

Switches de las 2960/2950 Series del Catalyst usando el ejemplo de la configuración de VLAN de la Voz

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Descripción del VLA N de la Voz](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[De acuerdo con el valor de confianza de CoS](#)

[Al usar un teléfono del IP del no Cisco](#)

[De acuerdo con el valor de confianza DSCP en el encabezado IP](#)

[Verificación](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de ejemplo de la VLAN de voz en los switches Cisco Catalyst 2960/2950 Series. Específicamente, este documento muestra cómo configurar la función de VLAN de voz en un switch Cisco Catalyst 2950.

[prerrequisitos](#)

[Requisitos](#)

Asegurese que usted cumple estos requisitos antes de que usted intente esta configuración:

- Tenga un conocimiento básico de la configuración en el Switches de las 2960/2950 Series del Cisco Catalyst.
- Tenga una comprensión básica del VLA N de la Voz.

[Componentes Utilizados](#)

La información en este documento se basa en el Cisco Catalyst 2950 Switch.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Expresa la descripción del VLA N

La característica del VLA N de la Voz permite que los puertos del switch lleven el tráfico de voz con la Prioridad IP de la capa 3 y acoden 2 valores del Clase de Servicio (CoS) de un teléfono del IP. De acuerdo con el **IEEE 802.1P CoS**, el Switch soporta el Calidad de Servicio (QoS) que utiliza la clasificación y la previsión para enviar el tráfico de la red del Switch. Usted puede configurar el Cisco IP Phone para remitir el tráfico con una prioridad del IEEE 802.1P, y configura el Switch para confiar en o para reemplazar la prioridad de tráfico asignada por un teléfono del IP.

Usted puede configurar el puerto del switch, que está conectado con un teléfono del IP, para utilizar un VLA N para el tráfico de voz y otro VLA N para el tráfico de datos de un dispositivo asociado al puerto de acceso del teléfono del IP. Usted puede configurar los puertos de acceso en el Switch para enviar los paquetes del **Cisco Discovery Protocol (CDP)** para dar instrucciones un teléfono del IP asociado para enviar el tráfico de voz al Switch por ninguno de estos métodos:

- En el VLA N de la Voz marcado con etiqueta con un valor de la capa 2 prioridad de Clase de servicio (CoS)
- En el VLA N del acceso marcado con etiqueta con un valor de la capa 2 prioridad de Clase de servicio (CoS)
- En el VLA N del acceso, untagged (ningún valor de la capa 2 prioridad de Clase de servicio (CoS))

El Switch puede procesar el tráfico de datos que viene del dispositivo asociado al puerto de acceso en el teléfono del IP. Usted puede configurar los puertos del switch que envían los paquetes CDP que dan instrucciones el teléfono del IP asociado para configurar el modo (confiado en o untrusted) del modo para el puerto de acceso en el teléfono.

En el **modo de confianza**, el puerto de acceso en el teléfono del IP pasa el tráfico del PC sin ningún cambio. En el **modo untrusted**, el puerto de acceso en el teléfono del IP recibe todo el tráfico en las tramas del IEEE 802.1Q que contienen un valor configurado del CoS de la capa 2. El valor predeterminado del CoS de la capa 2 es 0. modos untrusted es el valor por defecto.

Configurar

En esta sección, le presentan con la información para configurar las características del VLA N de la Voz descritas en este documento.

En el Switch, la característica del VLA N de la Voz se inhabilita por abandono. Cuando usted habilita el VLA N de la Voz en el puerto, todo el tráfico sin Tags se envía según el valor por defecto prioridad de Clase de servicio (CoS). Antes de que usted habilite el VLA N de la Voz, habilite el QoS en el Switch publicando los **qos** comando global configuration de los **mls** y

configure al estado confiable del puerto **para confiar** en publicando el comando interface configuration de **lechuga romana de la confianza de los qos de los mls**.

