc:/network/location:default`: este servicio depende del servicio `svc:/network/physical:default` y es responsable de la activación del perfil `Location` seleccionado por el daemon `nwamd`.

Nota – El servicio `svc:/network/location:default` tiene una propiedad que almacena el perfil de ubicación actual. No manipule directamente esta propiedad. En su lugar, utilice la interfaz gráfica de NWAM o la interfaz de línea de comandos para efectuar estos tipos de cambios.

Descripción general de la seguridad de NWAM

La seguridad de NWAM está diseñada para abarcar los siguientes componentes:

- Interfaz de línea de comandos (comandos `netcfg` y `netadm`)
- Interfaz gráfica de NWAM
- Daemon de depósito de perfil de NWAM (`netcfgd`)
- Daemon de motor de política (`nwamd`)
- Biblioteca de NWAM (`libnwam`)

El daemon `netcfgd` controla el depósito donde se almacena toda la información de configuración de red. El comando `netcfg`, la interfaz de usuario de NWAM y el daemon `nwamd` envían solicitudes al daemon `netcfgd` para acceder al depósito. Estos componentes funcionales realizan solicitudes a través de la biblioteca de NWAM, `libnwam`.

El daemon `nwamd` es el motor de políticas que recibe los eventos del sistema, configura la red y lee información de configuración de red. La interfaz gráfica de NWAM y el comando `netcfg` son herramientas de configuración que puede utilizar para ver y modificar la configuración de red. Estos componentes también se utilizan para refrescar el servicio NWAM cuando se debe aplicar una nueva configuración al sistema.

Autorizaciones y perfiles relacionados con NWAM

La implementación actual de NWAM utiliza las siguientes autorizaciones para realizar tareas específicas:

- `solaris.network.autoconf.read`: permite la lectura de datos de configuración NWAM, que verifica el daemon `netcfgd`
- `solaris.network.autoconf.write`: permite la escritura de datos de configuración de NWAM, que verifica el daemon `netcfgd`
- `solaris.network.autoconf.select`: permite que se apliquen nuevos datos de configuración, que verifica el daemon `nwamd`
- `solaris.network.autconf.wlan`: permite la escritura de datos de configuración de WLAN conocidas

Estas autorizaciones se registran en la base de datos `auth_attr`. Para obtener más información, consulte la página del comando `man auth_attr(4)`.

Se proporcionan dos perfiles de seguridad: Network Autoconf User y Network Autoconf Admin. El perfil User tiene autorizaciones read, select y wlan. El perfil Admin agrega la autorización write. El perfil Network Autoconf User está asignado al perfil Console User. Por lo tanto, de manera predeterminada, cualquier persona que se conecte a la consola puede ver, habilitar y deshabilitar perfiles. Como Console User no tiene la autorización solaris.network.autoconf.write asignada, este usuario no puede crear ni modificar NCP, NCU, ubicaciones ni ENM. Sin embargo, Console User puede ver, crear y modificar WLAN.

Autorizaciones necesarias para utilizar interfaces de usuario de NWAM

Los comandos NWAM, netcfg y netadm, se pueden usar para ver y habilitar perfiles NWAM por parte de cualquiera que tenga privilegios de Console User. Estos privilegios se asignan automáticamente a cualquier usuario conectado en el sistema desde /dev/console.

Para modificar perfiles de NWAM mediante el comando netcfg, necesita la autorización solaris.network.autoconf.write o el perfil Network Autoconf Admin.

Puede determinar los privilegios que están asociados a un perfil de derechos mediante el comando profiles con el nombre del perfil. Para obtener más información, consulte la página del comando man [profiles\(1\)](#).

Por ejemplo, para determinar privilegios que están asociados al perfil de derechos Console User, utilice el siguiente comando.

```
$ profiles -p "Console User" info
Found profile in files repository.
  name=Console User
  desc=Manage System as the Console User
  auths=solaris.system.shutdown,solaris.device.cdrw,solaris.smf.manage.vbiosd,
solaris.smf.value.vbiosd
  profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
Network Autoconf User,Desktop Removable Media User
  help=RtConsUser.html
```

La interfaz gráfica de NWAM incluye los siguientes tres componentes, que no tienen privilegios. Se otorgan autorizaciones a estos componentes, en función de cómo se inician y las tareas que deben realizar:

- **Presencia de panel específica de NWAM**

Este componente es el applet del panel en el escritorio que permite al usuario interactuar con NWAM. El panel puede ser ejecutado por cualquier usuario y se utiliza para supervisar la configuración automática del sistema y gestionar las notificaciones de eventos. El panel también se puede utilizar para realizar algunas tareas de configuración básicas de la red, por ejemplo, seleccionar una red Wi-Fi o cambiar ubicaciones manualmente. Para realizar estos tipos de tareas, se requiere el perfil de derechos Network Autoconf User. El perfil de

derechos está disponible en la configuración predeterminada, ya que el panel está ejecutándose con las autorizaciones del usuario conectado desde `/dev/console` y, por lo tanto, tiene el perfil `Console User`.

- **Interfaz gráfica de NWAM**

La interfaz gráfica de NWAM es el medio principal para interactuar con NWAM desde el escritorio. La interfaz gráfica se utiliza para ver el estado de la red, para crear y modificar NCP y perfiles de ubicación y para iniciar y detener ENM configurados. La interacción con la interfaz gráfica requiere cuatro de las autorizaciones de `solaris.network.autoconf` o el perfil `Network Autoconf Admin`. De manera predeterminada, el perfil `Console User` tiene suficientes autorizaciones para visualizar el estado y los perfiles de la red mediante el uso de la interfaz gráfica. Además, necesita la autorización `solaris.network.autoconf.write` o el perfil `Network Autoconf Admin` para modificar perfiles mediante la interfaz gráfica.

Puede obtener autorizaciones adicionales de una de las siguientes maneras:

- Asigne el perfil `Network Autoconf Admin` a un usuario específico.

Puede asignar autorizaciones adecuadas o perfiles de derechos directamente a un determinado usuario mediante la edición del archivo `/etc/user_attr` para ese usuario.

- Asigne el perfil `Network Autoconf Admin` al `Console User`.

Puede asignar este perfil al `Console User` en lugar del perfil `Network Autoconf User` que está asignado de manera predeterminada. Para asignar este perfil, edite la entrada en el archivo `/etc/security/prof_attr`.

Configuración de perfiles de NWAM (tareas)

En este capítulo, se describen las tareas de configuración de perfiles de NWAM que puede realizar con el comando `netcfg`. Estas tareas de configuración incluyen la creación, modificación y destrucción de perfiles, así como la gestión de los diferentes servicios SMF que controlan la configuración de NWAM. En este capítulo, se describe cómo utilizar el comando `netcfg` en modo interactivo y en modo de línea de comandos.

En este capítulo, se describen los siguientes temas:

- “Creación de perfiles” en la página 78
- “Eliminación de perfiles” en la página 97
- “Configuración y cambio de valores de propiedades de un perfil” en la página 99
- “Consulta al sistema sobre información de perfiles” en la página 102
- “Exportación y restauración de la configuración de un perfil” en la página 107
- “Gestión de configuración de red” en la página 111

Para obtener información sobre cómo mostrar estados de perfiles, activar y desactivar perfiles, y gestionar redes inalámbricas conocidas mediante el comando `netadm`, consulte el [Capítulo 5, “Administración de perfiles de NWAM \(tareas\)”](#).

Para obtener información sobre cómo interactuar con NWAM y cómo gestionar su configuración de red desde el escritorio, consulte el [Capítulo 6, “Acerca de la interfaz gráfica de usuario de NWAM”](#).

Para ver una introducción a NWAM, consulte el [Capítulo 2, “Introducción a NWAM”](#).

Para obtener más información general sobre NWAM, incluida una descripción de los modos de la interfaz de usuario `netcfg`, consulte el [Capítulo 3, “Configuración y administración de NWAM \(descripción general\)”](#).

Creación de perfiles

El comando `net cfg`, que se describe en la página del comando `man net cfg(1M)`, es uno de dos comandos administrativos en la interfaz de línea de comandos de NWAM.

El comando `net cfg` puede ser utilizado por cualquiera que tenga privilegios `Console User` para mostrar datos de configuración de perfiles y para mostrar, crear y modificar objetos de WLAN conocidas. Estos privilegios se asignan automáticamente a cualquier usuario que ha iniciado sesión en el sistema desde `/dev/console`. Los usuarios que tienen el perfil `Network Autoconf Admin` también pueden crear y modificar todos los tipos de perfiles de NWAM y objetos de configuración. Para obtener más información, consulte [“Descripción general de la seguridad de NWAM” en la página 73](#).

Puede utilizar el comando `net cfg` para seleccionar, crear, modificar y destruir perfiles definidos por usuarios. El comando se puede usar en modo interactivo o en modo de línea de comandos. El comando `net cfg` también admite la exportación de información de configuración de perfiles a archivos de comandos.

Puede crear, modificar y eliminar los siguientes perfiles y objetos de configuración:

- Perfiles de configuración de red (NCP)
- Perfiles de ubicación
- Modificadores de red externos (ENM)
- Redes de área local inalámbricas (WLAN) conocidas
- Unidades de configuración de red (NCU)

Creación de perfiles en modo de línea de comandos

La sintaxis básica del comando que se debe utilizar para crear un perfil desde la línea de comandos es la siguiente:

```
netcfg create [ -t template ] object-type [ class ] object-name
```

create Crea un perfil en la memoria (u objeto de configuración) del tipo y el nombre especificados.

-t *plantilla* Especifica que el nuevo perfil debe ser idéntico a *plantilla*, donde *plantilla* es el nombre de un perfil existente del mismo tipo. Si la opción **-t** no se utiliza, el perfil nuevo se crea con valores predeterminados.

tipo_objeto Especifica el tipo de perfil que se va a crear.

Puede especificar uno de los siguientes valores para la opción *tipo_objeto*:

- `ncp`
- `ncu`
- `loc`

- enm
- wlan

Todos los perfiles que se especifican mediante la opción *tipo_objeto*, con la excepción de una ncu, se deben crear en el ámbito global antes de poder utilizar el comando `netcfg select` para seleccionar el objeto determinado.

<i>clase</i>	Especifica la clase de perfil especificado por <i>tipo_objeto</i> . Este parámetro sólo se utiliza para el tipo de objeto ncu y tiene dos valores posibles, <i>phys</i> o <i>ip</i> .
<i>nombre_objeto</i>	Especifica el nombre del perfil definido por el usuario. Para una NCU, <i>nombre_objeto</i> es el nombre del enlace o de la interfaz correspondiente. Para todos los demás tipos de perfil, <i>nombre_objeto</i> es cualquier nombre definido por el usuario.

Por ejemplo, para crear un NCP denominado *User*, debe escribir el siguiente comando:

```
$ netcfg create ncp User
```

donde *ncp* es el *tipo_objeto* y *User* es el *nombre_objeto*.

Nota – Para la creación de NCP, la opción `class` no es necesaria.

Opcionalmente, puede utilizar una copia del NCP Automatic como plantilla y realizar cambios en dicho perfil, como se muestra aquí:

```
$ netcfg create -t Automatic ncp
```

Para crear un perfil de ubicación con el nombre `office`, debe escribir el siguiente comando:

```
$ netcfg create loc office
```

Creación de perfiles de forma interactiva

Puede utilizar el comando `netcfg` en modo interactivo para realizar las siguientes tareas:

- Crear un perfil.
- Seleccionar y modificar un perfil.
- Verificar que toda la información necesaria sobre un perfil esté configurada y sea válida.
- Confirmar los cambios de un nuevo perfil.
- Cancelar la configuración actual del perfil sin confirmar los cambios en el almacenamiento persistente.
- Revertir los cambios realizados en un perfil.

Creación de un NCP

La creación de un perfil en modo interactivo deriva en un símbolo del sistema que se encuentra en uno de los siguientes ámbitos:

- En el ámbito del NCP, si se crea un NCP.
- En el ámbito del perfil, si se crea un perfil de ubicación, un ENM o un objeto WLAN.

La creación de un NCP o una NCU desplaza el foco al ámbito de ese objeto y lo guía por las propiedades predeterminadas del perfil especificado.

Para crear de manera interactiva un NCP, debe empezar con el inicio de una sesión interactiva `net cfg`. A continuación, use el subcomando `create` para crear el nuevo NCP `User`, de la siguiente manera:

```
$ netcfg
netcfg> create ncp User
netcfg:ncp:User>
```

Creación de NCU para un NCP

El NCP es básicamente un contenedor que consta de un conjunto de NCU. Todos los NCP contienen NCU de enlace e interfaz. Las NCU de enlace especifican la configuración de enlaces y la política de selección de enlaces. Las NCU de interfaz especifican la política de configuración de interfaces. Si se requiere conectividad IP, se requieren tanto un enlace como una NCU de interfaz. Las NCU se deben agregar o eliminar explícitamente utilizando el comando `net cfg` o utilizando la interfaz gráfica de usuario.

Nota – Es posible agregar NCU que no estén correlacionadas con ningún enlace que esté instalado actualmente en el sistema. Además, puede eliminar NCU que están asignadas a un enlace que está instalado actualmente en el sistema.

Puede crear NCU mediante el comando `net cfg` en modo interactivo o modo de línea de comandos. Como la creación de una NCU implica varias operaciones, es más fácil y más eficaz crear NCU en modo interactivo, en lugar de intentar construir un comando de una sola línea que crea la NCU y todas sus propiedades. Las NCU se pueden crear al crear por primera vez un NCP o posteriormente. El proceso de creación o modificación de una NCU implica la configuración de propiedades generales de la NCU, así como la configuración de propiedades que se aplican específicamente a cada tipo de NCU.

Las propiedades que se le presentan durante el proceso de creación de NCU para un NCP son las más adecuadas según las selecciones que realiza durante la creación de ese NCP concreto.

Al crear una NCU de forma interactiva, `netcfg` recorre cada propiedad relevante y muestra tanto el valor predeterminado, donde existe un valor predeterminado, como los posibles valores. Si presiona la tecla de retorno sin especificar un valor, se aplica el valor predeterminado (o se deja la propiedad vacía si no hay ningún valor predeterminado), o usted puede especificar un valor alternativo. Las propiedades que se muestran durante el proceso de creación de NCU para un NCP son pertinentes según las selecciones que ya ha realizado. Por ejemplo, si selecciona `dhcp` para la propiedad `ipv4-addrsrc` de una NCU de interfaz, no se le pide que especifique un valor para la propiedad `ipv4-addr`.

En la siguiente tabla, se describen todas las propiedades de NCU que puede especificar al crear o modificar una NCU. Algunas propiedades se aplican a ambos tipos de NCU. Otras propiedades se aplican a una NCU de enlace o a una NCU de interfaz. Para obtener una descripción completa de todas las propiedades de NCU, incluidas las reglas y condiciones que se pueden aplicar al especificar estas propiedades, consulte la página del comando `man netcfg(1M)`.

TABLA 4-1 Propiedades de NCU para crear o modificar una NCU

Propiedad	Descripción	Valores posibles	Tipo de NCU
<code>type</code>	Especifica el tipo de NCU, ya sea de enlace o interfaz.	<code>link</code> o <code>interface</code>	Enlace e interfaz
<code>class</code>	Especifica la clase de NCU.	<code>phys</code> (para NCU de enlace) o <code>ip</code> (para NCU de interfaz)	Enlace e interfaz
<code>parent</code>	Especifica el NCP al que pertenece esta NCU.	<code>NCP_principal</code>	Enlace e interfaz
<code>enabled</code>	Especifica si la NCU está habilitada o deshabilitada. Esta propiedad es de sólo lectura. Sólo se cambia indirectamente al utilizar el comando <code>netadm</code> o la interfaz gráfica de usuario de NWAM para habilitar o deshabilitar la NCU.	<code>true</code> o <code>false</code>	Enlace e interfaz
<code>activation-mode</code>	Especifica el tipo de desencadenador para la activación automática de la NCU.	<code>manual</code> o <code>prioritized</code> El valor predeterminado es <code>manual</code> .	Enlace

TABLA 4-1 Propiedades de NCU para crear o modificar una NCU (Continuación)

Propiedad	Descripción	Valores posibles	Tipo de NCU
<code>priority-group</code>	Especifica el número de prioridad de grupo.	<p>0 (para enlaces con cable) o 1 (para enlaces inalámbricos)</p> <p>Para NCP definidos por el usuario, se pueden especificar diferentes políticas, por ejemplo, el enlace inalámbrico 1 es prioridad 1, el enlace con cable 1 es prioridad 2 y el enlace con cable 2 es prioridad 3.</p> <p>Nota – Un número inferior indica una prioridad mayor.</p>	Enlace
<code>priority-mode</code>	Especifica el modo que se utiliza para determinar el comportamiento de activación de un grupo de prioridades si la propiedad <code>activation-mode</code> se establece en <code>prioritized</code> .	<p><code>exclusive</code>, <code>shared</code> u <code>all</code></p> <p>Consulte la página del comando <code>man netcfg(1M)</code> para obtener las reglas que se aplican al especificar estos valores.</p>	Enlace
<code>link-mac-addr</code>	Especifica la dirección MAC asignada a este enlace. De manera predeterminada, NWAM utiliza la dirección MAC asignada de fábrica u otra dirección MAC predeterminada. Un valor diferente se puede establecer aquí para anular dicha selección.	Cadena que contiene una dirección MAC de 48 bits.	
<code>link-autopush</code>	Identifica los módulos que aparecen automáticamente cuando se abre el enlace.	<p>Lista de cadenas (módulos que aparecen al abrir el enlace).</p> <p>Consulte <code>autopush(1M)</code>.</p>	Enlace
<code>link-mtu</code>	Se establece automáticamente en la MTU predeterminada para el enlace físico. El valor se puede sustituir mediante la definición de esta propiedad en un valor diferente.	Tamaño de MTU para el enlace.	Enlace

TABLA 4-1 Propiedades de NCU para crear o modificar una NCU (Continuación)

Propiedad	Descripción	Valores posibles	Tipo de NCU
<code>ip-version</code>	Especifica la versión de IP que se debe utilizar. Se pueden asignar varios valores.	<code>ipv4</code> e <code>ipv6</code> El valor predeterminado es <code>ipv4</code> , <code>ipv6</code>	Interfaz
<code>ipv4-adrrsrc</code>	Identifica el origen de las direcciones IPv4 asignadas a esta NCU. Se pueden asignar varios valores.	<code>dhcp</code> y <code>static</code> El valor predeterminado es <code>dhcp</code> .	Interfaz
<code>ipv6-adrrsrc</code>	Identifica el origen de las direcciones IPv6 asignadas a esta NCU. Se pueden asignar varios valores.	<code>dhcp</code> , <code>autoconf</code> o <code>static</code> El valor predeterminado es <code>dhcp</code> , <code>autoconf</code> .	Interfaz
<code>ipv4-addr</code>	Especifica una o más direcciones IPv4 que se van a asignar a esta NCU.	Una o más direcciones IPv4 que se van a asignar.	Interfaz
<code>ipv6-addr</code>	Especifica una o más direcciones IPv6 que se van a asignar a esta NCU.	Una o más direcciones IPv6 que se van a asignar.	Interfaz
<code>ipv4-default-route</code>	Especifica la ruta predeterminada para una dirección IPv4.	Dirección IPv4	Interfaz
<code>ipv6-default-route</code>	Especifica la ruta predeterminada para una dirección IPv6.	Dirección IPv6	Interfaz

▼ Cómo crear de forma interactiva un NCP

El siguiente procedimiento describe cómo crear un NCP en modo interactivo.

Consejo – El proceso de recorrido que NWAM realiza durante la creación del perfil inicial garantiza que sólo se le soliciten las propiedades pertinentes, de acuerdo con las selecciones que ha realizado anteriormente. Además, el subcomando `verify` que se describe en este procedimiento verifica la configuración. Si los valores requeridos faltan, se le notifica. Puede utilizar el subcomando `verify` explícitamente al crear o modificar un perfil o implícitamente mediante el subcomando `commit` para guardar los cambios.

1 Inicie una sesión interactiva `netcfg`.

```
$ netcfg
netcfg>
```

2 Cree el NCP.

```
netcfg> create ncp User
netcfg:ncp:User>
```

donde `ncp` es el tipo de perfil y `User` es el nombre del perfil.

La creación del NCP lo lleva automáticamente al ámbito del NCP. Si estuviera creando una ubicación, un ENM o un objeto WLAN, el símbolo del sistema lo llevaría al ámbito del perfil.

3 Cree NCU de enlace e interfaz para el NCP.

a. Para crear la NCU de enlace, escriba el siguiente comando:

```
netcfg:ncp:User> create ncu phys net0
Created ncu 'net0', Walking properties ...
```

donde `ncu` es el tipo de objeto, `phys` es la clase y `net0` (por ejemplo, *sólo* propósitos) es el nombre del objeto.

La creación de una NCU lo lleva al ámbito de ese objeto y lo guía por las propiedades predeterminadas para el objeto.

b. Para crear una NCU de interfaz, escriba el siguiente comando:

```
netcfg:ncp:User> create ncu ip net0
Created ncu 'net0'. walking properties ...
```

donde `ncu` es el tipo de objeto, `ip` es la clase y `net0` (por ejemplo, *sólo* propósitos) es el nombre del objeto.

La creación de una NCU lo lleva al ámbito de ese objeto y lo guía por las propiedades predeterminadas para el objeto.

Durante la creación de una NCU, la opción `class` se utiliza para diferenciar entre los dos tipos de NCU. Esta opción resulta especialmente útil en situaciones donde diferentes tipos de NCU comparten el mismo nombre. Si se omite la opción `class`, resulta mucho más difícil distinguir NCU que comparten el mismo nombre.

4 Agregue las propiedades adecuadas para la NCU que ha creado.

Nota – Repita los pasos 3 y 4 hasta que se creen todas las NCU requeridas para el NCP.

5 Durante la creación de la NCU o al establecer valores de propiedades para una NCU determinada, utilice el subcomando `verify` para asegurarse de que los cambios realizados sean correctos.

```
netcfg:ncp:User:ncu:net0> verify
All properties verified
```

6 Confirme las propiedades que ha definido para la NCU.

```
netcfg:ncp:User:ncu:net0> commit
committed changes.
```

Como alternativa, puede utilizar el subcomando `end` para realizar una confirmación implícita, que mueve la sesión interactiva al siguiente ámbito superior. En esta instancia, si ha terminado de crear el NCP y ha terminado de agregar NCU a él, puede salir de la sesión interactiva directamente desde el ámbito del NCP.

Nota –

- En el modo interactivo, los cambios no se guardan en el almacenamiento persistente hasta que los confirma. Al utilizar el subcomando `commit`, se confirma el perfil entero. Para mantener la coherencia del almacenamiento persistente, la operación de confirmación también incluye un paso de verificación. Si la verificación falla, la confirmación también falla. Si una confirmación implícita falla, se le da la opción de finalizar la sesión interactiva sin confirmar los cambios actuales o de salir de ella de la misma manera. O bien puede permanecer en el ámbito actual y continuar realizando cambios en el perfil.
 - Para cancelar los cambios realizados, utilice el subcomando `cancel` o `revert`.
El subcomando `cancel` finaliza la configuración del perfil actual sin confirmar los cambios actuales en el almacenamiento persistente y, a continuación, pasa la sesión interactiva al siguiente ámbito superior. El subcomando `revert` deshace los cambios realizados y relee la configuración anterior. Al utilizar el subcomando `revert`, la sesión interactiva permanece en el mismo ámbito.
-

7 Utilice el subcomando `list` para mostrar la configuración del NCP.

8 Cuando termine de configurar el NCP, salga de la sesión interactiva.

```
netcfg:ncp:User> exit
```

Cada vez que utiliza el subcomando `exit` para terminar una sesión interactiva `netcfg`, el perfil actual se verifica y se confirma. Si falla la operación de confirmación o verificación, se emite un mensaje de error adecuado y se le da la oportunidad de salir sin confirmar los cambios actuales. O bien puede permanecer en el ámbito actual y continuar realizando cambios en el perfil.

Nota – Para salir del ámbito sin tener que salir de la sesión interactiva `netcfg`, escriba el comando `end`:

```
netcfg:ncp:User> end
netcfg>
```

Ejemplo 4–1 Creación de un NCP de forma interactiva

En el ejemplo siguiente, se crean un NCP y dos NCU (un enlace y una interfaz).

```
$ netcfg
netcfg> create ncp User
netcfg:ncp:User> create ncu phys net0
```

```

Created ncu 'net0', Walking properties ...
activation-mode (manual) [manual|prioritized]>
link-mac-addr>
link-autopush>
link-mtu>
netcfg:ncp:User:ncu:net0> end
Committed changes
netcfg:ncp:User> create ncu ip net0
Created ncu 'net0'. Walking properties ...
ip-version (ipv4,ipv6) [ipv4|ipv6]> ipv4
ipv4-addrsrc (dhcp) [dhcp|static]>
ipv4-default-route>
netcfg:ncp:User:ncu:net0> verify
All properties verified
netcfg:ncp:User:ncu:net0> end
Committed changes
netcfg:ncp:User> list
NCUs:
      phys    net0
      ip      net0
netcfg:ncp:User> list ncu phys net0
ncu:net0
      type                link
      class               phys
      parent              "User"
      activation-mode     manual
      enabled             true
netcfg:ncp:User> list ncu ip net0
ncu:net0
      type                interface
      class               ip
      parent              "User"
      enabled             true
      ip-version          ipv4
      ipv4-addrsrc        dhcp
      ipv6-addrsrc        dhcp,autoconf
netcfg:ncp:User> exit
$

```

En este ejemplo, debido a que se elige el valor `ipv4`, ningún símbolo del sistema aparece para la propiedad `ipv6-addrsrc`, ya que esta propiedad no se utiliza. Del mismo modo, para la NCU `phys`, se acepta el valor predeterminado (activación manual) para la propiedad `priority-group`, por lo que no se aplican otras propiedades relacionadas condicionalmente.

Ejemplo 4-2 Creación de una NCU para un NCP existente

Para crear una NCU para un NCP existente o para modificar las propiedades de cualquier perfil existente, utilice el comando `netcfg` con el subcomando `select`.

En el ejemplo siguiente, se crea una NCU de IP para un NCP existente. El proceso de modificación de un perfil existente en modo interactivo es similar al proceso de creación de un perfil. La diferencia entre el siguiente ejemplo y el [Ejemplo 4-1](#) es que, en este ejemplo, el subcomando `select` se utiliza en lugar del subcomando `create` porque el NCP ya existe.

```

$ netcfg
netcfg> select ncp User
netcfg:ncp:User> list
NCUs:
    phys    net0
netcfg:ncp:User> create ncu ip net0
Created ncu 'net0'. Walking properties ...
ip-version (ipv4,ipv6) [ipv4|ipv6]> ipv4
ipv4-addrsrc (dhcp) [dhcp|static]>
ipv4-default-route>
netcfg:ncp:User:ncu:net0> end
Committed changes
netcfg:ncp:User> list
NCUs:
    phys    net0
    ip      net0
netcfg:ncp:User> list ncu phys net0
ncu:net0
    type                link
    class                phys
    parent              "User"
    activation-mode      manual
    enabled              true
netcfg:ncp:User> list ncu ip net0
NCU:net0
    type                interface
    class                ip
    parent              "User"
    enabled              true
    ip-version           ipv4
    ipv4-addrsrc         dhcp
    ipv6-addrsrc         dhcp,autoconf
netcfg:ncp:User> exit
$

```

Creación de un perfil de ubicación

Un perfil de ubicación contiene las propiedades que definen los valores de configuración de red que no están relacionados directamente con la conectividad IP y de enlace básica. Algunos ejemplos incluyen valores de servicio de nombres y filtro IP que se aplican juntos, cuando es necesario. En cualquier momento, un perfil de ubicación y un NCP deben estar activos en el sistema. Existen ubicaciones definidas por el sistema y ubicaciones definidas por el usuario. Las ubicaciones del sistema son los valores predeterminados que NWAM elige bajo determinadas condiciones, por ejemplo, si no ha especificado una ubicación o si no hay ubicaciones manualmente activadas que estén habilitadas, y ninguna de las condiciones de las ubicaciones condicionalmente activadas se han cumplido. Las ubicaciones definidas por el sistema tienen un modo de activación `system`. Las ubicaciones definidas por el usuario son aquellas que están configuradas para ser activadas manualmente o condicionalmente, según las condiciones de red, por ejemplo, una dirección IP que se obtiene por una conexión de red.

Para obtener información sobre cómo activar (habilitar) manualmente un perfil de ubicación, consulte [“Activación y desactivación de perfiles” en la página 116](#).

Puede crear ubicaciones mediante el comando `netcfg` en modo interactivo o en modo de línea de comandos. Al crear un perfil de ubicación, debe definir las propiedades para la ubicación especificando valores que definen los parámetros de configuración concretos de esa ubicación. Las propiedades de ubicación están clasificadas por grupo, donde el grupo denota una clase concreta de preferencias de configuración.

Las propiedades de ubicación también se almacenan por NWAM en un depósito. Cuando se activa un perfil de ubicación concreto, NWAM configura de manera automática la red, según las propiedades que se definen para esa ubicación. La creación o modificación de ubicaciones implica la configuración de diversas propiedades que definen cómo se configura el perfil, que, a su vez, determina cómo NWAM configura de manera automática la red. Las propiedades que se le presentan durante el proceso de configuración son las más adecuadas, de acuerdo con las selecciones que ha realizado anteriormente.

En la siguiente tabla, se describen todas las propiedades de la ubicación que se pueden especificar. Tenga en cuenta que las propiedades de ubicación se clasifican por grupo. Para obtener una descripción completa de todas las propiedades de ubicación, incluidas las reglas, las condiciones y las dependencias que se pueden aplicar al especificar cualquiera de estas propiedades, consulte la página del comando `man netcfg(1M)`.

TABLA 4-2 Propiedades de ubicación y sus descripciones

Grupo de propiedades y descripción	Valor de propiedades y descripción
<p>Criterios de selección</p> <p>Especifica los criterios para determinar cómo y cuándo una ubicación se activa o se desactiva.</p>	<ul style="list-style-type: none"> ■ <code>activation-mode</code> Los valores posibles para la propiedad <code>activation-mode</code> son <code>manual</code>, <code>conditional-any</code> y <code>conditional-all</code>. ■ <code>conditions</code>
<p>Dominio del sistema</p> <p>Determina el nombre de dominio de un host para uso directo por el servicio de nombres NIS.</p>	<p>La propiedad <code>system-domain</code> consta de la propiedad <code>default-domain</code>. Esta propiedad especifica el dominio de todo el sistema que se utiliza para intercambios de llamada a procedimiento remoto (RPC).</p>

TABLA 4-2 Propiedades de ubicación y sus descripciones (Continuación)

Grupo de propiedades y descripción	Valor de propiedades y descripción
<p>Información de servicios de nombres</p> <p>Especifica el servicio de nombres que se debe utilizar y la configuración del conmutador del servicio de nombres.</p>	<p>A continuación, se muestra una lista de propiedades para el servicio de nombres especificado:</p> <ul style="list-style-type: none"> ■ domain-name ■ nameservices ■ nameservices-config-file ■ dns-nameservice-configsrc ■ dns-nameservice-domain ■ dns-nameservice-servers ■ dns-nameservice-search ■ dns-nameservice-sortlist ■ dns-nameservice-options ■ nis-nameservice-configsrc ■ nis-nameservice-servers ■ ldap-nameservice-configsrc ■ ldap-nameservice-servers <p>Para obtener más información sobre estas propiedades, consulte la sección “Propiedades de ubicación” en la página del comando <code>man netcfg(1M)</code>.</p>
<p>Dominio NFSv4</p> <p>Especifica el dominio NFSv4.</p>	<p>El valor que se utiliza para la propiedad <code>nfsmapid_domain</code> del sistema. Este valor se utiliza para establecer la propiedad SMF <code>nfsmapid_domain</code>, como se describe en la página del comando <code>man nfsmapid</code>, mientras la ubicación está activa. Si esta propiedad no está definida, <code>nfsmapid_property</code> del sistema se borra cuando la ubicación se activa. Consulte la página del comando <code>man nfsmapid(1M)</code> para obtener más información.</p>
<p>Configuración del filtro IP</p> <p>Especifica los parámetros que se utilizan para la configuración del filtro IP. Para estas propiedades, se especifican las rutas a los archivos <code>ipf</code> e <code>ipnat</code> adecuados que contienen reglas de NAT y filtro IP.</p>	<ul style="list-style-type: none"> ■ ipfilter-config-file ■ ipfilter-v6-config-file ■ ipnat-config-file ■ ippool-config-file <p>Si se especifica un archivo de configuración, las reglas que se encuentran en el archivo identificado se aplican al subsistema <code>ipfilter</code> adecuado.</p>
<p>Archivos de configuración para IPsec</p> <p>Especifica los archivos que se van a utilizar para la configuración de IPsec.</p>	<ul style="list-style-type: none"> ■ ike-config-file ■ ipsecpolicy-config-file

▼ Cómo crear un perfil de ubicación de forma interactiva

El siguiente procedimiento describe cómo crear un perfil de ubicación.

Consejo – El proceso de recorrido que NWAM realiza durante la creación de un perfil inicial sólo le solicita aquellas propiedades que son adecuadas, según los valores que ha introducido anteriormente. Además, el subcomando `verify` comprueba que su configuración sea correcta. Si los valores requeridos faltan, se le notifica. Tenga en cuenta que puede utilizar el subcomando `verify` explícitamente al crear o modificar la configuración de un perfil o implícitamente mediante el subcomando `commit` para guardar los cambios.

1 Inicie una sesión interactiva `netcfg`.

```
$ netcfg
netcfg>
```

2 Cree o seleccione la ubicación.

```
netcfg> create loc office
netcfg:loc:office>
```

En este ejemplo, se crea la ubicación `office`.

La creación de la ubicación lo pasa automáticamente al ámbito del perfil de esta ubicación.

3 Defina las propiedades adecuadas de la ubicación.

4 Visualice la configuración del perfil.

Por ejemplo, la siguiente salida muestra las propiedades de la ubicación `office`:

```
netcfg:loc:office> list
LOC:office
  activation-mode          conditional-any
  conditions               "ncu ip:wpi0 is active"
  enabled                  false
  nameservices             dns
  nameservices-config-file "/etc/nsswitch.dns"
  dns-nameservice-configsrc dhcp
  ipfilter-config-file    "/export/home/test/wifi.ipf.conf"
```

5 Verifique que la configuración del perfil sea correcta.

En el siguiente ejemplo, se verifica la configuración de la ubicación `office`:

```
netcfg:loc:office> verify
All properties verified
```

6 Al completar la verificación, confirme el perfil de ubicación en el almacenamiento persistente.

```
netcfg:loc:office> commit
Committed changes
```

Como alternativa, puede utilizar el subcomando `end` para terminar la sesión, que también guarda la configuración del perfil.

```
netcfg:loc:office> end
Committed changes
```

Nota –

- En el modo interactivo, los cambios no se guardan en el almacenamiento persistente hasta que los confirma. Al utilizar el subcomando `commit`, se confirma el perfil entero. Para mantener la coherencia del almacenamiento persistente, la operación de confirmación también incluye un paso de verificación. Si la verificación falla, la confirmación también falla. Si una confirmación implícita falla, se le da la opción de finalizar la sesión interactiva sin confirmar los cambios actuales o de salir de ella de la misma manera. O bien puede permanecer en el ámbito actual y continuar realizando cambios en el perfil.
- Para cancelar los cambios realizados, utilice el subcomando `cancel`.

El subcomando `cancel` finaliza la configuración del perfil actual sin confirmar los cambios actuales en el almacenamiento persistente y, a continuación, pasa la sesión interactiva al siguiente ámbito superior.

7 Salga de la sesión interactiva.

```
netcfg> exit
Nothing to commit
$
```

Ejemplo 4–3 Creación de un perfil de ubicación de forma interactiva

En el siguiente ejemplo, se crea una ubicación denominada `office`.

```
$ netcfg
netcfg> create loc office
Created loc 'office'. Walking properties ...
activation-mode (manual) [manual|conditional-any|conditional-all]> conditional-any
conditions> ncu ip:wpi0 is active
nameservices (dns) [dns|files|nis|ldap]>
nameservices-config-file ("/etc/nsswitch.dns")>
dns-nameservice-configsrc (dhcp) [manual|dhcp]>
nfsv4-domain>
ipfilter-config-file> /export/home/test/wifi.ipf.conf
ipfilter-v6-config-file>
ipnat-config-file>
ippool-config-file>
ike-config-file>
ipsecpolicy-config-file>
netcfg:loc:office> list
LOC:office
    activation-mode           conditional-any
    conditions                 "ncu ip:wpi0 is active"
    enabled                   false
    nameservices               dns
    nameservices-config-file  "/etc/nsswitch.dns"
    dns-nameservice-configsrc dhcp
    ipfilter-config-file      "/export/home/test/wifi.ipf.conf"
netcfg:loc:office> verify
All properties verified
netcfg:loc:office> commit
```

```
Committed changes
netcfg> list
NCPs:
  User
  Automatic
Locations:
  Automatic
  NoNet
  test-loc
WLANs:
  sunwifi
  ibahn
  gogoinflight
  admiralsclub
  hhonors
  sjcfreewifi
netcfg> exit
Nothing to commit
$
```

En este ejemplo, las siguientes propiedades se han especificado para la ubicación `office`:

- La propiedad `activation-mode` se definió en `conditional-any`, que resultó en un símbolo del sistema que permitió la especificación de las condiciones de activación.
- La condición de activación se especificó como `ncu ip:wpi0 is active`.

Nota – La propiedad `conditions` fue necesaria porque la propiedad `conditional-any` se había especificado en el paso anterior. Si, por ejemplo, la propiedad `manual` se hubiera especificado, la propiedad `conditions` no sería necesaria.

- Los siguientes valores predeterminados fueron aceptados presionando la tecla de retorno:
 - `nameservices`
 - `nameservices-config-file`
 - `dns-nameservice-configsrc`
 - `nfsv4-domain`
- Para la propiedad `ipfilter-config-file`, se especificó el archivo `/export/home/test/wifi.ipf.conf`.
- Los siguientes valores predeterminados fueron aceptados presionando la tecla de retorno:
 - `ipfilter-v6-config-file`
 - `ipnat-config-file`
 - `ippool-config-file`
 - `ike-config-file`
 - `ipsecpolicy-config-file`
- El subcomando `list` se ha utilizado para ver las propiedades del perfil de ubicación.
- El subcomando `verify` se ha utilizado para realizar una verificación de la configuración.

- El subcomando `commit` se ha utilizado para confirmar los cambios en el almacenamiento persistente.
- El subcomando `list` se ha utilizado nuevamente para garantizar que la nueva ubicación se haya creado correctamente y contenga la información correcta.
- El subcomando `exit` se ha utilizado para salir de la sesión interactiva `netcfg`.

Para obtener instrucciones sobre los valores que se pueden especificar para estas propiedades, consulte la página del comando `man netcfg(1M)`.

Creación de un perfil de ENM

Los ENM pertenecen a la configuración de aplicaciones que son externas a NWAM, por ejemplo, una aplicación VPN. Estas aplicaciones pueden crear y modificar la configuración de red. Los ENM también se pueden definir como servicios o aplicaciones que modifican directamente la configuración de la red cuando se activan o desactivan. Puede configurar NWAM para activar y desactivar ENM en las condiciones que especifica. A diferencia de un perfil de ubicación o un NCP, donde sólo uno de cada tipo de perfil puede estar activo en un sistema en cualquier momento, varios ENM pueden estar potencialmente activos en un sistema al mismo tiempo. Los ENM que están activos en un sistema en cualquier momento no dependen necesariamente del perfil de ubicación o NCP que también está activo en el sistema al mismo tiempo.

Nota – NWAM no reconoce automáticamente una aplicación para la que pueda crear un ENM. Estas aplicaciones, primero, se deben instalar y, luego, se deben configurar en el sistema antes de poder utilizar el comando `netcfg` para crear un ENM para ellas.

Para crear un ENM, escriba el siguiente comando:

```
$ netcfg
netcfg> create enm my_enm
Created enm 'my_enm'. Walking properties ...
```

donde `enm` es el perfil del ENM y `my_enm` es el nombre del objeto.

El proceso de creación de ENM lo lleva al ámbito del perfil del ENM recién creado y comienza a recorrer automáticamente las propiedades en el ENM recién creado. Desde aquí, puede establecer las propiedades para el ENM que determinan cuándo y cómo se activa el ENM, así como otras condiciones, incluido el método de inicio y detención de ENM.

Para obtener más instrucciones sobre cómo especificar propiedades de ENM, consulte la página del comando `man netcfg(1M)`.

En la siguiente tabla, se describen las propiedades que puede especificar al crear o modificar un ENM.

Nombre de propiedad	Descripción	Valores posibles
activation-mode	Modo que se utiliza para determinar la activación de un ENM.	conditional-any, conditional-all, manual
conditions	Si activation-mode es conditional-any o conditional-all, especifica la prueba para determinar si el ENM se debe activar.	Una cadena o varias cadenas con formato, como se especifica en la sección “Expresiones de condición” de la página del comando man <code>netcfg(1M)</code> si se utiliza la propiedad.
start	(Opcional) Ruta absoluta a la secuencia de comandos que se ejecutará tras la activación.	Ruta a la secuencia de comandos si se utiliza esta propiedad.
stop	(Opcional) Ruta absoluta a la secuencia de comandos que se ejecutará tras la desactivación.	Ruta a la secuencia de comandos si se utiliza esta propiedad.
fmri	(Opcional) El FMRI (identificador de recurso de gestión de errores) que se habilitará tras la activación del ENM. Nota – Se debe especificar un FMRI o una secuencia de comandos de inicio. Si se especifica un FMRI, se ignoran las propiedades start y stop.	Ruta a la secuencia de comandos.

EJEMPLO 4-4 Creación de un perfil de ENM de forma interactiva

En el ejemplo siguiente, se crea un ENM denominado `test-enm` en modo interactivo.

```
$ netcfg
netcfg> create enm test-enm
Created enm 'testenm'. Walking properties ...
activation-mode (manual) [manual|conditional-any|conditional-all]>
fmri> svc:/application/test-app:default
start>
stop>
netcfg:enm:test-enm> list
ENM:test-enm
  activation-mode    manual
  enabled            false
  fmri               "svc:/application/test-enm:default"
netcfg:enm:test-enm> verify
All properties verified
netcfg:enm:test-enm> end
Committed changes
netcfg> list
NCPs:
  User
  Automatic
Locations:
  Automatic
  NoNet
```

EJEMPLO 4-4 Creación de un perfil de ENM de forma interactiva (Continuación)

```

    test-loc
ENMs:
    test-enm
WLANs:
    sunwifi
    ibahn
    gogoinflight
    admiralsclub
    hhonors
    sjcfreewifi
netcfg> end
$

```

En este ejemplo, se creó un ENM denominado `test-enm` con los siguientes valores de propiedad:

- El valor predeterminado (`manual`) para la propiedad `activation-mode` se ha aceptado presionando la tecla de retorno.
- La propiedad FMRI de `SMF svc:/application/test-enm:default` se ha especificado como método para la activación y desactivación de la aplicación.
Tenga en cuenta que, debido a que se ha especificado un FMRI, se omitieron las propiedades del método `start` y `stop`.
- El subcomando `list` se utilizó para ver las propiedades del ENM.
- El subcomando `verify` se utilizó para garantizar que la configuración del perfil sea correcta.
- El subcomando `end` se utilizó para guardar implícitamente la configuración.
- El subcomando `end` se utilizó nuevamente para finalizar la sesión interactiva.

Creación de WLAN

NWAM mantiene una lista de WLAN conocidas de todo el sistema. WLAN son objetos de configuración que contienen información de configuración e historial para las redes inalámbricas a las que se conecta desde el sistema. Esta lista se utiliza para determinar el orden en que NWAM intenta conectarse a redes inalámbricas disponibles. Si una red inalámbrica de la lista de WLAN conocidas está disponible, NWAM se conecta automáticamente a esa red. Si hay dos o más redes conocidas disponibles, NWAM se conecta a la red inalámbrica que tiene la prioridad más alta (número menor). Cualquier red inalámbrica nueva a la que NWAM se conecta se agrega a la parte superior de la lista de WLAN conocidas y se convierte en la nueva red inalámbrica con prioridad más alta.

Para crear un objeto WLAN, escriba el siguiente comando:

```

$ netcfg
netcfg> create wlan mywifi
Created wlan 'mywifi'. Walking properties ...

```

donde `wlan` es el objeto WLAN y `mywifi` es el nombre del objeto.

El proceso de creación de un objeto WLAN lo lleva al ámbito del perfil de la WLAN recién creada y comienza a recorrer automáticamente las propiedades en la WLAN recién creada. Desde aquí, puede establecer las propiedades de la WLAN que definen su configuración.

En la siguiente tabla, se describen las propiedades que puede especificar al crear o modificar WLAN.

Propiedad de WLAN conocida	Tipo de datos para la propiedad
<code>name</code>	ESSID (nombre de red inalámbrica).
<code>bssids</code>	ID de estación base de WLAN a las que su sistema se ha conectado mientras estaba conectado a la WLAN especificada.
<code>priority</code>	Preferencia de conexión de WLAN (se prefieren valores más bajos).
<code>keyslot</code>	Número de ranura (de 1 a 4) en el que se encuentra la clave WEP.
<code>keyname</code>	Nombre de la clave WLAN que se crea mediante el comando <code>dladm create-secobj</code> .
<code>security-mode</code>	Tipo de clave de cifrado en uso. El tipo debe ser <code>none</code> , <code>wep</code> o <code>wpa</code> .

EJEMPLO 4-5 Creación de una WLAN

En el siguiente ejemplo, se crea un objeto WLAN denominado `mywifi`.

En este ejemplo, se supone que un objeto seguro denominado `mywifi-key`, que contiene la clave especificada por la propiedad `keyname` para la WLAN `mywifi`, se crea *antes* de agregar la WLAN.

El número de prioridad puede cambiar a medida que se agregan o se eliminan otras WLAN. Tenga en cuenta que dos WLAN no pueden tener el mismo número de prioridad asignado. Los números más bajos indican una prioridad mayor, en virtud de qué WLAN se prefieren. En este ejemplo, la WLAN tiene asignado el número de prioridad 100 para garantizar que tenga una prioridad más baja que cualquier otra WLAN conocida.

Cuando el subcomando `list` se utiliza al final del procedimiento, la nueva WLAN se agrega a la parte inferior de la lista, lo que indica que tiene la prioridad más baja de todas las WLAN conocidas existentes. Si la WLAN tuviera asignado un número de prioridad de cero (0), que es el predeterminado, se habría mostrado en la parte superior de la lista, lo que indica la prioridad más alta. Posteriormente, la prioridad de todas las otras WLAN existentes se habría reducido, y se habrían mostrado en la lista después de la WLAN recién agregada.

EJEMPLO 4-5 Creación de una WLAN (Continuación)

```

$ netcfg
netcfg> create wlan mywifi
Created wlan 'mywifi'. Walking properties ...
priority (0)> 100
bssids>
keyname> mywifi-key
keyslot>
security-mode [none|wep|wpa]> wpa
netcfg:wlan:mywifi> list
WLAN:mywifi
    priority          100
    keyname            "mywifi-key"
    security-mode     wpa
netcfg:wlan:mywifi> verify
All properties verified
netcfg:wlan:mywifi> end
Committed changes
netcfg> list
NCPs:
    User
    Automatic
Locations:
    Automatic
    NoNet
    test-loc
ENMs:
    test-enm
WLANS:
    sunwifi
    ibahn
    gogoinflight
    admiralsclub
    hhonors
    sjcfreewifi
    mywifi
netcfg> exit
Nothing to commit
$

```

Eliminación de perfiles

Puede eliminar todos los perfiles definidos por el usuario o un perfil definido por el usuario específico de la memoria y del almacenamiento persistente mediante el comando `net c fg destroy -a`.

Nota – Los perfiles definidos por el sistema, que incluyen el NCP Automatic y los perfiles de ubicación Automatic y NoNet, no se pueden eliminar.

La sintaxis del comando `des t roy` es la siguiente:

netcfg destroy *object-type* [*class*] *object-name*

Como alternativa, puede utilizar el siguiente comando para eliminar todos los perfiles definidos por el usuario en un sistema:

netcfg destroy -a

EJEMPLO 4-6 Eliminación de todos los perfiles definidos por el usuario mediante el modo de línea de comandos netcfg

Para eliminar todos los perfiles definidos por el usuario en un sistema, escriba el siguiente comando:

```
$ netcfg destroy -a
```

Porque, al menos, uno de los perfiles debe estar activo en el sistema en todo momento y para evitar errores en uso al eliminar perfiles definidos por el usuario, asegúrese de habilitar el NCP Automatic antes de utilizar el comando `destroy -a`.

EJEMPLO 4-7 Eliminación de un perfil definido por el usuario específico mediante el modo de línea de comandos netcfg

Para eliminar un perfil definido por el usuario específico en el sistema, por ejemplo, el NCP denominado `User`, escriba el siguiente comando:

```
$ netcfg destroy ncp User
```

El comando `destroy` también se puede utilizar para eliminar NCU de un NCP existente. En el siguiente ejemplo, una NCU de interfaz con el nombre `net1` se elimina del NCP definido por el usuario:

```
$ netcfg "select ncp User; destroy ncu ip net1"
```

Para confirmar que un perfil se haya eliminado, utilice el subcomando `list`, como se muestra aquí:

```
$ netcfg
netcfg> select ncp User
netcfg:ncp:User> list
NCUs:
    phys    net1
netcfg> exit
Nothing to commit
$
```

EJEMPLO 4-8 Eliminación de un perfil de forma interactiva

En el siguiente ejemplo, se elimina una NCU de IP denominada `net2`.

```
$ netcfg list
NCPs:
    Automatic
```

EJEMPLO 4-8 Eliminación de un perfil de forma interactiva (Continuación)

```

User
Locations:
  Automatic
  NoNet
  test
  foo
$ netcfg
netcfg> select ncp User
netcfg:ncp:User> list
NCUs:
  phys    net2
  ip      net2
netcfg:ncp:User> destroy ncu ip net2
Destroyed ncu 'net2'
netcfg:ncp:User> list
NCUs:
  phys    net2
netcfg:ncp:User> end
netcfg> exit
Nothing to commit
$

```

Configuración y cambio de valores de propiedades de un perfil

Los valores de propiedades de perfiles definidos por el usuario nuevos y existentes se establecen mediante el comando `netcfg` con el subcomando `set`. Este subcomando se puede utilizar en modo interactivo o en modo de línea de comandos. Si un valor de propiedad se establece o se cambia en modo de línea de comandos, el cambio se confirma de inmediato en el almacenamiento persistente.

La sintaxis del subcomando `set` es la siguiente:

```
netcfg set prop-name=value1[,value2...]
```

Si necesita recuperar un valor de propiedad determinado, utilice el comando `netcfg get`. Para obtener más información, consulte [“Obtención de valores de una propiedad concreta” en la página 104](#).

EJEMPLO 4-9 Establecimiento de valores de propiedades en el modo de línea de comandos `netcfg`

Si está utilizando el comando `netcfg` para definir un valor de propiedad en el modo de línea de comandos, varios subcomandos se deben escribir en la línea de comandos.

Por ejemplo, para establecer la propiedad `mtu` para una NCU de enlace denominada `net1`, debe escribir el siguiente comando:

```
$ netcfg "select ncp User; select ncu phys net1; set mtu=1492"
```

EJEMPLO 4-9 Establecimiento de valores de propiedades en el modo de línea de comandos netcfg
(Continuación)

En este ejemplo, el subcomando `select` se utiliza para seleccionar el perfil de nivel superior y luego, nuevamente, para seleccionar la NCU que contiene el valor de propiedad `mtu` que se modifica.

Se pueden establecer diversos valores para una propiedad determinada desde la línea de comandos al mismo tiempo. Al definir varios valores, cada valor debe estar separado por una coma (,). Si los valores individuales para una propiedad especificada también contienen una coma, la coma que forma parte del valor de propiedad debe estar precedida por una barra diagonal inversa (\ ,). Las comas dentro de propiedades que sólo tienen un valor único no se interpretan como delimitadores y, por lo tanto, no necesitan estar precedidas por una barra diagonal inversa.

En el siguiente ejemplo, se establece el valor de propiedad `ip-version` para la NCU, `myncu`, en el NCP User:

```
$ netcfg "select ncp User; select ncu ip myncu; set ip-version=ipv4,ipv6"
```

EJEMPLO 4-10 Configuración de valores de propiedades de un perfil de forma interactiva

Cuando se establecen valores de propiedades de manera interactiva, primero, debe seleccionar un perfil en el ámbito actual, que mueve la sesión interactiva al ámbito de dicho perfil. Desde este ámbito, puede seleccionar el objeto cuya propiedad desea modificar. El perfil seleccionado se carga en la memoria del almacenamiento persistente. En este ámbito, puede modificar el perfil o sus propiedades, como se muestra en el siguiente ejemplo:

```
$ netcfg
netcfg> select ncp User
netcfg:ncp:User> select ncu ip iw0
netcfg:ncp:User:ncu:iw0> set ipv4-default-route = 129.174.7.366
```

En el siguiente ejemplo, se establece la propiedad `ipfilter-config-file` de la ubicación `foo`:

```
$ netcfg
netcfg> list
NCPs:
  Automatic
  User
Locations:
  Automatic
  NoNet
  foo

netcfg> select loc foo
netcfg:loc:foo> list
LOC:foo
  activation-mode          manual
  enabled                  false
  nameservices             dns
```

EJEMPLO 4-10 Configuración de valores de propiedades de un perfil de forma interactiva
(Continuación)

```

    dns-nameservice-configsrc      dhcp
    nameservices-config-file       "/etc/nsswitch.dns"
netcfg:loc:foo> set ipfilter-config-file=/path/to/ipf-file
netcfg:loc:foo> list
LOC:foo
  activation-mode                  manual
  enabled                          false
  nameservices                     dns
  dns-nameservice-configsrc        dhcp
  nameservices-config-file         "/etc/nsswitch.dns"
  ipfilter-config-file             "/path/to/ipf-file"
netcfg:loc:foo> end
Committed changes
netcfg> exit
Nothing to commit
$

```

En el siguiente ejemplo, la propiedad `link-mtu` de la NCU `net0` en el NCP `User` se modifica de manera interactiva:

```

$ netcfg
netcfg> select ncp User
netcfg:ncp:User> select ncu phys net0
netcfg:ncp:User:ncu:net0> list
NCU:net0
  type                link
  class               phys
  parent              "User"
  enabled              true
  activation-mode     prioritized
  priority-mode       exclusive
  priority-group      1
netcfg:ncp:User:ncu:net0> set link-mtu=5000
netcfg:ncp:User:ncu:net0> list
NCU:net0
  type                link
  class               phys
  parent              "User"
  enabled              true
  activation-mode     prioritized
  priority-mode       exclusive
  priority-group      1
  link-mtu            5000
netcfg:ncp:User:ncu:net0> commit
Committed changes
netcfg:ncp:User:ncu:net0> exit
Nothing to commit
$

```

Consulta al sistema sobre información de perfiles

El comando `netcfg` se puede utilizar con el subcomando `list` para enumerar todos los perfiles, los pares propiedad-valor y los recursos que existen en el ámbito especificado o actual. Utilice el subcomando `list` para consultar al sistema información general sobre todos los perfiles o para recuperar información específica sobre un perfil concreto. El subcomando `list` se puede utilizar en modo interactivo o en modo de línea de comandos.

Si necesita obtener información sobre los perfiles y su estado actual, utilice el comando `netadm` con el subcomando `list`. Para obtener más información, consulte [“Visualización del estado actual de un perfil” en la página 114](#).

Enumeración de todos los perfiles en un sistema

El comando `netcfg list` muestra todos los perfiles definidos por el sistema y por el usuario en un sistema. Observe que el uso del subcomando `list` sin ninguna opción muestra todos los perfiles de nivel superior que se encuentran en un sistema. El comando no muestra el estado de cada perfil. Para visualizar una lista de los perfiles y su estado (en línea o fuera de línea), utilice el comando `netadm list`.

Para enumerar todos los perfiles de nivel superior en un sistema, escriba el siguiente comando:

```
$ netcfg list
NCPs:
    Automatic
    User
Locations:
    Automatic
    NoNet
    home
    office
ENMs:
    myvpn
    testenm
WLANS:
    workwifi
    coffeeshop
    homewifi
```

En este ejemplo, se muestran los siguientes perfiles:

- NCP
 - Se muestran dos NCP: el NCP `Automatic`, que es un perfil definido por el sistema, y un NCP definido por el usuario, denominado `User`.
- Ubicaciones
 - Se muestran cuatro perfiles de ubicación: dos ubicaciones definidas por el sistema (`Automatic` y `NoNet`) y dos ubicaciones definidas por el usuario (`home` y `office`).

- ENM

Se muestran dos ENM: un ENM para una aplicación VPN instalada y configurada, y un ENM de prueba.
- WLAN

Se muestran tres WLAN: una WLAN para el trabajo, una WLAN para la cafetería local y una WLAN para la red inalámbrica doméstica del usuario.

Nota – Sólo los perfiles definidos por el usuario se pueden crear, modificar o eliminar.

Enumeración de todos los valores de propiedades de un perfil específico

Utilice el comando `netcfg` con el subcomando `list` para enumerar todos los valores de propiedades de un perfil especificado.

La sintaxis del subcomando `list` es la siguiente:

```
$ netcfg list [ object-type [ class ] object-name ]
```

EJEMPLO 4-11 Enumeración de todos los valores de propiedades de una NCP

Por ejemplo, para mostrar una lista de todos los valores de propiedades de una NCU de IP en el NCP `User`, escriba el siguiente comando:

```
$ netcfg "select ncp User; list ncu ip net0"
NCU:net0
      type                interface
      class               ip
      parent              "User"
      enabled              true
      ip-version          ipv4
      ipv4-addrsrc        dhcp
      ipv6-addrsrc        dhcp,autoconf
```

EJEMPLO 4-12 Enumeración de todos los valores de propiedades de un ENM

En el siguiente ejemplo, se muestran todas las propiedades de un ENM denominado `myenm`.

```
$ list enm myenm
ENM:myenm
activation-mode manual
enabled          true
start            "/usr/local/bin/myenm start"
stop             "/bin/alt_stop"
```

EJEMPLO 4-12 Enumeración de todos los valores de propiedades de un ENM (Continuación)

En este ejemplo, la salida del subcomando `list` muestra la siguiente información:

- La propiedad `activation-mode` para este ENM se establece en `manual`.
- El ENM se habilita.
- Las propiedades de método `start` y `stop` se han especificado, en lugar de utilizar un FMRI.

Obtención de valores de una propiedad concreta

Puede utilizar el comando `netcfg` con el subcomando `get` para obtener el valor específico de una propiedad especificada. Este subcomando se puede utilizar en modo interactivo o en modo de línea de comandos.

La sintaxis del subcomando `get` es la siguiente:

```
netcfg get [ -V ] prop-name
```

Para obtener el valor de la propiedad `ip-version` de una NCU denominada `myncu`, que es parte del NCP User, escriba el siguiente comando. Por ejemplo:

```
$ netcfg "select ncp User; select ncu ip myncu; get -V ip-version"  
ipv4
```

Si la opción `-V` se utiliza con el subcomando `get`, sólo se muestra el valor de propiedad, como se indica aquí:

```
netcfg:ncp:User:ncu:net0> get -V activation-mode  
manual
```

De lo contrario, se muestran la propiedad y su valor. Por ejemplo:

```
netcfg:ncp:User:ncu:net0> get activation-mode  
activation-mode      manual
```

▼ Cómo obtener un valor de propiedad único de forma interactiva

En este procedimiento, se describe cómo obtener un valor de propiedad único mediante el comando `netcfg get` mientras está en el modo interactivo `netcfg`. En este procedimiento en particular, algunos de los ejemplos muestran cómo obtener un valor de propiedad único para una NCU en el NCP User. Estos ejemplos se utilizan *sólo* con fines demostrativos. La información que usted provee cuando utiliza este comando varía según el perfil y el valor de la propiedad que intenta recuperar.

Si desea ver todos los valores de propiedades de un perfil, puede usar alternativamente el subcomando `walkprop`. Este subcomando lo guía por todas las propiedades de un perfil

determinado, una a la vez, lo que permite modificar una o todas las propiedades del perfil. Para obtener más información, consulte “[Visualización y cambio de valores de propiedades de forma interactiva mediante el subcomando walkprop](#)” en la página 106.

1 Inicie una sesión interactiva netcfg.

```
$ netcfg
netcfg>
```

2 Seleccione el objeto de configuración o perfil que contiene el valor de propiedad que desea obtener.

```
netcfg> select object-type [ class ] object-name
```

Nota – El parámetro *class* sólo se aplica si está seleccionando una NCU. Además, el parámetro *class* se debe especificar si la NCU de clase *phys* e *ip* comparten el mismo nombre. Sin embargo, si el nombre de la NCU es único, el parámetro *class* no es necesario.

Por ejemplo, para seleccionar el NCP User, escriba:

```
netcfg> select User NCP
```

En este ejemplo, la selección del NCP User mueve la sesión interactiva al ámbito del objeto seleccionado.

3 (Opcional) Visualice los componentes del perfil.

```
netcfg:ncp:User> list
NCUs:
    phys    net0
    ip      net0
```

4 Seleccione el objeto que contiene el valor de propiedad que desea obtener.

En el siguiente ejemplo, se selecciona el NCU (*phys*) de enlace *net0* en el NCP User:

```
netcfg:ncp:User> select ncu phys net0
```

La selección de la NCU *net0* mueve la sesión interactiva al ámbito de ese objeto y carga las propiedades actuales de la NCU desde la memoria.

5 Obtenga el valor de propiedad especificado.

```
netcfg:ncp:User:ncu:net0> get property-value
```

Por ejemplo, para obtener el valor de la propiedad *activation-mode*, escriba:

```
netcfg:ncp:User:ncu:net0> get activation-mode
activation-mode      manual
```

Pasos siguientes En este punto, puede definir un nuevo valor para la propiedad utilizando el subcomando *set* o puede salir de la sesión interactiva sin efectuar ningún cambio. Tenga en cuenta que si modifica

un valor de propiedad mientras está en modo interactivo, debe utilizar el subcomando `commit` o `exit` para guardar los cambios. Para obtener información sobre cómo configurar un valor de propiedad en el modo interactivo `netcfg`, consulte [“Configuración y cambio de valores de propiedades de un perfil” en la página 99](#).

Visualización y cambio de valores de propiedades de forma interactiva mediante el subcomando `walkprop`

El subcomando `walkprop` se puede usar interactivamente para ver las propiedades de un perfil. Este subcomando lo “guía” a lo largo de un perfil, una propiedad a la vez, y muestra el nombre y el valor actual de cada propiedad. También se muestra un símbolo del sistema interactivo, que puede utilizar para cambiar el valor actual de la propiedad especificada. El delimitador para propiedades de varios valores es una coma (,). Si un valor individual de una propiedad especificada contiene una coma, debe estar precedida por una barra diagonal inversa (\). Las comas dentro de propiedades que sólo tienen un valor único no se interpretan como delimitadores y, por lo tanto, no necesitan estar precedidas por una barra diagonal inversa.

Nota – El subcomando `walkprop` es significativo cuando se utiliza sólo en modo interactivo.

EJEMPLO 4-13 Visualización y cambio de valores de propiedades de un perfil específico

En el siguiente ejemplo, la propiedad `activation-mode` para la ubicación `foo` se visualiza y luego se cambia usando el subcomando `walkprop`. Tenga en cuenta que cuando utiliza el subcomando `walkprop`, no necesita utilizar el subcomando `set` para establecer el valor de la propiedad.

```
$ netcfg
netcfg> select loc foo
netcfg:loc:foo> list
loc:foo
      activation-mode          manual
      enabled                  false
      nameservices             dns
      nameservices-config-file "/etc/nsswitch.dns"
      dns-nameservice-configsrc dhcp
      nfsv4-domain             "Central.oracle.com"
netcfg:loc:foo> walkprop
activation-mode (manual) [manual|conditional-any|conditional-all]> conditional-all
conditions> advertised-domain is oracle.com
nameservices (dns) [dns|files|nis|ldap]>
nameservices-config-file ("/etc/nsswitch.dns")>
dns-nameservice-configsrc (dhcp) [manual|dhcp]>
nfsv4-domain ("Central.oracle.com")>
ipfilter-config-file>
ipfilter-v6-config-file>
ipnat-config-file>
ippool-config-file>
ike-config-file>
```

EJEMPLO 4-13 Visualización y cambio de valores de propiedades de un perfil específico (Continuación)

```
ipsecpolicy-config-file>
netcfg:loc:foo> list
loc:foo
    activation-mode          conditional-all
    conditions               "advertised-domain is oracle.com"
    enabled                  false
    nameservices             dns
    nameservices-config-file "/etc/nsswitch.dns"
    dns-nameservice-configsrc dhcp
    nfsv4-domain            "Central.oracle.com"
netcfg:loc:foo> commit
Committed changes
netcfg:loc:foo> end
netcfg> exit
$
```

Nota – Sólo se recorren las propiedades relevantes. Por ejemplo, si la propiedad `ipv4-addrsrc` se define en `static`, la propiedad `ipv4-addr` se incluye en el recorrido. Sin embargo, si `ipv4-addrsrc` se establece en `dhcp`, la propiedad `ipv4-addr` no se recorre.

Exportación y restauración de la configuración de un perfil

Puede utilizar el subcomando `export` para guardar y restaurar configuraciones de perfiles. La exportación de un perfil puede ser útil para administradores de sistemas responsables del mantenimiento de múltiples servidores que requieren configuraciones de red idénticas. El subcomando `export` se puede utilizar en modo interactivo o en modo de línea de comandos. O bien puede utilizar el comando en modo de archivo de comandos para especificar un archivo como la salida del comando.

La sintaxis del comando para el subcomando `export` es la siguiente:

```
$ netcfg export [ -d ] [ -f output-file ] [ object-type [ class ] object-name ]
```

Nota – Las opciones `-d` y `-f` del subcomando `export` se pueden utilizar de forma independiente de las demás.

EJEMPLO 4-14 Exportación de la configuración de un perfil

En el ejemplo siguiente, el subcomando `export` se utiliza para mostrar la configuración del perfil de un sistema en la pantalla.

```
$ netcfg
netcfg> export
create ncp "User"
```

EJEMPLO 4-14 Exportación de la configuración de un perfil (Continuación)

```

create ncu ip "net2"
set ip-version=ipv4
set ipv4-addrsrc=dhcp
set ipv6-addrsrc=dhcp,autoconf
end
create ncu phys "net2"
set activation-mode>manual
set link-mtu=5000
end
create ncu phys "wpi2"
set activation-mode=prioritized
set priority-group=1
set priority-mode=exclusive
set link-mac-addr="13:10:73:4e:2"
set link-mtu=1500
end
end
create loc "test"
set activation-mode>manual
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domainl.oracle.com"
end
create loc "foo"
set activation-mode=conditional-all
set conditions="system-domain is oracle.com"
set nameservices=dns
set dns-nameservice-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create enm "myenm"
set activation-mode=conditional-all
set conditions="ip-address is-not-in-range 1.2.3.4"
set start="/my/start/script"
set stop="/my/stop/script"
end
create wlan "mywlan"
set priority=0
set bssids="0:13:10:73:4e:2"
end
netcfg> end
$

```

EJEMPLO 4-15 Exportación de la configuración de un perfil en modo interactivo netcfg

En el siguiente ejemplo, la opción `-d` se utiliza con el subcomando `export`. La opción `-d` agrega el comando `destroy -a` como la primera línea de la salida de `netcfg export`.

```

$ netcfg
netcfg> export -d
destroy -a
create ncp "User"
create ncu ip "net2"

```

EJEMPLO 4-15 Exportación de la configuración de un perfil en modo interactivo netcfg (Continuación)

```

set ip-version=ipv4
set ipv4-addrsrc=dhcp
set ipv6-addrsrc=dhcp,autoconf
end
create ncu phys "net2"
set activation-mode=manual
set link-mtu=5000
end
create ncu phys "wpi2"
set activation-mode=prioritized
set priority-group=1
set priority-mode=exclusive
set link-mac-addr="13:10:73:4e:2"
set link-mtu=1500
end
end
create loc "test"
set activation-mode=manual
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create loc "foo"
set activation-mode=conditional-all
set conditions="system-domain is oracle.com"
set nameservices=dns
set dns-nameservice-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create enm "myenm"
set activation-mode=conditional-all
set conditions="ip-address is-not-in-range 1.2.3.4"
set start="/my/start/script"
set stop="/my/stop/script"
end
create wlan "mywlan"
set priority=0
set bssids="0:13:10:73:4e:2"
end
netcfg> end
$

```

EJEMPLO 4-16 Exportación de la configuración de un perfil en el modo de archivo de comandos netcfg

En el siguiente ejemplo, la información de configuración del NCP User se escribe en un archivo mediante el comando `netcfg export` con la opción `-f`. La opción `-f` escribe la salida en un nuevo archivo denominado `user2`. La opción `-d` agrega el comando `destroy -a` como la primera línea de la salida de `netcfg export`.

```

$ netcfg export -d -f user2 ncp User

$ ls -al
drwx----- 3 root  root  4 Oct 14 10:53 .

```

EJEMPLO 4-16 Exportación de la configuración de un perfil en el modo de archivo de comandos netcfg
(Continuación)

```
drwxr-xr-x 37 root    root        40 Oct 14 10:06 ..
-rw-r--r--  1 root    root        352 Oct 14 10:53 user2
$
```

```
$ cat user2
destroy -a
create ncp "User"
create ncu ip "net2"
set ip-version=ipv4
set ipv4-addrsrc=dhcp
set ipv6-addrsrc=dhcp,autoconf
end
create ncu phys "net2"
set activation-mode=manual
set link-mtu=5000
end
create ncu phys "wpi2"
set activation-mode=prioritized
set priority-group=1
set priority-mode=exclusive
set link-mac-addr="13:10:73:4e:2"
set link-mtu=1500
end
end
create loc "test"
set activation-mode=manual
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create loc "foo"
set activation-mode=conditional-all
set conditions="system-domain is oracle.com"
set nameservices=dns
set nameservices-config-file="/etc/nsswitch.dns"
set dns-nameservice-configsrc=dhcp
set nfsv4-domain="domain.oracle.com"
end
create enm "myenm"
set activation-mode=conditional-all
set conditions="ip-address is-not-in-range 1.2.3.4"
set start="/my/start/script"
set stop="/my/stop/script"
end
create wlan "mywlan"
set priority=0
set bssids="0:13:10:73:4e:2"
end
$
```

Restauración de un perfil definido por el usuario

Puede restaurar un perfil definido por el usuario mediante el comando `netcfg` con la opción `-f`, de la siguiente forma:

```
$ netcfg [ -f ] profile-name
```

Por ejemplo:

```
$ netcfg -f user2
```

Este comando ejecuta el archivo de comandos que contiene la configuración exportada.

Gestión de configuración de red

La gestión de configuración de red está basada en el perfil y para su gestión se alterna entre los dos modos de configuración de red: manual y automático. Para cambiar entre los modos, active el NCP adecuado. Para la configuración de red manual, habilite el NCP `DefaultFixed`. Para la configuración de red automática (NWAM), habilite el NCP `Automatic` o un NCP definido por el usuario.

▼ Cómo cambiar del modo de configuración de red automático al modo de configuración de red manual

Si está utilizando funciones de red avanzadas que no son admitidas actualmente por la gestión de configuración de NWAM o si prefiere la gestión de configuración de red manual, puede habilitar el NCP `DefaultFixed`, como se muestra en el siguiente procedimiento.

- 1 **Conviértase en usuario `root`.**
- 2 **Habilite el NCP `DefaultFixed`.**
- 3 **Verifique que el servicio `network/physical:default` se haya reiniciado y esté en línea.**

```
# svcs -xv network/physical:default
svc:/network/physical:default (physical network interface configuration)
  State: online since Fri Aug 26 16:19:18 2011
    See: man -M /usr/share/man -s 1M ipadm
    See: man -M /usr/share/man -s 5 nwam
    See: /var/svc/log/network-physical:default.log
  Impact: None.
#
```

4 Verifique que el NCP DefaultFixed esté activo.

```
# netadm list
netadm: DefaultFixed NCP is enabled;
automatic network management is not available.
'netadm list' is only supported when automatic network management is active.
```

Nota – El comando `netadm` sólo se admite cuando la configuración de red está en el modo automático. Por consiguiente, en el modo manual, la salida del comando sólo se limita a indicar que el perfil `DefaultFixed` está habilitado. No se proporciona información acerca de los otros NCP en el sistema.

▼ Cómo cambiar del modo de configuración de red manual al modo de configuración de red automático

Para volver al modo de configuración de red automático desde el modo de configuración de red manual, habilite el perfil de configuración de red que desea utilizar.

1 Conviértase en usuario root.**2 Habilite un NCP, por ejemplo, Automatic.**

```
# netadm enable -p ncp Automatic
```

3 Verifique que el servicio `network/physical:default` se haya reiniciado y esté en línea.

```
# svcs -xv network/physical:default
svc:/network/physical:default (physical network interface configuration)
  State: online since Fri Aug 26 16:19:18 2011
    See: man -M /usr/share/man -s 1M ipadm
    See: man -M /usr/share/man -s 5 nwam
    See: /var/svc/log/network-physical:default.log
Impact: None.
#
```

4 Compruebe el estado del NCP y de los demás perfiles de NWAM.

```
# netadm list -x
TYPE          PROFILE      STATE      AUXILIARY STATE
ncp           Automatic   online    active
ncu:phys      net0        online    interface/link is up
ncu:ip        net0        online    interface/link is up
ncu:phys      net1        offline   interface/link is down
ncu:ip        net1        offline   conditions for activation are unmet
ncp           User        disabled  disabled by administrator
loc           Automatic   online    active
loc           NoNet       offline   conditions for activation are unmet
#
```

Administración de perfiles de NWAM (tareas)

En este capítulo, se describe cómo utilizar el comando `netadm` para administrar estos perfiles: NCP, ubicaciones, ENM y WLAN. El comando `netadm` también se puede utilizar para administrar NCU, que son los objetos de configuración individuales que conforman un NCP, y para interactuar con el daemon de NWAM (`nwamd`) en ausencia de la interfaz gráfica de usuario de NWAM. Para obtener más información sobre cómo utilizar el comando `netadm`, consulte la página del comando `man netadm(1M)`.

En este capítulo, se describen los siguientes temas:

- “Obtención de información sobre estados de perfiles” en la página 114
- “Activación y desactivación de perfiles” en la página 116
- “Realización de un análisis inalámbrico y conexión a redes inalámbricas disponibles” en la página 119
- “Resolución de problemas de configuración de red de NWAM” en la página 120

Para obtener más información sobre cómo crear perfiles y cómo configurar sus propiedades mediante el comando `netcfg`, consulte el [Capítulo 4, “Configuración de perfiles de NWAM \(tareas\)”](#).

Para obtener información sobre cómo interactuar con la configuración de NWAM y cómo gestionar su configuración de red desde el escritorio mediante la interfaz gráfica de usuario de NWAM, consulte el [Capítulo 6, “Acerca de la interfaz gráfica de usuario de NWAM”](#).

Para ver una introducción a NWAM, consulte el [Capítulo 2, “Introducción a NWAM”](#).

Para obtener más información sobre todos los componentes de NWAM, así como los detalles de configuración de NWAM, consulte el [Capítulo 3, “Configuración y administración de NWAM \(descripción general\)”](#).

Obtención de información sobre estados de perfiles

Puede utilizar el comando `netadm` con el subcomando `list` para mostrar todos los perfiles disponibles en un sistema y su estado actual, o para mostrar un perfil específico y su estado.

La sintaxis del subcomando `list` es la siguiente:

```
netadm list [ -p profile-type ] [ -c ncu-class ] [ profile-name ]
```

Por ejemplo, para mostrar todos los perfiles en un sistema y su estado, escriba el siguiente comando:

```
$ netadm list
TYPE          PROFILE      STATE
ncp           User         disabled
ncp           Automatic    online
ncu:ip        net1         offline
ncu:phys     net1         offline
ncu:ip        net0         online
ncu:phys     net0         online
loc           foo          disabled
loc           test         disabled
loc           NoNet        offline
loc           Automatic    online
$
```

En este ejemplo, se muestra cada perfil definido por el sistema y definido por el usuario que se encuentra en el sistema, y su estado actual. Tenga en cuenta que el subcomando `list` muestra el NCP habilitado y todas las NCU que componen ese NCP concreto.

Visualización del estado actual de un perfil

El tipo de perfil y la clase de NCU se pueden incluir en la sintaxis del comando para identificar un perfil específico. Si se proporciona sólo un tipo de perfil, se muestran todos los perfiles que son de ese tipo. Si un perfil es especificado por nombre, se muestra el estado actual de ese perfil. Si el nombre de perfil no es único, se muestran todos los perfiles con ese nombre.

Entre algunos posibles valores de estado para cada perfil, se incluyen los siguientes:

<code>disabled</code>	Indica un perfil manualmente activado que no se ha habilitado.
<code>offline</code>	Indica un perfil condicionalmente activado o activado por sistema que no se ha activado. Es posible que el perfil no esté activo porque sus condiciones no se han cumplido o porque otro perfil con condiciones más específicas que se han cumplido está activo.

Nota – El estado sin conexión ocurre con más frecuencia en el caso de tipos de perfil que se deben activar uno a la vez, como el perfil de ubicación.

online	Indica un perfil condicionalmente activado o activado por sistema que tiene condiciones que se han cumplido y que se ha activado correctamente. O bien un perfil manualmente activado que se ha habilitado correctamente ante la petición del usuario.
maintenance	Indica que se intentó realizar la activación del perfil, pero que la activación falló.
initialized	Indica que el perfil es válido, pero que no se ha llevado a cabo ninguna acción en el perfil.
uninitialized	Indica que el perfil no está presente en el sistema. Por ejemplo, este estado se puede producir cuando una NCU que corresponde a un enlace físico se elimina del sistema.

EJEMPLO 5-1 Visualización del estado actual de un perfil especificado

El siguiente ejemplo muestra el estado actual del NCP Automatic, que ha sido especificado por nombre:

```
$ netadm list Automatic
TYPE      PROFILE      STATE
ncp       Automatic    online
ncu:ip    net1         offline
ncu:phys  net1         offline
ncu:ip    net0         online
ncu:phys  net0         online
loc       Automatic    online
```

En el ejemplo siguiente, el subcomando `list` se utiliza con la opción `-p` para mostrar todas las ubicaciones que se encuentran actualmente en el sistema:

```
$ netadm list -p loc
TYPE      PROFILE      STATE
loc       foo          disabled
loc       test         disabled
loc       NoNet        offline
loc       Automatic    online
$
```

En el ejemplo siguiente, el subcomando `list` se utiliza con la opción `-c` para mostrar todas las NCU de la interfaz en el NCP actualmente activo:

```
$ netadm list -c ip
TYPE      PROFILE      STATE
ncu:ip    net0         online
```

EJEMPLO 5-1 Visualización del estado actual de un perfil especificado *(Continuación)*

```
ncu:ip      net1      disabled
$
```

Valores de estado auxiliar

El estado auxiliar de un perfil proporciona una explicación sobre el motivo por el que un perfil determinado está en línea o fuera de línea (habilitado o deshabilitado). Para mostrar los valores de estado auxiliar, utilice la opción `-x` con el subcomando `list`, como se muestra en el siguiente ejemplo:

```
$ netadm list -x
TYPE          PROFILE          STATE          AUXILIARY STATE
ncp           Automatic        disabled       disabled by administrator
ncp           User             online         active
ncu:phys     nge0             online         interface/link is up
ncu:ip       nge0             online         interface/link is up
ncu:phys     nge1             offline        interface/link is down
ncu:ip       nge1             offline        conditions for activation are unmet
loc          Automatic        offline        conditions for activation are unmet
loc          NoNet            offline        conditions for activation are unmet
loc          office           online         active
```

Los valores de estado auxiliar varían en función del tipo de perfil. Para obtener información detallada sobre estados auxiliares, consulte la página del comando `man nwamd(1M)`.

Activación y desactivación de perfiles

Los NCP definidos por el usuario, los perfiles de ubicación y los ENM tienen propiedades `activation-mode`. Los valores permitidos para cada perfil son determinados por su tipo.

Para habilitar o deshabilitar manualmente (activar o desactivar) un objeto de configuración o perfil, utilice el comando `netadm enable` o el comando `netadm disable`. Tanto el perfil definido por el sistema como el perfil definido por el usuario se pueden habilitar o deshabilitar si la propiedad `activation-mode` para el perfil especificado se establece en `manual`. La propiedad `activation-mode` se define al crear o modificar un perfil mediante el comando `netcfg`. Para obtener más información, consulte [“Activación de los perfiles NWAM” en la página 58](#).

En un momento dado, debe haber un NCP activo y un perfil de ubicación activo en el sistema. La habilitación de una ubicación o un NCP diferente con un `activation-mode` de `manual` desactiva implícitamente el perfil de ubicación o el NCP actualmente activo. La ubicación actual también se puede desactivar si su propiedad `activation-mode` se establece en `manual`. Si no hay otras ubicaciones disponibles, NWAM vuelve a una de las ubicaciones definidas por el sistema,

ya sea la ubicación automática si la configuración de IP se ha realizado correctamente o la ubicación NoNet. Las ubicaciones condicionales y del sistema se pueden activar manualmente, lo que significa que la ubicación permanece activa hasta que se deshabilite explícitamente. Este comportamiento facilita el cambio de un perfil de ubicación condicional a “siempre activado”. La deshabilitación de la ubicación condicional vuelve el sistema a su comportamiento condicional normal. Cuando cualquier ubicación se habilita de forma manual, el sistema no cambia la ubicación, aunque se cumplan las condiciones de una ubicación habilitada condicionalmente.

Nota – No puede deshabilitar de manera explícita el NCP que está actualmente activo en un sistema, ya que eso, en efecto, cerraría la conectividad de red básica del sistema. Un NCP se deshabilita implícitamente cuando otro NCP se habilita de forma manual. Sin embargo, no hay restricciones en cuanto a la activación de ENM. Ningún ENM o muchos ENM pueden estar activos en un sistema en un momento dado. Por lo tanto, la habilitación o deshabilitación de un ENM no tiene efecto sobre otros ENM actualmente activos.

También puede habilitar o deshabilitar manualmente NCU individuales. Tenga en cuenta que la NCU especificada debe formar parte del NCP actualmente activo y debe tener una propiedad `activation-mode` de `manual`. Si la clase de NCU no se especifica, todas las NCU (una NCU de enlace y una NCU de interfaz con ese nombre) se activan o se desactivan.

La activación y la desactivación de objetos se realizan de manera asíncrona. Por lo tanto, la solicitud para habilitar o deshabilitar puede tener éxito, mientras que la acción (activar o desactivar) falla. Un fallo de este tipo se refleja en el estado del perfil, que cambia a `maintenance`. Esto indica que la última acción realizada en el perfil falló. Para obtener información sobre cómo visualizar el estado de los perfiles, consulte [“Obtención de información sobre estados de perfiles” en la página 114](#).

EJEMPLO 5-2 Habilitación de un perfil

La sintaxis para habilitar manualmente un perfil es la siguiente:

```
netadm enable [ -p profile-type ] [ -c ncu-class ] profile-name
```

Si el nombre de perfil no es único, por ejemplo, si hay varios perfiles con el mismo nombre, pero de distintos tipos, en el sistema, también debe especificar el tipo de perfil.

