

# Preguntas frecuentes sobre Calidad de servicio (QoS)

## Contenido

[Introducción](#)

[General](#)

[Clasificación y marcado](#)

[Administración de congestión y colas](#)

[Detección temprana aleatoria ponderada \(WRED\) de prevención de congestión](#)

[Regulación del Tráfico y Modelado](#)

[Frame Relay de Calidad de servicio \(QoS\)](#)

[Calidad del servicio \(QoS\) en el Asynchronous Transfer Mode \(ATM\)](#)

[Voz y calidad de servicio \(QoS\)](#)

[Información Relacionada](#)

## Introducción

Este documento responde a las preguntas más frecuentes (FAQ) relacionadas con la Calidad de Servicio (QoS).

## General

P. ¿Qué es la calidad de servicio (QoS)?

R. QoS se refiere a la capacidad de una red de proporcionar un mejor servicio al tráfico de red seleccionado por medio de diversas tecnologías, entre ellas: Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet y redes 802.1, SONET y redes enrutadas por IP.

Calidad de servicio (QoS) es un conjunto de tecnologías que permite que las aplicaciones soliciten y reciban niveles de servicio predecibles en términos de la capacidad de rendimiento de datos (ancho de banda), variaciones de latencia (fluctuación) y retraso. En particular, las funciones de QoS ofrecen un servicio de red mejor y más previsible a través de los siguientes métodos:

- Admite un ancho de banda dedicado.
- Mejora de las características de pérdida.
- Cómo evitar y administrar la congestión de la red.
- Define el tráfico de red.

- Configuración de prioridades de tráfico en la red.

El Grupo de trabajo en ingeniería de Internet (IETF) define las dos arquitecturas siguientes para QoS:

- Servicios integrados (IntServ)
- Servicios diferenciados (DiffServ)

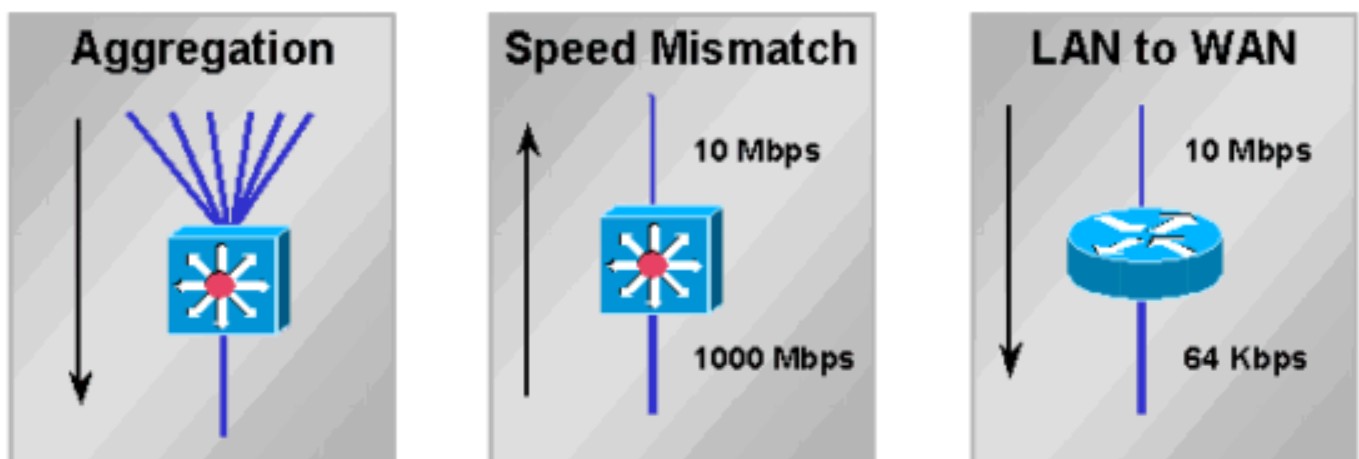
IntServ utiliza el protocolo de reserva del recurso (RSVP) para señalar expresamente las necesidades de QoS del tráfico de una aplicación en todos los dispositivos de un trayecto extremo a extremo a través de la red. Si cada dispositivo de la red junto con el trayecto puede reservar el ancho de banda necesario, la aplicación que se origina puede comenzar la transmisión. La petición de comentarios (RFC) 2205 define el RSVP, y la RFC 1633 define el IntServ.

DiffServ se centra en el agregado y el aprovisionamiento de QoS. En lugar de señalar los requisitos de QoS de una aplicación, DiffServ utiliza un Punto de código de servicios diferencias (DSCP) en el encabezado IP para indicar los niveles de QoS requeridos. La versión 12.1(5)T de software del IOS® de Cisco introdujo el cumplimiento DiffServ en los routers de Cisco. Si desea más información, consulte los siguientes documentos:

- [Servicio integrado en la versión 12.1 del IOS de Cisco](#)
- [Implementación de DiffServ para calidad de servicio de extremo a extremo](#)
- [Implementación de políticas de calidad del servicio \(QoS\) con DSCP](#)

P. ¿Qué son la congestión, el retraso y la fluctuación?

R. Una interfaz experimenta congestión cuando se presenta con más tráfico del que puede manejar. Los puntos de congestión de red son candidatos fuertes para los mecanismos de Calidad de Servicio (QoS). A continuación, un ejemplo de los puntos de congestión más comunes:



La congestión de red resulta en retardo. Una red y sus dispositivos introducen varios tipos de

retrasos, como se explica en [Conocimientos sobre el retraso en redes de paquetes de voz](#). La variación en el retardo se conoce como fluctuación, según se explica en [Comprensión de la fluctuación en redes de voz en paquetes \(plataformas de Cisco IOS\)](#). Es necesario controlar y minimizar tanto la demora como las fluctuaciones para admitir el tráfico en tiempo real e interactivo.

P. ¿Qué es el MQC?

R. MQC hace referencia a las políticas de calidad de servicio modular (QoS), Interfaz de línea de comando (CLI). Está diseñado para simplificar la configuración de QoS en los routers y switches de Cisco, mediante la definición de una sintaxis de comandos y un conjunto final de comportamientos de QoS en común entre las plataformas. Este modelo reemplaza al modelo anterior por el cual se definía una sintaxis única para cada función de calidad de servicio (QoS) y para cada plataforma.

El MQC comprende los tres pasos siguientes:

1. Definir una clase de tráfico ejecutando el comando class-map.
2. Cree una política de tráfico asociando la clase de tráfico con una o más funciones de calidad de servicio (QoS) al ejecutar el comando policy-map.
3. Adjuntar la directiva del tráfico a la interfaz, subinterfaz o circuito virtual (VC) ejecutando el comando service-policy.

Nota: Las funciones de condicionamiento del tráfico de DiffServ, como marcado y modelado, se implementan mediante la sintaxis MQC.

Para obtener más información, consulte [Interfaz de línea de comando de calidad del servicio modular](#).

