Gestión de enlaces de datos de red en Oracle® Solaris 11.2

Referencia: E53795-02
Septiembre de 2014

ORACLE

Contenido

Uso de esta documentación

- **Descripción general**: proporciona una descripción general de las funciones avanzadas que se utilizan para gestionar los enlaces de datos de red a fin de mejorar el rendimiento de la red. Describe cómo combinar enlaces en agregaciones mediante la agregación DLMP o de troncos, cómo dividir la red en subredes mediante redes de área local virtuales, cómo conectar segmentos de red separados mediante puentes, cómo intercambiar información de conectividad de red mediante el protocolo de descubrimiento de capa de enlace y cómo gestionar redes convergentes por medio del puente de centro de datos.
- **Destinatarios**: administradores de sistemas.
- **Conocimientos necesarios**: conocimientos básicos y algunos conocimientos avanzados sobre administración de redes.

Biblioteca de documentación del producto

En la biblioteca de documentación (http://www.oracle.com/pls/topic/lookup?ctx=E36784), se incluye información de última hora y problemas conocidos para este producto.

Acceso a My Oracle Support

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

Comentarios

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

♦ ♦ ♦ CAPÍTULO 1

Introducción a la gestión de enlaces de datos de red

En este capítulo, se presentan las funciones avanzadas que se utilizan para gestionar los enlaces de datos de red, que se describen en los siguientes capítulos de este libro. El uso de las distintas tecnologías descritas en este manual depende de circunstancias específicas. Asimismo, es posible que algunas configuraciones de hardware requieran el uso de un determinado tipo de función. Por lo tanto, no es necesario que complete todos los procedimientos de configuración que se incluyen en este manual. Por el contrario, seleccione e implemente las tecnologías que satisfagan sus requisitos de red.

Antes de realizar cualquiera de las configuraciones que se describen en este manual, debe haber completado la configuración de red básica y contar con conocimientos acerca de la configuración esencial de los enlaces de datos. Para obtener información sobre la configuración de red básica, consulte "Configuración y administración de componentes de red en Oracle Solaris 11.2 ". Para obtener información acerca de elementos de la gestión de la configuración de enlaces, consulte Capítulo 2, "Administración de la configuración de enlaces de datos en Oracle Solaris" de "Configuración y administración de componentes de red en Oracle Solaris 11.2 ".

Para obtener un resumen de las funciones de configuración de redes de Oracle Solaris, consulte Capítulo 1, "Resumen de la administración de redes en Oracle Solaris" de "Estrategias de administración de redes en Oracle Solaris 11.2 ".

Este capítulo se divide en los siguientes apartados:

Novedades de gestión de enlaces de datos de red de Oracle Solaris 11.2

Para los clientes existentes, esta sección destaca los siguientes cambios clave en esta versión:

- **Detección de fallos basada en sondeos en agregaciones de rutas múltiples de enlaces de datos (DLMP)**: detecta la pérdida de conectividad entre los enlaces agregados de DLMP y los destinos configurados. Este tipo de detección de fallos aborda las limitaciones del mecanismo de detección de fallos basada en enlaces, que sólo puede detectar los fallos provocados por la pérdida de conexión directa entre el enlace de datos y el conmutador de primer salto. Para obtener más información, consulte “Detección de fallos en la agregación DLMP” [23].
- **Transmisión de los valores recomendados de la selección de transmisión mejorada (ETS) al par**: la función ETS en el puente de centro de datos (DCB) se mejoró para permitir al host de Oracle Solaris recomendar recursos compartidos de ancho de banda al conmutador del siguiente salto en la red de DCB. Para obtener más información, consulte “Recomendación de configuración de ETS para el par” [116], “Configuración de las propiedades de enlace de datos relacionadas con ETS” [114] y el Ejemplo 6-8, “Cómo ver la capacidad del host local para sincronizar información de ETS”.
- **Visualización del valor real de las propiedades de enlace de datos**: el subcomando `dladm show-linkprop` se mejoró para mostrar el campo `EFFECTIVE` para algunas propiedades de enlace de datos. Los valores para el campo `EFFECTIVE` son determinados por el sistema según la disponibilidad del recurso, la capacidad del dispositivo subyacente o las negociaciones con el par. El valor activo no siempre es el mismo que el valor configurado. Una propiedad de enlace de datos puede tener un valor determinado, aunque la propiedad no esté configurada con un valor. Para obtener un ejemplo sobre cómo visualizar el campo `EFFECTIVE`, consulte “Visualización de propiedades de enlaces de datos” [110] and Ejemplo 6-7, “Cómo ver las propiedades de enlace de datos relacionadas con la ETS”.
- **Visualización de estadísticas de puentes**: el subcomando `dlstat show-bridge` muestra las estadísticas de los puentes y las estadísticas de los enlaces conectados a cada puente, y también muestra la vista anidada de las estadísticas de puentes. Para obtener más información, consulte “Visualización de información sobre puentes configurados” [77].

Funciones y componentes que se utilizan para gestionar los enlaces de datos de red

La gestión de los enlaces de datos de red hace referencia al uso de funciones y tecnologías para ajustar con precisión la manera en que los sistemas procesan el tráfico de red. Los sistemas que se configuran con estas tecnologías pueden gestionar mejor el tráfico de red, lo cual contribuye a la mejora del rendimiento total de la red. Aunque estas funciones abordan diferentes áreas de las operaciones de red, proporcionan beneficios comunes, como conectividad de red, administración de redes y eficacia.

Agregaciones de enlaces

Las agregaciones de enlaces le permiten agrupar recursos de varios enlaces de datos para administrarlos como una sola unidad. Puede mejorar el ancho de banda y proporcionar alta disponibilidad para las aplicaciones mediante la combinación de varias NIC físicas. La agregación de enlaces de datos de red garantiza que el sistema tenga acceso continuo a la red. La agregación de troncos y la agregación DLMP son los dos tipos de agregación de enlaces.

La agregación de troncos proporciona ancho de banda consolidado de los enlaces de datos subyacentes para los clientes configurados a través de la agregación. La agregación DLMP proporciona alta disponibilidad en varios conmutadores para los clientes configurados a través de la agregación. La agregación DLMP también admite la detección de fallos basada en enlaces y la detección de fallos basada en sondeos a fin de garantizar la disponibilidad continua de la red para enviar y recibir tráfico. Para obtener más información sobre los distintos tipos de agregación de enlaces y los procedimientos para configurar y administrar las agregaciones de enlaces, consulte el Capítulo 2, Configuración de alta disponibilidad mediante agregaciones de enlaces.

Redes de área local virtuales

Las redes de área local virtuales (VLAN) permiten dividir la red en subredes sin tener que agregar recursos al entorno de red física. Por lo tanto, las subredes son virtuales y se usan los mismos recursos de red física. Las VLAN proporcionan a las aplicaciones subredes aisladas a fin de que sólo las aplicaciones de la misma red VLAN puedan comunicarse entre sí. Puede configurar varias redes virtuales dentro de una única unidad de red, por ejemplo, un conmutador, mediante la combinación de VLAN y Oracle Solaris Zones. Para obtener más información sobre las redes VLAN y los procedimientos para configurarlas y administrarlas, consulte el Capítulo 3, Configuración de redes virtuales mediante redes de área local virtuales.

Redes con puentes

Los puentes conectan segmentos de red independientes y actúan como rutas entre dos nodos. Cuando están conectados por un puente, los segmentos de red se comunican como si fueran un solo segmento de red. Los puentes utilizan un mecanismo de reenvío de paquetes para conectar subredes y permitir a un sistema transmitir paquetes a sus destinos mediante las rutas de conexión más cortas. Para obtener más información sobre las redes con puentes y los procedimientos para administrar puentes, consulte Capítulo 4, Administración de funciones de puente.

Protocolo de descubrimiento de capa de enlace

El protocolo de descubrimiento de capa de enlace (LLDP) permite el intercambio de información de gestión y conectividad entre los sistemas de la red para fines de detección de topología. En esta información, puede que se incluyan las capacidades del sistema, las direcciones de gestión y otros aspectos relativos al funcionamiento de redes. El servicio de diagnósticos de red utiliza LLDP para detectar problemas que puedan provocar conectividad de red limitada o degradada. Para obtener más información sobre LLDP y los procedimientos para configurar LLDP, consulte el Capítulo 5, Intercambio de información de conectividad de red con el protocolo de descubrimiento de capa de enlace.

Puente del centro de datos

El puente del centro de datos (DCB) se utiliza para gestionar el ancho de banda, la prioridad relativa y el control de flujo de varios tipos de tráfico al compartir el mismo enlace de red, por ejemplo, cuando se comparte un enlace de datos entre los protocolos de almacenamiento y de redes. El DCB permite el intercambio de información entre iguales sobre las funciones que admiten la red convergente mediante LLDP. La información está relacionada con las configuraciones que afectan la integridad de los paquetes de red, especialmente en entornos de gran volumen de tráfico, como los centros de datos. DCB permite una infraestructura de red eficaz mediante la consolidación de la red de área de almacenamiento (SAN) y la red de área local (LAN), lo cual reduce los costos operativos y de gestión en los centros de datos.

Puede configurar las funciones de DCB, como el control de flujo basado en prioridades (PFC), para la prevención de pérdidas de paquetes y la selección de transmisión mejorada (ETS) para el uso compartido de ancho de banda entre paquetes en función de las prioridades de la clase de servicio (CoS). Para obtener más información, consulte el Capítulo 6, Gestión de redes convergentes mediante el puente de centro de datos.

♦ ♦ ♦ CAPÍTULO 2

Configuración de alta disponibilidad mediante agregaciones de enlaces

En este capítulo, se proporciona una descripción general de las agregaciones de enlaces y se describen los procedimientos para configurar y administrar las agregaciones de enlaces.

Este capítulo se divide en los siguientes apartados:

Descripción general de agregaciones de enlaces

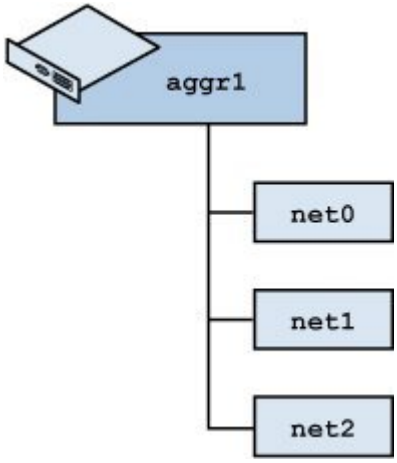
La agregación de enlaces es un método para combinar varios enlaces de datos físicos en un sistema a fin de mejorar el ancho de banda para las aplicaciones. Estos enlaces de datos físicos se configuran juntos como una sola unidad lógica para aumentar el rendimiento del tráfico de red y para lograr alta disponibilidad en la capa de enlace de datos.

Puede incluir cualquier agregación de enlaces que se muestre en las NIC disponibles como una interfaz individual mediante Oracle Enterprise Manager Ops Center. También puede mostrar los

detalles de la agregación DLMP y de troncos mediante Oracle Enterprise Manager Ops Center. Para obtener más información acerca de Oracle Enterprise Manager Ops Center, consulte http://www.oracle.com/pls/topic/lookup?ctx=oc122&id=OPCCM.

En la siguiente figura, se muestra un ejemplo de una agregación de enlaces simple configurada en un sistema.

FIGURA 2-1 Configuración de agregación de enlaces



La ilustración muestra una agregación `aggr1` que consta de tres enlaces de datos subyacentes, `net0`, `net1` y `net2`. Estos enlaces de datos se dedican para dar lugar al tráfico que atraviesa el sistema por medio de la agregación. Los enlaces subyacentes se ocultan de las aplicaciones externas. En su lugar, el enlace de datos lógico `aggr1` es accesible.

Ventajas de la agregación de enlaces

La agregación de enlaces tiene las siguientes ventajas:

- **Ancho de banda ampliado**: la capacidad de varios enlaces se combina en un enlace lógico.
- **Failover y failback automáticos**: el tráfico de un enlace con errores se conmuta automáticamente a otros enlaces activos en la agregación, por lo que se logra una alta disponibilidad.
- **Administración mejorada**: todos los enlaces subyacentes se administran como una única unidad.
- **Menos drenaje en la agrupación de direcciones de red**: puede asignarse una dirección IP a la agregación completa.

Dado que la agregación de enlaces agrupa varios enlaces en un único enlace de datos lógico, las funciones de los enlaces de datos como la protección de enlaces y la gestión de recursos funcionan bien con las agregaciones de enlaces. Para obtener información sobre la protección de enlaces, consulte el Capítulo 1, “Uso de protección de enlaces en entornos virtualizados” de “Protección de la red en Oracle Solaris 11.2 ”. Para obtener información sobre la gestión de recursos, consulte el Capítulo 7, “Gestión de recursos de red” de “Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ”.

La agregación de enlaces supera algunos de los problemas que se enfrentan al utilizar las funciones de alta disponibilidad con la virtualización de redes, por ejemplo, IPMP. Con la agregación de enlaces, la agregación se crea primero en una zona global y, a continuación, se especifica como el enlace subyacente al configurar la zona no global. Cuando se inicia la zona, se le asigna una tarjeta de interfaz de red virtual (VNIC) en la agregación de enlaces. A diferencia de IPMP, que se debe configurar en cada zona no global, las agregaciones de enlaces sólo se configuran en las zonas globales y proporcionan VNIC de alta disponibilidad a las zonas no globales. La zona global también puede configurar propiedades como el ancho de banda en las VNIC asignadas a la zona.

Nota - Las agregaciones de enlaces ejecutan funciones similares a las de las rutas múltiples de red IP (IPMP) para mejorar el rendimiento y la disponibilidad de la red en la capa de enlace de datos. Para ver una comparación de estas dos tecnologías, consulte Apéndice A, Agregaciones de enlaces e IPMP: comparación de funciones.

Se admiten los siguientes tipos de agregaciones de enlaces:

- Agregaciones de troncos
- Agregaciones de rutas múltiples de enlaces de datos (DLMP)

Para conocer las diferencias entre los dos tipos de agregación de enlaces, consulte “Comparación entre la agregación DLMP y de troncos” [41].

Agregaciones de troncos

Las agregaciones de troncos se basan en el estándar IEEE 802.3ad y funcionan mediante la activación de varios flujos de tráfico que se distribuyen en un conjunto de puertos agregados. El estándar IEEE 802.3ad requiere configuración del conmutador, además de extensiones de propiedad del proveedor del conmutador para poder trabajar en varios conmutadores. En las agregaciones de troncos, los clientes configurados por medio de las agregaciones obtienen un ancho de banda consolidado de los enlaces subyacentes, ya que cada puerto de red está asociado con cada enlace de datos configurado por medio de la agregación. Al crear una agregación de enlaces, de manera predeterminada, la agregación se crea en el modo de tronco. Puede utilizar una agregación de troncos en las siguientes situaciones:

- Para los sistemas de la red ejecutan aplicaciones con un gran volumen de tráfico distribuido, puede dedicar una agregación de troncos al tráfico de dicha aplicación para aprovechar el aumento del ancho de banda.
- 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 la agregación de troncos de enlaces de datos.
- Para las ubicaciones que necesitan ocultar enlaces de datos internos, la dirección IP de la agregación de troncos oculta estos enlaces de datos de las aplicaciones externas.
- Para las aplicaciones que necesitan una conexión de red confiable, la agregación de troncos protege las conexiones de red contra errores de enlace.

La agregación de troncos admite las siguientes funciones:

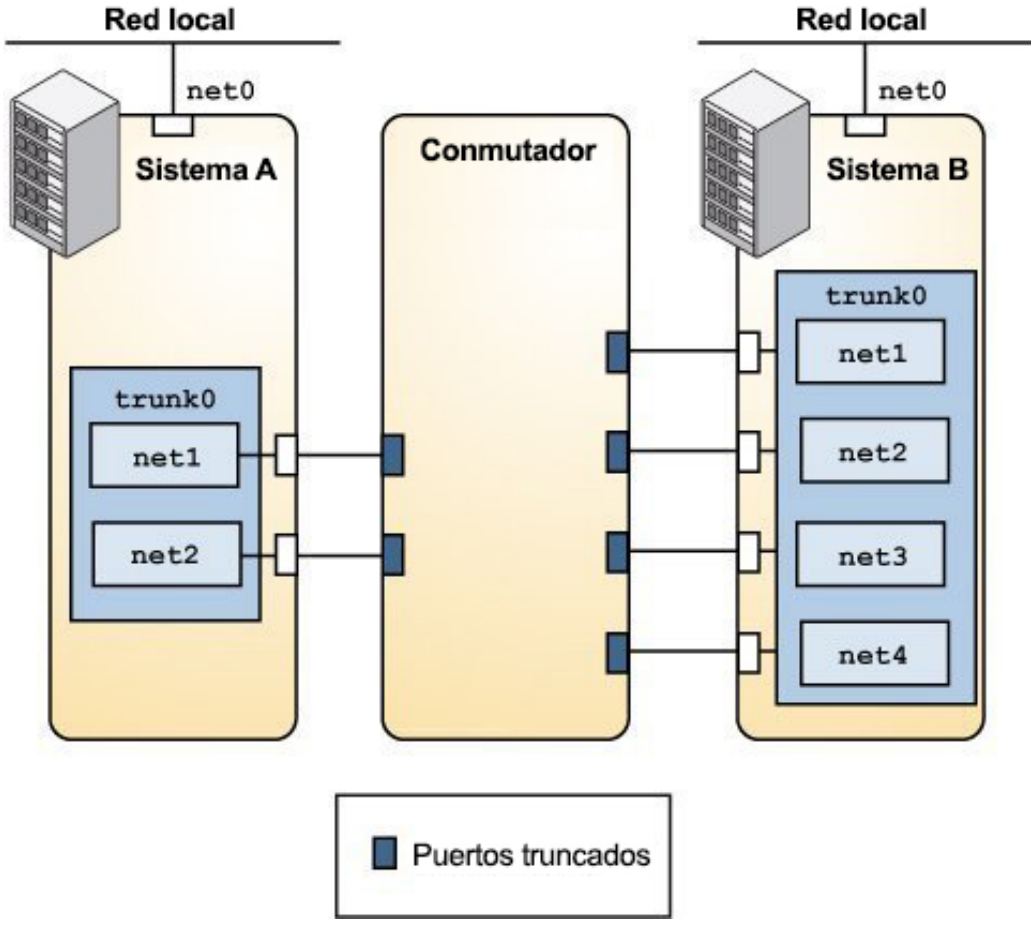
- Mediante conmutador
- Uso de un conmutador con el protocolo de control de agregación de enlaces (LACP)
- Configuración de agregaciones de troncos de extremo a extremo
- Equilibrio de la carga y políticas de agregación

Las secciones siguientes describen las funciones de las agregaciones de troncos.

Mediante conmutador

Los sistemas que se configuran con agregaciones de troncos pueden utilizar un conmutador externo para conectarse a otros sistemas. La figura siguiente muestra una red local con dos sistemas, en la que cada sistema tiene una agregación de troncos configurada.

FIGURA 2-2 Agregación de troncos mediante conmutador

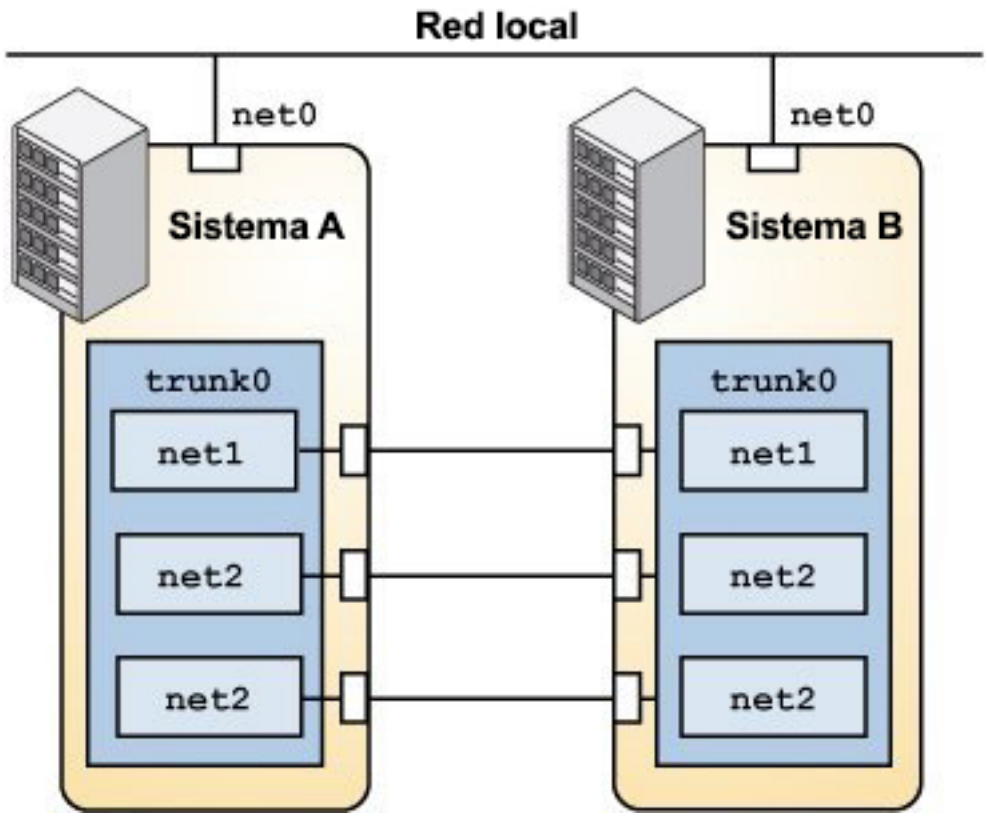


Los dos sistemas están conectados mediante un nodo (concentrador). El sistema A tiene una agregación de troncos que consta de dos enlaces de datos, `net1` y `net2`. Estos enlaces de datos están conectados al conmutador mediante puertos agregados. El sistema B tiene una agregación de troncos de cuatro enlaces de datos, de `net1` a `net4`. Estos enlaces de datos también están conectados a los puertos agregados del conmutador. En esta topología de agregación de troncos, el conmutador debe admitir el estándar IEEE 802.3ad, y los puertos del conmutador debe estar configurados para la agregación. Consulte la documentación del fabricante del conmutador para configurar el conmutador.

Configuración de agregaciones de troncos de extremo a extremo

Las agregaciones de troncos admiten la configuración de extremo a extremo. En lugar de utilizar un conmutador, se conectan dos sistemas directamente para ejecutar agregaciones paralelas, como se muestra en la siguiente figura.

FIGURA 2-3 Configuración de agregaciones de troncos de extremo a extremo



La ilustración muestra la agregación de troncos `trunk0` en el sistema A directamente conectada con la agregación de troncos `trunk0` en el sistema B por medio de los enlaces correspondientes entre sus respectivos enlaces de datos subyacentes. Esta configuración permite a los sistemas A y B proporcionar redundancia, alta disponibilidad y comunicación de alta velocidad entre ambos sistemas. Cada sistema también tiene la interfaz `net0` configurada para el flujo de tráfico de la red local.

La aplicación más común de una agregación de troncos de extremo a extremo es la configuración de servidores de base de datos reflejados en los centros de datos. Ambos servidores deben actualizarse a la vez y, por lo tanto, necesitan bastante ancho de banda, flujo de tráfico de alta velocidad y fiabilidad.

Mediante un conmutador con el protocolo de control de agregación de enlaces

Si la configuración de una agregación de troncos tiene un conmutador y el conmutador admite LACP, puede activar LACP para el conmutador y el sistema. Consulte la documentación del fabricante del conmutador para configurar el conmutador.

LACP permite un método de detección de fallos de enlace de datos más confiable. Sin LACP, una agregación de enlaces se basa únicamente en el estado del enlace informado por el controlador del dispositivo para detectar el fallo de un enlace de datos agregado. Con LACP, se intercambian LACPDU en intervalos regulares para garantizar que los enlaces de datos agregados pueden enviar y recibir tráfico. LACP también detecta algunos casos de configuración incorrecta, por ejemplo, cuando la agrupación de enlaces de datos no coincide entre los dos iguales.

LACP intercambia tramas especiales denominadas unidades de datos del protocolo de control de agregación de enlaces (LACPDU) entre la agregación y el conmutador si LACP está activado en el sistema. LACP utiliza estas LACPDU para mantener el estado de los enlaces de datos agregados.

Utilice el comando `dladm create-aggr` para configurar el LACP de una agregación en uno de los tres modos siguientes:

- `off`: el modo predeterminado para agregaciones. El sistema no genera LACPDU.
- `active`: el sistema genera LACPDU en intervalos especificados.
- `passive`: el sistema genera una LACPDU sólo cuando recibe una LACPDU del conmutador. Si la agregación y el conmutador están configurados en el modo `passive`, no pueden intercambiar LACPDU.

  Para obtener información sobre cómo configurar LACP, consulte Cómo crear una agregación de enlaces [27].

Definición de políticas de agregación para el equilibrio de carga

Puede definir una política para el tráfico saliente que especifica cómo distribuir la carga entre los enlaces disponibles de una agregación a fin de establecer un equilibrio de carga. Puede

utilizar los siguientes especificadores de carga para aplicar diferentes políticas de equilibrio de carga:

- L2: determina el enlace de salida usando el encabezado MAC (L2) de cada paquete
- L3: determina el enlace de salida usando el encabezado IP (L3) de cada paquete
- L4: determina el enlace de salida usando el encabezado TCP, UDP u otro ULP (L4) de cada paquete

También es válida cualquier combinación de estas directivas. La directiva predeterminada es L4.

Agregaciones de rutas múltiples de enlaces de datos

La agregación de rutas múltiples de enlaces de datos (DLMP) es un tipo de agregación de enlaces que proporciona alta disponibilidad en varios conmutadores sin necesidad de configurar el conmutador. La agregación DLMP admite la detección de fallos basada en enlaces y la detección de fallos basada en sondeos a fin de garantizar la disponibilidad continua de la red para enviar y recibir tráfico.

Ventajas de la agregación DLMP

La agregación DLMP proporciona las siguientes ventajas:

- El estándar IEEE 802.3ad implementado por las agregaciones de troncos no tienen disposiciones para abarcar varios conmutadores. Permitir el failover entre varios conmutadores en modo de tronco requiere utilizar en los conmutadores extensiones de propiedad del proveedor que no ofrecen compatibilidad entre diferentes proveedores. Las agregaciones DLMP permiten el failover entre varios conmutadores sin necesidad de extensiones de propiedad del proveedor.
- Usar IPMP para alta disponibilidad en el contexto de la virtualización de redes es muy complejo. Un grupo IPMP no se puede asignar directamente a una zona. Cuando las tarjetas de interfaz de red (NIC) tienen que compartirse entre varias zonas, se deben configurar VNIC de manera que cada zona obtenga una VNIC de cada una de las NIC físicas. Cada zona debe agrupar sus VNIC en un grupo IPMP para lograr alta disponibilidad. La complejidad aumenta a medida que se escalan las configuraciones, por ejemplo, en un escenario que incluye una gran cantidad de sistemas, zonas, NIC, NIC virtuales (VNIC) y grupos IPMP. Con las agregaciones DLMP, se crea una VNIC o se configura un recurso `anet` de la zona encima de la agregación, y la zona detecta una VNIC de alta disponibilidad.
- La agregación DLMP permite utilizar las funciones de capa de enlace, por ejemplo, la protección de enlaces, los flujos definidos por el usuario y la capacidad de personalizar las propiedades de enlace, como el ancho de banda.

