



UNIVERSIDAD AUTÓNOMA DE CHIAPAS

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN “CAMPUS I”

**LICENCIATURA EN INGENIERÍA EN DESARROLLO Y TECNOLOGÍAS DE
SOFTWARE**

CONMUTADORES Y REDES INALAMBRICAS

7º “M”

ALUMNO:

JORGE DAVID LEPE HERNÁNDEZ

DOCENTE: GUTIERREZ ALFARO LUIS, DR.

**ACT. 3.2 INVESTIGACIÓN DEL PROTOCOLO VTP EN UNA RED CONMUTADA
CONVERGENTE.**

TUXTLA GUTIÉRREZ, CHIAPAS A 07 DE OCTUBRE DE 2024

Contenido

INTRODUCCION	1
¿Qué es el VTP?	2
Descripción general del VTP	2
El desafío de administrar la VLAN con VTP	4
Componentes del VTP	6
Operación del VTP	8
Dominios de VTP	10
Modos de VTP	12
Configuración del VTP	12
Conclusión del VTP	16
Bibliografía	17

INTRODUCCION

El VTP (VLAN Trunking Protocol) es un protocolo creado por Cisco Systems que permite la administración centralizada de las VLANs (Virtual Local Area Networks) en una red compuesta por múltiples switches. En entornos donde se utilizan muchas VLANs, su configuración manual en cada switch sería laboriosa y propensa a errores. VTP automatiza este proceso al propagar los cambios de configuración desde un switch configurado como servidor a todos los demás switches dentro del mismo dominio VTP, asegurando que todas las VLANs sean consistentes en toda la red.

El funcionamiento de VTP se basa en el intercambio de anuncios periódicos que contienen la información sobre la configuración actual de las VLANs, como el número de VLANs, sus nombres y otros atributos. Estos anuncios se propagan a través de los enlaces trunk entre switches, asegurando que cualquier cambio en la configuración de VLAN en el switch servidor sea replicado automáticamente en los switches configurados como clientes. Esto reduce la complejidad y el esfuerzo de gestionar grandes redes, y disminuye el riesgo de errores de configuración manual.

Uno de los elementos clave del protocolo es el número de revisión de configuración, que se incrementa cada vez que se realiza un cambio en las VLANs. Los switches en un dominio VTP comparan este número con el suyo propio; si el número es más alto en un anuncio VTP recibido, los switches actualizan su configuración con la nueva información.

VTP ofrece tres modos de operación: servidor, cliente y transparente. El modo servidor permite crear, modificar y eliminar VLANs y propagar esos cambios. El modo cliente solo recibe y aplica las configuraciones, mientras que el modo transparente permite que el switch mantenga su propia base de datos de VLANs sin propagar ni recibir configuraciones de otros switches.

Sin embargo, VTP no está exento de riesgos. Un error en la configuración en el switch servidor puede propagarse por toda la red, causando problemas generalizados. Además, conectar un switch mal configurado o con un número de revisión más alto puede sobrescribir las configuraciones correctas en los demás switches del dominio. Para mitigar estos riesgos, se recomienda utilizar la versión más reciente del protocolo, VTP v3, que incluye medidas de seguridad como autenticación con contraseñas y mayor control sobre los cambios que pueden realizarse en la red.

¿Qué es el VTP?

El protocolo VTP (VLAN Trunking Protocol) es un protocolo de gestión de VLAN utilizado en redes informáticas. Permite la propagación de la información de VLAN a todos los equipos de la red, facilitando así la gestión de las VLAN en una red extendida.

El protocolo VTP es un tema clave para los profesionales de la gestión de redes, ya que ofrece una solución práctica para centralizar y simplificar la gestión de VLAN. Permite a los administradores configurar o modificar las VLAN en un solo conmutador, y luego difundir esa información a todos los demás conmutadores de la red.

Esto simplifica enormemente la configuración de las VLAN en redes de gran tamaño, permitiendo a los administradores ahorrar tiempo y minimizar errores de configuración. Sin embargo, es importante comprender las mejores prácticas de configuración para evitar problemas de seguridad y rendimiento.

