

Configuración de la calidad de servicio de LAN para telefonía IP de Cisco

A medida que se incrementa la cantidad de dispositivos y el tráfico de LAN, la segregación de tráfico, el control de acceso y la priorización del tráfico se convierten en los requisitos clave. Los switches administrados Cisco Small Business han mejorado la administración de la red y otras funciones compatibles con el crecimiento de una empresa al brindar mayor control sobre el tráfico de red.

Productos destacados

Este consejo útil describe el uso de un switch administrado Cisco Small Business de la serie 300 (modelo SF 300-48P) con varios puertos de switch con y sin alimentación por Ethernet (PoE, Power over Ethernet). Para obtener información sobre otros switches administrados Cisco de la serie 300, visite: <http://www.cisco.com/cisco/go/300switches>.

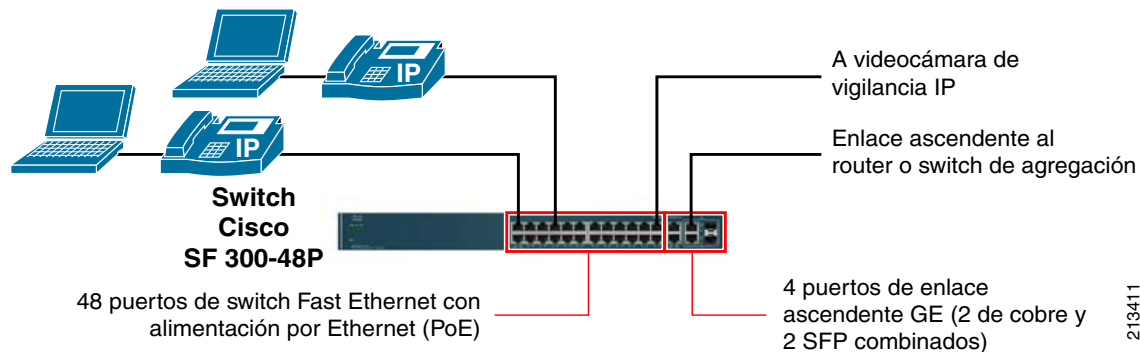
Figura 1 muestra un ejemplo de uso del switch Cisco SF 300-48P en un entorno LAN de una empresa en crecimiento.

¿Por qué calidad de servicio?

La calidad de servicio (QoS) en un dispositivo de red ayuda a ciertas aplicaciones, tales como voz, transmisión de video y otras aplicaciones con limitaciones de tiempo otorgando la prioridad y el ancho de banda adecuados durante una congestión de red. Las llamadas de voz y la transmisión de video pueden entrecortarse y distorsionarse si el tráfico total excede la capacidad de la red y, por ese motivo, el tráfico de voz y video deben recibir el tratamiento prioritario que brinda la clasificación de la calidad de servicio (QoS). Además, la calidad de servicio (QoS) puede brindar cantidades configuradas de ancho de banda al tráfico de otras aplicaciones importantes durante una congestión de la red, para asegurar de ese modo la continuidad comercial durante este tipo de eventos. Pese a que la calidad de servicio (QoS) posee una importancia crucial en un router WAN, un switch LAN también puede congestionarse, aunque con menos frecuencia; por ese motivo, un switch también requiere configuración de calidad de servicio para evitar cualquier degradación posible de la calidad de voz o video.

Este consejo útil describe los pasos para configurar un switch Cisco SF 300-48P con calidad de servicio (QoS) para admitir voz, transmisión de video (p. ej. videovigilancia) y otros tipos de tráfico que se encuentran generalmente en la red de una empresa en crecimiento. (Consulte la Figura 1).

Figura 1 LAN con calidad de servicio (QoS)



213411

Consejos de diseño

Clasificación del tráfico

En las soluciones Cisco Smart Design, la calidad de servicio (QoS) se usa para clasificar el tráfico en diversas clases, para que cada una de ellas pueda configurarse a fin de obtener el tipo de tratamiento de calidad de servicio que requiere. En las soluciones Smart Design, la clase de tráfico de un paquete se identifica mediante el valor de asignación de punto de código de servicios diferenciados (DSCP, Differentiated Services Code Point) o clase de servicio (CoS, class of service) del paquete. DSCP es un campo de 6 bits en el encabezado del paquete IP al que se le puede asignar un valor específico para representar el tipo de tratamiento de calidad de servicio que el tráfico necesita. Puede configurar la calidad de servicio (QoS) para que trate a todos los paquetes que transportan un valor de DSCP específico (o varios valores de DSCP específicos) como una sola clase de tráfico, distinta de las demás. Las clases de tráfico comunes, según se definen en Smart Designs, se muestran en las primeras dos columnas de la [Tabla 1](#).

Si bien los switches reenvían el tráfico basados en el encabezado Ethernet y no en el encabezado IP de un paquete, los switches administrados Cisco Small Business de la serie 300 leen el encabezado IP para clasificar el tráfico según el DSCP que transportan los paquetes IP.

De forma alternativa, un switch también puede clasificar paquetes que coincidan con un valor específico del campo de la clase de tráfico (CoS) de 3 bits que se encuentra en el encabezado Ethernet de los paquetes 802.1q.



Nota Para ciertos tipos de acciones de calidad de servicio, los switches administrados Cisco de la serie 300 permiten también clases de tráfico con base en una lista de control de acceso (ACL, access control list) relacionada.

El código de DSCP *EF* (Expedited Forwarding) significa reenvío acelerado y requiere que los paquetes de esta clase se reenvíen con un grado mínimo de demora, distorsión o pérdida de paquetes. En consecuencia, este DSCP se aplica a la clase de tráfico de voz o video en tiempo real.

