Configuración del sistema Oracle® Solaris 11.2 como enrutador o equilibrador de carga

Referencia: E53805-02
Septiembre de 2014

ORACLE

Contenido

Uso de esta documentación

- **Descripción general**: describe cómo configurar Oracle Solaris 11.2 como enrutador IPv4 o IPv6. Proporciona una descripción general e instrucciones de configuración para el protocolo de redundancia de enrutador virtual (VRRP, Virtual Router Redundancy Protocol) y el equilibrador de carga integrado (ILB, Integrated Load Balancer).
- **Destinatarios**: administradores de sistemas.
- **Conocimientos requeridos**: básicos y algunos conocimientos avanzados sobre 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.

Feedback

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

♦ ♦ ♦ CAPÍTULO 1

Introducción a los enrutadores y equilibradores de carga

En este capítulo se describe el modo en que los enrutadores y equilibradores de carga se utilizan en Oracle Solaris para conectar redes de equipos y para distribuir cargas de trabajo. Los enrutadores administran la actividad de enrutamiento mediante protocolos, como el protocolo de información de enrutamiento (RIP), la próxima generación RIP (RIPng), el descubrimiento de enrutador de protocolo de mensajes de control de Internet (RDISC), abrir la ruta de acceso más corta primero (OSPF), el protocolo de puerta de enlace de borde (BGP), el sistema intermedio a sistema intermedio (IS-IS) y el protocolo de redundancia de enrutador virtual (VRRP).

Equilibradores de carga distribuyen el tráfico de red en una cantidad de servidores. La distribución de la carga de trabajo de una red ayuda a lograr un uso compartido de recursos óptimo a fin de aumentar el rendimiento y la disponibilidad.

Este capítulo se divide en los siguientes apartados:

Descripción general del enrutador

Un enrutador es un dispositivo que se utiliza en una red de equipos para conectar los equipos y transferir paquetes de datos entre los equipos de la red. Un enrutador puede tener dos o más conexiones de redes diferentes. El enrutador lee la información de dirección desde los paquetes de datos entrantes para determinar su destino. A continuación, los paquetes se reenvían a la siguiente red al utilizar la información en la tabla de enrutamiento del enrutador. Este proceso de direccionamiento de tráfico de los enrutadores se repite hasta que los paquetes de datos alcancen el nodo de destino.

Protocolos de enrutamiento

Los protocolos de enrutamiento administran la actividad de enrutamiento en un sistema. Los enrutadores intercambiar información de enrutamiento con otros hosts para mantener las rutas conocidas a las redes remotas. Tanto los enrutadores como los hosts pueden ejecutar protocolos de enrutamiento. Los protocolos de enrutamiento del host se comunican con los daemons de enrutamiento de otros enrutadores y hosts. Estos protocolos ayudan al host a determinar a donde reenviar los paquetes. Cuando las interfaces de red están activas, el sistema automáticamente se comunica con los daemons de enrutamiento. Estos daemons supervisan los enrutadores de la red y anuncian las direcciones de los enrutadores a los hosts de la red local. Algunos protocolos de enrutamiento, aunque no todos, también guardan estadísticas que puede utilizar para medir el rendimiento del enrutamiento. De manera similar al reenvío de paquetes, debe configurar explícitamente el enrutamiento en un sistema Oracle Solaris.

RIP y RDISC son protocolos TCP/IP estándar. En la siguiente tabla se describen los protocolos de enrutamiento admitidos en Oracle Solaris.

TABLA 1-1 Protocolos de enrutamiento de Oracle Solaris

Protocolo	Daemon asociado	Descripción	Para obtener instrucciones
RIP	`in.routed`	Protocolo de portal interior (IGP) que enruta paquetes IPv4 y mantiene una tabla de enrutamiento	“Configuración de un enrutador IPv4” [17]
RDISC	`in.routed`	Les permite a los hosts descubrir la presencia de un enrutador en la red	“Activación del enrutamiento para sistemas de interfaz única” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”
RIPng	`in.ripngd`	IGP que enruta paquetes IPv6 y mantiene una tabla de enrutamiento	Cómo configurar un enrutador activado para IPv6 [23]
Protocolo ND	`in.ndpd`	Advierte la presencia de un enrutador IPv6 y descubre la presencia de hosts IPv6 en una red	“Cómo configurar un sistema para IPv6” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”

Para obtener más información sobre los tipos y tablas de enrutamiento, consulte “Tablas y tipos de enrutamiento” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”.

Protocolo de información de enrutamiento

El protocolo de información de enrutamiento (RIP) es un protocolo de enrutamiento vector-distancia. RIP utiliza un contador de salto como su métrica de enrutamiento. Se implementa mediante el daemon de enrutamiento `in.routed`. El daemon se inicia automáticamente cuando se inicia el sistema. Cuando se ejecuta en un enrutador con la opción `-s` especificada, el daemon `in.routed` completa la tabla de enrutamiento del núcleo a cada red accesible y comunica la

posibilidad de acceso mediante todas las interfaces de red. Cuando ejecuta un host con la opción `-q` especificada, el daemon `in.routed` extrae la información de enrutamiento pero no comunica las posibilidades de acceso.

En los hosts, la información de enrutamiento se puede extraer de lo dos modos siguientes:

- al *no* especificar el indicador (`S` mayúscula o modo de ahorro de espacio). El daemon `in.routed` crea una tabla de enrutamiento completa, al igual que en un enrutador.
- Al especificar el indicador. El daemon `in.routed` crea una tabla de núcleo mínima, que contiene una única ruta predeterminada para cada enrutador disponible.

Protocolo ICMP Router Discovery (RDISC)

Los hosts utilizan RDISC para obtener información de enrutamiento de los enrutadores. Cuando los hosts ejecutan RDISC, los enrutadores también deben ejecutar otro protocolo, como RIP, para poder intercambiar información de enrutadores.

RDISC se implementa mediante el daemon,`in.routed`, que debe ejecutarse tanto en enrutadores como hosts. En los hosts, `in.routed` utiliza RDISC para descubrir las rutas predeterminadas de los enrutadores que anuncian la dirección a través de RDISC. En los enrutadores, `in.routed` utiliza RDISC para dar a conocer las rutas predeterminadas a los hosts en las redes conectadas directamente. Consulte la página del comando man `in.routed`(1M) y la página del comando man `gateways`(4) para obtener más información.

Conjunto de protocolos de enrutamiento Quagga

Quagga es un conjunto de software de enrutamiento que permite la implementación de los protocolos RIP, RIPng, abrir la ruta de acceso más corta primero (OSPF), sistema intermedio a sistema intermedio (IS-IS) y puerta de enlace de borde (BGP) para plataformas UNIX incluido Oracle Solaris.

RIPng ofrece una extensión de RIP para poder admitir IPv6, incluidas varias mejoras para IPv6. Las funciones de RIPng son similares a las de RIP.

OSPF es un protocolo de enrutamiento que se utiliza para distribuir información de direccionamiento dentro de una red de sistema autónomo más grande. La última versión de OSPF, OSPFv3, agrega soporte para IPv6.

IS-IS es un protocolo de enrutamiento dinámico de estado del enlace que se utiliza para distribuir información de enrutamiento dentro de una red de provisión de servicios más grande.

BGP utiliza un conjunto antepuesto de redes IP para tomar decisiones de enrutamiento basadas en la ruta y las reglas en las redes de sistemas autónomos más grandes.

En la siguiente tabla, se muestran los protocolos de enrutamiento de código abierto Quagga que se admiten en Oracle Solaris.

TABLA 1-2 Conjunto de protocolos de enrutamiento Quagga

Protocolo	Daemon asociado	Descripción
RIP	`ripd`	Protocolo IGP vector-distancia para IPv4 que enruta paquetes IPv4 y muestra su tabla de enrutamiento a los vecinos
RIPng	`ripngd`	Protocolo IGP vector-distancia para IPv6 que enruta paquetes IPv6 y mantiene una tabla de enrutamiento
OSPF	`ospfd`	Protocolo IGP de estado de vínculo IPv4 para el enrutamiento de paquetes y las redes de gran disponibilidad.
BGP	`bgpd`	Protocolo de portal exterior (EGP) IPv4 e IPv6 para el enrutamiento en dominios administrativos
IS-IS	`isisd`	Protocolo IGP de estado de enlace IPv4 e IPv6 para el enrutamiento dentro de una red o un dominio administrativo

Para obtener más información sobre los protocolos Quagga, vaya al sitio en de Quagga Routing Suite en http://www.nongnu.org/quagga/index.html.

Protocolo de redundancia de enrutador virtual

VRRP proporciona una alta disponibilidad de direcciones IP, como las que se utilizan para los enrutadores y equilibradores de carga. VRRP es un protocolo estándar de Internet especificado en RFC 5798, Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6. Oracle Solaris proporciona una herramienta administrativa que configura y gestiona el servicio VRRP.

Además del VRRP de la capa 2 estándar existente, Oracle Solaris 11.2 proporciona un VRRP de capa 3 de propiedad exclusiva para admitir el VRRP a través de las interfaces IPMP e InfiniBand, y mejorar la compatibilidad para el VRRP en zonas.

Para obtener más información sobre el uso y la configuración de enrutadores VRRP, consulte Capítulo 3, Uso del protocolo de redundancia de enrutador virtual y Capítulo 4, Configuración y administración del protocolo de redundancia de enrutador virtual.

Descripción general del enrutador VRRP

Un enrutador VRRP es una imagen de enrutador única que se crea mediante el funcionamiento de uno o más enrutadores que utilizan el VRRP. El VRRP se ejecuta en cada enrutador VRRP y gestiona el estado del enrutador. Un host puede tener varios enrutadores VRRP configurados, donde cada enrutador VRRP pertenece a un enrutador virtual distinto.

El enrutador VRRP de la capa 2 utiliza un protocolo VRRP estándar y requiere la dirección MAC de enrutador virtual único. Las direcciones IP virtuales siempre se resuelven en la misma dirección MAC virtual. Debe crear una VNIC del VRRP para obtener la dirección MAC de enrutador virtual único. La función VRRP de la capa 3 de propiedad exclusiva en Oracle Solaris elimina por completo la necesidad de configurar las direcciones MAC virtuales VRRP únicas para enrutadores VRRP y, por lo tanto, proporciona compatibilidad para VRRP a través de las interfaces IPMP e InfiniBand.

Para obtener más información sobre el uso y la configuración de enrutadores VRRP, consulte Capítulo 3, Uso del protocolo de redundancia de enrutador virtual y Capítulo 4, Configuración y administración del protocolo de redundancia de enrutador virtual.

Descripción general del equilibrador de carga integrado

En Oracle Solaris, el equilibrador de carga integrado (ILB) proporciona capacidades de equilibrio de carga de la capa 3 y 4. ILB funciona en las capas de red (IP) y transporte (TCP/UDP) para el sistema operativo Oracle Solaris instalado en sistemas basados en SPARC y x86. ILB se puede utilizar para mejorar la fiabilidad y escalabilidad, y para minimizar el tiempo de respuesta de los servicios de red.

El ILB intercepta las solicitudes entrantes de los clientes, decide qué servidor back-end debe manejar las solicitudes en función de las reglas de equilibrio de carga y, luego, envía las solicitudes al servidor seleccionado. El ILB también se pueden utilizar como un enrutador para el servidor back-end. El ILB realiza comprobaciones de estado opcionales y proporciona los datos para los algoritmos de equilibrio de carga a fin de comprobar si el servidor seleccionado puede manejar las solicitudes entrantes.

Funciones del ILB

Entre las funciones clave del ILB se incluyen las siguientes:

- Admite los modos de funcionamiento sin estado de Retorno de servidor directo (DSR, Direct Server Return) y Traducción de direcciones de red (NAT, Network Address Translation) para IPv4 e IPv6.

  Para obtener información sobre los modos de funcionamiento DSR y NAT, consulte “Modos de funcionamiento del ILB” [50].
- Ayuda con el tráfico y la distribución de carga, y la selección del servidor al usar un juego de algoritmos para los dos modos de funcionamiento.
- Permite la administración del ILB mediante una interfaz de línea de comandos (CLI, Command-Line Interface).

Para obtener información sobre configuración del ILB mediante CLI, consulte “Configuración del ILB mediante la interfaz de línea de comandos” [58].

- Proporciona capacidades de supervisión del servidor mediante comprobaciones de estado.

  Para obtener información sobre capacidades de supervisión del servidor, consulte “Supervisión de las comprobaciones de estado en ILB” [64].

La siguiente tabla muestra y describe las funciones del ILB que están disponibles para distintos modos de funcionamiento.

TABLA 1-3 Funciones del ILB

Funciones	Descripción	Modo de funcionamiento
Permite que los clientes hagan ping a direcciones IP virtuales (VIP)	ILB responde las solicitudes de eco ICMP de clientes a direcciones VIP.	Ambos modos DSR y NAT
Permite agregar y eliminar servidores de un grupo de servidores sin interrumpir el servicio	ILB agrega de forma dinámica o elimina servidores del grupo de servidores.	Modo NAT
Permite configurar la persistencia de sesiones (permanencia)	El ILB le permite configurar la persistencia de sesión para que sus aplicaciones envíen las conexiones o los paquetes desde un cliente al mismo servidor back-end. El ILB le permite configurar la persistencia de sesiones (es decir, la persistencia de direcciones de origen) para un servicio virtual mediante el uso de la opción `-p` y la especificación de la opción `pmask` en el comando `ilbadm create-rule`. Para obtener más información, consulte “Creación de una regla del ILB” [68].	Ambos modos DSR y NAT
Permite realizar una purga de conexión	El ILB le impide el envío de nuevas conexiones a un servidor desactivado. Esta función es útil para cerrar un servidor sin alterar las conexiones o sesiones activas. Las conexiones existentes con el servidor siguen funcionando. Después de que finalizan todas las conexiones a ese servidor, el servidor se puede cerrar para realizar el mantenimiento. Cuando el servidor está listo para manejar solicitudes, se activa para que el equilibrador de carga le reenvíe nuevas conexiones.	Modo NAT
Permite el equilibrio de carga de puertos de protocolo de control de transmisión (TCP) y protocolo de datagramas de usuario (UDP)	El ILB equilibra la carga de todos los puertos en una dirección IP específica en diferentes grupos de servidores sin que se deba configurar reglas explícitas para cada puerto.	Ambos modos DSR y NAT
Permite especificar puertos independientes para servicios virtuales dentro del mismo grupo de servidores	El ILB le permite especificar diferentes puertos de destino para diferentes servidores en el mismo grupo de servidores.	Modo NAT
Permite controlar el equilibrio de carga de un intervalo de puertos simple	El ILB equilibra cargas en un intervalo de puertos en la VIP para un determinado grupo de servidores. Según sea necesario, puede conservar direcciones IP mediante el equilibrio de carga de diferentes intervalos de puertos en la misma VIP entre distintos grupos de servidores back-end.	Ambos modos DSR y NAT

Funciones	Descripción	Modo de funcionamiento
	Asimismo, cuando esté activada la persistencia de sesiones para el modo NAT, el ILB envía solicitudes de la misma dirección IP de cliente a diferentes puertos del intervalo del mismo servidor back-end.	
Permite el cambio y el cierre de intervalos de puertos	El cambio y el cierre de intervalos de puertos dependen del intervalo de puerto de un servidor en una regla de equilibrio de carga. Si el intervalo de puertos de un servidor es diferente del intervalo de puertos de la VIP, el cambio de puertos se implementa automáticamente. Si el intervalo de puertos del servidor tiene un único puerto, se implementa el cierre de puertos.	Modo NAT

Para obtener más información sobre los componentes del ILB, los modos de funcionamiento, los algoritmos y cómo funciona el ILB, consulte Capítulo 5, Descripción general de un equilibrador de carga integrado. Para obtener más información sobre la configuración y gestión del ILB, consulte Capítulo 6, Configuración y gestión del equilibrador de carga integrado y Capítulo 7, Configuración del ILB para Alta Disponibilidad.

¿Por qué utilizar enrutadores VRRP y equilibradores de carga?

Al configurar una red como red de área local (LAN, Local Area Network), es muy importante proporcionar un servicio de alta disponibilidad. La alta disponibilidad es un estado en el que un sistema redundante toma el control durante un fallo para garantizar la continuidad del negocio. También es relevante cuando una carga excesiva se descarga a un sistema redundante. La alta disponibilidad puede volverse significativa en situaciones como tiempo de inactividad planificado o no planificado, equilibrio de carga y recuperación después de un desastre.

Dentro de un dominio de red, la alta disponibilidad se puede implementar en varios niveles, como enlace, IP y enrutadores. Los equilibradores de carga y enrutadores tienen un rol significativo a fin de proporcionar un servicio de alta disponibilidad. En Oracle Solaris, los enrutadores VRRP y el ILB son los mecanismos de failover en el nivel de red y de uso compartido de carga que proporcionan alta disponibilidad.

Para obtener más información sobre cómo trabajar con enrutadores VRRP y configurarlos, consulte Capítulo 3, Uso del protocolo de redundancia de enrutador virtual. Para obtener más información sobre cómo trabajar con el ILB y configurarlo, consulte Capítulo 5, Descripción general de un equilibrador de carga integrado y Capítulo 6, Configuración y gestión del equilibrador de carga integrado.

♦ ♦ ♦ CAPÍTULO 2

Configuración de un sistema como enrutador

Un enrutador proporciona la interfaz entre dos o más redes. Debe asignar un nombre y una dirección IP exclusivos a cada interfaz de red física del enrutador. Cada enrutador tiene un nombre de host y una dirección IP asociados con su interfaz de red principal, además de otro nombre exclusivo y dirección IP, como mínimo, para cada interfaz de red adicional. En este capítulo se describe cómo configurar el sistema Oracle Solaris como un enrutador IPv4 o un enrutador IPv6.

Este capítulo se divide en los siguientes apartados:

- “Configuración de un enrutador IPv4” [17]
- “Configuración de un enrutador IPv6” [22]

Para obtener información sobre la configuración del enrutamiento para un host Oracle Solaris en una red, consulte “Activación del enrutamiento para sistemas de interfaz única” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”.

Para obtener información sobre los protocolos de enrutamiento, consulte “Protocolos de enrutamiento” [10] y “Acerca del enrutamiento de IPv6” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”.

