Planificación de la implementación de red en Oracle® Solaris 11.2

Referencia: E53780
Julio de 2014

Contenido

Uso de esta documentación

- **Descripción general**: incluye las tareas y los temas básicos para ayudar a planificar la implementación de redes IPv4 e IPv6.
- **Destinatarios**: administradores de sistemas.
- **Conocimientos necesarios**: comprensión básica de conceptos y prácticas de administración de redes.

Biblioteca de documentación del producto

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

Acceso a My Oracle Support

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

Comentarios

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

♦ ♦ ♦ CAPÍTULO 1

Planificación de la implementación de red

En este capítulo, se describen los diferentes aspectos que se deben tener en cuenta a la hora de planificar la implementación de una red TCP/IP. Las tareas de planificación que se describen pueden ayudar a implementar la red de una manera organizada y rentable. Tenga en cuenta que los detalles sobre la planificación de la red están fuera del alcance de este manual. Únicamente se proporcionan instrucciones generales. En este manual, también se da por sentado que está familiarizado con los conceptos y la terminología de red básicos.

Para obtener una descripción de cómo se implementa TCP/IP en Oracle Solaris y una descripción general de la administración de red en esta versión, consulte Capítulo 1, “Acerca de la administración de redes en Oracle Solaris” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”.

Para obtener más ayuda con la planificación del esquema de red general de su sitio, consulte las estrategias de red que se describen en Capítulo 1, “Resumen de la administración de redes en Oracle Solaris” de “Estrategias de administración de redes en Oracle Solaris 11.2 ”.

Este capítulo se divide en los siguientes apartados:

Determinación del hardware de red

El número de sistemas que espera admitir afecta la configuración de la red. Es posible que su organización requiera una pequeña red de varias docenas de sistemas independientes ubicados en una única planta de un edificio. También es posible que requiera la instalación de una red con más de 1.000 sistemas ubicados en varios edificios. Esta configuración podría hacer necesaria la división de la red en subdivisiones denominadas *subredes*.

A continuación, se presentan algunas de las decisiones de planificación relacionadas con el hardware que debe tomar:

- la topología de red, el diseño y las conexiones del hardware de red;
- el tipo y la cantidad de sistemas host que admite la red, incluidos los sistemas virtuales que pueden ser necesarios en el servidor;
- los dispositivos de red que se instalarán en estos sistemas;
- los tipos de medios de red que se utilizarán, como Ethernet, etcétera;
- el uso de puentes, enrutadores o firewalls para ampliar los medios de la red o conectar la red local a redes externas.

  Para obtener información sobre cómo funcionan los puentes, consulte "Descripción general de las redes con puentes" de "Gestión de enlaces de datos de red en Oracle Solaris 11.2 ".

  Para obtener una descripción sobre cómo funcionan los enrutadores, consulte "Planificación de enrutadores en la red" [13].

  Para obtener información sobre firewalls, consulte Capítulo 4, "Acerca del filtro IP en Oracle Solaris" de "Protección de la red en Oracle Solaris 11.2 ".

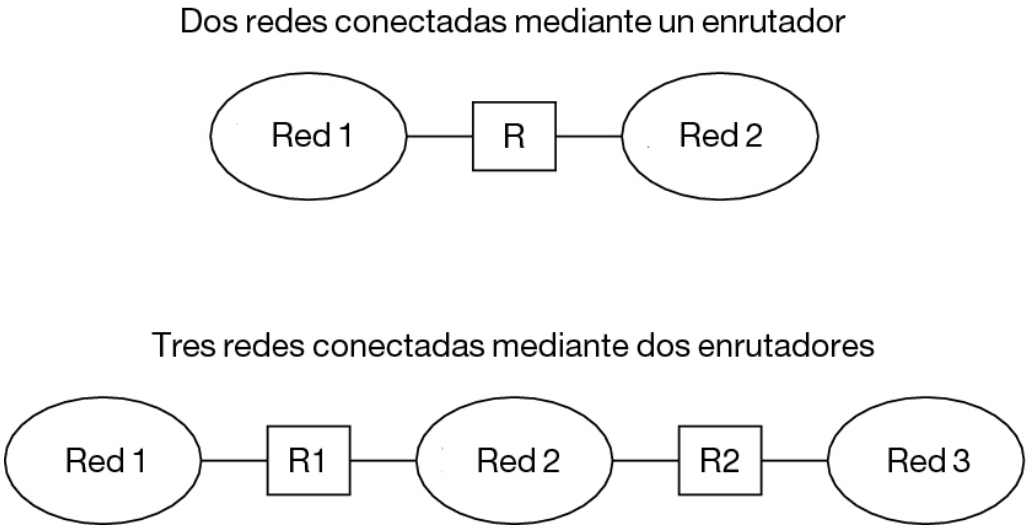
Descripción general de la topología de red

La topología de red describe cómo encajan las redes. Los enrutadores son las entidades que conectan las redes entre sí. Un enrutador es un equipo que tiene dos o más interfaces de red e implementa el reenvío de IP. Sin embargo, el sistema no podrá funcionar como enrutador hasta que se haya configurado de manera adecuada, como se describe en Capítulo 2, "Configuración de un sistema como enrutador" de "Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ".

Los enrutadores conectan dos o más redes para formar interredes más grandes. Debe configurar los enrutadores para transferir paquetes entre dos redes adyacentes. Los enrutadores también deben poder transferir paquetes a redes que se encuentran fuera de las redes adyacentes reenviándolos a otros enrutadores que están conectados a redes adyacentes.

La figura siguiente muestra las partes básicas de una topología de red. La parte superior de la ilustración muestra una configuración sencilla de dos redes conectadas mediante un único enrutador. La parte inferior de la ilustración muestra una configuración de tres redes interconectadas por dos enrutadores. En el primer ejemplo, el enrutador R une la red 1 y la red 2 en una interred mayor. En el segundo ejemplo, el enrutador 1 conecta las redes 1 y 2. El enrutador R2 conecta las redes 2 y 3. Las conexiones de una red que incluye las redes 1, 2 y 3.