La opción `-p` se puede usar para especificar uno de los siguientes tipos de perfil:

- `ncp`
- `ncu`
- `loc`
- `enm`

EJEMPLO 5-2 Habilitación de un perfil (Continuación)

Si el tipo de objeto de configuración es `ncu`, la opción `-c` se puede utilizar para distinguir la clase de NCU. La opción `-c` es útil cuando hay dos NCU con un nombre idéntico en el sistema.

Si se utiliza la opción `-c`, debe especificar el tipo de clase `phys` o `ip`.

En el siguiente ejemplo, una ubicación denominada `office` está habilitada:

```
$ netadm enable -p loc office
```

donde el *tipo_perfil* es `loc` y el *nombre_perfil* es `office`. Tenga en cuenta que la opción `-c` *clase_ncu* no se utiliza en este ejemplo porque el tipo de perfil es una ubicación y no un NCP.

```
$ netadm enable -p ncp user
Enabling ncp 'User'
.
.
.
```

Tenga en cuenta que al especificar nombres de perfil, el comando `netadm` distingue entre mayúsculas y minúsculas.

EJEMPLO 5-3 Deshabilitación de un perfil

La sintaxis para deshabilitar manualmente un perfil es la siguiente:

```
netadm disable [ -p profile-type ] [ -c ncu-class ] profile-name
```

Si el nombre de perfil no es único, también debe especificar el tipo de perfil.

La opción `-p` se puede usar para especificar uno de los siguientes tipos de perfil u objeto:

- `ncp`
- `ncu`
- `loc`
- `enm`

Si el tipo de objeto de configuración es `ncu`, la opción `-c` se debe utilizar para distinguir la clase de NCU.

La clase de NCU debe estar especificada como `phys` o `ip`.

Por ejemplo, para deshabilitar manualmente una NCU de enlace denominada `net1`, debe escribir el siguiente comando:

```
$ netadm disable -p ncu -c phys net1
```

EJEMPLO 5-3 Deshabilitación de un perfil (Continuación)

donde el *tipo_perfil* es *ncu*, la *clase_ncu* es *phys* y el *nombre_perfil* es *net1*. Tenga en cuenta que la opción `-c clase_ncu` se utiliza en este ejemplo porque el objeto de configuración es una NCU.

EJEMPLO 5-4 Cambio de perfiles

Para cambiar el NCP activo y habilitar la configuración manual, debe escribir el siguiente comando:

```
$ netadm enable -p ncp DefaultFixed
```

De forma similar, para activar la configuración automática (NWAM) con el NCP automático, debe escribir el siguiente comando:

```
$ netadm enable -p ncp Automatic
```

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

Realización de un análisis inalámbrico y conexión a redes inalámbricas disponibles

Puede buscar redes inalámbricas disponibles y conectarse a ellas mediante el comando `netadm`.

Utilice el comando `netadm scan-wifi nombre_enlace` para analizar un enlace inalámbrico y obtener una lista de redes inalámbricas disponibles.

Utilice el comando `netadm select-wifi nombre_enlace` para seleccionar una red inalámbrica de los resultados del análisis en el enlace especificado como *nombre_enlace* y conectarse a ella. El subcomando `select-wifi nombre_enlace` le solicita una selección Wi-Fi, una clave y una ranura de clave, si es necesario.

Nota – Ya debe haber creado una clave antes de usar el comando `netadm select-wifi`.

También puede desencadenar un análisis posterior de la red para buscar redes inalámbricas disponibles mediante el uso del comando `netadm scan-wifi nombre_enlace`. Tenga en cuenta que un análisis posterior podría no desencadenar un evento de análisis si los resultados nuevos del análisis son idénticos a los resultados existentes del análisis. El daemon `nwamd` realiza el análisis, independientemente de si los datos han cambiado desde el último análisis.

En el ejemplo siguiente, el comando `netadm scan-wifi` se utiliza para realizar un análisis del enlace inalámbrico, *net1*. El comando `netadm select-wifi` se utiliza para mostrar una lista de

redes inalámbricas para realizar la selección. La lista que se muestra se basa en los resultados del análisis que se ha realizado anteriormente en net1.

```
$ netadm select-wifi net1
1: ESSID home BSSID 0:b:e:85:26:c0
2: ESSID neighbor1 BSSID 0:b:e:49:2f:80
3: ESSID testing BSSID 0:40:96:29:e9:d8
4: Other
Choose WLAN to connect to [1-4]: 1
$
```

En este ejemplo, la red inalámbrica que está representada por el número 1 selecciona la red home.

Si la WLAN requiere una clave, se le pedirá que introduzca la clave y la ranura de clave si el WEP está especificado. Por ejemplo:

```
Enter WLAN key for ESSID home: mywlankey
Enter key slot [1-4]: 1
```

Resolución de problemas de configuración de red de NWAM

La información de esta sección describe cómo solucionar problemas de configuración de red de NWAM.

Supervisión del estado actual de todas las conexiones de red

El comando netadm se puede utilizar con el subcomando show-events para recibir y mostrar eventos que están siendo supervisados por el daemon de NWAM, nwamd. Este subcomando proporciona información útil sobre los eventos que están relacionados con el proceso de configuración para perfiles y objetos de configuración, ya que están configurados por NWAM.

La sintaxis del comando netadm show-events es la siguiente:

```
netadm show-events [-v]
```

En el ejemplo siguiente, el comando show-events se utiliza con la opción -v para mostrar eventos en modo detallado:

```
$ netadm show-events -v
EVENT          DESCRIPTION
LINK_STATE     net0 -> state down
OBJECT_STATE   ncu link:net0 -> state online*, interface/link is down
OBJECT_STATE   ncu link:net0 -> state offline, interface/link is down
```

```

OBJECT_STATE      ncu interface:net0 -> state online*, conditions for act
OBJECT_STATE      ncu interface:net0 -> state offline, conditions for act
IF_STATE          net0 -> state (0) flags 2004801
IF_STATE          net0 -> state (0) flags 2004800
IF_STATE          net0 -> state (0) flags 1004803
IF_STATE          net0 -> state index 4 flags 0x0 address fe80::214:4fff:
IF_STATE          net0 -> state (0) flags 1004802
IF_STATE          net0 -> state index 4 flags 0x0 address 129.156.235.229
IF_STATE          net0 -> state (0) flags 1004803
IF_STATE          net0 -> state (0) flags 1004802
IF_STATE          net0 -> state (0) flags 1004803
IF_STATE          net0 -> state (0) flags 1004802
IF_STATE          net0 -> state (0) flags 1004803
IF_STATE          net0 -> state (0) flags 1004802

```

Resolución de problemas de configuración de interfaz de red

El comando `netadm list -x` es útil para determinar por qué una interfaz de red podría no estar configurada correctamente. Este comando muestra las distintas entidades que son configuradas por NWAM, su estado actual y el motivo por el que estas entidades están en ese estado.

Por ejemplo, si un cable está desconectado, puede utilizar el comando `netadm list -x` para determinar si el estado del enlace es fuera de línea y por qué, por ejemplo, el “enlace no funciona”. De forma similar, para la detección de direcciones duplicadas, la salida del comando `netadm list -x` revela que el enlace físico está en línea (en funcionamiento), pero la interfaz IP está en el estado de mantenimiento. En esta instancia, el motivo que se da es que “se ha detectado una dirección duplicada”.

A continuación, se muestra un ejemplo de la salida del comando `netadm list -x`:

```

$ netadm list -x
TYPE          PROFILE      STATE          AUXILIARY STATE
ncp           Automatic   online         active
ncu:phys     net0        offline        interface/link is down
ncu:ip       net0        offline        conditions for activation are unmet
ncu:phys     net1        offline*       need WiFi network selection
ncu:ip       net1        offline        conditions for activation are unmet
ncp          User        disabled       disabled by administrator
loc          Automatic   offline        conditions for activation are unmet
loc          NoNet       online         active
loc          office      offline        conditions for activation are unmet
$

```

Después de determinar el motivo por el que un enlace o una interfaz está fuera de línea, puede corregir el problema. En el caso de una dirección IP duplicada, debe modificar la dirección IP estática que está asignada a la interfaz especificada mediante el comando `netcfg`. Para obtener instrucciones, consulte [“Configuración y cambio de valores de propiedades de un perfil” en la página 99](#). Después de confirmar los cambios, ejecute el comando `netadm list -x` otra vez para verificar que la interfaz ya esté configurada correctamente y que su estado se muestre como `online`.

Otro ejemplo de por qué una interfaz podría no estar configurada correctamente es si no hay WLAN conocidas disponibles. En este caso, el estado del enlace de Wi-Fi aparecerá como `offLine` y la razón sería que “necesita selección de Wi-Fi”. O si se realizó una selección de Wi-Fi, pero una clave es necesaria, la razón sería que “necesita una clave de “Wi-Fi”.

Acerca de la interfaz gráfica de usuario de NWAM

Este capítulo proporciona una introducción a la interfaz gráfica de usuario (GUI) de NWAM, que incluye una descripción de los componentes que conforman la GUI de NWAM. En este capítulo también se incluyen instrucciones básicas para interactuar con NWAM desde el escritorio, controlar las conexiones de red, agregar redes inalámbricas, y crear y gestionar perfiles de red.

En este capítulo no se proporcionan instrucciones paso a paso sobre la gestión de la red exclusivamente mediante la GUI. Para obtener instrucciones detalladas, consulte la ayuda en pantalla, a la que se puede acceder haciendo clic con el botón derecho del mouse en el icono de estado de red que aparece en el área de notificación de panel del escritorio en todo momento. Los enlaces dentro de la GUI lo llevan a páginas de la ayuda en pantalla que proporcionan información más detallada sobre cada tema. También puede navegar por la ayuda en pantalla haciendo clic en los enlaces que se muestran en el texto o haciendo clic en los diversos temas en el panel lateral.

En este capítulo, se describen los siguientes temas:

- “Introducción a la interfaz gráfica de usuario de NWAM” en la página 124
- “Componentes funcionales de la GUI de NWAM” en la página 126
- “Interacción con NWAM desde el escritorio” en la página 129
- “Incorporación y gestión de redes inalámbricas favoritas” en la página 132
- “Gestión de perfiles de red” en la página 135
- “Creación y gestión de ubicaciones” en la página 142
- “Sobre los modificadores de red externos” en la página 145

Introducción a la interfaz gráfica de usuario de NWAM

La interfaz gráfica de usuario (GUI) de NWAM es el equivalente gráfico a la interfaz de usuario de línea de comandos de NWAM. La GUI de NWAM permite ver y supervisar el estado de la red en el escritorio, así como interactuar con NWAM para gestionar Ethernet y la configuración inalámbrica. Además, puede realizar varias tareas de red desde el escritorio, como conectarse a una red con cables o inalámbrica al inicio y realizar la configuración de nuevas redes con cables o inalámbricas. La GUI de NWAM también se puede utilizar para crear y gestionar ubicaciones, que son perfiles que simplifican la tarea compleja de realizar la configuración de red en todo el sistema. La GUI incluye una función que muestra notificaciones sobre el estado actual de la conexión de red, así como información sobre el estado general de su entorno de red.

Entre las capacidades básicas de la GUI de NWAM se incluyen:

- Notificación de estado de red
- Detección de eventos de conexión directa
- Creación y gestión de perfiles de red
- Gestión de redes inalámbricas

La GUI de NWAM gestiona la configuración de red de la misma manera como lo hace la interfaz de línea de comandos de NWAM, ya que almacena los valores de propiedad deseados en forma de perfiles en el sistema. El servicio NWAM determina qué perfil debería estar activo en un momento determinado, en función de las condiciones de red actuales y, entonces, activa el perfil más apropiado.

Acceso a la GUI de NWAM desde el escritorio

Hay dos componentes que conforman la interfaz gráfica de NWAM: el icono de notificación de estado de red que se muestra continuamente en el panel del escritorio y los cuadros de diálogo de configuración de red a los que se puede acceder tanto desde el menú Sistema → Administración o haciendo clic con el botón derecho del mouse en el icono de notificación. La GUI de NWAM se comporta de la misma manera que cualquier otra aplicación que tiene un icono de notificación de estado continuo, por ejemplo, el icono de gestión de energía o el icono de impresora. Estas aplicaciones permiten realizar ciertas tareas mediante el acceso al menú contextual (botón derecho) o mediante los cuadros de diálogo de configuración a los que se accede desde el icono o desde distintos menús de preferencias.

El icono del panel es su punto de contacto con NWAM más frecuente. El icono muestra si está conectado actualmente a una red con cables o inalámbrica. Al pasar el mouse sobre el icono, una sugerencia de herramienta muestra información adicional, como el NCP y el perfil de ubicación actuales. Al hacer clic con el botón derecho en el icono, puede cambiar la configuración básica de la red de su sistema, por ejemplo, puede conectarse a una red inalámbrica diferente.

Si hace clic (con el botón izquierdo), el icono del panel abre el cuadro de diálogo de preferencias de red. Este cuadro de diálogo también se puede abrir desde el menú Sistema → Administración. Aquí puede realizar una configuración más detallada de la red, como definir direcciones IPv4 e IPv6 estáticas, establecer la prioridad de las conexiones, gestionar los modificadores de red externos (ENM) y crear grupos de ajustes de red para usar en distintas ubicaciones.

Diferencias entre la interfaz de línea de comandos de NWAM y la interfaz gráfica de usuario de NWAM

Puede gestionar la configuración de red mediante NWAM ya sea usando la interfaz de línea de comandos (CLI) o la interfaz gráfica de usuario (GUI). Puede utilizar ambas interfaces de usuario para gestionar la configuración de red e interactuar con la configuración de NWAM. El hecho de utilizar la CLI o la GUI para llevar a cabo una tarea concreta depende de la tarea y de la situación determinada. Para algunas tareas, la elección más lógica es utilizar la GUI de NWAM. Un ejemplo sería comprobar el estado de la conexión de red activa actualmente o seleccionar una red inalámbrica para conectarse en el inicio. Estas tareas se pueden realizar más fácil y rápidamente al interactuar directamente con NWAM desde el escritorio mediante la GUI. Para realizar tareas más complicadas, como especificar una secuencia de comandos, la hora de inicio y el método de detención para un ENM nuevo, puede elegir trabajar en el modo de CLI.

Aunque tanto la CLI como la GUI son fundamentalmente lo mismo, deben tenerse en cuenta las siguientes diferencias:

- **Diferencias de funcionalidad**

La GUI incluye una funcionalidad que le permite interactuar con NWAM y comprobar las conexiones de red desde el escritorio. El modo cómo se obtiene información sobre el estado de la red varía ligeramente entre las utilidades de GUI y de CLI. Si utiliza el componente de GUI, se muestran las notificaciones en el escritorio cuando se producen. Si utiliza la utilidad de línea de comandos, puede supervisar los eventos de NWAM a medida que ocurren mediante el comando `etadm show-events`. Para obtener más información, consulte [“Supervisión del estado actual de todas las conexiones de red”](#) en la página 120.

Además, para obtener información sobre el estado de su red mediante la GUI, puede comprobarlo visualmente al pasar el mouse o hacer clic en el icono de notificación de estado de red que se muestra en el escritorio. Para obtener información sobre el estado de la red desde la línea de comandos, utilice el comando `netadm` con el subcomando `list`. La salida de este comando proporciona información sobre el estado básico de cada objeto de red que esté configurado en el sistema. Sin embargo, la GUI proporciona información más completa y detalles acerca del estado de la red, como así también de la red inalámbrica a la que está conectado y la dirección IP de la conexión de red.

Algunos de los comandos que se pueden realizar mediante la CLI no se puede realizar mediante la GUI. Por ejemplo, no se puede exportar una configuración de perfil utilizando el componente de GUI. Para exportar una configuración de perfil, utilice el comando `net cfg export`. Para obtener más información, consulte [“Exportación y restauración de la configuración de un perfil” en la página 107](#).

- **Diferencias de nombre del componente y uso de terminología**

En la GUI, un perfil de configuración de red (NCP) es lo mismo que un *perfil de red*. Lo que se denomina unidades de configuración de red (NCU) en la CLI, se conocen como *conexiones de red* en la GUI.

La habilitación y deshabilitación de NCP mediante la interfaz de línea de comandos es la misma que la tarea de *cambio de perfiles de red o conexiones* si se utiliza la GUI.

Componentes funcionales de la GUI de NWAM

La GUI de NWAM incluye varios componentes funcionales que se utilizan para realizar prácticamente las mismas tareas que se pueden realizar mediante la CLI. La [Tabla 6-1](#) describe cada uno de estos componentes. Tenga en cuenta que se puede acceder a algunos cuadros de diálogo o se los puede abrir de varias formas diferentes. Además, algunos cuadros de diálogo muestran información distinta, en función de cómo se haya accedido a él. En las secciones relacionadas a lo largo de este capítulo puede obtener información específica sobre estas diferencias y en la ayuda en pantalla puede obtener explicaciones detalladas.

TABLA 6-1 Componentes principales de la GUI de NWAM

Componente	Función	Cómo acceder
Icono de notificación de estado de red	Método para ver el estado de la red e interactuar con NWAM desde el escritorio. El icono también contiene un menú contextual al que se puede acceder para crear y gestionar la configuración de red con la GUI.	<ul style="list-style-type: none"> ▪ Mediante el icono, que aparecerá en el área de notificación del panel del escritorio en todo momento. ▪ Al pasar el mouse sobre el icono para que aparezca una sugerencia de herramientas que proporciona información sobre el estado de la red actual. ▪ Al hacer clic en el icono, que muestra el cuadro de diálogo de preferencias de red. ▪ Al hacer clic con el botón derecho en el icono, que abre el menú contextual.

TABLA 6-1 Componentes principales de la GUI de NWAM (Continuación)

Componente	Función	Cómo acceder
Cuadro de diálogo Preferencias de red	<p>Método para activar y gestionar los dos tipos de perfil de red principales: el perfil automático definido por el sistema y los perfiles de red múltiples definidos por el usuario. Los perfiles de red automáticos y definidos por el usuario gestionan la configuración de red para las interfaces de red individuales.</p> <p>Este cuadro de diálogo también se utiliza para configurar las direcciones IPv4 e IPv6 en interfaces de red individuales y para gestionar redes inalámbricas favoritas.</p>	<ul style="list-style-type: none"> ■ Al hacer clic en el icono de notificación de estado de red en el escritorio. ■ Al seleccionar Sistema → Administración → Red en la barra del menú principal del panel del escritorio. ■ Al seleccionar las preferencias de red desde el menú del icono de notificación de estado de red.
Cuadro de diálogo Ubicaciones de red	<p>Método para crear, activar y gestionar las propiedades de los perfiles de ubicación definidos por el sistema y por el usuario. Las ubicaciones especifican ciertos elementos de una configuración de red, por ejemplo, la configuración de un servicio de nombres y del cortafuegos, que se aplican en conjunto cuando es necesario.</p>	<ul style="list-style-type: none"> ■ Al seleccionar ubicaciones de red desde el menú del botón derecho del icono de notificación de estado de red. ■ O bien, en la vista del Estado de conexión del cuadro de diálogo Preferencias de red, haga clic en el botón Ubicaciones.

TABLA 6-1 Componentes principales de la GUI de NWAM (Continuación)

Componente	Función	Cómo acceder
Cuadro de diálogo Incorporarse a red inalámbrica	Método para incorporar redes inalámbricas y gestionar una lista de redes favoritas. Nota – Este cuadro de diálogo se abre automáticamente si intenta agregar una red inalámbrica y más información sobre dicha red.	<ul style="list-style-type: none"> ■ Al seleccionar la opción Incorporarse a red inalámbrica que no está en la lista que aparece en el menú contextual del icono de notificación. ■ Al hacer clic en el botón Incorporarse a red inalámbrica que no está en la lista en el cuadro de diálogo del selector de red inalámbrica. ■ Al hacer clic en un mensaje de notificación que indica que no se encontraron redes inalámbricas y que haga clic en el mensaje para incorporarse a red inalámbrica que no está en la lista.
Cuadro de diálogo de selector de red inalámbrica	Método para elegir una red inalámbrica y conectarse a ella.	Al hacer clic en un mensaje de notificación que dice, “ <i>interfaz</i> desconectada de <i>ESSID</i> . Haga clic en este mensaje para ver otras redes disponibles”. Nota – Este cuadro de diálogo se abre automáticamente siempre que haya una elección de redes inalámbricas disponible para incorporarse.
Cuadro de diálogo Modificadores de red	Método para agregar aplicaciones del modificador de red externo que son capaces de la creación o modificación de la configuración de red.	<ul style="list-style-type: none"> ■ Al hacer clic en el botón Modificadores en la vista Estado de conexión del cuadro de diálogo Preferencias de red. ■ Al hacer clic con el botón derecho del mouse en el icono de notificación de estado de red y al seleccionar la opción del menú Preferencias de modificador de red.

Interacción con NWAM desde el escritorio

El icono de notificación de estado de red, que se muestra en el área de notificaciones del panel del escritorio en todo momento es el método principal para ver el estado de su red y para interactuar con los procesos de configuración de red automática. El icono de notificación de estado de red es también donde se muestran los mensajes informativos acerca de la red. El menú contextual (botón derecho) del icono le permite un acceso rápido a la funcionalidad de red esencial. El aspecto del icono indica el estado general de la red.

Comprobación del estado de la conexión de red

La forma más rápida de obtener información esencial acerca de la red consiste en fijarse en el icono de notificación de estado de la red que se muestra en el área de notificación de panel del escritorio. El icono de notificación de estado de la red es el método principal para ver el estado actual de la conexión de red activa y para interactuar con NWAM. El aspecto del icono cambia según el estado de la conexión de la red habilitada. Otra forma de poder visualizar información sobre su red actualmente conectada es pasar el puntero del mouse sobre el icono de notificación de estado de red. Para acceder al menú contextual del icono de la notificación, haga clic en el icono con el botón derecho del mouse. Desde aquí se puede cambiar la interfaz de red habilitada y ver información más detallada sobre la red inalámbrica (si la hay) a la que está conectado.

Nota – El icono de notificación de estado de la red sólo se muestra en el escritorio si está utilizando NWAM para configurar automáticamente la red.

La siguiente tabla ilustra la apariencia del icono de estado de red, que cambia para reflejar el estado de las conexiones de red habilitadas en su sistema.

Icono	Estado	Descripción
	Todas en línea (con cables)	Indica que todas las conexiones habilitadas manualmente que están en el perfil de red habilitado están en línea y que la cantidad requerida de conexiones en el grupo de perfil habilitado (si ese grupo existe) está en línea. La “cantidad requerida” es la siguiente: <ul style="list-style-type: none"> ■ Una conexión si el grupo tiene prioridad de tipo Exclusiva ■ Una o más conexiones si el grupo tiene prioridad de tipo Compartida ■ Todas las conexiones del grupo, si el grupo tiene prioridad del tipo Todas

Icono	Estado	Descripción
	Todas en línea (inalámbrica)	Indica que todas las conexiones habilitadas manualmente en el perfil de red habilitado están en línea y que la cantidad requerida de conexiones en el grupo de perfil habilitado (si ese grupo existe) está en línea. La cantidad requerida es igual a la que se describe en el estado <i>Todas en línea (con cables)</i> . Observe que al menos una conexión en línea es inalámbrica.
	Parcialmente en línea (con cables)	Indica que una o más conexiones de grupo de prioridad o habilitadas manualmente no están en línea, por lo que el estado ya no es <i>Todas en línea</i> . En este ejemplo, hay al menos una conexión con cables en línea. El icono de notificación de estado de red también se muestra como <i>Parcialmente en línea</i> si falta que el usuario realice una acción, por ejemplo, que elija una red inalámbrica disponible o que introduzca una contraseña de red inalámbrica.
	Sin conexión (con cables)	Indica que el servicio NWAM está desactivado o en modo de mantenimiento.

▼ Cómo mostrar detalles acerca de una conexión de red habilitada

- 1 Abra el cuadro de diálogo Preferencias de red y seleccione el estado de conexión de la lista desplegable, si es necesario.

Puede abrir el cuadro de diálogo Preferencias de red de una de las siguientes formas:

- Haga clic en el icono de notificación de estado de red en el escritorio.
- Seleccione Sistema → Administración → Red en la barra del menú principal del panel del escritorio.
- Haga clic con el botón derecho en el icono de notificación de estado de red para abrir su menú y, a continuación, seleccione Preferencias de red.

Para conexiones de red inalámbrica, se muestra la dirección IP, la intensidad de la señal, la velocidad de conexión y el tipo de seguridad.

- 2 **Para ver o editar más propiedades de una conexión de red específica, haga doble clic en la conexión en la lista o seleccione la conexión del menú desplegable de visualización que está ubicado en la parte superior del cuadro de diálogo.**

Control de las conexiones de red desde el escritorio

De manera predeterminada, NWAM intenta mantener una conexión de red en todo momento. Si una conexión red con cables falla, se realiza un intento de conexión a una de las redes inalámbricas favoritas. Si el intento falla, se prueban las demás redes inalámbricas disponibles con su permiso.

También puede cambiar manualmente entre conexiones con cables o inalámbricas, según sea necesario.

Nota – Para todos los tipos de conexiones, el comportamiento de conexión se establece para la sesión actual *solamente*. Al reiniciar el sistema o desconectarlo, se intenta establecer una conexión de red de acuerdo con las prioridades definidas por el perfil de red habilitado.

Puede controlar las conexiones de red desde el escritorio mediante NWAM de las siguientes formas:

- **Modifique la prioridad de conexión predeterminada.**

De manera predeterminada, todas las conexiones de red con cables tienen prioridad sobre todas las conexiones de red inalámbricas. Es decir, sólo se intenta una conexión de red inalámbrica si no se puede establecer una conexión con cables. Si hay más de una red inalámbrica disponible en la ubicación actual, se le solicita que seleccione la red para incorporarse. Este comportamiento es definido por el perfil de red automático, que se activa de manera predeterminada. Para forzar un comportamiento diferente, debe crear y activar un perfil de red diferente.

- **Pase de una red con cable a una red inalámbrica.**

Si el perfil de red automático está habilitado, desconecte los cables de red de todas las interfaces con cables habilitadas.

De manera predeterminada, si hay una de las redes inalámbricas favoritas disponibles, se intenta unirlas en el orden en el que aparecen en la lista de favoritos. De lo contrario, se muestra el cuadro de diálogo del selector inalámbrico. En este cuadro de diálogo puede seleccionar a qué red incorporarse.

Nota – Puede cambiar la forma de incorporación de redes inalámbricas en la ficha Inalámbrico de la vista de propiedades de conexión.

Si hay un perfil de red habilitado diferente del automático, el método que utilice para cambiar a una red inalámbrica depende de la definición de ese perfil de red.

Seleccione uno de los siguientes métodos:

- Use el submenú Conexiones del icono de notificación de estado de red para deshabilitar una conexión con cables y activar una conexión inalámbrica. Tenga en cuenta que este método sólo es posible si ambas conexiones tienen el tipo de activación manual.
- Edite el perfil de red habilitado para activar la conexión con cables y deshabilitar otras conexiones, según sea necesario.

Cuando la conexión inalámbrica está establecida, se muestra un mensaje de notificación.

- **Pase de una red inalámbrica a una red con cables.**

Si el perfil de red automático está habilitado, conecte un cable de red a una interfaz con cables disponible.

Si hay un perfil de red habilitado diferente del automático, el método que utilice para pasar a una red con cables depende de la definición de ese perfil de red.

Seleccione uno de los siguientes métodos:

- Use el submenú Conexiones del icono de notificación de estado de redes para deshabilitar una conexión inalámbrica y activar una conexión con cables. Tenga en cuenta que este método sólo es posible si ambas conexiones tienen el tipo de activación manual.
- Edite el perfil de red habilitado para habilitar la conexión con cables y deshabilitar la conexión inalámbrica.

Cuando la conexión con cables está establecida, se muestra un mensaje de notificación.

Para otras tareas que se pueden realizar mediante la GUI de NWAM, consulte la ayuda en línea.

Incorporación y gestión de redes inalámbricas favoritas

De manera predeterminada, cuando se habilitan conexiones de red inalámbrica, NWAM intenta conectarse a cualquier red disponible de la lista de favoritos, sin preguntar, en el orden de prioridad en el que se muestran las conexiones. Si no hay redes favoritas disponibles, se abre el cuadro diálogo del seleccionador inalámbrico. En este cuadro de diálogo, puede elegir a qué red inalámbrica incorporarse.

También puede modificar la manera en la que se intentan las conexiones inalámbricas en la ficha Inalámbrico de la vista Propiedades de conexión del cuadro de diálogo Preferencias. Si es necesario, puede conectarse manualmente a otra red inalámbrica; para esto puede acceder al menú contextual del icono de notificación de estado de red.

Consejo – Puede acceder a la vista de Propiedades de conexión para una red seleccionada mediante el cuadro de diálogo de Preferencias de red. Este cuadro de diálogo contiene una lista desplegable con la etiqueta Mostrar. Esta lista le permite alternar entre las vistas para una red determinada. En cada vista, hay diferentes tareas que puede realizar, así como información sobre la red seleccionada que es específica para esa vista.

Las siguientes vistas existen para cada conexión de red en cada perfil de red que está en el sistema:

- Estado de conexión
- Perfil de red
- Propiedades de conexión

Para obtener más información acerca del perfil de red, incluida una descripción del cuadro de diálogo de Preferencias de red, consulte, [“Gestión de perfiles de red” en la página 135](#).

▼ **Cómo incorporar una red inalámbrica**

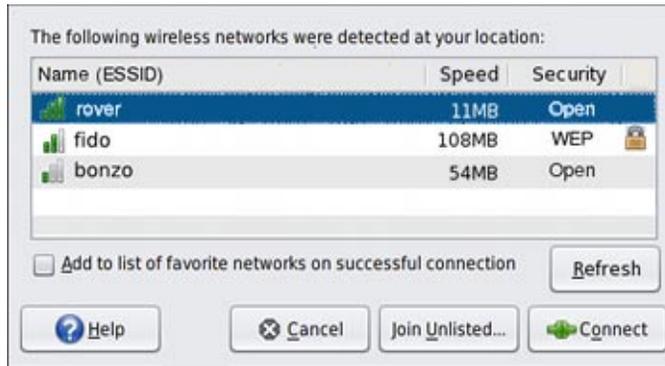
Las redes inalámbricas se incorporan mediante la selección de la opción Incorporarse a red inalámbrica a la que puede accederse haciendo clic con el botón derecho en el icono de notificación de estado de red. El cuadro de diálogo de selector de red inalámbrica es donde selecciona una red inalámbrica para conectarse, desde una lista de redes disponibles que se muestra.

1 Para conectarse manualmente a una red inalámbrica diferente, puede realizar una de las siguientes acciones:

- **Seleccione una red inalámbrica disponible desde el icono de notificación de estado de red del menú que aparece al hacer clic con el botón derecho.**
- **Seleccione la opción Incorporarse a red inalámbrica que no está en la lista del menú del icono de notificación de estado de red.**

Una red inalámbrica que no está en la lista es una red que ha sido configurada de modo que no se difunda su nombre de red pero que está disponible para incorporarse a ella.

- Seleccione una red inalámbrica disponible desde el cuadro de diálogo del selector de redes inalámbricas. Este cuadro de diálogo se muestra automáticamente siempre que haya una elección de redes inalámbricas disponible para a las que pueda incorporarse.



- 2 Si se abre el cuadro de diálogo Incorporarse a red inalámbrica, proporcione toda la información necesaria para la red inalámbrica que haya escogido.

Para obtener más detalles sobre la información que quizás deba proporcionar, consulte la ayuda en pantalla de la GUI de NWAM.

Gestión de redes favoritas

De manera predeterminada, cuando se une a una red inalámbrica por primera vez, aparece la casilla de selección Agregar a lista de redes favoritas cuando la conexión sea satisfactoria en el cuadro de diálogo Incorporarse a red inalámbrica.

- Para agregar la red inalámbrica a su lista de favoritas, si la conexión es satisfactoria, active esta casilla. Si no desea que se agregue la red a su lista de favoritas, desactive esta casilla. La casilla está activada de manera predeterminada.
- Para agregar una red inalámbrica que no está disponible actualmente o que no informa actualmente su nombre de red a su lista de favoritas, vaya a la ficha Inalámbrico de la vista Propiedades de conexión y haga clic en el botón Agregar. Para agregar una red, debe conocer su nombre de red, su tipo de seguridad y su clave de seguridad.



Gestión de perfiles de red

Cuando utilizando la GUI de NWAM, los perfiles de red son el equivalente a los NCP que se describen en [“Descripción de un NCP” en la página 48](#).

Un perfil de red especifica qué interfaces de red se pueden habilitar o deshabilitar en un momento dado. El uso de perfiles de red puede ser beneficioso en situaciones en las que tiene más de una interfaz disponible. Por ejemplo, la mayoría de las marcas modernas de equipos portátiles tienen tanto interfaces con cables como interfaces inalámbricas. En función de su ubicación física y su entorno de trabajo, quizás quiera usar solamente una de esas interfaces y deshabilitar las otras interfaces por seguridad o por otros motivos.

Hay dos tipos de perfiles de red disponibles en la GUI de NWAM, el perfil de red automático y el perfil de red definido por el usuario. Puede habilitar y deshabilitar ambos tipos de perfiles. Puede modificar los perfiles definidos por el usuario, pero no el perfil automático. No puede crear ni destruir el perfil automático mediante la GUI de NWAM o la CLI. Sin embargo, sí puede crear, modificar y destruir perfiles de red definidos por el usuario mediante la GUI o la CLI.

De manera predeterminada, el perfil automático primero intenta habilitar una conexión con cables. Si ese intento falla, intenta habilitar una conexión inalámbrica.

Acerca del cuadro de diálogo Preferencias de red

El cuadro de diálogo Preferencias de red muestra dónde se configuran las conexiones individuales de red y cómo se visualiza el estado actual de cada conexión. El cuadro de diálogo proporciona acceso a distintas vistas que puede alternar mediante la lista desplegable situada en la parte superior del cuadro de diálogo.

Puede abrir el cuadro de diálogo de las siguientes maneras:

- Al hacer clic en el icono de notificación de estado de red en el escritorio.
- Al seleccionar Sistema → Administración → Red en la barra del menú principal del panel del escritorio.
- Al seleccionar las preferencias de red desde el menú del icono de notificación de estado de red.

En la parte superior del cuadro de diálogo Preferencias de red hay una lista desplegable con la etiqueta Mostrar. Esta lista le permite alternar entre la vista de Estado de conexión, la vista de Perfil de red y la vista de Propiedades de conexión para cada conexión de red en cada perfil de red.

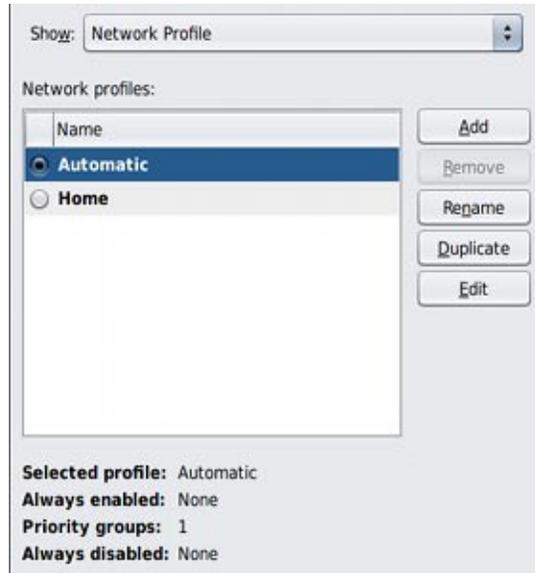
Vista de Estado de conexión

- La vista de Estado de conexión muestra información acerca de cada conexión de red habilitada en el perfil de red habilitado que tienen un tipo de activación manual y cada conexión (ya sea habilitada o deshabilitada) en el grupo de prioridad activo. La sección Conexiones habilitadas: muestra todas las conexiones habilitadas, en el mismo orden en que se muestran en la vista de perfil de red. Consulte [“Cómo mostrar detalles acerca de una conexión de red habilitada”](#) en la página 130.

Vista Perfil de red

- La información de perfil de red puede verse en la vista Perfil de red del cuadro de diálogo Preferencias de red.

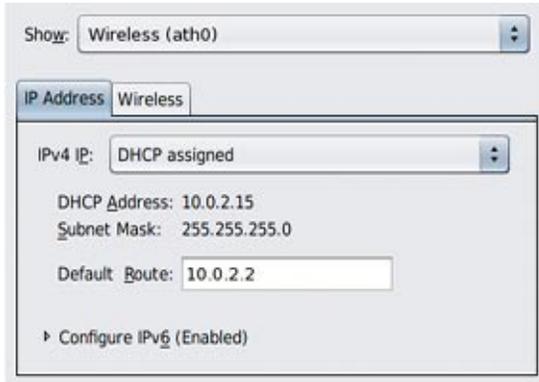
Para mostrar esta vista, seleccione Perfil de red de la lista desplegable que se encuentra en la parte superior del cuadro de diálogo Preferencias de red.



Vista de propiedades del conexión

- La vista Propiedades de conexión le permite ver y cambiar las propiedades de una conexión de red especificada. Para pasar a esta vista, seleccione el nombre de conexión desde la lista del menú desplegable Mostrar o haga doble clic en el nombre de la conexión mientras está en el Estado de conexión o en la vista Perfil de red. Se muestra una vista con fichas en las que puede ver o editar las propiedades de la conexión.

La vista Propiedades de conexión sólo tiene dos fichas: una ficha de dirección IP y una ficha de red inalámbrica. La ficha de conexión inalámbrica sólo se muestra si el tipo de conexión es inalámbrico. En esta ficha de dirección IP puede configurar las direcciones IPv4 e IPv6. En la ficha de redes inalámbricas, puede configurar la lista de redes favoritas y elegir cómo conectar las interfaces inalámbricas a las redes disponibles.



Visualización de información sobre los perfiles de red

La información de perfil de red puede verse en la vista Perfil de red del cuadro de diálogo Preferencias de red.

Para mostrar esta vista, seleccione Perfil de red de la lista desplegable que se encuentra en la parte superior del cuadro de diálogo Preferencias de red.

La lista de perfiles de red muestra el nombre de cada perfil de red disponible. El perfil habilitado actualmente se muestra con un indicador de botón de opción. De forma predeterminada, hay un perfil, el automático, que puede activar, pero no puede editarlo ni suprimirlo. Sin embargo, puede crear varios perfiles de red adicionales. Los perfiles de red que se crean manualmente se pueden activar, editar o suprimir, según sea necesario.

Debajo de la lista de perfiles de red hay un resumen del perfil seleccionado. Para ver el perfil seleccionado en su totalidad o editar el perfil, haga clic en el botón Editar.

Nota – El perfil *seleccionado* puede no coincidir con el perfil *habilitado*.

Cómo cambiar de un perfil de red a otro

1. Abra la vista Perfil de red del cuadro de diálogo Preferencias de red.
2. Seleccione el botón de opción situado junto al perfil de red que desea activar.
3. Para cambiar los perfiles de red, haga clic en Aceptar o haga clic en Cancelar para cerrar el cuadro de diálogo sin cambiar los perfiles.

Cómo agregar o eliminar un perfil de red

Para crear o editar un perfil de red, seleccione Perfil de red desde la lista desplegable que se encuentra en la parte superior del cuadro de diálogo Preferencias de red.

- Para crear un nuevo perfil de red, haga clic en el botón Agregar y, a continuación, escriba el nombre del nuevo perfil.
- Para duplicar un perfil de red existente, seleccione el perfil de la lista, haga clic en el botón Duplicar y, a continuación, escriba el nombre del nuevo perfil.
- Para eliminar un perfil de red, seleccione el perfil en la lista y, a continuación, haga clic en el botón Eliminar.

Nota – No puede eliminar el perfil de red automático.

Para obtener más información acerca de la edición de un perfil que haya agregado o duplicado, consulte [“Cómo editar perfiles de red” en la página 139](#).

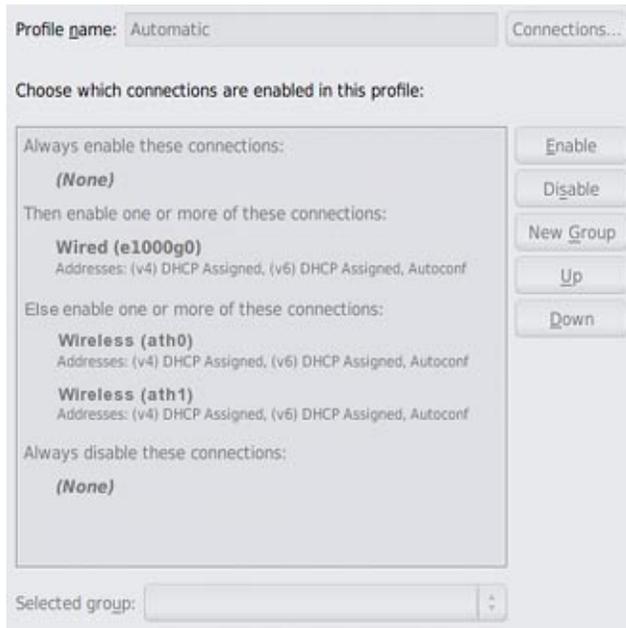
Cómo editar perfiles de red

Cuando agrega manualmente un nuevo perfil de red o duplica uno existente, debe editar el nuevo perfil para especificar las conexiones de red que están habilitadas y deshabilitadas para el nuevo perfil.

Nota – Puede editar y eliminar un perfil de red creado manualmente. Sin embargo, no puede editar o eliminar el perfil de red automático.

▼ Cómo abrir el cuadro de diálogo de perfil de red

- Para editar un perfil de red, seleccione el perfil en la vista Perfil de red del cuadro de diálogo Preferencias de red y, a continuación, haga clic en el botón Editar.



La lista de perfiles de red consta de un mínimo de dos descripciones de grupo de nivel superior. Por ejemplo, el perfil automático, que se muestra en la figura anterior, contiene cuatro descripciones de grupo que se explican con más detalles en las secciones siguientes.

Nota – El perfil de red Automático no se puede cambiar ni suprimir. En cualquier momento que se seleccione el perfil de red automático en el cuadro de diálogo Editar perfil de red, todos los botones de edición del perfil y listas desplegadas se deshabilitan.

Para obtener más información, consulte la ayuda en línea.

Trabajo con grupos de prioridades

Una conexión de red en el grupo “siempre habilitado” siempre está habilitada cuando el perfil de red seleccionado está activo.

Para mover una conexión de red al grupo “siempre habilitado”, primero seleccione la conexión y, a continuación, realice una de las siguientes acciones:

- Haga clic en el botón Habilitar.
- Haga clic en el botón Arriba hasta que la conexión se mueva al grupo “siempre habilitado”.

Una conexión de red en el grupo “siempre inhabilitado” está siempre inhabilitada cuando el perfil de red está activo.

Para mover una conexión de red al grupo “siempre inhabilitado”, primero seleccione la conexión y, a continuación, realice una de las siguientes acciones:

- Haga clic en el botón Inhabilitar.
- Haga clic en el botón Abajo hasta que la conexión se mueva al grupo “siempre inhabilitado”.

Puede crear un perfil de red que trate a una o más interfaces de red como un grupo. Si una o más de las interfaces del grupo de prioridad más alta no se pueden habilitar, según el tipo de prioridad de grupo, se toma en cuenta el grupo con la siguiente prioridad más alta.

En la siguiente tabla se describen los tres grupos diferentes de prioridades que están disponibles.

Tipo de prioridad	Descripción
Exclusive	Hay una conexión habilitada en el grupo, y todas las demás conexiones están inhabilitadas. Siempre que haya una conexión en el grupo habilitada (no necesariamente la misma todo el tiempo) no se realiza ningún intento de habilitar conexiones en ninguno de los demás grupos de prioridad más baja.
Shared	Se habilitan todas las conexiones del grupo que se pueden activar. Siempre que haya al menos una conexión en el grupo habilitada, no se intenta habilitar las conexiones en ningunos de los grupos de prioridades más bajas.
All	Se habilitan todas las conexiones del grupo. Si alguna de las conexiones se pierde, todas las conexiones del grupo se inhabilitan. Siempre que todas las conexiones permanezcan habilitadas, no se realizan intentos para habilitar conexiones en ninguno de los grupos de prioridades más bajas.

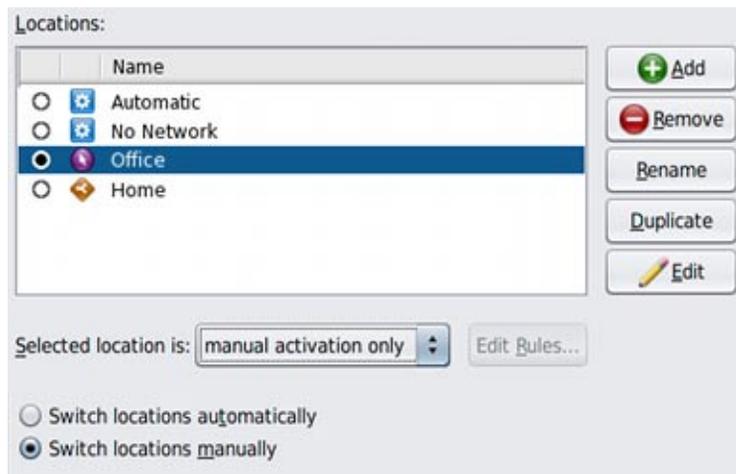
Por ejemplo, el perfil de red automático predeterminado contiene dos grupos de prioridad exclusiva. El grupo con la prioridad más alta contiene todas las conexiones de red *con cables*. El grupo con la prioridad más baja contiene todas las conexiones de red *inalámbricas*.

Para obtener instrucciones detalladas sobre la realización de estas y otras tareas, consulte la ayuda en pantalla.

Creación y gestión de ubicaciones

Una ubicación comprende ciertos elementos de configuración de una red, por ejemplo, ajustes de servicio de nombre y de cortafuegos, que se aplican en conjunto, cuando es necesario. Puede crear varias ubicaciones para varios usos. Por ejemplo, una ubicación se puede utilizar cuando está conectado en la oficina mediante la intranet de la empresa. Otra ubicación se puede utilizar en su casa cuando está conectado a la red pública de Internet mediante un punto de acceso inalámbrico. Las ubicaciones se pueden activar manual o automáticamente, según las condiciones ambientales, como la dirección IP que se obtiene mediante una conexión de red.

El cuadro de diálogo Ubicaciones de red le permite cambiar ubicaciones, editar propiedades de ubicación, crear nuevas ubicaciones y eliminar otras. Tenga en cuenta que sólo se pueden crear y eliminar ubicaciones creadas por el usuario. El cuadro de diálogo Ubicaciones puede abrirse desde la vista de estado de conexión del cuadro de diálogo Preferencias de red.



La lista Ubicaciones es similar a la lista en el menú del icono de la notificación de estado de red. Se muestra cada ubicación disponible, con un icono que representa su tipo de activación.

Los tipos de ubicación son los siguientes:

- Sistema: las ubicaciones con este tipo son ubicaciones definidas por el sistema (Automatic o NoNet), lo que significa que el sistema determina cuándo activar la ubicación, en función de las condiciones actuales de la red.
- Manual: las ubicaciones con este tipo se pueden habilitar o deshabilitar manualmente mediante el cuadro de diálogo Ubicaciones de red o mediante la interacción con el icono de notificación de estado de red.

- Condicional: las ubicaciones con este tipo se pueden habilitar o deshabilitar automáticamente, de acuerdo con las reglas que especifique durante la creación de la ubicación.

El tipo de activación de una ubicación seleccionada también se muestra en la lista desplegable del menú de Ubicación seleccionada. La ubicación habilitada se representa mediante un botón de opción seleccionado que se muestra en la primera columna de la lista.

▼ **Cómo cambiar el modo de activación de una ubicación**

La siguiente tarea describe cómo cambiar el modo de activación de una ubicación mediante la GUI de NWAM. Si está utilizando el comando `net cfg`, tendría que cambiar el modo de activación mediante la modificación de las propiedades de la ubicación especificada. Para obtener más información, consulte [“Configuración y cambio de valores de propiedades de un perfil” en la página 99](#).

- 1 Desde el submenú de ubicación del icono de notificación de estado de red, seleccione Ubicaciones de red. O bien, en la vista del Estado de conexión del cuadro de diálogo Preferencias de red, haga clic en el botón Ubicaciones.**
- 2 Para cambiar el modo de activación de una ubicación, seleccione la ubicación en la lista y, a continuación, seleccione el nuevo modo de activación en la lista desplegable Ubicación seleccionada.**

Nota – Tenga en cuenta que cuando se selecciona una ubicación en el sistema, la lista desplegable muestra Activado por sistema, y la lista desplegable y el botón Editar reglas aparecen inhabilitados.

Cuando se selecciona una ubicación manual o condicional, las opciones de la lista desplegable son las siguientes:

- Sólo activación manual: esta ubicación sólo se habilita cuando se selecciona manualmente. Cuando se selecciona esta opción, se *deshabilita* el botón Editar reglas.
 - Activado por reglas: esta ubicación se selecciona automáticamente en determinadas condiciones de red. Cuando se selecciona esta opción, se *habilita* el botón Editar reglas.
- 3 (Opcional) Para establecer reglas acerca de cómo y cuándo se activa una ubicación, haga clic en el botón Editar reglas.**

Para obtener más instrucciones, consulte el “cuadro de diálogo Trabajar con las reglas” en la ayuda en línea.

▼ **Cómo cambiar de una ubicación a otra**

La siguiente tarea describe cómo cambiar de una ubicación a otra ubicación mediante la GUI de NWAM. Para cambiar las ubicaciones utilizando la interfaz de la línea de comandos, utilice el comando `netadm` para activar una nueva ubicación. Como exactamente sólo puede haber una ubicación activada en el sistema en todo momento, la activación de una ubicación nueva deshabilita implícitamente la ubicación habilitada actualmente. La misma regla se aplica al activar un perfil de red. Para obtener más información sobre la activación y la desactivación de ubicaciones, consulte [“Activación y desactivación de perfiles” en la página 116](#).

- **Desde el submenú Ubicación del icono de notificación de estado de red, seleccione la ubicación que desea activar.**

Si se selecciona la opción para cambiar ubicaciones automáticamente en el menú de ubicaciones, no puede seleccionar una ubicación manualmente para activar. La ubicación de sistema o condicional más apropiada se activará automáticamente en cualquier momento determinado, de acuerdo con los cambios en el entorno de red.

Si se selecciona la opción para cambiar ubicaciones manualmente en el submenú de ubicaciones, puede activar cualquier ubicación disponible, sin importar el tipo de activación. La ubicación seleccionada permanece activa indefinidamente.

- **Como alternativa, puede cambiar las ubicaciones en el cuadro de diálogo Ubicaciones de red. Para ello, siga estos pasos:**

- a. **Desde el submenú de ubicación del icono de notificación de estado de red, seleccione Ubicaciones de red. O bien, en la vista del Estado de conexión del cuadro de diálogo Preferencias de red, haga clic en el botón Ubicaciones.**

- b. **Seleccione el botón de opción de la ubicación a la que desea cambiar y, a continuación, haga clic en Aceptar.**

- **Si se selecciona el botón de opción para cambiar ubicaciones automáticamente en el cuadro de diálogo Ubicaciones de red, no puede seleccionar una ubicación manualmente para activar. La ubicación de sistema o condicional más apropiada se activa automáticamente en cualquier momento determinado, de acuerdo con los cambios en el entorno de red.**
- **Si el botón de opción para cambiar ubicaciones manualmente está seleccionado en el cuadro de diálogo Ubicaciones de red, puede activar cualquier ubicación, sin importar el tipo de activación. Tenga en cuenta que la ubicación permanece activa indefinidamente.**

Edición de ubicaciones

Editar una ubicación mediante la GUI de NWAM es el equivalente a modificar las propiedades de una ubicación si está usando la CLI de NWAM.

Para editar una ubicación, seleccione Ubicaciones de red desde el submenú de ubicaciones del icono de notificación de estado de red. O bien, en la vista del Estado de conexión del cuadro de diálogo Preferencias de red, haga clic en el botón Ubicaciones.

Para editar las propiedades de una ubicación especificada, seleccione la ubicación en la lista y haga clic en Editar.

De manera alternativa, puede hacer doble clic en la ubicación de la lista.

Se abre el cuadro de diálogo Editar ubicación con las siguientes dos fichas disponibles:

Servicios de nombres	Permite configurar los servicios de nombres en la ubicación especificada.
Seguridad	Permite seleccionar los archivos de configuración que serán utilizados por el filtro IP y las funciones de IPsec, cuando la ubicación especificada está habilitada.

Para ver la información que se va a editar, seleccione la ficha correspondiente.

Sobre los modificadores de red externos

Los modificadores de red externos (ENM) son los perfiles que se crean para aplicaciones externas a NWAM. Sin embargo, estas aplicaciones pueden crear y modificar la configuración de red. Por ejemplo, las aplicaciones VPN permiten que sus conexiones de red se comuniquen con una red privada virtual. Los ENM se configuran y supervisan en la GUI de NWAM mediante el cuadro de diálogo *Modificadores de red*.

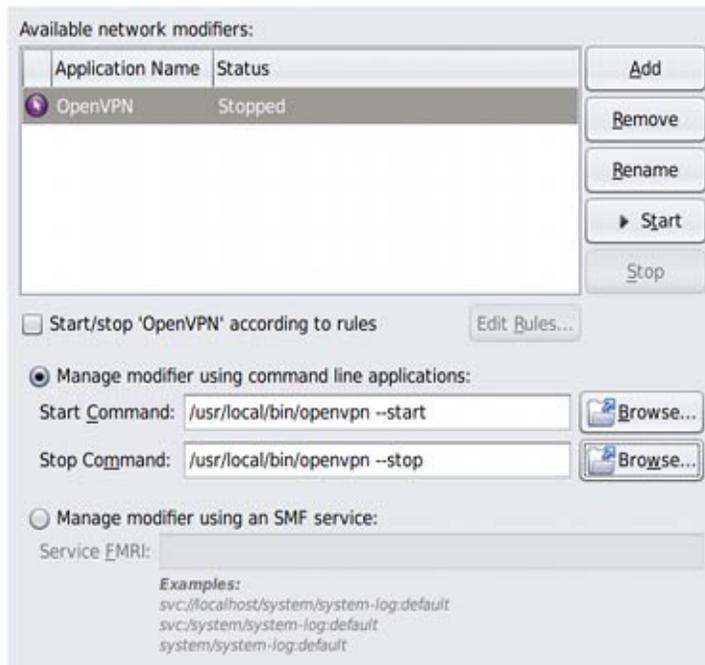
Nota – Antes de poder gestionar una aplicación de modificador de red o servicio mediante la GUI de NWAM, debe instalarla de forma manual y, a continuación, completar cualquier configuración inicial, como la instalación de un certificado o secreto compartido.

Un ENM se puede iniciar y detener manualmente, según sea necesario. Un ENM también se puede iniciar automáticamente, de acuerdo con reglas definidas por el usuario. Para que pueda ser gestionada mediante este cuadro de diálogo, una aplicación de modificador de red debe implementarse como una herramienta de línea de comandos o como un servicio SMF.

Para obtener más información sobre cómo crear y gestionar ENM mediante la CLI de NWAM, consulte [“Creación de un perfil de ENM” en la página 93](#).

Acerca del cuadro de diálogo Modificadores de red

Este cuadro de diálogo se usa para agregar o eliminar, iniciar y detener, y editar modificadores de red externos (ENM), aplicaciones que son capaces de crear y modificar la configuración de red.



Abra el cuadro de diálogo con uno de los siguientes métodos:

- Haga clic en el botón Modificadores en la vista Estado de conexión del cuadro de diálogo Preferencias de red.
- Haga clic con el botón derecho en el icono de notificación Estado de red y, a continuación, seleccione el elemento de menú Preferencias de modificador de red.

La sección principal del cuadro de diálogo es una lista de tres columnas que muestra la siguiente información para cada ENM:

- Estado de activación (manual o condicional)
- Nombre definido por el usuario, por ejemplo, “VPN de Cisco”
- Estado actual, “En ejecución” o “Detenido”

Se marca la casilla Iniciar/detener según las reglas si la aplicación de modificador de red seleccionada tiene el tipo de activación condicional y se anula la selección si el tipo de activación es manual. Para cambiar el tipo de activación, cambie la casilla de verificación.

▼ **Cómo agregar un MNE de línea de comandos**

El siguiente procedimiento describe cómo agregar un MNE de línea de comandos. Para obtener información sobre cómo agregar un servicio de aplicación de modificador de red, consulte la ayuda en pantalla.

- 1 Abra el cuadro de diálogo Modificadores de red mediante uno de los siguientes métodos:**
 - Desde la vista de estado de conexión del cuadro de diálogo de preferencias de red, haga clic en el botón Modificadores.
 - Haga clic con el botón derecho en el icono de notificación Estado de red y, a continuación, seleccione el elemento de menú Preferencias de modificador de red.
- 2 Haga clic en el botón Agregar.**
- 3 Escriba el nombre de la aplicación del nuevo modificador de red.**
- 4 Realice una de las siguientes acciones:**
 - **Para agregar una entrada nueva que tendrá el tipo activación Manual, presione Intro o Tab.**
Se habilitan los dos botones de opción de gestión de modificadores. El primero, Aplicaciones de línea de comandos, está seleccionado de manera predeterminada. Los campos de comando Iniciar y detener y los dos botones Examinar, también se activan.
 - **Para cancelar los cambios, presione Esc.**
- 5 Escriba el comando que inicia el modificador de red en el campo Comando de inicio.**

De manera alternativa, puede usar el botón Buscar para abrir un cuadro de diálogo donde puede seleccionar el comando que va a utilizar.

El botón Inicio permanece inhabilitado para el modificador de red hasta que se escriba un comando válido en el campo.
- 6 Escriba el comando que detiene el modificador de red en el campo Comando de detención.**

De manera alternativa, puede usar el botón Buscar para abrir un cuadro de diálogo donde puede seleccionar el comando que va a utilizar.

El botón Detención permanece inhabilitado para el modificador de red hasta que se escriba un comando válido en el campo.

- 7 Para agregar esta aplicación, haga clic en Aceptar.**
Se agrega el modificador de la red externa.

P A R T E I I

Configuración de interfaz y enlace de datos

En esta parte se analizan los procedimientos de configuración de interfaz y enlace de datos en el contexto de los perfiles de configuración de red, como se mencionó en la [Parte I](#). Los procedimientos se aplican a cualquier perfil fijo que se haya habilitado o activado.

Uso de comandos de configuración de interfaces y enlaces de datos en perfiles

En este capítulo, se describe el uso de comandos de configuración tradicionales, como `dladm` e `ipadm`, ya que se relacionan con la configuración de red basada en perfil.

Características principales de la configuración de red basada en perfil

En esta versión de Oracle Solaris, la configuración de red se basa en perfiles. La configuración de red de un sistema es gestionada por un perfil de configuración de red (NCP) específico y por un perfil de ubicación correspondiente. Para obtener una explicación más detallada de los NCP, los perfiles de ubicación y otros tipos de perfiles, sus propiedades y los comandos que se usan para manipular y supervisar perfiles, consulte la [Parte I](#).

Nota – Para la configuración de red, los tipos de perfiles principales son NCP, perfiles de ubicación, modificadores de red externos (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.
- Los valores de las diferentes propiedades de un NCP constituyen una política que controla cómo el perfil gestiona la configuración de red.

- Los cambios en las propiedades del NCP se implementan de inmediato como nuevos valores de propiedades, que pasan a formar parte de la política del perfil que gestiona la configuración de red.

Nota – En un sistema que ha sido actualizado de la versión Oracle Solaris 11.11 Express, la configuración de red operativa anterior a la actualización se convierte en el perfil activo después de la actualización. Si la configuración anterior fue creada por los comandos `dladm` e `ipadm`, esa configuración constituye el perfil `DefaultFixed`, que se vuelve activo en el sistema. De lo contrario, la configuración se convierte en el perfil `Automatic` que gestiona la configuración de red del sistema.

Herramientas de configuración y perfiles

Las herramientas que se utilizan para personalizar perfiles dependen del perfil activo. Si el perfil activo es reactivo, como `Automatic`, utilice los comandos `netcfg` y `netadm` para configurar y supervisar el perfil. Si el perfil activo es fijo, como `DefaultFixed`, utilice los comandos `dladm` e `ipadm`.

Los comandos `dladm` e `ipadm` sólo son efectivos en perfiles activos. Por lo tanto, antes de utilizar estos comandos, debe asegurarse de lo siguiente:

- Sabe qué perfil está activo para asegurarse de realizar los cambios en el perfil de destino correcto mediante los comandos apropiados.
- Sabe si el perfil de destino es reactivo o fijo para evitar que ocurran comportamientos inesperados 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.

Nota – El uso de la opción `-t` de los comandos `dladm` e `ipadm` para crear valores temporales sólo puede ser efectivo en un perfil fijo. La opción no se admite en perfiles reactivos.

Siga estos dos procedimientos para utilizar de manera adecuada los comandos `dladm` e `ipadm` en los perfiles.

▼ Cómo determinar el modo de gestión de redes

El modo de gestión de redes de un sistema es automático si un NCP reactivo, como `Automatic`, es el NCP activo en el sistema. Utilice este procedimiento para saber el modo de gestión de redes antes de realizar cualquier configuración de red. El procedimiento garantiza que esté utilizando los comandos correctos para implementar la configuración en el perfil adecuado.

1 Muestre los perfiles en el sistema.

```
# netadm list -x
TYPE          PROFILE      STATE        AUXILIARY STATE
ncp           Automatic    online       active
ncu:phys     net0         online       interface/link is up
ncu:ip       net0         online       interface/link is up
ncu:phys     net1         online       interface/link is up
ncu:ip       net1         offline*     waiting for IP address to be set
ncp          testcfg     disabled     disabled by administrator
loc          Automatic    offline      conditions for activation are unmet
loc          NoNet        offline      conditions for activation are unmet
loc          Lab          online       active
loc          User         disabled     disabled by administrator
```

La salida proporciona dos tipos de información:

- El comando `netadm list` sólo se admite si el modo de gestión de redes es automático. Por lo tanto, la generación de una lista de perfiles indica que la gestión de redes está en modo automático. De lo contrario, el comando `netadm list` habría generado el siguiente mensaje para indicar que el perfil `DefaultFixed` está activo en el sistema.

```
netadm: DefaultFixed NCP is enabled; automatic network management is not available.
'netadm list' is only supported when automatic network management is active.
```

- La lista de perfiles, si se genera, también identifica el NCP reactivo específico que está habilitado por medio del estado `online` de ese NCP. En la salida de ejemplo, el NCP `Automatic` aparece como el único NCP reactivo existente. Otros NCP creados por el usuario se habrían incluido en la lista si también estuvieran presentes en el sistema.

2 Asegúrese de que el perfil adecuado esté activo para las herramientas de configuración que desea utilizar.

Por ejemplo, los comandos `dladm` e `ipadm` solamente se pueden usar en el perfil `DefaultFixed`. Sin embargo, el comando `netcfg` solamente se puede usar en perfiles reactivos, como `Automatic`, donde la gestión de redes está en modo automático.

Si el perfil cuyas propiedades desea modificar con las herramientas de configuración seleccionadas no está activo, continúe con el siguiente paso para habilitar el perfil adecuado. De lo contrario, puede empezar a utilizar las herramientas para configurar la red.

Por ejemplo, no desea que la gestión de redes esté en modo automático, pero prefiere utilizar líneas de comando, como `dladm` e `ipadm`, para configurar enlaces de datos e interfaces manualmente. La salida en el paso 1 muestra que el perfil `Automatic` está habilitado. Para utilizar líneas de comando para la configuración de red, debe, por lo tanto, habilitar el perfil `DefaultFixed`.

3 Para configurar un perfil diferente, habilite ese perfil escribiendo lo siguiente:

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

Por ejemplo:

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

Además, puede utilizar la misma sintaxis de comando si la gestión de redes está en modo automático y desea utilizar un NCP reactivo diferente. De la salida de ejemplo del paso 1, suponga que desea activar el NCP creado por el usuario `testcfg` en lugar de `Automatic`. Por lo tanto, escribe:

```
# netadm enable -p ncp testcfg
```



Precaución – El comando alterna perfiles activos. Al alternar perfiles activos, la configuración de red existente se elimina y una nueva configuración se crea. Los cambios persistentes que se implementaron en un NCP previamente activo se excluyen en el nuevo NCP activo.

Pasos siguientes

En los siguientes capítulos, se describen los procedimientos que puede utilizar para realizar varios tipos de configuraciones de enlaces de datos e interfaces.

- Para configurar enlaces de datos, consulte el [Capítulo 8, “Configuración y administración de enlaces de datos”](#).
- Para configurar interfaces IP, consulte el [Capítulo 9, “Configuración de una interfaz IP”](#).
- Para configurar interfaces inalámbricas, consulte el [Capítulo 10, “Configuración de las comunicaciones mediante interfaces inalámbricas en Oracle Solaris”](#).
- Para configurar puentes, consulte el [Capítulo 11, “Administración de puentes”](#).
- Para configurar agregaciones de enlaces, consulte el [Capítulo 12, “Administración de agregaciones de enlaces”](#).
- Para configurar redes VLAN, consulte el [Capítulo 13, “Administración de VLAN”](#).
- Para configurar grupos IPMP, consulte el [Capítulo 14, “Introducción a IPMP”](#) y el [Capítulo 15, “Administración de IPMP”](#).
- Para configurar el protocolo de descubrimiento de capa de enlace (LLDP), consulte el [Capítulo 16, “Intercambio de información de conectividad de red con LLDP”](#).

Configuración y administración de enlaces de datos

En este capítulo, se trata el comando `d'ladm` y cómo se utiliza para configurar enlaces de datos.

Configuración de enlaces de datos (tareas)

En las siguientes tablas, se enumeran las diferentes tareas de configuración de enlaces de datos que se pueden realizar mediante el comando `d'ladm`. Además, se incluyen enlaces a los procedimientos paso a paso que le permiten completar las tareas.

TABLA 8-1 Configuración básica de enlaces de datos (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Cambiar el nombre de un enlace de datos.	Personaliza un nombre de enlace de datos en lugar de utilizar el nombre basado en hardware.	“Cómo cambiar el nombre de un enlace de datos” en la página 158
Mostrar atributos físicos de un enlace de datos.	Muestra información física que subyace a un enlace de datos, incluido el tipo de medio, la instancia de dispositivo asociada y otra información.	“Cómo visualizar información sobre atributos físicos de enlaces de datos” en la página 159
Mostrar el estado de enlaces de datos.	Muestra información sobre el estado de enlaces de datos.	“Cómo visualizar información sobre enlaces de datos” en la página 160
Eliminar un enlace de datos.	Elimina una configuración de enlace que está asociada a una NIC que ya no está en uso.	“Cómo eliminar un enlace de datos” en la página 161

TABLA 8-2 Configuración de propiedades de enlaces de datos (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Modificar el tamaño de la MTU.	Aumenta el tamaño de la MTU de la transmisión de paquetes para manejar tramas gigantes.	“Cómo habilitar la compatibilidad con tramas gigantes” en la página 163
Modificar la velocidad de enlace.	Desactiva la velocidad de enlace superior y anuncia sólo la velocidad de enlace inferior para permitir comunicaciones con un sistema antiguo.	“Cómo cambiar parámetros de velocidad de enlace” en la página 165
Mostrar información sobre propiedades de enlaces.	Muestra propiedades de enlaces y su configuración actual; muestra valores de parámetros de Ethernet.	“Cómo obtener información de estado sobre propiedades de enlaces de datos” en la página 166
Configurar el controlador para utilizar el enlace DMA.	Establece el umbral que hace que el controlador cambie entre el enlace DMA y la función <code>bcopy</code> durante la transmisión.	“Cómo establecer el controlador <code>e1000g</code> para usar el enlace de acceso directo a memoria” en la página 168
Establecer frecuencias de interrupciones.	Permite definir de forma manual las frecuencias a las que el controlador envía interrupciones, en lugar de definir las de forma automática.	“Cómo definir manualmente la frecuencia de interrupciones” en la página 168
Sustituir una tarjeta de interfaz de red (NIC).	Cambia una NIC en un sistema durante la reconfiguración dinámica (DR).	“Cómo sustituir una tarjeta de interfaz de red con reconfiguración dinámica” en la página 171
Establecer propiedades <code>autopush</code> por enlace.	Configura el módulo <code>STREAMS</code> para que se coloque en la parte superior de un enlace de datos.	“Cómo establecer módulos <code>STREAMS</code> en enlaces de datos” en la página 174

El comando `dladm`

Después de la implementación completa de la estructura de configuración del controlador `GLDv3`, el comando `dladm` adquiere capacidades ampliadas a lo largo del tiempo. La estructura mejora la configuración de controladores NIC, de la siguiente forma:

- 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 depósito `dladm` y se mantienen incluso después de reiniciar el sistema.

Para aprovechar las ventajas indicadas anteriormente 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 administrar enlaces de datos, debe utilizar los siguientes subcomandos `dladm`:

- `dladm rename-link` cambia el nombre de un enlace de datos.
- `dladm show-link` muestra enlaces de datos existentes en el sistema.
- `dladm show-phys` muestra atributos físicos de enlaces de datos.
- `dladm delete-phys` elimina un enlace de datos.
- `dladm show-linkprop` muestra las propiedades asociadas con el enlace de datos.
- `dladm set-linkprop` establece propiedades de enlaces de datos especificadas.
- `dladm reset-linkprop` restaura propiedades a sus valores predeterminados.
- `dladm show-ether` muestra valores de parámetros de Ethernet de un enlace de datos.

El comando `dladm` también se usa para realizar otros tipos de administración de enlaces, como los siguientes:

- Configuración de puentes. Consulte el [Capítulo 11, “Administración de puentes”](#).
- Configuración de agregaciones de enlaces. Consulte el [Capítulo 12, “Administración de agregaciones de enlaces”](#).
- Configuración de redes VLAN. Consulte el [Capítulo 13, “Administración de VLAN”](#).
- Configuración de túneles. Consulte el [Capítulo 6, “Configuración de túneles IP”](#) de *Administración de Oracle Solaris: servicios IP*.

Para obtener más información sobre los comandos, consulte la página del comando `man dladm(1M)`.

Los procedimientos siguientes muestran cómo utilizar el comando `dladm` para configurar enlaces de datos. En la mayoría de los casos, la configuración de enlaces de datos es una parte de la configuración de una interfaz IP mediante ese enlace. Por lo tanto, si corresponde, los procedimientos incluyen los pasos de configuración de la interfaz IP con el comando `ipadm`. Sin embargo, la configuración de la interfaz IP y el comando `ipadm` se tratan con mayor detalle en el [Capítulo 9, “Configuración de una interfaz IP”](#).

▼ Cómo cambiar el nombre de un enlace de datos

Utilice este procedimiento si desea cambiar el nombre de un enlace de datos por un nombre personalizado. Por ejemplo, es posible que algunos de los enlaces de datos en el sistema actualizado hayan conservado los nombres basados en hardware anteriores y que usted desee cambiar dichos nombres por nombres genéricos.

Antes de empezar

Asegúrese de haber estudiado y de estar preparado para otros pasos que necesita realizar en configuraciones asociadas que podrían verse afectadas por el cambio de nombres de enlaces. Para obtener más información, consulte [“Nombres de enlace en sistemas actualizados” en la página 29](#).

1 Conviértase en administrador.

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

2 Si una interfaz IP está configurada mediante el enlace de datos, elimine la interfaz IP.

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

3 Cambie el nombre de enlace actual del enlace.

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

nombre_enlace_anterior Hace referencia al nombre actual del enlace de datos. De manera predeterminada, el nombre del enlace está basado en hardware, como bge0.

nombre_enlace_nuevo Hace referencia a cualquier nombre que desea asignar al enlace de datos. Para obtener información sobre las reglas para asignar nombres de enlace, consulte [“Reglas para nombres de enlace válidos” en la página 31](#). Consulte también [“Nombres de enlace en sistemas actualizados” en la página 29](#) para obtener más información sobre el cambio de nombre de enlaces de datos.

Si no desea que el nombre nuevo del enlace se conserve tras un reinicio del sistema, utilice la opción `-t` inmediatamente después del subcomando. La opción cambia el nombre de un enlace temporalmente. El nombre original del enlace vuelve cuando el sistema se reinicia.

Nota – Puede utilizar `dladm rename-link` para transferir configuraciones de enlaces de un enlace de datos a otro. Para ver un ejemplo, consulte [“Cómo sustituir una tarjeta de interfaz de red con reconfiguración dinámica” en la página 171](#). Al cambiar el nombre de un enlace para este propósito, asegúrese de que el enlace que hereda la configuración no tenga ninguna configuración existente anterior. De lo contrario, la transferencia fallará.

Ejemplo 8-1 Cambio de la interfaz de red principal del sistema

El ejemplo siguiente muestra cómo puede cambiar la interfaz de red principal en el sistema por una segunda NIC cambiando el nombre de enlaces de datos. La interfaz de red principal del sistema es `net0`, el nombre genérico del enlace de datos en `e1000g0`. Esta interfaz de red principal cambiará del uso de `e1000g0` como interfaz subyacente a `nge0`. Puede utilizar este ejemplo como parte del procedimiento para crear un nuevo entorno de inicio.

```
# dladm show-phys
LINK   MEDIA   STATE   SPEED   DUPLEX   DEVICE
net0   Ethernet up      1000   full    e1000g0
net1   Ethernet up      1000   full    nge0

# dladm rename-link net0 oldnet0
# dladm rename-link net1 net0

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

▼ Cómo visualizar información sobre atributos físicos de enlaces de datos

Este procedimiento muestra los pasos para visualizar información sobre los atributos físicos de enlaces de datos de un sistema.

1 Conviértase en administrador.

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

2 Visualice información sobre los atributos físicos de los enlaces de datos que se encuentran actualmente en el sistema.

```
# dladm show-phys
```

Puede utilizar la opción `-P` con este comando para visualizar también el estado del indicador de cada enlace. Un enlace de datos deja de estar disponible si su hardware asociado se ha eliminado. Sin la opción `-P`, el comando muestra sólo los enlaces de datos disponibles.

Para ver la ruta `/devices` de los enlaces de datos, utilice la opción `-v`.

Ejemplo 8-2 Visualización de enlaces de datos disponibles

En el ejemplo siguiente, la opción `-P` incluye la columna `FLAGS` donde se indican los enlaces no disponibles. El indicador `r` del enlace de datos `net0` indica que el hardware que está asociado con el enlace (`nge`) se ha eliminado.

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net0      Ethernet  up         100Mb     full        e1000g0
net1      Infiniband down       0Mb       --         ibd0
net3      Ethernet  up         100Mb     full        bge0
net4      Ethernet  --         0Mb       --         nge0
```

En el siguiente ejemplo, se muestran los enlaces y sus ubicaciones físicas que aparecen al utilizar la opción -L.

```
# 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
```

▼ Cómo visualizar información sobre enlaces de datos

Este procedimiento muestra el estado de los enlaces disponibles.

1 Conviértase en administrador.

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

2 Visualice información de enlaces.

```
# dladm show-link
```

Ejemplo 8-3 Visualización de enlaces disponibles

En el siguiente ejemplo, se muestran enlaces persistentes y disponibles en el sistema.

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

La opción -P también muestra cualquier enlace persistente existente, pero no disponible. Un enlace persistente deja de estar disponible si el enlace se elimina temporalmente. Un enlace también deja de estar disponible si el hardware asociado se ha eliminado.

▼ Cómo eliminar un enlace de datos

Este procedimiento elimina las configuraciones de enlaces que están asociadas con NIC. Si desconecta una NIC sin intención de sustituirla, puede eliminar la configuración del enlace que está asociada con dicha NIC. Después de completar este procedimiento, el nombre del enlace se puede volver a utilizar.

1 Conviértase en administrador.

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

2 Visualice los enlaces de datos en el sistema, incluidos esos enlaces cuyo hardware ha sido eliminado.

Para incluir información sobre hardware eliminado, utilice la opción `-P`.

```
# dladm show-phys
```

3 Elimine la configuración del enlace del hardware eliminado que no pretende reemplazar.

```
# dladm delete-phys link
```

Ejemplo 8-4 Eliminación de un enlace de datos

En el ejemplo siguiente, el indicador `r` para `net2` indica que el hardware asociado del enlace (`e1000g0`) se ha eliminado. Por lo tanto, también puede eliminar el enlace `net2` y, luego, reasignar el nombre a un nuevo enlace de datos.

```
# dladm show-phys -P
LINK      DEVICE      MEDIA      FLAGS
net0      nge0        Ethernet   -----
net1      bge0        Ethernet   -----
net2      e1000g0     Ethernet   r-----

# dladm delete-phys net2
```

Configuración de propiedades de enlaces de datos

Además de realizar la configuración básica de enlaces de datos, también puede utilizar el comando `dladm` para definir propiedades de enlaces de datos y personalizarlas según las necesidades de la red.

Nota – 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 GLDv3, como `e1000g`. Para confirmar si el controlador específico admite esta función, consulte la página del comando `man` del controlador.

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 determinado tipo de medio, como la velocidad de enlace, la negociación automática para Ethernet o el tamaño de la 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.

Las propiedades de enlaces tienen, normalmente, valores predeterminados. Sin embargo, ciertos escenarios de redes podrían requerir el cambio de valores de propiedades específicos de un enlace de datos. Estos valores de propiedades pueden ser propiedades públicas o privadas. 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 necesitar ser modificadas para el controlador determinado. En Oracle Solaris, todos estos valores ahora se pueden restablecer mediante una sola herramienta administrativa, `dladm`.

Configuración de propiedades de enlaces de datos con el comando `dladm`

En la siguiente sección, se brindan procedimientos con ejemplos para establecer determinadas propiedades de enlaces de datos. Las propiedades seleccionadas son públicas y comunes para todos los controladores NIC. En una sección independiente, se describen propiedades de enlaces de datos que son específicas del controlador. Luego de esta sección, se indican los procedimientos para configurar propiedades privadas seleccionadas del controlador `e1000g`.

▼ **Cómo habilitar la compatibilidad con tramas gigantes**

La habilitación de la compatibilidad con tramas gigantes en una configuración de red es una tarea común para la mayoría de los escenarios de redes. La compatibilidad con tramas gigantes requiere el aumento del tamaño de la unidad de transmisión máxima (MTU) de un enlace de datos. En el siguiente procedimiento, se incluye el uso de nombres personalizados para identificar enlaces de datos. Para obtener una descripción general de nombres personalizados y su uso en la configuración de redes, consulte [“La pila de red en Oracle Solaris” en la página 22](#).

1 **Conviértase en administrador.**

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

2 **Para identificar el dispositivo Ethernet específico cuyo tamaño de MTU necesita restablecer, muestre los enlaces en el sistema.**

```
# dladm show-phys
```

Realice este paso especialmente si su configuración de red utiliza nombres personalizados para enlaces de datos. Gracias a los nombres personalizados, los enlaces de datos ya no son necesariamente identificados por sus nombres basados en hardware. Por ejemplo, el dispositivo Ethernet es `bge0`. Sin embargo, el nombre del enlace de datos sobre el dispositivo se ha cambiado a `net0`. Por lo tanto, debe configurar el tamaño de MTU de `net0`. Consulte [“Configuración de la interfaz IP \(tareas\)” en la página 179](#) para obtener ejemplos de tareas de configuración en enlaces de datos que utilizan nombres personalizados.

3 **(Opcional) Visualice el tamaño de MTU actual del enlace de datos y otras propiedades.**

- **Para visualizar una propiedad concreta de un enlace de datos, utilice la siguiente sintaxis:**

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

Este comando muestra los valores de la propiedad que usted especifica.

- **Para visualizar varias propiedades seleccionadas del enlace de datos, utilice la siguiente sintaxis:**

```
# dladm show-link datalink
```

Este comando muestra información del enlace de datos, incluido el tamaño de la MTU.

4 **Si una interfaz IP está configurada mediante el enlace de datos, elimine la interfaz IP.**

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

5 **Cambie el tamaño de la MTU del enlace a 9.000, el valor para tramas gigantes.**

```
# dladm set-linkprop -p mtu=9000 datalink
```

6 Cree la interfaz IP.

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

7 Configure la interfaz IP.

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

Para obtener más información sobre el comando `ipadm`, consulte [ipadm\(1M\)](#).

8 (Opcional) Verifique que la interfaz utilice el nuevo tamaño de MTU mediante una de las sintaxis del comando en el paso 3.

```
# dladm show-linkprop -p mtu datalink
```

9 (Opcional) Visualice los valores actuales de Ethernet del enlace.

```
# dladm show-ether datalink
```

Ejemplo 8-5 Habilitación de compatibilidad con tramas gigantes

El ejemplo siguiente, donde se habilita la compatibilidad con tramas gigantes, se basa en la siguiente situación:

- El sistema tiene dos NIC bge: bge0 y bge1.
- El dispositivo bge0 se utiliza como interfaz principal, mientras que el dispositivo bge1 se utiliza para fines de prueba.
- Usted desea habilitar la compatibilidad con tramas gigantes en bge1 y, a la vez, conservar el tamaño de la MTU predeterminado de la interfaz principal.
- La configuración de red utiliza nombres personalizados para enlaces de datos. El nombre del enlace de bge0 es net0. El nombre del enlace de bge1 es net1.

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net0      ether      up         100Mb     full        bge0
net1      ether      up         100Mb     full        bge1
net2      ether      up         100Mb     full        nge3
```

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

```
# ipadm delete-ip net1
# dladm set-linkprop -p mtu=9000 net1
# ipadm create-ip net1
# ipadm create-addr -T static -a 10.10.1.2/35 net1/v4
```

```
# dladm show-link web1
LINK      CLASS      MTU        STATE      BRIDGE      OVER
web1      phys      9000      up         --          --
```

Tenga en cuenta que el valor de la MTU ahora es 9.000. En este ejemplo, el comando `dladm` permite cambiar el tamaño de la MTU de `net1` directamente. El método anterior que utiliza el comando `ndd` habría requerido que también se eliminara `net0`, lo que habría interrumpido innecesariamente las operaciones de la interfaz principal.

▼ Cómo cambiar parámetros de velocidad de enlace

La mayoría de las configuraciones de red constan de una combinación de sistemas con distintas capacidades de velocidad. Por ejemplo, es posible que la velocidad anunciada entre un sistema antiguo y un sistema más nuevo se deba cambiar a una menor para permitir la comunicación. De manera predeterminada, se anuncian todas las capacidades de velocidad y dúplex de una tarjeta NIC. Este procedimiento muestra cómo desactivar las capacidades de gigabit y anunciar sólo las capacidades de megabit.

1 Conviértase en administrador.

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

2 (Opcional) Visualice el estado actual de la propiedad que desea modificar.

```
# dladm show-linkprop -p property datalink
```

3 Para anunciar capacidades de velocidades inferiores, desactive las capacidades de velocidades superiores para impedir que se anuncien.

```
# dladm set-linkprop -p property=value1 datalink
```

Ejemplo 8-6 Deshabilitación de anuncios de capacidades de gigabit de una NIC

En este ejemplo, se muestra cómo puede evitar que el enlace `net1` anuncie capacidades de gigabit.

