

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 modo de transferencia asíncrona \(ATM\)](#)

[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

Q. ¿Cuál es Calidad de Servicio (QoS)?

A. QoS refiere a la capacidad de una red de proporcionar un mejor servicio al tráfico de la red seleccionada sobre las diversas tecnologías subyacentes incluyendo el Frame Relay, Asynchronous Transfer Mode (ATM), los Ethernetes y 802.1 redes, SONET, y las redes ruteadas 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:

- Soportar el Ancho de banda dedicado.
- Mejora de las características de pérdida.
- Cómo evitar y administrar la congestión de la red.
- Formar el tráfico de la 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 Solicitud de comentarios (RFC) 2205 define RSVP, y el RFC 1633 define IntServ.

Focos del DiffServ en agregado y aprovisionado 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](#)

Q. ¿Qué significa congestión, retardo y fluctuación?

A. Una interfaz experimenta la congestión cuando se presenta con más tráfico que él puede dirigir. 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 varias clases de retardos, como se explica en [comprensión de los retrasos en la red de voz en paquetes](#). [La variación en el retardo se conoce como fluctuación, según se explica en Comprensión de la fluctuación en redes de voz en paquetes \(plataformas de Cisco IOS\)](#). Necesidad de la fluctuación y retraso de ser controlado y de ser minimizado para soportar el tiempo real y el tráfico interactivo.

Q. ¿Qué es MQC?

A. Comando line interface(cli) de la calidad de servicio modular de la significa MQC (QoS). Es diseñado para simplificar la configuración de QoS en los routers Cisco y el Switches definiendo un conjunto común de la sintaxis de los comandos y el resultar de los comportamientos de QoS a través de 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. Defina una clase de tráfico publicando 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. Asocie la política de tráfico a la interfaz, a la subinterfaz, o al virtual circuit (VC) publicando el **comando service-policy**.

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

Para más información, refiera a la [interfaz de línea de comando de calidad de servicio modular](#).

Q. ¿Qué significa que la política de servicio sólo es compatible en las interfaces VIP con el mensaje de DCEF habilitado?

A. En el Versatile Interface Processors (VIP) en las Cisco 7500 Series, solamente las características distribuidas del Calidad de Servicio (QoS) se soportan a partir del Cisco IOS 12.1(5)T, de 12.1(5)E, y de 12.0(14)S. Habilitar el Distributed Cisco Express Forwarding (dCEF) habilita automáticamente el calidad del servicio (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:

- [Class-Based Weighted Fair Queueing distribuido y Weighted Random Early Detection distribuido](#)
- [Low latency queueing 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 hacen una admite una política del Calidad de Servicio (QoS)?

A. En versiones del IOS de Cisco anteriores a la 12.2 usted podía definir un máximo de sólo 256 clases, y podía definir sólo 256 clases dentro de cada política si las mismas clases eran vueltas a usar para diferentes políticas. Si usted tiene dos directivas, el número total de clases de ambas directivas no debe exceder el 256. Si una directiva incluye el Mecanismo de cola de espera equitativo y ponderado basado en clases (CBWFQ) (significarlo contiene una declaración del [or priority] del ancho de banda dentro de las clases unas de los), el número total de clases soportadas es 64.

En las versiones deL Cisco IOS 12.2(12),12.2(12)T, y 12.2(12)S, esta limitación de class-maps global 256 fue cambiada, y es posible ahora configurar hasta 1024 class-maps globales y utilizar el 256 class-maps dentro del mismo directiva-mapa.

Q. ¿Cómo se procesan las actualizaciones de ruteo y el Keepalives del Point-to-Point Protocol (PPP)/del High-Level Data Link Control (HDLC) cuando una política de servicio es aplicada?