P. ¿Qué significa la política de servicio sólo se soporta en las interfaces VIP con el mensaje habilitado para DCEF?

R. En los Procesadores de interfaz versátil (VIP) en una serie Cisco 7500, solo se admiten funciones de calidad de servicio (QoS) distribuidas a partir de Cisco IOS 12.1(5)T, 12.1(5)E y 12.0(14)S. La acción de habilitar distributed Cisco Express Forwarding (dCEF) habilita automáticamente la QoS distribuida.

Interfaces no VIP, denominadas procesadores de interfaz heredada (IP), soportan las características QoS centrales del modo en que fueron habilitadas en el procesador de conmutación de ruta (RSP). Si desea más información, consulte los siguientes documentos:

- [Mecanismo de cola de espera equitativo y ponderado basado en clases distribuido y detección temprana aleatoria y ponderada distribuida](#)
- [Mecanismo de cola de baja latencia distribuido](#)

- [Modelado del tráfico distribuido](#)
- [Interfaz versátil de procesador distribuida FRF.11 y FRF.12 para el IOS de Cisco versión 12.1 T](#)

Q. ¿Cuántas clases admite una política de Calidad de servicio (QoS)?

R. En las versiones del IOS de Cisco anteriores a la 12.2 se podía definir un máximo de sólo 256 clases, y se podían definir hasta 256 clases dentro de cada política si las mismas clases se reutilizan para diferentes políticas. Si usted tiene dos políticas, el número total de clases de ambas políticas no debe superar 256. Si una política incluye el Mecanismo de cola de espera equitativo y ponderado basado en clases (CBWFQ) (lo que significa que contiene una declaración de ancho de banda [o prioridad] dentro de cualquiera de las clases), el número total de clases compatibles es 64.

En Cisco IOS versiones 12.2(12), 12.2(12)T y 12.2(12)S, esta limitación de 256 asignaciones de clase globales se ha cambiado, y ahora es posible configurar un máximo de 1024 asignaciones de clase globales y utilizar 256 asignaciones de clase dentro de la misma asignación de política.

P. ¿Cómo se procesan las actualizaciones de routing y las señales de mantenimiento del protocolo punto a punto (PPP) y del control de enlace de datos de alto nivel (HDLC) cuando se aplica una política de servicio?

R. Los routers Cisco IOS utilizan los siguientes dos mecanismos para dar prioridad a los paquetes de control:

- Precedencia IP
- pak\_priority

Ambos mecanismos están diseñados para garantizar que ni el router ni el sistema de colocación en cola interrumpen los paquetes de control clave o los interrumpen en último lugar cuando una interfaz de salida está congestionada. Para obtener más información, consulte la sección Introducción a de cómo se envían a cola las actualizaciones de ruteo y los paquetes de control en una interfaz con una política de servicio de QoS.

P. ¿Se admite la calidad de servicio (QoS) en las interfaces configuradas con Integrated Routing and Bridging (IRB)?

R. No. No puede configurar las funciones de QoS cuando la interfaz está configurada para IRB.

## Clasificación y marcado

P. ¿Qué es la preclasificación de calidad de servicio (QoS)?

R. La preclasificación de QoS le permite comparar y clasificar el contenido original del encabezado IP de los paquetes sometidos a encapsulación de túnel y/o encriptación. Esta función

no describe el proceso de copiar el valor original del byte del tipo de servicio (ToS) desde el encabezado del paquete original al encabezado de túnel. Si desea más información, consulte los siguientes documentos:

- [Configuración de QoS para redes virtuales privadas](#)
- [Calidad de servicio para Redes virtuales privadas, módulo de funciones 12.2\(2\)T](#)

P. ¿Qué campos de encabezado de paquete se pueden remarcar? ¿Qué valores están disponibles?

R. La función de marcado basado en clase permite establecer o marcar el encabezado de switching de etiquetas multiprotocolo (MPLS) de capa 2, capa 3 o de sus paquetes. Si desea más información, consulte los siguientes documentos:

- [Configuración de marcado de paquetes basado en clases](#)
- [¿Cuándo establece un router el bit CLP en una célula ATM?](#)
- ['Configuración del paquete de marcación en PVC de Frame Relay'](#)

P. ¿Puedo priorizar el tráfico según la URL?

R. Sí. El reconocimiento de la aplicación con base en la red (NBAR) le permite clasificar paquetes mediante la concordancia de campos en la capa de la aplicación. Antes de la introducción de NBAR, la clasificación más granular eran los números de puertos de protocolo de control de transmisión (TCP) y protocolo de datagramas de usuario (UDP) de capa 4. Si desea más información, consulte los siguientes documentos:

- [Preguntas y respuestas sobre el reconocimiento de aplicaciones basado en la red](#)
- [Red de aplicación NBAR](#)
- [Uso del reconocimiento de la aplicación basada en la red y Listas de control de acceso para el bloqueo del gusano "Código rojo](#)
- [Cómo proteger su red del virus Nimda](#)

P. ¿Qué plataformas y versiones de software de Cisco IOS son compatibles con el reconocimiento de aplicaciones basadas en red (NBAR)?

A. El soporte para NBAR se introdujo en las siguientes versiones del software del IOS de Cisco:

Platform	Versión mínima del Software del IOS de Cisco
7200	12.1(5)T
7100	12.1(5)T
3660	12.1(5)T

3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(2)T

Nota: Debe activar Cisco Express Forwarding (CEF) para utilizar NBAR.

NBAR distribuido (DNBAR) está disponible en las siguientes plataformas:

Platform	Versión mínima del Software del IOS de Cisco
7500	12.2(4)T, 12.1(6)E
FlexWAN	12.1(6)E

Nota: NBAR no es compatible con las interfaces VLAN de la tarjeta de función de switch multicapa (MSFC) de Catalyst 6000, la serie Cisco 12000 o el módulo de switch de ruta (RSM) para la serie Catalyst 5000. Si no ve incluida una plataforma en particular, póngase en contacto con su representante técnico de Cisco.

## Administración de congestión y colas

P. ¿Cuál es el propósito de la colocación en cola?

A. La formación de colas está diseñada para acomodar la congestión temporaria en una interfaz de dispositivo de red ya que almacena los paquetes en exceso en las memorias intermedias hasta que haya ancho de banda disponible. Los routers de Cisco IOS admiten varios métodos de colocación en cola para satisfacer los diferentes requisitos de ancho de banda, fluctuación y retardo de las distintas aplicaciones.

El mecanismo predeterminado en la mayoría de las interfaces es Primero en entrar primero en salir (FIFO). Algunos tipos de tráfico tienen requisitos de retardo/fluctuación más exigentes. De esta manera, uno de los siguientes mecanismos alternativos para formar la cola se deben configurar o habilitar por defecto.