Descripción general del VTP

A medida que aumenta el número de switches en una red de empresas pequeñas o medianas, la administración general requerida para administrar las VLAN y los enlaces troncales en una red se convierte en un desafío.

Suponga que las VLAN 10, 20, y 99 ya se implementaron y debe agregar ahora VLAN 30 a todos los switches. Agregar la VLAN manualmente en esta red incluiría la configuración de switches 12. En redes más grandes, la administración de VLAN puede volverse desalentadora.

El protocolo de troncal VLAN (VTP) permite que un administrador de redes maneje las VLAN en un switch configurado como servidor VTP. El servidor VTP distribuye y sincroniza la información de la VLAN en los enlaces troncales a los switches habilitados por el VTP en toda la red conmutada. Esto minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias de configuración.

Nota: El VTP solo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por la versión 1 o versión 2 de VTP. La versión 3 del VTP admite VLAN extendidas, pero no entra dentro del ámbito de este curso.

Nota: El VTP guarda configuraciones VLAN en una base de datos llamada **vlan.dat**.

La Tabla 1 ofrece una breve descripción de los componentes principales del VTP.

Componentes del VTP	Definición
Dominio del VTP	<ul style="list-style-type: none"> • Consiste en uno o más switches interconectados. • Todos los switches en un dominio comparten los detalles de configuración de la VLAN usando las publicaciones del VTP. • Los switches que están en diferentes dominios de VTP no intercambian las publicaciones del VTP. • Un router o switch de Capa 3 define el límite de cada dominio.
Publicaciones del VTP	<ul style="list-style-type: none"> • Cada switch en el dominio VTP envía publicaciones periódicas desde cada puerto de enlace troncal a una dirección de multidifusión reservada. • Los switches vecinos reciben estas publicaciones y actualizan sus configuraciones de VTP y VLAN según sea necesario.
Modos del VTP	<ul style="list-style-type: none"> • Un switch puede configurarse en modo cliente, transparente o servidor VTP.
Contraseña del VTP	<ul style="list-style-type: none"> • Los switches en el dominio VTP también pueden configurarse con una contraseña.

El desafío de administrar la VLAN con VTP

Administrar VLANs (Virtual Local Area Networks) utilizando VTP (VLAN Trunking Protocol) puede simplificar el proceso de gestión de VLANs en redes grandes, pero también conlleva ciertos desafíos y riesgos. Estos desafíos se relacionan principalmente con la seguridad, el control y la complejidad de la red. Aquí hay una descripción de los principales retos:

1. Pérdida o sobrescritura de la configuración de VLAN

Problema: El mayor riesgo con VTP ocurre cuando un switch con información incorrecta se conecta a la red y tiene un número de revisión de configuración de VLAN más alto que el resto. Debido a la forma en que funciona VTP, el switch propagará su configuración a los demás, sobrescribiendo las VLANs correctas en toda la red. Esto puede causar interrupciones significativas, como la pérdida de VLANs o la interrupción del servicio de red.

Solución: Es recomendable ajustar el número de revisión de VTP antes de conectar un switch a la red de producción. Los administradores deben asegurarse de que la información propagada sea la correcta.

2. Propagación no deseada de cambios

Problema: VTP facilita la actualización de configuraciones de VLAN en toda la red. Sin embargo, si un cambio se realiza de manera incorrecta o sin la debida planificación, este cambio se propagará a todos los switches del dominio VTP. Esto puede ser peligroso si no hay un control adecuado, ya que podría haber consecuencias no deseadas en la red, como colisiones de VLANs.

Solución: Para evitar este problema, se puede optar por usar VTP en modo transparente en switches donde no se desea que se propaguen cambios automáticos, permitiendo que los cambios sean manuales en lugar de automáticos.

3. Limitaciones en entornos grandes

Problema: En redes grandes y complejas, donde se gestionan numerosas VLANs y varios switches, el control centralizado de VLANs con VTP puede complicar la segmentación de la red, además de aumentar el riesgo de errores generalizados si algo sale mal.

Solución: Para gestionar mejor entornos grandes, es común segmentar la red en diferentes dominios VTP o usar herramientas de gestión de redes más avanzadas que permitan mayor granularidad en el control.