A. El Routers del Cisco IOS utiliza los dos mecanismos siguientes 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.](#)

Q. ¿El Calidad de Servicio (QoS) se soporta en las interfaces configuradas con el Integrated Routing and Bridging (IRB)?

A. No. Usted no puede configurar los featues de QoS cuando la interfaz se configura para el IRB.

Clasificación y marcado

Q. ¿Qué es la clasificación previa de calidad de servicio (QoS)?

A. La pre-clasificación de QoS le permite para hacer juego encendido y para clasificar el contenido del encabezado IP original de los paquetes que experimentan la encapsulación de túnel y/o el cifrado. Esta característica no describe el proceso de copiar el valor original del byte del Tipo de servicio (ToS) del encabezado de 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](#)

Q. ¿Qué campos del encabezado del paquete pueden ser observados? ¿Qué valores están disponibles?

A. La característica de marcación basada en la clase le permite configurar o marcar el encabezado de la capa 2, capa 3 o el Multiprotocol Label Switching (MPLS) de sus paquetes. Si desea más información, consulte los siguientes documentos:

- [Configurar la marca del paquete en base a la clase](#)
- [¿Cuándo establece un router el bit CLP en una célula ATM?](#)
- [Configuración del paquete de marcación en PVC de Frame Relay](#)

Q. ¿Puedo priorizar el tráfico basado en el URL?

A. 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 mayoría de la clasificación granular era números del puerto del Transmission Control Protocol (TCP) y del User Datagram Protocol (UDP) de la capa 4. Si desea más información, consulte los siguientes documentos:

- [Q&A del reconocimiento de la aplicación basada 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](#)

Q. ¿Qué plataformas y qué versiones del software IOS de Cisco y admiten el Reconocimiento de aplicación con base en la red (NBAR)

A. El soporte para el NBAR se introduce en las versiones del Cisco IOS Software siguientes:

Plataforma	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: Para utilizar NBAR debe activar Cisco Express Forwarding (CEF).

El NBAR distribuido (DNBAR) está disponible en las Plataformas siguientes:

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

Nota: Ni las interfaces VLAN con Tarjeta de función del switch multicapa (MSCF) de Catalyst 6000, ni la serie 12000 de Cisco ni el Módulo de conmutación de ruta (RSM) admiten NBAR. Si usted no ve una plataforma particular enumerada arriba, entre en contacto por favor su representante técnico de Cisco.

Administración de congestión y colas

Q. ¿Cuál es el propósito de la espera?

A. La espera es diseñada para acomodar la congestión temporal en una interfaz de dispositivo de red salvando los paquetes en exceso en los buffers hasta que el ancho de banda esté 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. Usted puede limpiar el tráfico entrante, pero usted no puede hacer cola generalmente entrante (una excepción es almacenamiento en búfer del lado receptor en un Cisco 7500 Series Router que usa el Distributed Cisco Express Forwarding (dCEF)

para remitir los paquetes del ingreso a la interfaz de egreso; para más información, refiera a [comprensión ejecución al 99% de CPU de VIP y almacenamiento en búfer en 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](#)

Q. ¿Cómo funciona la Colocación en cola equilibrada ponderada (WFQ) y la Colocación en cola equilibrada ponderada en función de la clase (CBWFQ)?

A. La espera justa intenta afectar un aparato un reparto justo del ancho de banda de una interfaz entre las conversaciones activas o el IP fluye. 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:

- $W=K/(\text{precedencia} +1)$

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.

El CBWFQ permite que usted defina una clase de tráfico y que le asigne una garantía mínima del ancho de banda. El algoritmo detrás de este mecanismo es WFQ, lo que explica el nombre. Para configurar CBWFQ, define clases específicas en enunciados map-class. Entonces usted asigna una directiva a cada clase en un directiva-mapa. 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](#)

Q. Si una clase del Almacenamiento en cola basado en clases con ponderación equilibrada (CBWFQ) no usa su ancho de banda, ¿pueden otras clases usar el ancho de banda?

A. 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.](#)

Q. ¿El Class Based Weighted Fair Queueing (CBWFQ) se soporta en las subinterfaces?

A. Las interfaces lógicas del IOS de Cisco no admiten de forma inherente un estado de congestión y no admiten la aplicación directa de una política de servicios que se aplica a un método de colocación en 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.](#)

Q. ¿Cuál es la diferencia entre las sentencias de prioridad y ancho de banda en una correlación de políticas?

A. Los comandos priority y bandwidth difieren en cuanto a funcionalidad y en qué aplicaciones se admiten. La tabla siguiente resume estas diferencias:

Función	Comando bandwidth	Comando priority
Garantía de ancho de banda mínimo	Sí	Sí
Garantía de ancho de banda máxima	No	Sí
Vigilante incorporado	No	Sí
Proporciona latencia baja	No	Sí