- Weighted Fair Queueing (WFQ)
- Class-Based Weighted Fair Queueing (CBWFQ)
- Almacenamiento en cola con latencia baja (LLQ), que en realidad es CBWFQ con cola de prioridades (PQ) (conocido como PQCBWFQ)
- Envío a cola prioritario (PQ)
- Almacenamiento en cola personalizado (CQ)

La colocación en cola se produce generalmente, sólo en las interfaces salientes. Un router coloca en cola los paquetes que salen de una interfaz. Puede supervisar el tráfico entrante, pero

normalmente no puede poner en cola el tráfico entrante (una excepción es el almacenamiento en búfer del lado de recepción en un router de la serie Cisco 7500 que utiliza Cisco Express Forwarding distribuido (dCEF) para reenviar paquetes desde el ingreso a la interfaz de egreso; para obtener más información, consulte [Introducción a la ejecución de CPU VIP al 99% y almacenamiento en búfer del lado de recepción](#). En las plataformas distribuidas de mayor capacidad como las de las series 7500 y 12000 de Cisco, la interfaz de entrada puede utilizar su propia memoria intermedia de paquetes para almacenar el exceso de tráfico conmutado a un interfaz de salida congestionada siguiendo la decisión de conmutación de la interfaz de entrada. En condiciones poco frecuentes, por lo general cuando la interfaz de entrada alimenta a una interfaz de salida más lenta, la interfaz de entrada puede experimentar un incremento en los errores ignorados cuando se queda sin memoria de paquetes. Una congestión excesiva puede conducir a caídas de cola de salida. Las caídas de cola de entrada en general tienen una causa de origen diferente. Si desea obtener más información para la resolución de problemas de pérdidas, consulte el siguiente documento:

- [Resolución de problemas en los paquetes descartados en las colas de entrada y salida](#)

Si desea más información, consulte los siguientes documentos:

- [Solución de problemas de errores "ignorados" en un adaptador de puerto ATM](#)
- [Resolución de problemas errores ignorados y "no memory drops" en el router de Internet de la serie 12000 de Cisco](#)

P. ¿Cómo funcionan el almacenamiento en cola equitativo ponderado (WFQ) y el almacenamiento en cola equitativo ponderado basado en clase (CBWFQ)?

R. Las colas con equilibrio buscan asignar, equitativamente, un ancho de banda de interfaz entre las conversaciones activas o los flujos IP. Clasifica a los paquetes en subcolas, identificadas por un número de identificación de conversación, por medio de un algoritmo de troceo basado en diversos campos del encabezado IP y en la longitud del paquete. El peso se calcula de la siguiente forma:

- $W=K/(precedencia +1)$

K= 4096 con versión 12.0(4)T o anterior del IOS de Cisco y 32384 con versión 12.0(5)T o posterior.

A menor peso, mayor prioridad y porción de ancho de banda. Además del peso, también se tiene en cuenta la longitud del paquete.

CBWFQ le permite definir una clase de tráfico y asignarle una garantía de ancho de banda mínimo. El algoritmo detrás de este mecanismo es WFQ, lo que explica el nombre. Para configurar CBWFQ, define clases específicas en enunciados map-class. Luego, puede asignar una política a cada clase en una asignación de políticas. Este mapa de política luego será adjuntado en la salida de una interfaz. Si desea más información, consulte los siguientes documentos:

- [Comprensión de Class Based Weighted Fair Queuing en ATM](#)
- [Introducción a Weighted Fair Queuing en ATM](#)

P. Si una clase de Class Based Weighted Fair Queueing (CBWFQ) no está utilizando su ancho de banda, ¿pueden otras clases utilizar el ancho de banda?

R. Sí. Si bien las garantías de ancho de banda proporcionadas por la ejecución de los comandos `priority` y `bandwidth` se han descrito con palabras tales como "reservado" y "ancho de banda a destinarse", ninguno de los dos comandos implementa una verdadera reserva. Esto significa que, si una clase de tráfico no utiliza su ancho de banda configurado, el ancho de banda sin utilizar se comparte entre las otras clases.

El sistema de envío a cola impone una excepción importante de clase prioritaria a esta regla. Tal como se observa arriba, la carga ofrecida de una clase de prioridad es medida por el regulador de tráfico. Durante condiciones de congestión, una clase de prioridad no puede utilizar ningún ancho de banda en exceso. Para obtener más información, consulte Comparación de los comandos `bandwidth` y `priority` de una política de servicio de QoS.

P. ¿Se soporta Class Based Weighted Fair Queueing (CBWFQ) en las subinterfaces?

R. Las interfaces lógicas del IOS de Cisco no admiten en sí un estado de congestión y no admiten la aplicación directa de una política de servicios que emplea un método de envío a cola. En cambio, primero se debe aplicar el modelado a la subinterfaz utilizando el modelado de tráfico genérico (GTS) o el modelado basado en la clase. Para mayor información consultar Características de aplicación QoS para subinterfaces Ethernet.

P. ¿Cuál es la diferencia entre las sentencias `priority` y `bandwidth` en un `policy-map`?

R. Los comandos `priority` y `bandwidth` difieren en la funcionalidad y en qué aplicaciones suelen admitir. En la siguiente tabla, se resumen esas diferencias:

Función	Comando <code>bandwidth</code>	Comando <code>priority</code>
Garantía de ancho de banda mínimo	Yes	Yes
Garantía de ancho de banda máxima	No	Yes
Vigilante incorporado	No	Yes
Proporciona latencia baja	No	Yes

Para obtener más información, consulte Comparación de los comandos `bandwidth` y `priority` de una política de servicio de QoS.



P. ¿Cómo se calcula el límite de cola en FlexWAN y los procesadores de interfaz versátil (VIP)?

R. Suponiendo que haya suficiente SRAM en el VIP o FlexWAN, el límite de cola se calcula basándose en un retraso máximo de 500ms con un paquete de tamaño promedio de 250 bytes. El siguiente es un ejemplo de una clase con un Mbps de ancho de banda:

$$\text{Límite de cola} = 1000000 / (250 \times 8 \times 2) = 250$$

Los límites de cola más pequeños son asignados a medida que la cantidad de memoria de paquete disponible disminuye y con un número mayor de Circuitos virtuales (VCS).

En el siguiente ejemplo, el PA-A3 se instala en una tarjeta FlexWAN para la serie Cisco 7600 y admite varias subinterfases con circuitos permanentes (PVC) de 2 MB. La política de servicio se aplica a cada VC.

```
<#root>
```

```
class-map match-any XETRA-CLASS
  match access-group 104
class-map match-any SNA-CLASS
  match access-group 101
  match access-group 102
  match access-group 103
policy-map
```

```
POLICY-2048Kbps
```

```
  class XETRA-CLASS
    bandwidth 320
  class SNA-CLASS
    bandwidth 512
```

```
interface ATM6/0/0
  no ip address
  no atm sonet ilmi-keepalive
  no ATM ilmi-keepalive
!
interface ATM6/0/0.11 point-to-point
  mtu 1578
  bandwidth 2048
  ip address 22.161.104.101 255.255.255.252
  pvc ABCD
    class-vc 2048Kbps-PVC
    service-policy out
```

```
POLICY-2048Kbps
```

La interfaz de Asynchronous Transfer Mode (ATM) adquiere un límite de almacenamiento en cola para toda la interfaz. El límite es una función del total de búferes disponibles, el número de interfaces físico en la FlexWAN, y el retardo de cola máximo permitido en la interfaz. Cada PVC obtiene una porción del límite de interfaz en base a la Velocidad sostenida de celda (SCR) o la

Velocidad mínima de celda (MCR) del PVC y cada clase obtiene una porción del límite del PVC basado en su asignación de ancho de banda.