```
# dladm show-linkprop -p adv_1000fdx_cap net1
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net1      adv_1000fdx_cap  1          --           1,0

# dladm show-linkprop -p adv_1000hdx_cap web1
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net1      adv_1000hdx_cap  1          --           1,0
```

Las propiedades que anuncian capacidades de gigabit del enlace son `adv_1000fdx_cap` y `adv_1000hdx_cap`. Para deshabilitar estas propiedades con el fin de que no sean anunciadas, debe escribir los siguientes comandos:

```
# dladm set-linkprop -p adv_1000fdx_cap=0 net1
# dladm set-linkprop -p adv_1000hdx_cap=0 net1
```

La enumeración de los valores de parámetros de Ethernet mostraría la siguiente salida:

```
# dladm show-ether net1
LINK      PTYPE      STATE      AUTO      SPEED-DUPLEX      PAUSE
net1      current    up         yes       1G-f              both
```

▼ Cómo obtener información de estado sobre propiedades de enlaces de datos

Puede obtener información sobre las propiedades del enlace de datos mostrando los valores de parámetros de Ethernet o las propiedades del enlace.

1 Conviértase en administrador.

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

2 Para obtener información sobre los valores de parámetros de Ethernet, utilice el siguiente comando:

```
# dladm show-ether [-x] datalink
```

Donde la opción `-x` incluye información adicional de parámetros sobre el enlace. Sin la opción `-x`, sólo se muestran los valores de parámetros actuales.

3 Para obtener información sobre todas las propiedades del enlace, utilice el siguiente comando:

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

Ejemplo 8-7 Visualización de valores de parámetros de Ethernet

En este ejemplo, se muestra una lista ampliada de información de parámetros sobre un enlace especificado.

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

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

- 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 habilitada y tiene un control de flujo bidireccional, en el que tanto el host como el asociado de enlace pueden enviar y recibir tramas de pausa.

- Independientemente de la configuración actual, se muestran las capacidades del dispositivo Ethernet. El tipo de negociación se puede establecer en automático, el dispositivo puede admitir velocidades de 1 Gb/s, 100 Mb/s y 10 Mb/s, tanto a dúplex medio como a dúplex completo. 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.

Ejemplo 8-8 Visualización de propiedades de enlaces

En este ejemplo, se muestra cómo enumerar todas las propiedades de un enlace. Si desea visualizar sólo propiedades específicas, utilice la opción `-p` con las propiedades concretas que desea supervisar.

```
# 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
```

Los valores de las capacidades de velocidad y dúplex del enlace se configuran manualmente en las propiedades de velocidad habilitadas que están etiquetadas en `*_cap`. Por ejemplo, `en_1000fdx_cap` es la propiedad para la capacidad de gigabit a dúplex completo y `en_100hdx_cap` es la propiedad para la capacidad de 100 Mb a dúplex medio. Los valores de estas propiedades de velocidad habilitadas se anuncian entre el host y su asociado de enlace mediante la correspondencia de propiedades de velocidad anunciadas, que están etiquetadas `adv*_cap`, como `adv_1000fdx_cap` y `adv_100hdx_cap`.

Normalmente, los valores de una determinada propiedad de velocidad habilitada 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`. Para obtener más detalles sobre las propiedades de velocidad habilitadas y anunciadas, consulte la página del comando `dladm(1M)`.

▼ **Cómo establecer el controlador e1000g para usar el enlace de acceso directo a memoria**

Este procedimiento y el siguiente procedimiento muestran cómo configurar propiedades privadas. Los dos procedimientos se aplican a propiedades específicas del controlador `e1000g`. Sin embargo, los pasos generales también se pueden utilizar para configurar propiedades privadas de otros controladores NIC.

El tráfico en masa, como transferencias de archivos, implica, normalmente, una negociación de grandes paquetes por medio de 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 sobrepasa el umbral, el enlace DMA se usa para transmitir. 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.

Para definir el umbral, realice los siguientes pasos:

1 **Conviértase en administrador.**

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

2 **Defina el valor adecuado para la propiedad `_tx_bcopy_threshold`.**

```
# dladm set-linkprop -p _tx_bcopy_threshold=value e1000g-datalink
```

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

Nota – Como con la configuración de propiedades públicas, la interfaz también se debe desconectar para que los valores de las propiedades privadas se puedan modificar.

3 **(Opcional) Verifique los nuevos valores del umbral.**

```
# dladm show-linkprop -p _tx_bcopy_threshold e1000g-datalink
```

▼ **Cómo definir manualmente la frecuencia de interrupciones**

Los parámetros que regulan la frecuencia a la que las interrupciones son enviadas por el controlador `e1000g` 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, defina los siguientes parámetros:

- `_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 habilitado. De manera predeterminada, este parámetro está habilitado.

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Si fuera necesario, identifique el dispositivo cuya propiedad de controlador desea modificar.

```
# dladm show-phys
```

3 Deshabilite el ajuste automático de la frecuencia de límite de interrupciones.

```
# dladm set-linkprop -p _intr_adaptive=0 e1000g-datalink
```

Nota – Cuando el ajuste automático de la frecuencia de límite de interrupciones está habilitado, cualquier valor existente para el parámetro `_intr_throttling_rate` se ignora.

4 Elimine cualquier interfaz IP que esté configurada mediante el enlace de datos.

5 Defina el valor para el nivel entre interrupciones mínimo.

```
# dladm set-linkprop -p _intr_throttling_rate=value e1000g-datalink
```

Nota – El valor predeterminado del parámetro `_intr_throttling_rate` es 550 en sistemas basados en SPARC y 260 en sistemas basados en x86. La configuración del nivel entre interrupciones mínimo en 0 deshabilita la lógica del límite de interrupciones.

6 Configure la interfaz IP.

7 (Opcional) Visualice la nueva configuración del umbral.

Ejemplo 8-9 Configuración para el enlace DMA y establecimiento de la frecuencia de límite de interrupciones

En este ejemplo, se utiliza un sistema basado en x86 con una NIC e1000g. El controlador se configura con una alternancia de valor de umbral entre el uso del enlace DMA o el modo bcopy para transmitir paquetes. El valor de la frecuencia de límite de interrupciones también se modifica. Además, el enlace de datos e1000g utiliza el nombre genérico predeterminado asignado por el sistema operativo. Por lo tanto, la configuración se realiza en el enlace de datos haciendo referencia al nombre personalizado, net0.

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

# dladm show-linkprop -p _tx_bcopy_threshold net0
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _tx_bcopy_threshold  512       512          --

# dladm show-linkprop -p _intr-throttling_rate
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _intr-throttling_rate  260       260          --

# ipadm delete-ip net0
# dladm set-linkprop -p _tx_bcopy_threshold=1024 net0
# dladm set-linkprop -p _intr_adaptive=0 net0
# dladm set-linkprop -p _intr-throttling_rate=1024 net0

# ipadm create-ip net0
# ipadm create-addr -T static -a 10.10.1.2/24 net0/v4addr
# dladm show-linkprop -p _tx_bcopy_threshold=1024 net0
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _tx_bcopy_threshold  1024      512          --

# dladm show-linkprop -p _intr_adaptive net0
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _intr_adaptive    0         1            --

# dladm show-linkprop -p _intr-throttling_rate
LINK      PROPERTY      VALUE      DEFAULT      POSSIBLE
net0      _intr-throttling_rate  1024     260          --
```

Tareas de configuración adicionales en enlaces de datos

En esta sección, se describen otros procedimientos de configuración comunes que se han simplificado mediante el uso del comando `dladm`, como, por ejemplo, la reconfiguración dinámica (DR) y el trabajo con módulos STREAMS.

▼ 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). Muestra cómo la DR ahora se ha facilitado gracias a la separación de la configuración del enlace de red de la configuración del hardware de red. Ya no necesario volver a configurar los enlaces de red después de completar la DR. En su lugar, simplemente se transfieren las configuraciones de enlaces de la NIC eliminada para que sean heredadas por la NIC de sustitución.

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.
- Asegúrese de que el perfil de configuración de red activo sea DefaultFixed. Consulte la sección *Reconfiguración dinámica y perfiles de configuración de red* en “Cómo funciona NWAM con otras tecnologías de red de Oracle Solaris” en la página 42 para obtener información sobre el uso de DR si el NCP activo del sistema no es DefaultFixed.
- Consulte el manual apropiado que describe los procedimientos de DR en el sistema. Para localizar documentación actual sobre la DR en servidores Sun de Oracle, busque dynamic reconfiguration en <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

Nota – El siguiente procedimiento sólo hace referencia a aspectos de DR que se relacionan específicamente con el uso de nombres flexibles para enlaces de datos. El procedimiento no contiene los pasos completos para llevar a cabo la DR. Debe consultar la documentación adecuada sobre la DR para el sistema.

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: 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 Realice los procedimientos de DR, tal como se detalla en la documentación del sistema, para eliminar una tarjeta NIC y luego insertar una NIC de sustitución.**
- 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 Si ya ha insertado la NIC de sustitución en la misma ranura que la NIC anterior, vaya al paso 6. De lo contrario, continúe con el siguiente paso.**
- Con la nueva NIC en la misma ubicación que ocupaba previamente la NIC anterior, la nueva NIC hereda el nombre del enlace y la configuración de la NIC anterior.
- 5 Realice uno de los pasos siguientes en función de la circunstancia que se aplique.**
- Si la NIC anterior que se va a sustituir permanece en su ranura en el sistema como una NIC no utilizada, realice los siguientes pasos:
 - a. Asigne un nombre diferente a la NIC que se va a sustituir.


```
# dladm rename-link oldNIC new-name
```

NIC_anterior Hace referencia a la NIC que se sustituye, pero que se mantiene en el sistema.

nombre_nuevo Hace referencia al nombre nuevo que se proporciona a la *NIC_eliminada*. El nombre no debe ser compartido por ningún otro enlace en el sistema.
 - b. Asigne el nombre de la NIC anterior a la NIC de sustitución.


```
# dladm rename-link replacementNIC oldNIC
```

NIC_sustitución Hace referencia a la nueva NIC que acaba de instalar. Esta NIC recibe automáticamente el nombre de enlace predeterminado en función de la ranura que ocupa en el sistema.

NIC_anterior Hace referencia a la NIC que se sustituye, pero que se mantiene en el sistema.
 - Si ha eliminado la NIC anterior e instala la NIC de sustitución en una ranura distinta, pero desea que la NIC herede las configuraciones de la NIC antigua, asigne el nombre de la NIC anterior a la NIC nueva.


```
# dladm rename-link replacementNIC oldNIC
```
- 6 Complete el proceso de DR mediante la habilitación de los recursos de la nueva NIC para que Oracle Solaris la pueda utilizar.**
- Por ejemplo, puede usar el comando `cfgadm` para configurar la NIC. Para obtener más información, consulte la página del comando `man cfgadm(1M)`.

7 (Opcional) Visualice información de enlaces.

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

Ejemplo 8–10 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`. Las configuraciones del enlace de `net0` se transfieren desde bge hasta `e1000g` después de que `e1000g` se conecta al sistema.

```
# 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
```

Realice pasos específicos de la DR, como el uso de `cfgadm` para eliminar bge e 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    ---
```

Configuración de módulos STREAMS en enlaces de datos

Si es necesario, puede definir hasta ocho módulos STREAMS para colocar en la parte superior de un 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 STREAMS para colocar en un determinado enlace de datos es controlada por la propiedad de enlace `autopush`. A su vez, el valor de la propiedad de enlace `autopush` se establece utilizando el subcomando `dladm set-linkprop`.

Un comando `autopush` independiente también se puede utilizar para definir los módulos `autopush STREAMS` por controlador. Sin embargo, el controlador siempre está enlazado a la NIC. Si se elimina la NIC subyacente del enlace de datos, también se elimina la información sobre la propiedad `autopush`.

Para configurar los módulos `STREAMS` para que sean colocados en la parte superior de un enlace de datos, utilice el comando `dladm set - linkprop`, en lugar del 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.

▼ Cómo establecer módulos `STREAMS` en enlaces de datos

El siguiente procedimiento describe cómo configurar módulos `STREAMS` con el comando `dladm set - linkprop`.

1 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Coloque los módulos en el flujo cuando se abre el enlace.

```
# dladm set-linkprop -p autopush=modulelist link
```

lista_módulos Especifica la lista de módulos que desea colocar de manera automática en el flujo. Se puede colocar un máximo de ocho módulos por medio de un enlace. Estos módulos se colocan en el orden en el que aparecen en la *lista_módulos*. Separe los módulos en la lista usando puntos como delimitadores.

enlace Especifica el enlace en el que los módulos se colocan.

Ejemplo 8-11 Configuración de la propiedad de enlace `autopush`

En este ejemplo, debe colocar los módulos `vpnmod` y `bufmod` en la parte superior del enlace `net0`. El dispositivo subyacente del enlace es `bge0`.

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

Si, más tarde, sustituye la tarjeta `bge` por `e1000g`, puede cambiar al nuevo enlace de datos sin tener que volver a configurar los valores de `autopush`. La tarjeta `e1000g` hereda automáticamente el nombre de enlace y la configuración de `bge`.

▼ **Cómo obtener los valores de la propiedad de enlace de autopush**

1 **Conviértase en administrador.**

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

2 **Visualice los valores de la propiedad de enlace de autopush.**

```
# dladm show-linkprop -p autopush [link]
```

Si no especifica un *enlace*, se muestra la información para todos los enlaces configurados.

▼ **Cómo eliminar los valores de la propiedad de enlace de autopush**

1 **Conviértase en administrador.**

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

2 **Elimine los valores de la propiedad de enlace de autopush de un enlace de datos específico.**

```
# dladm reset-linkprop [-t] -p autopush link
```

Utilice la opción `-t` para eliminar los valores de la propiedad temporalmente. Los valores se restauran al reiniciar el sistema.

Configuración de una interfaz IP

En este capítulo se ofrecen los procedimientos que se utilizan para configurar una interfaz IP mediante un enlace de datos.

Sobre la configuración de la interfaz IP

Después de instalar Oracle Solaris, puede realizar las siguientes tareas:

- Configurar una interfaz IP mediante un enlace de datos para una configuración de interfaz básica. En este capítulo se describen los procedimientos.
- Configurar interfaces inalámbricas. Los procedimientos se describen en el [Capítulo 10, “Configuración de las comunicaciones mediante interfaces inalámbricas en Oracle Solaris”](#).
- Configurar interfaces IP como miembros de un grupo IPMP. Los procedimientos se describen en el [Capítulo 15, “Administración de IPMP”](#).

El 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 valores de configuración persistentes. 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 del protocolo de Internet 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 valores de configuración persistentes. Anteriormente, los valores persistentes se podían simular para un escenario de red mediante la edición de las secuencias de comandos de inicio. Con la introducción de la función de SMF de 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 sustituir, 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.
- Proporciona una opción para implementar valores de configuración de dirección e interfaz persistentes.

Para obtener una lista de las opciones de `ifconfig` y sus subcomandos `ipadm` equivalentes, consulte [“Opciones de los comandos `ifconfig` y `ipadm`” en la página 202](#).

Como herramienta para definir propiedades de protocolo, el comando `ipadm` proporciona las siguientes ventajas:

- Puede definir propiedades de protocolo 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 parámetro 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.
- El comando `ipadm` también sigue una sintaxis de comando coherente y, por lo tanto, es más fácil de utilizar.

Para obtener una lista de las opciones de `ndd` y sus subcomandos `ipadm` equivalentes, consulte [“Opciones de los comandos `ndd` y `ipadm`” en la página 204](#).

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

Configuración de la interfaz IP (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.

TABLA 9-1 Configuración de interfaces IP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Definir 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 una interfaz sea única” en la página 179
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.	“Cómo configurar una interfaz IP” en la página 181
Personalizar una dirección IP con el comando <code>ipadm</code> .	Establece el ID de red de una dirección IP determinada.	“Cómo establecer la propiedad de una dirección IP” en la página 186
Obtener información de interfaces mediante el comando <code>ipadm</code> .	Muestra diferentes propiedades de interfaces, direcciones y protocolos, y sus valores de configuración correspondientes.	“Cómo obtener información sobre las interfaces de red” en la página 196

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

Algunas aplicaciones requieren que cada interfaz esté en un host para tener una dirección MAC exclusiva. Sin embargo, cada sistema basado en SPARC tiene una dirección MAC para todo el sistema, que utilizan todas las interfaces de modo predeterminado. A continuación se exponen dos situaciones en las que se podría configurar las direcciones MAC instaladas de fábrica para las interfaces en un sistema SPARC.

- Para las adiciones de vínculos, debe utilizar las direcciones MAC de fábrica de las interfaces en la configuración de la adición.
- Para los grupos IPMP, cada interfaz del grupo debe tener una dirección MAC exclusiva. Estas interfaces deben utilizar sus direcciones MAC de fábrica.

El parámetro EEPROM `local-mac-address?` determina si todas las interfaces del sistema 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 administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: 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 cambiar `local-mac-address?=false` a `local-mac-address?=true` para las adiciones.

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

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

Al reiniciar el sistema, las interfaces con las direcciones MAC de fábrica ahora utilizan esta configuración de fábrica, en lugar de la dirección MAC de todo el sistema. Las interfaces sin las direcciones MAC de fábrica siguen 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, todas 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 más de una interfaz de red con la misma dirección MAC. De lo contrario, vaya al 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.

Configuración de interfaces IP

En los procedimientos siguientes se muestra cómo utilizar el comando `ipadm` para satisfacer diferentes necesidades de configuración de IP. Aunque el comando `ifconfig` aún sirve para configurar interfaces, el comando `ipadm` debería ser la herramienta preferida. Para obtener una descripción general del comando `ipadm` y sus beneficios, consulte [“El comando ipadm” en la página 177](#).

Nota – Normalmente, la configuración de interfaz IP y la configuración de enlaces de datos se realizan al mismo tiempo. Por lo tanto, cuando corresponde, los procedimientos que figuran a continuación incluyen pasos de configuración de enlaces de datos con la utilización del comando `dladm`. Para obtener más información sobre el uso del comando `dladm` para configurar y administrar enlaces de datos, consulte el [Capítulo 8, “Configuración y administración de enlaces de datos”](#).

▼ Cómo configurar una interfaz IP

El siguiente procedimiento proporciona un ejemplo de cómo realizar una configuración básica de una interfaz IP.

Antes de empezar

Determine si desea renombrar los enlaces de datos en el sistema. Habitualmente, se utilizan los nombres genéricos que se hayan asignado a los enlaces de datos de manera predeterminada. Para cambiar los nombres de los enlaces, consulte [“Cómo cambiar el nombre de un enlace de datos” en la página 158](#).

1 Conviértase en administrador.

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

2 (Opcional) Muestre información sobre los atributos físicos de los enlaces de datos que se encuentran en el sistema.

```
# dladm show-phys
```

Este comando muestra las tarjetas de red físicas que están instaladas en el sistema y algunas de sus propiedades. Para obtener más información sobre este comando, consulte [Cómo visualizar información sobre atributos físicos de enlaces de datos](#).

3 Muestre información sobre los enlaces de datos que se encuentran actualmente en el sistema.

```
# dladm show-link
```

Este comando muestra los enlaces de datos y ciertas propiedades que se hayan definido para ellos, dentro de las cuales se incluyen las tarjetas físicas mediante las que se crearon los enlaces.

4 Cree la interfaz IP.

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

clase_interfaz 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 14, “Introducción a IPMP”](#) y el [Capítulo 15, “Administración de IPMP”](#).

interfaz Se refiere al nombre de la interfaz. Este nombre es idéntico al nombre del enlace por el que se crea la interfaz.

Nota – Debe crear la interfaz IP para poder asignarle la dirección IP.

5 Configure la interfaz IP con una dirección IP válida.

La sintaxis siguiente asigna una dirección estática a una interfaz. Consulte la página del comando `man ipadm(1M)` para otras opciones a fin de asignar direcciones IP.

```
# ipadm create-addr -T address-type -a address/prefixlen addrobj
```

-T tipo_dirección Especifica el tipo de dirección IP que se asigna a la interfaz, que es uno de los siguientes: `static`, `dhcp` o `addrconf`. `addrconf` hace referencia a las direcciones IPv6 generadas automáticamente.

-a Especifica la dirección IP que se debe configurar en la interfaz. Puede especificar solamente una dirección local o bien tanto una dirección local como una dirección remota si se efectúa la configuración del túnel. Por lo general, el usuario asigna solamente una dirección local. En este caso, puede especificar la dirección directamente con la opción *-a*, por ejemplo: *-a dirección*. La dirección se considera automáticamente una dirección local.

Si va a configurar túneles, puede que deba proporcionar la dirección local del sistema y, también, la dirección remota del sistema de destino. En este

caso, debe especificar `local` y `remote` para distinguir las dos direcciones, como se indica a continuación: -a

`local=dirección_local`, `remote=dirección_remota`. Para obtener más información acerca de la configuración de los túneles, consulte el [Capítulo 6, “Configuración de túneles IP” de *Administración de Oracle Solaris: servicios IP*](#).

Si utiliza una dirección IP numérica, utilice el formato `dirección/longitud_prefijo` para las direcciones en la notación CIDR, por ejemplo, `1.2.3.4/24`. Consulte la explicación de la opción `longitud_prefijo`.

De manera opcional, puede especificar un nombre de host para la `dirección` 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`.

<code>/longitud_prefijo</code>	Especifica la longitud del ID de red que forma parte de la dirección IPv4 cuando utiliza la notación CIDR. En la dirección <code>12.34.56.78/24</code> , <code>24</code> es <code>longitud_prefijo</code> . Si no incluye <code>longitud_prefijo</code> , la máscara de red se calcula según la secuencia que se lista para <code>netmask</code> en el servicio <code>name-service/switch</code> o mediante el uso de semántica de direcciones con clase.
<code>objeto_dirección</code>	Especifica un identificador para la dirección IP exclusiva o el conjunto de direcciones que se utiliza en el sistema. Las direcciones pueden ser de tipo IPv4 o IPv6. El identificador utiliza el formato <code>interfaz/cadena_especificada_usuario</code> . <code>interfaz</code> hace referencia a la interfaz IP a la que se asigna la dirección. La variable <code>interfaz</code> debe reflejar el nombre del enlace de datos en el que está configurada la interfaz IP. <code>cadena_especificada_usuario</code> hace referencia a una cadena de caracteres alfanuméricos que empieza por un carácter alfabético y tiene una longitud máxima de 32 caracteres. Luego, puede consultar <code>addrobj</code> en lugar de la

dirección IP numérica al utilizar cualquier subcomando `ipadm` que gestione direcciones en el sistema, como `ipadm show-addr` o `ipadm show-addr`.

6 (Opcional) Muestre información sobre la interfaz IP que acaba de configurar.

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

- Muestre el estado general de la interfaz.

```
# ipadm show-if [interface]
```

Si no especifica la interfaz, se muestra la información de todas las interfaces en el sistema.

- Muestre la información de la dirección de la interfaz.

```
# ipadm show-addr [addrobj]
```

Si no desea especificar *objeto_dirección*, se muestra la información para todos los objetos de dirección del sistema.

Para obtener más información sobre la salida del subcomando `ipadm show-*`, consulte [“Supervisión de direcciones e interfaces IP” en la página 196](#).

7 (Opcional) Agregue entradas para las direcciones IP en el archivo `/etc/hosts`.

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

Nota – Este paso se aplica solamente si está configurando direcciones IP estáticas que utilizan nombres de host. Si está configurando las direcciones DHCP, no es necesario actualizar el archivo `/etc/hosts`.

Ejemplo 9-1 Configuración de una interfaz de red con una dirección estática

```
# 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 static -a 192.168.84.3/24 net3/v4static

# ipadm show-if
IFNAME    CLASS      STATE      ACTIVE      OVER
lo0       loopback  ok         yes         --
net3      ip         ok         yes         --

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

```

lo0/?      static   ok       127.0.0.1/8
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

```

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 -T static -a campus01 net3/v4static
```

Ejemplo 9-2 Configuración automática de una interfaz de red con una dirección IP

En este ejemplo, se utiliza el mismo dispositivo de red que en el ejemplo anterior, pero se configura la interfaz IP 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/dhcp

# ipadm show-if
IFNAME    CLASS      STATE      ACTIVE      OVER
lo0       loopback   ok         yes         --
net3     ip         ok         yes         --

# ipadm show-addr net3/dhcp
ADDROBJ   TYPE      STATE      ADDR
net3/dhcp dhcp       ok         10.8.48.242/24

# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/?     static    ok         127.0.0.1/8
net3/dhcp dhcp       ok         10.8.48.242/24

```

Configuración de las propiedades de las direcciones IP

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

- La propiedad `prefixlen` de una dirección.
- 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.

Para listar las propiedades de una dirección IP, utilice la siguiente sintaxis:

```
# ipadm show-addrprop [-p property] [addrobj]
```

La información que se muestra depende de las opciones que utilice.

- Si no especifica ni una propiedad ni un objeto de dirección, se muestran todas las propiedades de todas las direcciones existentes.
- Si especifica solamente la propiedad, se muestra dicha propiedad para todas las direcciones.
- Si especifica solamente el objeto de dirección, se muestran todas las propiedades de ese objeto de dirección.

Nota – Solamente se puede establecer una propiedad de dirección por vez.

▼ Cómo establecer la propiedad de una dirección IP

Este procedimiento muestra los pasos generales para configurar una propiedad para una dirección IP.

1 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Liste las direcciones IP que se encuentran en uso en el sistema.

```
# ipadm show-addr
```

3 (Opcional) Determine la configuración actual de una propiedad específica de una dirección IP que desee cambiar.

```
# ipadm show-addrprop -p property addrobj
```

Si no conoce la propiedad, puede emitir un comando `ipadm show-addrprop` general. Al mostrar las direcciones IP con este comando, las direcciones aparecen con la configuración actual de todas sus propiedades.

4 Establezca la propiedad seleccionada en el valor deseado.

```
# ipadm set-addrprop -p property=value addrobj
```

5 Ve el nuevo valor para la propiedad.

```
# ipadm show-addrprop -p property addrobj
```

Ejemplo 9-3 Configuración de la propiedad `prefixlen` de una dirección

La propiedad `prefixlen` hace referencia a la máscara de red de una dirección IP. El siguiente ejemplo cambia la longitud de la propiedad `prefixlen` de la dirección IP de `net3`. En este ejemplo, la opción `-t` se utiliza para crear un solo cambio temporal en la propiedad. Si el sistema se reinicia, el valor de la propiedad vuelve a su configuración predeterminada.

```
# 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 -t -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
```

Configuración de las propiedades de la interfaz IP

Las interfaces IP, al igual que los enlaces de datos, tienen propiedades que se pueden personalizar según la configuración de red específica. Para cada interfaz, existen dos conjuntos de propiedades que se aplican a los protocolos IPv4 e IPv6, respectivamente. Algunas propiedades, como MTU, son iguales para los enlaces de datos y la interfaz IP. Por lo tanto, puede tener una configuración de MTU para un enlace de datos y otra configuración de MTU diferente para la interfaz configurada mediante ese enlace. Además, puede tener valores de configuración de MTU diferentes que se aplican a los paquetes de IPv4 e IPv6, respectivamente, que atraviesan esa interfaz IP.

El reenvío de IP es una propiedad de interfaz IP que normalmente se configura en escenarios de redes. El procedimiento siguiente muestra los pasos.

Habilitación de reenvío de paquetes

En una red, un host puede recibir paquetes de datos que estén destinados a otro sistema host. Mediante la habilitación 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 deshabilitado. En los dos procedimientos siguientes, se describe cómo hacer para

habilitar esta funcionalidad. En las versiones anteriores de Oracle Solaris, el comando `routedm` se utilizaba para habilitar el reenvío de paquetes. La sintaxis de `ipadm` en este procedimiento reemplaza el comando `routedm`.

Tenga en cuenta lo siguiente para determinar si utilizar el procedimiento basado en interfaz o el procedimiento basado en protocolo.

- Si desea emplear un modo selectivo para reenviar los paquetes, habilite el reenvío de paquetes en la interfaz. 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 habilitar el reenvío de paquetes solamente en algunas de las interfaces, no en todas. Consulte [“Cómo habilitar el reenvío de paquetes IP mediante la configuración de una propiedad de la interfaz” en la página 188.](#)
- Si desea implementar el reenvío de paquetes de manera global en el sistema, habilite la propiedad del protocolo `forwarding`. Para este segundo método, consulte [“Cómo habilitar el reenvío de paquetes mediante la configuración de la propiedad de protocolo” en la página 190.](#)

Nota – Los dos métodos de reenvío de paquetes no son mutuamente excluyentes. Por ejemplo, se puede habilitar el reenvío de paquetes globalmente y, luego, personalizar la propiedad `forwarding` para cada interfaz. Por lo tanto, el reenvío de paquetes puede seguir siendo selectivo para ese sistema en particular.

▼ **Cómo habilitar el reenvío de paquetes IP mediante la configuración de una propiedad de la interfaz**

Este procedimiento muestra cómo habilitar el reenvío de paquetes de modo selectivo mediante la configuración de la propiedad de reenvío IP en determinadas interfaces.

Nota – El reenvío de paquetes implica el uso del protocolo IP. Por lo tanto, en estos pasos, también se incluye la distinción entre las *versiones de protocolo* IP.

1 Conviértase en administrador.

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

2 Muestre la configuración actual de la propiedad de reenvío IP de una interfaz.

```
# ipadm show-ifprop -p forwarding [-m protocol-version] interface
```

donde `version_protocol` puede ser `ipv4` o `ipv6`. Si no especifica la versión, se muestra la configuración de los protocolos IPv4 e IPv6.

Nota – Para mostrar todas las propiedades de protocolos válidas de una interfaz dada, no especifique ninguna propiedad, como se indica a continuación:

```
# ipadm show-ifprop interface
```

Esta sintaxis también se muestra en el [Ejemplo 9-4](#).

- 3 Para cada interfaz en la que desee habilitar el reenvío de paquetes, escriba el comando siguiente:

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

- 4 (Opcional) Muestre los valores de la propiedad `forwarding` de una interfaz.

```
# ipadm show-ifprop -p forwarding interface
```

- 5 Para restaurar la propiedad `forwarding` a su valor predeterminado, escriba el comando siguiente:

```
# ipadm reset-ifprop -p forwarding -m protocol-version interface
```

Ejemplo 9-4 Habilitación de una interfaz para el reenvío de paquetes de IPv4 únicamente

El ejemplo siguiente muestra cómo implementar el reenvío de paquetes selectivo, donde el reenvío de paquetes de IPv4 se encuentra habilitado solamente en la interfaz `net0`. En las demás interfaces del sistema, el reenvío de paquetes viene deshabilitado de manera predeterminada.

```
# 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
```

La sintaxis de comando `ipadm show-ifprop` que utiliza la opción `-p property` proporciona solamente información sobre una propiedad concreta.

```
# 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
...
```

La sintaxis de comando `ipadm show-ifprop` sin la opción `-p property` muestra todas las propiedades de una interfaz con sus configuraciones correspondientes.

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

La sintaxis de comando `ipadm reset -ifprop` restablece la configuración predeterminada de la propiedad especificada.

▼ **Cómo habilitar el reenvío de paquetes mediante la configuración de la propiedad de protocolo**

Este procedimiento muestra cómo habilitar el reenvío de paquetes globalmente en el sistema.

1 **Conviértase en administrador.**

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 **Muestre el valor actual de la propiedad de reenvío IP.**

```
# ipadm show-prop -p forwarding protocol-version
```

donde *versión_protocolo* puede ser `ipv4` o `ipv6`.

Nota – Para mostrar todas las propiedades configurables válidas para un protocolo dado junto con sus configuraciones actuales, escriba el comando siguiente:

```
# ipadm show-prop protocol
```

donde *protocolo* puede ser `ip`, `ipv4`, `ipv6`, `udp`, `tcp`, `icmp` o `sctp`.

Esta sintaxis se muestra en el [Ejemplo 9–5](#).

3 **Para cada versión de protocolo en la que desee habilitar el reenvío, escriba el comando siguiente:**

```
# ipadm set-prop forwarding=on protocol-version
```

4 **(Opcional) Muestre la configuración de la propiedad de reenvío IP siguiendo uno de estos procedimientos:**

- Para mostrar todas las propiedades y las configuraciones actuales de un protocolo, escriba lo siguiente:

```
# ipadm show-prop protocol
```

- Para mostrar una propiedad específica de un protocolo, escriba lo siguiente:

```
# ipadm show-prop -p property protocol
```

- Para mostrar una propiedad específica de una versión de protocolo específica, escriba lo siguiente:

```
# ipadm show-prop -p property protocol-version
```

- 5 Para restablecer la configuración predeterminada de una propiedad específica de una versión de protocolo, escriba lo siguiente:

```
# ipadm reset-prop -p property protocol-version
```

Ejemplo 9-5 Habilitación del reenvío para paquetes IPv4 e IPv6

El ejemplo siguiente es análogo del ejemplo anterior acerca del reenvío de paquetes en interfaces. Los dos usos de `ipadm show-prop` muestran los valores de una propiedad especificada o de todas las propiedades de un protocolo y de sus correspondientes configuraciones.

```
# 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       --           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#
```

Administración de propiedades de protocolo

Además de utilizarse para configurar interfaces, el comando `ipadm` se puede utilizar para configurar propiedades de protocolo, también conocidas como valores ajustables. El comando `ipadm` reemplaza el comando `nnd`, que en las versiones anteriores generalmente se utilizaba para definir los valores ajustables. En esta sección se ofrecen procedimientos y ejemplos para personalizar las propiedades de protocolo TCP/IP seleccionadas.

Configuración de propiedades TCP/IP

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 en la zona. Las propiedades globales pueden tener diferentes configuraciones en diferentes zonas no globales. Para obtener una lista con las propiedades de protocolo admitidas, consulte la página del comando `man ipadm(1M)`.

Normalmente, la configuración predeterminada del protocolo de Internet TCP/IP es suficiente para que la red funcione. Sin embargo, si la configuración predeterminada resulta insuficiente para la topología de red, los procedimientos de la tabla siguiente ilustran cómo se pueden personalizar estas propiedades TCP/IP.

La tabla describe las tareas para configurar ciertas propiedades del protocolo y proporciona enlaces con los respectivos procedimientos.

TABLA 9-2 Configuración de las propiedades TCP/IP seleccionadas

Tarea	Descripción	Para obtener instrucciones
Marcar un puerto con privilegios.	Preservar el puerto de una interfaz a fin de restringir el acceso, excepto para los usuarios root.	“Cómo limitar el acceso de un puerto a un usuario root únicamente” en la página 192
Personalizar el comportamiento de paquetes IP que se reciben o transmiten en hosts múltiples.	Personalizar el enrutamiento simétrico en hosts múltiples.	“Implementación del enrutamiento simétrico en hosts múltiples” en la página 194
Visualizar información sobre la propiedad de un protocolo.	Mostrar la propiedad de un protocolo y su configuración actual.	“Supervisión de direcciones e interfaces IP” en la página 196

Nota – Para conocer los procedimientos que utilizan la herramienta `ipadm` para configurar interfaces de red y direcciones IP, consulte [“Configuración de interfaces IP” en la página 181](#).

▼ **Cómo limitar el acceso de un puerto a un usuario root únicamente**

En los protocolos de transporte como TCP, UDP y SCTP, los puertos 1–1023 son puertos con privilegios predeterminados con 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 con ese puerto. Para realizar este procedimiento, utilice las siguientes propiedades de protocolo de transporte:

- `smallest_nonpriv_port`
- `extra_priv_ports`

1 Determine si el puerto designado se encuentra en el rango de puertos comunes y, por tanto, puede utilizarse.

```
# ipadm show-prop -p smallest_nonpriv_port protocol
```

donde *protocolo* es el tipo de protocolo para el que desea configurar un puerto con privilegios, como IP, UDP, ICMP y otros.

En la salida del comando, el campo POSSIBLE muestra el rango de números de puertos con los que los usuarios comunes pueden vincularse. Si el puerto designado está dentro de este rango, entonces puede configurarse como un puerto con privilegios.

2 Compruebe que el puerto que desee reservar esté disponible y no se haya marcado como un puerto con privilegios.

```
# ipadm show-prop -p extra_priv_ports protocol
```

En la salida del comando, el campo CURRENT indica qué puertos están marcados como con privilegios. Si el puerto designado no está incluido en este campo, entonces puede configurarse como un puerto con privilegios.

3 Agregue el puerto designado como un puerto con privilegios.

```
# ipadm set-prop -p extra_priv_ports=port-number protocol
```

4 Por cada puerto adicional que desea agregar o eliminar como puerto con privilegios, repita uno de los siguientes:

- Para agregar un puerto como puerto con privilegios, escriba la siguiente sintaxis.

```
# ipadm set-prop -p extra_priv_ports+=portnumber protocol
```

Nota – Con el calificador representado por el signo más (+), puede asignar varios puertos como puertos con privilegios. El calificador representado por el signo más le permite crear una lista de estos puertos. Utilice esta sintaxis con el calificador para agregar puertos a la lista de manera individual. Si no desea utilizar el calificador, el puerto que asigna reemplaza todos los otros puertos que estaban listados anteriormente con privilegios.

- Para eliminar un puerto de la lista de puertos con privilegios, escriba la siguiente sintaxis.

```
# ipadm set-prop -p extra_priv_ports-=portnumber protocol
```

Nota – Con el calificador representado por el signo menos (-), puede eliminar el puerto de los puertos existentes que se listan como puertos con privilegios. Utilice la misma sintaxis para eliminar todos los puertos con privilegios adicionales, incluidos los puertos predeterminados.

5 Verifique el nuevo estado del puerto designado.

```
# ipadm show-prop -p extra_priv_ports protocol
```

En la salida del comando, asegúrese de que los puertos designados estén incluidos en el campo CURRENT.

Ejemplo 9-6 Configuración de un puerto con privilegios

En este ejemplo, se configuran los puertos 3001 y 3050 como puertos con privilegios. También se elimina el puerto 4045, que se encuentra listado como puerto con privilegios.

En la salida para la propiedad `smallest_nonpriv_port`, el campo `POSSIBLE` indica que el puerto 1024 es el puerto sin privilegios más bajo y que los puertos 3001 y 3050 designados se encuentran dentro del rango de los puertos sin privilegios que se pueden utilizar. En la salida para la propiedad `extra_priv_ports`, los puertos 2049 y 4045 del campo `CURRENT` están marcados como puertos con privilegios. Por lo tanto, puede configurar el puerto 3001 como puerto con privilegios.

```
# 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

# 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 del 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 Multipathing) para repartir el tráfico por las rutas.

En algunos casos, no resulta ideal repartir el tráfico de este modo. Un paquete IP podría recibir por medio de una interfaz del host múltiple que no está en la misma subred que la dirección IP de origen en el 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 clase de configuración de enrutamiento de tráfico se llama 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 por 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.

El siguiente procedimiento muestra cómo usar el comando `ipadm` para definir la propiedad `hostmodel` para una configuración de enrutamiento específica:

- 1 **En el host múltiple, asuma el rol de administrador.**
- 2 **Configure el enrutamiento de los paquetes de red en el sistema.**

```
# ipadm set-prop -p hostmodel=value protocol
```

La propiedad se puede configurar en uno de los siguientes tres valores:

<code>strong</code> (fuerte)	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> (débil)	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.

- 3 **(Opcional) Verifique la configuración de la propiedad `hostmodel`.**

```
# ipadm show-prop protocol
```

Ejemplo 9-7 Configuración del enrutamiento simétrico en un host múltiple

En este ejemplo, se implementa el enrutamiento simétrico de todo el tráfico IP de 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
```

Supervisión de direcciones e interfaces IP

El comando `ipadm` también es la herramienta preferida para supervisar las interfaces IP y sus propiedades o parámetros, y obtener información al respecto. Los subcomandos de `ipadm` para obtener información de las interfaces utilizan la siguiente sintaxis básica:

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

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

En esta sección se proporcionan diversos ejemplos de cómo usar el comando `ipadm` para obtener información sobre las interfaces de red. Para otros tipos de tareas de supervisión que debe realizar en la red, consulte el [Capítulo 5, “Administración de una red TCP/IP” de *Administración de Oracle Solaris: servicios IP*](#).

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

▼ Cómo obtener información sobre las interfaces de red

Este procedimiento describe cómo mostrar información sobre el estado general, la información de dirección y las propiedades IP de una interfaz.

1 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Para obtener la información del estado de una interfaz, escriba el siguiente comando:

```
# ipadm show-if [interface]
```

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:

IFNAME Hace referencia a la interfaz cuya información se muestra.

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

- `ip` hace referencia a una interfaz IP.

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

STATE	Hace referencia al estado de la interfaz, que puede ser <code>ok</code> , <code>offline</code> , <code>failed</code> , <code>down</code> o <code>disabled</code> .
	El estado <code>failed</code> 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 <code>down</code> hace referencia a una interfaz IP desconectada por el administrador.
	El estado <code>disable</code> hace referencia a la interfaz IP que se desconecta mediante el comando <code>ipadm disable-if</code> .
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.

3 Para obtener información de dirección de la interfaz, escriba el siguiente comando:

```
# ipadm show-addr [addrobj]
```

Si no se especifica un identificador de dirección, se proporciona la información de dirección de todos los identificadores de dirección del sistema.

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

ADDROBJ	Especifica el objeto de dirección cuya dirección se está mostrando.
TYPE	Indica si la dirección IP es <code>static</code> , <code>dhcp</code> o <code>addrconf</code> . La configuración <code>addrconf</code> indica que la dirección se obtuvo mediante la configuración de dirección sin estado o con estado.
STATE	Describe el objeto de dirección en su configuración activa actual. 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 mostrará las direcciones locales y remotas.

Para obtener más información acerca de los túneles, consulte el [Capítulo 6, “Configuración de túneles IP”](#) de *Administración de Oracle Solaris: servicios IP*.

4 Para obtener información sobre las propiedades de la interfaz, escriba el comando siguiente:

```
# ipadm show-ifprop [-p property] interface
```

Si no especifica una propiedad, se mostrarán todas las propiedades y su configuración.

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

IFNAME	Hace referencia a la interfaz cuya información se muestra.
PROPERTY	Se refiere a la propiedad de la interfaz. Una interfaz puede tener varias propiedades.
PROTO	Se refiere al protocolo al que se aplica la propiedad y 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	Se refiere a la configuración 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, se muestra la configuración como un signo de interrogación (?).

5 Para obtener información sobre una propiedad de dirección, escriba el siguiente comando:

```
# ipadm show-addrprop [-p property, ...] [addrobj]
```

La información que se muestra depende de las opciones que se utilizan.

- Si no se especifica una propiedad, se muestran todas las propiedades.
- Si se especifica sólo la propiedad, se muestra dicha propiedad para todas las direcciones.
- Si se especifica sólo el objeto de dirección, se muestran las propiedades de todas las direcciones existentes en el sistema.

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

ADDROBJ	Se refiere al objeto de dirección cuyas propiedades se muestran.
PROPERTY	Se refiere a la 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	Se refiere al valor real de la propiedad en la configuración actual.
PERSISTENT	Se refiere a la configuración 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.

Ejemplo 9-8 Uso del comando `ipadm` para supervisar interfaces

Este conjunto de ejemplos muestra el tipo de información que se puede obtener mediante los subcomandos de `ipadm show-*`. En primer lugar, se muestra la información general de la interfaz. Luego, se proporciona la información de dirección. Por último, se proporciona la información sobre una propiedad específica, la MTU de la interfaz `net1`. Los ejemplos incluyen interfaces de túnel e interfaces que utilizan un nombre personalizado.

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

```
# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/?        static    ok         127.0.0.1/8
net0/v4      static    ok         192.168.84.3/24
tun0/v4tunaddr static    ok         173.129.134.1-->173.129.134.2
```

Tenga en cuenta que un objeto de dirección que aparece como *interfaz/?* indica que la dirección fue configurada en la interfaz por una aplicación que no utilizó ninguna API de `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 *interfaz/cadena_definida_usuario*. Para ver ejemplos de la asignación de direcciones IP, consulte “[Cómo configurar una interfaz IP](#)” en la página 181.

```
# 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
```

```
# 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     --
```

Solución de problemas de configuración de interfaces

En esta sección, se tratan problemas habituales que pueden surgir durante el uso del comando `ipadm` para configurar interfaces IP.

El comando `ipadm` no funciona.

La configuración manual de la interfaz IP con los comandos `dladm` e `ipadm` sólo funciona en perfiles de configuración de red (NCP) de tipo fijo, como `DefaultFixed`. Si el NCP activo en el sistema es un perfil de tipo automático, cambie a un perfil de tipo fijo antes de utilizar los comandos `dladm` e `ipadm`.

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

# netadm enable -p ncp defaultfixed
```

La dirección IP no se puede asignar con el comando `ipadm create-addr`.

Con el comando `ifconfig` tradicional, puede conectar y asignar una dirección IP con una única sintaxis de comando. Al utilizar el comando `ipadm create-addr` para configurar una dirección IP, primero debe crear la interfaz IP con un comando separado.

```
# ipadm create-ip interface
# ipadm create-addr -T addr-type -a address addrobj
```

Durante la configuración de la dirección IP, aparece el mensaje `cannot create address object: Invalid argument provided`.

El objeto de dirección identifica una dirección IP específica enlazada a una interfaz IP. El objeto de dirección es un identificador único para cada dirección IP de la interfaz IP. Debe especificar un objeto de dirección diferente para identificar una segunda dirección IP que desea asignar a la

misma interfaz IP. Si desea utilizar el mismo nombre de objeto de dirección, debe eliminar la primera instancia del objeto de dirección antes de asignarlo para identificar una dirección IP distinta.

```
# ipadm show-addr
ADDROBJ  TYPE      STATE  ADR
lo0      static   ok     127.0.0.1/10
net0/v4  static   ok     192.168.10.1

# ipadm create-addr -T static -a 192.168.10.5 net0/v4b

o

# ipadm show-addr
ADDROBJ  TYPE      STATE  ADR
lo0      static   ok     127.0.0.1/10
net0/v4  static   ok     192.168.10.1

# ipadm delete-addr net0/v4
# ipadm create-addr -T static -a 192.168.10.5 net0/v4
```

Durante la configuración de la interfaz IP, aparece el mensaje **cannot create address: Persistent operation on temporary object.**

El comando `ipadm` crea una configuración persistente. Si la interfaz IP que está configurando se creó como una interfaz temporal, no podrá utilizar el comando `ipadm` para configurar valores persistentes en la interfaz. Después de verificar que una interfaz que está configurando es temporal, elimine dicha interfaz, vuelva a crearla como un objeto persistente y luego siga realizando la configuración.

```
# ipadm show-if -o all
IFNAME  CLASS      STATE  ACTIVE  CURRENT      PERSISTENT  OVER
lo0     loopback   ok     yes     -m46-v-----  46--        --
net0    ip         ok     yes     bm4-----    ----        --
```

La ausencia del indicador 4 para la configuración de IPv4 o del indicador 6 para la configuración de IPv6 en el campo `PERSISTENT` indica que `net0` se creó como una interfaz temporal.

```
# ipadm delete-ip net0
# ipadm create-ip net0
# # ipadm create-addr -T static -a 192.168.1.10 net0/v4
```

Tablas de comparación: comando ipadm y otros comandos de red

El comando `ipadm` es la herramienta preferida para realizar todas las tareas de configuración de las interfaces IP. Este comando reemplaza los comandos de las versiones anteriores que se utilizaban para la configuración de redes, como los comandos `ifconfig` y `ndd`. En las tablas siguientes se muestran las opciones de comando seleccionadas de estas herramientas que se utilizaban anteriormente y sus equivalentes en el comando `ipadm`.

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

Opciones de los comandos `ifconfig` y `ipadm`

La siguiente tabla muestra las opciones del comando `ifconfig` y los subcomandos aproximados `ipadm` correspondientes.

TABLA 9-3 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-imp</code> <code>ipadm enable-addr</code> <code>ipadm delete-ip</code> <code>ipadm delete-vni</code> <code>ipadm delete-imp</code> <code>ipadm disable-addr</code>
<code>[dirección[/longitud_prefijo] [dirección_destino]]</code> <code>[addif dirección[/longitud_prefijo]] [removeif</code> <code>dirección[/longitud_prefijo]][netmask</code> <code>máscara][destination</code> <code>dirección_destino]{auto-dhcp dhcp}[primary][wait</code> <code>segundos]extend release start</code>	<code>ipadm create-addr -T static</code> <code>ipadm create-addr -T dhcp</code> <code>ipadm create-addr -T addrconf</code> <code>ipadm show-addr</code> <code>ipadm delete-addr</code> <code>ipadm refresh-addr</code>

TABLA 9-3 Asignación de sintaxis entre los comandos ifconfig y ipadm (Continuación)

Comando ifconfig	Comando ipadm
[deprecated -deprecated] [preferred -preferred] [private -private] [zone nombre_zona -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 [nombre none] [router -router]	ipadm set-ifprop ipadm show-ifprop ipadm reset-ifprop
[ipmp] [group [nombre ""]] standby -standby] [failover -failover]	ipadm create-ipmp ipadm delete-ipmp ipadm add-ipmp ipadm remove-ipmp ipadm set-ifprop -p [standby] [group]
[tdst dirección_destino_túnel] [tsrc dirección_srcs_túnel] [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>Administración de Oracle Solaris: servicios IP</i> .
[auth_algs algoritmo_autenticación] [encr_algs algoritmo_cifrado] [encr_auth_algs algoritmo_autenticación_cifrado]	ipseconf Para obtener detalles, consulte la página del comando man ipsecconf(1M) y el Capítulo 15, “Configuración de IPsec (tareas)” de <i>Administración de Oracle Solaris: servicios IP</i> .
[auth_revarp] [ether [dirección]] [index if-index] [subnet dirección_subred] [broadcast dirección_difusión] [token dirección/longitud_prefijo] Opciones de dhcp: inform, ping, release, status, drop	Subcomandos equivalentes que no se encuentran disponibles en este momento.
modlist] [modinsert nombre_mod@pos] [modremove mod_name@pos]	Subcomandos equivalentes que no se encuentran disponibles en este momento.

Opciones de los comandos nnd y ipadm

La siguiente tabla muestra las opciones del comando nnd y los subcomandos aproximados ipadm correspondientes.

TABLA 9-4 Asignación de sintaxis entre los comandos nnd y ipadm

Comando nnd	Comando ipadm
Propiedades de recuperación	

TABLA 9-4 Asignación de sintaxis entre los comandos ndd y ipadm (Continuación)

Comando ndd	Comando ipadm
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)	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 ...
bash-3.2# ndd -get /dev/ip \ ip_def_ttl 100 bash-3.2# ndd -get /dev/ip \ ip6_def_hops 255	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
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)	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# ndd -get /dev/tcp ecn 1	tcp ecn rw passive -- passive never,passive,active
bash-3.2# ndd -get /dev/tcp sack 2	tcp sack rw active -- active never,passive,active
Propiedades de configuración	

TABLA 9-4 Asignación de sintaxis entre los comandos nnd y ipadm (Continuación)

Comando nnd	Comando ipadm
<pre>bash-3.2# nnd -set /dev/ip \ ip_def_ttl 64 bash-3.2# nnd -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>

Configuración de las comunicaciones mediante interfaces inalámbricas en Oracle Solaris

En este capítulo, se explica cómo configurar y usar las comunicaciones mediante interfaces inalámbricas en un equipo portátil que ejecuta Oracle Solaris. Se tratan los temas siguientes:

- Comunicación mediante interfaces Wi-Fi
- Búsqueda de una red Wi-Fi
- Conexión y uso de Wi-Fi en los sistemas Oracle Solaris
- Comunicaciones seguras mediante Wi-Fi

Mapa de tareas de comunicaciones Wi-Fi

Tarea	Descripción	Para obtener instrucciones
Planificar comunicaciones Wi-Fi en el sistema.	Configurar el equipo portátil o la configuración de redes inalámbricas en una ubicación que admita Wi-Fi (si se desea, se puede incluir un enrutador).	“Cómo preparar un sistema para comunicaciones Wi-Fi” en la página 209
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 210
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 214
Establecer comunicaciones Wi-Fi seguras.	Crear la clave WEP y utilizarla para establecer conexiones con una red Wi-Fi de manera segura.	“Cómo configurar una conexión de red Wi-Fi cifrada” en la página 216

Comunicación mediante interfaces Wi-Fi

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.

Oracle Solaris contiene funciones que permiten configurar un sistema como un cliente Wi-Fi. En esta sección se explica cómo utilizar las opciones de conectividad Wi-Fi del comando `dladm` para conectar un equipo portátil o doméstico a una red Wi-Fi local.

Nota – Oracle Solaris no incluye funciones para configurar servidores o puntos de acceso Wi-Fi.

Búsqueda de una red Wi-Fi

Las redes Wi-Fi normalmente vienen en tres variedades:

- Redes Wi-Fi disponibles en el mercado
- Redes Wi-Fi municipales
- Redes Wi-Fi privadas

Una ubicación en la que se ofrece Wi-Fi se denomina *zona activa*. Cada zona activa incluye un punto de acceso. El *punto de acceso* es un enrutador con una conexión “con cable” a Internet, como Ethernet o DSL. La conexión a Internet generalmente se establece mediante un proveedor de servicios de Internet inalámbrico (WISP) o un ISP tradicional.

Redes Wi-Fi comerciales

Muchos hoteles y cafeterías ofrecen conexión inalámbrica a Internet como un servicio a los clientes con equipos portátiles. Estas zonas activas comerciales tienen puntos de acceso en sus instalaciones. Los puntos de acceso son enrutadores con conexiones con cable a un WISP que presta servicio en estas ubicaciones comerciales. Los WISP típicos son los proveedores independientes y las compañías de telefonía celular.

Puede utilizar un equipo portátil con Oracle Solaris para conectarse a una red Wi-Fi que se ofrezca en un hotel o en otra zona activa comercial. Pida instrucciones en la zona activa para conectarse a la red Wi-Fi. Normalmente, el proceso de conexión consiste en proporcionar una clave en un explorador que se inicia al iniciar una sesión. Es posible que tenga que pagar una tarifa al hotel o al WISP para poder utilizar la red.

En general las ubicaciones comerciales que son zonas activas de Internet anuncian esta capacidad a sus clientes. También puede encontrar listas de zonas activas inalámbricas en varios sitios web, por ejemplo, [Wi-FiHotSpotList.com](http://www.wi-fihotspotlist.com) (<http://www.wi-fihotspotlist.com>).

Redes Wi-Fi municipales

Algunas ciudades del mundo han construido redes Wi-Fi municipales gratuitas, a las que los ciudadanos pueden acceder desde los sistemas de sus hogares. Las redes Wi-Fi municipales utilizan radiotransmisores en postes de teléfono u otros lugares exteriores para formar una “malla” en el área en la que presta servicio la red. Estos transmisores son los puntos de acceso a la red Wi-Fi municipal. Si en su área existe una red Wi-Fi municipal, es posible que su hogar esté incluido en la malla.

El acceso a la red Wi-Fi municipal generalmente es gratuito. Puede acceder a la red municipal desde un equipo portátil o personal en el que se ejecute Oracle Solaris. No necesita un enrutador doméstico para acceder a la red municipal desde su sistema. Sin embargo, se recomienda configurar un enrutador doméstico en las áreas donde la señal de la red municipal sea débil. También se recomienda el uso de enrutadores domésticos si se necesita una conexión segura mediante la red Wi-Fi. Para obtener más información, consulte “[Comunicaciones seguras mediante Wi-Fi](#)” en la página 216.

Redes Wi-Fi privadas

Como las redes Wi-Fi son relativamente fáciles de configurar, las empresas y universidades usan redes Wi-Fi privadas con acceso limitado a los empleados o los estudiantes. Para acceder a las redes Wi-Fi privadas generalmente es necesario proporcionar una clave al conectarse o ejecutar una VPN segura después de haberse conectado. Para establecer conexión con la red privada, se necesita un equipo portátil o personal adecuado con Oracle Solaris y permiso para utilizar las funciones de seguridad.

Planificación de comunicaciones Wi-Fi

Para poder conectar el sistema a una red Wi-Fi, siga las siguientes instrucciones.

▼ Cómo preparar un sistema para comunicaciones Wi-Fi

1 Equipar su sistema con una interfaz Wi-Fi compatible.

El sistema debe tener una tarjeta Wi-Fi compatible con Oracle Solaris, como las tarjetas que admiten los conjuntos de chips Atheros. Para obtener una lista de los controladores y los conjuntos de chips admitidos actualmente, consulte [Wireless Networking for OpenSolaris](http://hub.opensolaris.org/bin/view/Community+Group+laptop/wireless) (<http://hub.opensolaris.org/bin/view/Community+Group+laptop/wireless>).

Si la interfaz aún no está presente en el sistema, siga las instrucciones del fabricante para instalar la tarjeta de interfaz. Configure el software de interfaz durante el procedimiento de “[Cómo conectarse a una red Wi-Fi](#)” en la página 210.

2 Ubique el sistema en un lugar en el que una red Wi-Fi comercial, municipal o privada preste servicio.

El sistema debe estar cerca del punto de acceso de la red, lo cual normalmente no se tiene en cuenta para una zona activa de red comercial o privada. Sin embargo, si va a utilizar una red municipal gratuita, se debe ubicar cerca del punto de acceso transmisor.

3 (Opcional) Configure un enrutador inalámbrico para que actúe como punto de acceso adicional.

Si no hay una red Wi-Fi disponible en su ubicación, configure su propio enrutador. Por ejemplo, si tiene una línea DSL conecte el enrutador inalámbrico al enrutador DSL. A continuación, el enrutador inalámbrico se convertirá en el punto de acceso para los dispositivos inalámbricos.

Conexión y uso de Wi-Fi en los sistemas Oracle Solaris

Esta sección incluye tareas para establecer y supervisar las conexiones Wi-Fi en equipos portátiles o de escritorio que ejecuten Oracle Solaris.

▼ Cómo conectarse a una red Wi-Fi

Antes de empezar Para realizar el siguiente procedimiento, debe haber seguido las instrucciones de “Cómo preparar un sistema para comunicaciones Wi-Fi” en la página 209.

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Fijese qué enlaces se encuentran disponibles.

```
# dladm show-link
LINK      CLASS  MTU   STATE  BRIDGE  OVER
ath0      phys   1500  up     --      --
e1000g0   phys   1500  up     --      --
```

En este ejemplo, la salida indica que hay dos enlaces disponibles. El enlace `ath0` admite comunicaciones Wi-Fi. El enlace `e1000g0` se utiliza para anexas el sistema a una red con cables.

3 Configure la interfaz Wi-Fi.

Lleve a cabo los siguientes pasos para configurar la interfaz:

- Cree una interfaz que admita Wi-Fi:

```
# ipadm create-ip ath0
```

- Compruebe que el enlace esté conectado:

```
# ipadm show-if
IFNAME      CLASS      STATE      ACTIVE      OVER
```

```

lo0      loopback  ok      yes    --
e1000g0 ip        ok      yes    --
ath0    ip        ok      yes    --

```

4 Verifique las redes disponibles.

```

# dladm scan-wifi
LINK      ESSID          BSSID/IBSSID   SEC    STRENGTH  MODE  SPEED
ath0      net1           00:0e:38:49:01:d0 none   good      g     54Mb
ath0      net2           00:0e:38:49:02:f0 none   very weak g     54Mb
ath0      net3           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	Nombre del enlace que se va a utilizar en la conexión Wi-Fi.
ESSID	ID de conjunto de servicios extendidos. ESSID es el nombre de la red Wi-Fi, como <code>net1</code> , <code>net2</code> y <code>net3</code> , que aparecen en la salida de ejemplo.
BSSID/IBSSID	ID de conjunto de servicios básicos, identificador único para un ESSID en particular. BSSID es la dirección MAC de 48 bits del punto de acceso cercano que brinda a la red un determinado ESSID.
SEC	Tipo de seguridad necesaria para acceder a la red. Los valores son <code>none</code> o <code>WEP</code> . Para obtener más información sobre <code>WEP</code> , consulte “Comunicaciones seguras mediante Wi-Fi” en la página 216 .
STRENGTH	STRENGTH determina la fuerza de las señales de radio de las redes Wi-Fi que están disponibles en la ubicación.
MODE	Versión del protocolo 802.11 que ejecuta la red. Los modos pueden ser <code>a</code> , <code>b</code> o <code>g</code> , por separado o combinados.
SPEED	Velocidad en megabits por segundo de la red particular.

5 Conéctese a una red Wi-Fi.

Realice una de las siguientes acciones:

- 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-wi-fi` 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 addrobj
```

donde *addrobj* utiliza la convención de denominación *interfaz/cadena_definida_por_usuario*.

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 -T static -a address addrobj
```

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

```
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
ath0      connected   net3      none     very good g      36Mb
```

En este ejemplo, la salida indica que el sistema se encuentra conectado a la red net3. La salida anterior `scan-wi-fi` indicaba que net3 tenía la señal más fuerte entre las redes disponibles. El comando `dladm show-wi-fi` 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 navegador o una aplicación de su elección.
- Si el punto de acceso está en una zona activa comercial que requiere el pago de un arancel, siga las instrucciones que se proporcionan en la ubicación actual. Por lo general, deberá ejecutar un navegador, 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.

```
# dladm disconnect-wifi
```

- Termine una sesión Wi-Fi en particular cuando se esté ejecutando más de una sesión.

```
# dladm disconnect-wifi link
```

donde *enlace* representa la interfaz que se utilizó 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 10–1 Conexión con una red Wi-Fi determinada

El ejemplo siguiente muestra un escenario típico que puede surgir cuando se usa un equipo portátil que ejecuta Oracle Solaris en un cibercafé.

Determine si un enlace Wi-Fi se encuentra disponible.

```
# dladm show-wifi
ath0          type: non-vlan      mtu: 1500          device: ath0
```

El enlace `ath0` está instalado en el equipo portátil. Configure la interfaz `ath0` y compruebe que esté activa.

```
# ipadm create-ip ath0
IFNAME      STATE      CURRENT          PERSISTENT
lo0         ok        -m-v-----46   ---
ath0        ok        bm-----46    -46
```

Mire los enlaces Wi-Fi disponibles en su ubicación.

```
# dladm scan-wifi
LINK        ESSID          BSSID/IBSSID     SEC      STRENGTH  MODE  SPEED
ath0        net1           00:0e:38:49:01:d0 none     weak      g      54Mb
ath0        net2           00:0e:38:49:02:f0 none     very weak g      54Mb
ath0        net3           00:0d:ed:a5:47:e0 wep      very good g      54Mb
ath0        citinet        00:40:96:2a:56:b5 none     good      b      11Mb
```

La salida indica que `net3` tiene la mejor señal. `net3` requiere una clave por la que el proveedor del cibercafé cobra un arancel. `citinet` es una red libre proporcionada por la ciudad del lugar.

Conéctese a la red `citinet`.

```
# dladm connect-wifi -e citinet
```

La opción `-e` de `connect-wi-fi` toma el ESSID de la red Wi-Fi preferida como argumento. El argumento en este comando es `citinet`, el ESSID de la red local libre. El comando `dladm connect-wi-fi` ofrece varias opciones para conectarse a la red Wi-Fi. Para obtener más información, consulte la página del comando `man dladm(1M)`.

Configure la dirección IP para la interfaz Wi-Fi.

```
# ipadm create-addr -T static -a 10.192.16.3/8 ath0/v4
# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4       static    ok         127.0.0.1/8
e1000g0/v4   static    ok         129.146.69.34/24
ath0/v4static static    ok         10.192.16.3/8
lo0/v6       static    ok         ::1/128
```

Este ejemplo supone que el usuario tiene la dirección IP estática 10.192.16.3/24 configurada en el equipo portátil.

```
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
ath0      connected   citinet    none     good      g     11Mb
```

La salida indica que el equipo portátil se encuentra conectado a la red citinet.

```
# firefox
```

Se muestra la página de inicio del navegador Firefox.

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

```
# dladm disconnect-wifi
# dladm show-wifi
LINK      STATUS      ESSID      SEC      STRENGTH  MODE  SPEED
ath0      disconnected --         --         --         --         --
```

La salida de show-wi-fi verifica que se haya desconectado del enlace ath0 desde 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 con el subcomando linkprop.

1 Conviértase en administrador.

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

2 Conéctese a la red Wi-Fi, como se describe en [“Cómo conectarse a una red Wi-Fi” en la página 210](#).

3 Vea las propiedades del enlace.

Use la sintaxis siguiente:

```
# dladm show-linkprop interface
```

Por ejemplo, debe utilizar la siguiente sintaxis para mostrar el estado de la conexión establecida por el enlace ath0:

```
# dladm show-linkprop ath0
PROPERTY      VALUE      DEFAULT      POSSIBLE
channel       5          --           --
powermode     off        off          off,fast,max
radio         ?          on           on,off
speed         36        --           1,2,5,6,9,11,12,18,24,36,48,54
```

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 sobre el enlace.

```
# netstat -I ath0 -i 5
      input  ath0      output
packets errs packets errs  colls  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 10–2 Cómo establecer 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 ath0
PROPERTY      VALUE      DEFAULT      POSSIBLE
speed         24        --           1,2,5,6,9,11,12,18,24,36,48,54
# dladm set-linkprop -p speed=36 ath0

# dladm show-linkprop -p speed ath0
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. Para realizar este procedimiento debe utilizar esta clase de enrutadores y debe tener su documentación disponible. Además, el sistema ya debe estar enchufado al enrutador.

1 Inicie el software para configurar el enrutador para el hogar.

Consulte la documentación del fabricante para obtener instrucciones. Los fabricantes de enrutadores normalmente ofrecen una dirección web interna o una interfaz gráfica de usuario para la configuración de los enrutadores.

2 Genere el valor de la clave WEP.

Siga las instrucciones del fabricante para crear un clave segura para el enrutador. Puede que la GUI de configuración del enrutador le pida que proporcione una frase de contraseña de su

elección para la clave. A continuación, el software utilizará la frase de contraseña para generar una cadena hexadecimal, por lo general, de 5 bytes o 13 bytes de longitud. Esta cadena pasa a ser el valor que se utilizará para la clave WEP.

3 Aplique los cambios y guarde la configuración de la clave.

Consulte la documentación del fabricante para obtener instrucciones.

4 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

5 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 *nombre_clave* representa el nombre que desea dar a la clave.

6 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.

7 Vea el contenido de la clave que acaba de crear.

```
# dladm show-secobj
OBJECT          CLASS
keyname        wep
```

donde *nombre_clave* es el nombre del objeto seguro.

8 Establezca una conexión cifrada para la red Wi-Fi.

```
# dladm connect-wifi -e network -k keyname interface
```

9 Compruebe que la conexión sea segura.

```
# dladm show-wifi
LINK    STATUS    ESSID    SEC    STRENGTH    MODE    SPEED
ath0    connected  net1    wep    good        g        11Mb
```

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

Ejemplo 10-3 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.

```
# 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 ath0
```

Este comando establece una conexión cifrada para la red Wi-Fi `citinet` mediante el objeto seguro `mykey`.

```
# dladm show-wifi
LINK    STATUS    ESSID    SEC    STRENGTH  MODE  SPEED
ath0    connected  citinet  wep    good      g     36Mb
```

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

Administración de puentes

En este capítulo, se describen los puentes y cómo administrarlos.

En este capítulo, se tratan los siguientes temas:

- “Descripción general sobre puentes” en la página 219
- “Administración de puentes (mapa de tareas)” en la página 229

Descripción general sobre puentes

Los puentes se utilizan para conectar segmentos de red separados. Cuando están conectados por un puente, los segmentos de red se comunican como si fueran un solo segmento de red. Los puentes se implementan en la capa de enlace de datos (L2) de la pila de red. Los puentes utilizan un mecanismo de reenvío de paquetes para conectar subredes.

Si bien los puentes y el enrutamiento se pueden utilizar para distribuir información sobre las ubicaciones de los recursos de la red, difieren de varias formas. El enrutamiento se implementa en la capa IP (L3) y utiliza protocolos de enrutamiento. No se utilizan protocolos de enrutamiento en la capa de enlace de datos. En cambio, los destinos de los paquetes reenviados se determinan mediante el análisis del tráfico de red que se recibe en los enlaces conectados al puente.

Cuando se recibe un paquete, se analiza su dirección de origen. La dirección de origen del paquete asocia el nodo desde el que el paquete se envió con el enlace en el que se recibe. A partir de ese momento, cuando un paquete recibido utiliza la misma dirección como la dirección de destino, el puente reenvía el paquete por el enlace a dicha dirección.

El enlace asociado con una dirección de origen puede ser un enlace intermedio que está conectado a otro puente en la subred con puentes. Con el tiempo, todos los puentes dentro de la subred con puentes "aprenden" qué enlace envía un paquete hacia un nodo determinado. Por lo tanto, la dirección de destino del paquete se utiliza para dirigir el paquete a su destino final por medio de puentes salto a salto.

Una notificación local de “enlace inactivo” indica que todos los nodos de un enlace determinado ya no son accesibles. En esta situación, el reenvío de paquetes al enlace se detiene y todas las entradas de reenvío por el enlace se vacían. Las entradas de reenvío también caducan a lo largo del tiempo. Cuando un enlace se restaura, los paquetes recibidos por medio del enlace se tratan como nuevos. El proceso de “aprendizaje” basado en la dirección de origen de un paquete comienza de nuevo. Este proceso permite que el puente reenvíe correctamente paquetes por medio de dicho enlace cuando la dirección se utiliza como la dirección de destino.

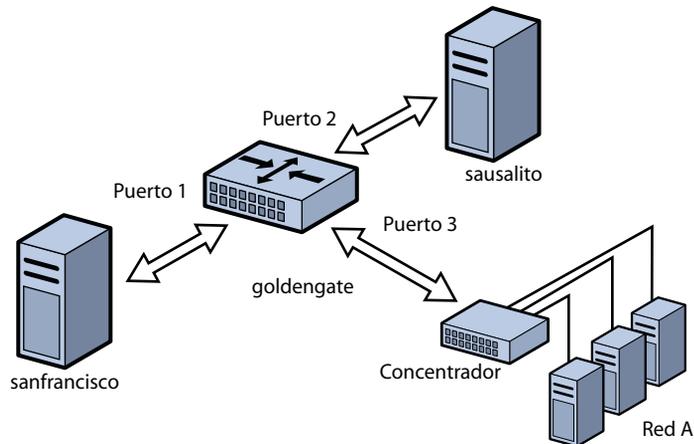
Para reenviar paquetes a sus destinos, los puentes deben escuchar en modo promiscuo en cada enlace que está conectado al puente. La escucha en modo promiscuo hace que los puentes se vuelvan vulnerables a la aparición de bucles de reenvío, en los cuales los paquetes circulan continuamente a máxima velocidad. Por lo tanto, los puentes utilizan el mecanismo de protocolo de árbol de expansión (STP) para evitar bucles de red que harían que las subredes se vuelvan inutilizables.

Además de utilizar el protocolo de árbol de expansión (STP) y el protocolo de árbol de expansión rápido (RSTP) para puentes, Oracle Solaris admite la mejora de la protección TRILL. El STP se utiliza de manera predeterminada; pero usted puede utilizar TRILL especificando la opción `-P trill` para los comandos de puentes.

El uso de una configuración de puentes simplifica la administración de los distintos nodos en la red conectándolos en una única red. Gracias a la conexión de estos segmentos por medio de un puente, todos los nodos comparten una única red de difusión. Por lo tanto, cada nodo puede acceder a los otros mediante protocolos de red, como IP, en lugar de hacerlo mediante enrutadores, para reenviar tráfico por segmentos de red. Si no utiliza un puente, debe configurar el enrutamiento IP para permitir el reenvío de tráfico IP entre nodos.

En la siguiente figura, se muestra una configuración de red con puentes sencilla. El puente, `goldengate`, es un sistema de Oracle Solaris que tiene configurado el establecimiento de puentes. `sanfrancisco` y `sausalito` son sistemas que están conectados físicamente al puente. La red A utiliza un concentrador que está conectado físicamente al puente en un lado y a los sistemas informáticos en el otro lado. Los puertos del puente son enlaces, como `bge0`, `bge1` y `bge2`.

FIGURA 11-1 Red con puentes simple



Las redes con puentes se pueden formar en anillos que conectan físicamente varios puentes juntos. Estas configuraciones son comunes en las redes. Este tipo de configuración podría causar problemas con paquetes antiguos que saturan los enlaces de red generando bucles constantes alrededor del anillo. Para protegerse contra tales condiciones de generación de bucles, los puentes de Oracle Solaris implementan los protocolos STP y TRILL. Recuerde que la mayoría de los puentes de hardware también implementan la protección contra bucles STP.

En la siguiente figura, se muestra una red con puentes configurada en un anillo. La configuración muestra tres puentes. Dos sistemas están conectados físicamente a westminster. Un sistema está conectado físicamente a waterloo. Y un sistema está conectado físicamente a tower. Los puentes están conectados físicamente entre ellos mediante los puertos.

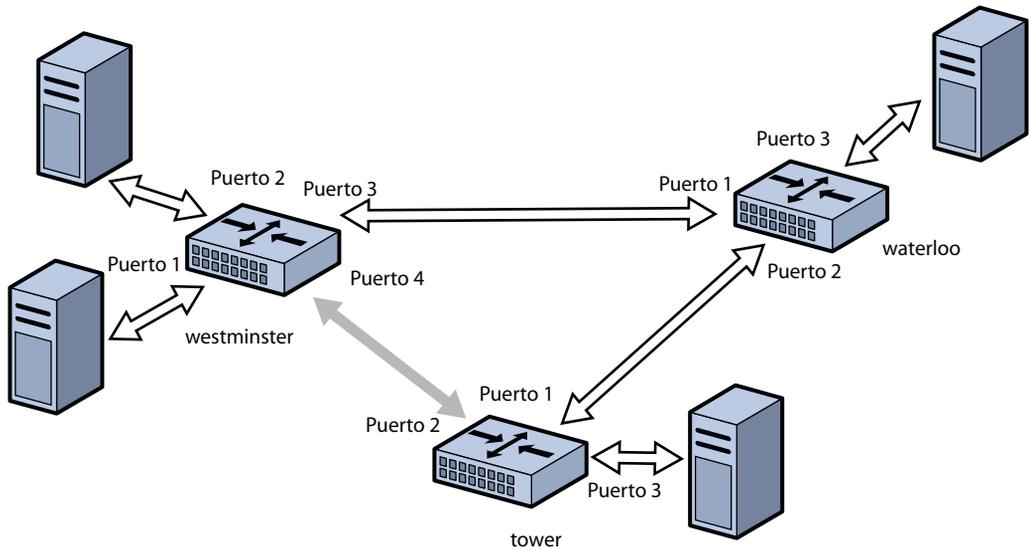
Cuando se utiliza STP o RSTP para la protección contra bucles, el bucle físico se mitiga evitando que una de las conexiones en el bucle reenvíe paquetes. En la figura, se muestra que el enlace físico entre los puentes westminster y tower no se utiliza para reenviar paquetes.

Tenga en cuenta que mediante el cierre de enlaces físicos utilizables para realizar la protección contra bucles, STP y RSTP consumen ancho de banda.

A diferencia de STP y RSTP, TRILL no cierra enlaces físicos para evitar bucles. En cambio, TRILL calcula la información de la ruta más corta para cada nodo TRILL de la red y utiliza dicha información para reenviar paquetes a destinos individuales.

Como resultado, TRILL permite que el sistema deje *todos* los enlaces en uso en todo momento. Los bucles no son un problema, ya que se manejan de forma similar a la forma en que IP maneja los bucles. Es decir, TRILL crea rutas cuando son necesarias y utiliza límites de salto de reenvío para evitar problemas causados por estados de bucles momentáneos.

FIGURA 11-2 Anillo de red con puentes



Precaución – No establezca `local-mac-address?=false` en plataformas SPARC, o los sistemas utilizarán de forma errónea la misma dirección MAC en varios puertos y en la misma red.

Nota – No configure un enlace en un puente cuando se requieren los mayores niveles posibles de rendimiento. El establecimiento de puentes *requiere* que las interfaces subyacentes se encuentren en modo promiscuo, lo que deshabilita un número de importantes optimizaciones que están en el hardware, el controlador y demás capas del sistema. La deshabilitación de estas mejoras de rendimiento es una consecuencia inevitable del mecanismo de puentes.

Puede utilizar un puente en un sistema donde *algunos* de los enlaces del sistema no están conectados y, por lo tanto, no están sujetos a dichas restricciones. Estos problemas de rendimiento sólo afectan a esos enlaces que están configurados para formar parte de un puente.

Para obtener información sobre STP, consulte IEEE 802.1D-1998. Para obtener información sobre RSTP, consulte IEEE 802.1Q-2004. Para obtener información sobre TRILL, consulte Internet Engineering Task Force (IETF) TRILL draft documents (<http://tools.ietf.org/wg/trill>).

Propiedades de enlaces

Estas propiedades de enlaces pueden ser mostradas y modificadas por los comandos `dladm show-linkprop`, `dladm set-linkprop` y `reset-linkprop`:

default_tag Define el ID de la red de área local virtual (VLAN) predeterminado para paquetes sin etiqueta que se envían al enlace y desde él. Los valores válidos van de 0 a 4094. El valor predeterminado es 1. Sólo los enlaces de tipo de tarjeta de la interfaz de red (VNIC) no virtual y no VLAN tienen esta propiedad. La configuración de este valor en 0 deshabilita el reenvío de paquetes sin etiqueta hacia el puerto y desde él. (Esta es una propiedad MAC).

Nota – Esta propiedad también se utiliza fuera del ámbito de puentes para especificar el identificador de VLAN de puerto (PVID) de IEEE para el enlace. Cuando `default_tag` no es cero, no puede crear una VLAN que tiene ese mismo ID en el enlace, porque el enlace base representa automáticamente el PVID por sí mismo.

Por ejemplo, si el PVID está definido como 5 en `net0`, no puede crear una VLAN con el ID 5 en `net0`. Para especificar VLAN 5 en esta situación, utilice `net0`.

No puede establecer `default_tag` igual al ID de cualquier VLAN existente que se crea en ese enlace. Por ejemplo, el comando siguiente crea VLAN 22 en `net0`:

```
# dladm create-vlan -l net0 -v 22 myvlan0
```

En esta situación, no puede establecer `default_tag` en 22, ya que haría que `net0` y `myvlan0` representen la misma VLAN.

Si establece `default_tag` en 0, permite que los paquetes sin etiqueta en `net0` no estén asociados con ninguna VLAN. Esta situación evita que los paquetes se reenvíen por un puente configurado.

forward Habilite y deshabilite el reenvío de tráfico por medio del puente. Esta propiedad existe en todos los enlaces, excepto para los enlaces VNIC. Los valores válidos son 1 (true) y 0 (false). El valor predeterminado es 1. Cuando está deshabilitada, una VLAN asociada con una instancia de enlace no reenvía tráfico por medio del puente. La deshabilitación del reenvío es equivalente a la eliminación de la VLAN del “conjunto permitido” para un

	puente tradicional. Esto significa que la E/S basada en VLAN al enlace subyacente de clientes locales continúa, pero no se realiza ningún reenvío basado en puentes.
<code>stp</code>	Habilite y deshabilite STP y RSTP. Los valores válidos son 1 (true) y 0 (false). El valor predeterminado es 1, que habilita STP y RSTP. Cuando se define en 0, el enlace no utiliza ningún tipo de protocolo de árbol de expansión y se coloca en modo de reenvío en todo momento. El modo de reenvío utiliza la protección de unidad de datos de protocolo de puente (BPDU). Deshabilite STP y RSTP cuando desee configurar enlaces punto a punto que estén conectados a nodos finales. Sólo enlaces de tipo no VLAN y no VNIC tienen esta propiedad.
<code>stp_cost</code>	Represente valores de costo de STP y RSTP para usar el enlace. Los valores válidos van de 1 a 65535. El valor predeterminado es 0, que se usa para señalar que el costo se calcula automáticamente por tipo de enlace. Los siguientes valores representan el costo de varios tipos de enlace: 100 para 10 Mbps, 19 para 100 Mbps, 4 para 1 Gbps y 2 para 10 Gbps.
<code>stp_edge</code>	Especifique si el puerto está conectado a otros puentes. Los valores válidos son 1 (true) y 0 (false). El valor predeterminado es 1. Si se define en 0, el daemon asume que el puerto está conectado a otros puentes, incluso si no se ve ninguna BPDU de ningún tipo.
<code>stp_p2p</code>	Especifique el tipo de modo de conexión. Los valores válidos son true, false y auto. El valor predeterminado es auto, que detecta automáticamente conexiones punto a punto. Especifique true para forzar el modo punto a punto y especifique false para forzar el modo multipunto normal.
<code>stp_priority</code>	Defina el valor de prioridad de puerto de STP y RSTP. Los valores válidos van de 0 a 255. El valor predeterminado es 128. El valor de prioridad de puerto de STP y RSTP se utiliza para determinar el puerto raíz preferido de un puente anteponiendo el valor al identificador del puerto. Cuanto más bajo sea el valor numérico, más alta será la prioridad.

Daemon de STP

Cada puente que crea usando el comando `dladm create-bridge` se representa como una instancia SMF denominada de manera idéntica de `svc:/network/bridge`. Cada instancia ejecuta una copia del daemon `/usr/lib/bridged`, que implementa el STP.

El siguiente comando de ejemplo crea un puente denominado `pontevecchio`:

```
# dladm create-bridge pontevecchio
```

El sistema crea un servicio SMF denominado `svc:/network/bridge:pontevecchio` y un nodo de observación denominado `/dev/net/pontevecchio0`.

Por motivos de seguridad, todos los puertos ejecutan el STP estándar de manera predeterminada. Un puente que no ejecuta alguna forma de protocolo de puentes, como STP, puede formar bucles de reenvío duraderos en la red. Debido a que Ethernet no tiene TLL o conteo de saltos en paquetes, cualquiera de dichos bucles son errores fatales para la red.

Cuando sabe que un puerto concreto no está conectado a otro puente (por ejemplo, una conexión punto a punto directa a un sistema host), puede deshabilitar administrativamente el STP de ese puerto. Incluso si todos los puertos de un puente tienen el STP deshabilitado, el daemon de STP se sigue ejecutando. El daemon se sigue ejecutando por los siguientes motivos:

- Para poder manejar los nuevos puertos que se agregan.
- Para implementar la protección de BPDU.
- Para habilitar o deshabilitar el reenvío en los puertos, según sea necesario.

Cuando un puerto tiene el STP deshabilitado, el daemon `bridged` escucha BPDU (protección de BPDU). El daemon utiliza `syslog` para marcar los errores y deshabilita el reenvío en el puerto para indicar un error grave de la configuración de la red. El enlace se habilita nuevamente cuando el estado del enlace se desactiva y se vuelve a activar, o cuando usted elimina manualmente el enlace y lo vuelve a agregar.

Si deshabilita la instancia del servicio SMF de un puente, el reenvío de puentes se detiene en dichos puertos porque el daemon de STP se detiene. Si la instancia se reinicia, el STP comienza desde su estado inicial.

Daemon de TRILL

Cada puente que crea usando el comando `dladm create-bridge -P trill` se representa como una instancia de SMF idénticamente denominada de `svc:/network/bridge` y `svc:/network/routing/trill`. Cada instancia de `svc:/network/routing/trill` ejecuta una copia del daemon `/usr/lib/trilld`, que implementa el protocolo TRILL.

El siguiente comando de ejemplo crea un puente denominado `bridgeofsighs`:

```
# dladm create-bridge -P trill bridgeofsighs
```

El sistema crea dos servicios SMF denominados `svc:/network/bridge:bridgeofsighs` y `svc:/network/routing/trill:bridgeofsighs`. Además, el sistema crea un nodo de observación denominado `/dev/net/bridgeofsighs0`.

Depuración de puentes

A cada instancia de puente se le asigna un "nodo de observación", que aparece en el directorio `/dev/net/` y se nombra por el nombre de puente y `0` al final.

El nodo de observación está destinado únicamente para su uso con las utilidades `snoop` y `wireshark`. Este nodo se comporta como una interfaz Ethernet estándar, excepto para la transmisión de paquetes, que se sueltan de manera silenciosa. No puede asociar una IP además de un nodo de observación y no puede realizar solicitudes de enlace (`DL_BIND_REQ`), a menos que utilice la opción pasiva.

Cuando se utiliza, el nodo de observación realiza una copia única sin modificaciones de cada paquete gestionado por el puente disponible para el usuario. Este comportamiento es similar a un puerto de "supervisión" en un puente tradicional y está sujeto a las reglas del "modo promiscuo" de DLPI habituales. Puede utilizar `pfmod` o las funciones en las utilidades `snoop` y `wireshark` para filtrar por ID de VLAN.

Los paquetes entregados representan los datos que son recibidos por el puente.



Precaución – En los casos donde el proceso de puentes agrega, elimina o modifica una etiqueta VLAN, los datos que se muestran describen el estado antes de que este proceso ocurra. Esta situación inusual puede resultar confusa si existen valores de `default_tag` distintos utilizados en diferentes enlaces.

Para ver los paquetes que se transmiten y se reciben en un enlace concreto (después de que el proceso de puentes se completa), ejecute `snoop` en los enlaces individuales, en lugar de ejecutarlo en el nodo de observación del puente.

Para obtener información sobre nodos de observación, consulte [“Funciones de observación para la virtualización de redes y el control de recursos” en la página 348](#).

Otros comportamientos de puentes

En las siguientes secciones, se describe cómo cambia el comportamiento de los enlaces cuando se utilizan puentes en la configuración.

Para obtener información sobre el comportamiento estándar de los enlaces, consulte [“Administración de redes de área local virtuales” en la página 249](#).

Comportamiento de DLPI

A continuación, se describen las diferencias en el comportamiento de enlaces cuando se habilita un puente:

- Las notificaciones de enlace activo (`DL_NOTE_LINK_UP`) y enlace inactivo (`DL_NOTE_LINK_DOWN`) se envían en el agregado. Esto significa que cuando todos los enlaces externos muestran el estado de enlace inactivo, los clientes de nivel superior que están utilizando las capas MAC también ven eventos de enlaces inactivos. Cuando cualquier enlace externo en el puente muestra el estado de enlace activo, todos los clientes de nivel superior ven eventos de enlaces activos.

Este informe de enlaces activos y enlaces inactivos del agregado se realiza por los siguientes motivos:

- Cuando se ve el enlace inactivo, los nodos en el enlace ya no son accesibles. Esto no es así cuando el código de puentes aún puede enviar y recibir paquetes mediante otro enlace. Las aplicaciones administrativas que necesitan el estado real de los enlaces pueden utilizar las estadísticas del núcleo de la capa MAC para revelar el estado. Estas aplicaciones difieren de los clientes regulares, como IP, en que brindan información sobre el estado del hardware y no participan en el reenvío.
- Cuando todos los enlaces externos están inactivos, el estado aparece como si el puente estuviera cerrado. En este caso particular, el sistema reconoce que nada podría ser accesible. La compensación es que los puentes no se pueden utilizar para permitir la comunicación sólo local en el caso de que todas las interfaces sean "reales" (no virtuales) y todas estén desconectadas.
- Todas las funciones específicas de enlaces se vuelven genéricas. Los enlaces que admiten funciones especiales de aceleración de hardware no pueden usar esas funciones porque la determinación real de enlaces de salida no es realizada totalmente por el cliente. La función de reenvío de puentes debe elegir un enlace de salida en función de la dirección MAC de destino, y dicho enlace de salida puede ser cualquier enlace en el puente.

Administración de VLAN

De manera predeterminada, las VLAN que se configuran en el sistema se reenvían entre todos los puertos en una instancia de puente. Al invocar al comando `dladm create-vlan` o `dladm create-vnic -v`, y el enlace subyacente forma parte de un puente, ese comando también permitirá el reenvío de la VLAN especificada en ese enlace de puente.

Para configurar una VLAN en un enlace y deshabilitar el reenvío hacia otros enlaces o desde ellos en el puente, debe deshabilitar el reenvío estableciendo la propiedad `forward` con el comando `dladm set-linkprop`.

Utilice el comando `dladm create-vlan` para habilitar automáticamente la VLAN para el establecimiento de puentes cuando el enlace subyacente se configura como parte de un puente.

Las VLAN se ignoran en el STP que cumple con los estándares. El protocolo de puentes calcula sólo una topología sin bucles mediante mensajes de BPDU sin etiquetas, y utiliza este árbol para habilitar y deshabilitar enlaces. Debe configurar los enlaces duplicados que se proporcionan en sus redes, de manera que cuando esos enlaces son deshabilitados de forma automática por el STP, las VLAN configuradas no se desconectan. Esto significa que debe ejecutar todas las VLAN en todas partes de la red principal con puentes o examinar con cuidado todos los enlaces redundantes.

TRILL no necesita seguir las reglas STP complejas. En cambio, TRILL encapsula automáticamente los paquetes que tienen la etiqueta de VLAN intacta y los transfiere por la red. Esto significa que TRILL enlaza VLAN aisladas donde el mismo ID de VLAN se ha reutilizado en una única red con puentes.

Ésta es una diferencia importante del STP donde podría reutilizar etiquetas de VLAN en secciones aisladas de la red para gestionar conjuntos de VLAN que superan el límite de 4094. Si bien no puede utilizar TRILL para gestionar redes de esta forma, es posible que pueda implementar otras soluciones, como redes VLAN basadas en proveedor.

En una red de STP con VLAN, puede resultar difícil configurar las características de conmutación por error para evitar la partición de VLAN cuando STP deshabilita el enlace “equivocado”. La pérdida de funcionalidad relativamente pequeña en redes VLAN aisladas está más que compensada por la solidez del modelo de TRILL.

Comportamiento de VLAN

El puente realiza reenvíos mediante el análisis del conjunto permitido de VLAN y la propiedad `default_tag` de cada enlace. El proceso general es el siguiente:

- **Determinación de VLAN de entrada.** Esta tarea empieza cuando se recibe un paquete en un enlace. Cuando se recibe un paquete, se comprueba si tiene una etiqueta de VLAN. Si dicha etiqueta no está presente o si la etiqueta es sólo de prioridad (etiqueta cero), la `default_tag` configurada en ese enlace (si no se ha definido en cero) se considera como la etiqueta de VLAN interna. Si la etiqueta no está presente o está definida en cero, y `default_tag` es cero, el paquete se ignora. No se realizan reenvíos sin etiquetas. Si la etiqueta está presente y es igual a `default_tag`, el paquete también es ignorado. De lo contrario, la etiqueta de entrada se toma como la VLAN de entrada.
- **Comprobación de pertenencia de enlace.** Si la VLAN de entrada no está configurada como una VLAN permitida en este enlace, el paquete se ignora. El reenvío se calcula, y la misma comprobación se realiza para el enlace de salida.
- **Actualización de etiquetas.** Si la VLAN (que no es cero en este punto) es igual a `default_tag` en el enlace de salida, la etiqueta en el paquete (si hay) se elimina, independientemente de la prioridad. Si la VLAN no es igual a `default_tag` en el enlace de salida, una etiqueta se agrega si no está presente en ese momento, y la etiqueta se define para el paquete de salida, con la prioridad actual copiada en el paquete.

Nota – En el caso en el que el reenvío se envía a varias interfaces (para difusión, multidifusión y destinos desconocidos), la comprobación de enlace de salida y la actualización de etiqueta se deben realizar de manera independiente para cada enlace de salida. Algunas transmisiones podrían estar etiquetadas, mientras que otras no.

Ejemplos de configuración de puentes

En los siguientes ejemplos, se muestra cómo ver información sobre configuraciones de puentes y servicios de puentes.

- Puede obtener información sobre puentes ejecutando el siguiente comando:

```
# dladm show-bridge
BRIDGE      PROTECT ADDRESS                PRIORITY DESROOT
tonowhere   trill  32768/66:ca:b0:39:31:5d 32768 32768/66:ca:b0:39:31:5d
sanluisrey  stp    32768/ee:2:63:ed:41:94 32768 32768/ee:2:63:ed:41:94
pontoon     trill  32768/56:db:46:be:b9:62 32768 32768/56:db:46:be:b9:62
```

- Puede obtener información sobre apodos de TRILL para un puente ejecutando el siguiente comando:

```
# dladm show-bridge -t tonowhere
NICK FLAGS LINK          NEXTHOP
38628 --  simblue2  56:db:46:be:b9:62
58753 L   --          --
```

Administración de puentes (mapa de tareas)

Oracle Solaris utiliza el comando `dladm` y la función SMF para administrar puentes. Utilice los comandos SMF para habilitar, deshabilitar y supervisar instancias de puentes mediante el identificador de recurso de gestión de errores (FMRI) de la instancia, `svc:/red/bridge`. Utilice el comando `dladm` para crear o destruir puentes, así como para asignar enlaces a puentes o para eliminar enlaces de ellos.

En la siguiente tabla, se hace referencia a las tareas que puede utilizar para administrar puentes.

Tarea	Descripción	Para obtener instrucciones
Ver información sobre puentes configurados.	Utilice el comando <code>dladm show-bridge</code> para ver información sobre puentes configurados en el sistema. Puede ver información sobre entradas de reenvíos de núcleos, estadísticas, enlaces y puentes configurados.	“Cómo ver información sobre puentes configurados” en la página 231
Ver información de configuración de enlaces que están conectados a un puente.	Utilice el comando <code>dladm show-link</code> para ver información sobre enlaces configurados en el sistema. Si el enlace está asociado a un puente, consulte la salida en el campo <code>BRIDGE</code> .	“Cómo ver información de configuración sobre enlaces de puentes” en la página 233
Crear un puente.	Utilice el comando <code>dladm create-bridge</code> para crear un puente y agregar enlaces opcionales. De manera predeterminada, los puentes se crean mediante STP. Para utilizar TRILL con el fin de crear un puente, agregue <code>-P trill</code> a la línea de comandos <code>dladm create-bridge</code> o utilice el comando <code>dladm modify-bridge</code> para habilitar TRILL.	“Cómo crear un puente” en la página 233
Modificar el tipo de protección de un puente.	Utilice el comando <code>dladm modify-bridge</code> para modificar el tipo de protección de un puente. De manera predeterminada, los puentes se crean mediante STP. Para utilizar TRILL con el fin de crear un puente, utilice <code>-P trill</code> con el comando <code>dladm modify-bridge</code> para habilitar TRILL.	“Cómo modificar el tipo de protección de un puente” en la página 234
Agregar un enlace a un puente.	Utilice el comando <code>dladm add-bridge</code> para agregar uno o más enlaces a un puente existente.	“Cómo agregar uno o más enlaces a un puente existente” en la página 235
Eliminar enlaces de un puente.	Utilice el comando <code>dladm remove-bridge</code> para eliminar enlaces de un puente. No puede eliminar un puente hasta que se eliminen todos sus enlaces.	“Cómo eliminar enlaces de un puente” en la página 235

Tarea	Descripción	Para obtener instrucciones
Eliminar un puente del sistema.	Utilice el comando <code>dladm delete-bridge</code> para eliminar un puente del sistema.	“Cómo eliminar un puente del sistema” en la página 236

▼ Cómo ver información sobre puentes configurados

Este procedimiento muestra cómo utilizar el comando `dladm show-bridge` con diversas opciones para mostrar diferentes tipos de información sobre puentes configurados.

Para obtener más información sobre las opciones del comando `dladm show-bridge`, consulte la página del comando `man dladm(1M)`.

1 Conviértase en administrador.

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

2 Visualice información sobre un puente o todos los puentes configurados.

- Visualice la lista de puentes.
`dladm show-bridge`
- Muestre estados relacionados con enlaces para el puente.
`dladm show-bridge -l bridge-name`
- Muestre estadísticas para el puente.
`dladm show-bridge -s bridge-name`

Nota – Los nombres y las definiciones de las estadísticas mostradas están sujetos a cambios.

- Muestre estadísticas relacionadas con enlaces para el puente.
`dladm show-bridge -ls bridge-name`
- Muestre entradas de reenvíos de núcleos para el puente.
`dladm show-bridge -f bridge-name`
- Muestre información de TRILL sobre el puente.
`dladm show-bridge -t bridge-name`

Ejemplo 11-1 Visualización de información sobre puentes

Los siguientes son ejemplos de uso del comando `dladm show-bridge` con diversas opciones.

- A continuación, se muestra información sobre todos los puentes que están configurados en el sistema:

```
# dladm show-bridge
BRIDGE      PROTECT ADDRESS                PRIORITY DESROOT
goldengate  stp      32768/8:0:20:bf:f      32768    8192/0:d0:0:76:14:38
baybridge   stp      32768/8:0:20:e5:8      32768    8192/0:d0:0:76:14:38
```

- El siguiente comando `dladm show-bridge -l tower` muestra información de estado relacionada con enlaces para una única instancia de puente, `tower`. Para ver los parámetros configurados, utilice el comando `dladm show-linkprop` en su lugar.