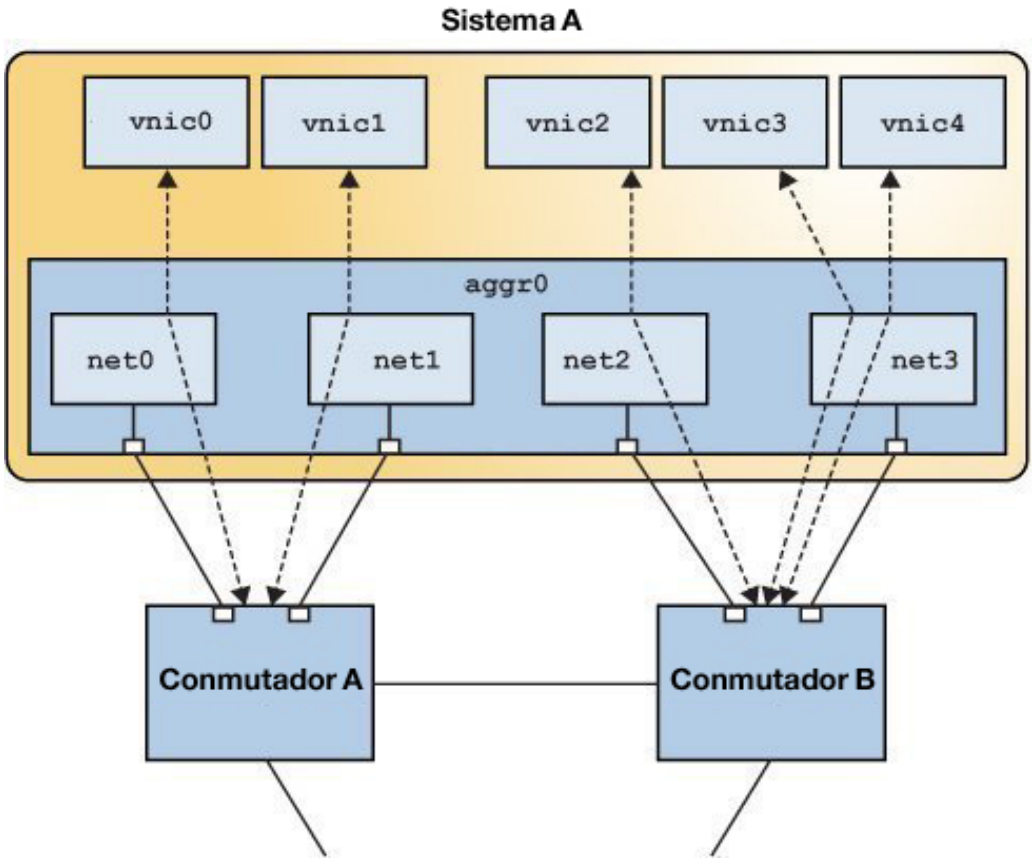
Nota - No debe configurar un grupo IPMP a través de una agregación DLMP. Sin embargo, puede configurar un grupo IPMP a través de una agregación de troncos.

Cómo funciona la agregación DLMP

En una agregación de troncos, cada puerto se asocia a cada enlace de datos configurado en la agregación. En una agregación DLMP, un puerto se asocia con cualquiera de los enlaces de datos configurados de la agregación.

En la siguiente figura, se muestra cómo funciona una agregación DLMP.

FIGURA 2-4 Agregación DLMP



La figura muestra el sistema A con la agregación de enlaces `aggr0`. La agregación consta de cuatro enlaces subyacentes, de `net0` a `net3`. Las VNIC de `vnic0` a `vnic4` también se configuran en la agregación. La agregación se conecta al conmutador A y al conmutador B que, a su vez, se conectan a otros sistemas de destino en la red más amplia.

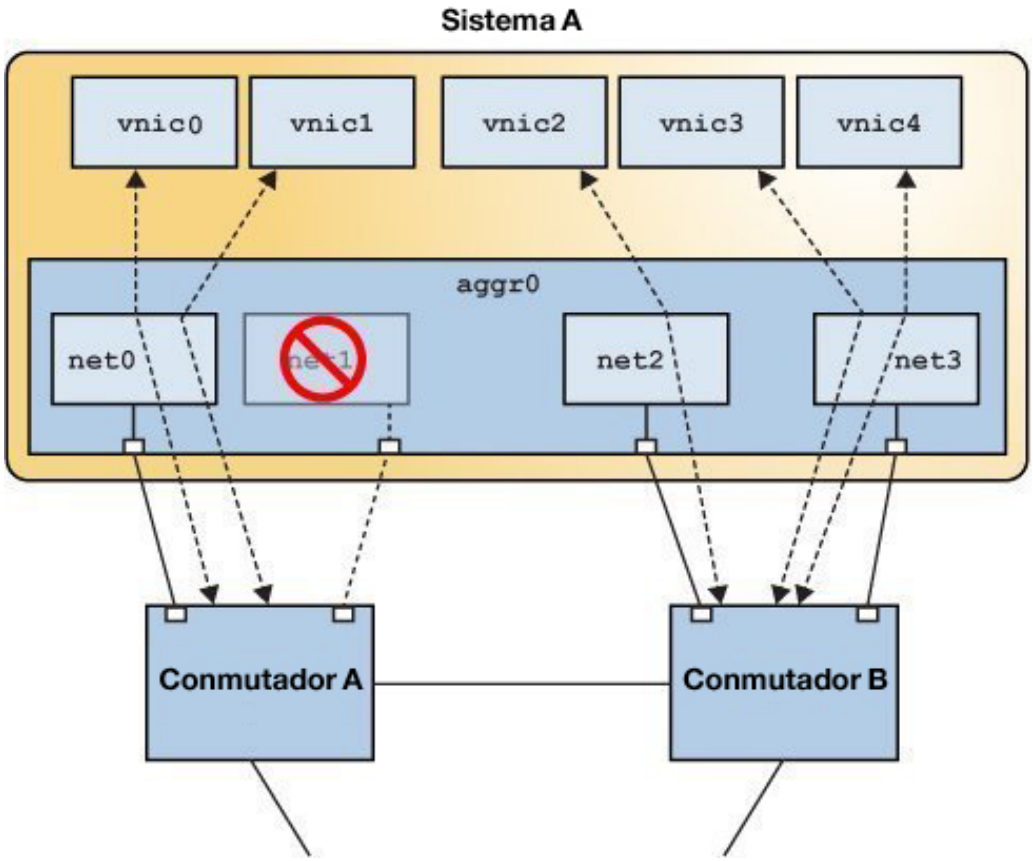
Las VNIC se asocian con los puertos agregados a través de los enlaces subyacentes. Por ejemplo, en la figura, las VNIC de `vnic0` a `vnic3` están asociadas con los puertos agregados a través de los enlaces subyacentes de `net0` a `net3`. Es decir, si el número de VNIC y el número de enlaces subyacentes son iguales, cada puerto se asocia con un enlace subyacente.

Si la cantidad de VNIC supera la cantidad de enlaces subyacentes, un puerto se asocia con varios enlaces de datos. Por ejemplo, en la figura, el número total de VNIC supera el número de enlaces subyacentes. Por lo tanto, `vnic4` comparte un puerto con `vnic3`.

Cuando un puerto agregado falla, todos los enlaces de datos que utilizan ese puerto se distribuyen entre los otros puertos; de esta forma, se proporciona alta disponibilidad de red durante el failover. Por ejemplo, si `net0` falla, la agregación DLMP comparte el puerto restante (`net1`) entre las VNIC. La distribución entre los puertos agregados se produce de manera transparente para el usuario e independientemente de los conmutadores externos conectados a la agregación.

En la siguiente figura, se muestra cómo funciona la agregación DLMP cuando un puerto falla. En la figura, `net1` ha fallado y el enlace entre el conmutador y `net1` está inactivo. `vnic1` comparte un puerto con `vnic0` a `net0`.

FIGURA 2-5 Agregación DLMP cuando falla un puerto



Detección de fallos en la agregación DLMP

La detección de fallos en la agregación DLMP es un método para detectar el fallo de los puertos agregados. Se considera que un puerto ha fallado cuando no puede enviar o recibir tráfico. El puerto puede fallar debido a los siguientes motivos:

- Daños o cortes en el cable
- Desactivación del puerto del conmutador
- Fallo en la ruta de red ascendente

La agregación DLMP realiza una detección de fallos en los puertos agregados para garantizar la disponibilidad continua de la red para enviar o recibir tráfico. Cuando un puerto falla, se hace failover de los clientes asociados con ese puerto a un puerto activo. Los puertos agregados con fallos siguen sin poder utilizarse hasta que se hayan reparado. Los puertos activos restantes siguen funcionando mientras los puertos existentes se implementan según sea necesario. Después de que el puerto con errores se recupera del fallo, los clientes de otros puertos activos pueden asociarse a él.

La agregación DLMP admite la detección de fallos basada en sondeos y basada en enlaces.

Detección de fallos basada en enlaces

La detección de fallos basada en enlaces detecta el fallo cuando el cable se corta o cuando el puerto del conmutador deja de funcionar. Por lo tanto, sólo puede detectar los fallos provocados por la pérdida de conexión directa entre el enlace de datos y el conmutador de primer salto. La detección de fallos basada en enlaces se activa de forma predeterminada cuando se crea una agregación DLMP.

Detección de fallos basada en sondeos

La detección de fallos basada en sondeos detecta fallos entre un host de finalización y los destinos configurados. Esta función supera las limitaciones conocidas de la detección de fallos basada en enlaces. La detección de fallos basada en sondeos es útil cuando un enrutador predeterminado está inactivo o cuando la red se vuelve inaccesible. La agregación DLMP detecta el fallo mediante el envío y la recepción de paquetes de sondeo.

Para activar la detección de fallos basada en sondeos en la agregación DLMP, debe configurar la propiedad `probe-ip`.

Nota - En una agregación DLMP, si `probe-ip` no está configurado, la detección de fallos basada en sondeos está desactivada y sólo se utiliza la detección de fallos basada en enlaces.

Al crear la primera agregación DLMP, el servicio `svc:/network/dlmp:default` se activa automáticamente. Este servicio inicia el daemon `in.dlmpd`, que realiza la detección de fallos basada en sondeos en las agregaciones DLMP. Este servicio está desactivado cuando no hay una agregación DLMP en el sistema. Para obtener más información, consulte “Configuración de la detección de fallos basada en sondeos para la agregación DLMP” [33].

La detección de fallos basada en sondeos se realiza mediante la combinación de dos tipos de sondeos: sondeos del protocolo de mensajes de control de Internet (ICMP) (L3) y sondeos transitivos (L2), que funcionan juntos para determinar el estado de los enlaces de datos físicos agregados.

- **Sondeo ICMP**

  Puede configurar una lista separada por comas de direcciones IP de origen y un nombre de host o dirección IP de destino opcional. La dirección IP de destino debe estar en la misma subred que la dirección IP de origen especificada. Puede especificar la dirección IP de origen de cuatro formas diferentes. Para obtener más información, consulte Cómo configurar la detección de fallos basada en sondeos para DLMP [33].

  El sondeo ICMP utiliza las direcciones IP de origen configuradas de la propiedad `probe-ip` sólo si las direcciones IP están asociadas con clientes, por ejemplo, VNIC. Un puerto se asocia con un cliente, como una VNIC, sólo cuando el puerto recibe el tráfico entrante y transmite el tráfico saliente para ese cliente. En cualquier momento dado, el tráfico entrante o saliente de un cliente siempre pasa a través de un solo puerto subyacente de la agregación DLMP. Las direcciones IP configuradas de la propiedad `probe-ip` se utilizan para supervisar el estado de los puertos sólo si las direcciones IP están asociadas con ese puerto.

  Para cada dirección IP de origen configurada, el daemon `in.dlmpd` envía paquetes de ICMP de unidifusión de forma periódica dirigidos a los destinos configurados. Si las direcciones IP de destino no están configuradas, `in.dlmpd` utiliza la tabla de enrutamiento para las rutas de la misma subred que la dirección IP de origen especificada y utiliza el próximo salto especificado como la dirección IP de destino.

  El tráfico de sondeos ICMP se envía únicamente a través del puerto asociado con ese cliente IP. El puerto se marca como *error de ICMP* si no se puede acceder a ninguno de los destinos para ese puerto específico. El puerto se marcado como *ICMP activo* si se puede acceder a, al menos, uno de los destinos desde dicho puerto a través de un sondeo ICMP.

- **Sondeo transitivo**

  El sondeo transitivo se realiza cuando no se puede determinar el estado de todos los puertos de la red mediante el sondeo ICMP. Por lo tanto, el sondeo transitivo se realiza si alguno de los puertos no está asociado con la dirección IP de origen configurada para la propiedad `probe-ip`. Por ejemplo, el sondeo transitivo se realiza cuando hay un puerto que no está asociado a un cliente IP o cuando el número de direcciones IP configuradas de la propiedad `probe-ip` es menor que el número total de puertos agregados. Los paquetes de sondeo se envían periódicamente desde los puertos que no están asociados con ningún cliente IP hacia los puertos del igual. Si un puerto puede comunicarse con cualquier puerto ICMP activo, se considera que ese puerto está *activo para L2*.

  Oracle Solaris incluye paquetes de protocolo de propiedad para los sondeos transitivos que se transmiten a través de la red. Para obtener más información, consulte el Apéndice B, Formato de paquete de los sondeos transitivos.

La detección de fallos basada en sondeos se realiza en la zona global cuando las VNIC de una agregación se crean en la zona global y se asignan a las zonas no globales. Sin embargo, el tráfico de sondeos se puede segregar de la zona no global con la ayuda de VLAN. Por ejemplo, cuando el tráfico de sondeos se ejecuta en una VLAN en una zona global, el tráfico de la zona no global puede ejecutarse en una VLAN diferente.

Requisitos para agregaciones de enlaces

La configuración de la agregación de enlaces tiene los siguientes requisitos:

- Los enlaces de datos que se deben configurar en una agregación no deben tener ninguna interfaz IP configurada sobre ellos.
- Puede crear agregaciones de enlaces sólo desde la zona global. No puede utilizar enlaces de datos para crear una agregación de enlaces desde una zona no global, incluso si no tiene ninguna interfaz IP configurada sobre los enlaces de datos. La agregación de enlaces sólo combina varias NIC físicas, pero en una zona no global todas las interfaces son virtuales. Por lo tanto, no puede crear una agregación de enlaces desde la zona no global.
- Todos los enlaces de datos de la agregación deben ejecutarse a la misma velocidad y en modo dúplex completo.
- Para las agregaciones DLMP, debe tener al menos un conmutador que conecte la agregación con los puertos en los otros sistemas. No puede utilizar una configuración de extremo a extremo cuando configura agregaciones DLMP.
- En los sistemas basados en SPARC, cada enlace de datos debe tener su propia dirección MAC. Para obtener información, consulte "Cómo asegurarse de que la dirección MAC de cada interfaz sea única" de "Configuración y administración de componentes de red en Oracle Solaris 11.2 ".
- (Para agregaciones de troncos solamente). Los dispositivos deben admitir la notificación del estado del enlace, como lo define el estándar de agregación de enlaces IEEE 802.3ad para que un puerto se conecte a una agregación de troncos o se desconecte de ella. 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 enlaces [27].

Creación de una agregación de enlaces

La agregación de enlaces agrupa los puertos subyacentes en un único grupo lógico. La agregación utiliza estos puertos subyacentes de manera exclusiva, y no se puede realizar ninguna otra operación, como la configuración de VNIC o la asignación de direcciones IP, en estos puertos. Sin embargo, puede configurar VNIC en la agregación y no en los puertos individuales.

Debe eliminar cualquier interfaz IP existente en estos puertos antes de crear la agregación de enlaces.

También puede configurar una VLAN y crear VNIC en la agregación de enlaces que haya creado. Para obtener más información sobre cómo crear VLAN en agregaciones de enlaces, consulte Cómo configurar VLAN a través de una agregación de enlaces [55].

Nota - Una agregación de enlaces sólo funciona en enlaces de punto a punto de dúplex completo y con velocidad idéntica. Asegúrese de que los enlaces de datos de su agregación cumplan este requisito.

▼ Cómo crear una agregación de enlaces

Antes de empezar Si está creando una agregación de troncos y utiliza un conmutador en la agregación, configure los puertos que se van a utilizar como una agregación en el conmutador. Si el conmutador admite LACP, configure LACP en el modo `active` o `passive`.

Consulte la documentación del fabricante del conmutador para configurar el conmutador.

1. **Conviértase en un administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Visualice la información de enlace de datos para identificar los enlaces de datos físicos para la agregación.**

   ```
   # dladm show-phys
   ```

3. **Asegúrese de que el enlace de datos que pretende agregar no esté siendo usado por ninguna aplicación.**

   Por ejemplo, si una interfaz IP se crea por medio del enlace de datos, primero elimine la interfaz IP.

   a. **Determine el estado del enlace.**

      ```
      # ipadm show-if
      IFNAME       CLASS        STATE     ACTIVE     OVER
      lo0          loopback     ok        yes        --
      net0         ip           ok        no         --
      ```

      La salida indica que existe una interfaz IP en el enlace de datos `net0`.

   b. **Elimine la interfaz IP.**

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

      Donde *interface* especifica la interfaz IP en el enlace. Para obtener más información, consulte la página del comando man `ipadm`(1M).

4. **Cree una agregación de enlaces.**

```
# dladm create-aggr [-f] [-m mode] [-P policy]  [-L LACP-mode] \
[-T time] [-u address] -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.

`-m` *mode* — El modo se debe configurar en uno de los siguientes valores. El modo predeterminado es `trunk`.

- `trunk`: modo de agregación de enlaces que cumple con IEEE 802.3ad
- `dlmp`: modo de rutas múltiples de enlaces de datos

`-P` *policy* — (Para agregación de troncos solamente). Especifica la política de equilibrio de carga para la agregación. Los valores admitidos son `L2`, `L3` y `L4`. Para obtener más información, consulte “Definición de políticas de agregación para el equilibrio de carga” [19].

`-L` *LACP-mode* — (Para agregación de troncos solamente). Especifica el modo de LACP si se utiliza. Los valores admitidos son `off`, `active` y `passive`. Para obtener información acerca de los modos, consulte “Mediante conmutador” [16].

`-T` *time* — (Para agregación de troncos solamente). Especifica el valor del temporizador de LACP. Los valores admitidos son `short` y `long`.

`-u` *address* — Especifica la dirección de unidifusión fija para la agregación.

`-l` *linkn* — Especifica los enlaces de datos que desea agregar.

aggr — Especifica el nombre de la agregación, que puede ser cualquier nombre personalizado. Para obtener información acerca de las reglas para asignar nombres, consulte “Reglas para nombres de enlaces válidos” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”.

5. (Opcional) Compruebe el estado de la agregación creada.

- Visualice las agregaciones y los enlaces con la información de estado.

```
# dladm show-link
```

- Visualice las agregaciones con el estado e información por puerto.

```
# dladm show-aggr -x
```

El estado de agregación debe ser `up`.

ejemplo 2-1 Creación de una agregación de troncos

En este ejemplo, se muestran los comandos para crear una agregación de enlaces con dos enlaces de datos subyacentes, `net0` y `net1`. La agregación también se configura para transmitir los paquetes LACP. El ejemplo comienza con la eliminación de las interfaces IP que existen en los enlaces de datos subyacentes.

```
# ipadm show-if
IFNAME       CLASS        STATE     ACTIVE     OVER
lo0          loopback     ok        yes        --
net0         ip           ok        no         --
# ipadm delete-ip net0
# dladm create-aggr -L active -l net0 -l net1 trunk0
# dladm show-aggr -x
LINK       PORT           SPEED DUPLEX   STATE     ADDRESS            PORTSTATE
trunk0     --             1000Mb full    up        8:0:27:49:10:b8    --
           net0           1000Mb full    up        8:0:27:49:10:b8    attached
           net1           1000Mb full    up        8:0:27:e4:d9:46    attached
```

ejemplo 2-2 Creación de una agregación DLMP y configuración de una interfaz IP en la agregación

En este ejemplo, se muestra cómo crear una agregación DLMP. La agregación tiene tres enlaces de datos subyacentes: `net0`, `net1` y `net2`. Se crea una interfaz IP en la agregación `aggr0` y se crea una VNIC `vnic1` sobre esta.

```
# dladm create-aggr -m dlmp -l net0 -l net1 -l net2 aggr0
# dladm show-link
LINK      CLASS     MTU     STATE   OVER
net0      phys      1500    up      --
net1      phys      1500    up      --
net2      phys      1500    up      --
aggr0     aggr      1500    up      net0 net1 net2
# dladm show-aggr -x
LINK       PORT           SPEED DUPLEX   STATE     ADDRESS            PORTSTATE
aggr0      --             1000Mb full    up        8:0:27:49:10:b8    --
           net0           1000Mb full    up        8:0:27:49:10:b8    attached
           net1           1000Mb full    up        8:0:27:e4:d9:46    attached
           net2           1000Mb full    up        8:0:27:38:7a:97    attached
# ipadm create-ip aggr0
# ipadm create-addr -T static -a local=10.10.10.1 aggr0/v4
# dladm create-vnic -l aggr0 vnic1
```

Pasos siguientes Puede realizar una configuración adicional de la agregación, como la creación de interfaces IP y VNIC. Puede utilizar la agregación creada para la configuración de zonas no globales y zonas de núcleo.

- Para obtener información acerca de la creación de interfaces IP, consulte Capítulo 3, “Configuración y administración de direcciones e interfaces IP en Oracle Solaris” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”.

- Para obtener información sobre la configuración de VLAN en una agregación de enlaces, consulte “Configuración de VLAN en una agregación de enlaces” [55].
- Para obtener información sobre la configuración de VNIC, consulte “Cómo configurar VNIC y etherstubs” de “Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ”.
- Para obtener información sobre la configuración de zonas, consulte “Creación y uso de zonas de Oracle Solaris ”.

Cómo agregar un enlace a una agregación

Puede incluir enlaces de datos adicionales a una agregación existente. Si desea agregar enlaces de datos a una agregación de troncos, es posible que tenga que volver a configurar el conmutador para incluir los enlaces de datos adicionales aunque LACP esté configurado en el conmutador.

▼ Cómo agregar un enlace a una agregación

1. **Conviértase en un administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Asegúrese de que no se configuren interfaces IP en el enlace. Si hay alguna interfaz IP configurada, suprímala.**

   ```
   # ipadm show-if
   # ipadm delete-ip interface
   ```

   Donde *interface* es la interfaz IP configurada mediante el enlace de datos.

3. **Agregue el enlace a la agregación.**

   ```
   # dladm add-aggr -l link [-l link] [...] aggr
   ```

   Donde *link* representa un enlace de datos que se va a agregar a la agregación y *aggr* es el nombre de la agregación.

4. **(Para agregación de troncos solamente). Si es necesario, vuelva a configurar el conmutador.**

   Es posible que necesite volver a configurar el conmutador para incluir los enlaces de datos adicionales en función de cómo está configurado el conmutador, incluso si LACP está activado en el conmutador.

Consulte la documentación del fabricante del conmutador para realizar cualquier tarea de reconfiguración en el conmutador.

ejemplo 2-3 Cómo agregar un enlace a una agregación

En este ejemplo, se muestra cómo agregar un enlace a la agregación `aggr0`.

```
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1
net3     phys      1500    up        --
# ipadm delete-ip net3
# dladm add-aggr -l net3 aggr0
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1 net3
net3     phys      1500    up        --
```

Cómo eliminar un enlace de una agregación

Puede eliminar los enlaces de datos individuales asociados a una agregación con el comando `dladm remove-aggr`. Al eliminar enlaces de la agregación, debe volver a configurar el conmutador.

Conviértase en administrador y utilice el siguiente comando:

```
# dladm remove-aggr -l link aggr
```

EJEMPLO 2-4 Cómo eliminar un enlace de una agregación

En este ejemplo, se muestra cómo eliminar un enlace de la agregación `aggr0` .

```
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1 net3
net3     phys      1500    up        --
# dladm remove-aggr -l net3 aggr0
# dladm show-link
```

```
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1
net3     phys      1500    unknown   --
```

Modificación de una agregación de troncos

Puede modificar los atributos seleccionados, como `policy`, `lacpmode` y `time`, para la agregación de troncos. Estos atributos no se admiten en las agregaciones DLMP.

- Para modificar la política de equilibrio de carga de la agregación, conviértase en administrador y ejecute el siguiente comando:

  `# dladm modify-aggr -P` *policy aggr*

policy	Representa una o varias de las políticas de equilibrio de carga L2, L3 y L4, como se explica en "Definición de políticas de agregación para el equilibrio de carga" [19].
aggr	Especifica la agregación cuya política se desea modificar.

- Para modificar el modo LACP de la agregación, conviértase en administrador y utilice el siguiente comando:

  `# dladm modify-aggr -L` *LACP-mode* `-T` *time aggr*

`-L` *LACP-mode*	Indica el modo LACP con el que debe funcionar la agregación. Los valores posibles son `active`, `passive` y `off`.
`-T` *time*	Indica el valor de temporizador de LACP, `short` o `long`.
aggr	Especifica la agregación del modo LACP que desea modificar.

EJEMPLO 2-5 Modificación de una agregación de troncos

En este ejemplo, se muestra cómo modificar la política de equilibrio de carga de la agregación de enlaces `aggr0` a L2 y cómo cambiar el modo LACP a `active`.

```
# dladm modify-aggr -P L2 aggr0
# dladm modify-aggr -L active -T short aggr0
# dladm show-aggr
LINK    MODE       POLICY  ADDRPOLICY      LACPACTIVITY   LACPTIMER
aggr0   trunk      L2      auto            active         short
```

Configuración de la detección de fallos basada en sondeos para la agregación DLMP

Debe configurar la propiedad `probe-ip` para una agregación DLMP a fin de activar el sondeo. De lo contrario, el sondeo está desactivado de manera predeterminada y sólo se utiliza la detección de fallos basada en enlaces. Para obtener más información, consulte “Detección de fallos en la agregación DLMP” [23].

Las siguientes propiedades de enlace de datos se utilizan para configurar la detección de fallos basada en sondeos:

- `probe-ip`: especifica una lista separada por comas de direcciones IP de origen y un nombre de host o dirección IP de destino. Las direcciones IP de origen se utilizan para el sondeo ICMP. La lista de direcciones IP de origen está seguida por una dirección de destino opcional. La dirección IP de destino debe estar en la misma subred que la dirección IP de origen especificada.

  Puede utilizar + para separar el origen del destino. Puede especificar los destinos como una dirección IP o el nombre de host del destino. Para obtener información sobre cómo especificar la dirección de origen y la dirección de destino, consulte Cómo configurar la detección de fallos basada en sondeos para DLMP [33].
- `probe-fdt`: especifica el tiempo de detección de fallos. Puede configurar el valor del tiempo de detección de fallos en segundos. El valor predeterminado es de 10 segundos.

▼ Cómo configurar la detección de fallos basada en sondeos para DLMP

Antes de empezar Cree una agregación DLMP. Para obtener más información, consulte Cómo crear una agregación de enlaces [27].

1. **Conviértase en un administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **(Opcional) Visualice todas las agregaciones existentes a fin de identificar la agregación para configurar la detección de fallos basada en sondeos.**

   ```
   # dladm show-aggr
   ```

3. **Defina los destinos de sondeo para la agregación para la cual desea configurar la detección de fallos basada en sondeos.**

   ```
   # dladm set-linkprop -p probe-ip=IP-address[/prefix-length]|hostname+[target] aggr
   ```

Las direcciones de origen y de destino para la propiedad `probe-ip` se puede especificar de las siguientes formas:

- `probe-ip=`*IP-address*[*/prefix-length*]|*hostname*+[*target*]

  La dirección IP y la longitud del prefijo. Por ejemplo, `10.130.10.1/24+`.

- `probe-ip=`*addr-obj-name*+[*target*]

  El nombre de objeto de la dirección. Por ejemplo, `vnic1/addr1+192.168.0.1`.

- `probe-ip=`*interface-name*+[*target*]

  El nombre de interfaz, que puede ser el nombre de la interfaz de agregación o cualquier VNIC configurada en la agregación. Por ejemplo, `[aggr1]+`.

- `probe-ip=+`[*target*]

  No hay ninguna dirección IP especificada. Cuando no se especifica la dirección IP de origen, todas las direcciones IP configuradas en la agregación y las VNIC se consideran posibles direcciones IP de origen para los sondeos ICMP. Por ejemplo, `+10.130.10.1`.

4. **(Opcional) Establezca el tiempo de detección de fallos.**

   ```
   # dladm set-linkprop -p probe-fdt=fdt  aggr
   ```

   Donde *fdt* es el tiempo de detección de fallos especificado en segundos. El valor predeterminado es de 10 segundos.

5. **(Opcional) Visualice la agregación para ver la información relacionada con el sondeo.**

   ```
   # dlstat show-aggr -n -P [[t],[i],[all]]
   ```

ejemplo 2-6 Configuración de detección de fallos basada en sondeos

1. Visualice las agregaciones existentes.

   ```
   # dladm show-aggr
   LINK    MODE       POLICY  ADDRPOLICY      LACPACTIVITY   LACPTIMER
   aggr0   dlmp       --      --              --             --
   aggr1   dlmp       --      --              --             --
   ```

2. Defina los destinos de sondeo para `aggr1`.

   ```
   # dladm set-linkprop -p probe-ip=+ aggr1
   ```

   Dado que no se ha especificado la dirección IP de origen, todas las direcciones IP configuradas en la agregación `aggr1` y las VNIC se convierten en direcciones IP de origen para los sondeos ICMP.

3. Establezca el tiempo de detección de fallos.

   ```
   # dladm set-linkprop -p probe-fdt=15 aggr1
   ```

4. Visualice las propiedades que están configuradas.

