Mejores prácticas para Switches de las 4500/4000 Series de la serie y del Catalyst del Catalyst 6500/6000 que funciona con el Cisco IOS Software

Contenido

Información Relacionada

Introducción

Este documento proporciona prácticas recomendadas para los switches Catalyst 6500/6000 y 4500/4000 Series que ejecutan Cisco IOS® Software en Supervisor Engine.

El Switches de las Catalyst 6500/6000 y Catalyst 4500/4000 Series soporta uno de estos dos sistemas operativos que se ejecuten en el Supervisor Engine:

- Catalyst OS (CatOS)
- Cisco IOS Software

Con CatOS, hay la opción para funcionar con el Cisco IOS Software en las placas hija o los módulos del router por ejemplo:

- El (MSFC) de la Multilayer Switch Feature Card en el Catalyst 6500/6000
- 4232 el módulo de la capa 3 (L3) en el Catalyst 4500/4000

En este modo, hay dos líneas de comando para la configuración:

- La línea de comando catos para conmutar
- La línea de comando del Cisco IOS Software para rutear

CatOS es el software del sistema, que se ejecuta en el Supervisor Engine. El Cisco IOS Software que se ejecuta en el módulo de ruteo es una opción que requiere el software del sistema de CatOS.

Para el Cisco IOS Software, hay solamente una línea de comando para la configuración. En este modo, las funciones de CatOS se han integrado en el Cisco IOS Software. La integración da lugar a una línea de comando único para la transferencia y la configuración de ruteo. En este modo, el Cisco IOS Software es el software del sistema, y substituye CatOS.

Los sistemas operativos de CatOS y del Cisco IOS Software se despliegan en las redes críticas. CatOS, con las placas hija y los módulos de la opción para router del Cisco IOS Software, se soporta en estas series del Switch:

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

El software del sistema del Cisco IOS se soporta en estas series del Switch:

- Catalyst 6500/6000
- Catalyst 4500/4000

Refiera a las mejores prácticas del documento para el Switches de los Catalyst 4500/4000, 5500/5000, y 6500/6000 Series que funciona con la configuración y la administración para información de CatOS en CatOS porque este software del sistema del Cisco IOS de los documentos abarca.

El software del sistema del Cisco IOS proporciona a los usuarios con algunas de estas ventajas:

- Una interfaz del único usuario
- Una plataforma de administración de redes unificada

- Características aumentadas de QoS
- Soporte del Distributed Switching

Este documento proporciona el guía para la configuración modular. Por lo tanto, usted puede leer cada sección independientemente y realizar los cambios en un acercamiento organizado. Este documento asume una Comprensión básica y una familiaridad con la interfaz de usuario del Cisco IOS Software. El documento no cubre el diseño de red de oficinas centrales total.

Antes de comenzar

Antecedente

Las soluciones que este documento ofrece representan los años de experiencia de campo de los ingenieros de Cisco que trabajan con las redes complejas y muchas de los clientes más grandes. Por lo tanto, este documento hace hincapié en las configuraciones reales que posibilitan el correcto funcionamiento de las redes. Este documento ofrece estas soluciones:

- Soluciones que tienen, estadístico, la exposición de campo más amplio y, así, el más poco arriesgado
- Soluciones que son simples, que negocian una cierta flexibilidad para los resultados deterministas
- Soluciones que son fáciles de manejar y que configuran los equipos de las operaciones de la red
- Soluciones que promueven la Alta disponibilidad y la alta estabilidad

Referencias

Hay muchos sitios de la referencia para las líneas de producto del Catalyst 6500/6000 y del Catalyst 4500/4000 en el cisco.com. Las referencias que esta sección enumera proporcionan la profundidad adicional en los temas que este documento discute.

Refiera al soporte del LAN Switching Technology para más información sobre los temas uces de los que este los documentos abarca. La página de soporte proporciona la Documentación del Producto así como troubleshooting y los documentos sobre configuración.

Este documento proporciona las referencias al material en línea público de modo que usted pueda leer más lejos. Pero, otras buenas referencias fundacionales y educativas sea:

- Esencial del ISP de Cisco
- Comparación del Cisco Catalyst y de los sistemas operativos del Cisco IOS para el Cisco Catalyst 6500 Series Switch
- El conmutar del Cisco LAN (serie del Desarrollo profesional CCIE)
- Redes de switch de múltiples capas constructivas de Cisco
- Funcionamiento y administración de fallas
- CAJA FUERTE: Un Plan General de Seguridad para Redes para Empresas
- Manual de campo de Cisco: Configuración del switch Catalyst

Configuración Básica

Esta sección discute las características se despliegan que cuando usted utiliza las mayorías de

las redes Catalyst.

Protocolos del Plano de Control de Catalyst

Esta sección se refiere a los protocolos que se ejecutan entre los switches en circunstancias normales de operación. Una Comprensión básica de los protocolos es útil cuando usted aborda cada sección.

Tráfico del Supervisor Engine

La mayoría de las características que se habilitan en una red Catalyst requieren dos o más Switches cooperar. Por lo tanto, debe haber un intercambio controlado de los mensajes de keepalive, de los parámetros de la configuración, y de los cambios de administración. Si estos protocolos son propietario de Cisco, tal como Cisco Discovery Protocol (CDP), o basado en estándares, por ejemplo el IEEE 802.1D (Spanning Tree Protocol [STP]), todos tienen ciertos elementos en el campo común cuando los protocolos se implementan en el Catalyst Series.

En el reenvío de tramas básico, las tramas de datos del usuario originan de los sistemas extremos. El source address (SA) y el Destination Address (DA) de los marcos de datos no se cambian en la capa 2 (dominios L2)-switched. Las tablas de búsqueda de memoria direccionable por contenido (CAM) en cada Supervisor Engine del Switch son pobladas por un proceso de aprendizaje SA. Las tablas indican qué puerto de egreso adelante cada trama se recibe que. Si el destino es desconocido o la trama se destina a un broadcast o a una dirección Multicast, el proceso de aprendizaje de direcciones es incompleto. Cuando el proceso es incompleto, la trama se remite (inundado) hacia fuera a todos los puertos en ese VLA N. El Switch debe también reconocer qué tramas deben ser conmutadas a través del sistema y qué tramas deben ser dirigidas al Switch CPU sí mismo. El Switch CPU también se conoce como el procesador de administración de red (NMP).

Las entradas especiales en la tabla CAM se utilizan para crear el avión del control del Catalyst. Estas entradas especiales se llaman las entradas del sistema. El avión del control recibe y dirige el tráfico al NMP en un puerto de switch interno. Así, con el uso de los protocolos con los MAC Address de destino conocido, el tráfico del plano del control se puede separar del tráfico de datos.

Cisco tiene un rango reservado del MAC Ethernet y de las direcciones de protocolo, pues la tabla en esta sección muestra. Este los documentos abarca cada dirección reservada detalladamente, pero esta tabla proporciona un resumen, para la conveniencia:

Función	Tipo de protocolo del HDLC[2] de la BROCHE[1]	MAC de Multicast de Destino
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+, RPVST+4	0x010b	01-00-0c-cc-cc-cd
VLAN Bridge	0x010c	01-00-0c-cd-cd-ce
UDLD5	0x0111	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP6	0x2004	01-00-0c-cc-cc-cc
STP UplinkFast	0x200a	01-00-0c-cd-cd-cd

Árbol de expansión IEEE 802.1D	N/A — DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00
ISL[9]	N/A	01-00-0c-00-00-00
VTP[10]	0x2003	01-00-0c-cc-cc-cc
Pausa 802.3x de IEEE	N/A - DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

[1] BROCHE = Subnetwork Access Protocol.

[2] HDLC = High-Level Data Link Control.

[3] PAgP = Port Aggregation Protocol.

[4] PVST+ = por el árbol de expansión de VLAN + y el RPVST+ = PVST+ rápido.

[5] UDLD = detección de link unidireccional.

[6] DTP = protocolo dynamic trunking.

[7] DSAP = punto de acceso del servicio de destino.

[8] SSAP = punto de acceso de servicio de origen.

[9] ISL = link entre switches.

[10] VTP = VLAN Trunk Protocol.

Las mayorías de los protocolos de control Cisco utilizan un encapsulado SNAP de IEEE 802.3, que incluye el Logical Link Control (LLC) 0xAAAA03 y el Identificador organizacional único (OUI) 0x00000C. Usted puede ver esto en una traza del analizador LAN.

Estos protocolos suponen conectividad de punto a punto. Observe que el uso deliberado de los permisos de las direcciones de destino de Multicast dos switches de Catalyst transparente de comunicar sobre el Switches del no Cisco. Los dispositivos que no entienden e interceptan las tramas las inundan simplemente. Sin embargo, las conexiones de punto a multipunto a través de los entornos de proveedores múltiples pueden dar lugar a la conducta incoherente. Evite generalmente las conexiones de punto a multipunto a través de los entornos de proveedores múltiples. Estos protocolos terminan en los 3 Router y la función de la capa solamente dentro de un dominio del Switch. Estos protocolos reciben prioridad sobre los datos del usuario mediante el procesamiento y la programación del Circuito Integrado para Aplicaciones Específicas (ASIC) de entrada.

Ahora las vueltas de la discusión al SA. Los protocolos del Switch utilizan una dirección MAC que se tome de un banco de las direcciones disponibles. Un EPROM en el chasis proporciona el banco de las direcciones disponibles. Publique el **comando show module** para visualizar los intervalos de direcciones que están disponibles para cada módulo para la compra de componentes del tráfico tal como Unidades STP (BPDU) o tramas ISL. Esto es una salida del comando de ejemplo:

```
>show module … Mod MAC-Address(es) Hw Fw Sw --- ---------------------------------------- ------ --
-------- ---------------- 1 00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2 6.1(3) 6.1(1d) 00-01-c9-
```

```
da-0c-1c to 00-01-c9-da-0c-1 00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff !--- These are the MACs for
sourcing traffic.
```

VLAN 1

VLAN 1 tiene un significado especial en las redes Catalyst.

Cuando el enlace, el Motor de Supervisor de Catalyst utiliza siempre el VLAN predeterminado, VLAN1, para marcar varios protocolos del control con etiqueta y de la Administración. Tales protocolos incluyen el CDP, el VTP, y el PAgP. Todos los puertos del switch, que incluye la interfaz interna del sc0, se configuran por abandono para ser los miembros de VLAN 1. Todos los trunks llevan el VLAN1 por abandono.

Estas definiciones son necesarias para ayudar a aclarar algunos términos bien-usados en las Conexiones de redes Catalyst:

- El VLAN de administración es donde el sc0 reside para CatOS y el Switches de menor capacidad. Usted puede cambiar este VLA N. Lleve esto en la mente cuando usted está intertrabajando el Switches de CatOS y del Cisco IOS.
- El VLAN nativo es el VLA N al cual un puerto vuelve cuando no es enlace. También, el VLAN nativo es el VLAN sin Tags en un trunk del IEEE 802.1Q.

Hay varios motivos válidos para ajustar una red y alterar el comportamiento de los puertos en la VLAN 1:

- Cuando el diámetro del VLAN1, como cualquier otro VLA N, consigue bastante grande ser un riesgo a la estabilidad, determinado de una perspectiva STP, usted necesita podar detrás el VLA N. Vea el administrador de switches sección interconectar y del VLAN nativo para los detalles.
- Usted necesita guardar los datos del avión del control sobre el VLAN1 a parte de los datos del usuario para simplificar el troubleshooting y maximizar los ciclos de la CPU disponibles. Evite los loopes de la capa 2 en el VLAN1 cuando usted diseña las redes de Campus multicapa sin el STP. Para evitar los loopes de la capa 2, manualmente VLAN1 claro de los puertos troncales.

En resumen, tenga en cuenta la siguiente información sobre los trunks:

- Las actualizaciones de CDP, VTP y PAgP siempre se reenvían en trunks con una etiqueta VLAN 1. Esto ocurre incluso si se eliminó la VLAN1 de los troncos y no es la VLAN nativa. Si usted borra el VLAN1 para los datos del usuario, la acción no tiene ningún impacto en el tráfico del plano del control que todavía se envía con el uso del VLAN1.
- En un trunk ISL, los paquetes DTP se envían a través de VLAN1. Éste es el caso incluso si el VLAN1 se ha borrado del trunk y es no más el VLAN nativo. En un trunk 802.1q, los paquetes DTP se envían a través de la VLAN nativa. Éste es el caso incluso si el VLAN nativo se ha borrado del trunk.
- En el PVST+, el 802.1Q IEEE BPDU se remite untagged en el VLAN1 del Common Spanning Tree para la Interoperabilidad con los otros vendedores, a menos que el VLAN1 se haya borrado del trunk. Este sucede independientemente de la configuración de la VLAN nativa. **Las BPDU de PVST+ de Cisco** se envían y etiquetan para el resto de las VLAN. Vea la sección del Spanning Tree Protocol para más detalles.
- Las BPDU de 802.1s 802.1s Multiple Spanning Tree (MST) siempre se envían por la VLAN 1 en los trunks ISL y 802.1Q. Esto se aplica incluso cuando el VLAN1 se ha borrado de los

trunks.
- No borre ni inhabilite VLAN 1 en los trunks entre los bridges MST y los bridges PVST+. Pero, en caso de que se inhabilite el VLAN1, el Bridge MST debe convertirse en raíz para que todos los VLA N eviten la colocación del Bridge MST de sus puertos del límite en el estado de la raíz contraria. Consulte Comprensión de Multiple Spanning Tree Protocol (802.1s)para conocer los detalles.

Características estándars

Esta sección del documento se centra en las características del Basic Switching que son comunes a cualquier entorno. Configure estas características en todos los dispositivos de Switching del Catalyst del Cisco IOS Software en la red del cliente.

VLAN Trunk Protocol

Propósito

Un dominio VTP, que también se llama un dominio de administración de VLAN, se compone de uno o más switches interconectados vía un trunk que compartan el mismo Domain Name VTP. El VTP se diseña para permitir que los usuarios realicen los cambios de configuración de VLAN centralmente en uno o más Switches. El VTP comunica automáticamente los cambios al resto de Switches en el dominio VTP (de la red). Usted puede configurar un Switch para estar en solamente un dominio VTP. Antes de que usted cree los VLA N, determine al modo VTP que debe ser utilizado en la red.

Información Operativa General

El VTP es un protocolo de mensajería de la capa 2. El VTP maneja la adición, cancelacíon, y la retitula de los VLA N en función de toda la red para mantener la congruencia en la configuración de VLAN. El VTP minimiza el misconfigurations y las incoherencias de configuración que pueden dar lugar a varios problemas. Los problemas incluyen los nombres, las especificaciones incorrectas de tipo de VLAN, y las violaciones de seguridad duplicados del VLA N.

Por abandono, el Switch está en el modo de servidor VTP y está en el estado del dominio de la ninguno-Administración. Estas configuraciones predeterminadas cambian cuando el Switch recibe un anuncio para un dominio sobre un link de troncal o cuando se configura un dominio de administración.

El protocolo VTP comunica entre el Switches con el uso de un MAC de multidifusión de destino bien conocido de los Ethernetes (01-00-0c-cc-cc-cc) y el tipo de Protocolo HDLC. RÁPIDO 0x2003. Similar a otros protocolos intrínsecos, el VTP también utiliza un encapsulado SNAP de IEEE 802.3, que incluye LLC 0xAAAA03 y OUI 0x00000C. Usted puede ver esto en una traza del analizador LAN. El VTP no trabaja sobre los puertos del nontrunk. Por lo tanto, los mensajes no pueden ser enviados hasta que el DTP haya traído el trunk para arriba. Es decir el VTP es un payload del ISL o del 802.1Q.

Los Tipos de mensaje incluyen:

- Anuncios de resumen cada 300 segundos (sec)
- Anuncios del subconjunto y anuncios de la petición cuando hay cambios

- Se une a cuando se habilita el recorte VTP

El número de revisión de la configuración VTP es incrementado por uno con cada cambio en un servidor, y las propagaciones de esa tabla a través del dominio.

En la cancelacíon de un VLA N, los puertos que eran una vez un miembro del VLA N ingresan un estado `inactivo`. Semejantemente, si un Switch en el modo cliente no puede recibir la tabla de VLAN VTP en el bootup, de un servidor VTP o de otro vtp client, todos los puertos en los VLA N con excepción del VLAN predeterminado 1 se desactivan.

Usted puede configurar la mayoría de los switches de Catalyst para actuar en de estos modos VTP:

- Servidor — En el modo de servidor VTP, usted puede:Crear VLANModifique los VLA NBorre los VLA NEspecifique otros parámetros de la configuración, tales como versión de VTP y recorte VTP, para el dominio VTP enteroLos servidores VTP hacen publicidad de su configuración de VLAN al otro Switches en el mismo dominio VTP. Los servidores VTP también sincronizan su configuración de VLAN con el otro Switches en base de los anuncios que se reciben sobre los links de troncal. El servidor VTP es el modo predeterminado.
- Cliente — Los clientes VTP se comportan igual que los servidores VTP. Pero usted no puede crear, cambiar, o borrar los VLA N en un vtp client. Por otra parte, el cliente no recuerda el VLA N después de una reinicialización porque no se escribe ninguna información de VLAN en el NVRAM.
- Transparente: los switches VTP transparente no participan en VTP. Un switch transparente VTP no hace publicidad de su configuración de VLAN y no sincroniza su configuración de VLAN en base de los anuncios recibidos. Pero, en la versión de VTP 2, los switches transparentes remiten los avisos VTP que el Switches recibe hacia fuera sus interfaces de tronco.

Función	Servidor	Cliente	Transparente	De1
Mensajes VTP fuente	Sí	Sí	No	
Escuchar mensajes VTP	Sí	Sí	No	
Crear VLAN	Sí	No	Sí (solo de importancia local)	
Recordar VLAN	Sí	No	Sí (solo de importancia local)	

[1] Cisco IOS Software no tiene la opción para inhabilitar el VTP con el uso del `modo desconectado`.

Esta tabla es un resumen de la configuración inicial:

Función	Valor Predeterminado
Nombre de Dominio de VTP	Nulo
Modo VTP	Servidor

Versión de VTP	Se habilita la versión 1
Recorte VTP	Inhabilitado

En el modo transparente VTP, las actualizaciones VTP se ignoran simplemente. El Multicast MAC Address bien conocido VTP se quita del CAM del sistema que se utiliza normalmente para coger las tramas de control y para dirigirlas al Supervisor Engine. Porque el protocolo utiliza a una dirección Multicast, el Switch en el modo transparente u otro switch de proveedor inunda simplemente la trama a otros switches Cisco en el dominio.

La versión de VTP 2 (VTPv2) incluye la flexibilidad funcional que esta lista describe. Pero, el VTPv2 no es interoperable con la versión de VTP 1 (VTPv1):

- Soporte Token Ring
- Soporte VTP desconocido — El Switches ahora propaga los valores que él no puede analizar.
- modo transparente Versión-dependiente — El modo transparente marca no más el Domain Name. Esto habilita el soporte de más de un dominio a través de un dominio transparente.
- Propagación del número de versión — Si el VTPv2 es posible en todo el Switches, todo el Switches se puede habilitar con la configuración de un un solo switch.

Refiera comprensión del VLAN Trunk Protocol (VTP) para más información.

Funcionamiento de VTP en Cisco IOS Software

Los cambios de configuración en CatOS se escriben al NVRAM inmediatamente después que se realiza un cambio. En cambio, el Cisco IOS Software no salva los cambios de configuración al NVRAM a menos que usted publique el **comando copy run start**. El vtp client y los sistemas del servidor requieren las actualizaciones VTP de otros servidores VTP ser guardados inmediatamente en el NVRAM sin la intervención del usuario. Los requisitos de la actualización VTP son cumplidos por la operación predeterminada de CatOS, pero el modelo de la actualización de Cisco IOS Software requiere una operación de actualización alternativa.

Para esta alteración, una base de datos de VLAN fue introducida en el Cisco IOS Software para el Catalyst 6500 como un método para salvar inmediatamente las actualizaciones VTP para los clientes y servidores VTP. En algunas versiones de software, esta base de datos de VLAN está bajo la forma de archivo distinto en el NVRAM, llamado el archivo del vlan.dat. Marque su versión de software para determinar si un respaldo de la base de datos de VLAN se requiere. Usted puede ver la información VTP/VLAN que se salva en el archivo del vlan.dat para el vtp client o el servidor VTP si usted publica el comando show vtp status.

La configuración entera VTP/VLAN no se guarda al archivo de la configuración de inicialización en el NVRAM cuando usted publica el **comando copy run start** en estos sistemas. Esto no se aplica a los sistemas que se ejecutan como VTP transparente. Los sistemas transparentes VTP salvan la configuración entera VTP/VLAN al archivo de la configuración de inicialización en el NVRAM cuando usted publica el **comando copy run start**.

En las versiones de Cisco IOS Software que son anteriores que el Cisco IOS Software Release 12.1(11b)E, usted puede configurar solamente el VTP y los VLA N vía el vlan database mode. El vlan database mode es un modo separado del modo de configuración global. La razón de estos requisitos para la configuración es que, cuando usted configura el dispositivo en el servidor modo VTP o el cliente de modo VTP, los vecinos VLAN pueden poner al día la base de datos de VLAN dinámicamente vía los avisos VTP. Usted no quisiera que estas actualizaciones propagaran automáticamente a la configuración. Por lo tanto, la base de datos de VLAN y la información VTP

no se salvan en la configuración principal, sino se salvan en el NVRAM en un archivo con el vlan.dat del nombre.

Este ejemplo muestra cómo crear las redes Ethernet VLAN en el vlan database mode:

```
Switch#vlan database Switch(vlan)#vlan 3 VLAN 3 added: Name: VLAN0003 Switch(vlan)#exit APPLY completed. Exiting....
```

En el Cisco IOS Software Release 12.1(11b)E y Posterior, usted puede configurar el VTP y los VLA N vía el vlan database mode o vía el modo de configuración global. En el servidor modo VTP o el modo VTP transparente, la configuración de los VLA N todavía pone al día el archivo del vlan.dat en el NVRAM. Sin embargo, estos comandos no se guardan en la configuración. Por lo tanto, los comandos no muestran en la configuración corriente.

Refiera a la *configuración de VLAN en la* sección del *modo de configuración global del* documento que configura los VLA N para más información.

Este ejemplo muestra cómo crear las redes Ethernet VLAN en el modo de configuración global y cómo verificar la configuración:

```
Switch#configure terminal Switch(config#vtp mode transparent Setting device to VTP TRANSPARENT mode. Switch(config#vlan 3 Switch(config-vlan)#end Switch# OR Switch#vlan database Switch(vlan#vtp server Switch device to VTP SERVER mode. Switch(vlan#vlan 3 Switch(vlan#exit APPLY completed. Exiting.... Switch#
```

Nota: La configuración de VLAN se salva en el archivo del vlan.dat, que se salva en memoria no volátil. Para realizar un respaldo completo de su configuración, incluya el archivo del vlan.dat en el respaldo junto con la configuración. Entonces, si el Switch entero o el módulo de Supervisor Engine requiere el reemplazo, el administrador de la red debe cargar ambos archivos para restablecer la configuración completa:

- El archivo del vlan.dat
- El archivo de configuración

VTP y VLA N extendidos

La característica extendida del ID del sistema se utiliza para habilitar la identificación del VLAN de alcance extendido. Cuando se habilita el ID del sistema extendido, inhabilita el pool de las direcciones MAC usadas para el árbol de expansión de VLAN, y deja una sola dirección MAC que identifique el Switch. IOS de Catalyst el Software Release 12.1(11b)EX y 12.1(13)E introduce el soporte extendido del ID del sistema para que el Catalyst 6000/6500 soporte 4096 VLA N de acuerdo con el estándar del IEEE 802.1Q. Esta característica se introduce en Cisco IOS Software Release12.1(12c)EW para el Switches del Catalyst 4000/4500. Estos VLA N se ordenan en varios rangos, que se pueden utilizar diferentemente. Algunos de estos VLA N se propagan al otro Switches en la red cuando usted utiliza el VTP. Los VLAN de alcances extendidos no se propagan, así que usted debe configurar los VLAN de alcances extendidos manualmente en cada dispositivo de red. Esta característica extendida del ID del sistema es equivalente a la característica de reducción de la dirección MAC en el Catalyst OS.

Esta tabla describe los rangos del VLA N:

VLAN	Rango	Uso	¿Propagado por el VTP?

0, 4095	Reservado	Para el uso del sistema solamente. Usted no puede ver o utilizar estos VLA N.	
1	Normal	Predeterminado de Cisco. Usted puede utilizar este VLA N, pero usted no puede borrarlo.	Sí
2 – 1001	Normal	Para las redes Ethernet VLAN. Usted puede crear, utilizar, y borrar estos VLA N.	Sí
1002 – 1005	Normal	Valores por defecto de Cisco para el FDDI y el Token Ring. Usted no puede borrar los VLA N 1002 – 1005.	Sí
1006 – 4094	Reservado	Para las redes Ethernet VLAN solamente.	No

Los protocolos del Switch utilizan una dirección MAC tomada de un banco de las direcciones disponibles que un EPROM proporciona en el chasis como parte de los identificadores de Bridge para los VLA N que se ejecutan bajo el PVST+ y el RPVST+. El Switches del Catalyst 6000/6500 y del Catalyst 4000/4500 soporta 1024 o 64 direcciones MAC que dependan del tipo del chasis.

Los switches de Catalyst con 1024 direcciones MAC no habilitan el ID del sistema extendido por abandono. Las direcciones MAC se afectan un aparato secuencialmente, con la primera dirección MAC en el rango asignado al VLAN1, la segunda dirección MAC en el rango asignado al VLAN2, y así sucesivamente. Esto permite al Switches para soportar 1024 VLA N y cada VLA N utiliza un identificador de Bridge único.

Tipo de Chasis	Dirección de chasis
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	64[1]
WS-C6509-E, WS-C6509, WS-C6509-NEB, WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR-7609-AC, OSR-7609-DC	1024
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO7609, CISCO7613	64[1]

[1] chasis con 64 direcciones MAC habilita el ID del sistema extendido por abandono, y la característica no puede ser inhabilitada.

Refiera a la *comprensión la* sección del *Bridge ID de* configurar STP y el IEEE 802.1S MST para más información.

Para los Catalyst Series Switch con 1024 direcciones MAC, habilitar el ID del sistema extendido permite que el soporte de 4096 VLA N que se ejecuten bajo el PVST+ o de 16 casos MISTP tenga Identificadores únicos sin el aumento del número de direcciones MAC que se requieran en

el Switch. El ID del sistema extendido reduce el número de direcciones MAC que sean requeridas por el STP a partir del uno por el caso del VLA N o MISTP a uno por el Switch.

Esta figura muestra el identificador de Bridge cuando el ID del sistema extendido no se habilita. El identificador de Bridge consiste en una prioridad de Bridge 2-byte y una dirección MAC 6-byte.

El ID del sistema extendido modifica la porción del identificador de Bridge del Spanning Tree Protocol (STP) del (BPDU) de las Unidades. El campo de prioridad original 2-byte está partido en 2-fields; Un campo de la prioridad de Bridge 4-bit y una extensión del ID del sistema 12-bit que permite la enumeración de Vlan de 0-4095.

Cuando el ID del sistema extendido se habilita en los switches de Catalyst para leverage los VLAN de alcances extendidos, necesita ser habilitado en todo el Switches dentro del mismo dominio STP. Esto es necesario mantener los cálculos de raíz STP en todo el Switches constantes. Una vez que se habilita el ID del sistema extendido, la prioridad de Root Bridge se convierte en un múltiplo de 4096 más el VLAN ID. El Switches sin el ID del sistema extendido puede demandar posiblemente la raíz inadvertidamente pues él tiene una granularidad más fina en la selección de su Bridge ID.

Mientras que se recomienda para mantener la configuración extendida constante del ID del sistema dentro del mismo dominio STP, no es práctico aplicar el ID del sistema extendido en todos los dispositivos de red cuando usted introduce el nuevo chasis con la dirección MAC 64 al dominio STP. Pero, es importante entender cuando dos sistemas se configuran con la misma prioridad del Spanning-tree, el sistema sin el ID del sistema extendido tiene una mejor prioridad del Spanning-tree. Publique este comando para habilitar la configuración extendida del ID del sistema:

el atravesar-árbol amplía el ID del sistema

Los VLA N internos se afectan un aparato en el orden ascendente, comenzando en el VLA N 1006. Se recomienda para asignar los VLAN de usuarios tan cerca al VLA N 4094 como posible para evitar los conflictos entre los VLAN de usuarios y los VLA N internos. Publique el comando show vlan internal usage en un Switch para visualizar internamente los VLAN asignados.

```
Switch#show vlan internal usage VLAN Usage ---- -------------------- 1006 online diag vlan0 1007
online diag vlan1 1008 online diag vlan2 1009 online diag vlan3 1010 online diag vlan4 1011
online diag vlan5 1012 PM vlan process (trunk tagging) 1013 Port-channel100 1014 Control Plane
Protection 1015 L3 multicast partial shortcuts for VPN 0 1016 vrf_0_vlan0 1017 Egress internal
vlan 1018 Multicast VPN 0 QOS vlan 1019 IPv6 Multicast Egress multicast 1020 GigabitEthernet5/1
1021 ATM7/0/0 1022 ATM7/0/0.1 1023 FastEthernet3/1 1024 FastEthernet3/2 ------deleted------
```

En el Native IOS, la **política de asignación interna vlan que desciende** puede ser configurada así que los VLA N internos se afectan un aparato en el orden descendente. El CLI equivalente para el software CatOS no se soporta oficialmente.

política de asignación interna vlan que desciende

Recomendación de la configuración de Cisco

Los VLA N se pueden crear cuando un Catalyst 6500/6000 está en el modo de servidor VTP, incluso sin el Domain Name VTP. Configure el Domain Name VTP primero, antes de que usted configure los VLA N en el Switches del Catalyst 6500/6000 que funciona con el software del sistema del Cisco IOS. La configuración en esta orden mantiene el estado coherente con otros switches de Catalyst que ejecuten CatOS.

No hay una recomendación específica acerca de si se debe utilizar los modos cliente/servidor de VTP o el modo transparente de VTP. Algunos clientes prefieren la facilidad de administración del modo cliente/servidor VTP, a pesar de algunas consideraciones las notas de esa esta sección. Se recomienda tener dos switches en modo de servidor en cada dominio para redundancia, normalmente los dos switches de capa de distribución. Fije el resto del Switches en el dominio al modo cliente. Cuando usted implementa al modo cliente/servidor con el uso del VTPv2, recuerde que un número de revisión más alto está validado siempre en el mismo dominio VTP. Si un Switch que se configura en el vtp client o el modo de servidor se introduce en el dominio VTP y tiene un número de revisión más alto que los servidores VTP que exista, éste sobregraba la base de datos de VLAN dentro del dominio VTP. Si el cambio de configuración es involuntario y se borran los VLA N, éste sobregraba puede causar una caída del sistema importante en la red. Para asegurarse de que el cliente o los switches del servidor tenga siempre un número de revisión de la configuración que sea más bajo que el del servidor, cambie el Domain Name del cliente VTP algo con excepción del nombre estándar, y después invierta de nuevo al estándar. Esta acción configura la revisión de la configuración en el cliente en 0.

La capacidad de VTP de realizar los cambios fácilmente en una red tiene ventajas y desventajas. Muchas empresas prefieren a un `modo transparente del` método cauteloso y del uso VTP por estas razones:

- Esta práctica anima el buen control de cambios porque el requisito de modificar un VLA N en un Switch o un puerto troncal se debe considerar un en un momento del Switch.
- El modo transparente VTP limita el riesgo de un error del administrador, tal como borrado accidental de un VLA N. Tales errores pueden afectar el dominio entero.
- Los VLA N se pueden podar de los trunks abajo al Switches que no tiene puertos en el VLA N. Esto da lugar a la inundación de trama para ser ancho de banda-más eficiente. El recorte manual también tiene un diámetro del árbol de expansión reducido. Vea la sección del protocolo dynamic trunking para más información. Una configuración de VLAN del por-Switch también anima esta práctica.
- No hay riesgo de la introducción en la red de un nuevo Switch con un número de revisión VTP mayor que sobregrabe la configuración de VLAN entera del dominio.
- Soportan al modo transparente del Cisco IOS Software VTP en el Campus Manager 3.2, que es la parte de CiscoWorks2000. Se ha quitado la restricción anterior que le requiere tener por lo menos un servidor en un dominio VTP.

Comandos vtp	**Comentarios**
Domain Name del vtp	El CDP marca el nombre para ayudar a prevenir el miscabling entre los dominios. Los Domain Name son con diferenciación entre mayúsculas y minúsculas.
modo del vtp {servidor | cliente | transparente}	El VTP actúa en uno de los tres modos.
***vlan_number* vlan**	Esto crea un VLA N con el ID proporcionado.

vlan_range **permitido switchport trunk**	Éste es un comando interface que permite a los trunks para llevar los VLA N donde necesitado. El valor por defecto es todos los VLA N.
vlan_range de la **poda del switchport trunk**	Esto es comando interface que limita al diámetro STP por el recorte manual, por ejemplo en los trunks de la capa de distribución a la capa de acceso, donde no existe el VLA N. Por abandono, todos los VLA N son pasa-elegibles.

Otras Opciones

El VTPv2 es un requisito en entornos token ring, en los que se recomienda firmemente el modo cliente/servidor.

La sección de la recomendación de la configuración de Cisco de este documento aboga las ventajas de los VLA N de la poda para reducir la inundación de la trama innecesaria. **El comando vtp pruning** poda los VLA N automáticamente, que para la inundación de trama no efectiva donde él no está necesario.

Nota: El distinto al manual VLAN Pruning, recorte automático no limita al diámetro del árbol de expansión.

El IEEE ha producido una arquitectura basada en estándares para lograr los resultados VTP-similares. Como miembro del protocolo generic attribute registration del 802.1Q (GARP), el Generic VLAN Registration Protocol (GVRP) permite la Interoperabilidad de la administración de VLAN entre los vendedores. Sin embargo, el GVRP está fuera del ámbito de este documento.

Nota: El Cisco IOS Software no tiene capacidad del modo desconectado VTP, y soporta solamente el VTPv1 y el VTPv2 con la poda.

Autonegotiation de los fast ethernet

Propósito

El autonegotiation es una función optativa del estándar del Fast Ethernet (FE) de IEEE 802.3u. Dispositivos de los permisos del autonegotiation para intercambiar automáticamente la información sobre las capacidades de la velocidad y dúplex sobre un link. El autonegotiation actúa en el Layer 1 (L1). La función se apunta en los puertos que se afectan un aparato a las áreas donde los usuarios transitorios o los dispositivos conectan con una red. Los ejemplos incluyen los switches de capa de acceso y el Hubs.

Información Operativa General

El autonegotiation utiliza una versión modificada de la prueba de integridad del link para que los dispositivos 10BaseT negocien la velocidad e intercambien otros parámetros de negociación automática. La prueba de integridad del link 10BASE-T original se conoce como impulso de link

normal (NLP). La versión modificada de la prueba de integridad del link para el autonegotiation 10/100-Mbps se refiere como Impulso de link rápido (FLP). Los dispositivos 10BaseT cuentan con un impulso de ráfaga cada 16 (+/--8) milisegundos (ms) como parte de la prueba de integridad del link. El FLP para el autonegotiation 10/100-Mbps envía estas explosiones cada 16 (+/--8) que pulsa el ms con el adicional cada 62.5 (+/--7) microsegundos. Los pulsos dentro de la secuencia de ráfagas generan palabras de código que se utilizan para los intercambios de compatibilidad entre socios de link.