```
# dladm show-bridge -l tower
LINK        STATE      UPTIME  DESROOT
hme0        forwarding 117     8192/0:d0:0:76:14:38
qfe1        forwarding 117     8192/0:d0:0:76:14:38
```

- El siguiente comando `dladm show-bridge -s` muestra estadísticas para el puente especificado, `terabithia`:

```
# dladm show-bridge -s terabithia
BRIDGE      DROPS      FORWARDS
terabithia  0          302
```

- El siguiente comando `dladm show-bridge -ls` muestra estadísticas para todos los enlaces en el puente especificado, `london`:

```
# dladm show-bridge -ls london
LINK        DROPS      RECV      XMIT
hme0        0          360832    31797
qfe1        0          322311    356852
```

- El siguiente comando `dladm show-bridge -f` muestra entradas de reenvíos de núcleos para el puente especificado, `avignon`:

```
# dladm show-bridge -f avignon
DEST        AGE      FLAGS  OUTPUT
8:0:20:bc:a7:dc 10.860  --     hme0
8:0:20:bf:f9:69  --     L      hme0
8:0:20:c0:20:26 17.420  --     hme0
8:0:20:e5:86:11  --     L      qfe1
```

- El siguiente comando `dladm show-bridge -t` muestra información de TRILL sobre el puente especificado, `key`:

```
# dladm show-bridge -t key
NICK  FLAGS  LINK      NEXTHOP
38628 --    london    56:db:46:be:b9:62
58753 L     --        --
```

▼ Cómo ver información de configuración sobre enlaces de puentes

La salida `dladm show-link` incluye un campo BRIDGE. Si un enlace es un miembro de un puente, este campo identifica el nombre del puente del cual es miembro. Este campo se muestra de manera predeterminada. Para los enlaces que no forman parte de un puente, el campo está en blanco si se utiliza la opción `-p`. En caso contrario, el campo muestra `--`.

El nodo de observación del puente también aparece en la salida `dladm show-link` como un enlace independiente. Para este nodo, el campo OVER existente muestra los enlaces que son miembros del puente.

1 Conviértase en administrador.

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

2 Visualice información de configuración sobre cualquier enlace que sea miembro de un puente.

```
# dladm show-link [-p]
```

La opción `-p` genera salida en un formato analizable.

▼ Cómo crear un puente

Este procedimiento muestra cómo utilizar STP para crear un puente, que es el valor predeterminado. Para obtener más información sobre opciones de creación de puentes, consulte la descripción de `dladm create-bridge` en la página del comando `man dladm(1M)`.

Nota – Para utilizar TRILL con el fin de crear un puente, agregue `-P trill` a la línea de comandos `dladm create-bridge` o utilice el comando `dladm modify-bridge` para habilitar TRILL.

El comando `dladm create-bridge` crea una instancia de puente y, opcionalmente, asigna uno o más enlaces de red al puente nuevo. Debido a que no hay instancias de puentes en el sistema de manera predeterminada, Oracle Solaris no establece puentes entre enlaces de red de manera predeterminada.

Para establecer puentes entre enlaces, debe crear, al menos, una instancia de puente. Cada instancia de puente es independiente. Los puentes no incluyen una conexión de reenvío entre ellos, y un enlace es miembro de, como máximo, un puente.

El *nombre_puente* es una cadena arbitraria que debe ser un nombre de instancia de servicio SMF legal. Este nombre es un componente FMRI que no tiene secuencias de escape, lo que significa que los espacios en blanco, los caracteres de control ASCII y los siguientes caracteres no pueden estar presentes:

```
; / ? : @ & = + $ , % < > # "
```

El nombre `default` se reserva, como todos los nombres que empiezan con la cadena `SUNW`. Los nombres que tienen dígitos finales se reservan para la creación de “dispositivos de observación”. Debido al uso de los dispositivos de observación, los nombres de instancias de puentes legales se restringen aún más a un nombre `d1pi(7P)` legal. El nombre debe comenzar y finalizar con un carácter alfabético o con un carácter de subrayado. El resto del nombre puede contener caracteres alfanuméricos y caracteres de subrayado.

1 Conviértase en administrador.

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

2 Cree el puente.

```
# dladm create-bridge [-l link]... bridge-name
```

La opción `-l enlace` agrega un enlace al puente. Tenga en cuenta que si alguno de los enlaces especificados no se puede agregar, el comando falla y el puente no se crea.

En el ejemplo siguiente, se muestra cómo crear el puente `brooklyn` mediante la conexión de enlaces `hme0` y `qfe1`:

```
# dladm create-bridge -l hme0 -l qfe1 brooklyn
```

▼ Cómo modificar el tipo de protección de un puente

En este procedimiento, se muestra cómo utilizar el comando `dladm modify-bridge` para modificar el tipo de protección de STP a TRILL o de TRILL a STP.

● Modifique el tipo de protección de un puente.

```
# dladm modify-bridge -P protection-type bridge-name
```

La opción `-P protection-type` especifica qué tipo de protección utilizar. De manera predeterminada, el tipo de protección es STP (`-P stp`). Para utilizar el tipo de protección TRILL en su lugar, utilice la opción `-P trill`.

En el siguiente ejemplo, se muestra cómo cambiar el tipo de protección para el puente `brooklyn` del STP predeterminado a TRILL:

```
# dladm modify-bridge -P trill brooklyn
```

▼ Cómo agregar uno o más enlaces a un puente existente

En este procedimiento, se muestra cómo agregar uno o más enlaces a una instancia de puente.

Un enlace puede ser miembro de, como máximo, un puente. Por lo tanto, si desea mover un enlace de una instancia de puente a otra, primero debe eliminar el enlace del puente actual antes de agregarlo a otro.

Los enlaces que se asignan a un puente no pueden ser VLAN, VNIC ni túneles. Sólo enlaces que serían aceptables como parte de una agregación o enlaces que son agregaciones en sí mismos se pueden asignar a un puente.

Los enlaces que se asignan a un puente deben tener el mismo valor de MTU. Tenga en cuenta que Oracle Solaris permite cambiar el valor de MTU en un enlace existente. En este caso, la instancia de puente pasa a estado de mantenimiento hasta que se eliminan o se cambian los enlaces asignados, de manera que los valores de MTU coincidan antes de reiniciar el puente.

Los enlaces que se asignan al puente deben ser un tipo de Ethernet, que incluye medios 802.3 y 802.11.

1 Conviértase en administrador.

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

2 Agregue un nuevo enlace al puente existente.

```
# dladm add-bridge -l new-link bridge-name
```

En el siguiente ejemplo, se muestra cómo agregar el enlace qfe2 al puente existente rialto:

```
# dladm add-bridge -l qfe2 rialto
```

▼ Cómo eliminar enlaces de un puente

En este procedimiento, se muestra cómo eliminar uno o más enlaces de una instancia de puente. Utilice este procedimiento si desea eliminar un puente. Antes de eliminar el puente, se deben eliminar todos sus enlaces.

1 Conviértase en administrador.

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

2 Elimine los enlaces del puente.

```
# dladm remove-bridge [-l link]... bridge-name
```

En el siguiente ejemplo, se muestra cómo eliminar los enlaces hme0, qfe1 y qfe2 del puente charles:

```
# dladm remove-bridge -l hme0 -l qfe1 -l qfe2 charles
```

▼ Cómo eliminar un puente del sistema

En este procedimiento, se muestra cómo eliminar una instancia de puente. Antes de poder eliminar un puente, primero debe desactivar los enlaces conectados ejecutando el comando `dladm remove-bridge`. Consulte [“Cómo eliminar enlaces de un puente”](#) en la página 235.

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos”](#) de *Administración de Oracle Solaris: servicios de seguridad*.

2 Elimine el puente del sistema.

```
# dladm delete-bridge bridge-name
```

En el ejemplo siguiente, se muestra cómo eliminar, primero, los enlaces hme0, qfe1 y qfe2 del puente coronado, cómo eliminar, luego, el puente del sistema:

```
# dladm remove-bridge -l hme0 -l qfe1 -l qfe2 coronado  
# dladm delete-bridge coronado
```

Administración de agregaciones de enlaces

En este capítulo se describen los procedimientos para configurar y mantener agregaciones de enlaces. Los procedimientos incluyen pasos para aprovechar las nuevas características, como la compatibilidad con nombres de enlaces flexibles.

Descripción general de agregaciones de vínculos

Oracle Solaris admite la organización de interfaces de red en agregaciones de vínculos. Una *agregación de vínculos* consiste en varias interfaces de un sistema que se configuran juntas como una unidad lógica única. Las agregaciones de vínculos, también denominadas *truncaciones*, se definen en [IEEE 802.3ad Link Aggregation Standard \(http://www.ieee802.org/3/index.html\)](http://www.ieee802.org/3/index.html).

El estándar IEEE 802.3ad Link Aggregation proporciona un método para combinar la capacidad de varios vínculos Ethernet duplex en un único vínculo lógico. Este grupo de agregación de vínculos se trata como si fuera un único vínculo.

A continuación se enumeran las funciones de agregaciones de vínculos:

- **Ancho de banda ampliado** – La capacidad de varios vínculos se combina en un vínculo lógico.
- **Recuperación de fallos automática** – El tráfico de un vínculo que ha fallado se transfiere a vínculos activos de la agregación.
- **Equilibrio de carga** – El tráfico entrante y saliente se distribuye de acuerdo con directivas de equilibrio de carga definidas por el usuario, como las direcciones MAC e IP de origen y destino.
- **Admisión de duplicación** – Dos sistemas pueden configurarse con agregaciones paralelas.
- **Administración mejorada** – Todas las interfaces se administran como una única unidad.
- **Menos drenaje en la agrupación de direcciones de red** – Puede asignarse una dirección IP a la agregación completa.

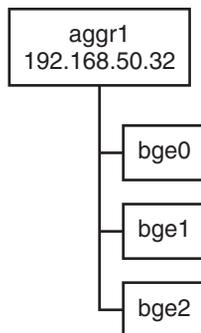
Conceptos básicos de agregaciones de vínculos

La configuración básica de una agregación de vínculos consta de una única agregación compuesta por un conjunto de interfaces físicas. Puede usar la agregación de vínculos básica en las siguientes situaciones:

- En sistemas con una aplicación con un gran volumen de tráfico distribuido, puede dedicar una agregación al tráfico de dicha aplicación.
- Para ubicaciones con espacio de direcciones IP limitado pero que requieren una gran cantidad de ancho de banda, sólo se necesita una dirección IP para una gran agregación de interfaces.
- Para ubicaciones que necesitan ocultar la existencia de interfaces internas, la dirección IP de la agregación oculta las interfaces a aplicaciones externas.

La [Figura 12–1](#) muestra una agregación de un servidor que aloja un sitio web muy visitado. Este sitio requiere un gran ancho de banda para el tráfico de peticiones entre los clientes en Internet y el servidor de base de datos del sitio. Por cuestiones de seguridad, la existencia de interfaces individuales en el servidor debe ocultarse a las aplicaciones externas. La solución es la agregación `aggr1` con la dirección IP `192.168.50.32`. Esta adición se compone de tres interfaces, de `bge0` a `bge2`. Estas interfaces se dedican a enviar el tráfico de respuesta a las peticiones de los clientes. La dirección saliente del tráfico de paquetes de todas las interfaces es la dirección IP de `aggr1`, `192.168.50.32`.

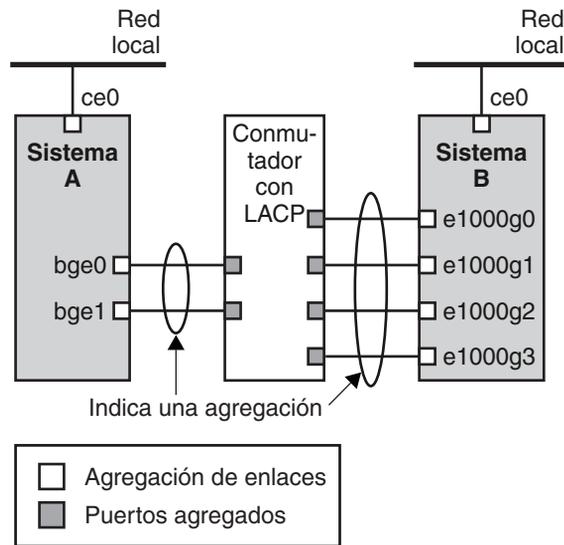
FIGURA 12–1 Configuración de agregación de vínculos básica



La [Figura 12–2](#) representa una red local con dos sistemas, cada uno con una agregación configurada. Los dos sistemas están conectados mediante un nodo (concentrador). Si necesita ejecutar una agregación a través de un nodo, el nodo debe admitir la tecnología de agregaciones. Este tipo de configuración resulta especialmente útil para sistemas de alta disponibilidad y con duplicación.

En la figura, el Sistema A tiene una agregación que consta de dos interfaces, bge0 y bge1. Estas interfaces están conectadas al nodo mediante puertos agregados. El Sistema B tiene una agregación de cuatro interfaces, de e1000g0 a e1000g3. Estas interfaces también están conectadas mediante puertos agregados del nodo.

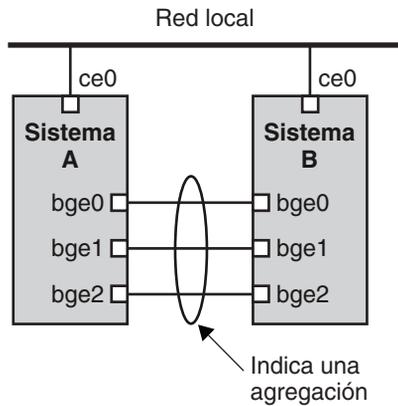
FIGURA 12-2 Configuración de agregación vínculos con nodo



Agregaciones de vínculos de extremo a extremo

La configuración de agregación de vínculos de extremo a extremo consta de dos sistemas independientes conectados directamente el uno al otro, como se muestra en la siguiente figura. Los sistemas ejecutan agregaciones paralelas.

FIGURA 12-3 Configuración de agregación de extremo a extremo básica



En esta figura, el dispositivo `bge0` del Sistema A está vinculado directamente a `bge0` en el Sistema B, etc. De este modo, los sistemas A y B permiten duplicación y alta disponibilidad, así como comunicaciones a alta velocidad entre ambos sistemas. Cada sistema también tiene la interfaz `ce0` configurada para el flujo de tráfico de la red local.

La aplicación más común para agregaciones de vínculo de extremo a extremo son los servidores de base de datos reflejados. Ambos servidores deben actualizarse a la vez y, por lo tanto, necesitan bastante ancho de banda, flujo de tráfico de alta velocidad y fiabilidad. El uso más habitual de las agregaciones de vínculos de extremo a extremo es en los centros de datos.

Directivas y equilibrio de la carga

Si planea utilizar una agregación de vínculos, es recomendable definir una directiva para el tráfico saliente. Esta directiva puede especificar cómo deben distribuirse los paquetes entre los vínculos disponibles de una agregación y, por lo tanto, establece el equilibrio de la carga. A continuación se enumeran los posibles especificadores de capa y su efecto en la directiva de agregación:

- **L2:** determina el vínculo de salida numerando el encabezado MAC (L2) de cada paquete
- **L3:** determina el vínculo de salida numerando el encabezado IP (L3) de cada paquete
- **L4:** determina el vínculo de salida numerando el encabezado TCP, UDP u otro ULP (L4) de cada paquete

También es válida cualquier combinación de estas directivas. La directiva predeterminada es L4. Si necesita más información, consulte la página de comando `man dladm(1M)`.

Modo de agregación y nodos

Si su configuración de agregación requiere conexión a través de un nodo, el nodo debe admitir el *protocolo de control de agregación de vínculos (LACP)*. Si el nodo admite LACP, debe configurar LACP para el nodo y la agregación. Sin embargo, puede definir uno de los siguientes *modos* de funcionamiento de LACP:

- **Modo inactivo:** el modo predeterminado para agregaciones. Los paquetes LACP, llamados *LACPDU* no se generan.
- **Modo activo:** el sistema genera paquetes LACPDU en intervalos regulares, que puede especificar el usuario.
- **Modo pasivo:** el sistema genera un LACPDU sólo cuando recibe un LACPDU del nodo. Si la agregación y el nodo están configurados en modo pasivo, no pueden intercambiar paquetes LACPDU.

Si necesita información sobre sintaxis, consulte la página de comando `man dladm(1M)` y la documentación del fabricante del nodo.

Requisitos para agregaciones de vínculos

La configuración de agregación de vínculos tiene los siguientes requisitos:

- Debe usar el comando `dladm` para configurar agregaciones.
- Una interfaz creada no puede ser miembro de una agregación.
- Todas las interfaces de la agregación deben ejecutarse a la misma velocidad y en modo duplex total.
- Debe definir el valor de direcciones MAC en “true” en el parámetro EEPROM `local-mac-address?` Si necesita instrucciones, consulte [Cómo asegurarse de que la dirección MAC de una interfaz sea única](#).

Algunos dispositivos no cumplen con el requisito del estándar de agregación de enlaces IEEE 802.3ad para admitir la notificación del estado del enlace. Esta compatibilidad debe existir para que un puerto se conecte con una agregación o se desconecte de una agregación. Los dispositivos que no admiten la notificación del estado del enlace sólo se pueden agregar utilizando la opción `-f` del comando `dladm crear-aggr`. Para tales dispositivos, el estado del enlace siempre se informa como UP. Para obtener información sobre el uso de la opción `-f`, consulte [“Cómo crear una agregación de vínculos” en la página 242](#).

Nombres flexibles para las agregaciones de enlaces

Los nombres flexibles se pueden asignar a las agregaciones de enlaces. Cualquier nombre significativo se puede asignar a una agregación de enlaces. Para obtener más información sobre nombres flexibles o personalizados, consulte [“Dispositivos de red y nombres de enlaces de](#)

datos” en la página 26. Las versiones anteriores de Oracle Solaris identifican una agregación de enlaces por el valor de una *clave* que se asigna a la agregación. Para obtener una explicación de este método, consulte [Descripción general de agregaciones de vínculos](#). Aunque ese método sigue siendo válido, es preferible utilizar nombres personalizados para identificar las agregaciones de enlaces.

De manera similar a como sucede con las configuraciones de enlaces de datos, las agregaciones de enlaces se administran con el comando `dladm`.

Administración de agregaciones de enlaces (mapa de tareas)

La siguiente tabla proporciona enlaces con los procedimientos para administrar las agregaciones de enlaces.

Tareas	Descripción	Para obtener instrucciones
Crear una agregación.	Configurar una agregación que conste de varios enlaces de datos.	“Cómo crear una agregación de vínculos” en la página 242
Modificar una agregación.	Cambiar el modo y la política de agregaciones.	“Cómo modificar una agregación” en la página 244
Modificar los enlaces que conforman una agregación.	Aumentar o reducir el número de enlaces de datos que subyacen a una agregación.	“Cómo agregar un enlace a una agregación” en la página 245 o “Cómo eliminar un enlace de una agregación” en la página 246
Eliminar una agregación.	Eliminar totalmente una agregación de enlaces de la configuración de red.	“Cómo eliminar una agregación” en la página 247

▼ Cómo crear una agregación de vínculos

Antes de empezar

Nota – Una agregación de vínculos sólo funciona en vínculos de punto a punto duplex total y con velocidad idéntica. Asegúrese de que las interfaces de su agregación cumplen este requisito.

Si utiliza un nodo en su configuración de agregación, asegúrese de hacer lo siguiente:

- Configure los puertos del nodo para que se utilicen como una agregación
- Si el nodo admite LACP, configure LACP en modo activo o pasivo

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Muestre la información de enlaces de datos de la red.

```
# dladm show-link
```

3 Asegúrese de que el enlace sobre el que está creando la agregación no se abra con cualquier aplicación.

Por ejemplo, si se crea la interfaz IP en el enlace, elimine la interfaz.

a. Para determinar si un enlace está siendo utilizado por alguna aplicación, examine la salida de las sintaxis `dladm show-link` o `ipadm show-if`.

- Si un enlace de datos está en uso, el campo STATE de la salida de `dladm show-link` indicará que el enlace es up, como se muestra a continuación:

```
# dladm show-link
LINK      CLASS      MTU      STATE      BRIDGE      OVER
qfe3     phys      1500     up         --         --
```

- Si el enlace de datos está en uso, la interfaz IP de ese enlace se incluirá en la salida de la sintaxis `ipadm show-if`, como se muestra a continuación:

```
# ipadm show-if
IFNAME      CLASS      STATE      ACTIVE      OVER
lo0         loopback   ok         yes         --
qfe3        ip         ok         no          --
```

Nota – Incluso si la salida muestra el estado `offline`, el enlace de datos todavía se utiliza porque existe una interfaz IP sobre el enlace.

b. Para eliminar la interfaz IP, escriba el siguiente comando:

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

donde

interfaz Especifica la interfaz IP que se crea sobre el enlace.

4 Cree una agregación de enlaces.

```
# dladm create-aggr [-f] -l link1 -l link2 [...] aggr
```

`-f` Fuerza la creación de la agregación. Utilice esta opción cuando intente agregar dispositivos que no admitan la notificación del estado del enlace.

linkn Especifica los enlaces de datos que desea agregar.

agregación Especifica el nombre que desee asignar a la agregación.

5 Cree una interfaz IP sobre la agregación.

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

6 Configure la interfaz IP con una dirección IP válida.

```
# ipadm create-addr interface -T static -a IP-address addrobj
```

donde *interfaz* debe llevar el nombre de la agregación y *objeto_dirección* utiliza la convención de denominación *interfaz/cadena_definida_por_usuario*.

7 Compruebe el estado de la agregación creada.

El estado de agregación debe ser UP.

```
# dladm show-aggr
```

Ejemplo 12-1 Creación de una agregación de vínculos

En este ejemplo, se muestran los comandos que se utilizan para crear una agregación de enlaces con dos enlaces de datos, subvideo0 y subvideo1. La configuración es persistente en los sucesivos reinicios del sistema.

```
# dladm show-link
LINK      CLASS      MTU      STATE   BRIDGE     OVER
subvideo0  phys       1500     up      --         ----
subvideo1  phys       1500     up46    --         ----

# ipadm delete-ip subvideo0
# ipadm delete-ip subvideo1
# dladm create-aggr -l subvideo0 -l subvideo1 video0
# ipadm create-ip video0
# ipadm create-addr -T static -a 10.8.57.50/24 video/v4
# dladm show-aggr
LINK      POLICY  ADDRPOLICY      LACPACTIVITY  LACPTIMER  FLAGS
video0    L4      auto             off            short      -----
```

Al visualizar la información del enlace, la agregación de enlaces se incluye en la lista.

```
# dladm show-link
LINK      CLASS      MTU      STATE   BRIDGE     OVER
subvideo0  phys       1500     up      --         ----
subvideo1  phys       1500     up      --         ----
video0     aggr      1500     up      --         subvideo0, subvideo1
```

▼ Cómo modificar una agregación

Este procedimiento muestra cómo realizar los siguientes cambios en una definición de agregación:

- Modificar la directiva de la agregación
- Cambiar el modo de la agregación

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Modifique la política de agregación.

```
# dladm modify-aggr -P policy-key aggr
```

clave_política Representa una o varias de las directivas L2, L3 y L4, como se explica en “Directivas y equilibrio de la carga” en la página 240.

agregación Especifica la agregación cuya política se desea modificar.

3 Modificar el modo del LACP de la agregación.

```
# dladm modify-aggr -L LACP-mode -T timer-value aggr
```

-L modo_LACP Indica el modo LACP de la agregación. Los valores son *active*, *passive* y *off*. Si el nodo utiliza LACP en modo pasivo, asegúrese de configurar el modo activo para la agregación.

-T valor_tiempo Indica el valor de tiempo LACP, *short* o *long*.

Ejemplo 12–2 Modificación de una agregación de vínculos

Este ejemplo muestra cómo modificar la política de agregación *video0* a L2 y, luego, habilitar el modo LACP activo.

```
# dladm modify-aggr -P L2 video0
# dladm modify-aggr -L active -T short video0
# dladm show-aggr
LINK      POLICY  ADDRPOLICY  LACPACTIVITY  LACPTIMER  FLAGS
video0    L2      auto        active         short      -----
```

▼ Cómo agregar un enlace a una agregación**1 Conviértase en administrador.**

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Asegúrese de que el enlace que desea agregar no tenga una interfaz IP conectada sobre el enlace.

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

3 Agregue el enlace a la agregación.

```
# dladm add-aggr -l link [-l link] [...] aggr
```

donde *enlace* representa un enlace de datos que está agregando a la agregación.

4 Realice otras tareas para modificar toda la configuración de agregación de enlaces después de que se agregan más enlaces de datos.

Por ejemplo, en el caso de una configuración que se ilustra en la [Figura 12–3](#), es posible que necesite agregar o modificar las conexiones de cable, y reconfigurar los conmutadores para que se incluyan los enlaces de datos adicionales. Consulte la documentación del conmutador para realizar cualquier tarea de reconfiguración en el conmutador.

Ejemplo 12–3 Cómo agregar un enlace a una agregación

En este ejemplo, se muestra cómo agregar un enlace a la agregación `video0`.

```
# dladm show-link
LINK      CLASS    MTU     STATE   BRODGE   OVER
subvideo0 phys     1500   up      --       ----
subvideo1 phys     1500   up      --       ----
video0    aggr     1500   up      --       subvideo0, subvideo1
net3      phys     1500   unknown --       ----

# ipadm delete-ip video0
# dladm add-aggr -l net3 video0
# dladm show-link
LINK      CLASS    MTU     STATE   BRIDGE   OVER
subvideo0 phys     1500   up      --       ----
subvideo1 phys     1500   up      --       ----
video0    aggr     1500   up      --       subvideo0, subvideo1, net3
net3      phys     1500   up      --       ----
```

▼ **Cómo eliminar un enlace de una agregación**

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Elimine un enlace de la agregación.

```
# dladm remove-aggr -l link aggr-link
```

Ejemplo 12–4 Cómo eliminar un enlace de una agregación

En este ejemplo, se muestra cómo eliminar un enlace de la agregación `video0`.

```
dladm show-link
LINK      CLASS    MTU     STATE   OVER
subvideo0 phys     1500   up      --       ----
subvideo1 phys     1500   up      --       ----
```

```

video0      aggr      1500    up      --      subvideo0, subvideo1, net3
net3        phys      1500    up      --      ----

# dladm remove-aggr -l net3 video0
# dladm show-link
LINK        CLASS     MTU      STATE   BRIDGE   OVER
subvideo0   phys     1500    up      --      ----
subvideo1   phys     1500    up      --      ----
video0      aggr     1500    up      --      subvideo0, subvideo1
net3        phys     1500    unknown --      ----

```

▼ Cómo eliminar una agregación

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Elimine la interfaz IP que se configura sobre la agregación.

```
# ipadm delete-ip IP-aggr
```

donde *IP-aggr* es la interfaz IP sobre la agregación de enlaces.

3 Elimine la agregación de enlaces.

```
# dladm delete-aggr aggr
```

Ejemplo 12-5 Cómo eliminar una agregación

En este ejemplo, se elimina la agregación `video0`. La eliminación persiste.

```
# ipadm delete-ip video0
# dladm delete-aggr video0
```


Administración de VLAN

En este capítulo se describen los procedimientos para configurar y mantener redes de área local virtuales (VLAN). Los procedimientos incluyen pasos en los que se aprovechan las características como la admisión de nombres de enlaces flexibles.

Administración de redes de área local virtuales

Una *red de área local virtual (VLAN)* es una subdivisión de una red de área local en la capa de vínculo de datos de la pila de protocolo TCP/IP. Puede crear redes VLAN para redes de área local que utilicen tecnología de nodo. Al asignar los grupos de usuarios en redes VLAN, puede mejorar la administración de red y la seguridad de toda la red local. También puede asignar interfaces del mismo sistema a redes VLAN diferentes.

Es recomendable dividir una red de área local en redes VLAN si necesita lo siguiente:

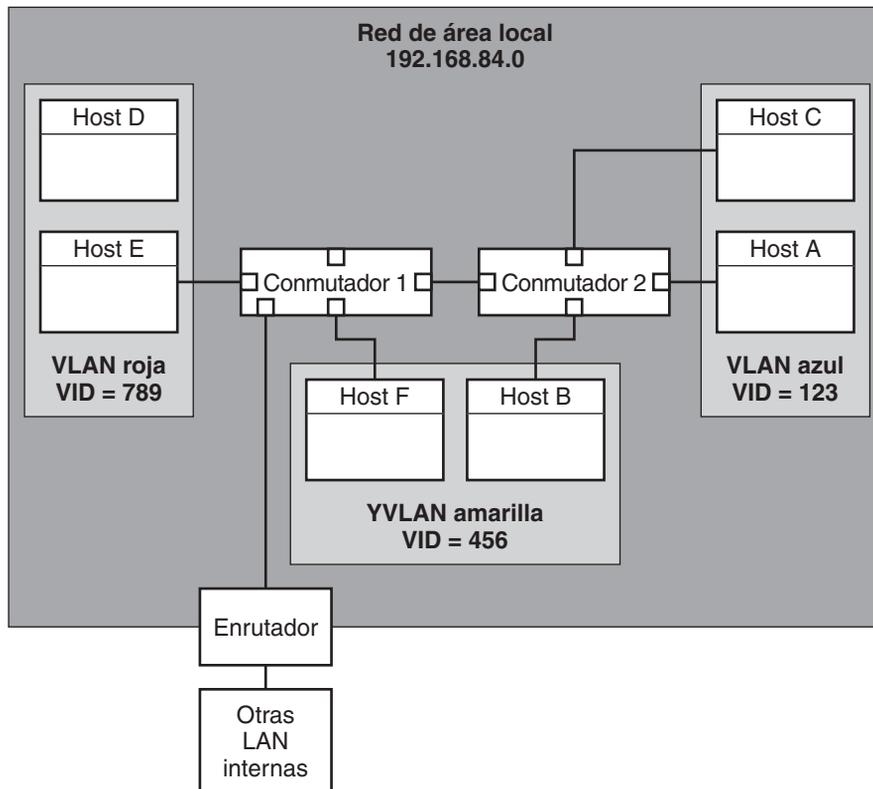
- Cree una división lógica de grupos de trabajo.
Por ejemplo, suponga que todos los hosts de la planta de un edificio están conectados mediante una red de área local con nodos. Puede crear una VLAN para cada grupo de trabajo de la planta.
- Diseñe diferentes directivas de seguridad para los grupos de trabajo.
Por ejemplo, las necesidades de seguridad del departamento de finanzas y el de informática son muy diferentes. Si los sistemas de ambos departamentos comparten la misma red local, puede crear una red VLAN independiente para cada departamento. Después, puede asignar la directiva de seguridad apropiada para cada VLAN.
- Divida los grupos de trabajo en dominios de emisión administrables.
El uso de redes VLAN reduce el tamaño de los dominios de emisión y mejora la efectividad de la red.

Descripción general de una configuración VLAN

La tecnología de red LAN con nodos permite organizar los sistemas de una red local en redes VLAN. Para poder dividir una red de área local en redes VLAN, debe tener nodos compatibles con la tecnología VLAN. Puede configurar todos los puertos de un nodo para que transfieran datos para una única VLAN o para varias VLAN, según el diseño de configuración VLAN. Cada fabricante utiliza procedimientos diferentes para configurar los puertos de un nodo.

En la figura siguiente se muestra una red de área local con la dirección de subred $192.168.84.0$. Esta red LAN está subdividida en tres redes VLAN, Roja, Amarilla y Azul.

FIGURA 13-1 Red de área local con tres redes VLAN

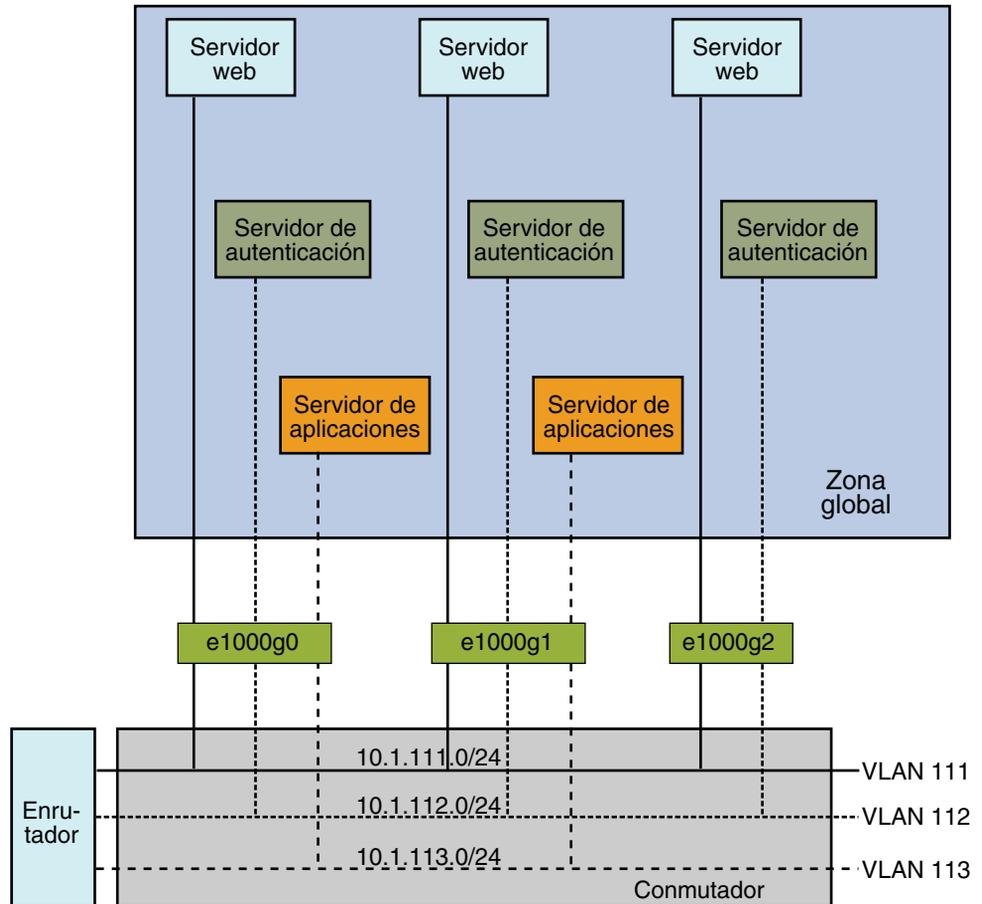


Los conmutadores 1 y 2 se encargan de la conexión a la red LAN $192.168.84.0$. La red VLAN contiene sistemas del grupo de trabajo Contabilidad. Los sistemas del grupo de trabajo Recursos humanos se encuentran en la red VLAN Amarilla. Los sistemas del grupo de trabajo Tecnologías de la información se asignan a la VLAN Azul.

Consolidación de la red mediante VLAN

Las VLAN en las zonas permiten configurar varias redes virtuales dentro de una única unidad de red, como un conmutador. Observe la siguiente ilustración de un sistema con tres NIC físicas:

FIGURA 13-2 Sistema con varias VLAN



Sin VLAN, tendría que configurar diferentes sistemas para realizar funciones específicas y conectarlos a redes separadas. Por ejemplo, los servidores web se tendrían que conectar a una LAN, los servidores de autenticación a otra y los servidores de aplicaciones a una tercera. Con las VLAN y las zonas, puede contraer los ocho sistemas y configurarlos como zonas en un único

sistema. Luego puede usar etiquetas VLAN o ID de VLAN (VID) para asignar una VLAN a cada juego de zonas que realiza las mismas funciones. La información proporcionada en la figura se puede tabular de la siguiente manera:

Función	Nombre de zona	Nombre de VLAN	VID	Dirección IP	NIC
Servidor web	webzone1	web1	111	10.1.111.0	e1000g0
Servidor de autenticación	authzone1	auth1	112	10.1.112.0	e1000g0
Application Server	appzone1	app1	113	10.1.113.0	e1000g0
Servidor web	webzone2	web2	111	10.1.111.0	e1000g1
Servidor de autenticación	authzone2	auth2	112	10.1.112.0	e1000g1
Application Server	appzone2	app2	113	10.1.113.0	e1000g1
Servidor web	webzone3	web3	111	10.1.111.0	e1000g2
Servidor de autenticación	authzone3	auth3	112	10.1.112.0	e1000g2

Para ver cómo crear la configuración que se muestra en la figura, consulte el [Ejemplo 13–1](#).

Nombres significativos para redes VLAN

En Oracle Solaris, puede asignar nombres significativos a las interfaces VLAN. Los nombres de VLAN constan de un nombre de enlace y el número de ID de VLAN (VID), como `sa1es0` debe asignar nombres personalizados al crear las VLAN. Para obtener más información sobre nombres de enlaces de datos personalizados, consulte “[Dispositivos de red y nombres de enlaces de datos](#)” en la [página 26](#). Para obtener más información sobre los nombres personalizados válidos, consulte “[Reglas para nombres de enlace válidos](#)” en la [página 31](#).

Administración de VLAN (mapa de tareas)

La siguiente tabla proporciona enlaces con diferentes tareas para administrar VLAN.

Tarea	Descripción	Para obtener instrucciones
Planificar una red de área local virtual (VLAN).	Llevar a cabo las tareas de planificación necesarias antes de crear una VLAN.	“ Cómo planificar la configuración de una VLAN ” en la página 253

Tarea	Descripción	Para obtener instrucciones
Configurar una VLAN.	Crear las VLAN en la red.	“Cómo configurar una VLAN” en la página 254
Configurar una VLAN en una agregación.	Desplegar tecnologías combinadas que usen tanto VLAN como agregaciones de enlaces.	“Cómo configurar VLAN a través de una adición de vínculos ” en la página 257
Mostrar información de VLAN.	Obtener información sobre una VLAN y sus componentes.	“Cómo visualizar la información de las VLAN” en la página 259
Eliminar una VLAN.	Seleccionar una VLAN para eliminarla de un conjunto de varias VLAN configuradas en un enlace de datos.	“Como eliminar una VLAN” en la página 260

Planificación de una red para redes VLAN

Utilice el procedimiento siguiente para planificar las VLAN de la red.

▼ Cómo planificar la configuración de una VLAN

- 1 **Examine la distribución de red local y determine dónde es apropiado realizar las subdivisiones en redes VLAN.**

Para ver un ejemplo básico de esta topología, consulte la [Figura 13-1](#).

- 2 **Cree un esquema numerado para los VID y asigne un VID a cada VLAN.**

Nota – Puede que ya haya un esquema numerado de VLAN en la red. En tal caso, deberá crear los VID dentro del esquema numerado de VLAN.

- 3 **En cada sistema, determine las interfaces que deben ser miembros de una VLAN determinada.**

- a. **Determine las interfaces que se configuran en un sistema.**

```
# dladm show-link
```

- b. **Identifique qué VID debe asociarse con cada vínculo de datos del sistema.**

- c. **Cree la VLAN usando el comando `dladm create-vlan`.**

- 4 **Compruebe las conexiones de las interfaces con los nodos de red.**

Anote el VID de cada interfaz y el puerto de nodo al que están conectadas.

- 5 **Configure cada puerto del nodo con el mismo VID de la interfaz al que está conectado.**
Consulte la documentación del fabricante del nodo para ver las instrucciones de configuración.

Configuración de redes VLAN

El procedimiento siguiente muestra cómo crear y configurar una VLAN. En Oracle Solaris, todos los dispositivos Ethernet pueden admitir VLAN. Sin embargo, existen algunas restricciones para algunos dispositivos. Para conocer estas restricciones, consulte [“VLAN en dispositivos heredados”](#) en la página 258.

▼ Cómo configurar una VLAN

Antes de empezar Los enlaces de datos ya deben estar configurados en el sistema antes de poder crear las VLAN. Consulte [“Cómo configurar una interfaz IP”](#) en la página 181.

- 1 **Conviértase en administrador.**

Para obtener más información, consulte [“Cómo obtener derechos administrativos”](#) de *Administración de Oracle Solaris: servicios de seguridad*.

- 2 **Determine los tipos de enlaces que se utilizan en el sistema.**

```
# dladm show-link
```

- 3 **Cree un enlace VLAN sobre un enlace de datos.**

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

enlace Especifica el enlace en el que se crea la interfaz VLAN.

VID Indica el número de ID de VLAN.

enlace_VLAN Especifica el nombre de la VLAN, que también puede ser un nombre elegido administrativamente.

- 4 **Verifique la configuración de la VLAN.**

```
# dladm show-vlan
```

- 5 **Cree una interfaz IP en la VLAN.**

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

donde *interfaz* utiliza el nombre de la VLAN.

- 6 **Configure la interfaz IP con una dirección IP.**

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

donde *objeto_dirección* utiliza la convención de denominación *interfaz/cadena_definida_por_usuario*.

Ejemplo 13-1 Configuración de una VLAN

En este ejemplo, se crea la configuración de la VLAN que se ilustra en la [Figura 13-2](#). En este ejemplo, se asume que ya ha configurado las diferentes zonas en el sistema. Para obtener más información sobre la configuración de las zonas, consulte la [Parte II, “Zonas de Oracle Solaris” de Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#).

```
global# dladm show-link
LINK          CLASS      MTU      STATE    BRIDGE    OVER
e1000g0      phys      1500    up       --        --
e1000g1      phys      1500    up       --        --
e1000g2      phys      1500    up       --        --

global# dladm create-vlan -l e1000g0 -v 111 web1
global# dladm create-vlan -l e1000g0 -v 112 auth1
global# dladm create-vlan -l e1000g0 -v 113 app1
global# dladm create-vlan -l e1000g1 -v 111 web2
global# dladm create-vlan -l e1000g1 -v 112 auth2
global# dladm create-vlan -l e1000g1 -v 113 app2
global# dladm create-vlan -l e1000g2 -v 111 web3
global# dladm create-vlan -l e1000g2 -v 112 auth3

global# dladm show-vlan
LINK          VID      OVER      FLAGS
web1          111     e1000g0  ----
auth1         112     e1000g0  ----
app1          113     e1000g0  ----
web2          111     e1000g1  ----
auth2         112     e1000g1  ----
app2          113     e1000g1  ----
web3          111     e1000g2  ----
auth3         113     e1000g2  ----
```

Cuando se muestra la información de enlace, las VLAN se incluyen en la lista.

```
global# dladm show-link
LINK          CLASS      MTU      STATE    BRIDGE    OVER
e1000g0      phys      1500    up       --        --
e1000g1      phys      1500    up       --        --
e1000g2      phys      1500    up       --        --
web1          vlan      1500    up       --        e1000g0
auth1         vlan      1500    up       --        e1000g0
app1          vlan      1500    up       --        e1000g0
web2          vlan      1500    up       --        e1000g1
auth2         vlan      1500    up       --        e1000g1
app2          vlan      1500    up       --        e1000g1
web3          vlan      1500    up       --        e1000g2
auth3         vlan      1500    up       --        e1000g2
```

Se asignan las VLAN a sus zonas respectivas. Por ejemplo, cuando busca información de red respecto de las zonas individuales, se mostrarían datos similares a los siguientes para cada zona:

```
global# zonecfg -z webzone1 info net
net:
  address not specified
  physical: web1
```

```
global# zonecfg -z authzone1 info net
net:
  address not specified
  physical: auth1
```

```
global# zonecfg -z appzone2 info net
net:
  address not specified
  physical: app2
```

El valor de la propiedad `physical` indica la VLAN que se define para una zona determinada.

Debe iniciar sesión en cada zona no global para configurar la VLAN con una dirección IP.

En `webzone1`:

```
webzone1# ipadm create-ip web1
webzone1# ipadm create-addr -T static -a 10.1.111.0/24 web1/v4
```

En `webzone2`:

```
webzone2# ipadm create-ip web2
webzone2# ipadm create-addr -T static -a 10.1.111.0/24 web2/v4
```

En `webzone3`:

```
webzone3# ipadm create-ip web3
webzone3# ipadm create-addr -T static -a 10.1.111.0/24 web3/v4
```

En `authzone1`:

```
authzone1# ipadm create-ip auth1
authzone1# ipadm create-addr -T static -a 10.1.112.0/24 auth1/v4
```

En `authzone2`:

```
authzone2# ipadm create-ip auth2
authzone2# ipadm create-addr -T static -a 10.1.112.0/24 auth2/v4
```

En `authzone3`:

```
authzone3# ipadm create-ip auth3
authzone3# ipadm create-addr -T static -a 10.1.112.0/24 auth3/v4
```

En `appzone1`:

```
appzone1# ipadm create-ip app1
appzone1# ipadm create-addr -T static -a 10.1.113.0/24 app1/v4
```

En appzone2:

```
appzone2# ipadm create-ip app2
appzone2# ipadm create-addr -T static -a 10.1.113.0/24 app2/v4
```

▼ Cómo configurar VLAN a través de una adición de vínculos

Del mismo modo en que se configura VLAN a través de una interfaz, también se pueden crear VLAN en una adición de vínculos. Las agregaciones de enlaces se describen en el [Capítulo 12, “Administración de agregaciones de enlaces”](#). En esta sección se combina la configuración de VLAN y las adiciones de vínculos.

Antes de empezar Primero cree la agregación de enlaces y luego configúrela con una dirección IP válida. Para crear adiciones de vínculos, consulte [“Cómo crear una agregación de vínculos” en la página 242](#).

1 Liste las agregaciones que estén configuradas en el sistema.

```
# dladm show-link
```

2 Para cada VLAN que desee crear por la agregación, emita el siguiente comando.

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

donde

enlace Especifica el enlace en el que se crea la interfaz VLAN. En este caso concreto, el vínculo se refiere a la agregación de enlaces.

VID Indica el número de ID de VLAN.

enlace_VLAN Especifica el nombre de la VLAN, que también puede ser un nombre elegido administrativamente.

3 Cree interfaces IP sobre la VLAN.

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

donde *interfaz* utiliza el nombre de la VLAN.

4 Configure interfaces IP sobre las VLAN con direcciones IP válidas.

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

donde *objeto_dirección* debe seguir la convención de denominación *interfaz_VLAN/cadena_definida_por_usuario*

Ejemplo 13–2 Configuración de varias VLAN a través de una adición de vínculos

En este ejemplo se configuran dos VLAN en una adición de vínculos. A las VLAN se asignan los VID 193 y 194, respectivamente.

```
# dladm show-link
LINK      CLASS  MTU   STATE  BRIDGE  OVER
subvideo0 phys   1500  up     --      ----
subvideo1 phys   1500  up     --      ----
video0    aggr   1500  up     --      subvideo0, subvideo1

# dladm create-vlan -l video0 -v 193 salesregion1
# dladm create-vlan -l video0 -v 194 salesregion2

# ipadm create-ip salesregion1
# ipadm create-ip salesregion2

# ipadm create-addr -T static -a 192.168.10.5/24 salesregion1/v4static
# ipadm create-addr -T static -a 192.168.10.25/24 salesregion2/v4static
```

VLAN en dispositivos heredados

Determinados dispositivos heredados manejan solamente los paquetes que tengan un tamaño de marco máximo de 1514 bytes. Los paquetes cuyo tamaño de marco supera el límite máximo se eliminan. En ese caso, siga el mismo procedimiento que aparece en [“Cómo configurar una VLAN” en la página 254](#). Sin embargo, al crear la VLAN, utilice la opción `-f` para forzar la creación de la VLAN.

Los pasos generales que se deben realizar son los siguientes:

1. Cree la VLAN con la opción `-f`.

```
# dladm create-vlan -f -l link -v VID [vlan-link]
```

2. Establezca un tamaño menor para la unidad de transmisión máxima (MTU, Maximum Transmission Unit); por ejemplo, 1496 bytes.

```
# dladm set-linkprop -p default_mtu=1496 vlan-link
```

Un valor de MTU menor da espacio para que la capa de enlace inserte el encabezado VLAN antes de la transmisión.

3. Realice el mismo paso para establecer el mismo valor menor para el tamaño de MTU de cada nodo de la VLAN.

Para obtener más información sobre cómo cambiar los valores de las propiedades de enlaces, consulte [“Configuración de enlaces de datos \(tareas\)” en la página 155](#).

Realización de otras tareas administrativas en redes VLAN

En esta sección, se describe el uso de nuevos subcomandos `dladm` para otras tareas VLAN. Estos comandos `dladm` también trabajan con nombres de enlaces.

▼ Cómo visualizar la información de las VLAN

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Muestre la información de la VLAN.

```
# dladm show-vlan [vlan-link]
```

Si no especifica el enlace de una VLAN, el comando muestra información de todas las VLAN configuradas.

Ejemplo 13-3 Visualización de la información de las VLAN

El ejemplo siguiente se basa en el sistema con varias VLAN que se ilustra en la [Figura 13-2](#) y muestra las VLAN disponibles en el sistema.

```
# dladm show-vlan
LINK      VID      OVER      FLAGS
web1      111      e1000g0   ----
auth1     112      e1000g0   ----
app1      113      e1000g0   ----
web2      111      e1000g1   ----
auth2     112      e1000g1   ----
app2      113      e1000g1   ----
web3      111      e1000g2   ----
auth3     113      e1000g2   ----
```

Las VLAN configuradas también aparecerán cuando emita el comando `dladm show-link`. En la salida del comando, las VLAN se identifican de manera adecuada en la columna `CLASS`.

```
# dladm show-link
LINK      CLASS    MTU      STATE    BRIDGE    OVER
e1000g0   phys    1500    up       --        --
e1000g1   phys    1500    up       --        --
e1000g2   phys    1500    up       --        --
web1      vlan    1500    up       --        e1000g0
auth1     vlan    1500    up       --        e1000g0
app1      vlan    1500    up       --        e1000g0
web2      vlan    1500    up       --        e1000g1
auth2     vlan    1500    up       --        e1000g1
app2      vlan    1500    up       --        e1000g1
web3      vlan    1500    up       --        e1000g2
auth3     vlan    1500    up       --        e1000g2
```

▼ Como eliminar una VLAN

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Determine qué VLAN desea eliminar.

```
# dladm show-vlan
```

3 Desconecte la interfaz IP de la VLAN.

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

donde *interfaz_VLAN* es la interfaz IP que se configura sobre la VLAN.

Nota – No se puede eliminar un VLAN que se está utilizando actualmente.

4 Elimine la VLAN realizando uno de los siguientes pasos:

- Para eliminar la VLAN temporalmente, utilice la opción `-t` de la siguiente manera:

```
# dladm delete-vlan -t vlan
```

- Para que la eliminación persista, realice las siguientes acciones:

- a. Elimine la VLAN.

```
# dladm delete-vlan vlan
```

Ejemplo 13-4 Eliminación de una VLAN

```
# dladm show-vlan
LINK      VID      OVER      FLAGS
web1      111      e1000g0   ----
auth1     112      e1000g0   ----
app1      113      e1000g0   ----
web2      111      e1000g1   ----
auth2     112      e1000g1   ----
app2      113      e1000g1   ----
web3      111      e1000g2   ----
auth3     113      e1000g2   ----

# ipadm delete-ip web1
# dladm delete-vlan web1
```

Combinación de tareas de configuración de red cuando se utilizan nombres personalizados

En esta sección, se proporciona un ejemplo que combina todos los procedimientos de los capítulos anteriores sobre configuración de enlaces, agregaciones de enlaces y VLAN cuando se utilizan nombres personalizados. Para obtener una descripción de otros escenarios de red que utilizan nombres personalizados, consulte el artículo que se encuentra en <http://www.oracle.com/us/sun/index.htm>.

EJEMPLO 13-5 Configuración de enlaces, VLAN y agregaciones de enlaces

En este ejemplo, un sistema que utiliza 4 NIC se debe configurar para que funcione como un enrutador para 8 subredes independientes. Para alcanzar este objetivo, se configuran 8 enlaces, uno para cada subred. En primer lugar, se crea una agregación de enlaces en todos los 4 NIC. Este enlace sin etiquetas se convierte en la subred sin etiquetas predeterminada para la red a la que apunta la ruta predeterminada.

Luego, las interfaces VLAN se configuran sobre la agregación de enlaces para las otras subredes. Se asignan nombres a las subredes en función de un esquema de códigos por colores. Los nombres de las VLAN se asignan de manera consecutiva para que se correspondan con sus respectivas subredes. La configuración final consta de 8 enlaces para las 8 subredes: 1 enlace sin etiquetas y 7 enlaces VLAN con etiquetas.

Para que las configuraciones persistan tras los reinicios, se aplican los mismos procedimientos que en las versiones anteriores de Oracle Solaris. Por ejemplo, las direcciones IP se tienen que agregar en los archivos de configuración como `/etc/inet/ndpd.conf`. O bien, se deben incluir reglas de filtro para las interfaces en un archivo de reglas. Estos últimos pasos no se incluyen en el ejemplo. Para llevar a cabo estos pasos, consulte los capítulos correspondientes en *Administración de Oracle Solaris: servicios IP*; en especial, *Administración de TCP/IP y DHCP*.

```
# dladm show-link
LINK          CLASS      MTU  STATE  BRIDGE  OVER
nge0          phys      1500 up     --      --
nge1          phys      1500 up     --      --
e1000g0       phys      1500 up     --      --
e1000g1       phys      1500 up     --      --

# dladm show-phys
LINK          MEDIA          STATE  SPEED  DUPLEX  DEVICE
nge0          Ethernet      up     1000Mb full   nge0
nge1          Ethernet      up     1000Mb full   nge1
e1000g0       Ethernet      up     1000Mb full   e1000g0
e1000g1       Ethernet      up     1000Mb full   e1000g1

# ipadm delete-ip nge0
# ipadm delete-ip nge1
# ipadm delete-ip e1000g0
# ipadm delete-ip e1000g1
```

EJEMPLO 13-5 Configuración de enlaces, VLAN y agregaciones de enlaces (Continuación)

```

# dladm rename-link nge0 net0
# dladm rename-link nge1 net1
# dladm rename-link e1000g0 net2
# dladm rename-link e1000g1 net3

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

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

# dladm create-aggr -P L2,L3 -l net0 -l net1 -l net2 -l net3 default0

# dladm show-link
LINK      CLASS      MTU  STATE  BRIDGE  OVER
net0      phys      1500 up     --      --
net1      phys      1500 up     --      --
net2      phys      1500 up     --      --
net3      phys      1500 up     --      --
default0  aggr      1500 up     --      net0 net1 net2 net3

# dladm create-vlan -v 2 -l default0 orange0
# dladm create-vlan -v 3 -l default0 green0
# dladm create-vlan -v 4 -l default0 blue0
# dladm create-vlan -v 5 -l default0 white0
# dladm create-vlan -v 6 -l default0 yellow0
# dladm create-vlan -v 7 -l default0 red0
# dladm create-vlan -v 8 -l default0 cyan0

# dladm show-link
LINK      CLASS      MTU  STATE  BRIDGE  OVER
net0      phys      1500 up     --      --
net1      phys      1500 up     --      --
net2      phys      1500 up     --      --
net3      phys      1500 up     --      --
default0  aggr      1500 up     --      net0 net1 net2 net3
orange0   vlan      1500 up     --      default0
green0    vlan      1500 up     --      default0
blue0     vlan      1500 up     --      default0
white0    vlan      1500 up     --      default0
yellow0   vlan      1500 up     --      default0
red0      vlan      1500 up     --      default0
cyan0     vlan      1500 up     --      default0

# dladm show-vlan
LINK      VID  OVER      FLAGS
orange0   2    default0  -----

```

EJEMPLO 13-5 Configuración de enlaces, VLAN y agregaciones de enlaces (Continuación)

```
green0          3  default0  -----
blue0           4  default0  -----
white0          5  default0  -----
yellow0        6  default0  -----
red0            7  default0  -----
cyan0           8  default0  -----

# ipadm create-ip orange0
# ipadm create-ip green0
# ipadm create-ip blue0
# ipadm create-ip white0
# ipadm create-ip yellow0
# ipadm create-ip red0
# ipadm create-ip cyan0

# ipadm create-addr -T static -a IP-address orange0/v4
# ipadm create-addr -T static -a IP-address green0/v4
# ipadm create-addr -T static -a IP-address blue0/v4
# ipadm create-addr -T static -a IP-address white0/v4
# ipadm create-addr -T static -a IP-address yellow0/v4
# ipadm create-addr -T static -a IP-address red0/v4
# ipadm create-addr -T static -a IP-address cyan0/v4
```


Introducción a IPMP

La ruta múltiple de red IP (IPMP) proporciona detección de errores de interfaz física, conmutación por error de acceso a la red de manera transparente y expansión de carga de paquetes para los sistemas con varias interfaces que están conectados a una determinada red de área local o LAN.

Este capítulo contiene la información siguiente:

- “Novedades con IPMP” en la página 265
- “Implementación de IPMP” en la página 266
- “Componentes de IPMP en Oracle Solaris” en la página 276
- “Tipos de configuraciones de interfaces IPMP” en la página 277
- “Direcciones IPMP” en la página 278
- “Detección de fallos y reparaciones en IPMP” en la página 279
- “IPMP y reconfiguración dinámica” en la página 284
- “Terminología y conceptos de IPMP” en la página 286

Nota – En toda la descripción de IPMP de este capítulo y en el [Capítulo 15, “Administración de IPMP”](#), toda referencia al término *interfaz* significa específicamente *interfaz IP*. A menos que se indique explícitamente un uso diferente del término, como una tarjeta de interfaz de red (NIC), el término siempre hace referencia a la interfaz que se configura en la capa IP.

Novedades con IPMP

Las siguientes funciones diferencian la implementación de IPMP actual de la implementación anterior:

- Un grupo IPMP se representa como una interfaz IP IPMP. Esta interfaz se trata como cualquier otra interfaz en la capa IP de la pila de red. Todas las tareas administrativas, tablas de enrutamiento, tablas de protocolo de resolución de direcciones (ARP), reglas de cortafuegos y otros procedimientos relacionados con IP funcionan con un grupo IPMP haciendo referencia a la interfaz IPMP.

- El sistema pasa a ser responsable de la distribución de direcciones de datos entre interfaces activas subyacentes. En la implementación de IPMP anterior, el administrador inicialmente determina la vinculación de direcciones de datos con sus correspondientes interfaces cuando se crea el grupo IPMP. En la implementación actual, cuando se crea el grupo IPMP, las direcciones de datos pertenecen a la interfaz IPMP como una agrupación de direcciones. El núcleo automáticamente y aleatoriamente vincula las direcciones de datos a las interfaces activas del grupo.
- La herramienta `ipmpstat` se presenta como la herramienta principal para obtener información sobre los grupos IPMP. Este comando proporciona información acerca de todos los aspectos de la configuración de IPMP, como las interfaces IP subyacentes del grupo, las direcciones de datos y las pruebas, los tipos de detección de fallos en uso y las interfaces que tuvieron errores. Las funciones `ipmpstat`, las opciones que puede utilizar y la salida que cada opción genera se describen en [“Supervisión de información de IPMP” en la página 315](#).
- A la interfaz IPMP se puede asignar un nombre personalizado para identificar el grupo IPMP más fácilmente dentro de la configuración de red. Para conocer los procedimientos para configurar grupos IPMP con nombres personalizados, consulte cualquier procedimiento que describa la creación de un grupo IPMP en [“Configuración de grupos IPMP” en la página 298](#).

Nota – Para utilizar IPMP, asegúrese de que el perfil `DefaultFixed` esté habilitado en el sistema. Para conocer los procedimientos, consulte [“Herramientas de configuración y perfiles” en la página 152](#). Para obtener más información sobre la configuración de red gestionada por perfiles, consulte el [Capítulo 4, “Configuración de perfiles de NWAM \(tareas\)”](#).

Implementación de IPMP

En esta sección se describen diversos temas sobre el uso de grupos IPMP.

Por qué debe utilizar IPMP

Diferentes factores pueden provocar que no se pueda utilizar una interfaz. Normalmente, una interfaz IP puede fallar. O bien, una interfaz podría dejarse sin conexión para mantenimiento de hardware. En tales casos, sin un grupo IPMP, no se puede contactar al sistema mediante ninguna de las direcciones IP asociadas con la interfaz que no se puede utilizar. Además, las conexiones existentes que utilizan esas direcciones IP se interrumpen.

Con IPMP, una o más interfaces IP se pueden configurar en un *grupo IPMP*. El grupo funciona como una interfaz IP con direcciones de datos para enviar o recibir tráfico de la red. Si una interfaz subyacente del grupo falla, las direcciones de datos se redistribuyen entre las restantes interfaces activas subyacentes del grupo. Por lo tanto, el grupo mantiene conectividad de red a

pesar de un fallo de la interfaz. Con IPMP, la conectividad de red siempre está disponible, siempre que un mínimo de una interfaz pueda ser utilizado por el grupo.

Asimismo, IPMP mejora el rendimiento global de la red al expandir automáticamente el tráfico de la red saliente por un conjunto de interfaces del grupo IPMP. Este proceso se denomina *expansión de carga* saliente. El sistema también indirectamente controla la expansión de carga entrante realizando una selección de direcciones de origen para los paquetes cuya dirección IP de origen no fue especificada por la aplicación. Sin embargo, si una aplicación ha seleccionado explícitamente una dirección IP de origen, el sistema no modifica esa dirección de origen.

Cuando se debe utilizar IPMP

La configuración de un grupo IPMP está determinada por las configuraciones del sistema. Tenga en cuenta las siguientes reglas:

- Varias interfaces IP en la misma red de área local o la LAN deben estar configuradas en un grupo IPMP. LAN hace referencia básicamente a una variedad de configuraciones de redes locales, incluidas las VLAN y redes locales inalámbricas y cableadas cuyos nodos pertenecen al *mismo dominio de emisión de capa de enlace*.

Nota – No se admiten varios grupos IPMP en el mismo dominio de emisión de capa de enlace (L2). Normalmente, un dominio de emisión L2 se asigna a una subred específica. Por lo tanto, debe configurar sólo un grupo IPMP por subred.

- Las interfaces IP subyacentes de un grupo IPMP no deben abarcar diferentes LAN.

Por ejemplo, supongamos que un sistema con tres interfaces está conectado a dos LAN separadas. Dos interfaces IP se enlazan a una única LAN mientras que una interfaz IP única se conecta a la otra. En este caso, las dos interfaces IP que se conectan a la primera LAN deben estar configuradas como un grupo IPMP, tal y como exige la primera regla. De conformidad con la segunda regla, la interfaz IP única que se conecta a la segunda LAN no puede convertirse en miembro de ese grupo IPMP. No es necesaria ninguna configuración de IPMP de la interfaz IP única. Sin embargo, puede configurar la interfaz única en un grupo IPMP para supervisar la disponibilidad de la interfaz. La configuración de IPMP de interfaz única se trata en profundidad en [“Tipos de configuraciones de interfaces IPMP” en la página 277](#).

Tenga en cuenta otro caso en que el enlace a la primera LAN consta de tres interfaces IP mientras que el otro enlace consta de dos interfaces. Esta configuración necesita la configuración de dos grupos IPMP: un grupo de tres interfaces que enlaza a la primera LAN y un grupo de dos interfaces para conectarse a la segunda.

Comparación IPMP y agregación de enlaces

IPMP y la agregación de enlaces son diferentes tecnologías para lograr un mejor rendimiento de la red y para mantener la disponibilidad de la red. En general, se implementa la agregación de enlaces para obtener un mejor rendimiento de la red, en cambio, se utiliza IPMP para garantizar una alta disponibilidad.

En la siguiente tabla se presenta una comparación general entre agregación de enlaces e IPMP.

	IPMP	Agregación de enlaces
Tipo de tecnología de red	Nivel 3 (capa IP)	Capa 2 (capa de enlace)
Herramienta de configuración	ipadm	dladm
Detección de fallos basada en enlaces	Compatible	Compatible
Detección de fallos basada en sondeos	Basada en ICMP, tiene como objetivo cualquier sistema definido en la misma subred IP como direcciones de prueba, entre varios niveles de conmutadores de Capa 2 participantes.	Basada en el protocolo de control de agregación de enlaces (LACP), tiene como objetivo un host o conmutador de igual inmediato.
Uso de interfaces de reserva	Compatible	No compatible
Conmutadores múltiples	Compatible	Por lo general no es compatible; algunos proveedores proporcionan soluciones de propiedad y no interoperables para abarcar conmutadores múltiples.
Compatibilidad de hardware	No requerida	Obligatorio. Por ejemplo, una agregación de enlaces en el sistema que ejecuta Oracle Solaris requiere que se agreguen también los puertos correspondientes en los conmutadores.
Requisitos de capa de enlace	Permite la difusión	Específica de ethernet.
Requisitos de estructura de controlador	Ninguna	Debe utilizar la estructura GLDv3.
Compatibilidad de expansión de carga	Presente, controlada por núcleo. La selección de dirección de origen afecta indirectamente la expansión de carga entrante.	Un control preciso del administrador sobre la expansión de carga de tráfico saliente mediante el comando dladm. Expansión de carga de entrante compatible.

En las agregaciones de enlaces, el tráfico entrante se extiende sobre los múltiples enlaces que componen la agregación. Por lo tanto, el rendimiento de la red mejora a medida que más NIC se instalan para agregar enlaces a la agregación. El tráfico de IPMP utiliza direcciones de datos de la interfaz IPMP que estén vinculadas a interfaces activas disponibles. Si, por ejemplo, todo el tráfico de datos fluye entre sólo dos direcciones IP, pero no necesariamente en la misma conexión, si se agregan más NIC no mejorará el rendimiento con IPMP porque sólo dos direcciones IP son utilizables.

Las dos tecnologías se complementan mutuamente y se pueden implementar juntas para proporcionar los beneficios combinados de rendimiento de la red y disponibilidad. Por ejemplo, excepto donde ciertos proveedores proporcionan soluciones de propiedad, las agregaciones de enlaces no pueden abarcar actualmente múltiples conmutadores. Por lo tanto, un conmutador se convertirá en un único punto de fallo de una agregación de enlaces entre el conmutador y un host. Si el conmutador falla, la agregación de enlaces posiblemente se pierda y disminuya el rendimiento de la red. Los grupos IPMP no enfrentan esta limitación de conmutador. Por lo tanto, en el caso de una LAN que utiliza conmutadores múltiples, las agregaciones de enlaces que se conectan con sus respectivos conmutadores se pueden combinar en un grupo IPMP en el host. Con esta configuración, se obtienen un rendimiento de red mejorado y una alta disponibilidad. Si un conmutador falla, las direcciones de datos de la agregación de enlaces para ese conmutador que ha fallado se redistribuyen entre las restantes agregaciones de enlaces del grupo.

Para obtener más información acerca de las agregaciones de enlaces, consulte el [Capítulo 12, “Administración de agregaciones de enlaces”](#).

Uso de nombres de enlace flexibles en la configuración IPMP

Con compatibilidad para nombres de enlace personalizados, la configuración de enlaces ya no está vinculada a la NIC física a la que el enlace está asociado. El uso de nombres de enlace personalizados le permite tener una mayor flexibilidad a la hora de administrar interfaces IP. Esta flexibilidad amplía también la administración IPMP. Si una interfaz subyacente de un grupo IPMP falla y se requiere un reemplazo, los procedimientos para reemplazar la interfaz se facilitan en gran medida. El reemplazo de la NIC, siempre que sea del mismo tipo que la NIC que ha fallado, se puede cambiar de nombre para heredar la configuración de la NIC que ha fallado. No tiene que crear nuevas configuraciones antes de poder agregar una nueva interfaz al grupo IPMP. Después de asignar el nombre de enlace de la NIC que ha fallado a la nueva NIC, la nueva NIC se configura con los mismos valores de la interfaz que ha fallado. El daemon de múltiples rutas implementa la interfaz según la configuración IPMP de interfaces activas y en espera.

Por lo tanto, para optimizar la configuración de red y facilitar la administración IPMP, debe emplear nombres de enlace flexibles para sus interfaces asignándoles nombres genéricos. En la siguiente sección “[Cómo funciona IPMP](#)” en la [página 270](#), todos los ejemplos utilizan nombres

de enlace flexibles para el grupo IPMP y sus interfaces subyacentes. Para obtener más información sobre los procesos que participan en los reemplazos de NIC en un entorno de red que utiliza nombres de enlace personalizados, consulte [“IPMP y reconfiguración dinámica” en la página 284](#). Para obtener una descripción general de la pila de red y el uso de nombres de enlace personalizados, consulte [“La pila de red en Oracle Solaris” en la página 22](#).

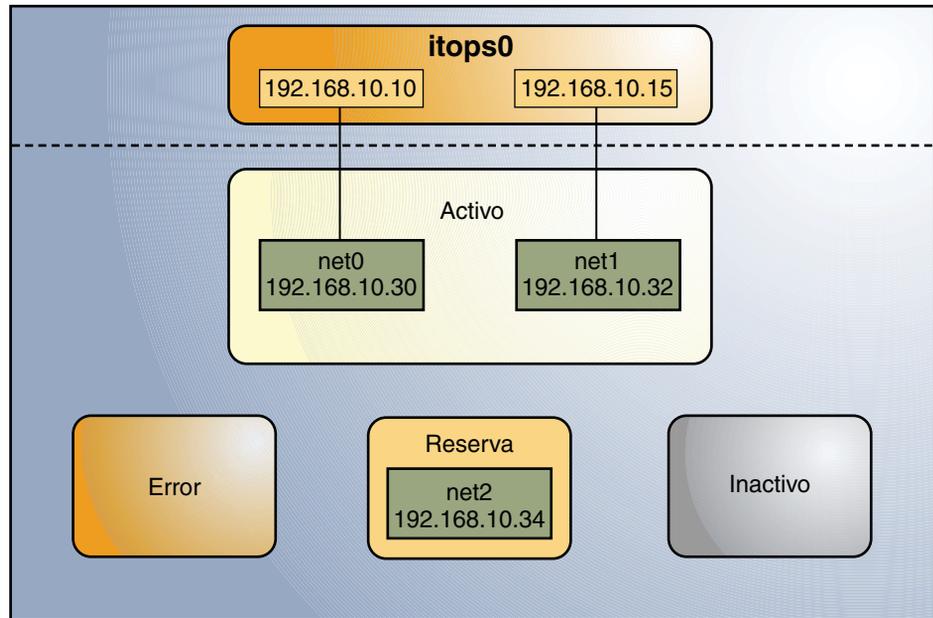
Cómo funciona IPMP

IPMP mantiene la disponibilidad de la red intentando conservar el número original de interfaces activas y en espera cuando el grupo se creó.

La detección de fallos IPMP puede estar basada en enlaces, basada en sondeos o ambas para determinar la disponibilidad de una interfaz IP subyacente específica del grupo. Si IPMP determina que una interfaz subyacente ha fallado, esa interfaz se marca como con fallos y ya no es utilizable. La dirección IP de datos asociada con la interfaz con fallos se redistribuye a otra interfaz en funcionamiento del grupo. Si está disponible, una interfaz en espera también se implementa para mantener el número original de interfaces activas.

Considere un grupo IPMP de tres interfaces `itops0` con una configuración activa/en espera como se ilustra en la [Figura 14–1](#).

FIGURA 14-1 Configuración activa/en espera IPMP



El grupo `itops0` se configura del siguiente modo:

- Dos direcciones de datos se asignan al grupo: `192.168.10.10` y `192.168.10.15`.
- Dos interfaces subyacentes se configuran como interfaces activas y se asignan nombres de enlace flexibles: `net0` y `net1`.
- El grupo posee una sola interfaz en espera, también con un nombre de enlace flexible: `net2`.
- La detección de fallos basada en sondeos se utiliza y, por consiguiente, las interfaces activas y en espera se configuran con direcciones de prueba, de la siguiente manera:
 - `net0`: `192.168.10.30`
 - `net1`: `192.168.10.32`
 - `net2`: `192.168.10.34`

Nota – Las áreas `Active`, `Offline`, `Reserve` y `Failed` en las figuras indican sólo el estado de interfaces subyacentes y no ubicaciones físicas. Ningún movimiento físico de interfaces o direcciones ni transferencia de interfaces IP se produce en esta implementación de IPMP. Las áreas sirven solamente para mostrar cómo una interfaz subyacente cambia de estado como resultado de un fallo o reparación.

Puede utilizar el comando `ipmpstat` con diferentes opciones para mostrar tipos determinados de información sobre grupos IPMP existentes. Para ver ejemplos adicionales, consulte [“Supervisión de información de IPMP” en la página 315](#).

La configuración de IPMP en la [Figura 14–1](#) se puede mostrar mediante el siguiente comando `ipmpstat`:

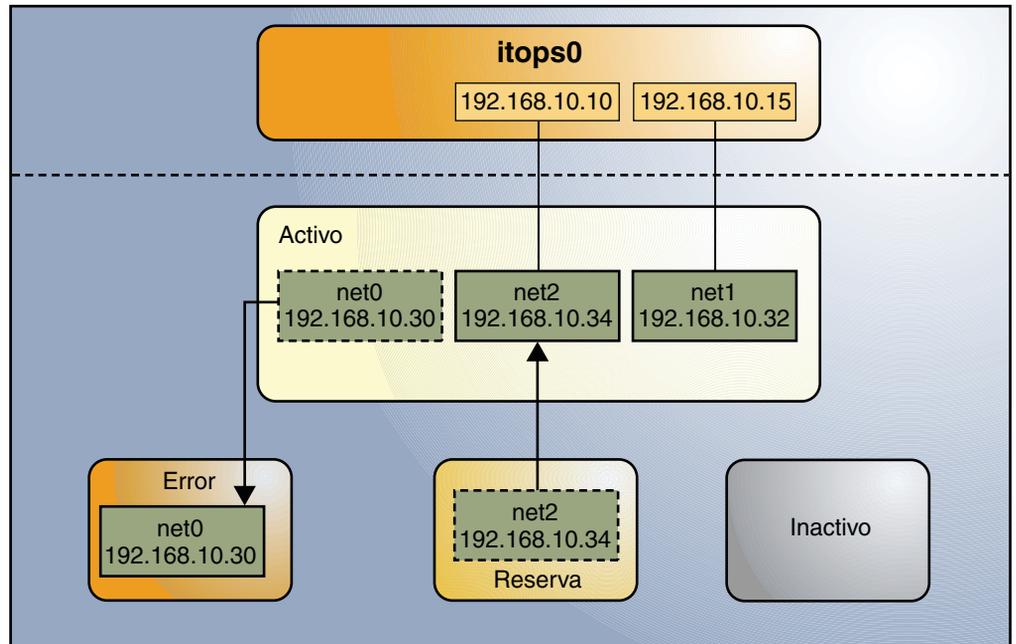
```
# ipmpstat -g
GROUP      GROUPNAME    STATE      FDT          INTERFACES
itops0     itops0       ok         10.00s       net1 net0 (net2)
```

Para mostrar información sobre las interfaces subyacentes del grupo, debe escribir lo siguiente:

```
# ipmpstat -i
INTERFACE  ACTIVE      GROUP      FLAGS        LINK        PROBE       STATE
net0       yes         itops0     - - - - -    up          ok          ok
net1       yes         itops0     - - mb - - - up          ok          ok
net2       no          itops0     is - - - - - up          ok          ok
```

IPMP mantiene la disponibilidad de la red administrando las interfaces subyacentes para mantener el número original de interfaces activas. Por lo tanto, si `net0` falla, entonces `net2` se implementa para asegurarse de que el grupo siga teniendo dos interfaces activas. La activación de `net2` se muestra en la [Figura 14–2](#).

FIGURA 14-2 Fallo de la interfaz en IPMP



Nota – La asignación uno a uno de direcciones de datos a interfaces activas en la [Figura 14-2](#) sólo sirve para simplificar la ilustración. El módulo de núcleo IP puede asignar direcciones de datos aleatoriamente sin que sea necesario adherirse a una relación uno a uno entre direcciones de datos e interfaces.

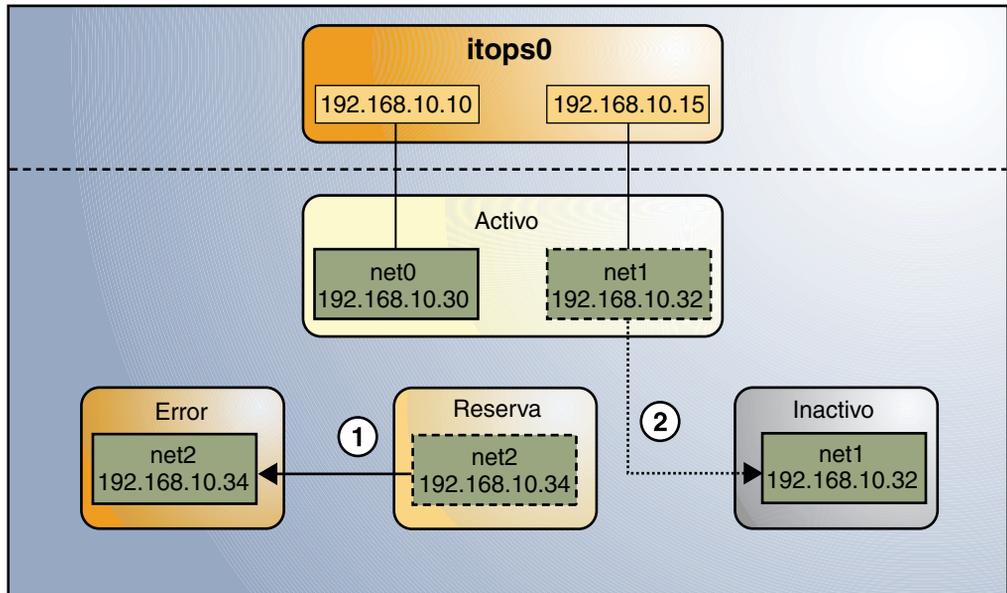
La utilidad `ipmpstat` muestra la información en la [Figura 14-2](#) de la siguiente manera:

```
# ipmpstat -i
INTERFACE  ACTIVE   GROUP   FLAGS   LINK    PROBE   STATE
net0       no      itops0  -s-----  up      failed  failed
net1       yes     itops0  --mb---  up      ok      ok
net2       yes     itops0  -s-----  up      ok      ok
```

Una vez que `net0` se ha reparado, vuelve a su estado como una interfaz activa. A su vez, `net2` vuelve a su estado en espera original.

Un escenario de fallo diferente se muestra en la [Figura 14-3](#), cuando la interfaz en espera `net` falla (1) y, posteriormente, una interfaz activa `net1` se cambia a sin conexión por el administrador (2). El resultado es que el grupo IPMP se deja con una única interfaz en funcionamiento, `net0`.

FIGURA 14-3 Fallo de interfaz en espera en IPMP

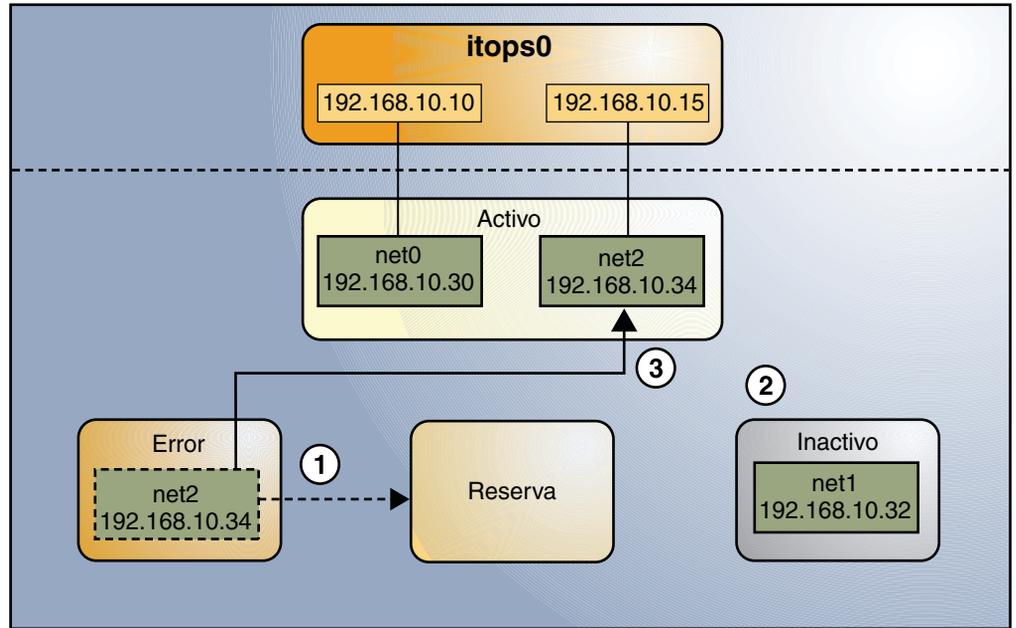


La utilidad `ipmpstat` mostrará la información ilustrada por la [Figura 14-3](#) de la siguiente manera:

```
# ipmpstat -i
INTERFACE  ACTIVE  GROUP  FLAGS  LINK  PROBE  STATE
net0       yes    itops0  -----  up    ok      ok
net1       no     itops0  --mb-d-  up    ok      offline
net2       no     itops0  is-----  up    failed  failed
```

Para este fallo en particular, la recuperación después de que una interfaz se ha reparado se comporta de manera diferente. La restauración depende del número original de interfaces activas del grupo IPMP en comparación con la configuración después de la reparación. El proceso de recuperación se representa de manera gráfica en la [Figura 14-4](#).

FIGURA 14-4 Proceso de recuperación de IPMP



En la [Figura 14-4](#), cuando se repara net2, vuelve a su estado original como una interfaz en espera (1). Sin embargo, el grupo IPMP no refleja el número original de dos interfaces activas, ya que net1 sigue estando sin conexión (2). Por lo tanto, IPMP implementa net2 como una interfaz activa en su lugar (3).

La utilidad `ipmpstat` mostrará el escenario de IPMP posterior a la reparación de la siguiente manera:

```
# ipmpstat -i
INTERFACE  ACTIVE  GROUP   FLAGS   LINK    PROBE   STATE
net0       yes    itops0  - - - - -  up      ok      ok
net1       no     itops0  - - m b - d -  up      ok      offline
net2       yes    itops0  - s - - - -  up      ok      ok
```

Una secuencia de restauración similar se produce si el fallo implica una interfaz activa que también está configurada en modo `FAILBACK=no`, donde una interfaz activa con fallos no se revierte inmediatamente al estado activo después de la reparación. Supongamos que net0 en la [Figura 14-2](#) se configura en modo `FAILBACK=no`. En ese modo, si net0 se repara cambia a un estado reservado como una interfaz en espera, incluso si originalmente era una interfaz activa. La interfaz net2 seguirá activa para mantener el número original de dos interfaces activas del grupo IPMP. La utilidad `ipmpstat` mostrará la información de recuperación como se indica a continuación:

```
# ipmpstat -i
INTERFACE  ACTIVE    GROUP    FLAGS    LINK     PROBE    STATE
net0       no       itops0   i----- up       ok       ok
net1       yes      itops0   --mb--- up       ok       ok
net2       yes      itops0   -s----- up       ok       ok
```

Para obtener más información sobre este tipo de configuración, consulte [“El modo FAILBACK=no” en la página 283](#).

Componentes de IPMP en Oracle Solaris

IPMP de Oracle Solaris implica el siguiente software:

El *daemon de múltiples rutas* `in.mpathd` detecta fallos de interfaces y reparaciones. El daemon realiza una detección de fallos basada en enlaces y una detección de fallos basada en sondeos si las direcciones de prueba se configuran para las interfaces subyacentes. Según el tipo de método de detección de fallos que se emplea, el daemon establece los indicadores adecuados en la interfaz o los borra para indicar si la interfaz ha fallado o se ha reparado. Como opción, el daemon también se puede configurar para supervisar la disponibilidad de todas las interfaces, incluidas aquellas que no se han configurado para que pertenezcan a un grupo IPMP. Para obtener una descripción de detección de fallos, consulte [“Detección de fallos y reparaciones en IPMP” en la página 279](#).

El daemon `in.mpathd` controla también la designación de interfaces activas del grupo IPMP. El daemon intenta mantener el mismo número de interfaces activas que se configuró originalmente cuando se creó el grupo IPMP. Por lo tanto, `in.mpathd` activa o desactiva interfaces subyacentes según sea necesario para ser consistente con la política configurada del administrador. Para obtener más información sobre la manera en que el daemon `in.mpathd` gestiona la activación de interfaces subyacentes, consulte [“Cómo funciona IPMP” en la página 270](#). Para obtener más información sobre el daemon, consulte la página del comando `man in.mpathd(1M)`.

El *módulo de núcleo IP* gestiona la expansión de carga saliente mediante la distribución del conjunto de direcciones de datos IP disponibles en el grupo por medio del conjunto de interfaces IP subyacentes disponibles en el grupo. El módulo también realiza una selección de direcciones de origen para gestionar la expansión de carga entrante. Ambos roles del módulo IP mejoran el rendimiento de tráfico de red.

El *archivo de configuración IPMP* `/etc/default/mpathd` se utiliza para configurar el comportamiento del daemon. Por ejemplo, puede especificar cómo el daemon realiza la detección de fallos basada en sondeos estableciendo la duración para sondear un destino a fin de detectar fallos o qué interfaces sondear. También puede especificar cuál es el estado que debe tener una interfaz con fallos posterior a su reparación. También puede establecer los parámetros de este archivo para especificar si el daemon debe supervisar todas las interfaces IP del sistema, no sólo las que están configuradas para pertenecer a los grupos de IPMP. Para obtener más información sobre procedimientos para modificar el archivo de configuración, consulte [“Cómo configurar el comportamiento del daemon IPMP” en la página 312](#).

La *utilidad ipmpstat* proporciona diferentes tipos de información sobre el estado de IPMP en general. La herramienta también muestra otra información específica sobre las interfaces IP subyacentes para cada grupo, así como datos y direcciones de prueba que se han configurado para el grupo. Para obtener más información sobre el uso de este comando, consulte “Supervisión de información de IPMP” en la [página 315](#) y la página del comando `man ipmpstat(1M)`.

Tipos de configuraciones de interfaces IPMP

Una configuración de IPMP típica consta de dos o más interfaces físicas en el mismo sistema que está conectado a la misma LAN. Estas interfaces pueden pertenecer a un grupo IPMP en cualquiera de las siguientes configuraciones:

- Configuración activa/activa: un grupo IPMP en el que todas las interfaces subyacentes están activas. Una *interfaz activa* es una interfaz IP que está actualmente disponible para ser utilizada por el grupo IPMP. De manera predeterminada, una interfaz subyacente se vuelve activa cuando configura la interfaz para que sea parte de un grupo IPMP. Para obtener información adicional sobre interfaces activas y otros términos de IPMP, consulte también “Terminología y conceptos de IPMP” en la [página 286](#).
- Configuración activa/en espera: un grupo IPMP en el que al menos una interfaz está configurada administrativamente como una reserva. La interfaz de reserva se denomina *interfaz en espera*. Aunque está inactiva, la interfaz IP en espera es supervisada por el daemon de múltiples rutas para realizar un seguimiento de la disponibilidad de la interfaz, en función de cómo la interfaz está configurada. Si la notificación de fallos por enlaces es admitida por la interfaz, se utiliza la detección de fallos basada en enlaces. Si la interfaz está configurada con una dirección de prueba, también se utiliza la detección de fallos basada en sondeos. Si una interfaz activa falla, la interfaz en espera se implementa automáticamente según sea necesario. Puede configurar tantas interfaces en espera como desee para un grupo IPMP.

Una única interfaz también se puede configurar en su propio grupo IPMP. El grupo IPMP de interfaz única tiene el mismo comportamiento que un grupo IPMP con múltiples interfaces. Sin embargo, esta configuración de IPMP no proporciona alta disponibilidad para el tráfico de la red. Si la interfaz subyacente falla, el sistema pierde toda capacidad de enviar o recibir tráfico. La finalidad de configurar un grupo de IPMP de una sola interfaz es la de supervisar la disponibilidad de la interfaz utilizando detección de fallos. Mediante la configuración de una dirección de prueba en la interfaz, puede definir el daemon para realizar un seguimiento de la interfaz mediante la detección de fallos basada en sondeos. Normalmente, una configuración de grupo IPMP de una sola interfaz se utiliza junto con otras tecnologías que tienen capacidades más amplias de conmutación por error, tales como el software Oracle Solaris Cluster. El sistema puede continuar para supervisar el estado de la interfaz subyacente. Pero el software Oracle Solaris Cluster proporciona funcionalidades para garantizar la disponibilidad de la red cuando se produce un fallo. Para obtener más información sobre el software Oracle Solaris Cluster, consulte [Sun Cluster Overview for Solaris OS](#).

Un grupo IPMP sin interfaces subyacentes también puede existir, como un grupo cuyas interfaces subyacentes se han eliminado. El grupo IPMP no se destruye, pero el grupo no se puede utilizar para enviar ni recibir tráfico. Cuando las interfaces IP subyacentes se ponen en línea para el grupo, las direcciones de datos de la interfaz IPMP se asignan a estas interfaces y el sistema reanuda el alojamiento de tráfico de la red.

Direcciones IPMP

Puede configurar la detección de fallos IPMP en redes IPv4 y de pila doble, y redes IPv4 e IPv6. Las interfaces que se configuran con IPMP admiten dos tipos de direcciones:

- *Las direcciones de datos* son direcciones IPv4 e IPv6 convencionales que se asignan a una interfaz IP dinámicamente al momento del inicio mediante el servidor DHCP, o de manera manual mediante el comando `ipadm`. Las direcciones de datos se asignan a la interfaz IPMP. El tráfico de paquetes IPv4 estándar y el tráfico de paquetes IPv6 (si es aplicable), se consideran *tráfico de datos*. El flujo de tráfico de datos utiliza las direcciones de datos que se encuentran alojadas en la interfaz IPMP y fluyen mediante las interfaces activas de ese grupo.
- *Las direcciones de prueba* son direcciones específicas de IPMP que utiliza el daemon `in.mpathd` para realizar la detección de fallos basada en sondeos y la reparación. Las direcciones de prueba también se pueden asignar dinámicamente mediante el servidor DHCP o de manera manual mediante el comando `ipadm`. Mientras que las direcciones de datos se asignan a la interfaz IPMP, sólo las direcciones de prueba se asignan a interfaces subyacentes del grupo. Para una interfaz subyacente de una red de doble pila, puede configurar una dirección de prueba IPv4, una dirección de prueba IPv6 o ambas. Cuando una interfaz subyacente falla, la dirección de prueba de la interfaz continúa siendo utilizada por el daemon `in.mpathd` para la detección de fallos basada en sondeos para comprobar la reparación subsecuente de la interfaz.

Nota – Sólo es necesario configurar direcciones de prueba si se va a utilizar específicamente la detección de fallos basada en sondeos. De lo contrario, puede habilitar el sondeo transitivo para detectar fallos sin utilizar direcciones de prueba. Para obtener más información sobre detección de fallos basada en sondeos con o sin el uso de direcciones de prueba, consulte [“Detección de fallos basada en sondeos” en la página 280](#).

En implementaciones de IPMP anteriores, las direcciones de prueba debían estar marcadas como DEPRECATED para evitar que se utilizaran aplicaciones especialmente durante fallos de la interfaz. En la implementación actual, las direcciones de prueba residen en las interfaces subyacentes. Por lo tanto, estas direcciones ya no pueden ser utilizadas accidentalmente por aplicaciones que son independientes de IPMP. Sin embargo, para asegurarse de que estas direcciones no se tendrán en cuenta como un posible origen para los paquetes de datos, el sistema marca de forma automática las direcciones con el indicador NOFAILOVER y también con DEPRECATED.

Direcciones de prueba IPv4

En general, puede utilizar cualquier dirección IPv4 en su subred como una dirección de prueba. Las direcciones de prueba IPv4 no necesitan ser enrutables. Dado que las direcciones IPv4 son un recurso limitado para muchos sitios, puede utilizar direcciones privadas RFC 1918 no enrutables como direcciones de prueba. Observe que el daemon `in.mpathd` intercambia sólo sondeos ICMP con otros hosts que se encuentran en la misma subred que la dirección de prueba. Si utiliza las direcciones de prueba RFC 1918, debe configurar otros sistemas, preferiblemente enrutadores, en la red con direcciones en la subred RFC 1918 pertinente. De este modo, el daemon `in.mpathd` podrá intercambiar correctamente los sondeos con los sistemas de destino. Para obtener más información acerca de direcciones privadas RFC 1918, consulte [RFC 1918, Address Allocation for Private Internets \(http://www.ietf.org/rfc/rfc1918.txt?number=1918\)](http://www.ietf.org/rfc/rfc1918.txt?number=1918).

Direcciones de prueba IPv6

La única dirección de prueba IPv6 válida es la dirección local de enlace de una interfaz física. No necesita una dirección IPv6 aparte para que cumpla la función de dirección de prueba IPMP. La dirección local de enlace IPv6 se basa en la dirección de control de acceso de medios (MAC) de la interfaz. Las direcciones locales de enlace se configuran automáticamente cuando la interfaz se habilita para IPv6 durante el inicio o cuando la interfaz se configura manualmente mediante `ipadm`.

Para obtener más información sobre las direcciones locales de enlace, consulte “[Link-Local Unicast Address](#)” de *System Administration Guide: IP Services*.

Cuando un grupo IPMP tiene conectadas direcciones tanto IPv4 como IPv6 en todas las interfaces del grupo, no es necesario configurar direcciones de IPv4 aparte. El daemon `in.mpathd` puede utilizar las direcciones locales de enlace IPv6 como direcciones de prueba.

Detección de fallos y reparaciones en IPMP

Para garantizar la disponibilidad continua de la red para enviar o recibir tráfico, IPMP realiza una detección de fallos en las interfaces IP subyacentes del grupo IPMP. Las interfaces con fallos siguen sin poder utilizarse hasta que se hayan reparado. Las interfaces activas restantes siguen funcionando mientras que las interfaces en espera se implementan según sea necesario.

Tipos de detección de fallos en IPMP

El daemon `in.mpathd` controla los siguientes tipos de detección de fallos:

- Detección de fallos basada en sondeos, de dos tipos:
 - No se configuran direcciones de prueba (sondeo transitivo).

- Se configuran las direcciones de prueba.
- Detección de fallos basada en enlaces, si la admite el controlador de la NIC.

Detección de fallos basada en sondeos

La detección de fallos basada en sondeos consiste en utilizar los sondeos ICMP para comprobar si una interfaz ha fallado. La implementación de este método de detección de fallos depende de si las direcciones de prueba se utilizan o no.

Detección de fallos basada en sondeos sin utilizar direcciones de prueba

Sin direcciones de prueba, este método se implementa con dos tipos de sondeos:

- Sondeos ICMP

Las interfaces activas en el grupo envían los sondeos ICMP para sondear destinos definidos en la tabla de enrutamiento. Una interfaz *activa* es la interfaz subyacente que puede recibir los paquetes IP entrantes dirigidos a la dirección de capa de enlace (L2) de la interfaz. El sondeo ICMP utiliza la dirección de datos como dirección de origen del sondeo. Si el sondeo ICMP alcanza su destino y obtiene una respuesta del mismo, la interfaz activa está en funcionamiento.

- Sondeos transitivos

Las interfaces alternativas en el grupo envían sondeos transitivos para sondear la interfaz activa. Una interfaz alternativa es una interfaz que no recibe activamente paquetes IP entrantes.

Por ejemplo, considere un grupo IPMP que consta de cuatro interfaces subyacentes. El grupo se configura con una dirección de datos pero no direcciones de prueba. En esta configuración, los paquetes salientes pueden utilizar todas las interfaces subyacentes. Sin embargo, los paquetes entrantes sólo se pueden recibir mediante la interfaz a la que la dirección de datos está vinculada. Las tres interfaces subyacentes restantes que no pueden recibir paquetes entrantes son las interfaces *alternativas*.

Si una interfaz alternativa puede enviar correctamente un sondeo para una interfaz activa y recibir una respuesta, la interfaz activa está en funcionamiento y, por ende, también lo está la interfaz alternativa que ha enviado el sondeo.

Nota – Debe habilitar el sondeo transitivo para utilizar este método de detección de fallos que no requiere direcciones de prueba.

Detección de fallos basada en sondeos utilizando direcciones de prueba

Este método de detección de fallos implica enviar y recibir mensajes de sondeo de ICMP que utilizan direcciones de prueba. Estos mensajes, también denominados *tráfico de sondeo* o tráfico de prueba, pasan por la interfaz y se dirigen a uno o más sistemas de destino de la misma red

local. El daemon sondea todos los destinos por separado mediante todas las interfaces que se han configurado para la detección de fallos basada en sondeos. Si no hay ninguna respuesta a cinco sondeos consecutivos en una interfaz específica, `in.mpathd` considera que la interfaz ha fallado. La velocidad de sondeo depende del *tiempo de detección de fallos* (FDT). El valor predeterminado del tiempo de detección de fallos es de 10 segundos. Sin embargo, puede ajustar el tiempo de detección de fallos en el archivo de configuración de IPMP. Para obtener instrucciones, vaya a [“Cómo configurar el comportamiento del daemon IPMP” en la página 312](#). Para optimizar la detección de fallos basada en sondeos, debe establecer varios sistemas de destino para recibir los sondeos del daemon de múltiples rutas. Teniendo múltiples sistemas de destino, puede determinar mejor la naturaleza de un fallo informado. Por ejemplo, la ausencia de una respuesta del único sistema de destino definido puede indicar un fallo en el sistema de destino o en una de las interfaces del grupo IPMP. Por el contrario, si sólo un sistema entre varios sistemas de destino no responde a un sondeo, es probable que el fallo se encuentre en el sistema de destino en lugar de en el grupo IPMP en sí.

El daemon `in.mpathd` determina qué sistemas de destino se deben sondear dinámicamente. En primer lugar, el daemon busca la tabla de enrutamiento para sistemas de destino en la misma subred de las direcciones de prueba que están asociadas a las interfaces del grupo IPMP. Si estos destinos se encuentran, el daemon los utiliza como destinos para el sondeo. Si no se encuentran sistemas de destino en la misma subred, `in.mpathd` envía paquetes de multidifusión para sondear hosts vecinos en el enlace. Un paquete multidifusión se envía a la dirección de multidifusión de todos los hosts, `224.0.0.1` en IPv4 y `ff02::1` en IPv6, para determinar qué hosts se utilizarán como sistemas de destino. Los primeros hosts que responden a los paquetes de eco se eligen como destinos para los sondeos. Si `in.mpathd` no encuentra enrutadores ni hosts que respondan a sondeos de multidifusión, los paquetes de eco ICMP `in.mpathd` no pueden detectar fallos basados en sondeos. En este caso, la utilidad `ipmstat -i` informará el estado de sondeo como `unknown`.

Puede utilizar las rutas `host` para configurar explícitamente una lista de sistemas de destino para utilizar con el comando `in.mpathd`. Para obtener instrucciones, consulte [“Configuración para la detección de fallos basada en sondeos” en la página 309](#).

Fallo de grupo

Un *fallo de grupo* tiene lugar cuando todas las interfaces de un grupo IPMP fallan al mismo tiempo. En este caso, ninguna interfaz es utilizable. Además, cuando todos los sistemas de destino fallan al mismo tiempo y la detección de fallos basada en sondeos está habilitada, el daemon `in.mpathd` vacía todos sus sistemas de destino y sondeos actuales para los nuevos sistemas de destino.

En un grupo IPMP que no tiene direcciones de prueba, una sola interfaz que puede sondear la interfaz activa se designará como encargado de los sondeos. Esta interfaz designada tendrá el indicador `FAILED` y `PROBER`. La dirección de datos está vinculada a esta interfaz que permite a la interfaz continuar con el sondeo del destino para detectar la recuperación.

Detección de fallos basada en enlaces

La detección de fallos basada en enlaces siempre está habilitada, cuando la interfaz admite este tipo de detección de fallos.

Para determinar si la interfaz de otro proveedor admite la detección de fallos basada en enlaces, utilice el comando `ipmpstat -i`. Si el resultado de una interfaz dada incluye un estado `unknown` para su columna `LINK`, dicha interfaz no admite detección de fallos basada en enlaces. Consulte la documentación del fabricante para obtener más información específica sobre el dispositivo.

Estos controladores de red que admiten la detección de fallos basada en enlaces supervisan el estado de enlace de la interfaz y notifican al subsistema de red si dicho estado cambia. Cuando se notifica un cambio, el subsistema de red establece o borra el indicador `RUNNING` para dicha interfaz, según sea preciso. Si el daemon `in.mpathd` detecta que el indicador `RUNNING` de la interfaz se ha borrado, el daemon hace fallar inmediatamente a la interfaz.

Detección de fallos y función del grupo anónimo

IPMP admite la detección de fallos en un grupo anónimo. De manera predeterminada, IPMP supervisa el estado sólo de interfaces que pertenecen a grupos IPMP. Sin embargo, el daemon IPMP se puede configurar también para realizar el seguimiento del estado de las interfaces que no pertenecen a ningún grupo IPMP. Por lo tanto, estas interfaces se consideran como parte de un "grupo anónimo". Cuando emite el comando `ipmpstat -g`, el grupo anónimo se muestra como guión doble (`--`). En grupos anónimos, las interfaces tendrían sus direcciones de datos funcionando también como direcciones de prueba. Debido a que estas interfaces no pertenecen a un grupo IPMP denominado, estas direcciones son visibles a las aplicaciones. Para habilitar el seguimiento de interfaces que no forman parte de un grupo IPMP, consulte [“Cómo configurar el comportamiento del daemon IPMP” en la página 312](#).

Detección de reparaciones de interfaces físicas

El *tiempo de detección de reparaciones* es el doble del tiempo de detección de fallos. El tiempo predeterminado para la detección de fallos es de 10 segundos. En consecuencia, el tiempo predeterminado de detección de reparaciones es de 20 segundos. Después de que una interfaz con fallos se ha marcado con el indicador `RUNNING` de nuevo y el método de detección de fallos ha detectado la reparación, `in.mpathd` borra el indicador `FAILED` de la interfaz. La interfaz reparada se vuelve a implementar en función del número de interfaces activas que el administrador ha definido originalmente.

Cuando una interfaz subyacente falla y se utiliza la detección de fallos basada en sondeos, el daemon `in.mpathd` sigue sondeando, ya sea mediante un encargado de sondeos cuando no se configuró ninguna dirección de prueba o mediante direcciones de prueba de la interfaz. Durante una reparación de interfaz, la restauración continúa en función de la configuración original de la interfaz con fallos:

- La interfaz con fallos era originalmente una interfaz activa: la interfaz reparada vuelve a su estado activo original. La interfaz en espera que funcionaba como un reemplazo durante el fallo se vuelve a cambiar al estado en espera si hay suficientes interfaces que están activas para el grupo según el administrador del sistema.

Nota – Una excepción a este paso son los casos en que la interfaz activa reparada también está configurada con el modo FAILBACK=no. Para obtener más información, consulte [“El modo FAILBACK=no” en la página 283](#)

- La interfaz con fallos era originalmente una interfaz en espera: la interfaz reparada vuelve a su estado en espera original, siempre que el grupo IPMP refleje el número original de interfaces activas. De lo contrario, la interfaz en espera se cambia para convertirse en una interfaz activa.

Para ver una presentación gráfica de cómo IPMP se comporta durante el fallo y la reparación de la interfaz, consulte [“Cómo funciona IPMP” en la página 270](#).

El modo FAILBACK=no

De manera predeterminada, las interfaces activas que han presentado fallos y se han reparado vuelven automáticamente a convertirse en interfaces activas en el grupo. Este comportamiento es controlado por la configuración del parámetro FAILBACK en el archivo de configuración del daemon. Sin embargo, es posible que incluso la interrupción insignificante que se genera a medida que las direcciones de datos son reasignadas a interfaces reparadas no sea aceptable para algunos administradores. Es posible que los administradores prefieran permitir que una interfaz en espera activada continúe como una interfaz activa. IPMP permite a los administradores reemplazar el comportamiento predeterminado para evitar que una interfaz se active automáticamente después de su reparación. Estas interfaces deben estar configuradas en el modo FAILBACK=no. Para conocer procedimientos relacionados, consulte [“Cómo configurar el comportamiento del daemon IPMP” en la página 312](#).

Cuando una interfaz activa en el modo FAILBACK=no falla y subsecuentemente se repara, el daemon IPMP restaura la configuración IPMP de la siguiente manera:

- El daemon conserva el estado INACTIVE de la interfaz, siempre que el grupo IPMP refleje la configuración original de interfaces activas.
- Si la configuración IPMP en el momento de la reparación no refleja la configuración original del grupo de interfaces activas, la interfaz reparada se vuelve a desplegar como una interfaz activa, a pesar del estado FAILBACK=no.

Nota – El modo FAILBACK=NO está configurado para todo el grupo IPMP. No es un parámetro ajustable por interfaz.

IPMP y reconfiguración dinámica

La función de reconfiguración dinámica (DR) permite volver a configurar el hardware del sistema, como las interfaces, mientras el sistema está en ejecución. DR sólo se puede utilizar en los sistemas que admiten esta función.

Normalmente se utiliza el comando `cfgadm` para llevar a cabo las operaciones de DR. Sin embargo, algunas plataformas proporcionan otros métodos. Asegúrese de consultar la documentación de la plataforma para obtener detalles para realizar una DR. Para los sistemas que utilizan Oracle Solaris, puede buscar documentación específica sobre DR en los recursos que se muestran en la [Tabla 14-1](#). Información actual sobre DR también está disponible en <http://www.oracle.com/technetwork/indexes/documentation/index.html> y se puede obtener si busca el tema "reconfiguración dinámica".

TABLA 14-1 Recursos de documentación para la reconfiguración dinámica

Descripción	Para obtener información
Información detallada sobre el comando <code>cfgadm</code>	Página del comando <code>man cfgadm(1M)</code>
Información específica sobre DR en el entorno de Oracle Solaris Cluster	<i>Guía de administración del sistema de Oracle Solaris Cluster</i>
Información específica sobre DR en servidores Sun de Oracle	Consulte la documentación suministrada con el servidor específico
Información introductoria sobre DR y el comando <code>cfgadm</code>	Capítulo 6, "Configuración dinámica de dispositivos (tareas)" de <i>Administración de Oracle Solaris: dispositivos y sistemas de archivos</i>
Tareas para administrar grupos IPMP en un sistema que admite DR	"Recuperación de configuración de IPMP con reconfiguración dinámica" en la página 313

Las secciones siguientes explican cómo DR interopera con IPMP.

En un sistema que admite la DR de NIC, IPMP se puede utilizar para mantener la conectividad y evitar la interrupción de las conexiones existentes. IPMP está integrado en la estructura del gestor de coordinación de reconfiguración (RCM). Por lo tanto, puede conectar, desconectar o volver a conectar de manera segura las NIC y RCM gestiona la reconfiguración dinámica de los componentes del sistema.

Conexión de nuevas NIC

Con compatibilidad de DR, puede conectar y agregar nuevas interfaces a grupos IPMP existentes. Si es preciso, puede configurar las interfaces que acaba de agregar en su propio grupo IPMP. Para obtener más información sobre procedimientos para configurar grupos IPMP, consulte "Configuración de grupos IPMP" en la [página 298](#). Después de que estas interfaces se

han configurado, están inmediatamente disponibles para que IPMP las utilice. Sin embargo, para beneficiarse de las ventajas de utilizar nombres de enlace personalizados, debe asignar nombres de enlace genéricos para reemplazar los nombres de enlace basados en hardware de la interfaz. Luego, debe crear los archivos de configuración correspondientes mediante el nombre genérico que acaba de asignar. Para obtener más información sobre procedimientos en los que se puede configurar una única interfaz mediante nombres de enlace personalizados, consulte [“Cómo configurar una interfaz IP” en la página 181](#). Después de asignar un nombre de enlace genérico a la interfaz, asegúrese de referirse siempre al nombre genérico al realizar cualquier configuración adicional en la interfaz como el uso de la interfaz para IPMP.

Desconexión de NIC

Todas las solicitudes para desconectar los componentes del sistema que contengan NIC se comprueban antes para garantizar el mantenimiento de la conectividad. Por ejemplo, de modo predeterminado no puede desconectar una NIC que no se encuentre en un grupo IPMP. Tampoco puede desconectar una NIC que contenga las únicas interfaces en funcionamiento de un grupo IPMP. Sin embargo, si debe eliminar el componente del sistema, puede modificar este comportamiento con la opción `-f` de `cfgadm`, tal como se explica en la página del comando `man cfgadm(1M)`.

Si las comprobaciones son correctas, el daemon establece el indicador `OFFLINE` para la interfaz. Todas las direcciones de prueba de las interfaces se desconfiguran. A continuación, la NIC se desconecta del sistema. Si falla alguno de estos pasos, o falla la DR de otro hardware del mismo componente del sistema, se restablece el estado original de la configuración anterior. Se mostrará un mensaje de estado sobre este evento. De lo contrario, la solicitud de desconexión se completará correctamente. Ya podrá eliminar el componente del sistema. Las conexiones existentes no se interrumpen.

Reemplazo de NIC

Cuando una interfaz subyacente de un grupo IPMP falla, una solución típica podría ser reemplazar la interfaz con fallos conectando una nueva NIC. RCM registra la información de configuración asociada con cualquier NIC que se desconecta de un sistema en ejecución. Si reemplaza una NIC con fallos con una NIC *idéntica*, RCM configura automáticamente la interfaz según las configuraciones persistentes que previamente habían sido definidas mediante el comando `ipadm`.

Por ejemplo, supongamos que reemplaza una interfaz `bge0` con fallos con otra interfaz `bge0`. Los valores de configuración de `bge0` con fallos que se definieron mediante el comando `ipadm` son los valores de configuración persistentes. Tras conectar la NIC `bge` de reemplazo, RCM conecta y, a continuación, configura la interfaz `bge0` según estos valores de configuración persistentes. Por lo tanto la interfaz se configura correctamente con la dirección de prueba y se agrega al grupo IPMP.

Puede reemplazar una NIC con fallos con otra NIC, siempre que ambas sean del mismo tipo, como Ethernet. En este caso, RCM sondea la nueva interfaz después de que se ha conectado. Si no ha utilizado nombres de enlace personalizados cuando configuró las interfaces por primera vez, tendrá que configurar la nueva NIC antes de poder agregar la interfaz al grupo IPMP.

Sin embargo, si ha utilizado nombres de enlace personalizados, los pasos de configuración adicionales son innecesarios. Si reasigna el nombre de enlace de la interfaz con fallos a la nueva interfaz, la nueva interfaz adquiere la configuración especificada en los valores de configuración persistentes de la interfaz eliminada. RCM configura la interfaz según esos valores. Para obtener más información sobre procedimientos para recuperar la configuración de IPMP mediante DR cuando una interfaz falla, consulte [“Recuperación de configuración de IPMP con reconfiguración dinámica”](#) en la página 313.

Terminología y conceptos de IPMP

En esta sección se presentan términos y conceptos que se utilizan en los capítulos de IPMP de este manual.

interfaz activa

Hace referencia a una interfaz subyacente que el sistema puede utilizar para enviar o recibir tráfico de datos. Una interfaz está activa si se cumplen las siguientes condiciones:

- Al menos una dirección IP está en la interfaz UP. Consulte la dirección UP.
- El indicador FAILED, INACTIVE u OFFLINE no está establecido en la interfaz.
- La interfaz no se ha marcado como si tuviera una dirección de hardware duplicada.

Comparar con una interfaz inutilizable, interfaz INACTIVE.

dirección de datos

Hace referencia a una dirección IP que puede utilizarse como dirección de origen o de destino para los datos. Las direcciones de datos forman parte de un grupo IPMP y se pueden usar para enviar y recibir tráfico en cualquier interfaz del grupo. Además, el conjunto de direcciones de datos de un grupo IPMP se puede utilizar continuamente siempre que funcione una interfaz en el grupo. En las implementaciones IPMP, las direcciones de datos se hospedaban en las interfaces subyacentes de un grupo IPMP. En la implementación actual, las direcciones de datos se encuentran hospedadas en la interfaz IPMP.

dirección DEPRECATED	Se refiere a una dirección IP que no puede ser utilizada como la dirección de origen para los datos. En general, las direcciones de prueba IPMP, que tienen el indicador NOFAILOVER, también se marcan automáticamente como DEPRECATED por el sistema. Ahora bien, cualquier dirección se puede marcar como DEPRECATED para impedir que pueda utilizarse como dirección de origen.
reconfiguración dinámica	Hace referencia a una función que permite volver a configurar un sistema aunque el sistema esté en ejecución, sin que se vean afectados en absoluto o en poca medida los procesos que están en curso. No todas las plataformas de Sun de Oracle admiten DR. Es posible que algunas plataformas sólo admitan DR de determinados tipos de hardware. En las plataformas que admiten DR de NIC, IPMP se puede utilizar para acceso de red ininterrumpido para el sistema durante DR. Para obtener más información sobre cómo IPMP admite DR, consulte “IPMP y reconfiguración dinámica” en la página 284.
creación de interfaz IPMP explícita	Se aplica sólo a la implementación de IPMP actual. El término se refiere al método de creación una interfaz IPMP mediante el comando <code>ipadm create-ipmp</code> . La creación de la interfaz IPMP explícita es el método preferido para crear grupos IPMP. Este método permite que el administrador establezca el nombre de la interfaz y el nombre de grupo IPMP.
modo FAILBACK=no	Comparar con la creación de interfaz IPMP implícita. Se refiere a una configuración de una interfaz subyacente que minimiza la revinculación de direcciones entrantes a interfaces evitando la redistribución durante la reparación de la interfaz. Específicamente, cuando se detecta una reparación de interfaz, se borra el indicador FAILED de la interfaz. Sin embargo, si el modo de la interfaz reparada es FAILBACK=no, entonces el indicador INACTIVE también se establece para evitar el uso de la interfaz, teniendo en cuenta de que también existe una segunda interfaz en funcionamiento. Si la segunda interfaz del

	<p>grupo IPMP falla, la interfaz <code>INACTIVE</code> es elegible para tomar su lugar. Aunque el concepto de recuperación tras los errores ya no se aplica en la implementación de IPMP actual, el nombre de este modo se mantiene para compatibilidad administrativa.</p>
interfaz <code>FAILED</code>	<p>Indica una interfaz que el daemon <code>in.mpathd</code> ha determinado como con mal funcionamiento. La determinación se consigue mediante cualquier detección de fallos, ya sea basada en enlaces o basada en sondeos. El indicador <code>FAILED</code> se establece en cualquier interfaz con fallos.</p>
detección de fallos	<p>Hace referencia al proceso en el que se detecta cuándo deja de funcionar una interfaz física o la ruta de una interfaz a un dispositivo de capa de Internet. Se implementan dos maneras de detección de fallos: detección basada en enlaces y detección basada en sondeos.</p>
creación de interfaz IPMP implícita	<p>Hace referencia al método de creación de una interfaz IPMP mediante el comando <code>ifconfig</code> para ubicar una interfaz subyacente en un grupo IPMP. La creación de interfaz IPMP implícita se admite para la compatibilidad con la implementación de IPMP en versiones anteriores de Oracle Solaris. Por lo tanto, este método no proporciona la posibilidad de configurar el nombre de la interfaz IPMP o el nombre del grupo IPMP. El comando <code>ipadm</code> no admite la creación de interfaz IPMP.</p>
interfaz <code>INACTIVE</code>	<p>Comparar con la creación de interfaz IPMP explícita.</p> <p>Hace referencia a una interfaz que está en funcionamiento, pero no se utiliza según la política de administración. El indicador <code>INACTIVE</code> se establece en cualquier interfaz <code>INACTIVE</code>.</p>
compatibilidad de grupo anónimo IPMP	<p>Comparar con interfaz activa, interfaz no utilizable.</p> <p>Indica una función IPMP en la que el daemon IPMP realiza el seguimiento del estado de todas las interfaces de red en el sistema, independientemente de si pertenecen a un grupo IPMP. Sin embargo, si las</p>

grupo IPMP	<p>interfaces en realidad no están en un grupo IPMP, las direcciones de estas interfaces no están disponibles en caso de fallo de la interfaz.</p>
interfaz de grupo IPMP nombre de grupo IPMP	<p>Hace referencia a un conjunto de interfaces de red que el sistema trata como intercambiables para mejorar la disponibilidad y el uso de la red. Cada grupo IPMP tiene un conjunto de direcciones de datos que el sistema pueden asociar a cualquier conjunto de interfaces activas en el grupo. El uso de este conjunto de direcciones de datos mantiene la disponibilidad de la red y mejora el uso de la red. El administrador puede seleccionar qué interfaces ubicar en un grupo IPMP. Sin embargo, todas las interfaces del mismo grupo deben compartir un conjunto común de propiedades, como estar conectadas al mismo enlace y configuradas con el mismo conjunto de protocolos (por ejemplo, IPv4 e IPv6).</p> <p>Consulte interfaz IPMP.</p> <p>Hace referencia al nombre de un grupo IPMP, que se puede asignar con el subcomando <code>ipadm set -i fprop</code>. Todas las interfaces subyacentes que tienen el mismo nombre de grupo IPMP se definen como parte del mismo grupo IPMP. En la implementación actual, a los nombres de grupo IPMP se les resta importancia en favor de nombres de interfaz IPMP. Se promueve que los administradores utilicen el mismo nombre para el grupo y las interfaces IPMP mediante el subcomando <code>ipadm create -ipmp</code> para crear el grupo IPMP.</p>
Interfaz IPMP	<p>Se aplica sólo a la actual implementación de IPMP. El término se refiere a la interfaz IP que representa un grupo IPMP determinado, cualquiera de las interfaces subyacentes de la interfaz o todas ellas, y todas las direcciones de datos. En la implementación de IPMP actual, la interfaz IPMP es el componente central para administrar un grupo IPMP y se utiliza en las tablas de enrutamiento, tablas ARP, reglas de cortafuegos, etc.</p>
nombre de interfaz IPMP	<p>Indica el nombre de una interfaz IPMP. En este documento se utiliza la convención de denominación de <code>ipmpN</code>. El sistema también utiliza la misma convención de denominación en la creación de</p>

	<p>interfaz IPMP implícita. Sin embargo, el administrador puede elegir cualquier nombre mediante la creación de interfaz IPMP explícita.</p>
instancia única IPMP	<p>Hace referencia a una configuración IPMP que el software Oracle Solaris Cluster utiliza para permitir que una dirección de datos también actúe como una dirección de prueba. Esta configuración se aplica, por ejemplo, cuando una sola interfaz pertenece a un grupo IPMP.</p>
detección de fallos basada en enlaces	<p>Especifica una forma pasiva de detección de fallos, en la que se supervisa el estado de enlace de la tarjeta de red para determinar el estado de la interfaz. La detección de fallos basada en enlaces comprueba únicamente si el enlace está activo. Este tipo de detección de fallos no es admitido por todos los controladores de tarjeta de red. La detección de fallos basada en enlaces no requiere configuración explícita y proporciona una detección instantánea de fallos de enlace.</p> <p>Comparar con detección de fallos basada en sondeos.</p>
expansión de carga	<p>Hace referencia al proceso de distribuir tráfico de entrada o salida en un conjunto de interfaces. A diferencia del equilibrio de carga, la expansión de carga no garantiza que la carga se distribuya de manera uniforme. Como consecuencia de la expansión de carga, se obtiene un mayor rendimiento. La expansión de carga sólo se produce cuando el tráfico de red fluye hacia varios destinos que utilizan múltiples conexiones.</p> <p>La expansión de carga entrante indica el proceso de distribución de tráfico entrante a través de un conjunto de interfaces en un grupo IPMP. La expansión de carga entrante no se puede controlar directamente con IPMP. El algoritmo de selección de dirección de origen manipula indirectamente el proceso.</p> <p>La expansión de carga saliente hace referencia al proceso de distribución de tráfico saliente a través de un conjunto de interfaces en un grupo IPMP. La expansión de carga saliente se realiza por destino</p>

	mediante el módulo IP y se ajusta según sea necesario en función del estado y los miembros de las interfaces del grupo IPMP.
dirección NOFAILOVER	Se aplica sólo a la implementación de IPMP anterior. Se refiere a una dirección que está asociada con una interfaz subyacente y, por lo tanto, permanece como no disponible si la interfaz subyacente falla. Todas las direcciones NOFAILOVER tienen establecido el indicador NOFAILOVER. Las direcciones de prueba IPMP deben designarse como NOFAILOVER y las direcciones de datos IPMP nunca se deben designar como NOFAILOVER. El concepto de conmutación por error no existe en la implementación de IPMP. Sin embargo, el término NOFAILOVER permanece para compatibilidad administrativa.
interfaz OFFLINE	Indica una interfaz que se ha deshabilitado de manera administrativa del uso del sistema, normalmente como preparación para ser eliminada del sistema. Por ejemplo, dichas interfaces tienen establecido el indicador OFFLINE. El comando <code>if_mpadm</code> se puede utilizar para alternar una interfaz a un estado sin conexión.
interfaz física	Consulte: interfaz subyacente.
sondeo	Se refiere a un paquete ICMP, similar a los paquetes que son utilizados por el comando <code>ping</code> . Este sondeo se utiliza para probar las rutas de envío y recepción de una interfaz determinada. Los paquetes de sondeo son enviados por el daemon en <code>.mpathd</code> , si la detección de fallos basada en sondeos está habilitada. Un paquete de sondeo utiliza una dirección de prueba IPMP como su dirección de origen.
detección de fallos basada en sondeos	Indica una forma activa de detección de fallos, en la que los sondeos se intercambian con destinos de sondeo para determinar el estado de la interfaz. Cuando está habilitada, la detección de fallos basada en sondeos comprueba toda la ruta de envío y recepción de cada interfaz. Sin embargo, este tipo de detección necesita que el administrador configure explícitamente cada interfaz con una dirección de prueba.

destino de sondeo	<p>Comparar con detección de fallos basada en enlaces.</p> <p>Hace referencia a un sistema en el mismo enlace que una interfaz en un grupo IPMP. El daemon <code>in.mpathd</code> selecciona el destino para ayudar a comprobar el estado de una interfaz determinada mediante la detección de fallos basada en sondeos. El destino de sondeo puede ser cualquier host en el enlace que sea capaz de enviar y recibir los sondeos ICMP. Los destinos de sondeo suelen ser enrutadores. Varios destinos de sondeo se utilizan normalmente para aislar la lógica de detección de fallos de los fallos de los destino de sondeo en sí.</p>
selección de dirección de origen	<p>Hace referencia al proceso de selección de una dirección de datos del grupo IPMP como la dirección de origen para un paquete en particular. La selección de dirección de origen la realiza el sistema siempre que una aplicación no haya seleccionado específicamente una dirección de origen a utilizar. Puesto que cada dirección de datos se asocia a sólo una dirección de hardware, la selección de dirección de origen controla indirectamente la expansión de carga entrante.</p>
interfaz STANDBY	<p>Indica una interfaz que se configura administrativamente para ser utilizada solamente cuando otra interfaz del grupo ha fallado. Todas las interfaces STANDBY tendrán establecido el indicador STANDBY.</p>
sistemas de destino	<p>Consulte destino de sondeo.</p>
dirección de prueba	<p>Hace referencia a una dirección IP que debe usarse como dirección de origen o destino para sondeos, y no debe emplearse como dirección de origen o destino para tráfico de datos. Las direcciones de prueba están asociadas a una interfaz subyacente. Si una interfaz subyacente está configurada con una dirección de prueba UP, el daemon <code>in.mpathd</code> supervisa esta dirección mediante la detección de fallos basada en sondeos. Todas las direcciones de prueba debe designarse como NOFAILOVER. El sistema marca estas direcciones automáticamente como DEPRECATED para garantizar que no serán consideradas como una posible dirección de origen para paquetes de datos.</p>

interfaz subyacente	Especifica una interfaz IP que forma parte de un grupo IPMP y está directamente asociada a un dispositivo de red real. Por ejemplo, si <code>ce0</code> y <code>ce1</code> se colocan en el grupo IPMP <code>ipmp0</code> , entonces <code>ce0</code> y <code>ce1</code> componen las interfaces subyacentes de <code>ipmp0</code> . En la implementación anterior, los grupos IPMP tienen sólo interfaces subyacentes. Sin embargo, en la implementación actual, estas interfaces están por debajo de la interfaz IPMP (por ejemplo, <code>ipmp0</code>) que representa el grupo, de ahí su nombre.
operación de anulación de desconexión	Hace referencia al acto de habilitar administrativamente una interfaz que anteriormente estaba sin conexión para que pueda ser utilizada por el sistema. El comando <code>if_mpadm</code> se puede utilizar para realizar una operación de anulación de desconexión.
interfaz no utilizable	Se refiere a una interfaz subyacente que no puede utilizarse para enviar o recibir tráfico de datos en su configuración actual. Una interfaz no utilizable se diferencia de una interfaz <code>INACTIVE</code> , es decir no está en uso pero se puede utilizar si una interfaz activa en el grupo se vuelve inutilizable. Una interfaz no es utilizable si existe una de las siguientes condiciones: <ul style="list-style-type: none"> ▪ La interfaz no tiene dirección UP. ▪ Se ha establecido el indicador <code>FAILED</code> u <code>OFFLINE</code> para la interfaz. ▪ La interfaz se ha marcado como que tiene la misma dirección de hardware que otra interfaz del grupo.
dirección UP	Se refiere a una dirección que se ha establecido como disponible administrativamente en el sistema mediante el indicador <code>UP</code> . Una dirección que no es <code>UP</code> se trata como no perteneciente al sistema y, por lo tanto, nunca se tiene en cuenta durante la selección de dirección de origen.

Administración de IPMP

En este capítulo se proporcionan las tareas para administrar grupos de interfaces con múltiples rutas de redes IP (IPMP). Se abordan los siguientes temas principales:

- “Mapas de tareas de administración de IPMP” en la página 295
- “Configuración de grupos IPMP” en la página 298
- “Mantenimiento de grupos IPMP” en la página 306
- “Configuración para la detección de fallos basada en sondeos” en la página 309
- “Recuperación de configuración de IPMP con reconfiguración dinámica” en la página 313
- “Supervisión de información de IPMP” en la página 315

Mapas de tareas de administración de IPMP

En Oracle Solaris, el comando `ipmpstat` es la herramienta preferida que se debe utilizar para obtener información sobre el grupo IPMP. En este capítulo, el comando `ipmpstat` sustituye ciertas funciones del comando `ifconfig` que se usaban en las versiones anteriores de Oracle Solaris para proporcionar información de IPMP.

Para obtener información sobre las diferentes opciones para el comando `ipmpstat`, consulte “Supervisión de información de IPMP” en la página 315.

Las siguientes secciones proporcionan los enlaces a las tareas en este capítulo.

Creación y configuración del grupo IPMP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Planificar un grupo IPMP.	Enumera toda la información auxiliar y las tareas necesarias para poder configurar un grupo IPMP.	“Cómo planificar un grupo IPMP” en la página 298
Configurar un grupo IPMP mediante el DHCP.	Proporciona un método alternativo para configurar grupos IPMP mediante el DHCP.	“Cómo configurar un grupo IPMP mediante el DHCP” en la página 300
Configurar un grupo IPMP de interfaz activa-activa.	Configura un grupo IPMP en el que se despliegan todas las interfaces subyacentes para alojar el tráfico de la red.	“Cómo configurar manualmente un grupo IPMP de interfaz activa-activa” en la página 302
Configurar un grupo IPMP de interfaz activa-en espera.	Configura un grupo IPMP en el que una interfaz subyacente se mantiene inactiva como reserva.	“Cómo configurar manualmente un grupo IPMP de interfaz activa-en espera” en la página 304

Mantenimiento del grupo IPMP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Agregar una interfaz a un grupo IPMP.	Configura una interfaz nueva como miembro de un grupo IPMP existente.	“Cómo agregar una interfaz a un grupo IPMP” en la página 306
Eliminar una interfaz de un grupo IPMP.	Elimina una interfaz de un grupo IPMP.	“Cómo eliminar una interfaz de un grupo IPMP” en la página 306
Agregar direcciones IP a un grupo IPMP o eliminar direcciones IP de él.	Agrega direcciones a un grupo IPMP o las elimina de él.	“Cómo agregar o eliminar direcciones IP” en la página 307
Cambiar una pertenencia a IPMP de la interfaz.	Mueve las interfaces entre los grupos IPMP.	“Cómo mover una interfaz de un grupo IPMP a otro grupo” en la página 308
Suprimir un grupo IPMP.	Suprime un grupo IPMP que ya no sea necesario.	“Cómo suprimir un grupo IPMP” en la página 309
Sustituir las tarjetas que fallaron.	Elimina o sustituye las NIC de un grupo IPMP que hayan fallado.	“Cómo reemplazar una tarjeta física que ha fallado” en la página 313

Configuración de la detección de fallos basada en sondeos (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Especificar manualmente sistemas de destino.	Identifica y agrega sistemas de destino para la detección de fallos basada en sondeos.	“Cómo especificar manualmente los sistemas de destino para la detección de fallos basada en sondeos” en la página 310
Configurar el comportamiento de la detección de fallos basada en sondeos.	Modifica los parámetros para determinar el comportamiento de la detección de fallos basada en sondeos.	“Cómo configurar el comportamiento del daemon IPMP” en la página 312

Supervisión de un grupo IPMP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Obtener información del grupo.	Muestra información sobre un grupo IPMP.	“Cómo obtener información de grupo IPMP” en la página 315
Obtener información de dirección de datos.	Muestra información sobre las direcciones de datos utilizadas por un grupo IPMP.	“Cómo obtener información de dirección de datos IPMP” en la página 316
Obtener información de interfaz IPMP.	Muestra información sobre las interfaces subyacentes de interfaces o grupos IPMP.	“Cómo obtener información sobre interfaces IP subyacentes de un grupo” en la página 317
Obtener información de destino de sondeo.	Muestra información sobre los destinos de la detección de fallos basada en sondeos.	“Cómo obtener información de destino de sondeo IPMP” en la página 319
Obtener información de sondeo.	Muestra información en tiempo real sobre los sondeos en el sistema.	“Cómo observar sondeos IPMP” en la página 320
Personalizar la visualización de la información para supervisar los grupos IPMP.	Determina la información de IPMP que aparece en la pantalla.	“Cómo personalizar la salida del comando <code>ipmpstat</code> en una secuencia de comandos” en la página 321

Configuración de grupos IPMP

Esta sección proporciona los procedimientos que se utilizan para planificar y configurar los grupos IPMP. La descripción general en el [Capítulo 14, “Introducción a IPMP”](#) describe la implementación de los grupos IPMP como una interfaz. Así, en este capítulo, los términos *grupo IPMP* e *interfaz IPMP* se utilizan indistintamente.

▼ Cómo planificar un grupo IPMP

El siguiente procedimiento incluye las tareas de planificación requeridas y la información que se debe obtener antes de configurar un grupo IPMP. No es necesario realizar las tareas por orden.

Nota – Debe configurar sólo un grupo IPMP para cada subred o dominio de emisión L2. Para obtener más información, consulte [“Cuando se debe utilizar IPMP” en la página 267](#).

1 **Determine la configuración general de IPMP que se ajuste a sus necesidades.**

Su configuración de IPMP depende de lo que necesita la red para manejar el tipo de tráfico que se aloja en el sistema. IPMP reparte paquetes de red salientes en las interfaces del grupo IPMP y, por lo tanto, mejora el rendimiento de la red. Sin embargo, para una determinada conexión TCP, el tráfico entrante normalmente sólo sigue una ruta física a fin de minimizar el riesgo de procesar paquetes fuera de servicio.

Por lo tanto, si la red maneja un gran volumen de tráfico saliente, la configuración de un gran número de interfaces en un grupo IPMP puede mejorar el rendimiento de la red. Si en su lugar, el sistema aloja mucho tráfico entrante, el número de interfaces en el grupo no necesariamente mejora el rendimiento al repartir la carga del tráfico. Sin embargo, tener más interfaces subyacentes ayuda a garantizar la disponibilidad de la red durante fallos de la interfaz.

2 **Para sistemas basados en SPARC, compruebe que cada interfaz del grupo tenga una dirección MAC exclusiva.**

Para configurar una dirección MAC exclusiva para cada interfaz en el sistema, consulte [“SPARC: Cómo asegurarse de que la dirección MAC de una interfaz sea única” en la página 179](#).

3 Asegúrese de que se inserte y configure el mismo conjunto de módulos STREAMS en todas las interfaces del grupo IPMP.

Todas las interfaces del mismo grupo deben tener configurados los mismos módulos STREAMS en el mismo orden.

a. Compruebe el orden de los módulos STREAMS en todas las interfaces del grupo IPMP potencial.

Puede imprimir una lista de los módulos STREAMS mediante el comando `ifconfig interfaz modlist`. Por ejemplo, la siguiente es la salida de `ifconfig` para una interfaz `net0`:

```
# ifconfig net0 modlist
 0 arp
 1 ip
 2 e1000g
```

Como se muestra en la salida, las interfaces existen normalmente como controladores de red directamente debajo del módulo IP. Estas interfaces no deberían requerir ninguna configuración adicional.

Sin embargo, determinadas tecnologías se insertan como módulo STREAMS entre el módulo IP y el controlador de red. Si un módulo STREAMS tiene estado, puede producirse un comportamiento inesperado en la conmutación por error, aunque se inserte el mismo módulo en todas las interfaces de un grupo. Sin embargo, puede utilizar módulos STREAMS sin estado, siempre y cuando los inserte en el mismo orden en todas las interfaces del grupo IPMP.

b. Inserte los módulos de una interfaz en el orden estándar para el grupo IPMP.

```
ifconfig interface modinsert module-name@position
```

```
ifconfig net0 modinsert vpnmod@3
```

4 Utilice el mismo formato de direcciones IP en todas las interfaces del grupo IPMP.

Si una interfaz está configurada para IPv4, todas las interfaces del grupo deben estar configuradas para IPv4. Por ejemplo, si agrega direcciones IPv6 a una interfaz, todas las interfaces del grupo IPMP se debe configurar para que admitan IPv6.

5 Determine el tipo de detección de fallos que desea implementar.

Por ejemplo, si desea implementar detección de fallos basada en sondeos, debe configurar las direcciones de prueba de las interfaces subyacentes. Para obtener información relacionada, consulte [“Tipos de detección de fallos en IPMP” en la página 279](#).

6 Asegúrese de que todas las interfaces del grupo IPMP estén conectadas a la misma red local.

Por ejemplo, puede configurar los conmutadores Ethernet en la misma subred IP en un grupo IPMP. Puede configurar cualquier número de interfaces en un grupo IPMP.

Nota – También puede configurar un grupo IPMP de interfaz única, por ejemplo, si el sistema tiene una única interfaz física. Para obtener información relacionada, consulte [“Tipos de configuraciones de interfaces IPMP” en la página 277.](#)

7 Asegúrese de que el grupo IPMP no contenga interfaces con diferentes tipos de medios de red.

Las interfaces que están agrupadas deben tener el mismo tipo de interfaz, de acuerdo con lo que se define en `/usr/include/net/if_types.h`. Por ejemplo, no puede combinar interfaces Ethernet y Token Ring en un grupo IPMP. Tampoco puede combinar una interfaz de bus Token con las interfaces de modalidad de transferencia asíncrona (ATM) del mismo grupo IPMP.

8 En el caso de IPMP con interfaces ATM, configure dichas interfaces en modo de emulación de LAN.

IPMP no se admite para las interfaces que utilicen IP clásica sobre ATM.

▼ **Cómo configurar un grupo IPMP mediante el DHCP**

En la implementación actual de IPMP, los grupos IPMP se pueden configurar con el protocolo de configuración dinámica de sistemas (DHCP).

Un grupo IPMP con varias interfaces se puede configurar con interfaces activas-activas o activas-en modo de espera. Para obtener información relacionada, consulte [“Tipos de configuraciones de interfaces IPMP” en la página 277.](#) En el siguiente procedimiento se describen los pasos para configurar un grupo IPMP de interfaces activas-en modo de espera mediante el DHCP.

Antes de empezar

Asegúrese de que las interfaces IP que estarán en el grupo IPMP hayan sido configuradas correctamente a través de los enlaces de datos de red del sistema. Puede crear una interfaz IPMP incluso si no existen interfaces IP subyacentes. Sin embargo, las configuraciones posteriores en esta interfaz IPMP fallarán.

Para conocer los procedimientos para configurar enlaces e interfaces IP, consulte [“Configuración de la interfaz IP \(tarear\)” en la página 179.](#) Para obtener información sobre la configuración de interfaces IPv6, consulte [“Configuración de una interfaz de IPv6” de Administración de Oracle Solaris: servicios IP.](#)

Además, si está utilizando un sistema SPARC, configure una dirección MAC exclusiva para cada interfaz. Para conocer procedimientos, consulte [“SPARC: Cómo asegurarse de que la dirección MAC de una interfaz sea única” en la página 179.](#)

Por último, si está usando el DHCP, asegúrese de que las interfaces subyacentes cuenten con concesiones infinitas. De lo contrario, en caso de un fallo de grupo, las direcciones de prueba caducarán, el daemon desactivará la detección de fallos basada en sondeos, y se usará la

detección de fallos basada en enlaces. Si la detección de fallos basada en enlaces detecta que la interfaz está funcionando, el daemon puede informar erróneamente que la interfaz ha sido reparada. Para obtener más información sobre la configuración del DHCP, consulte el [Capítulo 13, “Planning for DHCP Service \(Tasks\)”](#) de *System Administration Guide: IP Services*.

Nota – No puede utilizar IPMP si el perfil de red activo en el sistema es un perfil reactivo. Antes de configurar los grupos IPMP, si es necesario, active el perfil `DefaultFixed` para pasar a un perfil de configuración de red fija. Para conocer los procedimientos, consulte [“Herramientas de configuración y perfiles”](#) en la [página 152](#).

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos”](#) de *Administración de Oracle Solaris: servicios de seguridad*.

2 Cree una interfaz IPMP.

```
# ipadm create-ipmp ipmp-interface
```

donde

interface_ipmp especifica el nombre de la interfaz IPMP. Puede asignar cualquier nombre significativo a la interfaz IPMP. Al igual que con cualquier interfaz IP, el nombre está formado por una cadena y un número, como `ipmp0`.

3 Cree las interfaces IP subyacentes si todavía no existen.

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

donde *interfaz_subyacente* hace referencia a la interfaz IP que agregará al grupo IPMP.

4 Agregue al grupo IPMP las interfaces IP subyacentes que contendrán las direcciones de prueba.

```
# ipadm add-ipmp -i under-interface1 [-i under-interface2 ...] ipmp-interface
```

Puede crear tantas interfaces IP para el grupo IPMP como haya disponibles en el sistema.

5 Configure el DHCP y gestione las direcciones de datos en la interfaz IPMP.

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

obj_dir representa un objeto de dirección y utiliza el formato *interfaz/cadena*. En este paso, la *interfaz* es la interfaz IPMP. La *cadena* puede ser cualquier cadena definida por el usuario. Por lo tanto, si tiene varias direcciones de datos en la interfaz IPMP, los objetos de dirección correspondientes serían *interfaz_ipmp/cadena1*, *interfaz_ipmp/cadena2*, *interfaz_ipmp/cadena3*, y así sucesivamente.

6 Haga que el DHCP gestione las direcciones de prueba en las interfaces subyacentes.

Debe emitir el siguiente comando para cada interfaz subyacente en el grupo IPMP.

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

obj_dir representa un objeto de dirección y utiliza el formato *interfaz/cadena*. En este paso, la *interfaz* es la interfaz subyacente. La *cadena* puede ser cualquier cadena definida por el usuario. Por lo tanto, si cuenta con varias interfaces subyacentes para el grupo IPMP, los objetos de dirección correspondientes serían *interfaz_subyacente1/cadena*, *interfaz_ipmp2/cadena*, *interfaz_ipmp3/cadena*, y así sucesivamente.

Ejemplo 15-1 Configuración de un grupo IPMP con el DHCP

En este ejemplo se muestra cómo configurar un grupo IPMP con interfaz activa-en espera con el DHCP según la siguiente situación:

- Se configurarán tres interfaces subyacentes para el grupo IPMP sobre sus respectivos enlaces de datos *net0*, *net1* y *net2*, que son miembros designados del grupo IPMP.
- La interfaz IPMP *itops0* tiene el mismo nombre que el grupo IPMP.
- *net2* es la interfaz en espera designada.
- Para utilizar la detección de fallos basada en sondeos, se asigna direcciones de prueba a todas las interfaces subyacentes.

```
# ipadm create-ipmp itops0

# ipadm create-ip net0
# ipadm create-ip net1
# ipadm create-ip net2

# ipadm add-ipmp -i net0 -i net1 -i net2 itops0

# ipadm create-addr -T dhcp itops0/dhcp0
# ipadm create-addr -T dhcp itops0/dhcp1

# ipadm create-addr -T dhcp net0/test
# ipadm create-addr -T dhcp net2/test
# ipadm create-addr -T dhcp net3/test

# ipadm set-ifprop -p standby=on net2
```

▼ Cómo configurar manualmente un grupo IPMP de interfaz activa-activa

El siguiente procedimiento describe los pasos para configurar manualmente un grupo IPMP de interfaz activa-activa.

Antes de empezar

Asegúrese de que las interfaces IP que estarán en el eventual grupo IPMP hayan sido configuradas correctamente a través de los enlaces de datos de red del sistema. Para conocer los procedimientos para configurar enlaces e interfaces IP, consulte “[Configuración de la interfaz IP \(tareas\)](#)” en la [página 179](#). Para obtener más información sobre la configuración de interfaces IPv6, consulte “[Configuración de una interfaz de IPv6](#)” de *Administración de Oracle Solaris*:

servicios IP. Puede crear una interfaz IPMP incluso si no existen interfaces IP subyacentes. Sin embargo, las configuraciones posteriores en esta interfaz IPMP fallarán.

Además, si está utilizando un sistema SPARC, configure una dirección MAC exclusiva para cada interfaz. Para conocer procedimientos, consulte “SPARC: Cómo asegurarse de que la dirección MAC de una interfaz sea única” en la página 179.

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Cree una interfaz IPMP.

```
# ipadm create-ipmp ipmp-interface
donde
```

interface_ipmp especifica el nombre de la interfaz IPMP. Puede asignar cualquier nombre significativo a la interfaz IPMP. Al igual que con cualquier interfaz IP, el nombre está formado por una cadena y un número, como *ipmp0*.

3 Agregue interfaces IP subyacentes al grupo.

```
# ipadm add-ipmp -i under-interface1 [-i underinterface2 ...] ipmp-interface
```

donde *interfaz_subyacente* hace referencia a la interfaz subyacente del grupo IPMP. Puede agregar tantas interfaces IP como haya disponibles en el sistema.

Nota – En un entorno de doble pila, si se coloca una instancia IPv4 de una interfaz en un grupo específico, automáticamente también se coloca la instancia IPv6 en el mismo grupo.

4 Agregue direcciones de datos a la interfaz IPMP.

```
# ipadm create-addr -T static IP-address addrobj
```

La *dirección_IP* puede estar en notación CIDR.

obj_dir debe utilizar la convención de nomenclatura *interfaz_ipmp/cualquier_cadena*. Por lo tanto, si el nombre de la interfaz IPMP es *ipmp0*, la *obj_dir* puede ser *ipmp0/dataaddr*.

5 Agregue direcciones de prueba en las interfaces subyacentes.

```
# ipadm create-addr -T static IP-address addrobj
```

La *dirección_IP* puede estar en notación CIDR.

obj_dir debe utilizar la convención de nomenclatura *interfaz_subyacente/cualquier_cadena*. Por lo tanto, si el nombre de una interfaz subyacente es *net0*, la *obj_dir* puede ser *net0/testaddr*.

Nota – Sólo debe configurar una dirección de prueba si desea utilizar la detección de fallos basada en sondeos en una interfaz específica.

Todas las direcciones IP de prueba de un grupo IPMP deben utilizar el mismo prefijo de red. Las direcciones IP de prueba deben pertenecer a una única subred IP.

▼ **Cómo configurar manualmente un grupo IPMP de interfaz activa-en espera**

Para obtener más información sobre las interfaces en espera, consulte [“Tipos de configuraciones de interfaces IPMP” en la página 277](#). El siguiente procedimiento configura un grupo IPMP en el que una interfaz se mantiene como reserva. Esta interfaz se despliega sólo cuando la interfaz activa del grupo falla.

1 **Conviértase en administrador.**

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

2 **Cree una interfaz IPMP.**

```
# ipadm create-ipmp ipmp-interface
```

donde

interface_ipmp especifica el nombre de la interfaz IPMP. Puede asignar cualquier nombre significativo a la interfaz IPMP. Al igual que con cualquier interfaz IP, el nombre está formado por una cadena y un número, como *ipmp0*.

3 **Agregue interfaces IP subyacentes al grupo.**

```
# ipadm add-ipmp -i under-interface1 [-i underinterface2 ...] ipmp-interface
```

donde *interfaz_subyacente* hace referencia a la interfaz subyacente del grupo IPMP. Puede agregar tantas interfaces IP como haya disponibles en el sistema.

Nota – En un entorno de doble pila, si se coloca una instancia IPv4 de una interfaz en un grupo específico, automáticamente también se coloca la instancia IPv6 en el mismo grupo.

4 **Agregue direcciones de datos a la interfaz IPMP.**

```
# ipadm create-addr -T static IP-address addrobj
```

La *dirección_IP* puede estar en notación CIDR.

obj_dir debe utilizar la convención de nomenclatura *interfaz_ipmp/cualquier_cadena*. Por lo tanto, si el nombre de la interfaz IPMP es *ipmp0*, la *obj_dir* puede ser *ipmp0/dataaddr*.

5 Agregue direcciones de prueba en las interfaces subyacentes.

```
# ipadm create-addr -T static IP-address addrobj
```

La *dirección_IP* puede estar en notación CIDR.

obj_dir debe utilizar la convención de nomenclatura *interfaz_subyacente/cualquier_cadena*.

Por lo tanto, si el nombre de una interfaz subyacente es *net0*, la *obj_dir* puede ser *net0/testaddr*.

Nota – Sólo debe configurar una dirección de prueba si desea utilizar la detección de fallos basada en sondeos en una interfaz específica.

Todas las direcciones IP de prueba de un grupo IPMP deben utilizar el mismo prefijo de red. Las direcciones IP de prueba deben pertenecer a una única subred IP.

6 Configure una de las interfaces subyacentes como interfaz en espera.

```
# ipadm set-ifprop -p standby=yes under-interface
```

Ejemplo 15-2 Configuración de un grupo IPMP de interfaz activa-en espera

En este ejemplo se muestra cómo crear manualmente una configuración IPMP de interfaz activa-en espera. El ejemplo comienza con la creación de interfaces subyacentes.

```
# ipadm create-ip net0
# ipadm create-ip net1
# ipadm create-ip net2

# ipadm create-ipmp itops0

# ipadm add-ipmp -i net0 -i net1 -i net2 itops0
# ipadm create-addr -T static -a 192.168.10.10/24 itops0/v4add1
# ipadm create-addr -T static -a 192.168.10.15/24 itops0/v4add2

# ipadm create-addr -T static -a 192.168.85.30/24 net0/test
# ipadm create-addr -T static -a 192.168.85.32/24 net1/test
# ipadm create-addr -T static -a 192.168.85.34/24 net2/test

# ipadm set-ifprop -p standby=yes net2

# ipmpstat -g
GROUP      GROUPNAME  STATE      FDT          INTERFACES
itops0     itops0     ok         10.00s      net0 net1 (net2)

# ipmpstat -t
INTERFACE  MODE      TESTADDR    TARGETS
net0       routes   192.168.10.30  192.168.10.1
net1       routes   192.168.10.32  192.168.10.1
net2       routes   192.168.10.34  192.168.10.5
```

Mantenimiento de grupos IPMP

Esta sección contiene las tareas para mantener los grupos IPMP existentes y las interfaces dentro de esos grupos. Las tareas presuponen que ya se ha configurado un grupo IPMP, tal como se explica en [“Configuración de grupos IPMP” en la página 298](#).

▼ Cómo agregar una interfaz a un grupo IPMP

Antes de empezar Asegúrese de que la interfaz que agregue al grupo coincida con todas las restricciones que estarán en el grupo. Para obtener una lista de los requisitos de un grupo IPMP, consulte [“Cómo planificar un grupo IPMP” en la página 298](#).

1 Conviértase en administrador.

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

2 Si la interfaz IP subyacente aún no existe, créela.

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

3 Agregue la interfaz IP al grupo IPMP.

```
# ipadm add-ipmp -i under-interface ipmp-interface
```

Ejemplo 15-3 Adición de una interfaz a un grupo IPMP

Para agregar la interfaz net4 al grupo IPMP itops0, debe escribir los siguientes comandos:

```
# ipadm create-ip net4
# ipadm add-ipmp -i net4 itops0
# ipmpstat -g
GROUP  GROUPNAME  STATE      FDT      INTERFACES
itops0  itops0      ok         10.00s   net0 net1 net4
```

▼ Cómo eliminar una interfaz de un grupo IPMP

1 Conviértase en administrador.

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

2 Elimine la interfaz del grupo IPMP.

```
# ipadm remove-ipmp -i under-interface[, -i under-interface, ...] ipmp-interface
```

Puede eliminar tantas interfaces subyacentes en un comando único según sea necesario. La eliminación de todas las interfaces subyacentes no suprime la interfaz IPMP. En su lugar, existe como una interfaz o grupo IPMO vacío.

Ejemplo 15-4 Eliminación de una interfaz de un grupo

Para eliminar la interfaz `net4` del grupo IPMP `itops0`, debe escribir el siguiente comando:

```
# ipadm remove-ipmp net4 itops0
# ipmpstat -g
GROUP  GROUPNAME  STATE      FDT        INTERFACES
itops0 itops0     ok         10.00s    net0 net1
```

▼ Cómo agregar o eliminar direcciones IP

Puede utilizar el subcomando `ipadm create-addr` para agregar direcciones o el subcomando `ipadm delete-addr` para eliminar direcciones de las interfaces. En la implementación de IPMP actual, las direcciones de prueba se encuentran alojadas en la interfaz IP subyacente, mientras que las direcciones de datos se asignan a la interfaz IPMP. Los siguientes procedimientos describen cómo agregar o eliminar direcciones IP que son direcciones de prueba o direcciones de datos.

1 Conviértase en administrador.

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

2 Agregue o elimine direcciones de datos.

- Para agregar direcciones de datos al grupo IPMP, escriba el siguiente comando:

```
# ipadm create-addr -T static -a ip-address addrobj
```

obj_dir usa la convención de nomenclatura *interfaz_ipmp/cadena_usuario*.

- Para eliminar una dirección del grupo IPMP, escriba el siguiente comando:

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

obj_dir usa la convención de nomenclatura *interfaz_subyacente/cadena_usuario*.

3 Agregue o elimine direcciones de prueba.

- Para asignar una dirección de prueba a una interfaz subyacente del grupo IPMP, escriba el siguiente comando:

```
# ipadm create-addr -T static ip-address adrobj
```

- Para eliminar una dirección de prueba de una interfaz subyacente del grupo IPMP, escriba el siguiente comando:

```
# ipadm delete-addr adrobj
```

Ejemplo 15-5 Eliminación de una dirección de prueba de una interfaz

El siguiente ejemplo utiliza la configuración de `itops0` en el [Ejemplo 15-2](#). El paso elimina la dirección de prueba de la interfaz `net1`. En este ejemplo, se asume que la dirección de prueba se denomina `net1/test1`:

```
# ipmpstat -t
INTERFACE      MODE      TESTADDR      TARGETS
net1           routes    192.168.10.30  192.168.10.1

# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0          static    ok         127.0.0.1/8
...
net1/test1   static    ok         192.168.10.30

# ipadm delete-addr net1/test1
```

▼ Cómo mover una interfaz de un grupo IPMP a otro grupo

Puede colocar una interfaz en un grupo IPMP nuevo cuando la interfaz pertenece a un grupo IPMP existente. No es necesario eliminar la interfaz del grupo IPMP actual. Cuando coloca la interfaz en un grupo nuevo, se elimina automáticamente de cualquier grupo IPMP existente.

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Mueva la interfaz a un grupo IPMP nuevo.

```
# ipadm add-ipmp -i under-interface ipmp-interface
```

donde *interfaz_subyacente* hace referencia a la interfaz subyacente que desea mover y *interfaz_ipmp* hace referencia a la interfaz o grupo IPMP al que desea mover la interfaz subyacente.

Al colocar la interfaz en un grupo nuevo, se elimina automáticamente la interfaz de cualquier grupo existente.

Ejemplo 15-6 Cómo mover una interfaz a otro grupo IPMP

En este ejemplo se asume que las interfaces subyacentes del grupo son `net0`, `net11` y `net2`. Para mover `net0` al grupo IPMP `cs-link1`, debe escribir lo siguiente:

```
# ipadm add-ipmp -i net0 ca-link1
```

Este comando elimina la interfaz `net0` del grupo IPMP `itops0` y coloca `net0` en `cs-link1`.

▼ Cómo suprimir un grupo IPMP

Utilice este procedimiento si ya no necesita un grupo IPMP específico.

1 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Identifique el grupo IPMP y las interfaces IP subyacentes.

```
# ipmpstat -g
```

3 Suprima todas las interfaces IP que pertenecen actualmente al grupo IPMP.

```
# ipadm remove-ipmp -i under-interface[, -i under-interface, ...] ipmp-interface
```

Nota – Para suprimir correctamente una interfaz IPMP, no debe existir ninguna interfaz IP como parte del grupo IPMP.

4 Suprima la interfaz IPMP.