```
# dladm show-linkprop -p probe-ip,probe-fdt aggr1
LINK     PROPERTY         PERM   VALUE           EFFECTIVE    DEFAULT      POSSIBLE
aggr1    probe-ip         rw     192.168.85.137   --           --        --
aggr1    probe-fdt        rw     15               15           10          1-600
```

5. Visualice las estadísticas de los sondeos para la agregación.

```
# dlstat show-aggr -n -P t,i aggr1
TIME   AGGR   PORT  LOCAL           TARGET          PROBE  NETRTT     RTT
0.45s  aggr1  net0  net0            net1            t16148  --         --
0.45s  aggr1  net0  net0            net1            t16148  0.63ms     0.81ms
1.08s  aggr1  net1  net1            net0            t16148  --         --
1.08s  aggr1  net1  net1            net0            t16148  0.72ms     0.99ms
2.07s  aggr1  net1  192.168.85.137  192.168.85.137  i15535  --         --
2.07s  aggr1  net1  192.168.85.137  192.168.85.137  i15535  0.18ms     0.54ms
```

Supervisión de la detección de fallos basada en sondeos

Puede supervisar la detección de fallos basada en sondeos mediante los comandos `dladm show-aggr`, `dlstat show-aggr` y `ipadm show-addr`.

EJEMPLO 2-7 Visualización de información relacionada con los sondeos

El ejemplo siguiente muestra las estadísticas de los sondeos para una agregación DLMP. Con la opción del tipo de sondeo `-P`, puede proporcionar una lista de argumentos separada por comas (`t` para el sondeo transitivo, `i` para el sondeo ICMP, y `all` para los sondeos ICMP y transitivos) en el comando `dlstat show-aggr` para mostrar el tipo de sondeo correspondiente.

```
# dlstat show-aggr -n -P t,i aggr1
   TIME     AGGR     PORT   LOCAL        TARGET       PROBE  NETRTT     RTT
   0.53s    aggr1    net0   net0         net1         t16148  --         --
   0.53s    aggr1    net0   net0         net1         t16148  0.62ms     0.87ms
   1.17s    aggr1    net1   net1         net0         t16148  --         --
   1.17s    aggr1    net1   net1         net0         t16148  0.72ms     0.99ms
   2.24s    aggr1    net1   192.168.0.1  192.168.0.2  i15535  --         --
   2.24s    aggr1    net1   192.168.0.1  192.168.0.2  i15535  0.11ms     0.55ms
```

`TIME` Tiempo en el que se envió el sondeo en segundos. Este tiempo es relativo al momento en que se ejecuta el comando `dlstat`. Si el sondeo se envió antes de emitir el comando `dlstat`, el tiempo es negativo.

`AGGR` Nombre de la agregación para la que se envió el sondeo.

LOCAL	Sondeos ICMP: dirección IP de origen de los sondeos. Sondeos transitivos: nombre de puerto desde donde se origina el sondeo transitivo.
TARGET	Sondeos ICMP: dirección IP de destino de los sondeos. Sondeos transitivos: nombre de puerto del sondeo que se envía.
PROBE	Número de identificador que representa el sondeo. El prefijo `t` es para los sondeos transitivos y el prefijo `i` es para los sondeos ICMP.
NETRTT	Tiempo de ida y vuelta de red para el sondeo. Este valor es el período de tiempo entre el envío del sondeo y la recepción de la confirmación de la agregación DLMP.
RTT	Tiempo de ida y vuelta total para el sondeo. Este valor es el período de tiempo entre el envío del sondeo y la finalización del proceso de confirmación de la agregación DLMP.

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

EJEMPLO 2-8 Visualización de información detallada sobre el puerto agregado

El siguiente ejemplo muestra la información de agregación detallada en cada puerto subyacente.

```
# dladm show-aggr -x
LINK        PORT    SPEED  DUPLEX   STATE    ADDRESS            PORTSTATE
aggr1       --      100Mb  full     up       1e:34:db:fa:50:a2  --
            net0    100Mb  full     up       1e:34:db:fa:50:a2  attached
            net1    100Mb  full     up       b2:c0:6a:3e:c5:b5  attached
```

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

EJEMPLO 2-9 Visualización del estado de los puertos agregados

El ejemplo siguiente muestra el estado de los puertos de la agregación y las direcciones IP de destino de los puertos.

```
# dladm show-aggr -S -n
LINK        PORT        FLAGS    STATE    TARGETS         XTARGETS
aggr1       net1        u--3     active   192.168.0.2     net0
--          net0        u-2-     active   --              net1
```

EJEMPLO 2-10 Visualización de los valores de la propiedad `probe-ip`

El ejemplo siguiente muestra los detalles acerca de la propiedad de enlace `probe-ip` para la agregación DLMP especificada.

```
# dladm show-linkprop -p probe-ip aggr1
LINK     PROPERTY         PERM   VALUE         EFFECTIVE    DEFAULT      POSSIBLE
aggr1    probe-ip         rw     192.168.0.2   192.168.0.2  --           --
```

EJEMPLO 2-11 Visualización de la dirección IP y el estado de la agregación

En el ejemplo siguiente, se muestra la dirección IP y el estado de la agregación.

```
# ipadm show-addr aggr1
ADDROBJ           TYPE     STATE        ADDR
aggr1/local1      static   ok           192.168.0.1/24
```

Supresión de una agregación de enlaces

Puede suprimir una agregación de enlaces con el comando `dladm delete-aggr`. Debe eliminar la interfaz IP y las VNIC configuradas en la agregación de enlaces antes de suprimir la agregación.

▼ Cómo suprimir una agregación de enlaces

1. **Conviértase en un administrador.**
   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Suprima la interfaz IP que se configura sobre la agregación de enlaces.**

   ```
   # ipadm delete-ip IP-aggr
   ```

   Donde *IP-aggr* es la interfaz IP sobre la agregación de enlaces.

3. **Suprima la agregación de enlaces.**

   ```
   # dladm delete-aggr aggr
   ```

ejemplo 2-12 Supresión de una agregación de enlaces

En este ejemplo, se muestra cómo suprimir la agregación `aggr0`. La supresión persiste.

```
# ipadm delete-ip aggr0
# dladm delete-aggr aggr0
```

Cambio entre agregaciones de troncos y agregaciones DLMP

Cambiar entre una agregación de troncos y una agregación DLMP modifica toda la configuración, por lo que afecta a la agregación de un modo más integral, a diferencia de la modificación de las otras propiedades de agregación de enlaces.

▼ Cómo cambiar entre tipos de agregación de enlaces

Antes de empezar

- Si pasa de una agregación de troncos a una agregación DLMP, debe eliminar la configuración del conmutador creada previamente para la agregación de troncos.
- Si cambia una agregación DLMP, debe asegurarse de que todos los enlaces se encuentren en el mismo conmutador y que el conmutador esté configurado para la agregación.

1. **Conviértase en un administrador.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Determine el tipo actual de agregación de enlaces.**

   ```
   # dladm show-aggr
   ```

   El campo `MODE` de la salida indica el tipo actual de la agregación. El valor de `MODE` es `trunk` para una agregación de troncos y `dlmp` para una agregación DLMP.

3. **Cambie la agregación.**

   ```
   # dladm modify-aggr -m mode aggr
   ```

   Donde *mode* es `trunk` si se cambia a una agregación de troncos o `dlmp` si se cambia a una agregación DLMP, y *aggr* es el nombre de la agregación.

4. **Configure el conmutador en función de los requisitos del nuevo tipo de agregación de enlaces.**
   Consulte la documentación del fabricante del conmutador para configurar el conmutador.

5. **(Opcional) Verifique la configuración de agregación de enlaces actual.**

```
# dladm show-aggr
```

ejemplo 2-13 Cómo cambiar de una agregación de troncos a una agregación DLMP

En este ejemplo, se muestra cómo cambiar de una agregación de troncos a una agregación DLMP.

```
# dladm show-aggr
LINK    MODE       POLICY  ADDRPOLICY      LACPACTIVITY   LACPTIMER
aggr0   trunk      L2      auto            active         short

# dladm modify-aggr -m dlmp aggr0
# dladm show-aggr
LINK    MODE       POLICY  ADDRPOLICY      LACPACTIVITY   LACPTIMER
aggr0   dlmp       --      --              --             --
```

Una vez que la agregación cambie, debe eliminar la configuración anterior del conmutador que se aplicaba a la agregación de troncos.

Caso de uso: configuración de una agregación de enlaces

El siguiente caso de uso de extremo a extremo muestra cómo llevar a cabo las siguientes acciones:

- Cree una agregación DLMP.
- Agregar los enlaces a la agregación.
- Configurar una interfaz IP sobre la agregación.
- Configurar una VNIC sobre la agregación.
- Configurar la detección de fallos basada en sondeos para la agregación.
- Configurar la dirección IP de destino en la tabla de enrutamiento.
- Supervisar los sondeos transitivos e ICMP.

1. Conviértase en un administrador.

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.
2. Visualice la información de enlace de datos a fin de identificar los enlaces de datos para la agregación.

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

3. Asegúrese de que los enlaces de datos que desea agregar no tengan interfaces IP configuradas sobre el enlace. Suprima la interfaz si hay alguna interfaz configurada en cualquiera de los enlaces.

```
# ipadm show-if
IFNAME       CLASS        STATE     ACTIVE     OVER
lo0          loopback     ok        yes        --
net0         ip           ok        no         --
# ipadm delete-ip net0
```

4. Cree una agregación DLMP con los enlaces `net0` y `net1`.

```
# dladm create-aggr -m dlmp -l net0 -l net1 aggr1
```

5. Agregue otro enlace, `net2`, a la agregación.

```
# dladm add-aggr -l net2 aggr1
```

   Vuelva a configurar el conmutador para incluir los nuevos enlaces si la configuración de conmutador existente lo requiere. Consulte la documentación del fabricante del conmutador.

6. Configure una interfaz IP sobre la agregación `aggr1`.

```
# ipadm create-ip aggr1
# ipadm create-addr -T static -a local=10.10.10.1 aggr1/v4
```

7. Cree una VNIC sobre la agregación.

```
# dladm create-vnic -l aggr1 vnic1
```

8. Configure la detección de fallos basada en sondeos para la agregación.

```
# dladm set-linkprop -p probe-ip=+ aggr1
```

   La dirección IP de origen y la dirección IP de destino de los sondeos no se especifican. Por lo tanto, debe configurar el destino en la tabla de enrutamiento para activar el sondeo.

9. Configure el destino en la tabla de enrutamiento para que esté en la misma subred que la dirección IP especificada.

```
# route add -host 10.10.10.2 10.10.10.2 -static
```

10. Visualice el estado de los puertos agregados y los destinos.

```
# dladm show-aggr -S
LINK       PORT        FLAGS   STATE     TARGETS         XTARGETS
aggr1      net0        u--3    active    10.10.10.2      net2 net1
--         net1        u-2-    active       --           net2 net0
--         net2        u-2-    active       --           net0 net1
```

11. Supervise las estadísticas de sondeos ICMP.

```
# dlstat show-aggr -n -P i
   TIME     AGGR      PORT   LOCAL          TARGET        PROBE NETRTT  RTT
   1.16s    aggr1     net0   10.10.10.1     10.10.10.2    i33   --      --
```

```
1.16s    aggr1     net0   10.10.10.1     10.10.10.2    i33   0.08ms  0.33ms
2.05s    aggr1     net0   10.10.10.1     10.10.10.2    i34   --      --
2.05s    aggr1     net0   10.10.10.1     10.10.10.2    i34   0.01ms  0.64ms
4.05s    aggr1     net0   10.10.10.1     10.10.10.2    i35   --      --
4.05s    aggr1     net0   10.10.10.1     10.10.10.2    i35   0.10ms  0.35ms
5.54s    aggr1     net0   10.10.10.1     10.10.10.2    i36   --      --
5.54s    aggr1     net0   10.10.10.1     10.10.10.2    i36   0.08ms  0.34ms
```

12. Supervise las estadísticas de sondeos transitivos entre los puertos.

```
# dlstat show-aggr -n -P t
  TIME     AGGR   PORT        LOCAL       TARGET  PROBE NETRTT  RTT
  0.30s    aggr1  net2        net2        net0    t38   --      --
  0.30s    aggr1  net2        net2        net0    t38   0.46ms  0.59ms
  0.46s    aggr1  net0        net0        net1    t39   --      --
  0.46s    aggr1  net0        net0        net1    t39   0.46ms  0.50ms
  0.48s    aggr1  net1        net1        net0    t39   --      --
  0.48s    aggr1  net1        net1        net0    t39   0.34ms  0.38ms
  0.72s    aggr1  net2        net2        net1    t38   --      --
  0.72s    aggr1  net2        net2        net1    t38   0.38ms  0.42ms
  0.76s    aggr1  net0        net0        net2    t39   --      --
  0.76s    aggr1  net0        net0        net2    t39   0.33ms  0.38ms
  0.87s    aggr1  net1        net1        net2    t39   --      --
  0.87s    aggr1  net1        net1        net2    t39   0.32ms  0.38ms
  1.95s    aggr1  net2        net2        net0    t39   --      --
  1.95s    aggr1  net2        net2        net0    t39   0.36ms  0.42ms
  1.97s    aggr1  net2        net2        net1    t39   --      --
  1.97s    aggr1  net2        net2        net1    t39   0.32ms  0.38ms
  1.99s    aggr1  net0        net0        net1    t40   --      --
  1.99s    aggr1  net0        net0        net1    t40   0.31ms  0.36ms
  2.12s    aggr1  net1        net1        net0    t40   --      --
  2.12s    aggr1  net1        net1        net0    t40   0.34ms  0.40ms
  2.14s    aggr1  net0        net0        net2    t40   --      --
```

Se crea la agregación `aggr0` con una interfaz IP configurada. La VNIC `vnic1` se configura sobre la agregación `aggr0`. La detección de fallos basada en sondeos se configura sin especificar la dirección IP de origen ni la dirección IP de destino de los sondeos. Para activar el sondeo, el destino en la tabla de enrutamiento se configura con una dirección IP, `10.10.10.2`, en la misma subred que la dirección IP especificada, `10.10.10.1`. Se supervisan las estadísticas de los sondeos transitivos e ICMP.

Comparación entre la agregación DLMP y de troncos

En esta sección, se presenta una comparación general de los dos tipos de agregación de enlaces.

TABLA 2-1 Comparación entre las características de la agregación DLMP y de troncos

Característica	Agregaciones de troncos	Agregaciones DLMP
Detección de fallos basada en enlaces	Admitida	Admitida
LACP	Admitida	No admitida
Uso de interfaces de reserva	No admitida	No admitida[1]
Conmutadores múltiples	No admitidos, salvo que se use una solución de propiedad del proveedor	Admitida
Configuración del conmutador	Requerida	No requerida
Políticas para el equilibrio de carga	Admitida	NA
Expansión de carga en todos los puertos de la agregación	Admitida	Limitada[2]
Flujos definidos por el usuario para la gestión de recursos	Admitida	Admitida
Protección de enlaces	Admitida	Admitida
Configuración de extremo a extremo	Admitida	No admitida[3]

[1] Cada cliente DLMP está asociado con exactamente un puerto DLMP. Los puertos restantes actúan como los puertos disponibles para los clientes DLMP, pero no puede configurar estos puertos disponibles.

[2] La agregación extiende sus VNIC en todos los puertos. Sin embargo, las VNIC individuales no pueden expandir la carga en varios puertos.

[3] Las agregaciones DLMP siempre deben utilizar un conmutador intermediario para enviar paquetes a otros sistemas de destino. Sin embargo, no es necesaria la configuración del conmutador para DLMP.

♦ ♦ ♦ CAPÍTULO 3

Configuración de redes virtuales mediante redes de área local virtuales

En este capítulo, se tratan las características y las ventajas de las redes de área local virtuales (VLAN). En este capítulo, también se describen los procedimientos para configurar y modificar las VLAN.

Este capítulo se divide en los siguientes apartados:

Descripción general de la implementación de VLAN

Una red de área local virtual (VLAN) es una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo. Puede crear redes VLAN para redes de área local que utilicen tecnología de nodo. Puede asignar interfaces del mismo sistema a redes VLAN diferentes.

Cuándo utilizar redes VLAN

Puede implementar VLAN si necesita hacer lo siguiente:

- Crear una división lógica de grupos de trabajo.

  Por ejemplo, si todos los hosts de una planta de un edificio están conectados en una red local basada en conmutador, puede crear una VLAN diferente para cada grupo de trabajo de la planta.
- Aplicar diferentes políticas de seguridad para los grupos de trabajo.

  Por ejemplo, las necesidades de seguridad del departamento de finanzas y del departamento de informática son muy diferentes. Puede crear una VLAN independiente para cada departamento y asignar la política de seguridad apropiada para cada VLAN.
- Reducir el tamaño del dominio de emisión y mejorar la eficacia de la red. Puede dividir los grupos de trabajo en dominios de emisión gestionables.

  Por ejemplo, en un dominio de emisión que consta de 25 usuarios, si el tráfico de emisión está pensado sólo para 12 usuarios, configurar una VLAN independiente para esos 12 usuarios puede reducir el tráfico y mejorar la eficacia de la red.

Asignación de nombres de VLAN

Las VLAN demuestran la ventaja de utilizar nombres genéricos o personalizados. En versiones anteriores, la VLAN se identificaba por el punto físico de conexión (PPA, Physical Point of Attachment) que exigía la combinación del nombre basado en hardware del enlace de datos y el ID de VLAN. Sin embargo, ahora en Oracle Solaris puede seleccionar un nombre más significativo para identificar la VLAN. El nombre debe cumplir las reglas de denominación de enlaces de datos que se proporcionan en “Reglas para nombres de enlaces válidos” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”. Por ejemplo, puede asignar un nombre de VLAN personalizado, como `sales0` o `marketing1`.

Los nombres de las VLAN funcionan de manera conjunta con el ID de VLAN. Cada VLAN de una red de área local está identificada por un ID de VLAN, que es parte de la etiqueta de VLAN. El ID de VLAN se asigna durante la configuración de la VLAN. Al configurar los conmutadores para que admitan las VLAN, es necesario asignar un ID de VLAN a cada puerto. El ID de VLAN del puerto debe ser el mismo que el ID de VLAN asignado a la interfaz que se conecta al puerto.

De forma predeterminada, cada puerto tiene un ID de VLAN denominado ID de VLAN de puerto. Los paquetes que pertenecen a este ID de VLAN no tienen una etiqueta de VLAN. En Oracle Solaris, puede utilizar la propiedad de enlace de datos `default_tag` para mostrar y cambiar el ID de VLAN de puerto en una interfaz.

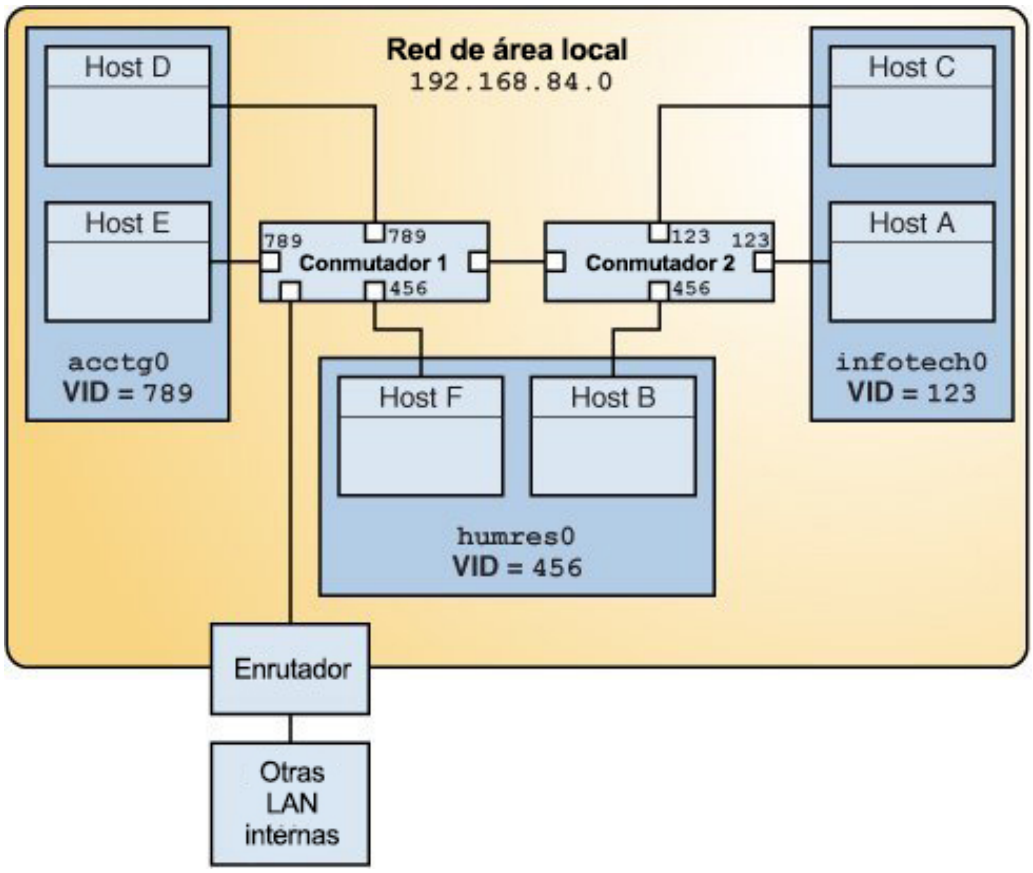
Topología de VLAN

La tecnología de LAN con conmutadores permite organizar los sistemas de una red local en redes VLAN. Para dividir una red de área local en redes VLAN, debe tener conmutadores

compatibles con la tecnología VLAN. Puede configurar todos los puertos de un conmutador para que transfieran datos para una única VLAN o para varias VLAN, según la topología de VLAN. Cada fabricante de conmutadores utiliza procedimientos diferentes para configurar los puertos de un conmutador.

En la siguiente figura, se muestra una red de área local que se ha dividido en tres VLAN.

FIGURA 3-1 Red de área local con tres redes VLAN



En la ilustración, la LAN tiene la dirección de subred `192.168.84.0`.

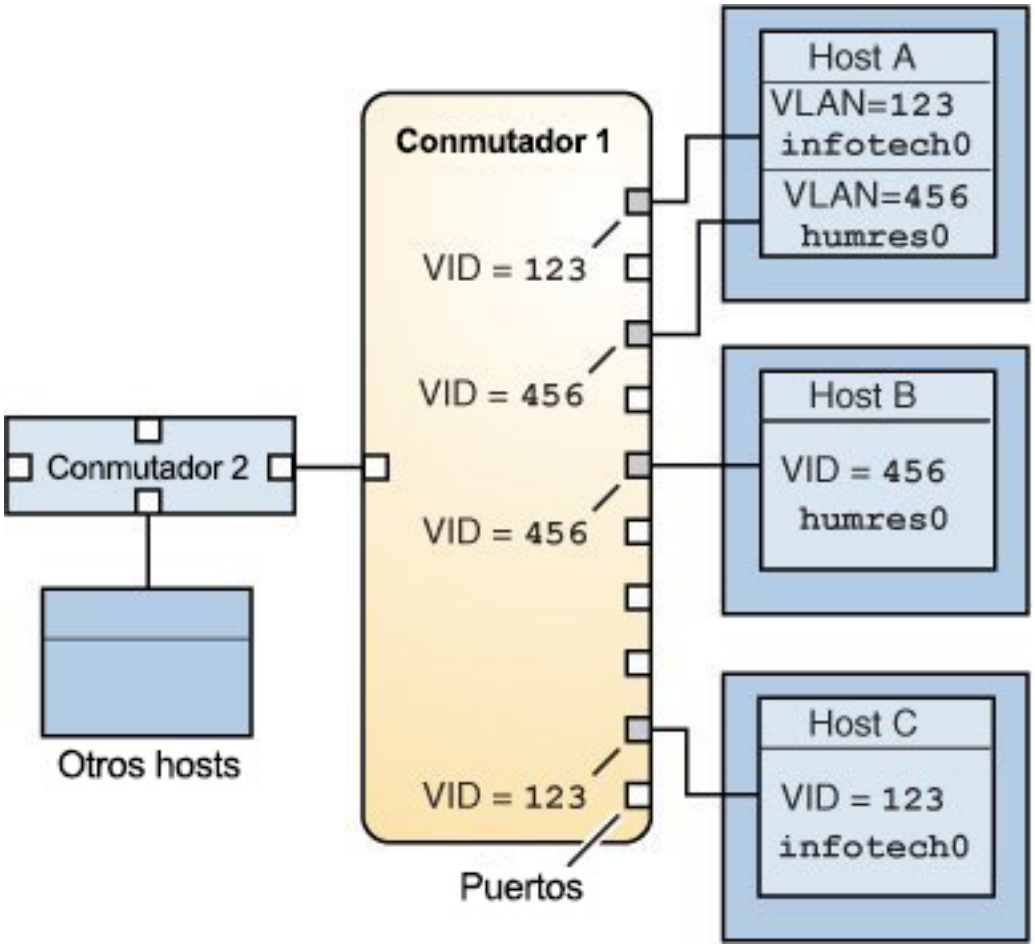
Esta LAN está subdividida en tres redes VLAN para que se correspondan con tres grupos de trabajo:

- `acctg0` con el ID de VLAN `789`: grupo de contabilidad. Este grupo posee los hosts D y E.

- `humres0` con ID de VLAN `456`: grupo de recursos humanos. Este grupo posee los hosts B y F.
- `infotech0` con ID de VLAN `123`: grupo de informática. Este grupo posee los hosts A y C.

Una variación de esta figura se muestra en la siguiente figura, donde se utiliza un solo conmutador, y varios hosts que pertenecen a diferentes VLAN se conectan a ese mismo conmutador.

FIGURA 3-2 Un conmutador que conecta varios hosts de diferentes VLAN



En la figura, los hosts A y C pertenecen a la VLAN de informática con el ID de VLAN `123`. Una de las interfaces del host A está configurada con el ID de VLAN `123`. Esta interfaz se

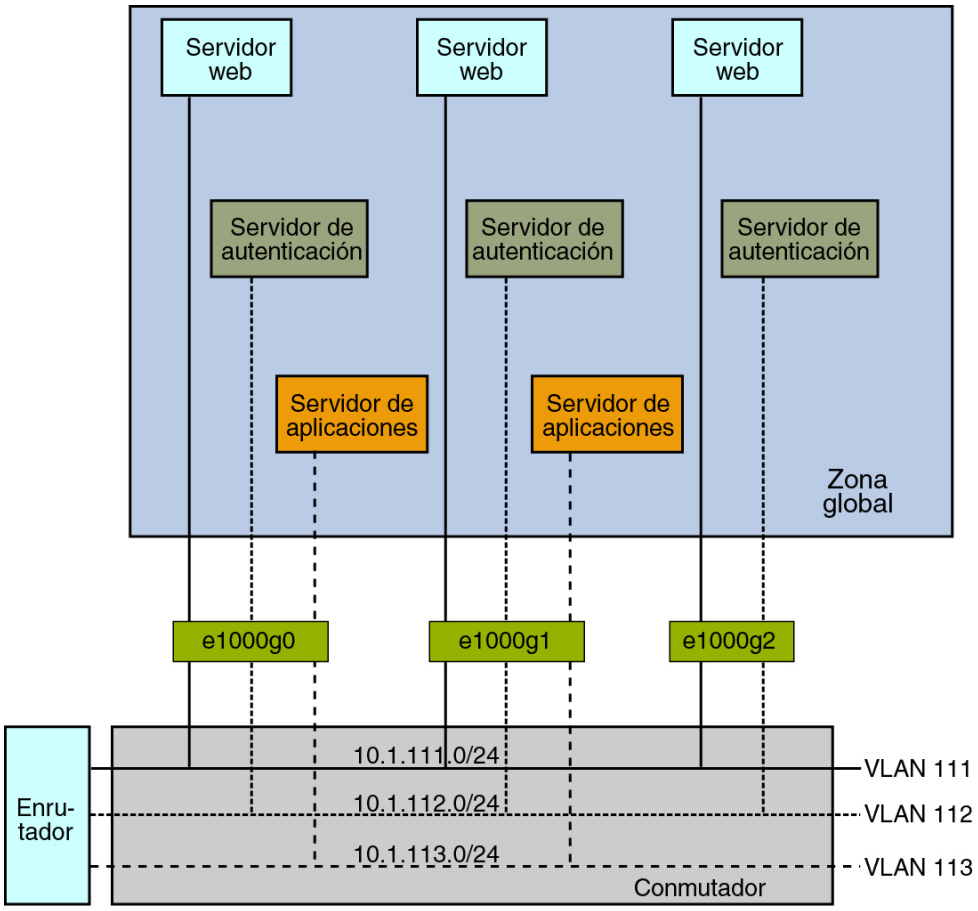
conecta al puerto 1 en el conmutador 1, que también se configura con el ID de VLAN `123`. El host B es miembro de la VLAN de recursos humanos con el ID de VLAN `456`. La interfaz del host B se conecta al puerto 5 en el conmutador 1, que se configura con el ID de VLAN `456`. Por último, la interfaz del host C se configura con el ID de VLAN `123`. La interfaz se conecta al puerto 9 en el conmutador 1. El puerto 9 también se configura con el ID de VLAN `123`.

En la ilustración, también se muestra que un único host puede pertenecer a varias VLAN. Por ejemplo, el host A tiene dos VLAN configuradas en la interfaz del host. La segunda VLAN está configurada con el ID de VLAN `456` y está conectada al puerto 3, que se configura con el ID de VLAN `456`. Por lo tanto, el host A es miembro de las VLAN `infotech0` y `humres0`.

Uso de VLAN con zonas

Puede configurar varias redes virtuales dentro de una única unidad de red, por ejemplo, un conmutador, mediante la combinación de VLAN y Oracle Solaris Zones. Tenga en cuenta la siguiente figura, que muestra un sistema con tres tarjetas de red físicas: `net0`, `net1` y `net2`.

FIGURA 3-3 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 tendrían que conectarse a una LAN; los servidores de autenticación, a otra; y los servidores de aplicaciones, a una tercera. Con las VLAN y las zonas, puede combinar los ocho sistemas y configurarlos como zonas en un único sistema. Luego, puede usar ID de VLAN para asignar una VLAN a cada conjunto de zonas que realiza las mismas funciones. La siguiente tabla muestra la información proporcionada en la figura.

Función	Nombre de zona	Nombre de VLAN	ID de VLAN	Dirección IP	NIC
Servidor web	`webzone1`	`web1`	`111`	`10.1.111.0`	`net0`

Función	Nombre de zona	Nombre de VLAN	ID de VLAN	Dirección IP	NIC
Servidor de autenticación	`authzone1`	`auth1`	`112`	`10.1.112.0`	`net0`
Servidor de aplicaciones	`appzone1`	`app1`	`113`	`10.1.113.0`	`net0`
Servidor web	`webzone2`	`web2`	`111`	`10.1.111.1`	`net1`
Servidor de autenticación	`authzone2`	`auth2`	`112`	`10.1.112.1`	`net1`
Servidor de aplicaciones	`appzone2`	`app2`	`113`	`10.1.113.1`	`net1`
Servidor web	`webzone3`	`web3`	`111`	`10.1.111.2`	`net2`
Servidor de autenticación	`authzone3`	`auth3`	`112`	`10.1.112.2`	`net2`

Para ver cómo crear la configuración que se muestra en la figura, consulte el Ejemplo 3-2, “Configuración de una VLAN con zonas”.

Planificación de una configuración de VLAN

La planificación de una configuración de VLAN implica los siguientes pasos:

1. Examine la topología de la LAN y determine dónde es apropiado realizar las subdivisiones en redes VLAN.

   Para ver un ejemplo básico de esta topología, consulte la Figura 3-1, “Red de área local con tres redes VLAN”.
2. Cree un esquema numerado para los ID de VLAN y asigne un ID de VLAN a cada VLAN.

Nota - Si ya existe un esquema de numeración de VLAN en la red, debe crear los ID de VLAN dentro del esquema de numeración de VLAN existente.

---

3. En cada sistema, determine las interfaces que son los componentes de una VLAN determinada.

   a. Determine qué enlaces se configuran en el sistema mediante el comando `dladm show-link`.
   b. Determine qué ID de VLAN debe asociarse con cada enlace de datos del sistema.
   c. Cree la VLAN.
4. Compruebe las conexiones de los enlaces de datos con los conmutadores de la red.

   Tenga en cuenta el ID de VLAN de cada enlace de datos y el puerto de conmutador al que está conectada cada interfaz.

5. Configure cada puerto del conmutador con el mismo ID de VLAN de la interfaz al que está conectado.

   Consulte la documentación del fabricante del nodo para ver las instrucciones de configuración.

Configuración de una VLAN

El siguiente procedimiento describe cómo crear una VLAN en un enlace de datos mediante el comando `dladm`. Puede crear una interfaz IP en una VLAN y configurar la interfaz con una dirección IP mediante el comando `ipadm`. Para obtener información acerca de los comandos `dladm` y `ipadm`, consulte las páginas del comando man `dladm`(1M) y `ipadm`(1M)

▼ Cómo configurar una VLAN

Antes de empezar En este procedimiento, se supone que ya se han creado las zonas en el sistema. Para obtener información sobre la configuración de zonas, consulte el Capítulo 1, “Cómo planificar y configurar zonas no globales” de “Creación y uso de zonas de Oracle Solaris ”.

1. **Conviértase en un administrador.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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
   ```

