Procedimientos recomendados de VLAN y consejos de seguridad para routers empresariales de Cisco

Objetivo

El objetivo de este artículo es explicar los conceptos y los pasos para realizar los procedimientos recomendados y los consejos de seguridad al configurar las VLAN en los equipos empresariales de Cisco.

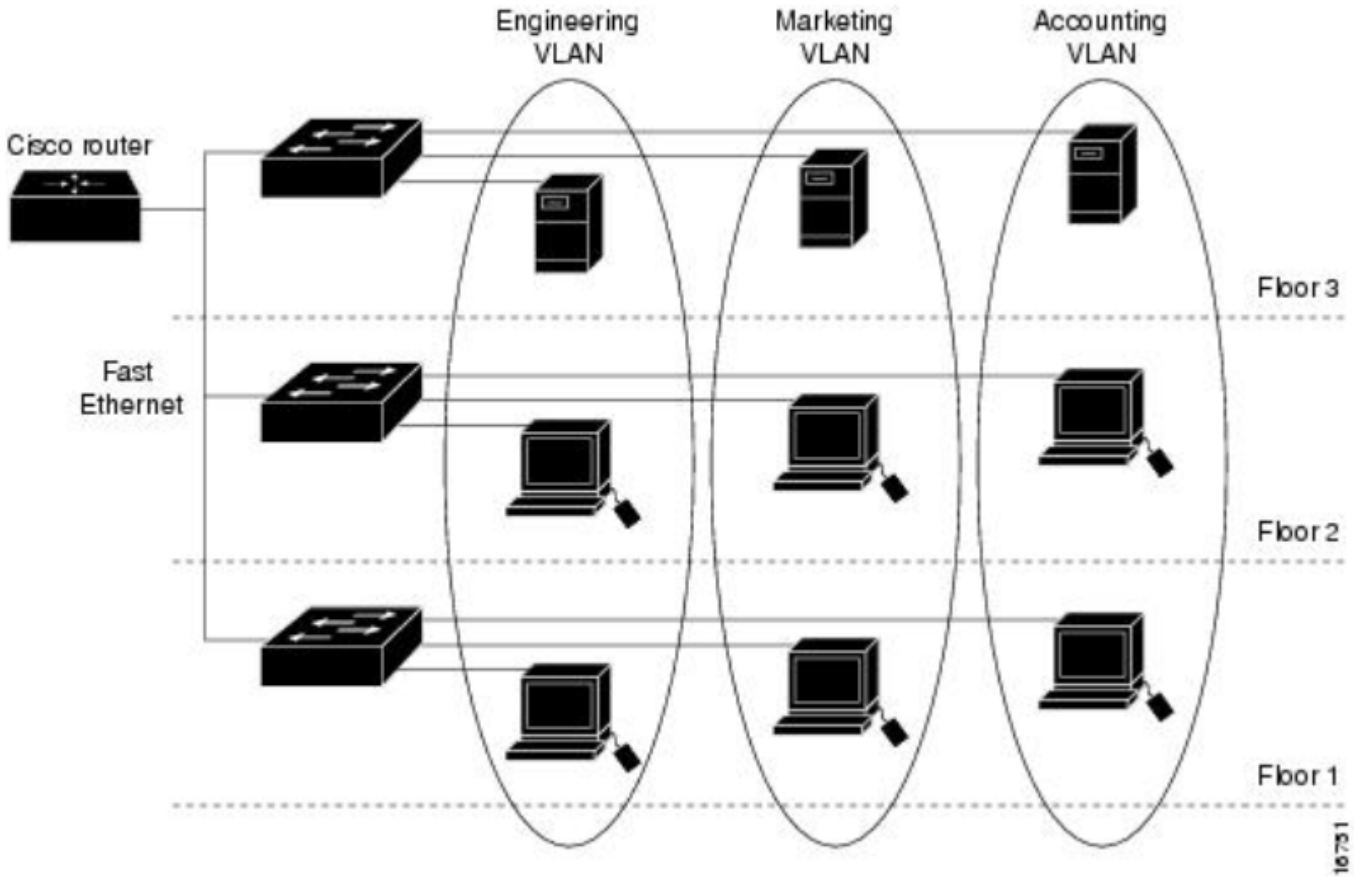
Table Of Contents

Introducción

¿Desea que su red empresarial sea más eficiente y, al mismo tiempo, que sea segura? Una de las formas de hacerlo es configurar correctamente las redes de área local virtuales (VLAN).