```
# ipadm delete-ipmp ipmp-interface
```

Después de eliminar la interfaz IPMP, cualquier dirección IP que esté asociada con la interfaz se suprime del sistema.

Ejemplo 15-7 Supresión de una interfaz IPMP

Para suprimir la interfaz `itops0` que tiene la interfaz IP subyacente `net0` y `net1`, debe escribir los siguientes comandos:

```
# ipmpstat -g
GROUP  GROUPNAME  STATE      FDT          INTERFACES
itops0  itops0      ok         10.00s      net0 net1

# ipadm remove-ipmp -i net0 -i net1 itops0

# ipadm delete-ipmp itops0
```

Configuración para la detección de fallos basada en sondeos

La detección de fallos basada en sondeos implica el uso de sistemas de destino, tal como se explica en “[Detección de fallos basada en sondeos](#)” en la [página 280](#). Para identificar destinos para la detección de fallos basada en sondeos, el daemon `in.mpathd` funciona en dos modos: modo de destino de enrutador o modo de destino de multidifusión. En el modo de destino de enrutador, el daemon de rutas múltiples sondea los destinos definidos en la tabla de

enrutamiento. Si no se han definido destinos, el daemon funciona en modo de destino de multidifusión, en el que se envían paquetes de multidifusión para sondear los hosts vecinos en la LAN.

Preferiblemente, debe configurar destinos de host para que sondee el daemon `in.mpathd`. Para algunos grupos IPMP, el enrutador predeterminado es suficiente como destino. Sin embargo, para algunos grupos IPMP, quizá desee configurar destinos específicos para la detección de fallos basada en sondeos. Para especificar los destinos, configure las rutas de host en la tabla de enrutamiento como destinos de sondeo. Cualquier ruta host configurada en la tabla de enrutamiento aparece enumerada antes del enrutador predeterminado. IPMP utiliza rutas host definidas explícitamente para la selección de destino. Por lo tanto, debe configurar rutas host para configurar destinos específicos de sondeo en lugar de utilizar el enrutador predeterminado.

Para configurar las rutas host en la tabla de enrutamiento, utilice el comando `route`. Puede utilizar la opción `-p` con este comando para agregar rutas persistentes. Por ejemplo, `route -p add` agrega una ruta que permanecerá en la tabla de enrutamiento incluso después de reiniciar el sistema. Por lo tanto, la opción `-p` permite agregar rutas persistentes sin necesidad de secuencias de comandos especiales para volver a crear estas rutas en cada inicio del sistema. Para utilizar de forma óptima la detección de fallos basada en sondeos, asegúrese de configurar varios destinos para recibir sondeos.

El procedimiento de ejemplo a continuación muestra la sintaxis exacta para agregar rutas persistente a los destinos para la detección de fallos basada en sondeos. Para obtener más información sobre las opciones para el comando `route`, consulte la página del comando [man route\(1M\)](#).

Considere los siguientes criterios cuando evalúe qué hosts de su red podrían ser destinos correctos.

- Asegúrese de que los posibles destinos estén disponibles y de que se estén ejecutando. Haga una lista de sus direcciones IP.
- Asegúrese de que las interfaces de destino se encuentren en la misma red que el grupo IPMP que está configurando.
- La máscara de red y la dirección de emisión de los sistemas de destino deben ser las mismas que las direcciones del grupo IPMP.
- El host de destino debe poder responder a las solicitudes de ICMP desde la interfaz que utiliza la detección de fallos basada en sondeos.

▼ **Cómo especificar manualmente los sistemas de destino para la detección de fallos basada en sondeos**

- 1 **Inicie sesión con su cuenta de usuario en el sistema en el que va a configurar la detección de fallos basada en sondeos.**

- 2 **Agregue una ruta a un host particular para utilizar como destino en la detección de fallos basada en sondeos.**

```
$ route -p add -host destination-IP gateway-IP -static
```

donde *IP_destino* e *IP_puerta de enlace* son direcciones IPv4 del host que se utilizará como un destino. Por ejemplo, para especificar el sistema de destino escribiría 192.168.10.137, que se encuentra en la misma subred que las interfaces del grupo IPMP *itops0*:

```
$ route -p add -host 192.168.10.137 192.168.10.137 -static
```

Esta nueva ruta se configurará automáticamente cada vez que se reinicie el sistema. Si desea definir sólo una ruta temporal para un sistema de destino para la detección de fallos basada en sondeos, no utilice la opción *-p*.

- 3 **Agregue rutas a los host adicionales de la red para utilizar como sistemas de destino.**

▼ **Cómo seleccionar qué método de detección de fallos utilizar**

De manera predeterminada, la detección de fallos basada en sondeos solamente se puede realizar mediante direcciones de prueba. Si el controlador NIC es compatible con ella, la detección de fallos basada en enlaces también se habilita automáticamente.

No puede desactivar la detección de fallos basada en enlaces si este método es compatible con el controlador NIC. Sin embargo, puede seleccionar qué tipo de detección de fallos basada en sondeos implementar.

- 1 **Para utilizar únicamente sondeo transitivo, realice los siguientes pasos:**

- a. **Use los comandos SMF apropiados para activar la propiedad IPMP *transitive-probing*.**

```
# svccfg -s svc:/network/ipmp setprop config/transitive-probing=true
# svcadm refresh svc:/network/ipmp:default
```

Para obtener más información sobre la configuración de esta propiedad, consulte la página del comando `man in.mpathd(1M)`.

- b. **Elimine cualquier dirección de prueba existente que se haya configurado para el grupo IPMP.**

- 2 **Para utilizar únicamente direcciones de prueba para el sondeo de fallos, realice los siguientes pasos:**

- a. **Si es necesario, desactive el sondeo transitivo.**

```
# svccfg -s svc:/network/ipmp setprop config/transitive-probing=false
# svcadm refresh svc:/network/ipmp:default
```

- b. **Asigne direcciones de prueba para las interfaces subyacentes del grupo IPMP.**

▼ Cómo configurar el comportamiento del daemon IPMP

Use el archivo de configuración IPMP `/etc/default/mpathd` con el fin de configurar los siguientes parámetros de todo el sistema para grupos IPMP.

- `FAILURE_DETECTION_TIME`
- `TRACK_INTERFACES_ONLY_WITH_GROUPS`
- `FAILBACK`

1 Conviértase en administrador.

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

2 Edite el archivo `/etc/default/mpathd`.

Cambie el valor predeterminado de uno o más de los tres parámetros.

a. Escriba el nuevo valor para el parámetro `FAILURE_DETECTION_TIME`.

```
FAILURE_DETECTION_TIME=n
```

donde *n* es el tiempo en segundos para que los sondeos ICMP detecten si se ha producido un fallo de la interfaz. El valor predeterminado es de 10 segundos.

b. Escriba el nuevo valor para el parámetro `FAILBACK`.

```
FAILBACK=[yes | no]
```

- *yes*: el valor *yes* es el comportamiento de recuperación tras fallos predeterminado de IPMP. Cuando se detecta la reparación de una interfaz fallida, el acceso de red recupera la interfaz reparada, tal como se describe en [“Detección de reparaciones de interfaces físicas” en la página 282](#).
- *no*: el valor *no* indica que el tráfico de datos no se devuelve a una interfaz reparada. Cuando se detecta la reparación de una interfaz fallida, se configura el indicador `INACTIVE` para dicha interfaz. Este indicador significa que la interfaz no se va a utilizar para el tráfico de datos. La interfaz se puede seguir utilizando para el tráfico de sondeos. Por ejemplo, el grupo IPMP `ipmp0` consta de dos interfaces: `net0` y `net1`. En el archivo `/etc/default/mpathd`, está definido el parámetro `FAILBACK=no`. Si `net0` falla, se marca como `FAILED` y se vuelve no utilizable. Tras la reparación, la interfaz se marca como `INACTIVE` y permanece no utilizable debido a la configuración `FAILBACK=no`.

Si `net1` falla y solamente `net0` está en el estado `INACTIVE`, se borra el indicador `INACTIVE` `net0` y la interfaz se vuelve utilizable. Si el grupo de IPMP tiene otras interfaces que también están en el estado `INACTIVE`, cualquiera de estas interfaces `INACTIVE`, y no necesariamente `net0`, se pueden borrar y convertir en utilizables cuando `net1`.

c. **Escriba el nuevo valor para el parámetro `TRACK_INTERFACES_ONLY_WITH_GROUPS` .**

```
TRACK_INTERFACES_ONLY_WITH_GROUPS=[yes | no]
```

Nota – Para obtener información sobre este parámetro y la función de grupo anónimo, consulte [“Detección de fallos y función del grupo anónimo” en la página 282.](#)

- *yes*: el valor *yes* es el predeterminado para el comportamiento de IPMP. Este parámetro hace que IPMP omita las interfaces de red que no están configuradas en un grupo IPMP.
- *no*: el valor *no* define la detección de fallos y la reparación para *todas* las interfaces de red, independientemente de si están configuradas en un grupo IPMP. Sin embargo, cuando se detecta un fallo o reparación en una interfaz que no está configurada en un grupo IPMP, no se desencadena ninguna acción en IPMP para mantener la funciones de red de dicha interfaz. Por tanto, el valor *no* sólo resulta útil para comunicar errores y no mejora directamente la disponibilidad de la red.

3 Reinicie el daemon `in.mpathd`.

```
# kill -HUP in.mpathd
```

Recuperación de configuración de IPMP con reconfiguración dinámica

Esta sección contiene los procedimientos relativos a la administración de sistemas que admiten reconfiguración dinámica (DR).

▼ **Cómo reemplazar una tarjeta física que ha fallado**

Este procedimiento explica cómo reemplazar una tarjeta física en un sistema que admite DR. El procedimiento asume las siguientes condiciones:

- El NCP activo de su sistema es `DefaultFixed`. Consulte la sección *Reconfiguración dinámica y perfiles de configuración de red* en [“Cómo funciona NWAM con otras tecnologías de red de Oracle Solaris” en la página 42](#) para obtener información sobre el uso de DR si el NCP activo del sistema no es `DefaultFixed`.
- Las interfaces IP del sistema son `net0` y `net1`.
- Ambas interfaces pertenecen al grupo IPMP `itops0`.
- La interfaz subyacente `net0` contiene una dirección de prueba.
- La interfaz subyacente `net0` ha fallado y necesita eliminar la tarjeta de `net0`, `bge`.
- Está sustituyendo la tarjeta `bge` por una tarjeta `e1000g`.

Antes de empezar

Los procedimientos para llevar a cabo la DR varían según el tipo de sistema. Por lo tanto, asegúrese de completar lo siguiente:

- Asegúrese de que el sistema admita DR.
- Consulte el manual apropiado que describe los procedimientos de DR en el sistema. Para el hardware Sun de Oracle, todos los sistemas que admiten DR son servidores. Para localizar documentación de DR actual en los sistemas Sun, busque “reconfiguración dinámica” en <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

Nota – Los pasos del procedimiento siguiente sólo hacen referencia a aspectos de DR que se relacionan específicamente con IPMP y con el uso de nombres de enlace. El procedimiento no contiene los pasos completos para llevar a cabo la DR. Por ejemplo, algunas capas más allá de la capa de IP requieren pasos de configuración manuales, como para ATM y otros servicios, si la configuración no es automática. Siga la documentación de DR apropiada para su sistema.

Para conocer el procedimiento detallado para sustituir las NIC, consulte “Cómo sustituir una tarjeta de interfaz de red con reconfiguración dinámica” en la página 171.

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Realice los pasos apropiados de la DR para eliminar del sistema la NIC con fallos.

Por ejemplo, debe eliminar la tarjeta bge.

3 Adjunte el reemplazo de la NIC al sistema.

Por ejemplo, instale la tarjeta e1000g en la misma ubicación que ocupaba la tarjeta bge. El enlace de datos de e1000g asume el nombre net0 y hereda la configuración del enlace de datos.

4 Complete el proceso de DR mediante la activación de nuevos recursos de NIC para que se pueda utilizar.

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

Después de este paso, según las configuraciones persistentes de net0, la nueva interfaz se configura con la dirección de prueba, se agrega como una interfaz subyacente del grupo IPMP y se despliega como una interfaz activa o en modo de espera. Entonces el núcleo puede asignar direcciones de datos a esta nueva interfaz según las configuraciones persistentes de la interfaz IPMP, `itops0`.

Supervisión de información de IPMP

Los siguientes procedimientos utilizan el comando `ipmpstat`, lo que le permite supervisar diferentes aspectos de los grupos IPMP en el sistema. Puede observar el estado del grupo IPMP como un todo o puede observar sus interfaces IP subyacentes. También puede verificar la configuración de los datos y direcciones de prueba para el grupo. Con el comando `ipmpstat`, también puede obtenerse información sobre la detección de fallos. Para obtener más detalles sobre el comando `ipmpstat` y sus opciones, consulte la página del comando [man ipmpstat\(1M\)](#).

De manera predeterminada, los nombres de host se muestran en la salida en lugar de las direcciones IP numéricas, siempre que haya nombres de host. Para mostrar las direcciones IP numéricas en la salida, utilice la opción `-n` junto con otras opciones para mostrar información específica del grupo IPMP.

Nota – En los siguientes procedimientos, el uso del comando `ipmpstat` no requiere privilegios de administrador del sistema, a menos que se especifique lo contrario.

▼ Cómo obtener información de grupo IPMP

Utilice este procedimiento para mostrar el estado de los distintos grupos IPMP en el sistema, incluido el estado de sus interfaces subyacentes. Si está habilitada la detección de fallos basada en sondeos para un grupo específico, el comando también incluye el tiempo de detección de fallos para ese grupo.

● Visualice la información del grupo IPMP.

```
$ ipmpstat -g
GROUP  GROUPNAME  STATE      FDT          INTERFACES
itops0  itops0     ok         10.00s      net0 net1
acctg1  acctg1     failed    --          [net3 net4]
field2  field2     degraded  20.00s      net2 net5 (net7) [net6]
```

GROUP Especifica el nombre de la interfaz IPMP. En el caso de un grupo anónimo, este campo estará vacío. Para obtener más información sobre los grupos anónimos, consulte la página del comando [man in.mpathd\(1M\)](#).

GROUPNAME Especifica el nombre del grupo IPMP. En el caso de un grupo anónimo, este campo estará vacío.

STATE Indica el estado actual de un grupo, que puede ser uno de los siguientes:

- **ok** indica que pueden usarse todas las interfaces subyacentes del grupo IPMP.
- **degraded** indica que algunas de las interfaces subyacentes del grupo son no utilizables.

- `failed` indica que todas las interfaces del grupo son no utilizables.
- FDT Especifica el tiempo de detección de fallos, si está habilitada la detección de fallos. Si la detección de fallos está deshabilitada, este campo estará vacío.
- INTERFACES Especifica las interfaces subyacentes que pertenecen al grupo. En este campo, primero se muestran las interfaces activas, luego las interfaces inactivas y, por último, las interfaces no utilizables. El estado de la interfaz está indicado por la manera en que se muestra:
 - *interfaz* (sin paréntesis ni corchetes) indica una interfaz activa. Las interfaces activas son las que están siendo usadas por el sistema para enviar o recibir tráfico de datos.
 - (*interfaz*) (con paréntesis) indica un funcionamiento, pero una interfaz inactiva. La interfaz no está en uso, según como lo define la directiva de administración.
 - [*interfaz*] (con corchetes) indica que la interfaz es no utilizable porque ha fallado o se ha puesto fuera de línea.

▼ Cómo obtener información de dirección de datos IPMP

Utilice este procedimiento para mostrar las direcciones de datos y el grupo al que cada dirección pertenece. La información que se muestra también incluye qué dirección está disponible para su uso, en función de si la dirección ha sido activada y desactivada mediante el comando `ipadm [up-addr/abajo-addr]`. También puede determinar en qué interfaz entrante o saliente se puede utilizar una dirección.

● Visualice la información de dirección IPMP.

```
$ ipmpstat -an
ADDRESS      STATE  GROUP      INBOUND    OUTBOUND
192.168.10.10 up     itops0     net0 net0 net1
192.168.10.15 up     itops0     net1 net0 net1
192.0.0.100  up     acctg1     --         --
192.0.0.101  up     acctg1     --         --
128.0.0.100  up     field2     net2       net2 net7
128.0.0.101  up     field2     net7       net2 net7
128.0.0.102  down   field2     --         --
```

ADDRESS Especifica el nombre del host o la dirección de datos, si se utiliza la opción `-n` junto con la opción `-a`.

STATE Indica si la dirección de la interfaz IPMP es `up` y, por lo tanto, es utilizable, o `down` y, por lo tanto, es no utilizable.

GROUP Especifica la interfaz IP IPMP que contiene una dirección de datos específica.

INBOUND	Identifica la interfaz que recibe los paquetes para una dirección determinada. La información de campo puede cambiar en función de eventos externos. Por ejemplo, si una dirección de datos está caída o si no quedan interfaces IP en el grupo IPMP, este campo estará vacío. El campo vacío indica que el sistema no acepta paquetes IP que están destinados a la dirección indicada.
OUTBOUND	Identifica la interfaz que envía los paquetes que utilizan una dirección dada como dirección de origen. Al igual que con el campo INBOUND, la información del campo OUTBOUND también puede cambiar en función de eventos externos. Un campo vacío indica que el sistema no envía paquetes con la dirección de origen determinada. El campo podría estar vacío ya sea porque la dirección está caída o porque no quedan interfaces IP activas en el grupo.

▼ Cómo obtener información sobre interfaces IP subyacentes de un grupo

Utilice este procedimiento para mostrar información sobre las interfaces IP subyacentes de un grupo IPMP. Para obtener una descripción de la relación correspondiente entre la NIC, el enlace de datos y la interfaz IP, consulte [“La pila de red en Oracle Solaris” en la página 22](#).

● Visualice la información de interfaz IPMP.

```
$ impstat -i
INTERFACE  ACTIVE  GROUP   FLAGS   LINK    PROBE   STATE
net0       yes    itops0  --mb--- up      ok      ok
net1       yes    itops0  ------ up      disabled ok
net3       no     acctg1  ------ unknown disabled offline
net4       no     acctg1  is----- down    unknown failed
net2       yes    field2  --mb--- unknown ok      ok
net6       no     field2  -i----- up      ok      ok
net5       no     filed2  ------ up      failed  failed
net7       yes    field2  --mb--- up      ok      ok
```

INTERFACE Especifica cada interfaz subyacente de cada grupo IPMP.

ACTIVE Indica si la interfaz está en funcionamiento y en uso (yes) o no (no).

GROUP Especifica el nombre de la interfaz IPMP. En el caso de grupos anónimos, este campo estará vacío. Para obtener más información sobre los grupos anónimos, consulte la página del comando `man in.mpathd(1M)`.

FLAGS Indica el estado de la interfaz subyacente, que puede ser uno de los siguientes o cualquier combinación de ellos:

- i indica que el indicador INACTIVE está configurado para la interfaz y que por lo tanto la interfaz no se usa para enviar o recibir datos de tráfico.
- s indica que la interfaz está configurada para ser una interfaz en modo de espera.

- m indica que la interfaz fue designada por el sistema para enviar y recibir tráfico de multidifusión IPv4 para el grupo IPMP.
 - b indica que la interfaz fue designada por el sistema para recibir el tráfico de difusión para el grupo IPMP.
 - M indica que la interfaz fue designada por el sistema para enviar y recibir tráfico de multidifusión IPv6 para el grupo IPMP.
 - d indica que la interfaz está caída y que, por lo tanto no es utilizable.
 - h indica que la interfaz comparte una dirección de hardware físico duplicada con otra interfaz y que ha sido puesta fuera de línea. El indicador h significa que la interfaz es no utilizable.
- LINK Indica el estado de la detección de fallos basada en enlaces, que es uno de los siguientes estados:
- up o down indican la disponibilidad o la no disponibilidad de un enlace.
 - unknown indica que el controlador no admite la notificación de si un enlace está up o down y, por lo tanto, no detecta los cambios de estado del enlace.
- PROBE Especifica el estado de la detección de fallos basada en sondeo para las interfaces que se configuraron con una dirección de prueba, de la siguiente manera:
- ok indica que la sonda funciona y está activa.
 - failed indica que la detección de fallos basada en sondeo ha detectado que la interfaz no funciona.
 - unknown indica que no se pudieron encontrar destinos de sondeo adecuados y que, por lo tanto, no se enviaron sondas.
 - disabled indica que no hay una dirección de prueba de IPMP configurada en la interfaz. Por lo tanto, la detección de fallos basada en sondeo está deshabilitada.
- STATE Especifica el estado general de la interfaz, de la siguiente manera:
- ok indica que la interfaz está en línea y que funciona normalmente según la configuración de los métodos de detección de fallos.
 - failed indica que la interfaz no funciona, ya sea porque el enlace de la interfaz está caído o porque la detección basada en sondeo determinó que la interfaz no puede enviar ni recibir tráfico.
 - offline indica que la interfaz no está disponible para su uso. Normalmente, la interfaz se cambia a sin conexión en las siguientes circunstancias:
 - La interfaz se está probando.
 - Se está realizando la reconfiguración dinámica.
 - La interfaz comparte una dirección de hardware duplicada con otra interfaz.

- unknown indica que el estado de la interfaz IPMP no se puede determinar porque no se pueden encontrar destinos de sondeo para la detección de fallos basada en sondeo.

▼ Cómo obtener información de destino de sondeo IPMP

Utilice este procedimiento para supervisar los destinos de sondeo que están asociados con cada interfaz IP en un grupo IPMP.

● Visualice los destinos de sondeo IPMP.

```
$ ipmpstat -nt
INTERFACE  MODE          TESTADDR      TARGETS
net0       routes       192.168.85.30 192.168.85.1 192.168.85.3
net1       disabled     --            --
net3       disabled     --            --
net4       routes       192.1.2.200   192.1.2.1
net2       multicast    128.9.0.200   128.0.0.1 128.0.0.2
net6       multicast    128.9.0.201   128.0.0.2 128.0.0.1
net5       multicast    128.9.0.202   128.0.0.1 128.0.0.2
net7       multicast    128.9.0.203   128.0.0.1 128.0.0.2
```

```
$ ipmpstat -nt
INTERFACE  MODE          TESTADDR      TARGETS
net3       transitive    <net1>        <net1> <net2> <net3>
net2       transitive    <net1>        <net1> <net2> <net3>
net1       routes       172.16.30.100 172.16.30.1
```

INTERFACE Especifica las interfaces subyacentes del grupo IPMP.

MODE Especifica el método para obtener los destinos de sondeo.

- routes indica que se usa la tabla de enrutamiento del sistema para encontrar destinos de sondeo.
- mcast indica que se usan sondas ICMP multidifusión para encontrar destinos de sondeo.
- disabled indica que se deshabilitó la detección de fallos basada en sondeo para la interfaz.
- transitive indica que se usa sondeo transitivo para la detección de fallos, como se muestra en el segundo ejemplo. Tenga en cuenta que no puede implantar la detección de fallos basada en sondeos si utiliza simultáneamente sondeos transitivos y direcciones de prueba. Si no desea utilizar las direcciones de prueba, debe pasar al sondeo transitivo. Si no desea utilizar el sondeo transitivo, debe configurar direcciones de prueba. Para obtener una descripción general, consulte [“Detección de fallos basada en sondeos” en la página 280.](#)

TESTADDR Especifica el nombre del host o, si la opción `-n` se utiliza junto con la opción `-t`, la dirección IP asignada a la interfaz para enviar y recibir sondeos.

Si se utiliza sondeo transitivo, entonces los nombres de interfaz hacen referencia a las interfaces IP subyacentes que no se usan activamente para recibir datos. Los nombres también indican que se envían sondeos de prueba transitivos con la dirección de origen de estas interfaces especificadas. Para las interfaces IP subyacentes activas que reciben datos, una dirección IP que se muestra indica la dirección de origen de los sondeos ICMP salientes.

Nota – Si una interfaz IP está configurada con la dirección de prueba IPv4 y la IPv6, la información de destino de prueba se muestra por separado para cada dirección de prueba.

TARGETS Muestra los destinos de sondeo actuales en una lista separada por espacios. Los destinos de sondeo se muestran como nombres de host o direcciones IP, si se usa la opción `-n` junto con la opción `-t`.

▼ Cómo observar sondeos IPMP

Utilice este procedimiento para observar sondeos en curso. Al emitir el comando para observar los sondeos, se muestra constantemente información sobre la actividad de sondeo del sistema hasta que detenga el comando con `Ctrl-C`. Debe tener privilegios de administrador principal para ejecutar este comando.

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Visualice la información acerca de los sondeos en curso.

```
# ipmpstat -pn
TIME    INTERFACE  PROBE    NETRTT   RTT      RTTAVG   TARGET
0.11s   net0       589     0.51ms  0.76ms  0.76ms   192.168.85.1
0.17s   net4       612     --      --      --       192.1.2.1
0.25s   net2       602     0.61ms  1.10ms  1.10ms   128.0.0.1
0.26s   net6       602     --      --      --       128.0.0.2
0.25s   net5       601     0.62ms  1.20ms  1.00ms   128.0.0.1
0.26s   net7       603     0.79ms  1.11ms  1.10ms   128.0.0.1
1.66s   net4       613     --      --      --       192.1.2.1
1.70s   net0       603     0.63ms  1.10ms  1.10ms   192.168.85.3
^C
```

```
# ipmpstat -pn
TIME    INTERFACE  PROBE    NETRTT   RTT      RTTAVG   TARGET
```

```

1.39S net4 t28 1.05ms 1.06ms 1.15ms <net1>
1.39s net1 i29 1.00ms 1.42ms 1.48ms 172.16.30.1

```

TIME	Especifica el tiempo de envío de un sondeo en relación con la fecha de emisión del comando <code>ipmpstat</code> . Si un sondeo se inició antes de <code>ipmpstat</code> , entonces, la hora se muestra con un valor negativo, en relación a cuándo se emitió el comando.
INTERFACE	Especifica la interfaz en la que se envió el sondeo.
PROBE	Especifica el identificador que representa el sondeo. Si se utiliza sondeo transitivo para la detección de fallos, el identificador tiene un prefijo <code>t</code> en el caso de los sondeos transitivos o un prefijo <code>i</code> en el caso de los sondeos ICMP.
NETRTT	Especifica el total de tiempo de recorrido de ida y vuelta en la red de la sonda; se mide en milisegundos. NETRTT cubre el tiempo entre el momento en que el módulo IP envía la sonda y el momento en que el módulo IP recibe los paquetes <code>ack</code> desde el destino. Si el daemon <code>in.mpathd</code> ha determinado que el sondeo está perdido, el campo estará vacío.
RTT	Especifica el total de recorrido de ida y vuelta del sondeo; se mide en milisegundos. RTT cubre el tiempo entre el momento en que el daemon ejecuta el código para enviar el sondeo y el momento en que el daemon termina de procesar los paquetes <code>ack</code> desde el destino. Si el daemon <code>in.mpathd</code> ha determinado que el sondeo está perdido, el campo estará vacío. Los picos que se producen en RTT que no están presentes en NETRTT podrían indicar que el sistema local está sobrecargado.
RTTAVG	Especifica el tiempo promedio de ida y vuelta del sondeo por la interfaz entre el sistema local y el destino. El tiempo de ida y vuelta promedio ayuda a identificar los destinos lentos. Si los datos no son suficientes para calcular el promedio, este campo estará vacío.
TARGET	Especifica el nombre del host <code>o</code> , si se utiliza la opción <code>-n</code> junto con <code>-p</code> , la dirección de destino a la que el sondeo se envía.

▼ Cómo personalizar la salida del comando `ipmpstat` en una secuencia de comandos

Cuando utiliza el comando `ipmpstat`, de manera predeterminada, se muestran los campos más significativos que entran en 80 columnas. En la salida, se muestran todos los campos que son específicos para la opción que se utilizan con el comando `ipmpstat`, excepto en el caso de la sintaxis `ipmpstat -p`. Si desea especificar los campos que se mostrarán, utilice la opción `-o` junto con otras opciones que determinan el modo de salida del comando. Esta opción es especialmente útil cuando se emite el comando desde una secuencia de comandos o mediante un alias de comando.

- **Para personalizar la salida, emita uno de los siguientes comandos:**

- Para mostrar los campos seleccionados del comando `ipmpstat`, utilice la opción `-o` junto con la opción de salida específica. Por ejemplo, para mostrar sólo los campos `GROUPNAME` y `STATE` del modo de salida de grupo, debe escribir lo siguiente:

```
$ ipmpstat -g -o groupname,state
```

```
GROUPNAME STATE
itops0      ok
accgt1      failed
field2      degraded
```

- Para mostrar todos los campos de un comando `ipmpstat` determinado, utilice la siguiente sintaxis:

```
# ipmpstat -o all
```

▼ **Cómo generar salidas analizables automáticamente del comando ipmpstat**

Puede generar información analizable automáticamente utilizando la sintaxis `ipmpstat -P`. La opción `-P` está diseñada para ser utilizada particularmente en las secuencias de comandos. La salida analizable automáticamente difiere de la salida normal de las siguientes formas:

- Las cabeceras se omiten.
- Los campos se separan con dos puntos (:).
- Los campos con valores vacíos están vacíos, en lugar de estar rellenos con el guión doble (--).
- En el caso de que se soliciten varios campos, si un campo contiene dos puntos (:) o barra invertida (\), se los puede evitar o excluir si se coloca antes una barra invertida (\).

Para usar correctamente la sintaxis `ipmpstat -P`, tenga en cuenta las siguientes reglas:

- Utilice `-o campos_opción` junto con la opción `-P`.
- Nunca utilice `-o all` con la opción `-P`.

Si ignora una de estas reglas, `ipmpstat -P` fallará.

- **Para mostrar el nombre del grupo en un formato analizable automáticamente, el tiempo de detección de fallos y las interfaces subyacentes, debe escribir lo siguiente:**

```
$ ipmpstat -P -o -g groupname,fdt,interfaces
itops0:10.00s:net0 net1
accgt1::[net3 net4]
field2:20.00s:net2 net7 (net5) [net6]
```

El nombre del grupo, el tiempo de detección de fallos y las interfaces subyacentes son campos de información de grupos. Por lo tanto, puede utilizar las opciones `-o -g` junto con la opción `-P`.

Ejemplo 15-8 Uso de `ipmpstat -P` en una secuencia de comandos

Esta secuencia de comandos de ejemplo muestra el tiempo de detección de fallos de un grupo IPMP determinado.

```
getfdt() {
    ipmpstat -gP -o group,fdt | while IFS=: read group fdt; do
        [[ "$group" = "$1" ]] && { echo "$fdt"; return; }
    done
}
```


Intercambio de información de conectividad de red con LLDP

En este capítulo, se describe cómo habilitar sistemas para intercambiar información sobre la conectividad de red y de sistemas en toda la red local mediante el protocolo de descubrimiento de capa de enlace (LLDP, Link Layer Discovery Protocol).

Descripción general de LLDP en Oracle Solaris

LLDP se utiliza para anunciar información en toda una red local con fines de detección de topología. Con este protocolo, un sistema puede anunciar la conectividad y la información de gestión para otros sistemas de la red. Esta información puede incluir las capacidades del sistema, las direcciones de gestión y otros aspectos relevantes. Este protocolo también habilita el mismo sistema para recibir información similar sobre otros sistemas que se encuentran en la misma red local.

En Oracle Solaris, el soporte para LLDP también incluye el puente del centro de datos (DCB, Data Center Bridging) para intercambiar información de configuración sobre las funciones de DCB, como el control de flujo basado en la prioridad (PFC, Priority-Based Flow Control) y el TLV de aplicación.

Con LLDP, el administrador del sistema puede detectar fácilmente las configuraciones del sistema que son defectuosas, especialmente en las redes complejas que incluyen redes de área local virtuales (VLAN), agregaciones de enlaces y otros tipos de enlaces.

Componentes de una implementación LLDP

LLDP se implementa con los siguientes componentes:

- El paquete LLDP debe estar instalado para que se habilite la función LLDP. Este paquete proporciona el daemon LLDP, las utilidades de la línea de comandos, las secuencias de comandos y el manifiesto de servicio, y otros componentes que son necesarios para que LLDP funcione.

- El servicio `lldpd` se habilita con el comando `svcadm`. Este servicio gestiona el daemon LLDP y es responsable de iniciar, detener, reiniciar y refrescar el daemon. El servicio está deshabilitado de manera predeterminada. Por lo tanto, para utilizar LLDP, primero se debe habilitar el servicio para el sistema de manera global. Una vez que se habilita el servicio `lldpd` y se inicia el daemon, se puede habilitar la funcionalidad LLDP en enlaces individuales, según lo que determine el administrador del sistema.
- El comando `lldpadm` administra LLDP en los enlaces individuales y se utiliza, por ejemplo, para configurar el modo de funcionamiento de LLDP, para especificar las unidades de tiempo-longitud-valor (TLV, Time-Length-Value) que se transmitirán y para configurar información de la aplicación DCB. Específicamente, el comando se utiliza para establecer las propiedades LLDP por agente y las propiedades LLDP globales. Los subcomandos generales del comando `lldpadm` son paralelos a los de los comandos `dladm` y `ipadm`.
 - El subcomando `lldpadm set -*` especifica la acción que se va a realizar en la que se definen uno o más valores en una propiedad LLDP determinada.
 - El subcomando `lldpadm show -*` muestra los valores que se establecen para una propiedad LLDP determinada.
 - El subcomando `lldpadm reset -*` restablece la configuración predeterminada de una propiedad LLDP especificada.

El uso de estos subcomandos se ilustra en las secciones subsiguientes. Para obtener más información sobre el comando `lldpadm`, consulte la página del comando [man lldpadm\(1M\)](#).

- La biblioteca LLDP (`liblldp.so`) proporciona las API que pueden utilizarse para recuperar información de LLDP en un enlace a fin de analizar los paquetes LLDP y ejecutar otras funciones.
- Los agentes LLDP son instancias LLDP que se asocian a las NIC físicas donde LLDP está habilitado. Un agente LLDP controla el comportamiento de LLDP en la NIC asociada. Los agentes LLDP pueden configurarse solamente en NIC físicas.
- El daemon LLDP (`lldpd`) funciona como gestor de los agentes LLDP en el sistema. También interactúa con `snmpd`, el daemon del protocolo simple de administración de red (SNMP, Simple Network Management Protocol), a fin de recuperar la información de LLDP que se recibe en el sistema mediante SNMP. Además, el daemon publica información de `sysevents` y responde a consultas de la biblioteca LLDP.

La siguiente sección describe los agentes LLDP de manera más detallada.

Funciones del agente LLDP

El agente LLDP transmite y recibe paquetes LLDP, que también se denominan *unidades de datos de protocolo (PDU, Protocol Data Units)*. El agente gestiona y almacena la información contenida en estos paquetes en dos tipos de almacenes de datos:

- Base de información de gestión local (MIB local). Este almacén de datos contiene información de red que pertenece al enlace específico en el que está habilitado el agente LLDP. Una MIB local contiene tanto información general como particular. Por ejemplo, el ID de chasis es información general que se comparte entre todos los agentes LLDP del sistema. Sin embargo, los números de puerto son diferentes para los enlaces de datos del sistema. Por lo tanto, cada agente gestiona su propia MIB local.
- MIB remota. La información de este almacén de datos pertenece a otros sistemas de la red local.

Configuración del modo de operación de los agentes LLDP

El agente LLDP se puede configurar para que opere en los siguientes modos:

- En el modo de transmisión únicamente (`txonly`), el agente no procesa paquetes entrantes LLDP. Por lo tanto, la MIB remota está vacía.
- En el modo de recepción únicamente (`rxonly`), el agente procesa solamente los paquetes LLDP entrantes y almacena la información en las MIB remotas. Sin embargo, no se transmite ninguna información de la MIB local.
- En el modo de transmisión y recepción (`both`), el agente envía y recibe paquetes LLDP. Ambos tipos de MIB se encuentran en uso de manera activa. Este modo también habilita automáticamente las funciones DCB admitidas por el enlace subyacente.
- En el modo de deshabilitación (`disable`), el agente no existe.

▼ Cómo habilitar LLDP

Este procedimiento permite habilitar LLDP en el sistema por primera vez.

1 Instale el paquete LLDP.

```
# pkg install lldp
```

Nota – Para obtener una descripción general de los paquetes de Oracle Solaris y su modo de instalación, consulte el [Capítulo 12, “Gestión de paquetes de software \(tarear\)”](#) de *Administración de Oracle Solaris: tareas comunes*.

2 Inicie el servicio LLDP en el sistema.

```
# svcadm enable svc:/network/lldp:default
```

3 Identifique el enlace de datos en el que desea habilitar LLDP.**4 Establezca el modo de operación para el agente LLDP del enlace de datos.**

```
# lldpadm set-agentprop -p mode=value agente
```

donde *valor* puede ser uno de los modos de operación, y *agente* utiliza el nombre del enlace de datos en el que LLDP está habilitado.

Nota – Los subcomandos del comando `lldpadm` se pueden escribir en su forma abreviada para facilitar el uso del comando. Por ejemplo, `lldpadm set-agentprop` se puede escribir como `lldpadm set-ap`. Consulte la página del comando `man lldpadm(1M)` para obtener los subcomandos y sus formas abreviadas.

5 Para confirmar el modo de operación de un agente LLDP, escriba el comando siguiente:

```
# lldpadm show-agentprop -p mode agente
```

6 Para deshabilitar un agente LLDP, utilice uno de los siguientes comandos:

- `lldpadm set-agentprop -p mode=disable agente`
- `lldpadm reset-agentprop -p mode agente`

7 Para deshabilitar LLDP en todo el sistema, escriba lo siguiente:

```
# svcadm disable svc:/network/lldp:default
```

Ejemplo 16–1 Habilitación de LLDP en varios enlaces de datos

En este ejemplo, un sistema tiene enlaces de datos, `net0` y `net1`, y el LLDP está habilitado en modos diferentes para cada agente LLDP. Un agente funciona tanto para transmitir como para recibir paquetes LLDP, mientras que el otro agente sólo transmite paquetes LLDP.

```
# svcadm enable svc:/network/lldp:default
# lldpadm set-agentprop -p mode=both net0
# lldpadm set-agentprop -p mode=txonly net1
```

Configuración de la información que se anunciará

El agente LLDP transmite información sobre el sistema y la conectividad en los paquetes LLDP o en las LLDPDU. Por ejemplo, los paquetes pueden contener unidades de información formateadas individualmente en TLV. Por lo tanto, las unidades de información también se

denominan unidades de TLV. Determinadas unidades de TLV son obligatorias y se incluyen en los paquetes LLDP de manera predeterminada cuando se habilita el LLDP. Las unidades de TLV obligatorias son las siguientes:

- ID de chasis
- ID de puerto
- TTL (tiempo de actividad)
- Final de PDU

El ID de chasis es la información que genera el comando `hostid` mientras el ID de puerto funciona como dirección MAC de la NIC física. Se pueden habilitar varios agentes LLDP en un único sistema en función del número de enlaces. El ID de chasis y el ID de puerto combinados identifican un agente de manera exclusiva y lo distinguen de los otros agentes del sistema.

No puede utilizar el comando `Udpadm` para excluir cualquiera de las unidades de TLV obligatorias de los paquetes LLDP.

Las unidades de TLV opcionales pueden agregarse a un paquete LLDP. Estas unidades de TLV opcionales son medios para que los proveedores inserten unidades de TLV específicas del proveedor para anunciarlas. Las unidades de TLV se identifican con identificadores únicos de organización individual (OUI, Individual Organization Unique Identifiers) y se escriben en función de si estos OUI son especificaciones IEEE 802.1 o especificaciones IEEE 802.3. Las propiedades del agente LLDP que corresponden a cada tipo TLV se crean para que se pueda definir la configuración para cada tipo.

La siguiente tabla muestra los tipos o grupos de TLV, sus nombres de propiedades correspondientes, las unidades de TLV de cada propiedad y sus descripciones.

TABLA 16-1 Unidades de TLV que pueden habilitarse para un agente LLDP

Tipo de TLV	Nombre de propiedad	TLV	Descripción
Gestión básica	<code>basic-tlv</code>	<code>sysname, portdesc, syscapab, sysdesc, mgmtaddr</code>	Especifica el nombre del sistema, la descripción del puerto, la capacidad del sistema, la descripción del sistema y la dirección de gestión que se anunciará
802.1 OUI	<code>dot1-tlv</code>	<code>vlanname, pvid, linkaggr, pfc, appln</code>	Especifica el nombre de la VLAN, el ID del puerto de la VLAN, la agregación de enlaces, la descripción del puerto y el TLV de aplicación que se anunciará

Tipo de TLV	Nombre de propiedad	TLV	Descripción
802.3 OUI	dot3-tlv	max-framesize	Especifica el tamaño máximo del marco que se anunciará
OUI específico de Oracle (definido como 0x0003BA)	virt-tlv	vnic	Especifica la VNIC que se anunciará si una red virtual está configurada

Debe configurar cualquiera de estas propiedades para especificar las unidades de TLV que se incluirán en los paquetes cuando se habilite el LLDP.

▼ Cómo especificar unidades de TLV para paquetes LLDP

Este procedimiento muestra cómo agregar una unidad TLV que se anunciará en el paquete LLDP. Para definir las unidades de TLV para los paquetes LLDP, utilice el subcomando `lldpdm set-agentprop`.

1 Si fuera necesario, identifique la propiedad del agente LLDP que pueda contener la unidad de TLV que desea agregar.

Este subcomando también muestra las unidades de TLV que ya se hayan establecido para cada propiedad.

```
# lldpdm show-agentprop agent
```

Sin especificar la propiedad, este subcomando muestra todas las propiedades del agente LLDP y sus valores de TLV.

2 Agregue la unidad TLV a la propiedad.

```
# lldpdm set-agentprop -p property[+|-]=value[,...] agent
```

Los calificadores `+` `|` `-` se utilizan para las propiedades que aceptan varios valores. Estos calificadores permiten agregar (`+`) o eliminar (`-`) los valores de la lista. Si no utiliza los calificadores, el valor que establece reemplaza todos los valores que se hayan definido previamente para la propiedad.

3 (Opcional) Muestre los nuevos valores para la propiedad.

```
# lldpdm show-agentprop -p property agent
```

Ejemplo 16-2 Cómo agregar unidades de TLV opcionales al paquete LLDP

En este ejemplo, el agente LLDP `net0` ya está configurado para anunciar información de la VLAN en el paquete. Se desea incluir las capacidades del sistema, la agregación de enlaces y la información de virtualización de redes para que también se anuncien. Sin embargo, se desea eliminar la descripción de la VLAN del paquete.

```

# lldpadm show-agentprop net0
# lldpadm set-agentprop -p dot1-tlv+=linkaggr net0
AGENT  PROPERTY  PERM  VALUE          DEFAULT  POSSIBLE
net0   mode       rw    both           disable  txonly,rxonly,both,
                                disable
net0   basic-tlv  rw    sysname,      none     none,portdesc,
                                sysname,sysdesc,
                                syscapab,mgmtaddr,
                                all
net0   dot1-tlv   rw    vllanname,    none     none,vllanname,pvid,
                                linkaggr,pfc,appln,
                                all
net0   dot3-tlv   rw    max-framesize none     none, max-framesize,
                                all
net0   virt-tlv   rw    none          none     none,vnic,all

# lldpadm set-agentprop -p basic-tlv+=syscapab,dot1-tlv+=linkaggr,virt-tlv=vnic net0
# lldpadm set-agentprop -p dot1-tlv-=pfc net0
# lldpadm show-agentprop -p net0
AGENT  PROPERTY  PERM  VALUE          DEFAULT  POSSIBLE
net0   mode       rw    both           disable  txonly,rxonly,both,
                                disable
net0   basic-tlv  rw    sysname,      none     none,portdesc,
                                sysname,sysdesc,
                                syscapab,mgmtaddr,
                                all
net0   dot1-tlv   rw    vllanname,    none     none,vllanname,pvid,
                                pvid,
                                linkaggr
                                all
net0   dot3-tlv   rw    max-framesize none     none, max-framesize,
                                all
net0   virt-tlv   rw    vnic          none     none,vnic,all

```

Gestión de las unidades de TLV

Cada unidad de TLV tiene propiedades que pueden configurarse aún más con valores específicos. Cuando la unidad de TLV está habilitada como propiedad de un agente LLDP, se anuncia en la red sólo con los valores especificados. Tenga en cuenta, por ejemplo, el valor de TLV `syscapab` que anuncia las capacidades del sistema. Estas capacidades pueden llegar a incluir soporte para enrutadores, puentes, repetidores, teléfonos y otros dispositivos. Sin embargo, puede configurar `syscapab` para que sólo se anuncien las capacidades que realmente se admiten en su sistema específico, como los enrutadores y los puentes.

El procedimiento de gestión de TLV depende de si se configuran TLV globales o TLV por agente.

Los *TLV globales* se aplican a todos los agentes LLDP en el sistema. La siguiente tabla muestra los valores de TLV globales y sus correspondientes configuraciones posibles.

TABLA 16-2 TLV globales y sus propiedades

Nombre de TLV	Nombre de propiedad de TLV	Posibles valores de propiedad	Descripción del valor
syscapab	supported	other, repeater, bridge, wlan-ap, router, telephone, docsis-cd, station, cvlan, sylvan, tpmr	Representan las principales funciones admitidas del sistema. Los valores predeterminados son router, station y bridge.
	enabled	Subconjunto de valores listados para supported	Representa las funciones habilitadas del sistema.
mgmtaddr	ipaddr	ipv4 o ipv6	Especifica el tipo de direcciones IP que se asociarán con el agente LLDP local. Las direcciones se utilizarán para alcanzar entidades de capas superiores y ayudará a efectuar el descubrimiento mediante la gestión de red. Se puede especificar solamente un tipo.

Las unidades de TLV que no pueden tener valores globales se gestionan en el nivel del agente LLDP. Con *las unidades de TLV por agente*, los valores que proporciona se utilizan cuando la unidad de TLV se encuentra habilitada para la transmisión por un determinado agente LLDP.

La siguiente tabla muestra los valores de TLV y sus correspondientes configuraciones posibles para un agente LLDP.

TABLA 16-3 Las unidades de TLV por agente y sus propiedades

Nombre de TLV	Nombre de propiedad de TLV	Posibles valores de propiedad	Descripción del valor
pfc	willing	on, off	Establece un agente LLDP para aceptar o rechazar la información de configuración de una máquina remota.

TABLA 16-3 Las unidades de TLV por agente y sus propiedades (Continuación)

Nombre de TLV	Nombre de propiedad de TLV	Posibles valores de propiedad	Descripción del valor
appLn	apt	Los valores se toman de la información que esté definida en la tabla de prioridad de aplicación.	Configura la tabla de prioridad de aplicación. Esta tabla contiene la lista de unidades de TLV de aplicación y sus correspondientes prioridades. La aplicación se identifica mediante el par <code>id/selector</code> . El contenido de la tabla utiliza el siguiente formato: <code>id/selector/priority</code>

El siguiente procedimiento muestra cómo definir los valores de TLV globales. Para obtener información sobre cómo definir las unidades de TLV por agente, consulte [“Establecimiento de puentes del centro de datos” en la página 334](#).

▼ Cómo definir los valores de TLV globales

Este procedimiento muestra cómo proporcionar los valores globales para unidades de TLV específicas. Para configurar valores de TLV globales, utilice el subcomando `lldpdm set-tlvprop`.

1 Configure la propiedad de TLV adecuada para contener los valores que desea anunciar.

Como referencia, consulte la [Tabla 16-2](#).

```
# lldpdm set-tlvprop -p tlv-property=value[,value,value,...] tlv
```

2 (Opcional) Muestre los valores de la propiedad que acaba de configurar.

```
# lldpdm show-tlvprop
```

Ejemplo 16-3 Cómo especificar las capacidades del sistema y la dirección IP de gestión

Este ejemplo cumple dos objetivos:

- Proporciona información específica sobre las capacidades del sistema que se deben anunciar en el paquete LLDP. Para alcanzar este objetivo, las propiedades `supported` y `enabled` de la unidad de TLV `sycapab` deben estar configuradas.
- Proporciona la dirección IP de gestión que se utiliza en el anuncio.

```
# lldpdm set-tlvprop -p supported=bridge,router,repeater sycapab
# lldpdm set-tlvprop -p enabled=router sycapab
# lldpdm set-tlvprop -p ipaddr=192.168.1.2 mgmtaddr
# lldpdm show-tlvprop
```

TLVNAME	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE
syscapab	supported	rw	bridge, router, repeater	bridge, router, station	other, router, repeater, bridge, wlan-ap, telephone, docis-cd, station, cvlan, svlan, tpmr
syscapab	enabled	rw	router	none	bridge, router, repeater
mgmtaddr	ipaddr	rw	192.162.1.2	none	--

Establecimiento de puentes del centro de datos

Para admitir el tráfico de canal de fibra por Ethernet (FCoE, Fibre Channel over Ethernet), la implementación de LLDP en Oracle Solaris admite el establecimiento de puentes del centro de datos (DCB, Data Center Bridging).

En las redes que utilizan Ethernet tradicional para el intercambio de tráfico, siempre existe el riesgo de que los paquetes se pierdan cuando la red está ocupada. Un requisito clave en el tráfico FCoE es que no se pierda ningún paquete durante la transmisión. Con la admisión de Data Center Bridging Exchange (DCBx), el control de flujo basado en la prioridad (PFC, Priority-Based Flow Control) de TLV y el TLV de aplicación se evita la pérdida de paquetes.

El PFC amplía el marco PAUSE estándar para incluir la información de prioridad para los paquetes. Normalmente, se envía un marco PAUSE en un enlace cuando el tráfico es muy pesado como para habilitar al receptor para que procese los paquetes que ya ha recibido. Con el PFC, en lugar de transmitir un marco PAUSE para detener todo el tráfico del enlace, el tráfico se pausa según las prioridades definidas para los paquetes. Un marco PFC puede enviarse para la prioridad para la que se debe detener el tráfico. El remitente detiene el tráfico para esa prioridad específica, mientras que el tráfico para otras prioridades no se ve afectado. Después de un tiempo especificado, se envía otro marco PFC a fin de señalar que el tráfico pausado se puede reanudar.

La información de configuración de PFC se intercambia entre estaciones iguales por medio de DCBx. Si los iguales de un intercambio de tráfico tienen configuraciones PFC coincidentes, el PFC puede pausar o reanudar la transmisión de tráfico según sea necesario. Para habilitar diferentes paquetes a los que se les asignarán diferentes prioridades, se usa el TLV de aplicación para definir información de prioridad. Si las configuraciones PFC de los iguales no coinciden, el PFC TLV se puede personalizar para aceptar la configuración del otro igual, como se muestra en el procedimiento que aparece a continuación.

El establecimiento de puentes del centro de datos es un caso específico que permite ilustrar cómo configurar unidades de TLV por agente, como se explica en [“Gestión de las unidades de TLV” en la página 331](#).

▼ Cómo establecer valores de TLV por agente

Este procedimiento muestra cómo establecer valores de TLV en el nivel de agente de LLDP con el subcomando `llpadm set-agenttlvprop`.

- 1 Configure la propiedad de TLV adecuada para contener los valores que desea anunciar mediante un agente LLDP determinado.

Para obtener referencias, consulte la [Tabla 16–3](#).

```
# lldpadm set-agenttlvprop -p tlv-property[+|-]=value[,value,value,...] -a agent tlv-name
```

- 2 (Opcional) Muestre los valores de la propiedad que acaba de configurar.

```
# lldpadm show-agenttlvprop
```

Ejemplo 16–4 Habilitación del agente LLDP para que acepte información y especificación de las prioridades de la aplicación de TLV

Este ejemplo muestra cómo se personalizan los valores de TLV pfc y appln. Las unidades de TLV de este ejemplo especifican cómo opera DCB para el tráfico FCoE. El sistema está configurado para aceptar la configuración PFC de iguales en caso de que la configuración local no coincida con la configuración del igual. El ejemplo muestra también cómo se establece la prioridad para el TLV de aplicación del agente LLDP.

```
# lldpadm set-agenttlvprop -p willing=on -a net0 pfc
# lldpadm set-agenttlvprop -p apt=8906/1/4 -a net0 appln
# lldpadm show-agenttlvprop
AGENT  TLVNAME  PROPERTY  PERM  VALUE      DEFAULT  POSSIBLE
net0   pfc       willing   rw    on         off      on,off
net0   appln     apt       rw    8906/1/4  --      --
```

Supervisión de agentes LLDP

El subcomando `lldpadm show-agent` muestra la información completa anunciada por un agente LLDP. En relación con un sistema determinado, el anuncio puede contener información acerca del sistema local que se transmite al resto de la red. También puede contener información que el sistema haya recibido de otros sistemas de la misma red.

▼ Cómo mostrar los anuncios

Este procedimiento enseña cómo mostrar la información que anuncia un agente LLDP. La información puede ser tanto local como remota. La información *local* viene del sistema local. La información *remota* se obtiene de otros sistemas de la red, que recibe el sistema local.

- Utilice el subcomando `lldpadm show-agent` con la opción adecuada para mostrar la información que desea.

- Para mostrar la información local que anuncia el agente LLDP, escriba el comando siguiente:

```
# lldpadm show-agent -l agent
```

- Para mostrar la información remota que recibe el agente LLDP, escriba el comando siguiente:


```
# lldpadm show-agent -r agent
```
- Para mostrar la información local o remota en detalle, escriba el comando siguiente:


```
# lldpadm show-agent -[l|r]v agent
```

Ejemplo 16–5 Cómo obtener información del agente LLDP que se anuncia

El ejemplo siguiente muestra cómo visualizar la información que anuncie un agente LLDP de manera local o remota. De manera predeterminada, la información se muestra de manera abreviada. Con la opción `-v`, puede obtener información detallada.

```
# lldpadm show-agent -l net0
AGENT CHASSISID PORTID
net0 004bb87f 00:14:4f:01:77:5d

# lldpadm show-agent -lv net0
Agent: net0
Chassis ID Subtype: Local(7)
Port ID Subtype: MacAddress(3)
Port ID: 00:14:4f:01:77:5d
Port Description: net0
Time to Live: 81 (seconds)
System Name: hosta.example.com
System Description: SunOS 5.11 dcb-clone-x-01-19-11 i86pc
Supported Capabilities: bridge,router
Enabled Capabilities: router
Management Address: 192.168.1.2
Maximum Frame Size: 3000
Port VLAN ID: --
VLAN Name/ID: vlan25/25
VNIC PortID/VLAN ID: 02:08:20:72:71:31
Aggregation Information: Capable, Not Aggregated
PFC Willing: --
PFC Cap: --
PFC MBC: --
PFC Enable: --
Application(s) (ID/Sel/Pri): --
Information Valid Until: 117 (seconds)

# lldpadm show-agent -r net0
AGENT SYSNAME CHASSISID PORTID
net0 hostb 0083b390 00:14:4f:01:59:ab

# lldpadm show-agent -rv net0
Agent: net0
Chassis ID Subtype: Local(7)
Port ID Subtype: MacAddress(3)
Port ID: 00:14:4f:01:59:ab
Port Description: net0
Time to Live: 121 (seconds)
System Name: hostb.example.com
System Description: SunOS 5.11 dcb-clone-x-01-19-11 i86pc
Supported Capabilities: bridge,router
Enabled Capabilities: router
```

```

Management Address: 192.168.1.3
Maximum Frame Size: 3000
Port VLAN ID: --
VLAN Name/ID: vlan25/25
VNIC PortID/VLAN ID: 02:08:20:72:71:31
Aggregation Information: Capable, Not Aggregated
PFC Willing: --
PFC Cap: --
PFC MBC: --
PFC Enable: --
Application(s) (ID/Sel/Pri): --
Information Valid Until: 117 (seconds)

```

▼ Cómo mostrar estadísticas LLDP

Puede mostrar las estadísticas LLDP para obtener información sobre los paquetes LLDP que anuncian el sistema local o los sistemas remotos. Las estadísticas se refieren a sucesos significativos que implican la transmisión y recepción de paquetes LLDP.

- 1 Para mostrar todas las estadísticas sobre transmisión y recepción de paquetes LLDP, utilice el siguiente comando:

```
# lldpadm show-agent -s agent
```

- 2 Para mostrar información sobre las estadísticas seleccionadas, utilice la opción `-o`.

```
# lldpadm show-agent -s -o field[,field,...]agent
```

donde *campo* hace referencia a cualquier nombre de campo en la salida del comando `show-agent -s`.

Ejemplo 16-6 Visualización de estadísticas de paquetes LLDP

En este ejemplo, se muestra cómo mostrar información sobre un anuncio de paquetes LLDP.

```
# lldpadm show-agent -s net0
AGENT IFRAMES IEER IDISCARD OFRAMES OLENERR TLVDISCARD TLVUNRECOG AGEOUT
net0      9      0      0      14      0      4      5      0
```

La salida del comando proporciona la siguiente información:

- AGENT especifica el nombre del agente LLDP, que es idéntico al enlace de datos en el que está habilitado el agente LLDP.
- IFRAMES, IEER y IDISCARD muestran información sobre los paquetes que se reciben, los paquetes entrantes con errores y los paquetes entrantes que se pierden.
- OFRAMES y OLENERR se refieren a los paquetes salientes y los paquetes que tienen errores de longitud.
- TLVDISCARD y TLVUNRECOG muestran información sobre las unidades de TLV que se desechan y las unidades de TLV que no se reconocen.

- AGEOUT hace referencia a los paquetes a los que se les agotó el tiempo de espera.

El ejemplo se indica que de los 9 marcos recibidos en el sistema, 5 TLV se reconocen, posiblemente porque no cumplen los estándares. El ejemplo también muestra que el sistema local transmitió 14 marcos a la red.

PARTE III

Virtualización de la red y gestión de los recursos

Introducción a la virtualización de redes y el control de recursos (descripción general)

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

- Virtualización de redes
- Tipos de redes virtuales
- Máquinas virtuales y zonas
- Control de recursos (incluida la gestión del flujo)
- Mejoras en la observación de las redes

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

Para realizar tareas específicas, consulte los siguientes capítulos:

- Capítulo 19, “Configuración de redes virtuales (tareas)”
- Capítulo 22, “Supervisión del tráfico de red y el uso de recursos”
- Capítulo 20, “Uso de la protección de enlaces en entornos virtualizados”
- Capítulo 21, “Gestión de recursos de red”

La virtualización de redes y las redes virtuales

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

El producto final de la virtualización de redes es la *red virtual*. Las redes virtuales se clasifican en dos clases principales: externas e internas. Las *redes virtuales externas* constan de varias redes locales que el software administra como una única entidad. Las partes que componen las redes

virtuales externas clásicas son el hardware de conmutación y la tecnología de software VLAN. Entre los ejemplos de redes virtuales externas, se incluyen las grandes redes corporativas y los centros de datos.

Las *redes virtuales internas* constan de un sistema que usa zonas o máquinas virtuales configuradas en, al menos, una pseudointerfaz de red. Estos contenedores pueden comunicarse entre sí como si estuvieran en la misma red local, por lo que proporcionan una red virtual en un único host. Las partes que componen la red virtual son las *tarjetas de interfaz de red virtual, o NIC virtuales (VNIC)*, y los conmutadores virtuales. La virtualización de red de Oracle Solaris proporciona una solución de redes virtuales internas.

Puede combinar los recursos de red para configurar tanto redes virtuales internas como externas. Por ejemplo, puede configurar los sistemas individuales con redes virtuales internas en las LAN que formen parte de una gran red virtual externa. Las configuraciones de red que se describen en esta parte incluyen ejemplos de redes virtuales internas y externas combinadas.

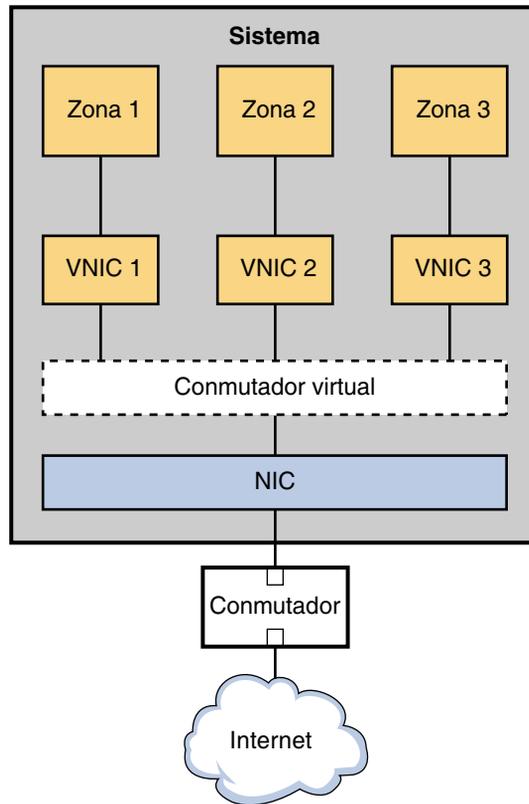
Partes de la red virtual interna

La red virtual interna incorporada en Oracle Solaris consta de las siguientes partes:

- Al menos una tarjeta de interfaz de red (NIC).
- Una NIC virtual (VNIC), que se haya configurado por encima de la interfaz de red.
- Un conmutador virtual, que se haya configurado al mismo tiempo que la primera VNIC en la interfaz.
- Un contenedor, como una zona o máquina virtual, que se haya configurado por encima de la VNIC.

En la figura siguiente, se muestran estas partes y se explica cómo se integran en un único sistema.

FIGURA 17-1 Configuración de la VNIC para una única interfaz



La figura muestra un único sistema con una NIC. La NIC está configurada con tres VNIC. Cada VNIC admite una sola zona. Por lo tanto, la zona 1, la zona 2 y la zona 3 se configuran en VNIC 1, VNIC 2 y VNIC 3, respectivamente. Las tres VNIC se conectan virtualmente a un conmutador virtual. Este conmutador proporciona la conexión entre las VNIC y la NIC física en la que se crean las VNIC. La interfaz física proporciona al sistema su conexión de red externa.

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

Las VNIC son dispositivos de redes virtuales que tienen la misma interfaz de enlace de datos como interfaz física. Las VNIC se configuran encima de una interfaz física. Para obtener la lista actual de interfaces físicas que admiten VNIC, consulte [las preguntas más frecuentes sobre virtualización de redes y control de recursos \(http://hub.opensolaris.org/bin/view/Project+crossbow/faq\)](http://hub.opensolaris.org/bin/view/Project+crossbow/faq). Se pueden configurar hasta 900 VNIC en una sola interfaz física. Cuando las VNIC se configuran, estas se comportan como NIC físicas. Además, los recursos del sistema tratan las VNIC como si fueran NIC físicas.

Cada VNIC se encuentra implícitamente conectada a un *conmutador virtual* que corresponde a la interfaz física. El conmutador virtual proporciona la misma conectividad entre las VNIC en una red que el hardware de conmutación proporciona para los sistemas conectados a los puertos del conmutador.

De acuerdo con el diseño de Ethernet, si un puerto del conmutador recibe un paquete saliente desde el host conectado a ese puerto, el paquete no puede acceder a un destino en el mismo puerto. Este diseño resulta inconveniente para los sistemas que están configurados con zonas o máquinas virtuales. Sin virtualización de redes, los paquetes salientes de una zona o máquina virtual con una pila exclusiva no se pueden pasar a otra máquina virtual o zona en el mismo sistema. Los paquetes salientes se envían a través de un puerto del conmutador hacia la red externa. Los paquetes entrantes no pueden alcanzar su zona o máquina virtual de destino porque los paquetes no pueden regresar a través del mismo puerto que se enviaron. Por lo tanto, cuando es necesario que se comuniquen las zonas y las máquinas virtuales en un mismo sistema, la ruta de los datos entre los contenedores debe abrirse en la máquina local. Los conmutadores virtuales proporcionan a estos contenedores el medio para transferir los paquetes.

¿Cómo se transfieren los datos mediante una red virtual?

La [Figura 17-1](#) ilustra una configuración de VNIC simple para una red virtual en un solo sistema.

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

Dadas las restricciones de Ethernet mencionadas anteriormente, ¿qué ocurre si una zona en una red virtual desea enviar paquetes a otra zona en la red virtual? Como se muestra en la [Figura 17-1](#), si, por ejemplo, la zona 1 necesita enviar tráfico en la zona 3, los paquetes se transfieren de la zona 1 mediante su VNIC 1 dedicada. Luego, el tráfico fluye por el conmutador virtual hasta la VNIC 3. A continuación, VNIC 3 transfiere el tráfico a la zona 3. El tráfico nunca deja el sistema y, por lo tanto, nunca infringe las restricciones de Ethernet.

¿Quién debería ejecutar redes virtuales?

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

- El hardware de NIC, incluidas las nuevas y poderosas interfaces que admiten anillos de hardware
- Varias direcciones MAC para las VNIC

- La gran cantidad de ancho de banda proporcionado por las interfaces más nuevas

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

¿Qué es el control de recursos?

El *control de recursos* es el proceso de asignación de los recursos del sistema de manera controlada. Las funciones de control de recursos de Oracle Solaris permiten que se comparta el ancho de banda entre las VNIC en la red virtual de un sistema. También puede utilizar funciones de control de recursos para asignar y gestionar el ancho de banda en una interfaz física sin VNIC ni máquinas virtuales. En esta sección, se presentan las principales funciones del control de recursos y se explica brevemente su funcionamiento.

Funcionamiento de la gestión del ancho de banda y del control del flujo

En [Searchnetworking.com](http://searchnetworking.techtarget.com) (<http://searchnetworking.techtarget.com>), se define el ancho de banda como "la cantidad de datos que se pueden transportar de un punto a otro en un período determinado (que suele ser un segundo)". La *gestión del ancho de banda* permite asignar una parte del ancho de banda disponible de una NIC física a un consumidor, como una aplicación o un cliente. Puede controlar el ancho de banda en función de las aplicaciones, los puertos, los protocolos o las direcciones. La gestión del ancho de banda garantiza el uso eficiente de la gran cantidad de ancho de banda disponible mediante las nuevas interfaces de red GLDv3.

Las funciones de control de recursos permiten implementar una serie de controles en el ancho de banda disponible de una interfaz. Por ejemplo, se puede establecer una *garantía* del ancho de banda de una interfaz para un consumidor en particular. Esa garantía será la cantidad mínima de ancho de banda que se asignará a la aplicación o la empresa. La cantidad asignada de ancho de banda se conoce como *recurso compartido*. Mediante la configuración de garantías, puede asignar suficiente ancho de banda para las aplicaciones que no funcionen correctamente sin una cierta cantidad de ancho de banda. Por ejemplo, los medios de transmisión por secuencias y la voz sobre IP consumen una gran cantidad de ancho de banda. Puede utilizar las funciones de control de recursos para garantizar que estas dos aplicaciones tengan suficiente ancho de banda para ejecutarse correctamente.

También puede establecer un *límite* para el recurso compartido. El límite es la asignación máxima de ancho de banda que el recurso compartido puede consumir. Mediante el uso de límites, se puede evitar que los servicios que no son críticos le saquen ancho de banda a los servicios críticos.

Por último, puede priorizar entre los varios recursos compartidos asignados a los consumidores. Puede asignar la máxima prioridad al tráfico crítico, como los paquetes de latidos para un clúster, y una menor prioridad a las aplicaciones que no son tan críticas.

Por ejemplo, los proveedores de servicios de aplicaciones (ASP, Application Service Providers) pueden ofrecer a los clientes niveles de servicio con distintos aranceles en función del recurso compartido de ancho de banda que el cliente compre. Mediante el acuerdo de nivel de servicios (SLA, Service Level Agreement), se garantiza una cantidad de ancho de banda para cada recurso compartido a fin de que no se supere el límite adquirido por el cliente. Para obtener más información sobre los acuerdos de nivel de servicio, consulte [“Utilización de acuerdos de nivel de servicio” de Administración de Oracle Solaris: servicios IP](#). Los controles de prioridad se pueden basar en los diferentes niveles del SLA o en los distintos precios que pagan los clientes del SLA.

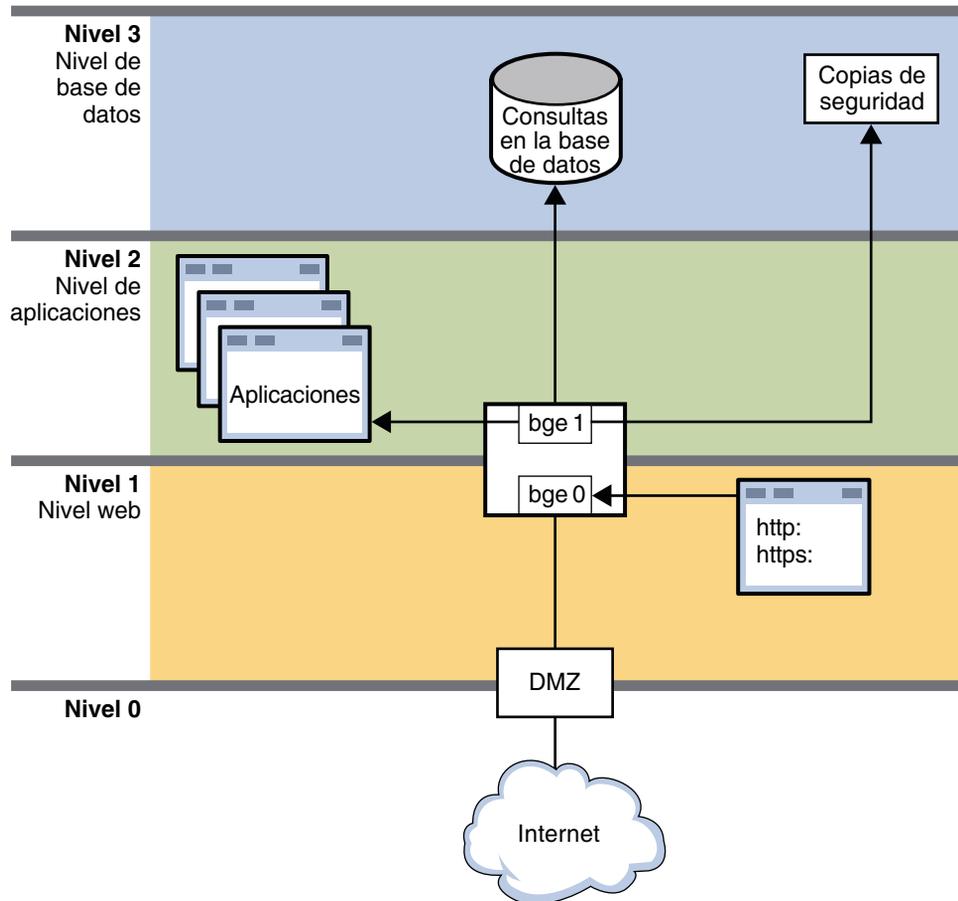
El uso del ancho de banda se controla mediante la gestión de flujo. El *flujo* es una secuencia de paquetes que tienen, todos, determinadas características, como el número de puerto o la dirección de destino. El flujo es gestionado por el transporte, el servicio o la máquina virtual, incluidas las zonas. El flujo no puede exceder la cantidad de ancho de banda que se garantiza para la aplicación o para el recurso compartido adquirido por el cliente.

Cuando se asigna una garantía a una VNIC o a un flujo, se asegura el ancho de banda asignado de la VNIC, incluso si otros flujos u otras VNIC también utilizan la interfaz. Sin embargo, las garantías asignadas se aplican solamente si no superan el ancho de banda máximo de la interfaz física.

Asignación de control de recursos y gestión del ancho de banda en una red

La siguiente figura muestra la topología de una red corporativa que utiliza el control de recursos para gestionar varias aplicaciones.

FIGURA 17-2 Red con los controles de recursos ubicados



Esta figura muestra una topología de red típica que utiliza controles de recursos para mejorar la eficacia y el rendimiento de la red. La red no implementa VNIC ni contenedores (como zonas y máquinas virtuales exclusivas). Sin embargo, las VNIC y los contenedores se podrían utilizar en esta red para la consolidación y otros propósitos.

La red se divide en cuatro niveles:

- El **Nivel 0** es una zona desmilitarizada (DMZ, Demilitarized Zone). Esta es una pequeña red local que controla el acceso desde y hacia el exterior. En los sistemas de la DMZ no se emplea el control de recursos.
- El **Nivel 1** es la capa web, que incluye dos sistemas. El primer sistema es un servidor proxy que efectúa el filtrado. Este servidor tiene dos interfaces: bge0 y bge1. El enlace bge0 conecta el servidor proxy con la DMZ en el Nivel 0. El enlace bge0 también conecta el servidor proxy con el segundo sistema, el servidor web. Los servicios de http y https comparten el ancho

de banda del servidor web con otras aplicaciones estándar. Debido al tamaño y al carácter crítico de los servidores web, los recursos compartidos de http y https exigen garantías y prioridad.

- El **Nivel 2** es la capa de aplicaciones, que también incluye dos sistemas. La segunda interfaz del servidor proxy, bge1, proporciona la conexión entre la capa web y la capa de aplicaciones. Mediante un conmutador, un servidor de aplicaciones se conecta a bge1 en el servidor proxy. El servidor de aplicaciones requiere el control de recursos para gestionar los recursos compartidos del ancho de banda asignado a las distintas aplicaciones que se ejecutan. Las aplicaciones críticas que necesitan un lote de ancho de banda deben tener mayores garantías y prioridades que las aplicaciones más pequeñas o menos críticas.
- El **Nivel 3** es la capa de base de datos. Los dos sistemas de esta capa se conectan con la interfaz bge1 del servidor proxy mediante un conmutador. El primer sistema, un servidor de base de datos, es necesario para emitir garantías y priorizar los distintos procesos que forman parte de las consultas de bases de datos. El segundo sistema es un servidor de copias de seguridad para la red. Este sistema probablemente consuma una gran cantidad de ancho de banda durante la creación de copias de seguridad. Sin embargo, estas actividades suelen llevarse a cabo durante la noche. Mediante los controles de recursos, puede controlar el momento en que los procesos de copias de seguridad tienen las mayores garantías de ancho de banda y las prioridades más altas.

¿Quién debería implementar las funciones de control de recursos?

Cualquier administrador de sistemas que desee mejorar la eficacia y el rendimiento de un sistema debería considerar la implementación de las funciones de control de recursos. Los consolidadores pueden delegar los recursos compartidos de ancho de banda en combinación con las VNIC para ayudar a equilibrar la carga de los servidores grandes. Los administradores de servidores pueden utilizar las funciones de asignación de recursos compartidos para implementar SLA, como los que ofrecen los ASP. Los administradores de sistemas tradicionales pueden utilizar las funciones de gestión de ancho de banda para aislar o priorizar determinadas aplicaciones. Por último, la asignación de recursos compartidos facilita la observación del uso del ancho de banda de los consumidores individuales.

Funciones de observación para la virtualización de redes y el control de recursos

La virtualización de redes y el control de recursos incluyen funciones de observación que ayudan a ver el uso de los recursos antes de configurar los controles como las VNIC y los flujos. En combinación con la contabilidad extendida de Oracle Solaris, las funciones de observación

del control de recursos permiten acumular registros con estadísticas del sistema. A continuación se mencionan las funciones de observación de la virtualización de redes y el control de recursos:

- Capacidad para controlar un sistema en ejecución.
- Capacidad para elaborar registros e informes con estadísticas.
- Funciones de contabilidad ampliadas que permiten registrar datos históricos.

El nuevo comando `flowadm` y las extensiones de los comandos `dladm` y `netstat` implementan las funciones de observación de la virtualización de redes. Puede utilizar estos comandos para controlar el uso actual del sistema y para recopilar datos estadísticos en registros.

Mediante el análisis de los registros históricos, puede determinar lo siguiente:

- Dónde se pueden consolidar los recursos de red, de muchos sistemas a un solo sistema, posiblemente con mayor ancho de banda, mediante la nueva generación de interfaces de red. Esto se debe realizar antes de configurar las VNIC y las zonas o máquinas virtuales exclusivas.
- Qué aplicaciones son las que consumen más ancho de banda. Esta información puede ayudar a configurar la gestión del ancho de banda para que las aplicaciones esenciales tengan garantizada la mayor cantidad de ancho de banda durante un período determinado. Por ejemplo, puede garantizar a una secuencia de vídeo la mayor cantidad del ancho de banda de una interfaz durante 20 h al día. Para un período designado de 4 h al día, puede otorgar la mayor prioridad al programa de copias de seguridad del sistema. Este paso debe ser parte de la implementación de la gestión del ancho de banda.
- Cuánto cobrar a los clientes por el ancho de banda que utilizan. Los proveedores de servicios de aplicaciones y otras empresas que alquilan espacio en un sistema pueden emplear las funciones de observación del control de recursos para determinar el uso de los clientes que compran el servicio. Algunas empresas ofrecen a los clientes acuerdos de nivel de servicio mediante los cuales se establece que el cliente compra un porcentaje de ancho de banda garantizado por el proveedor. Las funciones de observación le permiten ver la cantidad de ancho de banda que utiliza cada cliente para poder facturar aparte los posibles excesos de uso. Otras empresas ofrecen a los clientes un servicio de ancho de banda en función del uso. En este caso, las funciones de observación brindan una ayuda concreta en la facturación. Esto debe realizarse una vez implantado el control de recursos y, posiblemente, las VNIC y las máquinas virtuales en un sistema.

El siguiente capítulo, [Capítulo 18, “Planificación para la virtualización de red y el control de recursos”](#), contiene escenarios que muestran dónde se utilizan las funciones de observación para la consolidación de la planificación y el control de recursos.

Planificación para la virtualización de red y el control de recursos

Este capítulo contiene información y escenarios de ejemplo que lo ayudan a evaluar y a diseñar soluciones de virtualización de red y control de recursos para el sitio. El capítulo trata los siguientes escenarios:

- “Red virtual básica en un sistema único” en la página 352
- “Red privada virtual en un sistema único” en la página 354
- “Control de recursos basado en interfaz para una red tradicional” en la página 358

Cada escenario contiene sugerencias de “mejor uso” que explican los tipos de redes que más se benefician con un escenario determinado.

Mapa de tareas de virtualización de red y control de recursos

La siguiente tabla describe las tareas para configurar una red virtual e implementar controles de recursos en la red.

Tarea	Descripción	Para obtener instrucciones
Diseñar y planificar una red virtual en un host único	Consolida en un host único los servicios y las aplicaciones de red que ofrece la red local. Este escenario es especialmente útil para consolidadores y proveedores de servicios.	“Planificación y diseño de una red virtual” en la página 352
Diseñar y planificar una red virtual privada en un host único	Permite gestionar una red virtual que no permite acceso público. Este escenario es el recomendado para los administradores de sistemas que necesitan ejecutar un entorno de desarrollo.	“Red privada virtual en un sistema único” en la página 354

Tarea	Descripción	Para obtener instrucciones
Proporcionar gestión de ancho de banda y control de recursos para los sistemas por interfaz.	<p>Permite aislar, priorizar y asignar una cantidad específica ancho de banda de interfaz para tráfico de paquetes.</p> <p>Este escenario es útil para los sistemas que controlan un gran volumen de tráfico para servicios concretos, como un servicio web o un servidor de base de datos.</p>	<p>“Control de recursos basado en interfaz para una red tradicional” en la página 358</p>

Planificación y diseño de una red virtual

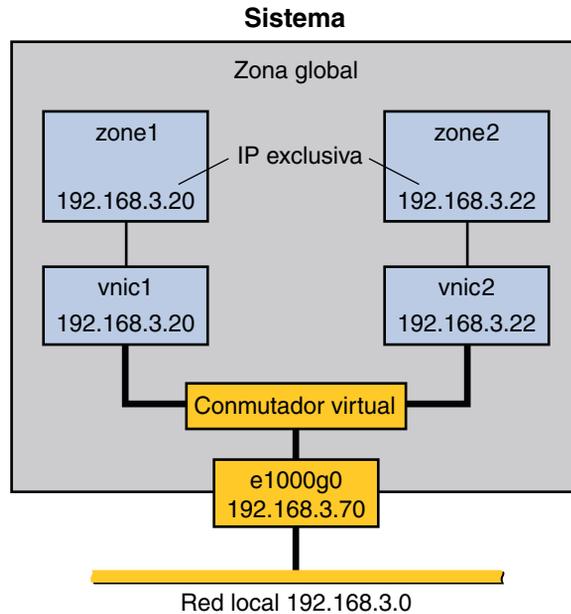
En esta sección se describen dos escenarios distintos para configurar una red virtual. Revise los escenarios para determinar qué es lo que más se ajusta a las necesidades de su sitio. A continuación, utilice ese escenario como base para diseñar su solución de virtualización específica. Los escenarios incluyen:

- Red virtual básica de dos zonas, especialmente útil para consolidar servicios de red de la red local en un host único.
- Red virtual privada, que resulta útil para un entorno de desarrollo en donde puede aislar las aplicaciones y los servicios de la red pública.

Red virtual básica en un sistema único

La [Figura 18–1](#) muestra la red virtual básica, o “red en una caja”, que se utiliza en ejemplos en toda la sección [“Configuración de componentes de virtualización de red en Oracle Solaris” en la página 364](#).

FIGURA 18-1 Red virtual en un host único



Esta red virtual consiste en lo siguiente:

- Una interfaz de red GLDv3 única e1000g0. Esta interfaz se conecta a la red pública 192.168.3.0/24. La interfaz e1000g0 tiene la dirección IP 192.168.3.70.
- Un conmutador virtual, que se configura automáticamente al crear la primera VNIC.
- Dos VNIC. vnic1 tiene la dirección IP 192.168.3.20 y vnic2 tiene la dirección IP 192.168.3.22.
- Dos zonas de IP exclusivas a las que se asignan las VNIC. vnic1 se asigna a zone1, y vnic2 se asigna a zone2.

Las VNIC y las zonas en esta configuración permiten el acceso al público. Por lo tanto, las zonas pueden pasar tráfico más allá de la interfaz e1000g0. Del mismo modo, los usuarios en las redes externas pueden alcanzar las aplicaciones y los servicios ofrecidos por las zonas.

Mejores usos para la red virtual básica

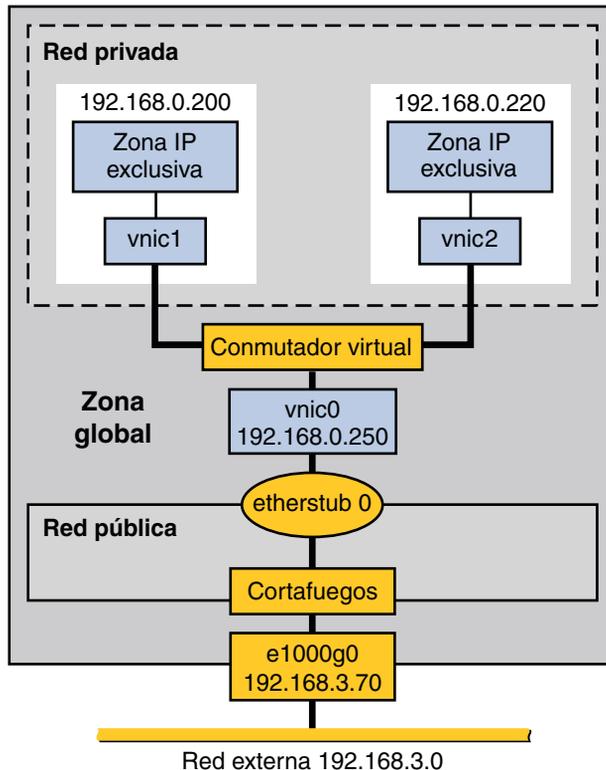
El escenario de red en una caja le permite aislar procesos y aplicaciones individuales en equipos virtuales individuales o zonas en un host único. Además, este escenario se puede ampliar para incluir varios contenedores, cada uno de los cuales con capacidad para ejecutar un conjunto de aplicaciones completamente aislado. El escenario mejora la eficiencia de un sistema y, por extensión, la eficiencia de la red local. Por lo tanto, este escenario es ideal para los siguientes usuarios:

- Consolidadores de red y otros que deseen consolidar los servicios de una LAN en un sistema único.
- Cualquier sitio que arriende servicios a los clientes. Puede arrendar equipos virtuales o zonas individuales, observar el tráfico y realizar estadísticas de medición de rendimiento o para fines de facturación en cada zona en la red virtual.
- Cualquier administrador que desee aislar los procesos y las aplicaciones para separar contenedores con el fin de mejorar el rendimiento del sistema.

Red privada virtual en un sistema único

La [Figura 18-2](#) muestra un sistema único con una red privada tras el software de filtro de paquetes que realiza la traducción de direcciones de red (NAT). En esta figura se muestra el escenario que está integrado en el [Ejemplo 19-5](#).

FIGURA 18-2 Red privada virtual en un host único



La topología presenta un sistema único con una red pública, incluido un cortafuegos, y una red privada en una pseudointerfaz etherstub. La red pública se ejecuta en la zona global y consta de los siguientes elementos:

- Interfaz de red GLDv3 e1000g0 con la dirección IP 192.168.3.70.
- Un cortafuegos implementado en el software de filtro IP. Para obtener una introducción a los filtros IP, consulte [“Introducción al filtro IP” de Administración de Oracle Solaris: servicios IP](#).
- etherstub0, una pseudointerfaz en la que se crea la topología de red virtual. *Etherstubs* proporciona la capacidad para crear una red virtual en un host. Dicha red está totalmente aislada de la red externa.

La red privada consta de los siguientes elementos:

- Un conmutador virtual que proporciona reenvío de paquetes entre las VNIC de la red privada.
- vnic0, que es la VNIC para la zona global, y tiene la dirección IP 192.168.0.250.
- vnic1 con la dirección IP 192.168.0.200 y vnic2 con la dirección IP 192.168.0.220. Las tres VNIC se configuran sobre etherstub0.
- vnic1 se asigna a zone1 y vnic2 se asigna a zone2.

Mejores usos para una red privada virtual

Considere la creación de una red privada virtual para un host que se utiliza en un entorno de desarrollo. Mediante la estructura etherstub, puede aislar totalmente un software o funciones en desarrollo de los contenedores de la red privada. Además, puede utilizar software de cortafuegos para la traducción de direcciones de red de los paquetes salientes que se originan desde los contenedores de la red privada. La red privada es una versión más pequeña del entorno de despliegue eventual.

Para obtener más información

- Para conocer los procedimientos que configuran una red virtual e implementan los escenarios que se describen en este capítulo, vaya a [“Creación de una red privada virtual” en la página 378](#).
- Para obtener información conceptual sobre VNIC y redes virtuales, vaya a [“La virtualización de redes y las redes virtuales” en la página 341](#).
- Para obtener información sobre las zonas, consulte el [Capítulo 15, “Introducción a Zonas de Oracle Solaris” de Administración de Oracle Solaris: zonas de Oracle Solaris 10 y gestión de recursos](#).
- Para obtener más información sobre los filtros IP, vaya a [“Introducción al filtro IP” de Administración de Oracle Solaris: servicios IP](#).

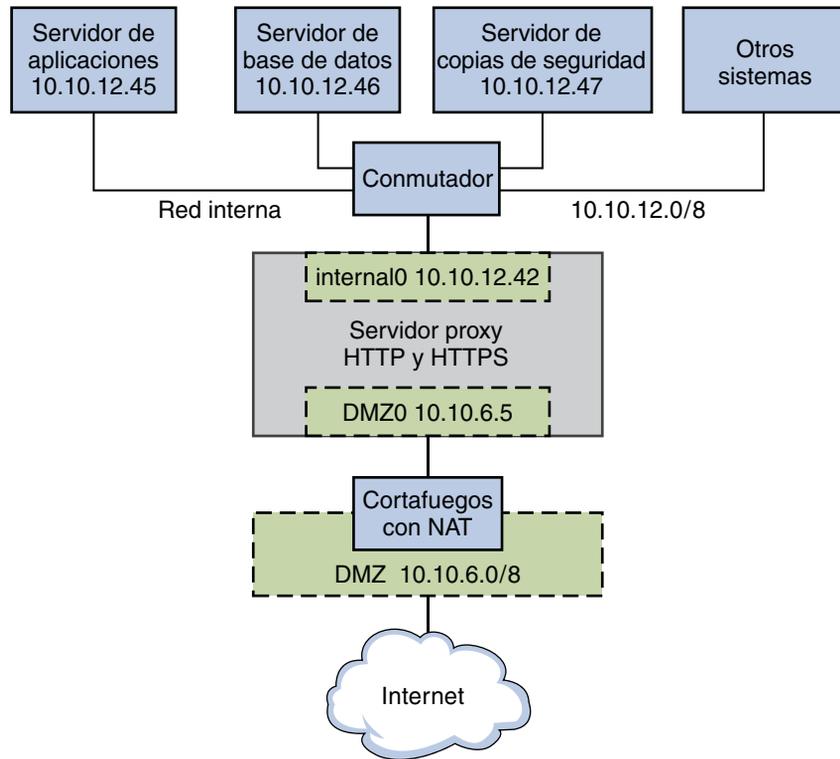
Aplicación de controles en los recursos de red

La virtualización de red le permite implementar su configuración de red de forma más eficaz a un precio más bajo mediante la construcción de una red en una caja. Para aumentar la eficacia, también puede implementar controles para determinar cómo los procesos de red utilizan los recursos. Las propiedades de enlace que se relacionan específicamente con recursos de red, como, anillos, CPU, etc., se pueden personalizar para procesar paquetes de red. Además, también puede crear flujos para gestionar el uso de la red. El control de recursos de red se examina en detalle en el [Capítulo 21, “Gestión de recursos de red”](#).

La [Figura 18–3](#) muestra la topología de red para una pequeña empresa que necesita gestionar el ancho de banda en su servidor proxy. El servidor proxy ofrece un sitio web público así como un proxy para clientes internos que necesitan servicios de distintos servidores de la red interna del sitio.

Nota – Este escenario no muestra cómo configurar el control de flujo para una red virtual y, en consecuencia, no incluye VNIC. Para el control de flujo en una red virtual, consulte [Control de flujo para una red virtual](#).

FIGURA 18-3 Control de recursos para un servidor proxy en una red tradicional



La figura muestra que la empresa tiene una red pública, $10.10.6.0/8$, que también sirve como zona desmilitarizada (DMZ). Un sistema en la DMZ proporciona traducción de nombre a dirección (NAT) a través de un cortafuegos de filtro IP. La empresa tiene un sistema grande que funciona como el servidor proxy. El sistema tiene dos interfaces con cables y 16 conjuntos de procesadores con identificadores del 0 al 16. Este sistema está conectado a la red pública a través de la interfaz `nge0`, con la dirección IP $10.10.6.5$. El nombre del enlace para la interfaz es `DMZ0`. A través `DMZ0`, el servidor proxy ofrece servicio HTTP y HTTPS a través del sitio web público de la empresa.

La figura también ilustra el red interna de la empresa, $10.10.12.0/24$. El servidor proxy se conecta a la red interna $10.10.12.0/8$ mediante la interfaz `nge1`, con la dirección IP $10.10.12.42$. El nombre del enlace para esta interfaz es `internal0`. A través del enlace de datos `internal0`, el servidor proxy funciona en nombre de clientes internos que solicitan los servicios de un servidor de aplicaciones, $10.10.12.45$, un servidor de base de datos, $10.10.12.46$ y un servidor de copia de seguridad, $10.10.12.47$.

Control de recursos basado en interfaz para una red tradicional

Mejor uso de control de recursos basados en interfaz en una red tradicional

Considere la posibilidad de establecer control de flujo para sistemas muy usados, especialmente para aquellos con las nuevas interfaces GLDv3 con grandes cantidades de ancho de banda disponible. El control de flujo basado en la interfaz mejora la efectividad de la interfaz, del sistema y, potencialmente, de la red. Puede aplicar control de flujo en cualquier sistema de cualquier tipo de red. Además, si su objetivo es mejorar la eficacia de la red, puede separar distintos servicios en flujos individuales. Esta acción asigna recursos de hardware y software independientes a los flujos individuales y, por lo tanto, los aísla de otros servicios en un sistema determinado. Después de establecer los flujos, puede observar el tráfico para cada flujo y recopilar estadísticas. A partir de ese momento, puede asignar la cantidad de ancho de banda y las prioridades para controlar el uso en las interfaces.

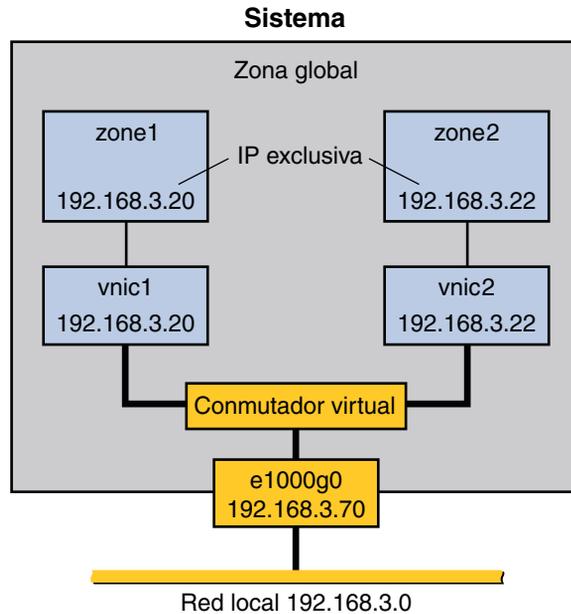
Para obtener más información

- Para conocer las tareas para implementar el control de flujo, consulte el [Capítulo 21, “Gestión de recursos de red”](#).
- Para obtener información conceptual sobre la gestión del ancho de banda y el control de recursos, consulte “¿Qué es el control de recursos?” en la [página 345](#).
- Para obtener información técnica detallada, consulte las páginas del comando `man dladm(1M)` y `flowadm(1M)`.

Control de flujo para la red virtual

Este escenario muestra cómo se utiliza el control de flujo en una red virtual, como la red virtual básica que se introduce en “[Red virtual básica en un sistema único](#)” en la [página 352](#).

FIGURA 18-4 Red virtual básica con control del flujo



La topología se describe en “Red virtual básica en un sistema único” en la página 352. Aquí un host tiene una interfaz de red, e1000g0, con dos VNIC, vnic1 y vnic2. zone1 se configura en vnic1, y zone2 se configura en vnic2. La gestión de recursos para la red virtual implica la creación de flujos según la VNIC. Estos flujos definen y aíslan los paquetes con características similares, tales como número de puerto o dirección IP del host de envío. Puede asignar ancho de banda según la política de uso para el sistema.

Otro uso común para los controles del flujo en el tráfico de VNIC es el de las empresas que arriendan zonas. Deberá crear diferentes acuerdos de nivel de servicio para los clientes, y arrendar zonas con una cantidad garantizada de ancho de banda. Al crear los flujos por zona, puede aislar y observar el tráfico de cada cliente y supervisar el uso del ancho de banda. Si el acuerdo de nivel de servicio se basa estrictamente en el uso, se pueden usar las funciones de estadísticas y de contabilidad para facturar a los clientes.

Los controles del flujo son eficaces para cualquier red que necesita gestión del ancho de banda para el tráfico por las zonas. Las organizaciones más grandes, como proveedores de servicios de aplicaciones (ASP) o proveedores de servicios de Internet (ISP), pueden aprovechar el control de recursos para VNIC para centros de datos y sistemas con varios procesadores. Las zonas individuales pueden ser arrendadas a los clientes para diferentes niveles de servicio. Por lo tanto, sería posible arrendar zone1 al precio estándar y ofrecer un ancho de banda estándar. Luego, podría alquilar zone2 con un precio premium y otorgar a ese cliente un nivel alto de ancho de banda.

▼ **Cómo crear una política de uso para las aplicaciones en una red virtual**

- 1 **Especifique las aplicaciones que desea ejecutar en el host.**
- 2 **Determine qué aplicaciones utilizan tradicionalmente el mayor ancho de banda o las que requieren más ancho de banda.**

Por ejemplo, la aplicación `telnet` podría no consumir grandes cantidades de ancho de banda en el sistema, pero podría ser muy usada. En cambio, las aplicaciones de base de datos consumen una gran cantidad de ancho de banda, pero es posible que sólo se las utilice de manera esporádica. Considere supervisar el tráfico de estas aplicaciones antes de asignarlos a las zonas. Puede utilizar la opción de estadísticas del comando `dladm show-link` para recopilar estadísticas, como se describe en [“Recopilación de estadísticas sobre el tráfico de red en enlaces” en la página 421.](#)

- 3 **Asigne estas aplicaciones a zonas separadas.**
- 4 **Cree flujos de cualquier aplicación que se ejecute en `zone1` cuyo tráfico desee aislar y controlar.**
- 5 **Asigne ancho de banda a los flujos en función de políticas de uso establecidas para el sitio.**

▼ **Cómo crear un acuerdo de nivel de servicio para la red virtual**

- 1 **Diseñe una política que ofrezca diferentes niveles de servicios a diferentes precios.**

Por ejemplo, puede crear niveles de servicio básicos, superiores y altos, y establecer el precio de cada nivel en consecuencia.

- 2 **Decida si desea cobrar a los clientes de manera mensual, por nivel de servicio o según el ancho de banda consumido.**

Si elige la última estructura de definición de precios, debe recopilar estadísticas de todos los usos del cliente.

- 3 **Cree una red virtual en un host, con los contenedores para cada cliente.**

Una forma muy común de implementación es darle a cada cliente su propio funcionamiento de zona en una VNIC.

- 4 **Cree flujos que aislen el tráfico para cada zona.**

Para aislar todo el tráfico de la zona, debe usar la dirección IP que se asigna a VNIC de la zona.

- 5 Asigne ancho de banda a cada VNIC en función del nivel de servicio adquirido por el cliente asignado a la zona de esa VNIC.**

Configuración de redes virtuales (tareas)

En este capítulo se incluyen tareas para configurar redes virtuales internas, o “redes en una caja”. Los siguientes son algunos de los temas que se tratan:

- “Mapa de tareas de redes virtuales” en la página 363
- “Configuración de componentes de virtualización de red en Oracle Solaris” en la página 364
- “Cómo trabajar con VNIC y zonas” en la página 369

Mapa de tareas de redes virtuales

En esta tabla se describen las tareas para configurar una red virtual y se incluyen enlaces a las tareas específicas. Tenga en cuenta que no todas las tareas se aplicarán al escenario de su red virtual.

Tarea	Descripción	Para obtener instrucciones
Crear VNIC en el sistema.	Cree una o varias interfaces de red virtual (VNIC). Las interfaces de red virtual son las pseudointerfaces sobre las que se crea la red virtual.	“Cómo crear una interfaz de red virtual” en la página 365
Crear etherstubs en el sistema.	Cree uno o varios etherstubs. Los etherstubs son conmutadores virtuales que permiten crear una red virtual privada aislada de la red más grande.	“Cómo crear etherstubs” en la página 367
Crear zonas para utilizar VNIC.	Cree VNIC y zonas nuevas, y configure ambas para crear una red virtual básica.	“Creación de zonas nuevas para utilizar con VNIC” en la página 369

Tarea	Descripción	Para obtener instrucciones
Modificar zonas para utilizar VNIC.	Cambie una zona existente para convertirla en una red virtual.	“Modificación de la configuración de zonas existentes para utilizar VNIC” en la página 374
Crear una red virtual privada.	Configure una red privada que esté aislada de la red mayor mediante etherstubs y VNIC.	“Creación de una red virtual privada” en la página 378
Eliminar VNIC.	Elimine las VNIC que se asignaron a una zona sin suprimir la zona.	“Cómo eliminar la red virtual sin eliminar las zonas” en la página 380

Configuración de componentes de virtualización de red en Oracle Solaris

En esta sección se incluyen tareas para configurar los elementos básicos de la virtualización de red en Oracle Solaris. Los siguientes son los componentes básicos:

- Tarjetas de interfaz de red virtual (VNIC)
- Etherstubs

Las *VNIC* son pseudointerfaces que se crean sobre los enlaces de datos. Una VNIC tiene una dirección MAC que se genera automáticamente. Según la interfaz de red en uso, puede asignar explícitamente a una VNIC una dirección MAC distinta de la dirección predeterminada, como se describe en la página del comando `man dladm(1M)`. Puede crear tantas VNIC sobre un enlace de datos como sea necesario.

Los *etherstubs* son pseudo NIC Ethernet que son gestionadas por el administrador del sistema. Puede crear VNIC sobre etherstubs en lugar de hacerlo sobre enlaces físicos. Las VNIC sobre un etherstub se independizan de las NIC físicas del sistema. Con etherstubs, puede construir una red virtual privada que esté aislada de las demás redes virtuales del sistema y de la red externa. Por ejemplo, desea crear un entorno de red cuyo acceso esté limitado únicamente a los desarrolladores de su empresa, y no a toda la red. Los etherstubs se pueden utilizar para crear este entorno.

Los etherstubs y las VNIC son sólo una parte de las funciones de virtualización de Oracle Solaris. Estos componentes se suelen utilizar junto con las zonas o los contenedores de Oracle Solaris. Mediante la asignación de VNIC o etherstubs para su uso en función de las zonas, puede crear una red en un único sistema.

▼ Cómo crear una interfaz de red virtual

Este procedimiento muestra cómo crear una tarjeta de interfaz de red virtual (VNIC).

1 Conviértase en administrador.

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

2 (Opcional) Para ver información sobre las interfaces físicas disponibles del sistema, escriba el comando siguiente:

```
# dladm show-phys
```

Este comando muestra las NIC físicas del sistema y los nombres de los enlaces de datos correspondientes. A menos que cree nombres personalizados para los enlaces de datos, el enlace de datos tiene el mismo nombre que el dispositivo de interfaz de red. Por ejemplo, el dispositivo `e1000g0` utilizará el nombre de enlace de datos `e1000g0` hasta que el nombre del enlace se sustituya por otro. Para obtener más información sobre nombres de enlaces de datos personalizados, consulte [“Dispositivos de red y nombres de enlaces de datos” en la página 26](#).

3 (Opcional) Para ver información sobre los enlaces de datos del sistema, escriba el comando siguiente:

```
# dladm show-link
```

Este comando muestra los enlaces de datos y su estado actual. Asegúrese de que el campo STATE del enlace de datos indique que el estado del enlace de datos es up. Puede configurar VNIC sólo mediante enlaces de datos con estado up.

4 (Opcional) Para ver información de dirección IP en interfaces configuradas, escriba el comando siguiente:

```
# ipadm show-addr
```

Este comando muestra las interfaces configuradas del sistema, incluidas las direcciones IP correspondientes.

5 Cree una VNIC mediante un enlace de datos.

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

- `enlace` es el nombre del enlace de datos mediante el que se configura la VNIC.
- `vnic` es la VNIC que puede etiquetar con un nombre personalizado, si lo desea.

6 Cree una interfaz IP de VNIC mediante el enlace.

```
# ipadm create-ip vnic
```

7 Configure la VNIC con una dirección IP válida.

Si asigna una dirección IP estática, utilice la siguiente sintaxis:

```
# ipadm create-addr -T static -a address addrobj
```

Donde *objeto_dirección* utiliza el formato de denominación *interfaz/cadena_definida_usuario*, como `e1000g0/v4globalz`. Para ver otras opciones para usar con este comando, consulte a la página del comando `man ipadm(1M)`.

- 8 Si está utilizando direcciones IP estáticas, agregue la información de dirección en el archivo `/etc/hosts`.
- 9 (Opcional) Para visualizar la configuración de direcciones de VNIC, escriba lo siguiente:

```
# ipadm show-addr
```
- 10 (Opcional) Para visualizar información sobre la VNIC, escriba lo siguiente:

```
# dladm show-vnic
```

Ejemplo 19-1 Creación de interfaces de red virtual

En este ejemplo se incluyen los comandos para crear VNIC. Debe iniciar sesión en el sistema como superusuario o el rol equivalente para ejecutar los comandos.

```
# dladm show-phys
LINK      MEDIA          STATE    SPEED DUPLEX    DEVICE
net0      Ethernet      up       1000 full    e1000g0
net1      Ethernet      unknown  0    half    e1000g1

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

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

# ipadm show-addr
ADDROBJ   TYPE      STATE    ADDR
lo0/?     static   ok       127.0.0.1/8
net0/v4addr static   ok       192.168.3.70/24

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

# dladm show-vnic
LINK      OVER          SPEED  MACADDRESS          MACADDRTYPE
vnic0     net0          1000 Mbps  2:8:20:c2:39:38    random
vnic1     net0          1000 Mbps  2:8:20:5f:84:ff    random
#
# ipadm create-ip vnic0
# ipadm create-ip vnic1

# ipadm create-addr -T static -a 192.168.3.80/24 vnic0/v4address
# ipadm create-addr -T static -a 192.168.3.85/24 vnic1/v4address
# ipadm show-addr
ADDROBJ   TYPE      STATE    ADDR
```

```

lo0/?          static    ok        127.0.0.1/8
net0/v4addr    static    ok        192.168.3.70/24
vnic0/v4address static    ok        192.168.3.80/24
vnic1/v4address static    ok        192.168.3.85/24

```

El archivo `/etc/hosts` del sistema debería contener información similar a la siguiente:

```

# cat /etc/hosts
#
::1          localhost
127.0.0.1    localhost
192.168.3.70 loghost    #For e1000g0
192.168.3.80 vnic1
192.168.3.85 vnic2

```

▼ Cómo crear etherstubs

Los etherstubs se utilizan para aislar la red virtual del resto de las redes virtuales del sistema y de la red externa a la que está conectado el sistema. No puede utilizar un etherstub sólo. En cambio, debe utilizar VNIC con un etherstub para crear las redes virtuales aisladas o privadas. Puede crear tantos etherstubs como sea necesario. También puede crear tantas VNIC mediante cada etherstub como sea necesario.

1 Conviértase en administrador.

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

2 Cree un etherstub.

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

3 Cree una VNIC mediante el etherstub.

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

4 Configure la VNIC con una dirección privada.

Nota – Para aislar la red para la que está configurando la VNIC mediante un etherstub, asegúrese de utilizar una dirección IP privada que no pueda ser reenviada por el enrutador predeterminado de la red externa. Por ejemplo, suponga que la interfaz física tiene una dirección `192.168.3.0/24` que indica que el sistema está en una red `192.168.3.x`. Por lo tanto, usted asigna otra dirección que es desconocida para el enrutador predeterminado, por ejemplo, `192.168.0.x`.

5 (Opcional) Para visualizar información sobre VNIC, escriba el siguiente comando.

```
# dladm show-vnic
```

Este comando muestra todas las VNIC del sistema y los enlaces de datos o los etherstubs mediante los que se crean las VNIC.

- 6 (Opcional) Para visualizar información sobre todos los enlaces físicos y virtuales del sistema, escriba el comando siguiente.**

```
# dladm show-link
```

Ejemplo 19-2 Creación de un etherstub

En el ejemplo siguiente se muestra cómo crear un etherstub y, luego, configurar una VNIC mediante el etherstub. En este ejemplo se desarrolla el ejemplo anterior agregando una tercera VNIC que se configura mediante el etherstub.

Debe iniciar sesión en el sistema como superusuario o un rol equivalente para ejecutar los siguientes comandos.

```
# dladm create-etherstub stub0
#
dladm show-vnic
LINK      OVER      SPEED  MACADDRESS      MACADDRTYPE
vnic1     net9      1000 Mbps  2:8:20:c2:39:38  random
vnic2     net0      1000 Mbps  2:8:20:5f:84:ff  random
#
# dladm create-vnic -l stub0 vnic3
# ipadm create-vnic vnic3
# ipadm create-addr -T static -a 192.168.0.10/24 vnic3/privaddr
#
# dladm show-vnic
LINK      OVER      SPEED  MACADDRESS      MACADDRTYPE
vnic1     net0      1000 Mbps  2:8:20:c2:39:38  random
vnic2     net0      1000 Mbps  2:8:20:5f:84:ff  random
vnic3     stub0     1000 Mbps  2:8:20:54:f4:74  random
#
# ipadm show-addr
ADDROBJ   TYPE      STATE   ADDR
lo0/?     static   ok      127.0.0.1/8
net0/v4addr  static   ok      192.168.3.70/24
vnic1/v4address  static   ok      192.168.3.80/24
vnic2/v4address  static   ok      192.168.3.85/24
vnic3/privaddr  static   ok      192.168.0.10/24
```

El archivo `/etc/hosts` del sistema debería contener información similar a la siguiente:

```
# cat /etc/hosts
#
::1       localhost
127.0.0.1 localhost
192.168.3.70 loghost #For e1000g0
192.168.3.80 vnic1
192.168.3.85 vnic2
192.168.0.10 vnic3
```

Cómo trabajar con VNIC y zonas

En esta sección se muestra cómo implementar los componentes de virtualización de red configurando estos componentes para que sean utilizados por las zonas. Esta sección proporciona dos métodos para trabajar con zonas para utilizar VNIC:

- Creación de zonas completamente nuevas y configuración de VNIC mediante estas zonas.
- Modificación de configuraciones de zonas existentes para utilizar VNIC.

Al iniciar sesión por primera vez en un sistema, se encuentra automáticamente en la *zona global*. Crea las VNIC en la zona global. A continuación, define otros valores de configuración para estas VNIC según si éstas serán utilizadas por la zona global o por zonas no globales exclusivas. Para obtener una introducción a las zonas, consulte [“Descripción general de las zonas” de Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#).

Creación de zonas nuevas para utilizar con VNIC

Utilice este método si no existen zonas configuradas en el sistema o si desea crear zonas nuevas para utilizar VNIC.

Para utilizar VNIC, se debe configurar una zona como zona de IP exclusiva. Los pasos que se indican a continuación permiten configurar zone1 con vnic1. Debe realizar los mismos pasos para configurar zone2. Para mayor claridad, los indicadores señalan en qué zona se ejecuta un comando específico. Sin embargo, la ruta real que muestran los indicadores puede variar según los valores de configuración del indicador del sistema específico.

▼ Cómo crear y configurar la zona de IP exclusiva

Al crear zonas, puede configurar varios parámetros. Los procedimientos relacionados con zonas incluidos en este capítulo se centran sólo en los parámetros que permiten que la zona funcione con VNIC. Para obtener información más detallada sobre la configuración de zonas, consulte la [Parte II, “Zonas de Oracle Solaris” de Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#).

Antes de empezar

Asegúrese de realizar, primero, lo siguiente:

- Crear las VNIC para las zonas, como se explicó en [“Cómo crear una interfaz de red virtual” en la página 365](#).
- Definir los nombres de zona.
- Determinar los directorios principales de las zonas.
- Determinar la VNIC específica que se asociará a una zona específica.
- Determinar las direcciones IP de las VNIC.

- Obtener otra información de red, como la dirección del enrutador para proporcionar a la zona.

1 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Para cada zona que cree, lleve a cabo los pasos siguientes.

a. Inicie la utilidad de configuración de zona y cree la zona.

```
global# zonecfg -z zone
zonecfg:zone> create
```

b. Establezca el directorio principal mediante la definición del parámetro zonepath.

```
zonecfg:zone> set zonepath=/home/export/zone
```

c. Habilite el inicio automático.

```
zonecfg:zone> set autoboot=true
```

d. Configure la zona para que sea una zona de IP exclusiva.

```
zonecfg:zone> set ip-type=exclusive
```

e. Establezca la interfaz de la zona para que sea una VNIC designada.

```
zonecfg:zone> add net
zonecfg:zone:net> set physical=vnic
zonecfg:zone:net> end
zonecfg:zone>
```

f. Verifique y confirme la configuración, y, a continuación, salga de la utilidad de configuración de zona.

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

g. (Opcional) Para verificar que la información de la zona es correcta, escriba lo siguiente:

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

Nota – Puede visualizar la misma información mientras se ejecuta la utilidad de configuración de zona escribiendo lo siguiente:

```
zonecfg:zone> info
```

3 Instale la zona.

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

Nota – El proceso de instalación puede tardar.

4 (Opcional) Una vez que la zona esté completamente instalada, compruebe el estado de la zona.

```
zoneadm list -iv
```

Nota – La opción `-iv` muestra todas las zonas configuradas, sin importar si se están ejecutando o no. En esta etapa, el estado de la zona que acaba de crear será “installed” en lugar de “running”. Si utiliza la opción `-v`, sólo se mostrarán las zonas que están en ejecución y se excluirá la zona que acaba de crear.

5 Inicie la zona.

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

6 (Opcional) Verifique que la zona se esté ejecutando.

```
global# zoneadm list -v
```

7 Después de que la zona se inicie por completo, conéctese a la consola de la zona.

```
# zlogin -C zone
```

8 Proporcione la información que se le solicita.

Parte de la información se relaciona con el tipo de terminal, la región, el idioma, etc. La mayor parte de la información se proporciona mediante la selección de una lista de opciones. Normalmente, las opciones predeterminadas son suficientes, a menos que la configuración del sistema requiera otra cosa.

La siguiente es información relacionada con el procedimiento actual que se debe proporcionar o verificar:

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

Una vez proporcionada la información necesaria para la zona, la zona se reinicia.

Ejemplo 19-3 Configuración de una red virtual básica mediante la creación de zonas y VNIC

En este ejemplo se fusionan todos los pasos que se proporcionaron anteriormente para la creación de zonas y VNIC a fin de configurar la red virtual. En este ejemplo se utiliza zone1 como la zona de ejemplo.

El ejemplo se basa en las siguientes suposiciones:

- VNIC: vnic1
- Nombre de zona: zone1
- Directorio principal de zona: /home/export/nombre_zona.
- Asignación de zona de VNIC: vnic1 para zone1
- Dirección IP: vnic1 utiliza 192.168.3.80
- Dirección IP de interfaz física: 192.168.3.70
- Dirección de enrutador: 192.168.3.25

```
global# dladm show-phys
LINK  MEDIA  STATE      SPEED  DUPLEX    DEVICE
net0  Ethernet up         1000   full    e1000g0
net1  Ethernet unknown    1000   full    bge0

global# dladm show-lnk
LINK  CLASS  MTU  STATE  BRIDGE  OVER
net0  phys   1500 up     --     --
net1  phys   1500 unknown --     --

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

global # ipadm show-addr
ADDROBJ  TYPE  STATE  ADDR
lo0/?    static ok      127.0.0.1/8
net0/v4addr static ok      192.168.3.70/24

global # dladm create-vnic -l net0 vnic1

global # dladm show-vnic
LINK  OVER  SPEED  MACADDRESS  MACADDRTYPE
vnic1 net0   1000 Mbps  2:8:20:5f:84:ff  random

global # ipadm create-ip vnic1
global # ipadm create-addr -T static -a 192.168.3.80/24 vnic1/v4address
global # ipadm show-addr
ADDROBJ  TYPE  STATE  ADDR
lo0/?    static ok      127.0.0.1/8
net0/v4addr static ok      192.168.3.70/24
vnic1/v4address static ok      192.168.3.80/24

global # cat /etc/hosts
::1      localhost
127.0.0.1 localhost
192.168.3.70 loghost #For net0
192.168.3.80 zone1 #using vnic1
```

```

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

zonecfg:zone1> info
zonename: zone1
zonepath: /export/home/zone1
brand:    native
autoboot: true
net:
    address not specified
    physical: vnic1

zonecfg:zone1> commit
zonecfg:zone1> exit
global#
global# zoneadm -z zone1 verify
WARNING: /export/home/zone1 does not exist, so it could not be verified.
When 'zoneadm install' is run, 'install' will try to create
/export/home/zone1, and 'verify' will be tried again,
but the 'verify' may fail if:
the parent directory of /export/home/zone1 is group- or other-writable
or
/export/home/zone1 overlaps with any other installed zones.

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

global# zoneadm list -iv
ID NAME      STATUS  PATH                                BRAND  IP
0  global     running /                                     native shared
-  zone1     installed /export/home/zone1                 native  excl

global# zoneadm -z zone1 boot
global# zoneadm list -v
ID NAME      STATUS  PATH                                BRAND  IP
0  global     running /                                     native shared
1  zone1     running /export/home/zone1                 native  excl

zlogin -C zone1
What type of terminal are you using?
.
.
.
8) Sun Workstation
9) Televideo 910
10) Televideo 925
11) Wyse Model 50

```

```
12) X Terminal Emulator (xterms)
13) CDE Terminal Emulator (dtterm)
14) Other
Type the number of your choice and press Return: 13
.
(More prompts)
..
```

Proporcione la información que se le solicita. Para obtener información de red, proporcione lo siguiente:

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

Pasos siguientes Puede utilizar varias herramientas para observar el tráfico de red y realizar estadísticas sobre el uso de la zona.

- Para verificar que la red se haya configurado correctamente, consulte el [Capítulo 5, “Administración de una red TCP/IP”](#) de *Administración de Oracle Solaris: servicios IP*.
- Para ver cómo observar el tráfico de la red, consulte “Control de transferencias de paquetes con el comando snoop” de *Administración de Oracle Solaris: servicios IP*.
- Para gestionar el modo en que la red utiliza los recursos del sistema, consulte el [Capítulo 21, “Gestión de recursos de red”](#).
- Para obtener estadísticas para fines contables, consulte el [Capítulo 22, “Supervisión del tráfico de red y el uso de recursos”](#).

Si necesita desensamblar la red virtual, consulte “Cómo eliminar la red virtual sin eliminar las zonas” en la [página 380](#).

Modificación de la configuración de zonas existentes para utilizar VNIC

Utilice este método si desea que las zonas existentes utilicen VNIC. En este caso, las zonas ya tienen nombres de zona y sus directorios principales o `zonepaths` ya están definidos.

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

Antes de empezar

Asegúrese de haber realizado lo siguiente:

- Crear las VNIC para las zonas, como se explicó en “[Cómo crear una interfaz de red virtual](#)” en la [página 365](#).
- Determinar la VNIC específica que se asociará a una zona específica.

- Determinar las direcciones IP de las VNIC.
- Obtener otra información de red, como la dirección del enrutador para proporcionar a la zona.

1 Conviértase en administrador.

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

2 Verifique que las zonas estén correctamente configuradas y en ejecución en el sistema.

```
global# zoneadm list -v
```

Nota – La opción `-v` muestra sólo las zonas que están en ejecución. Para ver una lista de todas las zonas configuradas incluidas las que no se han iniciado, utilice la opción `-iv`.

3 Realice los siguientes pasos en cada zona en que desee configurar VNIC:

a. Verifique la información sobre la zona.

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

Compruebe la información sobre el tipo de IP y la interfaz de red. La interfaz de red se designa mediante el parámetro *physical*. Para configurar una zona con una VNIC, la zona debe ser una zona de IP exclusiva y la interfaz de red debe especificar la VNIC.

b. Si es necesario, cambie la zona compartida por una zona de IP exclusiva.

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

c. Cambie la interfaz de la zona para utilizar una VNIC.

```
zonecfg:zone1> remove net physical=non-vnic-interface
zonecfg:zone1> add net
zonecfg:zone1:net> set physical=vnic
zonecfg:zone1:net> end
zonecfg:zone1>
```

d. Cambie otros valores de parámetros según corresponda.

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

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

f. Reinicie la zona.

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

- g. Una vez que se haya reiniciado la zona, verifique que la información de zona de `ip-type` y `physical` sea correcta.**

```
global# zonecfg -z zone info ip-type
global# zonecfg -z zone info net
```

La información debe mostrar que el tipo de IP de la zona es exclusiva y que utiliza la VNIC designada.

- 4 Inicie sesión en la zona.**

```
global# zlogin zone
```

- 5 Configure la VNIC con una dirección IP válida.**

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

```
zone# ipadm create-addr -T static -a address addrobj
```

Donde *dirección* puede utilizar la notación CIDR, mientras que *objeto_dirección* sigue la convención de denominación *interfaz/cadena_definida_usuario*.

- 6 (Opcional) Verifique la configuración de la interfaz en la zona.**

```
zone# ipadm show-if
```

o

```
zone# ipadm show-addr
```

Ejemplo 19-4 Configuración de una red virtual básica mediante la modificación de la configuración de una zona para que utilice VNIC

Este ejemplo utiliza el mismo sistema y se basa en las mismas suposiciones que el ejemplo anterior. Supongamos que en este sistema, `zone2` ya existe como una zona compartida. Desea modificar `zone2` para usar `vnic2`.

```
global# dladm show-link
LINK CLASS MTU STATE BRIDGE OVER
net0 phys 1500 up -- --
net1 phys 1500 unknown -- --
vnic1 vnic 1500 up -- e1000g0

global# ipadm show-if
IFNAME CLASS STATE ACTIVE OVER
lo0 loopback ok yes --
net0 ip ok yes --
vnic1 ip ok yes --

global # ipadm show-addr
ADDROBJ TYPE STATE ADDR
lo0/? static ok 127.0.0.1/8
net0/v4addr static ok 192.168.3.70/24
vnic1/v4address static ok 192.168.3.80/24
```

```

global # dladm create-vnic -l net0 vnic2
global # dladm show-vnic
LINK      OVER      SPEED      MACADDRESS      MACADDRTYPE
vnic1     net0      1000 Mbps  2:8:20:5f:84:ff  random
vnic2     net0      1000 Mbps  2:8:20:54:f4:74  random

```

```

global# zoneadm list -v
ID NAME      STATUS      PATH      BRAND      IP
0  global     running    /         native     shared
1  zone1     running    /export/home/zone1  native     excl
2  zone2     running    /export/home/zone2  native     shared

```

```

global# zonecfg -z zone2 info
zonename: zone2
zonepath: /export/home/zone2
brand: native
autoboot: true
bootargs:
pool: z2-pool
limitpriv:
scheduling-class:
ip-type: shared
hostid:
inherit-pkg-dir:
  dir: /lib
inherit-pkg-dir:
  dir: /platform
inherit-pkg-dir:
  dir: /sbin
inherit-pkg-dir:
  dir: /usr
inherit-pkg-dir:
  dir: /etc/crypto
net:
  address not specified
  physical: e1000g0
  defrouter not specified
global#

```

```

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

```

```

global# zonecfg -z zone2 info ip-type
ip-type: exclusive
global#

```

```

global# zonecfg -z zone2 info net
net:
  address ot specified
  physical: vnic2

```

```

defrouter not specified
global#

global# zlogin zone2
zone2# ipadm create-ip vnic2
zone2# ipadm create-addr -T static -a 192.168.3.85/24 vnic2/v4address

zone2# ipadm show-addr
ADDROBJ          TYPE      STATE      ADDR
lo0/v4           static    ok         127.0.0.1/8
vnic2/v4address  static    ok         192.168.3.85/24

zone1# exit
global#

global# vi /etc/hosts
#
::1              localhost
127.0.0.1        localhost
192.168.3.70     loghost      #For e1000g0
192.168.3.80     zone1        #using vnic1
192.168.3.85     zone2        #using vnic2

```

Pasos siguientes Puede modificar los valores de configuración de la red para personalizar el uso de los recursos del sistema, o usar diferentes herramientas para observar el tráfico de red y realizar estadísticas sobre el uso de los recursos.

- Para verificar que la red esté configurada correctamente, consulte
- Para observar el tráfico mediante la red, consulte
- Para gestionar la forma en que la red utiliza los recursos del sistema, consulte
- Para obtener estadísticas a efectos contables, consulte

Si necesita desensamblar la red virtual, consulte [“Cómo eliminar la red virtual sin eliminar las zonas” en la página 380](#)

Creación de una red virtual privada

En el ejemplo de esta sección se muestra cómo configurar una *red virtual privada* en un único sistema. Las redes virtuales privadas son diferentes de las redes privadas virtuales (VPN). El software de VPN crea un enlace punto a punto seguro entre dos sistemas de punto final. La red privada configurada mediante las tareas de esta sección es una red virtual en una caja a la que los sistemas externos no pueden acceder.

Para permitir que las zonas de la red privada envíen paquetes fuera del host, configure un dispositivo de traducción de direcciones de red (NAT). NAT convierte las direcciones IP privadas de la VNIC en direcciones IP enrutables de la interfaz de red física, pero sin exponer las direcciones IP privadas a la red externa. La configuración del enrutamiento también se incluye en el ejemplo siguiente.

EJEMPLO 19-5 Creación de la configuración de una red virtual privada

El siguiente ejemplo utiliza el mismo sistema y las mismas suposiciones que los ejemplos anteriores. En concreto, zone1 y zone2 ahora están configuradas como redes virtuales. Suponga que zone3 ya existe en el sistema. Va a modificar zone3 para convertirla en una red privada aislada del resto de la red. A continuación, configurará NAT y el reenvío de IP para permitir que la red privada virtual envíe paquetes fuera del host y oculte su dirección privada a la red externa.

```
global# dladm create-etherstub stub0

global# dladm create-vnic -l etherstub0 vnic3
global# dladm show-vnic
LINK      OVER      SPEED      MACADDRESS      MACADDRTYPE
vnic1     net0      1000 Mbps  2:8:20:5f:84:ff  random
vnic2     net0      1000 Mbps  2:8:20:54:f4:74  random
vnic3     stub0      0 Mbps    2:8:20:6b:8:ab   random
```

```
global# vi /etc/hosts
#
::1          localhost
127.0.0.1    localhost
192.168.3.70 loghost     #For e1000g0
192.168.3.80 zone1       #using vnic1
192.168.3.85 zone2       #using vnic2
```

En esta etapa, modifica zone3 para convertirla en una zona de IP exclusiva mediante vnic3.

```
global# zonecfg -z zone3
zonecfg:zone3> set ip-type=exclusive
zonecfg:zone3> remove net physical=e1000g0
zonecfg:zone3> add net
zonecfg:zone3:net> set physical=vnic3
zonecfg:zone3:net> end
zonecfg:zone3> vereify
zonecfg:zone3> commit
zonecfg:zone3> exit
global#

global# zonecfg -z zone3 info ip-type
ip-type: exclusive
global#

global# zonecfg -z zone3 info net
net:
    address ot specified
    physical: vnic3
    defrouter not specified
global#

global# zlogin zone3
zone3# ipadm create-ip vnic3
zone3# ipadm create-addr -T static -a 192.168.0.10/24 vnic3/privaddr

zone3# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4       static    ok         127.0.0.1/8
```

EJEMPLO 19-5 Creación de la configuración de una red virtual privada (Continuación)

```

vnic3/privaddr    static    ok          192.168.0.10/24
zone3# exit

global# ipadm show-addr
ADDROBJ          TYPE      STATE      ADDR
lo0/v4           static    ok         127.0.0.1/8
net0/v4addr      static    ok         192.168.3.70/24
vnic1/v4address  static    ok         192.168.3.80/24
vnic2/v4address  static    ok         192.168.3.85/24
vnic3/privaddr   static    ok         192.168.0.10/24

global# vi /etc/hosts
::1              localhost
127.0.0.1        localhost
192.168.3.70     loghost     #For e1000g0
192.168.3.80     zone1       #using vnic1
192.168.3.85     zone2       #using vnic2
192.168.0.10     zone3       #using vnic3

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

Routing services "route:default ripng:default"

global# ipadm set-ifprop -p forwarding=yes -m ipv4 e1000g0

global# vi /etc/ipf/ipnat.conf
map e1000g0 192.168.0.0/24 -> 0/32 portmap tcp/udp auto
map e1000g0 192.168.0.0/24 -> 0/32

global# svcadm enable network/ipfilter

global# zoneadm -z zone1 boot
global# zoneadm -z zone2 boot
global# zoneadm -z zone3 boot

```

▼ Cómo eliminar la red virtual sin eliminar las zonas

El siguiente procedimiento muestra cómo deshabilitar la red virtual de una zona y mantener la zona intacta.

Utilice este procedimiento si debe realizar cualquiera de las siguientes acciones:

- Utilizar las zonas que ya existen en una configuración diferente. Por ejemplo, es posible que necesite configurar las zonas como parte de una red privada que requiere que la zona se cree utilizando un etherstub.

- Migrar las zonas a otra red.
- Mover las zonas a una ruta de zona diferente.
- Clonar zonas, como se explica en “Clonación de una zona no global en el mismo sistema” de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

Antes de empezar Para realizar esta tarea, se supone que usted tiene una red virtual en ejecución que consta de zonas de IP exclusiva.

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Verifique el estado de las zonas configuradas actualmente.

```
# zoneadm list -v
```

Se visualiza información similar a la siguiente:

ID	NAME	STATUS	PATH	BRAND	IP
0	global	running	/	native	shared
1	zone1	running	/export/home/zone1	native	excl
2	zone2	running	/export/home/zone2	native	excl
3	zone3	running	/export/home/zone3	native	excl

3 Detenga las zonas de IP exclusiva de la red virtual.

Ejecute el siguiente comando por separado para cada zona que se detendrá.

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

Cuando se detiene la zona, se elimina el entorno de aplicación de la zona y se finalizan varias actividades del sistema, como se explica en “Cómo detener una zona” de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

4 Verifique que las zonas se hayan detenido.

```
# zoneadm list -iv
```

ID	NAME	STATUS	PATH	BRAND	IP
0	global	running	/	native	shared
-	zone1	installed	/export/home/zone1	native	excl
-	zone2	installed	/export/home/zone2	native	excl
-	zone3	installed	/export/home/zone3	native	excl

Observe que las zonas ya no están en ejecución, aunque permanecen instaladas. Para reiniciar una zona detenida, consulte “Cómo iniciar una zona” de *Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

5 Muestre las VNIC que se configuraron para las zonas detenidas.

```
# dladm show-vnic
```

LINK	OVER	SPEED	MACADDRESS	MACADDRTYPE
------	------	-------	------------	-------------

```
vnic1      net0      1000 Mbps  2:8:20:5f:84:ff  random
vnic2      net1      1000 Mbps  2:8:20:54:f4:74  random
vnic3      stub0     1000 MBps  2:8:20:c2:39:38  random
```

La salida muestra que las VNIC todavía están configuradas como enlaces de datos en la zona global. Sin embargo, las interfaces IP correspondientes se crearon y habilitaron en las zonas a las que estas VNIC están asociadas, y no en la zona global. Estas zonas no globales ahora están detenidas.

6 Suprima las VNIC.

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

Por ejemplo, para suprimir la VNIC en las zonas de la [Figura 18–1](#) debería escribir lo siguiente.

```
# dladm delete-vnic vnic1
# dladm delete-vnic vnic2
```

Uso de la protección de enlaces en entornos virtualizados

En este capítulo, se describe la protección de enlaces y el modo de configuración en los sistemas Oracle Solaris. En este capítulo se tratan los temas siguientes:

- “Descripción general de la protección de enlaces” en la página 383
- “Configuración de la protección de enlaces (mapa de tareas)” en la página 385

Descripción general de la protección de enlaces

Con la adopción cada vez más habitual de la virtualización en las configuraciones del sistema, el administrador del host puede dar a las máquinas virtuales (MV) de invitado acceso exclusivo a un enlace físico o virtual. Esta configuración mejora el rendimiento de la red porque permite aislar el tráfico de red del entorno virtual del tráfico general que se envía o recibe mediante el sistema host. Al mismo tiempo, esta configuración puede exponer el sistema y toda la red al riesgo de los paquetes peligrosos que podría generar un entorno de invitado.

La protección de enlaces ayuda a evitar el daño que puedan llegar a causar a la red las máquinas virtuales de invitado que sean maliciosas. Esta función ofrece protección contra las siguientes amenazas básicas:

- Falsificación de MAC e IP
- Falsificación de marco L2, como la unidad de datos de protocolo puente (BPDU, Bridge Protocol Data Unit)

Nota – La protección de enlaces no debe reemplazar la implementación de un cortafuegos, particularmente en las configuraciones con requisitos de filtrado más complejos.

Tipos de protección de enlaces

De manera predeterminada, el mecanismo de protección de enlaces viene deshabilitado. Para habilitar la protección de enlaces, especifique uno o más de los siguientes tipos de protección como valores de la propiedad de enlace `protection`:

- `mac-nospoof` Habilita la protección contra falsificación de MAC. La dirección MAC de origen de un paquete saliente debe coincidir con la dirección MAC configurada del enlace de datos. De lo contrario, el paquete se pierde. Si el enlace pertenece a una zona, la habilitación de `mac-nospoof` impide que el propietario de la zona modifique la dirección MAC del enlace.
- `ip-nospoof` Habilita la protección contra falsificación de IP. Cualquier paquete IP, ARP o NDP debe tener un campo de dirección que coincida con una dirección IP configurada con DHCP o una de las direcciones listadas en la propiedad de enlace `allowed-ips`. De lo contrario, el paquete se pierde.

La propiedad de enlace `allowed-ips` funciona con el tipo de protección `ip-nospoof`. De manera predeterminada, la lista especificada por esta propiedad está vacía. Si la propiedad está vacía o sin configurar, las siguientes direcciones IP se incluyen de manera implícita en la propiedad. Estas direcciones IP coinciden con la dirección IP de los paquetes salientes para determinar si los paquetes se transfieren o se pierden.

- Las direcciones IPv4 o IPv6 configuradas con DHCP configurado que se aprenden dinámicamente
- Las direcciones IPv6 locales de enlaces que cumplen con RFC 2464 y que se derivan de la dirección MAC del enlace

En la lista siguiente, se indica un protocolo y el correspondiente campo de la dirección asociada del paquete saliente que debe coincidir con una dirección de la propiedad `allowed-ips`. Si esta propiedad está vacía, la dirección del paquete debe coincidir con una dirección IP configurada con DHCP.

- IP (IPv4 o IPv6): dirección de origen del paquete
- ARP: dirección de protocolo del remitente del paquete

- `restricted` Restringe los paquetes salientes solamente a los paquetes de los tipos de protocolo IPv4, IPv6 y ARP. Los paquetes que no se incluyen en los tipos listados se pierden. Con este tipo de protección se impide que el enlace genere marcos de control L2 que puedan llegar a resultar perjudiciales.

Nota – El seguimiento de los paquetes que se pierden por la protección de enlaces se realizan mediante las siguientes estadísticas de núcleo: `mac_spoofed`, `ip_spoofed` y `restricted`. Estas estadísticas corresponden a los tres tipos protección. Utilice el comando `kstat` para recuperar estas estadísticas por enlace. Para obtener más información sobre la recuperación de estas estadísticas, consulte la página del comando `man kstat(1M)`.

Configuración de la protección de enlaces (mapa de tareas)

Para utilizar la protección de enlaces, utilice una de las opciones del comando `dladm` a fin de establecer las propiedades de enlace. Si el tipo de protección funciona con otros archivos de configuración, como `ip-nospoof` con `allowed-ips`, debe realizar dos acciones generales. Primero, debe habilitar la protección de enlaces. Luego, debe personalizar el archivo de configuración para determinar el modo de operación de la protección de enlaces.

Nota – Debe configurar la protección de enlaces en la zona global.

A continuación, se mencionan las tareas que se pueden utilizar para configurar la protección de enlaces en un servidor de Oracle Solaris.

Tarea	Descripción	Para obtener instrucciones
Habilitar el mecanismo de protección de enlaces.	Utilice el comando <code>dladm set-linkprop</code> para habilitar los tipos de protección de enlaces para un enlace.	“Cómo habilitar el mecanismo de protección de enlaces” en la página 386
Deshabilitar el mecanismo de protección de enlaces.	Utilice el comando <code>dladm reset-linkprop</code> para deshabilitar la protección de enlaces.	“Cómo deshabilitar la protección de enlaces” en la página 386
Personalizar el tipo de protección de enlaces IP.	Utilice el comando <code>dladm set-linkprop</code> para configurar o modificar los valores de la propiedad <code>allowed-ips</code> .	“Cómo especificar las direcciones IP para la protección contra la falsificación de IP” en la página 386
Ver la configuración de protección de enlaces.	Utilice el comando <code>dladm show-linkprop</code> para ver la configuración de protección de enlaces mediante la especificación de los nombres de las propiedades <code>protection</code> y <code>allowed-ips</code> .	“Cómo ver la configuración de protección de enlaces” en la página 387

▼ **Cómo habilitar el mecanismo de protección de enlaces**

Este procedimiento habilita uno o más de los siguientes tipos de protección de enlaces: `mac-nospoof`, `ip-nospoof` y `restricted`.

1 **Conviértase en administrador.**

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

2 **Habilite la protección de enlaces especificando uno o más tipos de protección.**

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

En el siguiente ejemplo, se habilitan los tres tipos de protección de enlaces en el enlace `vnic0`:

```
# dladm set-linkprop -p protection=mac-nospoof,ip-nospoof,restricted vnic0
```

▼ **Cómo deshabilitar la protección de enlaces**

Este procedimiento restablece la configuración predeterminada de la protección de enlaces, lo cual deshabilita la protección de enlaces.

1 **Conviértase en administrador.**

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

2 **Para deshabilitar la protección de enlaces, restablezca la configuración predeterminada de la propiedad `protection`.**

```
# dladm reset-linkprop -p protection link
```

▼ **Cómo especificar las direcciones IP para la protección contra la falsificación de IP**

Tenga en cuenta que la propiedad `allowed-ips` se utiliza solamente si la propiedad `protection` habilita el tipo de protección `ip-nospoof`.

1 **Conviértase en administrador.**

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

2 **Asegúrese de haber habilitado la protección contra la falsificación de IP.**

Si todavía no habilitó este tipo de protección de enlaces, emita el siguiente comando:

```
# dladm set-linkprop -p protection=ip-nospoof
```

3 Especifique una lista de direcciones IP como valores de la propiedad de enlace `allowed-ips`.

```
# dladm set-linkprop -p allowed-ips=IP-addr[,IP-addr,...] link
```

El ejemplo siguiente muestra cómo especificar las direcciones IP `10.0.0.1` y `10.0.0.2` como valores de la propiedad `allowed-ips` para el enlace `vnic0`:

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 vnic0
```

▼ Cómo ver la configuración de protección de enlaces

Los valores de las propiedades `protection` y `allowed-ips` indican cómo está configurada la protección de enlaces. Tenga en cuenta que la propiedad `allowed-ips` se utiliza solamente si la propiedad `protection` especifica el tipo de protección `ip-nospoof`.

1 Conviértase en administrador.

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

2 Vea los valores de propiedad de la protección de enlaces.

```
# dladm show-linkprop -p protection,allowed-ips link
```

En el siguiente ejemplo, se muestran los valores de las propiedades `protection` y `allowed-ips` del enlace `vnic0`:

```
# dladm show-linkprop -p protection,allowed-ips vnic0
```

LINK	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE
vnic0	protection	rw	ip-nospoof mac-nospoof restricted	--	--
vnic0	allowed-ips	rw	10.0.0.1, 10.0.0.2	--	--

Gestión de recursos de red

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

En este capítulo se tratan los temas siguientes:

- “Descripción general de la gestión de recursos de red” en la página 389
- “Gestión de recursos de red (mapa de tareas)” en la página 392
- “Gestión de recursos en enlaces de datos” en la página 393
- “Gestión de recursos en flujos” en la página 412

Descripción general de la gestión de recursos de red

En esta sección, se explica la gestión de recursos de red mediante la introducción de vías de red. También se describe cómo implementar la gestión de recursos de red mediante la definición de propiedades de enlaces de datos. Los flujos también se definen como otra manera de ajustar aún más la configuración de los controles de recursos para procesar el tráfico de la red.

Propiedades de enlaces de datos para el control de recursos

En las versiones anteriores de Oracle Solaris la implementación de la calidad de servicio es un proceso complicado. El proceso consiste en definir disciplinas de espera en cola, clases y reglas de filtro y en indicar relaciones entre todos estos componentes. Para obtener más información, consulte la [Parte V, “Calidad de servicio IP \(IPQoS\)” de *Administración de Oracle Solaris: servicios IP*](#).

En esta versión, la calidad del servicio se obtiene de manera más fácil y dinámica, mediante la gestión de recursos de red. La gestión de recursos de red incluye la configuración de las propiedades de enlaces de datos que pertenecen a los recursos de la red. Al establecer estas

propiedades, se determina qué parte de un determinado recurso se puede utilizar para procesos de red. Por ejemplo, un enlace se puede asociar a un número específico de CPU que se reservan exclusivamente para procesos de red. O bien, a un enlace se le puede asignar un ancho de banda determinado para procesar un tipo específico de tráfico de la red. Una vez que se define una propiedad de recurso, la nueva configuración se aplica inmediatamente. Este método permite la flexibilidad de la gestión de recursos. Puede definir propiedades de recursos al crear el enlace. Como alternativa, puede definir estas propiedades más tarde, por ejemplo, después de estudiar el uso de los recursos a lo largo del tiempo y de determinar la mejor manera de asignar mejor el recurso. Los procedimientos para asignar recursos se aplican tanto al entorno de red virtual como a las redes físicas tradicionales.

La gestión de recursos de red se puede comparar con la creación de vías de tráfico dedicadas. Al combinar distintos recursos para prestar servicio a tipos específicos de paquetes de red, esos recursos forman una *vía de red* para esos paquetes. Los recursos se pueden asignar de forma diferente para cada vía de red. Por ejemplo, puede asignar más recursos a una vía donde el tráfico de la red es más pesado. Al configurar las vías de red para que los recursos se distribuyan de acuerdo a las necesidades reales, se aumenta la eficiencia del sistema para procesar paquetes. Para obtener más información sobre vías de red, consulte [“Descripción general del flujo del tráfico de red” en la página 417](#).

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

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

Puede aislar, priorizar y controlar el tráfico de datos en un sistema individual, y realizar un seguimiento de éste, sin las definiciones de regla QoS complejas de las versiones anteriores.

Gestión de recursos de red mediante flujos

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

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

- Dirección IP
- Nombre del protocolo de transporte (UDP, TCP o SCTP)
- Número de puerto de aplicación, por ejemplo, el puerto 21 para FTP

- Atributo de campo DS, que se utiliza para la calidad de servicio en paquetes IPv6 únicamente. Para obtener más información sobre el campo DS, consulte [“Punto de código DS” de Administración de Oracle Solaris: servicios IP](#).

Un flujo se puede basar sólo en uno de los atributos de la lista. Por ejemplo, puede crear un flujo según el puerto que se esté utilizando, como el puerto 21 para FTP, o según las direcciones IP, como los paquetes de una dirección IP de origen específica. Sin embargo, no puede crear un flujo para los paquetes de una dirección IP especificada que se reciban en el puerto número 21 (FTP). Del mismo modo, no puede crear un flujo para todo el tráfico de la dirección IP 192 . 168 . 1 . 10 y, luego, crear un flujo para el tráfico de la capa de transporte en 192 . 168 . 1 . 10. Por lo tanto, puede configurar varios flujos en un sistema y hacer que cada flujo se base en un atributo diferente.

Comandos para la gestión de recursos de red

El comando para asignar recursos de red depende de si se trabaja directamente en enlaces de datos o en flujos.

- Para los enlaces de datos, utilice el subcomando `dladm` adecuado, según si está definiendo la propiedad al mismo tiempo que está creando el enlace o si está definiendo la propiedad de un enlace existente. Para crear un enlace y asignarle recursos simultáneamente, utilice la siguiente sintaxis:

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

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

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

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

Para obtener más detalles sobre el comando `dladm` y sobre las propiedades que gestiona este comando, consulte la página del comando `man dladm(1M)`.

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

- Ancho de banda: puede limitar el ancho de banda de un elemento de hardware para el uso de un enlace determinado.
- Anillos de NIC: si una NIC admite la asignación de anillos, sus anillos de transmisión y recepción se pueden asignar para el uso dedicado por parte de enlaces de datos. Los anillos de NIC se tratan en [“Anillos de transmisión y recepción” en la página 393](#).
- Agrupaciones de CPU: las agrupaciones de CPU se suelen crear y asociar con zonas específicas. Estas agrupaciones se pueden asignar a enlaces de datos para reservar los conjuntos de CPU para gestionar los procesos de red de las zonas asociadas. Las CPU y las agrupaciones se tratan en [“Agrupaciones y CPU” en la página 407](#).
- CPU: en un sistema con varias CPU, puede dedicar un número determinado de CPU para un procesamiento de red específico.

- Para flujos, utilice los subcomandos de `flowadm`. Primero, cree el flujo mediante el subcomando `flowadm add-flow`. A continuación, asigne recursos al flujo mediante el subcomando `flowadm set-flowprop`. El conjunto de atributos definidos que caracteriza los flujos y los une constituye la *política de control de flujo* del sistema.

Nota – Las propiedades de asignación de recursos que se pueden asignar a un flujo son las mismas que las propiedades que se asignan directamente a un enlace. Sin embargo, actualmente, sólo las propiedades de ancho de banda se pueden asociar a los flujos. Aunque los comandos para establecer propiedades para los enlaces de datos y para los flujos son diferentes, la sintaxis es similar. Para configurar las propiedades de ancho de banda, consulte los ejemplos que aparecen en [“Cómo configurar un flujo” en la página 413](#).

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

Gestión de recursos de red (mapa de tareas)

En la siguiente tabla se muestran diferentes métodos para establecer controles de recursos y determinar cómo estos recursos se asignan al procesamiento de red.

Tarea	Descripción	Para obtener instrucciones
Asignar anillos a clientes MAC.	Configure clientes MAC en un enlace de datos para utilizar anillos.	“Propiedades para la asignación de anillos” en la página 394
Asignar una agrupación de CPU a un enlace de datos.	Utilice la propiedad <code>pool</code> para asignar un conjunto de CPU para gestionar los procesos de red de una zona.	“Cómo configurar una agrupación de CPU para un enlace de datos” en la página 409
Asignar un conjunto de CPU a un enlace de datos definido.	En un sistema que tiene varias CPU, reserve un conjunto de CPU para fines relacionados con la red.	“Cómo asignar las CPU a los enlaces” en la página 411
Implementar la gestión de recursos de red mediante flujos en una red física.	Aísle el tráfico de la red en flujos individuales. A continuación, asigne a los flujos una cantidad fija de ancho de banda de interfaz entre otros flujos.	“Cómo configurar un flujo” en la página 413

Gestión de recursos en enlaces de datos

En esta sección, se describen las propiedades de enlace seleccionadas que se pueden definir para mejorar el rendimiento de la red para una red física o una red virtual.

Anillos de transmisión y recepción

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

Cientes MAC y asignación de anillos

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

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

Los clientes que no cumplen con ninguna de estas condiciones se denominan clientes MAC basados en el software.

A los clientes basados en hardware se les pueden asignar anillos para uso exclusivo en función de la NIC. Las NIC como `nxge` admiten la *asignación dinámica de anillos*. En estas NIC, puede configurar no sólo clientes basados en hardware. También tiene la flexibilidad para determinar el número de anillos para asignar a dichos clientes, suponiendo que los anillos siguen estando disponibles para la asignación. El uso de los anillos siempre se optimiza para la interfaz principal, por ejemplo, `nxge0`. La interfaz principal también se conoce como el *cliente principal*. Los anillos disponibles que no se han asignado para el uso exclusivo de otros clientes, se asignan automáticamente a la interfaz principal.

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

Asignación de anillos en VLAN

Con las VLAN, la asignación de anillos se lleva a cabo de forma diferente según cómo se haya creado la VLAN. Las VLAN se crean de una de estas dos maneras:

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

```
# dladm create-vlan -l link -v VID vlan
```
- Mediante el uso del subcomando `dladm create-vnic`:

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

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

Propiedades para la asignación de anillos

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

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

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

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

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

- `rxrings-available` y `txrings-available` indican el número de anillos de Rx y Tx que están disponibles para la asignación.

- `rxhwcnt-available` y `txhwcnt-available` indican el número clientes basados en hardware de Rx y Tx que se pueden configurar mediante una NIC.

Preparativos para la configuración de clientes basados en hardware

Antes de configurar clientes basados en hardware, debe conocer las capacidades de asignación de anillos de la NIC de su sistema. Para obtener la información necesaria, utilice el siguiente comando:

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

Donde *enlace* hace referencia al enlace de datos de la NIC específica.

Para mostrar las propiedades específicas, utilice el siguiente comando:

```
# dladm show-linkprop -p property[,property,...] link
```

Para configurar correctamente los clientes basados en hardware, debe determinar lo siguiente:

- Si la NIC admite clientes basados en hardware
 - Las propiedades `rxrings` y `txrings` de la salida del comando indican si una NIC admite clientes basados en hardware. De los mismos datos, también puede determinar el tipo de asignación de anillos que es compatible con la NIC.
- La disponibilidad de anillos para asignar a los clientes basados en hardware
 - Las propiedades `rxrings-available` y `txrings-available` de la salida del comando indican los anillos de Rx y de Tx disponibles que puede asignar a un cliente basado en hardware.
- La disponibilidad de clientes basados en hardware que puede configurar en el enlace
 - Los anillos se asignan como conjuntos. No hay una correspondencia de igual a igual entre el número de anillos disponibles y el número de clientes que pueden utilizar anillos dedicados. Por lo tanto, para asignar anillos, debe comprobar no sólo la disponibilidad de los anillos, sino también el número de clientes basados en hardware adicionales que todavía puede configurar para utilizar anillos dedicados. Puede asignar anillos sólo si hay anillos y clientes basados en hardware disponibles.
 - Las propiedades `rxhwcnt-available` y `txhwcnt-available` de la salida del comando indican cuántos clientes basados en hardware puede configurar que puedan utilizar anillos de Rx y de Tx dedicados.

Si la NIC admite la asignación de anillos, y los anillos y los clientes basados en hardware están disponibles, puede configurar este tipo de cliente en el sistema, como se explica en [“Cómo configurar un cliente basado en hardware” en la página 398](#). Como alternativa, en cambio, puede configurar un cliente basado en software, como se explica en [“Cómo crear un cliente basado en software” en la página 399](#).

En los ejemplos siguientes se muestra información diferente que se muestra para las propiedades de enlace relacionadas con anillos de una NIC `nxge`, una NIC `ixgbe` y una NIC `e1000g`.

EJEMPLO 21-1 Información de anillo de la NIC `nxge`

En el ejemplo siguiente se muestra la información de anillo de una NIC `nxge`.

```
# dladm show-linkprop nxge0
LINK      PROPERTY          PERM  VALUE  DEFAULT  POSSIBLE
...
nxge0    rxrings           rw    --    --       sw,<1-7>
...
nxge0    txrings           rw    --    --       sw,<1-7>
...
nxge0    rxrings-available r-    5     --       --
nxge0    txrings-available r-    5     --       --
nxge0    rxhwclnt-available r-    2     --       --
nxge0    txhwclnt-available r-    2     --       --
...
```

El campo `POSSIBLE` muestra `sw` y `<1-7>` como valores aceptables para las propiedades `rxrings` y `txrings`. Estos valores indican que `nxge` admite clientes basados en hardware y clientes basados en software. El rango `<1-7>` indica que el número de anillos de Rx o de Tx que se establece debe estar dentro del rango especificado. También puede deducir del rango que la NIC admite la asignación dinámica de anillos para la recepción y la transmisión.

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

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

EJEMPLO 21-2 Información de anillo de la NIC `ixgbe`

En el ejemplo siguiente se muestra la información de anillo de una NIC `ixgbe`.

```
# dladm show-linkprop ixgbe0
LINK      PROPERTY          PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings           rw    --    --       sw,hw
...
ixgbe0    txrings           rw    --    --       sw,hw,<1-7>
...
ixgbe0    rxrings-available r-    0     --       --
ixgbe0    txrings-available r-    5     --       --
ixgbe0    rxhwclnt-available r-    0     --       --
ixgbe0    txhwclnt-available r-    7     --       --
...
```

El campo `POSSIBLE` para las propiedades `rxrings` y `txrings` indica que se pueden configurar clientes basados en hardware y clientes basados en software en `ixgbe0`. Para los anillos de Rx

EJEMPLO 21-2 Información de anillo de la NIC ixgbe (Continuación)

sólo se admite la asignación estática de anillos, en la que el hardware asigna un conjunto fijo de anillos de Rx a cada cliente basado en hardware. Sin embargo, puede asignar los anillos de Tx dinámicamente, lo que significa que puede determinar el número de anillos de Tx que se pueden asignar a un cliente basado en hardware, en este ejemplo, hasta siete anillos.

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

Por último, en función de las propiedades `*hwcnt-available`, puede configurar siete clientes de Tx basados en hardware para utilizar anillos de Tx exclusivamente. Sin embargo, la asignación dinámica de anillos de Rx no se admite en las tarjetas ixgbe. Por lo tanto, no puede crear un cliente basado en hardware con un conjunto especificado de anillos de Rx dedicados.

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

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

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

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

```
# dladm show-linkprop ixgbe0
LINK      PROPERTY          PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings           rw    --    --        sw,hw
ixgbe0    txrings           rw    --    --        sw,hw,<1-7>
ixgbe0    rxrings-available r-    0     --        --
ixgbe0    txrings-available r-    0     --        --
...
```

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

EJEMPLO 21-3 Información de anillo de la NIC e1000g

En el ejemplo siguiente se muestra la información de anillo de una NIC `e1000g`.

EJEMPLO 21-3 Información de anillo de la NIC e1000g (Continuación)

```
# dladm show-linkprop e1000g0
LINK      PROPERTY          PERM  VALUE  DEFAULT  POSSIBLE
...
e1000g0   rxrings           rw    --    --    --
...
e1000g0   txrings           rw    --    --    --
...
e1000g0   rxrings-available r-    0     --    --
e1000g0   txrings-available r-    0     --    --
e1000g0   rxhwcCnt-available r-    0     --    --
e1000g0   txhwcCnt-available r-    0     --    --
...
```

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

▼ Cómo configurar un cliente basado en hardware

Este procedimiento muestra cómo configurar un cliente basado en hardware en una NIC que admite la asignación dinámica de anillos o en una NIC que admite la asignación estática de anillos.

Antes de empezar Asegúrese de contar con la siguiente información sobre la NIC de su sistema:

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

Para obtener información, consulte “Preparativos para la configuración de clientes basados en hardware” en la página 395.

1 Realice uno de los pasos siguientes según el tipo de asignación de anillos que admita su NIC:

- Si la NIC admite la asignación dinámica de anillos, utilice la siguiente sintaxis:

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

número Se refiere al número de anillos de Rx y de anillos de Tx que asigna al cliente. El número debe estar dentro del rango de del número de anillos disponibles para la asignación.

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

enlace Se refiere al enlace de datos mediante el que está creando el cliente.

vnic Se refiere al cliente que está configurando.

- Si la NIC admite la asignación estática de anillos, utilice la sintaxis siguiente:

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

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

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

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

▼ Cómo crear un cliente basado en software

Un cliente basado en software no tiene el uso exclusivo de los anillos. En cambio, el cliente comparte el uso de los anillos con el cliente principal o interactúa con otros clientes basados en software existentes. El recuento de anillos para los clientes basados en software depende del número de clientes basados en hardware existentes.

● Lleve a cabo uno de los pasos siguientes:

- Para crear un nuevo cliente basado en software, escriba el siguiente comando:

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

enlace Se refiere al enlace de datos mediante el que está creando el cliente.

vnic Se refiere al cliente que está configurando.

- Para configurar un cliente existente para compartir los anillos con otros clientes, escriba el comando siguiente:

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

Ejemplo 21–4 Configuración de clientes basados en hardware y clientes basados en software

En este ejemplo se muestra cómo configurar clientes basados en hardware y clientes basados en software en un sistema con una NIC ixgbe. Para mostrar cómo se implementa la asignación de anillos, el ejemplo se divide en partes. La información relacionada con el anillo se muestra y se explica en cada paso del proceso de configuración. La configuración se lleva a cabo de la siguiente manera:

1. Antes de configurar los clientes, visualice el uso de los anillos y los enlaces.
2. Configure el cliente principal.
3. Configure un cliente basado en software.

4. Configure otro cliente sin ningún anillo dedicado.
5. Asigne anillos de forma estática al cliente que acaba de configurar.
6. Configure un tercer cliente con anillos dedicados que se asignan dinámicamente.

En primer lugar, visualice los enlaces, el uso de los anillos y las propiedades relacionadas con los anillos.

```
# dladm show-link
LINK      CLASS  MTU    STATE   BRIDGE  OVER
ixgbe0    phys   1500   down    --      --

# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS  CLIENTS
ixgbe0    RX         0-1    <default,mcast>
ixgbe0    TX         0-7    <default>
ixgbe0    RX         2-3    --
ixgbe0    RX         4-5    --
ixgbe0    RX         6-7    --

# dladm show-linkprop ixgbe0
LINK      PROPERTY          PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings           rw    --     --       sw,hw
ixgbe0    rxrings-effective r     --     --       --
ixgbe0    txrings           rw    --     --       sw,hw,<1-7>
ixgbe0    txrings-effective r     --     --       --
ixgbe0    txrings-available r-    7     --     --
ixgbe0    rxrings-available r-    0     --     --
ixgbe0    rxhwclnt-available r-    3     --     --
ixgbe0    txhwclnt-available r-    7     --     --
...
```

La salida del comando muestra un único enlace `ixgbe0` en el sistema, pero no los clientes existentes. Además, de esta salida también se obtiene la siguiente información:

- La NIC tiene ocho anillos de Rx y ocho anillos de Tx (anillos de 0 a 7).
- Para los clientes basados en hardware, para los anillos de Rx sólo se admite la asignación estática de anillos, mientras que para los anillos de Tx se admiten las asignaciones tanto estáticas como dinámicas.
- Los clientes basados en software se pueden configurar para anillos de Rx y para anillos de Tx.
- Hay siete anillos de Tx, de 1 a 7, disponibles para ser asignados de forma dinámica a otros clientes (el anillo 0 normalmente se reserva para el cliente principal). No hay anillos de Rx disponibles porque no se admite la asignación dinámica de anillos para los anillos de Rx.
- Se pueden configurar tres clientes basados en hardware para utilizar anillos de Rx, mientras que se pueden configurar siete clientes basados en hardware para utilizar anillos de Tx.

Para obtener una explicación de las propiedades `*rings-effective`, consulte [“Cómo identificar asignaciones de anillos en la asignación estática de anillos” en la página 405](#).

A continuación, configure el cliente principal.

```
# ipadm create-ip ixgbe0
# ipadm create-addr -T static -a 192.168.10.10/24 ixgbe0/v4
# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS    CLIENTS
ixgbe0    RX        0-1      <default,mcast>
ixgbe0    TX        0-7      <default>ixgbe0
ixgbe0    RX        2-3      ixgbe0
ixgbe0    RX        4-5      --
ixgbe0    RX        6-7      --

# dladm show-linkprop ixgbe0
LINK      PROPERTY          PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings           rw    --    --        sw,hw
ixgbe0    rxrings-effective r     2     --    --
ixgbe0    txrings           rw    --    --        sw,hw,<1-7>
ixgbe0    txrings-effective r     8     --    --
ixgbe0    txrings-available r-    7     --    --
ixgbe0    rxrings-available r-    0     --    --
ixgbe0    rxhwclnt-available r-    3     --    --
ixgbe0    txhwclnt-available r-    7     --    --
...
```

La salida proporciona la siguiente información:

- ixgbe0, el cliente principal, recibe automáticamente dos anillos de Rx (los anillos 2 y 3) para uso dedicado. Sin embargo, ixgbe0 utiliza todos anillos de Tx. De manera predeterminada, todos los anillos no utilizados se asignan automáticamente al cliente principal.
- El número de anillos de Tx disponibles que se pueden asignar a otros clientes sigue siendo siete.
- El número de clientes basados en hardware disponibles que se pueden configurar con anillos de Rx sigue siendo tres. El número de clientes basados en hardware disponibles que se pueden configurar de forma dinámica con anillos de Tx sigue siendo siete.

A continuación, cree una VNIC como un cliente basado en software.

```
# dladm create-vnic -l ixgbe0 -p rxrings=sw,txrings=sw vnic0
# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS    CLIENTS
ixgbe0    RX        0-1      <default,mcast>,vnic0
ixgbe0    TX        0-7      <default>vnic0,ixgbe0
ixgbe0    RX        2-3      ixgbe0
ixgbe0    RX        4-5      --
ixgbe0    RX        6-7      --

# dladm show-linkprop vnic0
LINK      PROPERTY          PERM  VALUE  DEFAULT  POSSIBLE
...
vnic0     rxrings           rw    sw     --        sw,hw
...
vnic0     txrings           rw    sw     --        sw,hw,<1-7>
```

```

...
# dladm show-linkprop ixgbe0
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings       rw    --    --       --
ixgbe0    rxrings-effective  r     2     --       --
ixgbe0    txrings       rw    --    --       sw, hw, <1-7>
ixgbe0    txrings-effective  r     --    --       --
ixgbe0    txrings-available  r-    7     --       --
ixgbe0    rxrings-available  r-    0     --       --
ixgbe0    rxhwclnt-available  r-    3     --       --
ixgbe0    txhwclnt-available  r-    7     --       --
...

```

La salida proporciona la siguiente información:

- Como un cliente basado en software, `vnic0` se asigna automáticamente para utilizar los anillos de Rx 0 y 1. Otros clientes basados en software con anillos de Rx que se creen posteriormente se asignarán para utilizar este par de manera predeterminada. De manera predeterminada, a `vnic0` también se le asigna el uso de los ocho anillos de Tx (los anillos de 0 a 7). Otros clientes basados en software con anillos de Tx que se creen posteriormente se asignarán para utilizar este par de manera predeterminada.
- Como un cliente basado en software, las propiedades `rxrings` y `txrings` de `vnic0` se establecen de la manera correspondiente en `sw`.
- No se asignan anillos de Tx. Por lo tanto, el número de anillos de Tx disponibles que se pueden asignar a otros clientes sigue siendo siete.
- El número de clientes basados en hardware disponibles que se pueden configurar con anillos de Rx sigue siendo tres. El número de clientes basados en hardware disponibles que se pueden configurar con anillos de Tx sigue siendo siete.

A continuación, configure otro cliente sin ninguna asignación de anillo.

```

# dladm create-vnic -l ixgbe0 vnic1
# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS      CLIENTS
ixgbe0    RX        0-1        <default,mcast>,vnic0
ixgbe0    TX        0,2-7      <default>vnic0,ixgbe0
ixgbe0    RX        2-3        ixgbe0
ixgbe0    RX        4-5        vnic1
ixgbe0    RX        6-7        --
ixgbe0    TX        1          vnic1

# dladm show-linkprop vnic1
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
vnic1    rxrings       rw    --    --       sw, hw
vnic1    rxrings-effective  r-    2     --       --
vnic1    txrings       rw    --    --       sw, hw, <1-7>
vnic1    txrings-effective  r-    --    --       --
...

# dladm show-linkprop ixgbe0

```

LINK	PROPERTY	PERM	VALUE	DEFAULT	POSSIBLE
...					
ixgbe0	rxrings	rw	--	--	sw, hw
ixgbe0	rxrings-effective	r-	2	--	--
ixgbe0	txrings	rw	--	--	sw, hw, <1-7>
ixgbe0	txrings-effective	r-	--	--	--
ixgbe0	txrings-available	r-	7	--	--
ixgbe0	rxrings-available	r-	0	--	--
ixgbe0	rxhwcnt-available	r-	3	--	--
ixgbe0	txhwcnt-available	r-	7	--	--
...					

La salida proporciona la siguiente información:

- Cuando se admite la asignación de anillos, un cliente que está configurado se considera un cliente basado en hardware, aunque no se definan las propiedades `rxrings` y `txrings`. Por lo tanto, `vnic1` recibe automáticamente dos anillos de Rx dedicados (los anillos 4 y 5) para su uso. Del mismo modo, `vnic1` también recibe un anillo de Tx dedicado (el anillo 1).
- De los ocho anillos de Tx, `ixgbe0` y `vnic0` ahora comparten siete anillos (el anillo 0 y los anillos del 2 al 7). El anillo 1 se ha convertido en un anillo de Tx dedicado para `vnic1`.
- No se asignan anillos de Tx. Por lo tanto, el número de anillos de Tx disponibles que se pueden asignar a otros clientes sigue siendo siete.
- El número de clientes basados en hardware disponibles que se pueden configurar con anillos de Rx sigue siendo tres. El número de clientes basados en hardware disponibles que se pueden configurar con anillos de Tx sigue siendo siete.

A continuación, asigne anillos de manera estática al cliente que acaba de configurar, `vnic1`.

```
# dladm set-linkprop -p rxrings=hw,txrings=hw vnic1
# dladm show-phys -H ixgbe0
LINK    RINGTYPE  RINGS    CLIENTS
ixgbe0  RX        0-1      <default,mcast>,vnic0
ixgbe0  TX        0,2-7    <default>vnic0,ixgbe0
ixgbe0  RX        2-3      ixgbe0
ixgbe0  RX        4-5      vnic1
ixgbe0  RX        6-7      --
ixgbe0  TX        1        vnic1

# dladm show-linkprop vnic1
LINK    PROPERTY  PERM  VALUE  DEFAULT  POSSIBLE
...
vnic1  rxrings   rw    hw     --       sw, hw
vnic1  rxrings-effective r-    2     --       --
vnic1  txrings   rw    hw     --       sw, hw, <1-7>
vnic1  txrings-effective r-    --     --       --
...
# dladm show-linkprop ixgbe0
LINK    PROPERTY  PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0  rxrings   rw    --     --       sw, hw
ixgbe0  rxrings-effective r-    2     --       --
ixgbe0  txrings   rw    --     --       sw, hw, <1-7>
```

```

ixgbe0 txrings-effective r- -- -- --
ixgbe0 txrings-available r- 6 -- -- --
ixgbe0 rxrings-available r- 0 -- -- --
ixgbe0 rxhwcnt-available r- 3 -- -- --
ixgbe0 txhwcnt-available r- 6 -- -- --
...

```

La salida proporciona la siguiente información:

- La distribución de anillos de Rx y de Tx de vnic1 sigue siendo la misma que cuando se creó vnic1 sin asignación de anillos.
- De manera similar, la información de anillo sigue siendo la misma que cuando se creó vnic1 sin asignación de anillos.
- Las propiedades rxrings y txrings de vnic1 se definieron de manera explícita en hw. Por consiguiente, el número de anillos de Tx disponibles para la asignación dinámica se redujo a seis. Del mismo modo, el número de clientes basados en hardware disponibles que se pueden configurar se redujo a seis.

A continuación, configure un cliente basado en hardware con anillos de Tx asignados dinámicamente.

```

# dladm create-vnic -l ixgbe0 -p txrings=2 vnic2
# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS      CLIENTS
ixgbe0    RX         0-1        <default,mcast>,vnic0
ixgbe0    TX         0,4-7      <default>vnic0,ixgbe0
ixgbe0    RX         2-3        ixgbe0
ixgbe0    RX         4-5        vnic1
ixgbe0    RX         6-7        vnic2
ixgbe0    TX         1          vnic1
ixgbe0    TX         2-3        vnic2

# dladm show-linkprop vnic2
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
vnic2     rxrings        rw    --    --        sw,hw
vnic2     rxrings-effective r-    2    --        --
vnic2     txrings        rw    2    --        sw,hw,<1-7>
vnic2     txrings-effective r-    2    --        --
...

# dladm show-linkprop ixgbe0
LINK      PROPERTY      PERM  VALUE  DEFAULT  POSSIBLE
...
ixgbe0    rxrings        rw    --    --        sw,hw
ixgbe0    rxrings-effective r-    2    --        --
ixgbe0    txrings        rw    --    --        sw,hw,<1-7>
ixgbe0    txrings-effective r-    --    --        --
ixgbe0    txrings-available r-    4    --        --
ixgbe0    rxrings-available r-    0    --        --
ixgbe0    rxhwcnt-available r-    3    --        --
ixgbe0    txhwcnt-available r-    5    --        --
...

```

La salida proporciona la siguiente información:

- El hardware asignó automáticamente un par de anillos de Rx (los anillos 6 y 7) a `vnic2` para uso exclusivo. Sin embargo, los dos anillos de Tx dedicados de `vnic2` (los anillos 2 y 3) fueron asignados por el administrador.
- Como se asignaron administrativamente dos anillos de Tx a `vnic2`, el número de anillos de Tx que se pueden asignar a otros clientes se redujo a cuatro.
- Como `vnic2` se configuró como un cliente basado en hardware con dos anillos de Tx, el número de clientes disponibles que se pueden configurar se redujo a cinco.

▼ Cómo identificar asignaciones de anillos en la asignación estática de anillos

Al configurar un cliente basado en hardware con la asignación estática anillos, el hardware determina el número de anillos para asignar. Sin embargo, las propiedades `rxrings` y `txrings` se establecen en `hw` y no indican el número de anillos realmente asignados. En su lugar, el número se puede obtener activando las propiedades `rxrings-effective` y `txrings-effective`.

1 Configure un cliente basado en hardware con asignación estática de anillos realizando uno de los siguientes pasos:

- Para crear el cliente con asignación estática de anillos, escriba el comando siguiente:

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

enlace Se refiere al enlace de datos mediante el que está creando el cliente.

vnic Se refiere al cliente que está configurando.

- Para asignar estadísticamente anillos a un cliente existente, escriba el siguiente comando:

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

2 Para identificar el número de anillos que fueron asignados, realice los siguientes pasos secundarios:

a. Visualice las propiedades del cliente.

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

Donde *enlace* hace referencia al cliente basado en hardware o a la VNIC.

- b. Compruebe el valor de la propiedad `*rings-effective` que corresponde al tipo de anillo que asignó estáticamente.