Tabla 1 Nombres de las clases de tráfico, DSCP y valores de clase de servicio (CoS)

Descripción del tráfico	Nombre de la clase de tráfico	Código DSCP (valor decimal)	Clase de servicio (CoS)
Tráfico de voz en el portador	Voz	EF (46)	5
Tráfico de transmisión de video, por ejemplo, de una cámara de videovigilancia (opcional)	Transmisión de video	CS4 (32)	4
Tráfico de señalización para voz/video, y así sucesivamente	Señalización	CS3 (24), AF31 (26)	3
Tráfico de control Internetwork; paquetes de control, como routing dinámico generado por dispositivos de red	Control Internetwork	CS6 (48)	6
Tráfico de aplicaciones comerciales transaccionales importantes (opcional)	Datos	CS2 (16), AF21 (18)	2
Paquetes de la unidad de datos de protocolo puente (BPDU) intercambiados entre switches (sólo en switches)	BPDU	N/D	7
El resto del tráfico	Máximo esfuerzo	CS0 (0)	0

Por lo general, los códigos DSCP que comienzan con *AF* (Assured Forwarding o reenvío asegurado) van desde AF11 a AF13, AF21 a AF23, AF31 a AF33, o AF41 a AF43. El reenvío asegurado requiere que se garantice el reenvío del tráfico de esta clase siempre que no exceda cierto límite de ancho de banda configurable. Los dos dígitos siguientes al prefijo *AF* representan la clase de AF y la prioridad de descarte (alta, baja o media). Por ejemplo, en AF31, la clase de AF es 3 y la prioridad de descarte es 1 (prioridad de descarte 1= descarte bajo, 2= descarte medio, 3 = descarte alto).

Si se produce una congestión entre clases de tráfico con diferentes clases de AF (AF1x, AF2x, AF3x y AF4x), se prefiere el reenvío de la clase de tráfico con AF más alto. Sin embargo, si se produce una congestión entre clases de tráfico con la misma clase de AF (por ejemplo, entre AF11, AF12, AF13), primero se descarta el tráfico con prioridad de descarte alto.

Los códigos DSCP que comienzan con *CS* (Class Selector, selector de clase) van de CS0 a CS7 y se crearon para poseer compatibilidad retrospectiva con los sistemas de calidad de servicio (QoS) que utilizan prioridad de IP (en lugar de prioridad de DSCP) para la clasificación del tráfico. Sin embargo, en la práctica, prevalece en cierta medida una combinación de marcación de tráfico basada en CS y AF. Los códigos CS no poseen prioridad de descarte.

Marcación de tráfico

La marcación es el proceso de configurar o cambiar el valor de DSCP o clase de servicio (CoS) de un paquete según el tipo de tráfico. Las soluciones Cisco Smart Design marcan el tráfico de la siguiente manera:

- El tráfico de dispositivos conectados como servidores, almacenamiento conectado a la red (NAS) o cámaras de vigilancia se marcan para conformar la clasificación del tráfico descrita en la sección anterior, si la fuente del tráfico marca el tráfico de forma diferente o si no es confiable.
- El tráfico entrante con DSCP distintos a los incluidos en la lista de la [Tabla 1](#) se marca como DSCP CS0 (máximo esfuerzo).

Configuración de colas de tráfico

La configuración de colas se utiliza para permitir que distintas clases de tráfico compartan ancho de banda y que ciertos tipos de tráfico (como voz y video) reciban tratamiento prioritario respecto de otros. El switch Cisco de la serie 300 posee cuatro colas de hardware. Cada una de estas colas puede definirse como una cola prioritaria para el reenvío acelerado del tráfico ubicado en la cola, o como una cola de operación por turnos compartida (WRR, weighted round robin) que puede compartir ancho de banda con otras colas WRR en una proporción configurada. Además, cada cola puede modelarse de forma individual hasta una determinada velocidad máxima, para que se descarte el tráfico que supere esa velocidad. Tenga en cuenta que un puerto del switch también puede configurarse para limitar el tráfico; en cuyo caso también puede descartar el tráfico que exceda su velocidad configurada. Cada cola de WRR se configura con un "peso" (o un porcentaje del ancho de banda). El switch reenvía el tráfico de estas colas en proporción a sus pesos, lo que asegura un porcentaje mínimo de ancho de banda disponible para cada cola WRR después de brindar servicio a las colas prioritarias.

Este diseño asigna el tráfico a las cuatro colas de hardware de los switches Cisco Sx de la serie 300 según se muestra en [Tabla 2](#) (estos valores pueden modificarse en una implementación en caso de ser necesario)

Tabla 2 Asignaciones de configuración de colas de tráfico

Nombre de la clase de tráfico	DSCP	Cola #	Cola Tipo	Peso WRR	Observaciones
Voz	EF	4	Prioridad		Modelada al 10% de la velocidad de la línea
Transmisión de video	CS4	3	Prioridad		Modelada al 40% de la velocidad de la línea
Señalización	CS3, AF31				
Control Internetwork	CS6				
BPDU	CS7				
Datos	CS2, AF21	2	WRR	1 (33,33%)	Equivalente al 33,33% del ancho de banda restante después de brindar servicio a las dos colas prioritarias
Máximo esfuerzo	CS0	1	WRR	2 (66,67%)	66,67% del ancho de banda restante

Para el diseño descrito en la [Tabla 2](#), primero se brinda servicio al tráfico de la cola 4 (la cola prioritaria con la prioridad más alta). Cuando la cola 4 está vacía, se atiende el tráfico de la cola 3 (la cola prioritaria con menor prioridad). Solamente cuando estas dos colas estén vacías, el ancho de banda restante se compartirá entre las colas WRR en proporción a sus pesos. Los pesos mostrados anteriormente brindan el 33,67% del ancho de banda restante a la cola 1 y el 66,67% a la cola 2.

Modelado y política de colas prioritarias

Las colas prioritarias no poseen ningún límite de ancho de banda en la configuración predeterminada; por ese motivo, es posible que utilicen demasiado ancho de banda y priven de su uso al resto de las colas. En consecuencia, este diseño impone un límite de velocidad en cada cola prioritaria. Pese a que las velocidades límite de las colas prioritarias individuales pueden variar según la implementación, una recomendación general es limitar el tráfico prioritario total a través de todas las interfaces para que no supere el 50% del ancho de banda de cada interfaz. Este diseño modela el tráfico de voz y video para que utilice entre el 10% y el 40% del ancho de banda de la interfaz, ya que se asume que el tráfico de voz y video real esperado será mucho menor que estas velocidades modeladas.