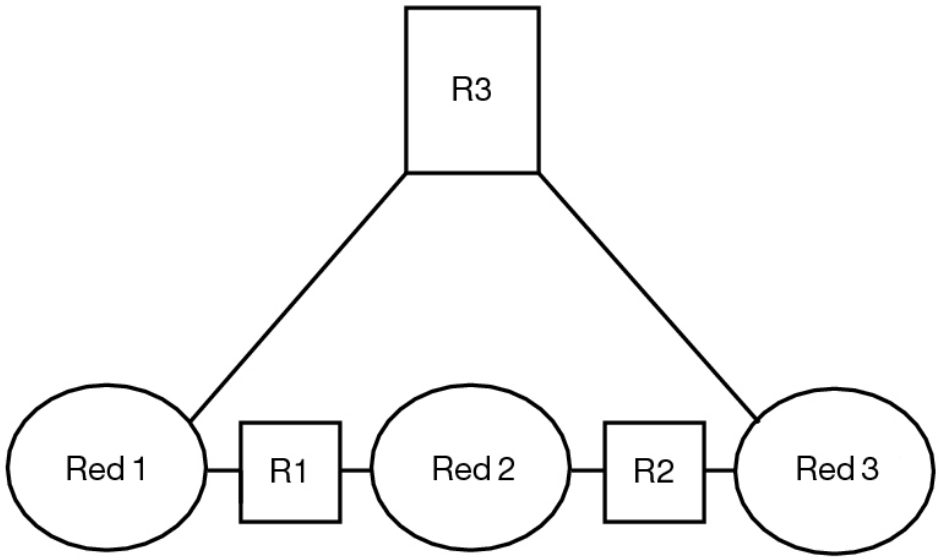
FIGURA 1-1 Topología de red básica



Además de unir las redes en interredes, los enrutadores transfieren los paquetes entre las redes que se basan en las direcciones de la red de destino. A medida que las interredes se hacen más complejas, cada enrutador debe tomar más decisiones sobre los destinos de los paquetes.

En la figura siguiente, se muestra un caso más complejo. El enrutador R3 conecta las redes 1 y 3. La redundancia aumenta la fiabilidad. Si la red 2 no funciona, el enrutador R3 continua proporcionando una ruta entre las redes 1 y 3. Se pueden interconectar muchas redes. No obstante, las redes deben utilizar los mismos protocolos de red.

FIGURA 1-2 Topología de red que proporciona una ruta adicional entre las redes



Los enrutadores se explican con más detalle en “Planificación de enrutadores en la red” [13].

Uso de subredes en la red

El uso de subredes está relacionado con la necesidad de contar con subdivisiones administrativas para abordar cuestiones de tamaño y control. Cuantos más hosts y servidores haya en una red, más compleja será la tarea de gestión. Mediante la creación de divisiones administrativas y el uso de subredes, la gestión de redes complejas resulta más fácil.

La decisión de configurar subdivisiones administrativas para su red la determinan los factores siguientes:

- **Tamaño de la red**

  Las subredes también son útiles incluso en una red relativamente pequeña cuyas subdivisiones están ubicadas a lo largo de una amplia área geográfica.

- **Necesidades comunes compartidas por grupos de usuarios**

  Por ejemplo, posiblemente tenga una red que esté limitada a un único edificio y que admita un número relativamente pequeño de máquinas. Estos equipos se reparten en una serie de subredes. Cada subred admite grupos de usuarios con diferentes necesidades. En este ejemplo, puede utilizar una subdivisión administrativa para cada subred.
- **Seguridad**

  Es posible que desee separar los servidores, los sistemas de escritorio y los servidores web con conexión a Internet críticos en subredes independientes donde puede establecer firewalls entre ellos.

Topología de sistemas autónomos IPv4

Los sitios con varios enrutadores y redes normalmente administran su topología de red como un dominio de enrutamiento único o un *sistema autónomo* (SA). En la Figura 1-3, “Sistema autónomo con varios enrutadores IPv4”, se muestra un SA que está dividido en tres redes locales: `10.0.5.0`, `172.20.1.0` y `192.168.5.0`.

La red se compone de los siguientes tipos de sistemas:

- Enrutadores

  Los enrutadores utilizan protocolos de enrutamiento para gestionar la forma en que los paquetes de red se dirigen o se enrutan desde el origen hasta los destinos dentro de la red local o hasta redes externas. Para obtener información sobre los protocolos de enrutamiento admitidos en Oracle Solaris e instrucciones sobre la configuración de un sistema como enrutador, consulte “Protocolos de enrutamiento” de “Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ”.

  Tipos de enrutadores:

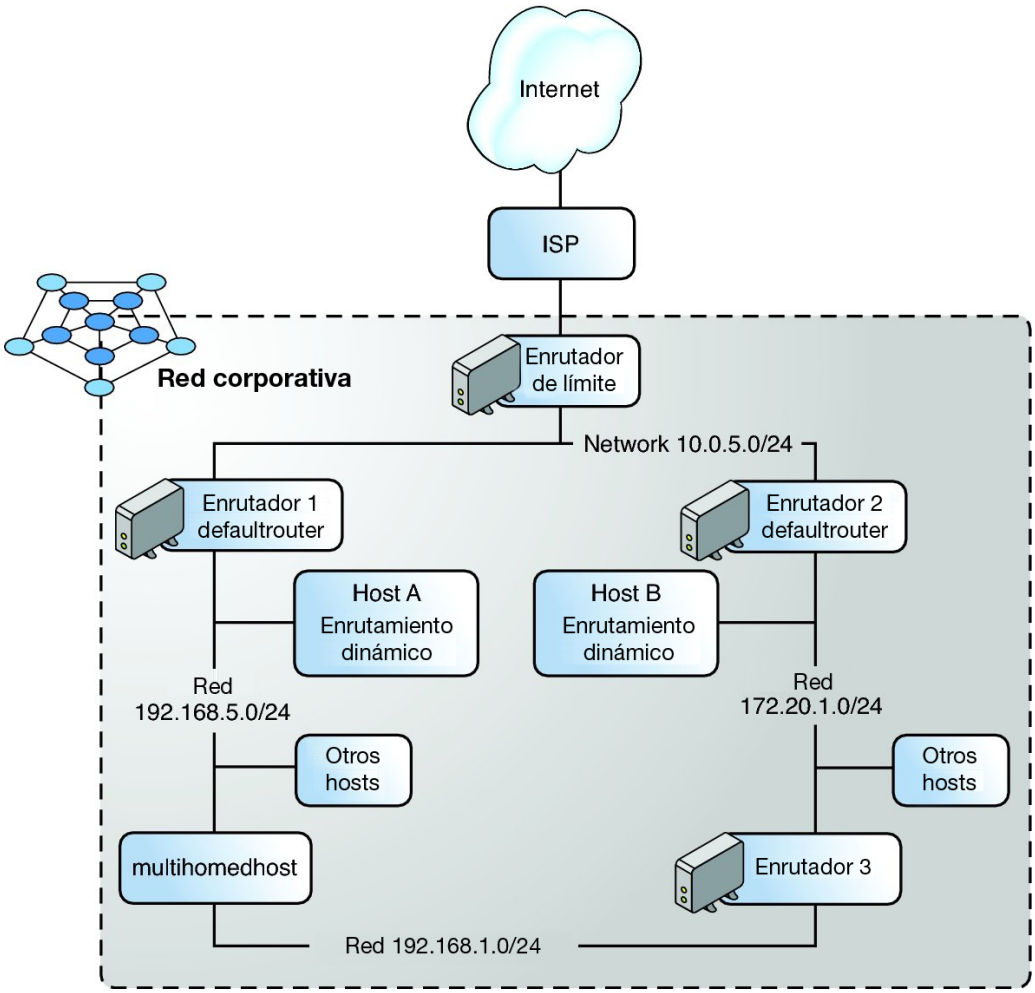
  - Enrutadores de límite: conectan la red local, como `10.0.5.0`, externamente con un proveedor de servicios.
  - Enrutadores predeterminados: gestionan el enrutamiento de paquetes en la red local, que, a su vez, puede incluir varias redes locales. Por ejemplo, en la Figura 1-3, “Sistema autónomo con varios enrutadores IPv4”, el enrutador 1 actúa como enrutador predeterminado para `192.168.5`. En el mismo momento, el enrutador 1 también está conectado a la red interna `10.0.5.0`. Las interfaces del enrutador 2 se conectan a las redes internas `10.0.5.0` y `172.20.1.0`.
  - Enrutadores de reenvío de paquetes: reenvían paquetes entre redes internas, pero no ejecutan protocolos de enrutamiento. En la Figura 1-3, “Sistema autónomo con varios enrutadores IPv4”, el enrutador 3 es un enrutador de reenvío de paquetes con conexiones a las redes `172.20.1` y `192.168.5`.
- Sistemas cliente

