

Gestión de calidad de servicio IP en Oracle® Solaris 11.1

Copyright © 1999, 2012, Oracle y/o sus filiales. Todos los derechos reservados.

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

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

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

U.S. GOVERNMENT END USERS:

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

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

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

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

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

Contenido

Prefacio	7
1 Introducción a IPQoS (descripción general)	11
Conceptos básicos de IPQoS	11
¿Qué son los servicios diferenciados?	11
Características de IPQoS	12
Dónde obtener más información sobre la teoría y práctica de la calidad del servicio	12
Ofrecimiento de calidad de servicio con IPQoS	14
Implementación de acuerdos de nivel de servicio	14
Garantía de calidad de servicio para una organización específica	14
Introducción a la política de calidad de servicio	14
Mejoramiento de la eficacia de la red con IPQoS	15
Cómo afecta el ancho de banda al tráfico de red	15
Utilización de clases de servicio para priorizar el tráfico	16
Modelo de servicios diferenciados	17
Descripción general del clasificador (ipgpc)	17
Descripción general de medidor (tokenmt y tswtclmt)	18
Descripción general de marcadores (dscpmk y dlcosmk)	19
Descripción general del control de flujo (flowacct)	20
Cómo fluye el tráfico a través de los módulos IPQoS	20
Reenvío del tráfico en una red con IPQoS	22
Punto de código DS	22
Comportamientos por salto	22
2 Planificación para una red con IPQoS (tareas)	27
Planificación de configuración IPQoS general (mapa de tareas)	27
Planificación de la distribución de la red Diffserv	28

Estrategias de hardware para la red Diffserv	28
Topologías de red IPQoS	29
Planificación de la política de calidad de servicio	31
Ayudas para planificar la política QoS	31
Planificación de la política QoS (mapa de tareas)	32
▼ Cómo preparar una red para IPQoS	33
▼ Cómo definir las clases de la política QoS	34
Definición de filtros	36
▼ Cómo definir filtros en la política QoS	37
▼ Cómo planificar el control de flujo	38
▼ Cómo planificar el comportamiento de reenvío	40
▼ Cómo planificar la recopilación de datos de flujo	43
Introducción al ejemplo de configuración IPQoS	44
Topología de IPQoS	44
3 Creación del archivo de configuración IPQoS (tareas)	47
Definición de una política QoS en el archivo de configuración IPQoS (mapa de tareas)	47
Herramientas para crear una política QoS	49
Archivo de configuración IPQoS básico	49
Creación de archivos de configuración IPQoS para servidores web	50
▼ Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico	52
▼ Cómo definir filtros en el archivo de configuración IPQoS	54
▼ Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS	56
▼ Cómo activar el control para una clase en el archivo de configuración IPQoS	59
▼ Cómo crear un archivo de configuración IPQoS para un servidor web "best-effort"	60
Creación un archivo de configuración IPQoS para un servidor de aplicaciones	63
▼ Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones	65
▼ Cómo configurar el reenvío para el tráfico de aplicaciones en el archivo de configuración IPQoS	67
▼ Cómo configurar el control de flujo en el archivo de configuración IPQoS	69
Suministro de servicios diferenciados en un enrutador	72
▼ Cómo configurar un enrutador en una red con IPQoS	72
4 Inicio y mantenimiento de IPQoS (tareas)	75
Administración IPQoS (mapa de tareas)	75

Aplicación de una configuración IPQoS	76
▼ Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS	76
▼ Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia	77
Activación del registro sys log para mensajes IPQoS	78
▼ Cómo activar el registro de mensajes IPQoS durante el inicio	78
Resolución de problemas con mensajes de error IPQoS	79
5 Uso de control de flujo y recopilación de estadísticas (tareas)	83
Establecimiento del control de flujo (mapa de tareas)	83
Registro de información sobre flujos de tráfico	84
▼ Cómo crear un archivo para datos de control de flujo	84
Recopilación de información estadística	86
6 IPQoS detallado (referencia)	89
Arquitectura IPQoS y el modelo Diffserv	89
Módulo clasificador	90
Módulo medidor	92
Módulo marcador	95
Módulo flowacct	99
Archivo de configuración IPQoS	102
Instrucción <code>action</code>	103
Definiciones de módulo	104
Cláusula <code>class</code>	104
Cláusula <code>filter</code>	105
Cláusula <code>params</code>	105
Utilidad de configuración <code>ipqosconf</code>	106
Índice	107

Prefacio

Bienvenido a Gestión de calidad de servicio IP en Oracle Solaris 11.1. Este manual forma parte de un conjunto de varios volúmenes que abarcan una parte significativa de la información de la administración del sistema Oracle Solaris. En este manual, se da por sentado que ya instaló Oracle Solaris. Debe estar listo para configurar la red o para configurar el software de red que se necesite.

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

Quién debe utilizar este manual

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

Acceso a Oracle Support

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

Convenciones tipográficas

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

TABLA P-1 Convenciones tipográficas

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

Indicadores de los shells en los ejemplos de comandos

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

TABLA P-2 Indicadores de shell

Shell	Indicador
Shell Bash, shell Korn y shell Bourne	\$
Shell Bash, shell Korn y shell Bourne para superusuario	#
Shell C	<code>nombre_sistema%</code>
Shell C para superusuario	<code>nombre_sistema#</code>

Introducción a IPQoS (descripción general)

La calidad de servicio IP (IPQoS) permite priorizar, controlar y realizar un seguimiento de las estadísticas de control. Utilizando IPQoS, puede ofrecer un nivel de servicio estable a los usuarios de la red. También puede administrar el tráfico para evitar que se congestione la red.

A continuación puede ver una lista de temas de este capítulo:

- “Conceptos básicos de IPQoS” en la página 11
- “Ofrecimiento de calidad de servicio con IPQoS” en la página 14
- “Mejoramiento de la eficacia de la red con IPQoS” en la página 15
- “Modelo de servicios diferenciados” en la página 17
- “Reenvío del tráfico en una red con IPQoS” en la página 22

Nota – Es posible que en futuras versiones se elimine la utilidad IPQoS. Se recomienda a los usuarios que, en su lugar, utilicen los comandos `ladm`, `flowadm` y comandos relacionados, que admiten funciones de control de los recursos de ancho de banda similares. Para obtener más información, consulte [Uso de redes virtuales en Oracle Solaris 11.1](#).

Conceptos básicos de IPQoS

IPQoS posibilita la arquitectura de servicios diferenciados (Diffserv) definida por el grupo de trabajo de servicios diferenciados de IETF (Internet Engineering Task Force). En Oracle Solaris, IPQoS se implementa en el nivel de IP de la pila de protocolo TCP/IP.

¿Qué son los servicios diferenciados?

Al activar IPQoS, puede proporcionar diferentes niveles de servicio de red para clientes seleccionados y aplicaciones específicas. Los diferentes niveles de servicios se denominan *servicios diferenciados*. Los servicios diferenciados que se proporcionan a los clientes pueden

estar basados en una estructura de niveles de servicio que su compañía ofrezca a los clientes. También puede ofrecer servicios diferenciados según las prioridades definidas para aplicaciones o usuarios de la red.

Para proporcionar calidad de servicio se deben llevar a cabo las siguientes actividades:

- Delegar los niveles de servicio a diferentes grupos, como clientes o departamentos de una empresa
- Priorizar los servicios de red que se ofrecen a grupos o aplicaciones específicos
- Descubrir y eliminar áreas de cuello de botella de la red y otros tipos de congestión
- Supervisar el rendimiento de la red y proporcionar estadísticas de rendimiento
- Regular el ancho de banda hasta y desde recursos de red

Características de IPQoS

IPQoS tiene las siguientes características:

- Herramienta de línea de comandos `ipqosconf` para configurar la política QoS
- Clasificador que selecciona acciones basadas en filtros que configuran la política QoS de la organización
- Módulo de medición para medir el tráfico de red que cumple el modelo Diffserv
- Diferenciación del servicio basada en la posibilidad de marcar el encabezado IP de un paquete con información de redirección
- Módulo de control de flujo que realiza un seguimiento de las estadísticas de flujo de tráfico
- Recopilación de estadísticas de clases de tráfico mediante el comando `ksstat` de UNIX®
- Compatibilidad con la arquitectura SPARC® y x86
- Compatibilidad con direcciones IPv4 e IPv6
- Interoperatividad con la arquitectura de seguridad IPsec
- Compatibilidad con marcados de prioridad de usuario 802.1D para redes de área local virtuales (VLAN)

Dónde obtener más información sobre la teoría y práctica de la calidad del servicio

Puede obtener información sobre servicios diferenciados y calidad del servicio de diferentes fuentes impresas y en línea.

Libros sobre la calidad del servicio

Si necesita más información sobre la teoría y la práctica de la calidad del servicio, consulte los siguientes libros:

- Ferguson, Paul y Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Kilkki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.

Petición de comentarios (RFC) sobre la calidad de servicio

La IPQoS cumple con las especificaciones descritas en las siguientes RFC y en los siguientes borradores de Internet:

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* (<http://www.ietf.org/rfc/rfc2474.txt?number=2474>): describe una mejora del campo de tipo de servicio (ToS) o campos DS de los encabezados de paquetes IPv4 e IPv6 para admitir servicios diferenciados.
- RFC 2475, *An Architecture for Differentiated Services* (<http://www.ietf.org/rfc/rfc2475.txt?number=2475>): proporciona una descripción detallada de la organización y de los módulos de la arquitectura Diffserv.
- RFC 2597, *Assured Forwarding PHB Group* (<http://www.ietf.org/rfc/rfc2597.txt?number=2597>): describe cómo funciona el comportamiento por salto del reenvío asegurado (AF).
- RFC 2598, *An Expedited Forwarding PHB* (<http://www.ietf.org/rfc/rfc2598.txt?number=2598>): describe cómo funciona el comportamiento por salto de reenvío acelerado (EF).
- Borrador de Internet, *Un modelo de administración informal para enrutadores Diffserv*: presenta un modelo para implementar la arquitectura Diffserv en enrutadores.

Sitios web con información sobre calidad del servicio

El grupo de trabajo sobre servicios diferenciados del IETF mantiene un sitio web con enlaces a borradores de Internet sobre Diffserv:

<http://www.ietf.org/html.charters/diffserv-charter.html>.

Los fabricantes de enrutadores, como Cisco Systems y Juniper Networks, proporcionan información en sus sitios web corporativos sobre cómo implementar servicios diferenciados en sus productos.

Páginas del comando man de IPQoS

La documentación de IPQoS incluye las siguientes páginas del comando man:

- `ipqosconf(1M)`: describe el comando para configurar el archivo de configuración IPQoS.
- `ipqos(7ipp)`: describe la implementación de IPQoS del modelo de arquitectura Diffserv.

- `ipgpc(7ipp)`: describe la implementación de IPQoS de un clasificador Diffserv.
- `tokenmt(7ipp)`: describe el medidor `tokenmt` de IPQoS.
- `tswtclmt(7ipp)`: describe el medidor IPQoS `tswtclmt`.
- `dscpmk(7ipp)`: describe el módulo de marcador DSCP.
- `dlcosmk(7ipp)`: describe el módulo de marcador de prioridad de usuario IPQoS 802.1D.
- `flowacct(7ipp)`: describe el módulo de control de flujo IPQoS.
- `acctadm(1M)`: describe el comando de configuración de utilidades de contabilidad ampliada de Oracle Solaris. El comando `acctadm` incluye extensiones IPQoS.

Ofrecimiento de calidad de servicio con IPQoS

Las funciones IPQoS permiten a los proveedores de Internet (ISP) y proveedores de aplicaciones (ASP) ofrecer diferentes niveles de servicio de red a los clientes. Estas funciones permiten a las empresas e instituciones educativas priorizar servicios para organizaciones internas o aplicaciones principales.

Implementación de acuerdos de nivel de servicio

Si su organización es un ISP o ASP, puede basar la configuración IPQoS en el *acuerdo de nivel de servicio* (SLA) que la empresa ofrezca a sus clientes. En un acuerdo SLA, un proveedor garantiza a un cliente un nivel de servicio de red específico según categorías de precios. Por ejemplo, un acuerdo SLA de máxima calidad garantiza que el cliente reciba la prioridad máxima para todos los tipos de tráfico de red 24 horas al día. Del mismo modo, un acuerdo SLA de calidad media garantiza que el cliente reciba prioridad máxima para el correo electrónico durante el horario de negocios. El resto del tráfico puede recibir prioridad media 24 horas al día.

Garantía de calidad de servicio para una organización específica

Si su organización es una empresa o una institución, también puede proporcionar funciones de calidad de servicio para la red. Puede garantizar que el tráfico de un grupo específico o de una aplicación determinada reciba un grado de servicio mayor o menor.

Introducción a la política de calidad de servicio

Para implementar la calidad de servicio debe definir una *política de calidad de servicio* (QoS). La política QoS define varios atributos de red, como prioridades de clientes o aplicaciones, y

acciones para tratar diferentes categorías de tráfico. La política QoS de la organización se define en un archivo de configuración IPQoS. Este archivo configura los módulos IPQoS que residen en el núcleo de Oracle Solaris. Un host con una política IPQoS se considera un *sistema con IPQoS*.

Normalmente, la política QoS define lo siguiente:

- Grupos independientes de tráfico de red denominados *clases de servicio*.
- Sistemas de medición para regular la cantidad de tráfico de red de cada clase. Estas medidas controlan el proceso de control del tráfico denominado *medición*.
- Una acción que un sistema IPQoS y un enrutador Diffserv deben aplicar al flujo de un paquete. Este tipo de acción se denomina *comportamiento por salto* (PHB).
- Cualquier seguimiento de estadísticas que necesite su organización para una clase de servicio. Un ejemplo es el tráfico generado por un cliente o aplicación específicos.

Cuando los paquetes se transfieren a la red, el sistema con IPQoS evalúa los encabezados de los paquetes. La acción que realiza el sistema IPQoS la determina la política QoS.

Las tareas para diseñar la política QoS se describen en la sección [“Planificación de la política de calidad de servicio” en la página 31](#).

Mejoramiento de la eficacia de la red con IPQoS

IPQoS incluye funciones que permiten mejorar el rendimiento de la red mediante el uso de la calidad de servicio. Con la expansión de las redes informáticas, también aumenta la necesidad de administrar el tráfico de red generado por el número creciente de usuarios y los procesadores más potentes. Algunos de los síntomas de una red saturada son la pérdida de datos y la congestión del tráfico. Ambos síntomas dan como resultado tiempos de respuesta lentos.

En el pasado, los administradores de sistemas solucionaban los problemas de tráfico de red añadiendo más ancho de banda. A menudo, el nivel de tráfico de los vínculos variaba de manera notable. Con IPQoS, puede administrar el tráfico de la red y determinar con facilidad si es necesario realizar una expansión, y dónde.

Por ejemplo, para una compañía o institución, es necesario mantener una red efectiva para evitar los cuellos de botella. También es necesario garantizar que un grupo o aplicación no consume más ancho de banda del asignado. Para un proveedor ISP o ASP, es necesario administrar el rendimiento de la red para garantizar que los clientes reciben el servicio de red por el que pagan.

Cómo afecta el ancho de banda al tráfico de red

Puede usar IPQoS para regular el *ancho de banda* de la red, es decir, la cantidad máxima de datos que puede transferir un dispositivo o un enlace de red. La política QoS debe priorizar el

uso del ancho de banda para proporcionar calidad de servicio a los clientes o usuarios. Los módulos de medición de IPQoS permiten medir y controlar la asignación de ancho de banda entre las diferentes clases de tráfico en un host con IPQoS.

Antes de poder administrar de manera efectiva el tráfico de la red, debe responder a estas preguntas sobre el uso del ancho de banda:

- ¿Cuáles son las áreas de problemas de tráfico de su red local?
- ¿Qué debe hacer para conseguir la utilización óptima del ancho de banda disponible?
- ¿Cuáles son las aplicaciones de mayor importancia de su organización que deben tener la prioridad máxima?
- ¿Qué aplicaciones pueden congestionarse?
- ¿Cuáles son las aplicaciones de menor importancia, que pueden tener la prioridad más baja?

Utilización de clases de servicio para priorizar el tráfico

Para implementar la calidad de servicio, debe analizar el tráfico de la red para determinar los grandes grupos en los que se puede dividir el tráfico. Después, debe organizar los grupos en clases de servicio con características y prioridades individuales. Estas clases forman las categorías básicas en las que se basa la política QoS de la organización. Las clases de servicio representan los grupos de tráfico que se desea controlar.

Por ejemplo, un proveedor puede ofrecer niveles de servicio platino, oro, plata y bronce, con una escala de diferentes precios. Un acuerdo SLA platino puede garantizar una prioridad máxima para el tráfico entrante destinado a un sitio web que el ISP aloja para el cliente. Por lo tanto, el tráfico entrante del sitio web del cliente podría ser una clase de tráfico.

Para una empresa, se pueden crear clases de servicio basadas en los requisitos de los departamentos. También se pueden crear clases basadas en el nivel de utilización de una aplicación específica en el tráfico de red.

A continuación puede ver algunos ejemplos de clases de tráfico de una empresa:

- Aplicaciones muy utilizadas, como correo electrónico y FTP saliente a un servidor específico, cada una podría ser una clase. Debido a que los empleados utilizan estas aplicaciones constantemente, su política QoS puede garantizar una pequeña cantidad de ancho de banda y una prioridad más baja al correo electrónico y FTP.
- Una base de datos de entrada que debe estar activa las 24 horas del día. Según la importancia de la aplicación de base de datos para la empresa, puede asignarle una gran cantidad de ancho de banda y una prioridad alta.

- Un departamento que realiza un trabajo de vital importancia o que debe tratarse con cuidado, como el departamento de salarios y nóminas. La importancia del departamento para la organización determina la prioridad y la cantidad de ancho de banda que se le asignará.
- Llamadas entrantes al sitio web externo de una compañía. A esta clase se le puede asignar una pequeña cantidad de ancho de banda con prioridad baja.

Modelo de servicios diferenciados

IPQoS incluye los siguientes módulos, que forman parte de la arquitectura de *servicios diferenciados (Diffserv)* definida en RFC 2475:

- Clasificador
- Medidor
- Marcador

IPQoS añade las siguientes mejoras al modelo Diffserv:

- Módulo de control de flujo
- Marcador de datagrama 802.1D

En esta sección se explican los módulos Diffserv tal y como se utilizan en IPQoS. Es necesario conocer estos módulos, sus nombres y su utilización para configurar la política QoS. Si necesita información detallada sobre cada módulo, consulte la sección “[Arquitectura IPQoS y el modelo Diffserv](#)” en la página 89.

Descripción general del clasificador (ipgpc)

En el modelo Diffserv, el *clasificador* selecciona los paquetes de un flujo de tráfico de red. Un *flujo de tráfico* consiste en un grupo de paquetes con información idéntica en los siguientes campos de encabezado de IP:

- Dirección de origen
- Dirección de destino
- Puerto de origen
- Puerto de destino
- Número de protocolo

En IPQoS, estos campos se conocen como *5-tuple*.

El módulo clasificador de IPQoS se llama *ipgpc*. El clasificador *ipgpc* organiza los flujos de tráfico en clases según las características definidas en el archivo de configuración IPQoS.

Si necesita información detallada sobre *ipgpc*, consulte la sección “[Módulo clasificador](#)” en la página 90.

Clases IPQoS

Una *clase* es un grupo de flujos de red que comparten características similares. Por ejemplo, un ISP puede definir clases que representen los diferentes niveles de servicio ofrecidos a los clientes. Un ASP puede definir acuerdos SLA que asignen diferentes niveles de servicio a distintas aplicaciones. En la política QoS de un ASP, una clase puede incluir tráfico FTP saliente destinado a una dirección IP de destino específica. El tráfico saliente del sitio web externo de una empresa también puede definirse como una clase.

Agrupar el tráfico en clases es una parte importante de la planificación de la política QoS. Al crear clases utilizando la herramienta `ipqosconf`, se está configurando el clasificador `ipgpc`.

Si necesita información sobre cómo definir clases, consulte la sección [“Cómo definir las clases de la política QoS” en la página 34.](#)

Filtros IPQoS

Los *filtros* son conjuntos de reglas que contienen parámetros denominados *selectores*. Cada filtro debe hacer referencia a una clase. IPQoS compara los paquetes con los selectores de cada filtro para determinar si el paquete pertenece a la clase del filtro. Se puede filtrar un paquete utilizando diferentes selectores, por ejemplo, 5-tuple de IPQoS y otros parámetros comunes:

- Dirección de origen y dirección de destino
- Puerto de origen y puerto de destino
- Números de protocolo
- ID de usuario
- ID de proyecto
- Punto de código de servicios diferenciados (DSCP)
- Índice de interfaz

Por ejemplo, un filtro sencillo puede incluir el puerto de destino con un valor de 80. A continuación, el clasificador `ipgpc` selecciona todos los paquetes que están vinculados con el puerto de destino 80 (HTTP) y gestiona los paquetes según lo estipulado en la política QoS.

Si necesita información sobre cómo crear filtros, consulte la sección [“Cómo definir filtros en la política QoS” en la página 37.](#)

Descripción general de medidor (tokenmt y tswtclmt)

En el modelo Diffserv, el *medidor* realiza un seguimiento de la tasa de transmisión de los flujos de tráfico por clase. El medidor evalúa la medida en que la tasa actual del flujo se ajusta a las tasas configuradas para determinar el resultado apropiado. Según el resultado de los flujos de tráfico, el medidor selecciona una acción subsiguiente. Las acciones subsiguientes pueden incluir enviar el paquete a otra acción o devolver el paquete a la red sin más procesamiento.

Los medidores IPQoS determinan si un flujo de red cumple la tasa de transmisión definida para su clase en la política QoS. IPQoS incluye dos módulos de medición:

- `tokenmt`: utiliza un esquema de medición con conjunto de dos tokens.
- `tswtclmt`: utiliza un esquema de medición de fase temporal de desplazamiento.

Ambos módulos de medición reconocen tres resultados: rojo, amarillo y verde. Las acciones que deben tomarse para cada resultado se definen en los parámetros `red_action_name`, `yellow_action_name` y `green_action_name`.

También puede configurar `tokenmt` para que reconozca colores. Una instancia de medición que tenga presente el color utiliza el tamaño del paquete, DSCP, tasa de tráfico y parámetros configurados para determinar el resultado. El medidor utiliza el DSCP para asignar el resultado del paquete al color verde, amarillo o rojo.

Si necesita información sobre cómo definir parámetros para los medidores IPQoS, consulte la sección [“Cómo planificar el control de flujo”](#) en la página 38.

Descripción general de marcadores (`dscpmk` y `dlcosmk`)

En el modelo Diffserv, el *marcador* marca un paquete con un valor que refleja un comportamiento de reenvío. El *marcado* es el proceso de colocar un valor en el encabezado del paquete para indicar cómo se debe reenviar el paquete a la red.

IPQoS contiene dos módulos de marcado:

- `dscpmk`: marca el campo DS del encabezado de un paquete IP con un valor numérico denominado *punto de código de servicios diferenciados* o DSCP. Un enrutador que admita Diffserv puede utilizar el punto de código DS para aplicar el comportamiento de reenvío correspondiente al paquete.
- `dlcosmk`: marca la etiqueta de red de área local virtual (VLAN) del encabezado de un frame Ethernet con un valor numérico denominado *prioridad de usuario*. La prioridad de usuario indica la *clase de servicio (CoS)*, que define el comportamiento de reenvío que debe aplicarse al datagrama.

`dlcosmk` es una agregación de IPQoS que no forma parte del modelo Diffserv designado por IETF.

Si necesita información sobre cómo utilizar un sistema de marcadores para la política QoS, consulte [“Cómo planificar el comportamiento de reenvío”](#) en la página 40.

Descripción general del control de flujo (flowacct)

IPQoS agrega el módulo de control `flowacct` al modelo Diffserv. El módulo `flowacct` puede usarse para recopilar estadísticas sobre el flujo de tráfico y cobrar a los clientes según su acuerdo SLA. El control de flujo también es útil para la planificación de la capacidad y la supervisión de sistemas.