link	Especifica el enlace en el que se crea la interfaz VLAN.
vid	Indica el número de ID de VLAN.
VLAN-link	Especifica el nombre de la VLAN, que también puede ser un nombre personalizado significativo. Para obtener información sobre los nombres de VLAN, consulte “Asignación de nombres de VLAN” [44].

4. **Verifique la configuración de la VLAN.**

   ```
   # dladm show-vlan
   ```

5. **Cree una interfaz IP en la VLAN.**

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

Donde *interface* especifica el nombre de la VLAN.

6. Configure la interfaz IP con una dirección IP.

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

ejemplo 3-1 Creación de una VLAN

En este ejemplo, se muestra cómo crear la configuración de la VLAN que se ilustra en la Figura 3-1, “Red de área local con tres redes VLAN”.

1. Compruebe los enlaces disponibles y cree las VLAN en los enlaces específicos.

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

2. Host A:

```
# dladm create-vlan -l net0 -v 123 infotech0
```

Host C:

```
# dladm create-vlan -l net0 -v 123 infotech0
```

Host F:

```
# dladm create-vlan -l net0 -v 456 humres0
```

Host B:

```
# dladm create-vlan -l net0 -v 456 humres0
```

Host D:

```
# dladm create-vlan -l net0 -v 789 acctg0
```

Host E:

```
# dladm create-vlan -l net0 -v 789 acctg0
```

3. Visualice las VLAN creadas.

```
# dladm show-vlan
LINK            VID     OVER        FLAGS
infotech0       123     net0        ----
```

```
infotech0       123     net0        ----
humres0         456     net0        ----
humres0         456     net0        ----
acctg0          789     net0        ----
acctg0          789     net0        ----
```

ejemplo 3-2 Configuración de una VLAN con zonas

En este ejemplo, se muestra cómo crear la configuración de la VLAN que se ilustra en la Figura 3-3, “Sistema con varias VLAN”. En este ejemplo, se asume que ya ha configurado diferentes zonas en el sistema. Para obtener información sobre la configuración de zonas, consulte “Creación y uso de zonas de Oracle Solaris ”.

1. Verifique qué enlaces hay disponibles para configurar redes VLAN y, a continuación, cree las VLAN mediante los enlaces específicos.

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

global# dladm create-vlan -l net0 -v 111 web1
global# dladm create-vlan -l net0 -v 112 auth1
global# dladm create-vlan -l net0 -v 113 app1
global# dladm create-vlan -l net1 -v 111 web2
global# dladm create-vlan -l net1 -v 112 auth2
global# dladm create-vlan -l net1 -v 113 app2
global# dladm create-vlan -l net2 -v 111 web3
global# dladm create-vlan -l net2 -v 112 auth3

global# dladm show-vlan
LINK      VID     OVER        FLAGS
web1      111     net0        ----
auth1     112     net0        ----
app1      113     net0        ----
web2      111     net1        ----
auth2     112     net1        ----
app2      113     net1        ----
web3      111     net2        ----
auth3     113     net2        ----
```

Cuando se muestra la información de enlace, las VLAN se incluyen en la lista.

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

```
net1      phys     1500     up        --
net2      phys     1500     up        --
web1      vlan     1500     up        net0
auth1     vlan     1500     up        net0
app1      vlan     1500     up        net0
web2      vlan     1500     up        net1
auth2     vlan     1500     up        net1
app2      vlan     1500     up        net1
web3      vlan     1500     up        net2
auth3     vlan     1500     up        net2
```

2. Asigne las VLAN a sus respectivas zonas y visualice información para cada zona similar a la siguiente:

```
global# zonecfg -z webzone1 info net
net:
address not specified
physical: web1
net:
address not specified
physical: web2
net:
address not specified
physical: web3

global# zonecfg -z authzone1 info net
net:
address not specified
physical: auth1
net:
address not specified
physical: auth2
net:
address not specified
physical: auth3

global# zonecfg -z appzone2 info net
net:
address not specified
physical: app1
net:
address not specified
physical: app2
```

   El valor de la propiedad `physical` indica la VLAN que se define para una zona determinada.

3. Visualice las VLAN asignadas en las zonas.

```
global# dladm show-vlan
LINK            VID  OVER  FLAGS
webzone1/web1   111  net0  --
authzone1/auth1 112  net0  --
appzone1/app1   113  net0  --
webzone1/web2   111  net1  --
authzone1/auth2 112  net1  --
appzone1/app2   113  net1  --
webzone1/web3   111  net2  --
authzone2/auth3 111  net2  --
```

4. Inicie 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 -a 10.1.111.0/24 web1
   ipadm: web1/v4
   ```

   En webzone2:

   ```
   webzone2# ipadm create-ip web2
   webzone2# ipadm create-addr -a 10.1.111.1/24 web2
   ipadm: web2/v4
   ```

   En webzone3:

   ```
   webzone3# ipadm create-ip web3
   webzone3# ipadm create-addr -a 10.1.111.2/24 web3
   ipadm: web3/v4
   ```

   En authzone1:

   ```
   authzone1# ipadm create-ip auth1
   authzone1# ipadm create-addr -a 10.1.112.0/24 auth1
   ipadm: auth1/v4
   ```

   En authzone2:

   ```
   authzone2# ipadm create-ip auth2
   autzone2# ipadm create-addr -a 10.1.112.1/24 auth2
   ipadm: auth2/v4
   ```

   En authzone3:

   ```
   authzone3# ipadm create-ip auth3
   authzone3# ipadm create-addr -a 10.1.112.2/24 auth3
   ipadm: auth3/v4
   ```

En appzone1:

```
appzone1# ipadm create-ip app1
appzone1# ipadm create-addr -a 10.1.113.0/24 app1
ipadm: app1/v4
```

En appzone2:

```
appzone2# ipadm create-ip app2
appzone2# ipadm create-addr -a 10.1.113.1/24 app2
ipadm: app2/v4
```

Cuando todas las VLAN se hayan configurado con las direcciones IP, se habrá completado la configuración. Las tres redes VLAN están activas y pueden alojar tráfico de sus respectivas zonas.

Configuración de VLAN en una agregación de enlaces

Puede crear redes VLAN en una agregación de enlaces de manera similar a la configuración de VLAN en una interfaz. Las agregaciones de enlaces se describen en el Capítulo 2, Configuración de alta disponibilidad mediante agregaciones de enlaces. En esta sección, se combina la configuración de VLAN y las agregaciones de enlaces.

▼ Cómo configurar VLAN a través de una agregación de enlaces

Antes de empezar Cree la agregación de enlaces. Para obtener información sobre cómo crear agregaciones de enlaces, consulte Cómo crear una agregación de enlaces [27].

1. **Indique las agregaciones de enlaces que estén configuradas en el sistema.**

   ```
   # dladm show-aggr
   ```

2. **Para cada VLAN que desee crear en la agregación de enlaces que haya seleccionado, puede usar el siguiente comando:**

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

   link Especifica el enlace en el que se crea la interfaz VLAN.

Nota - En este procedimiento, el enlace se refiere a la agregación de enlaces.

---

vid Indica el número de ID de VLAN.

VLAN-link Especifica el nombre de la VLAN.

3. **Para cada VLAN que haya creado en el paso anterior, cree una interfaz IP por medio de la red VLAN.**

   `# ipadm create-ip` *interface*

   Donde *interface* utiliza el nombre de la VLAN.

4. **Para cada interfaz IP en una VLAN, configure una dirección IP válida.**

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

ejemplo 3-3 Configuración de varias VLAN a través de una agregación de enlaces

En este ejemplo, se configuran dos VLAN en una agregación de enlaces. A las VLAN se les asignan los ID de VLAN `193` y `194`, respectivamente.

```
# dladm show-link
LINK     CLASS     MTU     STATE     OVER
net0     phys      1500    up        --
net1     phys      1500    up        --
aggr0    aggr      1500    up        net0 net1

# dladm create-vlan -l aggr0 -v 193 acctg0
# dladm create-vlan -l aggr0 -v 194 humres0

# ipadm create-ip acctg0
# ipadm create-ip humres0

# ipadm create-addr -a 192.168.10.0/24 acctg0
ipadm: acctg0/v4
# ipadm create-addr -a 192.168.20.0/24 humres0
ipadm: humres0/v4
```

Configuración de VLAN en un dispositivo antiguo

Determinados dispositivos antiguos gestionan únicamente los paquetes cuyo tamaño de unidad de transmisión máxima (MTU, Maximum Transmission Unit), también conocido como tamaño de trama, es de 1514 bytes. Los paquetes cuyo tamaño de trama supera el límite máximo se eliminan. En ese caso, siga el mismo procedimiento que aparece en Cómo configurar una VLAN [50]. Sin embargo, al crear la VLAN, utilice la opción `-f` para forzar la creación de la VLAN.

▼ Cómo configurar redes VLAN en un dispositivo antiguo

1. **Cree la VLAN con la opción `-f`.**

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

`-f`	Fuerza la creación de VLAN. Utilice esta opción al crear una VLAN en los dispositivos que no permiten tamaños de trama suficientemente grandes para incluir un encabezado de VLAN.
`-l` *link*	Especifica el enlace en el que se crea la interfaz VLAN. En este procedimiento, el enlace hace referencia al dispositivo antiguo.
`-v` *vid*	Indica el número de ID de VLAN.
VLAN-link	Especifica el nombre de la VLAN, que también puede ser un nombre elegido administrativamente.

2. **Establezca un tamaño menor para la unidad de transmisión máxima (`MTU`, Maximum Transmission Unit).**

   En el siguiente ejemplo, `mtu` se establece en `1496`.

   ```
   # dladm set-linkprop -p mtu=1496 VLAN-link
   ```

   Un valor de MTU menor proporciona espacio para que la capa de enlace inserte el encabezado VLAN antes de la transmisión.

3. **Repita el paso 2 para definir un valor de MTU para cada nodo de la VLAN.**

   Para obtener más información sobre cómo cambiar los valores de propiedades de enlace, consulte “Administración de propiedades de enlaces de datos” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”.

Visualización de información de VLAN

Puede utilizar el comando `dladm show-link` para mostrar información sobre las VLAN, ya que las VLAN son enlaces de datos. Utilice el comando `dladm show-vlan` para mostrar información específica sobre las VLAN.

En el ejemplo siguiente, se compara el tipo de información que puede obtener utilizando el comando `dladm show-link` o `dladm show-vlan`. El primer ejemplo utiliza el comando `dladm`

`show-link` para mostrar todos los enlaces de datos en el sistema, incluidos los que no son VLAN. El segundo ejemplo utiliza el comando `dladm show-vlan` para mostrar un subconjunto de información de enlaces de datos que sólo es relevante para las VLAN.

```
# dladm show-link
LINK     CLASS    MTU      STATE     OVER
net0     phys     1500     up        --
net1     phys     1500     up        --
net2     phys     1500     up        --
web1     vlan     1500     up        net0
auth1    vlan     1500     up        net0
app1     vlan     1500     up        net0
web2     vlan     1500     up        net1
auth2    vlan     1500     up        net1
app2     vlan     1500     up        net1
web3     vlan     1500     up        net2
auth3    vlan     1500     up        net2

# dladm show-vlan
LINK      VID     OVER     FLAGS
web1      111     net0     ----
auth1     112     net0     ----
app1      113     net0     ----
web2      111     net1     ----
auth2     112     net1     ----
app2      113     net1     ----
web3      111     net2     ----
auth3     113     net2     ----
```

Modificación de las VLAN

Puede modificar una VLAN usando el comando `dladm modify-vlan` de las siguientes maneras:

- Cambie el ID de una VLAN.
- Migre una VLAN a otro enlace subyacente.

Modificación del ID de una VLAN

Para cambiar el ID de VLAN de una VLAN, debe utilizar uno de los siguientes comandos:

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

  Donde *vid* especifica el nuevo ID de VLAN que se asigna a la VLAN y *datalink* hace referencia al enlace subyacente en el que se configura la VLAN.

Nota - Puede utilizar la sintaxis de comando `dladm modify-vlan -v` *vid* `-L` *datalink* sólo si existe una única VLAN en el enlace de datos. El comando falla si se utiliza en un enlace de datos que tiene varias VLAN configuradas porque cada VLAN en un enlace de datos debe tener un ID de VLAN exclusivo.

Si modifica el ID de VLAN en el enlace, también debe configurar el puerto de conmutador para el nuevo ID de VLAN.

- `dladm modify-vlan -v` *vid vlan*

  Utilice este comando para cambiar los ID de VLAN exclusivos de varias VLAN mediante un solo enlace de datos. Cada VLAN del enlace de datos tiene un único ID de VLAN, por lo que debe cambiar un ID de VLAN por vez. En la configuración que se muestra en la Figura 3-3, “Sistema con varias VLAN”, tendría que cambiar los ID de VLAN de `web1`, `auth1` y `app1` configurados en `net0` de la siguiente manera:

```
# dladm modify-vlan -v 123 web1
# dladm modify-vlan -v 456 app1
# dladm modify-vlan -v 789 auth1
```

Migración de una VLAN a otro enlace subyacente

Puede migrar una VLAN de un enlace de datos subyacente a otro enlace de datos subyacente sin suprimir ni modificar la configuración de la VLAN. El enlace subyacente puede ser un enlace físico, una agregación de enlaces o un etherstub. Para obtener más información acerca de etherstubs, consulte “Componentes de una red virtual” de “Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ”.

Para migrar correctamente una VLAN, el enlace de datos al que se moverá la VLAN debe tener la capacidad de alojar las propiedades de enlace de datos de la VLAN. Si estas propiedades no son admitidas, la migración fallará y el usuario será notificado. Una vez que la migración se realiza de manera correcta, todas las aplicaciones que utilizan la VLAN continúan funcionando normalmente, siempre que la VLAN permanezca conectada a la red.

Algunas propiedades que dependen del hardware pueden cambiar después de una migración de VLAN. Por ejemplo, una VLAN siempre comparte la misma dirección MAC que su enlace de datos subyacente. Por lo tanto, cuando migra una VLAN, la dirección MAC de la VLAN cambia a la dirección MAC principal del enlace de datos de destino. Otras propiedades que pueden verse afectadas son el estado del enlace de datos, la velocidad del enlace y el tamaño de MTU. Sin embargo, las aplicaciones continúan funcionando sin interrupción.

Nota - Una VLAN migrada no conserva ninguna de las estadísticas de vía de hardware en el enlace de datos original. Las vías de hardware disponibles para la VLAN en el enlace de datos de destino se convierten en una nueva fuente de información estadística. Sin embargo, las estadísticas de software que se muestran de manera predeterminada por el comando `dlstat` se mantienen.

Puede realizar una migración de VLAN de manera global o de manera selectiva.

Migración global

La migración global se utiliza para migrar todas las VLAN que están configuradas en un enlace de datos a otro enlace de datos. Para realizar una migración global, sólo tiene que especificar los enlaces de datos de origen y de destino. El siguiente ejemplo muestra cómo mover todas las VLAN de `ether0` a `net1`.

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

`-l` Hace referencia al enlace de datos de destino al que se migran las VLAN.

`-L` Hace referencia al enlace de datos de origen en el que se configuran las VLAN.

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

Migración selectiva

La migración selectiva se utiliza para migrar sólo las VLAN seleccionadas. Para realizar una migración selectiva de las VLAN, debe especificar las VLAN que desea mover. En el siguiente ejemplo basado en la Figura 3-3, “Sistema con varias VLAN”, las VLAN se mueven de `net0` a `net3`.

```
# dladm modify-vlan -l net3 web1,auth1,app1
```

Nota - Cuando migre las VLAN de manera selectiva, no incluya la opción `-L`, que sólo se aplica a la migración global.

Puede cambiar el ID de las VLAN cuando realiza una migración. Tomando la Figura 3-3, “Sistema con varias VLAN” como base, en el ejemplo siguiente se muestra cómo migrar varias VLAN y cambiar sus ID de VLAN a la vez.

```
# dladm show-vlan
LINK    VID      OVER     FLAGS
web1    111      net0     -----
auth1   112      net0     -----
```

```
app1    113      net0     -----

# dladm modify-vlan -l net3 -v 123 web1
# dladm modify-vlan -l net3 -v 456 auth1
# dladm modify-vlan -l net3 -v 789 app1
# dladm show-vlan
LINK    VID      OVER     FLAGS
web1    123      net3     -----
auth1   456      net3     -----
app1    789      net3     -----
```

Nota - Un comando paralelo, `dladm modify-vnic`, migra las VNIC configuradas como VLAN. Debe utilizar el subcomando correcto en función de si va a migrar VLAN o VNIC configuradas como VLAN. Utilice el subcomando `modify-vlan` en las VLAN que muestra el comando `dladm show-vlan`. Utilice el subcomando `modify-vnic` en las VNIC (incluidas las que tienen ID de VLAN) que muestra la salida del comando `dladm show-vnic`. Para obtener información sobre cómo modificar VNIC, consulte “Modificación de los ID de VLAN de las VNIC” de “Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ”.

Supresión de una VLAN

Utilice el comando `dladm delete-vlan` para suprimir las configuraciones de las VLAN en el sistema.

Nota - Primero debe suprimir todas las configuraciones de IP de la VLAN que desea suprimir antes de poder suprimir la VLAN. La supresión de una VLAN falla si existen interfaces IP en la VLAN.

EJEMPLO 3-4 Supresión de la configuración de una VLAN

En este ejemplo, se muestra cómo suprimir una configuración de VLAN.

```
# dladm show-vlan
LINK      VID     OVER     FLAGS
web1      111     net0     ----
auth1     112     net0     ----
app1      113     net0     ----
web2      111     net1     ----
auth2     112     net1     ----
app2      113     net1     ----
web3      111     net2     ----
auth3     113     net2     ----

# ipadm delete-ip web1
```

```
# dladm delete-vlan web1
```

Caso de uso: combinación de agregaciones de enlaces y configuraciones de VLAN

En esta sección, se proporciona un ejemplo de cómo crear una combinación de configuraciones de red que utiliza agregaciones de enlaces y VLAN.

En el ejemplo siguiente, un sistema que utiliza cuatro NIC debe estar configurado como entrutador para ocho subredes independientes. Por lo tanto, se configuran ocho enlaces, uno para cada subred. Primero, se crea una agregación de troncos en las cuatro NIC. Este enlace sin etiquetas que no incluye una etiqueta de VLAN en la trama de salida se convierte en la subred sin etiquetas predeterminada para la red a la que apunta la ruta predeterminada.

Las interfaces VLAN luego 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 consecuente para que se correspondan con sus respectivas subredes. La configuración final consta de ocho enlaces para las ocho subredes: un enlace sin etiquetas y siete enlaces VLAN con etiquetas. En el ejemplo, primero se verifica si las interfaces IP ya existen en el enlace de datos. Estas interfaces deben suprimirse antes de que los enlaces de datos se combinen en una agregación.

1. Elimine todas las interfaces IP que estén configuradas en los enlaces de datos.

```
# ipadm show-if
IFNAME    CLASS      STATE   ACTIVE   OVER
lo0       loopback   ok      yes      --
net0      ip         ok      yes      --
net1      ip         ok      yes      --
net2      ip         ok      yes      --
net3      ip         ok      yes      --

# ipadm delete-ip net0
# ipadm delete-ip net1
# ipadm delete-ip net2
# ipadm delete-ip net3
```

2. Cree la agregación de troncos `default0`.

```
# dladm create-aggr -P L2,L3 -l net0 -l net1 -l net2 -l net3 default0

# dladm show-link
LINK        CLASS     MTU   STATE    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
```

3. Configure una interfaz IP sobre la agregación.

```
# ipadm create-ip default0
# ipadm create-addr -a 10.2.3.4/24 default0
```

4. Cree las VLAN en `default0`.

```
# 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    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    -----
green0           3   default0    -----
blue0            4   default0    -----
white0           5   default0    -----
yellow0          6   default0    -----
red0             7   default0    -----
cyan0            8   default0    -----
```

5. Cree interfaces IP en los enlaces de VLAN y asigne direcciones IP a las interfaces.

```
# 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 -a 10.2.3.5/24 orange0
# ipadm create-addr -a 10.2.3.6/24 green0
# ipadm create-addr -a 10.2.3.7/24 blue0
# ipadm create-addr -a 10.2.3.8/24 white0
# ipadm create-addr -a 10.2.3.9/24 yellow0
# ipadm create-addr -a 10.2.3.10/24 red0
# ipadm create-addr -a 10.2.3.11/24 cyan0
```

♦ ♦ ♦ CAPÍTULO 4

Administración de funciones de puente

Puede utilizar los puentes para conectar segmentos de red separados de manera que se comunican como si fueran un solo segmento de red. En este capítulo, se describe cómo configurar y administrar las redes con puentes.