[Para obtener más información, consulte Comparación de los comandos bandwidth y priority de una política de servicio de QoS.](#)

Q. Cómo se calcula el límite de cola en los Procesadores de interfaz versátil (VIP) y FlexWAN.

A. Suficiente SRAM asumido en el VIP o el FlexWan, el límite de cola se calcula sobre la base de un retardo máximo de 500ms con el tamaño promedio de los paquetes de 250 bytes. Lo que sigue es un ejemplo de una clase con el Mbps de ancho de banda uno:

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

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 subinterfaces con circuitos permanentes (PVC) de 2 MB. La política de servicio se aplica a cada VC.

```
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 entonces se afecta un aparato una porción de los 50, tal y como se muestra en el producto siguiente:

```
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 búferes antes de alcanzar el límite de cola. En este caso, intente manualmente ajustar abajo del cola-límite en las clases no prioritarias. Para más información, refiera a [entender el límite de la cola de transmisión con el IP to ATM CoS](#).

Q. ¿Cómo verifica el valor de límite de la cola?

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

```
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
```

Q. ¿Puedo habilitar una colocación en cola equilibrada dentro de una clase?

A. La serie 7500 de Cisco con Calidad de servicio (QoS) distribuida admite el envío a cola equilibrado por clase. Otras Plataformas, incluyendo las Cisco 7200 Series y el Cisco Series 2600/3600, soporte cargaron la feria que hacía cola (WFQ) en el clase class-default; todas las clases de ancho de banda utilizan Primero en entrar, Primero en salir (FIFO).

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

A. Utilice los siguientes comandos de monitorear la espera:

- **show queue {interface} {interface number}** - En las plataformas de Cisco IOS con excepción de las Cisco 7500 Series, este comando visualiza las colas de administración del tráfico o las 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 hay congestión, usted todavía podrá ver algunos golpes 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 para formar la cola de la herencia como el Asignación de colas de prioridad (PQ), la Asignación personalizada de colas, y la feria cargada que hace cola (WFQ), no proporcionarán las estadísticas de clasificación. Solamente la Interfaz de Línea de Comando de Calidad de Servicio Modular (MQC) - las características basadas en las imágenes que 12.0(5)T proporciona más adelante 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. Los paquetes correspondidos con al revés indican el número de paquetes que corresponden con los criterios de la clase cuando la interfaz fue congestionada. 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.](#)
- Configuración de QoS basada en la clase y estadísticas MIB de Cisco - Proporciona las capacidades de monitoreo del Simple Network Management Protocol (SNMP).

Q. RSVP se puede utilizar conjuntamente con el 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 parece comportarse como si el CBWFQ no se configure con respecto a

disponibilidad del ancho de banda, la evaluación, y a la asignación.

A. Cuando utilice RSVP y CB-WFQ en el software del IOS de Cisco versión 12.1(5)T y posteriores, el router puede operar de tal forma que RSVP fluye y las clases CBWFQ comparten 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

Q. ¿Puedo activar Weighted Random Early Detection (WRED) y Low Latency Queueing (LLQ) o Class Based Weighted Fair Queueing (CBWFQ) al mismo tiempo?

A. Sí. La cola define el orden de los paquetes que dejan una cola. Esto significa que define un mecanismo de planificación de paquetes. También puede ser utilizada para proporcionar la asignación y las garantías mínimas del ancho de banda del ancho de banda justo. En cambio, la Solicitud de comentarios (RFC) 2475 define la caída como el "proceso de desechar los paquetes basados en 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 desconexión alternativo es el WRED de Detección temprana aleatoria (RED) y de Cisco, que comienza a caer los paquetes aleatoriamente antes de que la cola sea llena e intenta mantener una profundidad de cola promedio constante. WRED usa los valores de precedencia IP de los paquetes para tomar una decisión de caída diferenciada. Para más información, refiera al [Weighted Random Early Detection \(WRED\)](#).