Elusión de la congestión de TCP (opcional)

La función para eludir la congestión de TCP mitiga el efecto de la sincronización de TCP que produce una subutilización de la red. Esta función ayuda a mejorar el rendimiento de la red para el tráfico basado en TCP, al descartar paquetes al azar antes de que se produzca la congestión de la red.

Sin esta función, cuando se llena una cola se descartarán todos los paquetes entrantes adicionales. Este crecimiento repentino de paquetes descartados puede afectar a una gran cantidad de aplicaciones TCP. Todas estas aplicaciones se verán forzadas de forma simultánea a reducir drásticamente su velocidad de envío, y luego a aumentarla gradualmente de nuevo. Cuando la velocidad de envío en aumento supere un cierto límite que llene las colas, la cola descartará nuevamente todos los paquetes entrantes. Esto producirá una secuencia repetida de sobrecarga y subutilización de la red.

La función para eludir la congestión de TCP mitiga este problema al descartar paquetes al azar de las colas mucho antes de que estas se llenen. No espera que se llene la cola para descartar todo el tráfico entrante. La función de elusión de la congestión de TCP disemina los paquetes descartados a lo largo del tiempo y, de ese modo, evita descartar paquetes simultáneamente de una gran cantidad de flujos TCP.

En Cisco Smart Designs, esta función es esencial para el router WAN, pero es opcional en los switches LAN, debido a que la configuración en el router WAN también cubre el tráfico que fluye a través de la LAN. Sin embargo, si el router WAN no admite la función para evitar la congestión TCP, no podrá activarse en los switches LAN.

Consejos de configuración

La configuración descrita en esta sección se establece para cada uno de los puertos de un switch Cisco de la serie 300 (implementado como switch de acceso o como switch de agregación en una topología Cisco Smart Design) con funciones de colas para admitir las clases de tráfico que se definieron anteriormente. Además, esta configuración demuestra cómo configurar un puerto para limitar y marcar el tráfico entrante desde un dispositivo conectado al switch.

Las configuraciones no guardadas se perderán al reiniciar el switch, por eso se aconseja guardarlas con frecuencia en el archivo de configuración de inicio al realizar ajustes en el switch. Para eso debe completar estos pasos:

Paso 1 Haga clic en **Administration (Administración) > File Management (Administración de archivos) > Copy/Save Configuration (Copiar/Guardar configuración)**.

Se abrirá la página de copiar/guardar configuración.

Paso 2 Seleccione el nombre del archivo de origen que se copiará como *Running configuration (Configuración en ejecución)*.

Paso 3 Seleccione el nombre del archivo de destino como *Startup configuration (Configuración de inicio)*.

Paso 4 Haga clic en **Apply (Aplicar)**. Se guardará el archivo de configuración.

Modos básico y avanzado de calidad de servicio

Los switches Cisco Sx300 se pueden configurar para funcionar en modo de calidad de servicio (QoS) básico o avanzado. El modo de calidad de servicio (QoS) básico admite la funcionalidad de configuración de colas requerida (prioridad y configuración de colas WRR) y el modelado de colas prioritarias. Sin embargo, este diseño usa el modo de calidad de servicio (QoS) avanzado, ya que se requiere este modo para aplicar políticas/marcar el tráfico entrante desde los puertos del switch específicos. Es común marcar todo el tráfico desde fuentes como servidores, NAS y videocámaras, si estos dispositivos no marcan el tráfico, o si no son confiables (por no encontrarse dentro del control administrativo del administrador de la red o porque un atacante podría explotar sus vulnerabilidades). El modo de calidad de servicio (QoS) avanzado le permite especificar el tráfico para esa aplicación de políticas/marcación con gran granularidad; puede especificar las subredes/direcciones IP de origen/destino, sus protocolos TCP/UDP y sus puertos. Si no se requiere este tipo de aplicación de políticas/marcación de los flujos de tráfico en una implementación, el modo de calidad de servicio (QoS) básico es apropiado.

Los siguientes pasos de configuración presuponen que puede acceder a la pantalla de administración web del switch Cisco SF 300-48P. También se presupone que se han creado la VLAN de datos y la VLAN de voz en el switch y en cualquier otro lugar de la red según sea necesario, y que el switch está conectado con el router WAN, según se muestra en la Figura 1.

Para configurar la calidad de servicio (QoS) de la LAN, siga estos pasos:

Paso 1 Seleccione **Quality of Service (Calidad de Servicio) > General (General) > QoS Properties (Propiedades de calidad de servicio)**.

Aparecerá la pantalla de propiedades de calidad de servicio, según se muestra en la Figura 2.

Figura 2 Pantalla de propiedades de la calidad de servicio

Entry No.	Interface	Default CoS
1	e1	0
2	e2	0
3	e3	0
4	e4	0
5	e5	0

Paso 2 En el campo QoS Mode (Modo de calidad de servicio), seleccione *Advanced (Avanzado)* y haga clic en **Apply (Aplicar)**.

En la tabla de configuración de la interfaz de la clase de servicio (CoS), verifique que la CoS predeterminada para todos los puertos del switch sea 0.

Paso 3 Seleccione **Quality of Service (Calidad de servicio) > General (General) > QoS Properties (Propiedades de calidad de servicio)**.

Aparecerá la pantalla de configuración de colas, según se muestra en la Figura 3.

Figura 3 Pantalla de configuración de colas

Queue	Scheduling Method	WRR Weight	% of WRR Bandwidth
1	Strict Priority	1	33.33
2	WRR	2	66.67
3	WRR	4	
4	WRR	8	

Queue 1 has the lowest priority, queue 4 has the highest priority.