El siguiente ejemplo de resultado del comando show policy-map interface se deriva de una FlexWAN con 3687 búfers globales. Ejecute el comando show buffer para ver este valor. Cada dos Mbps se le asignan 50 paquetes al PVC basándose en el ancho de banda PVC de dos Mbps ( $2047/149760 \times 3687 = 50$ ). Cada clase luego recibe una parte de los 50, como se muestra en el siguiente resultado:

```
<#root>
```

```
service-policy output: POLICY-2048Kbps
  class-map: XETRA-CLASS (match-any)
    687569 packets, 835743045 bytes
    5 minute offered rate 48000 bps, drop rate 6000 BPS
    match: access-group 104
      687569 packets, 835743045 bytes
      5 minute rate 48000 BPS
    queue size 0,

queue limit 7

    packets output 687668, packet drops 22
    tail/random drops 22, no buffer drops 0, other drops 0
    bandwidth: kbps 320, weight 15

  class-map: SNA-CLASS (match-any)
    2719163 packets, 469699994 bytes
    5 minute offered rate 14000 BPS, drop rate 0 BPS
    match: access-group 101
      1572388 packets, 229528571 bytes
      5 minute rate 14000 BPS
    match: access-group 102
      1146056 packets, 239926212 bytes
      5 minute rate 0 BPS
    match: access-group 103
      718 packets, 245211 bytes
      5 minute rate 0 BPS
    queue size 0,

queue limit 12

    packets output 2719227, packet drops 0
    tail/random drops 0, no buffer drops 0, other drops 0
    bandwidth: kbps 512, weight 25
    queue-limit 100

  class-map: class-default (match-any)
    6526152 packets, 1302263701 bytes
    5 minute offered rate 44000 BPS, drop rate 0 BPS
    match: any
      6526152 packets, 1302263701 bytes
      5 minute rate 44000 BPS
    queue size 0,

queue limit 29
```

```
packets output 6526840, packet drops 259
tail/random drops 259, no buffer drops 0, other drops 0
```

Si sus flujos de tráfico usan tamaños de paquetes grandes, el resultado del comando `show policy-map interface` puede mostrar un valor en aumento para las caídas que no sean de búfer, dado que puede quedarse sin búfers antes de alcanzar el límite de cola. En este caso, intente reducir manualmente el límite de cola en las clases no prioritarias. Para obtener más información, consulte [Descripción del límite de cola de transmisión con CoS ATM IP](#).

P. ¿Cómo verifica el valor de límite de cola?

R. En las plataformas no distribuidas, el límite de cola es de 64 paquetes de forma predeterminada. El ejemplo de resultado que se muestra a continuación se tomó de un router de la serie 3600 de Cisco:

```
<#root>
november#
show policy-map interface s0

Serial0

Service-policy output: policy1

Class-map: class1 (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 BPS, drop rate 0 BPS
Match: ip precedence 5
Weighted Fair Queueing
  Output Queue: Conversation 265
  Bandwidth 30 (kbps) Max Threshold 64 (packets)

!--- Max Threshold is the queue-limit.

(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0

Class-map: class2 (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 BPS, drop rate 0 BPS
Match: ip precedence 2
Match: ip precedence 3
Weighted Fair Queueing
  Output Queue: Conversation 266
  Bandwidth 24 (kbps) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0

Class-map: class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 BPS, drop rate 0 BPS
Match: any
```

P. ¿Puedo habilitar la colocación en cola justa dentro de una clase?

R. La serie Cisco 7500 con calidad de servicio distribuida (QoS) admite colas justas por clase. Otras plataformas, incluidas las series 7200 y 2600/3600 de Cisco, admiten Weighted Fair Queueing (WFQ) en la clase class-default; todas las clases de ancho de banda utilizan First In First Out (FIFO).

P. ¿Qué comandos puedo utilizar para monitorear la colocación en cola?

A. Utilice los siguientes comandos para monitorear la colocación en cola:

- `show queue {interface}{interface number}` - En las plataformas de Cisco IOS que no sean de la serie 7500 de Cisco, este comando muestra las colas o conversaciones activas. Si la interfaz o el Circuito virtual (VC) no están congestionados no se enumerará ninguna cola. En la serie 7500 de Cisco, el comando `show queue` no está admitido.
- [show queueing interface interface-number \[vc \[\[vpi/\] vci\]](#) - [Esto muestra las estadísticas de colocación en cola de una interfaz o un VC.](#) Incluso cuando no haya congestión, podrá ver algunos resultados aquí. La razón de esto es que los paquetes conmutados de proceso siempre se cuentan independientemente de la congestión que pueda estar presente. Cisco Express Forwarding (CEF) y los paquetes de conmutado rápido no se cuentan a menos que haya una congestión. Los mecanismos de cola heredada como Cola prioritaria (PQ), Cola personalizada (CQ) y Cola equitativa ponderada (WFQ) no proporcionan estadísticas de clasificación. Solo las funciones basadas en la interfaz de línea de comando de calidad de servicio modular (MQC) en las imágenes posteriores a 12.0(5)T ofrecen estas estadísticas.
- `show policy interface {interfaz}{número de interfaz}` - El contador de paquetes cuenta la cantidad de paquetes que concuerdan con los criterios de la clase. Este contador se incrementa sin importar si la interfaz está congestionada o no. El contador de paquetes coincidentes indica el número de paquetes que cumplen los criterios de la clase cuando la interfaz se congestiona. Para obtener más información acerca de contadores de paquetes, consulte el siguiente documento:  
[Introducción a los contadores de paquetes en el resultado de show policy-map interface.](#)
- MIB de configuración y estadística de QoS basada en clases de Cisco - Proporciona capacidades de supervisión de Protocolo simple de administración de redes (SNMP).

P. RSVP se puede utilizar junto con Class Based Weighted Fair Queueing (CBWFQ). Cuando el Protocolo de reserva de recurso (RSVP) y CBWFQ se encuentran configurados para una interfaz, ¿RSVP y CBWFQ actúan de manera independiente, exhibiendo el mismo comportamiento que si se ejecutaran solos? RSVP se comporta como si CBWFQ no estuviera configurado con respecto a la asignación, evaluación y disponibilidad del ancho de banda.

R. Cuando se utiliza RSVP y CB-WFQ en Cisco IOS Software Release 12.1(5)T y posteriores, el

router puede funcionar de manera que los flujos RSVP y las clases CBWFQ compartan el ancho de banda disponible en una interfaz o PVC, sin sobresuscripción.

