Productos Cisco Small Business: Configuración de la calidad de servicio de LAN para la 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 el otorgamiento de prioridad al tráfico se convierten en requisitos clave. Los switches administrados Cisco Small Business han mejorado la administración de redes y otras funciones compatibles con el crecimiento de una empresa al brindar mayor control sobre el tráfico de red.

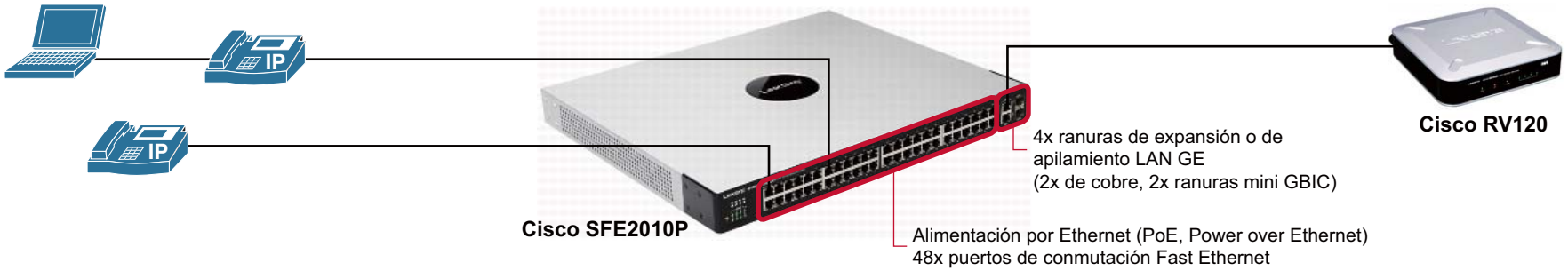
Productos destacados

Switches Ethernet administrados Cisco Small Business con PoE:

SFE2010P, SFE2000P, SFE1000P, SGE2010P, SGE2000P, SRW2024P, SRW2008MP, SRW2008P, SRW248G4P, SRW224G4P, SRW208MP, SRW208P

El switch SFE2010P se utiliza como ejemplo para este consejo útil. Para obtener detalles sobre un switch con PoE específica, visite: http://www.cisco.com/en/US/products/ps9967/index.html

Figura 1 LAN preparada para transmisión de voz



Consejos de diseño

Una VLAN es un mecanismo que separa diferentes tipos de tráfico al crear varios dominios de difusión dentro de una sola red física, que puede extenderse a lo largo de varios dispositivos. Para garantizar que el tráfico de voz reciba la calidad de servicio necesaria, una VLAN de voz debe incluir las funciones descritas en esta sección:

Red de área local virtual (VLAN): una VLAN es una red virtual que segmenta diferentes tipos de tráfico y usuarios, y que se identifica mediante un ID de VLAN de puerto (PVID, port VLAN ID) como 1, 10, 12 y así sucesivamente. Al agregar voz a una red, debe agregarse una VLAN separada a la red para el tráfico de voz. Entre las funciones que ayudan a garantizar una mayor calidad de la red, lo que es un requisito de una VLAN de voz, se encuentran las siguientes:

- **Port Fast**: permite que un dispositivo, como un teléfono IP, se conecte y desconecte rápidamente de la red.
- **Protección de Unidad de datos de protocolo puente (BPDU, Bridge Protocol Data Unit)**: ayuda a proteger la red al evitar que los atacantes pasen de una VLAN a otra sin autorización.
- **Control de tormentas**: ayuda a evitar tormentas, que son estallidos de tráfico poco usuales que pueden dañar el rendimiento de la red y alterar los procesos comerciales.
- **Seguridad de puertos**: ayuda a proteger la red contra amenazas, incluidos virus y gusanos, al evitar que los usuarios agreguen dispositivos no autorizados a la red.

