Pertenencia a VLAN privada en un switch Cisco Business 350

Objetivo

En este artículo se proporcionan instrucciones sobre cómo configurar los parámetros de VLAN privada en un switch Cisco Business serie 350.

Dispositivos aplicables | Versión de software

- CBS350 (hoja de datos) | 3.0.0.69 (descargue la última versión)
- CBS350-2X (hoja de datos) | 3.0.0.69 (descargue la última versión)
- CBS350-4X (hoja de datos) | 3.0.0.69 (descargue la última versión)

Introducción

Una red de área local virtual (VLAN) permite segmentar lógicamente una red de área local (LAN) en diferentes dominios de difusión. En situaciones en las que se pueden transmitir datos confidenciales en una red, se puede crear una VLAN para mejorar la seguridad mediante la designación de una transmisión a una VLAN específica. Solo los usuarios que pertenecen a una VLAN pueden acceder y manipular los datos en esa VLAN. Las VLAN también pueden utilizarse para mejorar el rendimiento al reducir la necesidad de enviar difusiones y multidifusiones a destinos innecesarios.

Una VLAN privada proporciona aislamiento de capa 2 entre los puertos. Esto significa que en el nivel de tráfico de bridging, a diferencia del ruteo IP, los puertos que comparten el mismo dominio de broadcast no pueden comunicarse entre sí. Los puertos en una VLAN privada se pueden ubicar en cualquier lugar de la red de capa 2, lo que significa que no tienen que estar en el mismo switch. La VLAN privada está diseñada para recibir tráfico sin etiqueta o con etiqueta de prioridad y transmitir tráfico sin etiqueta.

Los siguientes tipos de puertos pueden ser miembros en una VLAN privada:

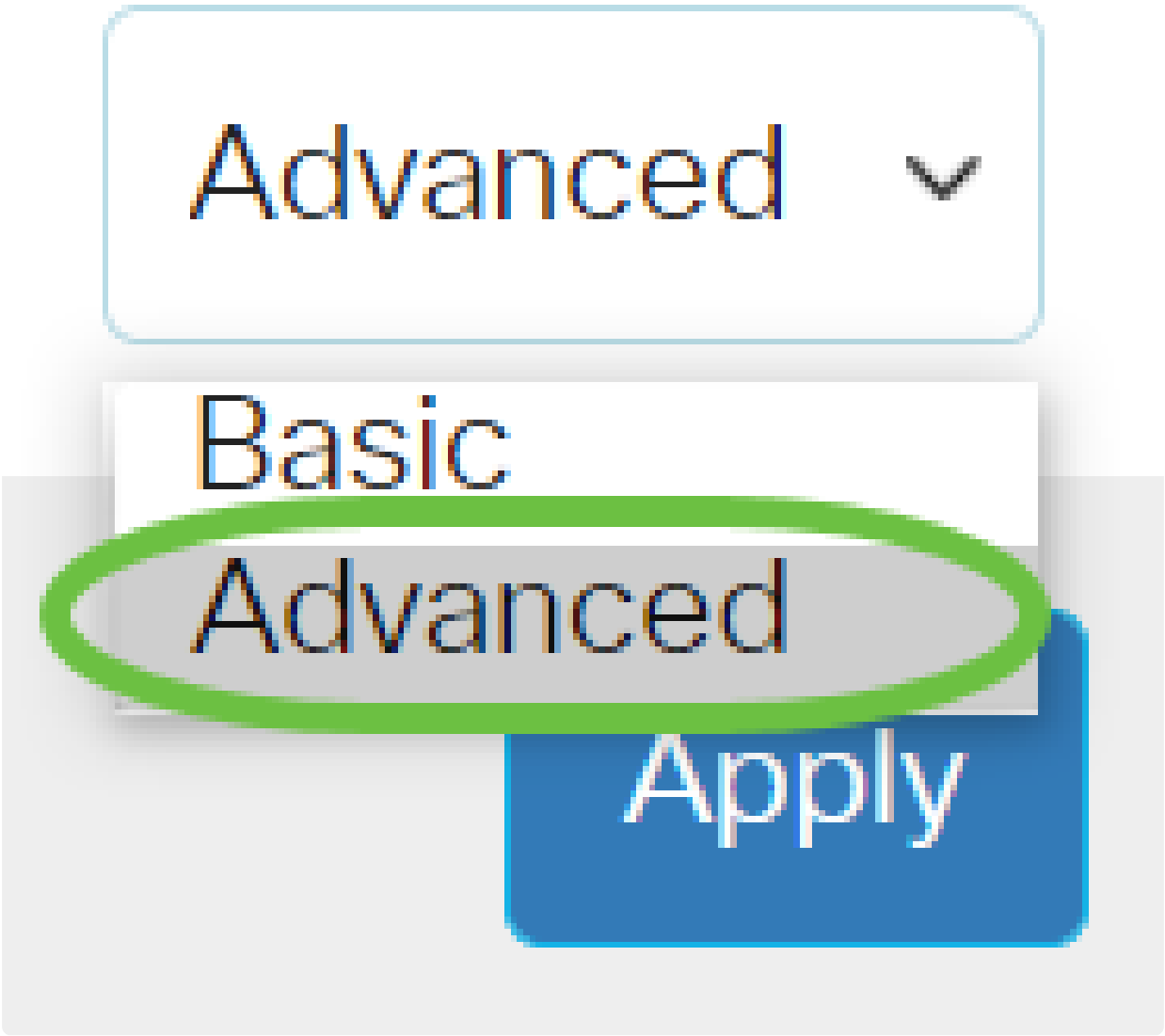
- Promiscuo - Un puerto promiscuo puede comunicarse con todos los puertos de la misma VLAN privada. Estos puertos conectan servidores y routers.
- Comunidad (host): los puertos comunitarios pueden definir un grupo de puertos que son miembros en el mismo dominio de capa 2. Están aislados en la capa 2 de otras comunidades y de puertos aislados. Estos puertos conectan los puertos host.
- Aislado (host): Un puerto aislado tiene aislamiento completo de Capa 2 de los otros puertos aislados y comunitarios dentro de la misma VLAN privada. Estos puertos conectan los puertos host.

El tráfico de host se envía en VLAN aisladas y de comunidad, mientras que el tráfico de servidor y router se envía en la VLAN principal.