En el 10BaseT, se envía un impulso de link siempre que suba una estación. Éste es un solo pulso que se envía cada ms 16. Los dispositivos 10BaseT también envían un impulso de link a cada ms 16 cuando el link está ocioso. Estos impulsos de link también se llaman latido del corazón o NLP.

Un dispositivo 100BASE-T envía el FLP. Este pulso se envía como explosión en vez de un pulso. La explosión se completa dentro de 2 ms y otra vez se relanza cada ms 16 sobre la inicialización, el dispositivo transmite un mensaje FLP de 16 bits al partner de link para la negociación de la velocidad, del duplex, y del control de flujo. Este mensaje de 16 bits se envía en varias ocasiones hasta que el mensaje sea reconocido por el partner.

Nota: Según la especificación de IEEE 802.3u, usted no puede configurar manualmente a un partner de link para el duplex del 100-Mbps por completo - duplex y todavía autonegociar a por completo - con el otro partner de link. Una tentativa de configurar a un partner de link para el 100-Mbps por completo - dupliqúese y el otro partner de link para los resultados del autonegotiation en una discordancia dúplex. La discordancia dúplex resulta porque un partner de link autonegocia y no ve ningunos parámetros de negociación automática del otro partner de link. El primer partner de link entonces omite el half duplex.

Todos los módulos del Ethernet Switching del Catalyst 6500 soportan el 10/100 Mbps y semidúplexes o por completo - duplex. Publique el **comando show interface capabilities** para verificar estas funciones en otros switches de Catalyst.

Una de la mayoría de las causas comunes de los problemas de rendimiento en los links Ethernet 10/100-Mbps ocurre cuando un puerto en el link actúa en el half duplex mientras que el otro puerto actúa en por completo - duplex. Esta situación sucede de vez en cuando cuando usted reajusta uno o vira hacia el lado de babor en un link y el proceso de negociación automática no da lugar a la misma configuración para ambos partners de link. La situación también sucede cuando usted configura de nuevo un lado de un link y olvida configurar de nuevo el otro lado. Usted puede evitar la necesidad de poner los visita de personal técnico por problemas de rendimiento si usted:

- Cree una directiva que requiera la configuración de puerto para el comportamiento requerido para todos los dispositivos permanentes
- Aplique la directiva con las medidas adecuadas del control de cambios

Los síntomas típicos del problema de rendimiento aumentan la Secuencia de verificación de tramas (FCS), la verificación por redundancia cíclica (CRC), la alineación, o a los contadores de fragmentos de tramas minúsculos en el Switch.

En el modo semidúplex, usted hace que un par de reciba y un par de transmite los alambres. Ambos alambres no se pueden utilizar al mismo tiempo. El dispositivo no puede transmitir cuando hay un paquete en el lado de recepción.

En el modo dúplex completo, usted hace que los mismos pares de reciban y transmitan los alambres. Sin embargo, ambos pueden ser utilizados al mismo tiempo porque la detección de portadora y la colisión detectan las funciones para haber sido inhabilitadas. El dispositivo puede

transmitir y recibir al mismo tiempo.

Por lo tanto, un semidúplex a la conexión de dúplex completo trabaja, pero hay un gran número de colisiones en el lado semidúplex que dan lugar al rendimiento pobre. Las colisiones ocurren porque el dispositivo se configura que mientras que por completo - el duplex puede transmitir a la vez que el dispositivo recibe los datos.

Los documentos en esta lista discuten el autonegotiation detalladamente. Estos documentos explican cómo el autonegotiation trabaja y discuten las diversas opciones de configuración:

- Configuración y resolución de problemas de negociación automática de half/full duplex para Ethernet 10/100/1000 Mb
- Troubleshooting de Problemas de Compatibilidad entre Cisco Catalyst Switches y NIC

Un concepto erróneo común sobre el autonegotiation es que es posible configurar manualmente a un partner de link para el duplex del 100-Mbps por completo - dupliqúese y autonegocie a por completo - con el otro partner de link. De hecho, si se intenta hacer esto, se obtienen modos dúplex desiguales. Esto es una consecuencia porque un partner de link autonegocia, no ve ningunos parámetros de negociación automática del otro partner de link, y omite el half duplex.

La mayoría de los módulos de los Catalyst de Ethernet soportan el 10/100 Mbps y el dúplex completo y semidúplex. Sin embargo, usted puede confirmar esto si usted publica el **comando capabilities del** */port Mod de la* **interfaz de la demostración**.

FEFI

El Far End Fault Indication (FEFI) protege 100BASE-FX (fibra) y las interfaces Gigabit, mientras que el autonegotiation protege 100BASE-TX (cobre) contra la Capa física/los incidentes señalización-relacionados.

Un far end fault es un error en el link que una estación puede detectar mientras que no puede la otra estación. Un disconnected transmite el alambre es un ejemplo. En este ejemplo, la estación remitente todavía recibe los datos válidos y detecta que el link es bueno vía el monitor de la integridad del link. La estación remitente no puede, sin embargo, detectar que la otra estación no recibe la transmisión. Una estación 100BASE-FX que detecta a tal falla remota puede modificar su secuencia ociosa transmitida para enviar a un patrón de bits especial para informar al vecino la falla remota. Refieren al patrón de bits especial como el `modelo FEFI-IDLE`. el patrón FEFI-IDLE apaga posteriormente el puerto remoto (errdisable). Vea la sección de la detección de link unidireccional de este documento para más información sobre la protección contra fallas.

Estos módulos/soporte del hardware FEFI:

- Catalyst 6500/6000 y 4500/4000:Todos los módulos 100BASE-FX y módulos GE

Recomendación del puerto de infraestructura de Cisco

Si configurar el autonegotiation en los links 10/100-Mbps o a la velocidad y dúplex dura del código depende en última instancia del tipo de partner de link o de dispositivo extremo que usted ha conectado con un puerto del switch Catalyst. La negociación automática entre los dispositivos extremos y los switches Catalyst generalmente funciona sin inconvenientes, y los switches Catalyst cumplen con la especificación IEEE 802.3u. Sin embargo, cuando no conforma el Network Interface Cards (NIC) o los switches de proveedor exactamente, los problemas pueden

resultar. Además, las funciones avanzadas específicas del proveedor que no se describen en la especificación de IEEE 802.3u para el autonegotiation 10/100-Mbps pueden causar la incompatibilidad del hardware y otros problemas. Estos tipos de funciones avanzadas incluyen el autopolarity y la integridad del cableado. Este documento proporciona un ejemplo:

- Alerta de campo: Problema de rendimiento con Intel Pro/1000T NICs conectado a CAT4K/6K

En algunas situaciones, usted necesita fijar el host, la velocidad de puerto, y el duplex. Complete generalmente estos pasos básicos para Troubleshooting:

- Aseegurese que el autonegotiation está configurado a ambos lados del link o que la codificación dura está configurada en los ambos lados.
- Marque los Release Note para las advertencias comunes.
- Verifique la versión del driver NIC o del sistema operativo que usted funciona con. El último driver o corrección se requiere a menudo.

En general, primer autonegotiation del uso para cualquier tipo de partner de link. Hay beneficios evidentes a la configuración del autonegotiation para los dispositivos transitorios tales como laptopes. El autonegotiation también trabaja bien con los otros dispositivos, por ejemplo:

- Con los dispositivos permanentes tales como servidores y puestos de trabajo fijos
- Del Switch a conmutar
- Del Switch al router

Pero, por algunas de las razones que las menciones de esta sección, los problemas de la negociación pueden presentarse. Refiera a configurar y a resolver problemas la negociación automática del dúplex completo y del semidúplex de los Ethernetes 10/100/1000Mb para los pasos básicos para Troubleshooting en estos casos.

Inhabilite el autonegotiation para:

- Puertos que soportan los dispositivos de la infraestructura de red tales como Switches y Routers
- Otros sistemas extremos nontransient tales como servidores e impresoras

Código siempre duro las configuraciones de la velocidad y dúplex para estos puertos.

Configure manualmente estas configuraciones de link 10/100-Mbps para la velocidad y dúplex, que son generalmente 100-Mbps por completo - duplex:

- Switch a switch
- Switch-a-servidor
- Switch-a-router

Si la velocidad de puerto se fija al auto en un acceso de Ethernet 10/100-Mbps, se autonegocian ambos la velocidad y dúplex. Publique este comando interface para fijar el puerto al auto:

```
Switch(config)#interface fastethernet slot/port Switch(config-if)#speed auto !--- This is the default.
```

Publique estos comandos interface para configurar la velocidad y dúplex:

```
Switch(config)#interface fastethernet slot/port Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Recomendaciones del puerto de acceso de Cisco

Usuarios finales, trabajadores móviles, y autonegotiation transitorio de la necesidad de los host para minimizar la Administración de estos host. Usted puede hacer el trabajo del autonegotiation con los switches de Catalyst también. Los últimos driveres NIC se requieren a menudo.

Publique estos comandos global para habilitar el autonegotiation de la velocidad para el puerto:

```
Switch(config)#interface fastethernet slot/port Switch(config-if)#speed auto
```

Nota: Si usted fija la velocidad de puerto al auto en un acceso de Ethernet 10/100-Mbps, se autonegocia amba velocidad y dúplex. Usted no puede cambiar al modo dúplex de puertos del autonegotiation.

Cuando los NIC o los switches de proveedor no se ajustan exactamente a la especificación de IEEE 802.3u, los problemas pueden resultar. Además, las funciones avanzadas específicas del proveedor que no se describen en la especificación de IEEE 802.3u para el autonegotiation 10/100-Mbps pueden causar la incompatibilidad del hardware y otros problemas. Tales funciones avanzadas incluyen el autopolarity y la integridad del cableado.

Otras Opciones

Cuando el autonegotiation se inhabilita entre el Switches, la indicación de falla del Layer 1 puede también ser con certeza problemas perdidos. Utilice los protocolos de la capa 2 para aumentar la detección de falla por ejemplo

El autonegotiation no detecta estas situaciones, incluso cuando se habilita el autonegotiation:

- Los puertos consiguen pegados y no reciben ni transmiten
- Un lado de la línea está para arriba pero el otro lado ha ido abajo
- Los cables de fibra son miswired

El autonegotiation no detecta estos problemas porque no están en la Capa física. Los problemas pueden llevar a los loopes STP o a los agujeros negros del tráfico.

El UDLD puede detectar todos estos casos y errdisable ambos los puertos en el link, si el UDLD se configura en los ambos extremos. De esta manera, el UDLD previene los loopes STP y a los agujeros negros del tráfico.

Autonegotiation de Gigabit Ethernet

Propósito

El Gigabit Ethernet (GE) tiene un procedimiento de autonegociación que sea más extenso que el procedimiento que se utiliza para los Ethernetes 10/100-Mbps (IEEE 802.3Z). Con los puertos de GE, el autonegotiation se utiliza para intercambiar:

- Parámetros de control de flujo
- Información de falla remota
- Información dúplex**Nota:** Modo dúplex completo del soporte de los puertos de GE del Catalyst Series solamente.

El IEEE 802.3Z ha sido reemplazado por espec. de IEEE 802.3:2000. Refiera a la suscripción de normas del Local y de las redes + de los proyectos de la área metropolitana (LAN/MAN 802s) para más información.

Información Operativa General

A diferencia de la autonegociación con 10/100-Mbps FE, el autonegotiation de GE no implica la negociación de la velocidad de puerto. También, usted no puede publicar el **comando set port speed** para inhabilitar el autonegotiation. La negociación de puerto GE se habilita de forma predeterminada, y los puertos en ambos extremos de un link GE deben tener la misma configuración. El link no sube si los puertos en cada extremo del link se fijan contrario, así que significa que los parámetros intercambiados son diferentes.

Por ejemplo, suponga que hay dos dispositivos, A y B. Cada dispositivo puede tener la función de negociación automática habilitada o inhabilitada. Ésta es una tabla que tiene las configuraciones posibles y sus estados respectivos del link:

Negociación	B Habilitado	B inhabilitada
A Habilitado	encendido en ambos lados	A apagado, B encendido
A Inhabilitado	A encendido, B apagado	encendido en ambos lados

En el GE, la sincronización y el negociación automática (si están habilitadas) se realizan tras el inicio del link mediante el uso de una secuencia especial de palabras reservadas para el código del link.

Nota: Hay un diccionario de las palabras válidas, y no todas las palabras posibles son válidas en GE.

La vida de una conexión GE se puede caracterizar de esta manera:

Una pérdida de sincronización significa que MAC detecta un link que no funciona. La pérdida de sincronización se aplica independientemente de si la negociación automática está habilitada o inhabilitada. La sincronización se pierde cuando ocurren ciertas fallas, como si se reciben tres palabras inválidas de forma consecutiva. Si esta condición persiste para el ms 10, se afirma una condición del fall del sincronizar y el link se cambia al estado del `link_down`. Después de que se pierde la sincronización, se necesitan tres palabras IDLE válidas consecutivas para que se inicie la resincronización. Otros eventos catastróficos, tales como la pérdida de la señal de recepción (Rx), hacen que un link deje de funcionar.

La negociación automática forma parte del proceso de conexión de link. Cuando el link está en funcionamiento, la negociación automática finaliza. Sin embargo, el switch todavía monitorea el estado del link. Si el autonegotiation se inhabilita en un puerto, la fase del autoneg es no más una opción.

La especificación del cobre de GE (1000BASE-T) soporta el autonegotiation vía un intercambio siguiente de la página. Next Page Exchange permite la negociación automática para las velocidades de 10/100/1000-Mbps en puertos de cobre.

Nota: Sin embargo, la especificación de fibra de GE adopta solamente las disposiciones para la negociación del duplex, del control de flujo, y de la detección de falla remota. Los puertos de fibra GE no negocian la velocidad de puerto. Consulte las secciones 28 a 37 de la especificación IEEE 802.3-2002 para obtener más información sobre la negociación automática.

La demora del reinicio de la sincronización es una función del software que controla el tiempo

total de la negociación automática. Si la negociación automática no resulta satisfactoria dentro de este período, el firmware reinicia la negociación automática por si se produce un interbloqueo. El comando del sincronización-reinicio-**retardo** tiene solamente un efecto cuando el autonegotiation se fija para habilitar.

Recomendación del puerto de infraestructura de Cisco

La configuración del autonegotiation es mucho más crítica en un entorno de GE que en un entorno del 10/100 Mbps. Solamente autonegotiation de la neutralización en estas situaciones:

- En los puertos del switch que asocian a los dispositivos que no pueden soportar la negociación
- Donde los problemas de conectividad se presentan de los problemas de interoperabilidad

Negociación Gigabit del permiso en todos los links entre switches y, generalmente, en todos los dispositivos de GE. El valor predeterminado en las interfaces Gigabit es autonegotiation. No obstante, publique este comando para asegurarse de que el autonegotiation está habilitado:

```
switch(config)#interface type slot/port switch(config-If)#no speed !--- This command sets the port to autonegotiate Gigabit parameters.
```

Una excepción conocida es cuando usted conecta con un router de switch Gigabit (GRS) que funcione con el Cisco IOS Software que es anterior que el Cisco IOS Software Release 12.0(10)S, la versión que agregó el control de flujo y el autonegotiation. En este caso, apague esas dos características. Si usted no apaga esas características, el puerto del switch señala no conectado y los errores de los informes GSR. Esto es una secuencia de comando interface de la muestra:

```
flowcontrol receive off flowcontrol send off speed nonegotiate
```

Recomendaciones del puerto de acceso de Cisco

Puesto que los FLP pueden variar entre los vendedores, usted debe mirar las conexiones del Switch-a-servidor caso por caso. Los clientes de Cisco han encontrado algunos problemas con la negociación Gigabit el Sun, HP, y los servidores de IBM. Haga que todos los dispositivos utilicen la negociación automática de Gigabit a menos que el proveedor de NIC estado específicamente de otra manera.

Otras Opciones

El control de flujo es una parte optativa de la especificación 802.3x. El control de flujo debe ser negociado si usted lo utiliza. Los dispositivos pueden o no pueden posiblemente poder enviar y/o responder a una trama de pausa (MAC bien conocido 01-80-C2-00-00-00 0F). Y los dispositivos no pueden estar de acuerdo posiblemente el pedido de control de flujo del vecino en el extremo lejano. Un puerto con memoria intermedia de entrada que comience a llenarse envía una trama de pausa al partner de link. El partner de link para la transmisión y lleva a cabo cualquier trama adicional en los búferes de salida del partner de link. Esta función no soluciona ningún problema de suscripción excesiva de estado estacionario. Pero, la función con eficacia hace memoria intermedia de entrada más grande por alguna fracción del buffer de salida del partner en las explosiones.

La función de la PAUSA es diseñada para prevenir el descarte innecesario de las tramas recibidas por los dispositivos (Switches, Routers, o estaciones terminales) debido a las condiciones del desbordamiento de búfer que la sobrecarga transitoria a corto plazo del tráfico

causa. Un dispositivo bajo sobrecarga del tráfico previene el desbordamiento del búfer interno cuando el dispositivo envía una trama de pausa. La trama de pausa contiene un parámetro que indique la longitud del tiempo para el lleno - partner dúplex a esperar antes de que el partner envíe más marcos de datos. El partner que recibe la trama de pausa deja de enviar los datos para el periodo especificado. Cuando expira este temporizador, la estación comienza a enviar los marcos de datos otra vez, de donde la estación dejada apagado.

Una estación que publica una PAUSA puede publicar otra trama de pausa que contenga un parámetro del tiempo cero. Esta acción cancela el resto del período de la pausa. Así pues, una trama de pausa recién recibida reemplaza cualquier operación de la PAUSA que esté actualmente en curso. También, la estación que publica la trama de pausa puede prolongar el período de la PAUSA. La estación publica otra trama de pausa que contenga un parámetro temporal distinto a cero antes de que la expiración del primer período de la PAUSA.

Esta operación de la PAUSA no es control de flujo de la tarifa basada. La operación es un mecanismo por marcha-parada simple que permite el dispositivo bajo tráfico, el que envió la trama de pausa, una ocasión de reducir su congestión del buffer.

El mejor uso de esta característica está en los links entre los puertos de acceso y los host extremos, donde está potencialmente tan grande el búfer de salida del host como memoria virtual. El uso switch-a-switch tiene ventajas limitadas.

Publique estos comandos interface para controlar esto en los puertos del switch:

```
flowcontrol {receive | send} {off | on | desired} >show port flowcontrol Port Send FlowControl
Receive FlowControl RxPause TxPause admin oper admin oper ----- -------- -------- -------- -----
--- ------- ------- 6/1 off off on on 0 0 6/2 off off on on 0 0 6/3 off off on on 0 0
```

Nota: Todos los módulos Catalyst responden a una trama PAUSAsi se negocian. Algunos módulos (por ejemplo, WS-X5410 y WS-X4306) nunca envían las tramas de pausa, incluso si negocian para hacer así pues, porque son no bloqueando.

Dynamic Trunking Protocol

Propósito

Para ampliar los VLA N entre los dispositivos, los trunks identifican y marcan temporalmente (local del link) las tramas de los Ethernet original. Esta acción habilita las tramas que se multiplexarán sobre un solo link. La acción también se asegura de que el broadcast de VLAN separado y los dominios de seguridad estén mantenidos entre el Switches. Las tablas CAM mantienen la trama a la asignación del VLA N dentro del Switches.

Información Operativa General

El DTP es la segunda generación de Dynamic ISL (DISL). DISL solamente ISL soportado. El DTP soporta el ISL y el 802.1Q. Este soporte se asegura de que el Switches en cualquier extremo de un trunk esté de acuerdo con los diversos parámetros de los bastidores del enlace. Tales parámetros incluyen:

- Tipo de encapsulación configurada
- VLAN nativa
- Capacidad del hardware

Las ayudas del soporte DTP también protegen contra la inundación de los bastidores marcados con etiqueta por los puertos del nontrunk, que es potencialmente un riesgo de seguridad importante. El DTP protege contra tal inundación porque se asegura de que los puertos y sus vecinos estén en los estados constantes.

Modo Trunking

El DTP es un protocolo de la capa 2 que negocia los parámetros de la configuración entre un puerto del switch y su vecino. El DTP utiliza otro Multicast MAC Address bien conocido de 01-00-0c-cc-cc-cc y un Tipo de protocolo RÁPIDO de 0x2004. Esta tabla describe la función en cada uno de los modos posibles de la negociación DTP:

Modo	Función	¿Tramas DTP transmitidas?	Etapa Final (Puerto Local)
`Auto dinámico` (equivalente al modo automático en CatOS)	Hace que el puerto sea capaz de convertir el link en un trunk. El puerto se convierte en un puerto troncal si el puerto vecino está configurado en modo encendido o deseable.	Sí, periódico	`Trunking`
`Trunk` (equivalente al modo `ENCENDIDO` en CatOS)	Pone el puerto en modo trunking permanente y negocia para convertir el link en un trunk. El puerto se convierte en puerto trunk aunque el puerto de vecindad no acepte el cambio.	Sí, periódico	`Enlace`, incondicional
`Nonegotiate`	Pone el puerto en el modo de concentración de links permanente pero no permite que el puerto genere las tramas DTP. Usted debe configurar manualmente el puerto de vecindad como un puerto troncal para establecer un link de troncal. Esto es útil para dispositivos que no soportan DTP.	No	`Enlace`, incondicional
`Deseable`	Hace que el puerto	Sí, periódico	Termina

`dinámico` (el comando comparable de CatOS es `deseable`)	intente convertir el link en un link trunk. El puerto se convierte en un puerto trunk si el puerto vecino está en modo encendido, deseable o automático.		en estado trunking solamente si el modo remoto es encendido, automático o deseable.
`Acceso`	Pone el puerto en el modo no troncal permanente y negocia para convertir el link en un link del nontrunk. El puerto se convierte en un puerto del nontrunk incluso si el puerto de vecindad no está de acuerdo el cambio.	No, en el estado constante, pero transmite informa para acelerar la detección de extremo remoto después de un cambio de `encendido`.	`NON-enlace`

Nota: El tipo de encapsulación ISL y del 802.1Q puede ser fijado o ser negociado.

En la configuración predeterminada, el DTP asume estas características en el link:

- Las conexiones Point-to-Point y los dispositivos de Cisco soportan los puertos de tronco 802.1q que son solamente de punto a punto.
- En la negociación DTP, los puertos no participan en el STP. El puerto se agrega al STP solamente después que el tipo de puerto hace uno de estos tres tipos:AccesoISL802.1QEl PAgP es el proceso siguiente a ejecutarse antes de que el puerto participe en el STP. El PAgP se utiliza para el autonegotation del EtherChannel.
- El VLAN1 está siempre presente en el puerto troncal. Si el puerto es enlace en el modo ISL, los paquetes DTP se envían en el VLAN1. Si el puerto no es enlace en el modo ISL, los paquetes DTP se envían en el VLAN nativo (para el enlace del 802.1Q o los puertos nontrunking).
- Los paquetes DTP transfieren el Domain Name VTP, más la configuración del tronco y el estado del administrador. El Domain Name VTP debe hacer juego para conseguir un link troncal negociado para subir. Estos paquetes se envían cada segundo en la negociación y cada 30 segundos después de la negociación. Si un puerto en el `modo deseado o automático` no detecta un paquete DTP en el plazo de 5 minutos (minuto), el puerto se fija como nontrunk.

Precaución: Usted debe entender que los modos troncales, `nonegocian`, y el `acceso` especifica explícitamente en qué estado termina el puerto para arriba. Una mala configuración puede llevar a un estado peligroso/inconsistente en cuál el lado es enlace y el otro no es enlace.

Consulte Configuración de Trunking de ISL en Catalyst 5500/5000 y 6500/6000 Family Switches para conocer más detalles sobre ISL. Consulte Trunking entre Catalyst 4500/4000, 5500/5000 y 6500/6000 Series Switches mediante la Encapsulación 802.1Q con el Software de Sistema CatOS de Cisco para obtener más detalles sobre 802.1Q.

Tipo de Encapsulación

Descripción General sobre el Funcionamiento de ISL

El ISL es un Trunking Protocol propietario de Cisco (esquema de Tagging del VLA N). El ISL ha sido funcionando durante muchos años. En cambio, el 802.1Q es mucho más nuevo, pero el 802.1Q es la norma IEEE.

El ISL encapsula totalmente la trama original en un esquema de Tagging de dos niveles. De esta manera, el ISL es con eficacia un Tunneling Protocol y, como beneficio adicional, lleva las tramas de los no Ethernetes. El ISL agrega una encabezado 26-byte y un 4-byte FCS a la trama Ethernet estándar. Los puertos que se configuran para ser trunks cuentan con y manejan las tramas Ethernet más grandes. ISL admite 1024 VLAN.

Formato de trama – Se sombrea la etiqueta ISL

Consulte Formato de Trama IEEE 802.1Q e InterSwitch Link para obtener más información.

Descripción General sobre el Funcionamiento de 802.1Q

Aunque el estándar del IEEE 802.1Q pertenezca solamente a los Ethernetes, el estándar especifica mucho más que los tipos de encapsulación. el 802.1Q incluye, entre otros protocolos generic attribute registration (GARP), las mejoras del Spanning Tree y marcar con etiqueta 802.1p QoS. Refiera a las normas IEEE en línea para más información

El formato de trama del 802.1Q preserva Ethernet original SA y DA. Sin embargo, el Switches debe ahora esperar recibir las tramas del Baby Giant, incluso en los puertos de acceso en donde los host pueden utilizar marcar con etiqueta para expresar la prioridad de usuario 802.1p para la Señalización de QoS. La etiqueta es 4 bytes. Las tramas del v2 de los Ethernetes del 802.1Q son 1522 bytes, que es un logro del grupo de trabajo de IEEE 802.3ac. También, el 802.1Q soporta el espacio de numeración para 4096 VLA N.

Todos los marcos de datos se transmiten que y recibido es el 802.1Q marcado con etiqueta, a excepción de esos marcos de datos que están en el VLAN nativo. En este caso, hay un Tag implícito que se basa en la configuración del puerto del switch de ingreso. Los capítulos en el VLAN nativo son siempre untagged transmitido y son normalmente untagged recibido. Sin embargo, estas tramas se pueden también recibir marcaron con etiqueta.

Si desea más información, consulte estos documentos:

- Interoperabilidad de VLAN
- Enlace entre el Switches de los Catalyst 4500/4000, 5500/5000, y 6500/6000 Series usando la encapsulación 802.1q con el software del sistema de Cisco CatOS

formato de trama 802.1Q/802.1p

Recomendación de la configuración de Cisco

Un elemento principal primario en el diseño de Cisco es esforzarse para el estado coherente en la red donde está posible el estado coherente. Todo el 802.1Q más nuevo y algo del soporte de productos Catalyst soportan solamente el 802.1Q, tal como módulos anteriores en las Catalyst 4500/4000 y Catalyst 6500 Series. Por lo tanto, todas las nuevas implementaciones necesitan seguir esta necesidad estándar y más vieja del IEEE 802.1Q de las redes de emigrar gradualmente del ISL.

Publique este los comandos interface para habilitar el enlace del 802.1Q en un puerto determinado:

```
Switch(config)#interface type slot#/port# Switch(config-if)#switchport !--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation dot1q
```

El estándar IEEE permite la interoperabilidad entre proveedores. La interoperabilidad entre vendedores es ventajosa en todos los entornos de Cisco como nuevo recibe 802.1p-capable NIC y dispositivos está disponible. Aunque las implementaciones ISL y del 802.1Q sean sólidas, la norma IEEE tiene en última instancia la mayor exposición al campo y mayor soporte de tercera persona, que incluye el soporte para los analizadores de red. También, una consideración menor es que el estándar del 802.1Q también tiene una tara de encapsulación más baja que el ISL.

Para lo completo, el marcar con etiqueta implícito en los VLAN nativos crea una observación de seguridad. La transmisión de los bastidores a partir de un VLA N, el VLA N X, a otro VLA N, VLAN Y, sin un router es posible. La transmisión puede ocurrir sin un router si el puerto de origen (el VLA N X) está en el mismo VLA N que el VLAN nativo de un tronco 802.1q en el mismo Switch. La solución alternativa es utilizar un VLA N simulado para el VLAN nativo del trunk.

Publique estos comandos interface para establecer un VLA N como natural (el valor por defecto) para el enlace del 802.1Q en un puerto determinado:

```
Switch(config)#interface type slot#/port# Switch(config-If)#switchport trunk native vlan 999
```

Porque todo el 802.1Q más nuevo de los soportes del hardware, hace que todas las nuevas implementaciones sigan el IEEE 802.1Q estándar y emigren gradualmente redes anteriores del ISL. Hasta hace poco tiempo, muchos módulos del Catalyst 4500/4000 no soportaron el ISL. Por lo tanto, el 802.1Q es la única opción para los troncales Ethernet. Refiera a la salida del **comando show interface capabilities**, o al **comando show port capabilities** para CatOS. Porque el soporte de links troncales requiere el hardware apropiado, un módulo que no soporta el 802.1Q puede nunca soportar el 802.1Q. Una actualización del software no consulta soporte para el 802.1Q. La mayoría del nuevo hardware para el Switches del Catalyst 6500/6000 y del Catalyst 4500/4000 soporta el ISL y el 802.1Q.

Si el VLAN1 se borra de un trunk, pues la sección de la interfaz y del VLAN nativo del administrador de switches discute, aunque no se transmita ni se reciba ningunos datos del usuario, el NMP continúa pasando los protocolos del control en el VLAN1. Los ejemplos de los protocolos del control incluyen el CDP y el VTP.

También, como la sección del VLAN1 discute, el CDP, el VTP, y los paquetes PAgP se envía siempre en el VLAN1 cuando enlace. Con el uso de la encapsulación del dot1q (802.1Q), estas tramas de control se marcan con etiqueta con el VLAN1 si se cambia el VLAN nativo del Switch. Si el enlace del dot1q a un router y al VLAN nativo se cambia en el Switch, una subinterfaz en el VLAN1 es necesaria para recibir las tramas CDP con Tag y proporcionar la visibilidad de vecinos CDP en el router.

Nota: Hay un potencial consideración de seguridad con el dot1q que el marcar con etiqueta implícito del VLAN nativo causa. La transmisión de los bastidores a partir de un VLA N a otro sin

un router puede ser posible. Refiera a la detección de intrusos FAQ para otros detalles. La solución alternativa es utilizar un VLAN ID para el VLAN nativo del trunk que no se utiliza para el acceso del usuario final. Para alcanzar esto, la mayoría de los clientes de Cisco deja simplemente el VLAN1 como el VLAN nativo en un trunk y asigna los puertos de acceso a los VLA N con excepción del VLAN1.

Cisco recomienda una configuración explícita del modo tronco de `deseable dinámico` en los ambos extremos. Este modo es el modo predeterminado. En este modo, los operadores de la red pueden confiar en los mensajes de estado del Syslog y de la línea de comandos que un puerto es `ascendente` y enlace. Este modo es diferente `en del` modo, que puede hacer que aparece un puerto para arriba aunque configuran mal al vecino. Además, los `modos troncales deseables` proporcionan la estabilidad en las situaciones en cuál el lado del link no puede convertirse en un trunk ni cae al `estado del tronco`.

Si negocian al tipo de encapsulación entre el Switches con el uso del DTP, y el ISL se elige como el ganador por abandono si los ambos extremos lo soportan, usted debe publicar este comando interface para especificar el dot1q[1]:

```
switchport trunk encapsulation dot1q
```

Los módulos determinados [1] que incluyen el WS-X6548-GE-TX y el WS-X6148-GE-TX no soportan la conexión troncal de ISL. Estos módulos no validan el comando switchport trunk encapsulation dot1q.

Nota: Publique el **comando switchport mode access** para inhabilitar los trunks en un puerto. Esta incapacidad ayuda a eliminar el tiempo de negociación perdido en que los puertos de host se traen para arriba.

```
Switch(config-if)#switchport host
```

Otras Opciones

Otra configuración del cliente común utiliza el `desirable mode dinámico` en la capa de distribución y la configuración predeterminada más simple (modo de `auto dinámico`) en la capa de acceso. Un poco de Switches, tal como el Catalyst 2900XL, Routers del Cisco IOS, o los dispositivos del otro vendedor, no soporta actualmente la negociación de tronco vía el DTP. Usted puede utilizar al `modo de no negociación` para fijar un puerto al trunk incondicional con estos dispositivos. Este modo puede ayudar a estandarizar en una configuración común a través del campus.

Cisco recomienda `nonegocia` cuando usted conecta con el Cisco IOS a un router. En el bridging, algunas tramas DTP que se reciben de un puerto que se configure con el **modo troncal del switchport** pueden volver al puerto troncal. Tras la recepción de la trama DTP, el puerto del switch intenta renegociar innecesariamente. Para renegociar, el puerto del switch `abajo` y después trae el trunk `para arriba`. Si se habilita el modo de no negociación , el switch no envía tramas DTP.