Una VLAN es un grupo lógico de estaciones de trabajo, servidores y dispositivos de red que parecen encontrarse en la misma red de área local (LAN) a pesar de su distribución geográfica. En pocas palabras, el hardware en las mismas VLAN permite que el tráfico entre los equipos sea independiente y más seguro.

Por ejemplo, podría tener un departamento de ingeniería, marketing y contabilidad. Cada departamento tiene trabajadores en diferentes plantas del edificio, pero todavía necesitan acceder y comunicar información dentro de su propio departamento. Es esencial para compartir documentos y servicios web.



Las VLAN deben configurarse según las prácticas recomendadas para mantener la seguridad de la red. Tome las siguientes decisiones inteligentes al configurar las VLAN. ¡No se arrepentirá!

Dispositivos aplicables

- RV042
- RV110W
- RV130
- RV132
- RV134W
- RV160W
- RV215W
- RV260
- RV260P
- RV260W
- RV320
- RV325
- RV340
- RV340W
- RV345
- RV345P

Tal vez le interese saber que los routers de las series RV160 o RV260 pueden transportar hasta 16 VLAN, mientras que los routers de la serie RV34x pueden transportar hasta 32 VLAN. El RV320 admite hasta 7 VLAN. Si desea saber cuántas VLAN puede transportar su router, consulte la hoja de datos de su modelo específico en el sitio web de Cisco. Seleccione **Soporte** e ingrese su número de modelo o simplemente busque la Hoja de datos y el número de modelo.

Vocabulario rápido para los novatos

Puerto de acceso: Un puerto de acceso transporta tráfico para una sola VLAN. Los puertos de acceso a menudo se denominan puertos sin etiquetas, ya que solo hay una VLAN en ese puerto y el tráfico se puede pasar sin etiquetas.

Puerto troncal: Puerto de un switch que transporta tráfico para más de una VLAN. Los puertos troncales a menudo se denominan puertos etiquetados, ya que hay más de una VLAN en ese puerto y el tráfico para todas las VLAN excepto una debe etiquetarse.

VLAN nativa: Una VLAN en un puerto trunk que no recibe una etiqueta. Cualquier tráfico que no tenga una etiqueta se enviará a la VLAN nativa. Es por eso que ambos lados de un trunk necesitan asegurarse de que tienen la misma VLAN nativa o el tráfico no irá al lugar correcto.