El módulo `flowacct` puede usarse con el comando `acctadm` para crear un archivo de registro de control. Un registro básico incluye IPQoS 5-tuple y dos atributos adicionales, como se muestra en la siguiente lista:

- Dirección de origen
- Puerto de origen
- Dirección de destino
- Puerto de destino
- Número de protocolo
- Número de paquetes
- Número de bytes

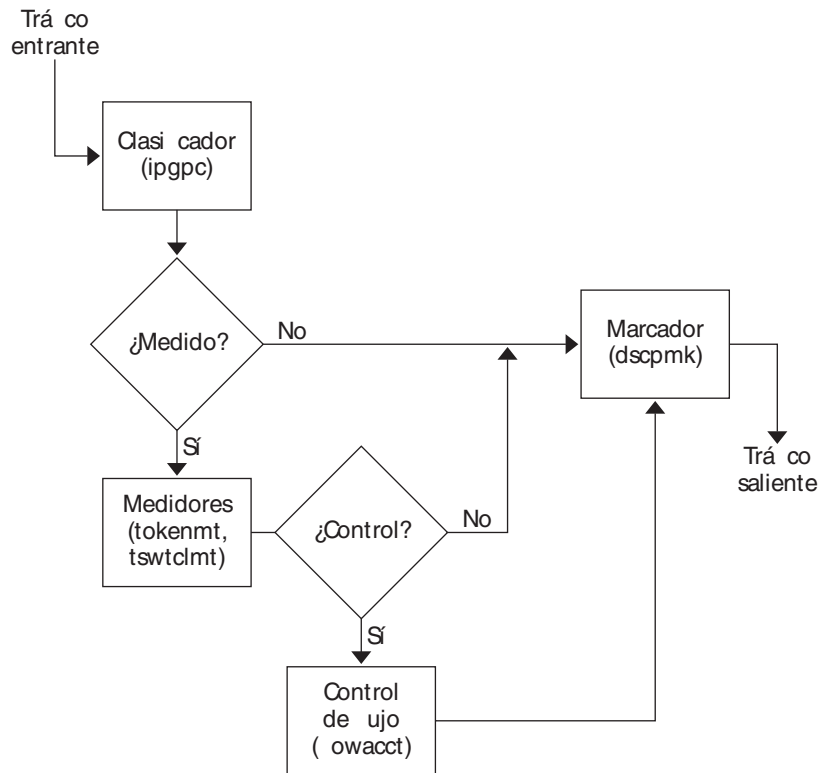
También puede recopilar estadísticas de otros atributos, como se describe en la sección [“Registro de información sobre flujos de tráfico” en la página 84](#), y en las páginas de comando `man flowacct(7ipp)` y `acctadm(1M)`.

Si necesita más información sobre cómo planificar una estrategia de control de flujo, consulte la sección [“Cómo planificar la recopilación de datos de flujo” en la página 43](#).

Cómo fluye el tráfico a través de los módulos IPQoS

En la siguiente figura se muestra una ruta que puede utilizar el tráfico entrante mediante algunos de los módulos IPQoS.

FIGURA 1-1 Flujo de tráfico a través de la implementación IPQoS del modelo Diffserv



Esta figura ilustra una secuencia de flujo de tráfico común en un sistema con IPQoS:

1. El clasificador selecciona todos los paquetes del flujo que cumplen los criterios de filtrado de la política QoS del sistema.
2. A continuación, se evalúan los paquetes para determinar la acción que se debe ejecutar.
3. El clasificador envía al marcador cualquier tráfico que no requiera control de flujo.
4. El tráfico que requiere control de flujo se envía al medidor.
5. El medidor fuerza la tasa configurada. A continuación, el medidor asigna un valor de cumplimiento de tráfico a los paquetes de flujo controlado.
6. Se evalúan los paquetes de flujo controlado para determinar si necesitan control.
7. El medidor envía al marcador el tráfico que no requiere control de flujo.
8. El módulo de control de flujo recopila estadísticas sobre los paquetes recibidos. A continuación, el módulo envía los paquetes al marcador.
9. El marcador asigna un punto de código DS al encabezado del paquete. Este DSCP indica el comportamiento por salto que un sistema con Diffserv debe aplicar al paquete.

Reenvío del tráfico en una red con IPQoS

En esta sección se explican los elementos relacionados con el reenvío de paquetes en una red con IPQoS. Un sistema con IPQoS gestiona cualquier paquete del flujo de la red con la dirección IP del sistema como destino. A continuación, aplica la política QoS al paquete para establecer servicios diferenciados.

Punto de código DS

El punto de código DS (DSCP) define en el encabezado del paquete la acción que cualquier sistema con Diffserv debe ejecutar en un paquete marcado. La arquitectura diffserv define un conjunto de puntos de código DS que utilizarán los sistemas con IPQoS y enrutadores diffserv. La arquitectura Diffserv también define un conjunto de acciones denominadas *comportamientos de reenvío*, que corresponden a los DSCP. El sistema IPQoS marca los bits precedentes del campo DS del encabezado del paquete con el DSCP. Cuando un enrutador recibe un paquete con un valor DSCP, aplica el comportamiento de reenvío asociado a dicho DSCP. Después, el paquete se envía a la red.

Nota – El marcador `d\cosmk` no utiliza el DSCP. En su lugar, `d\cosmk` marca los encabezados de frame Ethernet con un valor de CoS. Si quiere configurar IPQoS en una red que utiliza dispositivos VLAN, consulte la sección [“Módulo marcador” en la página 95](#).

Comportamientos por salto

En la terminología Diffserv, el comportamiento de reenvío asignado a un DSCP se denomina *comportamiento por salto (PHB)*. El PHB define la precedencia de reenvío que un paquete marcado recibe en relación con otro tráfico del sistema con Diffserv. Esta precedencia determina si el sistema con IPQoS o enrutador Diffserv reenvía o descarta el paquete marcado. Para un paquete reenviado, cada enrutador Diffserv que el paquete encuentra en la ruta hasta su destino aplica el mismo PHB. La excepción ocurre si otro sistema Diffserv cambia el DSCP. Si necesita más información sobre PHB, consulte la sección [“Utilización del marcador `ds cpmk` para reenviar paquetes” en la página 95](#).

El objetivo de PHB es proporcionar una cantidad específica de recursos de red a una clase de tráfico en la red contigua. Puede conseguir este objetivo en la política QoS. Defina los puntos DSCP que indican los niveles de precedencia para las clases de tráfico cuando los flujos de tráfico abandonan el sistema con IPQoS. Las precedencias pueden alternar entre alta precedencia/baja probabilidad de descarte y baja precedencia/alta probabilidad de descarte.

Por ejemplo, la política QoS puede asignar a una clase de tráfico un DSCP que garantice un PHB de baja probabilidad de descarte. Esta clase de tráfico recibirá un PHB de precedencia de baja probabilidad de descarte de cualquier enrutador con Diffserv, lo que garantiza el ancho de

banda para paquetes de esta clase. Puede añadir a la política QoS otros puntos DSCP que asignen diferentes niveles de precedencia a las clases de tráfico. Los sistemas Diffserv asignan ancho de banda a los paquetes de baja precedencia según las prioridades indicadas en los puntos DSCP de los paquetes.

IPQoS admite dos tipos de comportamientos de reenvío, definidos en la arquitectura Diffserv, reenvío acelerado y reenvío asegurado.

Reenvío acelerado

El comportamiento por salto de *reenvío acelerado (EF)* garantiza que cualquier clase de tráfico con DSCP relacionado con reenvíos EF tenga la prioridad más alta. El tráfico con DSCP EF no se pone en cola. EF proporciona una pérdida de datos, latencia y demora mínimas. El DSCP recomendado para EF es 101110. Un paquete que esté marcado con 101110 recibe una precedencia de baja probabilidad de descarte asegurada al atravesar redes Diffserv hacia su destino. Utilice DSCP EF al asignar prioridad a clientes o aplicaciones con un acuerdo SLA de nivel alto.

Reenvío asegurado

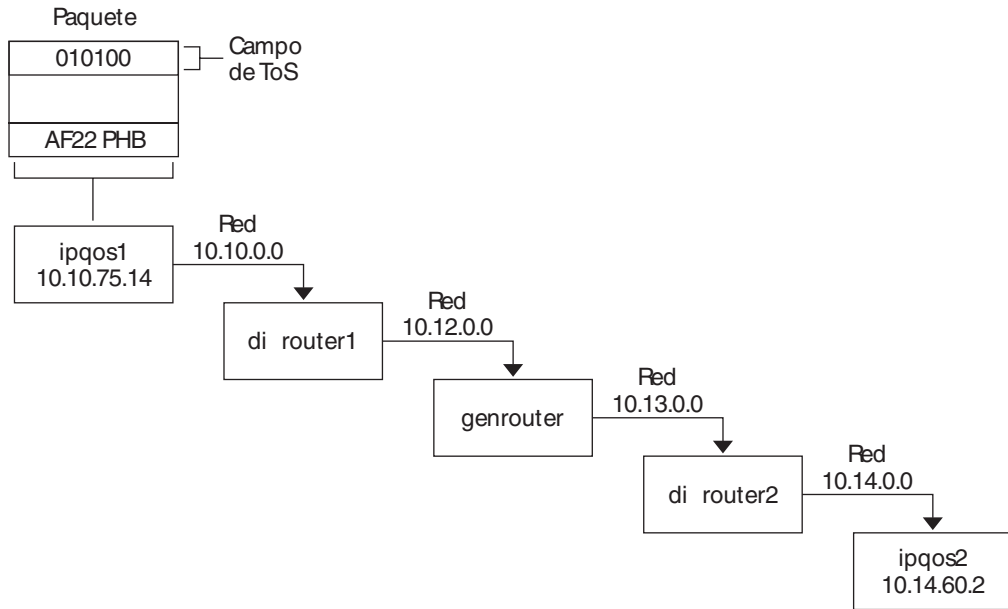
El comportamiento por salto de *reenvío asegurado (AF)* proporciona cuatro clases de reenvío diferentes que se pueden asignar a un paquete. Cada clase de reenvío proporciona tres precedencias de descarte, tal y como se muestra en la [Tabla 6-2](#).

Los diferentes puntos de código AF permiten asignar distintos niveles de servicio a clientes y aplicaciones. Puede priorizar tráfico y servicios de la red al planificar la política QoS. Después, puede asignar diferentes niveles AF para priorizar el tráfico.

Reenvío de paquetes en un entorno Diffserv

En la siguiente figura se muestra parte de una intranet de una compañía con un entorno que utiliza Diffserv parcialmente. En este escenario, todos los hosts de las redes 10.10.0.0 y 10.14.0.0 utilizan IPQoS, y los enrutadores locales de ambas redes utilizan Diffserv. Aunque las redes intermedias no están configuradas para utilizar Diffserv.

FIGURA 1-2 Reenvío de paquetes en saltos de red con Diffserv



Los siguientes pasos muestran el flujo del paquete mostrado en la figura. Los pasos comienzan con el progreso de un paquete originado en el host ipqos1. Los pasos continúan con varios saltos hasta el host ipqos2.

1. El usuario de ipqos1 ejecuta el comando ftp para acceder al host ipqos2, que está a tres saltos de distancia.
2. ipqos1 aplica su política QoS al flujo de paquetes resultante. ipqos1, luego, clasifica correctamente el tráfico ftp.

El administrador del sistema creó una clase para todo el tráfico ftp saliente que se origina en la red local 10.10.0.0. Al tráfico para la clase ftp se le asigna el comportamiento por salto AF22: clase dos, precedencia con probabilidad de descarte media. Se ha asignado una tasa de flujo de tráfico de 2 Mb/s a la clase ftp.

3. ipqos -1 mide el flujo ftp para determinar si excede la tasa asignada de 2 Mbit/s.
4. El marcador de ipqos1 marca los campos DS de los paquetes ftp salientes con el DSCP 010100, que corresponde a AF22 PHB.
5. El enrutador di ff router1 recibe los paquetes ftp. A continuación, di ff router1 comprueba el DSCP. Si di ff router1 está congestionado, los paquetes marcados con AF22 se descartan.
6. El tráfico ftp se reenvía al siguiente salto de acuerdo con el comportamiento por salto configurado para AF22 en los archivos de di ff router1.

7. El tráfico ftp atraviesa la red 10.12.0.0 hasta genrouter, que no utiliza Diffserv. Como resultado, el tráfico recibe el comportamiento de reenvío "mejor posible".
8. genrouter transfiere el tráfico ftp a la red 10.13.0.0, donde lo recibe diffrouter2.
9. diffrouter2 utiliza Diffserv. Por lo tanto, el enrutador reenvía los paquetes ftp a la red de acuerdo con el PHB definido en la política del enrutador para paquetes AF22.
10. ipqos2 recibe el tráfico ftp. ipqos2 solicita al usuario de ipqos1 un nombre de usuario y contraseña.

Planificación para una red con IPQoS (tareas)

Puede configurar IPQoS en cualquier sistema que ejecute Oracle Solaris. El sistema IPQoS funciona con enrutadores con Diffserv para proporcionar servicios diferenciados y administración del tráfico en una intranet.

Este capítulo contiene tareas de planificación para añadir sistemas con IPQoS a una red con Diffserv. Se tratan los temas siguientes.

- “Planificación de configuración IPQoS general (mapa de tareas)” en la página 27
- “Planificación de la distribución de la red Diffserv” en la página 28
- “Planificación de la política de calidad de servicio” en la página 31
- “Planificación de la política QoS (mapa de tareas)” en la página 32
- “Introducción al ejemplo de configuración IPQoS” en la página 44

Nota – Es posible que en futuras versiones se elimine la utilidad IPQoS. Se recomienda a los usuarios que, en su lugar, utilicen los comandos `dladm`, `flowadm` y comandos relacionados, que admiten funciones de control de los recursos de ancho de banda similares. Para obtener más información, consulte *Uso de redes virtuales en Oracle Solaris 11.1*.

Planificación de configuración IPQoS general (mapa de tareas)

Para la implementación de servicios diferenciados, como IPQoS, en una red se requiere una planificación exhaustiva. Debe considerarse no sólo la posición y función de cada sistema con IPQoS, sino también la relación de cada sistema con el enrutador de la red local. El mapa de tareas siguiente muestra las principales tareas de planificación para implementar IPQoS en la red, y contiene vínculos a procedimientos para realizar las tareas.

Tarea	Descripción	Para obtener instrucciones
1. Planificar una distribución de red Diffserv que incorpore los sistemas con IPQoS.	Adquirir conocimientos sobre las diferentes distribuciones de red Diffserv para determinar cuál es la mejor solución en su caso.	“Planificación de la distribución de la red Diffserv” en la página 28.
2. Planificar los diferentes tipos de servicios que ofrecerán los sistemas IPQoS.	Organizar los tipos de servicios que proporciona la red en acuerdos de nivel de servicio (SLA).	“Planificación de la política de calidad de servicio” en la página 31.
3. Planificar la política QoS para cada sistema IPQoS.	Decidir cuáles son las funciones de clases, medición y recopilación de datos necesarias para cada acuerdo SLA.	“Planificación de la política de calidad de servicio” en la página 31.
4. Si procede, planificar la política del enrutador Diffserv.	Establecer las políticas de planificación y espera en cola del enrutador Diffserv utilizado con los sistemas IPQoS.	Consulte la documentación del enrutador si necesita información sobre las políticas de espera en cola y planificación.

Planificación de la distribución de la red Diffserv

Para proporcionar servicios diferenciados para la red, necesita al menos un sistema con IPQoS y un enrutador con Diffserv. Puede expandir esta configuración básica de diferentes modos, como se explica en esta sección.

Estrategias de hardware para la red Diffserv

Normalmente, los clientes utilizan IPQoS en servidores y consolidaciones de servidores. También puede utilizar IPQoS en sistemas de escritorio, según las necesidades de la red.

La siguiente lista contiene posibles sistemas para una configuración IPQoS:

- Sistemas Oracle Solaris que ofrecen varios servicios, como servidores web o de base de datos
- Servidores de aplicaciones que ofrecen servicios de correo electrónico, FTP y otras aplicaciones de red comunes
- Servidores de caché web o proxy
- Redes de conjuntos de servidores con IPQoS administradas por equilibradores de carga con Diffserv
- Cortafuegos que administran el tráfico de una red heterogénea
- Sistemas IPQoS que forman parte de una red de área local (LAN) virtual

Puede integrar sistemas IPQoS en una distribución de red que ya tenga enrutadores con Diffserv en funcionamiento. Si el enrutador que utiliza no admite Diffserv, considere las

soluciones Diffserv que ofrecen Cisco Systems, Juniper Networks y otros fabricantes de enrutadores. Si el enrutador local no utiliza Diffserv, se limita a transferir los paquetes marcados al siguiente salto sin evaluar las marcas.

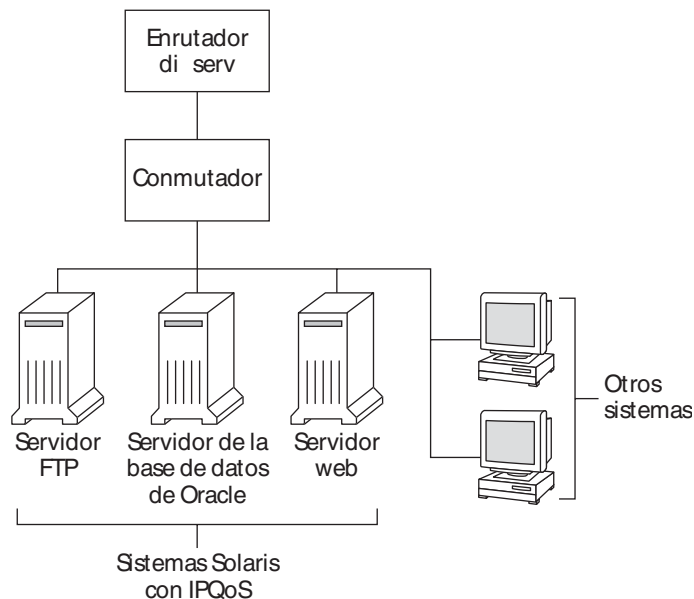
Topologías de red IPQoS

En esta sección se muestran las estrategias de IPQoS para las diversas necesidades de la red.

IPQoS en hosts individuales

En la siguiente figura se muestra una red de sistemas con IPQoS.

FIGURA 2-1 Sistemas IPQoS en un segmento de red



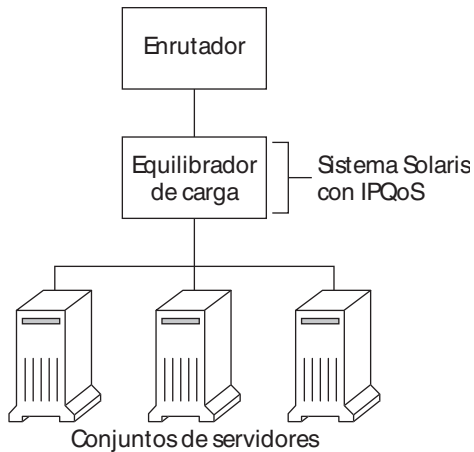
Esta red es sólo un segmento de una intranet empresarial. Activando IPQoS en los servidores de aplicaciones y servidores web, puede controlar la tasa a la que cada sistema IPQoS envía el tráfico saliente. Si configura el enrutador para utilizar Diffserv, puede obtener un mayor grado de control del tráfico entrante y saliente.

El ejemplo de esta guía utiliza una configuración con IPQoS en un único host. Para ver la topología de ejemplo que se utiliza en esta guía, consulte la [Figura 2-4](#).

IPQoS en una red de conjuntos de servidores

En la siguiente figura se muestra una red con varios conjuntos de servidores heterogéneos.

FIGURA 2-2 Red de conjuntos de servidores con IPQoS



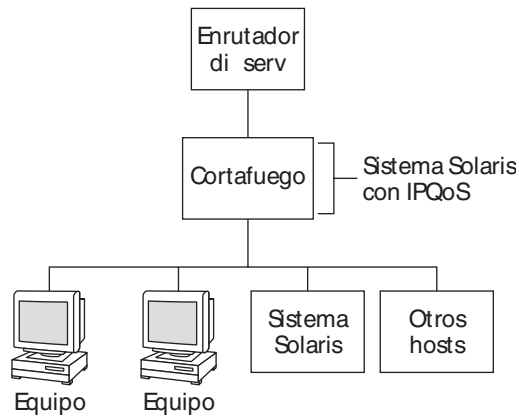
En esta distribución, el enrutador utiliza Diffserv y, por lo tanto, puede poner en cola y tasar el tráfico entrante y saliente. El equilibrador de carga también utiliza Diffserv y los conjuntos de servidores usan IPQoS. El equilibrador de carga permite realizar un filtrado adicional al del enrutador utilizando selectores como el ID de usuario o de proyecto. Estos selectores están incluidos en los datos de aplicación.

Esta configuración permite controlar el flujo y reenviar el tráfico para administrar la congestión en la red local. También evita que el tráfico saliente de los conjuntos de servidores sobrecargue otros sectores de la intranet.

IPQoS en un cortafuegos

En la siguiente figura se muestra un segmento de una red corporativa protegida de otros segmentos mediante un cortafuegos.

FIGURA 2-3 Red protegida por un cortafuegos con IPQoS



En esta configuración, el tráfico fluye hasta un enrutador con Diffserv que filtra y pone en cola los paquetes. Todo el tráfico entrante reenviado por el enrutador se transfiere al cortafuegos con IPQoS. Para utilizar IPQoS, el cortafuegos no debe omitir la pila de reenvío de IP.

La política de seguridad del cortafuegos determina si el tráfico entrante puede entrar o salir de la red interna. La política QoS controla los niveles de servicio para el tráfico entrante que ha pasado el cortafuegos. Según la política QoS, el tráfico saliente también puede marcarse con un comportamiento de reenvío.

Planificación de la política de calidad de servicio

Al planificar la política de calidad de servicio (QoS) debe revisar, clasificar y después priorizar los servicios que proporciona la red. También debe evaluar la cantidad de ancho de banda disponible para determinar la tasa a la que cada clase de tráfico se transfiere en la red.

Ayudas para planificar la política QoS

Recopile información para planificar la política QoS en un formato que incluya los datos necesarios para el archivo de configuración IPQoS. Por ejemplo, puede usar la siguiente plantilla para realizar una lista de las categorías de información principales que se utilizarán en el archivo de configuración IPQoS.

TABLA 2-1 Plantilla de planificación QoS

Clase	Prioridad	Filtro	Selector	Tasa	¿Reenvío?	¿Recopilación de datos?
Clase 1	1	Filtro 1 Filtro 3	Selector 1 Selector 2	Tasas de medidor, según tipo de medidor	Precedencia de descarte de marcador	Requiere estadísticas de recopilación de datos de flujo
Clase 1	1	Filtro 2	Selector 1 Selector 2	N/D	N/D	N/D
Clase 2	2	Filtro 1	Selector 1 Selector 2	Tasas de medidor, según tipo de medidor	Precedencia de descarte de marcador	Requiere estadísticas de recopilación de datos de flujo
Clase 2	2	Filtro 2	Selector 1 Selector 2	N/D	N/D	N/D

Puede dividir cada categoría principal para definir más la política QoS. En las siguientes secciones se explica cómo obtener información sobre las categorías mostradas en la plantilla.

Planificación de la política QoS (mapa de tareas)

En este mapa de tareas se muestran las tareas principales para planificar una política QoS y los enlaces a las instrucciones para realizar cada tarea.

Tarea	Descripción	Para obtener instrucciones
1. Diseñar la distribución de red para que sea compatible con IPQoS.	Identificar los hosts y enrutadores de la red para proporcionar servicios diferenciados.	“Cómo preparar una red para IPQoS” en la página 33
2. Definir las clases en las que los servicios de la red deben dividirse.	Examinar los tipos de servicios y acuerdos SLA que ofrece su organización y determinar las clases de tráfico independientes a las que pertenece cada servicio.	“Cómo definir las clases de la política QoS” en la página 34
3. Definir filtros para las clases.	Determinar el mejor modo de separar el tráfico de una clase específica del flujo de tráfico de la red.	“Cómo definir filtros en la política QoS” en la página 37

Tarea	Descripción	Para obtener instrucciones
4. Definir tasas de control de flujo para medir el tráfico cuando los paquetes salen del sistema IPQoS.	Determinar tasas de flujo aceptables para cada clase de tráfico.	“Cómo planificar el control de flujo” en la página 38
5. Definir los puntos DSCP o valores de prioridad de usuario que se deben utilizar en la política QoS.	Planificar un esquema para determinar el comportamiento de reenvío asignado a un flujo de tráfico cuando lo controla el enrutador o nodo.	“Cómo planificar el comportamiento de reenvío” en la página 40
6. Si procede, definir un plan de supervisión de estadísticas para los flujos de tráfico de la red.	Evaluar las clases de tráfico para determinar qué flujos de tráfico deben supervisarse por cuestiones de recopilación de datos o estadísticas.	“Cómo planificar la recopilación de datos de flujo” en la página 43

Nota – En el resto de esta sección se explica cómo planificar la política QoS de un sistema con IPQoS. Para planificar la política QoS del enrutador Diffserv, consulte la documentación y el sitio web del fabricante del enrutador.