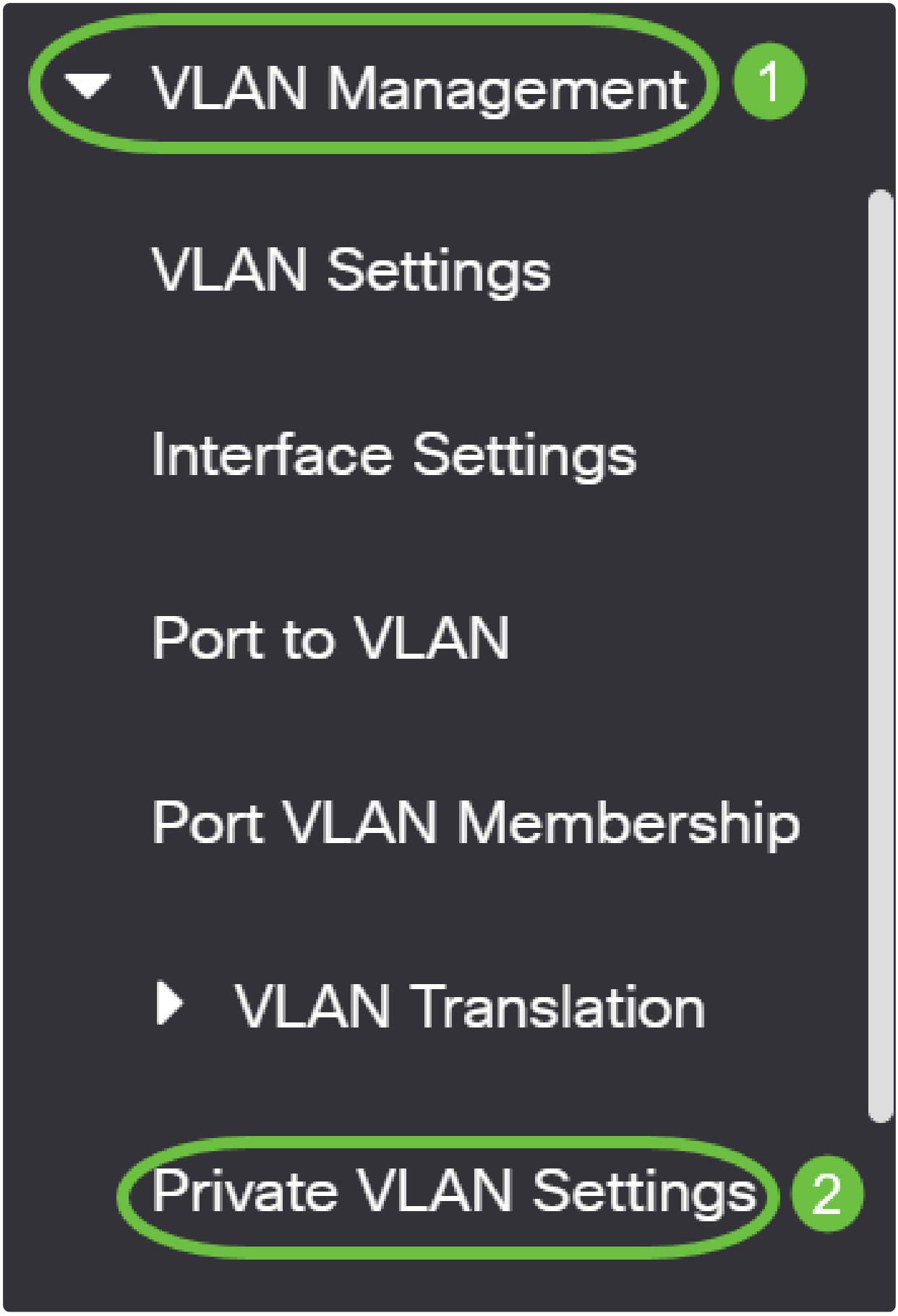
Configuración de los parámetros de VLAN privada en un switch

Importante: Antes de continuar con los pasos a continuación, asegúrese de que se hayan configurado las VLAN en el switch. Para saber cómo configurar los parámetros de VLAN en su switch, haga clic aquí para obtener instrucciones.

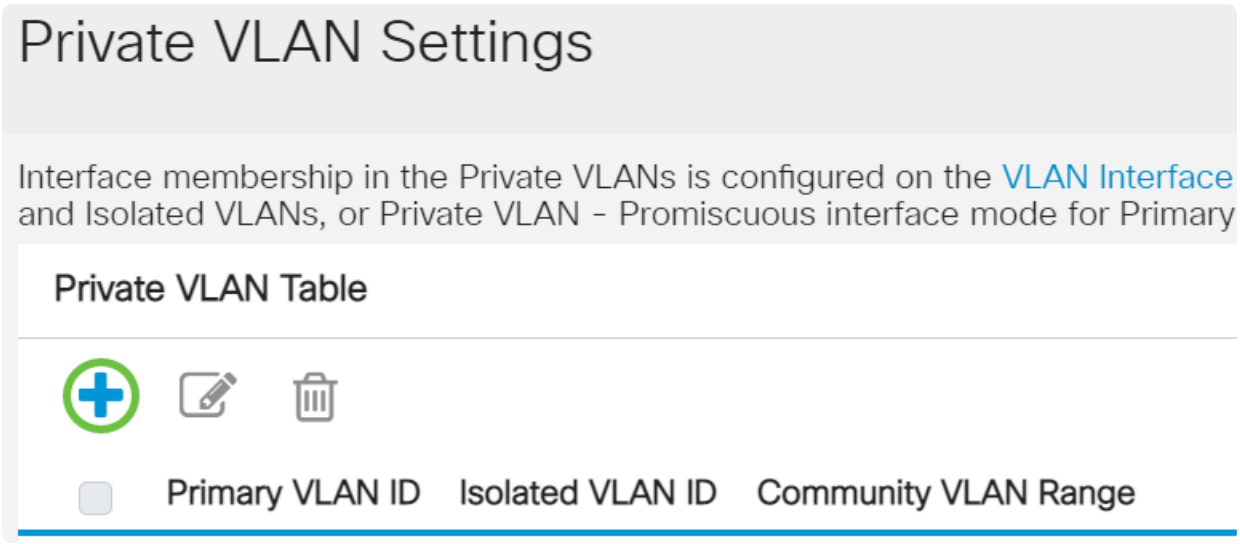
Paso 1. Inicie sesión en la utilidad basada en Web y seleccione Avanzado en la lista desplegable Modo de visualización.