Calidad de servicio (QoS, Quality of Service): ayuda a garantizar que las aplicaciones sensibles, como la voz, transiten la red con interrupciones limitadas a fin de mantener la calidad de una llamada de voz. A continuación se enumeran funciones que deben activarse o personalizarse al configurar la calidad de servicio (QoS) en la red:

- **Clase de servicio (CoS, Class of Service)**: se utiliza dentro de una red Ethernet para establecer la prioridad del tráfico que atraviesa la red y para ayudar a garantizar la calidad de las llamadas de voz.
- **Clasificación del Punto de código de servicios diferenciados (DSCP, Differentiated Service Code Point)**: ayuda a garantizar la calidad de voz en toda la red mediante la clasificación de paquetes y la prestación de un servicio garantizado para paquetes específicos, como los paquetes de voz.
- **Lista de control de acceso (ACL, Access Control List)**: se utiliza para crear políticas de seguridad para una empresa, como la limitación del acceso a servidores específicos y la prevención del acceso no autorizado desde Internet pública.
- **Procesamiento de prioridad (configuración de colas y planificación)**: ayuda a garantizar que el tráfico sensible, como las llamadas de voz, atraviese la red en primer lugar mediante la administración de la prioridad del tráfico.

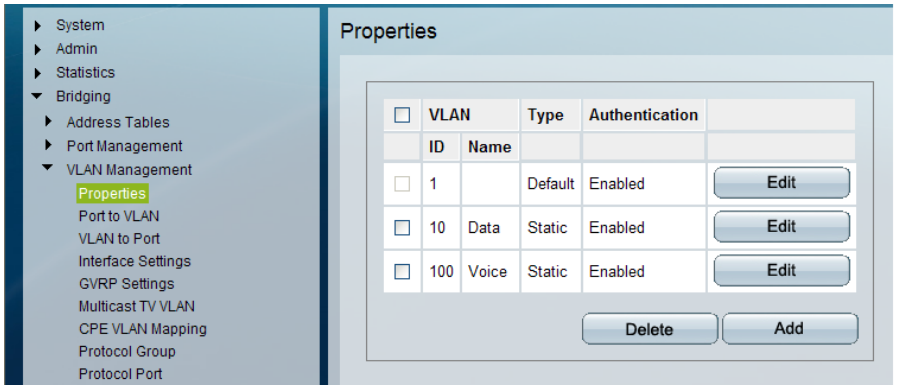
Consejos de configuración

Los siguientes pasos dan por sentado que puede acceder a la administración basada en web para la serie Cisco Small Business Pro de switches administrados. También se da por sentado que se han creado las VLAN de datos y voz en el router conectado al puerto de expansión/enlace ascendente del switch administrado, como se muestra en la Figura 1.

Configuración de la VLAN

Paso 1 Seleccione **Bridging (Puente) > VLAN Management (Administración de VLAN) > Properties (Propiedades)** y cree la VLAN 10 de datos y la VLAN 100 de voz.

Figura 2 Propiedades



Paso 2 Seleccione **Bridging (Puente) > VLAN Management (Administración de VLAN) > Interface Settings (Configuración de interfaz)**.

De forma predeterminada, todos los puertos están en modo Access (Acceso) con la PVID 1. Esto significa que los puertos están configurados para que una estación de trabajo se conecte en ID 1 de la VLAN de puerto. Al conectarse a un teléfono IP esto se debe modificar, ya que el puerto de LAN en el teléfono IP puede utilizarse para conectar una estación de trabajo a la red LAN.

1. Cambie el modo del puerto de enlace ascendente/expansión a Trunk (enlace troncal) con PVID 1.

Este puerto se utiliza para conectarse al router.

2. Cambie los puertos que se usarían para conectarse a los teléfonos IP Cisco a enlaces troncales con PVID 10.

Esto modifica la PVID de datos de 1 a 10.

Figura 3 Configuración de la interfaz

Paso 3 Seleccione **Bridging (Puente) > VLAN Management (Administración de VLAN) > Port to VLAN (De puerto a VLAN)**.