Configuración de un enrutador IPv4

Puede utilizar el siguiente procedimiento para configurar un sistema con una sola interfaz física (de modo predeterminado, un host) como enrutador. Puede configurar un sistema con una sola interfaz como enrutador si el sistema actúa como punto final en un enlace PPP, tal como se describe en “Planificación de un enlace de PPP por marcación telefónica” de “Gestión de redes seriales con UUCP y PPP en Oracle Solaris 11.2 ”.

▼ Configuración de un enrutador IPv4

El siguiente procedimiento presupone que está configurando interfaces para el enrutador tras la instalación de éste.

Antes de empezar Después de que el enrutador se instala físicamente en la red, configúrelo para que funcione en el modo de archivos locales. Con esta configuración, los enrutadores se iniciarán incluso si el servidor de configuración de red no funciona.

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 las interfaces IP para las tarjetas NIC en el sistema.**

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

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

   - **Para configurar una dirección estática, escriba el siguiente comando:**

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

   - **Para configurar una dirección no estática, escriba el siguiente comando:**

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

   Para obtener instrucciones detalladas sobre cómo configurar 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 ".

   Asegúrese de que cada interfaz IP esté configurada con la dirección IP de la red para la cual el sistema debe enrutar los paquetes. Por lo tanto, si el sistema presta servicio a las redes `192.168.5.0` y `10.0.5.0` , se debe configurar una NIC para cada red.

Atención - Asegúrese de conocer detalladamente la administración DHCP antes de configurar un enrutador IPv4 para utilizar DHCP.

4. **Agregue el nombre de host y la dirección IP de cada interfaz al archivo `/etc/inet/hosts`.**

   Por ejemplo, suponga que los nombres que asignó a las dos interfaces del enrutador son `krakatoa` y `krakatoa-1`, respectivamente. Las entradas del archivo `/etc/inet/hosts` son las siguientes:

   ```
   192.168.5.1      krakatoa        #interface for network 192.168.5.0
   10.0.5.1         krakatoa-1      #interface for network 10.0.5.0
   ```

5. **Realice el procedimiento "Cómo configurar un sistema para el modo de archivos locales" de "Configuración y administración de componentes de red en Oracle Solaris 11.2 " para configurar este enrutador a fin de que se ejecute en el modo de archivos locales.**

6. **Si el enrutador está conectado a cualquier red con subredes, agregue el número de red y la máscara de red al archivo `/etc/inet/netmasks`.**

   Por ejemplo, para notación de direcciones IPv4, como `192.168.5.0`, escriba lo siguiente:

   ```
   192.168.5.0    255.255.255.0
   ```

7. **Active el reenvío de paquetes IPv4 en el enrutador.**

   ```
   # ipadm set-prop -p forwarding=on ipv4
   ```

8. **(Opcional) Inicie un protocolo de enrutamiento.**

   Utilice uno de los siguientes comandos:

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

   donde la opción `-e` permite el enrutamiento IPv4 y la opción `-u` aplica la configuración actual al sistema que se está ejecutando.

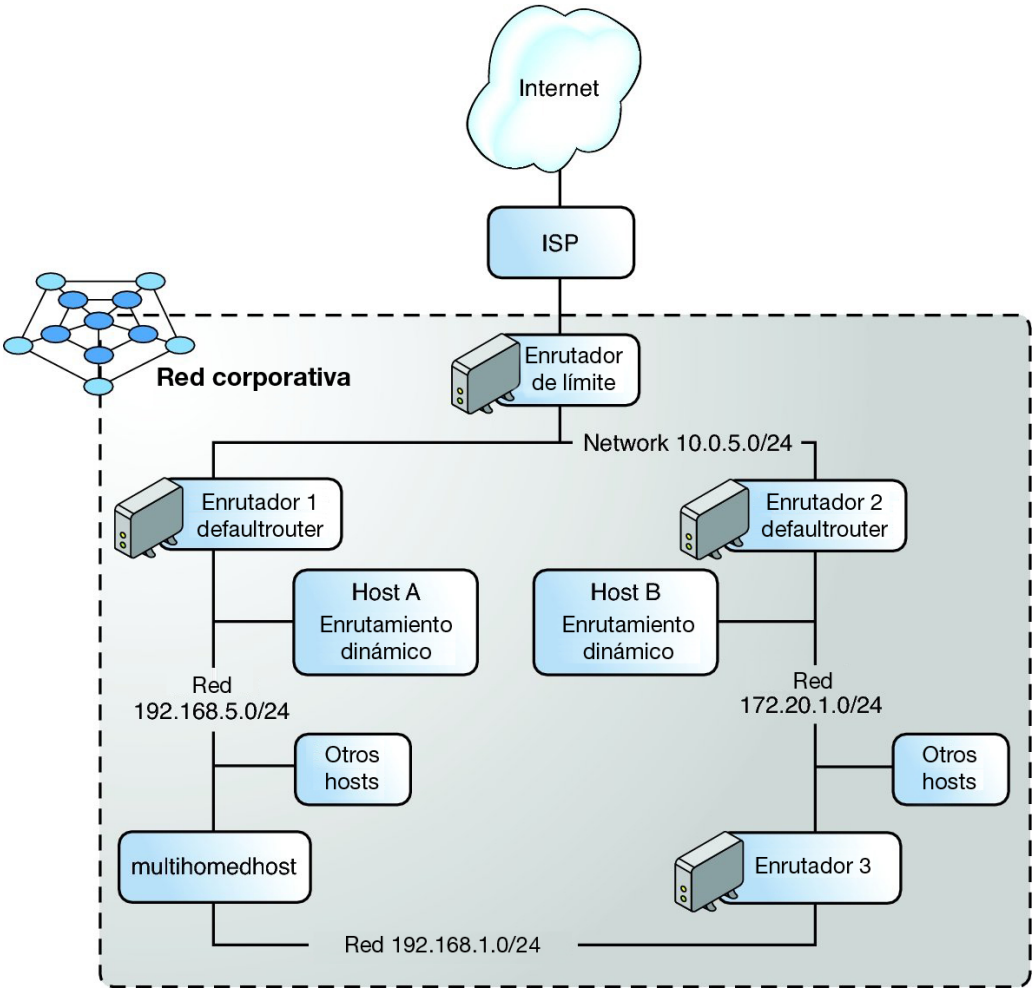
   ```
   # svcadm enable route:default
   ```

   Cuando inicia un protocolo de enrutamiento, el daemon de enrutamiento `/usr/sbin/in.routed` actualiza automáticamente la tabla de enrutamiento. Este proceso se conoce como *enrutamiento dinámico*. Para obtener más información sobre los tipos de enrutamiento, consulte “Tablas y tipos de enrutamiento” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”. Para obtener información sobre el comando `routeadm`, consulte la página del comando man `routeadm`(1M) y para más información sobre el comando `ipadm` command, consulte la página del comando man `ipadm`(1M).

   El identificador de recurso de gestión de errores (FMRI, Fault Management Resource Identifier) de la utilidad de gestión de servicios (SMF, Service Management Facility) asociado con el daemon `in.routed` es `svc:/network/routing/route`.

ejemplo 2-1 Configuración de un sistema como enrutador

Este ejemplo se basa en la siguiente figura.



El enrutador 2 contiene dos conexiones de red cableadas, una conexión a la red `172.20.1.0` y otra a la red `10.0.5.0`. El ejemplo muestra cómo configurar un sistema como enrutador (enrutador 2) de la red `172.20.1.0`. El ejemplo también supone que el enrutador 2 se ha configurado para funcionar en el modo de archivos locales como se describe en "Cómo configurar un sistema para el modo de archivos locales" de "Configuración y administración de componentes de red en Oracle Solaris 11.2 ".

1. Determine el estado de las interfaces del sistema.

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

```
# ipadm show-addr
ADDROBJ           TYPE     STATE        ADDR
lo0/v4            static   ok           10.0.0.1/8
net0/v4           static   ok           172.20.1.10/24
```

2. Únicamente `net0` se configuró con una dirección IP. Para convertir el enrutador 2 en el enrutador predeterminado, debe conectar físicamente la interfaz `net1` a la red `10.0.5.0`.

```
# ipadm create-ip net1
# ipadm create-addr -a 10.0.5.10/24 net1
# ipadm show-addr
ADDROBJ           TYPE     STATE        ADDR
lo0/v4            static   ok           192.168.0.1/8
net0/v4           static   ok           172.20.1.10/24
net1/v4           static   ok           10.0.5.10/24
```

3. Actualice las siguientes bases de datos de red con información sobre la interfaz recientemente configurada y la red a la que está conectada:

```
# pfedit /etc/inet/hosts
192.168.0.1       localhost
172.20.1.10        router2        #interface for network 172.20.1
10.0.5.10          router2-out    #interface for network 10.0.5
# pfedit /etc/inet/netmasks
172.20.1.0    255.255.255.0
10.0.5.0      255.255.255.0
```

4. Active el reenvío de paquetes y el daemon de enrutamiento `in.routed`.

```
# ipadm set-prop -p forwarding=on ipv4
# svcadm enable route:default
```

Ahora, el reenvío de paquetes IPv4 y el enrutamiento dinámico mediante RIP están activados en el enrutador 2. Sin embargo, para completar la configuración del enrutador predeterminado para la red `172.20.1.0` debe hacer lo siguiente:

- Modifique cada host de la red `172.20.1.0` de modo que obtenga la información de enrutamiento del nuevo enrutador predeterminado. Para obtener más información, consulte "Creación de rutas persistentes (estáticas)" de "Configuración y administración de componentes de red en Oracle Solaris 11.2 ".
- Defina una ruta estática para el enrutador de límite en la tabla de enrutamiento del enrutador 2. Para obtener más detalles, consulte "Tablas y tipos de enrutamiento" de "Configuración y administración de componentes de red en Oracle Solaris 11.2 ". Para obtener más información sobre el comando `ipadm`, consulte la página del comando man `ipadm`(1M).

Configuración de un enrutador IPv6

En esta sección, se describe cómo configurar un enrutador IPv6.

Daemon `in.ripngd`, para enrutamiento de IPv6

El daemon `in.ripngd` implementa la próxima generación del protocolo RIPng (Routing Information Protocol) para enrutadores IPv6. RIPng define el equivalente de IPv6 de RIP. Si se configura un enrutador de IPv6 con el comando `routeadm` y se activa el enrutamiento de IPv6, el daemon `in.ripngd` implementa el protocolo RIPng en el enrutador. Para obtener información sobre las opciones admitidas del protocolo ripng, consulte `in.ripngd`(1M).

Prefijos, mensajes y anuncios de enrutador

En vínculos con capacidad multidifusión y punto a punto, cada enrutador envía, de forma periódica, al grupo multidifusión un paquete de anuncios de enrutador que informa de su disponibilidad. Un host recibe anuncios de enrutador de todos los enrutadores, y confecciona una lista de enrutadores predeterminados. Los enrutadores generan anuncios de enrutador con la suficiente frecuencia para que los hosts aprendan su presencia en pocos minutos. Sin embargo, los enrutadores no anuncian con suficiente frecuencia como para que una falta de anuncios permita detectar un error de enrutador. La detección de errores es factible mediante un algoritmo de detección independiente que determina que los vecinos no puedan acceder.

Los anuncios de enrutador contienen una lista de prefijos de subred que se usan para determinar si un host se encuentra en el mismo enlace que el enrutador. La lista de prefijos también se utiliza en la configuración de direcciones autónomas. Los indicadores que se asocian con los prefijos especifican el uso concreto de un determinado prefijo. Los hosts utilizan los prefijos del vínculo anunciados para configurar y mantener una lista que se emplea para decidir si el destino de un paquete se encuentra en el vínculo o fuera de un enrutador. Un destino puede encontrarse en un vínculo aunque dicho destino no aparezca en ningún prefijo del vínculo que esté anunciado. En esos casos, un enrutador puede enviar una redirección. La redirección indica al remitente que el destino es un vecino.

Los anuncios de enrutador, y los indicadores de prefijo, permiten a los enrutadores informar a los hosts sobre cómo efectuar la configuración automática de direcciones sin estado.

Los mensajes de anuncio de enrutador contienen también parámetros de Internet, por ejemplo el límite de salto que los hosts deben emplear en los paquetes salientes. También es posible que los mensajes de anuncio de enrutador contengan parámetros de vínculo, por ejemplo la MTU de vínculo. Esta función permite la administración centralizada de los parámetros importantes. Los parámetros se pueden establecer en enrutadores y propagarse automáticamente a todos los hosts que estén conectados.

Los nodos llevan a cabo la resolución de direcciones enviando al grupo de multidifusión una solicitud de vecino que pide al nodo de destino que devuelva su dirección de capa de vínculo. Los mensajes de solicitud de vecino multidifusión se envían a la dirección multidifusión de nodo solicitado de la dirección de destino. El destino devuelve su dirección de capa de vínculo en un mensaje de anuncio de vecino unidifusión. Para que el iniciador y el destino resuelvan sus respectivas direcciones de capa de vínculo basta con un solo par de paquetes de solicitud-respuesta. El iniciador incluye su dirección de capa de vínculo en la solicitud de vecino.

▼ Cómo configurar un enrutador activado para IPv6

El siguiente procedimiento supone que ya ha configurado el sistema para IPv6. Para obtener instrucciones sobre los procedimientos, 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 ”.

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 el reenvío de paquetes IPv6 en todas las interfaces del enrutador.**

   ```
   # ipadm set-prop -p forwarding=on ipv6
   ```

3. **Inicie el daemon de enrutamiento.**

   El daemon `in.ripngd` se encarga del enrutamiento de IPv6. Active el enrutamiento de IPv6 mediante uno de los siguientes comandos:

   - Utilice el comando `routeadm`:

     ```
     # routeadm -e ipv6-routing -u
     ```

     donde la opción `-e` permite el enrutamiento IPv4 y la opción `-u` aplica la configuración actual al sistema que se está ejecutando.
   - Utilice el comando SMF adecuado:

     ```
     # svcadm enable ripng:default
     ```

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

4. **Cree el archivo `/etc/inet/ndpd.conf`. Archivo**

   Especifique el prefijo de sitio que debe anunciar el enrutador y demás datos de configuración en el archivo `/etc/inet/ndpd.conf`. El daemon `in.ndpd` lee este archivo e implementa el protocolo de descubrimiento de vecinos de IPv6.

Para obtener una lista de variables y valores permitidos, consulte la página del comando man `ndpd.conf`(4).

5. **Escriba el texto siguiente en el archivo `/etc/inet/ndpd.conf`:**

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

Este texto indica al daemon `in.ndpd` que envíe anuncios de enrutador en todas las interfaces del enrutador que se hayan configurado para IPv6.

6. **Para configurar el prefijo de sitio en las distintas interfaces del enrutador, agregue texto adicional al archivo `/etc/inet/ndpd.conf`.**

El texto se debe agregar en el siguiente formato:

`prefix` *global-routing-prefix*:*subnet ID*`/64` *interface*

En el siguiente archivo de ejemplo, el archivo `/etc/inet/ndpd.conf` configura el enrutador para que anuncie el prefijo de sitio `2001:0db8:3c4d::/48` en las interfaces `net0` y `net1`.

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on

if net0 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:15::0/64 net0

if net1 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:16::0/64 net1
```

7. **Reinicie el sistema.**

El enrutador de IPv6 comienza a anunciar en el vínculo cualquier prefijo de sitio que esté en el archivo `ndpd.conf`.

8. **Visualice la interfaz configurada para IPv6.**