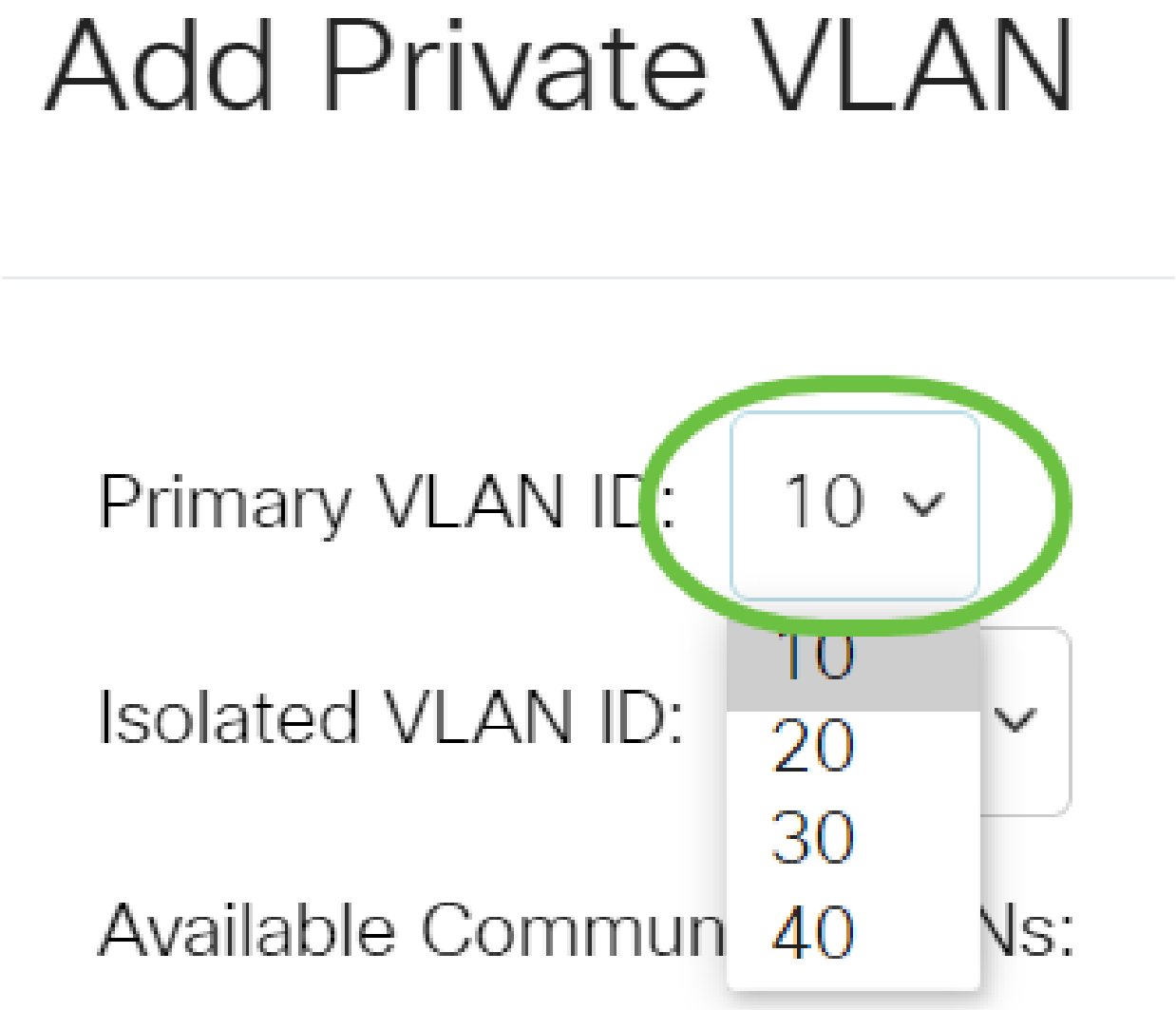
Paso 2. Elija VLAN Management >Private VLAN Settings.



Paso 3. Haga clic en el botón Agregar.