Para cada ID de VLAN, el estado de la interfaz puede ser Untagged (sin etiquetas), Tagged (con etiquetas) o Excluded (excluido). La PVID es la ID de VLAN nativa, que es la VLAN sin etiquetas.

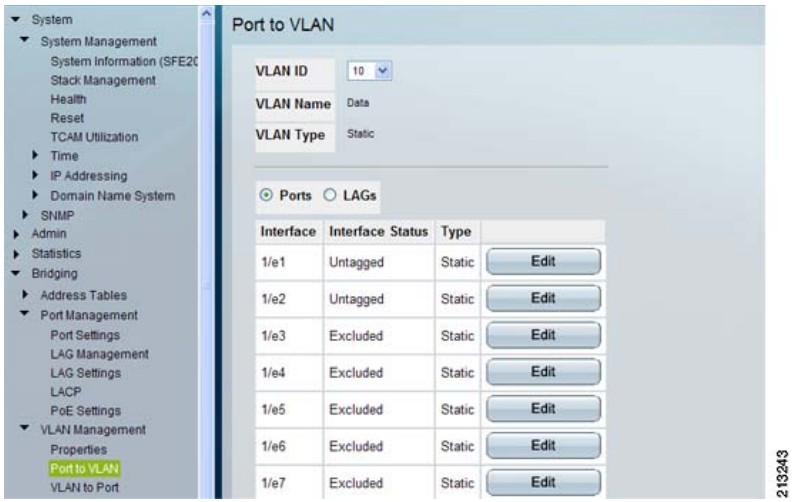
1. Edite el puerto de enlace ascendente con PVID 1 y etiquete las VLAN 10 y 100.

Esto agrega las VLAN requeridas para datos y voz.

2. Edite todos los puertos con PVID 10 que se conectan a los teléfonos IP Cisco y etiquete VLAN 100.

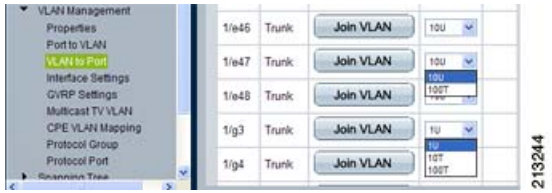
De esta forma se agrega la VLAN de voz. La VLAN 1 está excluida de los puertos utilizados para los teléfonos IP.

Figura 4 De puerto a VLAN



Paso 4 Seleccione **Bridging (Puente) > VLAN Management (Administración de VLAN) > VLAN to Port (De VLAN a puerto)** y verifique la asignación de la VLAN.

Figura 5 De VLAN a puerto



Configuración de la seguridad del switch

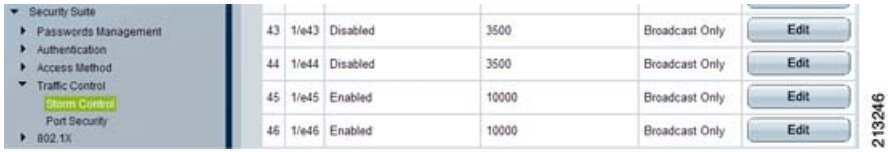
Paso 1 Seleccione **Bridging (Puente) > Spanning tree (Árbol de expansión) > Interface setting (Configuración de interfaz)** y active las opciones BPDU Guard (protección de BPDU) y Port-Fast.

Como se mencionó anteriormente, la protección de BDPU evita que se agreguen dispositivos no autorizados, mientras que Port-Fast permite que los dispositivos se conecten y desconecten rápidamente del puerto.

Figura 6 Spanning tree (Árbol de expansión) > Interface setting (Configuración de interfaz)

Paso 2 Seleccione **Security suite (Conjunto de seguridad) > Traffic control (Control de tráfico) > Storm control (Control de tormentas)** y active el control de difusión con un umbral de 10.000 kbps en modo Broadcast only (sólo difusión).