4. Seguridad

Problema: Si no se implementa correctamente, VTP puede ser un riesgo de seguridad. Cualquier switch que esté conectado a la red y sea parte del mismo dominio VTP puede potencialmente realizar cambios en la configuración de la VLAN si no está adecuadamente controlado. Además, la falta de autenticación en versiones anteriores de VTP puede permitir la propagación de configuraciones maliciosas.

Solución: Usar VTP v3, que ofrece autenticación mediante contraseñas y mayor control de la propagación de la configuración de VLANs. También es una buena práctica habilitar las medidas de seguridad adecuadas, como la autenticación MD5 en VTP y restringir qué dispositivos pueden unirse al dominio VTP.

5. Compatibilidad y actualizaciones

Problema: VTP tiene diferentes versiones (v1, v2 y v3) que no siempre son compatibles entre sí. Migrar de una versión a otra o integrar switches que no soportan versiones más avanzadas puede complicar la administración de VLANs y causar problemas de interoperabilidad.

Solución: Se debe hacer una planificación cuidadosa al actualizar el entorno a VTP v3 o mezclar dispositivos con diferentes versiones. Además, es fundamental asegurarse de que todos los dispositivos de la red sean compatibles.

Beneficios de usar VTP, pese a los desafíos:

Facilidad de administración: VTP reduce la carga de trabajo de los administradores al permitir la creación, modificación y eliminación de VLANs de forma centralizada.

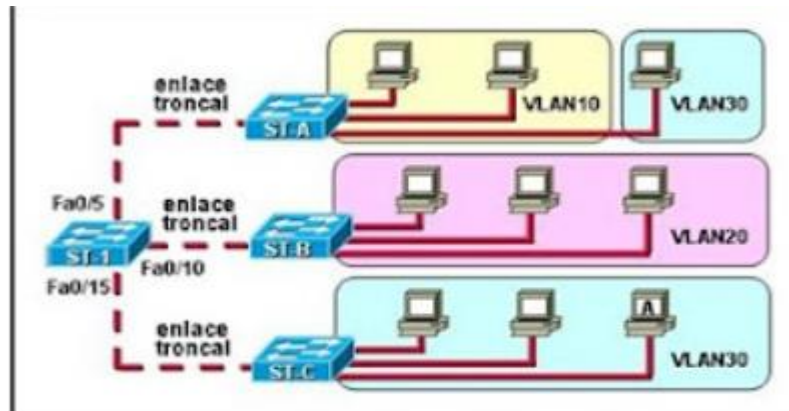
Automatización: Los cambios en las VLANs se propagan automáticamente en todos los switches del dominio VTP, evitando la necesidad de configuraciones manuales en cada switch.

Escalabilidad: Es útil para redes que están creciendo, ya que facilita la administración de VLANs en redes extensas.

Componentes del VTP

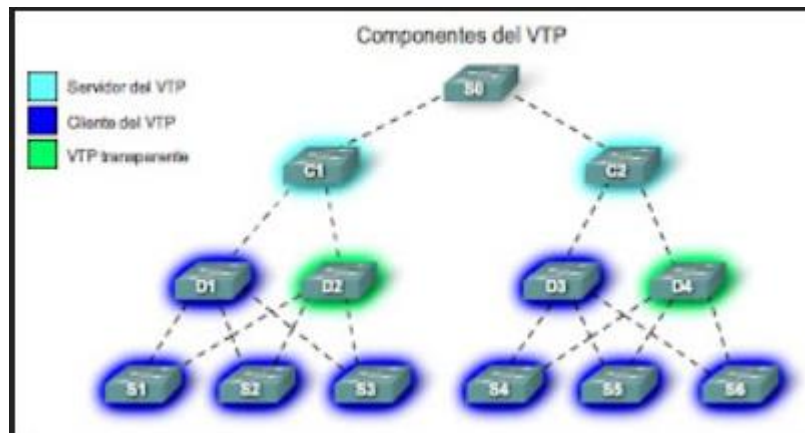
Existe un número de componentes clave el VTP:

- Dominio del VTP: Consiste en uno o más switches interconectados, todos los switches en un dominio comparten los detalles de configuración de la VLAN usando las publicaciones del VTP. Un router o switch de Capa 3 define el límite de cada dominio.