Q. ¿Cómo puedo monitorear el Weighted Random Early Detection (WRED) y verlo realmente el tomar del efecto?

A. El WRED monitorea la profundidad de cola promedio y comienza a caer los paquetes cuando el valor calculado pasa por encima el valor de umbral mínimo. Publique el **comando show policy-map interface** y monitoree el valor malo de la profundidad de espera en cola, tal y como se muestra en del siguiente ejemplo:

```
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 Random drop Tail
drop Minimum Maximum Mark (Prec) pkts/bytes pkts/bytes threshold threshold 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

Q. ¿Cuál es la diferencia entre regulación y formación?

A. El siguiente diagrama ilustra la diferencia fundamental. El modelado de tráfico conserva los paquetes en exceso en una cola y después programa el exceso para la transmisión posterior

sobre los incrementos del 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 más información, refiérase [Descripción general de la regulación y diseño de tráfico](#).

Q. ¿Cuál es un token bucket y cómo el algoritmo trabaja?

A. Una cubeta con ficha no posee una política de prioridad o descarte. 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.

Q. ¿Con un vigilante de tráfico tal como class-based policing, qué el committed burst (Bc) y la ráfaga en exceso (Be) significan y cómo deben yo seleccionar estos valores?

A. Un regulador de tráfico no almacena paquetes excedentes para transmitirlos luego, como sí sucede 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, puesto que usted no puede mitigar, el mejor que usted puede hacer es caer los paquetes menos agresivamente correctamente configurando la ráfaga ampliada. Por lo tanto, es importante entender que el policer utiliza la explosión normal y los valores de ráfaga ampliada para asegurar la Velocidad de información comprometida (CIR) configurada están alcanzados.

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.

La tabla siguiente describe el propósito y la fórmula recomendada por el normal y los valores de ráfaga ampliada:

Parámetro de ráfaga	Propósito	Fórmula recomendada
---------------------	-----------	---------------------

a		
explosión normal	<ul style="list-style-type: none"> • Implementa un compartimiento del Token estándar. • 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). • Determina cuán grande puede ser 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>CIR [BPS] * (1 byte)/(8 bits) * 1.5 seconds Nota: 1.5 segundos son el Round Trip Time típico.</p>
ráfaga extendida	<ul style="list-style-type: none"> • Pone en funcionamiento una cubeta con ficha con capacidad extendida de ráfaga. • Inhabilitado fijando el BC = sea. • Cuando el BC es igual ser, el regulador del tráfico no puede pedir prestados los tokens y cae simplemente el paquete cuando los tokens insuficientes están disponibles. 	<p>2 * normal burst</p>

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](#)

Q. ¿Cómo el Committed Access Rate (CAR) o el class-based policing decide a si un paquete conforma o excede 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.

A. Un regulador de tráfico utiliza los valores de ráfaga normal y ráfaga extendida para asegurar que se alcance la configuración CIR. 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 el CAR, publique el **comando show interface rate-limit** de monitorear la explosión actual y de determinarla si el valor visualizado está constantemente cerca del límite (Bc) y de los valores de (Be) del limite extendido.

```
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](#)
- [Switches de la serie del Catalyst G-L3 y WS-X4232-L3 módulos QoS FAQ de la capa 3](#)

Q. ¿Está la independiente de la explosión y del límite de cola de uno a?

A. Sí, la explosión del policer y el límite de cola son separados y independiente de uno a. Usted puede ver el policer como puerta que permita algunos paquetes (o los bytes) y la cola como compartimiento del *límite de cola* del tamaño que sostenga los paquetes admitidos antes de la transmisión en la red. Idealmente, usted quisiera que su compartimiento fuera bastante grande llevar a cabo una *explosión de los bytes/de los paquetes* admitidos por la puerta (policer).

Frame Relay de Calidad de servicio (QoS)

Q. Qué valores debería seleccionar para la Velocidad de información comprometida (CIR), la Ráfaga comprometida (BC), la Ráfaga en exceso (Be), y la CIR mínima (MinCIR).

A. El Control de tráfico de Frame Relay, que usted habilita publicando el **comando frame-relay traffic-shaping**, soporta 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 Frame Relay 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 \(fragmentación, diseño de tráfico y prioridad IP RTP\)](#)

Q. ¿La prioridad que hace cola en la interfaz principal de Frame Relay trabaja en el Cisco IOS 12.1?

A. Las interfaces de Frame Relay soportan los Mecanismos para formar la cola de la interfaz y los Mecanismos para formar la cola del Per-Virtual Circuit (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 Serial0/0.1 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:

```

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

```

Q. ¿El Control de tráfico de Frame Relay (FRTS) trabaja con el Distributed Cisco Express Forwarding (dCEF) y el Class Based Weighted Fair Queueing distribuido (dCBWFQ)?