- Sistemas de host múltiple o sistemas que tienen varias NIC. En Oracle Solaris, de manera predeterminada, estos sistemas pueden reenviar paquetes a otros sistemas del mismo segmento de red.
- Los sistemas de interfaz única confían en los enrutadores locales para reenviar paquetes y para recibir información de configuración.

Para obtener información relacionada con tareas, 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 ”.

Utilice la siguiente figura como una referencia al configurar componentes de red adicionales.

FIGURA 1-3 Sistema autónomo con varios enrutadores IPv4



Planificación de enrutadores en la red

Tenga en cuenta que en TCP/IP existen dos tipos de entidades en una red: hosts y enrutadores. Mientras que todas las redes requieren un host, no es necesario que tengan un enrutador. La topología física de la red determina la necesidad de enrutadores. En esta sección se introducen los conceptos de topología de red y enrutamiento. Estos conceptos son importantes cuando decide agregar otra red a su entorno de red.

Nota - Para ver las tareas y detalles completos para la configuración de los enrutadores en redes IPv4 e IPv6, consulte el Capítulo 2, “Configuración de un sistema como enrutador” de “Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ”.

Cómo transfieren los paquetes los enrutadores

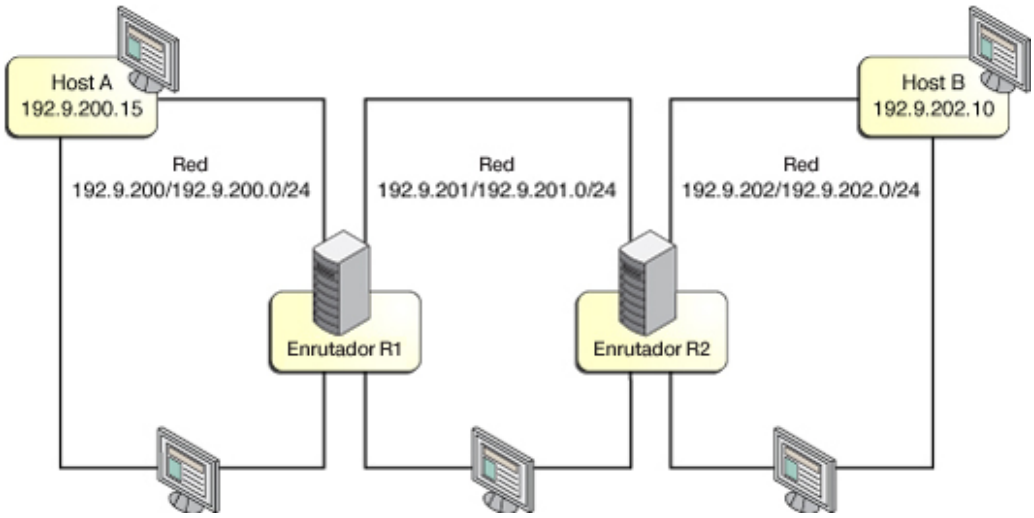
Los enrutadores transfieren paquetes de la siguiente manera:

- Todos los nodos en una red IP contienen información de enrutamiento en las tablas de enrutamiento. Estas tablas contienen información sobre cómo acceder a sistemas conectados a redes locales y remotas. Las tablas de enrutamiento se generan a partir de información de configuración local y mensajes de protocolo de enrutamiento que se intercambian con sistemas adyacentes.
- Cuando un sistema host envía inicialmente un paquete, busca la dirección de destino del paquete en la tabla de enrutamiento para determinar si el destino está en la red local. En caso de que así sea, el paquete va directamente al host con esa dirección IP. De lo contrario, el paquete va a un enrutador de la red local.
- Cuando un enrutador recibe un paquete, el enrutador comprueba su tabla de enrutamiento para determinar si la dirección de destino es para un sistema de una de sus redes conectadas o si el mensaje debe reenviarse mediante otro enrutador. Luego envía el mensaje al siguiente sistema en la ruta para el destino.
- Este proceso se repite en cada enrutador que recibe el mensaje hasta que el mensaje llega al sistema de destino.

Consulte Capítulo 2, “Configuración de un sistema como enrutador” de “Configuración del sistema Oracle Solaris 11.2 como enrutador o equilibrador de carga ”.

La figura siguiente muestra una topología de red con tres redes que están conectadas con dos enrutadores.

FIGURA 1-4 Topología de red con tres redes interconectadas



El enrutador R1 conecta las redes `192.9.200.0/24` y `192.9.201.0/24`. El enrutador R2 conecta las redes `192.9.201.0/24` y `192.9.202.0/24`.

Si el host A de la red `192.9.200.0/24` envía un mensaje al host B de la red `192.9.202`, ocurren los siguientes eventos:

1. El host A examina sus tablas de enrutamiento para la ruta a `192.9.202.10`. El intervalo de direcciones de la red local no cubre esta dirección, pero hay una ruta predeterminada previamente aprendida mediante el enrutador R1 que la cubre. Por lo tanto, el host A envía el paquete al enrutador R1.
2. El enrutador R1 examina sus tablas de enrutamiento. Ningún intervalo de direcciones de la red local cubre la dirección de destino, pero hay una ruta conocida a la red `192.9.202.0/24` mediante el enrutador R2 que cubre la dirección. El enrutador R1 envía el paquete al enrutador R2.
3. El enrutador R2 está conectado directamente a la red `192.9.202.0/24`. La consulta de la tabla de enrutamiento revela que `192.9.202.10` está en la red conectada. El enrutador R2 envía el paquete directamente al host B.