▼ Cómo preparar una red para IPQoS

El siguiente procedimiento contiene tareas generales que llevar a cabo antes de crear la política QoS.

- 1 Revise la distribución de la red. Después, planificar una estrategia que utilice sistemas IPQoS y enrutadores Diffserv.**
Para ver ejemplos de distribución de la red, consulte la sección [“Planificación de la distribución de la red Diffserv” en la página 28](#).

- 2 Identifique los hosts de la distribución de red que requieren IPQoS o que pueden ser buenos candidatos para el servicio IPQoS.**

- 3 Determine qué sistemas con IPQoS pueden usar la misma política QoS.**

Por ejemplo, si piensa activar IPQoS en todos los hosts de la red, identifique los hosts que pueden usar la misma política QoS. Cada sistema con IPQoS debe tener una política QoS local, que se implementa en el archivo de configuración IPQoS correspondiente. Aunque puede crear un archivo de configuración IPQoS que utilicen varios sistemas. Después puede copiar el archivo de configuración en los sistemas que tengan los mismos requisitos de política QoS.

- 4 Revise y realice cualquier tarea de planificación requerida por el enrutador Diffserv de la red.**
Consulte la documentación y el sitio web del fabricante del enrutador si necesita más información.

▼ **Cómo definir las clases de la política QoS**

El primer paso para definir la política QoS es organizar los flujos de tráfico en clases. No es necesario crear una clase para cada tipo de tráfico en una red Diffserv. Según la distribución de la red, puede que necesite crear una política QoS diferente para cada sistema con IPQoS.

Nota – Para ver una descripción general de las clases, consulte la sección “Clases IPQoS” en la página 18.

En el siguiente procedimiento se asume que ya ha determinado qué sistemas de la red utilizarán IPQoS, como se explica en la sección “Cómo preparar una red para IPQoS” en la página 33.

1 Cree una tabla de planificación QoS para organizar la información de política QoS.

Para ver sugerencias, consulte la [Tabla 2-1](#).

2 Realice el resto de los pasos para cada política QoS de la red.

3 Defina las clases que utilizar en la política QoS.

Las siguientes preguntas son una guía para analizar el tráfico de red para posibles definiciones de clases.

■ ¿Su empresa ofrece acuerdos de nivel de servicio a los clientes?

En caso afirmativo, evalúe los niveles de prioridad relativa de los acuerdos SLA que su empresa ofrece a los clientes. Las mismas aplicaciones pueden ofrecerse a clientes con niveles de prioridad diferentes garantizados.

Por ejemplo, su empresa puede ofrecer alojamiento de sitios web a cada cliente, lo que indica que necesita definir una clase para cada sitio web de cliente. Un acuerdo SLA puede ofrecer un sitio web de nivel alto como un nivel de servicio. Otro acuerdo SLA puede ofrecer un sitio web personal de mejor esfuerzo a clientes con descuento. Este factor no sólo implica diferentes clases de sitio web sino también diferentes comportamientos por salto que se asignan a las clases de sitio web.

■ ¿El sistema IPQoS ofrece aplicaciones comunes que necesitan control de flujo?

Puede mejorar el rendimiento de la red activando IPQoS en servidores que ofrecen aplicaciones comunes que generan mucho tráfico. Algunos ejemplos son el correo electrónico, noticias de red y FTP. Considere la posibilidad de crear clases independientes para el tráfico entrante y saliente para cada tipo de servicio, si corresponde. Por ejemplo, puede crear una clase mail-in y una clase mail-out para la política QoS de un servidor de correo.

■ ¿La red contiene aplicaciones que requieren comportamientos de reenvío de máxima prioridad?

Cualquier aplicación importante que requiera comportamientos de reenvío de prioridad más alta debe recibir la prioridad más alta en la cola del enrutador. Los ejemplos más típicos son el streaming de video y audio.

Definir clases de entrada y clases de salida para estas aplicaciones de alta prioridad. Después, añadir las clases a las políticas QoS del sistema con IPQoS que proporciona las aplicaciones y del enrutador Diffserv.

- **¿La red tiene flujos de tráfico que deben controlares porque consumen grandes cantidades de ancho de banda?**

Utilice `netstat`, `snoop` y otras utilidades de supervisión de la red para descubrir los tipos de tráfico que causan problemas en la red. Revisar las clases creadas hasta ahora y crear clases para cualquier categoría de tráfico con problemas no definidos. Si ya ha definido clases para una categoría de tráfico problemático, defina tasas para que el medidor controle el tráfico.

Crear clases para el tráfico problemático en cada sistema con IPQoS de la red. Después, cada sistema IPQoS puede gestionar el tráfico problemático limitando la tasa a la que el flujo de tráfico se envía en la red. Asegúrese de definir estas clases de problemas en la política QoS del enrutador Diffserv. Después, el enrutador puede poner en cola y planificar los flujos problemáticos de acuerdo con la configuración de la política QoS.

- **¿Necesita estadísticas sobre determinados tipos de tráfico?**

Una revisión rápida del acuerdo SLA permite determinar qué tipos de tráfico del cliente requieren recopilación de datos. Si su empresa ofrece acuerdos SLA, es probable que ya haya creado clases para el tráfico que requiere recopilación de datos. También puede definir clases para activar la recopilación de estadísticas en flujos de tráfico que esté supervisando. También es posible crear clases para tráfico al que se restringe el acceso por motivos de seguridad.

4 Enumere las clases definidas en la tabla de planificación QoS creada en el paso 1.

5 Asigne un nivel de prioridad a cada clase.

Por ejemplo, el nivel de prioridad 1 representa la clase de prioridad máxima y se asignan prioridades de nivel descendente al resto de clases. El nivel de prioridad que se asigna sólo tiene propósito organizativo. Los niveles de prioridad definidos en la plantilla de política QoS no se utilizan en IPQoS. De hecho, puede asignar la misma prioridad a varias clases, si es apropiado para la política QoS.

6 Cuando haya terminado de definir las clases, puede definir filtros para cada clase, como se explica en ["Cómo definir filtros en la política QoS" en la página 37](#).

Más información Priorización de las clases

Al crear clases, resulta fácil ver cuáles tiene la prioridad máxima, la prioridad media y la prioridad "best-effort". Un buen esquema para priorizar clases resulta especialmente

importante si se asignan comportamientos por salto al tráfico saliente, como se explica en la sección [“Cómo planificar el comportamiento de reenvío” en la página 40](#).

Además de asignar un PHB a una clase, también puede definir un selector de prioridad en un filtro para la clase. El selector de prioridad está activo sólo en el host con IPQoS. Imagine que varias clases con tasas iguales y puntos DSCP idénticos en ocasiones compiten por el ancho de banda al salir del sistema IPQoS. El selector de prioridad de cada clase puede ordenar el nivel de servicio que se asigna a dos clases con valores que de otro modo serían idénticos.

Definición de filtros

Puede crear filtros para identificar flujos de paquetes como miembros de una clase específica. Cada filtro contiene selectores, que definen los criterios para evaluar un flujo de paquetes. El sistema con IPQoS utiliza los criterios de los selectores para extraer paquetes de un flujo de tráfico. Después, el sistema IPQoS asocia los paquetes con una clase. Para ver una introducción a los filtros, consulte la sección [“Filtros IPQoS” en la página 18](#).

En la siguiente tabla se muestran los selectores más usados. Los primeros cinco selectores representan la 5-tupla de IPQoS, que el sistema IPQoS utiliza para identificar paquetes como miembros de un flujo. Para ver una lista completa de selectores, consulte la [Tabla 6–1](#).

TABLA 2–2 Selectores IPQoS comunes

Nombre	Definición
saddr	Dirección de origen.
daddr	Dirección de destino.
sport	Número de puerto de origen. Puede usar un número de puerto conocido, definido en <code>/etc/services</code> o un número de puerto definido por el usuario.
dport	Número de puerto de destino.
protocol	Número de protocolo IP o nombre de protocolo asignado al tipo de flujo de tráfico en <code>/etc/protocols</code> .
ip_version	Estilo de direcciones que usar. Se utiliza IPv4 o IPv6. IPv4 es el predeterminado.
dsfield	Contenido del campo DS, es decir, el punto DSCP. Utilice este selector para extraer paquetes entrantes que ya están marcados con un DSCP específico.
priority	Nivel de prioridad asignado a la clase. Si necesita más información, consulte “Cómo definir las clases de la política QoS” en la página 34 .
user	El ID de usuario de UNIX o nombre de usuario que se utiliza cuando se ejecuta la aplicación de nivel superior.
projid	ID de proyecto que se utiliza cuando se ejecuta la aplicación de nivel superior.
direction	Dirección del flujo de tráfico. El valor es LOCAL_IN, LOCAL_OUT, FWD_IN o FWD_OUT.

Nota – Elija los selectores con detenimiento. Utilice sólo los selectores necesarios para extraer paquetes de una clase. Cuantos más selectores defina, más se verá afectado el rendimiento IPQoS.

▼ Cómo definir filtros en la política QoS

Antes de empezar Antes de llevar a cabo los siguientes pasos, debe haber completado el procedimiento “Cómo definir las clases de la política QoS” en la página 34.

1 Cree al menos un filtro para cada clase de la tabla de planificación QoS creada en la sección “Cómo definir las clases de la política QoS” en la página 34.

Considere la posibilidad de crear filtros independientes para el tráfico entrante y saliente de cada clase, si procede. Por ejemplo, agregue un filtro `ftp-in` y un filtro `ftp-out` a la política QoS de un servidor FTP con IPQoS. Después puede definir un selector `direction` apropiado además de los selectores básicos.

2 Defina al menos un selector para cada filtro de una clase.

Utilice la tabla de planificación QoS que se ha introducido en la [Tabla 2-1](#) para rellenar los filtros de las clases definidas.

Ejemplo 2-1 Definición de filtros para el tráfico FTP

La tabla siguiente es un ejemplo de cómo definir un filtro para el tráfico FTP saliente.

Clase	Prioridad	Filtros	Selectores
ftp-traffic	4	ftp-out	saddr 10.190.17.44 daddr 10.100.10.53 sport 21 direction LOCAL_OUT

- Véase también**
- Para definir un esquema de control de flujo, consulte la sección “Cómo planificar el control de flujo” en la página 38.
 - Para definir comportamientos de reenvío para flujos que vuelven al flujo de red, consulte “Cómo planificar el comportamiento de reenvío” en la página 40.
 - Para planificar la recopilación de datos de flujo de determinados tipos de tráfico, consulte la sección “Cómo planificar la recopilación de datos de flujo” en la página 43.
 - Para añadir más clases a la política QoS, consulte la sección “Cómo definir las clases de la política QoS” en la página 34.

- Para añadir más filtros a la política QoS, consulte la sección [“Cómo definir filtros en la política QoS” en la página 37.](#)

▼ **Cómo planificar el control de flujo**

El control de flujo implica medir el flujo de tráfico de una clase y transferir los paquetes en la red a una tasa definida. Al planificar el control de flujo, se definen los parámetros que utilizarán los módulos de medición IPQoS. Los medidores determinan la tasa a la que se transfiere el tráfico en la red. Para ver una introducción a los módulos de medición, consulte la sección [“Descripción general de medidor \(tokenmt y tswtclmt\)” en la página 18.](#)

En el siguiente procedimiento se asume que ha definido filtros y selectores, como se describe en la sección [“Cómo definir filtros en la política QoS” en la página 37.](#)

1 Determine el ancho de banda máximo de la red.

2 Revise cualquier acuerdo SLA que ofrezca su red. Identifique los clientes y los tipos de servicio garantizados a cada cliente.

Para garantizar un nivel de servicio determinado, es posible que necesite medir ciertas clases de tráfico generadas por el cliente.

3 Revise la lista de clases creadas en la sección [“Cómo definir las clases de la política QoS” en la página 34.](#)

Determine si hay alguna otra clase, a parte de las asociadas con acuerdos SLA, que deba medirse.

Suponga que el sistema IPQoS incluye una aplicación que genera mucho tráfico. Después de clasificar el tráfico de la aplicación, mida los flujos para controlar la tasa a la que los paquetes del flujo vuelven a la red.

Nota – No es necesario medir todas las clases. Tenga en mente estas directrices al revisar la lista de clases.

4 Determine qué filtros de cada clase seleccionan el tráfico que necesita control de flujo. Después, refine la lista de clases que necesitan medición.

Las clases que tengan varios filtros pueden necesitar medición sólo para un filtro. Suponga que define filtros para el tráfico entrante y saliente de una clase específica. Puede llegar a la conclusión de que sólo el tráfico en una dirección requiere control de flujo.

5 Elija un módulo de medición para cada clase con control de flujo.

Agregue el nombre de módulo a la columna de medición de la tabla de planificación QoS.

6 Agregue las tasas de cada clase que se medirá a la tabla de organización.

Si utiliza el módulo `tokenmt`, deberá definir las siguientes tasas en bits por segundo:

- Tasa asignada
- Tasa máxima

Si estas tasas son suficientes para medir una clase específica, puede definir solamente la tasa asignada y ráfaga asignada para `tokenmt`.

Si es necesario, puede definir también las siguientes tasas:

- Ráfaga asignada
- Ráfaga máxima

Para ver una definición completa de las tasas de `tokenmt`, consulte la sección [“Configuración de tokenmt como medidor de doble tasa” en la página 93](#). También puede encontrar información detallada en la página del comando `man tokenmt(7ipp)`.

Si utiliza el módulo `twstc_lmt`, debe definir las siguientes tasas en bits por segundo.

- Tasa asignada
- Tasa máxima

También puede definir el tamaño de la ventana en milisegundos. Estas tasas están definidas en la sección [“Módulo de medición twstc_lmt” en la página 94](#) y en la página del comando `man twstc_lmt(7ipp)`.

7 Agregue resultados de cumplimiento del tráfico al tráfico medido.

Los resultados de ambos módulos de medición son verde, rojo y amarillo. Agregue a la tabla de organización QoS los resultados de cumplimiento del tráfico aplicables a las tasas definidas. Los resultados de los medidores están explicados en la sección [“Módulo medidor” en la página 92](#).

Debe determinar qué acciones deben realizarse con el tráfico que cumple, o no cumple, la tasa asignada. Normalmente, pero no siempre, la acción consiste en marcar el encabezado del paquete con un comportamiento por salto. Una acción aceptable para el tráfico de nivel verde es continuar el procesamiento mientras los flujos de tráfico no excedan la tasa asignada. Otra acción sería descartar los paquetes de la clase si los flujos exceden la tasa máxima.

Ejemplo 2-2 Definición de medidores

La tabla siguiente muestra entradas de medidor para una clase de tráfico de correo electrónico. La red en la que se encuentra el sistema IPQoS tiene un ancho de banda total de 100 Mbits/s, o 10000000 bits por segundo. La política QoS asigna una prioridad baja a la clase de correo electrónico. Esta clase también recibe un comportamiento de reenvío "best-effort".

Clase	Prioridad	Filtro	Selector	Tasa
email	8	mail_in	daddr10.50.50.5 dport imap direction LOCAL_IN	
email	8	mail_out	saddr10.50.50.5	medidor=tokenmt tasa asignada=5000000 ráfaga asignada =5000000 tasa máxima =10000000 ráfaga máxima=1000000 precedencia verde=continuar procesando precedencia amarilla=marcar PHB amarillo precedencia roja=descartar

- Véase también**
- Para definir los comportamientos de reenvío para flujos cuando los paquetes vuelven al flujo de red, consulte la sección [“Cómo planificar el comportamiento de reenvío” en la página 40.](#)
 - Para planificar la recopilación de datos de flujo de determinados tipos de tráfico, consulte la sección [“Cómo planificar la recopilación de datos de flujo” en la página 43.](#)
 - Para añadir más clases a la política QoS, consulte la sección [“Cómo definir las clases de la política QoS” en la página 34.](#)
 - Para añadir más filtros a la política QoS, consulte la sección [“Cómo definir filtros en la política QoS” en la página 37.](#)
 - Para definir otro esquema de control de flujo, consulte la sección [“Cómo planificar el control de flujo” en la página 38.](#)
 - Para crear un archivo de configuración IPQoS, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 52.](#)

▼ Cómo planificar el comportamiento de reenvío

El comportamiento de reenvío determina la prioridad y precedencia de descarte de los flujos de tráfico que se van a reenviar a la red. Puede elegir dos comportamientos de reenvío principales: priorizar los flujos de una clase en relación con otras clases de tráfico o descartar los flujos por completo.

El modelo Diffserv utiliza el marcador para asignar el comportamiento de reenvío elegido a los flujos de tráfico. IPQoS ofrece los siguiente módulos de marcador.

- `dscpmk`: se utiliza para marcar el campo DS de un paquete IP con un DSCP
- `d\cosmk`: se utiliza para marcar la etiqueta VLAN de un datagrama con un valor de clase de servicio (CoS)

Nota – Las sugerencias de esta sección hacen referencia específicamente a paquetes IP. Si el sistema IPQoS incluye un dispositivo VLAN, puede usar el marcador `d\cosmk` para marcar comportamientos de reenvío para datagramas. Si necesita más información, consulte la sección [“Uso del marcador `d\cosmk` con dispositivos VLAN” en la página 97.](#)

Para priorizar el tráfico IP, debe asignar un punto DSCP a cada paquete. El marcador `dscpmk` marca el campo DS del paquete con el DSCP. El DSCP de una clase se elige de un grupo de puntos de código conocidos asociados con el tipo de comportamiento de reenvío. Estos puntos de código conocidos son 46 (101110) para el comportamiento PHB EF y un conjunto de puntos de código para el comportamiento PHB AF. Para ver una descripción general de los puntos DSCP y el reenvío, consulte la sección [“Reenvío del tráfico en una red con IPQoS” en la página 22.](#)

Antes de empezar

En los siguientes pasos se asume que ha definido clases y filtros para la política QoS. Aunque normalmente se usa el medidor con el marcador para controlar el tráfico, puede usarse solamente el marcador para definir un comportamiento de reenvío.

1 Revise las clases creadas hasta ahora y las prioridades asignadas a cada clase.

No es necesario que se marquen todas las clases de tráfico.

2 Asigne el comportamiento por salto EF a la clase con la prioridad más alta.

El comportamiento PHB EF garantiza que los paquetes con el punto DSCP EF 46 (101110) se transfieren a la red antes que los paquetes con cualquier comportamiento PHB AF. Utilice el comportamiento PHB EF para el tráfico de mayor prioridad. Si necesita más información sobre EF, consulte la sección [“Reenvío acelerado \(EF\) PHB” en la página 96.](#)

3 Asigne comportamientos de reenvío a clases cuyo tráfico se va a medir.

4 Asigne puntos de código DS al resto de clases, de acuerdo con las prioridades asignadas a las clases.

Ejemplo 2-3 Política QoS para una aplicación de juegos

El tráfico se suele medir según los siguientes criterios:

- Un acuerdo SLA garantiza a los paquetes de esta clase un servicio de nivel alto o de nivel bajo cuando la red tiene mucho tráfico.
- Una clase con una prioridad más baja puede colapsar la red.

Se utiliza el marcador con el medidor para proporcionar servicios diferenciados y administración del ancho de banda a estas clases. Por ejemplo, la siguiente tabla muestra una parte de una política QoS. Esta política define una clase para una aplicación de juegos muy utilizada que genera un alto volumen de tráfico.

Clase	Prioridad	Filtro	Selector	Tasa	¿Reenvío?
games_app	9	games_in	sport 6080	N/D	N/D
games_app	9	games_out	dport 6081	medidor=tokenmt tasa asignada=5000000 ráfaga asignada=5000000 tasa máxima=10000000 ráfaga máxima=15000000 precedencia verde=continuar procesando precedencia amarilla=marcar PHB amarillo precedencia roja=descartar	verde = AF31 amarillo = AF42 rojo = descartar

Los comportamientos de reenvío asignan puntos DSCP de baja prioridad al tráfico games_app que cumple su tasa asignada o está por debajo de la tasa máxima. Cuando el tráfico games_app excede la tasa máxima, la política QoS indica que los paquetes de games_app deben descartarse. Todos los puntos de código AF se enumeran en la [Tabla 6-2](#).

- Véase también**
- Para planificar la recopilación de datos de flujo de determinados tipos de tráfico, consulte la sección [“Cómo planificar la recopilación de datos de flujo”](#) en la página 43.
 - Para añadir más clases a la política QoS, consulte la sección [“Cómo definir las clases de la política QoS”](#) en la página 34.

- Para añadir más filtros a la política QoS, consulte la sección [“Cómo definir filtros en la política QoS” en la página 37.](#)
- Para definir un esquema de control de flujo, consulte la sección [“Cómo planificar el control de flujo” en la página 38.](#)
- Para definir comportamientos de reenvío adicionales para flujos cuando los paquetes vuelven al flujo de red, consulte la sección [“Cómo planificar el comportamiento de reenvío” en la página 40.](#)
- Para crear un archivo de configuración IPQoS, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 52.](#)

▼ **Cómo planificar la recopilación de datos de flujo**

El módulo IPQoS `flowacct` se utiliza para supervisar los flujos de tráfico por motivos de facturación o de administración de la red. Utilice el siguiente procedimiento para determinar si su política QoS debe incluir recopilación de datos sobre flujo.

1 **¿Su empresa ofrece acuerdos SLA a los clientes?**

Si la respuesta es "sí", debe recopilar datos sobre el flujo. Revise los acuerdos SLA para determinar qué tipos de tráfico de red desea ofrecer su empresa a los clientes. A continuación, revise la política QoS para determinar qué clases seleccionan el tráfico que se facturará.

2 **¿Hay aplicaciones que deben supervisarse o comprobarse para evitar problemas de red?**

Si la respuesta es "sí", considere la posibilidad de recopilar datos sobre el flujo para observar el comportamiento de estas aplicaciones. Revise la política QoS para determinar qué clases ha asignado al tráfico que requiere supervisión.

3 **En la tabla de planificación QoS, marque una Y en la columna de recopilación de datos sobre el flujo de las clases que requieran recopilación de datos.**

Véase también

- Para añadir más clases a la política QoS, consulte la sección [“Cómo definir las clases de la política QoS” en la página 34.](#)
- Para añadir más filtros a la política QoS, consulte la sección [“Cómo definir filtros en la política QoS” en la página 37.](#)
- Para definir un esquema de control de flujo, consulte la sección [“Cómo planificar el control de flujo” en la página 38.](#)
- Para definir los comportamientos de reenvío para flujos cuando los paquetes vuelven al flujo de red, consulte la sección [“Cómo planificar el comportamiento de reenvío” en la página 40.](#)
- Para planificar la recopilación de datos adicional para determinados tipos de tráfico, consulte la sección [“Cómo planificar la recopilación de datos de flujo” en la página 43.](#)

- Para crear el archivo de configuración IPQoS, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico”](#) en la página 52.