Este capítulo se divide en los siguientes apartados:

Descripción general de las redes con puentes

Los puentes conectan distintos nodos de la red en una única red. Los segmentos de red comparten una única red de difusión y se comunican como si fueran un solo segmento de red cuando se conectan. Como resultado, cada nodo puede acceder a los otros mediante protocolos de red, como el protocolo 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.

Si bien tanto los puentes como el enrutamiento pueden utilizarse para distribuir información sobre las ubicaciones de los recursos de la red, difieren en varios aspectos. 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.

Los puentes se utilizan para distribuir información sobre las ubicaciones de los recursos de la red. En una red con puentes, los destinos de los paquetes reenviados se determinan mediante

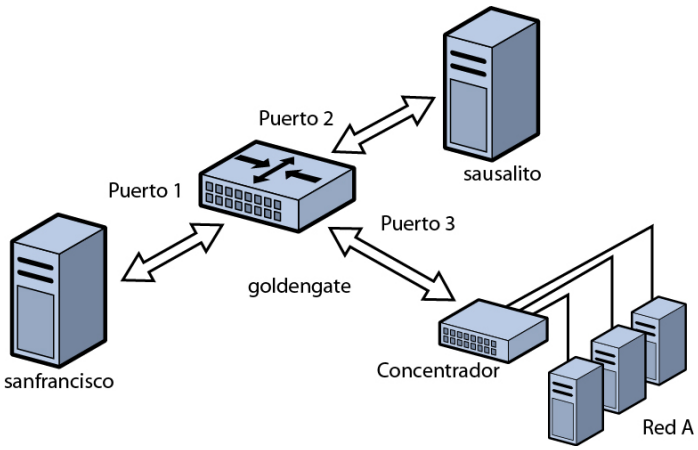
el análisis del tráfico de red que se recibe en los enlaces conectados al puente. Una red con puentes utiliza protocolos, como el protocolo de árbol de expansión (STP, Spanning Tree Protocol) y el protocolo de interconexión transparente de muchos enlaces (TRILL, Transparent Interconnection of Lots of Links). Para obtener más información, consulte “Protocolos de puentes” [70].

Atención - No establezca la propiedad `local-mac-address?` en `false` mediante el comando `eeprom` en los sistemas basados en SPARC® que utilizan puentes. Si lo hace, estos sistemas utilizan, de forma incorrecta, la misma dirección MAC en varios puertos y en la misma red.

Red con puentes simple

En la siguiente figura, se muestra una configuración de red con puentes sencilla.

FIGURA 4-1 Red con puentes simple

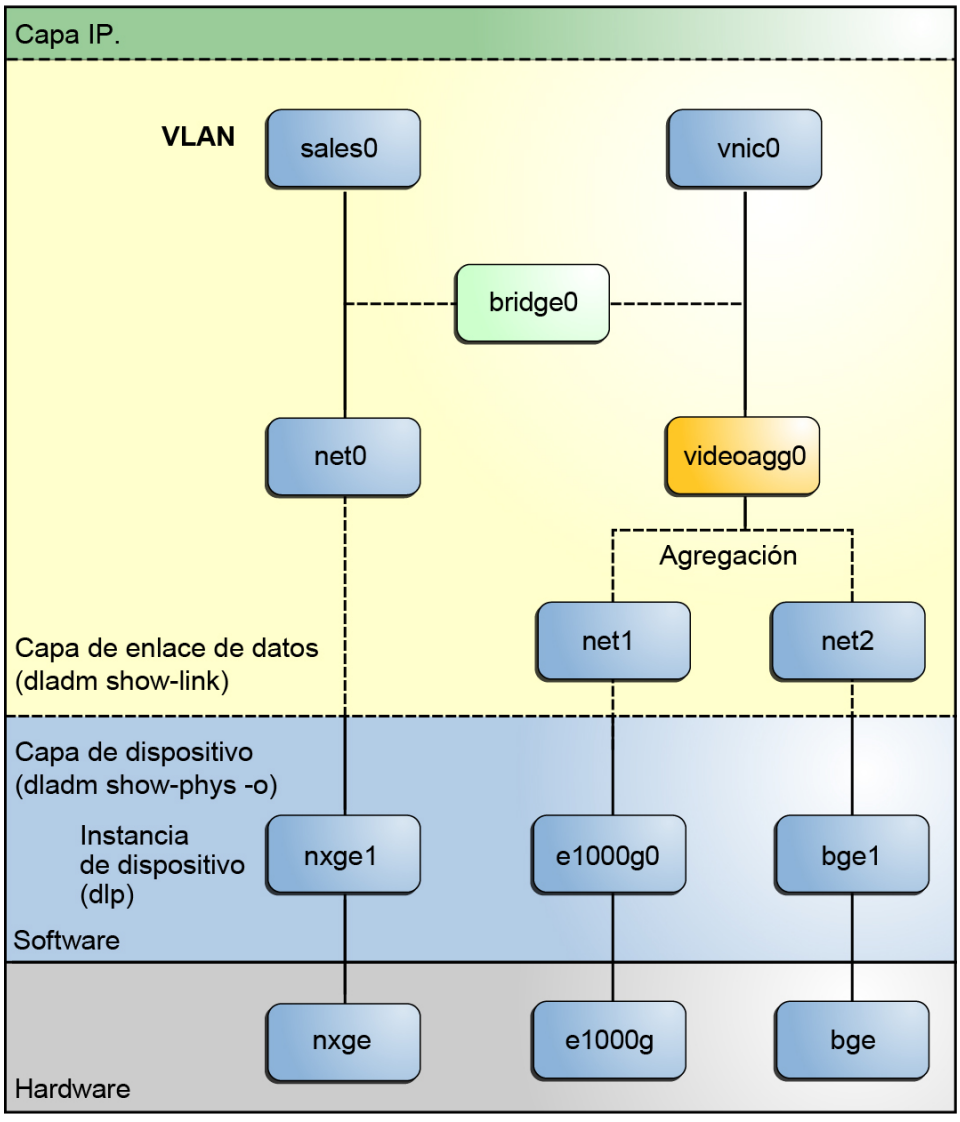


El puente, `goldengate`, es un sistema Oracle Solaris que tiene puentes configurados. Los sistemas `sanfrancisco` y `sausalito` están físicamente conectados al puente. La red A utiliza un hub que está conectado físicamente al puente en un lado y a tres sistemas informáticos en el otro lado. Los puertos del puente son los enlaces `net0`, `net1` y `net2`.

Cómo se implementan los puentes de Oracle Solaris en la pila de red

En Oracle Solaris, puede configurar puentes en la capa de enlace de datos de la misma implementación de pila de red, como se muestra en la siguiente figura.

FIGURA 4-2 Puentes en la pila de red para Oracle Solaris

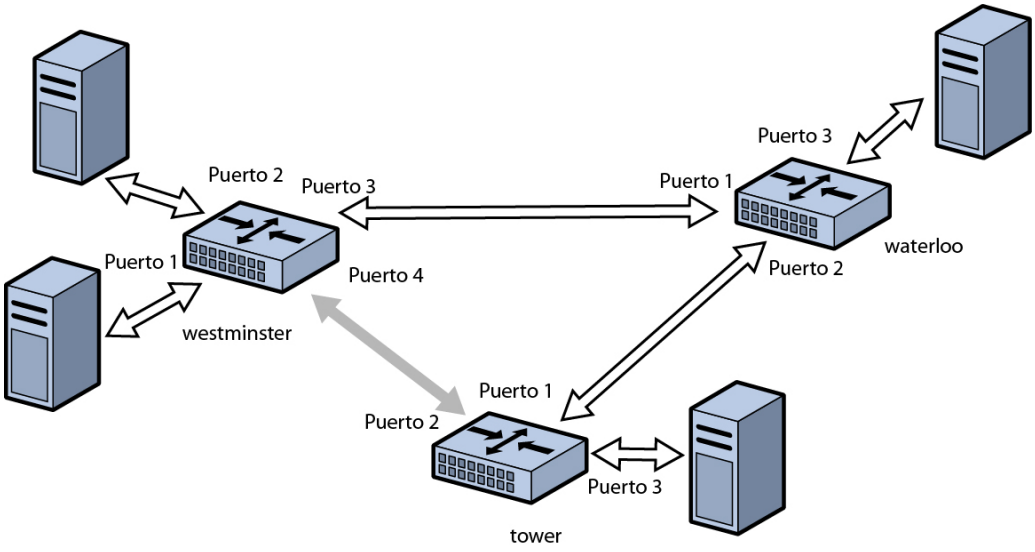


Se configuran dos interfaces, `net0` y `videoagg0`, como un puente, `bridge0`. Los paquetes que se reciben en una interfaz se reenvían a la otra interfaz. Después de la configuración del puente, ambas interfaces aún se pueden utilizar para configurar redes VLAN e interfaces IP.

Anillo de red con puentes

Las redes con puentes se pueden estructurar en forma de anillos que conectan físicamente varios puentes juntos. En la siguiente figura, se muestra una configuración de anillo de red con puentes.

FIGURA 4-3 Anillo de red con puentes



En la figura, se muestra una red con puentes configurada en un anillo. La configuración muestra tres puentes. Dos sistemas están conectados físicamente al puente `westminister`. Un sistema está conectado físicamente al puente `waterloo` y otro sistema está conectado físicamente al puente `tower`. Los puentes están conectados físicamente entre ellos mediante los puertos de puente.

Este tipo de configuración puede 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.

Cómo funciona una red con puentes

Cuando el puente 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 conectado a otro puente en la red con puentes. Con el tiempo, todos los puentes dentro de la red 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 anteriores también se van vaciando con el paso del tiempo. Cuando un enlace se restaura, los paquetes recibidos por medio del enlace se tratan como nuevos. El proceso de aprendizaje comienza nuevamente sobre la base de la dirección de origen de un paquete. Este proceso permite que el puente reenvíe correctamente paquetes por medio de dicho enlace cuando la dirección se utiliza como la dirección de destino.

Protocolos de puentes

Las redes con puentes utilizan los siguientes protocolos:

- Protocolo de árbol de expansión (STP)

  STP es el protocolo predeterminado que utilizan las redes con puentes. Los puentes utilizan el mecanismo de STP para evitar bucles de red que podrían hacer que las subredes se vuelvan inutilizables. 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 infinitamente a máxima velocidad.

Atención - 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 desactiva varias optimizaciones importantes que están en el hardware (NIC), el controlador y otras capas del sistema. La desactivación de estas mejoras de rendimiento es una consecuencia inevitable del mecanismo de puentes.

Estos problemas de rendimiento sólo afectan a esos enlaces que están configurados para formar parte de un puente. Puede utilizar un puente en un sistema donde algunos de los enlaces del sistema no están conectados mediante puentes y, por lo tanto, no están sujetos a dichas restricciones.

- Interconexión transparente de muchos enlaces (TRILL)

  Oracle Solaris admite la mejora de la protección de TRILL, lo cual evita los bucles sin desactivar enlaces. TRILL ayuda a equilibrar la carga del tráfico entre varias rutas hacia el destino.

Cuando STP se utiliza para la protección contra bucles, el bucle físico se mitiga evitando que una de las conexiones del bucle reenvíe paquetes. En la Figura 4-3, “Anillo de red con puentes”, se muestra que el enlace físico entre los puentes `westminster` y `tower` no se utiliza para reenviar paquetes.

A diferencia de STP, 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.

Puede utilizar TRILL especificando la opción `-P trill` en los comandos `dladm create-bridge` o `dladm modify-bridge`. Para obtener más información, consulte “Creación de un puente” [73] and “Modificación del tipo de protección de un puente” [74].

Para obtener información sobre STP, consulte IEEE 802.1D-1998. Para obtener información sobre TRILL, consulte Internet Engineering Task Force (IETF) TRILL draft documents (http://tools.ietf.org/wg/trill).

Daemon de STP

Cada puente que crea usando el comando `dladm create-bridge` se representa como una instancia de la utilidad de gestión de servicios (SMF, Service Management Facility) denominada de manera idéntica de `svc:/network/bridge`. Cada instancia ejecuta una copia del daemon `/usr/lib/bridged`, que implementa el STP.

Por ejemplo, el siguiente comando 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`. El nodo de observación está destinado para su uso con el comando `snoop` y el analizador de paquetes `wireshark`. Puede utilizar el comando `dlstat` para obtener las estadísticas de tiempo de ejecución del puente.

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 recuento de saltos ni valor de tiempo de vida (TTL) en los paquetes, cualquiera de esos bucles son críticos para la red.

Cuando sabe que un puerto concreto no está conectado a otro puente (por ejemplo, porque tiene una conexión punto a punto directa a un sistema host), puede desactivar administrativamente el STP de ese puerto. Incluso si todos los puertos de un puente tienen el STP desactivado, el daemon de STP se sigue ejecutando por los siguientes motivos:

- Para poder manejar los nuevos puertos que se agregan.
- Para implementar la protección de BPDU.
- Para activar o desactivar el reenvío en los puertos, según sea necesario.

Cuando un puerto tiene el STP desactivado, el daemon `bridged` escucha BPDU (protección de BPDU). El daemon utiliza `syslog` para marcar los errores y desactiva el reenvío en el puerto para indicar un error grave de la configuración de la red. El enlace se activa nuevamente cuando el estado del enlace se desactiva y se vuelve a activar, o cuando se elimina manualmente el enlace y se lo vuelve a agregar.

Si desactiva la instancia del servicio SMF de un puente, el puente se detiene en esos 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.

Por ejemplo, el siguiente comando 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`.

Creación de un puente

En Oracle Solaris, utilice el comando `dladm` y la función SMF para administrar puentes. Utilice los comandos SMF para activar, desactivar y supervisar instancias de puentes mediante el identificador de recurso de gestión de errores (FMRI, Fault-Managed Resource Identifier) de la instancia, `svc:/network/bridge`. Utilice el comando `dladm` para crear o destruir puentes, así como para asignar enlaces a puentes o para eliminar enlaces de ellos. Los enlaces que se asignan al puente deben ser un tipo de Ethernet, que incluye medios 802.3 y 802.11.

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 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 crea puentes entre enlaces de red de manera predeterminada.

Para crear un puente, utilice el siguiente comando:

```
# dladm create-bridge [–P protect] [–p priority] [–d forward-delay] [–l link...] bridge-name
```

`-P` *protect*
: Especifica el método de protección. Se puede establecer en uno de los siguientes valores.
  - `stp`: método de protección de STP (valor predeterminado)
  - `trill`: método de protección de TRILL

`-p` *priority*
: Especifica un valor de prioridad de STP de IEEE para un puente a fin de determinar el nodo de puente raíz de la red. El valor predeterminado es `32768`. Los valores válidos oscilan entre `0` (prioridad más alta) y `61440` (prioridad más baja), en incrementos de 4.096.

`-d` *forward-delay*
: Especifica el parámetro de retraso de reenvío de STP para el puente. Cuando el puente que se crea es el nodo raíz, todos los puentes de la red usan este temporizador para secuenciar los estados de enlace cuando se activa un puerto. El valor predeterminado es de `15` segundos. Los valores válidos van de `4` a `30` segundos.

`-l` *link*
: Agrega un enlace a un puente. Si alguno de los enlaces especificados no se puede agregar, el comando falla y el puente no se crea.

bridge-name es una cadena arbitraria que debe ser un nombre de instancia de servicio SMF legal. Este nombre es un componente de 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` y todos los nombres que empiezan con la cadena `SUNW` están reservados. Los nombres que contengan dígitos finales están reservados para la creación de dispositivos de observación, los cuales se utilizan para la depuración. Debido al uso de dispositivos de observación, los nombres de instancias de puentes legales se limitan aún más para que sean nombres `dlpi` legales. 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.

Para obtener más información sobre opciones de creación de puentes, consulte la descripción del comando `dladm create-bridge` en la página del comando man `dladm`(1M).

EJEMPLO 4-1 Creación de un puente

En el ejemplo siguiente, se muestra cómo crear el puente `brooklyn` mediante la conexión de los enlaces `net0` y `net1`.

```
# dladm create-bridge -P stp -d 12 -l net0 -l net1 brooklyn
# dladm show-bridge
BRIDGE       PROTECT ADDRESS           PRIORITY DESROOT
goldengate   stp     32768/8:0:20:bf:f 32768    8192/0:d0:0:76:14:38
brooklyn     stp     32768/8:0:20:e5:8 32768    8192/0:d0:0:76:14:38
```

En el ejemplo siguiente, se muestra cómo crear el puente `westminister` mediante la conexión de los enlaces `net0` y `net1`.

```
# dladm create-bridge -P trill -l net0 -l net1 westminister
# dladm show-bridge
BRIDGE       PROTECT ADDRESS           PRIORITY DESROOT
goldengate   stp     32768/8:0:20:bf:f 32768    8192/0:d0:0:76:14:38
westminister trill   32768/8:0:20:e5:8 32768    8192/0:d0:0:76:14:38
```

Modificación del tipo de protección de un puente

STP es un mecanismo para evitar bucles de red que podrían provocar que las subredes se vuelvan inutilizables. Además de utilizar STP para puentes, Oracle Solaris admite la mejora de la protección de TRILL. El STP se utiliza de manera predeterminada; pero usted puede utilizar TRILL especificando la opción `-P trill` para los comandos de puentes.

Para modificar el tipo de protección de STP a TRILL o de TRILL a STP, utilice el siguiente comando:

```
# dladm modify-bridge -P protection-type bridge-name
```

La opción `-P` *protection-type* especifica qué tipo de protección se debe utilizar, ya sea `stp` (el valor predeterminado) o `trill`.

EJEMPLO 4-2 Modificación del tipo de protección de un puente

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
```

En el siguiente ejemplo, se muestra cómo cambiar el tipo de protección para el puente `brooklyn` de TRILL a STP.

```
# dladm modify-bridge -P stp brooklyn
```

Agregación de enlaces a un puente existente

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 instancia de puente, primero debe eliminar el enlace del puente actual antes de agregarlo a otro puente.

Los enlaces que se asignan a un mismo puente deben tener el mismo valor de MTU. Aunque puede cambiar el valor de MTU en un enlace existente, la instancia de puente pasa al estado de mantenimiento hasta que se eliminan o cambian los enlaces asignados, de manera que los valores de MTU coincidan antes de reiniciar el puente.

Nota - Los enlaces que se asignan a un puente no pueden ser VLAN, VNIC ni túneles. Sólo se pueden asignar a un puente los enlaces que son aceptables como parte de una agregación o los enlaces que son agregaciones.

Para agregar un nuevo enlace a un puente existente, utilice el siguiente comando:

```
# dladm add-bridge -l new-link bridge-name
```

En el siguiente ejemplo, se muestra cómo agregar el enlace `net2` al puente existente `rialto`.

```
# dladm add-bridge -l net2 rialto
```

Eliminación de enlaces de un puente

Antes de suprimir cualquier puente, deben eliminarse todos sus enlaces. Para eliminar enlaces, utilice el siguiente comando:

```
# dladm remove-bridge [-l link]... bridge-name
```

En el siguiente ejemplo, se muestra cómo eliminar los enlaces `net0`, `net1` y `net2` del puente `charles`.

```
# dladm remove-bridge -l net0 -l net1 -l net2 charles
```

Configuración de propiedades de enlace de un puente

Puede definir las siguientes propiedades de enlace para puentes:

`default_tag` — El ID de VLAN predeterminado para paquetes sin etiquetas que se envían a un enlace y se reciben de un enlace. Los valores válidos van de `0` a `4094`. El valor predeterminado es `1`.

`forward` — Activa y desactiva el reenvío de tráfico por medio del puente. Esta propiedad existe en todos los enlaces, excepto los enlaces VNIC. Los valores válidos son `1` (true) y `0` (false). El valor predeterminado es `1`.

`stp` — Activa y desactiva STP y RSTP. Los valores válidos son `1` (true) y `0` (false). El valor predeterminado es `1`, que activa STP y RSTP.

`stp_cost` — Representa los 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.

`stp_edge` — Especifica si el puerto está conectado a otros puentes. Los valores válidos son `1` (true) y `0` (false). El valor predeterminado es `1`.

`stp_p2p` — Especifica el tipo de modo de conexión. Los valores válidos son `true`, `false` y `auto`. El valor predeterminado es `auto`.

`stp_priority` — Define el valor de prioridad de puerto de STP y RSTP. Los valores válidos van de `0` a `255`. El valor predeterminado es `128`.

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

Para modificar las propiedades de enlace de un puente, utilice el siguiente comando:

```
dladm set-linkprop -p prop=value  link
```

EJEMPLO 4-3 Configuración de propiedades de enlace de un puente

El ejemplo siguiente muestra cómo desactivar el reenvío de tráfico y definir el tipo de modo de conexión. A fin de definir las propiedades para el puente, debe definir las propiedades en los enlaces que conectan el puente.

```
# dladm create-bridge -P stp -d 12 -l net0 -l net1 brooklyn
# dladm set-linkprop -p forward=0 net0
# dladm set-linkprop -p stp_p2p=true net1
```

El siguiente ejemplo muestra cómo restablecer varias propiedades de un puente.

```
# dladm reset-linkprop -p default_tag,stp_priority brooklyn
```

Visualización de información de la configuración de un puente

Puede visualizar la información de configuración de un puente utilizando el comando `dladm show-bridge`.

Visualización de información sobre puentes configurados

Puede utilizar los comandos `dladm show-bridge` y `dlstat show-bridge` para mostrar diferentes tipos de información sobre los puentes configurados.

Utilice las siguientes opciones de comando:

- Para ver la lista de puentes:

  ```
  # dladm show-bridge
  ```

  ```
  # 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
  ```

- Para mostrar el estado de un puente en relación con los enlaces:

  ```
  # dladm show-bridge -l bridge-name
  ```

- Para mostrar estadísticas relacionadas con enlaces para el puente:

  ```
  # dlstat show-bridge bridge-name
  ```

- Para mostrar entradas de reenvíos de núcleos para el puente:

  ```
  # dladm show-bridge -f bridge-name
  ```

- Para mostrar información de TRILL sobre el puente:

  ```
  # dladm show-bridge -t bridge-name
  ```

- Para mostrar las estadísticas de cada puente y las estadísticas de los enlaces conectados a cada puente:

```
# dlstat show-bridge

BRIDGE     LINK       IPKTS    RBYTES     OPKTS    OBYTES     DROPS  FORWARDS
rbblue0     --        1.93K   587.29K     2.47K     3.30M         0         0
           simblue1     72     4.32K     2.12K     2.83M         0        --
           simblue2  1.86K   582.97K       348   474.04K         0        --
stbred0     --         975   976.69K     3.44K     1.13M         0        38
           simred3    347   472.54K     1.86K   583.03K         0        --
           simred4    628   504.15K     1.58K   551.51K         0        --
```

- Para mostrar todas estadísticas de cada puente y las estadísticas de los enlaces conectados a cada puente:

```
# dlstat show-bridge -o all
```

Para obtener más información sobre las opciones del comando `dladm show-bridge`, consulte la página del comando man dladm(1M); y, para obtener información sobre las opciones del comando `dlstat show-bridge`, consulte la página del comando man dlstat(1M).

EJEMPLO 4-4 Visualización de información de puentes

Los siguientes ejemplos muestran cómo utilizar el comando `dladm show-bridge` con diferentes opciones.

- El siguiente comando muestra información de estado relacionada con enlaces para una única instancia de puente, `tower`. Para ver las propiedades configuradas, utilice el comando `dladm show-linkprop`.

```
# dladm show-bridge -l tower
LINK         STATE        UPTIME   DESROOT
net0         forwarding   117      8192/0:d0:0:76:14:38
net1         forwarding   117      8192/0:d0:0:76:14:38
```

- El siguiente comando muestra las 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  --     net0
8:0:20:bf:f9:69  --      L      net0
8:0:20:c0:20:26  17.420  --     net0
8:0:20:e5:86:11  --      L      net1
```

- El siguiente comando muestra la 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     --          --
```

Visualización de información de configuración sobre enlaces de puentes

Se utiliza el comando `dladm show-link` con la opción `-o all` para mostrar el campo `BRIDGE` en la salida. Si un enlace es un miembro de un puente, este campo identifica el nombre del puente del cual es miembro. 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 de `dladm show-link` como un enlace separado. Para este nodo, el campo `OVER` existente muestra los enlaces que son miembros del puente.

Utilice el siguiente comando para ver 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.

Supresión de un puente del sistema

Antes de suprimir un puente, primero debe eliminar cualquier enlace conectado al puente.

▼ Cómo suprimir un puente del sistema

1. **Conviértase en un administrador.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Elimine todos los enlaces conectados al puente.**

   ```
   # dladm remove-bridge [-l link]... bridge-name
   ```

3. **Suprima el puente del sistema.**

   ```
   # dladm delete-bridge bridge-name
   ```

ejemplo 4-5 Supresión de un puente del sistema

En el ejemplo siguiente, se muestra cómo eliminar los enlaces `net0`, `net1` y `net2` del puente `coronado` y luego suprimir el puente del sistema.