Práctica recomendada #1 - Asignación de puerto VLAN

Fundamentos de asignación de puertos

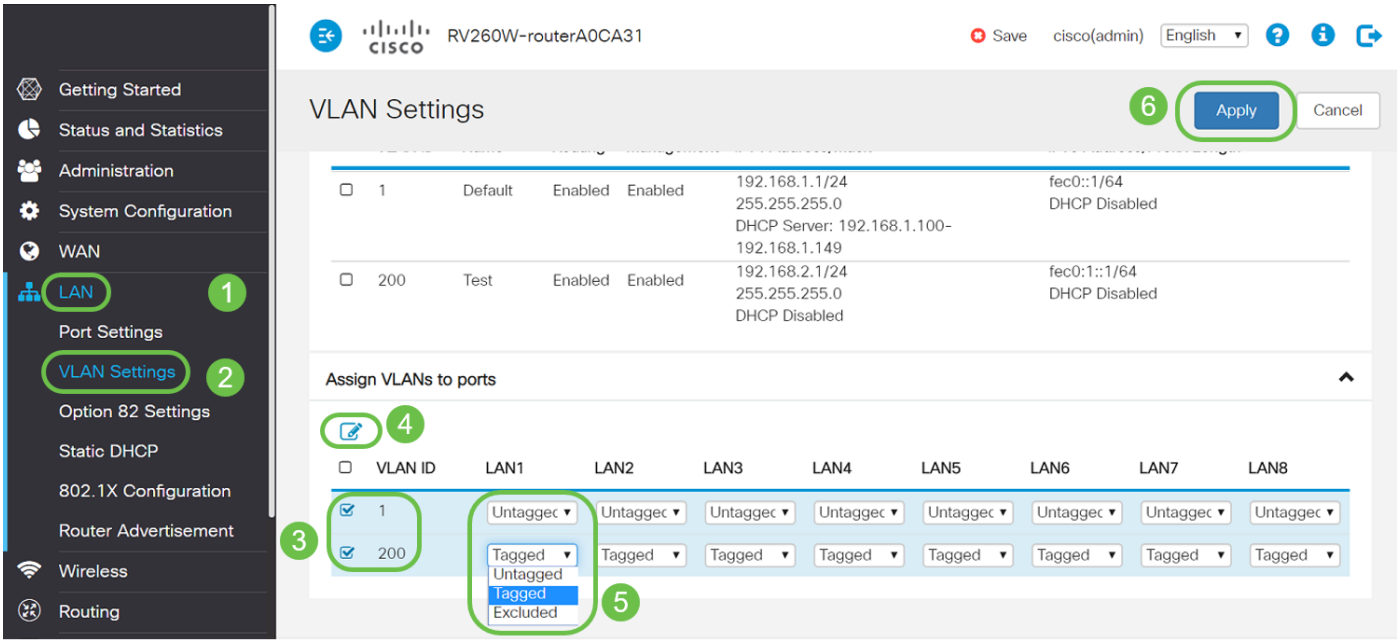
- Cada puerto LAN puede configurarse como puerto de acceso o puerto troncal.
- Las VLAN que no desee en el troncal deben excluirse.
- Una VLAN se puede colocar en más de un puerto.

Configuración de puertos de acceso

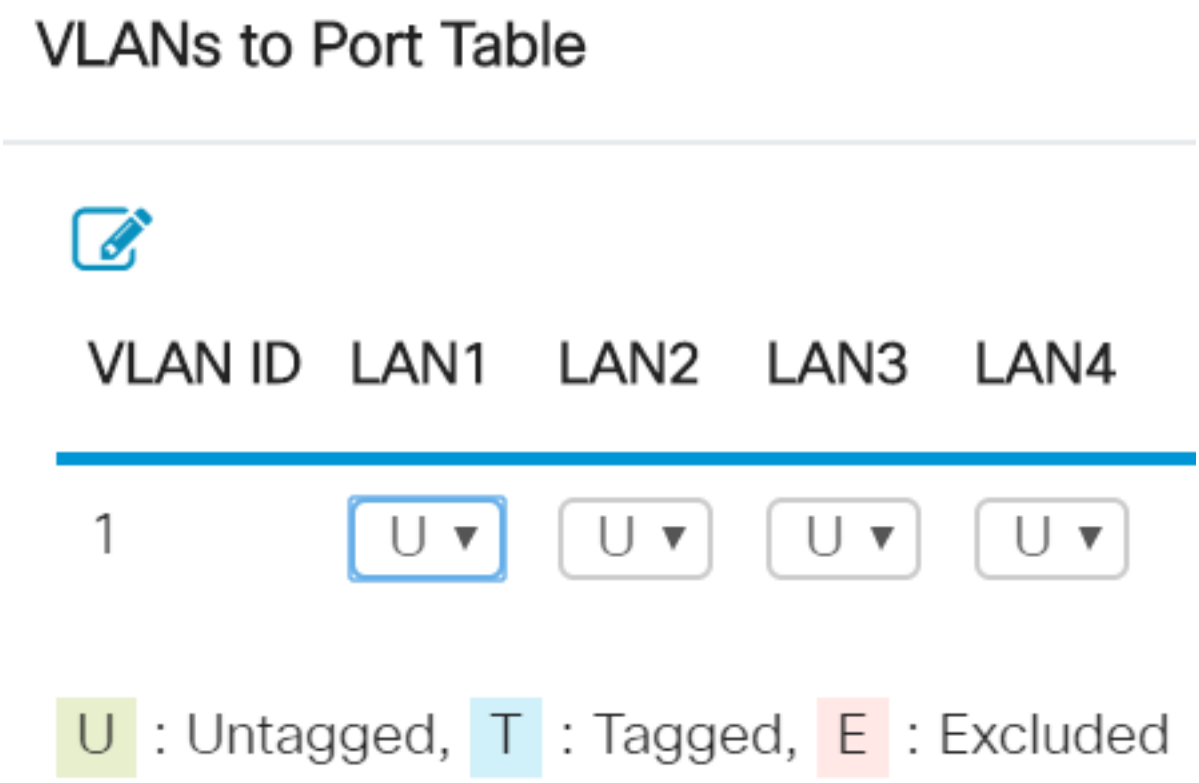
- Una VLAN asignada en un puerto LAN
- La VLAN que se asigna a este puerto debe etiquetarse como *Sin etiqueta*
- Todas las demás VLAN deben etiquetarse como *Excluded* para ese puerto