```
# ipadm show-addr
ADDROBJ      TYPE       STATE   ADDR
lo0/v4       static     ok      192.68.0.1/8
net0/v4      static     ok      172.16.15.232/24
net1/v4      static     ok      172.16.16.220/24
net0/v6      addrconf   ok      fe80::203:baff:fe11:b115/10
lo0/v6       static     ok      ::1/128
net0/v6a     static     ok      2001:db8:3c4d:15:203:baff:fe11:b115/64
net1/v6      addrconf   ok      fe80::203:baff:fe11:b116/10
net1/v6a     static     ok      2001:db8:3c4d:16:203:baff:fe11:b116/64
```

En el resultado, cada interfaz que fue configurada para IPv6 ahora dispone de dos direcciones. La entrada con el nombre de objeto de dirección, como *interface*`/v6`, muestra la dirección local de enlace para esa interfaz. La entrada con el nombre de objeto de dirección, como

interface`/v6a` muestra una dirección IPv6 global. Además del ID de la interfaz, esta dirección incluye el prefijo de sitio que configuró en el archivo `/etc/ndpd.conf`. Tenga en cuenta que la designación `v6a` es una cadena definida de forma aleatoria. Puede definir otras cadenas para constituir la segunda parte del nombre de objeto de dirección, siempre que *interface* refleje la interfaz mediante la cual está creando las direcciones IPv6, por ejemplo `net0/mystring`, `net0/ipv6addr`.

Véase también

- Para averiguar cómo configurar túneles desde los enrutadores que ha identificado en la topología de red IPv6, consulte "Administración de túneles IP" de "Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ".
- Para obtener información sobre cómo configurar conmutadores y concentradores en la red, consulte la documentación del fabricante.
- Para averiguar cómo mejorar la compatibilidad de IPv6 en los servidores, consulte "Configuración de interfaces activadas para IPv6 en servidores" de "Configuración y administración de componentes de red en Oracle Solaris 11.2 ".

♦ ♦ ♦ CAPÍTULO 3

Uso del protocolo de redundancia de enrutador virtual

Una forma de aumentar la fiabilidad de la red es proporcionar copias de seguridad de los componentes críticos de la red. Oracle Solaris proporciona una herramienta administrativa que configura y gestiona el uso del protocolo de redundancia de enrutador virtual (VRRP) a fin de proporcionar alta disponibilidad. VRRP es un protocolo estándar de Internet especificado en RFC 5798 (http://www.rfc-editor.org/rfc/rfc5798.txt).

Oracle Solaris 11.2 proporciona el VRRP de la capa 3 de propiedad exclusiva para admitir la creación de enrutadores VRRP a través de las interfaces IPMP e InfiniBand, y mejorar la compatibilidad para VRRP en zonas.

Nota - En este capítulo, todas las referencias al VRRP de la capa 2 (L2 VRRP) hacen referencia específicamente al VRRP estándar de Internet y todas las referencias al VRRP de la capa 3 (L3 VRRP) hacen referencia al VRRP de la capa 3 de propiedad exclusiva en Oracle Solaris.

En este capítulo se proporciona una descripción general del VRRP de la capa 2 y el VRRP de la capa 3 de propiedad exclusiva en Oracle Solaris.

Este capítulo se divide en los siguientes apartados:

Sobre el VRRP

El VRRP proporciona una alta disponibilidad de direcciones IP, como las que se utilizan para los enrutadores y equilibradores de carga. Los servicios que utilizan el VRRP también se

denominan enrutadores VRRP, aunque los servicios proporcionan otras funciones además del enrutamiento, como el equilibrio de carga. Para obtener más información sobre cómo se utiliza el VRRP con el equilibrio de carga para garantizar una alta disponibilidad, consulte Capítulo 7, Configuración del ILB para Alta Disponibilidad.

Un enrutador VRRP es un enrutador que está ejecutando el VRRP. El VRRP se ejecuta en cada enrutador VRRP y gestiona el estado del enrutador. Un host puede tener varios enrutadores en los cuales se ha configurado el VRRP y cada enrutador pertenece a un enrutador virtual distinto. Puede introducir enrutadores virtuales en una red de área local (LAN) al utilizar el VRRP para ofrecer la recuperación tras fallos para un enrutador.

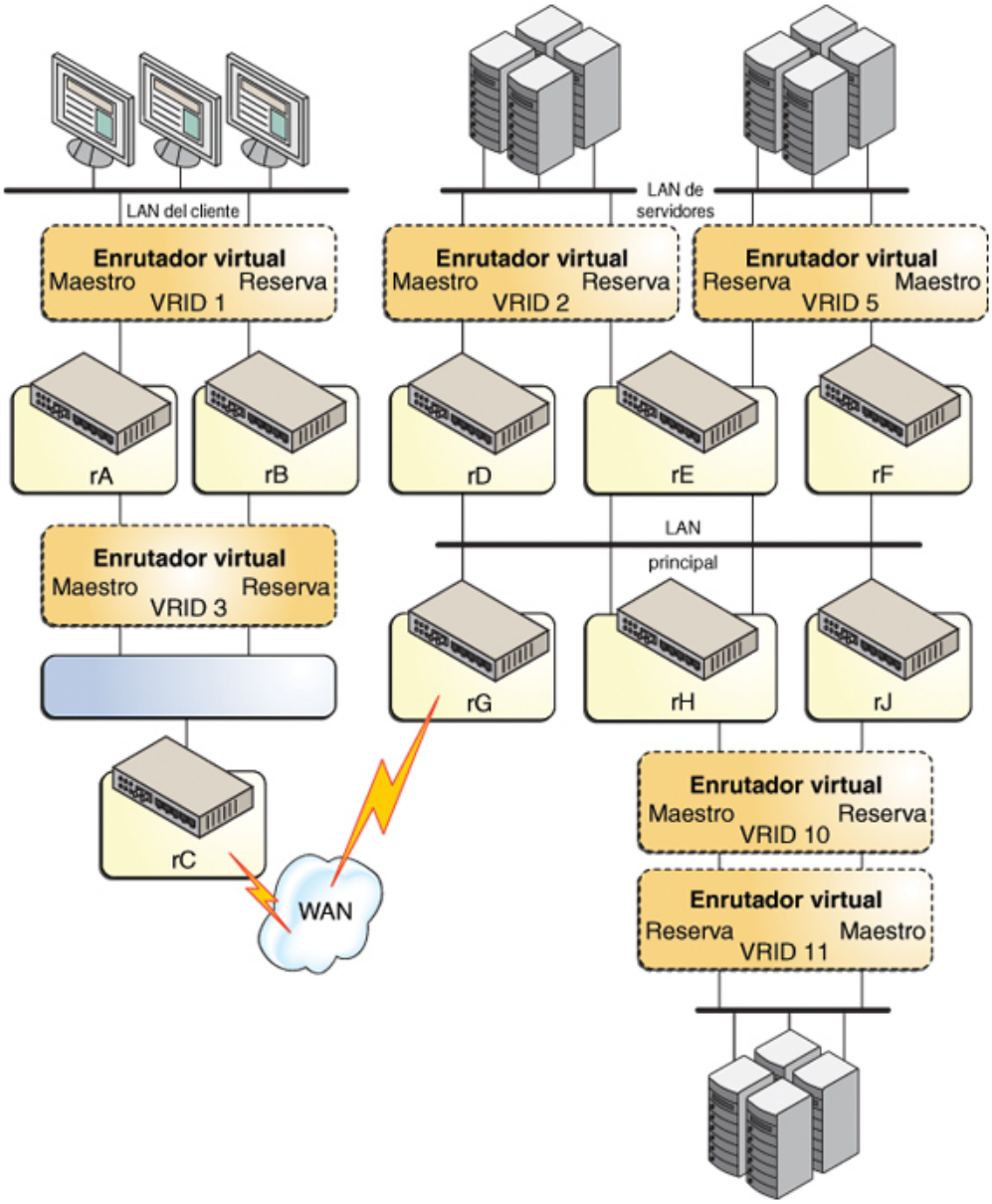
¿Cómo funciona el VRRP?

Tenga en cuenta los siguiente términos del enrutador VRRP:

- Nombre de enrutador : un identificador exclusivo para todo el sistema.
- ID de enrutador virtual (VRID, Virtual Router ID) : un número único que se utiliza para identificar un enrutador virtual en un segmento de red determinado. Los VRID identifican el enrutador virtual dentro de una LAN.
- Dirección IP principal : dirección IP de origen del anuncio del VRRP.
- Dirección IP virtual (VRIP, Virtual IP Address) : una dirección IP asociada con un VRID del cual otros hosts pueden obtener servicio de red. El VRIP gestiona las instancias del VRRP pertenecientes a un VRID.
- Enrutador maestro: una instancia de VRRP que realiza la función de enrutamiento para el enrutador virtual en un momento determinado. Únicamente hay un *enrutador maestro* activo a la vez para un VRID determinado. El enrutador maestro controla las direcciones IPv4 o IPv6 que están asociadas con el enrutador virtual. El enrutador virtual reenvía los paquetes que se envían a la dirección IP del enrutador maestro.
- Enrutador de copia de seguridad: una instancia de VRRP para un VRID que está activo, pero no en el estado maestro se denomina *enrutador de copia de seguridad*. Puede existir cualquier cantidad de enrutadores de copia de seguridad para un VRID. Un enrutador de copia de seguridad asume el rol de enrutador maestro si falla el enrutador maestro actual.
- Parámetros del VRRP: incluyen la prioridad, el intervalo de anuncios, el modo de preferencia y el modo de aceptación.
- Estadísticas e información de estado de VRRP.

La siguiente figura de configuración de uso compartido de carga del VRRP demuestra que pueden existir varios VRID en una única interfaz de enrutador. El texto adjunto explica los componentes del VRRP que se utilizan en la figura. Esta configuración de uso compartido de carga de VRRP demuestra que pueden existir varios VRID en una única interfaz de enrutador.

FIGURA 3-1 Configuración de uso compartido de carga del VRRP en una LAN



- El enrutador `rA` es el enrutador maestro para el enrutador virtual VRID 1 y el enrutador de reserva para VRID 3. El enrutador `rA` controla el enrutamiento de los paquetes que

se dirigen a la dirección IP virtual (VIP) para VRID 1 y está listo para asumir el rol de enrutamiento para VRID 3.

- El enrutador `rB` es el enrutador maestro para el enrutador virtual VRID 3 y el enrutador de reserva para VRID 1. El enrutador `rB` controla el enrutamiento de paquetes que se dirigen a la VIP para VRID 3 y está listo para asumir el rol de enrutamiento para VRID 1.
- El enrutador `rC` no tiene funciones de VRRP, pero utiliza la VIP para VRID 3 LAN, a fin de alcanzar la subred LAN del cliente.
- El enrutador `rD` es el enrutador maestro para VRID 2. El enrutador `rF` es el enrutador maestro para VRID 5. El enrutador `rE` es el enrutador de copia de seguridad para estos VRID. Si `rD` o `rF` fallan, `rE` se convierte en el enrutador maestro para ese VRID. `rD` y `rF` pueden fallar al mismo tiempo. Un enrutador VRRP puede ser el enrutador maestro para uno o más VRID.
- El enrutador `rG` es una puerta de enlace de red de área extensa (WAN, Wide Area Network) para la LAN principal. Todos los enrutadores conectados a la red principal comparten información de enrutamiento con los enrutadores de la WAN mediante un protocolo de enrutamiento dinámico como OSPF, que permite abrir la ruta más corta primero. VRRP no se involucra en este aspecto, aunque el enrutador `rC` anuncia que la ruta de acceso a la subred LAN del cliente se realiza mediante el VIP del VRID 3.
- El enrutador `rH` es el enrutador principal para VRID 10 y el enrutador de reserva para VRID 11. Del mismo modo, el enrutador `rJ` es el enrutador principal para VRID 11 y el enrutador de reserva para VRID 10.

Sobre la función VRRP de la capa 3

La función de protocolo de redundancia de enrutador virtual (VRRP) de la capa 3 (L3 VRRP) de propiedad exclusiva en Oracle Solaris elimina la necesidad de configurar direcciones MAC virtuales del VRRP únicas para enrutadores VRRP y, por lo tanto, brinda mejor compatibilidad para el VRRP a través de las interfaces IPMP e InfiniBand, y en zonas. El protocolo L3 VRRP no cumple con la especificación del VRRP estándar. En lugar de usar una dirección MAC virtual única entre los enrutadores VRRP en el mismo enrutador virtual, la implementación L3 VRRP usa los mensajes gratuitos del protocolo de resolución de direcciones (ARP) y los mensajes del protocolo ND (NDP) a fin de actualizar la asignación entre las direcciones IP virtuales y la dirección MAC del enrutador VRRP maestro actual.

El VRRP de la capa 3 brinda la ventaja de compatibilidad para VRRP a través de las interfaces IPMP e InfiniBand y mejor compatibilidad en zonas; además, elimina la necesidad de crear la VNIC del VRRP.

Comparación del VRRP de la capa 2 y la capa 3

En la siguiente tabla se proporciona una comparación del VRRP de la capa 2 con el de la capa 3.

TABLA 3-1 Comparación del VRRP de la capa 2 y la capa 3

Función	VRRP de la capa 2	VRRP de la capa 3
Creación de una VNIC de VRRP	Debe crear una VNIC del VRRP.	No es necesario crear una VNIC del VRRP porque la dirección MAC del VRRP virtual que proporciona la VNIC del VRRP no es necesaria.
Compatibilidad con IPMP	No admitida.	Admitida. Cuando un enrutador VRRP de la capa 3 se crea a través de un grupo IPMP, cada dirección IP virtual en el enrutador maestro se asocia con una dirección MAC de la interfaz subyacente IPMP activa, según la política IPMP existente. Si el failover se produce en el grupo IPMP, las asignaciones de la capa 2 o 3 se anuncian mediante los mensajes ARP o NDP gratuitos.
Compatibilidad con zonas	Existen problemas al ejecutar varios enrutadores VRRP que pertenecen al mismo enrutador virtual en zonas distintas. En un sistema con dos o más enrutadores VRRP que comparten la misma dirección MAC virtual del VRRP, el conmutador virtual incorporado interfiere en el flujo normal de los paquetes de anuncios del VRRP hacia el enrutador VRRP. Para obtener más información, consulte “Limitaciones del VRRP de la capa 2 y la capa 3” [32].	Admitida.
Compatibilidad con Infini Band	No admitida.	Admitida.
Dirección MAC única del enrutador virtual	Necesita una dirección MAC única del enrutador virtual. Las direcciones IP virtuales siempre se resuelven en la misma dirección MAC virtual.	No requerida. Utiliza la dirección MAC en la cual se crea el enrutador VRRP. La dirección MAC es diferente entre todos los enrutadores VRRP que se encuentran en el mismo enrutador virtual. La misma dirección MAC está asociada con las direcciones IP virtuales que están protegidas por este enrutador VRRP de la capa 3.
Configuración de direcciones IP virtuales del VRRP	Se deben configurar.	Se deben configurar.
Redirección de protocolo de	Puede utilizarse cuando el VRRP de la capa 2 se está ejecutando entre un grupo de enrutadores. Cuando un enrutador VRRP de la capa 2 necesita utilizar la redirección de ICMP, verifica la	Se debe desactivar las redirecciones de ICMP. Cuando se crean varios enrutadores VRRP a través de la misma interfaz, estos comparten la misma dirección MAC. Por lo tanto, el VRRP de

Función	VRRP de la capa 2	VRRP de la capa 3
mensajes de control de Internet (ICMP)	dirección MAC de destino (dirección MAC virtual del VRRP) de los paquetes que deben redirigirse. Mediante la dirección MAC de destino, el enrutador VRRP de la capa 2 determina el enrutador virtual al cual se envío inicialmente el paquete. Por lo tanto, el enrutador VRRP de la capa 2 puede seleccionar la dirección de origen y enviar el mensaje de redirección de ICMP al origen.	la capa 3 no puede determinar la dirección MAC de destino.
Elección de enrutador maestro	La elección del enrutador maestro es transparente para el host. Cuando el enrutador maestro cambia, el conmutador que existe entre el host y el enrutador identifica el nuevo puerto al cual enviar el tráfico mediante su capacidad de aprendizaje MAC.	La selección del enrutador maestro cambia la asignación de la capa 2 de las direcciones IP virtuales y la nueva asignación debe ser anunciada por los mensajes ARP o NDP gratuitos.
Tiempo de failover	Normal.	Puede ser superior por los requisitos adicionales de los mensajes ARP o NDP gratuitos cuando la elección del enrutador maestro cambia.

Limitaciones del VRRP de la capa 2 y la capa 3

Los VRRP de la capa 2 y la capa 3 tienen limitaciones comunes de manera que debe configurar las direcciones IP virtuales del VRRP de la capa 2 y la capa 3 de forma estática. No puede configurar automáticamente las direcciones virtuales del VRRP mediante el uso de las dos herramientas de configuración automática existentes para direcciones IP: `in.ndpd` para la configuración automática IPv6 y `dhcpagent` para la configuración del protocolo de configuración dinámica de host (DHCP). Además, el VRRP de la capa 2 y la capa 3 tienen limitaciones específicas.

La función del VRRP de la capa 2 tiene las siguientes limitaciones:

- **Compatibilidad con zonas de IP exclusiva**

  Cuando se crea cualquier enrutador VRRP en una zona de IP exclusiva, el servicio VRRP `svc:/network/vrrp/default` se activa automáticamente. El servicio de VRRP gestiona el enrutador VRRP para dicha zona. Sin embargo, la compatibilidad para una zona IP exclusiva está limitada de la siguiente manera:

  - Debido a que no se puede crear una tarjeta de la interfaz de red virtual (VNIC) dentro de una zona no global, debe crear primero la VNIC del VRRP en la zona global. Luego, debe asignar la VNIC a la zona no global en la que reside el enrutador VRRP. A continuación, puede crear el enrutador VRRP en la zona no global utilizando el comando `vrrpadm`.
  - En un sistema Oracle Solaris, no puede crear dos enrutadores VRRP en distintas zonas para que participen con el mismo enrutador virtual. Oracle Solaris no permite crear dos VNIC con la misma dirección MAC (control de acceso de medios).
- **Interacciones con otras funciones de red**

- El servicio VRRP de la capa 2 no funciona en una interfaz con rutas múltiples de red IP (IPMP). El VRRP requiere direcciones MAC específicas del VRRP, pero IPMP funciona por completo en la capa IP. Para obtener información sobre IPMP, consulte Capítulo 2, “Acerca de la administración de IPMP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.

  El VRRP se puede utilizar en las adiciones de enlaces en troncos o los modos de agregación DLMP. Para obtener más información sobre las adiciones, consulte Capítulo 2, “Configuración de alta disponibilidad mediante agregaciones de enlaces” de “Gestión de enlaces de datos de red en Oracle Solaris 11.2 ”.
- El servicio VRRP de la capa 2 no funciona en una interfaz IP a través de Infiniband (IPoIB).

- **Compatibilidad de Ethernet a través de InfiniBand**

  El VRRP de la capa 2 no admite la interfaz Ethernet a través de InfiniBand (EoIB). Debido a que cada enrutador VRRP de la capa 2 está asociado con una única dirección MAC virtual, los enrutadores VRRP que participan con el mismo enrutador virtual necesitan usar la misma dirección MAC virtual de forma simultánea, lo que no es admitido por la interfaz EoIB. El VRRP de la capa 3 supera esta limitación ya que utiliza una dirección MAC distinta entre todos los enrutadores VRRP que existen en el mismo enrutador virtual.

La función de VRRP de la capa 3 tiene las siguientes limitaciones:

- El uso de mensajes ARP o NDP gratuitos puede dar como resultado un tiempo de failover durante la elección del enrutador maestro.

  El VRRP de la capa 3 usa mensajes ARP o NDP gratuitos para anunciar la nueva asignación de la capa 2 o 3 cuando la elección del enrutador maestro cambia. Este requerimiento adicional de uso de mensajes ARP o NDP gratuitos puede dar como resultado un tiempo de failover más prolongado. En algunos casos, si se pierden todos los mensajes ARP o NDP gratuitos anunciados, el host puede demorar más en recibir la entrada NDP o ARP actualizada. Por lo tanto, el envío de paquetes hacia el nuevo enrutador maestro podría demorarse.
- No puede determinar la dirección MAC de destino al utilizar las redirecciones ICMP porque la misma dirección MAC de destino es compartida por varios enrutadores.

  Puede utilizar las redirecciones ICMP cuando utilice un VRRP entre un grupo de enrutadores en una topología de red que no sea simétrica. La dirección IPv4 o IPv6 de origen de una redirección ICMPv4 o ICMPv6 debe ser la dirección utilizada por el host de finalización al tomar la decisión de enrutamiento de próximo salto.

  Cuando un enrutador VRRP de la capa 3 necesita usar las redirecciones ICMP, el enrutador VRRP de la capa 3 comprueba la dirección MAC de destino (dirección MAC virtual del VRRP) de los paquetes que deben redireccionarse. Puesto que la misma dirección MAC de destino es compartida por varios enrutadores creados a través de la misma interfaz, el enrutador VRRP de la capa 3 no puede determinar la dirección MAC de destino. Por lo tanto, puede resultar útil desactivar las redirecciones ICMP cuando utilice los enrutadores VRRP de la capa 3. Puede desactivar las redirecciones ICMP mediante las propiedades de protocolo IPv4 y IPv6 públicas`send_redirects` de la siguiente manera:

```
# ipadm set-prop -m ipv4 -p send_redirects=off
```

- Las direcciones IP virtuales del VRRP no se pueden configurar automáticamente mediante `in.ndpd` o DHCP.

♦ ♦ ♦ CAPÍTULO 4

Configuración y administración del protocolo de redundancia de enrutador virtual

En este capítulo se describen las tareas para la configuración del VRRP de la capa 2 y la capa 3. Este capítulo se divide en los siguientes apartados:

Planificación de una configuración del VRRP

Planificar una configuración del VRRP de la capa 2 o la capa 3 implica los siguientes pasos:

1. Determinar si se debe configurar un enrutador VRRP de la capa 2 o la capa 3.
2. (Para el enrutador VRRP de capa 2 solamente) Crear una interfaz de red virtual (VNIC, virtual network interface) del VRRP. Para obtener más información, consulte "Creación de una VNIC del VRRP para el VRRP de la capa 2" [37].

   Puede crear automáticamente una VNIC del VRRP mediante la opción `-f` del comando `vrrpadm` al crear el enrutador VRRP de la capa 2.
3. Crear un enrutador VRRP. Para obtener más información, consulte "Creación de un enrutador VRRP" [37].
4. Configurar la dirección IP virtual para el enrutador VRRP. Para obtener más información, consulte "Configuración de la dirección IP virtual para enrutadores VRRP de la capa 2 y la capa 3" [40].

   Puede configurar las direcciones IP virtuales mediante el uso de la opción `-a` del comando `vrrpadm`. Para obtener más información, consulte "Creación de un enrutador VRRP" [37].

Instalación del VRRP

Debe instalar el VRRP para utilizarlo en el sistema.

▼ Cómo instalar el VRRP

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. **Verifique si el paquete del VRRP está instalado.**

   ```
   # pkg info vrrp
   ```
3. **Instale el paquete del VRRP si no está instalado.**

   ```
   # pkg install vrrp
   ```

Configuración del VRRP

Puede utilizar el comando `vrrpadm` para configurar un enrutador VRRP. El resultado de todos los subcomandos del comando `vrrpadm` se mantiene, excepto para el comando `vrrpadm show-router`. Por ejemplo, el enrutador VRRP que se crea mediante el comando `vrrpadm create-router` se mantiene después de reiniciar. Para obtener más información, consulte la página del comando man `vrrpadm`(1M).

Debe tener la autorización `solaris.network.vrrp`, que es parte del perfil de gestión de redes, para configurar el enrutador VRRP.

Nota - La operación de sólo lectura iniciada por el comando `vrrpadm show-router` no requiere autorización `solaris.network.vrrp`.

Atención - Cuando se utilizan los VRRP con el filtro IP empaquetado de Oracle Solaris, se debe comprobar si se permite el tráfico IP entrante o saliente para la dirección multidifusión estándar del VRRP, `224.0.0.18/32` mediante el comando `ipfstat -io`. Si no se permite el tráfico, tanto los enrutadores VRRP maestros y de la copia de seguridad tendrán el estado `MASTER`. Por lo tanto, debe agregar las reglas correspondientes a la configuración de filtro IP para cada enrutador VRRP. Para obtener más información, consulte “Resolución de problemas con VRRP y el filtro IP empaquetado de Oracle Solaris” de “Resolución de problemas de administración de redes en Oracle Solaris 11.2 ”.

Creación de una VNIC del VRRP para el VRRP de la capa 2

Las VNIC son interfaces de red virtuales configuradas en la parte superior de un adaptador de red física del sistema y son componentes fundamentales de la virtualización de la red. Una interfaz física puede tener más de una VNIC. Para obtener más información acerca de las VNIC, consulte “Gestión de virtualización de red y recursos de red en Oracle Solaris 11.2 ”.

Cada enrutador VRRP de la capa 2 requiere una VNIC del VRRP especial. Utilice la siguiente sintaxis de comando:

```
# dladm create-vnic [-t] [-R root-dir] -l link [-m vrrp -V VRID -A \
{inet | inet6}] [-v VLAN-ID] [-p prop=value[,...]] VNIC
```

Este comando crea una VNIC con una dirección MAC de enrutador virtual definida por la especificación del VRRP. Utilice el tipo de dirección VNIC `vrrp` para especificar el VRID y la familia de direcciones. La familia de direcciones es `inet` o `inet6`, que hace referencia a direcciones IPv4 o IPv6. Por ejemplo:

```
# dladm create-vnic -m vrrp -V 21 -A inet6 -l net0 vnic0
```

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

Nota - También puede crear una VNIC del VRRP mediante la opción `-f` con el comando `vrrpadm`. Para obtener más información, consulte “Creación de un enrutador VRRP” [37].

Creación de un enrutador VRRP

El comando `vrrpadm create-router` crea un enrutador VRRP de la capa 2 o la capa 3 con el VRID y la familia de direcciones junto con otros parámetros especificados. Para obtener más información, consulte la página del comando man `vrrpadm`(1M).

Para crear un enrutador VRRP, utilice la siguiente sintaxis:

```
# vrrpadm create-router [-T {l2 | l3}] [-f] -V VRID -I ifname \
-A [inet | inet6] [-a assoc-IPaddress] [-P primary-IPaddress] \
[-p priority] [-i adv-interval] [-o flags] router-name
```

`-T l2 | l3` Especifica el tipo del enrutador. Puede definir el tipo en uno de los siguientes valores. El valor predeterminado es `l2`.

- `l2`: enrutador VRRP del tipo capa 2

- `l3`: enrutador del tipo capa 3 del VRRP

`-f`
(VRRP de la capa 2 solamente) Especifica la creación de la VNIC del VRRP con un enrutador VRRP de la capa 2. Cuando especifica la opción `-f`, el comando `vrrpadm` comprueba si existe la VNIC del VRRP con el VRID y la familia de direcciones especificados. Se crea una VNIC del VRRP sólo si no existe ya. El sistema genera el nombre de la VNIC del VRRP con la convención de denominación: `vrrp-`*VRID_ifname_*`v`*4* | *6*. La `-f` no tiene ningún efecto cuando se crea un enrutador VRRP de la capa 3.

`-V` *VRID*
El identificador de enrutador virtual que define la VLAN si está asociado a la familia de direcciones.

`-I` *ifname*
La interfaz en la que se configura el enrutador VRRP. Para un VRRP de la capa 2, la interfaz puede ser un enlace físico, una VLAN o una agregación. Para un VRRP de la capa 3, la interfaz también puede incluir una interfaz IPMP, una interfaz mediante DHCP y una interfaz InfiniBand. Este enlace determina la LAN en el que se está ejecutando este enrutador VRRP.

`-A [inet | inet6]`
La familia de direcciones es `inet` o `inet6`, que hace referencia a direcciones IPv4 o IPv6.

`-a` *assoc-IPaddress*
Especifica la lista separada por comas de direcciones IP.

Puede especificar la dirección IP en cualquiera de los siguientes formatos:

- *IP-address*[/*prefix-length*]
- *hostname*[/*prefix-length*]
- `linklocal`

  Si especifica `linklocal`, se configura una dirección local de enlace IPv6 `vrrp` en función del VRID del enrutador virtual asociado. El formulario `linklocal` sólo se aplica a los enrutadores VRRP IPv6. Puede combinar la opción `-a` con la opción `-f` para que se cree la VNIC y se sondee automáticamente.

`-P` *primary-IPaddress*
Especifica la dirección IP principal del VRRP que se utiliza para enviar el anuncio del VRRP.

`-p` *priority*
La prioridad del enrutador VRRP especificado utilizada para la selección del maestro. El valor predeterminado es `255`. El enrutador con el mayor valor de prioridad se selecciona como enrutador maestro.

`-i` *adv-interval*
El intervalo del anuncio en milisegundos. El valor predeterminado es `1000`.

-o *flags*	Los modos de aceptación y de preferencia del enrutador VRRP. Los valores son `preempt` o `un_preempt`, y `accept` o `no_accept`. De forma predeterminada, los modos de aceptación y de preferencia se configuran en `preempt` y `accept` respectivamente.
router-name	El *router-name* es el identificador único de este enrutador VRRP. Los caracteres permitidos en el nombre del enrutador son: los caracteres alfanuméricos (`a-z`, `A-Z`, `0-9`) y el carácter de subrayado (_). La longitud máxima de un nombre de enrutador es 31 caracteres.

EJEMPLO 4-1 Creación de un enrutador VRRP de la capa 2

El siguiente ejemplo muestra cómo crear un enrutador mediante un enlace de datos `net0`.

```
# dladm create-vnic -m vrrp -V 12 -A inet -l net0 vnic1
# vrrpadm create-router -V 12 -A inet -p 100 -I net0 l2router1
# vrrpadm show-router l2router1
NAME       VRID  TYPE   IFNAME AF   PRIO ADV_INTV MODE  STATE  VNIC
l2router1  12    L2     net0   IPv4 100  1000     e-pa- BACK   vnic1
```

Un enrutador VRRP de la capa 2`l2router1` se crea mediante un enlace de datos `net0` con el VRID y la familia de direcciones IPv412. Para obtener información sobre el comando `vrrpadm show-router`, consulte “Visualización de las configuraciones del enrutador VRRP de la capa 2 y la capa 3” [42].

EJEMPLO 4-2 Creación de un enrutador VRRP de la capa 3

El siguiente ejemplo muestra cómo crear un enrutador VRRP de la capa 3 mediante una interfaz IPMP denominada `ipmp0`.

```
# vrrpadm create-router -V 6 -I ipmp0 -A inet -T l3 l3router1
# vrrpadm show-router
NAME      VRID TYPE IFNAME AF   PRIO ADV_INTV MODE  STATE VNIC
l3router1 6    L3   ipmp0  IPv4 255  1000     eopa- INIT  --
```

Un enrutador VRRP de la capa 3`l3router1` se crea mediante una interfaz IPMP `ipmp0` con el VRID y la familia de direcciones IPv4 `6`. Para obtener información sobre el comando `vrrpadm show-router`, consulte “Visualización de las configuraciones del enrutador VRRP de la capa 2 y la capa 3” [42].

Configuración de la dirección IP virtual para enrutadores VRRP de la capa 2 y la capa 3

Para configurar la dirección IP para un enrutador VRRP de la capa 2, debe configurar la dirección IP virtual del tipo `vrrp` mediante una VNIC del VRRP asociado con él.

Para configurar la dirección IP virtual para un enrutador VRRP de la capa 3, debe utilizar una dirección IP del tipo `vrrp` en la misma interfaz IP mediante la cual se configura el enrutador VRRP de la capa 3.

Nota - Para configurar una dirección IPv6, debe crear la VNIC de VRRP o el enrutador VRRP de L· mediante la especificación de la familia de direcciones del enrutador, como `inet6`.

Para configurar una dirección IP virtual para un enrutador VRRP, utilice la siguiente sintaxis:

```
# ipadm create-addr [-t] -T vrrp [-a local=addr[/prefix-length]] \
 [-n router-name].... addr-obj | interface
```

`-t`	Especifica que la dirección configurada es temporal y que los cambios se aplican sólo a la configuración activa.
`-T vrrp`	Especifica que la dirección configurada es del tipo `vrrp`.
`-n` *router-name*	La opción `-n` *router-name* es opcional para un enrutador VRRP de la capa 2 porque el nombre del enrutador VRRP se puede derivar de la VNIC del VRRP en la cual están configuradas las direcciones IP.

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

Nota - También puede configurar las direcciones IP virtuales mediante el uso de la opción `-a` del comando `vrrpadm`. Para obtener más información, consulte “Creación de un enrutador VRRP” [37].

EJEMPLO 4-3 Configuración de dirección IP virtual para un enrutador VRRP de la capa 2

Puede utilizar la dirección IP del tipo `vrrp` para configurar las direcciones IP virtuales para un enrutador VRRP de la capa 2. El siguiente ejemplo muestra cómo crear la dirección IP virtual para `l2router1`.

```
# ipadm create-ip vrrp_vnic1
# ipadm create-addr -T vrrp -n l2router1 -a 192.168.82.8/24 vrrp_vnic1/vaddr1
```

El siguiente ejemplo muestra cómo crear una dirección IP local de enlace IPv6 `vrrp` para `V6vrrp_vnic1/vaddr1`.

```
# ipadm create-ip V6vrrp_vnic1
# ipadm create-addr -T vrrp V6vrrp_vnic1/vaddr1
```

Para configurar la dirección IP local de enlace IPv6 `vrrp` para un enrutador VRRP, no necesita especificar la dirección local. Una dirección IP local de enlace IPv6 `vrrp` se crea según el tipo de VRID del enrutador VRRP asociado.

EJEMPLO 4-4 Configuración de dirección IP virtual para un enrutador VRRP de la capa 3

El siguiente ejemplo muestra cómo configurar la dirección IP virtual para `l3router1`.

```
# ipadm create-ip ipmp0
# ipadm create-addr -T vrrp -n l3router1 -a 172.16.82.8/24 ipmp0/vaddr1
```

El siguiente ejemplo muestra cómo configurar una dirección IP local de enlace IPv6 `vrrp` para el enrutador VRRP de la capa 3`l3V6router1`.

```
# ipadm create-ip ipmp1
# ipadm create-addr -T vrrp -n l3V6router1 ipmp1/vaddr0
```

Activación y desactivación de un enrutador VRRP

El enrutador VRRP se activará de manera predeterminada al crearlo por primera vez. Puede desactivar un enrutador VRRP y volver a activarlo. La interfaz mediante la cual se crea el enrutador VRRP (especificada con la opción `-I` cuando se crea el enrutador con `vrrpadm create-router`) debe existir cuando se activa el enrutador. De lo contrario, falla la activación. Para un enrutador VRRP de la capa 2, si la VNIC del VRRP del enrutador no existe, el enrutador no es eficaz. La sintaxis es la siguiente:

```
# vrrpadm enable-router router-name
```

En cualquier momento, es posible que necesite desactivar temporalmente un enrutador VRRP para realizar cambios de configuración y, luego, volver a activarlo. La sintaxis para desactivar un enrutador es la siguiente:

```
# vrrpadm disable-router router-name
```

Modificación de un enrutador VRRP

El comando `vrrpadm modify-router` cambia la configuración de un enrutador VRRP especificado. Puede modificar la prioridad, el intervalo de anuncio, el modo de preferencia y el modo de aceptación del enrutador. La sintaxis es la siguiente:

```
# vrrpadm modify-router [-p priority] [-i adv-interval] [-o flags] router-name
```

Visualización de las configuraciones del enrutador VRRP de la capa 2 y la capa 3

El comando `vrrpadm show-router` muestra la configuración y el estado de un enrutador VRRP especificado. Para obtener más información, consulte la página del comando man `vrrpadm`(1M). La sintaxis es la siguiente:

```
# vrrpadm show-router [-P | -x] [-p] [-o field[,...]] [router-name]
```

EJEMPLO 4-5 Visualización de la configuración del enrutador VRRP de la capa 2

Los siguientes ejemplos muestra el resultado del comando `vrrpadm show-router`.

```
# vrrpadm show-router vrrp1
NAME VRID TYPE  IFNAME  AF   PRIO ADV_INTV MODE  STATE  VNIC
vrrp1 1   L2    net1    IPv4 100  1000     e-pa- BACK   vnic1
```

`NAME` Nombre del enrutador VRRP.

`VRID` VRID del enrutador VRRP.

`TYPE` El tipo de enrutador VRRP, que es de la capa 2 o la capa 3.

`IFNAME` La interfaz en la que se configura el enrutador VRRP. Para un enrutador VRRP de la capa 2, la interfaz puede ser una Ethernet física, una VLAN o una agregación.

`AF` La familia de direcciones del enrutador VRRP. Puede ser IPv4 o IPv6.

`PRIO` La prioridad del enrutador VRRP, que se utiliza para la selección del maestro.

`ADV_INTV` El intervalo del anuncio se muestra en milisegundos.

`MODE` Un conjunto de indicadores que están asociados con el enrutador VRRP e incluyen los siguientes valores posibles:

- `e`: especifica que el enrutador está activado.
- `p`: especifica que el modo es `preempt`.
- `a`: especifica que el modo es `accept`.
- `o`: especifica que el enrutador es el propietario de la dirección virtual.

`STATE` El estado actual del enrutador VRRP. Los valores posibles son: `INIT` (inicializar), `BACK` (copia de seguridad) y `MAST` (maestro).

En este ejemplo, se muestra la información sobre el enrutador VRRP especificado `vrrp1`.

```
# vrrpadm show-router -x vrrp1
NAME  STATE PRV_STAT STAT_LAST VNIC  PRIMARY_IP VIRTUAL_IPS
vrrp1 BACK  MAST     1m17s     vnic1 10.0.0.100 10.0.0.1
```

`PRV_STAT` El estado anterior del enrutador VRRP.

`STAT_LAST` Tiempo desde la última transición de estado.

`PRIMARY_IP` La dirección IP principal seleccionada por el enrutador VRRP.

`VIRTUAL_IPS` Direcciones IP virtuales configuradas en el enrutador VRRP.

En este ejemplo, se muestra información adicional sobre el enrutador, como la dirección IP principal seleccionada por el enrutador VRRP, la dirección IP virtual configurada en el enrutador VRRP y el estado anterior del VRRP.