Por abandono, un puerto del switch cae cualquier trama marcada con etiqueta en hardware. Para validar marcó las tramas con etiqueta en un puerto del switch, uno de estos comandos se debe configurar en el puerto:

- **dot1p vlan de la Voz del switchport**
- **Voz V_VLAN_ID vlan del switchport**
- **switchport mode trunk**

Utilice el comando [vlan del dot1p de la Voz del switchport](#) para dar instrucciones el puerto del switch para utilizar el etiquetado de prioridad del IEEE 802.1P para remitir todo el tráfico de voz con una prioridad más alta con el VLA N nativo (del acceso).

Utilice el comando [vlan de la Voz V VLAN ID del switchport](#) para configurar un VLA N especificado de la Voz, así que el teléfono del IP puede enviar el tráfico de voz en las tramas del IEEE 802.1Q con un valor de CoS de la capa 2. El Cisco IP Phone puede también enviar el tráfico de voz untagged o puede utilizar su propia configuración para enviar el tráfico de voz al VLA N del acceso del Switch.

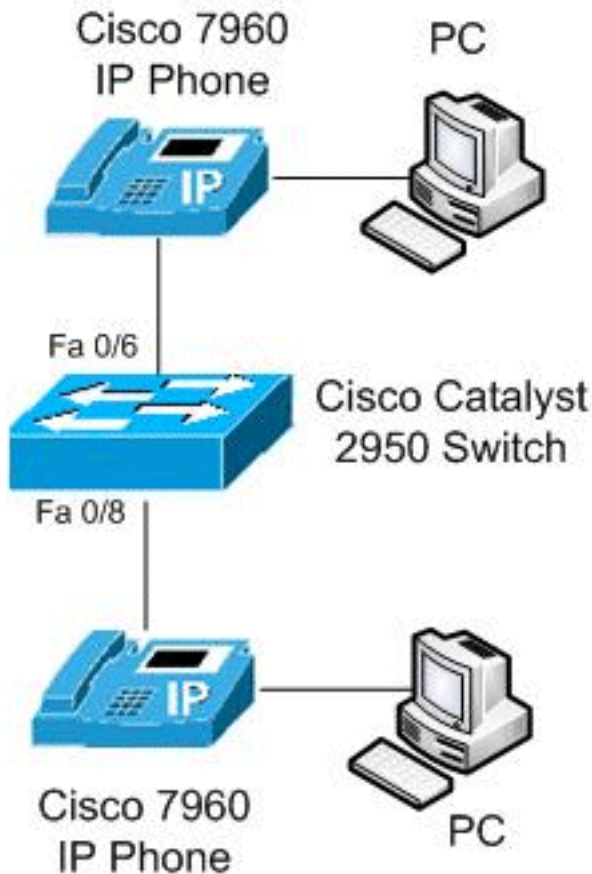
Utilice el [comando switchport priority extend trust](#) para extender al estado confiable al dispositivo (PC) conectado con el teléfono del IP. Publicando este comando, el Switch dará instrucciones el teléfono en cómo procesar los paquetes de datos del dispositivo asociado al puerto de acceso en el Cisco IP Phone. Los paquetes generados por el PC utilizan un valor asignado de CoS en la encabezado 802.1q. El teléfono no debe cambiar (confianza) la prioridad de los bastidores que llegan en el puerto telefónico del PC.

Usted debe habilitar el **CDP** en el puerto del switch con el cual el teléfono del IP está conectado. Por abandono, el CDP se habilita global en las interfaces del switch. El CDP es el mecanismo usado entre el Switch y el Cisco IP Phone para configurar el Cisco IP Phone para la comunicación con el puerto del switch. El CDP es propietario a Cisco Systems y los teléfonos de otros fabricantes pueden no poder utilizar este método para configurar el teléfono del IP para hacer juego la configuración del puerto del Switch.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



Este diagrama es un ejemplo de una configuración de VLAN de la Voz en un Cisco Catalyst 2950 Switch. El FastEthernet 0/6 y 0/8 de los puertos del switch está conectado con un Cisco IP Phone, y el puerto de acceso en ambos los Teléfonos IP está conectado con el PC.