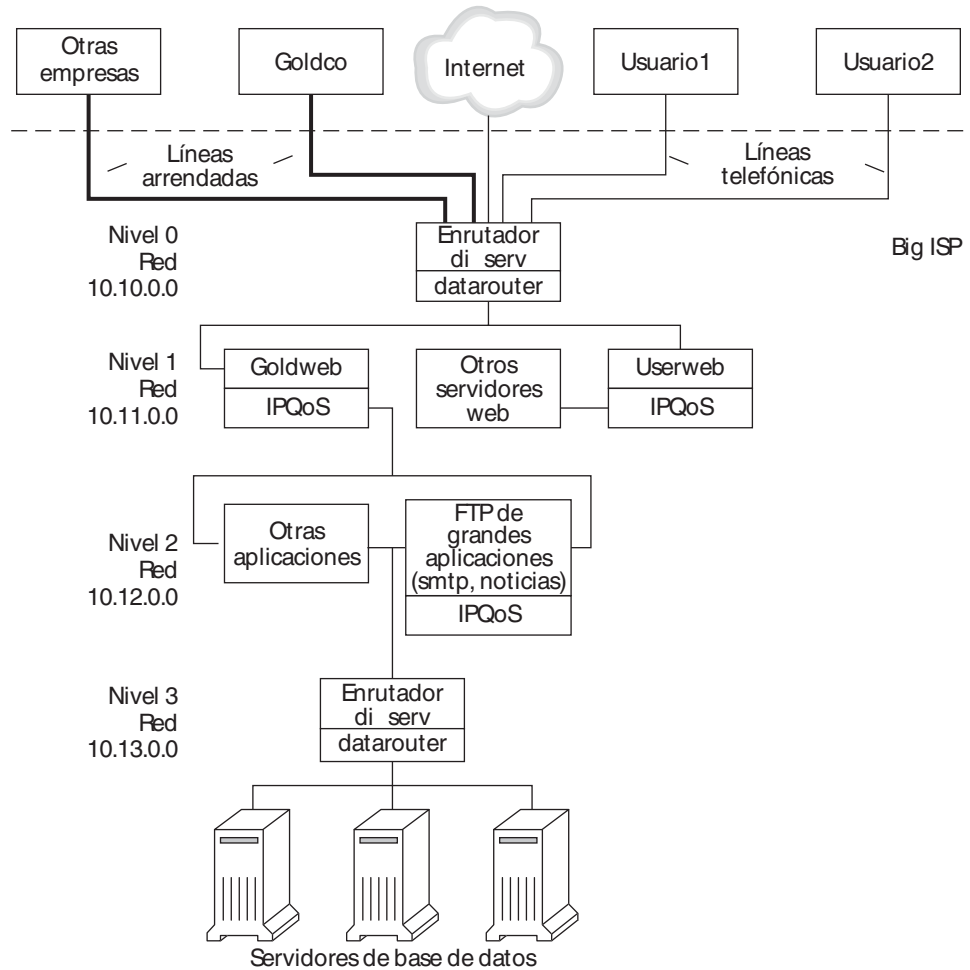
Introducción al ejemplo de configuración IPQoS

Las tareas de los siguientes capítulos de la guía utilizan la configuración IPQoS de ejemplo de esta sección. El ejemplo muestra la solución de servicios diferenciados de la intranet pública de BigISP, un proveedor de servicios ficticio. BigISP ofrece servicios a grandes empresas que acceden a BigISP a través de líneas arrendadas. Los individuos que se conectan desde módems también pueden adquirir servicios de BigISP.

Topología de IPQoS

En la siguiente figura se muestra la topología de red que se utiliza para la intranet pública de BigISP.

FIGURA 2-4 Ejemplo de topología de IPQoS



BigISP utiliza cuatro niveles en su intranet pública:

- Nivel 0:** la red `10.10.0.0` incluye un enrutador Diffserv grande llamado Bigrouter, con interfaces externa e interna. Varias empresas, entre ellas una organización llamada Goldco, han alquilado servicios de línea arrendada que finalizan en Bigrouter. EL nivel 0 también gestiona los clientes individuales que llaman desde líneas telefónicas o RDSI.
- Nivel 1:** la red `10.11.0.0` proporciona servicios web. El servidor Goldweb aloja el sitio web adquirido por Goldco como parte del servicio de alto nivel que Goldco ha adquirido de BigISP. El servidor Userweb aloja sitios web pequeños adquiridos por clientes individuales. Ambos servidores, Goldweb y Userweb utilizan IPQoS.

- **Nivel 2:** la red 10.12.0.0 proporciona aplicaciones para todos los clientes. BigAPPS, uno de los servidores de aplicaciones, utiliza IPQoS. BigAPPS proporciona servicios SMTP, de noticias y FTP.
- **Nivel 3:** la red 10.13.0.0 aloja grandes servidores de base de datos. El acceso al Nivel 3 está controlado por datarouter, un enrutador Diffserv.

Creación del archivo de configuración IPQoS (tareas)

En este capítulo se explica cómo crear archivos de configuración IPQoS. El capítulo trata los siguientes temas.

- “Definición de una política QoS en el archivo de configuración IPQoS (mapa de tareas)” en la página 47
- “Herramientas para crear una política QoS” en la página 49
- “Creación de archivos de configuración IPQoS para servidores web” en la página 50
- “Creación un archivo de configuración IPQoS para un servidor de aplicaciones” en la página 63
- “Suministro de servicios diferenciados en un enrutador” en la página 72

En este capítulo se asume que el usuario ha definido una política QoS completa y que está listo para utilizarla como base para el archivo de configuración IPQoS. Si necesita instrucciones sobre la planificación de políticas QoS, consulte el tema “[Planificación de la política de calidad de servicio](#)” en la página 31.

Nota – Es posible que en futuras versiones se elimine la utilidad IPQoS. Se recomienda a los usuarios que, en su lugar, utilicen los comandos `dladm`, `flowadm` y comandos relacionados, que admiten funciones de control de los recursos de ancho de banda similares. Para obtener más información, consulte *Uso de redes virtuales en Oracle Solaris 11.1*.

Definición de una política QoS en el archivo de configuración IPQoS (mapa de tareas)

En este mapa de tareas se muestran las tareas generales para crear un archivo de configuración IPQoS y los enlaces a las secciones en las que se describen los pasos para realizar estas tareas.

Tarea	Descripción	Para obtener instrucciones
1. Planificar la configuración de red con IPQoS.	Decida qué sistemas de la red local va a utilizar IPQoS.	“Cómo preparar una red para IPQoS” en la página 33
2. Planificar la política QoS para sistemas IPQoS de la red.	Identifique flujos de tráfico como diferentes clases de servicio. A continuación, determine qué flujos requieren administración del tráfico.	“Planificación de la política de calidad de servicio” en la página 31
3. Crear el archivo de configuración IPQoS y definir la primera acción.	Cree el archivo IPQoS, invoque el clasificador IP y defina una clase para procesar.	“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 52
4. Crear filtros para un clase.	Agregue los filtros que determinan qué tráfico se selecciona y se organiza en una clase.	“Cómo definir filtros en el archivo de configuración IPQoS” en la página 54
5. Agregar más clases y filtros al archivo de configuración IPQoS.	Cree más clases y filtros para que los procese el clasificador IP.	“Cómo crear un archivo de configuración IPQoS para un servidor web “best-effort”” en la página 60
6. Agregar una instrucción <code>action</code> con parámetros para configurar los módulos de medición.	Si la política QoS solicita control de flujo, asigne tasas de control de flujo y niveles de cumplimiento al medidor.	“Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 69
7. Agregar una instrucción <code>action</code> con parámetros para configurar el marcador.	Si la política QoS solicita comportamientos de reenvío diferenciados, defina cómo deben reenviarse las clases de tráfico.	“Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS” en la página 56
8. Agregar una instrucción <code>action</code> con parámetros para configurar el módulo de control de flujo.	Si la política QoS solicita recopilación de estadísticas sobre flujos de tráfico, defina cómo deben recopilarse las estadísticas de control.	“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 59
9. Aplicar el archivo de configuración IPQoS.	Agregue el contenido de un archivo de configuración IPQoS especificado a los módulos de núcleo apropiados.	“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 76
10. Configurar los comportamientos de reenvío en los archivos de enrutador.	Si algún archivo de configuración IPQoS de la red define los comportamientos de reenvío, agregue los puntos DSCP resultantes a los archivos de planificación correspondientes del enrutador.	“Cómo configurar un enrutador en una red con IPQoS” en la página 72

Herramientas para crear una política QoS

La política QoS de la red está definida en el archivo de configuración IPQoS. Este archivo de configuración se crea con un editor de texto. Después, se proporciona el archivo como un argumento a `ipqosconf`, la herramienta de configuración IPQoS. Al solicitar a `ipqosconf` que aplique la política definida en el archivo de configuración, la política se escribe en el núcleo del sistema IPQoS. Si necesita información detallada sobre el comando `ipqosconf`, consulte la página del comando `man ipqosconf(1M)`. Si necesita instrucciones sobre el uso de `ipqosconf`, consulte [“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 76.](#)

Archivo de configuración IPQoS básico

Un archivo de configuración IPQoS consiste en un árbol de instrucciones `action` que implementan la política QoS definida en la sección [“Planificación de la política de calidad de servicio” en la página 31](#). El archivo de configuración IPQoS configura los módulos IPQoS. Cada instrucción `action` contiene un conjunto de *clases*, *filtros* o *parámetros* que procesará el módulo al que llame la instrucción `action`.

Para ver la sintaxis completa del archivo de configuración IPQoS, consulte el [Ejemplo 6-3](#) y la página del comando `man ipqosconf(1M)`.

Configuración de la topología de ejemplo IPQoS

Las tareas de este capítulo explican cómo crear archivos de configuración IPQoS para tres sistemas con IPQoS. Estos sistemas forman parte de la topología de red de la compañía BigISP, que se presentó en la [Figura 2-4](#).

- **Goldweb:** un servidor web que aloja sitios web de clientes que tienen acuerdos SLA de nivel alto
- **Userweb:** un servidor web menos potente que aloja páginas personales de usuarios que tienen acuerdos SLA de tipo “best-effort”
- **BigAPPS:** servidor de aplicaciones que ofrece servicios de correo, noticas y FTP a clientes con servicios de nivel alto y “best-effort”

Estos tres archivos de configuración ilustran las configuraciones IPQoS más comunes. Puede usar los archivos de muestra de la siguiente sección como plantilla para su implementación IPQoS.

Creación de archivos de configuración IPQoS para servidores web

Esta sección es una introducción al archivo de configuración IPQoS en la que se muestra cómo crear una configuración para un servidor web de nivel alto. También se muestra cómo configurar un nivel de servicio diferente mediante otro archivo de configuración para un servidor que aloja páginas web personales. Ambos servidores forman parte del ejemplo de red que se muestra en la [Figura 2-4](#).

El siguiente archivo de configuración define actividades IPQoS para el servidor Goldweb. Este servidor aloja el sitio web de Goldco, la compañía que tiene un acuerdo SLA de nivel alto.

EJEMPLO 3-1 Archivo de configuración IPQoS de ejemplo para un servidor web de nivel alto

```
fmt_version 1.0

action {
  module ipgpc
  name ipgpc.classify
  params {
    global_stats TRUE
  }
  class {
    name goldweb
    next_action markAF11
    enable_stats FALSE
  }
  class {
    name video
    next_action markEF
    enable_stats FALSE
  }
  filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class goldweb
  }
  filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
  }
}

action {
  module dscpmk
  name markAF11
  params {
    global_stats FALSE
    dscp_map{0-63:10}
    next_action continue
  }
}
```

EJEMPLO 3-1 Archivo de configuración IPQoS de ejemplo para un servidor web de nivel alto
(Continuación)

```

action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
action {
    module flowacct
    name acct
    params {
        enable_stats TRUE
        timer 10000
        timeout 10000
        max_limit 2048
    }
}

```

El siguiente archivo de configuración define actividades IPQoS en Userweb. Este servidor aloja sitios web de usuarios con acuerdos SLA de bajo precio o "best-effort". Este nivel de servicio garantiza el mejor servicio que puede ofrecerse a clientes "best-effort" después de que el sistema IPQoS administre el tráfico de clientes con acuerdos SLA de nivel alto.

EJEMPLO 3-2 Configuración de muestra para un servidor web "best-effort"

```

fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name Userweb
        next_action markAF12
        enable_stats FALSE
    }
    filter {
        name webout
        sport 80
        direction LOCAL_OUT
        class Userweb
    }
}
action {
    module dscpmk
    name markAF12
    params {
        global_stats FALSE
    }
}

```

EJEMPLO 3-2 Configuración de muestra para un servidor web "best-effort" (Continuación)

```

    dscp_map{0-63:12}
    next_action continue
  }
}

```

▼ Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico

Puede crear el primer archivo de configuración IPQoS en el directorio que le resulte más fácil para su mantenimiento. En las tareas de este capítulo se utiliza el directorio `/var/ipqos` como ubicación para archivos de configuración IPQoS. En el siguiente procedimiento se genera el segmento inicial del archivo de configuración IPQoS introducido en el [Ejemplo 3-1](#).

Nota – Al crear el archivo de configuración IPQoS, asegúrese de comenzar y finalizar cada instrucción `action` y cláusula con llaves (`{ }`). Para ver un ejemplo del uso de llaves, consulte el [Ejemplo 3-1](#).

1 Inicie una sesión en el servidor web de nivel alto y cree un archivo de configuración IPQoS nuevo con una extensión `.qos`.

Los archivos de configuración IPQoS deben comenzar con el número de versión `fmt_version 1.0` como primera línea sin comentar.

2 A continuación del parámetro de apertura, escriba la instrucción `action` inicial, que configura el clasificador IP genérico `ipgpc`.

Esta primera acción inicia el árbol de instrucciones `action` que compone el archivo de configuración IPQoS. Por ejemplo, el archivo `/var/ipqos/Goldweb.qos` comienza con la instrucción `action` inicial para llamar al clasificador `ipgpc`.

```
fmt_version 1.0
```

```
action {
  module ipgpc
  name ipgpc.classify
}
```

`fmt_version 1.0` Inicia el archivo de configuración IPQoS.

`action {` Inicia la instrucción `action`.

`module ipgpc` Configura el clasificador `ipgpc` como la primera acción del archivo de configuración.

`name ipgpc.classify` Define el nombre de la instrucción `action` de clasificador, que siempre debe ser `ipgpc.classify`.

Si necesita información sintáctica detallada sobre instrucciones de acción, consulte la sección [“Instrucción action” en la página 103](#) y la página del comando `man ipqosconf(1M)`.

3 Agregue una cláusula `params` con el parámetro de estadísticas `global_stats`.

```
params {
    global_stats TRUE
}
```

El parámetro `global_stats TRUE` de la instrucción `ipgpc.classify` activa la recopilación de estadísticas para esa acción. `global_stats TRUE` también activa la recopilación de estadísticas por clase cuando una definición de cláusula de clase específica `enable_stats TRUE`.

Activar las estadísticas afecta al rendimiento. Puede ser útil recopilar estadísticas en un archivo de configuración IPQoS nuevo para verificar que IPQoS funciona correctamente. Más adelante, puede desactivar la recopilación de estadísticas cambiando el argumento de `global_stats` a `FALSE`.

Las estadísticas globales son tan solo uno de los parámetros que se pueden definir en la cláusula `params`. Para obtener información sobre la sintaxis y otros detalles de las cláusulas `params`, consulte la sección [“Cláusula params” en la página 105](#) y la página del comando `man ipqosconf(1M)`.

4 Defina una cláusula que identifique el tráfico vinculado al servidor de nivel alto.

```
class {
    name goldweb
    next_action markAF11
    enable_stats FALSE
}
```

Esta instrucción se denomina una *cláusula class*. Una cláusula `class` tiene el siguiente contenido.

<code>name goldweb</code>	Crea la clase <code>goldweb</code> para identificar el tráfico vinculado al servidor <code>Goldweb</code> .
<code>next_action markAF11</code>	Indica al módulo <code>ipgpc</code> que debe pasar los paquetes de la clase <code>goldweb</code> a la instrucción <code>action markAF11</code> . La instrucción <code>action markAF11</code> llama al marcador <code>dsccpmk</code> .
<code>enable_stats FALSE</code>	Activa la recopilación de estadísticas de la clase <code>goldweb</code> . Sin embargo, como el valor de <code>enable_stats</code> es <code>FALSE</code> , las estadísticas de esta clase no están activadas.

Para obtener información detallada sobre la sintaxis de la cláusula `class`, consulte la sección [“Cláusula class” en la página 104](#) y la página del comando `man ipqosconf(1M)`.

5 Defina una clase que identifique una aplicación que deba tener reenvío de máxima prioridad.

```
class {
    name video
```

```

        next_action marKEF
        enable_stats FALSE
    }

```

name video	Crea la clase video para identificar el tráfico saliente de video streaming del servidor Goldweb.
next_action marKEF	Indica al módulo ipgpc que debe pasar los paquetes de la clase video a la instrucción marKEF después de que ipgpc haya terminado el procesamiento. La instrucción marKEF llama al marcador dscpmk.
enable_stats FALSE	Activa la recopilación de estadísticas de la clase video. Sin embargo, como el valor de enable_stats es FALSE, la recopilación de estadísticas de esta clase no está activada.

- Véase también**
- Para definir filtros para la clase creada, consulte la sección “[Cómo definir filtros en el archivo de configuración IPQoS](#)” en la página 54.
 - Para crear otra cláusula para el archivo de configuración, consulte la sección “[Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico](#)” en la página 52.

▼ Cómo definir filtros en el archivo de configuración IPQoS

El siguiente procedimiento muestra cómo definir filtros para una clase en el archivo de configuración IPQoS.

Antes de empezar

En el procedimiento se asume que ya ha comenzado la creación del archivo y ha definido clases. Los pasos continúan con la generación del archivo `/var/ipqos/Goldweb.qos` creado en la sección “[Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico](#)” en la página 52.

Nota – Al crear el archivo de configuración IPQoS, asegúrese de comenzar y finalizar cada cláusula `class` y cada cláusula `filter` con llaves (`{}`). Para ver un ejemplo del uso de llaves, consulte el [Ejemplo 3-1](#).

1 Abra el archivo de configuración IPQoS y busque la última clase definida.

Por ejemplo, en el servidor con IPQoS Goldweb, empezaría después de la siguiente cláusula `class` en `/var/ipqos/Goldweb.qos`:

```

class {
    name video
    next_action marKEF

```

```

    enable_stats FALSE
}

```

2 Defina una cláusula `filter` para seleccionar el tráfico saliente del sistema IPQoS.

```

filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class goldweb
}

```

<code>name webout</code>	Asigna el nombre <code>webout</code> al filtro.
<code>sport 80</code>	Selecciona el tráfico con origen en el puerto 80, el puerto de tráfico HTTP (web).
<code>direction LOCAL_OUT</code>	Selecciona el tráfico saliente del sistema local.
<code>class goldweb</code>	Identifica la clase a la que pertenece el filtro, en este caso, la clase <code>goldweb</code> .

Si necesita información detallada y sintáctica sobre la cláusula `filter` del archivo de configuración IPQoS, consulte la sección “Cláusula `filter`” en la página 105.

3 Defina una cláusula `filter` para seleccionar el tráfico de video streaming del sistema IPQoS.

```

filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
}

```

<code>name videoout</code>	Asigna el nombre <code>videoout</code> al filtro.
<code>sport videosrv</code>	Selecciona el tráfico con un puerto de origen <code>videosrv</code> , un puerto definido anteriormente para la aplicación de video streaming en este sistema.
<code>direction LOCAL_OUT</code>	Selecciona el tráfico saliente del sistema local.
<code>class video</code>	Identifica la clase a la que pertenece el filtro, en este caso, la clase <code>video</code> .

- Véase también**
- Para definir comportamientos de reenvío para los módulos de marcador, consulte la sección “Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS” en la página 56.
 - Para definir parámetros de control de flujo para los módulos de medidor, consulte la sección “Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 69.
 - Para activar el archivo de configuración IPQoS, consulte la sección “Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 76.

- Para definir filtros adicionales, consulte la sección [“Cómo definir filtros en el archivo de configuración IPQoS”](#) en la página 54.
- Para crear clases para flujos de tráfico de aplicaciones, consulte la sección [“Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones”](#) en la página 65.

▼ Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS

El siguiente procedimiento muestra cómo definir el reenvío de tráfico añadiendo comportamientos por salto para una clase en el archivo de configuración IPQoS.

Antes de empezar

En el procedimiento se asume que ya tiene un archivo de configuración IPQoS con clases y filtros definidos. Los pasos continúan con la creación del archivo `/var/ipqos/Goldweb.qos` del [Ejemplo 3-1](#).

Nota – El procedimiento muestra cómo configurar el reenvío de tráfico utilizando el módulo de marcador `dscpmk`. Si necesita información sobre el reenvío de tráfico en sistemas VLAN utilizando el marcador `dlcosmk`, consulte la sección [“Uso del marcador `dlcosmk` con dispositivos VLAN”](#) en la página 97.

1 Abra el archivo de configuración IPQoS y localice el final del último filtro definido.

Por ejemplo, en el servidor con IPQoS Goldweb, empezaría después de la siguiente cláusula `filter` en `/var/ipqos/Goldweb.qos`:

```
filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
}
```

Observe que esta cláusula `filter` está al final de la instrucción `action` del clasificador `ipgpc`. Por lo tanto, necesita una llave de cierre para finalizar el filtro y otra para finalizar la instrucción `action`.

2 Invoque el marcador con la siguiente instrucción `action`.

```
action {
    module dscpmk
    name markAF11
```

`module dscpmk` Llama al módulo de marcador `dscpmk`.

`name markAF11` Asigna el nombre `markAF11` a la instrucción `action`.

La clase `goldweb` definida anteriormente incluye una instrucción `next_action markAF11`. Esta instrucción envía los flujos de tráfico a la instrucción `action markAF11` cuando el clasificador ha finalizado el procesamiento.

3 Defina las acciones que debe ejecutar el marcador en el flujo de tráfico.

```
params {
    global_stats FALSE
    dscp_map{0-63:10}
    next_action continue
}
```

<code>global_stats FALSE</code>	Activa la recopilación de estadísticas de la instrucción <code>action</code> del marcador <code>markAF11</code> . Sin embargo, como el valor de <code>enable_stats</code> es <code>FALSE</code> , no se recopilan estadísticas.
<code>dscp_map{0-63:10}</code>	Asigna un DSCP de valor <code>10</code> a los encabezados de paquetes de la clase de tráfico <code>goldweb</code> , que el marcador está procesando en ese momento.
<code>next_action continue</code>	Indica que no se necesita más procesamiento en los paquetes de la clase de tráfico <code>goldweb</code> , y que estos paquetes pueden volver al flujo de red.

El DSCP de valor `10` indica al marcador que debe definir todas las entradas del mapa `dscp` en el valor decimal `10` (binario `001010`). Este punto de código indica que los paquetes de la clase de tráfico `goldweb` están sujetos al comportamiento por salto `AF11`. `AF11` garantiza que todos los paquetes con DSCP de valor `10` reciben un servicio de alta prioridad y baja probabilidad de descarte. Por lo tanto, el tráfico saliente para clientes de nivel alto en `Goldweb` recibe la prioridad más alta disponible para el PHB de reenvío asegurado (AF). Para ver una tabla de puntos DSCP posibles para AF, consulte la [Tabla 6-2](#).

4 Inicie otra instrucción `action` de marcador.

```
action {
    module dscpmk
    name markEF
```

<code>module dscpmk</code>	Llama al módulo de marcador <code>dscpmk</code> .
<code>name markEF</code>	Asigna el nombre <code>markEF</code> a la instrucción <code>action</code> .

5 Defina acciones que deba ejecutar el marcador en el flujo de tráfico.

```
params {
    global_stats TRUE
    dscp_map{0-63:46}
    next_action acct
}
```

<code>global_stats TRUE</code>	Activa la recopilación de estadísticas en la clase <code>video</code> , que selecciona paquetes de video streaming.
--------------------------------	---

<code>dscp_map{0-63:46}</code>	Asigna un DSCP de valor 46 a los encabezados de paquetes de la clase de tráfico video, que el marcador está procesando en ese momento.
<code>next_action acct</code>	Indica al módulo <code>dscpmk</code> que debe pasar los paquetes de la clase video a la instrucción <code>acct action</code> cuando <code>dscpmk</code> haya completado el procesamiento. La instrucción <code>acct action</code> invoca el módulo <code>flowacct</code> .

El DSCP de valor 46 indica al módulo `dscpmk` que debe establecer todas las entradas del mapa `dscp` en el valor decimal 46 (binario 101110) en el campo DS. Este punto de código indica que los paquetes de la clase de tráfico video están sujetos al comportamiento por salto de reenvío acelerado (EF).

Nota – El punto de código recomendado para EF es 46 (binario 101110). Otros puntos DSCP asignan comportamientos PHB AF a un paquete.

El PHB EF garantiza que los paquetes con el DSCP de valor 46 reciben la máxima precedencia en sistemas IPQoS y Diffserv. Las aplicaciones streaming requieren el servicio de prioridad más alta, por eso se les asignan comportamientos PHB EF en la política QoS. Si necesita más información sobre PHB de reenvío acelerado, consulte la sección [“Reenvío acelerado \(EF\) PHB” en la página 96](#).

- 6 Agregue los puntos DSCP que ha creado a los archivos correspondientes del enrutador Diffserv.** Si necesita más información, consulte [“Cómo configurar un enrutador en una red con IPQoS” en la página 72](#).