```
# vrrpadm show-router -P vrrp1
NAME  PEER       P_PRIO  P_INTV  P_ADV_LAST  M_DOWN_INTV
vrrp1 10.0.0.123 120     1000    0.313s      3609
```

`PEER` La dirección IP principal del enrutador VRRP del igual.

`P_PRIO` La prioridad del enrutador VRRP equivalente, que forma parte del anuncio recibido desde el igual.

`P_INTV` El intervalo de anuncio (en milisegundos), que forma parte de los anuncios recibidos del igual.

`P_ADV_LAST` Tiempo desde el último anuncio recibido del igual.

`M_DOWN_INTV` Intervalo (en milisegundos) después de que el enrutador maestro se declara apagado.

La opción `-P` se utiliza sólo cuando el enrutador VRRP se encuentra en el estado de copia de seguridad.

EJEMPLO 4-6 Visualización del enrutador VRRP de la capa 3 en un sistema

```
# vrrpadm show-router
NAME   VRID  TYPE  IFNAME  AF    PRIO  ADV_INTV  MODE   STATE   VNIC
l3vr1  12    L3    net1    IPv6  255   1000      eopa-  INIT    –
```

En este ejemplo, el enrutador VRRP de la capa 3 `l3vr1`se configurada mediante la interfaz `net1`.

Visualización de direcciones IP que están asociadas con enrutadores VRRP

Puede mostrar la dirección IP asociada con un enrutador VRRP mediante el comando `ipadm show-addr`. El campo `ROUTER` en el resultado del comando `ipadm show-addr` muestra el nombre del enrutador VRRP que está asociado con un tipo de dirección IP específico `vrrp`.

Para la dirección de un enrutador IP del tipo `vrrp` de un VRRP de la capa 2, el nombre del enrutador VRRP se deriva de la VNIC del VRRP mediante la cual se configura la dirección IP. Si se emite el comando `ipadm show-addr` antes de crear el enrutador de la capa 2 para la VNIC del VRRP, el campo `ROUTER` muestra `?`. Para la dirección IP del tipo `vrrp` de un VRRP de la capa 3, el campo `ROUTER` siempre muestra el nombre del enrutador especificado. Para otras direcciones IP, el campo `ROUTER` no es aplicable y no se muestra `--`.

EJEMPLO 4-7 Visualización de direcciones IP que están asociadas con enrutadores VRRP

```
# ipadm show-addr -o addrobj,type,vrrp-router,addr
ADDROBJ              TYPE     VRRP-ROUTER   ADDR
lo0/v4               static   --               127.0.0.1/8
net1/p1              static   --               192.168.11.10/24
net1/v1              vrrp     l3router1        192.168.81.8/24
vrrp_vnic1/vaddr1    vrrp     l2router1        192.168.82.8/24
lo0/v6               static   --               ::1/128
```

En este ejemplo, `l3router1` está asociado con `vrrp` dirección IP del tipo `192.168.81.8/24` y `l2router1` está asociado con `vrrp` dirección IP del tipo `192.168.82.8/24`.

El resultado proporciona la siguiente información:

`ADDROBJ` El nombre del objeto de dirección.

`TYPE` El tipo de objeto de dirección, que puede ser uno de los siguientes:

- `from-gz`
- `static`

- `dhcp`
- `addrconf`
- `vrrp`

`VRRP-ROUTER` El nombre del enrutador VRRP.

`ADDR` La dirección numérica IPv4 o IPv6.

Supresión de un enrutador VRRP

El comando `vrrpadm delete-router` suprime un enrutador VRRP especificado. La sintaxis es la siguiente:

```
# vrrpadm delete-router router-name
```

Nota - La VNIC del VRRP, la dirección IP del tipo `vrrp`y la dirección IP principal que se crean al usar las opciones `-f`, `-a`, `-P` del comando `vrrpadm create-router` respectivamente no se suprimen como resultado del comando `vrrpadm delete-router`. Debe suprimirlos explícitamente mediante los comandos correspondientes `ipadm` y `dladm`.

Control de mensajes NDP y ARP gratuitos

Cuando un enrutador de copia de seguridad se convierte en enrutador VRRP maestro, el enrutador VRRP configura un indicador en todas las direcciones IP virtuales asociadas con el enrutador maestro y, por lo tanto, las direcciones IP virtuales están protegidas. Si no existen conflictos para las direcciones IP virtuales, se envían varios mensajes de anuncio ARP y de vecino gratuitos para anunciar la nueva asignación entre la dirección IP virtual y la dirección MAC del nuevo maestro.

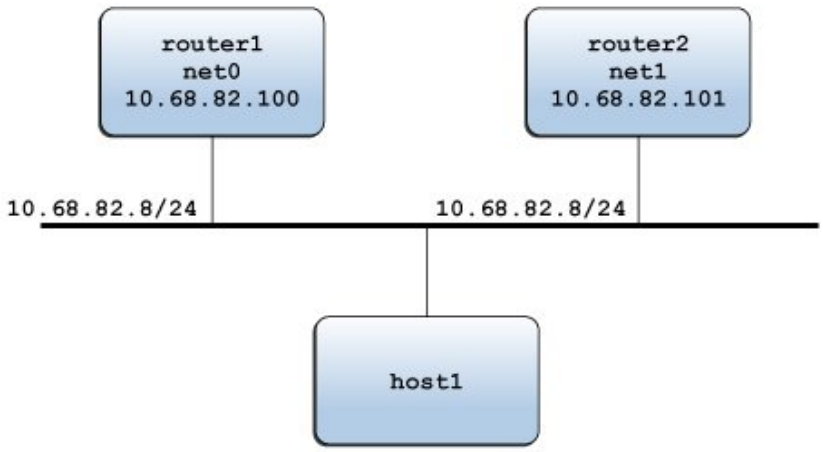
Para controlar el número de mensajes enviados y el intervalo entre el anuncio de mensajes, puede utilizar las siguientes propiedades del protocolo IP:

- `arp_publish_count`
- `arp_publish_interval`
- `ndp_unsolicit_count`
- `ndp_unsolicit_interval`

Para obtener más información sobre las propiedades del protocolo IP, consulte “Parámetros ajustables IP relacionados con la detección de direcciones duplicadas” de “Manual de referencia de parámetros ajustables de Oracle Solaris 11.2 ”.

Caso de uso: configuración de un enrutador VRRP de la capa 2

En la figura siguiente, se muestra una configuración típica de VRRP.



En este ejemplo, la dirección IP `10.68.82.8` se configura como puerta de enlace predeterminada para `host1`. Esta dirección IP es la dirección IP virtual que se protege mediante el enrutador virtual que consta de dos enrutadores VRRP: `router1` y `router2`. En un momento dado, sólo uno de los dos enrutadores puede funcionar como enrutador maestro y asumir las responsabilidades de enrutador virtual y reenviar paquetes procedentes de `host1`.

Asuma que el enrutador virtual del VRID es `12`. En los siguientes ejemplos, se muestran los comandos que se usan para configurar la configuración VRRP de ejemplo en `router1` y `router2`. `router1` es el propietario de la dirección IP virtual `10.68.82.8` y su prioridad es el valor predeterminado (`255`). `router2` es el enrutador en modo de espera, cuya prioridad es `100`.

Para obtener más información sobre los comandos que se utilizan para configurar el VRRP, consulte las páginas del comando man `vrrpadm`(1M), `dladm`(1M) y `ipadm`(1M).

Para `router1`:

1. Instale el paquete VRRP.

   ```
   # pkg install vrrp
   ```

2. Cree la VNIC `vnic0` mediante `net0` con el valor VRID como `12`.

```
# dladm create-vnic -m vrrp -V 12 -A inet -l net0 vnic0
```

3. Cree un enrutador VRRP `vrrp1` mediante `net0`.

```
# vrrpadm create-router -V 12 -A inet -I net0 vrrp1
```

4. Configure las interfaces IP `vnic0` y `net0`.

```
# ipadm create-ip vnic0

# ipadm create-addr -T vrrp -a 10.68.82.8/24 vnic0/router1

# ipadm create-ip net0

# ipadm create-addr -T static -a 10.68.82.100/24 net0/router1
```

5. Muestre la información del enrutador para `vrrp1`.

```
# vrrpadm show-router -x vrrp1
NAME  STATE   PRV_STAT STAT_LAST  VNIC  PRIMARY_IP    VIRTUAL_IPS
vrrp1 MASTER  INIT     14.444s    vnic0 10.68.82.100  10.68.82.8
```

Del mismo modo, para `router2`:

1. Cree la VNIC `vnic1` mediante `net1` con el valor VRID como `12`.

```
# dladm create-vnic -m vrrp -V 12 -A inet -l net1 vnic1
```

2. Cree un enrutador VRRP `vrrp2` mediante `net1`.

```
# vrrpadm create-router -V 12 -A inet -I net1 -p 100 vrrp2
```

3. Configure las interfaces IP en `vnic1` y `net1`.

```
# ipadm create-ip vnic1

# ipadm create-addr -T vrrp -a 10.68.82.8/24 vnic1/router2

# ipadm create-ip net1

# ipadm create-addr -T static -a 10.68.82.101/24 net1/router2
```

4. Muestre la información del enrutador para `vrrp2`.

```
# vrrpadm show-router -x vrrp2
NAME  STATE    PRV_STAT  STAT_LAST  VNIC  PRIMARY_IP    VIRTUAL_IPS
vrrp2 BACKUP   INIT      2m32s      vnic1 10.68.82.101  10.68.82.8
```

Utilizando la configuración de `router1` como ejemplo, debe configurar al menos una dirección IP en `net0`. Esta dirección IP de `router1` es la dirección IP principal, que se utiliza para enviar los paquetes de anuncios VRRP.

```
# vrrpadm show-router -x vrrp1
NAME  STATE   PRV_STAT STAT_LAST  VNIC  PRIMARY_IP    VIRTUAL_IPS
```

```
vrrp1 MASTER  INIT     14.444s    vnic1 10.68.82.100  10.68.82.8
```

♦ ♦ ♦ CAPÍTULO 5

Descripción general de un equilibrador de carga integrado

En este capítulo se describen los modos y componentes del ILB en los cuales opera el ILB, como el modo de retorno de servidor directo (DSR, Direct Server Return) y el modo de traductor de direcciones de red (DSR, Network Address Translator).

Este capítulo se divide en los siguientes apartados:

- “Componentes del ILB” [49]
- “Modos de funcionamiento del ILB” [50]
- “Funcionamiento del ILB” [55]

Para obtener más información sobre el ILB, consulte “Descripción general del equilibrador de carga integrado” [13].

Componentes del ILB

EL ILB se gestiona mediante el servicio `svc:/network/loadbalancer/ilb:default` de la utilidad de gestión de servicios (SMF). Para obtener más información sobre la SMF, consulte “Gestión de los servicios del sistema en Oracle Solaris 11.2 ”. Los tres componentes principales del ILB son:

- La interfaz de línea de comandos (CLI, Command-Line Interface) `ilbadm`: puede utilizar la CLI para configurar las reglas del equilibrio de carga, realizar comprobaciones de estado opcionales y ver las estadísticas.
- Biblioteca de configuración `libilb`: `ilbadm` y las aplicaciones de terceros pueden utilizar las funciones implementadas en `libilb` para la administración del ILB.
- Daemon `ilbd`: este daemon realiza las siguientes tareas:
  - Gestiona la configuración persistente después de cada reinicio y cada actualización de paquetes
  - Proporciona acceso serie al módulo del núcleo del ILB mediante el procesamiento de la información de configuración y su posterior envío al módulo del núcleo del ILB para su ejecución.

- Realiza comprobaciones de estado y envía los resultados al módulo del núcleo del ILB para que la distribución de la carga se ajuste de manera adecuada.

Modos de funcionamiento del ILB

El ILB admite los modos de funcionamiento DSR y NAT sin estado para IPv4 e IPv6 en topologías de segmento único y de segmento doble.

Modo retorno de servidor directo

En modo DSR, el ILB equilibra las solicitudes entrantes enviadas a los servidores back-end, pero permite que el tráfico devuelto de los servidores a los clientes las omita. Sin embargo, si configura el ILB para que sea utilizado como enrutador para el servidor back-end, la respuesta del servidor back-end al cliente se distribuye por medio del sistema que ejecuta el ILB. La implementación actual de DSR por parte del ILB no proporciona el seguimiento de la conexión TCP, es decir, no tiene ningún estado. Con el DSR sin estado, el ILB no guarda ninguna información del estado de los paquetes procesados, salvo estadísticas básicas. Al estar sin estado, el rendimiento es comparable con el rendimiento de reenvío de IP normal. El modo DSR es más adecuado para los protocolos sin conexión.

Ventajas:

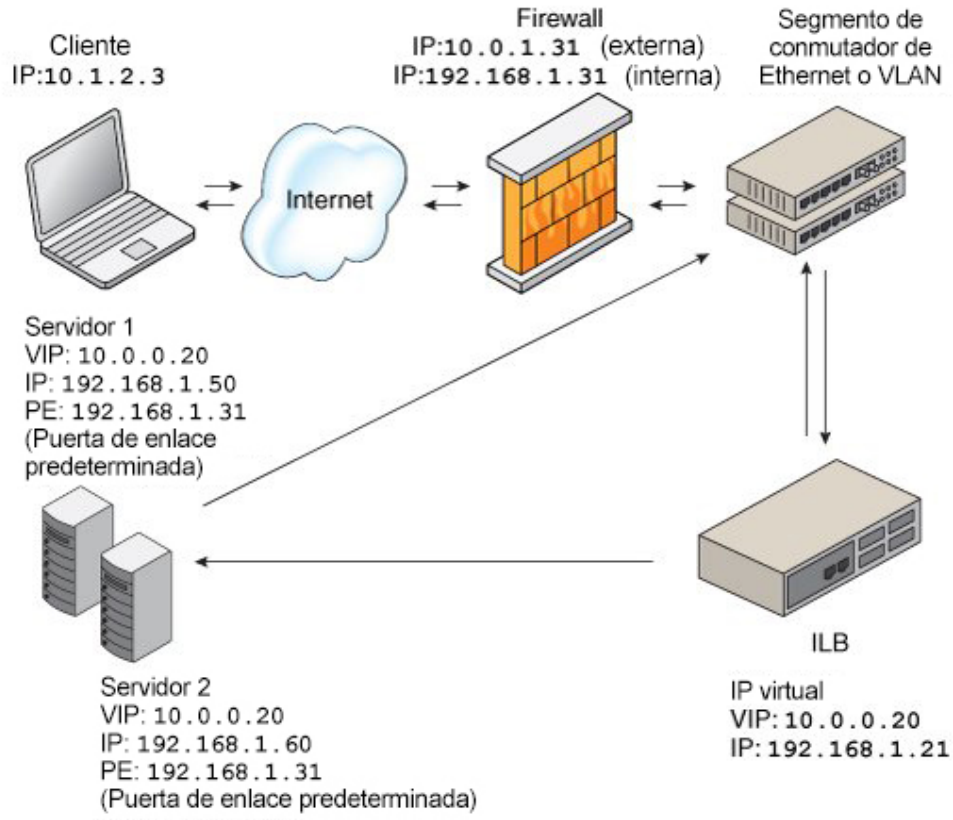
- El DSR proporciona un mejor rendimiento que NAT porque se modifica sólo la dirección MAC de destino de paquetes, y los servidores responden directamente a los clientes.
- Hay transparencia total entre el servidor y el cliente. Los servidores ven una conexión directamente desde la dirección IP del cliente y responden al cliente por medio de la puerta de enlace predeterminada.

Desventajas:

- El servidor back-end debe responder a su propia dirección IP (para las comprobaciones de estado) y a la dirección IP virtual (para el tráfico con equilibrio de carga).
- Estar sin estado, agregar o quitar servidores hace que se interrumpa la conexión.

En la figura siguiente, se muestra la implementación del ILB en el modo DSR.

FIGURA 5-1 Topología de retorno de servidor directo



En esta figura, ambos servidores back-end están en la misma subred (`192.168.1.0/24`) que la caja del ILB. Los servidores también están conectados al enrutador para que puedan responder directamente a los clientes después de recibir una solicitud reenviada por la caja del ILB.

Modo de traducción de direcciones de red

El ILB utiliza NAT en modo independiente estrictamente para una función de equilibrio de carga. En este modo, el ILB vuelve a escribir la información de encabezado y maneja el tráfico entrante y saliente. El ILB funciona tanto en el modo half-NAT como en el modo full-NAT. Sin embargo, full-NAT también reescribe la dirección IP de origen, lo que hace que para el servidor

parezca que todas las conexiones se originan del equilibrador de carga. NAT proporciona seguimiento de conexión TCP (es decir que tiene estado). El modo NAT proporciona una seguridad adicional y es más adecuado para el protocolo de transferencia de hipertexto (HTTP) o el tráfico de Secure Sockets Layer (SSL).

Ventajas:

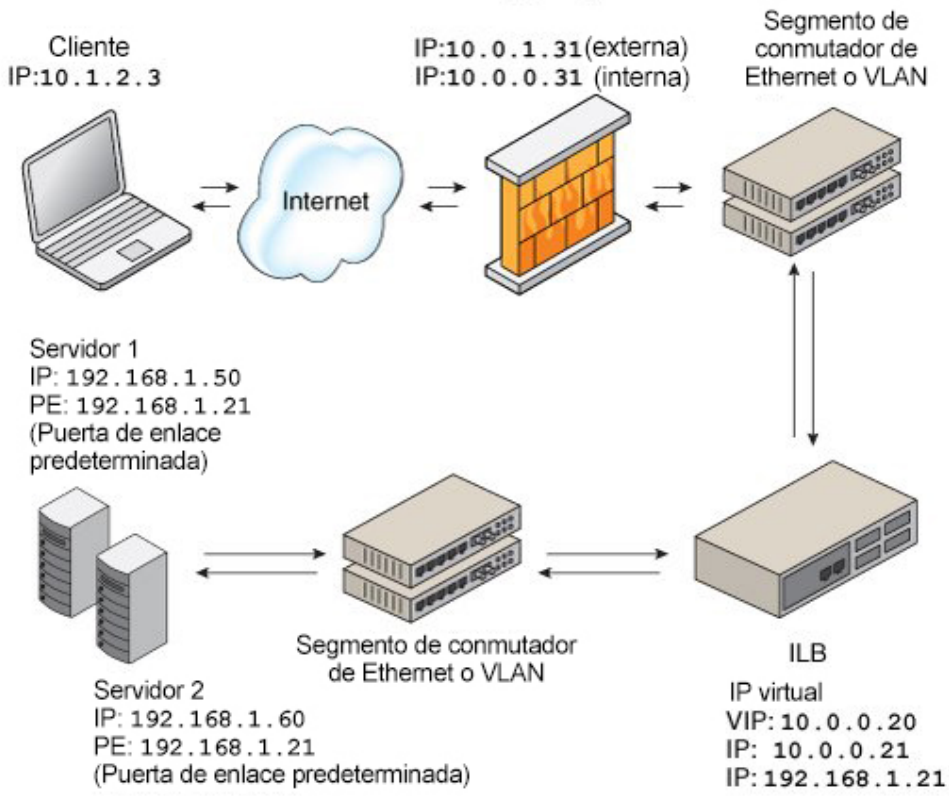
- Funciona con todos los servidores back-end si se cambia la puerta de enlace predeterminada para que apunte al equilibrador de carga
- Es posible agregar o quitar servidores sin interrumpir la conexión porque el equilibrador de carga mantiene el estado de conexión

Desventajas:

- El rendimiento puede ser menor que en DSR dado que el procesamiento implica la manipulación del encabezado IP, y los servidores envían respuestas al equilibrador de carga
- Todos los servidores back-end deben utilizar el equilibrador de carga como puerta de enlace predeterminada

La implementación general del modo NAT se muestra en la figura siguiente.

FIGURA 5-2 Topología de Traducción de direcciones de red



En este caso, todas las solicitudes realizadas a la dirección VIP utilizan el ILB y se reenvían a los servidores back-end. Todas las respuestas de los servidores back-end pasan por el ILB para NAT.

Atención - La ruta de código NAT que se implementa en ILB difiere de la ruta de código que se implementa en la función de filtro IP de Oracle Solaris. *No* utilice ambas rutas de código a la vez.

Modo de equilibrio de carga half-NAT

En el modo half-NAT de funcionamiento del ILB, el ILB reescribe sólo la dirección IP de destino en el encabezado de los paquetes. Si está utilizando la implementación NAT parcial, no puede conectarse a una dirección IP virtual (VIP) del servicio desde la misma subred en la que reside el servidor. En la tabla siguiente, se muestran las direcciones IP de los paquetes que fluyen entre el cliente y el ILB, y entre el ILB y los servidores back-end.

TABLA 5-1 Flujo de solicitud y flujo de respuesta para la implementación de half-NAT cuando el servidor y el cliente están en redes diferentes

	Flujo de solicitud	Dirección IP de origen	Dirección IP de destino
1.	Cliente –> ILB	Cliente	VIP de ILB
2.	ILB –> Servidor	Cliente	Servidor
	Flujo de respuesta		
3.	Servidor –> ILB	Servidor	Cliente
4.	ILB –> Cliente	VIP de ILB	Cliente

Si conecta el sistema cliente a la misma red que los servidores, el servidor en cuestión responde directamente al cliente y el cuarto paso en la tabla no se produce. Por lo tanto, la dirección IP de origen para respuesta del servidor al cliente no es válida. Cuando el cliente envía una solicitud de conexión al equilibrador de carga, la respuesta surge del servidor de destino. Desde este punto en adelante, la pila IP del cliente descarta correctamente todas las respuestas. En ese caso, el flujo de solicitud y el flujo de respuesta continúan como se muestra en la tabla siguiente.

TABLA 5-2 Flujo de solicitud y flujo de respuesta para la implementación de half-NAT cuando el servidor y el cliente están en la misma red

	Flujo de solicitud	Dirección IP de origen	Dirección IP de destino
1.	Cliente –> ILB	Cliente	VIP de ILB
2.	ILB –> Servidor	Cliente	Servidor
	Flujo de respuesta		
3.	Servidor –> Cliente	Servidor	Cliente

Modo de equilibrio de carga full-NAT

En la implementación de full-NAT del funcionamiento del ILB, las direcciones IP de origen y destino se reescriben para garantizar que el tráfico pase por el equilibrador de carga en ambas direcciones. El modo full-NAT hace que sea posible conectarse a la dirección VIP de la misma subred en que están los servidores.

En la tabla siguiente, se muestran las direcciones IP de los paquetes que fluyen entre un cliente y el ILB, y entre el ILB y un servidor back-end que use el modo full-NAT. No se requiere ninguna ruta predeterminada especial que use la caja del ILB en los servidores. Tenga en cuenta que el modo full-NAT requiere que el administrador reserve una dirección IP o un grupo de ellas para que el ILB las use como direcciones de origen para comunicarse con los servidores back-end. Suponga que las direcciones utilizadas pertenecen a la subred C. En este escenario, el ILB se comporta como proxy.

TABLA 5-3 Flujo de solicitud y flujo de respuesta para la implementación de full-NAT

	Flujo de solicitud	**Dirección IP de origen**	**Dirección IP de destino**
1.	Cliente –> ILB	Cliente	VIP de ILB
2.	ILB –> Servidor	Dirección de interfaz del equilibrador de carga (subred C)	Servidor
	Flujo de respuesta		
3.	Servidor –> ILB	Servidor	Dirección de interfaz del ILB (subred C)
4.	ILB –> Cliente	VIP de ILB	Cliente

Funcionamiento del ILB

En esta sección se describe el proceso del ILB, que implica procesar una solicitud de un cliente a la VIP, enviar la solicitud a un servidor back-end y procesar la respuesta.

El procesamiento de paquetes de cliente a servidor incluye los siguientes pasos:

1. EL ILB recibe una solicitud entrante enviada por el cliente a una dirección VIP y hace coincidir la solicitud con una regla de equilibrio de carga.
2. Si el ILB encuentra una regla de equilibrio de carga coincidente, utiliza un algoritmo de equilibrio de carga para reenviar la solicitud a un servidor back-end acorde al modo de funcionamiento.
   - En el modo DSR, el ILB reemplaza el encabezado MAC de la solicitud entrante con el encabezado MAC del servidor back-end seleccionado.
   - En el modo half-NAT, el ILB sustituye la dirección IP de destino y el número de puerto de protocolo de transporte de la solicitud entrante con la del servidor back-end seleccionado.
   - En el modo NAT completa, el ILB reemplaza la dirección IP de origen y el número de puerto del protocolo de transporte de la solicitud entrante con la dirección de origen NAT de la regla de equilibrio de carga. El ILB también reemplaza la dirección IP de destino y el número de puerto del protocolo de transporte de la solicitud entrante con la del servidor back-end seleccionado.
3. El ILB reenvía la solicitud entrante modificada para el servidor back-end seleccionado.

El procesamiento de paquetes de servidor a cliente incluye los siguientes pasos:

1. El servidor back-end envía una respuesta al ILB en respuesta a la solicitud entrante desde el cliente.
2. La acción del ILB después de recibir la respuesta del servidor back-end se basa en el modo de operación.
   - En el modo DSR, la respuesta del servidor back-end omite el ILB y va directamente al cliente. Sin embargo, si el ILB también se utiliza como enrutador para el servidor back-end, la respuesta del servidor back-end al cliente se distribuye por medio del sistema que ejecuta el ILB.
   - En los modos half-NAT y full-NAT, el ILB compara la respuesta del servidor back-end con la solicitud entrante y reemplaza la dirección IP y el número de puerto del protocolo de transporte modificados con los de la solicitud entrante original. El ILB reenvía la respuesta al cliente.

♦ ♦ ♦ CAPÍTULO 6

Configuración y gestión del equilibrador de carga integrado

El ILB se configura en las capas L3 y L4 de la pila de protocolos de la red. En este capítulo se describen las tareas para instalar el ILB, activar o desactivar el ILB, definir grupos de servidores y servidores back-end en ILB, y exportar e importar configuraciones del ILB mediante el comando `ilbadm`. Para obtener más información, consulte la página del comando man `ilbadm`(1M). Para obtener más información sobre la configuración del ILB de alta disponibilidad, consulte el Capítulo 7, Configuración del ILB para Alta Disponibilidad.

Para obtener información sobre cómo implementar un equilibrador de carga integrado de Oracle Solaris, consulte Implementación del equilibrador de carga integrado de Oracle Solaris en 60 minutos (http://www.oracle.com/technetwork/systems/hands-on-labs/hol-deploy-ilb-60mmin-2137812.html). Para obtener información sobre cómo agregar alta disponibilidad a la aplicación mediante Oracle Solaris Zones e ILB en Oracle Solaris, consulte Cómo configurar una aplicación de equilibrio de carga en dos Oracle Solaris Zones. (http://www.oracle.com/technetwork/articles/servers-storage-admin/loadbalancedapp-1653020.html).

Este capítulo se divide en los siguientes apartados:

Instalación del ILB

El ILB tiene instalaciones de núcleo y espacio de usuario. La instalación del núcleo del ILB se realiza automáticamente como parte de la instalación de Oracle Solaris. Sin embargo, debe realizar la instalación de espacio de usuario del ILB mediante el siguiente comando:

```
# pkg install ilb
```

Configuración del ILB mediante la interfaz de línea de comandos

La interfaz de línea de comandos (CLI, Command-Line Interface) del ILB se encuentra en el directorio `/usr/sbin/ilbadm`. La CLI incluye subcomandos para configurar las reglas del equilibrio de carga, los grupos de servidores y las comprobaciones de estado. También incluye subcomandos para mostrar estadísticas y ver los detalles de la configuración. Debe configurar la autorización de usuario para los subcomandos de configuración del ILB, excepto los subcomandos de visualización, como `ilbadm show-rule`, `ilbadm show-server` y `ilbadm show-healthcheck`. Debe contar con la autorización de control de acceso basado en roles (RBAC, role-based access control) `solaris.network.ilb.config` para ejecutar los siguientes subcomandos de configuración del ILB.

- Para descubrir cómo asignar la autorización a un usuario existente, consulte Capítulo 3, “Asignación de derechos en Oracle Solaris” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.
- También puede proporcionar la autorización al crear una cuenta de usuario nueva en el sistema.

  En el siguiente ejemplo, se crea un usuario `ilbadm` con el ID de grupo `10`, el ID de usuario `1210` y la autorización para administrar el ILB en el sistema.

  ```
  # useradd -g 10 -u 1210 -A solaris.network.ilb.config ilbadmin
  ```

  El comando `useradd` agrega un usuario nuevo a los archivos `/etc/passwd`, `/etc/shadow` y `/etc/user_attr`. La opción `-A` asigna la autorización al usuario.

Los subcomandos se pueden dividir en dos categorías:

- **Subcomandos de configuración**: estos subcomandos le permiten realizar las siguientes tareas:
  - Crear y suprimir reglas de equilibrio de carga
  - Activar y desactivar reglas de equilibrio de carga
  - Crear y suprimir grupos de servidores
  - Agregar y eliminar servidores de un grupo de servidores
  - Activar y desactivar servidores back-end
  - Crear y suprimir las comprobaciones de estado para un grupo de servidores en una regla de equilibrio de carga

---

Nota - Debe tener privilegios para administrar los subcomandos de configuración. Para crear el rol adecuado y asignarlo a un usuario, consulte “Creación de roles” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

- **Ver subcomandos**: estos subcomandos le permiten realizar las siguientes tareas:
  - Ver las reglas de equilibrio de carga, los grupos de servidores y las comprobaciones de estado que están configuradas
  - Ver las estadísticas del reenvío de paquetes
  - Ver la tabla de conexión NAT
  - Ver los resultados de comprobación de estado
  - Ver la tabla de asignación de persistencia de sesiones

Nota - No se requieren privilegios para administrar los subcomandos de visualización.

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

Activación o desactivación del ILB.

En esta sección se describe cómo activar el ILB después de que se haya instalado o desactivado si no se requieren los servicios del ILB.

▼ Cómo activar el ILB

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. **Active el servicio de reenvío adecuado, IPv4 o IPv6, o ambos.**
   Este comando no produce ninguna salida cuando se ejecuta correctamente.

   ```
   # ipadm set-prop -p forwarding=on ipv4
   # ipadm set-prop -p forwarding=on ipv6
   ```

3. **Active el servicio del ILB.**

   ```
   # svcadm enable ilb
   ```

4. **Verifique que el servicio del ILB esté activado.**

   ```
   # svcs ilb
   ```

   Este comando muestra información sobre las instancias de servicio según está registrado en el repositorio de configuración de servicio.

▼ Cómo desactivar el ILB

Cuando los servicios del ILB no son necesarios, puede desactivarlo.

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. **Desactive el servicio del ILB.**

   ```
   # svcadm disable ilb
   ```

3. **Verifique que el servicio del ILB esté desactivado.**

   ```
   # svcs ilb
   ```

   Este comando muestra información sobre las instancias de servicio según está registrado en el repositorio de configuración de servicio.

Pasos siguientes Después de que se desactiva el servicio del ILB, debe desactivar el reenvío de IP si no es necesario.

Gestión de un ILB

Puede configurar un ILB mediante la definición de los grupos de servidores, la supervisión de comprobaciones de estado y la creación de reglas de ILB después de haber activado el ILB.

Los temas de esta sección son los siguientes:

Definición de grupos de servidores y servidores back-end en ILB

En esta sección se describe cómo crear un grupo de servidores del ILB y agregar servidores back-end al grupo de servidores. Cuando un servidor se agrega mediante los subcomandos `create-servergroup` o `add-server`, el sistema genera los ID de servidor. Los ID de servidor son únicos dentro del grupo de servidores. Para obtener más información sobre los subcomandos `ilbadm`, consulte la página del comando man `ilbadm`(1M).

Creación de un grupo de servidores del ILB

Para crear un grupo de servidores del ILB, primero identifique los servidores que se van a incluir en el grupo de servidores. Los servidores se pueden especificar mediante su nombre de host o dirección IP y puertos opcionales. A continuación, como administrador, ejecute el siguiente comando:

```
# ilbadm create-servergroup -s servers=server1,server2,server3  servergroup
```

Los ID de servidor único precedidos por un carácter de subrayado (_) se generan para cada servidor agregado.

Nota - Un servidor puede tener varios ID si pertenece a varios grupos de servidores.

Agregación de servidores back-end a un grupo de servidores del ILB

Para agregar un servidor back-end a un grupo de servidores, conviértase en administrador y ejecute el siguiente comando:

```
# ilbadm add-server -s server=server1[,server2...]  servergroup
```

En las especificaciones del servidor, se debe incluir un nombre de host o dirección IP. También, se puede incluir un puerto opcional o un intervalo de puertos. No se permiten las entradas de servidor con la misma dirección IP dentro de un grupo de servidores. Los ID de servidor único precedidos por un carácter de subrayado (_) se generan para cada servidor agregado.

Nota - Las direcciones IPv6 deben ir entre corchetes.

EJEMPLO 6-1 Creación de un grupo de servidores del ILB y agregación de servidores back-end

En el ejemplo siguiente, se crea un grupo de servidores denominado `webgroup`, con tres servidores back-end:

```
# ilbadm create-servergroup -s \
servers=192.168.89.11,192.168.89.12,192.168.89.13 webgroup
# ilbadm show-servergroup
SGNAME         SERVERID            MINPORT MAXPORT IP_ADDRESS
webgroup       _webgroup.0         --      --      192.168.89.11
webgroup       _webgroup.1         --      --      192.168.89.12
webgroup       _webgroup.2         --      --      192.168.89.13
```

El siguiente ejemplo crea un grupo de servidores denominado `webgroup1` y agrega tres servidores back-end al grupo de servidores.

```
# ilbadm create-servergroup webgroup1
# ilbadm add-server -s server=[2001:0db8:7::feed:6]:8080,\
[2001:0db8:7::feed:7]:8080,[2001:0db8:7::feed:8]:8080 webgroup1
```

Activación y desactivación de un servidor back-end en un grupo de servidores del ILB

Primero, identifique la dirección IP, el nombre de host o el ID de servidor del servidor back-end que desea volver a activar o desactivar. Debe asociar el grupo de servidores con una regla antes de que los servidores en el grupo de servidores se puedan activar o desactivar.

Un servidor puede tener varios ID si pertenece a varios grupos de servidores. Debe especificar un ID de servidor para volver a activar o desactivar el servidor para las reglas específicas asociadas con el ID de servidor.

- Para desactivar un servidor activado, escriba el siguiente comando:

  ```
  # ilbadm disable-server server1
  ```

  El servidor seleccionado, que está activado, se ha desactivado. El núcleo no reenvía tráfico a este servidor.
- Para volver a activar el servidor desactivado, escriba el siguiente comando:

  ```
  # ilbadm enable-server server1
  ```

  El servidor seleccionado, que está desactivado, se ha vuelto a activar.
- Para mostrar el estado del servidor, escriba el siguiente comando:

  ```
  # ilbadm show-server [[-p] -o field[,field...]] [rulename]
  ```

Nota - Un servidor muestra el estado Activado o Desactivado sólo cuando el grupo de servidores al que pertenece el servidor está asociado con una regla.

EJEMPLO 6-2 Reactivación y desactivación de un servidor back-end en un grupo de servidores del ILB

En el ejemplo siguiente, un servidor con ID de servidor `_websg.1` primero se desactiva y, a continuación, se reactiva:

```
# ilbadm enable-server _websg.1
```

```
# ilbadm disable-server _websg.1
```

Supresión de un servidor back-end de un grupo de servidores del ILB

Para eliminar un servidor back-end de un grupo de servidores del ILB o de todos los grupos de servidores, use el comando `ilbadm remove-server`. Primero, identifique el ID de servidor del servidor que desea eliminar de un grupo de servidores.

```
ilbadm show-servergroup -o all
```

El ID de servidor es un nombre único para la dirección IP asignada a un sistema cuando el servidor se agrega a un grupo de servidores.

A continuación, suprima el servidor.

```
# ilbadm remove-server -s server=server-ID server-group
```

Si el servidor está siendo utilizado por una regla NAT o half-NAT, desactive el servidor mediante el subcomando `disable-server` antes de la eliminación. Para obtener más información, consulte “Activación y desactivación de un servidor back-end en un grupo de servidores del ILB” [62]. Cuando se desactiva un servidor, éste entra en el estado de purga de conexión. Compruebe periódicamente la tabla NAT utilizando el comando `ilbadm show-nat` para ver si el servidor aún tiene conexiones. Una vez purgadas todas la conexiones (el servidor no se muestra en la salida del comando `show-nat`), puede eliminar el servidor. Para ello, use el comando `remove-server`.

Si se establece el valor de tiempo de espera `conn-drain`, el estado de purga de conexión se completa una vez concluido el período de espera. El valor predeterminado de tiempo de espera `conn-drain` es `0`, lo que significa que la purga de conexión espera hasta que una conexión se cierre correctamente.

EJEMPLO 6-3 Supresión de un servidor back-end de un grupo de servidores del ILB

En el siguiente ejemplo, se quita el servidor con ID de servidor `_sg1.2` del grupo de servidores `sg1`.

```
# ilbadm remove-server -s server=_sg1.2 sg1
```

Supresión de grupos de servidores del ILB

En esta sección se describe cómo suprimir un grupo de servidores del ILB. No puede suprimir un grupo de servidores que se utilizará en cualquier regla activa.

En primer lugar, visualice la información disponible sobre todos los grupos de servidores.