- Publicaciones del VTP: El VTP usa una jerarquía de publicaciones para distribuir y sincronizar las configuraciones de la VLAN a través de la red.
- Modos del VTP: Un switch se puede configurar en uno de tres modos: servidor, cliente o transparente.
- Servidor del VTP: los servidores del VTP publican la información VLAN del dominio del VTP a otros switches habilitados por el VTP en el mismo dominio del VTP. Los servidores del VTP guardan la información de la VLAN para el dominio completo en la NVRAM. El servidor es donde las VLAN se pueden crear, eliminar o re denominar para el dominio.
- Cliente del VTP: los clientes del VTP funcionan de la misma manera que los servidores del VTP pero no pueden crear, cambiar o eliminar las VLAN en un cliente del VTP. Un cliente del VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN. Debe configurar el modo de cliente del VTP en un switch.
- VTP transparente: los switches transparentes envían publicaciones del VTP a los clientes del VTP y servidores del VTP. Los switches transparentes no participan en el

VTP. Las VLAN que se crean, re denominan o se eliminan en los switches transparentes son locales para ese switch solamente.



- **Depuración del VTP:** La depuración del VTP aumenta el ancho de banda disponible para la red mediante la restricción del tráfico saturado a esos enlaces troncales que el tráfico debe utilizar para alcanzar los dispositivos de destino. Sin la depuración del VTP, un switch satura el broadcast, el multicast y el tráfico desconocido de unicast a través de los enlaces troncales dentro de un dominio del VTP, aunque los switches receptores podrían descartarlos.

Operación del VTP

El **VTP (VLAN Trunking Protocol)** opera facilitando la creación, administración y propagación automática de configuraciones de **VLAN** entre switches dentro de una red. Su principal función es permitir que las configuraciones de VLAN que se realicen en un solo switch (configurado como servidor) se distribuyan automáticamente a otros switches (configurados como clientes) en el mismo **dominio VTP**. A continuación, se detalla cómo funciona el VTP en su operación diaria:

Elementos clave en la operación de VTP:

1. Dominio VTP:

- Un **dominio VTP** es un grupo de switches que comparten la misma base de datos de VLANs. Todos los switches dentro de un dominio deben tener el mismo **nombre de dominio VTP** para poder intercambiar información de VLAN.
- Los cambios de VLAN hechos en un switch servidor se propagan a todos los switches dentro de ese dominio.

2. Revisión de la configuración:

- Cada vez que se realiza un cambio en la configuración de VLAN (como agregar, modificar o eliminar una VLAN), el número de **revisión de configuración** del VTP aumenta en el switch servidor.
- Los switches dentro del mismo dominio comparan su número de revisión con el del switch que envía la información. Si el número es mayor en el switch que envía la información, este último reemplaza la configuración de los switches con el número inferior.

3. Modos de operación de VTP: Existen tres modos de operación que determinan cómo se comportan los switches en un dominio VTP:

- **Modo Servidor:**
 - Este es el modo por defecto en muchos switches Cisco.
 - Los switches en modo servidor pueden crear, modificar o eliminar VLANs, y propagan esta información a todos los demás switches en el dominio VTP.

- Los cambios realizados en un switch servidor se propagan a todos los switches en el dominio.
- **Modo Cliente:**
 - Los switches en modo cliente reciben actualizaciones de VLAN desde los switches en modo servidor, pero no pueden crear, modificar ni eliminar VLANs.
 - Solo aplican los cambios de configuración que reciben de los servidores VTP.
- **Modo Transparente:**
 - Los switches en modo transparente no participan en la propagación de las configuraciones de VLAN. No aplican actualizaciones VTP, pero permiten que el tráfico VTP pase a través de ellos a otros switches.
 - En este modo, el switch mantiene su propia configuración de VLAN local y no afecta ni es afectado por los switches en los modos servidor o cliente.