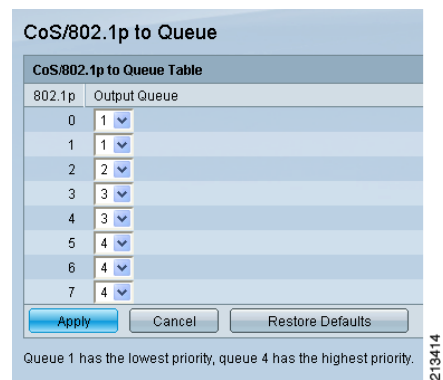
Paso 4 En la pantalla de configuración de colas, configure las colas 1 y 2 como colas WRR con pesos 1 y 2; configure las colas 3 y 4 como colas prioritarias y haga clic en **Apply** (Aplicar).

La cola 4 es para voz y la 3 para transmisión de video (si se implementan). Además, la cola 3 transporta tráfico de señalización. Tenga en cuenta que configurar esas colas prioritarias para voz y video es correcto cuando no se implementan voz ni video, ya que las colas prioritarias no reservan ancho de banda, y el resto de las clases de tráfico absorben el tráfico no utilizado.

Paso 5 Seleccione **Quality of Service (Calidad de servicio) > General (General) > QoS Properties (Propiedades de calidad de servicio) > QoS/802.1p to Queue (De QoS/802.1p a cola)**.

Aparecerá la pantalla de CoS/802.1P a cola, según se muestra en Figura 4.

Figura 4 Pantalla de CoS/802.1P a cola

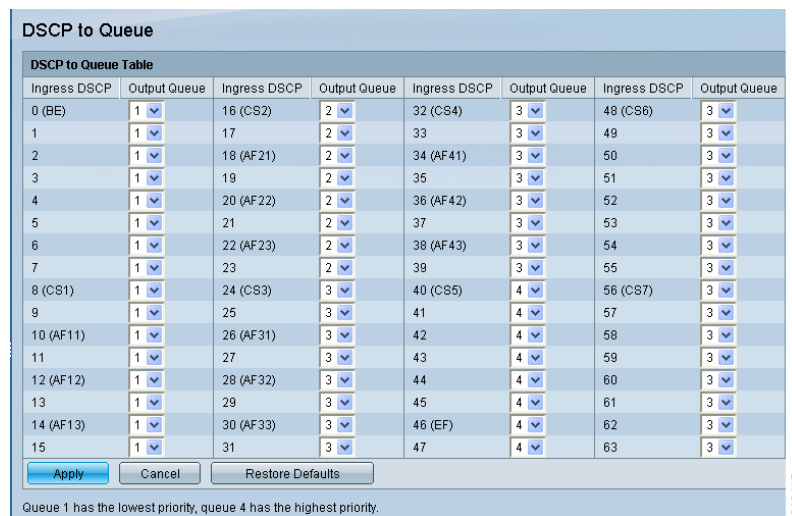


Paso 6 Verifique que los valores de la clase de servicio (CoS) estén asignados a las colas, como en la Figura 4, o cambie la asignación de forma acorde. A continuación, haga clic en **Apply** (Aplicar).

Paso 7 Seleccione **Quality of Service (Calidad de servicio) > General (General) > QoS Properties (Propiedades de calidad de servicio) > DSCP to Queue (De DSCP a cola)**.

Aparecerá la pantalla de DSCP a cola, según se muestra en la Figura 5.

Figura 5 Pantalla de DSCP a cola

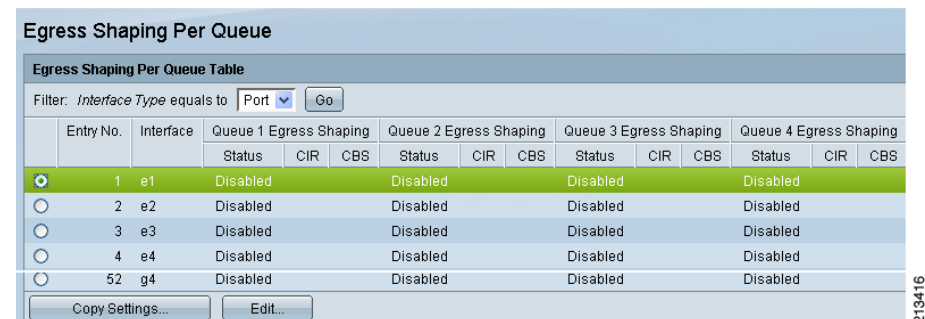


Paso 8 Verifique que los DSCP estén asignados a las colas, como en la Figura 5, o cambie la asignación de forma acorde. A continuación, haga clic en **Apply** (Aplicar).

Paso 9 Seleccione **Quality of Service (Calidad de servicio) > General (General) > QoS Properties (Propiedades de calidad de servicio) > Egress shaping per Queue (Modelado saliente por cola)**.

Aparecerá la pantalla de modelado saliente por cola, según se muestra en la Figura 6.

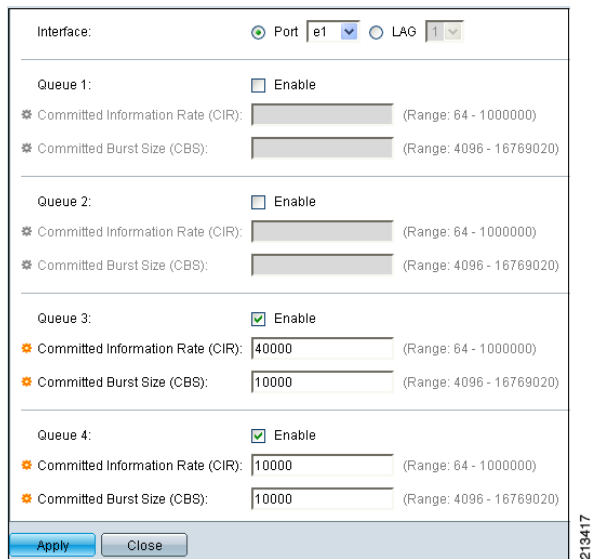
Figura 6 Pantalla de modelado saliente por cola



Paso 10 En la pantalla de modelado saliente por cola, seleccione el primer puerto E1, como en la Figura 6 y haga clic en **Edit** (Editar).