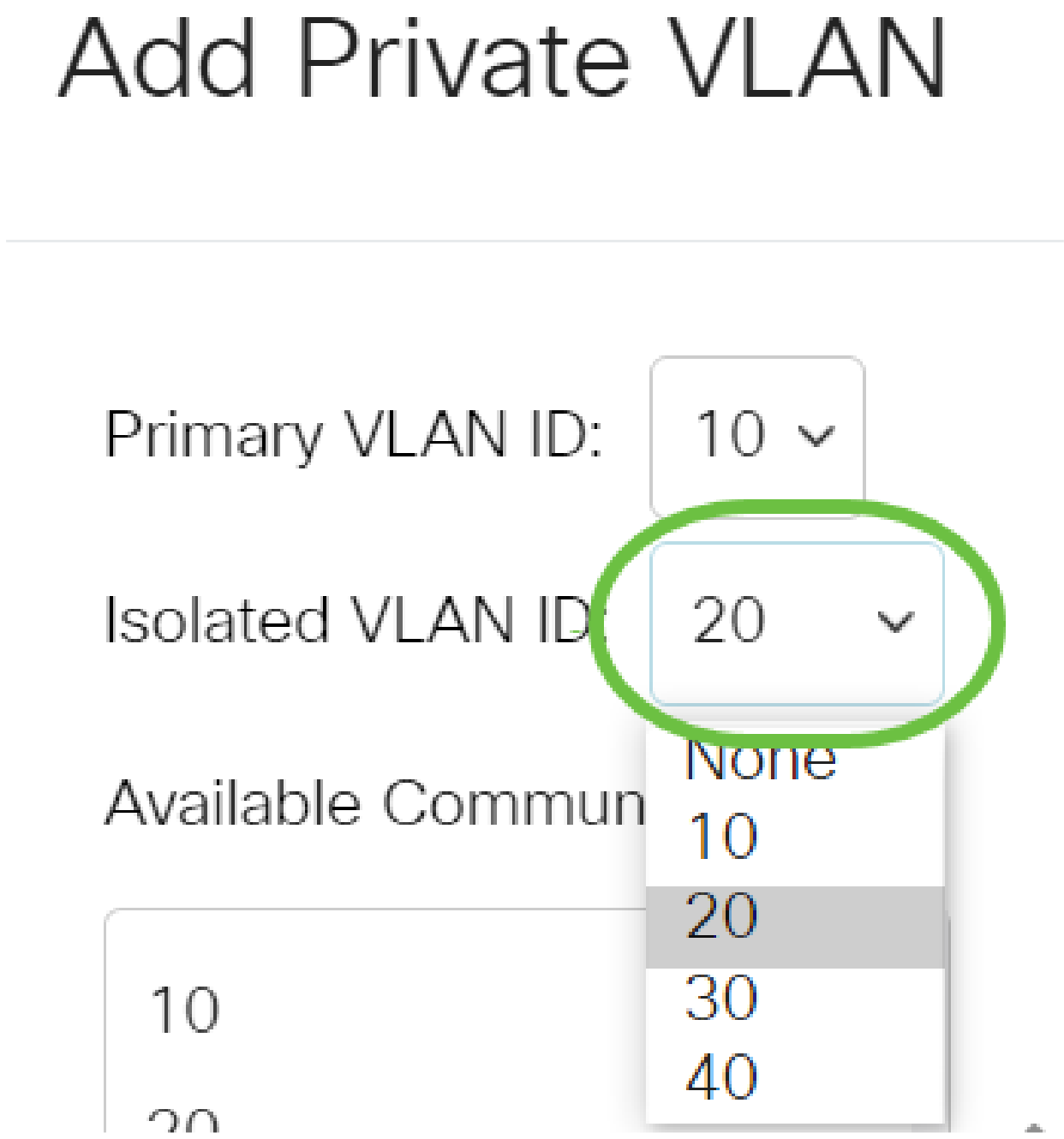


Paso 4. En la lista desplegable Primary VLAN ID (ID de VLAN principal), elija una VLAN para definirla como la VLAN principal en la VLAN privada. La VLAN principal se utiliza para permitir la conectividad de capa 2 desde puertos promiscuos a puertos aislados y a puertos de comunidad.



Nota: En este ejemplo, se elige el ID de VLAN 10.

Paso 5. Elija un ID de VLAN en la lista desplegable ID de VLAN aislada. Una VLAN aislada se utiliza para permitir que los puertos aislados envíen tráfico a la VLAN principal.

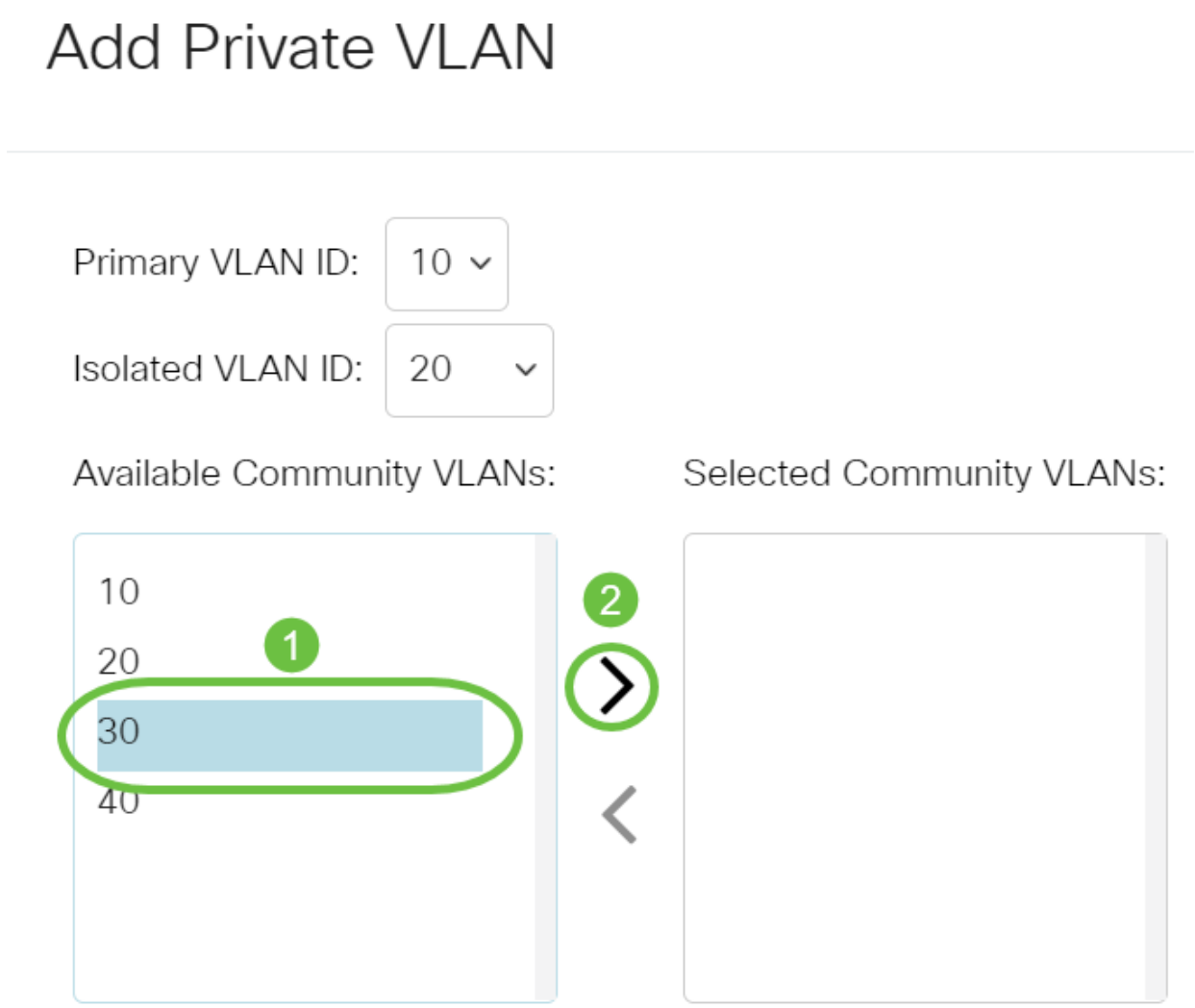


Nota: En este ejemplo, se elige el ID de VLAN 20.