Cómo decidir el formato de las direcciones IP para la red

Al planificar el esquema de direcciones de la red, debe tener en cuenta los siguientes factores:

- El tipo de dirección IP que desea utilizar: IPv4 o IPv6.
- El número de sistemas potenciales de la red.
- La cantidad de sistemas que son enrutadores o sistemas de host múltiple, que requieren varias tarjetas de interfaz de red (NIC), con sus propias direcciones IP individuales.
- Si se utilizarán direcciones privadas en la red.
- Si habrá un servidor DHCP que gestione las agrupaciones de direcciones IP.

Direcciones IPv4

Éste es el formato original de direcciones que se usa en redes TCP/IP. Las direcciones IPv4 tienen un tamaño de 32 bits. Las direcciones IPv4 originalmente estaban asignadas a varias organizaciones en bloques contiguos de 16777216 (clase A), 65536 (clase B) o 256 (clase C) direcciones. Cada organización que solicitaba un bloque de direcciones recibía un prefijo de dirección fijo y una máscara de prefijo implícita, ambos especificados en notación decimal con punto. Por ejemplo, la autoridad de números asignados de Internet (IANA) asignó el bloque de direcciones clase A `156.0.0.0` con máscara de red `255.0.0.0` al registro norteamericano de números de Internet (ARIN). Todas las direcciones cuyo primer byte es igual a 156 están dentro de este bloque de direcciones. ARIN subasignó el bloque de direcciones clase B `156.151.0.0` con máscara de red `255.255.0.0` de su bloque clase A a Sun Microsystems (ahora Oracle).

Más adelante, el grupo especial sobre ingeniería de Internet (IETF) desarrolló direcciones de *enrutamiento entre dominios sin clase* (CIDR) como una solución interina para remediar la escasez de direcciones IPv4 y la capacidad limitada de las tablas de enrutamiento de Internet globales. Las asignaciones de direcciones CIDR se subdividen en el límite de bits que mejor se adapte a los requisitos de una organización. Los bloques de direcciones se especifican como una dirección IPv4 en notación decimal con punto seguida de una barra y la longitud de prefijo de dirección en bits.

Para obtener más información, consulte los siguientes recursos:

- Internet Protocol DARPA Internet Program Protocol Specification (http://tools.ietf.org/html/rfc791) (Especificación del protocolo de Internet de DARPA Internet Program)
- Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan (http://tools.ietf.org/html/rfc4632) (Enrutamiento entre dominios sin clase [CIDR]: plan de agregación y asignación de direcciones de Internet)

En la siguiente tabla, se proporcionan ejemplos de especificaciones de longitud de subred en notación CIDR y en formato decimal con punto, además de la cantidad total de hosts que son posibles en una red con esa longitud de prefijo.

TABLA 1-1 Prefijos CIDR y sus equivalentes decimales

Longitud de prefijo de red CIDR	Máscara de subred decimal con punto correspondiente	Direcciones IP disponibles
/19	255.255.224.0	8.192

Longitud de prefijo de red CIDR	Máscara de subred decimal con punto correspondiente	Direcciones IP disponibles
/20	255.255.240.0	4.096
/21	255.255.248.0	2.048
/22	255.255.252.0	1.024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32

Direcciones privadas

El IANA ha reservado un bloque de direcciones IPv4. Las direcciones privadas se utilizan para tráfico de red dentro de una red privada. Las organizaciones que solicitan un bloque de direcciones IPv4 al proveedor de servicios de Internet posiblemente no reciban una asignación suficiente para tener una dirección única para cada uno de sus sistemas. Las organizaciones suelen asignar direcciones privadas a los sistemas de sus redes internas. Los sistemas pueden compartir con eficacia las direcciones limitadas proporcionadas por el proveedor de servicios de Internet (ISP) mediante el traductor de direcciones de red (NAT) y los servidores proxy de aplicación para comunicarse con otros sitios de Internet.

En la tabla siguiente, se muestran los intervalos de direcciones IPv4 privadas y sus correspondientes máscaras de red.

Longitud/prefijo de red	Intervalo de direcciones IPv4
10.0.0.0/8	10.0.0.0-10.255.255.255
172.16.0.0/125	172.16.0.0-172.31.255.25
192.168.0.0/16	192.168.0.0-192.168.255.255

Direcciones DHCP

El protocolo de configuración dinámica de sistemas (DHCP, Dynamic Host Configuration Protocol) permite a un sistema recibir información de configuración de un servidor DHCP, incluida una dirección IP, como parte del proceso de inicio. Los servidores DHCP cuentan con agrupaciones de direcciones IP desde las que se asignan direcciones a los clientes DHCP. Un sitio que usa DHCP puede usar una agrupación más pequeña de direcciones IP que la cantidad de direcciones IP que se requerirían si a cada cliente se le asignara una dirección IP permanente, siempre y cuando los clientes no estén continuamente conectados. En este caso, puede compartir direcciones entre clientes y, por lo tanto, reducir la cantidad total necesaria

de direcciones IP. Sin embargo, si no tiene un flujo suficiente de clientes, necesitará, en última instancia, la misma cantidad de direcciones IP. La ventaja más general de utilizar direcciones DHCP es que no necesita realizar tanta configuración de hosts individuales porque se configura un servidor DHCP con los detalles de configuración. De esta forma, los hosts requieren una mínima configuración manual o incluso pueden no requerir ninguna configuración. Puede configurar el servicio DHCP para gestionar las direcciones IP del sitio o parte de ellas. Para obtener más información, consulte “Uso de DHCP en Oracle Solaris 11.2 ”.

Direcciones IPv6

Estas direcciones IPv6 de 128 bits proporcionan un espacio de direcciones más grande que el que está disponible con IPv4. Las direcciones IPv6 se presentan como ocho conjuntos de cuatro dígitos hexadecimales, y cada grupo está separado por dos puntos. Se pueden eliminar los ceros iniciales en cada grupo. Uno o más grupos consecutivos de todos los ceros se pueden sustituir por dos puntos dobles, como se muestra en el siguiente ejemplo:

```
2001:db8:2f32:27:214:4fff:fe4a:9926
```

Como con las direcciones IPv4 en formato CIDR, las direcciones IPv6 no tienen clase y utilizan prefijos para designar la parte de la dirección que define la red del sitio, como se muestra en el siguiente ejemplo:

```
2001:db8:2f32::/48
```

Para obtener detalles sobre las direcciones IPv6, consulte IP Version 6 Addressing Architecture (http://tools.ietf.org/html/rfc4291).

Prefijos de documentación

Para las direcciones IPv6, el prefijo `2001:db8::/32` es un prefijo IPv6 especial que se utiliza específicamente para ejemplos de documentación. Los ejemplos de este manual utilizan direcciones IPv4 privadas y el prefijo de documentación de IPv6 reservado.

Cómo obtener el número de IP de la red

Una red IPv4 se define con una combinación de un número de red IPv4 más una *máscara de red*. Una red IPv6 se define mediante el *prefijo de sitio* y el *prefijo de subred* si se usan subredes.