Figura 7 Traffic control (Control de tráfico) > Storm control (Control de tormentas)



Paso 3 Seleccione **Security suite (Conjunto de seguridad) > Traffic control (Control de tráfico) > Port security (Seguridad de puertos)**.

1. En el caso de los puertos reservados para teléfonos IP, configure la seguridad de los puertos para que se permitan sólo tres direcciones MAC.

En realidad, un teléfono IP posee dos direcciones MAC, mientras que la tercera es para la PC que se conecta al puerto LAN del teléfono IP.

2. Active la captura y bloquee el puerto.

Figura 8 Control de tráfico (Traffic control) > Seguridad de puertos (Port security)

Configuración general de la calidad de servicio

Paso 1 Seleccione **Quality of Service (Calidad de servicio) > General (General) > CoS (CoS)**, elija la opción Advanced (Avanzada) en QoS Mode (Modo de QoS) y haga clic en **Apply (Aplicar)**.

El modo predeterminado de QoS es Basic (Básico).

Figura 9 General (General) > QoS (Calidad de servicio)

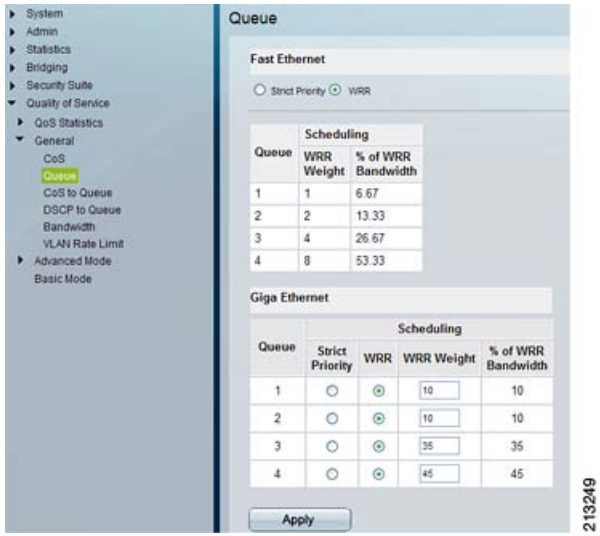
Paso 2 Seleccione **Quality of Service (Calidad de Servicio) > General (General) > Queue (Cola)**.

1. Seleccione el botón de opción WRR (Weighted Round Robin u operación por turnos compartida).

La WRR ayuda a administrar los paquetes en la red. En el caso de los puertos FastEthernet, el porcentaje del ancho de banda y el peso de la WRR están configurados previamente.

2. En el caso de Gigabit Ethernet, asigne el peso como se muestra a continuación.

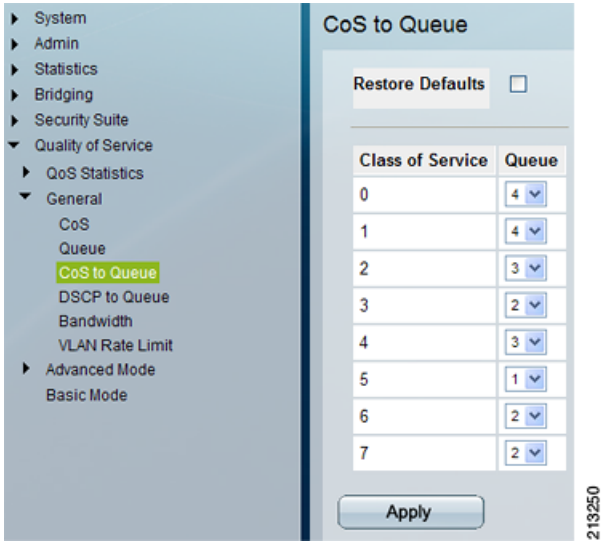
Figura 10 General (General) > Queue (Cola)



Paso 3 Seleccione **Quality of Service (Calidad de servicio) > General (General) > CoS to Queue (De CoS a cola)** y asigne los paquetes con diferentes valores de calidad de servicio a una de las cuatro colas de hardware de la siguiente manera (7 es la prioridad más alta):