Paso 6. Elija un ID de VLAN del área de VLAN de comunidad disponibles y luego haga clic en el botón > para mover las VLAN que desea que sean VLAN de comunidad a la lista de VLAN de comunidad seleccionadas.

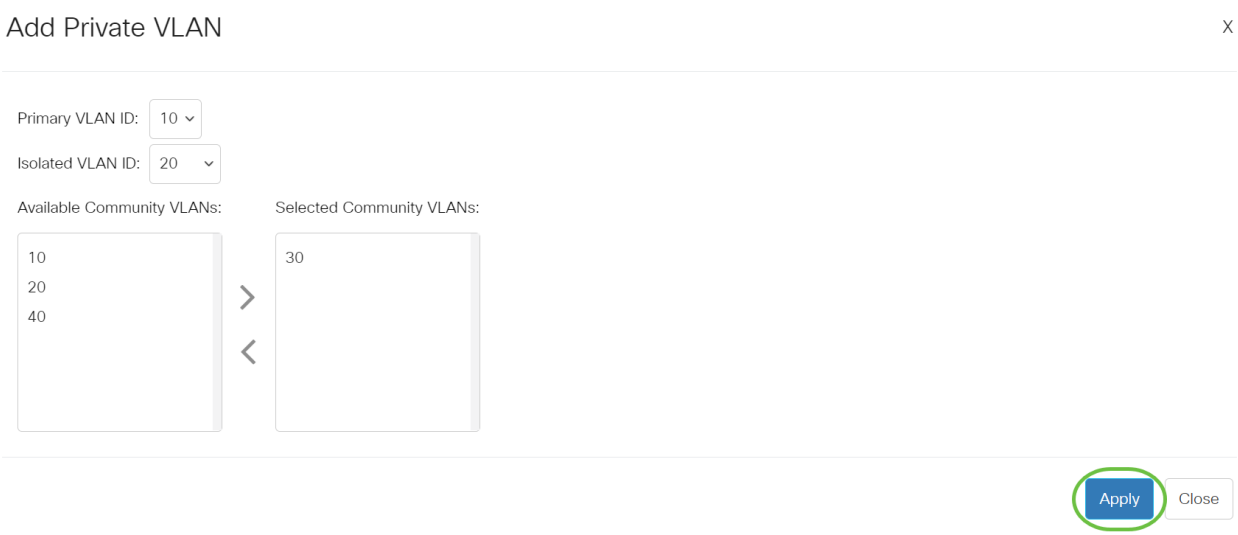
Nota: Para crear un subgrupo de puertos (comunidad) dentro de una VLAN, los puertos deben agregarse a una VLAN de comunidad. La VLAN de comunidad se utiliza para habilitar la

conectividad de Capa 2 desde los puertos de comunidad a los puertos promiscuos y a los puertos de comunidad de la misma comunidad. Puede haber una sola VLAN de comunidad para cada comunidad y pueden coexistir varias VLAN de comunidad en el sistema para la misma VLAN privada.

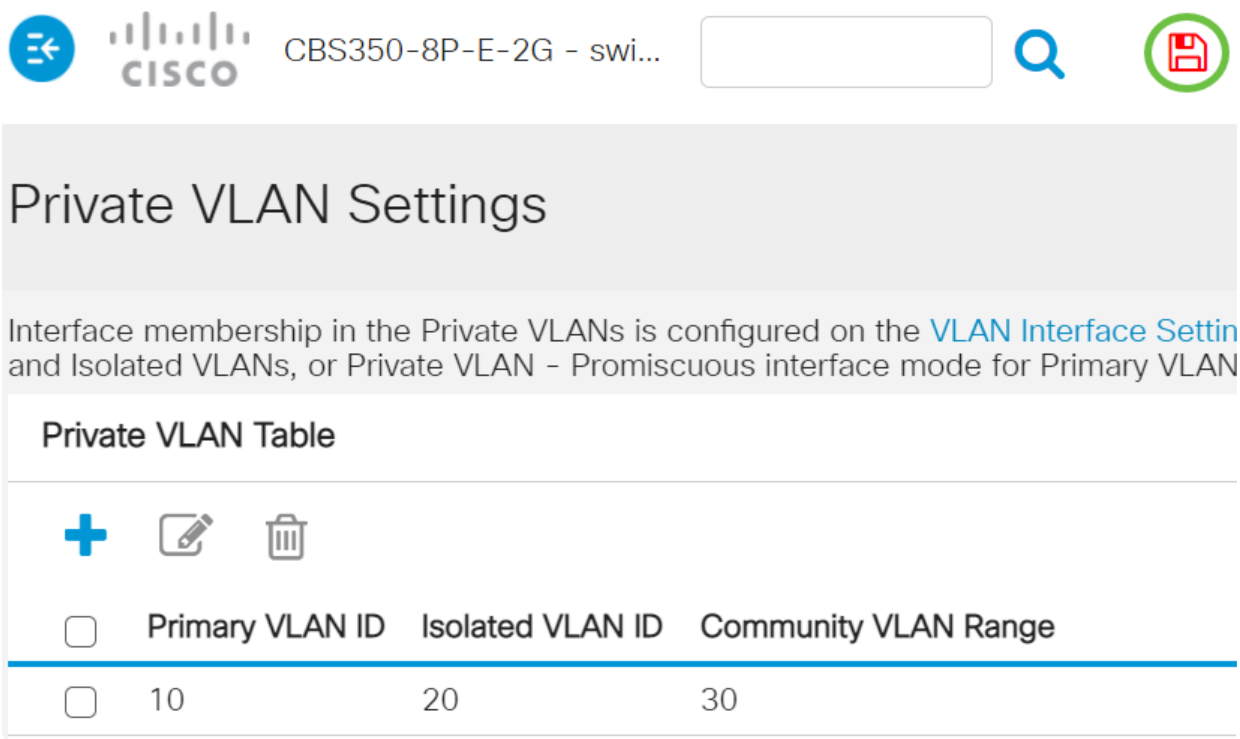


Nota: En este ejemplo, se elige el ID de VLAN 30.

Paso 7. Haga clic en Aplicar y luego haga clic en Cerrar.



Paso 8. (Opcional) Haga clic en Guardar para guardar los ajustes en el archivo de configuración de inicio.



Ya ha configurado los parámetros de VLAN privada en el switch Cisco Business serie 350.