```
# dladm remove-bridge -l net0 -l net1 -l net2 coronado
# dladm delete-bridge coronado
```

Administración de las VLAN en redes con puentes

De manera predeterminada, las VLAN que están configuradas en el sistema reenvían paquetes a todos los puertos de una instancia del bridge. Cuando se invocan los comandos `dladm create-vlan` o `dladm create-vnic -v`, y si el enlace subyacente es parte de un puente, los comandos también permitirán el reenvío de la VLAN especificada en el enlace de puente. Para obtener más información sobre las VLAN, consulte el Capítulo 3, Configuración de redes virtuales mediante redes de área local virtuales.

Para configurar una VLAN en un enlace y desactivar el reenvío hacia otros enlaces o desde ellos en el puente, debe desactivar el reenvío estableciendo la propiedad `forward` para la VLAN con el comando `dladm set-linkprop`. Para obtener más información, consulte “Configuración de propiedades de enlace de un puente” [76].

▼ Cómo configurar VLAN en un enlace de datos que forma parte de un puente

Antes de empezar Este procedimiento asume que el puente ya existe. Para obtener información sobre cómo crear un puente, consulte “Creación de un puente” [73].

1. **Conviértase en un administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Visualice la información relacionada con los enlaces del puente para determinar qué enlaces forman parte del puente.**

   ```
   # dladm show-bridge -l bridge-name
   ```

3. **Cree la VLAN en el enlace que forma parte del puente.**

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

link Especifica el enlace en el que se crea la interfaz VLAN.

Nota - En este procedimiento, el enlace debe ser parte del puente que ha creado.

vid Indica el número de ID de VLAN.

VLAN-link Especifica el nombre de la VLAN.

4. **Repita este comando para cada VLAN que desee crear. Para cada VLAN que haya creado, cree una interfaz IP en la VLAN.**

   # ipadm create-ip *interface*

   Donde *interface* es el nombre de la VLAN.

5. **Para cada interfaz IP en una VLAN, configure una dirección IP válida.**

   # ipadm create-addr -a *IP-address interface*

Las redes VLAN y los protocolos STP y TRILL

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 esta topología de árbol para activar y desactivar enlaces. Debe configurar los enlaces duplicados que se proporcionan en sus redes, de manera que cuando esos enlaces son desactivados de forma automática por el STP, las VLAN configuradas no se desconectan. Debe ejecutar todas las VLAN en toda la red principal con puentes o examinar con cuidado todos los enlaces redundantes.

El protocolo TRILL no sigue las reglas STP complejas. En cambio, TRILL encapsula automáticamente los paquetes que tienen la etiqueta de VLAN intacta y los transfiere por la red.

Depuración de puentes

A cada instancia de puente se le asigna un *nodo de observación* que aparece en el directorio `/dev/net/` y se la denomina con el nombre de puente seguido de `0`, por ejemplo, `/dev/net/bridgeofsighs0`.

El nodo de observación está destinado para su uso con el comando `snoop` y el analizador de paquetes `wireshark`. Este nodo funciona como una interfaz Ethernet estándar, excepto para la

transmisión de paquetes, que se descartan de manera silenciosa. No puede asociar IP además de un nodo de observación y no puede realizar solicitudes de enlace (`DL_BIND_REQ`), a menos que utilice la opción `passive`, que sólo permite recibir paquetes y no enviarlos.

El nodo de observación realiza una copia única sin modificaciones de cada paquete gestionado por el puente. Está disponible para supervisión y depuración por parte del usuario. Este comportamiento es similar a la supervisión de un puerto en un puente tradicional y está sujeto a las reglas habituales del modo promiscuo de la interfaz de proveedor de enlace de datos (DLPI, Data Link Provider Interface). Puede utilizar el comando `pfmod` o las funciones del comando `snoop` y el analizador de paquetes `wireshark` para filtrar paquetes en función del ID de la VLAN.

Los paquetes entregados, que son los paquetes que se envían al nodo de observación, representan los datos recibidos por el puente.

Nota - Cuando el proceso de puente agrega, elimina o modifica una etiqueta de VLAN, los datos que muestran el comando `snoop` y el analizador de paquetes `wireshark` describen el estado previo a los procesos. Esta situación inusual puede resultar confusa si existen valores `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 puente se completa), ejecute el comando `snoop` en los enlaces individuales, en lugar de ejecutarlo en el nodo de observación del puente.

También puede obtener estadísticas sobre cómo los paquetes de red usan los recursos de red en los enlaces mediante el comando `dlstat`. Para obtener información, consulte el Capítulo 8, “Supervisión del tráfico de red y el uso de recursos” de “Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ”.

♦ ♦ ♦ CAPÍTULO 5

Intercambio de información de conectividad de red con el protocolo de descubrimiento de capa de enlace

En este capítulo, se describe cómo activar 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).

Este capítulo se divide en los siguientes apartados:

Descripción general de LLDP

Los sistemas en una red de área local (LAN) utilizan LLDP para intercambiar información de configuración y gestión entre sí. Con este protocolo, un sistema puede anunciar la conectividad y la información de gestión para otros sistemas de la red. En esta información, puede que se incluyan las capacidades del sistema, las direcciones de gestión y otros aspectos relativos al funcionamiento de redes. Este protocolo también permite a los sistemas recibir información similar sobre otros sistemas que se están en la misma red local.

En cualquier LAN, los componentes individuales, como los sistemas y los conmutadores, no se configuran de manera aislada. Para alojar el tráfico de red de manera eficaz, la configuración de todos los sistemas de la red tiene que estar coordinada.

Al configurar manualmente cada sistema, conmutador y otros componentes, es difícil garantizar la compatibilidad entre los componentes. La configuración manual de los sistemas es riesgosa y puede ocasionar errores en la configuración fácilmente, en particular si varios administradores

trabajan de manera independiente en distintos sistemas. Una alternativa mejor es utilizar LLDP, que permite a los sistemas transmitir su información de configuración individual a sistemas iguales y ayuda a detectar las configuraciones incorrectas.

Oracle Solaris admite el uso de LLDP para promover el intercambio de información sobre la conectividad de red y el sistema entre los sistemas de la red, lo que reduce el riesgo de errores de configuración en los recursos de red.

En esta versión, el servicio de diagnóstico de red utiliza LLDP para detectar automáticamente los problemas que pueden limitar o degradar la conectividad de red. Activar el servicio de LLDP mejora la capacidad para realizar diagnósticos de red en el sistema Oracle Solaris. Para obtener más información sobre la realización de diagnósticos de red, consulte el Capítulo 4, “Realización de diagnósticos de red con la network-monitor Utilidad del módulo de transporte” de “Resolución de problemas de administración de redes en Oracle Solaris 11.2 ”.

En Oracle Solaris, el LLDP también se utiliza para intercambiar unidades de tiempo-longitud-valor (TLV, Time-Length-Value) del protocolo de intercambio del puente de centro de datos (DCBX, Data Center Bridging Exchange Protocol). DCBX proporciona información de configuración de funciones de DCB, como el control de flujo basado en prioridades (PFC, Priority-Based Flow Control) y la selección de transmisión mejorada (ETS, Enhanced Transmission Selection). Para obtener más información acerca de DCB, consulte el Capítulo 6, Gestión de redes convergentes mediante el puente de centro de datos.

Con LLDP, el administrador del sistema puede detectar fácilmente las configuraciones del sistema defectuosas, especialmente en las redes complejas, como las redes de área local virtuales (VLAN) y las agregaciones de enlaces. La información sobre la topología de red se puede obtener fácilmente sin necesidad de realizar un seguimiento de las conexiones físicas entre servidores, conmutadores u otros dispositivos que componen la red.

Componentes de una implementación LLDP

LLDP se implementa con los siguientes componentes:

- **Paquete LLDP**: se instala este paquete para activar LLDP. Este paquete incluye 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 el LLDP funcione.
- **Servicio de LLDP**: puede activar el servicio de LLDP con el comando `svcadm`. Este servicio utiliza el identificador de recurso de gestión de errores (FMRI) de la instancia del servicio de la utilidad de gestión de servicios (SMF), `svc:/network/lldp:default`, para gestionar el daemon LLDP, `lldpd`. Este servicio de LLDP es responsable de iniciar, detener, reiniciar y refrescar el daemon `lldpd`. Este servicio se activa automáticamente después de instalar el paquete LLDP.
- **Comando** `lldpadm`: puede utilizar este comando para administrar el LLDP en enlaces individuales y para configurar el modo de funcionamiento de LLDP, para especificar las

unidades de TLV que se transmiten y para configurar las unidades de TLV de DCBX. Para obtener información sobre las unidades de TLV, consulte “Información anunciada por el agente LLDP” [86].

Debe utilizar este comando para establecer las propiedades de LLDP globales y las propiedades de LLDP por agente, y para obtener la información de LLDP para un agente determinado o su igual.

En las siguientes secciones, se describen los subcomandos `lldpadm`. Para obtener más información sobre el comando `lldpadm`, consulte la página del comando man `lldpadm`(1M).

- **Daemon LLDP**: los servicios de LLDP gestionan los agentes LLDP en el sistema. También interactúan 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.
- **Agentes LLDP**: los agentes LLDP son las instancias de LLDP que están asociadas a un enlace de datos físico en el que LLDP está activado. Los agentes LLDP transmiten información sobre el enlace de datos a su igual y también reciben información del igual. Puede configurar un agente LLDP para anunciar información específica sobre el enlace de datos físico asociado. Sólo puede activar LLDP en los enlaces de datos físicos.

Fuentes de información del agente LLDP

El agente LLDP transmite y recibe unidades de datos de LLDP (LLDPDU). El agente gestiona y almacena la información contenida en estas LLDPDU en los siguientes tipos de almacenes de datos:

- **Base de información gestionada local (MIB)**: este almacén de datos contiene información de red que pertenece a un enlace específico de un sistema en el que el agente LLDP está activado. 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 ID 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 se recibe de agentes LLDP de hosts iguales.

Modos del agente LLDP

El agente LLDP funciona en los siguientes modos:

- Modo de transmisión únicamente (`txonly`): el agente LLDP no procesa LLDPDU entrantes. Por lo tanto, la MIB remota está vacía.

- Modo de recepción únicamente (`rxonly`): el agente LLDP procesa únicamente LLDPDU entrantes y almacena la información en MIB remotas. Sin embargo, no se transmite ninguna información de la MIB local.
- Modo de transmisión y recepción (`both`): el agente transmite la información local y procesa LLDPDU entrantes, y, por lo tanto, mantiene tanto MIB locales como remotas.
- Modo de desactivación (`disable`): el agente no existe.

Para obtener más información sobre la configuración de modos del agente, consulte Cómo activar LLDP para puertos específicos [91].

Información anunciada por el agente LLDP

El agente LLDP transmite información sobre el sistema y la conectividad en los paquetes LLDP o en las LLDPDU. Los paquetes pueden contener unidades de información formateadas individualmente en TLV. Las unidades de información también se denominan *unidades de TLV*.

Unidades de TLV obligatorias

Determinadas unidades de TLV son obligatorias y se incluyen en los paquetes LLDP de manera predeterminada cuando se activa el LLDP. No puede utilizar el comando `lldpadm` para excluir ninguna de estas unidades.

Las siguientes unidades de TLV son obligatorias:

- ID de chasis: información que genera el comando `hostid`
- ID de puerto: dirección MAC de la NIC física
- TTL (tiempo de actividad)
- Final de la unidad de datos de protocolo (PDU)

Se pueden activar varios agentes LLDP en un único sistema en función del número de enlaces. La combinación del ID de chasis con el ID de puerto identifica un agente de manera exclusiva y lo distingue de los otros agentes del sistema.

EJEMPLO 5-1 Visualización del ID de chasis y el ID de puerto

El ejemplo siguiente muestra el ID de chasis y el ID de puerto para un agente LLDP.

```
# hostid
004e434e

# dladm show-phys -m net4
LINK                SLOT     ADDRESS            INUSE CLIENT
net4                primary  0:1b:21:87:8b:b4   yes   net4
```

```
# lldpadm show-agent -l net4
AGENT               CHASSISID           PORTID
net4                004e434e            00:1b:21:87:8b:b4
```

Los agentes LLDP de Oracle Solaris usan `hostid` como el ID de chasis y la dirección MAC del puerto como el ID de puerto.

Unidades de TLV opcionales

Se pueden agregar unidades de TLV opcionales a un paquete LLDP. Estas unidades de TLV opcionales permiten a los proveedores insertar unidades de TLV específicas del proveedor para anunciarlas. LLDP permite definir unidades de TLV adicionales mediante identificadores únicos de organización (OUI, Individual Organization Unique Identifiers). Un OUI identifica la categoría para una unidad de TLV en función de si el OUI cumple con el estándar IEEE 802.1 o IEEE 802.3. Las propiedades del agente LLDP se pueden configurar para activar o desactivar la transmisión de estas unidades de TLV opcionales.

En la siguiente tabla, se muestran los grupos de TLV, sus nombres correspondientes, las unidades de TLV de cada propiedad y sus descripciones. Debe configurar cualquiera de estas propiedades para especificar las unidades de TLV que se incluirán en los paquetes cuando se active el LLDP.

TABLA 5-1 Unidades de TLV opcionales para un agente LLDP

Grupo de TLV	Nombre de TLV	Unidades de TLV	Descripción
Gestión básica	`basic-tlv`	`sysname`, `portdesc`, `syscapab`, `sysdesc`, `mgmtaddr`	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.
OUI 802.1	`dot1-tlv`	`vlanname`, `pvid`, `linkaggr`, `pfc`, `appln`, `evb`, `etscfg`, `etsreco`	Especifica que se anuncie lo siguiente: nombre de VLAN, ID de VLAN de puerto, agregaciones de enlaces, unidades de TLV para control de flujo basado en prioridades, aplicación, selección de transmisión mejorada y puente virtual perimetral.
OUI 802.3	`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.

Propiedades de las unidades de TLV

Cada unidad de TLV tiene propiedades que pueden configurarse aún más con valores específicos. Si la unidad de TLV está activada como propiedad de un agente LLDP, se anuncia

en la red sólo con los valores especificados. Por ejemplo, tenga en cuenta la unidad 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 configuración de las unidades de TLV depende de si se configuran *unidades de TLV globales* o *unidades de TLV por agente*. Para obtener información sobre cómo configurar las unidades de TLV, consulte "Especificación de las unidades de TLV y los valores para el paquete LLDP de un agente" [93].

Las unidades de TLV globales se aplican a todos los agentes LLDP del sistema. La siguiente tabla muestra las unidades de TLV globales y sus correspondientes configuraciones posibles.

TABLA 5-2 Las unidades de TLV globales y sus propiedades

Unidad de TLV	Nombre de propiedad	Posibles valores de propiedad	Descripción del valor
`syscapab`	`supported`	`other`, `repeater`, `bridge`, `wlan-ap`, `router`, `telephone`, `docsis-cd`, `station`, `cvlan`, `sylvan`, `tpmr`	Representa las principales funciones admitidas del sistema. Los valores predeterminados son `router`, `station` y `bridge`.
	`enabled`	Subconjunto de valores listados para `supported`	Representa las funciones activadas del sistema.
`mgmtaddr`	`ipaddr`	`ipv4` o `ipv6`	Especifica el tipo de direcciones IP que se asocian con el agente LLDP local. Las direcciones se utilizan para alcanzar entidades de capas superiores y ayudar a efectuar el descubrimiento mediante la gestión de red. Se puede especificar solamente un tipo.

Las unidades de TLV que son específicas del agente LLDP se gestionan por agente. Con las unidades de TLV por agente, los valores que proporciona se utilizan cuando la unidad de TLV se encuentra activada 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 5-3 Las unidades de TLV por agente y sus propiedades

Unidad de TLV	Nombre de propiedad	Posibles valores de propiedad	Descripción del valor
`pfc`	`willing`	`on`, `off`	Establece un agente LLDP para que acepte o rechace la información de configuración desde una máquina remota que pertenezca al control de flujo basado en prioridades.
`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

Unidad de TLV	Nombre de propiedad	Posibles valores de propiedad	Descripción del valor
			el par `id`/`selector`. El contenido de la tabla utiliza el siguiente formato: `id/selector/priority` Para obtener más información, consulte "Configuraciones de prioridades de la aplicación" [113].
`etscfg`	`willing`	`on`, `off`	Establece un agente LLDP para que acepte o rechace la información de configuración desde una máquina remota que pertenezca a la selección de transmisión mejorada.

Para obtener información sobre las unidades de TLV por agente, consulte el Capítulo 6, Gestión de redes convergentes mediante el puente de centro de datos.

Activación de LLDP en el sistema

Puede configurar el LLDP para intercambiar información del sistema con otros hosts o iguales en la red.

La propiedad de SMF `auto-enable-agents` controla la forma en la que puede activar los agentes LLDP en el sistema. Con esta propiedad, puede optar por activar LLDP globalmente en todos los enlaces físicos o sólo en un enlace por vez.

La propiedad de SMF `auto-enable-agents` puede tener uno de los siguientes tres valores posibles:

- `yes` activa el LLDP en todos los puertos en el modo de transmisión y recepción (`both`) siempre que no exista ninguna configuración de LLDP anterior en el puerto. Si existe una configuración anterior en un puerto, se mantiene la configuración de ese puerto. Por ejemplo, si el puerto se ha configurado anteriormente con LLDP en el modo `rxonly`, el servicio de LLDP no modificará el agente para que se ejecute en los modos de transmisión y recepción (`both`). El LLDP en dicho puerto seguirá estando en el modo `rxonly`. Este es el valor predeterminado de la propiedad de SMF `auto-enable-agents`.
- `force` activa el LLDP en los modos de transmisión y recepción (`both`) en todos los puertos y sustituye cualquier configuración de LLDP existente en cualquier puerto. Por ejemplo, si una configuración de LLDP anterior en un puerto se ejecuta en modo `rxonly`, el agente LLDP se modifica para que se ejecute en el modo de transmisión y recepción (`both`), que es el modo predeterminado de LLDP.
- `no` desactiva la activación automática de LLDP en todos los puertos, excepto en los que ya tengan configuraciones de LLDP existentes. En estos puertos, se mantiene la configuración de LLDP existente.

Nota - Cada vez que personaliza la propiedad `auto-enable-agents`, debe reiniciar el servicio de LLDP para que se active el nuevo valor.

▼ Cómo instalar el paquete DNS

De manera predeterminada, el LLDP está activado y listo para usar una vez completada la instalación del paquete LLDP.

1. **Conviértase en un administrador.**

   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Instale el paquete.**

   ```
   # pkg install lldp
   ```

3. **Determine si el servicio de LLDP se haya iniciado.**

   ```
   # svcs lldp
   STATE          STIME    FMRI
   online         Jul_10   svc:/network/lldp:default
   ```

   Si el servicio de LLDP está desactivado, inícielo con el siguiente comando:

   ```
   # svcadm enable svc:/network/lldp:default
   ```

▼ Cómo activar LLDP globalmente

Antes de empezar Para activar LLDP, primero debe instalar el paquete LLDP. Para obtener más información, consulte Cómo instalar el paquete DNS [90].

1. **Conviértase en un administrador.**

   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Cambie la propiedad de SMF `auto-enable-agents` a `yes` si está definida en `no`.**

   ```
   # svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "yes"
   ```

   De manera predeterminada, el valor de esta propiedad es `yes`.

3. **Reinicie el servicio de LLDP.**

```
# svcadm restart svc:/network/lldp:default
```

4. **(Opcional) Personalice las unidades de TLV globales.**

   ```
   # lldpadm set-tlvprop -p property=value global-TLV
   ```

   Donde *property* hace referencia a la propiedad de la unidad de TLV global.

Pasos siguientes

Para obtener una explicación acerca de las unidades de TLV globales, consulte "Propiedades de las unidades de TLV" [87].

Para mostrar una lista de las unidades de TLV globales, escriba `lldpadm show-tlvprop` o consulte la Tabla 5-2, "Las unidades de TLV globales y sus propiedades".

Para obtener instrucciones sobre cómo definir los valores de TLV, consulte Cómo definir las unidades de TLV [95].

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

▼ Cómo activar LLDP para puertos específicos

Antes de empezar

Para activar LLDP, primero debe instalar el paquete LLDP. Para obtener más información, consulte Cómo instalar el paquete DNS [90].

1. **Conviértase en un administrador.**
   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Cambie la propiedad de SMF `auto-enable-agents` a `no` si está definida en `yes`.**

   ```
   # svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "no"
   ```

   De manera predeterminada, el valor de esta propiedad es `yes`.

3. **Reinicie el servicio de LLDP si ha cambiado la propiedad de SMF `auto-enable-agents` en el paso 2.**

   ```
   # svcadm restart svc:/network/lldp:default
   ```

4. **Active los agentes LLDP en determinados puertos o enlaces.**

   ```
   # lldpadm set-agentprop -p mode=value agent
   ```

   Donde *agent* es el agente LLDP y se identifica mediante el enlace físico en el que el agente está activado. Por ejemplo, si activa el LLDP en `net0`, el agente es `net0`.

La propiedad `mode` puede establecerse en uno de cuatro valores posibles que representan los modos de funcionamiento del agente LLDP: `txonly`, `rxonly`, `both` y `disable`. Para obtener una explicación sobre estos valores, consulte “Modos del agente LLDP” [85].

5. **Especifique las unidades de TLV que el agente LLDP puede anunciar.**

   ```
   # lldpadm set-agentprop -p property=value agent
   ```

   Para obtener una explicación de las propiedades del agente LLDP, consulte “Información anunciada por el agente LLDP” [86].

   Para mostrar una lista de las otras propiedades del agente LLDP, escriba `lldpadm show-agentprop` o consulte la Tabla 5-1, “Unidades de TLV opcionales para un agente LLDP”.

   Para obtener instrucciones sobre cómo especificar las unidades de TLV para el paquete LLDP de un agente, consulte Cómo especificar unidades de TLV para el paquete LLDP de un agente [94].

6. **(Opcional) Personalice las unidades de TLV por agente.**

   ```
   # lldpadm set-agenttlvprop -p property=value -a agent per-agent-TLV
   ```

   Donde *property* hace referencia a la propiedad de la unidad de TLV por agente.

   Para obtener una explicación acerca de las unidades de TLV por agente, consulte “Propiedades de las unidades de TLV” [87].

   Para mostrar una lista de TLV por agente, escriba `lldpadm show-agenttlvprop` o consulte la Tabla 5-3, “Las unidades de TLV por agente y sus propiedades”.

   Para obtener instrucciones sobre cómo definir los valores de TLV, consulte Cómo definir las unidades de TLV [95].

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

ejemplo 5-2 Personalización de la propiedad de SMF `auto-enable-agents`

En el siguiente ejemplo, se muestra la manera diferente en que se activa el LLDP si cambia el valor de la propiedad de SMF `auto-enable-agents`. Por ejemplo, en un sistema con cuatro puertos, el LLDP se configura en dos puertos, de la siguiente manera:

- `net0`: modo `both`
- `net1`: modo `rxonly`
- `net2` y `net3`: ninguno

Si la propiedad de SMF `auto-enable-agents` tiene el valor predeterminado `yes`, LLDP se activa automáticamente en `net2` y `net3`. Puede mostrar la configuración de LLDP de la siguiente manera:

```
# lldpadm show-agentprop -p mode
AGENT   PROPERTY   PERM   VALUE   DEFAULT   POSSIBLE
net0    mode       rw     both    disable   txonly,rxonly,both,disable
net1    mode       rw     rxonly  disable   txonly,rxonly,both,disable
net2    mode       rw     both    disable   txonly,rxonly,both,disable
net3    mode       rw     both    disable   txonly,rxonly,both,disable
```

Si cambia la propiedad de SMF a `no`, la configuración se modifica cuando se reinicia el servicio.

```
# svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "no"
# svcadm restart svc:/network/lldp:default
# lldpadm show-agentprop -p mode
AGENT   PROPERTY   PERM   VALUE    DEFAULT   POSSIBLE
net0    mode       rw     both     disable   txonly,rxonly,both,disable
net1    mode       rw     rxonly   disable   txonly,rxonly,both,disable
net2    mode       rw     disable  disable   txonly,rxonly,both,disable
net3    mode       rw     disable  disable   txonly,rxonly,both,disable
```

En la salida de ejemplo, `net2` y `net3`, cuyos modos de LLDP se habían activado antes automáticamente, ahora están marcados como desactivados. Sin embargo, no se produce ningún cambio en `net0` y `net1`, cuyos agentes de LLDP se habían configurado previamente.

ejemplo 5-3 Activación de LLDP en varios enlaces de datos

En este ejemplo, se muestra cómo activar LLDP de manera selectiva. El sistema tiene dos enlaces de datos, `net0` y `net1`. En `net0`, para que el agente transmita y reciba los paquetes LLDP, y en `net1`, para que el agente sólo transmita los paquetes LLDP, escriba los siguientes comandos:

```
# svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "no"
# svcadm restart svc:/network/lldp:default
# lldpadm set-agentprop -p mode=both net0
# lldpadm set-agentprop -p mode=txonly net1
# lldpadm show-agentprop -p mode
AGENT   PROPERTY   PERM   VALUE    DEFAULT   POSSIBLE
net0    mode       rw     both     disable   txonly,rxonly,both,disable
net1    mode       rw     txonly   disable   txonly,rxonly,both,disable
```

Especificación de las unidades de TLV y los valores para el paquete LLDP de un agente

Puede especificar unidades de TLV como `dot1-tlv` y `basic-tlv` como valores de propiedad para un agente LLDP. Puede configurar aún más estos valores de propiedad. Para especificar unidades de TLV, utilice el comando `lldpadm set-agentprop`. Para obtener más información, consulte la página del comando man `lldpadm`(1M). Cuando la unidad de TLV se especifica como una propiedad de un agente LLDP, se anuncia en la red sólo con los valores que ha

especificado para las unidades de TLV. Para obtener información sobre las unidades de TLV y sus propiedades, consulte “Propiedades de las unidades de TLV” [87].

▼ Cómo especificar unidades de TLV para el paquete LLDP de un agente

En este procedimiento, se explica cómo especificar unidades de TLV que se vayan a anunciar en un paquete LLDP que transmita un agente.

1. **Conviértase en un administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **(Opcional) Identifique la propiedad del agente LLDP que pueda contener la unidad de TLV que desea agregar mostrando las unidades de TLV.**

   ```
   # lldpadm show-agentprop agent
   ```

   Este comando le permite ver las unidades de TLV que ya se han establecido para cada propiedad. Si no especifica una propiedad, este comando muestra todas las propiedades del agente LLDP y sus valores de TLV. Para obtener una lista de las propiedades del agente, consulte la Tabla 5-1, “Unidades de TLV opcionales para un agente LLDP”.

3. **Agregue o elimine la unidad de TLV en la propiedad.**

   ```
   # lldpadm set-agentprop -p property[+|-]=value[,...] agent
   ```

   Puede utilizar calificadores para agregar (+) o eliminar (-) valores de la lista de valores para las propiedades que aceptan varios valores.

   Si no utiliza los calificadores para agregar (+) o eliminar (-), el valor que establece reemplaza todos los valores que se hayan definido previamente para la propiedad.

4. **(Opcional) Muestre los nuevos valores para la propiedad.**

   ```
   # lldpadm show-agentprop -p property agent
   ```

ejemplo 5-4 Cómo agregar unidades de TLV opcionales a un paquete LLDP

En el ejemplo siguiente, el agente LLDP tiene configurado `net0` para anunciar la información de VLAN en el paquete LLDP. El paquete LLDP además está configurado para incluir información de las capacidades del sistema, la agregación de enlaces y la NIC virtual como elementos que el LLDP puede anunciar. Luego, la descripción de VLAN se elimina del paquete.

1. Visualice las propiedades existentes del agente.

```
# lldpadm show-agentprop net0
AGENT   PROPERTY   PERM   VALUE          DEFAULT   POSSIBLE
net0    mode       rw     both           disable   txonly,rxonly,both,disable
net0    basic-tlv  rw     sysname,        none     none,portdesc,
                          sysdesc                  sysname,sysdesc,
                                                   syscapab,mgmtaddr,
                                                   all
net0    dot1-tlv   rw     vlanname,       none     none,vlanname,pvid,
                          pvid,pfc                 linkaggr,pfc,appln,
                                                   evb,etscfg,etsreco,all
net0    dot3-tlv   rw     max-framesize   none     none, max-framesize,
                                                   all
net0    virt-tlv   rw     none            none     none,vnic,all
```

La salida muestra los valores posibles, predeterminados y existentes para cada propiedad del agente LLDP.

2. Defina información sobre las capacidades del sistema, la agregación de enlaces y la virtualización de red como elementos para anunciar mediante la red.

```
# lldpadm set-agentprop -p basic-tlv+=syscapab,dot1-tlv+=linkaggr,virt-tlv=vnic net0
```

3. Elimine la descripción de VLAN del paquete.

```
# lldpadm set-agentprop -p dot1-tlv-=vlanname net0
```

4. Visualice las propiedades del agente.