```
# ilbadm show-servergroup -o all
sgname      serverID       minport     maxport     IP_address
specgroup   _specgroup.0   7001        7001        192.168.68.18
specgroup   _specgroup.1   7001        7001        192.168.68.19
test123     _test123.0     7002        7002        192.168.67.18
test123     _test123.1     7002        7002        192.168.67.19
```

Escriba el siguiente comando:

```
# ilbadm delete-servergroup servergroup
```

Si el grupo de servidores está siendo utilizado por una regla activa, la supresión fallará.

En el siguiente ejemplo, se elimina el grupo de servidores denominado `webgroup`.

```
# ilbadm delete-servergroup webgroup
```

Supervisión de las comprobaciones de estado en ILB

El ILB proporciona los siguientes tipos de comprobaciones de estado del servidor opcionales:

- Sondeos de ping integrado
- Sondeos de TCP integrado
- Sondeos de UDP integrado
- Pruebas personalizadas proporcionadas por el usuario que se pueden ejecutar como comprobaciones de estado

De manera predeterminada, el ILB no realiza ninguna comprobación de estado. Puede especificar las comprobaciones de estado para cada grupo de servidores cuando crea una regla de equilibrio de carga. Solo se puede configurar una comprobación de estado por regla de equilibrio de carga. Siempre que un servicio virtual esté activado, las comprobaciones de estado del grupo de servidores asociado con el servicio virtual se inician automáticamente y se repiten periódicamente. Las comprobaciones de estado se detienen cuando se desactiva el servicio virtual. Los estados de la comprobación anterior no se conservan cuando el servicio virtual se vuelva a activar.

Cuando se especifica un TCP, UDP o sondeo de prueba personalizada para ejecutar una comprobación de estado, el ILB envía un sondeo de ping, de manera predeterminada, para establecer si se puede acceder al servidor antes de enviarle el TCP, UDP o sondeo de prueba personalizada. Si el sondeo de ping falla, el servidor correspondiente se desactiva con el estado de comprobación `unreachable`. Si el sondeo de ping se efectúa correctamente, pero el TCP, el UDP o el sondeo de prueba personalizada fallan, el servidor se desactivará con el estado de comprobación `dead`.

Puede desactivar el sondeo de ping predeterminado, excepto para el sondeo del UDP. El sondeo de ping es siempre el valor de sondeo predeterminado para las comprobaciones de estado del UDP.

Creación de una comprobación de estado

Puede crear una comprobación de estado y asignarla a un grupo de servidores al crear una regla de equilibrio de carga. En el siguiente ejemplo, se crean dos objetos de comprobación de estado, `hc1` y `hc-myscript`. La primera comprobación de estado utiliza el sondeo de TCP incorporado. La segunda comprobación de estado utiliza una prueba personalizada, `/var/tmp/my-script`.

```
# ilbadm create-healthcheck -h hc-timeout=3,\
hc-count=2,hc-interval=8,hc-test=tcp hc1
# ilbadm create-healthcheck -h hc-timeout=3,\
hc-count=2,hc-interval=8,hc-test=/var/tmp/my-script hc-myscript
```

Los argumentos son los siguientes:

`hc-timeout`	Especifica el tiempo de espera para considerar que la comprobación de estado ha fallado si no se completa.
`hc-count`	Especifica el número de intentos para ejecutar la comprobación de estado `hc-test`.
`hc-interval`	Especifica el intervalo entre dos comprobaciones de estado consecutivas. Para evitar el envío de sondeos a todos los servidores al mismo tiempo, el intervalo real es aleatorio entre `0.5 * hc-interval` y `1.5 * hc-interval`.
`hc-test`	Especifica el tipo de comprobación de estado. Puede especificar la comprobación de estado incorporada, como `tcp`, `udp` y `ping`, o la comprobación de estado externa, que debe estar especificada con el nombre de ruta completo.

Nota - La especificación del puerto para `hc-test` se define mediante la palabra clave `hc-port` en el subcomando `create-rule`. Para obtener más información, consulte la página del comando man `ilbadm`(1M).

Una prueba personalizada proporcionada por el usuario puede ser un código binario o una secuencia de comandos.

- La prueba puede residir en cualquier parte del sistema. Debe especificar la ruta absoluta al utilizar el subcomando `create-healthcheck`.

Si especifica la prueba (por ejemplo, `/var/tmp/my-script`) como parte de la especificación de comprobación de estado en el subcomando `create-rule`, el daemon `ilbd` realiza la bifurcación de un proceso y ejecuta la prueba, de la siguiente manera:

```
/var/tmp/my-script $1 $2 $3 $4 $5
```

Los argumentos son los siguientes:

`$1`	VIP (dirección IPv4 o IPv6 literal)
`$2`	IP del servidor (dirección IPv4 o IPv6 literal)
`$3`	Protocolo (UDP, TCP como cadena)
`$4`	Rango numérico de puertos (el valor especificado por el usuario para `hc-port`)
`$5`	Tiempo máximo (en segundos) que debe esperar la prueba antes de informar un fallo. Si la prueba se ejecuta durante un tiempo mayor al especificado, esta podría detenerse, y se consideraría que la prueba falló. Este valor está definido por el usuario y especificado en `hc-timeout`.

- La prueba proporcionada por el usuario, no tiene que utilizar todos los argumentos, pero *debe* devolver uno de los siguientes valores:
  - Tiempo de recorrido de ida y vuelta (RTT, Round-Trip Time) en microsegundos
  - 0 si la prueba no calcula el RTT
  - -1 en caso de fallo

De manera predeterminada, las pruebas de comprobación de estado se ejecutan con los siguientes privilegios: `PRIV_PROC_FORK`, `RIV_PROC_EXEC` y `RIV_NET_ICMPACCESS`.

Si se requiere un conjunto de privilegios más amplio, debe implementar `setuid` en la prueba. Para obtener más detalles sobre los privilegios, consulte la página del comando man `privileges`(5).

Enumeración de comprobaciones de estado

Para obtener información detallada sobre las comprobaciones de estado configuradas, emita el siguiente comando:

```
# ilbadm show-healthcheck
HCNAME      TIMEOUT COUNT   INTERVAL DEF_PING TEST
hc1         3       2       8        Y        tcp
hc2         3       2       8        N        /var/usr-script
```

Visualización de resultados de comprobación de estado

Puede utilizar el subcomando `ilbadm list-hc-result` para obtener los resultados de la comprobación de estado. Si una regla o una comprobación de estado no se especifica, el subcomando lista todas las comprobaciones de estado.

En el ejemplo siguiente, se muestran los resultados de las comprobaciones de estado asociados con una regla denominada `rule1`.

```
# ilbadm show-hc-result rule1
RULENAME   HCNAME     SERVERID   STATUS   FAIL LAST      NEXT      RTT
rule1      hc1        _sg1:0     dead     10   11:01:19  11:01:27  941
rule1      hc1        _sg1:1     alive    0    11:01:20  11:01:34  1111
```

Nota - El comando `show-hc-result` sólo muestra el resultado de las comprobaciones de estado cuando las reglas tienen comprobaciones de estado asociadas.

En la columna `LAST` del resultado, se muestra hace cuánto tiempo se realizó una comprobación de estado en un servidor. La columna `NEXT` muestra la hora a la que se realizará la próxima comprobación de estado.

Supresión de una comprobación de estado

Para suprimir una comprobación de estado, utilice con el comando `ilbadm delete-healthcheck`. En el siguiente ejemplo, se suprime una comprobación de estado denominada `hc1`.

```
# ilbadm delete-healthcheck hc1
```

Configuración de las reglas del ILB

En esta sección, se describe cómo usar el comando `ilbadm` para crear, suprimir y mostrar las reglas de equilibrio de carga.

Algoritmos del ILB

Los algoritmos del ILB controlan la distribución de tráfico y proporcionan varias características de distribución de la carga y selección de servidores.

El ILB proporciona los siguientes algoritmos para los dos modos de funcionamiento:

- Asignación en rueda (round-robin): en un algoritmo de asignación en rueda, el equilibrador de carga asigna las solicitudes a un grupo de servidores en orden rotativo. Una vez que se asigna una solicitud a un servidor, el servidor se mueve al final de la lista.
- Hash *src-IP*: en la dirección IP de origen, con el método hash, el equilibrador de carga selecciona un servidor basado en el valor hash de la dirección IP de origen de la solicitud entrante.
- Hash *src-IP, port*: en la dirección IP de origen, con el método hash de puerto, el equilibrador de carga selecciona un servidor basado en el valor hash de la dirección IP de origen y el puerto de origen de la solicitud entrante.
- Hash *src-IP, VIP*: en la dirección IP de origen, con el método hash de VIP, el equilibrador de carga selecciona un servidor basado en el valor hash de la dirección IP de origen y la dirección IP de destino de la solicitud entrante.

Creación de una regla del ILB

En un ILB, un servicio virtual está representado por una regla de equilibrio de carga y está definido por los parámetros siguientes:

- Dirección IP virtual
- Protocolo de transporte: TCP o UDP
- Número de puerto (o un intervalo de puertos)
- Algoritmo de equilibrio de carga
- Modo de equilibrio de carga (DSR, full-NAT o half-NAT)
- Grupo de servidores que consta de un conjunto de servidores back-end
- Comprobaciones de estado del servidor opcionales que se pueden ejecutar para cada servidor del grupo de servidores
- Puerto opcional que se va a utilizar para las comprobaciones de estado

---

Nota - Puede especificar comprobaciones de estado en un puerto determinado o en cualquier puerto que el daemon `ilbd` seleccione aleatoriamente del rango de puertos para el servidor.

- Nombre de regla para representar un servicio virtual

Antes de poder crear una regla, debe hacer lo siguiente:

- Cree un grupo de servidores que incluya los servidores back-end apropiados. Para obtener más información, consulte “Definición de grupos de servidores y servidores back-end en ILB” [60].
- Cree una comprobación de estado para asociar la comprobación de estado del servidor con la regla. Para obtener más información, consulte “Creación de una comprobación de estado” [65].

- Identifique el VIP, el puerto y el protocolo opcional que se asociarán a la regla.
- Identifique la operación que desea utilizar (DSR, half-NAT o full-NAT).
- Identifique el algoritmo de equilibrio de carga que se va a utilizar. Para obtener más información, consulte “Algoritmos del ILB” [67].

Para crear una regla del ILB, utilice el comando `ilbadm create-rule`. Para obtener más información sobre el uso del comando `ilbadm create-rule`, consulte la página del comando man `ilbadm`(1M).

La sintaxis es la siguiente:

```
# ilbadm create-rule -e -i vip=IPaddr,port=port,protocol=protocol \
-m lbalg=lb-algorithm,type=topology-type,proxy-src=IPaddr1-IPaddr2,\
pmask=value -h hc-name=hc1 -o servergroup=sg rule1
```

Nota - La opción `-e` activa la regla que se está creando, de lo contrario se puede desactivar de forma predeterminada.

EJEMPLO 6-4 Creación de una regla full-NAT con persistencia de sesión de comprobación de estado

En este ejemplo, se crea una comprobación de estado denominada `hc1` y un grupo de servidores `sg1`. El grupo de servidores está formado por dos servidores, cada uno de ellos con un intervalo de puertos. El último comando crea y activa una regla llamada `rule1`, y asocia la regla al grupo de servidores y la comprobación de estado. Esta regla implementa el modo de operación full-NAT. Tenga en cuenta que la creación del grupo de servidores y la comprobación de estado debe ser anterior a la creación de la regla.

```
# ilbadm create-healthcheck -h hc-test=tcp,hc-timeout=2,\
hc-count=3,hc-interval=10 hc1
# ilbadm create-servergroup -s server=192.168.0.10:6000-6009,192.168.0.11:7000-7009 sg1
# ilbadm create-rule -e -p -i vip=10.0.0.10,port=5000-5009,\
protocol=tcp -m lbalg=rr,type=NAT,proxy-src=192.168.0.101-192.168.0.104,pmask=24 \
-h hc-name=hc1 -o servergroup=sg1 rule1
```

Al crear una asignación persistente, las posteriores solicitudes de conexiones, de paquetes o de ambas cosas en un servicio virtual que tenga una dirección IP de origen del cliente que coincida se reenvían al mismo servidor back-end. La longitud del prefijo en la notación del enrutamiento entre dominios sin clase (CIDR, Classless Inter-Domain Routing) es un valor dentro del intervalo `0-32` para IPv4 y `0-128` para IPv6.

Al crear una regla half-NAT o full-NAT, especifique el valor para el tiempo de espera `connection-drain`. El valor predeterminado de tiempo de espera `conn-drain` es `0`, lo que significa que la purga de conexión espera hasta que una conexión se cierre correctamente.

Enumeración de reglas del ILB

Para enumerar los detalles de configuración de una regla, emita el siguiente comando. Si no se especifica el nombre de la regla, la información se ofrece para todas las reglas.

```
# ilbadm show-rule
RULENAME        STATUS   LBALG           TYPE    PROTOCOL VIP           PORT
rule-http       E        hash-ip-port    NAT     TCP      10.0.0.1      80
rule-dns        D        hash-ip         NAT     UDP      10.0.0.1      53
rule-abc        D        roundrobin      NAT     TCP      2001:db8::1   1024
rule-xyz        E        ip-vip          NAT     TCP      2001:db8::1   2048-2050
```

Supresión de una regla ILB

El comando `ilbadm delete-rule` se utiliza para suprimir una regla. Agregue la opción `-a` para suprimir todas las reglas. En el siguiente ejemplo, se suprime la regla llamada `rule1`.

```
# ilbadm delete-rule rule1
```

Caso de uso: configuración de un ILB

En esta sección, se describen los pasos de configuración del ILB para utilizar una topología half-NAT para equilibrar la carga de tráfico entre dos servidores. Consulte la implementación de la topología NAT en “Modos de funcionamiento del ILB” [50].

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 el grupo de servidores en el ILB.

   Los dos servidores son `192.168.1.50` y `192.169.1.60`. Cree un grupo de servidores `srvgrp1`, compuesto de estos dos servidores. Para ello, escriba el siguiente comando. Para obtener más información sobre cómo configurar un grupo de servidores en el ILB, consulte “Creación de un grupo de servidores del ILB” [61].

   ```
   # ilbadm create-sg -s servers=192.168.1.50,192.168.1.60 srvgrp1
   ```

3. Configure los servidores back-end.

   Los servidores back-end están configurados para utilizar el ILB como enrutador predeterminado en este escenario. Ejecute el siguiente comando en ambos servidores:

   ```
   # route add -p default 192.168.1.21
   ```

Después de ejecutar este comando, inicie las aplicaciones de servidor en ambos servidores. Suponga que es una aplicación de TCP de recepción en el puerto 5000. Para obtener más información sobre la configuración de servidores back-end, consulte “Agregación de servidores back-end a un grupo de servidores del ILB” [61].

4. Configure una comprobación de estado simple denominada `hc-srvgrp1`. Cree la comprobación de estado. Para ello, escriba el siguiente comando:

```
# ilbadm create-hc -h hc-test=tcp,hc-timeout=3,\
hc-count=3,hc-interval=60 hc-srvgrp1
```

   Se utiliza una comprobación de estado de nivel de TCP simple para detectar si la aplicación de servidores es accesible. Esta comprobación se realiza cada 60 segundos. La comprobación de estado intenta al menos 3 veces y espera hasta 3 segundos entre pruebas para comprobar el estado de un servidor. Si los 3 intentos fallan, se marca el servidor como `dead`. Para obtener más información sobre la supervisión y la creación de las comprobaciones de estado, consulte “Supervisión de las comprobaciones de estado en ILB” [64].

5. Configure una regla del ILB con el siguiente comando:

```
# ilbadm create-rule -e -p -i vip=10.0.2.20,port=5000 -m \
lbalg=rr,type=half-nat,pmask=32 \
-h hc-name=hc-srvgrp1 -o servergroup=srvgrp1 rule1_rr
```

   En esta regla, se utiliza la persistencia (con máscara de 32 bits). El algoritmo de equilibrio de carga es `round robin`. Para obtener información sobre los algoritmos diferentes del ILB, consulte “Algoritmos del ILB” [67]. Se utiliza el grupo de servidores `srvgrp1` y el mecanismo de comprobación de estado `hc-srvgrp1`. Para obtener más información sobre la creación de reglas del ILB, consulte “Creación de una regla del ILB” [68].

Visualización de estadísticas del ILB

En esta sección, se describe cómo usar el comando `ilbadm` para obtener información, por ejemplo, acerca de la impresión de estadísticas para un servidor o para una regla. También puede visualizar la información de la tabla NAT y la tabla de asignación persistencia de sesiones.

Visualización de información estadística

Utilice el comando `ilbadm show-statistics` para ver los detalles de distribución de carga como se muestra en el siguiente ejemplo.

```
# ilbadm show-statistics
PKT_P   BYTES_P   PKT_U   BYTES_U   PKT_D   BYTES_D
9       636        0        0        0        0
```

PKT_P	Paquetes procesados
BYTES_P	Bytes procesados
PKT_U	Paquetes sin procesar
BYTES_U	Bytes sin procesar
PKT_D	Paquetes descartados
BYTES_D	Bytes descartados

Visualización de la tabla de conexión NAT

Utilice el comando `ilbadm show-nat` para mostrar la tabla de conexión NAT. Tenga en cuenta que las posiciones relativas de los elementos en ejecuciones consecutivas de este comando no son importantes. Por ejemplo, si ejecuta el comando `ilbadm show-nat 10` dos veces, es posible que no vea los mismos 10 elementos cada vez que lo ejecute, especialmente en un sistema ocupado. Si no se especifica un valor de recuento, se muestra toda la tabla de conexión NAT.

EJEMPLO 6-5 Entradas de la tabla de conexión NAT

En el siguiente ejemplo, se muestran cinco entradas de la tabla de conexión NAT.