¿Desea obtener más información sobre las VLAN para los switches empresariales de Cisco? Consulte cualquiera de los siguientes enlaces para obtener más información.

Creación de VLAN Pertenencia de puerto a VLAN Acceso y puertos troncales Grupos basados en protocolo a VLAN Configuración de puerto a VLAN VLAN basada en subred Configuración del grupo de televisión multidifusión a VLAN Grupos de VLAN basados en protocolo Acceso al puerto Multidifusión TV Pertenencia a VLAN Puerto del cliente Multidifusión TV Pertenencia a VLAN

Esqueleto del artículo con contenido

Objetivo

En este artículo se proporcionan instrucciones sobre cómo configurar los parámetros de VLAN privada en un switch Cisco Business serie 350.

Una VLAN privada proporciona aislamiento de capa 2 entre los puertos. Esto significa que en el nivel de tráfico de bridging, a diferencia del ruteo IP, los puertos que comparten el mismo dominio de broadcast no pueden comunicarse entre sí. Los puertos en una VLAN privada se pueden ubicar en cualquier lugar de la red de capa 2, lo que significa que no tienen que estar en el mismo switch. La VLAN privada está diseñada para recibir tráfico sin etiqueta o con etiqueta de prioridad y transmitir tráfico sin etiqueta.

Dispositivos aplicables | Versión de software

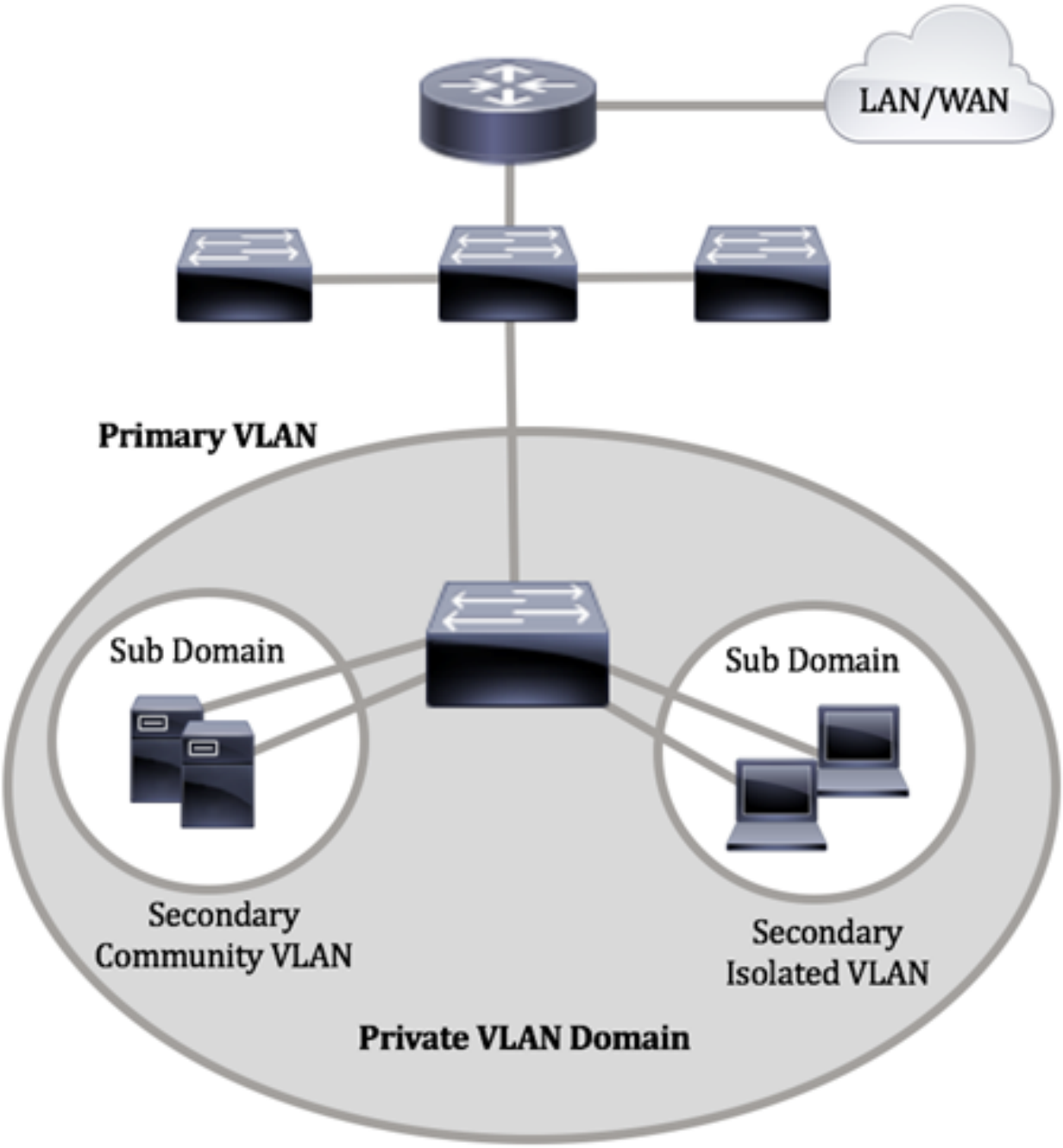
- CBS350 (hoja de datos) | 3.0.0.69 (descargue la última versión)
- CBS350-2X (hoja de datos) | 3.0.0.69 (descargue la última versión)
- CBS350-4X (hoja de datos) | 3.0.0.69 (descargue la última versión)

Introducción

Una red de área local virtual (VLAN) permite segmentar lógicamente una red de área local (LAN) en diferentes dominios de difusión. En situaciones en las que se pueden transmitir datos confidenciales en una red, se puede crear una VLAN para mejorar la seguridad mediante la designación de una transmisión a una VLAN específica. Solo los usuarios que pertenecen a una VLAN pueden acceder y manipular los datos en esa VLAN. Las VLAN también pueden utilizarse para mejorar el rendimiento al reducir la necesidad de enviar difusiones y multidifusiones a destinos innecesarios.

Nota: Para obtener información sobre cómo configurar los parámetros de VLAN en su switch mediante la utilidad web, haga clic aquí. Para obtener instrucciones basadas en la CLI, haga clic aquí.