```
# 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,
                          sysdesc,                 sysname,sysdesc,
                          syscapab                 syscapab,mgmtaddr,
                                                   all
net0    dot1-tlv   rw     pvid,pfc        none     none,vlanname,pvid,
                          linkaggr                 linkaggr,pfc,appln,
                                                   evb,etscfg,etsreco,all
net0    dot3-tlv   rw     max-framesize   none     none, max-framesize,
                                                   all
net0    virt-tlv   rw     vnic            none     none,vnic,all
```

▼ Cómo definir las unidades de TLV

En este procedimiento, se explica cómo proporcionar los valores para unidades de TLV específicas.

Sugerencia - Puede restablecer las propiedades de TLV a sus valores predeterminados con el comando `lldpadm reset-tlvprop` para las unidades de TLV globales y el comando `lldpadm reset-agenttlvprop` para las unidades de TLV por agente.

1. **Conviértase en un administrador.**

   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Configure una unidad de TLV global o por agente.**

   - **Para configurar una unidad de TLV global, establezca la propiedad de TLV correspondiente para que contenga los valores que desea anunciar.**

     ```
     # lldpadm set-tlvprop -p TLV-property=value[,value,value,...] TLV-name
     ```

     Donde *TLV-name* es el nombre de la unidad de TLV global y *TLV-property* es una propiedad de dicha unidad de TLV. Se pueden asignar varios valores a la propiedad. Para obtener una lista de las unidades de TLV globales y sus propiedades, consulte la Tabla 5-2, "Las unidades de TLV globales y sus propiedades".

   - **Para configurar una unidad de TLV por agente, configure la propiedad de TLV correspondiente del agente LLDP para que contenga los valores que desea que el agente anuncie.**

     ```
     # lldpadm set-agenttlvprop -p TLV-property[+|-]=value[,value,value,...] -a agent TLV-name
     ```

     Donde *TLV-name* es el nombre de la unidad de TLV por agente y *TLV-property* es una propiedad de dicha unidad de TLV. Se pueden asignar varios valores a la propiedad. Para obtener una lista de las unidades de TLV por agente y sus propiedades, consulte la Tabla 5-3, "Las unidades de TLV por agente y sus propiedades".

     Puede utilizar calificadores para agregar (+) o eliminar (-) valores de la lista de valores para las propiedades que aceptan varios valores.

3. **(Opcional) Visualice los valores de la propiedad de TLV que configuró.**

   - **Para mostrar los valores de las propiedades de TLV globales:**

     ```
     # lldpadm show-tlvprop
     ```

   - **Para mostrar los valores de la propiedad de TLV de un agente:**

     ```
     # lldpadm show-agenttlvprop
     ```

ejemplo 5-5 Definición de valores de TLV para las unidades de TLV `syscapab` y `mgmtaddr`

En el siguiente ejemplo, se configura información específica sobre las capacidades del sistema que se deben anunciar en el paquete LLDP y la dirección IP de gestión.

1. Configure las propiedades `supported` y `enabled` de la unidad de TLV `syscapab`.

```
# lldpadm set-tlvprop -p supported=bridge,router,repeater syscapab
# lldpadm set-tlvprop -p enabled=router syscapab
```

2. Especifique la dirección IP de gestión para la unidad de TLV `mgmtaddr`.

```
# lldpadm set-tlvprop -p ipaddr=192.168.1.2 mgmtaddr
```

3. Visualice los valores de TLV de las propiedades del agente.

```
# lldpadm show-tlvprop
TLVNAME    PROPERTY   PERM  VALUE        DEFAULT         POSSIBLE
syscapab   supported  rw    bridge,      bridge,router,  other,router,
                            router,      station         repeater,bridge,
                            repeater                     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            --
```

   La salida incluye los valores predeterminados de las unidades de TLV y también los valores posibles que se pueden definir para la propiedad.

Para obtener información sobre la configuración de las propiedades de TLV por agente, consulte el Capítulo 6, Gestión de redes convergentes mediante el puente de centro de datos.

Desactivación de LLDP

En esta sección, se describe cómo desactivar el LLDP de manera selectiva en puertos individuales.

▼ Cómo desactivar LLDP

Para desactivar el LLDP en todas las interfaces del sistema, realice los pasos que se indican a continuación.

1. **Conviértase en un administrador.**

Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Cambie la propiedad LLDP de SMF a `no`, lo cual desactiva la activación automática de LLDP en todos los puertos, excepto en los que ya tengan configuraciones de LLDP.**

```
# svccfg -s svc:/network/lldp:default setprop lldp/auto-enable-agents = "no"
```

3. **Reinicie el servicio de LLDP.**

```
# svcadm restart svc:/network/lldp:default
```

4. **Desactive el LLDP en cada puerto cuya configuración de LLDP se mantenga.**

   - **Para desactivar el LLDP cambiando el modo del agente:**

     ```
     # lldpadm set-agentprop -p mode=disable agent
     ```

     Donde *agent* representa el agente LLDP y se identifica mediante el enlace físico en el que el agente está activado. Por ejemplo, si activa el LLDP en `net0`, el agente es `net0`.

   - **Para desactivar el LLDP mediante la eliminación de la configuración de LLDP del puerto:**

     ```
     # lldpadm reset-agentprop -p mode agent
     ```

     En este comando, no se establece un valor para la propiedad `mode`.

Atención - Si la propiedad `auto-enable-agents` definida en `no` se cambia a `yes`, el LLDP se comporta de manera diferente que si el modo del agente de ese puerto simplemente se desactivara.

Supervisión de agentes LLDP

El comando `lldpadm show-agent` muestra la información completa anunciada por un agente LLDP. Según el sistema, el anuncio puede contener información sobre el sistema local que se transmite al resto de la red o información que el sistema recibe de otros sistemas de la misma red.

Visualización de la información anunciada

La información puede ser tanto local como remota. La información *local* proviene del agente LLDP local. La información *remota* proviene de otros agentes LLDP de la red y es recibida por el agente LLDP local.

Utilice el comando `lldpadm show-agent` para mostrar la información anunciada.

```
# lldpadm show-agent -[l|r][v] agent
```

- `-l` muestra la información local anunciada por el agente LLDP local.
- `-r` muestra la información remota recibida por el agente LLDP.
- `-v` muestra la información local o remota detallada.

EJEMPLO 5-6 Visualización de información anunciada por el agente LLDP

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.

Para mostrar la información local que anuncia el agente LLDP:

```
# lldpadm show-agent -l net0
AGENT   CHASSISID   PORTID
net0    004bb87f    00:14:4f:01:77:5d
```

Para mostrar la información remota que anuncia el agente LLDP:

```
# lldpadm show-agent -r net0
AGENT   SYSNAME   CHASSISID   PORTID
net0    hostb     0083b390    00:14:4f:01:59:ab
```

Para mostrar la información local en el modo detallado, utilice la opción -v:

```
# lldpadm show-agent -l -v net4
                                Agent: net4
                  Chassis ID Subtype: Local(7)
                          Chassis ID: 00843300
                     Port ID Subtype: MacAddress(3)
                             Port ID: 00:1b:21:89:03:d0
                    Port Description: --
                        Time to Live: 21 (seconds)
                         System Name: --
                    System Description: --
                Supported Capabilities: --
                  Enabled Capabilities: --
                     Management Address: --
                     Maximum Frame Size: --
```

```
                              Port VLAN ID: --
                              VLAN Name/ID: vlan1/22
                         VNIC PortID/VLAN ID: 02:08:20:63:2d:9d,02:08:20:e5:6c:af/21
                      Aggregation Information: --
                                  PFC Willing: On
                                      PFC Cap: 8
                                      PFC MBC: False
                                   PFC Enable: 4
                                  PFC Pending: True
                 Application(s)(ID/Sel/Pri): --
                                  ETS Willing: On
                          ETS Configured CBS: 0
                          ETS Configured TCS: 8
                          ETS Configured PAT: 0,1,2,3,4,5,6,7
                          ETS Configured BAT: 40,20,0,40,0,0,0,0
                          ETS Configured TSA: 2,2,2,2,2,2,2,2
                        ETS Recommended PAT: 0,1,2,3,4,5,6,7
                        ETS Recommended BAT: 40,20,0,40,0,0,0,0
                        ETS Recommended TSA: 2,2,2,2,2,2,2,2
                                  EVB Mode: Station
                            EVB GID (Station): Not Supported
                      EVB ReflectiveRelay REQ: Not Requested
                 EVB ReflectiveRelay Status: RR Not Enabled
                           EVB GID (Bridge): Not Supported
       EVB ReflectiveRelay Capable (RRCAP): Not Supported
       EVB ReflectiveRelay Control (RRCTR): Not Enabled
                       EVB max Retries (R): 0
         EVB Retransmission Exponent (RTE): 0
             EVB Remote or Local(ROL) and
                 Resource Wait Delay (RWD): Local
             EVB Resource Wait Delay (RWD): 0
            EVB Remote or Local (ROL) and
                   Reinit Keep Alive (RKA): Local
               EVB Reinit Keep Alive (RKA): 0
                  Next Packet Transmission: 4 (seconds)
```

Para mostrar la información remota en el modo detallado, utilice la opción -v:

```
# lldpadm show-agent -r -v net4
                                    Agent: net4
                          Chassis ID Subtype: Local(7)
                                  Chassis ID: 00843300
                             Port ID Subtype: MacAddress(3)
                                     Port ID: 00:1b:21:89:03:d0
                            Port Description: --
                                Time to Live: 21 (seconds)
                                 System Name: --
                            System Description: --
                         Supported Capabilities: --
                           Enabled Capabilities: --
                             Management Address: --
                             Maximum Frame Size: --
                                   Port VLAN ID: --
                                   VLAN Name/ID: vlan1/22
```

```
                VNIC PortID/VLAN ID: 02:08:20:63:2d:9d,02:08:20:e5:6c:af/21
             Aggregation Information: --
                         PFC Willing: On
                             PFC Cap: 8
                             PFC MBC: False
                          PFC Enable: 4
      Application(s)(ID/Sel/Pri): --
                         ETS Willing: On
                 ETS Configured CBS: 0
                 ETS Configured TCS: 8
                 ETS Configured PAT: 0,1,2,3,4,5,6,7
                 ETS Configured BAT: 40,20,0,40,0,0,0,0
                 ETS Configured TSA: 2,2,2,2,2,2,2,2
               ETS Recommended PAT: 0,1,2,3,4,5,6,7
               ETS Recommended BAT: 40,20,0,40,0,0,0,0
               ETS Recommended TSA: 2,2,2,2,2,2,2,2
                           EVB Mode: Station
                 EVB GID (Station): Not Supported
          EVB ReflectiveRelay REQ: Not Requested
       EVB ReflectiveRelay Status: RR Not Enabled
                  EVB GID (Bridge): Not Supported
EVB ReflectiveRelay Capable (RRCAP): Not Supported
EVB ReflectiveRelay Control (RRCTR): Not Enabled
              EVB max Retries (R): 0
  EVB Retransmission Exponent (RTE): 0
      EVB Remote or Local(ROL) and
          Resource Wait Delay (RWD): Local
     EVB Resource Wait Delay (RWD): 0
    EVB Remote or Local (ROL) and
           Reinit Keep Alive (RKA): Local
       EVB Reinit Keep Alive (RKA): 0
           Information Valid Until: 19 (seconds)
```

Visualización de estadísticas de 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.

- Para mostrar todas las estadísticas sobre la transmisión y recepción de paquetes LLDP:

  ```
  # lldpadm show-agent -s agent
  ```

- Para mostrar información sobre las estadísticas seleccionadas, utilice la opción `-o`:

  ```
  # lldpadm show-agent -s -o field[,field,...]agent
  ```

  Donde *field* hace referencia a cualquier nombre de campo en la salida del comando `show-agent -s`.

EJEMPLO 5-7 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 IERR IDISCARD OFRAMES OLENERR TLVDISCARD TLVUNRECOG AGEOUT
net0        9    0        0      14       0          4          5      0
```

En esta salida, se proporciona la siguiente información:

- `AGENT` especifica el nombre del agente LLDP, que es idéntico al enlace de datos en el que está activado el agente LLDP.
- `IFRAMES`, `IERR` e `IDISCARD` muestran información sobre los paquetes que se reciben, los paquetes entrantes con errores y los paquetes entrantes que se pierden.
- `OFRAMES` y `OLENERR` hacen referencia 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.

En el ejemplo, se indica que, de los 9 marcos recibidos en el sistema, 5 unidades de TLV no se reconocen, posiblemente porque no cumplen los estándares. El ejemplo también muestra que el sistema local transmitió 14 marcos a la red.

EJEMPLO 5-8 Visualización de estadísticas seleccionadas de paquetes LLDP

En este ejemplo, se muestra cómo visualizar información sobre las estadísticas seleccionadas.

```
# # lldpadm show-agent -s -o iframes,oframes net4
IFRAMES  OFRAMES
0        10
```

♦ ♦ ♦ CAPÍTULO 6

Gestión de redes convergentes mediante el puente de centro de datos

Tradicionalmente, se utilizan redes diferentes para la gestión del tráfico según los requisitos de la aplicación y la distribución de cargas del tráfico de red que se basa en el ancho de banda disponible. Por ejemplo, la red de área local (LAN) utiliza Ethernet y la red de área de almacenamiento (SAN) utiliza canal de fibra. Sin embargo, el puente de centro de datos mejora Ethernet haciendo que sea más adecuada para ejecutar distintos tipos de tráfico, lo cual constituye tráfico convergente, y también para admitir funciones como la capacidad de evitar toda pérdida. El DCB permite una infraestructura de red eficaz mediante la consolidación de SAN y LAN, lo cual reduce los costos operativos y de gestión en los centros de datos.

Este capítulo se divide en los siguientes apartados:

Descripción general del puente de centro de datos

El puente del centro de datos se utiliza para gestionar el ancho de banda, la prioridad relativa y el control de flujo de varios tipos de tráfico al compartir el mismo enlace de red, por ejemplo, cuando se comparte un enlace de datos entre los protocolos de almacenamiento y de redes. El canal de fibra puede dedicarse a alojar este tipo de tráfico. Sin embargo, el uso de enlaces dedicados para atender sólo el tráfico del canal de fibra puede resultar costoso. Por lo tanto, el

canal de fibra mediante Ethernet (FCoE) suele utilizarse más habitualmente. DCB aborda la sensibilidad de los canales de fibra para la pérdida de paquetes al atravesar una red Ethernet.

DCB distingue el tráfico en función de las prioridades, que también se denominan prioridades de clase de servicio (CoS). El host y el siguiente salto utilizan el protocolo de intercambio de DCB (DCBX) para negociar una configuración de red, como la capacidad de evitar toda pérdida de tráfico y el recurso compartido de ancho de banda mínimo, en función de las prioridades. Este proceso permite que los paquetes de distintas aplicaciones en el host y en la red sean manejados según sus prioridades y que la configuración correspondiente se negocie mediante DCBX.

Cada paquete de una red de DCB tiene un encabezado VLAN que contiene un valor de prioridad de 3 bits de DCB, que es una prioridad de DCB. Este valor de prioridad de IEEE 802.1p diferencia cada paquete Ethernet de la red de los demás paquetes. Según los valores de prioridad de los paquetes, puede configurar DCB para que asigne un ancho de banda específico a los paquetes. Por ejemplo, todos los paquetes con una prioridad `1` deben tener el PFC activado y todos los paquetes con una prioridad `2` deben tener el PFC desactivado y un recurso compartido de ancho de banda del 10%.

Puede configurar las funciones de DCB, como el control de flujo basado en prioridades (PFC) y la selección de transmisión mejorada (ETS), en función de las prioridades. Para obtener más información sobre PFC y ETS, consulte “Control de flujo basado en prioridades” [105] y “Selección de transmisión mejorada” [106].

La propiedad de enlace de datos `cos` de DCB permite especificar la propiedad o CoS del enlace de datos. El valor `cos` que se define en un enlace de datos primario no se aplica a las VNIC que se crean mediante este enlace físico. Para obtener información sobre la personalización de PFC basada en la propiedad `cos`, consulte “Personalización del control de flujo basado en prioridades para DCB” [108]. Para obtener información sobre la personalización de ETS basada en la propiedad `cos`, consulte “Personalización de la selección de transmisión mejorada para DCB” [114].

En Oracle Solaris, el LLDP se usa para intercambiar unidades de tiempo-longitud-valor (TLV, Time-Length-Value) de DCBX. Para obtener más información sobre LLDP, consulte el Capítulo 5, Intercambio de información de conectividad de red con el protocolo de descubrimiento de capa de enlace. Siempre que la tarjeta de interfaz de red (NIC) subyacente admita funciones de DCB, como el control de flujo basado en prioridades y la selección de transmisión mejorada, la información de configuración para estas funciones se puede compartir con los hosts peer de la red, de la siguiente manera:

- El PFC evita la pérdida de paquetes mediante la implementación de un mecanismo que pone en pausa el flujo de tráfico para paquetes con prioridad de clase de servicio (CoS) definida. Para obtener más información acerca de CoS, consulte la descripción de la propiedad de enlace `cos` en la página del comando man `dladm`(1M).
- ETS permite compartir ancho de banda entre paquetes en función de la CoS definida. Consulte “Selección de transmisión mejorada” [106].

Consideraciones para el uso de DCB

Tenga en cuenta las siguientes consideraciones para el uso de DCB:

- DCB *sólo* se admite en NIC físicas Intel Niantic.

  Para verificar si la NIC admite DCB, emita el siguiente comando:

  ```
  # dladm show-linkprop -p ntcs agent
  ```

  Un valor de propiedad mayor que cero (`0`) indica que la NIC admite DCB.
- Los puertos de DCB que están configurados en modo DCB no se pueden agregar (modo DLMP o de tronco).
- Dado que DCB sólo admite la versión IEEE de DCBX (no las versiones CEE ni CIN), los puentes externos deben admitir la versión IEEE para interoperar con Oracle Solaris DCB.
- DCB admite TLV de recomendaciones y configuración de ETS
- DCB sólo se admite en la configuración de ocho clases de tráfico.
- DCB no admite la notificación de congestión (CN).

Control de flujo basado en prioridades

El control de flujo basado en prioridades (PFC) amplía el marco PAUSE estándar de IEEE 802.3x para incluir los valores de CoS de IEEE 802.1p. Con PFC, en lugar de detener todo el tráfico en el enlace cuando se envía una trama PAUSE, el tráfico se pone en pausa sólo para los valores de CoS que están activados en la trama PFC. Se envía una trama de PFC para el valor de la propiedad `cos` activado para el cual debe detenerse el tráfico. El host remitente detiene el tráfico para ese valor de la propiedad `cos`, mientras que el tráfico para otros valores de las propiedad `cos` desactivados no se ve afectado. Después de un intervalo de tiempo que se especifica en la trama de PFC, la transmisión se reanuda para los paquetes en pausa.

Pausar según los valores de CoS garantiza que los paquetes no se descarten para ese valor de la propiedad `cos`. No se envían tramas PAUSE para los paquetes sin ningún valor de CoS definido o con valores de CoS que no tienen el PFC activado. Por lo tanto, el tráfico sigue fluyendo, y quizá se pierdan paquetes durante una congestión del tráfico. El manejo de la pérdida de paquetes depende de la pila de protocolo, por ejemplo, TCP.

Existen dos tipos de información de DCB en el host: información de DCB local e información de DCB remota. Para que las funciones del PFC resulten eficaces, los tipos de información de DCB local y remota para el PFC en el host deben ser simétricos. El host local debe poder hacer coincidir la información de DCB que recibe del igual. Si activa DCB en su sistema, DCB sincroniza la información de DCB con el par.

En la mayoría de los casos, la configuración predeterminada para el PFC es suficiente. Esta configuración se establece automáticamente cuando se activa el LLDP. Sin embargo,

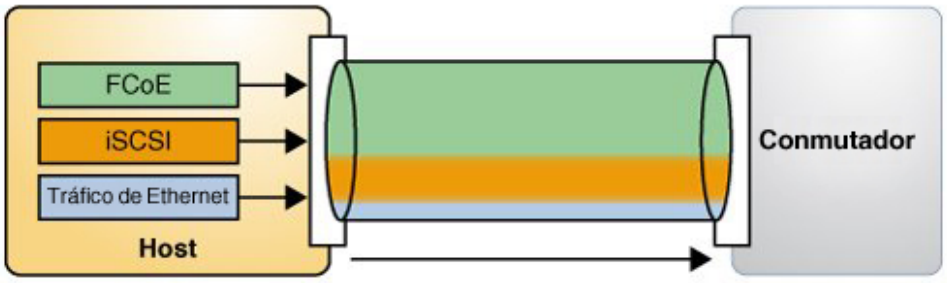
puede ajustar diferentes opciones al configurar el PFC. Para obtener más información, consulte “Personalización del control de flujo basado en prioridades para DCB” [108] y “Visualización de información de configuración del PFC” [110].

Selección de transmisión mejorada

ETS es una función de DCB que le permite asignar ancho de banda en una NIC a las aplicaciones en función de la su prioridad de DCB.

La siguiente figura muestra la función de ETS de DCB en una red.

FIGURA 6-1 Selección de transmisión mejorada en DCB



El host en la figura tiene diferentes tipos de tráfico, como iSCSI y FCoE, que comparten el ancho de banda de enlace. En la figura, la prioridad y el ancho de banda como se muestra en la siguiente tabla se asignan para diferentes tipos de tráfico.

Tráfico	Prioridad	Ancho de banda
FCoE	3	60%
iSCSI	4	30%
Tráfico Ethernet (no iSCSI)	0	10%

El TLV de ETS de DCBX con la asignación de ancho de banda de ETS correspondiente es el siguiente:

Prioridad	0	1	2	3	4	5	6	7

Porcentaje de asignación de ancho de banda	10	0	0	60	30	0	0	0

Para utilizar la función de ETS, la NIC debe admitir la función y ejecutarse en el modo DCB. Al activar LLDP, la configuración predeterminada para la función de ETS se configura automáticamente si el enlace subyacente admite DCB. Sin embargo, puede modificar la configuración predeterminada. Para obtener más información, consulte “Personalización de la selección de transmisión mejorada para DCB” [114], “Recomendación de configuración de ETS para el par” [116] y “Visualización de información de configuración de ETS” [118].

Activación de DCBX

La compatibilidad con DCBX se activa automáticamente al activar LLDP. Este procedimiento ofrece pasos manuales alternativos en caso de que fallen ciertos procesos automáticos.

▼ Cómo activar la función de intercambio del puente de centro de datos manualmente

Antes de empezar Asegúrese de instalar LLDP. Para obtener más información sobre la activación de LLDP, consulte “Activación de LLDP en el sistema ” [89].

1. **Conviértase en un administrador.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Compruebe que se esté ejecutando el servicio de LLDP.**

   ```
   # svcs lldp
   ```

   Si el servicio de LLDP está desactivado, inícielo con el siguiente comando:

   ```
   # svcadm enable svc:/network/lldp:default
   ```

3. **Asegúrese de que el agente LLDP se esté ejecutando en los modos Rx y Tx.**

   ```
   # lldpadm show-agentprop -p mode agent
   ```

   Si el agente LLDP no está activado en ambos modos, escriba el siguiente comando:

   ```
   # lldpadm set-agentprop -p mode=both agent
   ```

   Para conocer otras posibles configuraciones de los agentes LLDP, consulte “Activación de LLDP en el sistema ” [89].

4. **Compruebe que la NIC subyacente admita DCB.**

```
# dladm show-linkprop -p ntcs agent
```

Un valor de propiedad mayor que cero (`0`) indica que la NIC admite DCB.

Personalización del control de flujo basado en prioridades para DCB

PFC y ETS están activados de manera predeterminada sólo si la NIC subyacente está en modo DCB. Si prefiere utilizar sólo PFC, debe eliminar `etscfg` de la propiedad `dot1 -tlv` del agente LLDP mediante el siguiente comando:

```
# lldpadm set-agentprop -p dot1-tlv-=etscfg net0
```

Para obtener una lista de los posibles valores para `dot1 -tlv`, consulte la Tabla 5-1, “Unidades de TLV opcionales para un agente LLDP”.

Configuración de las propiedades de enlace de datos relacionadas con el PFC

La función de PFC de DCB proporciona las siguientes propiedades de enlace de datos:

- `pfcmap`: proporciona información sobre las definiciones y las asignaciones de prioridades. La propiedad `pfcmap` hace referencia a una máscara de 8 bits (`0`–`7`) que representa las prioridades. El bit más bajo representa la prioridad `0`y el bit más alto representa la prioridad `7`. Cada bit en esta máscara indica si el PFC está activado para una prioridad dada. De manera predeterminada, `pfcmap` se establece en `1111111`, lo que significa que el PFC está activado para todas las prioridades.
- `pfcmap-rmt`: especifica la asignación de PFC operativa en el par remoto. Esta propiedad es de sólo lectura.

En una red DCB, cuando un receptor no puede mantenerse a la par de la velocidad de entrada del tráfico, envía una trama de PFC al remitente para solicitarle que ponga en pausa el tráfico para las prioridades que tengan activado el PFC. Para cualquier paquete que se transmita mediante un enlace, DCB envía una trama de PFC al host emisor si la congestión del tráfico se acumula en el host de recepción. Para enviar tramas de PFC correctamente, los hosts que se comunican deben tener información de configuración de DCB simétrica. Un sistema puede ajustar automáticamente sus configuraciones de PFC para que coincidan con las configuraciones del igual remoto. Puede determinar la asignación de PFC operativa en el host

local mediante el comando `dladm show-linkprop` que muestra el valor `EFFECTIVE` para la propiedad `pfcmap`. Para obtener más información, consulte “Visualización de propiedades de enlaces de datos” [110].

▼ Cómo personalizar el control de flujo basado en prioridades para DCB

1. **Conviértase en un administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Asegúrese de que la propiedad `flowctrl` del enlace de datos esté establecida en `pfc`.**

   ```
   # dladm show-linkprop -p flowctrl datalink
   ```

   Si la propiedad no está establecida en `pfc` o `auto`, utilice el siguiente comando:

   ```
   # dladm set-linkprop -p flowctrl=pfc datalink
   ```

3. **Establezca la propiedad `pfcmap` en un valor distinto del valor predeterminado `11111111`.**

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

   Por ejemplo, para activar prioridad sólo en la prioridad de CoS 6, escriba el siguiente comando:

   ```
   # dladm set-linkprop -p pfcmap=01000000 net0
   ```

Configuración de las unidades de TLV del PFC

DCB utiliza unidades de TLV del PFC para intercambiar información del PFC entre hosts. Ambos hosts deben tener el mismo valor para la propiedad `pfcmap` o, al menos, un host debe estar dispuesto a aceptar la configuración de su igual. Puede establecer la propiedad `pfcmap` mediante el comando `dladm set-linkprop`.

La propiedad de TLV `willing` indica si el host está listo para aceptar la configuración del igual en caso de que la configuración de host sea diferente de la configuración del igual. De forma predeterminada, el valor de la propiedad `willing` se establece en `on`, lo cual indica que el host aceptará la configuración del igual.

Para verificar que el host puede sincronizar la información del PFC con la información del PFC del igual remoto, debe determinar si `willing` se establece en `on` mediante el siguiente comando:

```
# lldpadm show-agenttlvprop -p willing -a agent pfc
```

Si la propiedad de TLV del PFC `willing` está establecida en `off`, escriba el siguiente comando para establecer la propiedad `willing` en `on` y activar la sincronización.

```
# lldpadm set-agenttlvprop -p willing=on -a agent pfc
```

donde *agent* es el enlace de datos en el que está activado el agente.

EJEMPLO 6-1 Activación de la sincronización entre el host y el par

Para activar la sincronización para un enlace de datos `net0`, escriba el siguiente comando:

```
# lldpadm set-agenttlvprop -p willing=on -a net0 pfc

# dladm show-linkprop -p pfcmap,pfcmap-rmt net0
LINK   PROPERTY    PERM  VALUE      EFFECTIVE  DEFAULT    POSSIBLE
net0   pfcmap      rw    11111111   00010000   11111111   00000000-11111111
net0   pfcmap-rmt  r-    --         00010000   11111111   --
```

En el ejemplo, las propiedades `pfcmap` y `pfcmap-rmt` tienen el valor `00010000`. Esto indica que el host local se ha sincronizado con el par. Por lo tanto, el PFC está activado con prioridad 4tanto en el host como en el par.

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

Visualización de información de configuración del PFC

En esta sección, se describen los comandos para mostrar información relacionada con el PFC después de que se configuran LLDP y DCB y proporciona ejemplos para mostrar el uso de estos comandos.

Visualización de propiedades de enlaces de datos

El siguiente comando muestra las definiciones de prioridad y las asignaciones eficaces del PFC en el enlace de datos:

```
# dladm show-linkprop -p pfcmap,pfcmap-rmt datalink
```

En un enlace de datos que tenga información del PFC coincidente entre el par local y el par remoto, los valores de la columna `EFFECTIVE` para las propiedades `pfcmap` y `pfcmap-rmt` son idénticos, independientemente del valor definido para `pfcmap`. Si la capacidad de sincronización

está desactivada en el host local, el campo `EFFECTIVE` para la propiedad `pfcmap` refleja el valor de la propiedad `pfcmap` para el host local.