La versión 12.2(1)T y posteriores de software del IOS permiten que RSVP realice el control de admisión mediante su propio agrupamiento de "ancho de banda rsvp ip", al mismo tiempo que CBWFQ clasifica, regula y planifica los paquetes RSVP. Esto asume los paquetes premarcados por el remitente y que los paquetes no RSVP están marcados de otro modo.

## Detección temprana aleatoria ponderada (WRED) de prevención de congestión

P. ¿Puedo habilitar la detección temprana aleatoria ponderada (WRED) y la cola de latencia baja (LLQ), o la cola equilibrada ponderada basada en clase (CBWFQ) al mismo tiempo?

R. Sí. La cola define el orden de los paquetes que dejan una cola. Esto significa que define un mecanismo de planificación de paquetes. También se puede utilizar para proporcionar una asignación equitativa de ancho de banda y garantías de ancho de banda mínimo. Por el contrario, la petición de comentarios (RFC) 2475 define el descarte como el "proceso de descartar paquetes según las reglas especificadas". El mecanismo de eliminación predeterminado es eliminación de cola, en el cual la interfaz elimina paquetes cuando la cola está completa. Un mecanismo de descarte alternativo es Detección temprana aleatoria (RED) y WRED de Cisco, que comienza a descartar paquetes de forma aleatoria antes de que la cola esté llena e intenta mantener un promedio uniforme de profundidad de la cola. WRED usa los valores de precedencia IP de los paquetes para tomar una decisión de caída diferenciada. Para obtener más información, consulte [Detección temprana aleatoria y ponderada \(WRED\)](#).

P. ¿Cómo puedo monitorear la Detección temprana aleatoria ponderada (WRED) y ver que realmente tiene efecto?

Una WRED monitorea la profundidad promedio de una cola y comienza a soltar paquetes cuando el valor calculado supera el valor de umbral mínimo. Ejecute el comando `show policy-map interface` y supervise el valor de profundidad media de la cola, como se muestra en el ejemplo siguiente:

```
<#root>
```

```
Router#
```

```
show policy interface s2/1
```

```
Serial2/1
output : p1
Class c1
  Weighted Fair Queueing
    Output Queue: Conversation 265
```

```
Bandwidth 20 (%)
(pkts matched/bytes matched) 168174/41370804
(pkts discards/bytes discards/tail drops) 20438/5027748/0
mean queue depth: 39
```

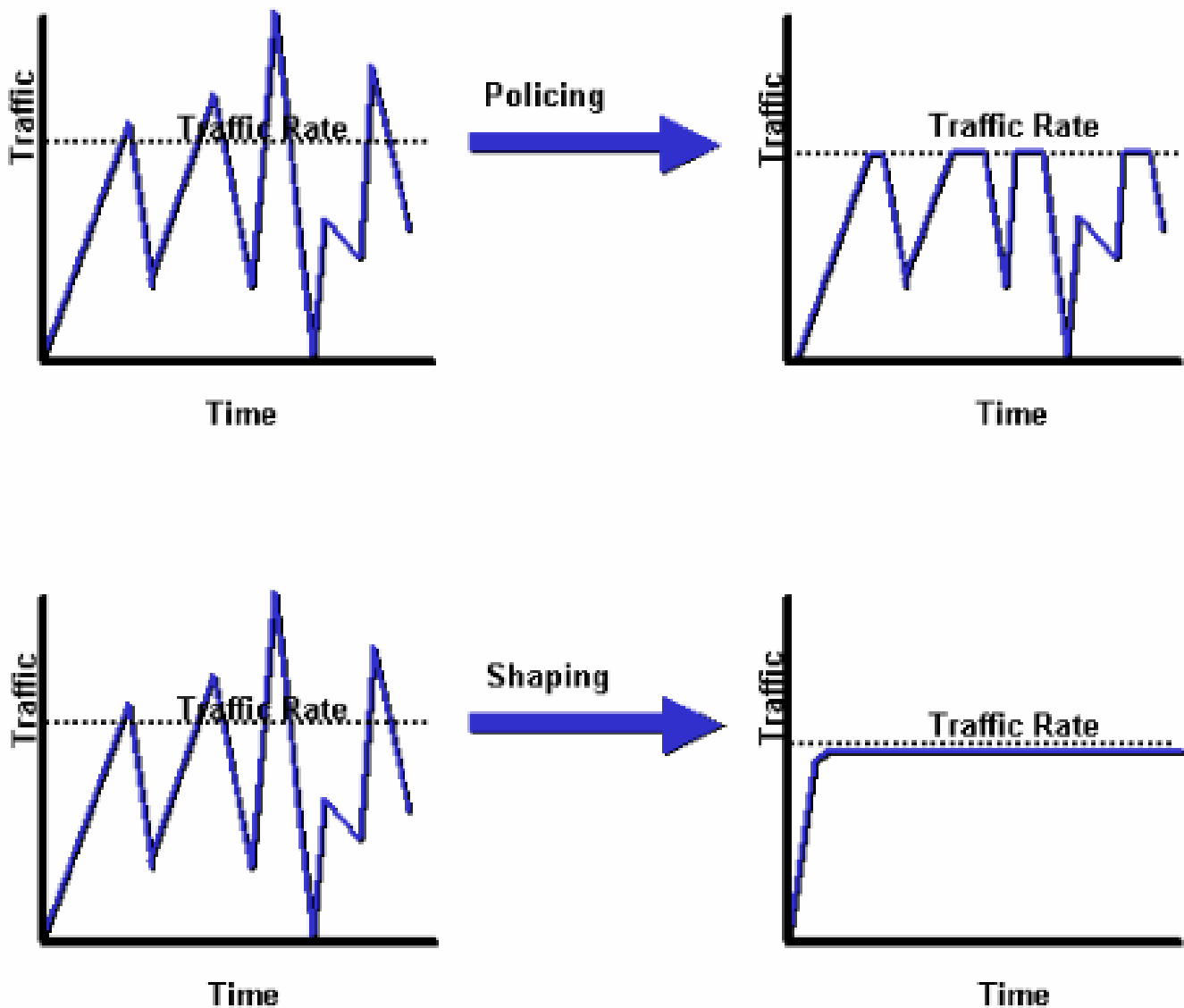
Dscp (Prec)	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum threshold	Maximum threshold	Mark probability
0(0)	2362/581052	1996/491016	20	40	1/10
1	0/0	0/0	22	40	1/10
2	0/0	0/0	24	40	1/10

[output omitted]

## Regulación del Tráfico y Modelado

P. ¿Cuál es la diferencia entre la regulación y el modelado?

A. El siguiente diagrama ilustra la diferencia clave. El modelado del tráfico conserva los paquetes en exceso en una cola y luego programa el exceso para la transmisión posterior en incrementos de tiempo. El resultado del diseño del tráfico es una velocidad atenuada del paquete de salida. Por el contrario, la regulación de tráfico propaga las ráfagas. Cuando la velocidad del tráfico alcance la velocidad máxima configurada, el tráfico en exceso se suprime (o remarca). El resultado es una velocidad de salida que tiene la apariencia de un diente de sierra, con crestas y depresiones.