Para configurarlos correctamente, navegue hasta **LAN > VLAN Settings**. Seleccione los *ID de VLAN* y **haga clic** en el icono **edit**. Seleccione el menú desplegable para cualquiera de las interfaces LAN para las VLAN enumeradas para editar el etiquetado de VLAN. Haga clic en Apply (Aplicar).

Consulte este ejemplo de cada VLAN asignada a su propio puerto LAN:



Esta imagen de interfaz gráfica de usuario (GUI) se tomó de un router RV260W. Sus opciones pueden parecer ligeramente diferentes. Por ejemplo, en la serie RV34x, las etiquetas *Untagged*, *Excluded* y *Tagged* se abrevian como la primera letra. El proceso sigue siendo el mismo.

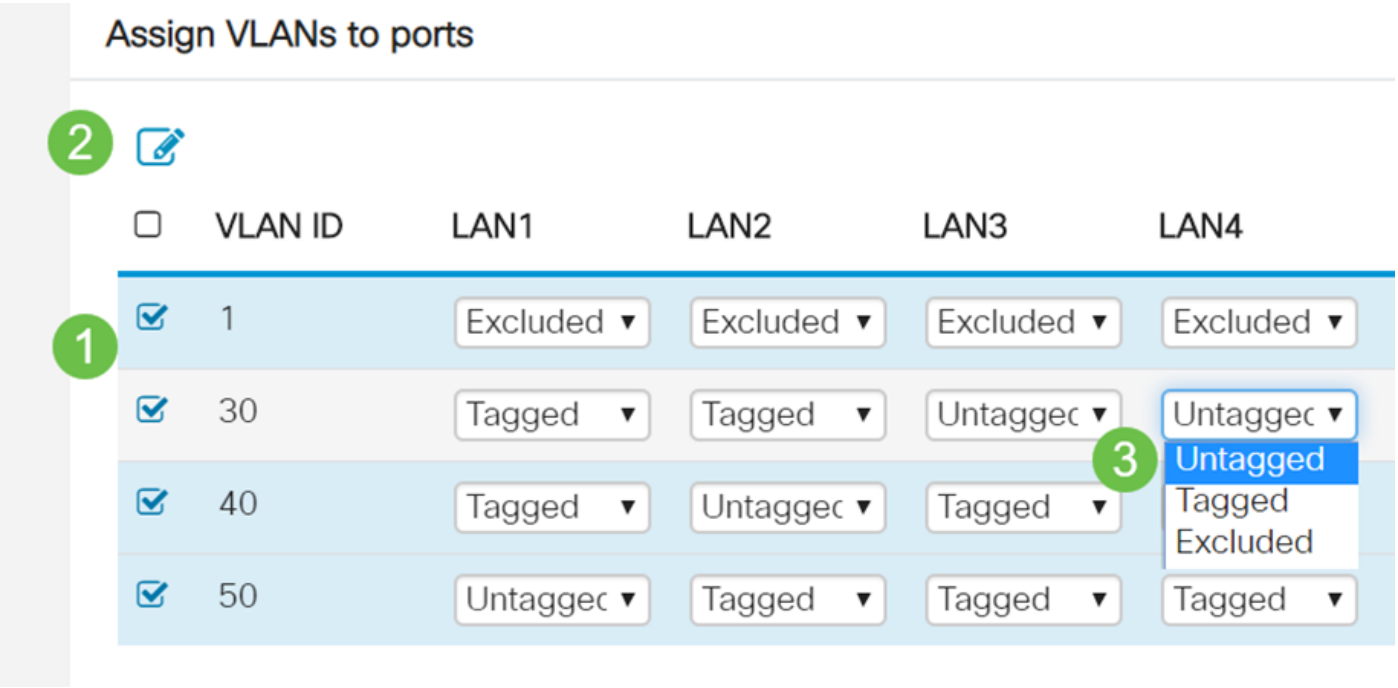


Configuración de puertos troncales

- Dos o más VLAN comparten un puerto LAN
- Una de las VLAN se puede etiquetar como *Untagged*.
- El resto de las VLAN que forman parte del puerto troncal deben etiquetarse como *Tagged*.
- Las VLAN que no forman parte del puerto trunk deben etiquetarse como *Excluded* para ese puerto.

Eche un vistazo a este ejemplo de varias VLAN que se encuentran en puertos troncales. Para configurarlos correctamente, seleccione los *ID de VLAN* que deben editarse. **Haga clic** en el icono *de edición*. Cámbielos en función de sus necesidades, siguiendo las recomendaciones

anteriores. Por cierto, ¿notó que la VLAN 1 está excluida de cada puerto LAN? Esto se explicará en la sección Práctica recomendada para la VLAN 1 predeterminada.



Preguntas Frecuentes

¿Por qué se deja una VLAN sin etiqueta cuando es la única VLAN en ese puerto?

Dado que hay una sola VLAN asignada en un puerto de acceso, el tráfico saliente del puerto se envía sin ninguna etiqueta VLAN en las tramas. Cuando la trama alcanza el puerto del switch (tráfico entrante), el switch agregará la etiqueta VLAN.