EJEMPLO 6-2 Cómo ver las propiedades de enlace de datos relacionadas con el PFC

En este ejemplo, se muestra cómo visualizar el estado de las propiedades de enlace de datos físico relacionadas con el control de flujo basado en prioridades.

```
# dladm show-linkprop -p pfcmap,pfcmap-rmt net0
LINK   PROPERTY      PERM   VALUE      EFFECTIVE  DEFAULT    POSSIBLE
net0   pfcmap        rw     11111111   11111111   11111111   00000000-11111111
net0   pfcmap-rmt    r-     --         --         --         --
```

En el ejemplo, el campo `value` para la propiedad `pfcmap` tiene el valor `11111111`. Este valor indica que la asignación del PFC en el host local tiene el valor predeterminado en el que las ocho prioridades están activadas. Los valores `EFFECTIVE` para las propiedades `pfcmap` y `pfcmap-rmt` son `11111111` y `--`. Los valores con discrepancias para el campo `EFFECTIVE` indican que el host local no ha sincronizado su información del PFC con el par remoto.

Puede utilizar el comando `lldpadm show-agenttlvprop` para verificar el valor de la propiedad `willing` y el comando `lldpadm show-agent -r` para comprobar la información de TLV del PFC del igual.

Cómo ver la capacidad del host local para sincronizar información del PFC

El siguiente comando muestra la propiedad de TLV del PFC que controla la capacidad de un host de sincronizar su asignación del PFC con un igual.

```
# lldpadm show-agenttlvprop -a agent pfc
```

Donde *agent* se identifica mediante el enlace de datos en que LLDP está activo.

EJEMPLO 6-3 Cómo ver la capacidad del host local para sincronizar información del PFC

En este ejemplo, se muestra cómo visualizar el estado actual de la capacidad del host para adaptarse a las configuraciones del PFC del igual.

```
# lldpadm show-agenttlvprop -a net0 pfc
AGENT   TLVNAME   PROPERTY   PERM   VALUE   DEFAULT   POSSIBLE
net0    pfc       willing    rw     off     on        on,off
```

Para obtener más información, consulte “Configuración de las unidades de TLV del PFC” [109].

Visualización de información de asignación del PFC entre el host y el par

El valor `PFC Pending` devuelve el estado `True` si la información del PFC entre el host y el par no coincide. Una vez que se resuelve la discrepancia, el estado de `PFC Pending` vuelve a `False`.

El siguiente comando le alerta cuando hay discrepancias entre la información de asignación del PFC del host local y del igual.

```
# lldpadm show-agent -lv -o "PFC Pending" agent
```

```
# lldpadm show-agent -lv -o "PFC Pending" agent
```

EJEMPLO 6-4 Cómo verificar la simetría de la información del PFC entre el host y el peer

En el siguiente ejemplo, se muestra cómo verificar en tiempo real de ejecución si la información del PFC está sincronizada entre el host y el par, o si se produce una discrepancia.

```
# lldpadm show-agent -lv -o "PFC Pending" net0
PFC Pending: True
```

Para ver toda la información que un agente anuncia, utilice la opción `-v` (verbose) del comando `lldpadm show-agent`:

```
# lldpadm show-agent -v net0
```

Visualización de definiciones de prioridades

El siguiente comando muestra información del PFC sobre la línea física en lo que respecta a prioridades activadas en la NIC:

```
# dladm show-phys -D pfc datalink
```

EJEMPLO 6-5 Cómo mostrar definiciones de prioridades de CoS

En este ejemplo, se muestra cómo ver las definiciones de prioridades actuales en un enlace de datos físico específico basado en el valor de la propiedad `pfcmap`. Por ejemplo, supongamos que `pfcmap` se configura como `01000000` . Para mostrar las asignaciones de prioridad correspondientes en el enlace físico, siga estos pasos:

```
# dladm show-phys -D pfc net0
```

```
LINK  COS    PFC   PFC_EFFECT   CLIENTS
net0   0     YES   NO           net0,vnic1
       1     YES   YES          vnic2
       2     YES   NO           vnic3
       3     YES   NO           vnic4
       4     YES   NO           vnic5
       5     YES   NO           vnic6
       6     YES   NO           vnic7
       7     YES   NO           vnic8
```

Para el enlace físico `net0`, la prioridad está activada para todos los clientes de VNIC configurados por medio del enlace de datos. Sin embargo, el host local ajusta su asignación del PFC a la asignación del PFC en el par, como se muestra en los valores del campo `PFC_EFFECT`, donde la prioridad está desactivada en `COS 0` y `2-7`. Como resultado, no se intercambian tramas PFC para el tráfico en ninguna VNIC, excepto `vnic2`, independientemente de la disponibilidad de los recursos. Con esta configuración, se permite el descarte de paquetes en el tráfico que fluye en todas las VNIC, excepto `vnic2`. Para el tráfico de `vnic2`, los marcos PAUSE del PFC se envían cuando la congestión del tráfico se produce para evitar la pérdida de paquetes en el cliente.

Configuraciones de prioridades de la aplicación

DCBX intercambia la información de prioridad asociada a la aplicación. Las unidades de TLV de aplicación que se intercambian a través de DCBX contienen información sobre la prioridad que se utilizará para una aplicación en el host. La prioridad se define en la tabla de prioridades de aplicaciones. Cada entrada de la tabla contiene el nombre de la aplicación y la prioridad asignada a la aplicación. Al definir una prioridad para una aplicación, toda la configuración de DCB del PFC y ETS de esa prioridad se aplican a la aplicación. El TLV de aplicación utiliza los datos de la tabla para intercambiar la información de prioridad de la aplicación con otros hosts.

De forma predeterminada, la función de la aplicación acepta las asignaciones de prioridades del igual. La propiedad `willing` del TLV de la aplicación `appln` es similar al PFC y permite el intercambio de información entre los pares.

Las entradas de la tabla tienen el formato siguiente:

protocol-ID/*selector*/*priority*

El par *protocol-ID*/*selector* identifica la aplicación. La prioridad para una aplicación correspondiente se identifica mediante una prioridad que contiene un valor de `0` a `7`.

Para intercambiar esta información sobre la prioridad de una aplicación con otros hosts, se establece un TLV de aplicación, como se muestra a continuación:

```
# lldpadm set-agenttlvprop -p property=value -a agent appln
```

Por ejemplo, para el tráfico del FCoE, el ID de protocolo es `0x8906` y el ID de selector es `1`. Suponga que se asigna la prioridad `4` a esta aplicación. En función de la Tabla 5-3, “Las unidades de TLV por agente y sus propiedades”, que muestra los parámetros para la definición de un TLV de aplicación, se debe escribir el siguiente comando:

```
# lldpadm set-agenttlvprop -p apt=8906/1/4 -a net0 appln
# lldpadm show-agenttlvprop -a net0 appln
AGENT   TLVNAME   PROPERTY   PERM   VALUE      DEFAULT   POSSIBLE
net0    appln     apt        rw     8906/1/4   --        --
```

Personalización de la selección de transmisión mejorada para DCB

La configuración predeterminada se establece automáticamente cuando se activa el LLDP y el enlace subyacente admite el DCB. En esta configuración predeterminada, al valor `cos 0` se le asigna todo el ancho de banda. Sin embargo, puede utilizar el comando `dladm set-linkprop` para configurar los valores `cos` en un enlace de datos a fin de asignarle parte del ancho de banda.

Los TLV de recomendaciones y configuración de ETS están activados de manera predeterminada para una NIC. Para obtener una lista de los posibles valores para `dot1–tlv`, consulte la Tabla 5-1, “Unidades de TLV opcionales para un agente LLDP”.

Si desea eliminar el TLV `pfc`, escriba el siguiente comando:

```
# lldpadm set-agenttlvprop -p dot1-tlv-=pfc agent
```

Configuración de las propiedades de enlace de datos relacionadas con ETS

Las propiedades de los enlaces de datos que hacen referencia a la información de PFC se aplican a la prevención de pérdidas de paquetes en función en las prioridades definidas para los paquetes. Las propiedades de ETS se relacionan con la asignación de los recursos compartidos del ancho de banda del enlace subyacente en función de las prioridades.

DCB proporciona las siguientes propiedades relacionadas con ETS:

- `cos`: especifica la clase de servicio o prioridad del enlace de datos. El valor de esta propiedad oscila entre `0` y `7`. El valor predeterminado es `0`. El valor `cos` se establece en la etiqueta de VLAN de los paquetes que se transmiten a través de este enlace.

- `etsbw-lcl`: indica el ancho de banda de ETS asignado en el lado de transmisión (Tx) para el enlace de datos. Esta propiedad se puede configurar sólo si la NIC física subyacente tiene capacidades de DCB y admite ETS, y la propiedad `cos` del enlace no se establece en `0`. Puede definir un valor para esta propiedad en un enlace de datos especificando el porcentaje de ancho de banda total del enlace físico subyacente. La suma de los valores para la propiedad `etsbw-lcl` para todos los enlaces de datos de la misma NIC física no debe exceder el 100%.

  El porcentaje de ancho de banda que se define en `etsbw-lcl` no se reserva sólo para ese enlace de datos. Si el ancho de banda asignado no se utiliza, puede ser utilizado por otros enlaces de datos de esa NIC física. Además, la asignación de ancho de banda se aplica sólo en el lado de la transmisión del tráfico del host.
- `etsbw-rmt-advice`: especifica el valor de ancho de banda de ETS recomendado que se envía al par. De forma predeterminada, se recomienda al par el valor de la propiedad `etsbw-lcl` configurado de forma local. Sin embargo, puede recomendar un valor diferente de la propiedad `etsbw-lcl` configurando la propiedad del enlace de datos `etsbw-rmt-advice` de forma explícita.

  La configuración de la propiedad `etsbw-rmt-advice` es útil si la asignación de ancho de banda para un enlace de datos es asimétrica, lo cual significa que el ancho de banda de recepción (Rx) y el de transmisión (Tx) son diferentes. Cuando la propiedad `etsbw-rmt-advice` se define explícitamente, la transmisión del TLV de DCBX de recomendación de ETS se inicia automáticamente.
- `etsbw-lcl-advice`: especifica el recurso compartido de ancho de banda recomendado para el enlace de datos, que el par envía al host local. Esta es una propiedad de sólo lectura.
- `etsbw-rmt`: especifica el recurso compartido de ancho de banda que está configurado en el par para el enlace de datos. Esta es una propiedad de sólo lectura.

Para configurar la prioridad y asignar un ancho de banda a la VNIC, utilice los siguientes comandos:

- Para definir la prioridad en la VNIC:

  ```
  # dladm set-linkprop -p cos=value VNIC
  ```
- Para asignar un porcentaje del ancho de banda del enlace físico subyacente a una VNIC:

  ```
  # dladm set-linkprop -p etsbw-lcl=value VNIC
  ```

  El valor que se asigna a la propiedad `etsbw-lcl` representa un porcentaje de la capacidad de ancho de banda total del enlace subyacente. La suma de todos los valores de ancho de banda que se asignan a los clientes no debe sobrepasar el 100%.
- Para recomendar de manera explícita el ancho de banda que se envía al par:

  ```
  # dladm set-linkprop -p etsbw-rmt-advice=value VNIC
  ```

Puede determinar el recurso compartido de ancho de banda real que se implementa en el enlace de datos del host local y el recurso compartido de ancho de banda que se configura en el enlace

de datos del igual mediante el comando `dladm show-linkprop`. El valor del campo `EFFECTIVE` de la salida para las propiedades `etsbw-lcl` y `etsbw-rmt` muestra el recurso compartido de ancho de banda real implementado. Para obtener más información, consulte “Visualización de información de configuración de ETS” [118].

Para que se utilice el ancho de banda adecuado para los paquetes con prioridades específicas, se recomienda la información de ETS simétrica o sincronizada entre los hosts que se comunican. Específicamente, debe ser el sistema local que puede ajustar su recurso compartido de ancho de banda al valor de `etsbw-lcl-advice`. Un sistema Oracle Solaris puede ajustar automáticamente sus configuraciones de ETS a fin de que coincidan con la recomendación de ETS del igual.

Configuración de unidades de TLV de ETS

La configuración de TLV de ETS (`etscfg`) determina la forma en que el host responde a las recomendaciones de ETS del igual. Esta unidad de TLV sólo tiene una propiedad configurable, `willing`. De manera predeterminada, esta propiedad se establece en `on` y permite que el host local sincronice su configuración de ETS con la recomendación de ETS del igual remoto.

Para verificar que el host pueda sincronizar su información de ETS con la información de ETS del igual remoto, utilice el siguiente comando:

```
# lldpadm show-agenttlvprop -p willing -a agent etscfg
```

Si la propiedad `willing` está establecida en `off`, escriba el siguiente comando para establecer la sincronización:

```
# lldpadm set-agenttlvprop -p willing=on -a agent etscfg
```

Para evitar la sincronización de información para un agente determinado, establezca la propiedad `willing` en `off`, como se muestra a continuación:

```
# lldpadm set-agenttlvprop -p willing=off -a agent etscfg
```

donde *agent* es el enlace de datos en el que está activado el agente.

Recomendación de configuración de ETS para el par

Los valores de ancho de banda de ETS (`etsbw-lcl`) configurados para cada prioridad se pueden recomendar al par a fin de que este pueda configurar los mismos valores. Debe activar la propiedad `etsreco` en el tipo `dot1-tlv` del agente LLDP en la NIC para recomendar los valores de ancho de banda de ETS. Los valores recomendados pueden ser los mismos que los valores

de ETS configurados de forma local, o también se pueden configurar explícitamente los valores recomendados mediante la definición de la propiedad del nuevo enlace de datos `etsbw-rmt-advice` con el comando `dladm set-linkprop`. La configuración de la propiedad `etsbw-rmt-advice` es útil si el ancho de banda asignado para un enlace de datos es asimétrico, lo cual significa que el ancho de banda de recepción (Rx) y el de transmisión (Tx) son diferentes.

De forma predeterminada, los valores configurados de la propiedad `etsbw-lcl` se utilizan para recomendar valores al par. Sin embargo, puede recomendar un valor de ETS diferente mediante la definición de un valor distinto para la propiedad `etsbw-rmt-advice`. Por ejemplo, si el tráfico de red es superior para Tx, puede configurar un valor de ETS mayor para la propiedad `etsbw-lcl` (Tx en el host) y un valor menor para la propiedad `etsbw-rmt-advice` (Rx al host).

EJEMPLO 6-6 Recomendación de configuración de ETS para el par

1. Asegúrese de que la propiedad `etsreco` esté activada mediante la visualización de la propiedad del tipo `dot1-tlv` del agente LLDP para `net5`.

```
# lldpadm show-agentprop -p dot1-tlv net5
AGENT        PROPERTY   PERM VALUE          DEFAULT        POSSIBLE
net5         dot1-tlv   rw   etsreco,etscfg none           none,vlanname,pvid,
                                                           linkaggr,pfc,appln,
                                                           evb,etscfg,etsreco,
                                                           all
```

2. Asigne un recurso compartido del 20% del ancho de banda del enlace subyacente para `vnic1`.

```
# dladm set-linkprop -p etsbw-lcl=20 vnic1
# dladm show-linkprop -p etsbw-lcl vnic1
LINK     PROPERTY        PERM VALUE        EFFECTIVE    DEFAULT   POSSIBLE
vnic1    etsbw-lcl       rw   20           20           0         --
```

   De forma predeterminada, se recomienda el mismo valor para el par.

```
# dladm show-linkprop -p etsbw-rmt-advice vnic1
LINK     PROPERTY         PERM VALUE  EFFECTIVE    DEFAULT   POSSIBLE
vnic1    etsbw-rmt-advice rw   --      20           0         --
```

3. Visualice la información intercambiada mediante LLDP.

```
# lldpadm show-agent -l -v net5
```

4. Visualice el ancho de banda recomendado para el par.

```
# dladm show-phys -D ets -r net5
LINK      COS ETSBW_RMT_EFFECT ETSBW_RMT_ADVICE CLIENTS
--         0   0                80               net5
```

```
1   0               0               --
2   0               0               --
3   0               20              vnic1
4   0               0               --
5   0               0               --
6   0               0               --
7   0               0               --
```

De forma predeterminada, los valores configurados para la propiedad `etsbw-lcl` de cada prioridad en `net5` se envían como los valores recomendados al par. `ETSBW_RMT_ADVICE` muestra los valores recomendados al par. La salida también muestra que el par no ha configurado ningún ancho de banda de ETS. También puede mostrar el ancho de banda recomendado al par mediante el comando `lldpadm show-agent`.

5. Recomiende un valor diferente para el par.

```
# dladm set-linkprop -p etsbw-rmt-advice=10 vnic1
# dladm show-linkprop -p etsbw-rmt-advice vnic1
LINK     PROPERTY          PERM VALUE     EFFECTIVE    DEFAULT   POSSIBLE
vnic1    etsbw-rmt-advice  rw   10         10           0         --
```

6. Visualice el ancho de banda recomendado para el par.

```
# dladm show-phys -D ets -r net5
LINK                COS ETSBW_RMT_EFFECT ETSBW_RMT_ADVICE CLIENTS
--                  0   0                90               net5
                    1   0                0                --
                    2   0                0                --
                    3   0                10               vnic2
                    4   0                0                --
                    5   0                0                --
                    6   0                0                --
                    7   0                0                --
```

El campo `ETSBW_RMT_EFFECT` muestra el valor `0` para `vnic2`, el cual indica que el par no ha definido ningún ancho de banda, aunque ya se han recomendado valores de ancho de banda. Esta situación significa que es posible que el par no tenga activado LLDP o no admita ETS.

Visualización de información de configuración de ETS

Puede utilizar los siguientes comandos para mostrar información sobre la configuración de ETS:

- `# dladm show-linkprop -p etsbw-lcl,etsbw-rmt,etsbw-lcl-advice,etsbw-rmt-advice` *datalink*

  Este comando muestra la información relacionada con ETS en un enlace físico.

- `# dladm show-phys -D ets` *phys-link*

Este comando muestra la configuración de ETS local y remota del enlace físico en relación con la asignación de ancho de banda y la distribución mediante el enlace.

- `# lldpadm show-agenttlvprop -a` *agent* `etscfg`

  Donde *agent* es el enlace de datos en que LLDP está activado. Este comando muestra la propiedad del TLV de ETS que controla la capacidad de un host para sincronizar la información de ETS con un igual.

EJEMPLO 6-7 Cómo ver las propiedades de enlace de datos relacionadas con la ETS

En este ejemplo, se muestra cómo visualizar el estado de las propiedades de enlace de datos relacionadas con la ETS antes de que se active la sincronización.

```
# dladm show-linkprop -p cos,etsbw-lcl,etsbw-rmt,etsbw-lcl-advice, \
etsbw-rmt-advice vnic1
LINK    PROPERTY           PERM  VALUE  EFFECTIVE  DEFAULT    POSSIBLE
vnic1   cos                rw    2      2          0          0-7
vnic1   etsbw-lcl          rw    10     10         0          --
vnic1   etsbw-rmt          r-    20     20         --         --
vnic1   etsbw-lcl-advice   r-    20     20         --         --
vnic1   etsbw-rmt-advice   rw    10     10         0          --
```

La salida muestra que el host ha definido y recomendado un valor de ETS del 10% para `vnic1` con un valor `cos` de `2`. Sin embargo, el par ha definido y recomendado un valor de ETS del 20% con un valor `cos` de `2` para `vnic1`. Dado que la sincronización no está activada (`willing` no está activado), el host no ha aceptado la recomendación del igual, lo cual se refleja en el valor `EFFECTIVE` de la propiedad `etsbw-lcl` (valor configurado de forma local).

EJEMPLO 6-8 Cómo ver la capacidad del host local para sincronizar información de ETS

En este ejemplo, se muestra cómo visualizar el estado actual de la capacidad del host local para adaptarse a las configuraciones de ETS del igual.

```
# lldpadm show-agenttlvprop -a net0 etscfg
AGENT   TLVNAME   PROPERTY   PERM   VALUE   DEFAULT   POSSIBLE
net0    etscfg    willing    rw     off     on        on,off
```

Para activar la sincronización, escriba los siguientes comandos:

```
# lldpadm set-agenttlvprop -p willing=on -a net0 etscfg

# dladm show-linkprop -p  cos,etsbw-lcl,etsbw-rmt, \
etsbw-lcl-advice,etsbw-rmt-advice vnic1
LINK    PROPERTY           PERM  VALUE   EFFECTIVE  DEFAULT    POSSIBLE
vnic1   cos                rw    2       2          0          0-7
vnic1   etsbw-lcl          rw    10      20         0          --
vnic1   etsbw-rmt          r-    20      20         --         --
```

```
vnic1   etsbw-lcl-advice   r-    20      20         --         --
vnic1   etsbw-rmt-advice   rw    10      10         0          --
```

Dado que la sincronización está activada (la propiedad `willing` está activada), el host ha aceptado la recomendación del igual, lo cual se refleja en el valor `EFFECTIVE` de `etsbw-lcl`.

El ejemplo siguiente muestra los valores de ETS en el host y el par para cada valor de prioridad del enlace físico.

```
# dladm show-phys -D ets net4
LINK     COS ETSBW_LCL_EFFECT ETSBW_RMT_EFFECT ETSBW_LCL_SOURCE CLIENTS
net4      0   0               30               local            net4
          1   0               0                local            --
          2   0               0                local            --
          3   0               0                local            --
          4   0               70               local            --
          5   0               0                local            --
          6   0               0                local            --
          7   0               0                local            --
```

`ETSBW_LCL_EFFECT` Muestra el ancho de banda de ETS como un porcentaje para la prioridad.

`ETSBW_RMT_EFFECT` Muestra el ancho de banda de ETS como un porcentaje para el valor de prioridad en el par.

`ETSBW_LCL_SOURCE` Indica el origen para el valor `ETSBW_LCL_EFFECT`. Este valor puede ser `local`, que es el valor configurado, o `remote`, que es el valor recomendado.

El ejemplo siguiente muestra la información de ETS local, incluidos los valores configurados localmente, los valores locales activos y los valores recomendados por el par.

```
# dladm show-phys -D ets -l net5
LINK                COS ETSBW_LCL ETSBW_LCL_EFFECT ETSBW_LCL_ADVICE CLIENTS
--                  0   80        80               0                net5
                    1   0         0                0                --
                    2   0         0                0                --
                    3   20        20               0                vnic2
                    4   0         0                0                --
                    5   0         0                0                --
                    6   0         0                0                --
                    7   0         0                0                --
```

Debido a que el par no ha recomendado ningún valor, el valor local activo (`ETSBW_LCL_EFFECT`) se establece usando el valor configurado local (`ETSBW_LCL`).

El siguiente ejemplo muestra información sobre el par.

```
# dladm show-phys -D ets -r net5
LINK                COS ETSBW_RMT_EFFECT ETSBW_RMT_ADVICE CLIENTS
--                  0   0                20               net5
```

```
1   0               0               --
2   0               0               --
3   0               80              vnic2
4   0               0               --
5   0               0               --
6   0               0               --
7   0               0               --
```

El resultado muestra que el par remoto no tiene ningún valor definido en el campo `ETSBW_RMT_EFFECT` aunque el host había recomendado al par definir el 80% para la prioridad `3`.

♦ ♦ ♦ APÉNDICE A

Agregaciones de enlaces e IPMP: comparación de funciones

La agregación de enlaces e IPMP son tecnologías diferentes que permiten lograr un mejor rendimiento de la red y mantener la disponibilidad de la red.

En la siguiente tabla se presenta una comparación general entre agregación de enlaces e IPMP.

Característica	Agregación de enlaces	IPMP
Tipo de tecnología de red	Capa 2 (capa de enlace).	Capa 3 (capa IP).
Herramienta de configuración	`dladm`.	`ipadm`.
Detección de fallos basada en enlaces	Admitida.	Admitida.
Detección de fallos basada en sondeos	Troncos: Basada en LACP, tiene como objetivo el conmutador o el host peer inmediato. DLMP: Admitida. Basada en ICMP, tiene como objetivo cualquier sistema definido en la misma subred como direcciones DLMP, entre varios niveles de conmutadores de capa 2 participantes.	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.
Uso de interfaces de reserva	Troncos: No admitida. DLMP: no admitido.	Admitida. Se pueden configurar interfaces en espera.
Conmutadores múltiples	Troncos: Admitida. Sin embargo, se necesitan extensiones del proveedor del conmutador. DLMP: Admitida.	Admitida.
Configuración del conmutador	Troncos: Requerida. DLMP: No requerida.	No requerida.
Configuración de extremo a extremo	Admitida.	No admitida.
Tipos de medios compatibles	Específica de Ethernet.	Permite la difusión.

Característica	Agregación de enlaces	IPMP
Compatibilidad de expansión de carga	Troncos: Admitida y controlada por el administrador mediante el comando `dladm`. Se admite la expansión de carga entrante. DLMP: Admitida entre clientes y VNIC de la agregación. Sin embargo, no se admite la expansión de carga realizada por VNIC y clientes individuales mediante la agregación.	Admitida. Controlada por el núcleo. La selección de dirección de origen afecta indirectamente la expansión de carga entrante.
Nivel de compatibilidad en la integración con las VNIC	Excelente compatibilidad. La agregación se configura en el dominio de control o en la zona global solamente y es transparente para las zonas.	Admitida. Sin embargo, las propiedades de VNIC, como el límite de ancho de banda, los anillos Tx o Rx dedicados o la protección de enlaces, no se pueden aplicar a un grupo IPMP. Requiere asignar varias VNIC a las zonas y se debe configurar en cada zona.
Flujos definidos por el usuario para la gestión de recursos	Admitida.	No admitida.
Protección de enlaces	Admitida.	No admitida.
Requisitos del protocolo	Ninguno.	Ninguno.

En las agregaciones de enlaces, el tráfico entrante se extiende sobre los múltiples enlaces que componen la agregación en el modo de tronco. Por lo tanto, el rendimiento de la red mejora a medida que se instalan más NIC para agregar enlaces a la agregación.

Las agregaciones DLMP abarcan varios conmutadores. Como son una tecnología de capa 2, las agregaciones se integran bien con otras tecnologías de virtualización de Oracle Solaris.

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.

♦ ♦ ♦ APÉNDICE B

Formato de paquete de los sondeos transitivos

El paquete de los sondeos transitivos es un paquete de protocolo de propiedad con un tipo de Ethernet, `ETHERTYPE_ORCL` (`0x881b`). Para obtener más información sobre los sondeos transitivos, consulte "Detección de fallos basada en sondeos" [24]. Para obtener un ejemplo de cómo mostrar las estadísticas de los sondeos, consulte el Ejemplo 2-7, "Visualización de información relacionada con los sondeos". La figura siguiente muestra el formato de paquete de los sondeos transitivos.

FIGURA B-1 Paquetes de sondeo transitivo

Campo	Descripción
`Dest MAC`	Dirección MAC de destino.
`Src MAC`	Dirección MAC de origen.
`Proto#`	Número de protocolo. La carga útil de capa 2 de los paquetes `ETHERTYPE_ORCL` debe comenzar con un número de protocolo de 16 bits, que es `1` para el paquete de sondeo transitivo.
`Typ`	Tipo de paquete de sondeo. El tipo de paquete de sondeo es `0` para la solicitud y `1` para la respuesta.

Campo	Descripción
`Pad`	Relleno (todos ceros).
`Seq#`	Número de secuencia de sondeo.
`Timestamp`	Registro de hora del sondeo.
`TL`	Longitud de la información de destino. Para Ethernet, la longitud de destino es de 6 bits (longitud de la dirección MAC de Ethernet)
`Target`	Dirección MAC del puerto de destino.
`SL`	Longitud de la información de origen. Para Ethernet, la longitud de origen es de 6 bits.
`Source`	Dirección MAC del puerto de origen.

Índice

E

G

I

L

M

N

P

R

S

T

U

V