```
# ilbadm show-nat 5
UDP: 124.106.235.150.53688 > 85.0.0.1.1024 >>> 82.0.0.39.4127 > 82.0.0.56.1024
UDP: 71.159.95.31.61528 > 85.0.0.1.1024 >>> 82.0.0.39.4146 > 82.0.0.55.1024
UDP: 9.213.106.54.19787 > 85.0.0.1.1024 >>> 82.0.0.40.4114 > 82.0.0.55.1024
UDP: 118.148.25.17.26676 > 85.0.0.1.1024 >>> 82.0.0.40.4112 > 82.0.0.56.1024
UDP: 69.219.132.153.56132 > 85.0.0.1.1024 >>> 82.0.0.39.4134 > 82.0.0.55.1024
```

El formato de las entradas es el siguiente:

```
T: IP1 > IP2 >>> IP3 > IP4
```

T	Protocolo de transporte utilizado en esta entrada
IP1	Puerto y dirección IP del cliente
IP2	VIP y puerto
IP3	En el modo half-NAT, puerto y dirección IP del cliente.

En el modo full-NAT, puerto y dirección IP del cliente.

`IP4` Puerto y dirección IP del servidor back-end

Visualización de la tabla de asignación de persistencia de sesiones

Utilice el comando `ilbadm show-persist` para ver la tabla de asignación de persistencia de sesiones.

EJEMPLO 6-6 Entradas de la tabla de asignación persistencia de sesiones

En el siguiente ejemplo, se muestran cinco entradas de la tabla de asignación de persistencia de sesiones.

```
# ilbadm show-persist 5
rule2: 124.106.235.150 --> 82.0.0.56
rule3: 71.159.95.31 --> 82.0.0.55
rule3: 9.213.106.54 --> 82.0.0.55
rule1: 118.148.25.17 --> 82.0.0.56
rule2: 69.219.132.153 --> 82.0.0.55
```

El formato de las entradas es el siguiente:

```
R: IP1 --> IP2
```

`R` Regla a la que está asociada la entrada de persistencia.

`IP1` Dirección IP del cliente

`IP2` Dirección IP del servidor back-end

Configuraciones de importación y exportación

Los subcomandos de exportación e importación se utilizan para mover una configuración de un sistema a otro. Por ejemplo, si desea configurar una copia de seguridad del ILB mediante el VRRP para tener una configuración activa-pasiva, simplemente puede exportar la configuración a un archivo e importarlo al sistema de copia de seguridad. El comando `ilbadm export` exporta la configuración actual del ILB a un archivo especificado por el usuario. Esta información se puede utilizar como entrada para el comando `ilbadm import`.

El comando `ilbadm import` suprime la configuración existente antes de importar, excepto que se indique específicamente que ésta debe retenerse. La omisión de un nombre de archivo indica al comando que lea desde `stdin` o escriba en `stdout`.

Para exportar una configuración del ILB, hay que utilizar el comando `export-config`. En el ejemplo siguiente, se exporta la configuración actual al archivo `/var/tmp/ilb_config` en un formato adecuado para importar mediante el comando `import`.

```
# ilbadm export-config /var/tmp/ilb_config
```

Para exportar una configuración del ILB, use el comando `import-config`. En el ejemplo siguiente, se lee el contenido del archivo, `/var/tmp/ilb_config`, y se anula la configuración existente.

```
# ilbadm import-config /var/tmp/ilb_config
```

♦ ♦ ♦ CAPÍTULO 7

Configuración del ILB para Alta Disponibilidad

En este capítulo se describe la configuración de alta disponibilidad (HA, high availability) del ILB al utilizar la función VRRP. El ILB se configura para alta disponibilidad mediante la utilización de topologías DSR y half-NAT. Las topologías half-NAT y DSR utilizan el VRRP para proteger la dirección IP virtual de una regla del ILB. Sin embargo, en la topología half-NAT, el VRRP también se utiliza para proteger la dirección IP del equilibrador de carga principal dirigido a los servidores back end. Esto ayuda a garantizar que, cuando el equilibrador de carga principal falla, los servidores back end pasen a usar el equilibrador de carga en espera (pasivo).

Para obtener más información sobre VRRP, consulte Capítulo 3, Uso del protocolo de redundancia de enrutador virtual y para obtener más información sobre cómo configurar y gestionar el ILB, consulte Capítulo 6, Configuración y gestión del equilibrador de carga integrado.

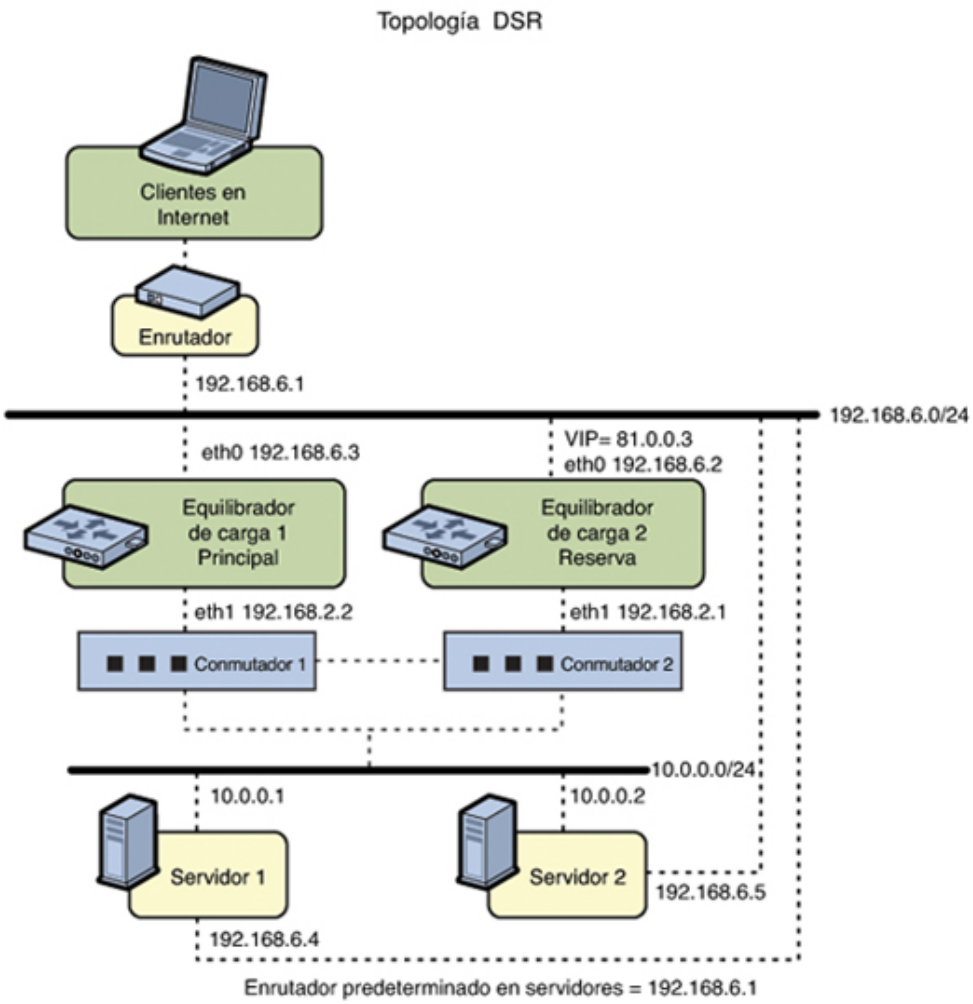
Este capítulo se divide en los siguientes apartados:

Configuración del ILB para la alta disponibilidad mediante la topología DSR

Puede configurar dos equilibradores de carga, uno como equilibrador de carga principal y otro como equilibrador de carga en espera. El equilibrador de carga principal actúa como enrutador maestro y el equilibrador de carga en espera (pasivo) actúa como enrutador de copia de seguridad. La dirección IP virtual de una regla del ILB actúa como la dirección IP del enrutador virtual. El subsistema VRRP comprueba si el equilibrador de carga principal ha fallado. Si el equilibrador de carga principal falla, el equilibrador de carga en espera asume el rol del equilibrador de carga principal.

En la siguiente figura, se muestra la topología DSR para configurar las conexiones del ILB a fin de alcanzar la alta disponibilidad.

FIGURA 7-1 Configuración del ILB para la alta disponibilidad mediante la topología DSR



Todas las VIP en los equilibradores de carga se configuran en interfaces dirigidas a la subred 192.168.6.0/24.

Cómo configurar el ILB para la alta disponibilidad mediante la topología DSR

Puede configurar los equilibradores de carga de datos principales y en espera a fin de que tengan las mismas configuraciones para regla del ILB, el grupo de servidores y la comprobación de estado. Puede configurar ambos equilibradores de carga a fin de utilizar el VRRP. También, puede configurar la dirección IP virtual de la regla que sea la dirección del enrutador virtual. El subsistema VRRP se asegura entonces de que uno de los equilibradores de carga esté siempre activo.

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 los equilibradores de carga principal y en espera (pasivo) para que tengan la misma configuración.**

   ```
   # ilbadm create-servergroup -s server=10.0.0.1,10.0.0.2 sg1
   # ilbadm create-rule -i vip=10.81.0.3,port=9001 \
   -m lbalg=hash-ip-port,type=DSR -o servergroup=sg1 rule1
   ```

3. **Configure el equilibrador de carga 1 para que funcione como equilibrador de carga principal.**

   ```
   LB1# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
   LB1# vrrpadm create-router -V 1 -A inet -l eth0 -p 255 vrrp1
   LB1# ipadm create-ip vnic1
   LB1# ipadm create-addr -d -a 10.81.0.3/24 vnic1
   ```

   La prioridad del enrutador `vrrp1` se configura en `255` mediante el comando `vrrpadm`. El valor de prioridad hace que el enrutador se convierta en el enrutador maestro y, por lo tanto, el equilibrador de carga activo.

4. **Configure el equilibrador de carga 2 para que funcione como equilibrador de carga en espera.**

   ```
   LB2# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
   LB2# vrrpadm create-router -V 1 -A inet -l eth0 -p 100 vrrp1
   LB2# ipadm create-ip vnic1
   LB2# ipadm create-addr -d -a 10.81.0.3/24 vnicl
   ```

   La configuración anterior proporciona protección ante los siguientes escenarios de fallo:

   - Si falla el equilibrador de carga 1, el equilibrador de carga 2 se convierte en el equilibrador de carga principal. Luego, el equilibrador de carga 2 se apodera de la resolución de direcciones para la VIP `10.81.0.3` y gestiona todos los paquetes de los clientes con la dirección IP de destino `10.81.0.3`.

Cuando el equilibrador de carga 1 se recupera, el 2 vuelve a estar en espera.

- Si falla una o las dos interfaces del equilibrador de carga 1, el equilibrador de carga 2 asume como equilibrador de carga principal. Luego, el equilibrador de carga 2 se apodera de la resolución de direcciones para la VIP `10.81.0.3` y gestiona todos los paquetes de los clientes con la dirección IP de destino `10.81.0.3`.

  Cuando las dos interfaces del equilibrador de carga 1 están en buen estado, el equilibrador de carga 2 vuelve a estar en espera.

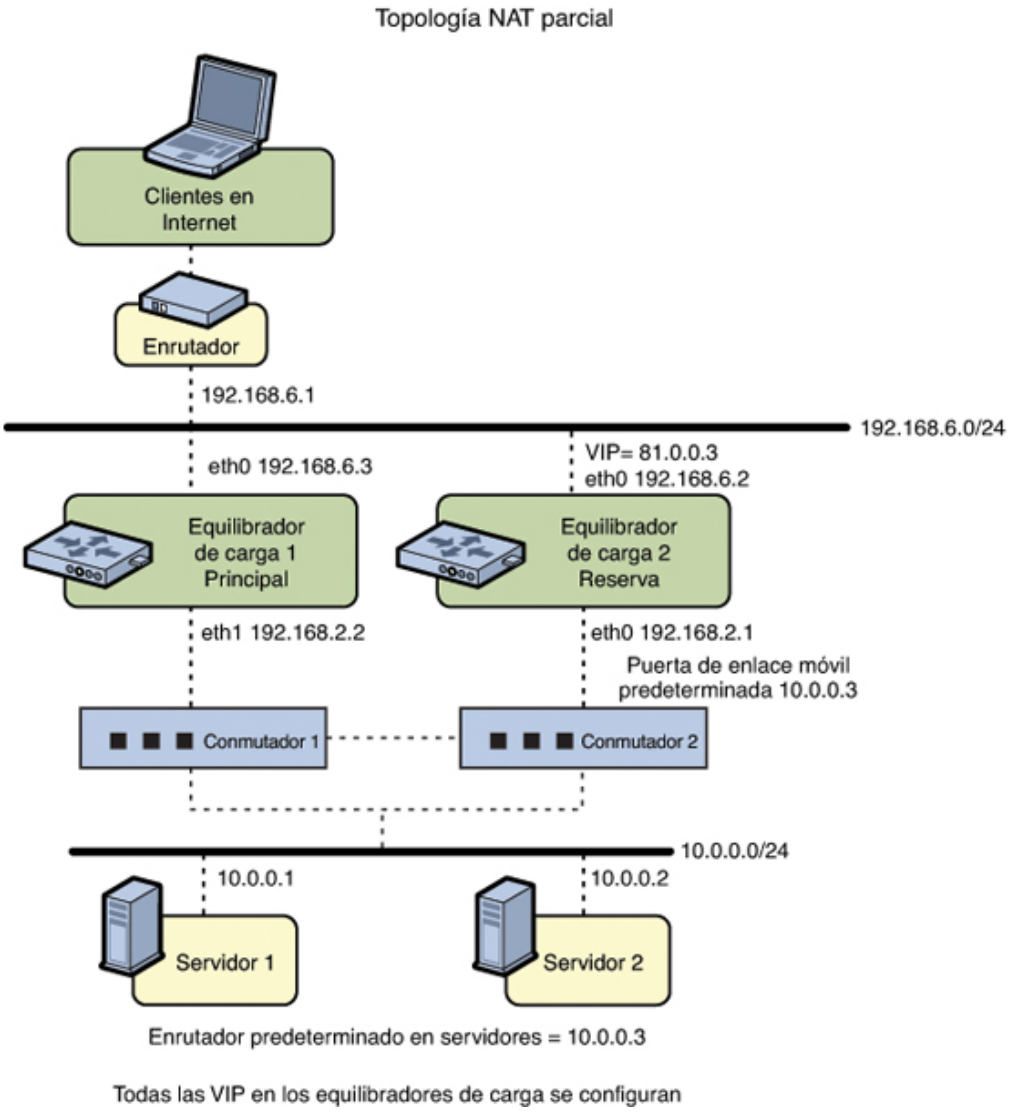
Configuración del ILB para la alta disponibilidad mediante la topología half-NAT

En esta sección, se describe cómo configurar las conexiones del ILB para lograr alta disponibilidad mediante la topología NAT parcial. Debe configurar dos equilibradores de carga, uno como equilibrador de carga principal y otro como equilibrador de carga en espera. Si el equilibrador de carga principal falla, el equilibrador de carga en espera asume el rol del equilibrador de carga principal.

Nota - La implementación actual del ILB no sincroniza el equilibrador de carga principal y el equilibrador de carga en espera. Cuando falla el equilibrador de carga principal y el equilibrador de carga en espera toma el control, fallan las conexiones existentes. Sin embargo, la alta disponibilidad sin sincronización sigue siendo útil en las circunstancias en que se produce un error en la base de datos primaria de equilibrio de carga.

En la siguiente figura, se muestra la topología half-NAT para configurar las conexiones del ILB a fin de alcanzar la alta disponibilidad.

FIGURA 7-2 Configuración del ILB para la alta disponibilidad mediante la topología half-NAT



▼ Cómo configurar el ILB para la alta disponibilidad mediante la topología half-NAT

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 el equilibrador de carga principal y el equilibrador de carga en espera.**

```
# ilbadm create servergroup -s server=10.0.0.1,10.0.0.2 sg1
# ilbadm create-rule -ep -i vip=10.81.0.3,port=9001-9006,protocol=udp \
-m lbalg=roundrobin,type=HALF-NAT,pmask=24 \
-h hc-name=hc1,hc-port=9006 \
-t conn-drain=70,nat-timeout=70,persist-timeout=70 -o servergroup=sg1 rule1
```

3. **Configure el equilibrador de carga 1 para que funcione como equilibrador de carga principal.**

```
LB1# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB1# ipadm create-ip vnic1
LB1# ipadm create-addr -d -a 10.81.0.3/24 vnic1
LB1# vrrpadm create-router -V 1 -A inet -l eth0 -p 255 vrrp1
LB1# dladm create-vnic -m vrrp -V 2 -A inet -l eth1 vnic2
LB1# ipadm create-ip vnic2
LB1# ipadm create-addr -d -a 10.0.0.3/24 vnic2
LB1# vrrpadm create-router -V 2 -A inet -l eth1 -p 255 vrrp2
```

4. **Configure el equilibrador de carga 2 para que funcione como equilibrador de carga en espera.**

```
LB2# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB2# ipadm create-ip vnic1
LB2# ipadm create-addr -d -a 10.81.0.3/24 vnic1
LB2# vrrpadm create-router -V 1 -A inet -l eth0 -p 100 vrrp1
LB2# dladm create-vnic -m vrrp -V 2 -A inet -l eth1 vnic2
LB2# ipadm create-ip vnic2
LB2# ipadm create-addr -d -a 10.0.0.3/24 vnic2
LB2# vrrpadm create-router -V 2 -A inet -l eth1 -p 100 vrrp2
```

5. **Agregue la dirección IP de la puerta de enlace predeterminada flotante para ambos servidores.**

```
# route add default 10.0.0.3
```

   La configuración proporciona protección contra los escenarios de fallo siguientes:

   - Si falla el equilibrador de carga 1, el equilibrador de carga 2 se convierte en el equilibrador de carga principal. Luego, el equilibrador de carga 2 se apodera de la resolución de direcciones para la VIP `10.81.0.3` y gestiona todos los paquetes de los clientes con la

dirección IP de destino `10.81.0.3`. El equilibrador de carga 2 también gestiona todos los paquetes que se envían a la dirección de puerta de enlace flotante `10.0.0.3`.

Cuando el equilibrador de carga 1 se recupera, el 2 vuelve a estar en espera.

- Si falla una o las dos interfaces del equilibrador de carga 1, el equilibrador de carga 2 asume como equilibrador de carga principal. Luego, el equilibrador de carga 2 se apodera de la resolución de direcciones para la VIP `10.81.0.3` y gestiona todos los paquetes de los clientes con la dirección IP de destino `10.81.0.3`. El equilibrador de carga 2 también gestiona todos los paquetes que se envían a la dirección de puerta de enlace flotante `10.0.0.3`.

  Cuando las dos interfaces del equilibrador de carga 1 están en buen estado, el equilibrador de carga 2 vuelve a estar en espera.

Índice

G

I

M

N

O

P

Q

R

S

T

V