Aparecerá la pantalla emergente que se muestra en la Figura 7.

Figura 7 Pantalla emergente



Paso 11 En la pantalla emergente que se muestra en la Figura 7, siga estos pasos:

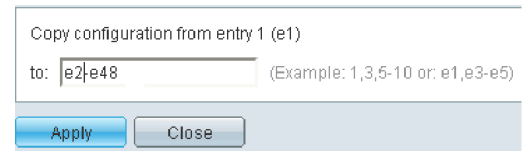
- Haga clic en los botones de selección para activar el modelado en las colas 3 y 4.
- Ingrese los valores según se muestran en la Figura 7 para modelar la cola 3 con CIR 40000 Kbps y con CBS 10000.
- Modele la cola 4 con CIR 10000 Kbps y CBS 10000.
- Haga clic en **Apply** (Aplicar).
- Cuando aparezca el mensaje "Success" (Resultado satisfactorio), haga clic en **Close** (Cerrar).

Se cerrará la pantalla emergente y aparecerá la pantalla de modelado saliente por cola. Verifique que el puerto E1 ahora muestre los valores de modelado ingresados en la pantalla de modelado saliente por cola.

Paso 12 En la pantalla de configuración saliente por cola, haga clic en **Copy Settings** (Copiar configuración) para copiar la configuración de modelado del puerto E1 al resto de los puertos del switch.

En la pantalla emergente, ingrese el rango de los puertos Fast Ethernet del switch, según se muestran en la Figura 8 y haga clic en **Apply** (Aplicar).

Figura 8 Pantalla emergente de copiar configuración



Se cerrará la pantalla emergente de copiar configuración. Verifique que la pantalla de modelado saliente por cola ahora muestre los valores de modelado de todos los puertos del switch.

Repita este paso para los puertos Gigabit Ethernet (de G1 a G4). Use CIR=400000 y CBS=100000 para la cola 3, y CIR=100000 y CBS=100000 para la 4.

Opcional: este paso y los siguientes son necesarios si desea aplicar políticas y/o marcar el tráfico entrante desde un dispositivo conectado al switch. Este ejemplo aplica políticas al tráfico desde una cámara de videovigilancia (dirección IP 10.1.20.5) a 500 Kbps. El tráfico que supera los 500 Kbps se descartará, mientras que el tráfico dentro de la velocidad límite se marcará con DSCP CS4.

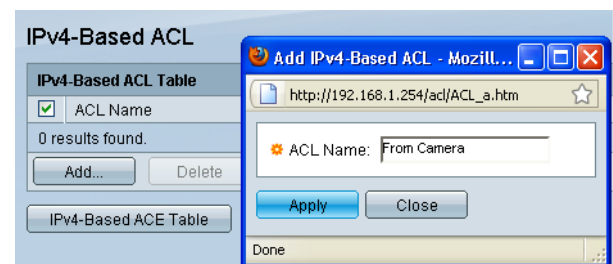
Este procedimiento incluye los siguientes pasos principales:

- Crear una clase de tráfico mediante una lista de control de acceso (ACL) que coincida con la dirección IP de la videocámara
- Crear una tabla de políticas de calidad de servicio (QoS) que contenga una o más asignaciones de clases de políticas
- Crear una asignación de clases de políticas que especifique las acciones de aplicación de políticas/marcación que se deben realizar en la clase de tráfico específica
- Adjuntar la asignación de clases de políticas al puerto del switch que está conectado a la videocámara

Paso 13 Para crear una ACL que identifique el tráfico de la cámara, seleccione **Access Control (Control de acceso) > IPv4 based ACL (ACL basada en IPv4)**.

Aparecerá la pantalla ACL basada en IPv4, según se muestra en la Figura 9.

Figura 9 Pantalla ACL basada en IPv4



Paso 14 Haga clic en el cuadro de selección **ACL Name** (Nombre de ACL) y haga clic en **Add** (Agregar).

Aparecerá la pantalla emergente de agregar ACL basada en IPv4, según se muestra en la Figura 9.

Paso 15 Ingrese el nombre de la ACL (por ejemplo, *From Camera*) (Desde la cámara) y haga clic en **Apply** (Aplicar).

Desaparecerá la pantalla emergente de ingreso de datos y, en su lugar, aparecerán los datos ingresados en la pantalla de ACL basada en IPv4.

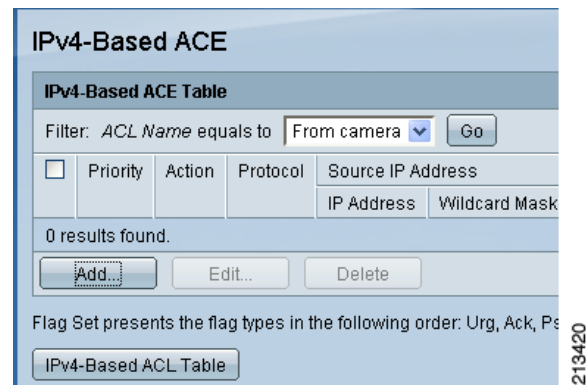
Paso 16 Haga clic en el botón **IPv4-Based ACE Table** (Tabla ACE basada en IPv4).

Aparecerá la pantalla ACE basada en IPv4, (mostrada parcialmente en la Figura 10).



Nota Una ACL consiste de una o más expresiones de control de acceso (ACE, access control expressions).