¿Por qué se etiquetan las VLAN cuando forman parte de un tronco?

Esto se hace para que el tráfico que pasa no se envíe a la VLAN incorrecta en ese puerto. Las VLAN comparten ese puerto. Similar a los números de apartamento agregados a una dirección para asegurarse de que el correo va al apartamento correcto dentro de ese edificio compartido.

¿Por qué el tráfico no se etiqueta cuando forma parte de la VLAN nativa?

Una VLAN nativa es una manera de transportar tráfico sin etiqueta a través de uno o más switches. El switch asigna cualquier trama sin etiqueta que llegue a un puerto etiquetado a la VLAN nativa. Si una trama en la VLAN nativa deja un puerto trunk (etiquetado), el switch elimina la etiqueta VLAN.

¿Por qué se excluyen las VLAN cuando no están en ese puerto?

Esto mantiene el tráfico en ese trunk solamente para las VLAN que el usuario específicamente desea. Se considera una práctica óptima.

Práctica recomendada #2: VLAN 1 predeterminada y puertos sin utilizar

Todos los puertos deben asignarse a una o más VLAN, incluida la VLAN nativa. Los routers Cisco Business vienen con VLAN 1 asignada a todos los puertos de forma predeterminada.

Una VLAN de administración es la VLAN que se utiliza para administrar, controlar y supervisar de forma remota los dispositivos de la red mediante Telnet, SSH, SNMP, syslog o FindIT de Cisco. De forma predeterminada, también es VLAN 1. Una buena práctica de seguridad consiste en separar el tráfico de datos de usuarios y administración. Por lo tanto, se recomienda que cuando configure las VLAN, utilice la VLAN 1 solamente para fines de administración.