- Véase también**
- Para empezar a recopilar estadísticas de control de flujo sobre el tráfico, consulte la sección [“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 59](#).
 - Para definir comportamientos de reenvío para los módulos de marcador, consulte la sección [“Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS” en la página 56](#).
 - Para definir parámetros de control de flujo para los módulos de medidor, consulte la sección [“Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 69](#).
 - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 76](#).
 - Para definir filtros adicionales, consulte la sección [“Cómo definir filtros en el archivo de configuración IPQoS” en la página 54](#).
 - Para crear clases para flujos de tráfico de aplicaciones, consulte la sección [“Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones” en la página 65](#).

▼ Cómo activar el control para una clase en el archivo de configuración IPQoS

El siguiente procedimiento muestra como activar el control de una clase de tráfico en el archivo de configuración IPQoS. El procedimiento muestra como definir el control de flujo para la clase video, introducida en la sección “[Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico](#)” en la página 52. Esta clase selecciona el tráfico de video streaming, que debe formar parte de un acuerdo SLA de nivel alto del cliente.

Antes de empezar

En el procedimiento se asume que ya tiene un archivo de configuración IPQoS con clases, filtros y acciones de medición definidas, si corresponde, y acciones de marcado, si corresponde. Los pasos continúan con la creación del archivo `/var/ipqos/Goldweb.qos` del [Ejemplo 3-1](#).

1 Abra el archivo de configuración IPQoS y localice el final de la última instrucción `action` definida.

Por ejemplo, en el servidor con IPQoS Goldweb, empezaría después de la siguiente instrucción `markEF action` en `/var/ipqos/Goldweb.qos`.

```
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

2 Inicie una instrucción `action` que llame al control de flujo.

```
action {
    module flowacct
    name acct
```

`module flowacct` Invoca al módulo de control de flujo `flowacct`.

`name acct` Asigna el nombre `acct` a la instrucción `action`

3 Defina una cláusula `params` para el control de la clase de tráfico.

```
params {
    global_stats TRUE
    timer 10000
    timeout 10000
    max_limit 2048
    next_action continue
}
```

`global_stats TRUE` Activa la recopilación de estadísticas de la clase video, que selecciona paquetes de video streaming.

<code>timer 10000</code>	Especifica la duración del intervalo, en milisegundos, que se utiliza al explorar la tabla de flujos para detectar flujos con tiempo de espera superado. En este parámetro, el intervalo es de 10000 milisegundos.
<code>timeout 10000</code>	Especifica el valor de tiempo de espera de intervalo mínimo. El tiempo de espera de un flujo se supera cuando los paquetes del flujo no se envían durante un intervalo de tiempo de espera. En este parámetro, se supera el tiempo de espera de paquetes cuando transcurren 10000 milisegundos.
<code>max_limit 2048</code>	Determina el número máximo de registros de flujos en la tabla de flujos para esta instancia de acción.
<code>next_action continue</code>	Indica que no es necesario más procesamiento en los paquetes de la clase de tráfico video y que los paquetes pueden volver al flujo de red.

El módulo `flowacct` recopila información estadística sobre los flujos de paquetes de una clase específica hasta que se alcanza un valor de `timeout` determinado.

- Véase también**
- Para configurar comportamientos por salto en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS”](#) en la página 72.
 - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS”](#) en la página 76.
 - Para crear clases para flujos de tráfico de aplicaciones, consulte la sección [“Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones”](#) en la página 65.

▼ **Cómo crear un archivo de configuración IPQoS para un servidor web "best-effort"**

El archivo de configuración IPQoS para un servidor web "best-effort" es ligeramente diferente al de un servidor web de nivel alto. Como muestra, en el procedimiento se utiliza el archivo de configuración del [Ejemplo 3-2](#).

- 1 **Inicie una sesión en el servidor web "best-effort".**
- 2 **Cree un archivo de configuración IPQoS con extensión `.qos`.**

```
fmt_version 1.0
action {
    module ipgpc
    name ipgpc.classify
    params {
```

```

    global_stats TRUE
}

```

El archivo `/var/ipqos/userweb.qos` debe comenzar con la instrucción `action` parcial para invocar el clasificador `ipgpc`. Además, la instrucción `action` también tiene una cláusula `params` para activar la recopilación de estadísticas. Si necesita una explicación de esta instrucción `action`, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico”](#) en la página 52.

3 Defina una clase que identifique el tráfico vinculado con el servidor web "best-effort".

```

class {
    name userweb
    next_action markAF12
    enable_stats FALSE
}

```

`name userweb` Crea una clase llamada `userweb` para reenviar el tráfico web de usuarios.

`next_action markAF12` Indica al módulo `ipgpc` que debe transferir los paquetes de la clase `userweb` a la instrucción `action markAF12` cuando `ipgpc` haya completado el procesamiento. La instrucción `action markAF12` invoca al marcador `dscpmk`.

`enable_stats FALSE` Activa la recopilación de estadísticas para la clase `userweb`. Sin embargo, como el valor de `enable_stats` es `FALSE`, no se produce la recopilación de estadísticas para esta clase.

Para ver una explicación de la tarea de la cláusula `class`, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico”](#) en la página 52.

4 Defina una cláusula `filter` para seleccionar los flujos de tráfico de la clase `userweb`.

```

filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class userweb
}
}

```

`name webout` Asigna el nombre `webout` al filtro.

`sport 80` Selecciona el tráfico con origen en el puerto 80, el puerto de tráfico HTTP (web).

`direction LOCAL_OUT` Selecciona el tráfico saliente del sistema local.

`class userweb` Identifica la clase a la que pertenece el filtro, en este caso, la clase `userweb`.

Para ver una explicación de la tarea de la cláusula `filter`, consulte [“Cómo definir filtros en el archivo de configuración IPQoS” en la página 54.](#)

5 Inicie la instrucción `action` para invocar el marcador `dscpmk`.

```
action {
  module dscpmk
  name markAF12
```

`module dscpmk` Invoca al módulo de marcador `dscpmk`.

`name markAF12` Asigna el nombre `markAF12` a la instrucción `action`.

La clase `userweb` definida anteriormente incluye una instrucción `next_action markAF12`. Esta instrucción envía flujos de tráfico a la instrucción `action markAF12` cuando el clasificador finaliza el procesamiento.

6 Defina los parámetros que debe usar el marcador para procesar el flujo de tráfico.

```
  params {
    global_stats FALSE
    dscp_map{0-63:12}
    next_action continue
  }
}
```

`global_stats FALSE` Activa la recopilación de estadísticas para la instrucción `action` del marcador `markAF12`. Sin embargo, como el valor de `enable_stats` es `FALSE`, no se produce la recopilación de estadísticas.

`dscp_map{0-63:12}` Asigna un valor DSCP de 12 a los encabezados de paquetes de la clase de tráfico `userweb`, que esté procesando el marcador en ese momento.

`next_action continue` Indica que no es necesario más procesamiento en los paquetes de la clase de tráfico `userweb`, y que los paquetes pueden volver al flujo de red.

El valor DSCP de 12 indica al marcador que debe definir todas las entradas del mapa `dscp` en el valor decimal 12 (binario 001100). Este punto de código indica que los paquetes de la clase de tráfico `userweb` están sujetos al comportamiento por salto AF12. AF12 garantiza que todos los paquetes con el DSCP de valor 12 en el campo DS reciben un servicio de probabilidad de descarte media y prioridad alta.

7 Cuando haya completado el archivo de configuración IPQoS, aplique la configuración.

- Véase también**
- Para agregar clases y otra configuración para flujos de tráfico de aplicaciones, consulte la sección [“Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones” en la página 65.](#)
 - Para configurar comportamientos por salto en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS” en la página 72.](#)

- Para activar el archivo de configuración IPQoS, consulte la sección “[Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS](#)” en la página 76.

Creación un archivo de configuración IPQoS para un servidor de aplicaciones

En esta sección se explica cómo crear un archivo de configuración para un servidor de aplicaciones que proporciona aplicaciones básicas a clientes. En el procedimiento, se utiliza como ejemplo el servidor BigAPPS de la [Figura 2-4](#).

El siguiente archivo de configuración define actividades IPQoS para el servidor BigAPPS. Este servidor aloja FTP, correo electrónico (SMTP) y noticias de red (NNTP) para clientes.

EJEMPLO 3-3 Archivo de configuración IPQoS para un servidor de aplicaciones

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name smtp
        enable_stats FALSE
        next_action markAF13
    }
    class {
        name news
        next_action markAF21
    }
    class {
        name ftp
        next_action meterftp
    }
    filter {
        name smtpout
        sport smtp
        class smtp
    }
    filter {
        name newsout
        sport nntp
        class news
    }
    filter {
        name ftpout
        sport ftp
        class ftp
    }
}
```

EJEMPLO 3-3 Archivo de configuración IPQoS para un servidor de aplicaciones (Continuación)

```
    filter {
        name ftpdata
        sport ftp-data
        class ftp
    }
}
action {
    module dscpmk
    name markAF13
    params {
        global_stats FALSE
        dscp_map{0-63:14}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
action {
    module tokenmt
    name meterftp
    params {
        committed_rate 50000000
        committed_burst 50000000
        red_action_name AF31
        green_action_name markAF22
        global_stats TRUE
    }
}
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
}
```


▼ Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones

- 1 **Inicie sesión en el servidor de aplicaciones con IPQoS y cree un archivo de configuración IPQoS con una extensión .qos.**

Por ejemplo, cree el archivo `/var/ipqos/BigAPPS.qos` para el servidor de aplicaciones.

Empiece con los siguientes comandos necesarios para iniciar la instrucción `action` que invoca al clasificador `ipgpc`:

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
}
```

Si necesita una explicación de la instrucción `action` inicial, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico”](#) en la página 52.

- 2 **Cree clases para seleccionar el tráfico desde tres aplicaciones en el servidor BigAPPS.**

Agregue las definiciones de clases después de la instrucción `action` de apertura.

```
class {
    name smtp
    enable_stats FALSE
    next_action markAF13
}
class {
    name news
    next_action markAF21
}
class {
    name ftp
    enable_stats TRUE
    next_action meterftp
}
```

<code>name smtp</code>	Crea una clase llamada <code>smtp</code> , que incluye los flujos de tráfico de correo electrónico que debe administrar la aplicación SMTP
<code>enable_stats FALSE</code>	Activa la recopilación de estadísticas para la clase <code>smtp</code> . Sin embargo, como el valor de <code>enable_stats</code> es <code>FALSE</code> , no se recopilan las estadísticas de esta clase.
<code>next_action markAF13</code>	Indica al módulo <code>ipgpc</code> que debe transferir los paquetes de la clase <code>smtp</code> a la instrucción <code>action markAF13</code> cuando <code>ipgpc</code> haya completado el procesamiento.

<code>name news</code>	Crea una clase llamada <code>news</code> , que incluye los flujos de tráfico de noticias de red que debe administrar la aplicación NNTP.
<code>next_action markAF21</code>	Indica al módulo <code>ipgpc</code> que debe transferir los paquetes de la clase <code>news</code> a la instrucción <code>action markAF21</code> cuando <code>ipgpc</code> haya completado el procesamiento.
<code>name ftp</code>	Crea una clase llamada <code>ftp</code> , que administra el tráfico saliente gestionado por la aplicación FTP.
<code>enable_stats TRUE</code>	Activa la recopilación de estadísticas para la clase <code>ftp</code> .
<code>next_action meterftp</code>	Indica al módulo <code>ipgpc</code> que debe transferir los paquetes de la clase <code>ftp</code> a la instrucción <code>action meterftp</code> cuando <code>ipgpc</code> haya completado el procesamiento.

Si necesita más información sobre cómo definir clases, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico”](#) en la página 52.

3 Defina cláusulas `filter` para seleccionar el tráfico de las clases definidas en el Paso 2.

```

filter {
    name smtpout
    sport smtp
    class smtp
}
filter {
    name newsout
    sport nntp
    class news
}
filter {
    name ftpout
    sport ftp
    class ftp
}
filter {
    name ftpdata
    sport ftp-data
    class ftp
}
}

```

<code>name smtpout</code>	Asigna el nombre <code>smtpout</code> al filtro.
<code>sport smtp</code>	Selecciona el tráfico con puerto de origen 25, el puerto para la aplicación <code>sendmail</code> (SMTP).
<code>class smtp</code>	Identifica la clase a la que pertenece el filtro, en este caso, la clase <code>smtp</code> .
<code>name newsout</code>	Asigna el nombre <code>newsout</code> al filtro.
<code>sport nntp</code>	Selecciona el tráfico con nombre de puerto origen <code>nntp</code> , el nombre de puerto para la aplicación de noticias de red (NNTP).

<code>class news</code>	Identifica la clase a la que pertenece el filtro, en este caso, la clase <code>news</code> .
<code>name ftpout</code>	Asigna el nombre <code>ftpout</code> al filtro.
<code>sport ftp</code>	Selecciona los datos de control con un puerto origen 21, el número de puerto para tráfico FTP.
<code>name ftpdata</code>	Asigna el nombre <code>ftpdata</code> al filtro.
<code>sport ftp-data</code>	Selecciona el tráfico con puerto de origen 20, el número de puerto para tráfico FTP.
<code>class ftp</code>	Identifica la clase a la que pertenecen los filtros <code>ftpout</code> y <code>ftpdata</code> , en este caso <code>ftp</code> .

- Véase también**
- Para definir filtros, consulte la sección “[Cómo definir filtros en el archivo de configuración IPQoS](#)” en la página 54.
 - Para definir comportamientos de reenvío para el tráfico de aplicaciones, consulte la sección “[Cómo configurar el reenvío para el tráfico de aplicaciones en el archivo de configuración IPQoS](#)” en la página 67.
 - Para configurar el control de flujo utilizando los módulos de medición, consulte la sección “[Cómo configurar el control de flujo en el archivo de configuración IPQoS](#)” en la página 69.
 - Para configurar la recopilación de datos sobre el flujo, consulte la sección “[Cómo activar el control para una clase en el archivo de configuración IPQoS](#)” en la página 59.

▼ Cómo configurar el reenvío para el tráfico de aplicaciones en el archivo de configuración IPQoS

En el siguiente procedimiento se muestra cómo configurar el reenvío para el tráfico de aplicaciones. En el procedimiento, se definen comportamientos por salto para clases de tráfico de aplicaciones que pueden tener precedencia más baja que otro tráfico de la red. Los pasos continúan con la creación del archivo `/var/ipqos/BigAPPS.qos` del [Ejemplo 3-3](#).

Antes de empezar En el procedimiento se asume que ya tiene un archivo de configuración IPQoS con clases y filtros definidos para las aplicaciones que se van a marcar.

- 1 **Abra el archivo de configuración IPQoS creado para el servidor de aplicaciones y localice el final de la última cláusula `filter`.**

En el archivo `/var/ipqos/BigAPPS.qos`, el último filtro es el siguiente:

```
filter {
    name ftpdata
    sport ftp-data
    class ftp
```

```
    }
}
```

2 Invoque el marcador del siguiente modo:

```
action {
    module dscpmk
    name markAF13
}
```

`module dscpmk` Invoca al módulo de marcador `dscpmk`.

`name markAF13` Asigna el nombre `markAF13` a la instrucción `action`.

3 Defina el comportamiento por salto que debe marcarse en los flujos de tráfico de correo electrónico.

```
    params {
        global_stats FALSE
        dscp_map{0-63:14}
        next_action continue
    }
}
```

`global_stats FALSE` Activa la recopilación de estadísticas para la instrucción `action` del marcador `markAF13`. Sin embargo, como el valor de `enable_stats` es `FALSE`, no se recopilan estadísticas.

`dscp_map{0-63:14}` Asigna un DSCP de valor 14 a los encabezados de paquetes de la clase de tráfico `smtp`, que esté procesando el marcador en ese momento.

`next_action continue` Indica que no se necesita más procesamiento en los paquetes de la clase de tráfico `smtp`. Estos paquetes pueden volver al flujo de red.

El valor DSCP de 14 indica al marcador que debe definir todas las entradas del mapa `dscp` en el valor decimal 14 (binario 001110). El DSCP de valor 14 define el comportamiento por salto AF13. El marcador marca los paquetes de la clase de tráfico `smtp` con el valor DSCP de 14 en el campo DS.

AF13 asigna todos los paquetes con un DSCP de 14 a una precedencia de alta probabilidad de descarte. Aunque, debido a que AF13 también garantiza una prioridad de Clase 1, el enrutador sigue garantizando una alta prioridad en cola al tráfico de correo electrónico saliente. Para ver una tabla de códigos para AF, consulte la [Tabla 6-2](#).

4 Agregue una instrucción `action` de marcador para definir un comportamiento por salto para el tráfico de noticias de red:

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

```
    }
}
```

`name markAF21` Asigna el nombre `markAF21` a la instrucción `action`.

`dscp_map{0-63:18}` Asigna un valor DSCP de 18 a los encabezados de paquetes de la clase de tráfico `nntp` que esté procesando el marcador en ese momento.

El valor DSCP de 18 indica al marcador que debe definir todas las entradas del mapa `dscp` en el valor decimal 18 (binario 010010). El valor DSCP 18 define el comportamiento por salto AF21. El marcador marca los paquetes de la clase de tráfico `news` con el valor DSCP de 18 en el campo DS.

AF21 garantiza que todos los paquetes con un valor DSCP de 18 reciben una precedencia de baja probabilidad de descarte, pero sólo con prioridad Clase 2. Por lo tanto, la posibilidad de que se descarte el tráfico de noticias de red es bajo.

- Véase también**
- Para agregar información de configuración para servidores web, consulte la sección “[Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico](#)” en la página 52.
 - Para configurar el control de flujo utilizando los módulos de medición, consulte la sección “[Cómo configurar el control de flujo en el archivo de configuración IPQoS](#)” en la página 69.
 - Para configurar la recopilación de datos sobre el flujo, consulte la sección “[Cómo activar el control para una clase en el archivo de configuración IPQoS](#)” en la página 59.
 - Para configurar comportamientos de reenvío en un enrutador, consulte la sección “[Cómo configurar un enrutador en una red con IPQoS](#)” en la página 72.
 - Para activar el archivo de configuración IPQoS, consulte la sección “[Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS](#)” en la página 76.

▼ **Cómo configurar el control de flujo en el archivo de configuración IPQoS**

Para controlar la tasa a la que un flujo de tráfico específico se envía en la red, debe definir parámetros para el medidor. Puede usar cualquiera de los dos módulos de medidor, `tokenmt` o `tswtclmt`, en el archivo de configuración IPQoS.

En el siguiente procedimiento, se continúa con la creación del archivo de configuración IPQoS para el servidor de aplicaciones del [Ejemplo 3-3](#). En el procedimiento, no sólo se configura el medidor, sino también las acciones de marcador a las que se llama desde la instrucción `action`.

- Antes de empezar** En los pasos se asume que ya ha definido una clase y un filtro para controlar el flujo de la aplicación.

1 Abra el archivo de configuración IPQoS que ha creado para el servidor de aplicaciones.

En el archivo `/var/ipqos/BigAPPS.qos`, empiece después de la siguiente acción de marcador:

```
action {
  module dscpmk
  name markAF21
  params {
    global_stats FALSE
    dscp_map{0-63:18}
    next_action continue
  }
}
```

2 Cree una instrucción `action` de medidor para controlar el flujo de tráfico de la clase `ftp`.

```
action {
  module tokenmt
  name meterftp
```

`module tokenmt` Invoca al medidor `tokenmt`.

`name meterftp` Asigna el nombre `meterftp` a la instrucción `action`.

3 Agregue parámetros para configurar la tasa del medidor.

```
params {
  committed_rate 50000000
  committed_burst 50000000
```

`committed_rate 50000000` Asigna una tasa de transmisión de 50.000.000 bps al tráfico de la clase `ftp`.

`committed_burst 50000000` Dedicar un tamaño de ráfaga de 50.000.000 de bits al tráfico de la clase `ftp`.

Para ver una explicación de los parámetros `tokenmt`, consulte la sección [“Configuración de `tokenmt` como medidor de doble tasa” en la página 93](#).

4 Agregue parámetros para configurar las precedencias de cumplimiento de tráfico:

```
  red_action markAF31
  green_action_name markAF22
  global_stats TRUE
}
```

`red_action_name markAF31` Indica que si el flujo de tráfico de la clase `ftp` excede la tasa asignada, los paquetes se envían a la instrucción `action` del marcador `markAF31`.

`green_action_name markAF22` Indica que si los flujos de tráfico de la clase `ftp` cumplen la tasa asignada, los paquetes se envían a la instrucción `action` de `markAF22`.

`global_stats TRUE` Activa las estadísticas de medición para la clase `ftp`.

Si necesita más información sobre el cumplimiento del tráfico, consulte la sección “[Módulo medidor](#)” en la [página 92](#).

5 Agregue una instrucción `action` de marcador para asignar un comportamiento por salto a los flujos de tráfico de la clase `ftp` que no cumplan la tasa.

```
action {
  module dscpmk
  name markAF31
  params {
    global_stats TRUE
    dscp_map{0-63:26}
    next_action continue
  }
}
```

`module dscpmk` Invoca al módulo de marcador `dscpmk`.

`name markAF31` Asigna el nombre `markAF31` a la instrucción `action`.

`global_stats TRUE` Activa las estadísticas para la clase `ftp`.

`dscp_map{0-63:26}` Asigna un valor DSCP de 26 a los encabezados de paquetes de la clase de tráfico `ftp` cuando el tráfico excede la tasa asignada.

`next_action continue` Indica que no se requiere más procesamiento para los paquetes de la clase de tráfico `ftp`. Estos paquetes pueden devolverse al flujo de red.

El valor DSCP de 26 indica al marcador que debe establecer todas las entradas del mapa `dscp` en el valor decimal 26 (binario 011010). El valor DSCP 26 define el comportamiento por salto AF31. El marcador marca los paquetes de la clase de tráfico `ftp` con el valor DSCP de 26 en el campo DS.

AF31 garantiza que todos los paquetes con un valor DSCP de 26 reciben una precedencia de baja probabilidad de descarte, pero sólo con prioridad Clase 3. Por lo tanto, la posibilidad de que se descarte el tráfico FTP que no cumple la tasa es baja. Para ver una tabla de códigos para AF, consulte la [Tabla 6-2](#).

6 Agregue una instrucción `action` de marcador para asignar un comportamiento por salto a los flujos de tráfico `ftp` que cumplen la tasa asignada.