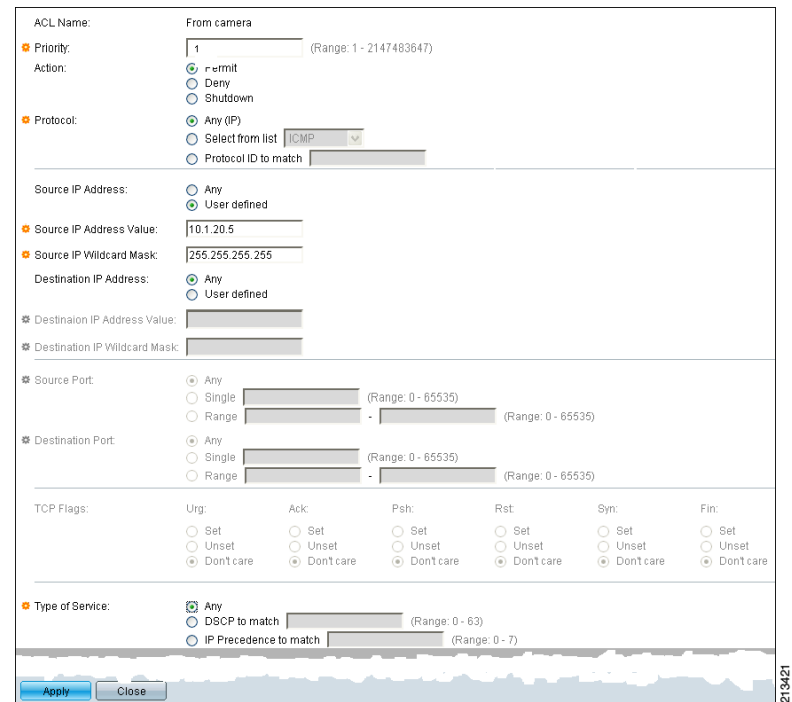
Figura 10 Pantalla de agregar ACE basada en IPv4



Paso 17 Haga clic en **Add** (Agregar).

Aparecerá la pantalla mostrada parcialmente en Figura 11 para ingresar detalles de las entradas de control de acceso (ACE) que deben incluirse en la ACL *From Camera* (Desde la cámara). Si lo desea, puede incluir varias ACE.

Figura 11 Ingreso de los detalles de la ACE



Paso 18 Ingrese los datos de la ACE de la siguiente manera:

- Prioridad: 1 (la prioridad determina el orden en el cual se evalúan las diversas ACE de una ACL, si existe alguna)
- La dirección IP de origen, al igual que la de la cámara: 10.1.20.5
- Máscara comodín de la IP de origen: 255.255.255.255

Paso 19 Haga clic en **Apply** (Aplicar).

Se creará la ACL con la ACE individual que acaba de ingresar.

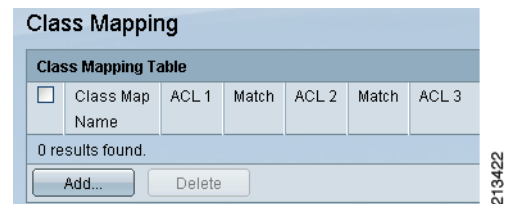


Nota De forma adicional, puede especificar dirección IP/subred de destino, protocolo, y puerto TCP/UCP en la entrada ACE, según corresponda para cualquier ACE.

Paso 20 Seleccione **Quality of Service (Calidad de servicio) > QoS Advanced Mode (Modo de calidad de servicio avanzado) > Class Mapping (Asignación de clases)**.

Aparecerá la pantalla de asignación de clases, según se muestra en la [Figura 12](#). Una asignación de clase define la regla para identificar la clase de tráfico (en este caso, utiliza una ACL predefinida para que coincida con el tráfico de la videocámara, según se muestra a continuación).

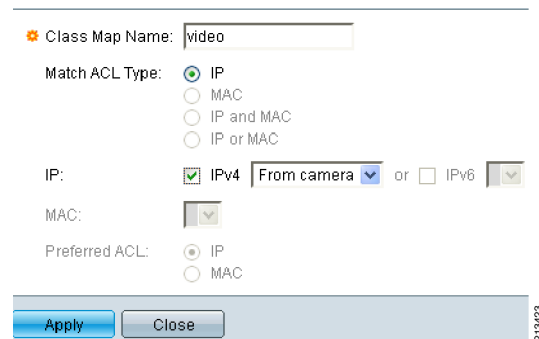
Figura 12 Pantalla de asignación de clases



Paso 21 Haga clic en **Add** (Agregar) para agregar una nueva asignación de clase mediante la ACL recientemente creada.

Aparecerá la pantalla emergente para crear una nueva asignación de clase, según se muestra en la [Figura 13](#).

Figura 13 Creación de una nueva asignación de clase



Paso 22 En la pantalla emergente, siga estos pasos:

- En el campo Class Map Name (Nombre de asignación de clase), ingrese *video*.
- En el campo Match ACL Type (Coincidencia de tipo de ACL), marque **IP**.
- En el campo IP, marque **IPv4**.
- En la lista desplegable, seleccione la ACL **From Camera** (Desde la cámara).
- Haga clic en **Apply** (Aplicar) y verifique que la operación fue satisfactoria.

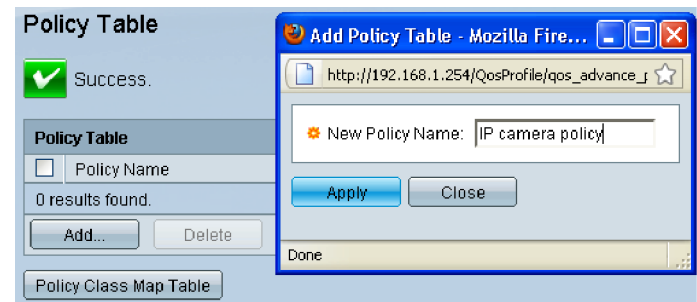
Paso 23 Seleccione **Quality of Service (Calidad de servicio) > QoS Advanced Mode (Modo de calidad de servicio avanzado) > Policy Table (Tabla de políticas)**.

Aparecerá la pantalla de tabla de políticas.

Paso 24 Haga clic en **Add** (Agregar) para agregar una política nueva.

Aparecerá la pantalla emergente que se muestra en la [Figura 14](#).

Figura 14 Pantalla de tabla de políticas



Paso 25 Ingrese el nombre de la tabla de políticas (*Política de cámaras IP*, en este ejemplo).