Para activar la red privada para que se comunique con redes externas en Internet, debe obtener un número de IP registrado para su red de la organización pertinente. Esta dirección pasará a ser

el número de red para el esquema de direcciones IPv4 o el prefijo de sitio para el esquema de direcciones IPv6.

Los ISP proporcionan direcciones IP para las redes cuyos precios se basan en los distintos niveles de servicio. Compare los diferentes ISP para determinar cuál de ellos proporciona el mejor servicio para su red. Los ISP normalmente ofrecen a las empresas direcciones asignadas dinámicamente o direcciones IP estáticas. Algunos ISP ofrecen direcciones tanto IPv4 como IPv6.

Si su sitio es un ISP, obtiene bloques de direcciones IP para los clientes a través de un registro de Internet (IR) para su configuración regional. IANA es la principal responsable de la delegación de direcciones IP registradas a los registros de Internet de todo el mundo. Cada IR cuenta con información de registro y plantillas para la configuración regional en la que el IR ofrece el servicio. Para obtener información sobre la IANA y sus IR, consulte la página de servicio de direcciones IP de IANA (http://www.iana.org/ipaddress/ip-addresses.htm).

Uso de entidades de denominación en la red

Los protocolos TCP/IP localizan un sistema en una red utilizando su dirección IP. Sin embargo, un nombre de host le permite identificar sistemas más fácilmente que las direcciones IP.

Desde el punto de vista del protocolo TCP/IP, una red es un conjunto de entidades con nombre. Un host es una entidad con un nombre. Un enrutador es una entidad con un nombre. La red es una entidad con un nombre. Del mismo modo, se puede asignar un nombre a un grupo o departamento en el que esté instalada la red, así como a una división, región o compañía. En teoría, la jerarquía de nombres que se pueden utilizar para identificar una red prácticamente no tiene límites.

Nombres de dominio

Muchas redes organizan sus hosts y enrutadores en una jerarquía de dominios administrativos. Si utiliza el servicio de información de red (NIS) o el sistema de nombres de dominio (DNS), debe seleccionar un nombre de dominio para la organización que sea exclusivo en todo el mundo. Para asegurarse de que su nombre de dominio sea exclusivo, debe registrarlo en *InterNIC*. Se necesita un nombre de dominio único si desea permitir que otros sitios de Internet localicen sus sistemas a través de DNS.

Un nombre de dominio que se ubica en otro dominio suele denominarse subdominio. La estructura del nombre de dominio es jerárquica. Un nuevo dominio normalmente se ubica debajo de un dominio relacionado que ya existe. Por ejemplo, el nombre de dominio para una compañía subsidiaria puede ubicarse debajo el dominio de su compañía principal. Si el nombre de dominio no tiene otra relación, una organización puede colocar su nombre de dominio directamente debajo de uno de los dominios existentes de nivel superior, como `.com`, `.org`, `.edu`, `.gov`, etcétera.

Selección de un servicio de nombres y un servicio de directorios

En Oracle Solaris, puede seleccionar entre tres tipos de servicios de nombres: archivos locales, NIS y DNS. Los servicios de nombres contienen información crítica sobre los equipos de una red, como los nombres de host, las direcciones IP, etc. También puede utilizar el servicio de directorios LDAP además del servicio de nombres o en lugar de él. LDAP es un protocolo de red seguro que se utiliza para acceder a servidores de directorios en busca de nombres distribuidos y otros servicios de directorios. Este protocolo basado en estándares admite una estructura de base de datos jerárquica. Se puede utilizar el mismo protocolo para proporcionar servicios de nombres que estén en UNIX y en entornos de varias plataformas. Para obtener una introducción a los servicios de nombres de Oracle Solaris, consulte Capítulo 1, “Acerca de los servicios de nombres y directorios” de “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

La configuración de las bases de datos de red es imprescindible. Por lo tanto, debe decidir qué servicio de nombres o directorios utilizará como parte del proceso de planificación de la red. Asimismo, la decisión de utilizar servicios de nombres también determina si organizará la red en un dominio administrativo.

Para un servicio de nombres o directorios, puede seleccionar entre las opciones siguientes:

- NIS o DNS: los servicios de nombres NIS y DNS conservan bases de datos de red en varios servidores de la red. En “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”, se describen estos servicios de nombres y se explica cómo configurar las bases de datos. Además, en la guía, se explican con más detalle los conceptos de *espacio de nombre* y *dominio administrativo*.
- LDAP: también puede utilizar el servicio de directorios LDAP además del servicio de nombres o en lugar de él. LDAP es un protocolo de red seguro que se utiliza para acceder a servidores de directorios en busca de nombres distribuidos y otros servicios de directorios.
- Archivos locales: si no desea implementar NIS, DNS ni LDAP, la red utiliza *archivos locales* para proporcionar el servicio de nombres. El término "archivos locales" hace referencia a la serie de archivos del directorio `/etc` que utilizan las bases de datos de red. En los procedimientos de este manual, se presupone que está utilizando archivos locales para el servicio de nombres, a menos que se especifique lo contrario.

Nota - Si decide utilizar archivos locales como servicio de nombres para la red, puede configurar otro servicio de nombres posteriormente.

Administración de nombres de host

Planifique un esquema de denominación para los sistemas que compondrán la red. Cada equipo en la red debe tener un nombre de host TCP/IP que corresponde a la dirección IP en su interfaz

de red principal. El nombre de host debe ser único en el subdominio del sistema. Como las máquinas físicas, los sistemas virtuales también deben tener una dirección IP y un nombre de host únicos.

Un sistema puede tener lo siguiente:

- Varios nombres de host que se asignan a la dirección IP del sistema. Por ejemplo, `systema.mycompany.com` también se puede conocer como `www.mycompany.com`.
- El mismo nombre de host para direcciones IPv4 e IPv6.
- Una dirección IP nueva y una dirección IP antigua y descartada que están configuradas con el mismo nombre de host durante un tiempo para permitir la numeración de red.
- Varias interfaces de red en subredes diferentes, cada una con una dirección IP y un nombre de host únicos.

Cuando planifique su red, realice una lista de las direcciones IP y sus nombres de host asociados para poder acceder a ellos fácilmente durante el proceso de configuración. Dicha lista le ayudará a verificar que todos los nombres de host sean exclusivos.

Nota - El nombre de host TCP/IP de la interfaz principal es una entidad distinta del *nombre de host del sistema* que se define con el comando `hostname`. Aunque Oracle Solaris no lo requiere, el mismo nombre se utiliza normalmente para ambos. Algunas aplicaciones de red dependen de esta regla. Consulte la página del comando man `hostname`(1) para obtener más información.

♦ ♦ ♦ CAPÍTULO 2

Planificación para el uso de direcciones IPv6

Este capítulo complementa al Capítulo 1, Planificación de la implementación de red y describe consideraciones adicionales que deben tenerse en cuenta al decidir utilizar direcciones IPv6 en la red.