Un dominio de VLAN privada consta de uno o más pares de VLAN. La VLAN principal constituye el dominio; y cada par de VLAN forma un subdominio. Las VLAN de un par se denominan VLAN principal y VLAN secundaria. Todos los pares de VLAN dentro de una VLAN privada tienen la misma VLAN principal. El ID de VLAN secundario es lo que diferencia un subdominio de otro.



Un dominio de VLAN privada sólo tiene una VLAN principal. Cada puerto de un dominio de VLAN privada es miembro de la VLAN principal; la VLAN principal es todo el dominio de VLAN privada.

Las VLAN secundarias proporcionan aislamiento entre los puertos dentro del mismo dominio de VLAN privada. Los dos tipos siguientes son VLAN secundarias dentro de una VLAN principal:

- VLAN aisladas: los puertos de una VLAN aislada no pueden comunicarse directamente entre sí en el nivel de capa 2.
- VLAN de comunidad: los puertos de una VLAN de comunidad pueden comunicarse entre sí, pero no pueden comunicarse con los puertos de otras VLAN de comunidad o de cualquier VLAN aislada en el nivel de capa 2.

Dentro de un dominio de VLAN privada, hay tres designaciones de puerto separadas. Cada designación de puerto tiene su propio conjunto único de reglas que regulan la capacidad de un

terminal para comunicarse con otros terminales conectados dentro del mismo dominio de VLAN privada. A continuación se indican las tres designaciones de puerto:

- Promiscuo - Un puerto promiscuo puede comunicarse con todos los puertos de la misma VLAN privada. Estos puertos conectan servidores y routers.
- Comunidad (host): los puertos comunitarios pueden definir un grupo de puertos que son miembros en el mismo dominio de capa 2. Están aislados en la capa 2 de otras comunidades y de puertos aislados. Estos puertos conectan los puertos host.
- Aislado (host): Un puerto aislado tiene aislamiento completo de Capa 2 de los otros puertos aislados y comunitarios dentro de la misma VLAN privada. Estos puertos conectan los puertos host.

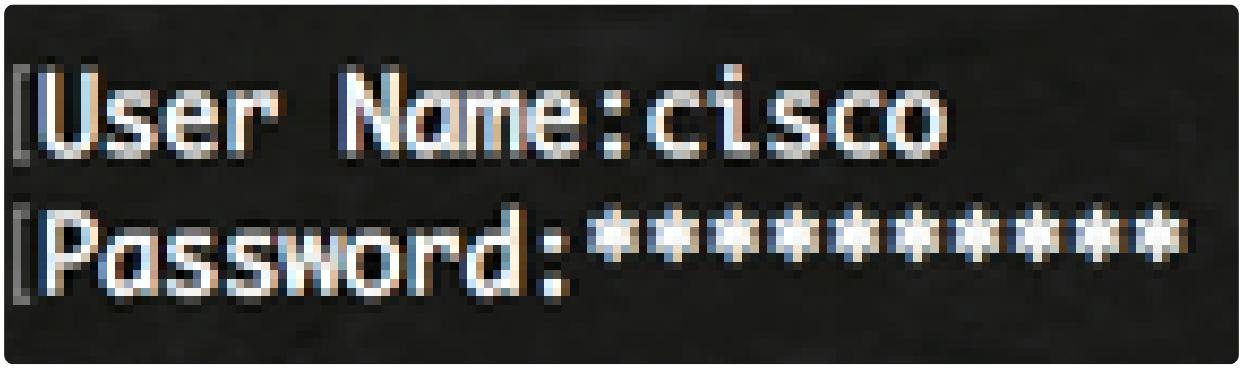
El tráfico de host se envía en VLAN aisladas y de comunidad, mientras que el tráfico de servidor y router se envía en la VLAN principal.

> ⓘ Note:
> Para configurar la VLAN privada mediante la utilidad basada en Web del switch, haga clic aquí.

Configuración de los parámetros de VLAN privada en el switch a través de la CLI

Creación de una VLAN principal privada

Paso 1. Inicie sesión en la consola del switch. La contraseña y el nombre de usuario predeterminados son cisco/cisco. Si ha configurado una nueva contraseña o nombre de usuario, introduzca las credenciales.



> ⓘ Note:
> Los comandos pueden variar según el modelo exacto del switch.

Paso 2. En el modo EXEC con privilegios del switch, ingrese al modo de configuración global escribiendo lo siguiente:

```
CBS350#  configure
```

Paso 3. En el modo de configuración global, ingrese el contexto de configuración de interfaz escribiendo lo siguiente:

```
CBS350(config)#  interface [vlan-id]
```

- vlan-id: especifica el ID de VLAN que se va a configurar.

Paso 4. En el contexto de Configuración de la Interfaz, configure la interfaz VLAN como la VLAN privada principal ingresando lo siguiente:

```
CBS350(config-if)#  private-vlan primary
```

> ⓘ Note:
> De forma predeterminada, no hay VLAN privadas configuradas en el switch.

Importante: Asegúrese de recordar las siguientes pautas al configurar una VLAN privada:

- El tipo de VLAN no se puede cambiar si hay un puerto de VLAN privada que es miembro de la VLAN.
- El tipo de VLAN no se puede cambiar si está asociado con otras VLAN privadas.
- El tipo de VLAN no se mantiene como una propiedad de la VLAN cuando se elimina la VLAN.

Paso 5. (Opcional) Para devolver la VLAN a su configuración de VLAN normal, introduzca lo siguiente:

```
CBS350(config-if)#  no private-vlan
```

Paso 6. (Opcional) Para volver al modo EXEC privilegiado del switch, introduzca lo siguiente:

```
CBS350(config-if)#  end
```

Paso 7. (Opcional) En el modo EXEC con privilegios del switch, guarde los parámetros configurados en el archivo de configuración de inicio ingresando lo siguiente:

```
CBS350#  copy running-config startup-config
```

Paso 8. (Opcional) Presione S para Sí o N para No en su teclado cuando aparezca el mensaje: Sobrescriba el archivo [startup-config].

Ahora ha creado correctamente la VLAN principal en el switch a través de la CLI.