4. Anuncio VTP (VTP Advertisements):

- Los switches en un dominio VTP intercambian **anuncios periódicos** para sincronizar la base de datos de VLANs. Estos anuncios incluyen el número de revisión de configuración, el nombre del dominio VTP y la lista de VLANs configuradas.
- Estos anuncios se envían por los enlaces de **trunk** y permiten que los cambios realizados en un switch servidor se propaguen rápidamente a los switches clientes.

Dominios de VTP

VTP utiliza dominios para agrupar a los switches que van a compartir la misma información de VLANs.

Dentro de un dominio de VTP se intercambia la siguiente información gracias a los anuncios de VTP:

- Nombre del Dominio
- Versión de VTP
- Lista de VLANs
- Parámetros específicos de cada VLAN

Publicación del VTP

El VTP (VLAN Trunking Protocol) fue desarrollado y publicado por Cisco Systems como parte de su suite de protocolos de red para la administración y configuración de VLANs en redes grandes. Aunque la fecha exacta de su introducción no es fácil de precisar con exactitud, el protocolo fue lanzado a mediados de la década de los 90, con la creciente adopción de redes VLAN y la necesidad de mecanismos eficientes para su administración.

Versiones de VTP:

- VTP v1 (aproximadamente en 1996):

Fue la primera versión del protocolo y permitía la creación y administración automática de VLANs en redes que usaban switches Cisco.

Permitía la propagación de configuraciones de VLAN dentro de un dominio VTP.

- VTP v2 (introducida poco después de VTP v1):

Mejóro la interoperabilidad y corrigió algunos problemas de la primera versión.

Permitió que las VLAN token ring fueran soportadas.

Permitió el uso de VTP Transparent mode, lo que brindaba flexibilidad al dejar que algunos switches no participaran en la propagación de cambios de VLAN.

Esta versión es compatible con VTP v1.

- VTP v3 (lanzada en 2009):

Introdujo una serie de mejoras significativas en comparación con las versiones anteriores, particularmente en cuanto a seguridad y control.

Añadió autenticación y protección mediante contraseña para evitar que switches no autorizados modificaran la configuración de la VLAN.

Introdujo soporte para VLANs privadas y Extended VLANs (VLANs numeradas más allá del rango de 1-1005).

Ofreció un mayor control sobre qué dispositivos pueden actuar como servidores VTP y permitir cambios.

Mejóro la capacidad de recuperación ante errores y la interoperabilidad.

- Propósito de la publicación del VTP:

La publicación de VTP tenía el objetivo de simplificar y centralizar la administración de VLANs en entornos grandes, donde múltiples switches están conectados entre sí y donde una configuración manual de cada uno sería tediosa y propensa a errores. Cisco desarrolló VTP para facilitar el trabajo de los administradores de red al permitir que los cambios de configuración de las VLANs se propaguen automáticamente desde un switch servidor VTP a todos los switches clientes en el mismo dominio VTP, reduciendo los errores y el tiempo de configuración.

- Uso en la actualidad:

Si bien VTP sigue siendo utilizado en muchas redes empresariales, especialmente donde se emplean dispositivos Cisco, algunos administradores prefieren desactivar VTP o utilizarlo en modo transparente debido a los riesgos asociados con la pérdida de configuraciones o errores de propagación no deseada en redes más grandes. VTP v3, sin embargo, ha mitigado algunos de estos riesgos al incorporar autenticación y control más granular.

Cisco continúa proporcionando actualizaciones y soporte para VTP en sus dispositivos más recientes, especialmente en entornos donde la automatización y la gestión eficiente de VLANs siguen siendo una prioridad.