Si tiene previsto utilizar direcciones IPv6 además de direcciones IPv4, asegúrese de que el ISP actual admita ambos tipos de direcciones.

Para obtener una introducción a los conceptos sobre IPv6, consulte Internet Protocol, Version 6 (IPv6) Specification (http://www.ietf.org/rfc/rfc2460.txt).

Para las tareas de configuración de IPv6, consulte "Configuración de interfaces IPv6" de "Configuración y administración de componentes de red en Oracle Solaris 11.2 ".

Para obtener información sobre la resolución de problemas de redes IPv6, consulte "Resolución de problemas con la implementación de IPv6" de "Resolución de problemas de administración de redes en Oracle Solaris 11.2 ".

Este capítulo se divide en los siguientes apartados:

Tareas de planificación de IPv6

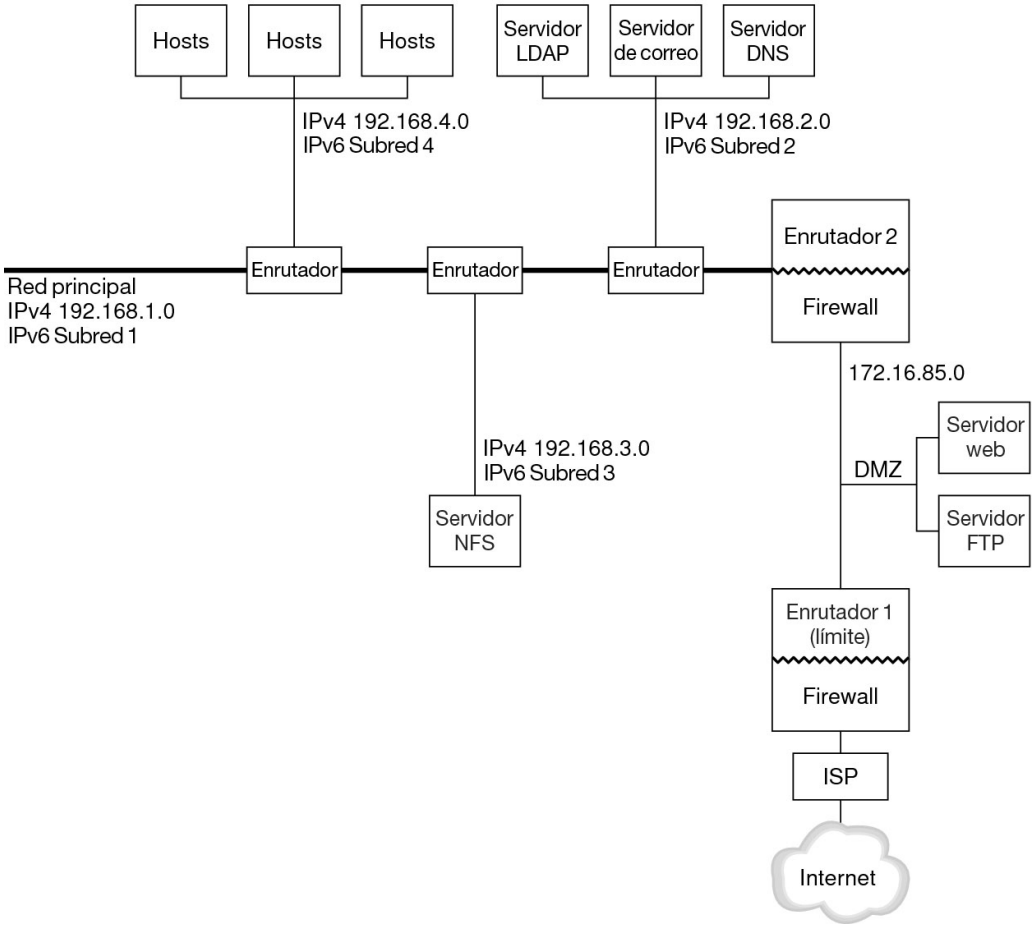
En la tabla siguiente, se describen diferentes consideraciones que deben tenerse en cuenta al planificar la implementación de IPv6 en la red. Si va a migrar de una red IPv4 existente a una red IPv6, consulte "Migración de una red IPv4 a una red IPv6" de "Configuración y administración de componentes de red en Oracle Solaris 11.2 " para obtener más instrucciones.

Tarea	Descripción	Para obtener instrucciones
Preparar el hardware para admitir IPv6.	Compruebe que el hardware se pueda actualizar a IPv6.	“Cómo garantizar la compatibilidad de hardware para IPv6” [26]
Asegurarse de que las aplicaciones estén preparadas para funcionar con IPv6.	Verifique que las aplicaciones puedan funcionar en un entorno IPv6.	“Configuración de servicios de red para admitir IPv6” [28]
Diseñar un plan para el uso de túneles.	Establezca los enrutadores que deben ejecutar túneles a otras subredes o redes externas.	“Planificación para el uso de túneles en la red” [30]
Planificar cómo proteger las redes y desarrollar una política de seguridad IPv6.	Por motivos de seguridad, se precisa un plan de direcciones para la DMZ y sus entidades antes de configurar IPv6. Decida cómo implementará la seguridad, por ejemplo, con un filtro IP, una arquitectura de seguridad IP (IPsec), el intercambio de claves de Internet (IKE) y otras funciones de seguridad de esta versión.	“Aspectos relacionados con la seguridad en la implementación de IPv6” [31] “Protección de la red en Oracle Solaris 11.2 ”
Crear un plan de direcciones para sistemas de la red.	Se debe planificar la dirección de servidores, enrutadores y hosts antes de configurar IPv6. Este paso implica obtener un prefijo de sitio para la red, además de planificar subredes IPv6, si es necesario.	“Creación de un plan de direcciones IPv6 para nodos” [27]

Descripción general de la topología de red IPv6

Por lo general, IPv6 se utiliza en una topología de red mixta que también utiliza IPv4, como se muestra en la figura siguiente. La siguiente figura se utiliza como referencia en la descripción de las tareas de configuración de IPv6 que se describen en este capítulo.

FIGURA 2-1 Situación hipotética de topología de red IPv6



La situación de red empresarial que se muestra en la figura se compone de cinco subredes con cuatro direcciones IPv4 existentes. Los vínculos de la red se corresponden directamente con las subredes administrativas. Las cuatro redes internas se muestran con direcciones IPv4 privadas en formato RFC 1918, solución habitual ante la falta de direcciones IPv4.

Estas redes internas utilizan el siguiente esquema de direcciones:

- La subred 1 es la red principal interna `192.168.1`.
- La subred 2 es la red interna `192.168.2`, con LDAP, `sendmail` y servidores DNS.
- La subred 3 es la red interna `192.168.3`, con los servidores NFS de la empresa.

- La subred 4 es la red interna `192.168.4`, que contiene hosts para los empleados de la empresa.