Para obtener más información, consulte [Descripción general de modelado y políticas](#).

P. ¿Qué es una cubeta con ficha y cómo funciona el algoritmo?

R. Una cubeta con ficha en sí no tiene política de descarte o prioridad. A continuación, hay un ejemplo de cómo funciona la metáfora de cubeta con fichas:

- Los token ingresan al bloque de memoria a una velocidad determinada.
- Cada Token es un permiso para que la fuente envíe una cierta cantidad de bits.
- Para enviar un paquete, el regulador del tráfico debe ser capaz de retirar de la cubeta una cantidad de fichas equivalente al tamaño del paquete.
- Si no hay suficientes fichas en la cubeta como para enviar un paquete, el paquete espera hasta que la cubeta tenga suficientes fichas (en el caso de un modelador) o el paquete se descarta o se rebaja (en el caso de un vigilante).
- La cubeta posee una capacidad especificada. Si la capacidad del compartimiento de

memoria se encuentra completa, todos los símbolos nuevos que lleguen serán descartados y no estarán disponibles para paquetes futuros. De esta manera, en cualquier momento, la ráfaga más grande que una fuente puede enviar a la red es más o menos proporcional al tamaño de la cubeta. El token bucket permite la saturación, pero la limita.

P. Con un regulador de tráfico como la regulación basada en clases, ¿qué significan Committed Burst (BC) y Excess Burst (Be) y cómo debo seleccionar estos valores?

R. Un regulador de tráfico no almacena en búfer los paquetes excedentes y los transmite más tarde, como ocurre con un modelador. En cambio, el regulador de tráfico ejecuta una política de envío simple o de no envío sin almacenar en la memoria intermedia. Durante los períodos de congestión, ya que no puede almacenar en búfer, lo mejor que puede hacer es descartar paquetes de forma menos agresiva configurando correctamente las ráfagas excesivas. Por lo tanto, es importante tener en cuenta que la regulación utiliza los valores de ráfaga normal y de ráfaga excesiva para garantizar que se cumpla con la tasa de información comprometida (CIR) configurada.

Los parámetros de ráfaga son modelados ampliamente en la regla genérica de almacenamiento en memoria intermedia para los routers. La regla recomienda configurar el almacenamiento en el búfer igual a la velocidad del trayecto de ida y vuelta para acomodar las ventanas pendientes del Protocolo de control de transmisión (TCP) de todas las conexiones en momentos de congestión.

En la tabla siguiente, se describe la finalidad y la fórmula recomendada para los valores de ráfaga normal y extendida:

Parámetro de ráfaga	Propósito	Fórmula recomendada
ráfaga normal	<ul style="list-style-type: none"> <li>• Implementa un token bucket estándar.</li> <li>• Configura el tamaño máximo de de la cubeta de tokens (a pesar de que los tokens pueden tomarse prestados si Be es mayor que BC).</li> <li>• Determina cuán grande puede ser</li> </ul>	<pre>&lt;#root&gt; CIR [BPS] * (1 byte)/(8 bits) * 1.5 seconds</pre> <p>Nota: 1,5 segundos es el tiempo de ida y vuelta habitual.</p>



	<p>la cubeta con tokens ya que los tokens recientemente llegados están descartados y no están disponibles para futuros paquetes si la cubeta completa toda su capacidad.</p>	
<p>ráfaga extendida</p>	<ul style="list-style-type: none"> <li>• Pone en funcionamiento una cubeta con ficha con capacidad extendida de ráfaga.</li> <li>• Se deshabilita estableciendo <math>BC = Be</math>.</li> <li>• Cuando <math>BC</math> es igual a <math>Be</math>, la regulación de tráfico no puede pedir prestados tokens y simplemente descarta el paquete cuando no hay suficientes tokens disponibles.</li> </ul>	<pre>&lt;#root&gt; 2 * normal burst</pre>

No todas las plataformas utilizan o admiten el mismo rango de valores para un regulador de tráfico. Consulte el siguiente documento para conocer los valores compatibles con una plataforma específica:

- [Descripción general de la regulación y diseño de tráfico](#)

P. ¿Cómo decide la Velocidad de acceso comprometida (CAR) o la regulación basada en clases si un paquete cumple o supera la Velocidad de información comprometida (CIR)? El router está liberando paquetes e informando una velocidad excesiva aunque la velocidad conformada sea menor que la CIR configurada.

R. Un regulador de tráfico utiliza los valores normales de ráfaga y ráfaga extendida para asegurarse de que se alcanza la CIR configurada. La configuración de valores de ráfaga suficientemente elevados es importante para asegurar un buen rendimiento. Si los valores de ráfaga se configuran demasiado bajos, la velocidad alcanzada puede ser mucho menor que la velocidad configurada. Exigirle demasiado a las ráfagas temporarias puede tener un impacto adverso sobre el rendimiento del Protocolo de control de transmisión (TCP). Con CAR, ejecute el comando `show interface rate-limit` para supervisar la ráfaga actual y determinar si el valor mostrado se acerca de modo uniforme a los valores de límite (BC) y límite extendido (Be).

```
<#root>
```

```
rate-limit 256000 7500 7500 conform-action continue exceed-action drop
rate-limit 512000 7500 7500 conform-action continue exceed-action drop
```

```
router#
```

```
show interfaces virtual-access 26 rate-limit
```

```
Virtual-Access26 Cable Customers
```

```
Input
```

```
matches: all traffic
```

```
params: 256000 BPS, 7500 limit, 7500 extended limit
```

```
conformed 2248 packets, 257557 bytes; action: continue
```

```
exceeded 35 packets, 22392 bytes; action: drop
```

```
last packet: 156ms ago, current burst: 0 bytes
```

```
last cleared 00:02:49 ago, conformed 12000 BPS, exceeded 1000 BPS
```

```
Output
```

```
matches: all traffic
```

```
params: 512000 BPS
```

```
, 7500 limit, 7500 extended limit
```

```
conformed 3338 packets, 4115194 bytes; action: continue
```

```
exceeded 565 packets, 797648 bytes; action: drop
```

```
last packet: 188ms ago,
```

```
current burst: 7392 bytes
```

```
last cleared 00:02:49 ago,
```

```
conformed 194000 BPS, exceeded 37000 BPS
```

Si desea más información, consulte los siguientes documentos:

- [Descripción general de la regulación y diseño de tráfico](#)

- [QoS Policing en el Catalyst 6000](#)
- [Preguntas frecuentes sobre la calidad de servicio en Catalyst 4000](#)
- [Preguntas frecuentes sobre la QoS de los módulos WS-X4232-L3 de capa 3 y switches Catalyst de la serie G-L3](#)

P. ¿Son independientes entre sí la ráfaga y el límite de cola?

R. Sí, la ráfaga del regulador y el límite de cola son independientes entre sí. Puede considerar la regulación como una puerta de entrada que permite un determinado número de paquetes (o bytes) y la cola como un contenedor de tamaño límite de cola que retiene los paquetes admitidos antes de la transmisión en la red. Lo ideal sería que el contenedor sea lo suficientemente grande como para retener una ráfaga de bytes/paquetes admitidos por la puerta de entrada (regulación).