A. A partir del Cisco IOS 12.1(5)T, solamente la versión distribuida de las características de QoS se soporta en los VIP en las Cisco 7500 Series. 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 modo de transferencia asíncrona (ATM)

Q. ¿Dónde se aplica 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 directivas de servicio del soporte del Cisco IOS 12.2, de las interfaces ATM 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](#)

Q. ¿Qué bytes son contados por el IP a la espera del Clase de Servicio (CoS) del Asynchronous Transfer Mode (ATM)?

A. Los comandos bandwidth y priority configurados en una política de servicio para activar el mecanismo de cola de espera equitativo y ponderado basado en clases (CBWFQ) y la cola de baja latencia (LLQ), respectivamente, utilizan un valor de Kbps que cuenta los mismos bytes suplementarios que cuenta el resultado 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?](#)

Q. ¿Cuántos circuitos virtuales (VCS) pueden soportar una política de servicio simultáneamente?

A. El documento siguiente proporciona a los guías útiles en el número del Asynchronous Transfer Mode (ATM) VCS que puede soportar. Cerca de 200 a 300 circuitos virtuales permanentes VBR-NRT (PVC) se han desplegado con seguridad:

- [Guía de diseño de la 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 perceptiblemente el mayor rendimiento que un VIP2-50.
- Cantidad de memoria de paquete disponible. 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 más alto es el número de PVC activos configurados, el más bajo su velocidad continua de celda (SCR) necesitaría ser, y por lo tanto más corta es la cola requerida por el WRED para actuar encendido el PVC. 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.

Q. ¿Qué hardware de Asynchronous Transfer Mode (ATM) soporta las características (COS, clase de servicio) IP a ATM, incluidas el Class Based Weighted Fair Queueing (CBWFQ) y Low Latency Queueing (LLQ)?

A. El IP to ATM CoS refiere a un conjunto de características que se habilita sobre una base del Per-Virtual Circuit (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 Queueing 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)

Q. ¿Cómo funcionan la Fragmentación y el entrelazado de link (LFI)?

A. El tráfico interactivo tal como Telnet y voz sobre IP es susceptible a la mayor latencia cuando la red procesa los paquetes grandes tales como transferencias del File Transfer Protocol (FTP) sobre 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 \(LLQ/ prioridad IP RTP , LFI, cRTP\)](#)

Q. ¿Qué herramientas puedo utilizar para monitorear el funcionamiento de la voz sobre IP?

A. Cisco ofrece actualmente varias opciones para monitorear el Calidad de Servicio (QoS) en las redes usando las soluciones de la 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. Las herramientas de Agilent (HP) y de NetIQ son para este propósito disponible. Sin embargo, Cisco ofrece las herramientas que proporcionan una cierta idea de la Calidad de voz que usted está experimentando midiendo el retardo, del jitter y de la pérdida del paquete. Para más información, refiérase [con el Cisco Service Assurance Agent y el Internetwork Performance Monitor para manejar la calidad de servicio en las redes de la voz sobre IP](#).

Q. %SW_MGR-3-CM_ERROR_FEATURE_CLASS: Error de la característica del administrador de conexión: Clase SS: (QoS) - instale el error, ignoran.

A. La característica instala el error observado es una conducta esperada cuando una configuración no válida se aplica a una plantilla. Indica que la política de servicio no era aplicado debido a un conflicto. Usted no debe configurar generalmente el shaping en el class-default de la política hija en las correspondencias de la política de jerarquía, en lugar la configura en la política controlante de la interfaz. Este mensaje junto con el traceback se imprime por consiguiente.

Con las directivas basadas sesión, el formar en el class-default tiene que ser hecho solamente en la sub-interfaz o el nivel PVC. El formar en la interfaz física no se soporta. Si la configuración se hace en la interfaz física, el acontecimiento de este mensaje de error es una conducta esperada.

En el caseof LNS, otra razón pudo ser que la política de servicio podría ser provisionado vía el servidor de RADIUS cuando se sacan a colación las sesiones. Publique el **comando show tech** para ver la configuración de servidor de RADIUS y para ver cualquier política de servicio ilegal que esté instalada vía el servidor de RADIUS cuando la sesión sube o agita.

[Información Relacionada](#)

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