Por ejemplo, si asignó anillos de Rx de manera estática, active la propiedad `rxrings-effective`. Si asignó anillos de Tx de manera estática, active la propiedad `txrings-effective`. El número indica la cantidad de anillos que fueron asignados por el hardware.

- 3 Para verificar qué anillos se asignaron de manera estática, realice los siguientes pasos secundarios:

- a. Visualice el uso del anillo de la NIC.

```
# dladm show-phys -H link
```

Donde *enlace* hace referencia al cliente principal.

- b. En la salida del comando, compruebe qué anillos de Rx o de Tx fueron asignados al cliente basado en hardware que configuró en el primer paso.

Ejemplo 21-5 Identificación de anillos asignados de manera estática

En este ejemplo se muestra cómo se asignaron anillos de Rx de forma estática a un cliente que está configurado mediante una NIC `ixgbe`. En esta NIC, sólo se admite la asignación estática de anillos de Rx. El ejemplo continúa de la siguiente manera:

1. Visualice los enlaces del sistema. En este ejemplo, el sistema sólo tiene un enlace, que es `ixgbe0`.
2. Cree `vnic1` como un cliente basado en hardware con anillos de Rx que se asignan de manera estática.
3. Visualice la información de anillo para conocer el número de anillos asignados por el hardware.
4. Visualice el uso del anillo para identificar qué anillos fueron asignados.

```
# dladm show-link
LINK      CLASS  MTU    STATE  BRIDGE  OVER
ixgbe0    phys   1500   down   --      --

# dladm create-vnic -l ixgbe0 -p rxrings=hw vnic1
# dladm show-linkprop vnic1
LINK      PROPERTY          PERM  VALUE  DEFAULT  POSSIBLE
...
vnic1     rxrings           rw    hw     --      sw, hw
vnic1     rxrings-effective r-    2      --      --
vnic1     txrings           rw    --     --      sw, hw, <1-7>
vnic1     txrings-effective r-    --     --      --

# dladm show-phys -H ixgbe0
LINK      RINGTYPE  RINGS  CLIENTS
```

```

ixgbe0  RX      0-1      <default,mcast>
ixgbe0  TX      0,2-7    <default>
ixgbe0  RX      2-3      vnic1
ixgbe0  RX      4-5      --
ixgbe0  RX      6-7      --
ixgbe0  TX      1        vnic1
...

```

La salida indica que, después de haber configurado `vnic1` con anillos de Rx, el hardware asignó dos anillos de Rx dedicados, como se refleja en la propiedad `rxrings-effective`. Según la salida del comando `dladm show-phys -H`, se dedicaron los anillos de Rx 2 y 3 para ser utilizados por `vnic1`.

Como resultado de haber sido configurado como cliente, `vnic1` también recibió automáticamente el anillo de Tx 1 para su uso dedicado. Sin embargo, la propiedad `txrings-effective` no muestra ningún valor porque la propiedad `txrings` no se estableció de manera explícita.

Agrupaciones y CPU

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

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

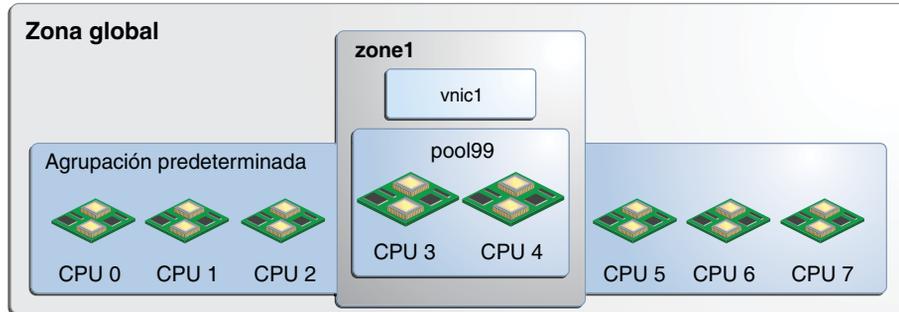
Nota – Una propiedad aparte, `cpu`, se puede establecer para asignar CPU específicas a un enlace de datos. Las dos propiedades, `cpu` y `pool`, son mutuamente excluyentes. No puede definir ambas propiedades para un enlace de datos determinado. Para asignar recursos de CPU a un enlace de datos mediante la propiedad `cpu`, consulte [“Cómo asignar las CPU a los enlaces” en la página 411](#).

Para obtener más información sobre agrupaciones dentro de una zona, consulte el [Capítulo 13, “Creación y administración de agrupaciones de recursos \(tareas\)” de Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#). Para obtener

más información sobre cómo crear agrupaciones y asignar conjuntos de CPU a las agrupaciones, consulte la página del comando `man poolcfg(1M)`.

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

FIGURA 21-1 Propiedad `pool` de una VNIC asignada a una zona

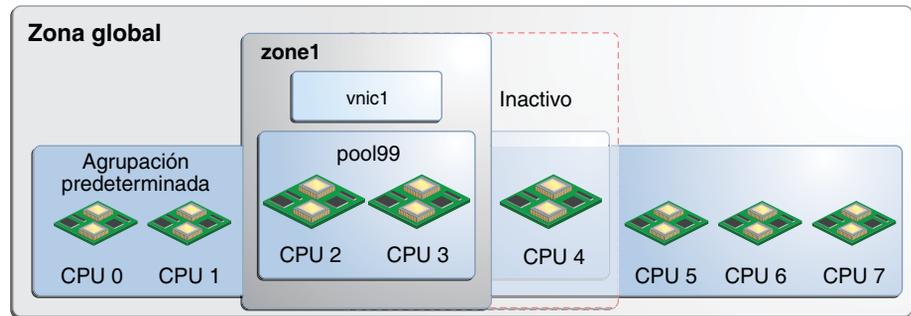


En la figura, el sistema tiene ocho CPU. Cuando no se configuran agrupaciones en el sistema, todas las CPU pertenecen a la *agrupación predeterminada* y son utilizadas por la zona global. Sin embargo, en este ejemplo, se creó la agrupación `pool99`, que está compuesta por CPU 3 y CPU 4. Esta agrupación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

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

Por ejemplo, suponga que en el sistema de la [Figura 21-1](#), se desconecta CPU 4. Como la propiedad `pool` es dinámica, el software automáticamente asocia una CPU adicional a la agrupación. Por lo tanto, se conserva la configuración original de dos CPU de la agrupación. Para `vnic1`, el cambio es transparente. En la siguiente figura, se muestra la configuración ajustada.

FIGURA 21-2 Reconfiguración automática de la propiedad pool



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

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

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

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

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

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

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

Establece la propiedad `pool` mientras crea la VNIC. Para establecer la propiedad `pool` de una VNIC existente, utilice la sintaxis siguiente:

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

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

Antes de empezar

Primero, debe realizar lo siguiente:

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

Nota – Para ver las instrucciones para completar estos requisitos previos, consulte [“Cómo modificar una configuración” de Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos.](#)

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

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

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

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

- Si la VNIC existe, utilice la sintaxis siguiente:

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

2 Establezca una zona para utilizar la VNIC.

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

Nota – Para ver todos los pasos que explican cómo asignar una interfaz de red a una zona, consulte [“Configuración, verificación y confirmación de una zona” de Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos.](#)

Ejemplo 21–6 Asignación de una agrupación de CPU de un enlace a una zona con un tipo de IP exclusiva

En este ejemplo se muestra cómo se asigna una agrupación al enlace de datos de una zona. El escenario se basa en la configuración en la [Figura 21–1](#). En el ejemplo, se presupone que una

agrupación de CPU denominada `pool99` ya fue configurada para la zona. La agrupación se asigna a una VNIC. Por último, la zona no global `zone1` se configura para usar la VNIC como la interfaz de red.

```
# dladm create-vnic -l e1000g0 -p pool99 vnic0

# zonecfg -c zone1
zonecfg:zone1> set ip-type=exclusive
zonecfg:zone1> add net
zonecfg:zone1>net> set physical=vnic0
zonecfg:zone1>net> end
zonecfg:zone1> exit
```

▼ Cómo asignar las CPU a los enlaces

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

1 Compruebe las asignaciones de CPU para la interfaz.

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

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

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

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

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

3 Asigne las CPU al enlace.

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

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

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

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

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

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

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

Ejemplo 21-7 Asignación de CPU a la interfaz

En este ejemplo se muestra cómo dedicar CPU específicas a la interfaz `internal0` en la [Figura 18-3](#).

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

- De manera predeterminada, `internal0` no tiene CPU dedicada. Por lo tanto `VALUE` es `--`.
- La interrupción de `internal0` está asociada a la CPU 18.
- Después de que se asignan las CPU, `internal0` muestra una nueva lista de CPU en `VALUE`.

```
# dladm show-linkprop -p cpus internal0
LINK          PROPERTY    PERM    VALUE    DEFAULT    POSSIBLE
internal0     cpus       rw      --       --         --

# echo ::interrupts | mdb -k
  Device  Shared  Type  MSG #   State  INO   Mondo  Pil  CPU
external#0  no     MSI   3     enbl   0x1b  0x1b   6    0
internal#0  no     MSI   2     enbl   0x1a  0x1a   6    18

# dladm set-linkprop -p cpus=14,18,19,20 internal0

# dladm show-linkprop -p cpus internal0
LINK          PROPERTY    PERM    VALUE    DEFAULT    POSSIBLE
internal0     cpus       rw      14,18,19,20  --         --
```

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

Gestión de recursos en flujos

Los flujos están compuestos por paquetes de red que se organizan según un atributo. Los flujos permiten asignar más recursos de red. Para obtener una descripción general de los flujos, consulte [“Gestión de recursos de red mediante flujos” en la página 390](#).

Para utilizar flujos para gestionar recursos, realice los siguientes pasos generales:

1. Cree el flujo sobre la base de un atributo específico como se muestra en [“Gestión de recursos de red mediante flujos” en la página 390](#).
2. Personalice el uso de recursos del flujo mediante la configuración de las propiedades que pertenecen a los recursos de la red. Actualmente, sólo se puede configurar el ancho de banda para el procesamiento de los paquetes.

Configuración de flujos en la red

Se pueden crear flujos tanto en la red física como en la red virtual. Para configurar flujos, utilice el comando `flowadm`. Para obtener más información técnica, consulte la página del comando `man flowadm(1M)`.

▼ Cómo configurar un flujo

- 1 (Opcional) Determine el enlace en el que configurará los flujos.

```
# dladm show-link
```

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

```
# ipadm show-addr
```

- 3 Cree flujos según el atributo que haya determinado para cada flujo.

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

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

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

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

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

- 4 Implemente controles de recursos en los flujos mediante el establecimiento de propiedades de flujo adecuadas.

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

Puede especificar las siguientes propiedades de flujo para controlar recursos:

`maxbw` La cantidad máxima de ancho de banda del enlace que pueden utilizar los paquetes identificados con este flujo. El valor que se define debe estar dentro del rango de valores permitido para el ancho de banda del enlace. Para mostrar el rango de valores posibles para el ancho de banda de un enlace, active el campo POSSIBLE en la salida que se genera mediante el siguiente comando:

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

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

- 5 (Opcional) Muestre los flujos que ha creado mediante el enlace.

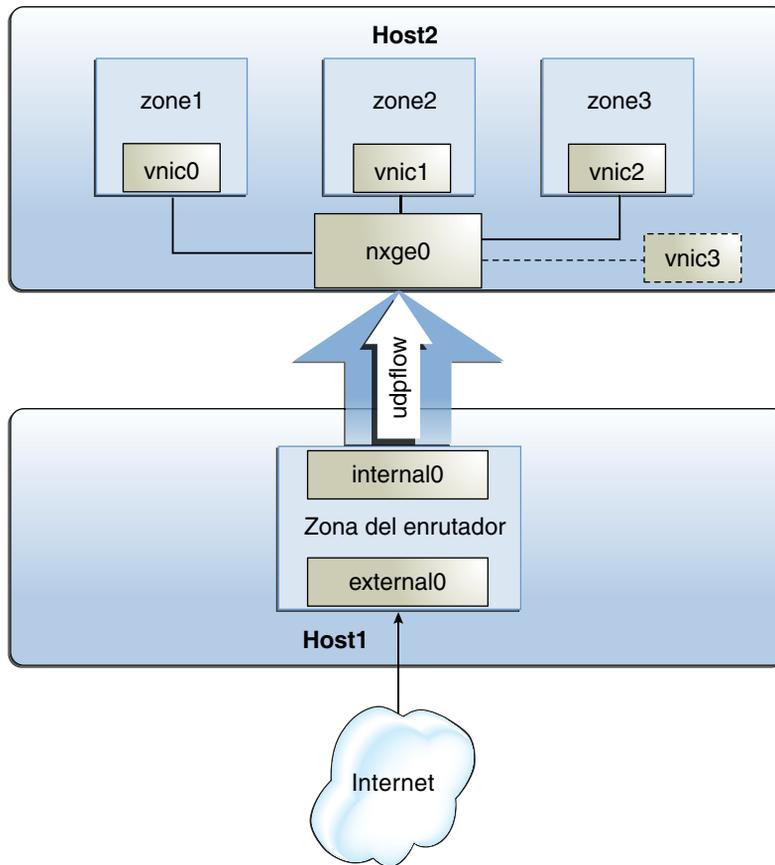
```
# flowadm show-flow -l link
```

6 (Opcional) Muestre los valores de configuración de las propiedades de un flujo especificado.

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

Ejemplo 21-8 Gestión de recursos mediante la configuración de propiedades de flujos y enlaces

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



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

- Host1 tiene la siguiente configuración:
 - Tiene una zona no global que actúa como una zona enrutadora. Se asignan dos interfaces a la zona: `external0` se conecta a Internet, mientras que `internal0` se conecta a la red interna, incluido el segundo host.

- Los nombres de las interfaces IP se han cambiado por nombres personalizados. Aunque no sea necesario, el uso de nombres personalizados en los enlaces y las interfaces proporciona ventajas para la administración de la red. Consulte [“Dispositivos de red y nombres de enlaces de datos” en la página 26.](#)
- Un flujo se configura mediante `internal0` para aislar el tráfico UDP e implementar el control sobre el modo en que los paquetes UDP utilizan los recursos. Para obtener información sobre la configuración de flujos, consulte [“Gestión de recursos en flujos” en la página 412.](#)
- Host2 tiene la siguiente configuración:
 - Tiene tres zonas no globales y sus respectivas VNIC. Las VNIC se configuran mediante una tarjeta `nxge` que admite la asignación dinámica de anillos. Para obtener más información sobre la asignación de anillos, consulte [“Anillos de transmisión y recepción” en la página 393.](#)
 - La carga de procesamiento de red de cada zona es diferente. Para este ejemplo, la carga de `zone1` es pesada, la carga de `zone2` es media y la carga de `zone3` es liviana. Los recursos se asignan a estas zonas según sus cargas.
 - Se configura una VNIC aparte como un cliente basado en software. Para obtener una descripción general de clientes MAC, consulte [“Clientes MAC y asignación de anillos” en la página 393.](#)

Las tareas de este ejemplo incluyen lo siguiente:

- Crear un flujo y configurar controles de flujo: se crea un flujo mediante `internal0` para crear controles de recursos independientes respecto de los paquetes UDP recibidos por Host2.
- Configurar propiedades de recursos de red para las VNIC en Host2: según la carga de procesamiento de cada zona, se configura la VNIC de cada zona con un conjunto de anillos dedicados. También se configura una VNIC independiente sin anillos dedicados como un ejemplo de un cliente basado en software.

Tenga en cuenta que el ejemplo no incluye ningún procedimiento para la configuración de zonas. Para configurar zonas, consulte [Capítulo 17, “Planificación y configuración de zonas no globales \(tareas\)” de Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos.](#)

En primer lugar, vea la información acerca de los enlaces y las interfaces IP en Host1.

```
# dladm show-phys
LINK          MEDIA        STATE        SPEED DUPLEX    DEVICE
internal0    Ethernet    up           1000 full    nge1
e1000g0      n           unknown     0      half     e1000g0
e1000g1      n           unknown     0      half     e1000g1
external0    Ethernet    up           1000 full    nge0

# dladm show-link
```

```
LINK      CLASS  MTU   STATE  BRIDGE  OVER
internal0 phys   1500  up     --      nge1
e1000g0   phys   1500  unknown --      --
e1000g1   phys   1500  unknown --      --
external0 phys   1500  up     --      nge0
```

```
# ipadm show-addr
ADDROBJ   TYPE    STATE    ADDR
lo0/4     static  ok       127.0.0.1/8
external0 static  ok       10.10.6.5/24
internal0 static  ok       10.10.12.42/24
```

A continuación, cree un flujo mediante `internal0` para aislar el tráfico UDP al `Host2`. A continuación, implemente los controles de recursos en el flujo.

```
# flowadm add-flow -l external0 -a transport=udp udpflow
# flowadm set-flowprop -p maxbw=80 udpflow
```

Luego, compruebe la información sobre el flujo creado.

```
flowadm show-flow
FLOW      LINK      IPADDR  PROTO  PORT  DFSLD
udpflow   internal0 --      udp    --    --

# flowadm show-flowprop
SECURE OUTPUT FOR THIS
```

En el `host2`, configure las VNIC mediante `nxge0` para cada zona. Implemente los controles de recursos en cada VNIC. A continuación, asigne las VNIC a las zonas respectivas.

```
# dladm create-vnic -l nxge0 vnic0
# dladm create-vnic -l nxge0 vnic1
# dladm create-vnic -l nxge0 vnic2

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

# zone1>zonecfg>net> set physical=vnic0
# zone2>zonecfg>net> set physical=vnic1
# zone3>zonecfg>net> set physical=vnic2
```

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

```
# dladm set-prop -p pool=pool01 vnic0
```

Por último, cree un cliente basado en software que comparta los anillos con `nxge0`, la interfaz principal.

```
dladm create-vnic -p rxrings=sw,txrings=sw -l nxge0 vnic3
```

Supervisión del tráfico de red y el uso de recursos

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

Se analizan los siguientes temas:

- “Descripción general del flujo del tráfico de red” en la página 417
- “Supervisión de tráfico y uso de recursos (mapa de tareas)” en la página 420
- “Recopilación de estadísticas sobre el tráfico de red en enlaces” en la página 421
- “Recopilación de estadísticas sobre tráfico de red en flujos” en la página 427
- “Configuración de la contabilidad de la red” en la página 429

Descripción general del flujo del tráfico de red

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

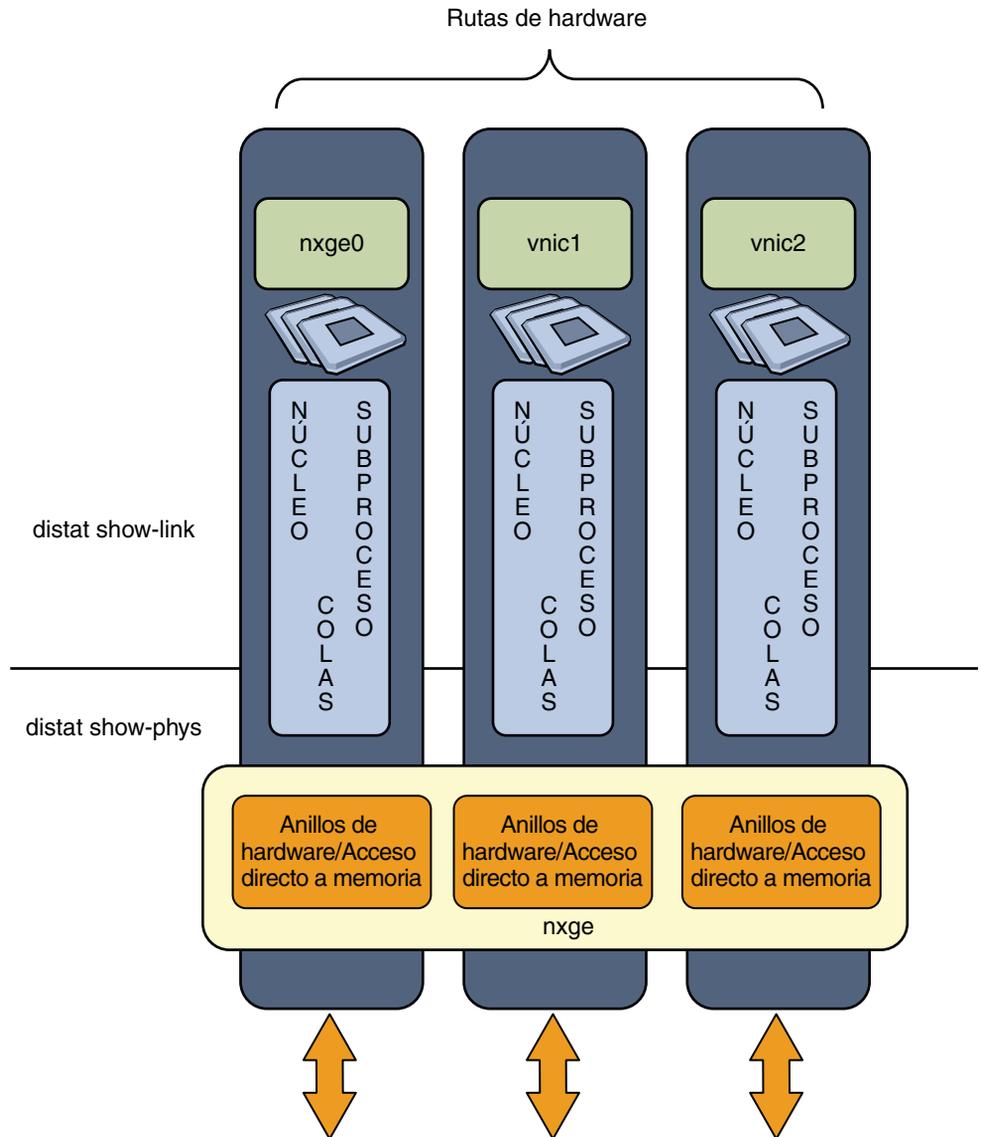
En el [Capítulo 21, “Gestión de recursos de red”](#) se presenta el concepto de vías de red. Una combinación de los recursos del sistema que se asignan para gestionar el tráfico de la red constituye una vía de red. Por lo tanto, las *vías de red* son rutas personalizadas para determinados tipos de tráfico de red. Cada vía puede ser una vía de *hardware* o una vía de *software*. Además, cada tipo de vía puede ser una vía de *recepción* o una vía de *transmisión*. La diferencia entre las vías de hardware y de software se basa en la capacidad de una NIC de admitir la asignación de anillos. Para obtener más información sobre la asignación de anillos, consulte [“Anillos de transmisión y recepción” en la página 393](#). Este capítulo se centra principalmente en el tráfico de entrada que se recibe mediante las vías de recepción.

En las vías de hardware, los anillos se dedican a los paquetes que utilizan esas vías. Por el contrario, los anillos de las vías de software se comparten entre los enlaces de datos. Los enlaces de datos se configuran para compartir anillos por los siguientes motivos:

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

Tenga en cuenta la siguiente figura que muestra diferentes vías de hardware:

FIGURA 22-1 Vías de hardware



La figura muestra la siguiente configuración:

- El sistema tiene una única NIC, `nxge`.
- Los enlaces se configuran mediante el dispositivo físico: `nxge0`, `vnic1` y `vnic2`. Tenga en cuenta que, como un enlace de datos, a `nxge0` se le puede asignar un nombre personalizado. Sin embargo, en la figura, el enlace conserva el nombre de dispositivo predeterminado.

- El sistema tiene varias CPU.
- La NIC admite la asignación dinámica de anillos. Por lo tanto, se puede asignar un conjunto de anillos de hardware a cada enlace para constituir una vía de hardware. Además, también se asigna un conjunto de CPU a cada vía.

Supervisión de tráfico y uso de recursos (mapa de tareas)

Puede obtener información sobre cómo los paquetes utilizan los recursos de red observando el flujo de paquetes en las vías de red. El comando `d1stat` proporciona esta información sobre los enlaces de datos. El comando `flowstat` realiza funciones similares para los flujos existentes.

En la siguiente tabla se muestran los diferentes métodos que se pueden utilizar para obtener estadísticas sobre el tráfico de la red y el uso de los recursos del sistema.

Tarea	Descripción	Para obtener instrucciones
Obtener información estadística sobre el tráfico de la red.	Vea el tráfico entrante y saliente de las interfaces de red de un sistema.	“Cómo obtener estadísticas básicas sobre el tráfico de la red” en la página 422
Obtener información estadística sobre el uso de anillos.	Vea cómo se distribuye el tráfico entrante y saliente entre los anillos de una NIC.	“Cómo obtener estadísticas sobre el uso anillos” en la página 423
Obtener información estadística sobre el tráfico de red en vías específicas.	Vea información detallada sobre el tráfico entrante y saliente a medida que los paquetes recorren las vías de red que están configuradas en las interfaces de red de un sistema.	“Cómo obtener estadísticas sobre el tráfico de red en vías” en la página 425
Obtener información estadística sobre el tráfico de los flujos.	Vea información sobre el tráfico entrante y saliente que recorre los flujos definidos por el usuario.	“Cómo obtener estadísticas de flujos” en la página 427
Configurar la contabilidad del tráfico de red.	Configure la contabilidad de red para capturar información de tráfico a efectos contables.	“Cómo configurar la contabilidad de red ampliada” en la página 430
Obtener estadísticas históricas del tráfico de la red.	Extraiga información del archivo de registro de contabilidad de red ampliada para obtener estadísticas históricas del tráfico de red en vías y flujos.	“Cómo obtener estadísticas históricas del tráfico de la red” en la página 431

Para obtener una descripción de los pasos para configurar flujos, consulte [“Gestión de recursos en flujos” en la página 412](#). Para obtener más información acerca de estos dos comandos, consulte las páginas del comando `man d1stat(1M)` y `flowstat(1M)`.

Recopilación de estadísticas sobre el tráfico de red en enlaces

Los comandos `dlstat` y `flowstat` son herramientas para supervisar el tráfico de red en enlaces de datos y flujos, y obtener estadísticas al respecto. Estos comandos son paralelos a los comandos `dladm` y `flowadm`. En la siguiente tabla se muestra el paralelismo entre el par de comandos `*adm` y el par de comandos `*stat`, y sus respectivas funciones:

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

Las siguientes variantes del comando `dlstat` se pueden utilizar para recopilar información sobre el tráfico de la red:

- `dlstat`: muestra información general sobre los paquetes que son recibidos o transmitidos por un sistema.
- `dlstat show-phys`: muestra información sobre el uso de los anillos de recepción y de transmisión. Este comando corresponde al comando `dladm show-phys`, que muestra información no relacionada con el tráfico de un dispositivo físico de red. Para ver una ilustración del nivel de la vía de red a la que se aplica este comando, consulte la [Figura 22-1](#).
- `dlstat show-link`: muestra información detallada sobre el flujo de tráfico en una vía determinada. La vía se identifica mediante su enlace de datos. Este comando corresponde a los comandos `dladm show-link` y `dladm show-vnic`, que muestran información no relacionada con el tráfico de los enlaces de datos. Para ver una ilustración del nivel de la vía de red a la que se aplica el comando `dlstat show-link`, consulte la [Figura 22-1](#).
- `dlstat show-aggr`: muestra información sobre el uso de puertos en una agregación de enlaces. Este comando corresponde al comando `dladm show-aggr`, que muestra información no relacionada con el tráfico de una agregación de enlace.

▼ Cómo obtener estadísticas básicas sobre el tráfico de la red

1 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Observe el flujo de tráfico básico de todos los enlaces de datos.

```
# dlstat [-r|-t] [-i interval] [link]
```

`[-r|-t]` Muestra sólo las estadísticas de recepción (opción `-r`) o sólo las estadísticas de transmisión (opción `-t`). Si no utiliza estas opciones, se muestran las estadísticas tanto de recepción como de transmisión.

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

`enlace` Indica que desea supervisar las estadísticas del enlace de datos especificado únicamente. Si no utiliza esta opción, se muestra información sobre todos los enlaces de datos.

Si se utiliza solo, el comando `dlstat` muestra información sobre los paquetes entrantes y salientes en todos los enlaces de datos configurados.

La mayoría de las opciones que se utilizan con el comando `dlstat` muestran la siguiente información:

- Enlaces del sistema que se han configurado con interfaces IP y que pueden recibir o transmitir tráfico
- Tamaños de paquetes y de bytes
- Estadísticas de sondeo MAC e interrupciones
- Longitudes de cadena de paquetes

Ejemplo 22-1 Visualización de estadísticas básicas de recepción y transmisión

En este ejemplo se muestra información sobre el tráfico de red que se está recibiendo y enviando en todos los enlaces de datos configurados del sistema.

```
# dlstat
LINK      IPKTS  RBYTES  OPKTS  OBYTES
e1000g0  101.88K  32.86M  40.16K  4.37M
nxge1    4.50M   6.78G   1.38M   90.90M
vnic1         8     336         0         0
```

Ejemplo 22-2 Visualización de estadísticas de recepción cada intervalos de un segundo

En este ejemplo se muestra información sobre el tráfico que se está recibiendo en todos los enlaces de datos. La información se refresca cada un segundo. Para detener el refrescamiento de la visualización, presione Control-C.

```
# dlstat -r -i 1
LINK IPKTS RBYTES INTRS POLLS CH<10 CH10-50 CH>50
e1000g0 101.91K 32.86M 87.56K 14.35K 3.70K 205 5
nxge1 9.61M 14.47G 5.79M 3.82M 379.98K 85.66K 1.64K
vnic1 8 336 0 0 0 0 0
e1000g0 0 0 0 0 0 0 0
nxge1 82.13K 123.69M 50.00K 32.13K 3.17K 724 24
vnic1 0 0 0 0 0 0 0
...
^C
```

En esta salida, las estadísticas de interrupción (INTRS) son significativas. Un número bajo de interrupciones indica una mayor eficacia en el rendimiento. Si el número de interrupciones es alto, es posible que sea necesario agregar más recursos al enlace específico.

Ejemplo 22-3 Visualización estadísticas de transmisión cada intervalos de cinco segundos

En este ejemplo se muestra información sobre el tráfico que se está enviando en todos los enlaces de datos. La información se refresca cada 5 segundos.

```
# dlstat -t -i 5
LINK OPKTS OBYTES BLKCNT UBLKCNT
e1000g0 40.24K 4.37M 0 0
nxge1 9.76M 644.14M 0 0
vnic1 0 0 0 0
e1000g0 0 0 0 0
nxge1 26.82K 1.77M 0 0
vnic1 0 0 0 0
...
^C
```

▼ Cómo obtener estadísticas sobre el uso anillos

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Visualice las estadísticas de anillos.

```
# dlstat show-phys [-r|-t] [-i interval] [link]
```

<code>[-r] [-t]</code>	Muestra sólo las estadísticas de recepción (opción <code>-r</code>) o sólo las estadísticas de transmisión (opción <code>-t</code>). Si no utiliza estas opciones, se muestran las estadísticas tanto de recepción como de transmisión.
<code>-i intervalo</code>	Especifica cada cuántos segundos desea que se refresquen las estadísticas mostradas. Si no utiliza esta opción, se muestra una salida estática.
<code>enlace</code>	Indica que desea supervisar las estadísticas del enlace de datos especificado únicamente. Si no utiliza esta opción, se muestra información sobre todos los enlaces de datos.

Si se utiliza solo, el comando `dlstat show-phys` muestra información sobre los paquetes entrantes y salientes en todos los enlaces de datos configurados.

Ejemplo 22-4 Visualización de estadísticas de anillos de recepción de un enlace de datos

En este ejemplo se muestra el uso de los anillos de recepción del enlace de datos.

```
# dlstat show-phys -r nxge1
LINK TYPE INDEX  IPKTS  RBYTES
nxge1  rx      0      21    1.79K
nxge1  rx      1       0       0
nxge1  rx      2    1.39M    2.10G
nxge1  rx      3       0       0
nxge1  rx      4    6.81M   10.26G
nxge1  rx      5    4.63M    6.97G
nxge1  rx      6    3.97M    5.98G
nxge1  rx      7       0       0
```

El dispositivo `nxge` tiene ocho anillos de recepción que se identifican en el campo `INDEX`. Una distribución uniforme de paquetes por anillo constituye una configuración ideal que indica que los anillos están asignados correctamente a los enlaces según la carga de los enlaces. Una distribución desigual puede indicar una distribución desproporcionada de los anillos por enlace. La resolución depende de si la NIC admite la asignación dinámica de anillos, que permite redistribuir los anillos por enlace. Para obtener más información acerca de la asignación dinámica de anillos, consulte [“Anillos de transmisión y recepción” en la página 393](#).

Ejemplo 22-5 Visualización de estadísticas de anillos de transmisión de un enlace de datos

En este ejemplo se muestra el uso de los anillos de transmisión del enlace de datos.

```
# dlstat show-phys -t nxge1
LINK TYPE INDEX  OPKTS  OBYTES
nxge1  tx      0      44    3.96K
nxge1  tx      1       0       0
nxge1  tx      2    1.48M   121.68M
nxge1  tx      3    2.45M   201.11M
nxge1  tx      4    1.47M   120.82M
nxge1  tx      5       0       0
```

nxge1	tx	6	1.97M	161.57M
nxge1	tx	7	4.59M	376.21M
nxge1	tx	8	2.43M	199.24M
nxge1	tx	9	0	0
nxge1	tx	10	3.23M	264.69M
nxge1	tx	11	1.88M	153.96M

▼ Cómo obtener estadísticas sobre el tráfico de red en vías

1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Visualice las estadísticas sobre las vías de red.

```
# dlstat show-link [-r [F]]-t] [-i interval] [link]
```

`[-r|-t]` Muestra sólo las estadísticas de recepción (opción `-r`) o sólo las estadísticas de transmisión (opción `-t`). Si no utiliza estas opciones, se muestran las estadísticas tanto de recepción como de transmisión.

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

`enlace` Indica que desea supervisar las estadísticas del enlace de datos especificado únicamente. Si no utiliza esta opción, se muestra información sobre todos los enlaces de datos.

Si se admite la agrupación de anillos y se configuraron anillos dedicados, se muestran las estadísticas de vía de hardware. Si no se configuraron anillos dedicados, se muestran las estadísticas de vía de software.

Ejemplo 22-6 Visualización de estadísticas de recepción de una vía

En este ejemplo se muestra la siguiente información:

- Cómo se reciben los paquetes en una vía de hardware
- Cómo se reciben los paquetes en una vía de software
- Cómo se reciben los paquetes en una vía de software y se transmiten a las CPU asignadas

El siguiente comando muestra las estadísticas de recepción del enlace específico. La información indica el uso de anillos. Sin embargo, es posible que los datos también reflejen la implementación de otras asignaciones de recursos, como límites de ancho de banda y procesamiento de prioridades.

```
# dlstat show-link -r nxge1
LINK TYPE ID INDEX IPKTS RBYTES INTRS POLLS CH<10 CH10-50 CH>50
nxge1 rx local -- 0 0 0 0 0 0 0
nxge1 rx hw 1 0 0 0 0 0 0 0
nxge1 rx hw 2 1.73M 2.61G 1.33M 400.22K 67.03K 7.49K 38
nxge1 rx hw 3 0 0 0 0 0 0 0
nxge1 rx hw 4 8.44M 12.71G 4.35M 4.09M 383.28K 91.24K 2.09K
nxge1 rx hw 5 5.68M 8.56G 3.72M 1.97M 203.68K 43.94K 854
nxge1 rx hw 6 4.90M 7.38G 3.11M 1.80M 168.59K 42.34K 620
nxge1 rx hw 7 0 0 0 0 0 0 0
```

El siguiente comando muestra las estadísticas de recepción del enlace específico. En la salida, el campo ID indica si los anillos de hardware se asignaron de manera exclusiva o se comparten entre los clientes. En la tarjeta ixgbe, los anillos de Rx se comparten si otros clientes, como las VNIC, también se configuran mediante el enlace. Por lo tanto, en este ejemplo específico, los anillos de Rx se comparten, según lo indicado por el valor sw del campo ID.

```
# dlstat show-link -r ixgbe0
LINK TYPE ID INDEX IPKTS RBYTES INTRS POLLS CH<10 CH10-50 CH>50
ixgbe0 rx local -- 0 0 0 0 0 0 0
ixgbe0 rx sw -- 794.28K 1.19G 794.28K 0 0 0 0
```

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

```
# dlstat show-link -r -F nxge1
LINK ID INDEX FOUT IPKTS
nxge1 local -- 0 0
nxge1 hw 0 0 382.47K
nxge1 hw 0 1 0
nxge1 hw 1 0 367.50K
nxge1 hw 1 1 433.24K
```

Ejemplo 22-7 Visualización de estadísticas de transmisión de una vía

En el siguiente ejemplo se muestran estadísticas sobre los paquetes salientes en una vía determinada.

```
# dlstat show-link -t nxge1
LINK TYPE ID INDEX OPKTS OBYTES BLKCNT UBLKCNT
nxge1 tx hw 0 32 1.44K 0 0
nxge1 tx hw 1 0 0 0 0
nxge1 tx hw 2 1.48M 97.95M 0 0
nxge1 tx hw 3 2.45M 161.87M 0 0
nxge1 tx hw 4 1.47M 97.25M 0 0
nxge1 tx hw 5 0 276 0 0
nxge1 tx hw 6 1.97M 130.25M 0 0
```

nxge1	tx	hw	7	4.59M	302.80M	0	0
nxge1	tx	hw	8	2.43M	302.80M	0	0
nxge1	tx	hw	9	0	0	0	0
nxge1	tx	hw	10	3.23M	213.05M	0	0
nxge1	tx	hw	11	1.88M	123.93M	0	0

Recopilación de estadísticas sobre tráfico de red en flujos

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

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

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

`[-r|-t]` Muestra sólo las estadísticas de recepción (opción `-r`) o sólo las estadísticas de transmisión (opción `-t`). Si no utiliza estas opciones, se muestran las estadísticas tanto de recepción como de transmisión.

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

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

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

▼ Cómo obtener estadísticas de flujos

Antes de empezar Puede utilizar el comando `flowstat` sólo si existen flujos en la configuración de red. Para configurar flujos, consulte el [Capítulo 21, “Gestión de recursos de red”](#).

- 1 **En el sistema en el que previamente configuró el control de flujo, conviértase en un administrador en la zona global.**

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*.

- 2 **Para ver un ejemplo de cómo observar el tráfico de red en los flujos, ejecute cualquiera de los siguientes comandos:**

- Visualice las estadísticas de paquetes entrantes y salientes en todos los flujos.

flowstat

Este comando proporciona una visualización estática de la información del tráfico en todos los flujos configurados.

- Visualice estadísticas básicas del tráfico de red en todos los flujos según un intervalo especificado.

flowstat -i interval

La visualización de estadísticas se refresca en función del intervalo especificado, hasta que se detiene la generación de la salida presionando Control-C.

- Visualice estadísticas sobre los paquetes entrantes en todos los flujos configurados mediante un enlace de datos especificado.

flowstat -r -l link

- Visualice estadísticas sobre los paquetes salientes en un flujo especificado según un intervalo especificado.

flowstat -t -i interval flow

Ejemplo 22-8 Visualización de estadísticas de tráfico de todos los flujos cada intervalos de un segundo

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

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

Ejemplo 22-9 Visualización de estadísticas de transmisión de todos los flujos

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

Ejemplo 22-10 Visualización de estadísticas de recepción de todos los flujos en un enlace especificado

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

```
# flowstat -r -i 2 -l net0
FLOW      IPKTS    RBYTES    IERRS
tcp-flow  183.11K  270.24M    0
udp-flow      0         0         0
tcp-flow  373.83K  551.52M    0
udp-flow      0         0         0
tcp-flow  372.35K  549.04M    0
udp-flow      0         0         0
tcp-flow  372.87K  549.61M    0
udp-flow      0         0         0
tcp-flow  371.57K  547.89M    0
udp-flow      0         0         0
tcp-flow  191.92K  282.95M    0
udp-flow  206.51K  310.70M    0
tcp-flow      0         0         0
udp-flow  222.75K  335.15M    0
tcp-flow      0         0         0
udp-flow  223.00K  335.52M    0
tcp-flow      0         0         0
udp-flow  160.22K  241.07M    0
tcp-flow      0         0         0
udp-flow  167.89K  252.61M    0
tcp-flow      0         0         0
udp-flow   9.52K  14.32M     0
^C
```

Configuración de la contabilidad de la red

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

Para configurar la utilidad de contabilidad ampliada, utilice el comando `acctadm`.

▼ Cómo configurar la contabilidad de red ampliada

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

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

- 2 **Vea el estado de la contabilidad de red ampliada en el sistema.**

```
# acctadm net
```

Se pueden habilitar cuatro tipos de contabilidad ampliada mediante el comando `acctadm`:

- Contabilidad del proceso
- Contabilidad de tareas
- Contabilidad de flujo para la calidad de servicio IP (IPQoS)
- Contabilidad de red para enlaces y flujos

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

Nota – La contabilidad de red también se aplica a los flujos que se gestionan mediante los comandos `flowadm` y `flowstat`, como se explicó en “[Gestión de recursos en flujos](#)” en la [página 412](#). Por lo tanto, para configurar la contabilidad de estos flujos, utilice la opción `net` con el comando `acctadm`. No use la opción `flow` que habilita la contabilidad de flujo y que se aplica a configuraciones de IPQoS.

- 3 **Habilite la contabilidad ampliada para el tráfico de red.**

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

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

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

```
# acctadm net
```

Ejemplo 22–11 Configuración de contabilidad ampliada para tráfico de red

En este ejemplo se muestra cómo capturar y visualizar información histórica sobre el tráfico de red en enlaces de datos y cualquier flujo configurado en el sistema.

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

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

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

A continuación, habilite la contabilidad de red ampliada.

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

Después de habilitar la contabilidad de red, puede utilizar los comandos `dlstat` y `flowstat` para extraer información del archivo de registro. El procedimiento siguiente explica los pasos.

▼ Cómo obtener estadísticas históricas del tráfico de la red

Antes de empezar Para poder visualizar los datos históricos de la red, debe habilitar la contabilidad ampliada para la red. Además, para visualizar los datos históricos del tráfico en los flujos, primero, debe configurar los flujos del sistema como se explica en [“Gestión de recursos en flujos” en la página 412](#).

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

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

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

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

-h	Muestra un resumen de la información histórica sobre el uso de los recursos por parte de los paquetes entrantes y salientes en los enlaces de datos.
-a	Muestra el uso de los recursos en todos los enlaces de datos, incluidos los que ya se eliminaron después de la captura de los datos.
-f <i>nombre_archivo</i>	Especifica el archivo de registro que se definió al habilitar la contabilidad red con el comando <code>acctadm</code> .
-d	Muestra la información registrada para las fechas, cuando la información está disponible.
-F <i>formato</i>	Muestra los datos en un formato específico. Actualmente, <code>gnuplot</code> es el único formato admitido.
-s <i>tiempo_inicio</i> , -e <i>tiempo_fin</i>	Muestra la información registrada disponible para un rango de fecha y hora especificado. Utilice el formato <code>MM/DD/YYYY, hh:mm:ss</code> . La hora (hh) debe utilizar la notación de reloj de 24 horas. Si no incluye la fecha, se muestran los datos para el rango de tiempo de la fecha actual.
<i>enlace</i>	Muestra los datos históricos para un enlace de datos determinado. Si no utiliza esta opción, se muestran los datos de red históricos para todos los enlaces de datos configurados.

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

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

-h	Muestra un resumen de la información histórica sobre el uso de los recursos por parte de los paquetes entrantes y salientes en los enlaces de datos.
-a	Muestra el uso de los recursos en todos los enlaces de datos, incluidos los que ya se eliminaron después de la captura de los datos.
-f <i>nombre_archivo</i>	Especifica el archivo de registro que se definió al habilitar la contabilidad red con el comando <code>acctadm</code> .
-d	Muestra la información registrada para las fechas, cuando la información está disponible.
-F <i>formato</i>	Muestra los datos en un formato específico. Actualmente, <code>gnuplot</code> es el único formato admitido.
-s <i>tiempo_inicio</i> , -e <i>tiempo_fin</i>	Muestra la información registrada disponible para un rango de fecha y hora especificado. Utilice el formato <code>MM/DD/YYYY, hh:mm:ss</code> . La hora

(hh) debe utilizar la notación de reloj de 24 horas. Si no incluye la fecha, se muestran los datos para el rango de tiempo de la fecha actual.

enlace Muestra los datos históricos para un enlace de datos determinado. Si no utiliza esta opción, se muestran los datos de red históricos para todos los enlaces de datos configurados.

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

Ejemplo 22-12 Visualización de información histórica sobre el uso de los recursos en enlaces de datos

En el siguiente ejemplo se muestran estadísticas históricas sobre el tráfico de la red y el uso de recursos en un enlace de datos especificado.

```
# dlstat show-link -h -f /var/log/net.log
LINK      DURATION  IPACKETS  RBYTES    OPACKETS  OBYTES    BANDWIDTH
e1000g0   80        1031     546908    0         0         2.44 Kbps
```

Ejemplo 22-13 Visualización de información histórica sobre el uso de los recursos en flujos

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

Visualice estadísticas históricas del uso de recursos por tráfico en un flujo:

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

Visualice estadísticas históricas del uso de recursos por tráfico en un flujo durante un determinado rango de fechas y horas.

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

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

Visualice estadísticas históricas del uso de recursos por tráfico en un flujo durante un determinado rango de fechas y horas. Visualice la información con el formato gnuplot.

```
# flowstat -h -s 02/19/2008,10:39:06 -e 02/19/2008,10:40:06 \  
-F gnuplot -f /var/log/net.log flowtcp  
# Time tcp-flow  
10:39:06 3.23  
10:39:26 5.40  
10:39:46 0.18  
10:40:06 0.00
```

Glosario

3DES	Consulte Triple-DES .
administración de claves	El modo en que puede gestionar asociaciones de seguridad (SA).
AES	Advanced Encryption Standard. Una técnica de cifrado de datos en bloques de 128 bits simétricos. En octubre de 2000, el gobierno de los Estados Unidos adoptó la variante Rijndael del algoritmo como estándar de cifrado. AES sustituye al cifrado DES como estándar gubernamental.
anuncio de enrutador	Proceso en el que los enrutadores anuncian su presencia junto con otros parámetros de enlace e Internet, de manera periódica o como respuesta a un mensaje de solicitud de enrutador.
anuncio de vecinos	Respuesta a mensaje de solicitud de vecino o proceso de un nodo que envía anuncios de vecino no solicitados para anunciar un cambio de dirección de capa de enlace.
ataque smurf	Uso de paquetes de solicitud de ICMP echo dirigidos a una dirección de difusión IP o a varias direcciones de difusión desde ubicaciones remotas para crear interrupciones o congestiones graves de la red.
autoconfiguración	Proceso mediante el cual un host configura automáticamente su dirección IPv6 a partir del prefijo del sitio y la dirección MAC local.
autoconfiguración sin estado	Proceso mediante el cual un host genera sus propias direcciones IPv6 combinando su dirección MAC y un prefijo de IPv6 anunciado por un enrutador IPv6 local.
autoridad de certificación	Organización externa o empresa que ofrece confianza y que emite los certificados digitales utilizados para crear firmas digitales y pares de claves públicas-privadas. La autoridad de certificación garantiza la identidad de la persona a la que se concede el certificado exclusivo.
base de datos de directivas de seguridad (SPD)	Base de datos que determina el nivel de protección que debe aplicarse a un paquete. La SPD filtra el tráfico de IP para establecer si se debe descartar un paquete, autorizarle el paso o protegerlo con IPsec.
Blowfish	Algoritmo cifrado de bloques simétricos con una clave de tamaño variable que va de 32 a 448 bits. Bruce Schneier, su creador, afirma que Blowfish se optimiza en el caso de aplicaciones en que la clave se modifica con poca frecuencia.
CA	Consulte autoridad de certificación .
capa de enlace	Capa inmediatamente inferior a IPv4/IPv6 .

carga de seguridad encapsuladora (ESP)	Encabezado de extensión que proporciona integridad y confidencialidad a los datagramas. ESP es uno de los cinco componentes de la arquitectura para seguridad IP (IPsec).
carga útil	Los datos que se transportan en un paquete. La carga útil no incluye la información de encabezado que se necesita para que el paquete llegue a su destino.
cifrado de claves asimétricas	Sistema de cifrado en el que el emisor y el receptor de un mensaje emplean claves distintas para cifrar y descifrar dicho mensaje. Las claves asimétricas se usan para establecer un canal seguro de cifrado simétrico de claves. protocolo de Diffie-Hellman es un ejemplo de protocolo de claves asimétricas. Se contrapone a criptografía de clave simétrica .
clase	En IPQoS, grupo de flujos de datos de red que comparten características similares. Las clases se definen en el archivo de configuración de IPQoS.
código de autenticación de mensajes (MAC)	MAC proporciona seguridad en la integridad de los datos y autentica el origen de los datos. MAC no proporciona protección contra intromisiones externas.
contabilidad de flujos	En IPQoS, proceso de recopilación y registro de información relativa a los flujos de tráfico. La contabilidad de flujos se establece definiendo los parámetros del módulo <code>flowacct</code> en el archivo de configuración de IPQoS.
cortafuegos	Cualquier programa o dispositivo que aisle la intranet o red de una organización particular de Internet, con lo cual queda protegida de intrusiones externas. Un cortafuegos puede abarcar filtrado de paquetes, servidores proxy y NAT (Network Address Translation, traducción de direcciones de red).
criptografía de clave simétrica	Sistema de cifrado en que el emisor y el receptor de un mensaje comparten una sola clave común. Esa clave común se emplea para cifrar y descifrar el mensaje. Las claves simétricas se usan para cifrar la mayor parte de las transmisiones de datos en IPsec. DES constituye un ejemplo de sistema de claves simétricas.
criptografía por clave pública	Sistema criptográfico basado en dos claves. La clave pública es de dominio general. La clave privada sólo la conoce el destinatario del mensaje. IKE proporciona claves públicas para IPsec.
datagrama	Consulte datagrama IP .
datagrama IP	Paquete de información que se transfiere por IP. Un datagrama IP contiene un encabezado y datos. En el encabezado figuran las direcciones del origen y el destino del datagrama. Otros campos del encabezado permiten identificar y volver a combinar los datos con los datagramas adjuntos en el destino.
DES	Siglas en inglés de Data Encryption Standard, estándar de cifrado de datos. Un método de cifrado de claves simétricas que se desarrolló en 1975 y que la ANSI estandarizó en 1981 como ANSI X.3.92. DES utiliza una clave de 56 bits.
descubrimiento de enrutadores	Proceso de los hosts que buscan enrutadores residentes en un enlace conectado.
descubrimiento de vecinos	Mecanismo de IP que permite a los host encontrar otros host que residen en un enlace conectado.

detección de errores	Proceso en el que se detecta que deja de funcionar una interfaz o la ruta de una interfaz a un dispositivo de capa de Internet. Las rutas múltiples de red IP incluyen dos tipos de detección de errores: detección en enlaces (predeterminada) o en sondeos (opcional).
detección de reparaciones	Proceso en el que se detecta si una tarjeta de interfaz de red o la ruta de dicha tarjeta a un dispositivo de capa 3 comienza a funcionar correctamente después de un fallo.
dirección de datos	Dirección IP que puede utilizarse como origen o destino de datos. Las direcciones de datos forman parte de un grupo IPMP y se pueden usar para enviar y recibir tráfico en cualquier interfaz del grupo. Además, el conjunto de direcciones de datos de un grupo IPMP se puede utilizar continuamente siempre que funcione una interfaz en el grupo.
dirección de difusión	Direcciones de red IPv4 cuya parte principal de la dirección es de bits de todo cero (10.50.0.0) o todo uno (10.50.255.255). Un paquete que se envía a una dirección de difusión desde un equipo de la red local se distribuye a todos los equipos de dicha red.
dirección de difusión por proximidad	Dirección IPv6 que se asigna a un grupo de interfaces (en general pertenecientes a nodos distintos). El paquete que se envía a una dirección de difusión por proximidad se dirige a la interfaz <i>más próxima</i> que contenga dicha dirección. La ruta del paquete se atiene a la medición de distancia del protocolo de enrutamiento.
dirección de enrutamiento entre dominios sin clase (CIDR)	Formato de dirección IPv4 que no se basa en clases de red (clase A, B y C). Las direcciones CIDR tienen un tamaño de 32 bits. Utilizan la notación decimal con puntos IPv4 estándar, más un prefijo de red. Dicho prefijo define el número de red y la máscara de red.
dirección de multidifusión	Dirección IPv6 que identifica un grupo de interfaces de una manera determinada. Un paquete enviado a una dirección multidifusión se distribuye a todas las interfaces del grupo. La dirección de multidifusión IPv6 funciona de manera similar a la dirección de emisión IPv4.
dirección de prueba	Dirección IP en un grupo IPMP que debe usarse como dirección de origen o destino de sondas; no debe emplearse como dirección de origen o destino para tráfico de datos.
dirección de unidifusión	Dirección IPv6 que identifica una sola interfaz de un nodo compatible con IPv6. Una dirección de unidifusión se compone de prefijo de sitio, ID de subred e ID de interfaz.
dirección de uso local	Dirección de unidifusión que sólo tiene un ámbito de enrutamiento local (dentro de una subred o una red de suscriptores). Esta dirección puede tener también un ámbito de exclusividad local o global.
dirección de uso local de sitio	Designación que se usa para dirección en un solo sitio.
dirección DEPRECATED	Dirección IP que no sirve como dirección de origen de datos que están en un grupo IPMP. En general, las direcciones de prueba IPMP son del tipo DEPRECATED . Ahora bien, cualquier dirección se puede marcar como DEPRECATED para impedir que pueda utilizarse como dirección de origen.
dirección local de enlace	En IPv6, designación que se usa para asignar una dirección a un solo enlace para, por ejemplo, la configuración automática de direcciones. De forma predeterminada, la dirección local de enlace se crea a partir de la dirección MAC del sistema.

dirección privada	Dirección IP que no se puede enrutar por Internet. Las redes internas utilizan las direcciones privadas en los host que no necesitan conexión con Internet. Las direcciones están definidas en Address Allocation for Private Internets (http://www.ietf.org/rfc/rfc1918.txt?number=1918) y con frecuencia se las denomina direcciones “1918”.
dispositivo LAN virtual (VLAN)	Interfaces de red que proporcionan reenvío de tráfico en el nivel de Ethernet (enlace de datos) del protocolo de pila IP.
dominio de interpretación (DOI)	El dominio de interpretación define los formatos de los datos, los tipos de intercambio de tráfico de red y las convenciones de denominación de información relacionada con la seguridad. Ejemplos de información relacionada con la seguridad son los algoritmos y modos criptográficos, y las directrices de seguridad.
DSA	Siglas en inglés de Digital Signature Algorithm, algoritmo de firma digital. Algoritmo de clave pública con un tamaño de clave variable que va de 512 a 4096 bits. DSS, el estándar del gobierno de los Estados Unidos, llega hasta los 1024 bits. DSA se basa en el algoritmo SHA-1 para las entradas.
encabezado	Consulte encabezado IP .
encabezado de autenticación	Encabezado de extensión que proporciona autenticación e integridad, sin confidencialidad, a datagramas IP.
encabezado de paquete	Consulte encabezado IP .
encabezado IP	Veinte bytes de datos que identifican un paquete de Internet de forma exclusiva. El encabezado contiene direcciones de origen y destino del paquete. Una opción del encabezado permite agregar más bytes.
encapsulado	Proceso de colocación de un encabezado y carga útil en el primer paquete, que posteriormente se coloca en la carga útil del segundo paquete.
encapsulado mínimo	Forma opcional de túnel de IPv4 en IPv4 válida para agentes internos, externos y nodos móviles. El encapsulado mínimo presenta 8 o 12 bytes menos de estructura general que IP en encapsulado IP.
enlace IP	Infraestructura o medio de comunicación que permite a los nodos comunicarse en la capa de enlace. La capa de enlace es la capa inmediatamente inferior a IPv4/IPv6. Ejemplos son las redes Ethernet (simple o con puente) o ATM. Se asignan uno o más números o prefijos de subred IPv4 a un enlace IP. No se puede asignar el mismo número o prefijo de subred a más de un enlace IP. En ATM LANE, un enlace IP es una sola LAN emulada. Al utilizar ARP, el ámbito del protocolo ARP es un solo enlace IP.
enrutador	Sistema que, en general, tiene más de una interfaz, ejecuta protocolos de enrutamiento y reenvía paquetes. Un sistema se puede configurar con una sola interfaz como enrutador si el sistema es el punto final de un enlace PPP.
expansión de carga	Proceso de distribuir tráfico de entrada o salida en un conjunto de interfaces. Como consecuencia de la expansión de carga, se obtiene un mayor rendimiento. La expansión de carga sólo se produce cuando el tráfico de red fluye hacia varios destinos que utilizan múltiples conexiones. Hay dos clases de expansión de carga: expansión de carga de entrada, para tráfico de entrada, y de salida, para tráfico de salida.

filtro	Conjunto de reglas que establecen las características de una clase en el archivo de configuración de IPQoS. El sistema IPQoS selecciona para procesar cualquier flujo de tráfico de datos que se adecua a los filtros de su archivo de configuración de IPQoS. Consulte filtro de paquetes .
filtro de paquetes	Función de cortafuegos que se puede configurar para permitir o denegar el paso de determinados paquetes a través de un cortafuegos.
filtro de paquetes con estado	Un filtro de paquetes que puede supervisar el estado de las conexiones activas y recurrir a la información obtenida para establecer los paquetes de red que podrán pasar a través del cortafuegos . Al efectuar el seguimiento y relacionar solicitudes y respuestas, un filtro de paquetes con estado puede detectar respuestas que no coincidan con una consulta.
filtro de paquetes dinámico	Consulte filtro de paquetes con estado .
firma digital	Código digital que se vincula con un mensaje transmitido electrónicamente y que identifica al remitente de forma exclusiva.
grupo de difusión por proximidad	Grupo de interfaces que tienen la misma dirección de dirección por proximidad IPv6. La implementación de IPv6 en Oracle Solaris no permite crear direcciones ni grupos de difusión por proximidad. Ahora bien, los nodos IPv6 de Oracle Solaris pueden enviar tráfico a grupos de difusión por proximidad.
grupo IPMP	Grupo con varias rutas IP, compuesto por una serie de interfaces de red con un conjunto de direcciones de datos que el sistema trata como intercambiables para mejorar la disponibilidad y utilización de la red. El grupo IPMP, incluidas todas sus direcciones de datos e interfaces IP subyacentes, lo representa una interfaz IPMP.
HMAC	Un método de hashing por clave para autenticar mensajes. HMAC es un algoritmo de autenticación de claves secretas. HMAC se utiliza junto a una función de hash criptográfica iterativa, como por ejemplo MD5 o SHA-1, en combinación con una clave secreta compartida. La capacidad criptográfica de HMAC depende de las propiedades de la función de hash subyacente.
host	Sistema que no reenvía paquetes. Al instalar Oracle Solaris, de forma predeterminada un sistema se convierte en host. Es decir, el sistema no puede reenviar paquetes. En general, un host tiene una interfaz física, aunque también puede constar de varias interfaces.
host multired	Sistema con más de una interfaz física y que no reenvía paquetes. Un host multired puede ejecutar protocolos de enrutamiento.
ICMP	Siglas inglesas de Internet Control Message Protocol (protocolo de mensajes de control de Internet). Se utiliza para administrar e intercambiar mensajes de control.
IKE	Siglas inglesas de Internet Key Exchange (intercambio de claves en Internet). IKE automatiza el suministro de material de claves autenticadas para las asociaciones de seguridad (SA) de IPsec.
inactividad	Interfaz física que no se emplea para transportar tráfico de datos a menos que otra interfaz física haya sufrido algún problema.
índice de parámetros de seguridad	Valor entero que indica la fila de la base de datos de asociaciones de seguridad (SDAB) que debe utilizar un destinatario para descifrar un paquete recibido.

interfaz de red virtual (VNIC)	Se trata de una pseudointerfaz que proporciona conexión de red virtual aunque no esté configurada en una interfaz de red física. Los contenedores tales como dominios xVM o zonas IP exclusivos se configuran conforme a interfaces de red virtual (VNIC) para formar una red virtual.
interfaz física	Conexión de un sistema con un enlace. Esta conexión se suele implementar entre un controlador de dispositivo y una tarjeta de interfaz de red. Algunas tarjetas de interfaz de red pueden presentar varios puntos de conexión, por ejemplo, <code>igb</code> .
IP	Consulte protocolo de Internet (IP) , IPv4 , IPv6 .
IP en encapsulado IP	Mecanismo para colocar en túneles paquetes IP dentro de paquetes IP.
IPQoS	Función de software que permite la implementación del estándar modelo DiffServ , además de contabilidad de flujo y marcación 802.1 D para LAN virtuales. Mediante IPQoS se pueden proporcionar varios niveles de servicios de red a clientes y aplicaciones, según lo que se establezca en el archivo de configuración de IPQoS.
IPsec	Seguridad IP. Arquitectura de seguridad que proporciona protección a los datagramas IP.
IPv4	Internet Protocol version 4. IPv4 en ocasiones se denomina IP. Esta versión admite un espacio de direcciones de 32 bits.
IPv6	Internet Protocol version 6. IPv6 admite espacio de direcciones de 128 bits.
lista de revocación de certificados (CRL)	Lista de certificados de claves públicas revocados por una autoridad de certificación. Estas listas se almacenan en la base de datos de CRL que se mantiene con IKE.
marcador	<ol style="list-style-type: none">Módulo de la arquitectura DiffServ e IPQoS que marca el campo DS de un paquete IP con un valor que indica la forma en que se reenvía el paquete. En la implementación de IPQoS, el módulo <code>marker</code> es <code>ds_cpmk</code>.Módulo de la implementación de IPQoS que marca la etiqueta de LAN virtual de un datagrama de Ethernet con un valor de prioridad de usuario. El valor de prioridad de usuario indica la forma en que los datagramas deben reenviarse en una red con dispositivos VLAN. Este módulo se denomina <code>d_lcosmk</code>.
MD5	Una función de hash criptográfica iterativa utilizada para autenticar mensajes, incluso las firmas digitales. Rivest desarrolló esta función en 1991.
medidor	Módulo de la arquitectura DiffServ que mide la velocidad del flujo de tráfico de una determinada clase. La implementación de IPQoS presenta dos medidores, <code>tokenmt</code> y <code>tswtclmt</code> .
modelo DiffServ	Estándar de arquitectura de Internet Engineering Task Force para implementar distintas clases de servicios en redes IP. Los módulos principales son <code>classifier</code> (clasificador), <code>meter</code> (medidor), <code>marker</code> (marcador), <code>scheduler</code> (programador) y <code>dropper</code> (descartador). IPQoS implementa los módulos <code>classifier</code> , <code>meter</code> y <code>marker</code> . El modelo DiffServ se describe en RFC 2475, <i>An Architecture for Differentiated Services</i> .
MTU	Siglas en inglés de Maximum Transmission Unit, unidad de transmisión máxima. El tamaño, en octetos, que puede transmitirse por un enlace. Por ejemplo, una red Ethernet tiene una MTU de 1500 octetos.
NAT	Consulte traducción de la dirección de red .

nodo	En IPv6, cualquier sistema compatible con IPv6, ya sea host o enrutador.
nombre de keystore	Nombre que un administrador asigna a un área de almacenamiento o keystore, en una tarjeta de interfaz de red . El nombre de keystore también se denomina token o ID de token.
paquete	Grupo de información que se transmite como una unidad a través de líneas de comunicaciones. Contiene un encabezado IP y una carga útil .
paquete icmp echo request	Paquete que se envía a un sistema en Internet para solicitar una respuesta. Esta clase de paquetes suelen denominarse "ping".
PFS (Perfect Forward Secrecy)	En PFS, la clave que se emplea para proteger la transmisión de datos no se aplica en la derivación de claves adicionales. La fuente de la clave que se usa para proteger la transmisión de datos tampoco se emplea en la derivación de claves adicionales. PFS sólo se aplica en el intercambio de claves autenticadas. Consulte también protocolo de Diffie-Hellman .
PHB (Per-Hop Behavior, comportamiento por salto)	Prioridad que se asigna a una clase de tráfico. PHB indica la prioridad que tienen los flujos de datos de esa clase respecto a otras clases de tráfico.
pila	Consulte pila de IP .
pila de IP	TCP/IP se suele denominar "pila". Este término designa las capas (TCP, IP y en ocasiones otras) a través de las cuales se transfieren todos los datos en los extremos de cliente y servidor de un intercambio de datos.
pila de protocolos	Consulte pila de IP .
pila doble	Pila de protocolo TCP/IP con IPv4 e IPv6 en la capa de red; el resto de la pila permanece idéntico. Si al instalar Oracle Solaris se habilita IPv6, el sistema recibe la versión de pila doble de TCP/IP.
PKI	Siglas en inglés de Public Key Infrastructure, infraestructura de clave pública. Sistema de certificados digitales, autoridades de certificación y otras autoridades de registro que verifican y autentican la validez de cada parte que interviene en una transacción por Internet.
prioridad de usuario	Valor de 3 bits que implementa marcas de CoS (Class-of-Service, clase de servicio), que definen la forma en que los datagramas de Ethernet se reenvían en una red de dispositivos VLAN.
protocolo de Diffie-Hellman	También se lo denomina "criptografía de claves públicas". Se trata de un protocolo de claves criptográficas asimétricas que desarrollaron Diffie y Hellman en 1976. Este protocolo permite a dos usuarios intercambiar una clave secreta mediante un medio no seguro, sin ningún otro secreto. El protocolo IKE utiliza el de Diffie-Hellman.
protocolo de Internet (IP)	Método o protocolo con el cual se envían datos de un sistema a otro por Internet.
punto de código DS	Valor de 6 bits que, al incluirse en el campo DS o un encabezado IP, indica la manera en que se reenvía un paquete.

reconfiguración dinámica (DR)	Función que permite volver a configurar un sistema aunque esté ejecutándose, sin apenas afectar o sin afectar en absoluto a los procesos que estén en curso. No todas las plataformas Sun de Oracle admiten DR. Es posible que algunas plataformas sólo admitan DR de determinados tipos de hardware, como NIC.
red privada virtual (VPN)	Una sola red lógica y segura que emplea túneles en una red pública como Internet.
red virtual	Se trata de una combinación de recursos de red de software y hardware y de funciones que se administran de manera conjunta como una única entidad de software. Una red virtual <i>interna</i> consolida los recursos de red en un único sistema, el cual en ocasiones se denomina “red en una caja”.
redireccionar	En un enrutador, proceso para informar a un host sobre un primer salto más apropiado para llegar a un determinado destino.
repetición de ataque	En IPsec, ataque en el cual un intruso se apropia de un paquete. El paquete almacenado sustituye o repite el original posteriormente. Para protegerse contra tales ataques, un paquete puede contener un campo que se incrementa durante la vida útil de la clave secreta que protege el paquete.
resultado	Acción que se realiza como consecuencia de la medición del tráfico. Los medidores de IPQoS tienen tres resultados, rojo, amarillo y verde, que se definen en el archivo de configuración de IPQoS.
RSA	Método para la obtención de firmas digitales y criptosistemas de claves públicas. Dicho método lo describieron sus creadores, Rivest, Shamir y Adleman, en 1978.
SA	Consulte SA (Security Association) .
SA (Security Association)	Asociación que establece las propiedades de seguridad entre un primer host y un segundo.
SADB	Siglas en inglés de Security Associations Database, base de datos de asociaciones de seguridad. Tabla en la que se especifican claves y algoritmos criptográficos. Las claves y los algoritmos se utilizan en la transmisión segura de datos.
salto	Medida que se usa para identificar la cantidad de enrutadores que hay entre dos hosts o sistemas. Si un origen y un destino están separados por tres enrutadores, los sistemas están a una distancia de cuatro saltos.
SCTP	Consulte protocolo SCTP (Streams Control Transport Protocol).
SCTP	Siglas en inglés de Stream Control Transport Protocol, protocolo de transporte de control del flujo. Protocolo de capas de transporte que brinda comunicaciones relativas a las conexiones de manera parecida a TCP. Además, SCTP permite varias direcciones permanentes, en que uno de los puntos finales de la conexión puede tener más de una dirección IP.
selector	Elemento que define los criterios de aplicación en los paquetes de una determinada clase, a fin de seleccionar ese tráfico en el flujo de datos de la red. Los selectores se definen en la cláusula de filtro en el archivo de configuración de IPQoS.
servidor proxy	Servidor que se emplaza entre una aplicación cliente, por ejemplo un navegador de web, y otro servidor. Se utiliza para filtrar solicitudes, por ejemplo para impedir el acceso a determinados sitios web.

SHA-1	Siglas en inglés de Secure Hashing Algorithm, algoritmo de hash seguro. El algoritmo funciona en cualquier tamaño de entrada que sea inferior a 2^{64} para generar un resumen del mensaje. El algoritmo SHA-1 es la entrada de DSA.
sniff	Acceso no autorizado a redes de equipos; con frecuencia se usa como parte de programas automatizados para tamizar información, por ejemplo contraseñas de texto no cifrado, de última hora.
solicitud de enrutador	Proceso de los hosts que solicitan enrutadores para la generación inmediata de anuncios de enrutador, en lugar de hacerlo la próxima vez que se hubiera programado.
solicitud de vecino	Solicitud enviada por un nodo para determinar la dirección de capa de enlace de un vecino. Asimismo, una solicitud de vecino verifica que se pueda contactar con un vecino mediante una dirección de capa de enlace almacenada en la antememoria.
SPD	Consulte base de datos de directivas de seguridad (SPD) .
SPI	Consulte índice de parámetros de seguridad .
spoof	Obtener acceso no autorizado a un equipo mediante el envío de un mensaje con una dirección IP indicando que el mensaje procede de un host de confianza. Para efectuar spoofing en IP, el agresor debe recurrir a una serie de técnicas para averiguar la dirección IP de un host de confianza; a continuación, debe modificar los encabezados de paquete para suplantar dicha identidad y simular que los paquetes proceden de ese host.
tarjeta de interfaz de red	Tarjeta de adaptador de red que actúa como interfaz de una red. Algunas tarjetas de interfaz de red pueden tener varias interfaces físicas, por ejemplo la tarjeta igb.
TCP/IP	TCP/IP (Transmission Control Protocol/Internet Protocol) es el protocolo o lenguaje de comunicaciones básico de Internet. También se usa como protocolo de comunicaciones en redes privadas (tanto intranets como extranets).
traducción de la dirección de red	También se conoce como NAT (del inglés Network Address Translation). Traducción de una dirección IP que se utiliza en una red a otra dirección IP conocida en otra red. Se utiliza para limitar la cantidad de direcciones IP globales que se necesitan.
Triple-DES	Acrónimo en inglés de Triple-Data Encryption Standard. Método de cifrado de claves simétricas. Triple-DES necesita un tamaño de clave de 168 bits. Triple-DES también se escribe 3DES.
túnel	La ruta a la que sigue un datagrama cuando se encapsula. Consulte encapsulado .
túnel bidireccional	Túnel capaz de transmitir datagramas en ambos sentidos.
túnel inverso	Túnel que comienza en la dirección de auxilio del nodo móvil y termina en el agente interno.
valor hash	Número que se genera a partir de una cadena de texto. Las funciones hash se usan para asegurarse de que no se alteren los mensajes transmitidos. MD5 y SHA-1 son ejemplos de funciones hash de una dirección.

Índice

A

agente LLDP, *Ver* LLDP, agentes
agregaciones
 configuraciones
 con nodo, 239
 de extremo a extremo, 239
 crear, 242–244
 definición, 237
 directiva de equilibrio de la carga, 240
 distribuciones
 básicas, 238
 eliminación de enlaces, 246–247
 funciones, 237
 modificar, 244–245
 requisitos, 241
agregaciones de vínculos, *Ver* agregaciones
agrupación de anillos
 Ver también asignación de anillos
 dinámica y estática, 393–407
agrupación dinámica de anillos, *Ver* agrupación de anillos
agrupación estática de anillos, *Ver* agrupación de anillos
anillos, transmisión y recepción, 393–407
anillos de hardware, 393–407
archivo `/etc/default/mpathd`
 Ver IPMP, archivo de configuración
archivo `/net/if_types.h`, 299
asignación de anillos
 Ver también agrupación de anillos
 en VLAN, 394
 pasos para la implementación, 395
asignación de CPU, 411–412

ATM, compatibilidad con IPMP para, 299

B

BSSID, *Ver* Wi-Fi

C

clientes basados en hardware, 393
clientes MAC, 393
 asignación de anillos, 395
 basados en hardware, 393, 395
 basados en software, 393, 399
 configuración, 395
comando `dladm`
 configurar una VLAN, 254–257
 enlaces de datos
 cambio de nombre, 158
 cambio de tamaño MTU, 163–165
 eliminación de enlaces de datos, 161
 visualización de atributos físicos, 159
 visualización de información sobre, 160
 modificación de una agregación, 245
 para configuración Wi-Fi, 211
 para la gestión de recursos de red, 391
comando `d1stat`, 417, 421
 show-phys, 423–425
comando `flowadm`, 412–416
 gestión de recursos en flujos, 391
comando `flowstat`, 417

comando `ifconfig`
 comprobación de orden de módulos
 STREAMS, 299
 y comando `ipadm`, 202

comando `ipadm`
 administración de propiedades de TCP/IP, 177
 conexión de una interfaz, 182
 configuración de interfaces IP, 181
 configuración de propiedades de direcciones IP, 185
 creación de interfaces IPMP, 302–304
 eliminación de una interfaz, 243
 subcomandos para IPMP, 303
 supervisión de interfaces, 196
 y comando `ifconfig`, 202

comando `impstat`, 265–266, 277, 295, 315–323

comando `netstat`, comprobación de flujo de paquetes
 sobre un enlace Wi-Fi, 215

configuración, protección de enlaces, 385–387

configuración de conmutador
 en una topología de agregación, 238
 protocolo de control de agregación de vínculos
 (LACP), 241

configuración de enlace persistente, creación, 184

configuración de la clave WEP, 216

configuración del conmutador, modos del protocolo de
 control de agregación de enlaces (LACP), 245

consideraciones de seguridad, Wi-Fi, 216

control de flujo, *Ver* flujos

control de recursos, *Ver* gestión de recursos de red

CPU dedicadas para interfaces, 411–412

D

daemon `in.mpathd`, *Ver* IPMP, daemon `in.mpathd`

destino de sondeo, en IPMP, definición, 292

destinos de sondeo, en IPMP, 276

detección de fallos, en IPMP, 279, 288
 basada en sondeos, 280–281
 detección de fallos basada en enlaces, 282
 tiempo de detección, 280–281

detección de fallos basada en enlaces, 282

detección de fallos basada en sondeos, 280–281
Ver también IPMP, direcciones de prueba
Ver también IPMP, sin las direcciones de prueba

detección de fallos basada en sondeos (*Continuación*)
 configuración de sistemas de destino, 309–313
 sondeo transitivo, 280
 y direcciones de prueba, 280–281

dirección local de enlace, en IPMP, 279

dirección MAC
 comprobar exclusividad, 179–181
 requisito para IPMP, 298–300

direcciones de datos, *Ver* IPMP, direcciones de datos

direcciones de prueba
Ver IPMP, direcciones de prueba

direcciones IP, propiedades, 185

directivas, para agregaciones, 240

E

enlaces de datos
Ver también comando `dladm`
 administración de propiedades de enlaces, 156
 cambio de nombre de un enlace, 158
 configuración de una interfaz de IP por un link, 182
 convenciones de denominación, 26–31
 eliminación de enlaces de datos, 161
 módulo STREAMS, 174
 nombres de enlace, 29–31
 uso en configuraciones IPMP, 269–270
 nombres de enlaces, 26–31
 parámetros de Ethernet, 166–168
 parámetros de velocidad de enlace, 165–166
 reglas para usar nombres personalizados, 31
 tamaños MTU, 163–165
 visualización de información sobre, 160

equilibrio de la carga, entre agregaciones, 240

ESSID, *Ver* Wi-Fi

estadísticas de la red, *Ver* supervisión del uso de la red

estadísticas de tráfico de red, por anillo, 423–425

estructura del gestor de coordinación de
 reconfiguración (RCM), 285–286

expansión de carga, 267, 290

F

fallos de grupo, IPMP, 281

falsificación, protección de enlaces, 383–385
 flujos, 390, 412–416

G

gestión de recursos de red, 389
 comandos `dladm` para la implementación, 391
 en enlaces, 389
 mediante flujos, 390
 grupo anónimo, 282, 288
 grupo IPMP, 289
 Ver también interfaz IPMP
 adición de una interfaz a un grupo, 306
 adición o eliminación de direcciones, 307–308
 conexión de nuevas NIC mediante DR, 284–285
 configuración con DHCP, 300–302
 eliminación de NIC mediante DR, 285
 eliminar una interfaz de un grupo, 306–307
 fallos de grupo, 281
 mover una interfaz entre grupos, 308
 reemplazo de NIC mediante DR, 285–286
 tareas de planificación, 298–300
 visualización de información sobre, 315–323

I

interfaces
 configuración
 interfaces Wi-Fi, 210
 por un enlace de datos, 182
 configurar
 como parte de una VLAN, 254–257
 en agregaciones, 242–244
 creación de una configuración persistente, 184
 detección de reparaciones con IPMP, 282–284
 en espera, en IPMP, 277
 orden de los módulos STREAMS en una
 interfaz, 299
 tipos de configuración en IPMP, 277
 tipos de Wi-Fi, 209
 verificar exclusividad de dirección MAC, 179–181
 VLAN, 249–263

interfaces activas-activas
 IPMP, 302–304, 304–305
 interfaces activas/activas, IPMP, 277
 interfaces activas/en espera, IPMP, 277
 interfaces inalámbricas, *Ver* Wi-Fi
 interfaz en espera
 Ver también comando `ifconfig`, opciones para
 IPMP
 rol en un grupo IPMP, 277
 interfaz física, 238–239
 Ver también interfaces
 interfaz IPMP, 265–266, 289
 configuración para grupos IPMP, 302–304
 fallo de interfaces subyacentes, 270
 visualización de información sobre, 270, 315–323
 interfaz no utilizable, 293
 interfaz subyacente, 292
`ip-nospoof`, tipos de protección de enlaces, 384
`ipadm`
 `set-addrprop`, 185
 `show-addrprop`, 185
 IPMP
 administración, 306–309
 archivo de configuración, 276, 312–313
 compatibilidad con ATM, 299
 compatibilidad con Ethernet, 299
 compatibilidad con Token ring, 299
 componentes de software, 276
 configuración de sistemas de destino, 310–311
 `daemon.in.mpathd`, 276, 281
 descripción general, 266–267
 destino de sondeo, 292
 detección de fallos, 279, 280–281, 288
 detección de reparaciones, 282–284
 direcciones de datos, 278, 286
 direcciones de prueba, 278
 expansión de carga, 267, 290
 grupo anónimo, 282, 288
 reconfiguración dinámica, 284–286, 287
 reemplazo de interfaces, DR, 313–314
 requisitos básicos, 298–300
 requisitos IP, 279
 terminología, 286
 tipos de configuración de interfaz, 277

IPMP (Continuación)

- tráfico de sondeos, 280–281
- visualización de información con `ipmpstat`, 315–323
- y agregaciones de enlaces, 268–269

L

- LLDP, 325
 - agentes, 327–331
 - componentes en Oracle Solaris, 325–326
 - modos de operación, 327–331
 - unidades TLV, 328–331
- LLDPU, *Ver* LLDP, unidades de TLV

M

- `mac-nospoof`, tipos de protección de enlaces, 384
- MIB, 327–331
- migración de direcciones, 266
 - Ver también* IPMP, direcciones de datos
- modo `FAILBACK=no`, 283
- módulos STREAMS, y enlaces de datos, 174
- MTU, *Ver* unidad de transmisión máxima
- múltiples rutas de redes IP (IPMP), *Ver* IPMP

N

- nombres de enlaces, *Ver* enlaces de datos
- nombres personalizados, *Ver* enlaces de datos, nombres de enlaces
- nuevas funciones, Wi-Fi, 208

P

- parámetros TCP/IP, configuración con el comando `ipadm`, 177
- perfiles de configuración de red (NCP), 151–152
- pila de red, 22, 24
- propiedad `CPU pool`, 407
- protección de enlaces, 383–385

protección de enlaces (Continuación)

- configuración, 385–387
- protocolo de control de agregación de enlaces (LACP), modificación de modos del LACP, 245
- protocolo de control de agregación de vínculos (LACP), modos, 241
- puertos con privilegios, configuración con el comando `ipadm`, 192
- punto de acceso, Wi-Fi, 208, 210
- punto físico de conexión (PPA), 252

R

- reconfiguración dinámica (DR)
 - Ver también* tarjeta de interfaz de red (NIC)
 - definición, 287
 - flexibilidad con los nombres de enlace personalizados, 31
 - interoperación con IPMP, 313–314
 - interoperatividad con IPMP, 284–286
 - sustitución de NIC, 171
 - trabajo con interfaces, IPMP, 284–285, 285, 313–314
- recurso de agrupación de CPU, asignación a enlaces, 409
- `restricted`, tipos de protección de enlaces, 384

S

- sistema de destino, en IPMP, configuración manual, 310–311
- sondeo transitivo, 280
- supervisión de interfaz, mediante el comando `ipadm`, 196
- supervisión del uso de la red, 417

T

- tarjeta de interfaz de la red (NIC)
 - fallo y conmutación por error, 288
 - reconfiguración dinámica, 287
 - reemplazo con DR, 285–286

tarjeta de interfaz de red (NIC)
 parámetros de velocidad de enlace, 165–166
 propiedades públicas y privadas de controladores NIC, 162
 reemplazo, con DR, 313–314
 sustitución, con DR, 171
 valores de parámetros de Ethernet, 166–168
 tiempo de detección de reparaciones, 282–284
 tipos de protección de enlaces, 384–385
 ip-nospoof, 384
 mac-nospoof, 384
 restricted, 384
 TLV, *Ver* LLDP, unidades de TLV
 Token ring, compatibilidad con IPMP para, 299
 tráfico de sondeos, 280–281
 tramas gigantes, habilitación de compatibilidad con, 163–165
 truncaciones, *Ver* agregaciones

U

unidad de transmisión máxima (MTU), 163–165

V

vías de red, 389
 vías de hardware, 417
 vías de software, 417
 virtualización y calidad de servicio, 389
 VLAN
 configuración, 249–263
 configuraciones, 250–252
 creación sobre agregaciones de enlaces, 257–258
 definición, 249–263
 escenarios de muestra, 249
 nombres de VLAN, 252
 planificar, 253–254
 PPA hack, 252
 punto físico de conexión (PPA), 252

VNIC

asignación de recursos de agrupación de CPU, 409
 asociación, 374–378

W

Wi-Fi

cifrado de una conexión, 216
 conexión a una red Wi-Fi, 210
 conexión con una red Wi-Fi, 211, 212
 definición, 208
 ejemplo, configuración de la velocidad de un enlace, 215
 ejemplo de comunicaciones cifradas, 218
 ejemplo de configuración Wi-Fi, 213
 enlaces Wi-Fi seguros, 216
 especificación IEEE 802.11, 208
 generación de la clave WEP, 216
 ID de conjunto de servicios básicos (BSSID, Basic Service Set ID), 211
 ID de conjunto de servicios extendidos (ESSID, Extended Service Set ID), 211
 interfaces admitidas, 209
 preparación de un sistema para ejecutar Wi-Fi, 209
 supervisión de un enlace, 214
 tipos de redes Wi-Fi, 208
 zona activa, 208

Z

zona activa, Wi-Fi
 búsqueda de una zona activa, 209
 definición, 208