```
action {
  module dscpmk
  name markAF22
  params {
    global_stats TRUE
    dscp_map{0-63:20}
    next_action continue
  }
}
```

`name markAF22` Asigna el nombre `markAF22` a la acción `marker`.

`dscp_map{0-63:20}` Asigna un valor DSCP de 20 a los encabezados de paquetes de la clase de tráfico ftp cuando el tráfico ftp cumple la tasa configurada.

El valor DSCP de 20 indica al marcador para definir todas las entradas del mapa dscp en el valor decimal 20 (binario 010100). El valor DSCP de 20 define el comportamiento por salto AF22. El marcador marca los paquetes de la clase de tráfico ftp con el valor DSCP de 20 en el campo DS.

AF22 garantiza que todos los paquetes con un valor DSCP de 20 reciben una precedencia de probabilidad de descarte media con prioridad de Clase 2. Por lo tanto, el tráfico FTP que cumple la tasa tiene garantizada una precedencia con probabilidad de descarte media entre los flujos enviados simultáneamente por el sistema IPQoS. Aunque el enrutador asigna una prioridad de reenvío más alta a las clases de tráfico con una marca de precedencia de probabilidad de descarte media de Clase 1 o superior. Para ver una tabla de códigos para AF, consulte la [Tabla 6-2](#).

7 Agregue los puntos DSCP que ha creado para el servidor de aplicaciones a los archivos correspondientes del enrutador Diffserv.

- Véase también**
- Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS”](#) en la página 76.
 - Para agregar información de configuración para servidores web, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico”](#) en la página 52.
 - Para configurar la recopilación de datos sobre el flujo, consulte la sección [“Cómo activar el control para una clase en el archivo de configuración IPQoS”](#) en la página 59.
 - Para configurar comportamientos de reenvío en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS”](#) en la página 72.

Suministro de servicios diferenciados en un enrutador

Para proporcionar servicios diferenciados reales, debe incluir un enrutador con Diffserv en su topología de red, como se describe en [“Estrategias de hardware para la red Diffserv”](#) en la página 28. Los pasos necesarios para configurar Diffserv en un enrutador y actualizar los archivos del enrutador no se explican en esta guía.

En esta sección se detallan los pasos generales para coordinar la información de reenvío entre varios sistemas con IPQoS en la red y el enrutador Diffserv.

▼ Cómo configurar un enrutador en una red con IPQoS

En el siguiente procedimiento se utiliza como ejemplo la topología de la [Figura 2-4](#).

Antes de empezar En el siguiente procedimiento se asume que ya ha configurado los sistemas IPQoS de la red realizando las tareas anteriores de este capítulo.

1 Revise los archivos de configuración de todos los sistemas con IPQoS de la red.

2 Identifique cada punto de código utilizado en las políticas QoS.

Muestre los puntos de código, y los sistemas y las clases a los que se aplican. La siguiente tabla ilustra áreas en las que puede haberse usado el mismo punto de código. Esta práctica es aceptable. Sin embargo, debe especificar otros criterios en el archivo de configuración IPQoS, como un selector precedence, para determinar la precedencia de las clases con marcas idénticas.

Por ejemplo, en la red de muestra que se utiliza en los procedimientos de este capítulo, puede generar la siguiente tabla de puntos de código.

Sistema	Clase	PHB	Punto de código DS
Goldweb	video	EF	46 (101110)
Goldweb	goldweb	AF11	10 (001010)
Userweb	webout	AF12	12 (001100)
BigAPPS	sntp	AF13	14 (001110)
BigAPPS	news	AF18	18 (010010)
BigAPPS	ftp conformant traffic	AF22	20 (010100)
BigAPPS	ftp nonconformant traffic	AF31	26 (011010)

3 Agregue los puntos de código de los archivos de configuración IPQoS de la red a los archivos correspondientes del enrutador Diffserv.

Los puntos de código proporcionados deben facilitar la configuración del mecanismo de planificación Diffserv del enrutador. Consulte la documentación y el sitio web del fabricante del enrutador si necesita instrucciones.

Inicio y mantenimiento de IPQoS (tareas)

Este capítulo contiene tareas para activar un archivo de configuración IPQoS y para el registro de eventos relacionados con IPQoS. Contiene los temas siguientes:

- [“Administración IPQoS \(mapa de tareas\)”](#) en la página 75
- [“Aplicación de una configuración IPQoS”](#) en la página 76
- [“Activación del registro syslog para mensajes IPQoS”](#) en la página 78
- [“Resolución de problemas con mensajes de error IPQoS”](#) en la página 79

Nota – Es posible que en futuras versiones se elimine la utilidad IPQoS. Se recomienda a los usuarios que, en su lugar, utilicen los comandos `dladm`, `flowadm` y comandos relacionados, que admiten funciones de control de los recursos de ancho de banda similares. Para obtener más información, consulte *Uso de redes virtuales en Oracle Solaris 11.1*.

Administración IPQoS (mapa de tareas)

Esta sección contiene el conjunto de tareas para iniciar y mantener el servicio IPQoS en un sistema Oracle Solaris. Antes de utilizar las tareas, debe tener un archivo de configuración IPQoS completado, como se describe en [“Definición de una política QoS en el archivo de configuración IPQoS \(mapa de tareas\)”](#) en la página 47.

La tabla siguiente enumera y describe esas tareas y contiene vínculos a las secciones que describen cómo realizarlas.

Tarea	Descripción	Para obtener instrucciones
1. Configurar IPQoS en un sistema.	Utilice el comando <code>ipqosconf</code> para activar el archivo de configuración IPQoS en un sistema.	“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 76

Tarea	Descripción	Para obtener instrucciones
2. Hacer que los comandos de inicio de Oracle Solaris apliquen el archivo de configuración IPQoS depurado cada vez que se inicie el sistema.	Asegúrese de que la configuración IPQoS se aplica cada vez que se reinicia el sistema.	“Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia” en la página 77
3. Activar el registro sys log para IPQoS.	Agregue una entrada para activar el registro sys log de mensajes IPQoS.	“Cómo activar el registro de mensajes IPQoS durante el inicio” en la página 78
4. Solucionar cualquier problema IPQoS que surja.	Solucione los problemas IPQoS utilizando mensajes de error.	Consulte los mensajes de error de la Tabla 4–1

Aplicación de una configuración IPQoS

La configuración IPQoS se activa y manipula con el comando `ipqosconf`.

▼ Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS

Se utiliza el comando `ipqosconf` para leer el archivo de configuración IPQoS y para configurar los módulos IPQoS del núcleo UNIX. En el siguiente procedimiento se utiliza como ejemplo el archivo `/var/ipqos/Goldweb.qos`, creado en la sección “[Creación de archivos de configuración IPQoS para servidores web](#)” en la página 50. Para obtener información detallada, consulte la página del comando `man ipqosconf(1M)`.

1 Conviértase en administrador.

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

2 Aplique la nueva configuración.

```
# /usr/sbin/ipqosconf -a/var/ipqos/Goldweb.qos
```

`ipqosconf` escribe la información en el archivo de configuración IPQoS especificado de los módulos IPQoS del núcleo de Oracle Solaris. En este ejemplo, el contenido de `/var/ipqos/Goldweb.qos` se aplica al núcleo de Oracle Solaris actual.

Nota – Cuando se aplica un archivo de configuración IPQoS con la opción `-a`, las acciones del archivo sólo se activan para la sesión actual.

3 Compruebe y depure la nueva configuración IPQoS.

Utilice las herramientas de UNIX para supervisar el comportamiento IPQoS y recopilar estadísticas sobre la implementación IPQoS. Esta información permite determinar si la configuración funciona como se esperaba.

- Véase también**
- Para ver estadísticas sobre cómo funcionan los módulos IPQoS, consulte la sección [“Recopilación de información estadística” en la página 86.](#)
 - Para registrar los mensajes `ipqosconf`, consulte la sección [“Activación del registro `syslog` para mensajes IPQoS” en la página 78.](#)
 - Para asegurarse de que la configuración IPQoS actual se aplica en cada inicio, consulte la sección [“Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia” en la página 77.](#)

▼ Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia

Debe hacer que la configuración IPQoS sea persistente en cada reinicio. En caso contrario, la configuración actual sólo se aplica hasta que el sistema se reinicia. Cuando la configuración IPQoS funcione correctamente en un sistema, haga lo siguiente para que la configuración sea persistente cada vez que se reinicia.

1 Conviértase en administrador.

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

2 Compruebe si existe una configuración IPQoS en los módulos de núcleo.

```
# ipqosconf -l
```

Si existe una configuración, `ipqosconf` la muestra en pantalla. Si no recibe ninguna respuesta, aplique la configuración, como se explica en la sección [“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 76.](#)

3 Asegúrese de que la configuración IPQoS existente se aplique cada vez que se reinicia el sistema IPQoS.

```
# /usr/sbin/ipqosconf -c
```

La opción `-c` hace que la configuración IPQoS actual esté presente en el archivo de configuración de inicio `/etc/inet/ipqosinit.conf`.

Activación del registro syslog para mensajes IPQoS

Para registrar mensajes de inicio IPQoS, es necesario modificar el archivo `/etc/syslog.conf` como se explica en el siguiente procedimiento.

▼ Cómo activar el registro de mensajes IPQoS durante el inicio

1 Conviértase en administrador.

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

2 Abra el archivo `/etc/syslog.conf`.

3 Agregue el siguiente texto como última entrada en el archivo.

```
user.info                /var/adm/messages
```

Utilice tabuladores en lugar de espacios entre las columnas.

La entrada registra todos los mensajes de inicio generados por IPQoS en el archivo `/var/adm/messages`.

4 Reinicie el sistema para aplicar los mensajes.

Ejemplo 4-1 Salida IPQoS de `/var/adm/messages`

Al revisar `/var/adm/messages` después de reiniciar el sistema, la salida puede contener mensajes de registro IPQoS similares a los siguientes.

```
May 14 10:44:33 ipqos-14 ipqosconf: [ID 815575 user.info]
  New configuration applied.
May 14 10:44:46 ipqos-14 ipqosconf: [ID 469457 user.info]
  Current configuration saved to init file.
May 14 10:44:55 ipqos-14 ipqosconf: [ID 435810 user.info]
  Configuration flushed.
```

También puede encontrar mensajes de error IPQoS similares a los siguientes en el archivo `/var/adm/messages` del sistema con IPQoS.

```
May 14 10:56:47 ipqos-14 ipqosconf: [ID 123217 user.error]
  Missing/Invalid config file fmt version.
May 14 10:58:19 ipqos-14 ipqosconf: [ID 671991 user.error]
  No ipgpc action defined.
```

Para ver una descripción de estos mensajes de error, consulte la [Tabla 4-1](#).

Resolución de problemas con mensajes de error IPQoS

En esta sección se incluye una tabla de mensajes de error generados por IPQoS y su posible solución.

TABLA 4-1 Mensajes de error IPQoS

Mensaje de error	Descripción	Solución
Undefined action in parameter <i>parameter-name's</i> action <i>action-name</i>	En el archivo de configuración IPQoS, el nombre de acción especificado en <i>parameter-name</i> no existe en el archivo de configuración.	Cree la acción. O haga referencia a otra acción en el parámetro.
action <i>action-name</i> involved in cycle	En el archivo de configuración IPQoS, <i>action-name</i> forma parte de un ciclo de acciones, lo que no está permitido por IPQoS.	Determine el ciclo de acciones. A continuación, elimine una de las referencias cíclicas del archivo de configuración IPQoS.
Action <i>action-name</i> isn't referenced by any other actions	Una definición de acción no <i>ipgpc</i> no es referenciada por ninguna otra acción definida en la configuración IPQoS, lo que no está permitido por IPQoS.	Elimine la acción no referenciada. También puede hacer que otra acción haga referencia a la acción no referenciada.
Missing/Invalid config file <i>fmt_version</i>	El formato del archivo de configuración no está especificado como primera entrada del archivo como requiere IPQoS.	Agregue la versión de formato, como se explica en “ Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico ” en la página 52.
Unsupported config file format version	La versión de formato especificada en el archivo de configuración no es compatible con IPQoS.	Cambie la versión de formato a <i>fmt_version 1.0</i> , que se requiere a partir de la versión Solaris 9 9/02 de IPQoS.
No <i>ipgpc</i> action defined.	No ha definido una acción para el clasificador <i>ipgpc</i> en el archivo de configuración, como requiere IPQoS.	Defina una acción para <i>ipgpc</i> , como se muestra en la sección “ Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico ” en la página 52.
Can't commit a null configuration	Cuando ejecutó <i>ipqosconf -c</i> para confirmar una configuración, dicha configuración estaba vacía, lo que no está permitido por IPQoS.	Asegúrese de aplicar un archivo de configuración antes de intentar confirmar una configuración. Si necesita instrucciones, consulte “ Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS ” en la página 76.
Invalid CIDR mask on line <i>line-number</i>	En el archivo de configuración, ha utilizado una máscara CIDR como parte de la dirección IP que está fuera del intervalo de direcciones IP válidas.	Cambie el valor de máscara por uno que se encuentre entre 1–32 para IPv4 y 1–128 para IPv6.
Address masks aren't allowed for host names line <i>line-number</i>	En el archivo de configuración, ha definido una máscara CIDR para un nombre de host, lo que no está permitido en IPQoS.	Elimine la máscara o cambie el nombre de host por una dirección IP.

TABLA 4-1 Mensajes de error IPQoS (Continuación)

Mensaje de error	Descripción	Solución
Invalid module name line <i>line-number</i>	En el archivo de configuración, el nombre de módulo que ha especificado en una instrucción <code>action</code> no es válido.	Compruebe que el nombre de módulo esté bien escrito. Para ver una lista de módulos IPQoS, consulte la Tabla 6-5 .
ipgpc action has incorrect name line <i>line-number</i>	El nombre asignado a la acción <code>ipgpc</code> en el archivo de configuración no es el nombre <code>ipgpc.classify</code> requerido.	Cambie el nombre de la acción <code>ipgpc.classify</code> .
Second parameter clause not supported line <i>line-number</i>	En el archivo de configuración, ha especificado dos cláusulas de parámetro para una única acción, lo que no está permitido por IPQoS.	Combine todos los parámetros de la acción en una única cláusula de parámetro.
Duplicate named action	En el archivo de configuración, ha asignado el mismo nombre a dos acciones.	Cambie el nombre de una de las acciones o elimínela.
Duplicate named filter/class in action <i>action-name</i>	Ha asignado el mismo nombre a dos filtros o dos clases en la misma acción, lo que no se permite en el archivo de configuración IPQoS.	Cambie el nombre de uno de los filtros o clases, o elimínelo.
Undefined class in filter <i>filter-name</i> in action <i>action-name</i>	En el archivo de configuración, el filtro hace referencia a una clase no definida en la acción.	Cree la clase, o cambie la referencia del filtro a una clase existente.
Undefined action in class <i>class-name</i> action <i>action-name</i>	La clase hace referencia a una acción no definida en el archivo de configuración.	Cree la acción, o cambie la referencia a una acción existente.
Invalid parameters for action <i>action-name</i>	En el archivo de configuración, uno de los parámetros no es válido.	Para ver el módulo al que llama la acción especificada, consulte la entrada de módulo de la sección “Arquitectura IPQoS y el modelo Diffserv” en la página 89 . También puede consultar la página del comando <code>man ipqosconf(1M)</code> .
Mandatory parameter missing for action <i>action-name</i>	No ha definido un parámetro requerido para una acción en el archivo de configuración.	Para ver el módulo al que llama la acción especificada, consulte la entrada de módulo de la sección “Arquitectura IPQoS y el modelo Diffserv” en la página 89 . También puede consultar la página del comando <code>man ipqosconf(1M)</code> .
Max number of classes reached in ipgpc	Ha especificado más clases de las permitidas en la acción <code>ipgpc</code> del archivo de configuración IPQoS. El número máximo es 10007.	Revise el archivo de configuración y elimine las clases innecesarias. También puede aumentar el número máximo de clases agregando al archivo <code>/etc/system</code> la entrada <code>ipgpc_max_classes class-number</code> .
Max number of filters reached in action ipgpc	Ha especificado más filtros de los permitidos en la acción <code>ipgpc</code> del archivo de configuración IPQoS. El número máximo es 10007.	Revise el archivo de configuración y elimine los filtros innecesarios. También puede aumentar el número máximo de filtros agregando al archivo <code>/etc/system</code> la entrada <code>ipgpc_max_filters filter-number</code> .

TABLA 4-1 Mensajes de error IPQoS (Continuación)

Mensaje de error	Descripción	Solución
Invalid/missing parameters for filter <i>filter-name</i> in action <i>ipgpc</i>	En el archivo de configuración, el filtro <i>filter-name</i> tiene parámetros no válidos o no especificados.	Consulte la página del comando <code>man ipqosconf(1M)</code> para ver una lista de parámetros válidos.
Name not allowed to start with '!', line <i>line-number</i>	Inicia una acción, un filtro o un nombre de clase con un signo de exclamación (!), lo cual no está permitido en el archivo IPQoS.	Elimine el signo de exclamación o cambie el nombre completo de la acción, clase o filtro.
Name exceeds the maximum name length line <i>line-number</i>	Ha definido un nombre de una acción, clase o filtro en el archivo de configuración que excede la longitud máxima de 23 caracteres.	Asigne un nombre más corto a la acción, clase o filtro.
Array declaration line <i>line-number</i> is invalid	En el archivo de configuración, la declaración de matriz del parámetro de la línea <i>line-number</i> no es válido.	Para ver la sintaxis correcta de la declaración de matriz a la que llama la instrucción <code>act ion</code> con la matriz no válida, consulte “Arquitectura IPQoS y el modelo Diffserv” en la página 89 . También puede consultar la página del comando <code>man ipqosconf(1M)</code> .
Quoted string exceeds line, <i>line-number</i>	La cadena no tiene las comillas de cierre en la misma línea, lo que es obligatorio en el archivo de configuración.	Asegúrese de que la cadena citada empieza y termina en la misma línea en el archivo de configuración.
Invalid value, line <i>line-number</i>	El valor definido en la línea <i>line-number</i> del archivo de configuración no es compatible con el parámetro.	Para ver los valores aceptables para el módulo al que llama la instrucción <code>act ion</code> , consulte la descripción del módulo en “Arquitectura IPQoS y el modelo Diffserv” en la página 89 . También puede consultar la página del comando <code>man ipqosconf(1M)</code> .
Unrecognized value, line <i>line-number</i>	El valor de <i>line-number</i> del archivo de configuración no es un valor de enumeración admitido para este parámetro.	Compruebe que el valor de enumeración es correcto para el parámetro. Para ver una descripción del módulo al que llama la instrucción <code>act ion</code> con el número de línea no reconocido, consulte “Arquitectura IPQoS y el modelo Diffserv” en la página 89 . También puede consultar la página del comando <code>man ipqosconf(1M)</code> .
Malformed value list line <i>line-number</i>	La enumeración especificada en <i>line-number</i> del archivo de configuración no cumple la sintaxis de especificación.	Para ver la sintaxis correcta del módulo al que llama la instrucción <code>act ion</code> con la lista de valores mal formada, consulte la descripción del módulo en “Arquitectura IPQoS y el modelo Diffserv” en la página 89 . También puede consultar la página del comando <code>man ipqosconf(1M)</code> .
Duplicate parameter line <i>line-number</i>	Se ha especificado un parámetro duplicado en <i>line-number</i> , lo que no está permitido en el archivo de configuración.	Elimine uno de los parámetros duplicados.

TABLA 4-1 Mensajes de error IPQoS (Continuación)

Mensaje de error	Descripción	Solución
Invalid action name line <i>line-number</i>	Ha asignado a la acción de <i>line-number</i> del archivo de configuración un nombre que utiliza el nombre predefinido “continue” o “drop”.	Cambie el nombre de la acción de modo que no utilice un nombre predefinido.
Failed to resolve src/dst host name for filter at line <i>line-number</i> , ignoring filter	ipqosconf no ha podido determinar la dirección de origen o destino definida para el filtro en el archivo de configuración. Por lo tanto, se omite el filtro.	Si el filtro es importante, intente aplicar la configuración más adelante.
Incompatible address version line <i>line-number</i>	La versión IP de la dirección de <i>line-number</i> es incompatible con la versión de una dirección IP especificada previamente o parámetro ip_version.	Cambie las dos entradas en conflicto para que sean compatibles.
Action at line <i>line-number</i> has the same name as currently installed action, but is for a different module	Ha intentado cambiar el módulo de una acción que ya existe en la configuración IPQoS del sistema, lo que no está permitido.	Vacíe la configuración actual antes de aplicar la nueva configuración.

Uso de control de flujo y recopilación de estadísticas (tareas)

En este capítulo se explica como obtener datos de control y estadísticas sobre el tráfico administrador por un sistema IPQoS. Se explican los siguientes temas:

- “Establecimiento del control de flujo (mapa de tareas)” en la página 83
- “Registro de información sobre flujos de tráfico” en la página 84
- “Recopilación de información estadística” en la página 86

Nota – Es posible que en futuras versiones se elimine la utilidad IPQoS. Se recomienda a los usuarios que, en su lugar, utilicen los comandos `dladm`, `flowadm` y comandos relacionados, que admiten funciones de control de los recursos de ancho de banda similares. Para obtener más información, consulte *Uso de redes virtuales en Oracle Solaris 11.1*.

Establecimiento del control de flujo (mapa de tareas)

En el siguiente mapa de tareas se enumeran las tareas genéricas para obtener información sobre flujos de tráfico utilizando el módulo `flowacct`. El mapa también ofrece vínculos a los procedimientos para realizar estas tareas.

Tarea	Descripción	Para obtener instrucciones
1. Crear un archivo para guardar la información de control de flujos de tráfico.	Utilice el comando <code>acctadm</code> para crear un archivo en el que se almacenarán los resultados del procesamiento de <code>flowacct</code> .	“Cómo crear un archivo para datos de control de flujo” en la página 84
2. Definir los parámetros <code>flowacct</code> en el archivo de configuración IPQoS.	Defina valores para los parámetros <code>timer</code> , <code>timeout</code> y <code>max_limit</code> .	“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 59

Registro de información sobre flujos de tráfico

El módulo `flowacct` de IPQoS se utiliza para recopilar información sobre flujos de tráfico. Por ejemplo, puede recopilar direcciones de origen y destino, número de paquetes de un flujo y datos similares. El proceso de recopilar y registrar información sobre flujos se denomina *control de flujo*.

Los resultados del control de flujo de tráfico de una clase determinada se guardan en una tabla de *registros de flujo*. Cada registro de flujo contiene una serie de atributos. Estos atributos contienen datos sobre flujos de tráfico de una clase determinada en un intervalo de tiempo. Para ver una lista de los atributos de `flowacct`, consulte la [Tabla 6-4](#).

El control de flujo es especialmente útil para facturar a los clientes según lo definido en sus acuerdos de nivel de servicio (SLA). También puede utilizar el control de flujo para obtener estadísticas de aplicaciones importantes. En esta sección se incluyen las tareas para utilizar `flowacct` con la utilidad de contabilidad ampliada de Oracle Solaris para obtener datos sobre flujos de tráfico.

La siguiente información se encuentra en otras fuentes, no en este capítulo:

- Para obtener instrucciones para crear una instrucción de acción para `flowacct` en el archivo de configuración IPQoS, consulte “[Cómo configurar el control de flujo en el archivo de configuración IPQoS](#)” en la página 69.
- Para aprender cómo funciona `flowacct`, consulte “[Módulo clasificador](#)” en la página 90.
- Para obtener información técnica, consulte la página del comando `man flowacct(7ipp)`.

▼ Cómo crear un archivo para datos de control de flujo

Antes de agregar una acción `flowacct` al archivo de configuración IPQoS, debe crear un archivo para los registros de flujo desde el módulo `flowacct`. Para esto se utiliza el comando `acctadm`. `acctadm` puede registrar atributos básicos o ampliados en el archivo. Todos los atributos `flowacct` aparecen en la [Tabla 6-4](#). Para obtener información detallada sobre `acctadm`, consulte la página del comando `man acctadm(1M)`.

1 Conviértase en administrador.

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

2 Cree un archivo de control de flujo básico.

En el siguiente ejemplo se muestra cómo crear un archivo de control de flujo básico para el servidor web configurado en el [Ejemplo 3-1](#).

```
# /usr/sbin/acctadm -e basic -f /var/ipqos/goldweb/account.info flow
```

<code>acctadm -e</code>	Invoca a <code>acctadm</code> con la opción <code>-e</code> . La opción <code>-e</code> activa los argumentos que hay a continuación.
<code>basic</code>	Determina que sólo los datos de los ocho atributos básicos <code>flowacct</code> se registran en el archivo.
<code>/var/ipqos/goldweb/account.info</code>	Especifica el nombre de ruta completo del archivo que contendrá los registros de flujo de <code>flowacct</code> .
<code>flow</code>	Indica a <code>acctadm</code> que debe activar el control de flujo.

3 Para ver la información de control de flujo del sistema IPQoS, escriba `acctadm` sin argumentos.

`acctadm` genera la siguiente salida:

```
Task accounting: inactive
  Task accounting file: none
  Tracked task resources: none
  Untracked task resources: extended
    Process accounting: inactive
    Process accounting file: none
  Tracked process resources: none
  Untracked process resources: extended,host,mstate
    Flow accounting: active
    Flow accounting file: /var/ipqos/goldweb/account.info
  Tracked flow resources: basic
  Untracked flow resources: dsfield,ctime,lseen,projid,uid
```

Todas las entradas, menos las cuatro últimas, se deben utilizar con la función Oracle Solaris Resource Manager. En la siguiente tabla se explican las entras específicas de IPQoS.

Entrada	Descripción
<code>Flow accounting: active</code>	Indica que el control de flujo está activado.
<code>Flow accounting file: /var/ipqos/goldweb/account.info</code>	Da el nombre del archivo de control de flujo actual.
<code>Tracked flow resources: basic</code>	Indica que sólo se supervisan los atributos de flujo básicos.
<code>Untracked flow resources: dsfield,ctime,lseen,projid,uid</code>	Enumera los atributos <code>flowacct</code> que no se supervisan en el archivo.

4 (Opcional) Agregue los atributos ampliados al archivo de control.

```
# acctadm -e extended -f /var/ipqos/goldweb/account.info flow
```

5 (Optativo) Vuelva a registrar sólo los atributos básicos en el archivo de control.