Configuraciones

En este documento, se utilizan estas configuraciones:

De acuerdo con el valor de confianza de CoS

En el 2950 Switch, el FastEthernet 0/6 puerto tiene el VLAN configurado **10** para el VLAN de la Voz con el **dot1p** para utilizar el etiquetado de prioridad del **IEEE 802.1P** para el tráfico de voz, y modo configurado de la **confianza** para el tráfico de datos del PC que está conectado con el puerto de acceso del Cisco IP Phone. Aquí, el Cisco IP Phone **está confiando en que una laptop o un PC** vía CoS y el tráfico de datos utiliza el **VLAN nativo**. Esta configuración se utiliza típicamente para las estaciones de trabajo de administración, los usuarios prioritarios, o una aplicación del valor de CoS del alto.

Cuando un Teléfono de Cisco hace el CDP con el Switch, el límite de confianza se amplía siempre al teléfono del IP. Es decir, los paquetes del teléfono del IP nunca se cambian de CoS 5 al valor por defecto de CoS. Por eso utilizan al [comando switchport priority extend trust](#) para la laptop o el PC. Se envía vía el CDP para decir el teléfono del IP no reescribir los paquetes con prioridad alta.

El FastEthernet 0/8 puerto se configura con los VLAN distintos para el tráfico de voz y de datos. En este ejemplo, el **VLAN10** se utiliza para el tráfico de voz y el **VLAN20** se utiliza para el tráfico de datos. Esta configuración se utiliza para los Teléfonos IP típicos de Cisco **sin confiar en la**

laptop o el PC. El tráfico utiliza el tipo de trama del IEEE 802.1Q.

Con el [comando mls qos trust cos](#), el puerto del switch de Catalyst mira el valor de CoS en el encabezado Ethernet para clasificar el Tráfico de ingreso y confía en el valor de CoS del paquete con Tag que origina del Cisco IP Phone. Por abandono, el acceso de Ethernet llega a ser untrusted, así que el tráfico que viene del VLA N de la Voz y del VLAN de dato no será confiado en.

Utilice el **comando priority-queue out** para dar los privilegios del jefe de line de los paquetes de voz al intentar de salir el puerto que previene el jitter. [El comando spanning-tree portfast](#) quita la interfaz del Spanning Tree Protocol, y el comando del [bpduguard](#) protege la red si alguien intenta conectar un nuevo Switch con él después de desenchufar el teléfono del IP. Si se enchufara un Switch, el puerto iría al err-disable. Éstos se agregan típicamente a los puertos telefónicos.

Cisco Catalyst 2950 Switch

```
Switch#configure terminal Switch(config)#mls qos
Switch(config)#interface fastethernet 0/6 !--- Set the
interface to classify incoming traffic packets by using
the packet CoS value. Switch(config-if)#mls qos trust
cos !--- Configure the phone to use IEEE 802.1p priority
tagging for voice traffic. Switch(config-if)#switchport
voice vlan dot1p Switch(config-if)#switchport voice vlan
10 !--- Trust the CoS value the PC sends in on the data
VLAN. Switch(config-if)#switchport priority extend trust
Switch(config-if)#priority-queue out Switch(config-
if)#spanning-tree portfast Switch(config-if)#spanning-
tree bpduguard enable Switch(config-if)#exit
Switch(config)#interface gigabitethernet0/8
Switch(config-if)#mls qos trust cos !--- Configure
specified VLANs for voice and data traffic.
Switch(config-if)#switchport voice vlan 10
Switch(config-if)#switchport access vlan 20
Switch(config-if)#priority-queue out Switch(config-
if)#spanning-tree portfast Switch(config-if)#spanning-
tree bpduguard enable Switch(config-if)#exit
```

[Al usar un teléfono del IP del no Cisco](#)

Si usted está utilizando un teléfono del IP del no Cisco que no reconozca Cisco CDP propietario y automáticamente configura el puerto troncal, usted tendrá que configurar el trunk manualmente. En este ejemplo de configuración, restringimos los VLA N a 10 y a 20, y bloqueamos el VLAN nativo predeterminado 1 o el VLAN0. **VLAN10** se utiliza para el tráfico de voz y el **VLAN20** se utiliza para el tráfico de datos. El teléfono del IP del no Cisco aprende el VLA N correcto para sus paquetes con Tag con la configuración manual o vía el archivo TFTP descarga durante el inicio para arriba. Este ejemplo utiliza esta configuración:

Cisco Catalyst 2950 Switch

```
Switch#configure terminal Switch(config)#interface
fastethernet 0/6 !---Trusts tagged packets CoS value;
all untagged packets reset DSCP value in IP header to 0.
Switch(config-if)#mls qos trust cos !--- Turn off DTP
(dynamic trunking protocol). Switch(config-
if)#switchport nonegotiate !--- Forces the port into
trunking mode. Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 20 !---
Restricts the VLANs. Switch(config-if)#switchport trunk
allowed vlans 10,20 Switch(config-if)#priority-queue out
```

```
Switch(config-if)#spanning-tree portfast trunk
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit
```

[De acuerdo con el valor de confianza DSCP en el encabezado IP](#)

Aquí, utilizamos un valor de confianza de los puntos del código de DiffService (DSCP) en vez de un valor de CoS, porque CoS ofrece una manera de entender la importancia del paquete apenas mirando su encabezado L2. El DSCP es un campo 6-bit dentro del paquete del IP. Utilice el [comando mls qos trust dscp](#) para confiar en el valor DSCP en el encabezado IP. En este caso, los conjuntos de teléfono del IP su DSCP correctamente en sus paquetes y la laptop fijarían su DSCP correctamente. Este ejemplo utiliza esta configuración:

Cisco Catalyst 2950 Switch

```
Switch#configure terminal Switch(config)#interface
fastEthernet 0/6 !---Trust the DSCP value in the IP
header. Switch(config-if)#mls qos trust DSCP !--- IP
phone VLAN Switch(config-if)#switchport voice vlan 10
Switch(config-if)#switchport access vlan 20 !--- Trust
the DSCP value the PC sends in on the data VLAN.
Switch(config-if)#switchport priority extend trust
Switch(config-if)#priority-queue out Switch(config-
if)#spanning-tree portfast Switch(config-if)#spanning-
tree bpduguard enable Switch(config-if)#exit
```

[Verificación](#)

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- Utilice el [comando show interfaces interface-id switchport](#) para verificar su configuración de VLAN de la Voz. Por ejemplo: Switch#show interfaces FastEthernet 0/6 switchport Name: Fa0/6 Switchport: Enabled Administrative Mode: dynamic desirable Operational Mode: static access Administrative Trunking Encapsulation: dot1q Operational Trunking Encapsulation: native Negotiation of Trunking: On Access Mode VLAN: 1 (default) Trunking Native Mode VLAN: 1 (default) **Voice VLAN: dot1p** Administrative private-vlan host-association: none Administrative private-vlan mapping: none Administrative private-vlan trunk native VLAN: none Administrative private-vlan trunk encapsulation: dot1q Administrative private-vlan trunk normal VLANs: none Administrative private-vlan trunk private VLANs: none Operational private-vlan: none Trunking VLANs Enabled: ALL Pruning VLANs Enabled: 2-1001 Capture Mode Disabled Capture VLANs Allowed: ALL Protected: false Unknown unicast blocked: disabled Unknown multicast blocked: disabled **Appliance trust: trusted**
- Utilice el comando de la *id del interfaz del show running-config interface* para verificar sus entradas del VLAN de la Voz para una interfaz particular. Por ejemplo: Switch#show running-config interface fastEthernet 0/6 Building configuration... Current configuration : 139 bytes ! interface FastEthernet0/6 switchport voice vlan dot1p switchport voice vlan 10 switchport priority extend trust mls qos trust cos priority-queue out spanning-tree portfast spanning-tree bpduguard enable end Switch#show running-config interface fastEthernet 0/8 Building configuration... Current configuration : 137 bytes ! interface FastEthernet0/8 switchport voice vlan 10 switchport access vlan 20 mls qos trust cos priority-queue out spanning-tree portfast spanning-tree bpduguard enable end

[Información Relacionada](#)

- [Página de soporte de los Cisco Catalyst 2950 Series Switch](#)
- [Página de soporte de los Cisco Catalyst 2960 Series Switch](#)
- [Soporte de Productos de Switches](#)
- [Soporte de Tecnología de LAN Switching](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)