- 0: predeterminado (mejor esfuerzo)
- 1: segundo plano
- 2: repuesto
- 3: esfuerzo excelente
- 4: carga controlada
- 5: video
- 6: voz
- 7: control de red

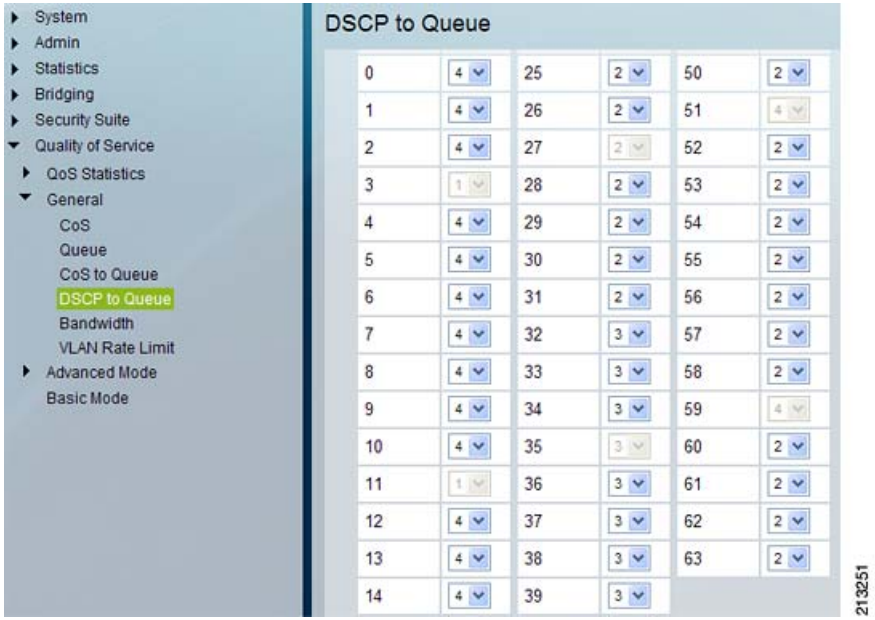
Figura 11 De CoS a cola



Paso 4 Seleccione **QoS (Calidad de servicio) > General (General) > DSCP to Queue (De DSCP a cola)** y asigne las colas para diversos valores de DSCP, de la siguiente manera:

- (0-15) a 4
- (16-23) a 3
- (24-31) a 2
- (32-39) a 3
- (40-47) a 1
- (48-63) a 2

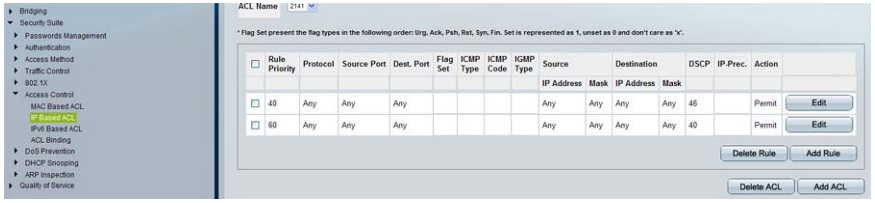
Figura 12 De DSCP a cola



Configuración del control de acceso y las políticas de calidad de servicio

Paso 1 Seleccione **Security suite (Conjunto de seguridad) > Access Control (Control de acceso) > IP Based ACL (ACL basada en IP)** y agregue ACL para identificar el tráfico.

Figura 13 ACL para tráfico de datos VoIP



Esta ACL define la clase de tráfico para cualquier tráfico de datos VoIP y le asigna los valores de DSCP 46 y 40 a este tráfico.