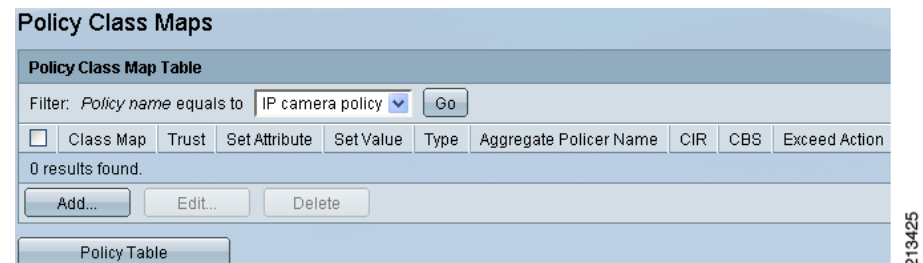
Paso 26 Haga clic en **Apply** (Aplicar).

Desaparecerá la pantalla emergente y aparecerá "Success" (Resultado satisfactorio) en la pantalla de tabla de políticas, junto con el nombre de la política creada recientemente.

Paso 27 Para agregar la política de tráfico concreta (aplicación de políticas, marcación, y así sucesivamente) y que se incluya en la tabla de políticas recién creada, seleccione **Quality of Service (Calidad de servicio) > QoS Advanced Mode (Modo de calidad de servicio avanzado) > Policy Class Map (Asignación de clase de políticas)**.

Aparecerá la pantalla de asignaciones de clase de políticas, según se muestra en la [Figura 15](#).

Figura 15 Pantalla de asignaciones de clase de políticas



Paso 28 En el menú desplegable, seleccione el nombre de la política (*Política de cámara IP*) y haga clic en **Add** (Agregar).

Aparecerá la pantalla que se muestra en la [Figura 16](#) para agregar las acciones de aplicación de políticas/marcación que se deben seguir que coincidirán con esta política.

Figura 16 Incorporación de las acciones de aplicación de políticas/marcación

Policy Name: IP camera policy

Class Map Name: video

Action Type: None Trust CoS/802.1p, DSCP Set DSCP New Value: 32 (Range: 0-63)

Police Type: None Single Aggregate

Aggregate Policer: [Dropdown]

Ingress Committed Information Rate (CIR): 1000 kbits/sec. (Range: 100 - 1000000)

Ingress Committed Burst Size (CBS): 20000 Bytes (Range: 3000 - 19173960)

Exceed Action: None Drop Out of Profile DSCP

Apply Close

Paso 29 En la pantalla que se muestra en la Figura 16, siga estos pasos:

- En la lista desplegable, seleccione la asignación de clase **video**.
- Haga clic en el botón de opción para seleccionar Set operation (Configurar operación) y seleccione **DSCP** en la lista desplegable correspondiente.
- En el campo New Value (Valor nuevo), ingrese **32** (es decir, DSCP CS4). Esto configurará el DSCP como CS4 para todo el tráfico que coincida con la asignación de clase *video*.
- Si se presume que desea aplicar políticas del tráfico desde la cámara IP a 1 Mbps y descartar el tráfico excedente, ingrese los valores **1000 Kbps** en el campo Ingress Committed Information Rate (Velocidad de información comprometida de ingreso) y **20000** en el campo Ingress Committed Burst Size (Tamaño de ráfagas comprometidas de ingreso).
- En el campo Exceed Action (Acción excedente), marque **Drop** (Descartar).
- Haga clic en **Apply** (Aplicar).
- Verifique que aparezca el mensaje "Success" (Resultado satisfactorio) para indicar que la operación fue exitosa.
- Haga clic en **Close** (Cerrar) para cerrar la pantalla emergente.

Paso 30 Seleccione **Quality of Service (Calidad de servicio) > QoS Advanced Mode (Modo de calidad de servicio avanzado) > Policy Binding (Entrelazado de políticas)**.

Aparecerá la pantalla de entrelazado de políticas, según se muestra en la Figura 17.

Figura 17 Pantalla de entrelazado de políticas

Policy Binding

Filter: Policy Name equals to IP camera policy

AND Interface Type equals to Port Go

e1	e2	e3	e4	e5	e6	e7	e8	e9	e10	e11	e12
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e25	e26	e27	e28	e29	e30	e31	e32	e33	e34	e35	e36
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
g1	g2	g3	g4								
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>								

Apply Cancel

Policy Binding Table

Filter: Interface Type equals to Port

Interface	Policy Name
e1	

Esto se utiliza para aplicar la política creada recientemente al puerto del switch conectado a la cámara de videovigilancia IP (puerto del switch *E35*, en este ejemplo).

Paso 31 En la pantalla de entrelazado de políticas, siga estos pasos:

- En la lista desplegable de políticas, seleccione el nombre (*Política de cámara IP*) para aplicar los cambios.
- En la lista desplegable, seleccione el tipo de interfaz como *port* (puerto).
- Haga clic en el cuadro de selección para indicar el puerto del switch (*E35*, en este ejemplo) donde se aplicará la *Política de cámara IP* (también puede aplicar una política individual en más de un puerto del switch, si es necesario).
- Haga clic en **Apply** (Aplicar).

Como confirmación, aparecerá el mensaje "Success" (Resultado satisfactorio) en la pantalla, y también aparecerá el nombre de la política (*Política de cámara IP*) junto al puerto *E35* en la tabla de entrelazado de políticas.

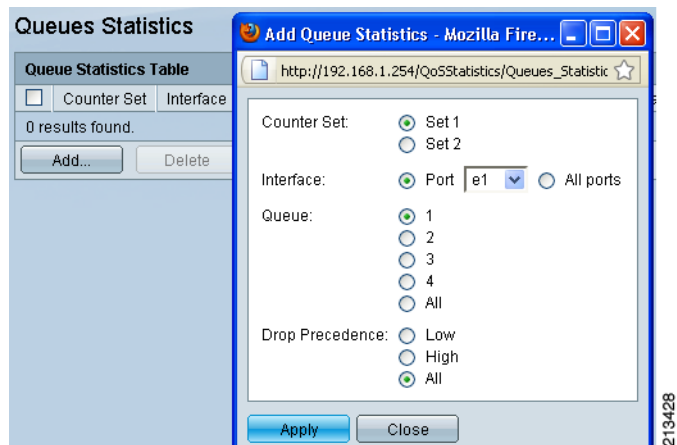
Con este paso se completa la configuración de la calidad de servicio (QoS) en el switch.