Modos de VTP

Los switches dentro de un dominio de VTP pueden funcionar de tres formas diferentes:

- **Modo servidor:** Los servidores son los encargados de crear y mantener la información de todas las VLANs en la red y son los encargados de pasar esta información al resto de switches. Por defecto los switches Cisco estan en modo servidor.
- **Modo cliente:** Los switches en modo cliente no pueden hacer ninguna modificación en las VLANs y mantienen la información de VLANs gracias a los mensajes que son enviados desde los servidores
- **Modo transparente:** Los switches en modo transparente no participan en el proceso de VTP y reenvían los mensajes de VTP, pero de forma diferente dependiendo de la versión de VTP. Si es VTP versión 1 sólo se reenvían los mensajes de VTP que tengan como versión 1 y que correspondan al nombre de dominio que tengan configurado. En VTP versión 2 sin embargo los switches transparentes son capaces de reenviar los mensajes VTP, aunque no correspondan ni a la versión que tiene el switch configurado ni al dominio en el que esté incluido este switch en modo transparente

Configuración del VTP

La configuración de VTP en los switches Cisco con IOS es bastante sencilla ya que lo único que tenemos que configurar es el dominio de VTP y el modo, opcionalmente la versión, password, etc...

Por defecto la configuración que se utilizará al configurar VTP es la versión 1, aunque la versión 2 tiene las siguientes ventajas sobre la versión 1:

- En los switches en modo transparente la versión 2 permitirá que se reenvíen los anuncios recibidos de VTP independientemente de su versión o dominio.
- La versión 2 realiza una comprobación de consistencia al introducir los comandos por CLI o mediante SNMP, pero no realizaría esta comprobación en los anuncios recibidos desde otros switches.
- Soporte para Token Ring

Configurar la versión de VTP es tan simple como introducir este comando de configuración global:

```
switch(config)#vtp version {1 | 2 | 3}
```

Para configurar el modo y la password en las actualizaciones VTP utilizaremos estos comandos:

```
switch(config)#vtp mode { server | transparent | client}  
switch(config)#vtp password password
```

Así pues un ejemplo de configuración podría ser el siguiente:

```
switch(config)#vtp version 2  
switch(config)#vtp mode server  
switch(config)#vtp password mi_super_password
```

VTP Pruning

El VTP Pruning es un método que impide que las actualizaciones de VTP se reenvíen por todos los puertos de trunk, de esta forma podemos limitar la propagación de VTP a una porción de la red bien definida, reduciendo así el proceso de información y el tráfico innecesario por los trunks. Recordemos que VTP utiliza mensajes multicast y estos al igual que los mensajes de broadcast por defecto se reenvían por todos los puertos de la VLAN excepto por el que se ha recibido.

La configuración de VTP Pruning tampoco resulta ser demasiado engorrosa, lo único que tenemos que tener en cuenta es que por defecto viene deshabilitado y será necesario habilitarlo de la siguiente forma:

```
switch(config)#vtp                                     pruning  
switch(config-if)#switchport trunk pruning vlan { add | except | none | remove } lista-de-  
vlans
```

Como se puede apreciar se utiliza la misma terminología que en los comandos de configuración de trunks, con lo que no es necesario explicar ya que se han explicado con anterioridad.

Troubleshooting de VTP

VTP es un protocolo sencillo de configurar, pero complicado teniendo en cuenta los parámetros globales entre switches a tener en cuenta, por eso es importante reparar la siguiente lista en caso de problemas:

- Si el switch es transparente comprobar la versión que se está utilizando, hay que tener en cuenta que si no reenvía anuncios de VTP puede ser por estar utilizando la versión 1 que es la que viene por defecto

- Comprobar que no haya más de un switch en modo servidor
- Comprobar que todos los trunks estén configurados como trunk y no como puertos de acceso
- Comprobar que el nombre de dominio VTP sea el mismo en todos los switches
- Comprobar que la password sea la misma
- Comprobar la versión en todos los switches para que coincida

Los siguientes comandos son los que nos van a ayudar a realizar el troubleshooting de VTP:

Switch# show vtp status

VTP Version : 2

Configuration Revision : 250

Maximum VL nabled

VTP V2 Mode : Enabled

VTP Traps Generation : Disabled

MD5 digest : 0xE6 0xF8 0x3E 0xDD 0xA4 0xF5 0xC2 0x0E

Configuration last modified by 172.20.52.18 at 9-22-99 11:18:20

Local updater ID is 172.20.52.18 on interface Vl1 (lowest numbered VLAN interface found)

Switch#

Switch# show vtp counters

VTP statistics:

Summary advertisements received : 1

Subset advertisements received : 1

Request advertisements received : 0

Summary advertisements transmitted : 31

Subset advertisements transmitted : 1

Request advertisements transmitted : 0

Number of config revision errors : 0

Number of config digest errors : 0

Number of V1 summary errors : 0

VTP pruning statistics:

Trunk Join Transmitted Join Received Summary advts received from non-pruning-capable device

Fa5/9 1555 1564 0

Switch#

Switch# show vlan brief

VLAN Name Status Ports

1 default active Fa5/9

2 VLAN0002 active Fa5/9

3 VLAN0003 active Fa5/9

4 VLAN0004 active Fa5/9

5 VLAN0005 active Fa5/9

10 VLAN0010 active Fa5/9

.

.

Switch# show interfaces switchport module 1

Name:Gi1/1

Switchport:Enabled

Administrative Mode:dynamic auto

Operational Mode:down

Administrative Trunking Encapsulation:negotiate

Negotiation of Trunking:On

Access Mode VLAN:1 (default)

Trunking Native Mode VLAN:1 (default)

Administrative private-vlan host-association:none

Administrative private-vlan mapping:none

Operational private-vlan:none

Trunking VLANs Enabled:ALL

Pruning VLANs Enabled:2-1001

Conclusión del VTP

El VLAN Trunking Protocol (VTP) de Cisco es una herramienta poderosa y eficiente que simplifica la administración de VLANs en redes grandes, al permitir la propagación automática de configuraciones entre switches dentro de un mismo dominio VTP. Esta automatización reduce significativamente el esfuerzo manual necesario para gestionar redes extensas, ayudando a evitar errores humanos en la configuración y garantizando la consistencia en la estructura de VLANs de toda la red. Al utilizar VTP, los administradores de red pueden implementar, modificar o eliminar VLANs en un solo switch y tener la certeza de que dichos cambios se aplicarán de manera uniforme en todos los switches conectados.

No obstante, el uso de VTP también conlleva ciertos riesgos, como la sobrescritura accidental de configuraciones correctas si no se controla adecuadamente el número de revisión o si un switch mal configurado es agregado al dominio. Estos problemas pueden generar interrupciones importantes en el servicio y complicaciones en la recuperación de la red. Para mitigar estos riesgos, es recomendable implementar VTP v3, que ofrece mayor seguridad mediante el uso de autenticación y permite un control más estricto sobre qué dispositivos pueden realizar cambios en la red.

En conclusión, VTP es una solución ideal para la gestión centralizada de VLANs en redes grandes y complejas, pero su uso debe estar acompañado de buenas prácticas de seguridad y administración, tales como la autenticación de dispositivos y una planificación cuidadosa de las configuraciones. Esto asegura que las ventajas del protocolo, como la facilidad de gestión y la escalabilidad, se maximicen sin poner en riesgo la estabilidad de la red.

Bibliografía

Walton, A. (2024, 8 febrero). *¿Qué es VTP (VLAN Trunking Protocol)?*: Comprende su Función. CCNA Desde Cero. https://ccnadesdecero.es/vtp-vlan-trunking-protocol-que-es/#VTP_Vlan_Trunk_Protocol

Descripción general del VTP. (s. f.).

<https://redesconfiguracion.blogspot.com/2018/04/descripcion-general-del-vtp.html>

Unknown. (s. f.). *Componentes del VTP.* [https://caracteristicas-de-](https://caracteristicas-de-vtp.blogspot.com/2013/06/componentes-del-vtp.html)

[vtp.blogspot.com/2013/06/componentes-del-vtp.html](https://caracteristicas-de-vtp.blogspot.com/2013/06/componentes-del-vtp.html)

Aprende Redes.com » Modos de operación VTP. (s. f.).

<https://aprenderedes.com/2020/03/modos-de-operacion-vtp/>

Collado, E. (2019, 28 febrero). *VTP, VLAN Trunking Protocol - Eduardo Collado.*

Eduardo Collado. <https://www.eduardocollado.com/2018/04/02/pocast-142-vtp-vlan-trunking-protocol/>