Para comunicarse remotamente con un switch de Cisco con fines de administración, el switch debe tener una dirección IP configurada en la VLAN de administración. Los usuarios de otras VLAN no podrán establecer sesiones de acceso remoto al switch a menos que se enruten a la VLAN de administración, lo que proporciona una capa adicional de seguridad. Además, el switch debe configurarse para aceptar solamente sesiones SSH cifradas para la administración remota. Para leer algunas discusiones sobre este tema, haga clic en los siguientes enlaces en el sitio web de la Comunidad de Cisco:

- Discusión sobre VLAN de administración #1
- Discusión sobre VLAN de administración #2

Preguntas Frecuentes

¿Por qué no se recomienda la VLAN 1 predeterminada para segmentar virtualmente la red?

La razón principal es que los actores hostiles saben que la VLAN 1 es la predeterminada y que se utiliza con frecuencia. Pueden utilizarlo para obtener acceso a otras VLAN a través del "salto de VLAN". Como su nombre indica, el actor hostil puede enviar tráfico simulado que se hace pasar por VLAN 1, lo que permite el acceso a los puertos troncales y, por lo tanto, a otras VLAN.

¿Puedo dejar un puerto sin usar asignado a la VLAN 1 predeterminada?

Para mantener la seguridad de su red, no debería hacerlo. Se recomienda configurar todos los puertos que se asociarán con VLAN distintas de la VLAN 1 predeterminada.

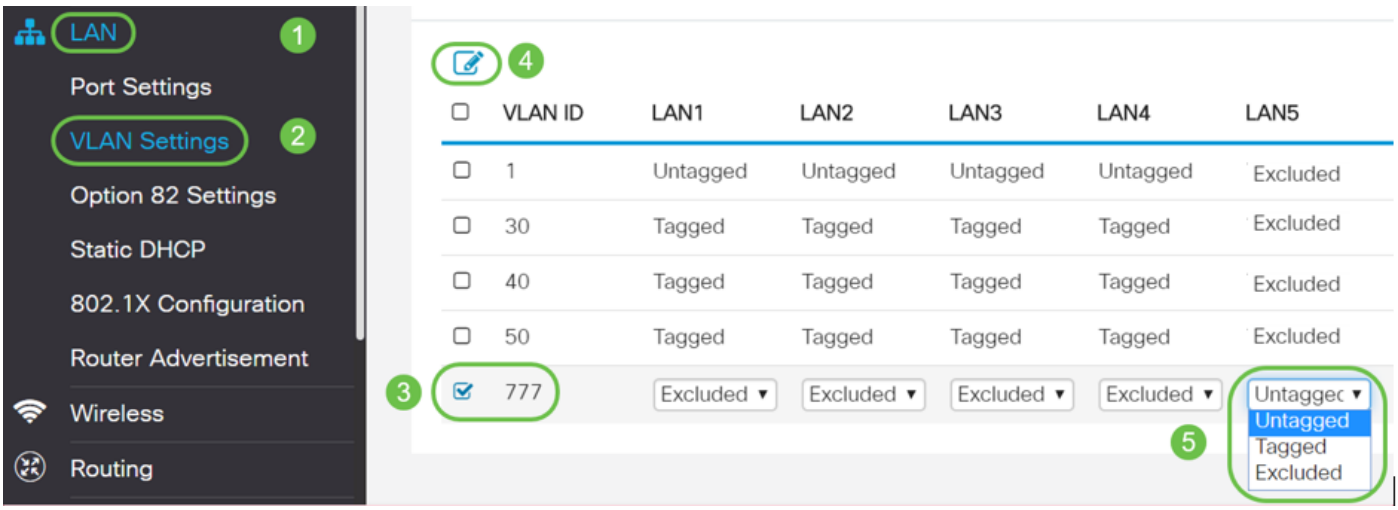
No deseo asignar ninguna de mis VLAN de producción a un puerto no utilizado. ¿Qué puedo hacer?