Figura 14 ACL para tráfico de control de VoIP

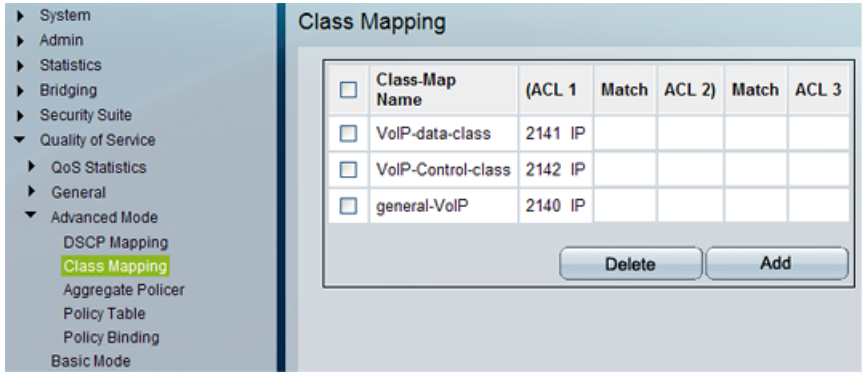
Esta ACL le asigna el valor 24 IP y 26 al tráfico de control de VoIP.

Figura 15 ACL para tráfico IP general

Esto define una ACL para el tráfico IP general, que utiliza los valores de DSCP predeterminados.

Paso 2 Seleccione **Quality of Service (Calidad de servicio) > Advance Mode (Modo avanzado) > Class Mapping (Asignación de clases)** y cree asignaciones de clases al hacer coincidir la ACL apropiada para el tráfico interesante.

Figura 16 Asignación de clases

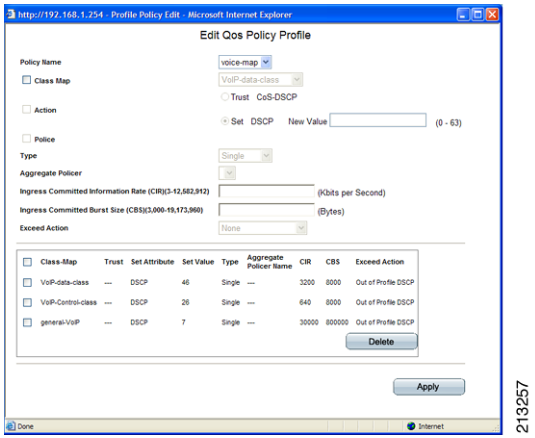


Paso 3 Seleccione **Quality of Service (Calidad de servicio) > Advance Mode (Modo avanzado) > Policy Table (Tabla de políticas)** y agregue una política denominada voice-map.

Figura 17 Tabla de políticas

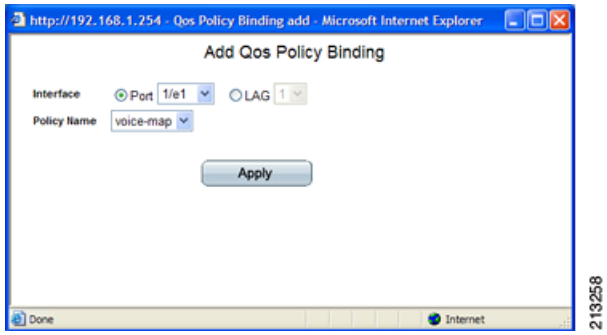
Paso 4 Configure la política voice-map mediante la conexión de todas las siguientes class-map y configure los diversos atributos que se muestran a continuación.

Figura 18 Edición del perfil de políticas de calidad de servicio



Paso 5 Seleccione **Quality of Service (Calidad de servicio) > Advance Mode (Modo avanzado) > Policy Binding (Vínculo de políticas)** y haga clic en **Add (Agregar)** para vincular la política voice-map con los puertos FastEthernet donde se conectarán los teléfonos IP.

Figura 19 Incorporación de un vínculo de política de calidad de servicio



Después de completar los pasos descritos en este consejo útil, ahora la red proporciona lo siguiente:

- Una experiencia de voz de alta calidad para los usuarios finales
- Una capa de seguridad para voz y partes de la red de datos