Crear una VLAN secundaria

Paso 1. En el modo EXEC con privilegios del switch, ingrese al modo de configuración global escribiendo lo siguiente:

```
CBS350#  configure
```

Paso 2. En el modo de configuración global, ingrese el contexto de configuración de interfaz escribiendo lo siguiente:

```
CBS350(config)#  interface [vlan-id]
```

Paso 3. En el contexto de Configuración de la Interfaz, configure la interfaz VLAN como la VLAN privada secundaria ingresando lo siguiente:

```
CBS350(config-if)#  private-vlan [community | isolated]
```

Las opciones son:

- community - Designe la VLAN como VLAN de comunidad.
- aislado: designe la VLAN como VLAN aislada.

Paso 4. (Opcional) Repita los pasos 2 y 3 para configurar una VLAN secundaria adicional para su VLAN privada.

Paso 5. (Opcional) Para devolver la VLAN a su configuración de VLAN normal, introduzca lo siguiente:

```
CBS350(config-if)#  no private-vlan
```

Paso 6. (Opcional) Para volver al modo EXEC privilegiado del switch, introduzca lo siguiente:

```
CBS350(config-if)#  end
```

Ahora ha creado correctamente VLAN secundarias en el switch a través de la CLI.

Asociar la VLAN secundaria a la VLAN privada principal

Paso 1. En el modo EXEC con privilegios del switch, ingrese al modo de configuración global escribiendo lo siguiente:

```
CBS350#  configure
```

Paso 2. Ingrese el contexto de configuración de la interfaz VLAN de la VLAN principal ingresando lo siguiente:

```
CBS350(config)#  vlan [primary-vlan-id]
```

Paso 3. Para configurar la asociación entre la VLAN principal y las VLAN secundarias, ingrese lo siguiente:

```
CBS350(config-if)# private-vlan association [add | remove]secondary-vlan-list
```

Las opciones son:

- add secondary-vlan-list - Lista de ID de VLAN de tipo secundario para agregar a una VLAN principal. Separe las ID de VLAN no consecutivas con una coma y sin espacios. Utilice un guión para designar un rango de ID. Ésta es la acción predeterminada.
- remove secondary-vlan-list - Lista de ID de VLAN de tipo secundario para quitar la asociación de una VLAN principal. Separe las ID de VLAN no consecutivas con una coma y sin espacios. Utilice un guión para designar un rango de ID.

Paso 4. Para volver al modo EXEC privilegiado del switch, introduzca lo siguiente:

```
CBS350(config-if)# end
```

Ahora ha asociado correctamente las VLAN secundarias a la VLAN privada principal del switch mediante la CLI.

Configuración de Puertos para las VLAN Privadas Primarias y Secundarias

Paso 1. En el modo EXEC con privilegios del switch, ingrese al modo de configuración global escribiendo lo siguiente:

```
CBS350# configure
```

Paso 2. En el modo de configuración global, ingrese el contexto de configuración de interfaz escribiendo lo siguiente:

```
CBS350(config)# interface [interface-id | range vlan vlan-range]
```

Las opciones son:

- interface-id: especifica una ID de interfaz para configurar.
- range vlan vlan-range: especifica una lista de VLAN. Separe las VLAN no consecutivas con una coma y sin espacios. Utilice un guión para designar un rango de VLAN.

Paso 3. En el contexto de configuración de interfaz, utilice el comando switchport mode para configurar el modo de pertenencia de la VLAN.

```
CBS350(config-if-range)# switchport mode private-vlan [promiscuous | host]
```

- promiscuous - Especifica un puerto promiscuo de VLAN privada. Si se utiliza esta opción, vaya directamente al paso 5.
- host: especifica un puerto de host de VLAN privada. Si se utiliza esta opción, vaya directamente al paso 6.

Paso 4. (Opcional) Para devolver el puerto o el rango de puertos a la configuración predeterminada, introduzca lo siguiente:

```
CBS350(config-if-range)#  no switchport mode
```

Paso 5. Para configurar la asociación de un puerto promiscuo con VLAN primarias y secundarias de la VLAN privada, ingrese lo siguiente:

```
CBS350(config-if)#  switchport private-vlan mapping [primary-vlan-id] add [secondary-vlan-id]
```

Las opciones son:

- primary-vlan-id: especifica el ID de VLAN de la VLAN principal.
- secondary-vlan-id - Especifica el ID de VLAN de la VLAN secundaria.

Paso 6. Para configurar la asociación de un puerto de host con VLAN primarias y secundarias de la VLAN privada, ingrese lo siguiente:

```
CBS350(config-if)#  switchport private-vlan host-association[primary-vlan-id][secondary-vlan-id]
```

Las opciones son:

- primary-vlan-id: especifica el ID de VLAN de la VLAN principal.
- secondary-vlan-id - Especifica el ID de VLAN de la VLAN secundaria.

Paso 7. Para salir del contexto de configuración de la interfaz, introduzca lo siguiente:

```
CBS350(config-if-range)#  exit
```

Paso 8. (Opcional) Repita los pasos 2 a 7 para configurar puertos host y promiscuos más y asignarlos a las VLAN privadas primarias y secundarias correspondientes.

Paso 9. Introduzca el comando end para volver al modo EXEC con privilegios:

```
CBS350(config-if)#  end
```

Paso 10. (Opcional) Para verificar las VLAN privadas configuradas en su switch, ingrese lo siguiente:

```
CBS350#  show vlan private-vlan tag[vlan-id]
```

Paso 11. (Opcional) En el modo EXEC con privilegios del switch, guarde los parámetros configurados en el archivo de configuración de inicio ingresando lo siguiente:

```
CBS350#  copy running-config startup-config
```

Paso 12. (Opcional) Presione S para Sí o N para No en su teclado cuando aparezca el mensaje: Sobrescriba el archivo [startup-config].

Ahora ha configurado correctamente la asociación de puertos promiscuos y de host con VLAN privadas primarias y secundarias en su switch a través de la CLI.

¿Desea obtener más información sobre las VLAN para los switches empresariales de Cisco? Consulte cualquiera de los siguientes enlaces para obtener más información.

Creación de VLAN Pertenencia de puerto a VLAN Acceso y puertos troncales Grupos basados en protocolo a VLAN Configuración de puerto a VLAN VLAN basada en subred Configuración del grupo de televisión multidifusión a VLAN Grupos de VLAN basados en protocolo Acceso al puerto Multidifusión TV Pertenencia a VLAN Puerto del cliente Multidifusión TV Pertenencia a VLAN

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

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

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