Se recomienda crear una VLAN "sin conexión" siguiendo las instrucciones de la siguiente sección de este artículo.

Práctica recomendada #3 - Crear una VLAN "sin salida" para puertos no utilizados

Paso 1. Vaya a **LAN > VLAN Settings**.

Elija cualquier número aleatorio para la VLAN. Asegúrese de que esta VLAN no tenga habilitado DHCP, el ruteo entre VLAN o la administración de dispositivos. Esto mantiene las otras VLAN más seguras. Coloque cualquier puerto LAN no utilizado en esta VLAN. En el siguiente ejemplo, se creó *VLAN 777* y se asignó a *LAN5*. Esto debe hacerse con todos los puertos LAN no utilizados.



Observe que las otras VLAN están excluidas de este puerto LAN.

Paso 2. **Haga clic** en el botón *Aplicar* para guardar los cambios de configuración que ha realizado.

Práctica recomendada #4 - Teléfonos IP en una VLAN

El tráfico de voz presenta estrictos requisitos de calidad de servicio (QoS). Si su empresa tiene ordenadores y teléfonos IP en la misma VLAN, cada uno intenta utilizar el ancho de banda disponible sin tener en cuenta el otro dispositivo. Para evitar este conflicto, se recomienda utilizar VLAN independientes para el tráfico de voz y de datos de telefonía IP. Para obtener más información sobre esta configuración, consulte los siguientes artículos y vídeos:

- Charla técnica de Cisco: Configuración y configuración de VLAN de voz mediante productos Cisco Small Business (vídeo)
- Configuración de VLAN de voz automática con QoS en el switch de la serie SG500
- Configuración de VLAN de voz en los switches gestionados serie 200/300
- Charla técnica de Cisco: Configuración de la VLAN de voz automática en los switches de las series SG350 y SG550 (vídeo)

Práctica recomendada #5 - Routing entre VLAN

Las VLAN se configuran de modo que el tráfico pueda ser independiente, pero a veces se necesitan VLAN para poder rutear entre sí. Esto es ruteo entre VLAN y generalmente no se recomienda. Si es necesario para su empresa, configúrela de la forma más segura posible. Cuando utilice el ruteo entre VLAN, asegúrese de restringir el tráfico usando las Listas de control de acceso (ACL), a los servidores que contienen información confidencial.

Las ACL realizan el filtrado de paquetes para controlar el movimiento de paquetes a través de una red. El filtrado de paquetes proporciona seguridad al limitar el acceso del tráfico a una red, restringir el acceso de usuarios y dispositivos a una red e impedir que el tráfico salga de una red. Las listas de acceso IP reducen la posibilidad de que se produzcan ataques de suplantación y denegación de servicio, y permiten el acceso temporal y dinámico de usuarios a través de un firewall.

- Routing entre VLAN en un router RV34x con restricciones de ACL dirigidas
- Charla técnica de Cisco: Configuración del routing Inter-VLAN en switches de la serie SG250 (vídeo)
- Charla técnica de Cisco: Configuración Inter-VLAN en RV180 y RV180W (vídeo)
- Limitación de Acceso entre VLAN RV34x (corrección de errores CSCvo92300)

Conclusión

Ahí lo tiene, ahora conoce algunas prácticas recomendadas para configurar VLAN seguras. Tenga en cuenta estos consejos al configurar las VLAN para su red. A continuación se enumeran algunos artículos que tienen instrucciones paso a paso. Esto le permitirá avanzar hacia una red productiva y eficiente, adecuada para su empresa.

- Configuración de los parámetros de VLAN en el RV160 y el RV260
- Configuración de los parámetros de red de área local virtual (VLAN) en un router de la serie RV34x
- Configuración de la pertenencia a VLAN en routers VPN RV320 y RV325
- Configuración de la pertenencia a una red de área local virtual (VLAN) en un router de la serie RV
- Configuración de la dirección IPv4 de la interfaz VLAN en un switch Sx350 o SG350X a través de la CLI