```
# acctadm -d extended -e basic -f /var/ipqos/goldweb/account.info
```

La opción `-d` desactiva la contabilidad ampliada.

6 Ve el contenido de un archivo de control de flujo.

Para obtener instrucciones para ver el contenido de un archivo de control de flujo, consulte “Interfaz Perl para libexacct” de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

- Véase también**
- Para obtener información detallada sobre la función de control ampliada, consulte el Capítulo 4, “Contabilidad ampliada (descripción general)” de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.
 - Para definir parámetros flowacct en el archivo de configuración IPQoS, consulte “Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 59.
 - Para imprimir los datos en el archivo creado con el comando acctadm, consulte “Interfaz Perl para libexacct” de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

Recopilación de información estadística

Puede utilizar el comando `kstat` para generar información estadística de los módulos IPQoS. Use la sintaxis siguiente:

```
/bin/kstat -m ipqos-module-name
```

Puede especificar cualquier nombre de módulo IPQoS válido, como se muestra en la [Tabla 6-5](#). Por ejemplo, para ver estadísticas generadas por el marcador `dscpmk`, utilice el siguiente comando de `kstat`:

```
/bin/kstat -m dscpmk
```

Si necesita información técnica, consulte la página del comando `man kstat(1M)`.

EJEMPLO 5-1 Estadísticas `kstat` de IPQoS

A continuación se muestra un ejemplo del posible resultado al ejecutar `kstat` para obtener estadísticas sobre el módulo `flowacct`.

```
# kstat -m flowacct
module: flowacct           instance: 3
name: Flowacct statistics  class:  flacct
      bytes_in_tbl         84
      crtime                345728.504106363
      epackets              0
      flows_in_tbl         1
      nbytes                84
      npackets              1
      snaptime              345774.031843301
      usedmem               256
```

EJEMPLO 5-1 Estadísticas `kstat` de IPQoS (Continuación)

<code>class: flacct</code>	Da el nombre de la clase a la que pertenecen los flujos de tráfico, en este caso <code>flacct</code> .
<code>bytes_in_tbl</code>	Número total de bytes en la tabla de flujo. El número total de bytes es la suma en bytes de todos los registros de flujo actuales de la tabla de flujo. La cantidad total de bytes de esta tabla de flujo es de 84. Si no hay ningún flujo en la tabla, el valor de <code>bytes_in_tbl</code> es 0.
<code>crtime</code>	La última vez que se creó esta salida de <code>kstat</code> .
<code>epackets</code>	Número de paquetes que resultaron en un error durante el procesamiento, en este ejemplo 0.
<code>flows_in_tbl</code>	Número de registros de flujo que hay en la tabla de flujos, en este ejemplo es 1. Si no hay ningún registro en la tabla, el valor de <code>flows_in_tbl</code> es 0.
<code>nbytes</code>	Número total de bytes observados por esta instancia de acción <code>flowacct</code> , que en este ejemplo es 84. El valor incluye bytes que se encuentran actualmente en la tabla de flujo. El valor también incluye bytes obsoletos que ya no se encuentran en la tabla de flujo.
<code>npackets</code>	Número total de paquetes observados por esta instancia de acción <code>flowacct</code> , que en este ejemplo es 1. <code>npackets</code> incluye paquetes que actualmente están en la tabla de flujo. <code>npackets</code> también incluye paquetes obsoletos, que ya no están en la tabla de flujo.
<code>usedmem</code>	Memoria en bytes en uso por la tabla de flujo mantenida por esta instancia <code>flowacct</code> . En el ejemplo, el valor <code>usedmem</code> es 256. El valor de <code>usedmem</code> es 0 cuando la tabla de flujo no contiene ningún registro de flujo.

IPQoS detallado (referencia)

Este capítulo contiene material de referencia con información detallada sobre los siguientes temas de IPQoS:

- “Arquitectura IPQoS y el modelo Diffserv” en la página 89
- “Archivo de configuración IPQoS” en la página 102
- “Utilidad de configuración `ipqos conf`” en la página 106

Para obtener una descripción general, consulte el [Capítulo 1, “Introducción a IPQoS \(descripción general\)”](#). Si necesita información sobre la planificación, consulte el [Capítulo 2, “Planificación para una red con IPQoS \(tareas\)”](#). Para ver los procedimientos para configurar IPQoS, consulte el [Capítulo 3, “Creación del archivo de configuración IPQoS \(tareas\)”](#).

Nota – Es posible que en futuras versiones se elimine la utilidad IPQoS. Se recomienda a los usuarios que, en su lugar, utilicen los comandos `dladm`, `flowadm` y comandos relacionados, que admiten funciones de control de los recursos de ancho de banda similares. Para obtener más información, consulte *Uso de redes virtuales en Oracle Solaris 11.1*.

Arquitectura IPQoS y el modelo Diffserv

En esta sección se describe la arquitectura IPQoS y cómo IPQoS implementa el modelo de servicios diferenciados (Diffserv) definido en [RFC 2475, An Architecture for Differentiated Services \(<http://www.ietf.org/rfc/rfc2475.txt?number=2475>\)](#). Los siguientes elementos del modelo Diffserv están incluidos en IPQoS:

- Clasificador
- Medidor
- Marcador

Además, IPQoS incluye el módulo de control de flujo y el marcador `d1cosmk` para su uso en dispositivos de red de área local virtual (VLAN).

Módulo clasificador

En el modelo Diffserv, el módulo *clasificador* se encarga de organizar los flujos de tráfico seleccionados en grupos a los que se aplican diferentes niveles de servicio. Los clasificadores definidos en RFC 2475 se diseñaron originalmente para enrutadores de límite de sistema. En cambio, el clasificador IPQoS *ipgpc* está diseñado para administrar flujos de tráfico en hosts internos de la red local. Por lo tanto, una red con sistemas IPQoS y un enrutador Diffserv puede proporcionar un alto nivel de servicios diferenciados. Para ver una descripción técnica de *ipgpc*, consulte la página del comando `man ipgpc(7ipp)`.

El clasificador *ipgpc* se encarga de lo siguiente:

1. Selecciona los flujos de tráfico que cumplen los criterios especificados en el archivo de configuración IPQoS en el sistema con IPQoS.

La política QoS define varios criterios que deben estar presentes en los encabezados de paquetes. Estos criterios se denominan *selectores*. El clasificador *ipgpc* compara estos selectores con los encabezados de paquetes que recibe el sistema IPQoS. A continuación, *ipgpc* selecciona todos los paquetes coincidentes.

2. Separa los flujos de paquetes en *clases*, tráfico de red con las mismas características, como se ha definido en el archivo de configuración IPQoS.
3. Examina el valor del campo de servicios diferenciados (DS) del paquete para comprobar si contiene un punto de código de servicios diferenciados (DSCP).

La presencia de un punto de código DSCP indica si el tráfico entrante ha sido marcado en su origen con un comportamiento de reenvío.

4. Determina qué otras acciones están especificadas en la configuración IPQoS para paquetes de una clase específica.
5. Transfiere los paquetes al siguiente módulo IPQoS especificado en el archivo de configuración IPQoS, o los devuelve al flujo de red.

Para ver una descripción general del clasificador, consulte [“Descripción general del clasificador \(ipgpc\)” en la página 17](#). Si necesita información sobre cómo invocar al clasificador en el archivo de configuración IPQoS, consulte [“Archivo de configuración IPQoS” en la página 102](#).

Selectores IPQoS

El clasificador *ipgpc* admite varios selectores que se pueden usar en la cláusula `filter` del archivo de configuración IPQoS. Al usar un filtro, utilice siempre el número mínimo de selectores necesarios para extraer el tráfico de una clase determinada. El número de filtros definidos repercute en el rendimiento de IPQoS.

En la siguiente tabla se muestran los selectores disponibles para *ipgpc*.

TABLA 6-1 Selectores de filtro para el clasificador IPQoS

Selector	Argumento	Información seleccionada
saddr	Número de dirección IP.	Dirección de origen.
daddr	Número de dirección IP.	Dirección de destino.
sport	Un número de puerto o nombre de servicio, definido en <code>/etc/services</code> .	Puerto de origen del que proviene una clase de tráfico.
dport	Un número de puerto o nombre de servicio, definido en <code>/etc/services</code> .	Puerto de destino de una clase de tráfico.
protocol	Un número o nombre de protocolo, definido en <code>/etc/protocols</code> .	Protocolo que usará esta clase de tráfico.
dsfield	Punto de código DS (DSCP) con un valor de 0–63.	DSCP que define cualquier comportamiento de reenvío que deb aplicarse al paquete. Si se especifica este parámetro, el parámetro <code>dsfield_mask</code> también debe especificarse.
dsfield_mask	Máscara de bit con un valor de 0–255.	Se utiliza en combinación con el selector <code>dsfield</code> . <code>dsfield_mask</code> se aplica al selector <code>dsfield</code> para determinar qué bit se utiliza para la comparación.
if_name	Nombre de interfaz.	Interfaz que se utiliza para el tráfico entrante o saliente de una clase determinada.
user	Número del ID de usuario o nombre de usuario de UNIX que se seleccionará. Si no hay ningún ID de usuario ni nombre de usuario en el paquete, se utilizará la opción predeterminada <code>-1</code> .	ID de usuario que se suministra a una aplicación.
projid	Número de ID de proyecto que se seleccionará.	ID de proyecto que se suministra a una aplicación.
priority	Número de prioridad. La prioridad más baja es 0.	Prioridad que se asigna a paquetes de esta clase. La prioridad se utiliza para ordenar la importancia de filtros de la misma clase.
direction	El argumento puede ser uno de los siguientes: <code>LOCAL_IN</code> <code>LOCAL_OUT</code> <code>FWD_IN</code> <code>FWD_OUT</code>	Dirección del flujo de paquete en el equipo IPQoS. Tráfico de entrada local del sistema IPQoS. Tráfico de salida local del sistema IPQoS. Tráfico de entrada que se debe reenviar. Tráfico de salida que se debe reenviar.
precedence	Valor de precedencia. La precedencia más alta es 0.	La precedencia se utiliza para ordenar filtros con la misma prioridad.
ip_version	V4 o V6	Esquema de direcciones utilizado por los paquetes, IPv4 o IPv6.

Módulo medidor

El *medidor* realiza un seguimiento de la tasa de transmisión de los flujos por paquete. Después, determina si el paquete cumple los parámetros configurados. El módulo medidor determina la siguiente acción para un paquete de un conjunto de acciones, que dependen del tamaño del paquete, los parámetros configurados y la tasa de flujo.

El medidor consta de dos módulos de medición, `tokenmt` y `tswtclmt`, que se configuran en el archivo de configuración IPQoS. Puede configurar uno de los módulos, o ambos, para una clase.

Al configurar un módulo de medición, puede definir dos parámetros de tasa:

- `committed-rate`: define la tasa de transmisión aceptable, en bits por segundo, para paquetes de una clase determinada.
- `peak-rate`: define la tasa de transmisión máxima, en bits por segundo, que se permite para paquetes de una clase determinada.

Una acción de medición en un paquete puede dar tres resultados:

- `green`: el paquete permite que el flujo se mantenga en la tasa aprobada.
- `yellow`: el paquete hace que el flujo sobrepase su tasa aprobada pero no la máxima.
- `red`: el paquete hace que el flujo sobrepase su tasa máxima.

Puede configurar cada resultado con acciones diferentes en el archivo de configuración IPQoS. La tasa aprobada y la tasa máxima se explican en la siguiente sección.

Módulo de medición `tokenmt`

El módulo `tokenmt` utiliza *token buckets* para medir la tasa de transmisión de un flujo. Puede configurar `tokenmt` para que funcione como medidor de tasa única o de doble tasa. Una instancia de acción `tokenmt` mantiene dos conjuntos de tokens que determinan si el flujo de tráfico cumple los parámetros configurados.

En la página del comando `man tokenmt(7ipp)` se explica de qué manera IPQoS utiliza el paradigma de medidor de tokens. Puede encontrar más información general sobre conjuntos de tokens en el documento *Differentiated Services for the Internet* escrito por Kalevi Kilkki y en varias páginas web.

Los parámetros de configuración para `tokenmt` son los siguientes:

- `committed_rate`: especifica la tasa aprobada para el flujo, en bits por segundo.
- `committed_burst`: especifica el tamaño de ráfaga aprobado en bits. El parámetro `committed_burst` define cuántos paquetes de una clase determinada pueden transmitirse a la red a la tasa aprobada.
- `peak_rate`: especifica la tasa máxima en bits por segundo.

- `peak_burst`: especifica el tamaño de ráfaga máxima en bits. El parámetro `peak_burst` asigna a una clase de tráfico un tamaño de ráfaga máxima que sobrepasa la tasa aprobada.
- `color_aware`: establece `tokenmt` en modo de activación.
- `color_map`: define una matriz de enteros que asigna valores DSCP a verde, amarillo o rojo.

Configuración de `tokenmt` como medidor de tasa única

Para configurar `tokenmt` como un medidor de tasa única, no especifique un parámetro `peak_rate` para `tokenmt` en el archivo de configuración IPQoS. Para configurar una instancia de `tokenmt` de tasa única para que dé un resultado rojo, verde o amarillo, debe especificar el parámetro `peak_burst`. Si no utiliza el parámetro `peak_burst`, puede configurar `tokenmt` para que sólo dé un resultado rojo o verde. Para ver un ejemplo de `tokenmt` de tasa única con dos resultados, consulte el [Ejemplo 3-3](#).

Cuando `tokenmt` funciona como medidor de tasa única, el parámetro `peak_burst` en realidad es el tamaño de ráfaga de exceso. Los parámetros `committed_rate` y `committed_burst` o `peak_burst` deben ser números enteros positivos distintos de cero.

Configuración de `tokenmt` como medidor de doble tasa

Para configurar `tokenmt` como medidor de doble tasa, especifique un parámetro `peak_rate` para la acción `tokenmt` en el archivo de configuración IPQoS. Un `tokenmt` de doble tasa siempre tiene los tres resultados: rojo, amarillo y verde. Los parámetros `committed_rate`, `committed_burst` y `peak_burst` deben ser números enteros positivos distintos de cero.

Configuración de `tokenmt` para que reconozca los colores

Para configurar un `tokenmt` de doble tasa para que reconozca los colores, debe agregar parámetros para agregar específicamente "reconocimiento de color". A continuación se muestra un ejemplo de instrucción `action` que configura `tokenmt` para que reconozca colores.

EJEMPLO 6-1 Acción `tokenmt` de reconocimiento de color para el archivo de configuración IPQoS

```
action {
  module tokenmt
  name meter1
  params {
    committed_rate 4000000
    peak_rate 8000000
    committed_burst 4000000
    peak_burst 8000000
    global_stats true
    red_action_name continue
    yellow_action_name continue
    green_action_name continue
    color_aware true
    color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
  }
}
```

EJEMPLO 6-1 Acción tokenmt de reconocimiento de color para el archivo de configuración IPQoS
(Continuación)

```
}
```

Para activar el reconocimiento de color, hay que establecer el parámetro `color_aware` en `true`. Como medidor con reconocimiento de color, `tokenmt` asume que el paquete ya ha sido marcado como rojo, amarillo o verde por una acción `tokenmt` anterior. `tokenmt` con reconocimiento de color evalúa los paquetes utilizando el punto de código DSCP del encabezado, además de los parámetros de un medidor de doble tasa.

El parámetro `color_map` contiene una matriz en la que se asigna el punto de código DSCP del encabezado del paquete. Observe la siguiente matriz `color_map`:

```
color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
```

Los paquetes con un DSCP de 0–20 y 22 se asignan al verde. Los paquetes con un DSCP de 21 y 23–42 se asignan al rojo. Los paquetes con un DSCP de 43–63 se asignan al amarillo. `tokenmt` mantiene un mapa de color predeterminado. Sin embargo, puede cambiar los valores predeterminados según sea necesario, utilizando los parámetros `color_map`.

En los parámetros `color_action_name`, puede especificar `continue` para completar el procesamiento del paquete. También puede añadir un argumento para enviar el paquete a una acción de marcador, por ejemplo `yellow_action_name mark22`.

Módulo de medición `tswtclmt`

El módulo de medición `tswtclmt` realiza una estimación del ancho de banda medio para una clase de tráfico utilizando un *estimador de tasa* basado en tiempo. `tswtclmt` siempre funciona como medidor con tres resultados. El estimador de tasa proporciona una estimación de la tasa de llegada del flujo. Esta tasa debe ser aproximada al ancho de banda medio del flujo de tráfico en un periodo de tiempo determinado, la *fase temporal*. El algoritmo de estimación de tasa se toma de RFC 2859, *un marcador de tres colores con fase temporal de desplazamiento*.

Para configurar `tswtclmt` se utilizan los siguientes parámetros:

- `committed_rate`: especifica la tasa aprobada en bits por segundo.
- `peak_rate`: especifica la tasa máxima en bits por segundo.
- `window`: define la fase temporal, en milisegundos en los cuales se mantiene el historial de ancho de banda medio.

Para obtener información técnica sobre `tswtclmt`, consulte la página del comando `man tswtclmt(7ipp)`. Para obtener información general sobre formadores de tasa similares a `tswtclmt`, consulte RFC 2963, *A Rate Adaptive Shaper for Differentiated Services* (<http://www.ietf.org/rfc/rfc2963.txt?number=2963>).

Módulo marcador

IPQoS incluye dos módulos de marcador, `ds cpmk` y `d lcosmk`. Esta sección contiene información sobre cómo usar ambos marcadores. Normalmente se utiliza `ds cpmk`, porque `d lcosmk` sólo está disponible para sistemas IPQoS con dispositivos VLAN.

Si necesita información técnica sobre `ds cpmk`, consulte la página del comando `man ds cpmk(7ipp)`. Para obtener información técnica sobre `d lcosmk`, consulte la página del comando `man d lcosmk(7ipp)`.

Utilización del marcador `ds cpmk` para reenviar paquetes

El marcador recibe los flujos de tráfico después de que los flujos han sido procesados por el clasificador o por los módulos de medición. El marcador marca el tráfico con un comportamiento de reenvío. Este comportamiento de reenvío es la acción que se realizará en los flujos cuando salgan del sistema IPQoS. El comportamiento de reenvío para una clase de tráfico se define en el *comportamiento por salto (PHB)*. El PHB asigna una prioridad a una clase de tráfico, que indica los flujos de precedencia de esa clase en relación con otras clases de tráfico. Los comportamientos PHB sólo determinan los comportamientos de reenvío en la red contigua del sistema IPQoS. Si necesita más información sobre comportamientos PHB, consulte [“Comportamientos por salto” en la página 22](#).

El *reenvío de paquetes* es el proceso de enviar tráfico de una clase determinada a su siguiente destino en una red. En un host como un sistema IPQoS, un paquete se reenvía del host al flujo de red local. Para un enrutador Diffserv, un paquete se reenvía de la red local al siguiente salto del enrutador.

El marcador marca el campo DS del encabezado del paquete con un comportamiento de reenvío común, definido en el archivo de configuración IPQoS. A partir de ahí, el sistema IPQoS y los sistemas con Diffserv siguientes, reenvían el tráfico como se indica en el campo DS, hasta que cambia la marca. Para asignar un PHB, el sistema IPQoS marca un valor en el campo DS del encabezado del paquete. Este valor se denomina punto de código de servicios diferenciados (DSCP). La arquitectura Diffserv define dos tipos de comportamientos de reenvío, EF y AF, que utilizan diferentes puntos DSCP. Si necesita información general sobre DSCP, consulte [“Punto de código DS” en la página 22](#).

El sistema IPQoS lee el punto de código DSCP del flujo de tráfico y evalúa la precedencia del flujo con respecto a otros flujos de tráfico saliente. A continuación, el sistema IPQoS prioriza todos los flujos de tráfico concurrentes y envía cada flujo a la red según su prioridad.

El enrutador Diffserv recibe los flujos de tráfico saliente y lee el campo DS de los encabezados de los paquetes. El punto de código DSCP permite al enrutador priorizar y programar los flujos de tráfico concurrentes. El enrutador reenvía cada flujo según la prioridad indicada en el PHB. Tenga en cuenta que el PHB no puede aplicarse fuera del enrutador de límite de sistema de la red, a no ser que haya sistemas con Diffserv en los siguientes puntos que también reconozcan el mismo PHB.

Reenvío acelerado (EF) PHB

El *reenvío acelerado* (EF) garantiza que los paquetes con el punto de código EF recomendado, 46 (101110), reciban el mejor tratamiento posible al enviarse a la red. El reenvío acelerado puede compararse con una línea alquilada. Los paquetes con el punto de código 46 (101110) tienen garantizado un tratamiento preferencial por todos los enrutadores Diffserv que se encuentren hasta el destino del paquete. Si necesita información técnica sobre EF, consulte RFC 2598, *Un PHB de reenvío acelerado*.

Reenvío asegurado (AF) PHB

El *reenvío asegurado* (AF) proporciona cuatro clases diferentes de comportamientos de reenvío que se pueden especificar para el marcador. La siguiente tabla muestra las clases, las tres precedencias de descarte proporcionadas para cada clase y los puntos de código DSCP recomendados asociados con cada precedencia. Cada DSCP está representado por su valor AF, su valor decimal y su valor binario.

TABLA 6-2 Puntos de código de reenvío asegurado

	Clase 1	Clase 2	Clase 3	Clase 4
Precedencia con baja probabilidad de descarte	AF11 = 10 (001010)	AF21 = 18 (010010)	AF31 = 26 (011010)	AF41 = 34 (100010)
Precedencia con probabilidad de descarte media	AF12 = 12 (001100)	AF22 = 20 (010100)	AF32 = 28 (011100)	AF42 = 36 (100100)
Precedencia con alta probabilidad de descarte	AF13 = 14 (001110)	AF23 = 22 (010110)	AF33 = 30 (011110)	AF43 = 38 (100110)

Cualquier sistema con Diffserv puede utilizar el punto de código AF como guía para proporcionar comportamientos de reenvío diferenciados a diferentes clases de tráfico.

Cuando estos paquetes llegan a un enrutador con Diffserv, el enrutador evalúa los puntos de código de los paquetes junto con los puntos de código DSCP de otro tráfico en cola. Después, el enrutador reenvía o descarta paquetes, según el ancho de banda disponible y las prioridades asignadas por los puntos DSCP de los paquetes. Los paquetes marcados con PHB EF tienen ancho de banda garantizado con respecto a paquetes marcados con cualquier comportamiento PHB AF.

El marcado de paquetes debe coordinarse entre cualquier sistema IPQoS de la red y el enrutador Diffserv, para garantizar que los paquetes se reenvían de manera apropiada. Por ejemplo, suponga que los sistemas IPQoS de la red marcan los paquetes con puntos de código AF21 (010010), AF13 (001110), AF43 (100110) y EF (101110). Deberá añadir los puntos de código DSCP AF21, AF13, AF43 y EF al archivo correspondiente del enrutador Diffserv.

Para obtener una explicación técnica sobre la tabla de puntos de código AF, consulte RFC 2597. En las páginas web de los fabricantes de enrutadores Cisco Systems y Juniper Networks puede encontrar información detallada acerca de la configuración de comportamientos AF PHB. Puede usar esta información para definir comportamientos PHB AF para sistemas IPQoS y enrutadores. La documentación del fabricante del enrutador contiene instrucciones para definir puntos de código DS en el equipo.

Suministro de un DSCP al marcador

El DSCP tiene un tamaño de 6 bits. El campo DS tiene un tamaño de 1 byte. Al definir un DSCP, el marcador marca los 6 primeros bits significativos del encabezado del paquete con el punto de código DS. Los 2 bits menos significativos no se utilizan.

Para definir un DSCP, se utiliza el siguiente parámetro en una instrucción de acción de marcador:

```
dscp_map{0-63:DS_codepoint}
```

El parámetro `dscp_map` es una matriz de 64 elementos, que se rellena con el valor (DSCP). `dscp_map` se utiliza para asignar puntos DSCP entrantes a puntos DSCP salientes aplicados por el marcador `dscpmk`.

Debe especificar el valor DSCP de `dscp_map` en notación decimal. Por ejemplo, debe convertir el punto de código EF 101110 en el valor decimal 46, que da como resultado `dscp_map{0-63:46}`. Para puntos de código AF, debe convertir los diferentes puntos de código que se muestran en la [Tabla 6-2](#) en notación decimal para usarlos con `dscp_map`.

Uso del marcador `d\cosmk` con dispositivos VLAN

El módulo de marcador `d\cosmk` marca un comportamiento de reenvío en el encabezado MAC de un datagrama. `d\cosmk` sólo se puede usar en un sistema IPQoS con una interfaz VLAN.

`d\cosmk` agrega cuatro bytes, denominados *etiqueta VLAN*, al encabezado MAC. La etiqueta VLAN incluye un valor de prioridad de usuario de 3 bits, definido en el estándar IEEE 801.D. Los nodos de red con Diffserv que admitan VLAN pueden leer el campo de prioridad de usuario en un datagrama. Los valores de prioridad de usuario 801.D utilizan marcas CoS (Class of Service), que son comunes e interpretables para nodos de red comerciales.

Puede utilizar los valores de prioridad de usuario de la acción de marcador `d\cosmk` definiendo la clase de marcas de servicio de la siguiente tabla.

TABLA 6-3 Valores de prioridad de usuario 801.D

Clase de servicio	Definición
0	Mejor posible

TABLA 6-3 Valores de prioridad de usuario 801.D (Continuación)

Clase de servicio	Definición
1	Segundo plano
2	Momentos libres
3	Excelente
4	Carga controlada
5	Video, latencia de menos de 100ms
6	Video, latencia de menos de 10ms
7	Control de red

Para obtener más información sobre `dlcosmk`, consulte la página del comando `man dlcosmk(7ipp)`.

Configuración IPQoS para sistemas con dispositivos VLAN

En esta sección se presenta un escenario de red simple para mostrar cómo utilizar IPQoS en sistemas con dispositivos VLAN. El escenario incluye dos sistemas IPQoS, `machine1` y `machine2`, conectados mediante un conmutador. El dispositivo VLAN de `machine1` tiene la dirección IP `10.10.8.1`. El dispositivo VLAN de `machine2` tiene la dirección IP `10.10.8.3`.

El siguiente archivo de configuración IPQoS de `machine1` muestra una solución simple para marcar el tráfico que se transmite por medio del conmutador hasta `machine2`.

EJEMPLO 6-2 Archivo de configuración IPQoS para un sistema con un dispositivo VLAN

```

fmt_version 1.0
action {
    module ipgpc
    name ipgpc.classify

    filter {
        name myfilter2
        daddr 10.10.8.3
        class myclass
    }

    class {
        name myclass
        next_action mark4
    }
}

action {
    name mark4
    module dlcosmk
    params {
        cos 4
    }
}

```

EJEMPLO 6-2 Archivo de configuración IPQoS para un sistema con un dispositivo VLAN
(Continuación)

```

        next_action continue
    global_stats true
}

```

En esta configuración, todo el tráfico de `machine1` destinado para el dispositivo VLAN de `machine2` se transfiere al marcador `dlcosmk`. La acción de marcador `mark4` indica a `dlcosmk` que debe añadir una marca VLAN a datagramas de la clase `myclass` con un valor CoS de 4. El valor de prioridad de usuario 4 indica que el conmutador que existe entre los dos equipos debe proporcionar un reenvío de carga controlada a los flujos de tráfico `myclass` desde `machine1`.

Módulo `flowacct`

El módulo IPQoS `flowacct` registra información sobre flujos de tráfico, un proceso que se denomina *control de flujo*. El control de flujo genera datos que pueden utilizarse para la facturación de clientes o para evaluar la cantidad de tráfico de una clase determinada.

El control de flujo es optativo. `flowacct` es, generalmente, el último módulo que los módulos medidos o marcados encuentras antes de enviarse al flujo de red. Para ver una ilustración de la ubicación de `flowacct` en el modelo Diffserv, consulte la [Figura 1-1](#). Para ver información técnica detallada sobre `flowacct`, consulte la página del comando `man flowacct(7ipp)`.

Para activar el control de flujo, debe usar la herramienta de control de Oracle Solaris `exacct` y el comando `acctadm`, además de `flowacct`. Para ver los pasos necesarios para configurar el control de flujo, consulte la sección “[Establecimiento del control de flujo \(mapa de tareas\)](#)” en la [página 83](#).

Parámetros `flowacct`

El módulo `flowacct` recopila información sobre flujos en una *tabla de flujo* compuesta por *registros de flujo*. Cada entrada de la tabla contiene un registro de flujo. No se puede ver una tabla de flujo.

En el archivo de configuración IPQoS, se definen los siguientes parámetros `flowacct` para medir los registros de flujo y escribirlos en la tabla de flujo:

- `timer`: define un intervalo, en milisegundos, en el que los flujos con tiempo de espera superado se eliminan de la tabla de flujo y se escriben en el archivo creado por `acctadm`.
- `timeout`: define un intervalo, en milisegundos, que especifica cuánto tiempo debe estar inactivo un flujo de paquete para que se supere el tiempo de espera del flujo.

Nota – Puede configurar `timer` y `timeout` para que tengan valores diferentes.

- `max_limit`: define el límite máximo para el número de registros de flujo que pueden almacenarse en la tabla de flujo.

Para ver un ejemplo de cómo se utilizan los parámetros `flowacct` en el archivo de configuración IPQoS, consulte “Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 69.

Tabla de flujo

El módulo `flowacct` mantiene una tabla de flujo que registra todos los flujos de paquetes observados por una instancia de `flowacct`.

Un flujo se identifica mediante los siguientes parámetros, que incluyen la 8-tupla `flowacct`:

- Dirección de origen
- Dirección de destino
- Puerto de origen
- Puerto de destino
- DSCP
- ID de usuario
- ID de proyecto
- Número de protocolo

Si todos los parámetros de 8-tupla de un flujo siguen siendo los mismos, la tabla de flujo contiene sólo una entrada. El parámetro `max_limit` determina el número de entradas que puede contener una tabla de flujo.

La tabla de flujo se explora en el intervalo especificado en el archivo de configuración IPQoS del parámetro `timer`. El tiempo predeterminado es 15 segundos. El tiempo de espera de un flujo se supera cuando el sistema IPQoS no envía los paquetes del flujo en el intervalo `timeout` definido en el archivo de configuración IPQoS. El intervalo de tiempo de espera predeterminado es de 60 segundos. Las entradas con tiempo de espera superado se escriben en el archivo de control creado con el comando `acctadm`.

Registros `flowacct`

Un registro `flowacct` contiene los atributos descritos en la siguiente tabla.

TABLA 6-4 Atributos de un registro `flowacct`

Nombre de atributo	Contenido de atributo	Tipo
<code>src-addr-address-type</code>	Dirección de origen del originador. <i>address-type</i> es v4 para IPv4 o v6 para IPv6, especificado en el archivo de configuración IPQoS.	Básico

TABLA 6-4 Atributos de un registro flowacct (Continuación)

Nombre de atributo	Contenido de atributo	Tipo
dest-addr-address-type	Dirección de destino de los paquetes. El <i>address-type</i> es v4 para IPv4 o v6 para IPv6, especificado en el archivo de configuración IPQoS.	Básico
src-port	Puerto de origen del que proviene el flujo.	Básico
dest-port	Número de puerto de destino al que está vinculado el flujo.	Básico
protocol	Número de protocolo del flujo.	Básico
total-packets	Número de paquetes del flujo.	Básico
total-bytes	Número de bytes del flujo.	Básico
action-name	Nombre de la acción flowacct que ha registrado este flujo.	Básico
creation-time	Primera vez que flowacct examina un paquete del flujo.	Sólo ampliado
last-seen	Última vez que se observó un paquete del flujo.	Sólo ampliado
diffserv-field	DSCP en los encabezados del paquete saliente del flujo.	Sólo ampliado
user	ID o nombre de usuario UNIX, obtenido de la aplicación.	Sólo ampliado
projid	ID de proyecto, obtenido de la aplicación.	Sólo ampliado

Utilización de acctadm con el módulo flowacct

El comando `acctadm` se utiliza para crear un archivo en el que se almacenan los registros de flujo generados por `flowacct`. `acctadm` funciona en combinación con la utilidad de contabilidad ampliada. Para obtener información técnica sobre `acctadm`, consulte la página del comando `man acctadm(1M)`.

El módulo `flowacct` observa los flujos y rellena la tabla de flujo con registros de flujo. A continuación, `flowacct` evalúa los parámetros y atributos en el intervalo especificado por `timer`. Cuando un paquete no se detecta durante el tiempo definido en el valor `last_seen` más el valor `timeout`, se supera su tiempo de espera. Todas las entradas con tiempo de espera superado se suprimen de la tabla de flujo. Estas entradas se escriben en el archivo de control cada vez que pasa el intervalo de tiempo especificado en el parámetro `timer`.

Para invocar `acctadm` para utilizarlo con el módulo `flowacct`, utilice la siguiente sintaxis:

```
acctadm -e file-type -f filename flow
```

`acctadm -e` Invoca a `acctadm` con la opción `-e`. "`-e`" indica que a continuación hay una lista de recursos.

file-type Especifica los atributos que se deben recopilar. *file-type* se debe reemplazar por `basic` o `extended`. Para ver una lista de atributos de cada tipo de archivo, consulte la [Tabla 6-4](#).

- *file-name* Crea el archivo *file-name* que contendrá los registros de flujo.
- flow Indica que acctadm debe ejecutarse con IPQoS.

Archivo de configuración IPQoS

En esta sección se incluye información detallada sobre las secciones del archivo de configuración IPQoS. La política IPQoS activada en el inicio se almacena en el archivo `/etc/inet/ipqosinit.conf`. Aunque puede editar este archivo, el mejor método para un sistema IPQoS nuevo es crear un archivo de configuración con un nombre diferente. Las tareas necesarias para aplicar y depurar una configuración IPQoS se encuentran en el [Capítulo 3, “Creación del archivo de configuración IPQoS \(tareas\)”](#).

La sintaxis del archivo de configuración IPQoS se muestra en el [Ejemplo 6-3](#).

El ejemplo utiliza las siguientes convenciones:

- **texto con estilo de ordenador:** información sintáctica proporcionada para explicar las secciones del archivo de configuración. El usuario no necesita escribir el texto con estilo de ordenador en ningún momento.
- **texto en negrita:** texto literal que debe escribir en el archivo de configuración IPQoS. Por ejemplo, siempre debe empezar el archivo de configuración IPQoS con **fmt_version**.
- *texto en cursiva:* texto variable que se reemplaza con información descriptiva sobre la configuración. Por ejemplo, siempre debe reemplazar *action-name* o *module-name* por la información perteneciente a su configuración.

EJEMPLO 6-3 Sintaxis del archivo de configuración IPQoS

```
file_format_version ::= fmt_version version

action_clause ::= action {
    name action-name
    module module-name
    params-clause | ""
    cf-clauses
}
action_name ::= string
module_name ::= ipgpc | dlcosmk | dscpmk | tswtclmt | tokenmt | flowacct

params_clause ::= params {
    parameters
    params-stats | ""
}
parameters ::= prm-name-value parameters | ""
prm_name_value ::= param-name param-value

params_stats ::= global-stats boolean

cf_clauses ::= class-clause cf-clauses |
```

EJEMPLO 6-3 Sintaxis del archivo de configuración IPQoS (Continuación)

```

        filter-clause cf-clauses | ""

class_clause ::= class {
    name class-name
    next_action next-action-name
    class-stats | ""
}
class_name ::= string
next_action_name ::= string
class_stats ::= enable_stats boolean
boolean ::= TRUE | FALSE

filter_clause ::= filter {
    name filter-name
    class class-name
    parameters
}
filter_name ::= string

```

El texto restante describe cada sección principal del archivo de configuración IPQoS.

Instrucción action

Las instrucciones `action` se utilizan para invocar los diferentes módulos IPQoS descritos en [“Arquitectura IPQoS y el modelo Diffserv” en la página 89](#).

Al crear el archivo de configuración IPQoS, siempre se debe empezar por el número de versión. A continuación, se debe agregar la siguiente instrucción `action` para invocar el clasificador:

```

fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
}

```

Después de la instrucción `action` de clasificador, se debe agregar una cláusula `params` o `class`.

Utilice la siguiente sintaxis para el resto de las instrucciones `action`:

```

action {
    name action-name
    module module-name
    params-clause | ""
    cf-clauses
}

name action_name Asigna un nombre a la acción.

```

<code>module</code>	Identifica el módulo IPQoS que se debe invocar, que debe ser uno de los módulos de la Tabla 6-5 .
<code>module_name</code>	
<code>params_clause</code>	Pueden ser parámetros que debe procesar el clasificador, como estadísticas globales, o la siguiente acción que procesar.
<code>cf_clauses</code>	Conjunto de cero o más cláusulas <code>class</code> o <code>filter</code> .

Definiciones de módulo

La definición de módulo indica qué módulo procesará los parámetros de la instrucción `action`. El archivo de configuración IPQoS puede incluir los siguientes módulos.

TABLA 6-5 Módulos IPQoS

Nombre de módulo	Definición
<code>ipgpc</code>	Clasificador IP
<code>dscpmk</code>	Marcador que se debe utilizar para crear puntos de código DSCP en paquetes IP
<code>dlcosmk</code>	Marcador que se debe utilizar con dispositivos VLAN
<code>tokenmt</code>	Medidor de conjunto de tokens
<code>tswtclmt</code>	Medidor de fase temporal de desplazamiento
<code>flowacct</code>	Módulo de control de flujo

Cláusula `class`

Se define una cláusula `class` para cada clase de tráfico.

Utilice esta sintaxis para definir las clases restantes de la configuración IPQoS:

```
class {
    name class-name
    next_action next-action-name
}
```

Para activar la recopilación de estadísticas de una clase determinada, primero, debe activar las estadísticas globales en la instrucción `action ipgpc.classify`. Si necesita más información, consulte [“Instrucción `action`” en la página 103](#).

Utilice la instrucción `enable_stats TRUE` cuando quiera activar la recopilación de estadísticas de una clase. Si no necesita recopilar estadísticas de una clase, puede especificar `enable_stats FALSE`. También puede eliminar la instrucción `enable_stats`.

El tráfico de una red con IPQoS que no esté definido específicamente pertenece a la *clase predeterminada*.

Cláusula `filter`

Los *filtros* están compuestos por selectores que agrupan los flujos de tráfico en clases. Estos selectores definen específicamente los criterios que deben aplicarse al tráfico de la clase creada en la cláusula `class`. Si un paquete coincide con todos los selectores del filtro de prioridad más alta, se considera un miembro de la clase del filtro. Para ver una lista completa de los selectores que pueden usarse con el clasificador `ipgpc`, consulte la [Tabla 6-1](#).

Los filtros se definen en el archivo de configuración IPQoS utilizando una *cláusula filter*, que tiene la siguiente sintaxis:

```
filter {
    name filter-name
    class class-name
    parameters (selectors)
}
```

Cláusula `params`

La cláusula `params` contiene instrucciones de procesamiento para el módulo definido en la instrucción `action`. Utilice la siguiente sintaxis para la cláusula `params`:

```
params {
    parameters
    params-stats | ""
}
```

En la cláusula `params` se utilizan parámetros aplicables al módulo.

El valor `params-stats` de la cláusula `params` es `global_stats TRUE` o `global_stats FALSE`. La instrucción `global_stats TRUE` activa estadísticas de estilo UNIX para la instrucción `action` en la que se invocan las estadísticas globales. Puede ver las estadísticas con el comando `kstat`. Debe activar las estadísticas de la instrucción `action` antes de poder activar las estadísticas por clase.

Utilidad de configuración `ipqosconf`

Se utiliza la utilidad `ipqosconf` para leer el archivo de configuración IPQoS y para configurar los módulos IPQoS del núcleo UNIX. `ipqosconf` realiza las siguientes acciones:

- Aplica el archivo de configuración a los módulos de núcleo IPQoS (`ipqosconf -a nombre de archivo`)
- Indica el archivo de configuración IPQoS actual del núcleo (`ipqosconf -l`)
- Asegura que la configuración IPQoS actual se lee y aplica cada vez que se reinicia el equipo (`ipqosconf -c`)
- Vacía los módulos de núcleo IPQoS actuales (`ipqosconf -f`)

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

Índice

A

- acuerdo de nivel de servicio (SLA), 14
 - clases de servicio, 18
 - facturación a clientes, según el control de flujo, 84
 - ofrecimiento de diferentes clases de servicio, 16
- administración del tráfico
 - reenvío del tráfico, 22, 24
 - regulación del ancho de banda, 15
- archivos de configuración IPQoS de ejemplo
 - configuración de dispositivo VLAN, 98
 - segmento de reconocimiento de colores, 93
 - servidor de aplicaciones, 63
 - servidor web "best-effort", 51
 - servidor web de nivel alto, 50

C

- calidad de servicio (QoS)
 - política de QoS, 14–15
 - tareas, 12
- clases, 18
 - definición, en el archivo de configuración IPQoS, 61, 65
 - selectores, lista de, 90
 - sintaxis de la cláusula `class`, 104
- clases de servicio, *Ver* clases
- clasificador `ipgpc`, *Ver* módulo clasificador
- cláusula `class`, en el archivo de configuración IPQoS, 53
- cláusula `class`, en el archivo de configuración IPQoS, 104

- cláusula `filter`, del archivo de configuración IPQoS, 55
- cláusula `filter`, en el archivo de configuración IPQoS, 105
- cláusula `params`
 - definición de estadísticas globales, 53, 105
 - para `flowacct action`, 59
 - para un marcador `action`, 57
 - para una instrucción `action` de medición, 70
 - sintaxis, 105
- comando `acctadm`, para control de flujo, 20, 101
- comando `acctadm`, para el control de flujo, 85
- comando `ipqosconf`
 - aplicación de una configuración, 76, 77
 - opciones de comando, 106
 - visualización de la configuración actual, 77
- comando `kstat`, uso con IPQoS, 86
- comportamiento por salto (PHB), 22
 - definición, en el archivo de configuración IPQoS, 71
 - reenvío AF, 23
 - reenvío EF, 23
 - uso, con marcador `dscpmk`, 95–97
- control de flujo, 84–86, 99
 - tabla de registro de flujo, 100
- control del flujo, mediante los módulos de medición, 19
- cumplimiento del tráfico
 - definir, 70
 - parámetros de tasa, 92
 - planificación
 - resultados en la política QoS, 39
 - tasas en la política QoS, 39

cumplimiento del tráfico (*Continuación*)
resultados, 19, 92

D

dispositivos de LAN virtual (VLAN) en una red
IPQoS, 97–99

E

ejemplo de red de IPQoS, 49
enrutador con Diffserv
 evaluación de puntos de código DS, 96
 planificación, 33
equilibrio de la carga, en una red con IPQoS, 30
estadísticas de IPQoS
 activación de estadísticas globales, 53
 activación de las estadísticas globales, 104
 activar estadísticas basadas en clases, 104
 generación, con el comando `kstat`, 86

F

filtros, 18
 creación, en el archivo de configuración IPQoS, 61,
 66
 planificación, en la política QoS, 36
 selectores, lista de, 90
 sintaxis de la cláusula `filter`, 105

G

gestión de tráfico
 cómo priorizar los flujos de tráfico, 16–17
 control del flujo, 18–19
 planificación de topologías de red, 29
 reenvío de tráfico, 23

H

hardware para redes con IPQoS, 28–29

I

instrucción `action`, 103
IPQoS, 11
 archivo de configuración, 49, 102
 cláusula `class`, 53
 cláusula `filter`, 55
 instrucción `action` de marcador, 56
 instrucción `action` inicial, 103
 instrucción `action` inicial, 52
 lista de módulos IPQoS, 104
 sintaxis, 102
 sintaxis de la instrucción `action`, 103
características, 12
compatibilidad con dispositivos VLAN, 97–99
ejemplo de configuración, 44–46
ejemplo de red, 49
enrutadores en una red IPQoS, 72
funciones de administración del tráfico, 17
funciones de gestión de tráfico, 15
generación de estadísticas, 86
implementación del modelo Diffserv, 17–21
mensajes de error, 79
páginas del comando `man`, 13–14
planificación de la configuración, 27
planificar la política QoS, 31
registro de mensajes, 78
RFC relacionadas, 13
topologías de red admitidas, 28, 29, 30
`ipqosconf`, 49

M

mapa de tareas
 IPQoS
 planificación de la configuración, 27
mapas de tareas
 IPQoS
 configuración de control de flujo, 83
 creación de archivo de configuración, 47

- mapas de tareas, IPQoS (*Continuación*)
 planificación de política QoS, 32
- marca de clase de servicio (CoS), 19
- marcador `dLcosmk`, 19
 etiquetas VLAN, 97
 planificar el reenvío de datagramas, 41
 valores de prioridad de usuario, tabla de, 97
- marcador `dscpmk`, 19
 comportamientos PHB para el reenvío de paquetes, 95–97
 invocación, en una instrucción `action` de marcador, 56, 62, 68, 71
 planificación del reenvío de paquetes, 41
- medidor `tokenmt`, 19
 configuración de reconocimiento de colores, 19, 93
 medición de tasas, 92–94
 medidor de doble tasa, 93
 medidor de tasa única, 93
 parámetros de tasa, 92
- medidor `tswtcLmt`, 19, 94
 medición de tasas, 94
- mensajes de error de IPQoS, 79
- modelo Diffserv
 ejemplo de flujo, 20
 implementación de IPQoS, 17–21, 20
 implementación IPQoS, 20
 módulo clasificador, 17–18
 módulos de marcador, 19
 módulos de medidor, 18–19
- módulo clasificador, 17–18
 funciones de clasificador, 90
 instrucción `action`, 52
- módulo `flowacct`, 20, 99
 atributos de registros de flujo, 100
 comando `acctadm`, para crear un archivo de control de flujo, 101
 instrucción `action` para `flowacct`, 59
 parámetros, 99–100
 registros de flujo, 84
 tabla de registro de flujo, 100
- módulos de marcador, 19
Ver también marcador `dLcosmk`
Ver también marcador `dscpmk`
 compatibilidad con dispositivos VLAN, 97–99
- módulos de marcador (*Continuación*)
 especificación de un punto de código DS, 97
 PHB, para el reenvío de paquetes IP, 22
- módulos de medición
Ver también medidor `tokenmt`
Ver también medidor `tswtcLmt`
 introducción, 18–19
 invocar, en el archivo de configuración IPQoS, 70
 resultados de medición, 19, 92
- ## P
- peticiones de comentarios (RFC), IPQoS, 13
- política QoS, 15
 creación de filtros, 36
 implementación, en el archivo de configuración IPQoS, 47
 mapa de tareas de planificación, 32
 plantilla para organizar la política, 31
- punto de código DS (DSCP), 19, 22
 configuración, en un enrutador `diffserv`, 73
 configuración de reconocimiento de color, 94
 configurar, en un enrutador `diffserv`, 95
 definición, en el archivo de configuración IPQoS, 57
 parámetro `dscp_map`, 97
 PHB y DSCP, 22
 planificación, en la política QoS, 41
 punto de código de reenvío AF, 23, 96
 punto de código de reenvío EF, 23, 96
- ## R
- reconocimiento de colores, 19, 93
- reenvío acelerado (EF), 23, 96
 definición, en el archivo de configuración IPQoS, 58
- reenvío asegurado (AF), 23, 96
 para una instrucción `action` de marcador, 57
 tabla de puntos de código AF, 96
- reenvío de tráfico
 efecto de comportamientos PHB en el reenvío de paquetes, 95–97
 flujo del tráfico mediante redes Diffserv, 23
 planificación, en la política QoS, 35

- reenvío del tráfico
 - reenvío de datagramas, 97–99
 - reenvío de paquetes IP, con DSCP, 22
- registro de archivo `syslog.conf` para IPQoS, 78
- regulación de ancho de banda, planificación, en la política QoS, 35
- regulación del ancho de banda, 15–16

S

- selectores, 18
 - 5-tupla de IPQoS, 17
 - planificación, en la política QoS, 36
 - selectores, lista de, 90
- servicios diferenciados, 11–12
 - modelo de servicios diferenciados, 17–21
 - ofrecimiento de diferentes clases de servicio, 16
 - topologías de red, 28
- servidor de aplicaciones, configurar para IPQoS, 63
- servidores web
 - configuración para IPQoS, 51, 60, 62
 - configurar para IPQoS, 50

T

- topologías de red para IPQoS, 28–29
 - ejemplo de configuración, 44
 - LAN con conjuntos de servidores con IPQoS, 29
 - LAN con cortafuegos con IPQoS, 30
 - Red LAN con hosts con IPQoS, 29

V

- valor de prioridad de usuario, 19