## Frame Relay de Calidad de servicio (QoS)

P. ¿Qué valores debo seleccionar para Velocidad de confirmación de información (CIR), Ráfaga comprometida (BC), Ráfaga excesiva (Be) y CIR mínima (MinCIR)?

R. El modelado de tráfico de Frame Relay, que se habilita al ejecutar el comando frame-relay traffic-shaping, admite varios parámetros configurables. Estos parámetros incluyen frame-relay cir, frame-relay mincir y frame-relay BC. Consulte los siguientes documentos para más información sobre la selección de estos valores y para poder comprender los comandos show relacionados:

- [Configuración del modelado del tráfico de retransmisión de tramas en routers 7200 y plataformas inferiores](#)
- [Comandos show para el modelado de tráfico de retransmisión de tramas](#)
- [VoIP sobre Frame Relay con calidad de servicio \(fragmentación, diseño de tráfico y prioridad IP RTP\)](#)

P. ¿Funciona la cola prioritaria sobre la interfaz principal Frame Relay en el IOS de Cisco versión 12.1?

R. Las interfaces Frame Relay admiten tanto mecanismos de cola de interfaz como mecanismos de cola por circuito virtual (VC). A partir de la versión 12.0(4)T del IOS de Cisco, la cola de interfaz admite el sistema Primero en entrar, primero en salir (FIFO) o Prioridad de Cola por Interfaz (PIPQ) solamente cuando usted configura el Modelado del tráfico de Frame Relay (FRTS). Por lo tanto, la siguiente configuración dejará de funcionar si actualiza a Cisco IOS 12.1.

```
interface Serial0/0
  frame-relay traffic-shaping
  bandwidth 256
  no ip address
```

```

encapsulation frame-relay IETF
priority-group 1

!
interface Serial10/0.1 point-to-point
bandwidth 128
ip address 136.238.91.214 255.255.255.252
no ip mroute-cache
traffic-shape rate 128000 7936 7936 1000
traffic-shape adaptive 32000
frame-relay interface-dlci 200 IETF

```

Si FRTS no está habilitado, puede aplicar un método alternativo de colocación en cola, tal como la Colocación en cola equilibrada ponderada en función de la clase (CBWFQ), a la interfaz principal, que actúa como un único conducto de ancho de banda. Además, a partir de la versión 12.1.1(T) del IOS de Cisco, puede habilitar la colocación en cola prioritaria de la interfaz (PIPQ) de los circuitos virtuales permanentes (PVC) de Frame Relay en una interfaz principal de Frame Relay. Puede definir la prioridad PVC en alta, media, normal o baja y emitir el comando `frame-relay interface-queue priority` en la interfaz principal, como se muestra en el ejemplo siguiente:

```
<#root>
```

```

interface Serial3/0
description framerelay main interface
no ip address
encapsulation frame-relay
no ip mroute-cache
frame-relay traffic-shaping

```

```
frame-relay interface-queue priority
```

```

interface Serial3/0.103 point-to-point
description frame-relay subinterface
ip address 1.1.1.1 255.255.255.252
frame-relay interface-dlci 103
class frameclass

```

```

map-class frame-relay frameclass
frame-relay adaptive-shaping becn
frame-relay cir 60800
frame-relay BC 7600
frame-relay be 22800
frame-relay mincir 8000
service-policy output queueingpolicy

```

```
frame-relay interface-queue priority low
```

P. ¿La Formación del tráfico de Frame Relay (FRTS) funciona con Distributed Cisco Express Forwarding (dCEF) y con Distributed Class Based Weighted Fair Queueing (dCBWFQ)?

A. A partir de Cisco IOS 12.1(5)T, sólo la versión distribuida de las características QoS se admiten en los VIP de la serie Cisco 7500. Para habilitar el modelado de tráfico en las interfaces de Frame Relay, use el Modelado de tráfico distribuido (DTS). Si desea más información, consulte los siguientes documentos:

- [Interfaz versátil de procesador distribuida FRF.11 y FRF.12 para el IOS de Cisco versión 12.1 T](#)
- [Modelado del Tráfico de Frame Relay con QoS distribuido en las series Cisco 7500](#)

## Calidad del servicio (QoS) en el Asynchronous Transfer Mode (ATM)

P. ¿Dónde aplico una política de servicio con Class Based Weighted Fair Queueing (CBWFQ) y Low Latency Queueing (LLQ) en una interfaz de Asynchronous Transfer Mode (ATM)?

A. A partir de Cisco IOS 12.2, las interfaces ATM admiten políticas de servicio en tres niveles o interfaces lógicas: interfaz principal, subinterfaz y circuito virtual permanente (PVC). Dónde aplicar la política es una función de la capacidad de Calidad de servicio (QoS) que está habilitando. Las políticas de formación en cola deben ser aplicadas por Circuito virtual (VC) ya que la interfaz ATM monitorea el nivel de congestión por VC y mantiene las colas para paquetes en exceso por VC. Si desea más información, consulte los siguientes documentos:

- [¿Dónde se debe aplicar una política de servicio QoS en una interfaz ATM?](#)
- [Información sobre la cola de transmisión Per-VC en las interfaces ATM NM-1 y PA-A3](#)

P. ¿Qué bytes cuentan las colas de clase de servicio (CO) de IP a modo de transferencia asíncrona (ATM)?

R. Los comandos bandwidth y priority configurados en una política de servicio para habilitar la colocación en cola equilibrada ponderada basada en clase (CBWFQ) y la colocación en cola de latencia baja (LLQ), respectivamente, utilizan un valor de Kbps que cuenta los mismos bytes de sobrecarga que cuentan los resultados del comando show interface. Específicamente, el sistema de cola de la capa 3 cuenta el Control de link lógico / Protocolo de acceso a la subred (LLC/SNAP). No considera lo siguiente:

- Cola de capa 5 de adaptación ATM (AAL5)
- Relleno para lograr que la última celda sea un múltiplo par de 48 bytes.
- Encabezado de celdas de cinco bytes
- [¿Qué bytes se cuentan por IP para la cola de ATM CoS?](#)

P. ¿Cuántos circuitos virtuales (VCS) pueden admitir una política de servicio simultáneamente?

R. El siguiente documento proporciona pautas útiles sobre el número de VCS de modo de transferencia asíncrono (ATM) que pueden admitir. Se han implementado de forma segura de 200 a 300 circuitos virtuales permanentes con velocidad de bits variable en tiempo no real (VBR-nrt):

- [Guía de diseño de clase de servicio IP a ATM](#)

También tenga en cuenta lo siguiente:

- Utilice un procesador potente y con capacidad. Por ejemplo, un VIP4-80 proporciona un rendimiento muy superior al de un VIP2-50.
- Cantidad de memoria disponible para paquetes. En el NPE-400, se reservan hasta 32 MB (en un sistema con 256 MB) para el búfer de paquetes. En un NPE-200, se destinan hasta 16 MB para memoria intermedia de paquetes en un sistema con 128 MB.
- Las configuraciones con Detección temprana aleatoria ponderada (WRED) por VC que opera simultáneamente en hasta 200 ATM PVC han sido probadas ampliamente. La cantidad de memoria del paquete en VIP2-50 que puede utilizarse para las colas por VC es finita. Por ejemplo, un VIP2-50 con SRAM de 8 MB brinda 1085 memorias intermedias de paquetes disponibles para IP a ATM CO por cola de VC en la que funciona WRED. Si se configuraran 100 PVC de ATM y si todos los VCS experimentaran congestión excesiva simultáneamente (como se podría simular en los entornos de prueba en los que se utilizaría una fuente de flujo controlado sin TCP), cada PVC en promedio tendría aproximadamente 10 paquetes de almacenamiento en memoria intermedia, lo que puede ser demasiado corto para que WRED funcione correctamente. Los dispositivos VIP2-50 con una SRAM de gran tamaño son, por lo tanto, muy recomendables en diseños con una cantidad elevada de ATM PVC que ejecutan WRED por VC y que pueden experimentar una congestión de manera simultánea.
- Cuanto mayor sea el número de circuitos virtuales permanentes activos configurados, se necesitará menos velocidad de celda sostenida (SCR) y, por lo tanto, más breve será la cola que la WRED necesita para funcionar en el circuito. De esta manera, como sucede cuando se utilizan los perfiles WRED predeterminados de la función Clase de servicio (CoS) IP a ATM de la Fase 1, la configuración de los umbrales inferiores de caída WRED, cuando WRED por VC se activa en un gran número de PVC ATM congestionados de baja velocidad, minimizaría el riesgo de escasez de búfer en VIP. La escasez de búfer en el VIP no causa ningún error de funcionamiento. En el caso de que exista una insuficiencia en el búfer en el VIP, la característica de la fase 1 de IP a ATM CO simplemente se degrada a la eliminación de la cola según una estructura primero en entrar, primero en salir (FIFO) durante el período de insuficiencia del búfer (es decir que la misma política de caída que ocurriría si la característica IP a ATM CO no se activara en este PVC).
- Número máximo de VCS simultáneos que se pueden admitir de manera razonable.

P. ¿Qué hardware de modo de transferencia asíncrono (ATM) es compatible con las funciones de clase de servicio (CO) IP a ATM, incluidas las de cola equilibrada ponderada basada en clase (CBWFQ) y cola de latencia baja (LLQ)?

A. La CoS IP a ATM se refiere a un conjunto de funciones que se activan por Circuito virtual (VC). Dada esta definición, el IP a los CO ATM no es soportado en el Procesador de interfaz ATM (AIP), PA-A1 o en los procesadores de red ATM 4500. Este hardware ATM no admite cola por canal virtual como la definen PA-A3 y la mayoría de los módulos (excepto ATM-25). Si desea más información, consulte el siguiente documento:

- [Descripción de la compatibilidad del hardware ATM por IP para ATM CoS](#)
- [Cola justa ponderada por VC basada en la clase en las plataformas basadas en RSP](#)
- [Class-Based Weighted Fair Queuing por VC \(por VC CBWFQ\) en los routers Cisco 7200, 3600, y 2600](#)
- [Almacenamiento en cola por VC en el adaptador de puerto PA-A3-8T/E1 IMA ATM](#)
- [Configuración de cola ATM por VC en MC3810](#)

## Voz y calidad de servicio (QoS)

P. ¿Cómo funciona la fragmentación y entrelazado de enlaces (LFI)?

A. El tráfico interactivo como Telnet o Voz sobre IP es susceptible de generar una mayor latencia cuando los grandes paquetes de procesos de red como el protocolo de transferencia de archivos (FTP) transfiere a través de una WAN. La demora de paquete para el tráfico interactivo es importante cuando los paquetes FTP son colocados en la cola en links WAN más lentos. Se diseñó un método para fragmentar los paquetes más grandes, y enviar a la cola los paquetes (de voz) más pequeños entre los fragmentos de los paquetes (FTP) más grandes. Los routers Cisco IOS soportan diferentes mecanismos de fragmentación capa 2. Si desea más información, consulte los siguientes documentos:

- [Descripción General de los Mecanismos de Eficiencia de Links](#)
- [VoIP sobre Frame Relay con calidad de servicio \(fragmentación, diseño de tráfico y prioridad IP RTP\)](#)
- [Voz sobre IP sobre links PPP con calidad de servicio \(LLQ/ prioridad IP RTP , LFI, cRTP\)](#)

P. ¿Qué herramientas puedo utilizar para supervisar el rendimiento de voz sobre IP?

R: Actualmente, Cisco ofrece diversas opciones para la supervisión de Calidad de servicio (QoS) en redes mediante las soluciones Voz sobre IP de Cisco. Estas soluciones no miden la calidad de voz utilizando Perpetual Speech Quality Measurement (PSQM) o algunos de los nuevos

algoritmos propuestos para la medición de la calidad vocal. Para este fin, se dispone de herramientas de Agilent (HP) y NetIQ. Sin embargo, Cisco ofrece herramientas que dan una idea de la calidad de voz que está experimentando mediante la medición del retraso, la fluctuación y la pérdida de paquetes. Para obtener más información, consulte [Uso del agente de garantía del servicio de Cisco y supervisión del rendimiento de Internetwork para administrar la calidad del servicio en redes de Voz por IP](#).

P. %SW\_MGR-3-CM\_ERROR\_FEATURE\_CLASS: Error de característica de Connection Manager: clase SSS: (QoS) - error de instalación, omitir.

R. El error de instalación de la función observado es un comportamiento esperado cuando se aplica una configuración no válida a una plantilla. Indica que no se ha aplicado la política de servicio debido a un conflicto. En general, no se debe configurar el modelado del valor predeterminado de clase de la política secundaria en asignaciones de políticas jerárquicas; configúrelo en la política principal de la interfaz. Este mensaje, junto con la trazabilidad, aparece como una consecuencia.

Con las políticas basadas en la sesión, el modelado del valor predeterminado de clase debe realizarse solo en el nivel del circuito virtual permanente o la subinterfaz. No se admite el modelado en la interfaz física. Si la configuración se realiza en la interfaz física, la aparición de este mensaje de error es un comportamiento previsto.

En caso de LNS, otro motivo podría ser que la política de servicio podría provisionarse a través del servidor Radius cuando aparecen las sesiones. Ejecute el comando show tech para ver la configuración del servidor Radius y para ver cualquier política de servicio ilegal que se instale a través del servidor Radius cuando la sesión se reactiva o está intermitente.

## Información Relacionada

- [Fundamentos del ajuste de rendimiento](#)
- [Soporte de Calidad de servicio \(QoS\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).