La red pública externa `172.16.85` funciona como DMZ de la corporación. Esta red contiene servidores web, servidores FTP anónimos y demás recursos que la empresa ofrece al entorno exterior. El enrutador 2 ejecuta un firewall y separa la red pública `172.16.85` de la red principal interna. En el otro extremo de la zona desmilitarizada (DMZ), el enrutador 1 ejecuta un firewall y actúa como enrutador de límite de la empresa.

En la Figura 2-1, “Situación hipotética de topología de red IPv6”, la DMZ pública presenta la dirección privada RFC 1918 `172.16.85`. En un entorno real, la DMZ pública debe tener registrada una dirección IPv4. La mayoría de los sitios de IPv4 emplean una combinación de direcciones públicas y direcciones privadas RFC 1918. Sin embargo, en el ámbito de IPv6 el concepto de direcciones públicas y privadas es distinto. Debido a que IPv6 dispone de mucho más espacio de direcciones, las direcciones públicas IPv6 se utilizan en redes públicas y privadas.

La pila doble de protocolos de Oracle Solaris permite operaciones simultáneas de IPv4 e IPv6. Puede ejecutar correctamente operaciones relacionadas con IPv4 durante la implementación de IPv6 en la red y después de ella. Al implementar IPv6 en una red operativa que ya utiliza IPv4, asegúrese de no interrumpir las operaciones en curso.

Cómo garantizar la compatibilidad de hardware para IPv6

Consulte la documentación de los fabricantes para conocer la compatibilidad de IPv6 con los siguientes tipos de hardware:

- enrutadores
- firewalls
- servidores
- conmutadores

Nota - Todos los procedimientos de este manual suponen que los equipos, en especial los enrutadores, se pueden actualizar a IPv6. Sin embargo, algunos modelos de enrutador no se pueden actualizar a IPv6. Para obtener más información y una solución alternativa, consulte “No se puede actualizar el enrutador IPv4 a IPv6” de “Resolución de problemas de administración de redes en Oracle Solaris 11.2 ”.

Preparación de un plan de direcciones IPv6

Una parte importante de la transición de IPv4 a IPv6 incluye el desarrollo de un plan de direcciones, que implica los siguientes preparativos:

- “Obtención de un prefijo de sitio” [27]
- “Creación del esquema de numeración de IPv6” [27]

Para las tareas de migración real, consulte “Migración de una red IPv4 a una red IPv6” de “Configuración y administración de componentes de red en Oracle Solaris 11.2 ”.

Obtención de un prefijo de sitio

Debe obtenerse un prefijo de sitio antes de configurar IPv6. El prefijo de sitio se emplea en la derivación de direcciones IPv6 para todos los nodos de la implementación de IPv6.

Un ISP que admita IPv6 puede brindar a las empresas prefijos de sitio de IPv6 de 48 bits. Si el ISP sólo admite IPv4, se puede buscar otro que sea compatible con IPv6 y mantener el ISP actual para IPv4. En tal caso, existen las siguientes soluciones alternativas. Para obtener más información, consulte “El ISP actual no admite IPv6” de “Resolución de problemas de administración de redes en Oracle Solaris 11.2 ”.

Si su organización es un ISP, los prefijos de sitio de sus clientes se obtienen del pertinente registro de Internet. Para obtener más información, consulte la página de IANA (Internet Assigned Numbers Authority) (http://www.iana.org).

Creación del esquema de numeración de IPv6

A menos que la red IPv6 que se proponga sea totalmente nueva, la topología de IPv4 ya configurada sirve de base para el esquema de numeración de IPv6.

Creación de un plan de direcciones IPv6 para nodos

En la mayoría de los hosts, la configuración automática sin estado de direcciones IPv6 para sus interfaces constituye una estrategia válida y eficaz. Cuando el host recibe el prefijo de sitio del enrutador más próximo, el protocolo ND genera de forma automática direcciones IPv6 para cada interfaz del host.

Los servidores necesitan direcciones IPv6 estables. Si no configura manualmente las direcciones IPv6 de un servidor, siempre que se reemplaza una tarjeta NIC del servidor se configura automáticamente una dirección IPv6.

Al crear direcciones para servidores, debe tenerse en cuenta lo siguiente:

- Proporcione a los servidores unos ID de interfaz descriptivos y estables. Un método consiste en aplicar un sistema de numeración consecutiva a los ID de interfaz. Por ejemplo, la interfaz interna del servidor LDAP que aparece en la Figura 2-1, “Situación hipotética de topología de red IPv6” podría convertirse en `2001:db8:3c4d:2::2`.

- Si habitualmente no cambia la numeración de la red IPv4, es buena idea utilizar como ID de interfaz las direcciones IPv4 ya creadas de los enrutadores y servidores. En la Figura 2-1, "Situación hipotética de topología de red IPv6", suponga que la interfaz del enrutador 1 para DMZ tiene la dirección IPv4 `192.168/16`. La dirección IPv4 puede convertirse a hexadecimal y aplicar el resultado como ID de interfaz. El nuevo ID de interfaz será `::7bc8:156F`.

  Este planteamiento se utiliza sólo si se es el propietario de la dirección IPv4 registrada, en lugar de haber obtenido la dirección de un ISP. Si utiliza una dirección IPv4 proporcionada por un ISP, se crea una dependencia que puede causar problemas en caso de cambiar los ISP.

Debido a la cantidad limitada de direcciones IPv4 que hay disponibles, en el pasado, un diseñador de red debía tener en cuenta si iba a utilizar direcciones registradas globales y direcciones RFC 1918 privadas. No obstante, el concepto de direcciones IPv4 globales y privadas no es aplicable a las direcciones IPv6 . Puede utilizar *direcciones unidifusión globales*, que incluyen el prefijo de sitio, en todos los enlaces de la red, incluida la DMZ pública.

Creación de un esquema de numeración para subredes

Inicie el esquema de numeración asignando las subredes IPv4 ya configuradas a subredes IPv6 equivalentes. Por ejemplo, fíjese en las subredes que se muestran en la Figura 2-1, "Situación hipotética de topología de red IPv6". Las subredes 1–4 utilizan la designación de redes privadas IPv4 de RFC 1918 para los primeros 16 bits de sus direcciones, además de los dígitos 1–4 para indicar la subred. A modo de ejemplo, suponga que el prefijo de IPv6 `2001:db8:3c4d/48` se ha asignado al sitio.

La tabla siguiente muestra la asignación de prefijos de IPv4 privados a prefijos de IPv6.

Prefijo de subred IPv4	Prefijo de subred IPv6 equivalente
`192.168.1.0/24`	`2001:db8:3c4d:1::/64`
`192.168.2.0/24`	`2001:db8:3c4d:2::/64`
`192.168.3.0/24`	`2001:db8:3c4d:3::/64`
`192.168.4.0/24`	`2001:db8:3c4d:4::/64`

Configuración de servicios de red para admitir IPv6

Los siguientes servicios de red IPv4 típicos también funcionan con IPv6:

- DNS
- HTTP (versiones Apache 2 u Orion)
- LDAP

- NFS
- `sendmail`

El servicio de correo IMAP sólo es apto para IPv4.