Verificación

Paso 1 Seleccione **Quality of Service (Calidad de servicio) > QoS Statistics (Estadísticas de calidad de servicio) > Queues Statistics (Estadísticas de colas)**.

Aparecerá la pantalla de estadísticas de colas, que le permite configurar un máximo de dos conjuntos de contadores de paquetes, según se muestra en la Figura 18.

Figura 18 Pantalla de estadísticas de colas



Paso 2 Haga clic en **Add (Agregar)** para agregar el primer conjunto de contadores.

Aparecerá la pantalla de agregar estadísticas de colas, según se muestra en la Figura 18.

Paso 3 En la pantalla emergente **Agregar estadísticas de colas**, siga estos pasos:

- Ingrese los valores seleccionados de puerto del switch, cola y prioridad de descarte para las estadísticas.
- Haga clic en **Apply (Aplicar)**.
- Verifique que aparezca el mensaje "Success" (Resultado satisfactorio) para indicar que la operación fue exitosa.
- Haga clic en **Close (Cerrar)**.

Aparecerán los conteos de paquetes reales, según se muestra en la Figura 19.

Figura 19 Verificación de los conteos de paquetes reales

Queues Statistics						
Queue Statistics Table						
<input type="checkbox"/>	Counter Set	Interface	Queue	Drop Precedence	Total packets	Tail Drop packets
<input type="checkbox"/>	1	e1	1	All	4815	0
<input type="checkbox"/>	2	e1	4	All	1386	0

Buttons: Add..., Delete, Clear Counters

Puede borrar los contadores si marca el botón **Clear Counters** (Borrar contadores). Verifique periódicamente que el aumento en la cantidad de paquetes en las diversas colas se deba a la configuración de la calidad de servicio (QoS).

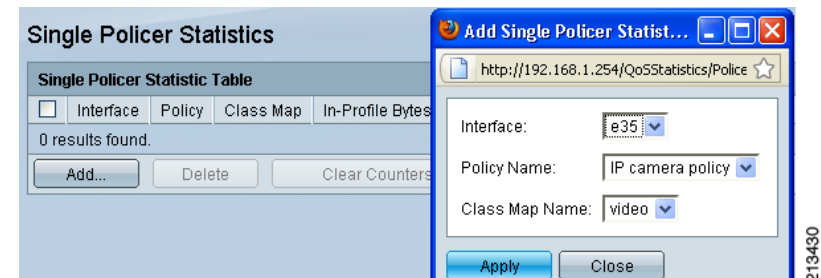
Paso 4 Seleccione **Quality of Service (Calidad de servicio) > QoS Statistics (Estadísticas de calidad de servicio) > Single Policer Statistics (Estadísticas de vigilantes individuales)**.

Aparecerá la pantalla de estadísticas de vigilantes individuales, que le permite especificar puerto, nombre de la política y demás datos, hasta completar las variables de las que se requieren estadísticas.

Paso 5 Haga clic en **Add (Agregar)**.

Aparecerá la pantalla emergente para agregar vigilante individual, según se muestra en la Figura 20.

Figura 20 Pantalla emergente para agregar vigilante individual



Paso 6 Ingrese el nombre del puerto del switch (**E35**), el nombre de la política y el nombre de la asignación de clase de su interés y, a continuación, haga clic en **Apply (Aplicar)**.

Aparecerán las estadísticas de aplicaciones de políticas, como se muestra en la Figura 21.

Figura 21 Pantalla de estadísticas de vigilante individual

Interface	Policy	Class Map	In-Profile Bytes	Out-of-Profile Bytes	
<input type="checkbox"/>	e35	IP camera policy	video	0	0

Para comprobar si las políticas funcionan o no, configure temporalmente la velocidad límite con un valor bajo y verifique que el tráfico excedente que supera la velocidad límite se cuente como bytes fuera de perfil.

Resumen

Este consejo útil define los diversos tipos de funciones de la calidad de servicio (QoS) que pueden utilizarse dentro de una red, con especial énfasis en la red LAN. Cuando se configura la calidad de servicio (QoS) dentro de los switches Cisco Small Business de la serie 300, puede facilitarse el tratamiento de apropiado de la calidad de servicio para las clases de tráfico de Cisco Smart Design. El switch administrado Cisco de la serie 300 admite funcionalidades de calidad de servicio (QoS) adicionales que pueden utilizarse en caso de ser necesarias.

Para obtener más información sobre la configuración de los switches administrados Cisco de la serie 300, consulte la Guía del administrador en la siguiente dirección URL: http://www.cisco.com/en/US/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, el logotipo de Cisco, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (diseño), Flip Ultra, Flip Video, Flip Video (diseño), Instant Broadband y Welcome to the Human Network son marcas comerciales; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (diseño), Cisco:Financed (estilo), Cisco Store, Flip Gift Card y One Million Acts of Green son marcas de servicio; y Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, el logotipo de Cisco Certified Internetwork Expert, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, el logotipo de Cisco Systems, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, el logotipo de IronPort, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (diseño), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, y el logotipo de WebEx son marcas registradas de Cisco o de sus filiales en Estados Unidos y en otros países.

Todas las demás marcas comerciales mencionadas en este documento o en el sitio web pertenecen a sus respectivos propietarios. El uso de la palabra "partner" no implica la existencia de una asociación entre Cisco y cualquier otra compañía. (1002R)

Las direcciones de Protocolo de Internet (IP) utilizadas en este documento no son direcciones reales. Los ejemplos, los resultados en pantalla de los comandos y las cifras incluidos en este documento se muestran solamente con fines ilustrativos. Cualquier uso de direcciones IP reales en los ejemplos es accidental e imprevisto.

©2010 Cisco Systems, Inc. Todos los derechos reservados.