Los nodos configurados para IPv6 pueden ejecutar servicios de IPv4. Al activar IPv6, no todos los servicios aceptan conexiones IPv6. Los servicios conectados a IPv6 aceptarán una conexión. Los servicios que no estén conectados a IPv6 seguirán funcionando con la parte de IPv4 de la pila de protocolos.

Al actualizar los servicios a IPv6 pueden surgir algunos problemas. Para obtener detalles, consulte “Problemas encontrados al actualizar los servicios para admitir IPv6” de “Resolución de problemas de administración de redes en Oracle Solaris 11.2 ”.

▼ Cómo preparar servicios de red para admitir IPv6

1. **Actualice los servicios de red siguientes para que admitan IPv6:**

   - servidores de correo
   - servidores NIS
   - NFS

   Nota - LDAP admite IPv6 sin tener que realizar tareas de configuración propias de IPv6.

   ---

2. **Verifique que el hardware del firewall ya esté preparado para IPv6.**

   Para obtener instrucciones, consulte la documentación pertinente sobre servidores de seguridad.

3. **Verifique que otros servicios de la red se hayan conectado a IPv6.**

   Para obtener más información, consulte la publicidad adicional y la documentación relativa al software.

4. **Si el sitio implementa los servicios siguientes, asegúrese de haber tomado las medidas apropiadas:**

   - **Firewalls**: considere fortalecer las políticas establecidas para IPv4 a fin de admitir IPv6. Para otros aspectos sobre seguridad, consulte “Aspectos relacionados con la seguridad en la implementación de IPv6” [31].
   - **Correo**: en el registro de intercambiado de correo (registro MX) para DNS, considere la posibilidad de agregar la dirección IPv6 del servidor de correo.
   - **DNS**: para cuestiones específicas de DNS, consulte Cómo preparar DNS para admitir IPv6 [30].
   - **IPQoS**: use las mismas políticas *Diffserv* en un host que se usaban para IPv4.

5. **Audite los servicios de red que ofrezca un nodo antes de convertir a IPv6 dicho nodo.**

▼ Cómo preparar DNS para admitir IPv6

Oracle Solaris admite la resolución de DNS tanto en el cliente como en el servidor. Utilice el procedimiento siguiente con el fin de preparar servicios DNS para IPv6.

Para obtener más información relativa a la compatibilidad de DNS con IPv6, consulte “Trabajo con servicios de nombres y de directorio en Oracle Solaris 11.2: DNS y NIS ”.

1. **Compruebe que el servidor DNS que ejecuta la resolución de nombres recursivos esté en una pila doble (IPv4 e IPv6) o sólo en IPv4.**

2. **En el servidor DNS, rellene la base de datos de DNS con los pertinentes registros AAAA de base de datos de IPv6 en la zona de reenvío.**

Nota - Los servidores que ejecutan varios servicios fundamentales necesitan atención especial. Verifique que la red funcione correctamente. Compruebe también que todos los servicios fundamentales tengan conexión con IPv6. A continuación, agregue la dirección IPv6 del servidor a la base de datos de DNS.

---

3. **Incorpore los registros PTR relativos a los registros AAAA en la zona inversa.**

4. **Agregue datos sólo de IPv4, o de IPv6 e IPv4, en el registro NS que describe zonas.**

Planificación para el uso de túneles en la red

La implementación de IPv6 permite varias configuraciones de túneles para actuar como mecanismos de transición cuando la red migra a una combinación de IPv4 e IPv6. Los túneles posibilitan la comunicación entre redes IPv6 aisladas. Como en Internet se ejecuta mayoritariamente IPv4, los paquetes de IPv6 del sitio deben desplazarse por Internet a través de túneles hacia las redes IPv6 de destino.

A continuación se presentan varias de las situaciones hipotéticas más destacadas sobre el uso de túneles en la topología de red IPv6:

- El ISP del que adquiere servicios IPv6 permite crear un túnel desde el enrutador de límite del sitio hasta la red del ISP. La Figura 2-1, “Situación hipotética de topología de red IPv6”

muestra un túnel de esta clase. En tal caso, se debe ejecutar IPv6 manual a través de un túnel de IPv4.

- Se administra una red distribuida de gran tamaño con conectividad IPv4. Para conectar los sitios distribuidos que utilizan IPv6, puede ejecutar un túnel de 6to4 desde el enrutador de límite de cada subred.
- En ocasiones, un enrutador de la infraestructura no se puede actualizar a IPv6. En tal caso, la alternativa es crear un túnel manual en el enrutador de IPv4 con dos enrutadores de IPv6 como puntos finales.

Para obtener información sobre la configuración de túneles, consulte Capítulo 5, “Administración de túneles IP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”. Para obtener información conceptual sobre túneles, consulte “Resumen de la función Túnel IP” de “Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 11.2 ”.

Aspectos relacionados con la seguridad en la implementación de IPv6

Al implementar IPv6 en una red ya configurada, debe tener la precaución de no poner en riesgo la seguridad del sitio.

Durante las sucesivas fases en la implementación de IPv6, tenga en cuenta los siguientes aspectos relacionados con la seguridad:

- Los paquetes de IPv6 e IPv4 necesitan la misma cantidad de filtrado.
- A menudo, los paquetes de IPv6 pasan por un túnel a través de un firewall.

  Por lo tanto, debe aplicar cualquiera de las siguientes situaciones hipotéticas:

  - Haga que el firewall inspeccione el contenido en el túnel.
  - Coloque un firewall de IPv6 con reglas parecidas en el punto final del túnel del extremo opuesto.
- Determinados mecanismos de transición utilizan IPv6 sobre el protocolo de datagramas de usuario (UDP) a través de túneles IPv4. Dichos mecanismos pueden resultar peligrosos generando un cortocircuito en el firewall.
- Los nodos de IPv6 son globalmente asequibles desde fuera de la red empresarial. Si la política de seguridad prohíbe el acceso público, debe establecer reglas más estrictas con relación al firewall. Por ejemplo, considere la configuración de un *firewall con estado*.

En este manual, se incluye información sobre las siguientes características de seguridad, que pueden usarse en una implementación de IPv6:

- La función de IPsec (IP architecture security, arquitectura de seguridad IP) posibilita la protección criptográfica de paquetes IPv6. Para obtener más información, consulte Capítulo

6, “Acerca de la arquitectura de seguridad IP” de “Protección de la red en Oracle Solaris 11.2 ”.

- La función de intercambio de claves de Internet (IKE) automatiza la gestión de claves de IPsec. Para obtener más información, consulte Capítulo 8, “Acerca del intercambio de claves de Internet” de “Protección de la red en Oracle Solaris 11.2 ”.

Índice

R

S

T