```
switch(config)#interface type slot#/port# switch(config-if)#switchport mode dynamic desirable !-- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with multiple VLANs. !--- And... switch(config-if)#switchport mode trunk !--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or... switch(config-if)#switchport nonegotiate !--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers. switch(config-if)#switchport access vlan vlan_number !--- Configure a fallback VLAN for the interface. switch(config-if)#switchport trunk native vlan 999 !--- Set the native VLAN. switch(config-if)#switchport trunk allowed vlan vlan_number_or_range !--- Configure the VLANs that are allowed on the trunk.
```

Spanning Tree Protocol

Propósito

El spanning tree mantiene un entorno de Capa 2 libre de loops en redes conmutadas redundantes y puenteadas. Sin el STP, las tramas colocan y/o se multiplican indefinidamente. Esto genera un colapso de la red porque el tráfico elevado interrumpe todos los dispositivos en el dominio de broadcast.

En algún sentido, el STP es un protocolo temprano que fue desarrollado inicialmente para las especificaciones basadas en software lentas del Bridge (IEEE 802.1D). Sin embargo, el STP puede ser complicado para implementarlo con éxito en las redes de switch grandes que tienen:

- Muchos VLA N
- Mucho Switches en un dominio
- Soporte de proveedores múltiples
- Más nuevas mejoras de IEEE

El software del sistema del Cisco IOS ha adquirido los nuevos desarrollos de STP. Las nuevas normas IEEE que incluyen los protocolos multiple spanning-tree STP rápido y 802.1s 802.1w proporcionan el escalamiento plano de la convergencia rápida, de la carga a compartir y del control. Además, las características de la mejora del STP como RootGuard, el BPDU que filtra, el protector Portfast BPDU y Loopguard proporcionan la protección adicional contra los loopes de envío de la capa 2.

Descripción general del funcionamiento PVST+

La elección del root bridge por VLAN es realizada por el switch con el identificador por bridge (BID) raíz más bajo. El BID es la prioridad de bridge combinada con la dirección MAC del switch.

Inicialmente, los BPDU se envían de todo el Switches y contienen la OFERTA de cada Switch y del costo del trayecto para alcanzar ese Switch. Esto habilita la determinación del Root Bridge y del trayecto de costo más bajo a la raíz. Parámetros de la configuración adicionales que son adentro llevados BPDU de la anulación de raíz esos parámetros que localmente se configuren de modo que la red completa utilice los temporizadores consistentes. Para cada BPDU que un Switch reciba de la raíz, NMP central de Catalyst procesa un nuevo BPDU y lo envía hacia fuera con la información de la raíz.

La topología luego converge con estos pasos:

1. Un solo Root Bridge se elige para atravesar entero - dominio del árbol.
2. Un puerto raíz (ese hace frente al Root Bridge) se elige en cada Bridge del nonroot.
3. Se elige un puerto designado para el reenvío de BPDU en cada segmento.
4. Los puertos Nondesignated llegan a ser de bloqueo.

Si desea más información, consulte estos documentos:

- Configurar STP y el IEEE 802.1S MST
- Introducción al Rapid Spanning Tree Protocol [protocolo de árbol de expansión rápida] (802.1w)

Valor por defecto básico	Nombre	Función

de los temporizadores		
sec 2	hola	Controla la salida de los BPDU.
sec 15	retardo de reenvío (Fwd delay)	Controla la longitud del tiempo que un puerto pasa en el `estado de escucha` y el `estado de aprendizaje` e influencia el proceso del cambio de la topología.
sec 20	maxage	Controla la longitud del tiempo que el Switch mantiene la topología actual antes de que el Switch busque un trayecto alternativo. Después del tiempo máximo del envejecimiento (maxage), un BPDU se considera añejo y el Switch busca un nuevo puerto raíz del pool de los puertos de bloqueo. Si no hay puerto bloqueado disponible, el Switch demanda ser la raíz sí mismo en los puertos señalados.

Cisco recomienda que usted no cambia los temporizadores porque esto puede afectar al contrario a la estabilidad. La mayoría de las redes se despliega que no está ajustada. Los temporizadores STP simples que son accesibles vía la línea de comando (tal como intervalo de saludo, maxage, y así sucesivamente) ellos mismos se comprenden de los complejos conjuntos de otros temporizadores intrínsecos y supuestos. Por lo tanto, es difícil ajustar los temporizadores y considerar todas las ramificaciones. Por otra parte, usted puede minar la protección UDLD. Vea la sección de la detección de link unidireccional para más detalles.

Observe en los temporizadores STP:

Los valores del temporizador del STP predeterminado se basan en un cómputo que considere a un diámetro de la red de siete Switches (siete conmutan los saltos de la raíz al borde de la red), y el tiempo que es necesario para que un BPDU viaje del Root Bridge a los Edge Switch en la red, que son siete saltos lejos. Esta suposición computa los valores del temporizador que sea aceptable para la mayoría de las redes. Pero, usted puede cambiar estos temporizadores a más valores óptimos para acelerar los tiempos de convergencia en los cambios de la topología de red.

Usted puede configurar el Root Bridge con el diámetro de la red para un VLA N específico, y los valores del temporizador se computan por consiguiente. Cisco recomienda que, si usted debe realizar los cambios, sólo configuración el diámetro y los parámetros opcionales del tiempo de saludo en el Root Bridge para el VLA N.

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-
time]] !--- This command needs to be on one line.
```

Esta macro hace la raíz del Switch para el VLAN especificado, computa los nuevos valores del temporizador en base del diámetro y del tiempo de saludo especificados, y propaga esta información en los BPDU de configuraciones al resto del Switches en la topología.

Los nuevos estados de puerto y funciones del puerto de la sección describen 802.1D STP y comparan y ponen en contraste 802.1D STP con STP rápido (RSTP). Refiera comprensión del protocolo rapid spanning-tree (802.1w) para más información sobre el RSTP.

Nuevos Estados y Funciones de Puerto

802.1D se define en cuatro diversos estados de puerto:

- Escucha
- Aprendizaje
- Bloqueo
- Reenvío

Vea la tabla en la sección de los estados de puerto para más información. El estado del puerto es mezclado (si bloquea o adelante tráfico), al igual que el papel que el puerto desempeña en la topología activa (puerto raíz, puerto designado, y así sucesivamente). Por ejemplo, desde un punto de vista operativo, no hay diferencia entre un puerto en el estado de bloqueo y un puerto en el estado de escucha. Ambas tramas del descarte y no aprenden las direcciones MAC. La diferencia real miente en el papel que el atravesar - el árbol asigna al puerto. Usted puede asumir con seguridad que un puerto de escucha está señalado o raíz y está en su manera al estado de reenvío. Desafortunadamente, el puerto está una vez en el estado de reenvío, no hay manera de deducir del estado de puerto si el puerto es raíz o señalado. Esto demuestra el error de esta terminología basada en el estado. El RSTP se dirige a este error porque el RSTP desempareja el papel y el estado de un puerto.

Estados de Puertos

Estados de puerto en STP 802.1D

Estados de puertos	Significa	Sincronizaciones predeterminadas al estado siguiente
`Inhabilitado`	Sin funcionamiento desde el punto de vista administrativo.	
Bloqueo	Recibe los BPDU y para los datos del usuario.	Monitorea la recepción de los BPDU. segundo espera 20 para la expiración del maxage o el cambio inmediato si detectan a la falla de link directa/local.
`Escucha`	Envía o recibe los BPDU para marcar si la vuelta al bloqueo es necesaria.	Espera 15 segundos Fwddelay.
Aprendizaje	Construye la tabla topology/CAM.	Espera 15 segundos Fwddelay.

Reenvío	Envía/recibe los datos.	

El cambio total de topología básica es:

- 20 + sec 2 (15) = 50, si espera el maxage para expirar
- 30 segundos para la falla de link directo

Hay solamente tres estados de puerto que se salen en el RSTP, que corresponden a los tres estados operacionales posibles. Los estados de 802.1d desactivado (disabled), bloqueo (blocking) y escucha (listening) se han combinado en un único estado de descarte (discarding) de 802.1w.

Estado de Puerto de STP (802.1D)	Estado de Puerto RSTP (802.1w)	¿El puerto está incluido en la topología activa?	¿El puerto detecta direcciones MAC?
Inhabilitado	Descarte	No	No
Bloqueo	Descarte	No	No
Escucha	Descarte	Sí	No
Aprendizaje	Aprendizaje	Sí	Sí
Reenvío	Reenvío	Sí	Sí

Funciones de Puerto

El papel ahora es una variable que se asigna a un puerto dado. El puerto raíz y los papeles del puerto designado permanecen, pero el papel del puerto de bloqueo ahora está partido en los papeles del respaldo y del puerto alternativo. El Algoritmo del árbol de expansión (STA) determina el papel de un puerto en base de los BPDU. Recuerde esto sobre los BPDU para mantener las cosas simples: hay siempre una manera de comparar cualquier dos BPDU y de decidir a si uno es más útil que el otro. La base de la decisión es el valor que se salva en el BPDU y, de vez en cuando, el puerto en los cuales se recibe el BPDU. El resto de esta sección explica los acercamientos muy prácticos a las funciones del puerto.

Papel del puerto raíz

El puerto que recibe la mejor BPDU en un bridge es el puerto root. Este es el puerto más cercano al bridge root en términos de costo de trayectoria. STA selecciona un solo bridge root de toda la red puenteada (por VLAN). El Root Bridge envía los BPDU que son más útiles que los que cualquier otro Bridge puede enviar. El bridge root es el único bridge en la red que no tiene un puerto root. Todos los demás bridges reciben BPDU en al menos un puerto.

Función de Puerto Designado

Se señala un puerto si puede enviar el mejor BPDU en el segmento con el cual el puerto está conectado. los Bridges 802.1D conectan juntos diversos segmentos (segmentos Ethernet, por ejemplo) para crear un dominio Bridged. En un segmento dado, puede haber solamente una trayectoria hacia el Root Bridge. Si hay dos trayectorias, hay un Bridging Loop en la red. Todos los Bridges que están conectados con un segmento dado escuchan los BPDU de los otros y están de acuerdo con el Bridge que envía el mejor BPDU como el Bridge designado para el segmento.

El puerto correspondiente en ese puente está designado.

Funciones de Puerto Alternativo y de Respaldo

Estas dos funciones de puerto corresponden al estado de bloqueo de 802.1d. La definición de un puerto bloqueado es un puerto que no es haber señalado o el puerto raíz. Un puerto bloqueado recibe un más BPDU útil que el BPDU que envía en su segmento. Recuerde que un puerto requiere necesariamente recibir las BPDU para permanecer bloqueado. RSTP introduce estas dos funciones para ese propósito.

Un puerto alternativo es un puerto que es bloqueado recibiendo más BPDU útiles de otro Bridge. Este diagrama ilustra:

Un puerto de backup es un puerto que es bloqueado recibiendo más BPDU útiles del mismo Bridge que el puerto está prendido. Este diagrama ilustra:

Esta diferenciación ya se realizó internamente en 802.1d. Esto es esencialmente cómo funciona UplinkFast de Cisco. El fundamento detrás de esto es que un puerto alternativo proporciona un trayecto alterno al Root Bridge. Por lo tanto, este puerto puede substituir el puerto raíz si falla. Por supuesto, un puerto de respaldo proporciona conectividad redundante al mismo segmento y no puede garantizar una conectividad alternativa al bridge root. Por lo tanto, el puerto de backup fue excluido del grupo de links ascendentes.

Como consecuencia, el RSTP calcula la topología final para atravesar - árbol con el uso exactamente de los mismos criterios que 802.1D. No hay cambio en la manera que el diversos Bridge y prioridades de puerto se utilizan. El nombre blocking (bloqueo) se utiliza para el estado de descarte en la implementación de Cisco. Las versiones de la versión 7.1 de CatOS y posterior todavía visualizan a los estados de escucha y de aprendizaje, que da aún más información sobre un puerto que la norma IEEE requiere. Pero, la nueva función es que ahora hay una diferencia entre el papel que el protocolo ha determinado para un puerto y su estado actual. Por ejemplo, ahora es perfectamente válido que un puerto sea designado y de bloqueo al mismo tiempo. Mientras que esto sucede típicamente por mismo los períodos cortos, significa simplemente que este puerto está en un estado transitorio hacia la expedición señalada.

Interacciones STP con los VLA N

Hay tres maneras diferentes de correlacionar las VLAN con el Spanning tree:

- Un solo Spanning-tree para todos los VLA N, o protocolo del Common Spanning Tree (CST), por ejemplo el IEEE 802.1D
- Un Spanning Tree por VLAN, o Spanning Tree compartido, como Cisco PVST
- Un Spanning-tree por el conjunto de VLAN, o Múltiples Árboles de expansión (MST), por ejemplo el IEEE 802.1S

De un punto de vista de la configuración, estos tres tipos de modos del árbol de expansión como se relacionan con la interacción con los VLA N pueden ser configurados en uno de tres tipos de modos:

- **pvst** — Per-VLAN Spanning Tree. Esto implementa realmente el PVST+, pero se observa en Cisco IOS Software como simplemente PVST.
- **rápido-PVST** — La evolución del estándar 802.1D aumenta los tiempos de convergencia e incorpora las propiedades basadas en estándares (802.1w) de UplinkFast y del

BackboneFast.

- **mst** — Éste es el estándar 802.1s para atravesar - árbol por el conjunto de VLAN o los MST. Esto también incorpora el componente rápido 802.1w dentro del estándar.

Un Spanning Tree único para todos las VLAN permite una topología activa solamente y, por lo tanto, no permite ningún balanceo de carga. Los bloques de un puerto bloqueado STP para todos los VLA N y no llevan ningún dato.

Un Spanning-tree por el VLA N o el PVST+ permite el Equilibrio de carga pero requiere MÁS BPDU CPU el proceso mientras que el número de VLA N aumenta.

El nuevo estándar 802.1s (MST) permite la definición de hasta 16 casos activos/de las topologías STP, y la asignación de todos los VLA N a estos casos. En un entorno de campus típico, solamente dos casos necesitan ser definidos. Esta técnica permite la escala STP a muchos millares de VLA N mientras que habilita el Equilibrio de carga.

El soporte para el Rápido-PVST y el MST PRE-estándar se introduce en el Cisco IOS Software Release 12.1(11b)EX y 12.1(13)E para el Catalyst 6500. Las versiones del Cisco IOS Software Release 12.1(12c)EW y Posterior del Catalyst 4500with soportan el MST PRE-estándar. El soporte rápido PVST se agrega en Cisco IOS Software Release12.1(19)EW para la plataforma del Catalyst 4500. El MST obediente estándar se soporta en el Cisco IOS Software Release 12.2(18)SXF para el Catalyst 6500 y Cisco IOS Software Release12.2(25)SG para los Catalyst 4500 Series Switch.

Refiera comprensión del protocolo rapid spanning-tree (802.1w) y comprensión del protocolo multiple spanning-tree (802.1s) para más información.

Puertos lógicos del Spanning-tree

El Catalyst 4500 y 6500 Release Note proporcionan la dirección en el número de puertos lógicos en el Spanning-tree por el Switch. La suma de todos los puertos lógicos iguala el número de trunks en el Switch por el número de VLAN activos en los trunks, más el número de interfaces del NON-enlace en el Switch. El Cisco IOS Software genera un mensaje del registro del sistema si el número máximo de interfaces lógicas excede la limitación. Se recomienda para no exceder la dirección recomendada.

Esta tabla compara el número de puertos lógicos soportados con el diversos modo STP y tipo de supervisor:

Supervisor	PVST+	RPVST+	MST
Catalyst 6500 Supervisor 1	6,000[1] total 1,200 por el módulo de switching	6,000 totales 1,200 por el módulo de switching	25,000 totales 3,000[2] por el módulo de switching
Catalyst 6500 Supervisor 2	13,000[1] total 1,800[2] por el módulo de switching	10,000 totales 1,800[2] por el módulo de switching	50,000 totales 6,000[2] por el módulo de switching
Catalyst 6500 Supervisor	13,000 totales 1,800[2] por el	10,000 totales 1,800[2] por el	50,0003 totales 6,000[2] por el módulo

720	módulo de switching	módulo de switching	de switching
Supervisor II del Catalyst 4500 más	1,500 totales	1,500 totales	25,000 totales
Supervisor II plus-10GE del Catalyst 4500	1,500 totales	1,500 totales	25,000 totales
Supervisor IV del Catalyst 4500	3,000 totales	3,000 totales	50,000 totales
Supervisor del Catalyst 4500 V	3,000 totales	3,000 totales	50,000 totales
Supervisor del Catalyst 4500 V 10GE	3,000 totales	3,000 totales	80,000 totales

[1] el número máximo de puertos lógicos totales soportados en el PVST+ que el Cisco IOS Software Release 12.1(13)E es anterior 4,500.

[2] 10 Mbps, 10/100 Mbps, y 100 Mbps que conmutan los módulos soportan un máximo de 1,200 interfaces lógicas por el módulo.

[3] el número máximo de puertos lógicos totales soportados en el MST antes del Cisco IOS Software Release 12.2(17b)SXA es 30,000.

Recomendación

Es difícil proporcionar una recomendación del modo del árbol de expansión sin la información detallada tal como soporte físico, software, número de dispositivos y número de VLA N. Generalmente si el número de puertos lógicos no excede la guía de consulta recomendada, el modo rápido PVST se recomienda para la nueva instrumentación de red. El modo rápido PVST proporciona la convergencia de red rápida sin la necesidad de la configuración adicional tal como Backbone Fast y Uplink Fast. Publique el siguiente comando del thise de fijar el atravesar-árbol en el modo Rápido-PVST:

```
spanning-tree mode rapid-pvst
```

Otras Opciones

En una red con una mezcla de soporte físico de la herencia y de un más viejo software, se recomienda el modo PVST+. Publique este comando de fijar el atravesar-árbol en el modo PVST+:

```
spanning-tree mode pvst ----This is default and it shows in the configuration.
```

Recomiendan el modo MST para el diseño de red del VLA N por todas partes con el número grande de VLA N. Para esta red, la suma de los puertos lógicos puede exceder la guía de consulta para el PVST y el Rápido-PVST. Publique este comando de fijar el atravesar-árbol en el modo MST:

```
spanning-tree mode mst
```

Formatos BPDU

Para soportar el estándar del IEEE 802.1Q, Cisco amplió el protocolo PVST que existe para proporcionar el protocolo PVST+. El PVST+ agrega el soporte para los links a través de mono atravesar del IEEE 802.1Q - región del árbol. El PVST+ es compatible con mono atravesar del IEEE 802.1Q - árbol y los protocolos PVST de Cisco que existan. Además, el PVST+ agrega marcar los mecanismos para asegurarse de que no hay incoherencia de configuración del link troncal de puerto y del VLAN ID a través del Switches. El PVST+ es compatible listo para el uso con el PVST, sin el requisito de un nuevo comando line interface (cli) o configuración.

Aquí están algunos resaltados de la teoría operativa del protocolo PVST+:

- El PVST+ interopera con mono atravesar del 802.1Q - árbol. El PVST+ interopera con el Switches 802.1Q-compliant en el STP común a través del enlace del 802.1Q. El Common Spanning Tree está en el VLAN1, el VLAN nativo, por abandono. Un Common Spanning Tree BPDU se transmite o se recibe con la dirección MAC del bridge-group de la norma IEEE (01-80-c2-00-00-00, el Tipo de protocolo 0x010c) a través de los links del 802.1Q. El Common Spanning Tree se puede arraigar en el PVST o mono atravesar - región del árbol.
- El PVST+ hace un túnel el PVST BPDU a través de la región de VLAN del 802.1Q como datos de multidifusión. Para cada VLA N en un trunk, los BPDU con la dirección MAC compartida Cisco STP (SSTP) (01-00-0c-cc-cd) se transmiten o se reciben. Para los VLA N que son iguales al identificador del puerto VLAN (PVID), el BPDU es untagged. Para el resto de los VLA N, se marcan con etiqueta los BPDU.
- El PVST+ es compatible con versiones anteriores con el switch de Cisco existente en el PVST a través de la conexión troncal de ISL. Los BPDU encapsulados por ISL se transmiten o se reciben a través de los troncales ISL, que es lo mismo que con Cisco anterior PVST.
- Comprobaciones para PVST+ el puerto y las inconsistencias de VLAN. El PVST+ bloquea esos puertos que reciban los BPDU contrarios para prevenir el acontecimiento de los loopes de la expedición. El PVST+ también notifica a los usuarios vía los mensajes de Syslog sobre cualquier inconsistencia.

Nota: En las redes ISL, todos los BPDU se envían con el uso de la dirección MAC de IEEE.

Recomendaciones de la configuración de Cisco

Todos los switches Catalyst tienen el STP habilitado de forma predeterminada. Incluso si usted elige un diseño que no incluya los loopes de la capa 2 y el STP no se habilita para mantener activamente un puerto bloqueado, deje la característica habilitada por estas razones:

- Si hay un loop, el STP previene los problemas que se pueden hacer peores por los datos del Multicast y del broadcast. A menudo, el mispatching, un mún cable, u otra causa induce un loop.
- El STP protege contra una falla de EtherChannel.

- La mayoría de las redes se configuran con el STP, y por lo tanto, consiga la exposición máxima de campo. Más exposición compara generalmente a un más código estable.
- El STP protege contra el mal comportamiento de las NIC del dóblese asociado (o el bridging habilitado en los servidores).
- Muchos protocolos están estrechamente vinculados al STP en el código. Los ejemplos incluyen:PAgPSnooping del (IGMP) del protocolo de mensaje del Grupo de InternetTrunkingSi usted se ejecuta sin el STP, usted puede conseguir los resultados no deseables.
- Durante una interrupción del funcionamiento informado de la red, los ingenieros de Cisco sugieren generalmente que el nonusage del STP esté en el centro del incidente, si en todo concebible.

Para habilitar atravesar - el árbol en todos los VLA N, publica estos comandos global:

```
Switch(config)#spanning-tree vlan vlan_id !--- Specify the VLAN that you want to modify.
Switch(config)#default spanning-tree vlan vlan_id !--- Set spanning-tree parameters to default values.
```

No cambie los temporizadores, que pueden afectar al contrario a la estabilidad. La mayoría de las redes se despliega que no está ajustada. Los temporizadores STP simples que son accesibles vía la línea de comando, tal como intervalo de saludo y maxage, tienen complejos conjuntos de otros temporizadores intrínsecos y supuestos. Por lo tanto, usted puede tener dificultad si usted intenta ajustar los temporizadores y considerar todas las ramificaciones. Por otra parte, usted puede minar la protección UDLD.

Lo ideal es que mantenga el trafico de los usuarios fuera de la VLAN de administración. Esto no se aplica en el Switch del Cisco IOS del Catalyst 6500/6000. No obstante, usted necesita respetar esta recomendación en el Switches y los switches CatOS del Cisco IOS del pequeño-fin que pueden tener una interfaz de administración separada y necesitar ser integrado con el Switches del Cisco IOS. Especialmente con procesadores del switch Catalyst más viejos, guarde el VLAN de administración a parte de los datos del usuario para evitar los problemas con el STP. Una estación terminal en mal funcionamiento puede potencialmente mantener el procesador del Supervisor Engine tan ocupado con los paquetes de broadcast que el procesador puede faltar uno o más BPDU. Pero, un más nuevo Switches con CPU más potentes y los controles que estrangulan alivie esta consideración. Vea el administrador de switches sección interconectar y del VLAN nativo de este documento para más detalles.

No hace la Redundancia del overdesign. Esto puede llevar a demasiados puertos de bloqueo y puede afectar al contrario a la estabilidad a largo plazo. Guarde al diámetro STP total bajo siete saltos. Intente diseñar a Cisco el modelo de multicapa dondequiera que este diseño sea posible. Las características del modelo:

- Dominios conmutados más pequeños
- Triángulos STP
- Puertos bloqueados deterministas

Refiera Gigabit Campus al diseño de red para los detalles.

Influencie y sepa donde residen la funcionalidad raíz y los puertos bloqueados. Documente esta información sobre el Diagrama de topología. Conozca su topología del árbol de expansión, que es esencial para resolver problemas. Los puertos bloqueados son donde el Troubleshooting de STP comienza. La causa del cambio del bloqueo al envío es a menudo la parte clave de Análisis de la causa de raíz. Elija la distribución y las capas del núcleo como la ubicación de la raíz/de la raíz secundaria porque estas capas se consideran a las partes de más estables la red. Marque para

saber si hay la capa óptima 3 y el Hot Standby Router Protocol (HSRP) cubrió con las trayectorias del reenvío de datos de la capa 2.

Este comando es una macro que configura la prioridad de Bridge. La raíz establece la prioridad para ser mucho más baja que el valor por defecto (32,768), y el secundario establece la prioridad para ser razonablemente más bajo que el valor por defecto:

```
Switch(config)#interface type slot/port Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

Nota: Esta macro establece la prioridad raíz para ser cualquiera:

- 8192 por abandono
- La prioridad raíz actual menos 1, si se sabe otro Root Bridge
- La prioridad raíz actual, si su dirección MAC es más baja que la raíz actual

Vlanes innecesaria de la pasa de los puertos troncales, que es un ejercicio bidireccional. Los límites de acción el diámetro del STP y NMP que procesan la tara en las porciones de la red donde ciertos VLA N no se requieren. El recorte automático de VTP no quita el STP de un trunk. Usted puede también quitar el VLAN predeterminado 1 de los trunks.

Consulte Problemas del Spanning Tree Protocol y Consideraciones de Diseño Relacionadas para obtener información adicional.

Otras Opciones

Cisco tiene otro protocolo STP, llamado **VLAN-bridge**, que actúa con el uso de un MAC Address de destino conocido de **01-00-0c-cd-cd-ce** y del Tipo de protocolo de 0x010c.

Este protocolo es el más útil si hay una necesidad de interligar nonroutable o los protocolos heredados entre los VLA N sin interferencia con los casos del árbol de expansión IEEE que se ejecutan en esos VLA N. Si las interfaces VLAN para el tráfico nonbridged se bloquean para el tráfico de la capa 2, el tráfico de sobreposición de la capa 3 se poda inadvertidamente apagado también, que es un efecto secundario indeseado. Este bloqueo de la capa 2 puede suceder fácilmente si las interfaces VLAN para el tráfico nonbridged participan en el mismo STP que los VLA N IP. El VLAN Bridge es un caso de STP aparte para los Bridged Protocol. El protocolo proporciona una topología distinta que se pueda manipular sin un efecto sobre el tráfico IP.

Funcione con el protocolo del VLAN Bridge si el interligar se requiere entre los VLA N en los routeres Cisco tales como el MSFC.

Característica del STP portfast

Usted puede utilizar PortFast para desviar atravesar normal - operación del árbol en los puertos de acceso. PortFast acelera la Conectividad entre las estaciones terminales y los servicios con los cuales las estaciones terminales necesitan conectar después de la inicialización del link. La implementación de DHCP de Microsoft necesita considerar el puerto de acceso en el `modo de reenvío` inmediatamente después que el estado del link sube para pedir y recibir una dirección IP. Algunos protocolos, tales como intercambio de paquetes del Intercambio de paquetes entre redes (IPX) /Sequenced (SPX), necesitan considerar que el puerto de acceso en el `modo de reenvío` inmediatamente después que el estado del link sube para evitar consiga los problemas más cercanos del servidor (GNS).

Consulte Uso de Portfast y de Otros Comandos de Reparar Demoras en la Conectividad de Inicialización de Estaciones de Trabajopara obtener más información.

Descripción general del funcionamiento de PortFast

PortFast salta `escuchar`, el `aprendizaje`, y a los `estados de reenvío` normales de STP. La característica mueve un puerto directamente desde el `bloqueo al modo de reenvío` después de que el link se considere como `para arriba`. Si esta función no está habilitada, el STP desecha todos los datos del usuario hasta que decide que el puerto está listo para pasar al modo de reenvío. Este proceso puede tomar (2 x ForwardDelay) el tiempo, que es 30 segundos por abandono.

`El modo Portfast` previene la generación de una notificación del cambio de topología STP (TCN) cada vez los cambios de un estado de puerto del `aprendizaje al envío`. Los TCN son normales. Pero, una ola de TCN que golpea el Root Bridge pueden prolongar el tiempo de convergencia innecesariamente. Una ola de TCN ocurren a menudo por la mañana, cuando la gente gira sus PC.

Recomendaciones para la configuración del puerto de acceso de Cisco

Fije el STP portfast a `encendido` para todos los puertos de host habilitados. También, STP portfast explícitamente fijado a `apagado` para los links del switch switch y puertos que son parados.

Publique el comando macro del **host del switchport** en el modo de configuración de la interfaz para implementar la configuración recomendada para los puertos de acceso. La configuración también ayuda al autonegotiation y al rendimiento de la conexión perceptiblemente:

```
switch(config)#interface type slot#/port# switch(config-if)#switchport host switchport mode will be set to access spanning-tree portfast will be enabled channel group will be disabled !--- This macro command modifies these functions.
```

Nota: PortFast no significa que atravesando - el árbol no se ejecuta en absoluto en los puertos. Aún se envían, se reciben y se procesan BDPU. El Spanning-tree es esencial para a completamente - LAN funcional. Sin la detección del loop y el bloqueo, un loop puede derribar involuntariamente el LAN entero rápidamente.

También, enlace de la neutralización y canalización para todos los puertos de host. Cada puerto de acceso está habilitado de manera predeterminada para trunking y canalización, aunque los vecinos de conmutación no están previstos por diseño en los puertos de host. Si usted deja estos protocolos para negociar, el retraso subsiguiente en la activación de puerto puede llevar a las situaciones indeseables. Los paquetes iniciales de los puestos de trabajo, tales como solicitudes del DHCP y IPX, no se remiten.

Una mejor opción es configurar PortFast por abandono en el modo de configuración global con el uso de este comando:

```
Switch(config)#spanning-tree portfast enable
```

Entonces, en cualquier puerto de acceso que tenga un concentrador o un Switch en solamente un VLA N, inhabilite la característica portfast en cada interfaz con el **comando interface**:

```
Switch(config)#interface type slot_num/port_num Switch(config-if)#spanning-tree portfast disable
```

Otras Opciones

El protector Portfast BPDU proporciona un método para prevenir los loopes. La protección BPDU

se traslada un puerto nontrunking a un `estado de errDisable` en la recepción de un BPDU en ese puerto.

En condiciones normales, nunca reciba cualquier paquete BPDU en un puerto de acceso que se configure para PortFast. Un BPDU entrante indica una configuración no válida. La mejor acción es apagar el puerto de acceso.

El software del sistema del Cisco IOS ofrece un comando global útil que habilite automáticamente el `BPDU-ROOT-GUARD` en cualquier puerto que se habilite para UplinkFast. Utilice *siempre* este comando. El comando trabaja en por switch, y no por puerto.

Publique este comando global para habilitar el `BPDU-ROOT-GUARD`:

```
Switch(config)#spanning-tree portfast bpduguard default
```

Un Trap del Simple Network Management Protocol (SNMP) o un mensaje de Syslog notifica al administrador de la red si va el puerto abajo. Usted puede también configurar un tiempo de recuperación automática para los puertos `errDisabled`. Vea la sección de la detección de link unidireccional de este documento para más detalles.

Refiera a la mejora de la protección BPDU del árbol de expansión Portfast para otros detalles.

Nota: PortFast para los puertos troncales fue introducido en el Cisco IOS Software Release 12.1(11b)E. PortFast para los puertos troncales se diseña para aumentar los tiempos de convergencia para las redes de la capa 3. Cuando usted utiliza esta característica, esté seguro de inhabilitar la protección BPDU y el filtro BPDU sobre una base de la interfaz.

UplinkFast

Propósito

UplinkFast provee una rápida convergencia STP luego de una falla de enlace directo en la capa de acceso de la red. UplinkFast actúa sin la modificación del STP. El propósito es acelerar el tiempo de convergencia en una circunstancia específica a menos de tres segundos, bastante que el segundo retardo 30 típicos. Refiera a entender y a configurar la Función UplikFast de Cisco.

Información Operativa General

Con diseño multicapa de Cisco el modelo en la capa de acceso, el link ascendente de bloqueo se mueve inmediatamente a un `estado de reenvío` si se pierde el link ascendente de reenvío. La característica no espera a los `estados de escucha y de aprendizaje`.

Un grupo de links ascendentes es un conjunto de puertos por el VLA N que usted puede pensar en como puerto raíz y un puerto raíz de backup. En condiciones normales, los puertos raíz aseguran la Conectividad del acceso hacia la raíz. Si esta conexión de raíz primaria falla por cualquier motivo, el link de raíz de backup golpea con el pie adentro inmediatamente, sin la necesidad de pasar con los 30 segundos típicos del retardo de la convergencia.

Porque UplinkFast desvía con eficacia la topología de STP normal cambio-que dirige el proceso (`escuchando` y `aprendiendo`), un mecanismo de corrección de topología alternativa es necesario. El mecanismo necesita poner al día el Switches en el dominio con la información que las estaciones del extremo local son accesibles vía un trayecto alterno. Así, el switch de capa de acceso que ejecuta UplinkFast también genera las tramas para cada dirección MAC en su tabla CAM a un

Multicast MAC Address bien conocido (01-00-0c-cd-cd-cd Protocolo HDLC. 0x200a). Este proceso pone al día la tabla CAM en todo el Switches en el dominio con la nueva topología.

Recomendación de Cisco

Cisco recomienda que usted habilita UplinkFast para los switches de acceso con los puertos bloqueados si usted ejecuta 802.1D que atraviesa - árbol. No utilice UplinkFast en el Switches sin el conocimiento de topología implícita de un link de raíz de backup — típicamente distribución y los switches del núcleo en diseño multicapa de Cisco. De modo general, no habilite UplinkFast en un Switch con más de dos maneras fuera de una red. Si el Switch está en un ambiente de acceso complejo y usted tiene más de una expedición de bloqueo y una del link del link, evite el uso de esta característica en el Switch o consulte a su ingeniero del Advanced Services.

Publique este comando global para habilitar UplinkFast:

```
Switch(config)#spanning-tree uplinkfast
```

Este comando en Cisco IOS Software no ajusta automáticamente todos los valores de prioridad de Bridge a un valor alto. Bastante, el comando cambia solamente esos VLA N con una prioridad de Bridge que no se ha cambiado manualmente a un cierto otro valor. Además, a diferencia de CatOS, cuando usted restablece un Switch que tenía UplinkFast habilitado, la ninguna forma de este comando (**no spanning-tree uplinkfast**) invierte todos los valores cambiados a sus valores por defecto. Por lo tanto, cuando usted utiliza este comando, usted *debe* marcar el estado actual de las prioridades de Bridge antes y después de que para asegurar que el resultado deseado está alcanzado.

Nota: Usted necesita **toda la palabra clave de los protocolos** para el comando uplinkfast cuando se habilita la característica del filtrado de protocolo. Porque el CAM registra el Tipo de protocolo así como el MAC y la información de VLAN cuando se habilita el filtrado de protocolo, una trama de UplinkFast se debe generar para cada protocolo en cada dirección MAC. La palabra clave **rate** indica los paquetes por segundo de las tramas de actualización de la topología de uplinkfast. Se recomienda el valor predeterminado. Usted no necesita configurar UplinkFast con el RSTP porque el mecanismo se incluye nativo y se habilita automáticamente en el RSTP.

BackboneFast

Propósito

BackboneFast proporciona una convergencia rápida después de que se produce una falla de link indirecto. El BackboneFast reduce los tiempos de convergencia del valor por defecto de 50 segundos a, típicamente, 30 segundos y, de esta manera, agrega las funciones al STP. Una vez más esta característica es solamente aplicable cuando usted ejecuta 802.1D. No configure la característica cuando usted ejecuta el PVST o el MST rápido (que incluyen el componente rápido).

Información Operativa General

Se inicia el BackboneFast cuando un puerto raíz o un puerto bloqueado en un Switch recibe los BPDU inferiores del Bridge designado. El puerto recibe típicamente los BPDU inferiores cuando un Switch rio abajo pierde la conexión a la raíz y comienza a enviar los BPDU para elegir una nueva raíz. Una BPDU inferior identifica a un switch como el root bridge y el bridge designado a la vez.

Bajo atravesar normal - las reglas del árbol, el Switch de recepción ignoran los BPDU inferiores por el tiempo del maxage se configura que. Por abandono, el maxage es el sec 20. Pero, con el BackboneFast, el Switch considera el BPDU inferior como señal de un cambio posible en la topología. El Switch utiliza el Root Link Query (RLQ) BPDU para determinar si tiene un trayecto alterno al Root Bridge. Esta adición al protocolo RLQ permite que un Switch marque si la raíz está todavía disponible. El RLQ mueve un puerto bloqueado al `envío` anterior y notifica el switch aislado que envió el BPDU inferior que la raíz todavía está allí.

Aquí están algunos resaltados de la operación de protocolo:

- Un Switch transmite el paquete RLQ hacia fuera el puerto raíz solamente (que significa que el paquete va hacia la raíz).
- Un Switch que recibe un RLQ puede contestar si es el switch de la raíz, o si ese Switch sabe que ha perdido la conexión con la raíz. Si el Switch no conoce estos hechos, debe remitir a la interrogación hacia fuera su puerto raíz.
- Si un Switch ha perdido la conexión a la raíz, el Switch debe contestar en la negativa a esta interrogación.
- La contestación se debe mandar solamente el puerto del cual la interrogación vino.
- El switch raíz debe responder siempre a esta consulta con una respuesta positiva.
- Si la contestación se recibe en un puerto del nonroot, deseche la contestación.

La operación puede reducir los tiempos de la convergencia de STP por hasta 20 segundos porque el maxage no necesita expirar. Consulte Comprensión y Configuración de BackboneFast en Switches Catalyst para obtener más información.

Recomendación de Cisco

Habilite el BackboneFast en todo el Switches que ejecute el STP solamente si el dominio entero del atravesar-árbol puede soportar esta característica. Usted puede agregar la característica sin la interrupción a una red de producción.

Publique este comando global para habilitar el BackboneFast:

```
Switch(config)#spanning-tree backbonefast
```

Nota: Usted debe configurar este comando global-level en todo el Switches en un dominio. El comando agrega las funciones al STP que todo el Switches necesita entender.

Otras Opciones

El BackboneFast no se soporta en los Catalyst 2900XL y 3500XL Switches. Usted necesita generalmente habilitar el BackboneFast si el dominio del Switch contiene este Switches además del Catalyst 4500/4000, 5500/5000, y 6500/6000 del Switches. Cuando usted implementa el BackboneFast en los entornos con los switches XL, bajo topologías estrictas, usted puede habilitar la característica donde está el Switch más reciente de la línea y está conectado solamente el switch XL con la base en dos lugares. No implemente esta característica si la arquitectura de los switches XL está en la manera de la cadena margarita.

Usted no necesita configurar el BackboneFast con el RSTP o 802.1w porque el mecanismo se incluye nativo y se habilita automáticamente en el RSTP.

Función de Protección contra Loops de Spanning Tree Protocol

La función de protección contra loops es una optimización propiedad de Cisco para el protocolo STP. El Loop Guard protege las redes de la capa 2 contra los loopes que ocurren debido a un malfuncionamiento de la interfaz de la red, un CPU ocupado, o cualquier cosa que previene la expedición normal de los BPDU. Un STP loop se crea cuando un puerto de bloqueo en las transiciones erróneas de una topología redundante al estado de reenvío. Esto sucede generalmente porque uno de los puertos en una topología redundante (no no necesariamente el puerto de bloqueo) paró físicamente el recibir de los BPDU.

El Loop Guard es solamente útil en las redes de switch en donde el Switches es conectado por los enlaces punto a punto, al igual que el caso en la mayoría de las redes modernas del campus y del centro de datos. La idea es que, en un enlace punto a punto, un Bridge designado no puede desaparecer sin el envío de un BPDU inferior o derribar el link. La característica del STP Loop Guard fue introducida en el Cisco IOS Software Release 12.1(13)E del Cisco IOS Software del Catalyst para el Catalyst 6500 y del Cisco IOS Software Release 12.1(9)EA1 para los Catalyst 4500 Switch.

Consulte Mejoras en Spanning-Tree Protocol con las Funciones Protección contra Loops y Detección de Desviación del Tiempo de Llegada de las BPDU para obtener más información sobre la protección contra loops.

Información Operativa General

El Loop Guard marca si un puerto raíz o un suplente/un puerto raíz de backup recibe los BPDU. Si el puerto no recibe los BPDU, el Loop Guard pone el puerto en un estado incoherente (bloqueo) hasta que comience a recibir los BPDU otra vez. Un puerto en el estado inconsistente no transmite BPDU. Si dicho puerto recibe BPDU nuevamente, el puerto y el link se vuelven a considerar viables. La condición sin consistencia en loop se quita del puerto, y el STP determina al estado de puerto. De esta manera, la recuperación es automática.

La función de protección contra loops aísla la falla y deja que el spanning tree converja en una topología estable sin el link o el bridge de la falla. El Loop Guard previene los loopes STP con la velocidad de la versión de STP que es funcionando. No hay dependencia en el STP sí mismo (802.1D o 802.1w) o al ajustar los temporizadores STP. Por estas razones, Cisco recomienda que usted implementa el Loop Guard conjuntamente con el UDLD en las topologías que confían en el STP y donde software support las características.

Cuando el Loop Guard bloquea un puerto contrario, se registra este mensaje:

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

Después de que el BPDU se reciba en un puerto en un estado sin consistencia en loop STP, las transiciones de puerto en otro estado STP. Según el BPDU recibido, esto significa que la recuperación es automática, y no hay intervención necesaria. Después de la recuperación, se registra este mensaje:

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

Interacción con Otras Funciones de STP

Protección de raíz

La protección de raíz hace que un puerto siempre sea puerto designado. El Loop Guard es eficaz solamente si el puerto es puerto raíz o un puerto alternativo, así que significa que sus funciones están mutuamente - la exclusiva. Por lo tanto, el Loop Guard y la protección raíz no se pueden

habilitar en un puerto al mismo tiempo.

UplinkFast

La protección contra loops es compatible con UplinkFast. Si el Loop Guard pone un puerto raíz en un estado de bloqueo, UplinkFast pone en el estado de reenvío un nuevo puerto raíz. Además, UplinkFast no selecciona un puerto es estado loop-inconsistent como puerto raíz.

BackboneFast

La protección contra loops es compatible con BackboneFast. El BackboneFast es accionado por la recepción de un BPDU inferior que venga de un Bridge designado. Porque los BPDU se reciben de este link, el Loop Guard no golpea con el pie adentro. Por lo tanto, el BackboneFast y el Loop Guard son compatibles.

PortFast

PortFast hace que un puerto ingrese en el estado de reenvío designado inmediatamente después de la conexión. Porque un puerto activado por Portfast no es una raíz/un puerto alternativo, el Loop Guard y PortFast son mutuamente - exclusiva.

PAgP

La protección contra loops utiliza los puertos conocidos para STP. Por lo tanto, la protección contra loops puede aprovechar la abstracción de puertos lógicos que PAgP proporciona. Pero, para formar un canal, todos los puertos físicos agrupados en el canal deben tener configuraciones compatibles. El PAgP aplica la configuración uniforme del Loop Guard en todos los puertos físicos para formar un canal. Observe estas advertencias cuando usted configura el Loop Guard en un EtherChannel:

- El STP escoge siempre el primer puerto operativo en el canal para enviar los BPDU. Si ese link llega a ser unidireccional, la protección contra loops bloquea el canal, incluso si otros links en el canal funcionan correctamente.
- Si un conjunto de puertos que son bloqueadas ya por el Loop Guard se agrupa junto para formar un canal, los STP pierdes toda la información del estado para esos puertos, y el nuevo puerto del canal pueden lograr posiblemente al estado de reenvío con un papel señalado.
- Si la protección contra loops bloquea un canal y este deja de funcionar, STP pierde toda la información relativa al estado. Los puertos de los físicos individuales pueden lograr posiblemente al estado de reenvío con un papel señalado, incluso si uno o más de los links que formaron el canal son unidireccionales.

En estos dos casos más recientes, hay una posibilidad de un loop hasta que el UDLD detecte el error. Pero el Loop Guard no puede detectarlo.

Comparación de Protección contra Loops y UDLD

El Loop Guard y la funcionalidad de UDLD solapan parcialmente, en parte en el sentido esos que ambos protegen contra las fallas del STP que los links unidireccionales causan. Estas dos características son diferentes en el acercamiento al problema y también en las funciones. Específicamente, hay fallas unidireccionales específicas que el UDLD no puede detectar, por ejemplo los errores que son causados por un CPU que no envíe los BPDU. Además, el uso del modo agresivo de RSTP y de temporizadores STP puede dar lugar a la formación de loops antes de que UDLD pueda detectar las fallas.

El Loop Guard no trabaja en los links compartidos o en las situaciones donde ha estado unidireccional el link desde la conexión. En el caso de un link que ha sido unidireccional desde la conexión, el puerto nunca recibe los BPDU y se señala. Éste puede ser comportamiento normal, así que el Loop Guard no cubre este caso particular. UDLD brinda protección contra tal escenario.

La habilitación del UDLD y del Loop Guard proporciona el del más alto nivel de la protección. Para más información sobre una comparación de la característica entre el Loop Guard y el UDLD, refiérase:

- *Loop Guard contra la* sección de la *detección de link unidireccional de las* mejoras del Spanning-Tree Protocol usando el Loop Guard y las características de detección oblicua BPDU
- Sección UDLD de este documento

Recomendación de Cisco

Cisco recomienda la habilitación global de la protección contra loops en una red de switch con loops físicos. Usted puede habilitar el Loop Guard global en todos los puertos. De hecho, la función se habilita en todos los links punto a punto. Al estado dúplex del link detecta al enlace punto a punto. Si el modo es dúplex completo, el link se considera de punto a punto.

```
Switch(config)#spanning-tree loopguard default
```

Otras Opciones

Para el Switches que no soporta una configuración de Loop Guard global, la recomendación es habilitar la característica en todos los puertos individuales, que incluye los puertos del Canal de puerto. Aunque no haya ventajas si usted habilita el Loop Guard en un puerto designado, no considere la habilitación un problema. Además, la reconvergencia de un spanning tree válido puede en realidad transformar un puerto designado en un puerto raíz, y esto hace que la función se vuelva útil en este puerto.

```
Switch(config)#interface type slot#/port# Switch(config-if)#spanning-tree guard loop
```

Las redes con topologías sin loops pueden, aún así, obtener beneficios con esta función en caso de que los loops se introduzcan accidentalmente. Pero, la habilitación del Loop Guard en este tipo de topología puede llevar a los problemas del Aislamiento de la red. Si usted construye una topología sin Loops y desea evitar los problemas del Aislamiento de la red, usted puede inhabilitar el Loop Guard global o individualmente. No habilite la protección contra loops en links compartidos.

```
Switch(config)#no spanning-tree loopguard default !--- This is the global configuration.
```

o

```
Switch(config)#interface type slot#/port# Switch(config-if)#no spanning-tree guard loop !---
This is the interface configuration.
```

Función de Protección de Raíz de Spanning Tree

La función de protección de raíz proporciona una manera de asegurar la posición de root bridge en la red. La protección raíz se asegura de que el puerto que habilita esta función sea el puerto designado. Normalmente, los puertos root bridge son todos puertos designados, a menos que dos o más puertos del root bridge estén conectados. Si el bridge recibe BPDU STP superiores en un puerto con la función de protección de raíz habilitada, el bridge hace que este puerto ingrese a un estado STP root-inconsistent. Este estado root-inconsistent es con eficacia igual a un estado de escucha. No se reenvía tráfico a través de este puerto. De esta manera, la protección raíz aplica

la posición del Root Bridge. La protección raíz está disponible en el Cisco IOS Software Release 12.1E y Posterior muy temprano.

Información Operativa General

La protección de raíz es un mecanismo incorporado de STP. La protección raíz no tiene un temporizador sus los propio y confía en la recepción de los BPDU solamente. Cuando aplican a la protección raíz a un puerto, niega a este puerto la posibilidad de convertirse en un puerto raíz. Si la recepción de un BPDU acciona una convergencia del árbol de expansión que haga que un puerto designado se convierte en un puerto raíz, el puerto entonces se pone en un estado incoherente de la raíz. Este mensaje de Syslog ilustra:

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

Después de que el puerto deja de enviar BPDU superiores, vuelve a desbloquearse. Vía el STP, el puerto va del estado de escucha al estado de aprendizaje, y eventual de las transiciones al estado de reenvío. Este mensaje de Syslog muestra la transición:

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

La recuperación es automática. No hay intervención humana necesaria.

Porque la protección raíz fuerza un puerto para ser señalada y el Loop Guard es eficaz solamente si el puerto es un puerto raíz o un puerto alternativo, las funciones son mutuamente - exclusiva. Por lo tanto, usted no puede habilitar el Loop Guard y a la protección raíz en un puerto al mismo tiempo.

Consulte Mejora de Protección de Raíz en Spanning-Tree Protocol para obtener más información.

Recomendación de Cisco

Cisco recomienda que habilite la función de protección de raíz en los puertos que se conectan con los dispositivos de red que no se encuentran bajo control administrativo directo. Para configurar a la protección raíz, utilice estos comandos cuando usted está en el modo de configuración de la interfaz:

```
Switch(config)#interface type slot#/port# Switch(config-if)#spanning-tree guard root
```

EtherChannel

Propósito

El EtherChannel abarca un algoritmo de distribución de trama que multiplexe eficientemente las tramas a través del componente 10/100-Mbps o de los links Gigabit. El algoritmo de distribución de trama permite el multiplexión inversa de los múltiples canales en un solo link lógico. Aunque cada plataforma diferencie de la plataforma siguiente en la implementación, usted debe entender estas propiedades en común:

- Debe haber un algoritmo para multiplexar estadístico las tramas sobre los múltiples canales. En los switches de Catalyst, esto es relacionada con hardware. Aquí están los ejemplos:Catalyst 5500/5000s — La presencia o la falta de un Ethernet Bundling Chip (EBC) en el móduloCatalyst 6500/6000s — Un algoritmo que puede leer más lejos en la trama y multiplexar por la dirección IP
- Hay la creación de un canal lógico para poder funcionar con una instancia única del STP o un

solo peering de la encaminamiento pueda ser utilizado, que depende encendido si es un EtherChannel de la capa 2 o de la capa 3.
- Hay un Management Protocol a marcar para saber si hay coherencia de parámetros en cualquier extremo del link y a ayudar a manejar liar la recuperación de la falla de link o de la adición. Este protocolo puede ser el PAgP o el protocolo link aggregation control (LACP).

Información Operativa General

El EtherChannel abarca un algoritmo de distribución de trama que multiplexe eficientemente las tramas a través del componente 10/100-Mbps, del gigabit o de los links 10-Gigabit. Las diferencias en algoritmos por plataforma surgen de la capacidad de cada tipo de hardware de extraer la información de encabezado de trama para tomar la decisión de distribución.

El algoritmo de la distribución de carga es una opción global para ambos protocolos del control de canal. PAgP y LACP utilizan el algoritmo de distribución de tramas porque el estándar IEEE no indica ningún algoritmo de distribución en particular. Pero, cualquier algoritmo de distribución se asegura de que, cuando se reciben las tramas, el algoritmo no cause misordering de los bastidores que son parte de cualquier conversación dada o duplicación de los bastidores.

Esta tabla ilustra el algoritmo de distribución de trama detalladamente para cada plataforma de la lista:

Plataforma	Algoritmo de Balanceo de Carga del Canal
Catalyst 3750 Series	La carga del Cisco IOS Software del Catalyst 3750 que se ejecuta equilibra el algoritmo que utiliza las direcciones MAC o los IP Addresses, y el Origen de los mensajes o destino del mensaje, o ambos.
Catalyst 4500 Series	El Catalyst 4500 que funciona con la carga del Cisco IOS Software equilibra el algoritmo que utiliza las direcciones MAC, los IP Addresses, o acoda 4 números del puerto (el L4), y el Origen de los mensajes o destino del mensaje, o ambos.
Serie del Catalyst 6500/6000	Hay dos algoritmos de troceo que pueden ser utilizados, que depende del hardware del motor supervisor. El hash es un polinomio de decimoséptimo grado que se implementa en hardware. En todos los casos, el hash toma el MAC, la dirección IP, o el número del puerto IP TCP/UDP y aplica el algoritmo para generar un valor 3-bit. Este proceso ocurre por separado para los SA y los DA. La operación XOP entonces se utiliza con los resultados para generar otro valor 3-bit. El valor determina que viran hacia el lado de babor en el canal se utilizan para remitir el paquete. Los canales en el Catalyst 6500/6000 se pueden formar entre los puertos en cualquier módulo y pueden ser hasta ocho puertos.

Esta tabla indica los métodos de distribución que se soportan en los diversos modelos de Supervisor Engine del Catalyst 6500/6000. La tabla también muestra el comportamiento predeterminado:

Hardware	Descripción	Métodos de Distribución
WS-F6020A (motor) de la capa 2 WS-F6K-PFC (motor de la capa 3)	Supervisor Engine I posterior y placa de función 1 (PFC1) del Supervisor Engine IA/Policy del Supervisor Engine IA	Capa 2 MAC: SA; DA; IP de la capa 3 SA y DA: SA; DA; Dirección de origen y dirección de destino (valor predeterminado)
WS-F6K-PFC2	Supervisor Engine II/PFC2	Capa 2 MAC: SA; DA; IP de la capa 3 SA y DA: SA; DA; Sesión (predeterminada) de la capa 4 SA y DA: Puerto de origen; Puerto de destino; Puerto S y D
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor Engine 720/PFC3BXL del motor 32/PFC3B del Supervisor Engine 720/Supervisor del Supervisor Engine 720/PFC3A	Capa 2 MAC: SA; DA; IP de la capa 3 SA y DA: SA; DA; Sesión (predeterminada) de la capa 4 SA y DA: Puerto de origen; Puerto de destino; Puerto S y D

Nota: Con la distribución de la capa 4, el primer paquete fragmentado utiliza la distribución de la capa 4. Todos los paquetes subsiguientes utilizan la distribución de la capa 3.

Nota: Refiera a estos documentos para encontrar más detalles sobre el soporte EtherChannel en otras Plataformas y cómo configurar y resolver problemas el EtherChannel:

- Introducción a la Redundancia y el Balanceo de Carga de Etherchannel en Switches Catalyst
- Configurando el EtherChannel de la capa 3 y de la capa 2 (guía de configuración del Cisco IOS Software de las Catalyst 6500 Series, 12.2SX)
- Configurando el EtherChannel de la capa 3 y de la capa 2 (guía de configuración del Cisco IOS Software de las Catalyst 6500 Series, 12.1E)
- Configurando el EtherChannel (guía de configuración del Cisco IOS Software del Catalyst 4500 Series Switch, 12.2(31)SG)
- Configurando los EtherChanneles (guía de configuración de software del Catalyst 3750 Switch, 12.2(25)SEE)
- Configuración de EtherChannel en Switches Catalyst 4500/4000, 5500/5000 y 6500/6000 que funcionan con el software del sistema CatOS

Recomendación de Cisco

El Catalyst 3750, el Catalyst 4500, y los Catalyst 6500/6000 Series Switch realizan el Equilibrio de

carga desmenuzando ambos los IP Address de origen y de destino por abandono. Esto se recomienda, con la suposición que el IP es el protocolo dominante. Ejecute este comando para configurar el balanceo de carga:

```
port-channel load-balance src-dst-ip !--- This is the default.
```

Otras Opciones

Dependiendo de los flujos de tráfico, usted puede utilizar la distribución de la capa 4 para mejorar el Equilibrio de carga si el mayor parte del tráfico está entre el mismo IP Address de origen y de destino. Usted debe entender que, cuando se configura la distribución de la capa 4, el desmenuzar incluye solamente los puertos de origen y de destino de la capa 4. No combina los IP Addresses de la capa 3 en el algoritmo de troceo. Ejecute este comando para configurar el balanceo de carga:

```
port-channel load-balance src-dst-port
```

Nota: La distribución de la capa 4 no es configurable en los Catalyst 3750 Series Switch.

Ejecute el comando **show etherchannel load-balance** para comprobar la política de distribución de tramas.

Dependiendo de las plataformas de hardware, usted puede utilizar los comandos CLI para determinar que interconectan en el EtherChannel adelante el flujo de tráfico específico, con la directiva de distribución de tramas como base.

Para los Catalyst 6500 Switch, publique el **comando switch del registro remoto** para iniciar sesión remotamente a la consola del switch processor (SP). Luego, ejecute el comando **test etherchannel load-balance interface port-channel** *number* **{ip | l4port | mac} [***source_ip_add* | *source_mac_add* | ***source_l4_port]*** **[***dest_ip_add* | *dest_mac_add* | ***dest_l4_port]*** .

Para los Catalyst 3750 Switch, publique el *número de canal del puerto de la* **interfaz del balance de la carga del EtherChannel de la prueba {IP | mac} [***source_ip_add* | ***source_mac_add*****]** **[***dest_ip_add* | comando del *dest_mac_add*].

Para el Catalyst 4500, el comando equivalente no está todavía disponible.

Pautas y Restricciones para la Configuración de EtherChannel

EtherChannel verifica las propiedades de todos los puertos físicos antes de agregar puertos compatibles en un solo puerto lógico. Las pautas y las restricciones de configuración varían para diversas plataformas de switch. Complete estas guías de consulta y restricciones para evitar liar los problemas. Por ejemplo, si se habilita QoS, los EtherChanneles no se forman al liar los módulos de la transferencia de la serie del Catalyst 6500/6000 con diversas capacidades de Calidad de servicio (QoS). Para los Catalyst 6500 Switch que funcionan con el Cisco IOS Software, usted puede inhabilitar el control del atributo del puerto de QoS en la agrupación de EtherChannel con el **ningún** comando de la interfaz de canal de puerto del canal-**estado coherente de los qos de los mls**. *El /port Mod de la* **capacidad del** comando show interface visualiza la capacidad de puerto de QoS y la determina si los puertos son compatibles.

Refiera a estas guías de consulta para diversas Plataformas para evitar los problemas de configuración:

- Configurando el EtherChannel de la capa 3 y de la capa 2 (guía de configuración del Cisco IOS Software de las Catalyst 6500 Series, 12.2SX)
- Configurando el EtherChannel de la capa 3 y de la capa 2 (guía de configuración del Cisco IOS Software de las Catalyst 6500 Series, 12.1E)
- Configurando el EtherChannel (guía de configuración del Cisco IOS Software del Catalyst 4500 Series Switch, 12.2(31)SG)
- Configurando los EtherChanneles (guía de configuración de software del Catalyst 3750 Switch, 12.2(25)SEE)

El número máximo de EtherChanneles que se soporten también depende de la plataforma de hardware y de las versiones de software. Catalyst 6500 Switch que funcionan con el soporte del Cisco IOS Software Release 12.2(18)SXE y Posterior un máximo de las interfaces de canal de puerto 128. Versiones de software que son anteriores que el soporte del Cisco IOS Software Release 12.2(18)SXE al máximo de 64 interfaces de canal de puerto. El número de grupo configurable puede ser 1 con el 256, sin importar la versión de software. Los Catalyst 4500 Series Switch soportan un máximo de 64 EtherChanneles. Para los Catalyst 3750 Switch, la recomendación no es configurar más de 48 EtherChanneles en el stack del Switch.

Cálculo de costos del puerto de árbol de expansión

Usted debe entender el cálculo de costos del puerto de árbol de expansión para los EtherChanneles. Usted puede calcular el coste del puerto de árbol de expansión para los EtherChanneles con el método corto o largo. Por abandono, el costo de puerto se calcula en el modo corto.

Esta tabla ilustra el puerto de árbol de expansión costado para un EtherChannel de la capa 2 en base del ancho de banda:

Ancho de banda	Viejo valor STP	Nuevo valor largo STP
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
Gbps N X1	3	6660
10 Gbps	2	2,000
100 Gbps	N/A	200
1 Tbps	N/A	20
10 Tbps	N/A	2

Nota: En CatOS, el coste del puerto de árbol de expansión para un EtherChannel permanece lo mismo después del error del link de miembro del Canal de puerto. En Cisco IOS Software, el costo de puerto para el EtherChannel se pone al día inmediatamente para reflejar el nuevo ancho de banda disponible. Si la conducta deseada es evitar los cambia la topología del árbol de expansión innecesarios, usted puede configurar estáticamente el coste del puerto de árbol de expansión con el uso del comando del *coste del* **coste del atravesar-árbol**.

Port Aggregation Protocol (PAgP)

Propósito

El PAgP es un Management Protocol que marca para saber si hay coherencia de parámetros en

cualquier extremo del link. El PAgP también ayuda al canal con la adaptación a la falla de link o a la adición. Aquí están las características del PAgP:

- PAgp requiere que todos los puertos del canal pertenezcan a la misma VLAN o estén configurados como puertos trunk. Porque los VLAN dinámicos pueden forzar el cambio de un puerto en un diverso VLA N, los VLAN dinámicos no se incluyen en la participación EtherChannel.
- Cuando existe un conjunto ya y la configuración de un puerto se modifica, todos los puertos en el conjunto se modifican para hacer juego esa configuración. Un ejemplo de tal cambio es un cambio del VLA N o de un cambio de `modo de concentración links`.
- El PagP no agrupa puertos que operan a velocidades diferentes ni dúplex de puerto. Si se modifica la velocidad y dúplex cuando existe un conjunto, PAgP modifica la velocidad del puerto y el dúplex para todos los puertos del agrupamiento.

Información Operativa General

El puerto del PAgP controla cada puerto de los físicos individuales (o lógico) que deba ser agrupado. El mismo Multicast Group MAC Address que se utiliza para los paquetes CDP se utiliza para enviar los paquetes PAgP. La dirección MAC es 01-00-0c-cc-cc-cc. Pero, el valor del protocolo es 0x0104. Este es un resumen del funcionamiento del protocolo:

- Mientras el puerto físico esté para arriba, los paquetes PAgP se transmiten cada segundo durante la detección, y cada 30 segundos en el estado constante.
- Si se reciben los paquetes de datos pero no se recibe ningunos paquetes PAgP, se asume que el puerto está conectado con un dispositivo que no sea PAgP capaz.
- Esté atentos los paquetes PAgP que prueban que el puerto físico tiene una conexión bidireccional a otro dispositivo habilitado para PAgP.
- Tan pronto como dos tales paquetes se reciban en un grupo de puertos físicos, intente formar un puerto agregado.
- Si los paquetes PAgP se detienen durante un período, el estado de PAgP se derriba.

Procesamiento Normal

Estos conceptos ayudan a demostrar el comportamiento del protocolo:

- Agport — Un puerto lógico que se compone de todos los puertos físicos en la misma agregación y se puede identificar por su propio ifIndex SNMP. Un agport no contiene los puertos no operacional.
- Canal — Una agregación que satisface los criterios de formación. Un canal puede contener los puertos no operacional y es un superconjunto del agport. Los protocolos, que incluyen el STP y el VTP pero excluyen el CDP y el DTP, se ejecutan sobre el PAgP sobre el agports. Ningunos de estos protocolos pueden enviar o recibir los paquetes hasta que el PAgP asocie el agports a uno o más puertos físicos.
- Capacidad del grupo — Cada puerto físico y el agport posee un parámetro de la configuración que se llame la `cpacidad de grupo`. Un puerto físico se puede agregar con cualquier otro puerto físico que tenga la misma `cpacidad de grupo`, y solamente con tal puerto físico.
- Procedimiento de agrupamiento — Cuando un puerto físico alcanza el `UpData` o al `estado UpPAgP`, el puerto se asocia a un agport apropiado. Cuando el puerto sale de cualquiera de esos estados para otro estado, el puerto es separado del agport.

Esta tabla proporciona más detalles sobre los estados:

Estado	Significado
`UpData`	No se han recibido paquetes PAgP. Se envían paquetes PAgP. El puerto físico es el único puerto que está conectado con el agport. Los paquetes no PAgP se pasan adentro y hacia fuera entre el puerto físico y el agport.
`BiDir`	Se recibió exactamente un paquete PagP que comprueba que hay una conexión bidireccional con exactamente un vecino. El puerto físico no está conectado a ningún puerto agregado. Los paquetes PAgP se envían y reciben.
`UpPAgP`	Este puerto físico, tal vez en asociación con otros puertos físicos, está conectado a un puerto agregado. Los paquetes PAgP se envían y reciben en el puerto físico. Los paquetes no PAgP se pasan adentro y hacia fuera entre el puerto físico y el agport.

Los ambos extremos de ambas conexiones deben estar de acuerdo con agrupar. El agrupar se define como el grupo de puertos más grande del agport que los ambos extremos del permiso de la conexión.

Cuando un puerto físico alcanza al `estado UpPAgP`, el puerto se asigna al agport que tiene puertos físicos del miembro que hagan juego la `cpacidad de grupo del` nuevo puerto físico y que estén en el estado del `BiDir` o el `estado UpPAgP`. Tales puertos del `BiDir` se mueven al `estado UpPAgP` al mismo tiempo. Si no hay agport que tiene parámetros constitutivos del puerto físico que sean compatibles con el puerto físico nuevamente listo, el puerto se asigna a un agport con los parámetros apropiados que no tiene ningún puerto físico asociado.

Un tiempo de espera de PagP agotado puede ocurrir en el vecino más reciente que se conoce en el puerto físico. El puerto que los tiempos hacia fuera están quitados del agport. Al mismo tiempo, todos los puertos físicos en el mismo agport que tienen temporizadores que también han medido el tiempo hacia fuera se quitan. Esto activa un puerto agregado cuyo otro extremo ha muerto para ser derribado al mismo tiempo, en lugar de un puerto físico por vez.

Comportamiento en caso de Fallas

Si un link en un canal que exista se falla, el agport es actualizado y el tráfico se desmenuza sobre los links que sigue habiendo sin la pérdida. Los ejemplos de tal error incluyen:

- Se desenchufa el puerto
- Se quita el Convertidor de la interfaz de Gigabit (GBIC)
- La fibra está quebrada

Nota: Cuando usted falla un link en un canal con un poder apagado o el retiro de un módulo, el comportamiento puede ser diferente. Por definición, un canal requiere dos puertos físicos. Si un puerto se pierde del sistema en un canal con dos puertos, se derriba el puerto agregado lógico y el puerto físico original está reinicializado en cuanto a atravesar - árbol. El tráfico puede ser desechado hasta que el STP permita que el puerto esté disponible para los datos otra vez.

Esta diferencia en los dos modos de la falla es importante cuando usted planea el mantenimiento de una red. Puede haber un cambio de topología STP cuyo usted necesita tener en cuenta cuando usted realiza un retiro o una inserción en línea de un módulo. Usted debe manejar cada vículo físico en el canal con el sistema de administración de la red (NMS) porque el agport puede seguir siendo imperturbado a través de un error.

Complete una de estas recomendaciones para atenuar los cambios de topología no deseados en el Catalyst 6500/6000:

- Si un puerto único se utiliza por el módulo para formar un canal, utilice tres o más módulos (tres totales).
- Si el canal atraviesa dos módulos, utilice dos puertos en cada módulo (cuatro totales).
- Si un canal con dos puertos es necesario a través de dos indicadores luminosos LED amarillo de la placa muestra gravedad menor, utilice solamente los puertos del Supervisor Engine.

Opciones de Configuración

Usted puede configurar los EtherChanneles en diversos modos, pues esta tabla resume:

Modo	Opciones Configurables
Encendido	El PAgP no es en funcionamiento. Los Canales de puerto, sin importar cómo se configura el puerto de vecino. Si el puerto del vecino está encendido se forma un canal.
Auto	La agregación está bajo el control de PAgP. Un puerto se coloca en un estado de negociación pasivo. No se envía ningunos paquetes PAgP en la interfaz hasta que por lo menos un paquete PAgP se reciba que indica que el remitente actúa en el `desirable mode`.
Deseable	La agregación está bajo el control de PAgP. Un puerto se coloca en un estado de negociación activa, en quien el puerto inicia las negociaciones con otros puertos vía la transmisión de paquetes PAgP. Un canal está formado con otro grupo de puertos, ya sea en modo deseable o automático.
`No silencioso` éste es el valor por defecto en la fibra FE del Catalyst 5500/5000 y los puertos de GE.	Un modo de palabra clave automático o deseable. Si no se recibe ningunos paquetes de datos en la interfaz, la interfaz nunca se asocia a un agport y no se puede utilizar para los datos. Este control del bidirectionality fue proporcionado para el hardware específico del Catalyst 5500/5000 porque algunas fallas de link dan lugar a una rotura aparte del canal. Cuando usted habilita al `modo no silencioso`, un puerto de vecino de recuperación nunca se permite venir salvaguardia y romper el canal aparte innecesariamente. el liar Más-flexible y los controles mejorados del bidirectionality están presentes por abandono en el Catalyst 4500/4000 y hardware de las 6500/6000

	Series.
`Silencioso` éste es el valor por defecto en todo el Catalyst 6500/6000 y 4500/4000 de los puertos, así como 5500/5000 de los puertos de cobre.	Un modo de palabra clave automático o deseable. Si no se recibe ningunos paquetes de datos en la interfaz, después de un período de agotamiento del tiempo de espera 15-second, la interfaz se asocian solamente a un agport. Así, la interfaz se puede utilizar para la Transmisión de datos. El modo silencioso además permite la operación del canal en el caso de un socio que puede ser un analizador o un servidor que nunca envía PAgP.

`Los parámetros de silencio o de no silencio` afectan a cómo los puertos reaccionan a las situaciones que causan el tráfico unidireccional. Cuando un puerto no puede transmitir debido a una interfaz física fallada o una fibra dañada o un cable, el puerto de vecino se puede todavía salir en un estado operacional. El partner continúa transmitiendo los datos. Pero, se pierden los datos porque el tráfico de retorno no puede ser recibido. Los Spanning-Tree Loop pueden también formar debido al carácter unidireccional del link.

Algunos puertos de fibra tienen la capacidad deseada para traer el puerto a un estado no operacional cuando el puerto pierde su recibe la señal (FEFI). Esta acción hace el puerto del partner llegar a ser nonoperational y hace con eficacia los puertos en los ambos extremos del link ir abajo.

Cuando usted utiliza los dispositivos que transmiten los datos (BPDU), y le no puede detectar las condiciones unidireccionales, utilice al `modo no silencioso` para permitir que los puertos sigan siendo nonoperational hasta que reciba los datos sean presente y el link se verifica para ser bidireccional. El tiempo que toma el PAgP para detectar un link unidireccional es cerca de 3.5 * 30 segundos = el sec 105. Treinta segundos son el tiempo entre dos mensajes PAgP sucesivos. Use el UDLD, que es el detector más rápido de enlaces unidireccionales.

Cuando usted utiliza los dispositivos que no transmiten ningunos datos, utilice al `modo silencioso`. El uso del `modo silencioso` fuerza el puerto para llegar a ser conectado y operativo, sin importar si los datos recibidos están presentes o no. Además, para esos puertos que puedan detectar la presencia de una condición unidireccional, utilizan al `modo silencioso` por abandono. Los ejemplos de estos puertos son más nuevas Plataformas que utilizan el Layer 1 FEFI y UDLD.

Para dar vuelta apagado a la canalización en una interfaz, publique el comando **ningún número del grupo de canales**:

```
Switch(config)#interface type slot#/port# Switch(config-if)#no channel-group 1
```

Verificación

La tabla en esta sección proporciona un resumen de todos los escenarios de modo de canalización posibles del PAgP entre dos directamente switches conectados, Switch A y switches B. Algunas de estas combinaciones pueden hacer el STP poner los puertos en el lado de canalización en el `estado de errDisable`, así que significa que esas combinaciones apagan los puertos en el lado de canalización. La función de protección del error de configuración EtherChannel se habilita por abandono.

Modo del canal del Switch A	Modo del canal del switch B	Estado del canal del Switch A	Estado del canal del switch B
Encendido	Encendido	Canal (no PAgP)	Canal (no PAgP)
Encendido	No configurado	Sin Canal (puerto errDisable)	Sin Canal
Encendido	Auto	Sin Canal (puerto errDisable)	Sin Canal
Encendido	Deseable	Sin Canal (puerto errDisable)	Sin Canal
No configurado	Encendido	Sin Canal	Sin Canal (puerto errDisable)
No configurado	No configurado	Sin Canal	Sin Canal
No configurado	Auto	Sin Canal	Sin Canal
No configurado	Deseable	Sin Canal	Sin Canal
Auto	Encendido	Sin Canal	Sin Canal (puerto errDisable)
Auto	No configurado	Sin Canal	Sin Canal
Auto	Auto	Sin Canal	Sin Canal
Auto	Deseable	Canal PAgP	Canal PAgP
Deseable	Encendido	Sin Canal	Sin Canal
Deseable	No configurado	Sin Canal	Sin Canal
Deseable	Auto	Canal PAgP	Canal PAgP
Deseable	Deseable	Canal PAgP	Canal PAgP

[Recomendación de la configuración de Cisco para los canales L2]

Habilite el PAgP y utilice una configuración de `deseable deseable` en todos los links

EtherChanneles. Vea esta salida para más información:

```
Switch(config)#interface type slot#/port# Switch(config-if)#no ip address !--- This ensures that there is no IP !--- address that is assigned to the LAN port. Switch(config-if)#channel-group number mode desirable !--- Specify the channel number and the PAgP mode.
```

Verifique la configuración de esta manera:

```
Switch#show run interface port-channel number Switch#show running-config interface type slot#/port# Switch#show interfaces type slot#/port# etherchannel Switch#show etherchannel number port-channel
```

Prevenga los errores de las configuraciones de EtherChannel

Usted puede configurar mal un EtherChannel y crear un Spanning-Tree Loop. Este misconfiguration puede abrumar el proceso del Switch. El software del sistema del Cisco IOS incluye la característica del **misconfig del guardia del EtherChannel del atravesar-árbol** para prevenir este problema.

Publique este comando configuration en todos los switches de Catalyst que funcionen con el Cisco IOS Software como software del sistema:

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

Otras Opciones

Al canalizar dos dispositivos que no soporten el PAgP sino soportar el LACP, la recomendación es habilitar el LACP con la configuración del active LACP en los ambos extremos de los dispositivos. Vea la sección del protocolo link aggregation control (LACP) de este documento para más información.

Al canalizar a los dispositivos que no soportan el PAgP o el LACP, usted debe cifrar difícilmente el canal a `encendido`. Este requisito se aplica a estos dispositivos de ejemplo:

- Servidores
- Local Director
- Switches de contenido
- Routers
- Switches con el software anterior
- Catalyst 2900XL/3500XL Switch
- Catalyst 8540s

Ejecute estos comandos:

```
Switch(config)#interface type slot#/port# Switch(config-if)#channel-group number mode on
```

Protocolo link aggregation control (LACP)

El LACP es un protocolo que permite a los puertos con características similares formar un canal a través de la negociación dinámica con switches contiguos. El PAgP es un protocolo de propiedad de Cisco que usted puede funcionar con solamente en los switches Cisco y eso Switches que autorizaron la versión de los vendedores. Pero LACP, que se define como IEEE 802.3ad, permite a los switches Cisco administrar la canalización Ethernet con cualquier dispositivo que cumpla con la especificación 802.3ad.

El LACP se soporta con estas Plataformas y versiones:

- Catalyst 6500/6000 series con Cisco IOS Software Release 12.1(11b)EX y posteriores
- Catalyst 4500 Series con el Cisco IOS Software Release 12.1(13)EW y Posterior
- Catalyst 3750 Series con el Cisco IOS Software Release 12.1(14)EA1 y Posterior

Existen pocas diferencias entre LACP y PAgP desde una perspectiva funcional. Ambos protocolos soportan un máximo de ocho puertos en cada canal, y las propiedades del mismo puerto se marcan antes de formar al conjunto. Estas propiedades del puerto incluyen las siguientes:

- Velocidad
- Dúplex
- Tipo del VLAN nativo y del enlace

Las diferencias notables entre el LACP y el PAgP son las siguientes:

- El protocolo LACP puede ejecutarse solamente en los puertos dúplex completo y no soporta los puertos semi dúplexes.
- Puertos de la espera en caliente de los soportes a protocolo LACP. El LACP intenta siempre configurar el número máximo de puertos compatibles en un canal, hasta el máximo que el hardware permite (ocho puertos). Si el LACP no puede agregar todos los puertos que son compatibles (por ejemplo, si el sistema remoto tiene limitaciones del hardware más-restrictivas), todos los puertos que no se pueden incluir activamente en el canal se ponen en el estado de la espera en caliente y se utilizan solamente si uno de los puertos usados falla.

Nota: Para los Catalyst 4500 Series Switch, el número máximo de puertos para los cuales usted pueda asignar la misma clave administrativa es ocho. Para los Catalyst 6500 y 3750 Switches que funciona con el Cisco IOS Software, el LACP intenta configurar el número máximo de puertos compatibles en un EtherChannel, hasta el máximo que el hardware permite (ocho puertos). Los ocho puertos adicionales se pueden configurar como puertos de la espera en caliente.

Información Operativa General

El LACP controla cada puerto de los físicos individuales (o lógico) que se liará. Los paquetes LACP se envían con el uso del Multicast Group MAC Address **01-80-c2-00-00-02**. El valor de tipo/valor es 0x8809 con un subtipo de 0x01. Este es un resumen del funcionamiento del protocolo:

- El protocolo depende de los dispositivos para anunciar sus capacidades de agregación e información del estado. Las transmisiones se envían en un asiduo, forma periódica en cada link aggregatable.
- Siempre que el puerto físico está en funcionamiento, los paquetes PAgP son transmitidos cada segundo durante la detección y cada 30 segundos en estado estable.
- Los Partners en un link aggregatable escuchan la información que se envía dentro del protocolo y deciden qué acción o acciones a tomar.
- Los puertos compatibles se configuran en un canal, hasta el máximo que el hardware permite (ocho puertos).
- Las agregaciones se mantienen por intercambio regular y oportuno de información de estado actualizada entre los socios de links. Si los cambios de configuración (debido a una falla de link, por ejemplo), los Partners del protocolo miden el tiempo hacia fuera y toman la acción apropiada basada en el nuevo estado del sistema.
- Además de las transmisiones periódicas de la unidad de datos LACP (LACPDU), si hay un cambio a la información del estado, el protocolo transmite un LACPDU evento-conducido a los Partners. Los Partners del protocolo toman la acción apropiada basada en el nuevo

estado del sistema.

Parámetros LACP

Para permitir que el LACP determine si un conjunto de los links conecta con el mismo sistema y si esos links son compatibles desde el punto de vista de la agregación, es necesario poder establecer:

- Identificador único A global - para cada sistema que participa en la agregación del link.Cada sistema que ejecute el LACP se debe asignar una prioridad que se puede elegir o automáticamente (con la prioridad predeterminada de 32768) o por el administrador. La prioridad del sistema se utiliza principalmente en conjunto con una dirección MAC del sistema para formar el identificador de sistema.
- Medios de identificar el conjunto de las capacidades que se asocian a cada puerto y a cada aggregator, según lo entendido por un sistema dado.Cada puerto en el sistema se debe asignar una prioridad o automáticamente (con la prioridad predeterminada del 128) o por el administrador. La prioridad se utiliza en conjunto con el número de puerto para formar el identificador del puerto.
- Medios de identificar un grupo de la agregación del link y su aggregator asociado.La capacidad de un puerto de agregar con otro es resumida por un parámetro de 16 bits simple del número entero estrictamente mayor de cero que se llame dominante. Cada clave se determina en base de diversos factores, por ejemplo:Las características físicas del puerto, que incluyen la velocidad de datos, duplexity, y Punto a punto o medio compartidoRestricciones de configuración que son establecidas por el administrador de la redDos claves se asocian a cada puerto:Una clave administrativaUna clave operativaLa clave administrativa permite la manipulación de los valores de la clave de la Administración y, por lo tanto, el usuario puede elegir esta clave. La clave operativa es utilizada por el sistema para formar las agregaciones. El usuario no puede elegir o cambiar esta clave directamente. El conjunto de puertos en un sistema dado que comparte el mismo valor de la clave operativo reputa a los miembros del mismo grupo dominante.

Así, dado dos sistemas y un conjunto de puertos con la misma clave administrativa, cada sistema intenta agregar los puertos, a partir del puerto con la prioridad más alta en el sistema más prioritario. Este comportamiento es posible porque cada sistema conoce estas prioridades:

- Su propia prioridad, que el usuario o el software asignó
- Su prioridad del partner, que fue descubierta a través de los paquetes LACP

Comportamiento en caso de Fallas

El comportamiento de falla para el LACP es lo mismo que el comportamiento de falla para el PAgP. Si un link en un canal existente se falla (por ejemplo, si se desenchufa un puerto, un GBIC se quita, o una fibra está quebrada), el agport es actualizado y el tráfico se desmenuza sobre los links restantes dentro de 1 segundos. Ningún tráfico que no requiera rehashing después de que el error (que es el tráfico que continúa enviando encendido el mismo link) no sufre ninguna pérdida. Restablecer el link fallido acciona otra actualización al agport, y el tráfico se desmenuza otra vez.

Opciones de Configuración

Usted puede configurar los LACP EtherChanneles en diversos modos, pues esta tabla resume:

Modo	Opciones Configurables

Encendido	Se obliga la formación de agregado de links sin negociación LACP. El switch no envía el paquete LACP ni procesa ningún paquete LACP entrante. Si el puerto del vecino está encendido se forma un canal.
(O) de no configurado	El puerto no está canalizando, independientemente de cómo se configura el vecino.
Pasivo (valor predeterminado)	Esto es similar al modo automático en PagP. El switch no inicia el canal, pero entiende los paquetes LACP entrantes. Par (en el estado activo) inicia negociación (enviando un paquete LACP) a que el Switch recibe y a cuál contesta el Switch, formando eventual el canal de la agregación con el par.
Activo	Esto es similar al modo deseable en el PAgP. El Switch inicia la negociación para formar un link global. Se forma el link agregado si el otro extremo se ejecuta en el modo activo o modo pasivo de LACP.

El LACP utiliza un temporizador por intervalos 30-second (Slow_Periodic_Time) después de que se establezcan los LACP EtherChanneles. El número de segundos antes de la invalidación de información de LACPDU recibida al usar los descansos largos (3 veces el Slow_Periodic_Time) es 90. El UDLD se recomienda como más detector rápido de los links unidireccionales. Usted no puede ajustar los temporizadores LACP, y en este momento, usted no puede configurar el Switches para utilizar la transmisión rápida del unidad de datos del protocolo (PDU) (cada segundo) para mantener el canal después de que se forme el canal.

Verificación

La tabla en esta sección proporciona un resumen de todos los escenarios de modo de canalización posibles LACP entre dos directamente switches conectados (el Switch A y el Switch B). Algunas de estas combinaciones pueden hacer al guardia del EtherChannel poner los puertos en el lado de canalización en el estado de errDisable. La función de protección del error de configuración EtherChannel se habilita por abandono.

Modo del canal del Switch A	Modo del canal del switch B	Estado del canal del Switch A	Estado del canal del switch B
Encendido	Encendido	Canal (no LACP)	Canal (no LACP)
Encendido	Desactivado	Sin Canal (puerto errDisable)	Sin Canal
Encendido	Pasivo	Sin Canal (puerto errDisable)	Sin Canal
Encendido	Activo	Sin Canal (puerto	Sin Canal

		errDisable)	
Desactivado	Desactivado	Sin Canal	Sin Canal
Desactivado	Pasivo	Sin Canal	Sin Canal
Desactivado	Activo	Sin Canal	Sin Canal
Pasivo	Pasivo	Sin Canal	Sin Canal
Pasivo	Activo	Canal LACP	Canal LACP
Activo	Activo	Canal LACP	Canal LACP

Recomendaciones de Cisco

Cisco recomienda habilitar PAgP en las conexiones de canales entre los switches de Cisco. Al canalizar dos dispositivos que no soporten el PAgP sino soportar el LACP, la recomendación es habilitar el LACP con la configuración del active LACP en los ambos extremos de los dispositivos.

En el Switches que funciona con CatOS, todos los puertos en un Catalyst 4500/4000 y un protocolo del canal del PAgP del uso del Catalyst 6500/6000 por abandono. Para configurar los puertos para utilizar el LACP, usted debe fijar el protocolo del canal en los módulos al LACP. El LACP y el PAgP no pueden ejecutarse en el mismo módulo de los switches que ejecutan CatOS. Esta limitación no se aplica al Switches que funciona con el Cisco IOS Software. El Switches que funciona con el Cisco IOS Software puede soportar el PAgP y el LACP en el mismo módulo. Publique estos comandos para fijar modo de canal LACP al active y asignar un número dominante administrativo:

```
Switch(config)#interface range type slot#/port# Switch(config-if)#channel-group admin_key mode active
```

El comando show etherchannel summary visualiza un resumen uno line por el grupo de canal que incluye esta información:

- Números de grupo
- Números de Canal de puerto
- Estatus de los puertos
- Los puertos que son parte del canal

El comando show etherchannel port-channel visualiza la información detallada del Canal de puerto para todos los grupos de canal. La salida incluye esta información:

- Estatus del canal
- Protocolo se utiliza que
- El tiempo puesto que los puertos fueron liados

Para visualizar la información detallada para un grupo de canal específico, con los detalles de cada puerto mostrado por separado, utiliza el **comando detail del** *channel_number del* **EtherChannel de la demostración**. La salida de comando incluye los detalles del partner y los detalles del Canal de puerto. Refiera a configurar LACP (802.3ad) entre un Catalyst 6500/6000 y un Catalyst 4500/4000 para más información.

Otras Opciones

Con los dispositivos de canal que no soportan el PAgP o el LACP, usted debe cifrar difícilmente el canal a `encendido`. Este requisito se aplica a estos dispositivos:

- Servidores

- Local Director
- Switches de contenido
- Routers
- Switches con un más viejo software
- Catalyst 2900XL/3500XL Switch
- Catalyst 8540s

Ejecute estos comandos:

```
Switch(config)#interface range type slot#/port# Switch(config-if)#channel-group admin_key mode on
```

Detección de Link Unidireccional

Propósito

UDLD es propiedad de Cisco, protocolo liviano desarrollado para detectar instancias de comunicaciones unidireccionales entre los dispositivos. Hay otros métodos para detectar el estado bidireccional de los medios de transmisión, tales como FEFI. Pero, hay los casos en los cuales los mecanismos de detección del Layer 1 no son suficientes. Estos escenarios pueden dar lugar a:

- La operación impredecible del STP
- El incorrecto o la Inundación excesiva de los paquetes
- El envío del tráfico a agujeros negros

La característica UDLD dirige estas condiciones de falla en las interfaces de Ethernet de la fibra y del cobre:

- Monitorea las configuraciones del cableado físico — Apaga como `errDisabled` cualquier puerto del miswired.
- Protege contra los links unidireccionales — En la detección de un link unidireccional que ocurra debido a los media o el funcionamiento incorrecto de puerto/interfaz, el puerto afectado se apaga según lo `errDisabled`. Se genera un mensaje de Syslog correspondiente.
- Además, controles del modo agresivo UDLD que un link bidireccional previamente juzgado no pierde la Conectividad en caso que el link llegue a estar inutilizable debido a la congestión. El modo agresivo UDLD realiza las pruebas de conectividad en curso a través del link. El propósito primario del modo agresivo UDLD es evitar el envío a agujeros negros del tráfico en ciertas condiciones falladas que no alocución por el modo normal UDLD.

Consulte Comprensión y Configuración de la Característica del Unidirectional Link Detection Protocol (UDLD) para más detalles.

El Spanning-tree tiene un flujo BPDU unidireccional de estado estacionario y puede tener los errores las listas de esa esta sección. Un puerto puede no poder repentinamente transmitir los BPDU, que causa un cambio de estado STP del `bloqueo al envío` en el vecino. Con todo, un loop todavía existe porque el puerto puede todavía recibir.

Información Operativa General

El UDLD es un protocolo de la capa 2 que trabaja sobre la capa LLC (MAC de destino 01-00-0c-cc-cc-cc, tipo de Protocolo HDLC. RÁPIDO 0x0111). Cuando usted ejecuta el UDLD conjuntamente con los mecanismos del Layer 1 FEFI y del autonegotiation, usted puede validar la

integridad física (L1) y lógica (L2) de un link.

El UDLD tiene disposiciones para las características y la protección que el FEFI y el autonegotiation no pueden realizarse. Estas características incluyen:

- La detección y el caché de la información de vecino
- El apagar de cualquier puertos inadecuadamente conectados
- Detección de malos funcionamientos de puerto/interfaz lógica o de incidentes en los links que no son de punto a punto**Nota:** Cuando los links no son de punto a punto, atraviesan los conversores de medios o el Hubs.

El UDLD emplea estos dos mecanismos básicos.

1. El UDLD aprende sobre los vecinos y mantiene la información actualizada a caché local.
2. El UDLD envía un tren de las sondas UDLD/de los mensajes de la generación de eco (hola) en la detección de un nuevo vecino o siempre que un vecino pida una resincronización del caché.

El UDLD envía constantemente las sondas/los mensajes de eco en todos los puertos. En la recepción de un mensaje UDLD correspondiente en un puerto, se acciona una fase y un proceso de validación de la detección. Se habilita el puerto si se cumplen todas las condiciones válidas. Se cumplen las condiciones si el puerto es bidireccional y se ata con alambre correctamente. Si las condiciones no se cumplen, el puerto `errDisabled`, que acciona este mensaje de Syslog:

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

Para una lista completa de mensajes del sistema por el recurso, que incluye los eventos UDLD, refiera a los mensajes UDLD (Mensajes del sistema Cisco IOS System, el volumen 2 de 2).

Después de que el establecimiento de un link y de su clasificación como bidireccional, UDLD continúe haciendo publicidad de las sondas/de los mensajes de eco en un intervalo predeterminado del sec 15.

Esta tabla proporciona la información sobre los estados de puerto:

Estado de Puerto	Comentario
Indeterminado	Se ha inhabilitado el UDLD en curso/vecino de la detección.
No aplicable	Se ha inhabilitado el UDLD.
Apagado	Se ha detectado el link unidireccional y se ha inhabilitado el puerto.
Bidireccional	Se ha detectado el link bidireccional.

Mantenimiento de la memoria caché de vecino

El UDLD envía periódicamente hola la sonda/los paquetes de eco en cada interfaz activa para

mantener la integridad del caché del vecino UDLD. En la recepción de un mensaje Hello Messages, el mensaje se oculta y se mantiene la memoria por un período máximo, que se define como el tiempo en espera. Cuando expira el tiempo en espera, la entrada de caché correspondiente se envejece hacia fuera. Si un nuevo mensaje Hello Messages se recibe dentro del período del tiempo en espera, el nuevo substituye la más vieja entrada y se reajusta el temporizador correspondiente del Tiempo para vivir.

Siempre que se inhabilite una interfaz habilitada para UDLD o siempre que se reajusta un dispositivo, todas las entradas de caché existente para las interfaces que las influencias del cambio de configuración se borran. Esta liquidación mantiene la integridad del caché UDLD. El UDLD transmite por lo menos un mensaje para informar a los respectivos vecinos la necesidad de vaciar las entradas correspondientes del caché.

Mecanismo de detección de la generación de eco

El mecanismo de eco forma la base del algoritmo de detección. Siempre que un dispositivo UDLD aprenda sobre un nuevo vecino o reciba un pedido de resincronización de un vecino del hacia fuera-de-sincronizar, el dispositivo enciende o recomienza la ventana de detección en su lado de la conexión y envía las ráfagas de mensaje de eco en la contestación. Porque este comportamiento debe ser lo mismo a través de todos los vecinos, el remitente de la generación de eco espera recibir las generaciones de eco detrás en la contestación. Si los fines de la ventana de detección sin la recepción de cualesquiera mensajes de respuesta válidos, el link se consideran unidireccionales. De esta punta, un reestablecimiento o un proceso de cierre de puerto del link puede ser accionado. Otro, los estados anómalos raros para las cuales el dispositivo marcan es:

- El circuito hecho atrás transmite las fibras (del tx) al conector del rx del mismo puerto
- Miswirings en el caso de una interconexión de los medios compartidos (por ejemplo, un concentrador o un dispositivo similar)

Tiempo de Convergencia

Para prevenir los loopes STP, el Cisco IOS Software Release 12.1 y Posterior ha reducido el intervalo de mensajes predeterminado UDLD a partir de 60 segundos a 15 segundos. Este intervalo fue cambiado para apagar un link unidireccional antes de que antes un puerto bloqueado en 802.1D que atravesaba - el árbol puede a la transición a un estado de reenvío. El valor del intervalo de mensajes determina la velocidad en la que un vecino envía las sondas UDLD después de la fase de conexión o de detección. El intervalo de mensaje no necesita coincidir con ambos extremos de un link, aunque la configuración coherente sea deseable, en lo posible. Cuando establecen a los vecinos UDLD, el intervalo entre mensajes configurado se envía al vecino, y el intervalo de tiempo de espera para ese par se calcula como:

```
3 * (message interval)
```

Como tal, una relación de peer mide el tiempo hacia fuera después de que se falten tres hellos consecutivos (o las sondas). Porque los intervalos entre mensajes son diferentes en cada lado, este valor de agotamiento del tiempo es simplemente diferente en cada lado, y un lado reconoce un error más rápidamente.

La hora aproximada que es necesaria para que el UDLD detecte una falla unidireccional de un link previamente estable está aproximadamente:

```
2.5 * (message interval) + 4 seconds
```

Éste es aproximadamente 41 segundos con el intervalo de mensajes predeterminado de 15 segundos. Esta cantidad de tiempo es lejos más corta que los 50 segundos que son generalmente necesarios para el STP al reconverge. Si el NMP CPU tiene algunos ciclos de repuesto y si el usuario monitorea cuidadosamente su nivel de utilización (una práctica adecuada), una reducción del intervalo entre mensajes (incluso) al mínimo de 7 segundos es aceptable. También, las ayudas de esta reducción del intervalo entre mensajes aceleran la detección por un factor importante.

Nota: El mínimo es 1 segundo en el Cisco IOS Software Release 12.2(25)SEC.

Por lo tanto, el UDLD tiene una dependencia asumida de los temporizadores del spanning tree predeterminado. Si el STP está ajustado para converger más rápidamente que el UDLD, considere un mecanismo alternativo, tal como la característica del STP Loop Guard. Considere un mecanismo alternativo en este caso cuando usted implementa RSTP (802.1w), también, porque el RSTP tiene características de convergencia en el ms, dependiendo de la topología. Para estos casos, utilice el Loop Guard conjuntamente con el UDLD para proporcionar la mayoría de la protección. El Loop Guard previene los loopes STP con la velocidad de la versión de STP que es funcionando. Y el UDLD toma el cuidado de la detección de conexiones unidireccionales en los links EtherChanneles individuales o en los casos en los cuales los BPDU no fluyen a lo largo de la dirección quebrada.

Nota: El UDLD es independiente del STP. El UDLD no coge cada situación de la falla del STP, tal como esos errores que sean causados por un CPU que no envíe los BPDU por una época que sea mayor que (2 * Fwddelay + maxage). Por esta razón, Cisco recomienda que usted implementa el UDLD conjuntamente con el Loop Guard en las topologías que confían en el STP.

Precaución: Guárdese de las versiones anteriores del UDLD en el Switches 2900XL/3500XL que utiliza un nonconfigurable, 60-segundo intervalo de mensajes predeterminado. Él es susceptible a las condiciones del Spanning-Tree Loop.

Modo Agresivo UDLD

El UDLD agresivo fue creado para dirigir específicamente esos pocos casos en los cuales una prueba en curso de la conectividad bidireccional es necesaria. Como tal, la característica del modo agresivo proporciona protección mejorada contra las condiciones peligrosas de link unidireccional en estas situaciones:

- Cuando la pérdida de UDLD PDU es simétrica y los ambos extremos miden el tiempo hacia fuera. En este caso, ninguno de los dos puertos errdisabled.
- Un lado de un link tiene un puerto pegado (tx y rx).
- Un lado del link permanece arriba mientras que el otro lado desciende.
- Se inhabilita el autonegotiation, u otro mecanismo de la detección de falla del Layer 1.
- Una reducción en la confianza en los mecanismos FEFI del Layer 1 es deseable.
- Usted necesita la protección máxima contra los Errores de link unidireccional en los links de punto a punto FE/GE. Específicamente, donde no hay admisible error entre dos vecinos, las sondas UDLD-agresivas se pueden considerar como latido del corazón, la presencia cuyo garantiza la salud del link.

El caso más común para una implementación del UDLD agresiva es realizar el control de la Conectividad en un miembro de un conjunto cuando el autonegotiation u otro mecanismo de la detección de falla del Layer 1 está inhabilitado o inutilizable. Es determinado útil con las conexiones EtherChannel porque el PAgP y el LACP, incluso si está habilitado, no utilizan los

temporizadores de saludo muy bajos en el estado constante. En este caso, el UDLD agresivo tiene la ventaja agregada de prevenir los Spanning-Tree Loop posibles.

Es importante entender que el modo de UDLD normal marca para saber si hay una condición del link unidireccional, incluso después un link alcanza el estado bidireccional. El UDLD se significa para detectar los problemas de la capa 2 que causan los loopes STP, y esos problemas son generalmente unidireccionales (porque los BPDU fluyen solamente en una dirección en el estado constante). Por lo tanto, el uso del UDLD normal conjuntamente con el autonegotiation y el Loop Guard (para las redes que confían en el STP) es casi siempre suficiente. Con el modo agresivo UDLD habilitado, después de que todos los vecinos de un puerto hayan envejecido hacia fuera, en el anuncio o en la fase de la detección, el modo agresivo UDLD recomienza la secuencia de la conexión en un esfuerzo para resincronizar con potencialmente hacia fuera-de-sincroniza a los vecinos. Si después de que un tren rápido de los mensajes (ocho recomprobaciones falladas) el link todavía se juzgue indeterminado, el puerto se pone en el estado de errDisable.

Nota: Algunos switches no son aptos para el modo UDLD agresivo. Actualmente, el Catalyst 2900XL y Catalyst 3500XL ha cifrado difícilmente los intervalos entre mensajes de 60 segundos. Esto no se considera suficientemente rápido proteger contra los loopes potenciales STP (con los parámetros del STP predeterminado presuntos).

Recuperación automática de los links UDLD

La recuperación errdisable global se inhabilita de forma predeterminada. Después de que se habilite global, si un puerto entra el estado de errDisable, se vuelve a permitir automáticamente después de un intervalo de tiempo seleccionado. El tiempo predeterminado es 300 segundos, que es un temporizador global y es mantenido para todos los puertos en un switch. Dependiendo de la versión de software, usted puede prevenir manualmente un reenablement del puerto si usted fija el tiempo de espera errdisable para ese puerto para inhabilitar con el uso del mecanismo de recuperación del tiempo de espera errdisable para el UDLD:

```
Switch(config)#errdisable recovery cause udld
```

Considere el uso de la función de tiempo en espera errdisable al implementar el modo UDLD agresivo con las capacidades de administración de red no fuera de banda, particularmente en la capa de acceso o en cualquier dispositivo que pueda tornarse aislado de la red en el caso de una situación errdisable.

Refiera a la recuperación errDisable (referencia del comando cisco ios de las Catalyst 6500 Series, 12.1 E) para más detalles en cómo configurar un período de agotamiento del tiempo de espera para los puertos en el estado de errDisable.

La recuperación errDisable puede ser especialmente importante para el UDLD en la capa de acceso cuando los switches de acceso se distribuyen a través de un entorno de campus y la visita manual de cada Switch para volver a permitir ambo uplinks tarda el tiempo considerable.

Cisco no recomienda la recuperación errDisable en la base de la red porque hay típicamente puntas de la entrada múltiple en una base, y la recuperación automática en la base puede llevar a los problemas que se repiten. Por lo tanto, usted debe volver a permitir manualmente un puerto en la base si el UDLD inhabilita el puerto.

UDLD en los Links Ruteados

Con el fin de esta discusión, un link ruteado es cualquiera uno de estos dos Tipos de conexión:

- Punto a punto entre dos nodos del router (configurados con una máscara de subred 30-bit)
- UN VLA N con los puertos múltiples pero ese soporta solamente las conexiones ruteadas, tales como adentro una topología de la base de la capa 2 de la fractura

Cada Interior Gateway Routing Protocol (IGRP) tiene características únicas con respecto a cómo administra las relaciones de vecinos y la convergencia de ruta. Esta sección describe el (EIGRP) de las características que son relevantes a esta discusión, que pone en contraste dos de los Routing Protocol más frecuentes que se utilizan hoy, del protocolo del Open Shortest Path First (OSPF) y del IGRP mejorado.

Nota: Un Layer 1 o casi acoda el error 2 en cualquier resultado de punto a punto de la red ruteada en el desmembramiento inmediato de la conexión de la capa 3. Porque el único puerto del switch en ése los VLAN cambios a un estado no-conectado sobre el error de la capa 1/Layer 2, la característica del estado Auto de la interfaz sincroniza a los estados de puerto de la capa 2 y de la capa 3 en aproximadamente dos segundos y ponga la interfaz VLAN de la capa 3 en un estado encendido/apagado (Line Protocol que está abajo).

Si usted asume los valores de temporizador predeterminado, el OSPF envía los mensajes Hello Messages cada 10 segundos y tiene un Intervalo muerto de 40 segundos (4 * hola). Estos temporizadores son constantes para el OSPF de punto a punto y las redes de broadcast. Porque el OSPF requiere la comunicación bidireccional para formar una adyacencia, el tiempo de la Conmutación por falla del malo-caso es 40 segundos. Esto es verdad incluso si el error de la capa 1/Layer 2 no es puro en una conexión Point-to-Point y deja un escenario mal concebido del cual el protocolo de la capa 3 deba ocuparse. Porque el tiempo de detección del UDLD es muy similar al tiempo de detección de un temporizador de emergencia OSPF que expira (aproximadamente 40 segundos), las ventajas de la configuración del modo de UDLD normal en un enlace punto a punto de la capa 3 OSPF son limitadas.

En muchos casos, el EIGRP converge más rápidamente que el OSPF. Pero es importante observar que la comunicación bidireccional no es un requisito para que los vecinos intercambien la información de ruteo. En los escenarios de falla males concebido muy específicos, el EIGRP es vulnerable al envío a agujeros negros del tráfico que dura hasta que un cierto otro evento traiga las rutas vía ese active del vecino. El modo de UDLD normal puede paliar estas circunstancias porque detecta el Error de link unidireccional y el error inhabilita el puerto.

Para las conexiones ruteadas de la capa 3 que utilizan cualquier Routing Protocol, el UDLD normal todavía proporciona la protección contra los problemas que están presentes sobre la activación del link inicial, tal como miscabling o hardware defectuoso. Además, el modo agresivo UDLD proporciona estas ventajas en las conexiones ruteadas de la capa 3:

- Previene el envío a agujeros negros innecesario del tráfico (con los temporizadores mínimos requeridos en algunos casos)
- Coloca un link inestable en el estado errdisable
- Protege contra los loopes que resultan de las configuraciones de EtherChannel de la capa 3

Comportamiento predeterminado del UDLD

El UDLD está globalmente desactivado y preparado para la habilitación en puertos de fibra de manera predeterminada. Porque el UDLD es un protocolo de la infraestructura que es necesario entre el Switches solamente, el UDLD se inhabilita por abandono en los puertos de cobre, que tienden a ser utilizados para el acceso del host. Observe que usted debe habilitar el UDLD global y en el nivel de la interfaz antes de que los vecinos puedan alcanzar el estado bidireccional. El intervalo de mensajes predeterminado es 15 segundos. Pero, el intervalo de mensajes predeterminado puede mostrar como siete segundos en algunos casos. Refiera al Id. de bug

Cisco CSCea70679 (clientes registrados solamente) para más información. El intervalo de mensajes predeterminado es configurable entre siete y 90 segundos, y inhabilitan al modo agresivo UDLD. El Cisco IOS Software Release 12.2(25)SEC más futuro reduce estos temporizadores mínimos al segundo.

Recomendación de la configuración de Cisco

En el amplia mayoría de los casos, Cisco recomienda que usted habilita el modo de UDLD normal en todos los links del Punto a punto FE/GE entre los switches Cisco, y fija el intervalo de mensaje de UDLD a 15 segundos cuando usted utiliza 802.1D predeterminado que atraviesa - los temporizadores del árbol. Además, donde las redes confían en el STP para la Redundancia y la convergencia (que significa que hay uno o más puertos en el estado de bloqueo STP en la topología), el uso UDLD conjuntamente con las características apropiadas y los protocolos. Tales características incluyen el FEFI, autonegotiation, Loop Guard, y así sucesivamente. Típicamente, si se habilita el autonegotiation, el modo agresivo no es necesario porque el autonegotiation compensa la detección de falla en el Layer 1.

Publique uno del comando options estos dos para habilitar el UDLD:

Nota: El sintaxis ha cambiado a través de las diversas Plataformas/versión.

- `udld enable !--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default. udld port O`
- `udld enable !--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled by individual port command.`

Usted debe habilitar manualmente los puertos que se apagan debido a los síntomas del link unidireccional. Utilice uno de estos métodos:

```
udld reset !--- Globally reset all interfaces that UDLD shut down. no udld port udld port
[aggressive] !--- Per interface, reset and reenable interfaces that UDLD shut down.
```

Los comandos global configuration del *intervalo del* **intervalo del udld** y de la **recuperación errDisable de la causa de la recuperación errDisable** pueden ser utilizados para recuperarse automáticamente del estado de error inhabilitado UDLD.

Cisco recomienda que usted utiliza solamente el mecanismo de la recuperación errDisable en la capa de acceso de la red, con los temporizadores de recuperación de 20 minutos o más, si el acceso físico al Switch es difícil. La mejor situación es dar un plazo de la hora para la estabilización y el troubleshooting de la red, antes del puerto se trae detrás en la línea y causa la inestabilidad de la red.

Cisco recomienda que usted *no* utiliza los mecanismos de recuperación en la base de la red porque ésta puede causar la inestabilidad que se relaciona con los eventos de la convergencia cada vez que un link defectuoso está traído la salvaguardia. El diseño redundante de una red del núcleo proporciona un trayecto de backup para un link fallido y da un plazo de la hora para una investigación de las razones del error UDLD.

Utilice el UDLD sin el STP Loop Guard

Para la capa 3 Puntos a punto, o los links de la capa 2 donde hay una topología de STP sin loop (ningunos puertos que bloquean), Cisco recomiendan que usted habilita el UDLD agresivo en los

links de punto a punto FE/GE entre los switches Cisco. En este caso, el intervalo entre mensajes se fija a siete segundos, y 802.1D STP utiliza los temporizadores predeterminados.

UDLD en los EtherChanneles

Si el STP Loop Guard está desplegado o no desplegado, recomiendan el modo agresivo UDLD para cualquier configuración de EtherChannel, conjuntamente con el modo de canal deseable. En configuraciones de EtherChannel, un error en el link del canal que lleva atravesar - el árbol BPDU y tráfico de control del PAgP puede causar los loopes inmediatos entre los partners de canal si los links del canal se desmontonan. El modo agresivo UDLD apaga un puerto fallado. El PAgP (auto/modo de canal deseable) puede entonces negociar un nuevo link de control y eliminar con eficacia un link fallido del canal.

UDLD con el Spanning-tree 802.1w

Para prevenir los loopes cuando usted utiliza más nuevo atravesar - versiones del árbol, modo de UDLD normal del uso y STP Loop Guard con los RSTP como 802.1w. El UDLD puede proporcionar la protección contra los links unidireccionales durante una fase de la conexión, y el STP Loop Guard puede prevenir los loopes STP en caso que los links lleguen a ser unidireccionales *después de que el* UDLD haya establecido los vínculos como bidireccionales. Porque usted no puede configurar el UDLD para ser menos que los temporizadores del valor por defecto 802.1w, el STP Loop Guard es necesario para prevenir completamente los loopes en topologías redundantes.

Consulte Comprensión y Configuración de la Característica del Unidirectional Link Detection Protocol (UDLD) para más detalles.

Probar y Monitorear el UDLD

No es fácil probar UDLD sin un componente genuinamente defectuoso/unidireccional en el laboratorio, como GBIC defectuoso. El protocolo fue diseñado para detectar los escenarios de falla menos comunes que los escenarios que se emplean generalmente en un laboratorio. Por ejemplo, si usted realiza una prueba simple tal como desenchufar un hilo de una fibra para ver al `estado de errDisable` deseado, usted necesita primero apagar el autonegotiation del Layer 1. De lo contrario, el puerto físico se desactiva, lo que reajusta la comunicación de mensaje UDLD. El extremo remoto se mueve al estado `indeterminado` en el modo de UDLD normal, y se mueve al estado de errDisable solamente con el uso del modo agresivo UDLD.

Un método de pruebas adicional simula la pérdida de PDU vecino para el UDLD. El método es utilizar los filtros de la Capa MAC para bloquear UDLD/CDP a la dirección de hardware mientras que usted permite que otros direccionamientos pasen. Un poco de Switches no envía las tramas UDLD cuando el puerto se configura para ser un destino del Switched Port Analyzer (SPAN), que simula a un vecino UDLD insensible.

Para monitorear el UDLD, utilice este comando:

```
show udld gigabitethernet1/1 Interface Gi1/1 --- Port enable administrative configuration
setting: Enabled Port enable operational state: Enabled Current bidirectional state:
Bidirectional Current operational state: Advertisement - Single neighbor detected Message
interval: 7 Time out interval: 5
```

También, del enable mode en el Switches del Cisco IOS Software Release 12.2(18)SXD o Posterior, usted puede publicar el **comando show udld neighbor** ocultado para marcar el

contenido del caché UDLD (de la manera que lo hace el CDP). Es a menudo muy útil comparar el caché UDLD a memoria caché CDP para verificar si hay una anomalía del protocol específico. Siempre que el CDP también se afecte, significa típicamente que todos los BPDU/PDU son afectados. Por lo tanto, también marque el STP. Por ejemplo, verifique las modificaciones recientes de identidad o cambios en la ubicación de los puertos raíz o designados.

Usted puede monitorear el estado UDLD y la coherencia de la configuración con el uso de las variables del SNMP MIB de Cisco UDLD.

Multilayer Switching

Información general

En software del sistema del Cisco IOS, el Multilayer Switching (MLS) se soporta en la serie del Catalyst 6500/6000, y solamente internamente. Esto significa que el router debe ser instalado en el Switch. Un más nuevo soporte de motores del supervisor del Catalyst 6500/6000 MLS CEF, en el cual la tabla de ruteo se descarga a cada indicador luminoso LED amarillo de la placa muestra gravedad menor. Esto requiere el hardware adicional, que incluye la presencia de un Distributed Forwarding Card (DFC). Los DFC no se soportan en software CatOS, incluso si usted opta utilizar el Cisco IOS Software en el indicador luminoso LED amarillo de la placa muestra gravedad menor del router. Los DFC se soportan solamente en software del sistema del Cisco IOS.

Caché MLS que se utiliza para habilitar las estadísticas de Netflow en los switches de Catalyst son el caché del flujo basado que los switches de Catalyst del indicador luminoso LED amarillo de la placa muestra gravedad menor y de la herencia del Supervisor Engine I utilizan para habilitar el Layer 3 Switching. El MLS se habilita por abandono en el Supervisor Engine 1 (o el Supervisor Engine 1A) con el MSFC o el MSFC2. No hay configuración de MLS adicional necesaria para las funciones predeterminadas MLS. Usted puede configurar caché MLS en uno de tres modos:

- destino
- origen de destino
- puerto de origen de destino

La máscara del flujo se utiliza para determinar al modo MLS del Switch. Estos datos se utilizan posteriormente para habilitar los flujos de la capa 3 en los switches de Catalyst del IA-aprovisionado del Supervisor Engine. Las cuchillas del Supervisor Engine II no utilizan caché MLS para conmutar los paquetes porque este indicador luminoso LED amarillo de la placa muestra gravedad menor es el hardware CEF-habilitado, que es una mucho más tecnología extensible. Caché MLS se mantiene en el indicador luminoso LED amarillo de la placa muestra gravedad menor del Supervisor Engine II para habilitar la exportación estadística del Netflow solamente. Por lo tanto, el Supervisor Engine II se puede habilitar para el flujo completo en caso necesario, sin el impacto negativo en el Switch.

Configuración

El tiempo de envejecimiento MLS se aplica a todas las entradas de memoria caché de MLS. El valor de tiempo de envejecimiento se aplica directamente a la desactualización del modo de destino. Usted divide el valor de tiempo de envejecimiento MLS por dos para derivar el tiempo de envejecimiento del modo del fuente-a-destino. Divida el valor de tiempo de envejecimiento MLS por ocho para encontrar el tiempo de envejecimiento a todo régimen. El valor de tiempo de envejecimiento del valor por defecto MLS es el sec 256.

Usted puede configurar el tiempo de envejecimiento normal en el rango de 32 a 4092 segundos en ocho segundos incrementos. Cualquier valor de tiempo de envejecimiento que no sea un múltiplo de ocho segundos se ajusta al múltiplo más cercano del sec 8. Por ejemplo, un valor de 65 se ajusta a 64 y un valor de 127 se ajusta al 128.

Otros eventos pueden causar la purgación de las entradas de MLS. Tales eventos incluyen:

- Cambios de ruteo
- Un cambio en el estado del linkPor ejemplo, el link PFC está abajo.

Para guardar caché MLS el tamaño bajo 32,000 entradas, habilite estos parámetros después de que usted publique los **mls que envejecen el** comando:

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

Configuración

Una entrada de caché típica se quita que es la entrada para los flujos a y desde un Domain Name Server (DNS) o el servidor TFTP que puedan nunca ser utilizados posiblemente otra vez después de que se cree la entrada. La detección y el ageout de estas entradas guarda el espacio en caché MLS para el otro tráfico de datos.

Si usted necesita habilitar el tiempo del envejecimiento rápido MLS, fije el valor inicial al sec 128. Si el tamaño del caché MLS continúa creciendo sobre 32,000 entradas, disminuya la configuración hasta que el tamaño de la memoria caché permanezca bajo 32,000. Si el caché continúa creciendo sobre 32,000 entradas, disminuya el tiempo de envejecimiento normal MLS.

Configuración de MLS recomendada de Cisco

Deje el MLS en el valor predeterminado, destino solamente, a menos que se requiera la exportación de NetFlow. Si se requiere el Netflow, habilite el flujo completo MLS solamente en los sistemas del Supervisor Engine II.

Publique este comando para habilitar el destino de flujo MLS:

```
Switch(config)#mls flow ip destination
```

Tramas gigantes

Unidad máxima de transmisión (MTU)

La Unidad máxima de transmisión (MTU) (MTU) es el datagrama o el tamaño de paquetes más grande de los bytes que una interfaz puede enviar o recibir sin hacer fragmentos del paquete.

Según el estándar de IEEE 802.3, el tamaño de trama Ethernet máximo es:

- **1518 bytes** para las tramas regulares (1500 bytes más 18 bytes adicionales del encabezado Ethernet y de la cola CRC)
- **1522 bytes** para las tramas 802.1Q-encapsulated (1518 más 4 bytes de marcar con etiqueta)

baby giants: El bebé que Giants ofrece permite que el Switch pase por/los paquetes delanteros que son levemente más grandes que los Ethernetes IEEE MTU, bastante que declarando las tramas de gran tamaño y desechándolas.

Jumbo: La definición del tamaño de trama es vendedor-dependiente, pues los tamaños de tramas no son parte de la norma IEEE. Las Tramas gigantes son las tramas que son más grandes que el tamaño de trama Ethernet estándar (que es 1518 bytes, que incluye la encabezado de la capa 2 y el [FCS] de la secuencia de verificación de tramas).

El tamaño de MTU predeterminado es 9216 bytes después de que el soporte de trama Jumbo se haya habilitado en el puerto individual.

Cuándo contar con los paquetes que son más grandes de 1518 bytes

Para transportar el tráfico a través de las redes de switch, esté seguro que el tráfico transmitido MTU no excede el que se soporte en las plataformas del switch seleccionar. Hay diversas razones que la talla del MTU de ciertos bastidores puede ser truncada:

- **Requisitos específicos del vendedor** — Las aplicaciones y ciertos NIC pueden especificar una talla del MTU que sea fuera del estándar 1500 bytes. Este cambio ha ocurrido debido a los estudios que prueban que un aumento en el tamaño de una trama Ethernet puede aumentar la producción media.
- Enlace: para transportar información VLAN-ID entre switches u otros dispositivos de red, se usó trunking para incrementar la trama Ethernet estándar. Hoy, dos la mayoría de las formas comunes de conexión troncal son:Encapsulación ISL del propietario de Cisco802.1Q
- **Multiprotocol Label Switching (MPLS)** — Después de que usted habilite el MPLS en una interfaz, el MPLS tiene el potencial para aumentar el tamaño de trama de un paquete, que depende del número de escrituras de la etiqueta en la pila de etiquetas para un paquete MPLS-marcado con etiqueta. El tamaño total de la etiqueta es 4 bytes. El tamaño total de una pila de etiquetas es:`n * 4 bytes`Si se forma una pila de etiquetas, es posible que las tramas excedan la MTU.
- **el hacer un túnel del 802.1Q** — el 802.1Q que hace un túnel los paquetes contiene dos etiquetas del 802.1Q, cuyo uno a la vez es solamente generalmente visible al hardware. Por lo tanto, la etiqueta interna agrega 4 bytes al valor MTU (tamaño del contenido).
- **El Tunneling Protocol del Universal Transport Interface (UTI) /Layer 2 versión 3 (capa 2TPv3)** — UTI/Layer 2TPv3 encapsula los datos de la capa 2 que se remitirán sobre la red del IP. UTI/Layer 2TPv3 puede aumentar el tamaño de trama original en hasta 50 bytes. La nueva trama incluye una nueva encabezado del encabezado IP (20-byte), de la capa 2TPv3 (12-byte), y una nueva encabezado de la capa 2. El payload de la capa 2TPv3 consiste en la trama completa de la capa 2, que incluye la encabezado de la capa 2.

Propósito

(1-Gbps y 10-Gbps) la transferencia basado en hardware de alta velocidad ha hecho las Tramas

gigantes una solución muy concreta a los problemas de la producción subóptima. Aunque no hay estándar del funcionario para los tamaños de trama Jumbo, un valor común que se adopta a menudo en el campo es bastante 9216 bytes (9 KB).

Consideración de la eficacia de la red

Usted puede calcular la eficacia de la red para un reenvío de paquete si usted divide su Tamaño de carga útil por la suma del valor de arriba y del Tamaño de carga útil.

Incluso si el aumento de la eficacia del establecimiento de una red con las Tramas gigantes es solamente modesto, y va a partir del 94.9 por ciento (1500 bytes) al 99.1 por ciento (9216 bytes), a los gastos indirectos de proceso (utilización de la CPU) de los dispositivos de red y a las disminuciones de los host extremos proporcional al tamaño de paquetes. Esta es la razón por la cual el LAN de alto rendimiento y las tecnologías de interconexión de redes PÁLIDAS tienden a preferir los tamaños máximos del marco bastante grandes.

La mejora del rendimiento es solamente posible cuando se realizan las Transferencias de datos largas. Las aplicaciones de ejemplo incluyen:

- Comunicación continua del servidor (por ejemplo, transacciones del [NFS] del sistema de archivos de red)
- Clúster del servidor
- Respaldos de datos de alta velocidad
- Interconexión de alta velocidad del superordenador
- Transferencias de datos gráficas de las aplicaciones

Consideración del Rendimiento de la Red

El rendimiento del TCP sobre WAN (Internet) se ha estudiado en profundidad. Esta ecuación explica cómo el rendimiento de procesamiento de TCP tiene un límite superior basado encendido:

- El Maximum Segment Size (MSS), que es la longitud MTU menos la longitud de los encabezados TCP/IP
- El Round Trip Time (RTT)
- La pérdida de paquetes

Según esta fórmula, el rendimiento de procesamiento de TCP realizable máximo es directamente proporcional al MSS. Esto significa que, con el RTT constante y la pérdida del paquete, usted puede doblar el rendimiento de procesamiento de TCP si usted el tamaño de paquetes doble. Del mismo modo, cuando utiliza tramas jumbo en lugar de tramas 1518 byte, un aumento de seis veces el tamaño brinda una mejora potencial de seis veces en el rendimiento TCP de una conexión de Ethernet.

Información Operativa General

La especificación estándar de IEEE 802.3 define un tamaño de trama Ethernet máximo de **1518**. Las tramas 802.1Q-encapsulated, con una longitud entre de 1519 y 1522 bytes, fueron agregadas a la especificación 802.3 ulteriormente con el addendum de IEEE Std 802.3ac-1998. Se refieren a veces en la literatura como **gigantes del bebé**.

Los paquetes se clasifican generalmente como **tramas gigantes** cuando exceden el Largo máximo especificado de los Ethernetes para una conexión de Ethernet específica. Los paquetes Baby giant también se conocen como tramas Jumbo.

El punto principal de confusión sobre las Tramas gigantes es la configuración: diversas interfaces soportan diversos tamaños máximos de paquete y, tratan a veces los paquetes grandes en levemente las maneras diferentes.

Catalyst 6500 Series

Esta tabla intenta resumir las tallas del MTU que son soportadas actualmente por diversos indicadores luminosos LED amarillo de la placa muestra gravedad menor en la plataforma del Catalyst 6500:

Tarjeta de línea	Talla de la MTU
Predeterminado	9216 bytes
WS-X6248-RJ-45, WS-X6248A-RJ-45, WS-X6248-TEL, WS-X6248A-TEL, WS-X6348-RJ-45, WS-X6348-RJ45V, WS-X6348-RJ-21, y WX-X6348-RJ21V	8092 bytes (limitado por el chip PHY)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V), WS-X6148-45AF, y WS-X6148-21AF	9100 bytes (en el 100 Mbps) 9216 bytes (en el 10 Mbps)
WS-X6516-GE-TX	8092 bytes (en el 100 Mbps) 9216 bytes (en 10 o el 1000 Mbps)
WS-X6148(V)-GE-TX, WS-X6148-GE-45AF, WS-X6548(V)-GE-TX, y WS-X6548-GE-45AF	1500 bytes
OS ATM (OC12c)	9180 bytes
OS CHOC3, CHOC12, CHOC48, y CT3	9216 bytes (OCx y DS3) 7673 bytes (T1/E1)
FlexWAN	7673 bytes (CT3 T1/DS0) 9216 bytes (OC3c POS) 7673 bytes (T1)
WS-X6148-GE-TX, y WS-X6548-GE-TX	Ningún soporte

Refiera a configurar los Ethernetes, los fast ethernet, Gigabit Ethernet, y la transferencia de los Ethernet de 10 Gigabit para más información.

Soporte de Jumbo de la capa 2 y de la capa 3 en Cisco IOS Software del Catalyst 6500/6000

Hay soporte de Jumbo de la capa 2 y de la capa 3 con PFC/MSFC1, PFC/MSFC2, y el PFC2/MSFC2 en todos los puertos de GE que se configuren como interfaces físicas de la capa 2 y de la capa 3. Los soportes existen sin importar si estos puertos son enlace o canalización. Esta característica está disponible en el Cisco IOS Software Release 12.1.1E y Posterior.

- Las tallas del MTU de todos los puertos físicos enorme-habilitados se atan juntas. Un cambio en una de ellas cambia todos. Guardan siempre la misma talla del MTU de la trama Jumbo después de que se habiliten.
- Durante la configuración, habilite todos los puertos en el mismo VLA N según lo enorme-habilitado, o no habilite ninguno de él enorme-habilitada.
- La talla del MTU del Switched Virtual Interface (SVI) (interfaz VLAN) se fija por separado de los puertos físicos MTU. Un cambio en los puertos físicos MTU no cambia la talla del MTU SVI. También, un cambio en el SVI MTU no afecta a los puertos físicos MTU.
- El soporte de Trama Jumbo de la capa 2 y de la capa 3 en las interfaces FE comenzó en el Cisco IOS Software Release 12.1(8a) EX01. **El comando mtu 1500** inhabilita el jumbo en el FE, y los permisos del comando **MTU 9216** enormes en el FE. Refiera al Id. de bug Cisco CSCdv90450 (clientes registrados solamente).
- Las Tramas gigantes de la capa 3 en las interfaces VLAN se soportan solamente encendido:PFC/MSFC2 (Cisco IOS Software Release 12.1(7a)E y Posterior)PFC2/MSFC2 (Cisco IOS Software Release 12.1(8a)E4 y Posterior)
- No se recomienda para utilizar las Tramas gigantes con PFC/MSFC1 para las interfaces VLAN (SVI) porque el MSFC1 no puede posiblemente poder manejar la fragmentación según lo deseado.
- No se soporta ninguna fragmentación para los paquetes dentro del mismo VLA N (jumbo de la capa 2).
- Los paquetes que necesitan la fragmentación a través de los VLA N/de las subredes (jumbo de la capa 3) se envían al software para la fragmentación.

Entienda el soporte de Trama Jumbo en Cisco IOS Software del Catalyst 6500/6000

Una trama Jumbo es una trama que es más grande que el tamaño de trama Ethernet predeterminado. Para habilitar el soporte de Trama Jumbo, usted configura una talla del MTU del grande-que-valor por defecto en un puerto o la interfaz VLAN y, con el Cisco IOS Software Release 12.1(13)E y Posterior, configura la talla del MTU global del puerto LAN.

Cisco IOS Software interligado y del tráfico ruteado del tamaño del incorporar

Tarjeta de línea	Acceso	Egress
10, 10/100-, puertos del 100-Mbps	Se hace el control de la talla del MTU. El soporte de Trama Jumbo compara el tamaño del Tráfico de ingreso con la talla del MTU global del puerto LAN en el ingreso 10, 10/100-, y los Ethernetes del 100-Mbps y los puertos LAN 10-GE que tienen una talla del MTU del nondefault configurada. El puerto cae el tráfico que es de gran tamaño.	El control de la talla del MTU no se hace. Los puertos que se configuran con una talla del MTU del nondefault transmiten las tramas que contienen los paquetes de cualquier bytes más grande del tamaño de 64. Con una talla del MTU del nondefault configurada, 10, 10/100-, y los puertos del LAN Ethernet del 100-Mbps

		no marcan para saber si hay tramas de salida de gran tamaño.
Puertos de GE	El control de la talla del MTU no se hace. Los puertos que se configuran con una talla del MTU del nondefault validan las tramas que contienen los paquetes de cualquier tamaño más grande de 64 bytes y no marcan para saber si hay el ingreso de gran tamaño enmarcan.	Se hace el control de la talla del MTU. El soporte de Trama Jumbo compara el tamaño del tráfico de salida con la talla del MTU global del puerto LAN de la salida en los puertos LAN GE y 10-GE de la salida que tienen una talla del MTU del nondefault configurada. El puerto cae el tráfico que es de gran tamaño.
Puertos 10-GE	Se hace el control de la talla del MTU. El puerto cae el tráfico que es de gran tamaño.	Se hace el control de la talla del MTU. El puerto cae el tráfico que es de gran tamaño.
SVI	El control de la talla del MTU no se hace. El SVI no marca para saber si hay tamaño de trama en el lado del ingreso.	Se hace el control de la talla del MTU. La talla del MTU se comprueba el lado de la salida del SVI.
	PFC	
Todo el tráfico ruteado	Para el tráfico que debe ser ruteado, el soporte de Trama Jumbo en el PFC compara los tamaños del tráfico a las tallas del MTU configuradas y proporciona el Layer 3 Switching para el tráfico enorme entre las interfaces que se configuran con las tallas del MTU que son bastante grandes acomodar el tráfico. Entre las interfaces que no se configuran con grande-bastantes las tallas del MTU: • Si el bit del don't fragment (DF) no se fija, el PFC envía el tráfico al MSFC para ser hecho fragmentos y para ser ruteado en el software. • Si se fija el bit DF, el PFC cae el tráfico.	

Recomendaciones de Cisco

Si están implementadas correctamente, las Tramas gigantes pueden proporcionar una mejora multiplicada por seis potencial en el rendimiento de procesamiento de TCP de una conexión de Ethernet, con la tara de fragmentación reducida (más una tara de la CPU más baja en los dispositivos extremos).

Usted debe aseegurarse que no hay dispositivo entre eso no puede manejar la talla del MTU especificada. Si los fragmentos de este dispositivo y adelante los paquetes, él anulan todo el

proceso. Esto puede dar lugar a agregado por encima en este dispositivo para la fragmentación y volver a montar de los paquetes.

En estos casos, los remitentes de las ayudas del IP Path MTU Discovery para encontrar la Longitud del paquete común mínima que es conveniente transmitir el tráfico a lo largo de cada trayectoria. Alternativamente, usted puede configurar los dispositivos hostes trama-enterados del jumbo con una talla del MTU que sea el mínimo todos los que se soportan en la red.

Usted debe marcar cuidadosamente cada dispositivo para aseegurarse que puede soportar la talla del MTU. Vea la tabla del soporte de la talla del MTU en esta sección.

El soporte de Trama Jumbo se puede habilitar en estos tipos de interfaces:

- Interfaz del Canal de puerto
- SVI
- Interfaz física (capa 2/Layer 3)

Usted puede habilitar las Tramas gigantes en el Canal de puerto o las interfaces físicas que participan en el Canal de puerto. Es muy importante aseegurarse que el MTU en todas las interfaces físicas es lo mismo. Si no, una interfaz suspendida puede resultar. Usted necesita cambiar el MTU de una interfaz del Canal de puerto porque cambia el MTU de todos los puertos de miembro.

Nota: Si el MTU de un puerto de miembro no se puede cambiar al nuevo valor porque el puerto de miembro es el puerto de bloqueo, se suspende el Canal de puerto.

Aseegurese siempre que todas las interfaces físicas en un VLA N están configuradas para las Tramas gigantes antes de que usted configure el soporte de Trama Jumbo en un SVI. El MTU de un paquete no se comprueba el lado del ingreso de un SVI. Pero, se comprueba el lado de la salida de un SVI. Si el paquete MTU es más grande que la salida SVI MTU, el paquete es hecho fragmentos por el software (si el bit DF no se fija), que da lugar al rendimiento pobre. La fragmentación de software sucede solamente para el Layer 3 Switching. Cuando un paquete se remite a un puerto de la capa 3 o a un SVI con un MTU más pequeño, la fragmentación de software ocurre.

El MTU de una necesidad SVI siempre de ser más pequeño que el MTU más pequeño entre todos los puertos del switch en el VLA N.

Catalyst 4500 Series

Las Tramas gigantes se soportan principalmente en los puertos no bloqueando del linecards del Catalyst 4500. Estos puertos no bloqueando de GE tienen conexiones directas al Switching Fabric del Supervisor Engine y soportan las Tramas gigantes:

- Motores del supervisorWS-X4515, WS-X4516 — Dos puertos GBIC del uplink en el Supervisor Engine IV o VWS-X4516-10GE — Dos uplinks 10-GE y los cuatro uplinks enchufables del (SFP) del pequeño factor de forma 1-GEWS-X4013+ — Dos uplinks 1-GEWS-X4013+10GE — Dos uplinks 10-GE y los cuatro uplinks 1-GE SFPWS-X4013+TS — 20 puertos 1-GE
- LinecardsWS-X4306-GB — Módulo del acceso seises 1000BASE-X (GBIC) GEWS-X4506-GB-T — Acceso seises 10/100/1000-Mbps y SFP de seis puertosWS-X4302-GB — Módulo cuadripolo 1000BASE-X (GBIC) GELos primeros dos puertos GBIC de un servidor 18-port

que conmuta el módulo de GE (WS-X4418-GB) y puertos GBIC del módulo WS-X4232-GB-RJ
- Switches de configuración fijaWS-C4948 — Los 48 puertos 1-GEWS-C4948-10GE — Los 48 puertos 1-GE y dos puertos 10-GE

Usted puede utilizar estos puertos no bloqueando de GE para soportar las Tramas gigantes 9-KB o la supresión de broadcast del hardware (Supervisor Engine IV solamente). El resto del Baby Giant tramas del soporte del linecards. Usted puede utilizar los gigantes del bebé para el bridging del MPLS o para Q en el passthrough Q con un payload máximo de 1552 bytes.

Nota: Los aumentos del tamaño de trama con las etiquetas ISL/802.1Q.

Los gigantes y las Tramas gigantes del bebé son transparentes a otras características deL Cisco IOS con los motores IV y V. del supervisor.

Funciones de seguridad del Cisco IOS Software

Funciones de Seguridad Básicas

Al mismo tiempo, la Seguridad fue pasada por alto a menudo en los diseños para oficinas centrales. Pero, la Seguridad ahora es una parte esencial de cada red para empresas. Normalmente, el cliente ha establecido ya una política de seguridad para ayudar a definir qué herramientas y Tecnologías de Cisco son aplicables.

Protección de la contraseña básica

La mayoría de los dispositivos del Cisco IOS Software se configuran con dos niveles de contraseñas. El primer nivel está para el acceso de Telnet al dispositivo, que también se conoce como acceso del vty. Después de que se conceda el acceso del vty, usted necesita conseguir el acceso al enable mode o al modo EXEC privilegiado.

Asegure el enable mode del Switch

La contraseña habilitada permite que un usuario tenga el acceso completo a un dispositivo. Dé la contraseña habilitada solamente a la gente de confianza.

```
Switch(config)#enable secret password
```

Esté seguro que la contraseña obedece estas reglas:

- La contraseña debe contener entre una y 25 mayúsculos y los caracteres alfanuméricos minúsculos.
- La contraseña no debe tener un número como el primer carácter.
- Usted puede utilizar los espacios principales, pero se ignoran. Se reconocen el intermedio y los espacios finales.
- El control de contraseña es con diferenciación entre mayúsculas y minúsculas. Por ejemplo, la contraseña secreta es diferente que la contraseña secreta.

Nota: El comando enable secret utiliza una función de troceo criptográfica unidireccional de la publicación de mensaje 5 (MD5). Si usted publica el **comando show running-config**, usted puede ver esta contraseña encriptada. El uso del **comando enable password** es otra manera de fijar la contraseña habilitada. Pero, el algoritmo de encripción que se utiliza con el **comando enable**

password es débil y se puede invertir fácilmente para obtener la contraseña. Por lo tanto, no utilice el **comando enable password**. Utilice el comando enable secret para mayor seguridad: Refiera a los hechos de la encripción de contraseña del Cisco IOS para más información.

Asegure el acceso Telnet/VTY al Switch

Por abandono, el Cisco IOS Software apoya a cinco sesiones Telnet activas. Estas sesiones se refieren como vty 0 a 4. Usted puede habilitar estas líneas para el acceso. Pero para habilitar el login, usted también necesita el conjunto la contraseña para estas líneas.

```
Switch(config)#line vty 0 4 Switch(config-line)#login Switch(config-line)#password password
```

El comando login configura estas líneas para el acceso de Telnet. **El comando password** configura una contraseña. Esté seguro que la contraseña obedece estas reglas:

- El primer carácter no puede ser un número.
- La cadena puede contener cualquier carácter alfanumérico, hasta 80 caracteres. Los caracteres incluyen los espacios.
- Usted no puede especificar la contraseña en el número-espacio-carácter del formato. El espacio después del número causa los problemas. Por ejemplo, hola 21 es una contraseña legal, pero 21 hola no es una contraseña legal.
- El control de contraseña es con diferenciación entre mayúsculas y minúsculas. Por ejemplo, la contraseña secreta es diferente que la contraseña secreta.

Nota: Con esta configuración de línea del vty, el Switch salva la contraseña en el texto claro. Si alguien publica el **comando show running-config**, esta contraseña es visible. Para evitar esta situación, utilice el **comando service password-encryption**. El comando cifra libremente la contraseña. El comando cifra solamente la contraseña de línea del vty y la contraseña habilitada que se configura con el **comando enable password**. La contraseña habilitada que se configura con el **comando enable secret** utiliza un cifrado más fuerte. La configuración con el **comando enable secret** es el método recomendado.

Nota: Para tener más flexibilidad en Administración de seguridad, esté seguro que todos los dispositivos del Cisco IOS Software implementan el modelo de seguridad del Authentication, Authorization, and Accounting (AAA). AAA puede emplear bases de datos locales, RADIUS y TACACS+. Vea autenticación de TACACS+ la sección de configuración para más información.

Servicios de seguridad AAA

Descripción general del funcionamiento AAA

Controles del control de acceso que tiene permiso para acceder el Switch y qué servicios pueden utilizar estos usuarios. Los servicios de seguridad de la red AAA proporcionan el marco primario para configurar el control de acceso en su Switch.

Éstos seccionan describen los diversos aspectos del AAA detalladamente:

- Autenticación — Este proceso valida la identidad demandada de un usuario final o de un dispositivo. Primero, se especifican los diversos métodos que se pueden utilizar para autenticar al usuario. Estos métodos definen el tipo de autenticación para realizarse (por ejemplo, TACACS+ o RADIUS). La secuencia en la cual intentar estos métodos de autentificación también se define. Los métodos entonces se aplican a las interfaces

apropiadas, que activa la autenticación.
- Autorización — Este proceso concede los derechos de acceso a un usuario, los grupos de usuarios, el sistema, o un proceso. El proceso AAA puede realizar la autorización única o la autorización sobre una base de la por-tarea. El proceso define los atributos (en el servidor de AAA) en lo que tiene el usuario permiso para realizarse. Siempre que el usuario intente iniciar un servicio, el Switch pregunta al servidor de AAA y pide el permiso para autorizar al usuario. Si el servidor de AAA aprueba, autorizan al usuario. Si el servidor de AAA no aprueba, el usuario no consigue el permiso para ejecutar ese servicio. Usted puede utilizar este de proceso para especificar que algunos usuarios pueden ejecutar solamente ciertos comandos.
- El considerar — Este proceso le permite para seguir los servicios que acceso de usuarios y la cantidad de recursos de red que los usuarios consumen. Cuando se habilita el considerar, el Switch señala la actividad del usuario al servidor de AAA bajo la forma de registros de contabilidad. Los ejemplos de actividad del usuario que está señalado incluyen el tiempo de la sesión y la hora de inicio y de detención. Entonces, el análisis de esta actividad puede ocurrir para la Administración o los fines de facturación.

Aunque el AAA sea el primario y el método recomendado para el control de acceso, el Cisco IOS Software proporciona las características adicionales para el control de acceso simple que están fuera del ámbito de AAA. Estas características adicionales incluyen:

- Autenticación del nombre de usuario local
- Autenticación de contraseña de línea
- Autenticación de contraseña habilitada

Pero estas características no proporcionan el mismo grado de control de acceso que sea posible con el AAA.

Para entender mejor el AAA, refiera a estos documentos:

- Autenticación, autorización y administración (AAA)
- Configuración de AAA básico en un servidor de acceso
- Comparación de TACACS+ y RADIUS

Estos documentos no mencionan necesariamente el Switches. Pero los conceptos de AAA que los documentos describen son aplicables al Switches.

TACACS+

Propósito

Por abandono, nonprivileged y las contraseñas de modo de privilegio sea global. Estas contraseñas se aplican a cada usuario que acceda el Switch o al router, del puerto de la consola o vía una sesión telnet a través de la red. La implementación de estas contraseñas en los dispositivos de red es larga y noncentralized. También, usted puede tener dificultad con la implementación de las restricciones de acceso con el uso del Listas de control de acceso (ACL) que puede ser Errores de configuración propensos. Para superar estos problemas, tome un acercamiento centralizado cuando usted configura los nombres de usuario, las contraseñas, y el acceso limpia en un servidor central. Este servidor puede ser el Cisco Secure Access Control Server (ACS) o cualquier servidor de tercera persona. Los dispositivos se configuran para utilizar estas bases de datos centralizadas para las funciones AAA. En este caso, los dispositivos son Switches del Cisco IOS Software. El protocolo que se utiliza entre los dispositivos y el servidor central puede ser:

- TACACS+
- RADIUS
- Kerberos

El TACACS+ es una instalación común en las redes de Cisco y es el foco de esta sección. El TACACS+ proporciona estas características:

- Autenticación — El proceso que identifica y verifica a un usuario. Varios métodos se pueden utilizar para autenticar a un usuario. Pero la mayoría del método usual incluye una combinación de nombre de usuario y contraseña.
- Autorización — Cuando el usuario intenta ejecutar un comando, el Switch puede marcar con el servidor TACACS+ para determinar si conceden el usuario el permiso para utilizar ese comando determinado.
- El considerar — Este proceso registra lo que hace un usuario o ha hecho en el dispositivo.

Refiera a la Comparación entre TACACS+ y RADIUS para una comparación entre el TACACS+ y el RADIUS.

Información Operativa General

TACACS+ del protocolo los nombres de usuario y contraseña adelante al servidor centralizado. La información se cifra sobre la red con el picado unidireccional MD5. Refiera al RFC 1321 para más información. El TACACS+ utiliza el puerto TCP 49 como el Transport Protocol, que ofrece estas ventajas sobre el UDP:

Nota: El RADIUS utiliza el UDP.

- Transporte orientado por conexión
- Separe el acuse de recibo que se ha recibido una petición ([ACK] del acuse de recibo TCP), sin importar cómo está cargado el mecanismo de autenticación final es
- Indicación inmediata de una caída del servidor (paquetes del [RST] de la restauración)

Durante una sesión, si la comprobación de autorización adicional es necesaria, el Switch marca con el TACACS+ para determinar si conceden el usuario el permiso para utilizar un comando determinado. Este paso proporciona el mayor control sobre los comandos que se pueden ejecutar en el Switch y proporciona el desemparejamiento del mecanismo de autenticación. Con el uso de las estadísticas del comando, usted puede auditoría los comandos que un usuario determinado ha publicado mientras que asocian al usuario a un dispositivo de red determinado.

Este diagrama muestra el proceso de la autorización que está implicado:

Cuando un usuario autentica a un dispositivo de red con el uso del TACACS+ en una tentativa del acceso ASCII simple al sistema, este proceso ocurre típicamente:

- Cuando se establece la conexión, el Switch entra en contacto la daemon TACACS+ para obtener un prompt de nombre de usuario. El Switch entonces visualiza el prompt para el usuario. El usuario ingresa un nombre de usuario, y el switch entra en contacto con el daemon de TACACS+ para obtener una indicación de contraseña. El Switch visualiza el prompt de contraseña para el usuario, que ingresa una contraseña que también se envíe al daemon TACACS+.
- El dispositivo de red recibe finalmente una de estas respuestas del daemon de TACACS+:`VALIDE` — Autentican al usuario y el servicio puede comenzar. Si el dispositivo de

red se configura para requerir la autorización, la autorización comienza en este momento.RECHAZO — El usuario no ha podido autenticar. El usuario es acceso posterior negado o indicado para revisar la secuencia de inicio de sesión. El resultado depende de la daemon TACACS+.ERROR — Un error ocurrió en algún momento durante la autenticación. El error puede estar en la daemon o en la conexión de red entre la daemon y el Switch. Si se recibe una `respuesta de error`, el dispositivo de red intenta típicamente utilizar un método alternativo para autenticar al usuario.CONTINÚE — Indican al usuario para la información de autenticación adicional.

- Los usuarios deben primero completar con éxito la autenticación de TACACS+ antes de pasar a la autorización de TACACS+.
- Si autorización TACACS+ se requiere, la daemon TACACS+ se entra en contacto otra vez. La daemon TACACS+ devuelve una respuesta de autorización del VALIDAR o del RECHAZO. Si se devuelve una `respuesta ACCEPT`, la respuesta contiene los datos bajo la forma de atributos que se utilicen para dirigir el EXEC o a la `sesión de red` para ese usuario. El determina que ordena al usuario puede acceder.

Pasos básicos de la configuración AAA

La configuración del AAA es relativamente simple después de que usted entienda el proceso básico. Para configurar la Seguridad en un router Cisco o un servidor de acceso con el uso del AAA, realice estos pasos:

1. Para habilitar el AAA, publique el comando global configuration **de modelo nuevo aaa**.`Switch(config)#aaa new-model` **Consejo:** Salve su configuración antes de que usted configure sus comandos aaa. Salve la configuración otra vez solamente después que usted ha completado todas sus configuraciones AAA y se satisface que la configuración trabaja correctamente. Entonces, usted puede recargar el Switch para recuperarse de los bloqueos imprevistos (antes de que usted salva la configuración), en caso necesario.
2. Si usted decide utilizar un servidor de seguridad separado, los parámetros del Security Protocol de la configuración tales como RADIUS, el TACACS+, o el Kerberos.
3. Utilice el **comando aaa authentication** para definir las listas de métodos para la autenticación.
4. Utilice el **comando login authentication** para aplicar las listas de métodos a una interfaz particular o a una línea.
5. Publique el **comando aaa authorization** opcional para configurar la autorización.
6. Publique el **comando aaa accounting** opcional para configurar las estadísticas.
7. Configure al servidor externo AAA para procesar las peticiones de la autenticación y autorización del Switch.**Nota:** Refiera a su documentación del servidor de AAA para más información.

Autenticación de TACACS+ configuración

Realice estos pasos para configurar autenticación de TACACS+:

1. Publique el **comando aaa new-model** en el modo de configuración global para habilitar el AAA en el Switch.
2. Defina el servidor TACACS+ y la clave asociada.Esta clave se utiliza para cifrar el tráfico entre el servidor TACACS+ y el Switch. En el comando del **mysecretkey de la clave de**

1.1.1.1 del host del TACACS-servidor, el servidor TACACS+ está en la dirección IP 1.1.1.1, y la clave de encripción es mysecretkey. Para verificar que el Switch pueda alcanzar el servidor TACACS+, inicie un ping del Internet Control Message Protocol (ICMP) del Switch.

3. Defina una lista de métodos.Una lista de métodos define la secuencia de mecanismos de autenticación para intentar para los diversos servicios. Los diversos servicios pueden ser, por ejemplo:HabilitarLogin (para el vty/el acceso de Telnet)**Nota:** Vea la sección de las funciones de seguridad básica de este documento para la información sobre el vty/el acceso de Telnet.ConsolaEste ejemplo considera el **login** solamente. Usted debe aplicar la lista de métodos a las interfaces/línea:`Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line Switch(config)#line vty 0 4 Switch(config-line)#login authentication METHOD-LIST-LOGIN Switch(config-line)#password hard_to_guess` En esta configuración, el **comando aaa authentication login** utiliza el nombre de la lista construido METHOD-LIST-LOGIN y utiliza el método tacacs+ antes de que utilice la línea del método. Autentican a los usuarios con el uso del servidor TACACS+ como el primer método. Si el servidor TACACS+ no responde ni envía un mensaje de error, la contraseña que se configura en la línea se utiliza como el segundo método. Pero si el servidor TACACS+ niega al usuario y responde con un mensaje del RECHAZO, el AAA considera la transacción acertada y no utiliza el segundo método.**Nota:** La configuración no es completa hasta que usted aplique la lista (METHOD-LIST-LOGIN) a la línea del vty. Publique el comando de la **autenticación de inicio de sesión METHOD-LIST-LOGIN** en el modo de configuración de línea, como el ejemplo muestra.**Nota:** El ejemplo crea una entrada posterior para cuando el servidor TACACS+ es inasequible. Los administradores de seguridad pueden o no pueden validar posiblemente la implementación de una entrada posterior. Esté seguro que la decisión para implementar tales entradas posteriores cumple con las políticas de seguridad del sitio.

Configuración de la autenticación de RADIUS

La configuración de RADIUS es casi idéntica a la configuración TACACS+. Substituya simplemente la palabra RADIUS para el TACACS en la configuración. Esto es una configuración de RADIUS de la muestra para el acceso del puerto COM:

```
Switch(config)#aaa new-model Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line Switch(config)#line
con 0 Switch(config-line)#login authentication METHOD-LIST-LOGIN Switch(config-line)#password
hard_to_guess
```

Banners de Login

Cree los anuncios de dispositivo apropiados que estado específicamente medidas que se toman en el acceso no autorizado. No haga publicidad del nombre del sitio o de la información de red a los usuarios no autorizados. Los banners proporcionan el recurso en caso de que se comprometa un dispositivo y cogen al autor. Publique este comando para crear los anuncios de inicio de sesión:

```
Switch(config)#banner motd ^C *** Unauthorized Access Prohibited *** ^C
```

Seguridad Física

Esté seguro que la autorización apropiada es para físicamente dispositivos de acceso necesarios. Mantenga el equipo un espacio (bloqueado) controlado. Para asegurarse de que la red permanezca operativa e inafectada por tratar de forzar o los factores del entorno malévolos, esté seguro que todo el equipo tiene:

- Un (UPS) apropiado de la fuente de alimentación ininterrumpible, con las fuentes redundantes en lo posible
- Control de temperatura (aire acondicionado)

Recuerde que, si una persona con el intento malicioso viola el acceso físico, la interrupción vía la recuperación de contraseña o los otros medios es mucho más probable.

Configuración de la Administración

Diagramas de la Red

Propósito

Los diagramas de redes limpios son fundamentales en el funcionamiento de las redes. Los diagramas llegan a ser críticos durante el troubleshooting, y son el solo vehículo más importante para la comunicación de información durante la escalada a los vendedores y Partners durante una caída del sistema. No subestime la preparación, la disposición, y la accesibilidad que los diagramas de la red proporcionan.

Recomendación

Estos tres tipos de diagramas son necesarios:

- **Diagrama total** — Incluso para las redes más grandes, un diagrama que muestra la comprobación de punta a punta o la conectividad lógica es importante. A menudo, empresas que han implementado un documento del diseño jerárquico cada capa por separado. Cuando usted planea y el problema soluciona, un buen conocimiento de cómo los dominios conectan juntos es qué importa.
- **Diagrama físico** — Este diagrama muestra todo el Switch y hardware de router y cableado. Esté seguro que el diagrama etiqueta cada uno de estos aspectos:TrunksLinksVelocidadesGrupos de canalNúmeros de puertoRanurasTipos del chasisSoftwareDominios VTPRoot BridgePrioridad de Root Bridge de BackupDirección MACPuertos bloqueados por el VLA NPara una mejor claridad, represente los dispositivos internos tales como el router MSFC del Catalyst 6500/6000 como router en un palillo que esté conectado vía un trunk.
- **Diagrama lógico** — Este diagrama muestra solamente las funciones de la capa 3, así que significa que muestra el Routers como objetos y los VLA N como segmentos Ethernet. Esté seguro que el diagrama etiqueta estos aspectos:IP AddressesSubredesDireccionamiento secundarioHSRP activo y esperaCapas de la memoria-distribución del accesoInformación de ruteo

Interfaz y VLAN nativo del administrador de switches

Propósito

Esta sección describe la significación y los problemas potenciales del uso del VLAN predeterminado 1. Esta sección también cubre los problemas potenciales cuando usted ejecuta el tráfico de administración al Switch en el mismo VLA N que el tráfico de usuarios en el Switches de

las 6500/6000 Series.

Los procesadores en los motores del supervisor y los MSFC para la serie del Catalyst 6500/6000 utilizan el VLAN1 para varios protocolos del control y de la Administración. Los ejemplos incluyen:

- Protocolos del control del Switch:STP BPDUVTPDTPCDP
- Protocolos de la Administración:SNMPTelnetProtocolo secure shell (SSH)Syslog

Cuando el VLA N se utiliza de esta manera, se refiere como el VLAN nativo. La configuración del switch predeterminado fija el VLAN1 como el VLAN nativo predeterminado en los puertos troncales del Catalyst. Usted puede dejar el VLAN1 como el VLAN nativo. Pero tenga presente que cualquier Switches que funcione con el software del sistema del Cisco IOS en su red fija todas las interfaces que se configuren como puertos del 2 Switch de la capa a los puertos de acceso en el VLAN1 por abandono. Muy probablemente, un Switch en alguna parte en el VLAN1 de los usos de la red como VLA N para el tráfico de usuarios.

La preocupación principal con el uso del VLAN1 es ésa, el Supervisor Engine NMP no necesita generalmente ser interrumpido por mucho del broadcast y del tráfico Multicast que las estaciones terminales generan. Las aplicaciones de multidifusión particularmente tienden a enviar muchos datos entre los servidores y los clientes. El Supervisor Engine no necesita ver estos datos. Si los recursos o los buffers del Supervisor Engine se ocupan completamente mientras que el Supervisor Engine escucha el tráfico innecesario, el Supervisor Engine puede no poder ver los paquetes de administración que pueden causar un Spanning-Tree Loop o una falla de EtherChannel (en el peor de los casos escenario).

Los contadores del /port del *slot del interface_type de las* interfaces de la demostración ordenan y el comando show ip traffic puede darle una cierta indicación de:

- La proporción de broadcast al tráfico de unidifusión
- La proporción de IP al tráfico no IP (que no se ve típicamente en los VLAN de administraciones)

El VLAN1 marca y maneja la mayor parte del tráfico del plano del control con etiqueta. La VLAN1 se habilita en todos los trunks de forma predeterminada. Con redes de oficinas centrales más grandes, usted necesita tener cuidado del diámetro del dominio STP del VLAN1. La inestabilidad en una parte de la red puede afectar al VLAN1 y puede influenciar la estabilidad y la estabilidad del STP planas del control para el resto de los VLA N. Usted puede limitar la transmisión del VLAN1 de los datos del usuario y la operación del STP en una interfaz. No configure simplemente el VLA N en la interfaz de tronco.

Esta configuración no para la transmisión de los paquetes de control del Switch para conmutar en el VLAN1, como con un analizador de red. Pero no se remite ningunos datos, y el STP no se ejecuta sobre este link. Por lo tanto, usted puede utilizar esta técnica para romper para arriba el VLAN1 en dominios de falla más pequeños.

Nota: Usted no puede VLAN1 claro de los trunks al Catalyst 2900XL/3500XLs.

Incluso si usted tiene cuidado de obligar los VLAN de usuarios relativamente a los dominios del switch pequeño y correspondientemente al pequeño error/a la capa 3 de los límites, todavía tientan a algunos clientes para tratar el VLAN de administración diferentemente. Estos clientes intentan cubrir la red completa con una sola subred de administración. No hay motivo técnico que una aplicación NMS central debe ser la capa 2-adjacent a los dispositivos que la aplicación maneja, ni está ésta un argumento de seguridad calificado. Limite el diámetro de los VLAN de administraciones a la misma estructura de dominio ruteada que el de los VLAN de usuarios.

Considere la administración fuera de banda y/o el soporte de SSH como manera de aumentar la Seguridad de la Administración de redes.

Otras Opciones

Hay aspectos del diseño para estas Recomendaciones de Cisco en algunas topologías. Por ejemplo, un deseable y un común diseño multicapa de Cisco es uno que evita el uso de un active que atraviesa - árbol. De esta manera, el diseño pide el obstáculo de cada IP subnet/VLAN a un solo switch de capa de acceso (o al cluster del Switches). En estos diseños, ningún enlace se puede configurar abajo a la capa de acceso.

¿Usted crea un enlace del VLAN de administración aparte y del permiso para llevarlo entre el acceso de la capa 2 y acodar 3 capas de distribución? No hay respuesta fácil a esta pregunta. Considere estas dos opciones para la revisión del diseño con su ingeniero de Cisco:

- **Opción 1** — VLA N únicos del trunk dos o tres de la capa de distribución abajo a cada switch de capa de acceso. Esta configuración permite un VLAN de dato, un VLA N de la Voz, y un VLAN de administración, y todavía tiene la ventaja que el STP está inactivo. Un paso de la configuración extra es necesario para borrar el VLAN1 de los trunks. En esta solución, hay también puntas del diseño a considerar para evitar temporalmente el tráfico ruteado del envío a agujeros negros durante la recuperación de errores. Utilice el STP portfast para los trunks (en el futuro) o la sincronización Autostate del VLA N con el reenvío STP.
- **Opción 2** — Un solo VLA N para los datos y la Administración puede ser aceptable. Si usted quiere guardar la interfaz del sc0 a parte de los datos del usuario, un hardware más nuevo del Switch hace este escenario menos de un problema que estaba una vez. El hardware más nuevo proporciona:CPU más potentes y controles de la limitación de la tarifa de la controle de planoUn diseño con los dominios de broadcast relativamente pequeños según lo abogado por el diseño multicapaPara tomar una decisión final, examinar el perfil del tráfico broadcast para el VLA N y discutir las capacidades del hardware del Switch con su ingeniero de Cisco. Si el VLAN de administración contiene a todos los usuarios en ese switch de capa de acceso, utilice los filtros de entrada IP para asegurar el Switch de los usuarios, según la sección de las funciones de seguridad del Cisco IOS Software.

Interfaz de administración de Cisco y recomendación del VLAN nativo

Interfaz de administración

El software del sistema del Cisco IOS le da la opción para configurar las interfaces como interfaces de la capa 3 o como puertos del 2 Switch de la capa en un VLA N. Cuando usted utiliza el **comando switchport** en Cisco IOS Software, todos los puertos del switch son puertos de acceso en el VLAN1 por abandono. Así pues, a menos que usted configure de otra manera, los datos del usuario pueden también existir posiblemente por abandono en el VLAN1.

Haga que el VLAN de administración un VLA N con excepción del VLA N 1. guarda todo el VLAN de administración de los de los datos del usuario. En lugar, configure una interfaz del loopback0 como la interfaz de administración en cada Switch.

Nota: Si usted utiliza el protocolo OSPF, éste también hace el router para OSPF ID.

Esté seguro que el Loopback Interface tiene una máscara de subred de 32 bits, y configura el

Loopback Interface como interfaz pura de la capa 3 en el Switch. Aquí tiene un ejemplo:

```
Switch(config)#interface loopback 0 Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end Switch#
```

VLAN nativa

Configure el VLAN nativo para ser un VLA N de la falsa evidente que nunca se habilita en el router. Cisco recomendó el VLA N 999 en el pasado, pero la opción es puramente arbitraria.

Publique estos comandos interface para establecer un VLA N como el natural (valor por defecto) para el enlace del 802.1Q en un puerto determinado:

```
Switch(config)#interface type slot/port Switch(config-if)#switchport trunk native vlan 999
```

Para las recomendaciones adicionales de la configuración de conexión de troncal, vea la sección del protocolo dynamic trunking de este documento.

Administración Fuera de Banda

Propósito

Usted puede hacer la Administración de redes más altamente disponible si usted construye una infraestructura de administración aparte alrededor de la red de producción. Esta configuración permite a los dispositivos para ser accesible remotamente, a pesar del tráfico se conduce que o los eventos de la controle de plano que ocurren. Estos dos enfoques son típicos:

- Administración fuera de banda con un LAN exclusivo
- Administración fuera de banda con los servidores terminales

Información Operativa General

Usted puede proporcionar cada router y Switch en la red con una interfaz de administración de Ethernet fuera de banda en un VLAN de administración. Usted configura un acceso de Ethernet en cada dispositivo en el VLAN de administración y lo telegrafía fuera de la red de producción a un Switched Management Network distinto.

Nota: El Switches del Catalyst 4500/4000 tiene una interfaz especial del me1 en el Supervisor Engine que deba ser utilizada para la administración fuera de banda solamente y no como puerto del switch.

Además, usted puede alcanzar la conectividad del servidor terminal si usted configura a un Cisco 2600 o 3600 Router con los cables seriales RJ-45 para acceder el puerto de la consola de cada router y Switch en la disposición. El uso de un servidor terminal también evita la necesidad de configurar los escenarios de backup, tales como módems en los puertos auxiliares para cada dispositivo. Usted puede configurar un solo módem en el puerto auxiliar del servidor terminal. Esta configuración proporciona el servicio de dial up a los otros dispositivos durante una falla de conectividad de red. Refiera a conectar un módem con el puerto de la consola en los switches de Catalyst para más información.

Recomendación

Con este arreglo, dos trayectos fuera de banda a cada Switch y el router son posibles, además de

los trayectos dentro de la banda numerosos. El arreglo habilita la Administración de redes altamente disponible. Las ventajas son:

- El arreglo separa el tráfico de administración de los datos del usuario.
- El IP Address de administración está en una subred distinta, un VLA N, y un Switch para la Seguridad.
- Hay garantía más alta para la entrega de datos de administración durante los desperfectos de la red.
- Hay el atravesar no activo - árbol en el VLAN de administración. La Redundancia aquí no es crítica.

Este diagrama muestra la administración fuera de banda:

Registro del Sistema

Propósito

Los mensajes de Syslog son Cisco específico y pueden dar más responsivo y la información precisa que el SNMP estandardizado. Por ejemplo, las plataformas de administración tales como Fundamentos del Resource Manager de Cisco (RME) y herramientas de análisis de red (NATKit) hacen el uso potente de la Información de syslog para recoger el inventario y los cambios de configuración.

Recomendación de la configuración de syslog de Cisco

El Registro del sistema es un campo común y una práctica operativa validada. Un registro del sistema UNIX puede capturar y analizar la información/los eventos en el router por ejemplo:

- Estatus de la interfaz
- Alertas de seguridad
- Condiciones del medio ambiente
- Proceso de la CPU cerdo
- Otros eventos

El Cisco IOS Software puede hacer UNIX que registra a un servidor Syslog UNIX. El formato del registro del sistema UNIX de Cisco es compatible con 4.3 Berkeley Standard Distribution (BSD) UNIX. Utilice estas configuraciones de registro del Cisco IOS Software:

- **ninguna consola de registro** — Por abandono, todos los mensajes del sistema se envían a la consola del sistema. El registro de la consola es una tarea prioritaria en Cisco IOS Software. Esta función fue diseñada sobre todo para proporcionar los mensajes de error al operador del sistema antes de una falla del sistema. Inhabilite la consola que abre una sesión todas las configuraciones del dispositivo para evitar una situación en la cual el router/el Switch pueda colgar mientras que el dispositivo espera una respuesta de una terminal. Pero los mensajes de la consola pueden ser útiles durante la identificación del problema. En estos casos, registro de la consola del permiso. Publique el **comando logging console level** para obtener el nivel deseado de registro de mensaje. Los niveles de registro son a partir la 0 a 7.
- **no logging monitor** — Este comando inhabilita el registro para los línea de la terminal con excepción de la consola del sistema. El registro de monitoreo puede ser requerido (con el uso del **logging monitor debugging** o de otro comando option). En este caso, registro de monitoreo

del permiso en el nivel de registro específico que es necesario para la actividad. No vea el **ningún** elemento de la **consola de registro** en esta lista para más información sobre los niveles de registro.

- **el registro mitigó 16384** — **El comando logging buffered** necesita ser agregado para registrar los mensajes del sistema en el búfer del registro interno. Memoria intermedia de registro es circular. Una vez que se llena memoria intermedia de registro, más viejas entradas son sobregrabadas por más nuevas entradas. El tamaño de memoria intermedia de registro es utilizador configurable y se especifica en los bytes. El tamaño del búfer del sistema varía por la plataforma. 16384 es un buen valor por defecto que proporciona adecuado abriendo una sesión la mayoría de los casos.
- **notificaciones de la trampa de registro** — Este comando proporciona la Mensajería del nivel de notificación (5) al servidor de Syslog especificado. El nivel de registro predeterminado para todos los dispositivos (consola, monitor, buffer, y desvíos) está haciendo el debug de (el nivel 7). Si usted deja el nivel de registro del desvío en 7, se presentan muchos mensajes extraños que son de poco o nada de interés a la salud de la red. Fije el nivel de registro predeterminado para los desvíos a 5.
- **local7 de la instalación de explotación forestal** — Este comandos estableces la instalación de explotación forestal/el nivel predeterminados para el syslogging de UNIX. Configure al servidor de Syslog que recibe estos mensajes para el mismo recurso/nivel.
- **host de registro** — Este comandos estableces la dirección IP del servidor de registro de UNIX.
- **logging source-interface loopback0** — Este comandos estableces IP predeterminado SA para los mensajes de Syslog. Código duro el SA de registración para hacer la identificación del host que envió el mensaje más fácil.
- **demostración-timezone milisegundo del localtime del service timestamps debug datetime** — Por abandono, los mensajes del registro no son con impresión horaria. Usted puede utilizar este comando de habilitar timestamping de los mensajes del registro y timestamping de la configuración 6system debug (Depuración del sistema) de los mensajes. Timestamping proporciona la sincronización relativa de los eventos registrados y aumenta el debugging en tiempo real. Esta información es especialmente útil cuando los clientes envían la salida de debbuging a su personal de soporte técnico para la ayuda. Para habilitar timestamping 6system debug (Depuración del sistema) de los mensajes, utilice el comando en el modo de configuración global. El comando tiene solamente un efecto cuando se habilita el hacer el debug de.

Nota: Además, registro del permiso para el estado de link y estatus del conjunto en todas las interfaces Gigabit de la infraestructura.

El Cisco IOS Software proporciona un solo mecanismo para fijar el recurso y el registro llanos para todos los mensajes del sistema que se destinen a un servidor de Syslog. Fije el nivel de trampa de registro a la notificación (nivel 5). Si usted fija el nivel de mensaje trampa a la notificación, usted puede minimizar el número de mensajes de información que se remitan al servidor de Syslog. Esta configuración puede reducir perceptiblemente la cantidad de tráfico del Syslog en la red y puede aminorar el impacto en los recursos del servidor de Syslog.

Agregue estos comandos a cada router y Switch que funcionen con el Cisco IOS Software para habilitar la mensajería de syslog:

- Comandos de configuración de syslog globales:
  no logging console no logging monitor logging buffered 16384 logging trap notifications

```
logging facility local7 logging host-ip logging source-interface loopback 0 service
timestamps debug datetime localtime show-timezone msec service timestamps log datetime
localtime show-timezone msec
```

- Comandos de configuración de syslog de la interfaz:
```
logging event link-status logging event bundle-status
```

SNMP

Propósito

Usted puede utilizar el SNMP para extraer las estadísticas, los contadores, y las tablas que se salvan en el MIB del dispositivo de red. Los NMS tales como HP OpenView pueden utilizar la información para:

- Genere las alertas en tiempo real
- Mida la Disponibilidad
- Presente la información sobre planificación de capacidad
- Ayude a realizar las verificaciones de configuración y de Troubleshooting

Operación de la interfaz de la administración de SNMP

El SNMP es un protocolo de la capa de aplicación que proporciona un formato de mensaje para la comunicación entre los administradores y agentes de SNMP. El SNMP proporciona un marco estandardizado y un idioma común para el monitor y la administración de dispositivos en una red.

Framework SNMP consiste en estas tres piezas:

- Un SNMP Manager
- Un agente SNMP
- UN MIB

El SNMP Manager es el sistema que utiliza el SNMP para controlar y monitorear las actividades de los Host de red. La mayoría del sistema de administración común se llama un NMS. Usted puede aplicar el término NMS a cualquier un dispositivo dedicado que se utilice para la Administración de redes o las aplicaciones que se utilizan en tal dispositivo. Una variedad de aplicaciones de administración de red están disponibles para el uso con el SNMP. Estas aplicaciones se extienden de las aplicaciones CLI simples a los ricos de la característica GUI tales como la línea de productos de los CiscoWorks.

El agente SNMP es el componente del software dentro del dispositivo administrado que mantiene los datos para el dispositivo y señala estos datos, cuanto sea necesario, manejo de los sistemas. El agente y el MIB residen en el dispositivo de ruteo (el router, el servidor de acceso, o el Switch). Para habilitar el agente SNMP en un dispositivo de ruteo de Cisco, usted debe definir la relación entre el administrador y el agente.

El MIB es una área de almacenamiento de información virtual para la información de administración de red. El MIB consiste en las colecciones de objetos administrados. Dentro del MIB, hay colecciones de objetos relacionados que se definan en los módulos MIB. Los módulos MIB se escriben en el lenguaje del módulo del SNMP MIB, como STD 58, RFC 2578 , RFC 2579 , y el RFC 2580 define.

Nota: Los módulos de MIB individuales también se refieren como MIB. Por ejemplo, el grupo MIB

(IF-MIB) de las interfaces es un módulo MIB dentro del MIB en su sistema.

El agente SNMP contiene las variables MIB, los valores cuyo el SNMP Manager puede pedir o cambiar consiga a través o las operaciones determinadas. Un administrador puede conseguir un valor de un agente o salvar un valor en ese agente. El agente recopila los datos del MIB, que es el repositorio para la información sobre los parámetros del dispositivo y los datos de red. El agente puede también responder a las peticiones del administrador de conseguir o de fijar los datos.

Un administrador puede enviar las peticiones del agente de conseguir y de fijar los valores MIB. El agente puede responder a estas peticiones. La independiente de esta interacción, el agente puede enviar las notificaciones no solicitadas (los desvíos o informan) al administrador para notificar al administrador de los estados de la red. Con algunos mecanismos de seguridad, un NMS puede extraer la información en el MIB con `consigue` y `consigue las` peticiones `siguientes`, y puede publicar el **comando set** para cambiar los parámetros. Además, usted puede configurar un dispositivo de red para generar un mensaje trampa al NMS para las alertas en tiempo real. El puerto 161 y 162 del IP UDP se utiliza para los desvíos.

Descripción general del funcionamiento de las notificaciones SNMP

Una característica fundamental del SNMP es la capacidad de generar las notificaciones de un agente SNMP. Estas notificaciones no requieren las peticiones de ser enviado del SNMP Manager. Las notificaciones (asíncronas) no solicitadas pueden ser generadas como desvíos o informar a las peticiones. Los desvíos son los mensajes que alertan al SNMP Manager a una condición en la red. Informe a las peticiones (informa) son los desvíos que incluyen un pedido la confirmación del recibo del SNMP Manager. Las notificaciones pueden indicar los eventos importantes por ejemplo:

- Autenticación de usuario impropia
- Reinicios
- El cierre de una conexión
- La pérdida de conexión a un router vecino
- Otros eventos

Los desvíos son menos confiables que informan porque el receptor no envía ningún acuse de recibo cuando el receptor recibe un desvío. El remitente no puede determinar si el desvío fue recibido. Un SNMP Manager que recibe una petición de la información reconoce el mensaje con un unidad de datos del protocolo (PDU) de la respuesta SNMP. Si el administrador no recibe una petición de la información, el administrador no envía una respuesta. Si el remitente nunca recibe una respuesta, el remitente puede enviar la petición de la información otra vez. Informs es más probable alcanzar el destino deseado.

Pero los desvíos se prefieren a menudo porque informa consumen más recursos en el router y en la red. Se desecha un desvío tan pronto como se envíe. Pero una petición de la información se debe llevar a cabo en la memoria hasta que se reciba una respuesta o los tiempos de la petición hacia fuera. También, los desvíos se envían solamente una vez, mientras que una información se puede revisar varias veces. Los reintentos incrementan el tráfico y contribuyen a una sobrecarga mayor en la red. Así, los desvíos e informan a las peticiones proporcionan un equilibrio entre la confiabilidad y los recursos. Si usted necesita al SNMP Manager recibir cada notificación, el uso informa a las peticiones. Pero si usted tiene preocupaciones por el tráfico en su red o la memoria en el router y usted no necesita recibir cada notificación, utilice los desvíos.

Estos diagramas ilustran las diferencias entre los desvíos e informan a las peticiones:

Este diagrama ilustra cómo el router del agente envía con éxito un desvío al SNMP Manager. Aunque el administrador reciba el desvío, el administrador no envía ningún acuse de recibo al agente. El agente no tiene ninguna manera de saber que el desvío alcanzó el destino.

Este diagrama ilustra cómo el router del agente envía con éxito una petición de la información al administrador. Cuando el administrador recibe la petición de la información, el administrador envía una respuesta al agente. De esta manera, el agente sabe que la petición de la información alcanzó el destino. Note que, en este ejemplo, hay dos veces mìas tráfico. Pero el agente sabe que el administrador recibió la notificación.

En este diagrama, el agente envía un desvío al administrador, pero el desvío no alcanza al administrador. El agente no tiene ninguna manera de saber que el desvío no alcanzó el destino, y así que el desvío no se envía otra vez. El administrador nunca recibe el desvío.

En este diagrama, el agente envía una petición de la información al administrador, pero la petición de la información no alcanza al administrador. Porque el administrador no recibió la petición de la información, no hay respuesta. Después de un período de tiempo, el agente vuelve a enviar la petición de la información. La segunda vez que, el administrador recibe la petición de la información y contesta con una respuesta. En este ejemplo, hay más tráfico. Pero la notificación alcanza al SNMP Manager.

MIB de Cisco y referencia RFC

Los documentos RFC definen típicamente los módulos MIB. Los documentos RFC se presentan a la Fuerza de tareas de ingeniería en Internet (IETF) (IETF), un cuerpo de Normas internacionales. Los individuos o los grupos escriben los RFC para la consideración del Internet Society (ISOC) y de la comunidad de Internet en conjunto. Refiera al Home Page del Internet Society para aprender sobre el proceso de los estándares y las actividades del IETF. Refiera al Home Page IETF para leer el texto completo de todos los RFC, Borradores de Internet (Yo-Ds), y STD a que los documentos de Cisco se refieran.

La implementación de Cisco de las aplicaciones SNMP:

- Las definiciones de las variables MIB II que el RFC 1213 describe
- Las definiciones del SNMP traps que el RFC 1215 describe

Cisco proporciona sus propias extensiones de MIB privadas con cada sistema. El MIB del Cisco Enterprise cumple con las guías de consulta que los RFC relevantes describen, a menos que la documentación observe de otra manera. Usted puede encontrar los archivos de definición del módulo MIB y una lista del MIB que se soporta en cada Plataforma de Cisco en el Home Page de Cisco MIB.

Versiones de SNMP

El Cisco IOS Software soporta estas versiones del SNMP:

- SNMPv1 — Norma para toda la Internet un ese RFC 1157 define. El RFC 1157 substituye las versiones anteriores que fueron publicadas como el RFC 1067 y RFC 1098 . La Seguridad se basa en las cadenas de comunidad.
- SNMPv2C — El SNMPv2C es la estructura administrativa basada en string de la comunidad para SNMPv2. El SNMPv2C (la c representa a la comunidad) es un protocolo de Internet experimental que el RFC 1901 , el RFC 1905 , y el RFC 1906 definen. El SNMPv2C es una

actualización de las operaciones de protocolo y de los tipos de datos de SNMPv2p (obra clásica SNMPv2). El SNMPv2C utiliza el modelo de seguridad basado en la comunidad del SNMPv1.

- SNMPv3 — El SNMPv3 es protocolo basado en estándares de interoperabilidad un ese RFC 2273 , RFC 2274 , y el RFC 2275 define. El SNMPv3 proporciona el acceso seguro a los dispositivos con una combinación de autenticación y una encripción de paquetes sobre la red.Las funciones de seguridad que el SNMPv3 proporciona son:Integridad del mensaje — Se asegura de que un paquete no se haya tratado de forzar con adentro transite.Autenticación — Determina que el mensaje es de una fuente válida.Cifrado — Revuelve el contenido de un paquete, que previene la detección por una fuente no autorizada.

El SNMPv1 y el SNMPv2C utilizan una forma basada en la Comunidad de Seguridad. Una dirección IP ACL y la contraseña definen la comunidad de administradores que puede acceder el MIB de agente.

El soporte SNMPv2C incluye un mecanismo de recuperación global y un mensaje de error más-detallado que señalan a las estaciones de administración. El mecanismo de recuperación global soporta la extracción de las tablas y de una gran cantidad de información, que minimiza el número de De ida y vueltas que sean necesarias. El soporte mejorado SNMPv2C del manejo de error incluye los códigos de error ampliados que distinguen los diferentes tipos de condiciones de error. estas condiciones se notifican por medio de un único código de error en SNMPv1. Los códigos de retorno del error ahora señalan el tipo de error.

El SNMPv3 prevé los modelos de seguridad y los niveles de seguridad. Un modelo de seguridad es una estrategia de autenticación que se configura para un usuario y para el grupo en el que el usuario reside. Un nivel de seguridad es el nivel de seguridad permitido dentro de un modelo de seguridad. La combinación de un modelo de seguridad y de un nivel de seguridad determina qué mecanismo de seguridad a utilizar cuando se maneja un paquete snmp.

Configuración general de SNMP

Publique estos comandos en todo el Switches del cliente para habilitar la administración de SNMP:

- Ordene para SNMP ACL:`Switch(config)#`**`access-list 98 permit`** *`ip_address`* *`!--- This is the SNMP device ACL.`*
- Comandos SNMP globales:
  `!--- These are sample SNMP community strings.` `Switch(config)#`**`snmp-server community RO-community ro 98 snmp-server community RW-community rw 98 snmp-server contact Glen Rahn (Home Number) snmp-server location`** *`text`*

Recomendación de Notificaciones de Trampa de SNMP

El SNMP es la fundación para la Administración de redes, y se habilita y se utiliza en todas las redes.

Un agente SNMP puede comunicar con los varios administradores. Por este motivo, usted puede configurar el software para soportar las comunicaciones con una estación de administración con el uso del SNMPv1, y otra estación de administración con el uso de SNMPv2. La mayoría de los clientes y de los NMS todavía utilizan el SNMPv1 y el SNMPv2C porque se retrasa el soporte del dispositivo de red del SNMPv3 en las plataformas NMS algo.

Habilite el SNMP traps para todas las características que sean funcionando. Usted puede inhabilitar las otras funciones, si usted desea. Después de que usted habilite un desvío, usted puede publicar el **comando test snmp** y configurar la dirección apropiada en el NMS para el error. Los ejemplos de tal dirección incluyen una alerta de radiolocalizador o un popup.

Todos los desvíos se inhabilitan por abandono. Habilite todos los desvíos en los switches del núcleo, como este ejemplo muestra:

```
Switch(config)#snmp trap enable Switch(config)#snmp-server trap-source loopback0
```

También, las trampas de puerto del permiso para los puertos claves, tales como infraestructura conectan al Routers y al Switches, y a los puertos de servidor de la clave. La habilitación no es necesaria para otros puertos, tales como puertos de host. Publique este comando para configurar la notificación arriba/abaja del link del puerto y del permiso:

```
Switch(config-if)#snmp trap link-status
```

Después, especifique los dispositivos para recibir los desvíos y para actuar en los desvíos apropiadamente. Usted puede ahora configurar cada destino capturado como beneficiario del SNMPv1, SNMPv2, o del SNMPv3. Para los dispositivos del SNMPv3, confiable informa puede ser enviado bastante que los desvíos UDP. Ésta es la configuración:

```
Switch(config)#snmp-server host ip_address [traps | informs] [version {1 | 2c | 3}] community-string !--- This command needs to be on one line. !--- These are sample host destinations for SNMP traps and informs. snmp-server host 172.16.1.27 version 2c public snmp-server host 172.16.1.111 version 1 public snmp-server host 172.16.1.111 informs version 3 public snmp-server host 172.16.1.33 public
```

Recomendaciones de la Consulta SNMP

Esté seguro que este MIB es el MIB dominante que se sondea o se monitorea en las redes de oficinas centrales:

Nota: Esta recomendación es del grupo consultor de administración de red de Cisco.

Network Time Protocol

Propósito

El Network Time Protocol (NTP), RFC 1305 , sincroniza el timekeeping entre un conjunto de los Servidores de tiempo y de los clientes distribuidos. El NTP permite la correlación de eventos en la creación de los registros del sistema y cuando ocurren otros eventos tiempo-específicos.

Información Operativa General

El RFC 958 documentó NTP primero. Pero el NTP se ha desarrollado con el RFC 1119 (versión NTP 2). El RFC 1305 ahora define el NTP, que está en su tercera versión.

El NTP sincroniza la época de una computadora cliente o de un servidor a otro servidor o fuente horaria de la referencia, tal como una radio, un receptor satelital, o un módem. El NTP proporciona la precisión en el cliente que está típicamente dentro de un ms en los LAN y hasta algunos diez del ms en los WAN, en relación con un servidor primario sincronizado. Por ejemplo, usted puede utilizar el NTP para coordinar el tiempo universal coordinado (UTC) vía un receptor del Global Positioning Service (GPS).

Las configuraciones NTP típicas utilizan servidores redundantes múltiples y diversos trayectos de red para alcanzar una elevada precisión y confiabilidad. Algunas configuraciones incluyen la autenticación criptográfica para prevenir los ataques maliciosos o accidentales al protocolo.

El NTP ejecuta encima el UDP, que a su vez, ejecuta encima el IP. Toda comunicación NTP utiliza UTC, que es el mismo tiempo que la Hora Media de Greenwich.

Actualmente, el NTP versión 3 (NTPv3) y las implementaciones de la versión 4 NTP (NTPv4) está disponible. La versión de último software que se está trabajando encendido es NTPv4, pero la norma de Internet oficial sigue siendo NTPv3. Además, algunos vendedores del sistema operativo personalizan la aplicación del protocolo.

Salvaguardias NTP

La implementación NTP también intenta evitar la sincronización a una máquina en la cual el tiempo no pueda posiblemente ser exacto. El NTP hace esto de dos maneras:

- El NTP no sincroniza a una máquina que no se sincronice.
- El NTP compara siempre el tiempo que es señalado por varias máquinas, y no lo sincroniza a una máquina en la cual el tiempo sea perceptiblemente diferente que los otros, incluso si esa máquina tiene un estrato más bajo.

Asociaciones

Las comunicaciones entre las máquinas que ejecutan el NTP, que se conocen como asociaciones, generalmente se configuran estáticamente. Cada máquina se da los IP Addresses de todas las máquinas con las cuales necesitan formar las asociaciones. El ahorro preciso de tiempo es posible con el intercambio de los mensajes NTP entre cada par de máquinas con una asociación. Pero en un entorno LAN, usted puede configurar el NTP para utilizar los mensajes del broadcast IP. Con esta alternativa, usted puede configurar la máquina para enviar o para recibir los mensajes de broadcast, pero la precisión en el mantenimiento de la hora marginal se reduce porque el flujo de información es unidireccional solamente.

Si la red se aísla del Internet, la implementación de Cisco NTP permite que usted configure una máquina de modo que actúe como si se sincroniza con el uso del NTP, cuando ha determinado realmente el tiempo con el uso de otros métodos. Otras máquinas sincronizan a esa máquina con el uso del NTP.

Una asociación NTP puede ser cualquiera:

- Una asociación de peersEsto significa que este sistema puede sincronizar al otro sistema o permitir que el otro sistema sincronice a él.
- Una asociación del servidorEsto significa que solamente este sistema sincroniza al otro sistema. El otro sistema no sincroniza a este sistema.

Si usted quiere crear una asociación NTP con otro sistema, utilice uno de estos comandos en el modo de configuración global:

Comando	Propósito
[prefer] del [source interface] del [key key-id] del [version number] del [normal-sync] del IP Address de Peer NTP	Crea una asociación de peers con otro sistema

[prefer] del [source interface] del [key key-id] del [version number] del dirección IP del servidor NTP	Forma una asociación del servidor con otro sistema

Nota: Solamente un final de una asociación necesita ser configurado. El otro sistema establece automáticamente la asociación.

Servidores temporizadores públicos del acceso

La subred NTP incluye actualmente sobre 50 servidores públicos primarios que sean sincronizados directamente al UTC por la radio, el satélite, o el módem. Normalmente, las estaciones de trabajo clientes y los servidores con un número de clientes relativamente pequeño no sincronizan con los servidores primarios. Hay cerca de 100 servidores públicos secundarios que se sincronizan a los servidores primarios. Estos servidores proporcionan la sincronización a un total superior a 100,000 clientes y servidores en Internet. La página de los servidores públicos NTP mantiene los objetos listes actuales y se pone al día con frecuencia.

También, hay numerosos privados primarios y los servidores secundarios que no están normalmente disponibles para el público. Refiera al proyecto del protocolo Network Time Protocol (Universidad de Delaware) para las listas del servidor público NTP e información sobre cómo utilizarlos. No hay garantía que estos servidores NTP de Internet públicas están disponibles y producen la hora correcta. Por lo tanto, usted debe considerar las otras opciones. Por ejemplo, haga uso de los diversos dispositivos GPS autónomos que están conectados directamente con vario Routers.

Otra opción es el uso del diverso Routers, conjunto como master del estrato 1. Pero el uso de tal router no se recomienda.

Estrato

El NTP utiliza un estrato para describir el número de saltos NTP lejos que una máquina es de una fuente de tiempo válida. Un Servidor de tiempo del estrato 1 tiene una radio o un reloj atómico que se asocien directamente. Un Servidor de tiempo del estrato 2 recibe su tiempo de un Servidor de tiempo del estrato 1, y así sucesivamente. Una máquina que ejecuta el NTP automáticamente elige como su fuente horaria la máquina con el número de estrato más bajo con el cual se configura para comunicar con el NTP. Esta estrategia construye con eficacia un árbol de altavoces NTP de auto-organización.

El NTP evita la sincronización a un dispositivo en el cual el tiempo no sea posiblemente exacto. Vea la sección de las *salvaguardias NTP del* protocolo Network Time Protocol para los detalles.

Relación Peer del Servidor

- Un servidor responde a los pedidos de cliente pero no intenta incorporar ninguna información de la fecha de una fuente del tiempo de cliente.
- Un par responde a los pedidos de cliente e intenta utilizar el pedido de cliente como candidato potencial para una mejor fuente horaria y ayudarlo en la estabilización de su frecuencia del reloj.
- Para ser peeres verdaderos, los ambos lados de la conexión deben ingresar en una relación de peer, bastante que una situación en cuál el usuario sirve como el par y el otro usuario sirve como servidor. Tenga claves del intercambio de los pares de modo que solamente los host

confiables puedan hablar con otros como pares.
- En un pedido de cliente a un servidor, el servidor contesta al cliente y olvida que el cliente hizo una pregunta.
- En un pedido de cliente a un par, el servidor contesta al cliente. El servidor guarda la información del estado sobre el cliente para seguir como de bien el cliente hace en el timekeeping y qué servidor Stratum funciona con el cliente.

Un servidor NTP puede manejar muchos miles de clientes sin el problema. Pero cuando un servidor NTP dirige más que algunos clientes (hasta unas centenas), hay un impacto en la memoria en la capacidad del servidor de conservar la información del estado. Cuando un servidor NTP dirige más que la cantidad recomendada, consumen a más recursos de la CPU y ancho de banda en el cuadro.

Modos de comunicación con el servidor NTP

Éstos son dos modos separados a comunicar con el servidor:

- Modo de broadcast
- Modo cliente/servidor

En el modo de broadcast, los clientes escuchan. En el modo cliente/servidor, los clientes sondean el servidor. Usted puede utilizar el ntp broadcast si no hay link PÁLIDO implicado debido a su velocidad. Para ir a través de un link PÁLIDO, utilice al modo cliente/servidor (sondeando). Diseñan al modo de broadcast para un LAN, en el cual muchos clientes pueden necesitar posiblemente sondear el servidor. Sin el modo de broadcast, tal interrogación puede generar posiblemente un gran número de paquetes en la red. El Multicast NTP no está todavía disponible en NTPv3, sino está disponible en NTPv4.

Por abandono, el Cisco IOS Software comunica con el uso de NTPv3. Pero el software es compatible con versiones anteriores con las versiones anteriores del NTP.

Sondeo

El protocolo NTP permite que un cliente pregunte un servidor en cualquier momento.

Cuando usted primero configura el NTP en un cuadro de Cisco, el NTP envía ocho interrogaciones en la sucesión rápida en `NTP_MINPOLL` (los intervalos del sec 2^4=16). `NTP_MAXPOLL` son los segundos 2^14 (16,384 sec o 4 horas, el sec 33 el minuto, 4). Este período de tiempo es el período más largo antes de que el NTP sondee otra vez para una respuesta. Actualmente, Cisco no tiene un método para permitir que el usuario fuerce manualmente el tiempo de la `ENCUESTA`.

El contador de la interrogación NTP comienza en el sec 2^6 (64), o 1 minuto, el sec 4. Este tiempo es incrementado por los poderes de 2, mientras que los dos servidores sincronizan con uno a, a 2^10. Usted puede esperar que los mensajes de sincronización sean enviados en un intervalo de uno de 64, 128, 256, el sec 512, o 1024, según el servidor o la configuración de peer. El tiempo más largo entre las encuestas ocurre mientras que el reloj actual llega a ser más estable debido a los loopes sincronizados en fase. Los loopes sincronizados en fase cortan el cristal del reloj local, hasta 1024 segundos (minuto 17).

El tiempo varía entre 64 segundos y 1024 segundos como poder de 2 (que compare una vez a cada 64, 128, 256, sec 512, o 1024). El tiempo se basa en el loop sincronizado en fase que envía y recibe los paquetes. Si hay mucho jitter en el tiempo, el sondear ocurre más a menudo. Si el reloj de referencia es exacto y la conectividad de red es constante, los tiempos de la encuesta

convergen 1024 los segundos entre cada encuesta.

El intervalo de encuesta NTP cambia mientras que la conexión entre el cliente y servidor cambia. Con una mejor conexión, el intervalo de encuesta es más largo. En este caso, una mejor conexión significa que el cliente NTP ha recibido ocho respuestas para las ocho peticiones más recientes. El intervalo de encuesta entonces se dobla. Una sola respuesta equivocada hace el intervalo de encuesta ser reducida por la mitad. El intervalo de encuesta comienza en 64 segundos y va a un máximo del sec 1024. En las mejores circunstancias, el tiempo requerido para que el intervalo de encuesta vaya a partir 64 segundos a 1024 segundos es un poco más de 2 horas.

Difusiones

Las broadcasts NTP nunca se reenvían. Si usted publica el **comando ntp broadcast**, el router comienza a originar los broadcasts NTP en la interfaz en la cual se configura.

Típicamente, usted publica el **comando ntp broadcast** para enviar los broadcasts NTP hacia fuera sobre un LAN para mantener las estaciones y los servidores del extremo del cliente.

Sincronización horaria

La sincronización de un cliente a un servidor consiste en varios intercambios de paquetes. Cada intercambio es un par de la petición/de la contestación. Cuando un cliente envía una petición, el cliente salva su hora local en el paquete enviado. Cuando un servidor recibe el paquete, salva su propia estimación de la hora actual en el paquete, y se vuelve el paquete. Cuando se recibe la contestación, el receptor una vez más registra su propio tiempo del recibo para estimar el tiempo de viaje del paquete.

Estas diferencias de tiempo se pueden utilizar para estimar el tiempo que era necesario para que el paquete transmita del servidor al solicitante. Que el tiempo del viaje de ida y vuelta está tenido en cuenta para una valoración de la hora actual. Cuanto más corto el tiempo del viaje de ida y vuelta es, más exacta es la estimación de la hora actual.

El tiempo no se valida hasta que hayan ocurrido varios intercambios de paquetes de aprobación. Algunos valores esenciales se ponen en los filtros graduales para estimar la calidad de las muestras. Generalmente, cerca de 5 minutos son necesarios para que un cliente NTP sincronice a un servidor. Interesante, esto es también verdad para los relojes de referencia locales que no tienen ningún retardo en absoluto por definición.

Además, la calidad de la conexión de red también influencia la exactitud final. Las redes lentas e imprevisibles con los retardos diversos tienen los efectos nocivos en la sincronización horaria.

Una diferencia de tiempo menos que el ms 128 se requiere para que el NTP sincronice. La exactitud típica en Internet se extiende del ms cerca de 5 al ms 100, que puede variar con los retrasos de la red.

Niveles de Tráfico de NTP

El ancho de banda que el NTP utiliza es mínimo. El intervalo entre los mensajes de la interrogación que los pares intercambian generalmente los trinquetes de nuevo a no más que un mensaje cada minuto 17 (sec 1024). Con las hojas de operación (planning) cuidadosas, usted puede mantener esto dentro de las redes del router sobre los links PÁLIDOS. Tenga el par de los clientes NTP a los servidores NTP locales y no hasta el final a través de WAN a los routeres principales de sitio central, que son los servidores del estrato 2.

Las aplicaciones de un cliente de NTP en convergencia sobre 0.6-bits por segundo (los BPS) hacen un promedio por el servidor.

Recomendación NTP de Cisco

- Cisco recomienda que usted tiene los Servidores de tiempo y trayectos de redes diversos múltiples para alcanzar la alta precisión y la confiabilidad. Algunas configuraciones incluyen la autenticación criptográfica para prevenir los ataques maliciosos o accidentales al protocolo.
- Según el RFC, el NTP se diseña realmente para permitir que usted sondee varios servidores de momento diferente y que utilice la análisis estadístico complicada para subir con un tiempo válido, incluso si usted no está seguro que todos los servidores que usted encuesta es autoritario. El NTP estima los errores de todos los relojes. Por lo tanto, todos los servidores NTP vuelven el tiempo así como una estimación del error actual. Cuando usted utiliza a los Servidores de tiempo múltiples, el NTP también quisiera que estos servidores estuvieran de acuerdo con una cierta hora.
- La implementación de Cisco del NTP no soporta el servicio del estrato 1. Usted no puede conectar con una radio o un reloj atómico. Cisco recomienda que deriven al servicio de tiempo para su red de los servidores públicos NTP que están disponibles en Internet IP.
- Permita a todo el Switches del cliente para enviar regularmente las peticiones de la hora a un servidor NTP. Usted puede configurar hasta 10 servidores/direcciones de peer por el cliente de modo que usted pueda alcanzar la sincronización rápida.
- Para reducir la tara de protocolo, los servidores secundarios distribuyen el tiempo vía el NTP a los host restantes de la local-red. En interés de la confiabilidad, usted puede equipar los host seleccionados de los relojes menos-exactos pero menos-costosos para utilizar para el respaldo en el caso de un error del primario y/o de servidores secundarios o de los trayectos de comunicación entre ellos.
- **ntp update-calendar** — El NTP cambia generalmente solamente el reloj del sistema. Este comando permite que el NTP ponga al día la fecha/la información de tiempo en el calendario. Se hace la actualización solamente si se sincroniza el tiempo NTP. Si no, el calendario guarda su propio tiempo y es inafectado por el tiempo o el reloj del sistema NTP. Utilice siempre esto en los routeres de mayor capacidad.
- **clock calendar-valid** — Este comando declara que la información del calendario es válida y sincronizada. Utilice esta opción en el master NTP. El si esto no está configurado, el router de mayor capacidad que todavía tiene el calendario piensa que su tiempo es no autoritativo, incluso si tiene la línea del master NTP.
- Cualquier número de estrato que esté sobre 15 se considera unsynchronized. Esta es la razón por la cual usted ve el estrato 16 en la salida del **comando show ntp status** en el Routers para quien los relojes son unsynchronized. Si sincronizan al master con un servidor público NTP, aseegurese que el número de estrato en la línea del master NTP es uno o dos más alto que el número de estrato más alto en los servidores públicos que usted sondea.
- Muchos clientes hacen el NTP configurar en el modo de servidor en sus Plataformas del Cisco IOS Software, sincronizadas de varias alimentaciones confiables de Internet o de una radio reloj. Internamente, una alternativa más simple al modo de servidor cuando usted actúa un gran número de Switches es habilitar el NTP en el modo de broadcast en el VLAN de administración en un dominio conmutado. Este mecanismo permite que el Catalyst reciba un reloj de los mensajes de broadcast único. Pero la precisión en el mantenimiento de la hora marginal se reduce porque el flujo de información es unidireccional.
- El uso de los Loopback Address como la fuente de actualizaciones puede también ayudar

con el estado coherente. Usted puede dirigir los problemas de seguridad de dos maneras:Con el control de las actualizaciones del servidor, que Cisco recomiendaPor la autenticación

Comandos global configuration NTP

```
!--- For the client: clock timezone EST -5 ???? ntp source loopback 0 ????? ntp server ip_address key 1 ntp peer ip_address !--- This is for a peer association. ntp authenticate ntp authentication-key 1 md5 xxxx ntp trusted-key 1 !--- For the server: clock timezone EST -5 clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00 clock calendar-valid ntp source loopback0 ntp update-calendar !--- This is optional: interface vlan_id ntp broadcast !--- This sends NTP broadcast packets. ntp broadcast client !--- This receives NTP broadcast packets. ntp authenticate ntp authentication-key 1 md5 xxxxx ntp trusted-key 1 ntp access-group access-list !--- This provides further security, if needed.
```

Comando del estado NTP

```
show ntp status Clock is synchronized, stratum 8, reference is 127.127.7.1 nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18 reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005) clock offset is 0.0000 msec, root delay is 0.00 msec root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

Éste es el direccionamiento del reloj de referencia para el router Cisco cuando el router actúa como master NTP. Si no han sincronizado al router con ningún servidor NTP, el router utiliza este direccionamiento como la referencia ID. Para los detalles en la configuración y los comandos, refiera a la sección *NTP que configura de* realizar la administración del sistema básico.

Cisco Discovery Protocol

Propósito

El CDP ejecuta encima la capa 2 (capa del link de datos) en todos los routeres Cisco, Bridges, Access Servers, y Switches. El CDP permite las aplicaciones de administración de red para descubrir los dispositivos de Cisco que son vecinos de los dispositivos ya-sabidos. Particularmente, las aplicaciones de administración de red pueden descubrir a los vecinos que funcionan con los protocolos transparentes de la capa inferior. Con el CDP, las aplicaciones de administración de red pueden aprender el tipo de dispositivo y el direccionamiento del agente SNMP de los dispositivos de vecindad. Esta característica permite a las aplicaciones para enviar las interrogaciones SNMP a los dispositivos de vecindad.

Los comandos show que se asocian a la característica CDP permiten al ingeniero de red para determinar esta información:

- El número del /port del módulo de otro, dispositivos CDP activados adyacentes
- Estos direccionamientos del dispositivo adyacente:Dirección MACDIRECCIÓN IPDireccionamiento de canal del puerto
- La versión de software del dispositivo adyacente
- Esta información sobre el dispositivo adyacente:VelocidadDúplexDominio VTPConfiguración del VLAN nativo

La sección de Descripción general del funcionamiento resalta algunas de las mejoras de la versión de CDP 2 (CDPv2) sobre la versión de CDP 1 (CDPv1).

Información Operativa General

El CDP se ejecuta en todo el LAN y medios WAN que soporten la BROCHE.

Cada dispositivo CDP-configurado envía los mensajes periódicos a una dirección Multicast. Cada dispositivo hace publicidad por lo menos de un direccionamiento en el cual el dispositivo pueda recibir los mensajes snmp. Los anuncios también contienen el Tiempo para vivir, o el tiempo en espera, información. Esta información indica la longitud del tiempo para que un dispositivo receptor lleve a cabo la información CDP antes del descarte.

El CDP utiliza la encapsulación SNAP con el código de tipo 2000. En los Ethernetes, se utiliza la atmósfera, y el FDDI, la dirección de multidifusión de destino 01-00-0c-cc-cc-cc. En Token Rings, se utiliza la dirección funcional c000.0800.0000. Las tramas CDP se envían periódicamente cada minuto.

Los mensajes CDP contienen uno o más mensajes que permitan que el dispositivo de destino recopile y salve la información sobre cada dispositivo vecino.

Esta tabla proporciona los parámetros que el CDPv1 soporta:

Parámetro	Tipo	Descripción
1	ID del dispositivo	Nombre del host del dispositivo o del número de serie del hardware en el ASCII
2	Dirección	El direccionamiento de la capa 3 de la interfaz que envía la actualización
3	Identificación del puerto	El puerto en el cual se envía la actualización de CDP
4	Capacidades	Describe las capacidades funcionales del dispositivo de esta manera: • Router: 0x01 • Bridge SR1: 0x04 • Switch: 0x08 (proporciona la capa 2 y/o el Layer 3 Switching) • Host: 0x10 • Filtración condicional IGMP: 0x20 • El Bridge o el Switch no remite los paquetes de informe IGMP en los puertos del nonrouter.
5	Versión	Una cadena de carácter que contiene la versión de software **Nota:** La salida del **comando show version** muestra la misma información.
6	Plataforma	La plataforma de hardware, por ejemplo, WS-C5000, WS-C6009, y Cisco RSP2

[1] SENIOR = Source-Route.

[2] RSP = Route Switch Processor.

En el CDPv2, han presentado al tipo adicional, longitud, los valores (TLV). El CDPv2 soporta cualquier TLV. Pero esta tabla proporciona los parámetros que pueden ser determinado útiles en los entornos conmutados y que las aplicaciones del software Catalyst.

Cuando un Switch ejecuta el CDPv1, el Switch cae las tramas del CDPv2. Cuando un Switch ejecuta el CDPv2 y recibe una trama del CDPv1 en una interfaz, el Switch comienza a enviar las tramas del CDPv1 de esa interfaz, además de las tramas del CDPv2.

Parámetro	Tipo	Descripción
9	Dominio de VTP	El dominio VTP, si se configura en el dispositivo
10	VLAN nativa	En el dot1q, las tramas para el VLA N, que el puerto es adentro si el puerto no es enlace, siguen siendo untagged. Esto se refiere generalmente como el VLAN nativo.
11	Dúplex Medio/Total	Este TLV contiene la configuración dúplex del puerto de envío.
14	Dispositivo VLAN-ID	Permite que el tráfico de VoIP sea distinguido del otro tráfico mediante un VLAN distinto ID (VLAN auxiliar).
16	Consumo de Energía	La cantidad máxima de poder que se espera que sea consumido, en el mW, por el dispositivo conectado.
17	MTU (unidad de transmisión básica)	El MTU de la interfaz por la cual la trama CDP es transmitida.
18	Confianza extendida	Indica que el puerto está en el modo extendido de la confianza.
19	COS para los puertos untrusted	El valor del Clase de Servicio (CoS) que se utilizará para marcar todos los paquetes que se reciben en puerto no confiable de un dispositivo de Switching conectado.
20	SysName	Nombre de dominio totalmente calificado (FQDN) del dispositivo (0, si desconocido).
25	Poder	Transmitido por un dispositivo powerable

	pedido	para negociar un nivel de potencia conveniente.
26	Poder disponible	Transmitido por un Switch. Permite que un dispositivo powerable negocie y seleccione una configuración de energía apropiada.

CDPv2/Power sobre los Ethernetes

Un poco de Switches, como el Catalyst 6500/6000 y el 4500/4000, tiene la capacidad de suministrar el poder vía los cables del par trenzado sin blindaje (UTP) a los dispositivos powerable. La información que se recibe vía CDP (parámetros 16, 25, 26) ayuda a la optimización de la administración de la energía del Switch.

Interacción del teléfono del IP CDPv2/Cisco

Los Teléfonos IP de Cisco proporcionan la Conectividad para un dispositivo Ethernet externamente asociado 10/100-Mbps. Esta Conectividad se alcanza con la integración de un 2 Switch interno de la capa del tres-puerto dentro del teléfono del IP. Los puertos de switch internos se refieren como:

- P0 (dispositivo interno del teléfono del IP)
- P1 (puerto del externo 10/100-Mbps)
- P2 (puerto del externo 10/100-Mbps que conecta con el Switch)

Usted puede transferir el tráfico de voz en un VLAN distinto en el puerto del switch si usted configura los puertos troncales del acceso del dot1q. Este VLA N adicional se conoce como el auxiliar (CatOS) o VLA N de la Voz (Cisco IOS Software). Por lo tanto, el tráfico con Tag del dot1q del teléfono del IP se puede enviar en el VLA N auxiliar/de la Voz, y el tráfico sin Tags se puede enviar vía el puerto del externo 10/100-Mbps del teléfono vía el VLA N del acceso.

Los switches de Catalyst pueden informar a un teléfono del IP la Voz VLAN ID vía CDP (Parameter-14: Dispositivo VLAN-ID TLV). Como consecuencia, el teléfono del IP marca todos los paquetes con etiqueta VoIP-relacionados con la prioridad apropiada VLAN ID y 802.1p. Este CDP TLV también se utiliza para identificar si un teléfono del IP está conectado vía el parámetro de la identificación del dispositivo.

Este concepto puede ser explotado cuando usted desarrolla a política de calidad de servicio (QoS). Usted puede configurar el switch de Catalyst para obrar recíprocamente con el teléfono del IP de tres maneras:

- Cisco IP Phone del dispositivo de la confianzaCondicional confianza CoS solamente cuando un teléfono del IP se detecta vía el CDP. Siempre que un teléfono del IP se detecte vía CDP Parameter-14, fijan al estado de confianza del puerto para confiar en COS. Si no se detecta ningún teléfono del IP, el puerto es untrusted.
- Confianza extendidaEl Switch puede informar al teléfono del IP vía CDP (Parameter-18) para confiar en todas las tramas que se reciban en su puerto del dispositivo del externo 10/100-Mbps.
- Reescritura COS para los puertos untrustedEl Switch puede informar al teléfono del IP vía CDP (Parameter-19) para reescribir los valores 802.1p CoS que se reciben en su puerto del dispositivo del externo 10/100-Mbps.**Nota:** Por abandono, todo el tráfico que se recibe en los puertos externos 10/100-Mbps del teléfono del IP es untrusted.

Nota: Esto es un ejemplo de configuración para que cómo conecte el teléfono del IP del no Cisco con un Switch.

Nota: Por ejemplo,

```
Switch(config)#interface gigabitEthernet 2/1 Switch(config-if)#switchport mode trunk !--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-if)#switchport trunk native vlan 10 Switch(config-if)#switchport trunk allow vlan 10,30 Switch(config-if)#switchport voice vlan 30 Switch(config-if)#spanning-tree portfast trunk !--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Recomendación de la configuración de Cisco

La información que el CDP proporciona puede ser una extremadamente útil cuando usted resuelve problemas los problemas de conectividad de la capa 2. Habilite el CDP en todos los dispositivos que soporten su operación. Ejecute estos comandos:

- Para habilitar el CDP global en el Switch:`Switch(config)#cdp run`
- Para habilitar el CDP en una basada en cada puerto:`Switch(config)#interface type slot#/port# Switch(config-if)#cdp enable`

Configuración de Lista de Verificación

Comandos globales

El login, habilita, y ingresa al modo de configuración global para comenzar el proceso de la configuración del switch.

```
Switch>enable Switch# Switch#configure terminal Switch(Config)#
```

Comandos global genéricos (para toda la empresa)

Esta sección de comandos global enumera los comandos global de aplicarse a todo el Switches en la red para empresas del cliente.

Esta configuración contiene los comandos global recomendados de agregar a la configuración inicial. Usted debe cambiar los valores en la salida antes de que usted copie y pegue el texto en el CLI. Publique estos comandos para aplicar la configuración global:

```
vtp domain domain_name vtp mode transparent spanning-tree portfast bpduguard spanning-tree etherchannel guard misconfig cdp run no service pad service password-encryption enable secret password clock timezone EST -5 clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00 clock calendar-valid ip subnet-zero ip host tftpserver your_tftp_server ip domain-name domain_name ip name-server name_server_ip_address ip name-server name_server_ip_address ip classless no ip domain-lookup no ip http server no logging console no logging monitor logging buffered 16384 logging trap notifications logging facility local7 logging syslog_server_ip_address logging syslog_server_ip_address logging source-interface loopback0 service timestamps debug datetime localtime show-timezone msec service timestamps log datetime localtime show-timezone msec access-list 98 permit host_ip_address_of_primary_snmp_server access-list 98 permit host_ip_address_of_secondary_snmp_server snmp-server community public ro 98 snmp-server community laneng rw 98 snmp-server enable traps entity snmp-server host host_address traps public snmp-server host host_address traps public banner motd ^CCCCC This is a proprietary system, NOT for public or personal use. All work products, communications, files, data or information directly or indirectly created, input or accessed on this system are and shall become the sole property of the company. This system is actively monitored and accessed by
```

```
the company. By logging onto this system, the user consents to such monitoring and access. USE
OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT THE USER TO
DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES ^C line console 0 exec-timeout 0 0 password cisco
login transport input none line vty 0 4 exec-timeout 0 0 password cisco login length 25 clock
calendar-valid ntp server ntp_server_ip_address ntp server ntp_server_ip_address ntp update-
calendar
```

Comandos global que son específicos a cada chasis del switch

Los comandos global en esta sección son específicos a cada chasis del switch que esté instalado en la red.

Configuraciones variables Chasis-específicas

Para fijar la fecha y hora, publique este comando:

```
Switch#clock set hh:mm:ss day month year
```

Para fijar el nombre del host del dispositivo, publique estos comandos:

```
Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with
CNTL/Z. Switch(config)#hostname Cat6500
```

Para configurar el Loopback Interface para la Administración, publique estos comandos:

```
CbrCat6500(config)#interface loopback 0 Cat6500(config-if)#description Cat6000 - Loopback
address and Router ID Cat6500(config-if)#ip address ip_address subnet_mask Cat6500(config-
if)#exit
```

Para mostrar la revisión del Cisco IOS Software del Supervisor Engine, publique estos comandos:

```
Cbrcat6500#show version | include IOS IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9,
EARLY DEPLOYMENT RELE ASE SOFTWARE (fc1) cat6500#
```

Para mostrar la revisión de archivo de arranque MSFC, publique este comando:

```
Cat6500#dir bootflash: Directory of bootflash:/ 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-
mz.121-19.E1a 15990784 bytes total (14111616 bytes free
```

Para especificar la información de contacto y la ubicación del servidor SNMP, publique estos comandos:

```
Cat6500(config)#snmp-server contact contact_information Cat6500(config)#snmp-server location
location_of_device
```

Para copiar la configuración de inicio de un motor del supervisor existente a un nuevo Supervisor Engine, podía haber algo pierde de la configuración, por ejemplo, la configuración en las interfaces del supervisor existente. Cisco recomienda copiar la configuración a un archivo de texto y pegarla en los segmentos en la consola para ver si hay algunos problemas de configuración que ocurran.

Comandos de interfaz

Tipos de puerto funcionales de Cisco

Los puertos del switch en Cisco IOS Software se refieren como interfaces. Hay dos tipos de modos de la interfaz en Cisco IOS Software:

- Interfaz ruteada de la capa 3
- Interfaz del 2 Switch de la capa

La función de la interfaz se refiere a cómo usted ha configurado el puerto. La configuración del puerto puede ser:

- Interfaz ruteada
- Switched Virtual Interface (SVI)
- Puerto de acceso
- Trunk
- EtherChannel
- Una combinación de éstos

El tipo de interfaz refiere a un tipo de puerto. El tipo de puerto puede ser cualquiera:

- FE
- GE
- Canal de puerto

Esta lista describe abreviadamente diversas funciones de la interfaz del Cisco IOS Software:

- Interfaz física ruteada (valor por defecto) — Cada interfaz en el Switch es una interfaz ruteada de la capa 3 por abandono, que es similar a cualquier router Cisco. La interfaz ruteada debe caer en una subred de IP única.
- Interfaz del puerto del switch de acceso — Esta función se utiliza para poner las interfaces en el mismo VLA N. Los puertos se deben convertir de una interfaz ruteada a un Switched Interface.
- SVI — Un SVI se puede asociar a un VLA N que contenga los puertos del switch de acceso para el InterVLAN Routing. Configure el SVI que se asociará a un VLA N cuando usted quiere una ruta o un Bridge entre los puertos del switch de acceso en diversos VLA N.
- Interfaz del puerto del switch del trunk — Esta función se utiliza para llevar los VLAN múltiples a otro dispositivo. Los puertos se deben convertir de una interfaz ruteada a un puerto del switch de trunk.
- EtherChannel — Un EtherChannel se utiliza para liar los puertos individuales en un solo puerto lógico para la Redundancia y el Equilibrio de carga.

Recomendaciones funcionales del tipo de puerto de Cisco

Utilice la información en esta sección para ayudar a determinar los parámetros para aplicarse a las interfaces.

Nota: Incorporan a algunos comandos interface-specific en lo posible.

Autonegotiation

No utilice el autonegotiation en tampoco de estas situaciones:

- Para los puertos que soportan los dispositivos de la infraestructura de red tales como Switches y Routers
- Para otros sistemas extremos nontransient tales como servidores e impresoras

Configure manualmente para la velocidad y dúplex estas configuraciones de link 10/100-Mbps. Las configuraciones son generalmente FULL-duplex del 100-Mbps:

- Switch a switch del link del 100 MB
- Switch-a-servidor del link del 100 MB
- Switch-a-router del link del 100 MB

Usted puede configurar estas configuraciones de esta manera:

```
Cat6500(config-if)#interface [type] mod#/port# Cat6500(config-if)#speed 100 Cat6500(config-if)#duplex full
```

Cisco recomienda las configuraciones de link 10/100-Mbps para los usuarios finales. Los trabajadores móviles y los host transitorios necesitan el autonegotiation, pues este ejemplo muestra:

```
Cat6500(config-if)#interface [type] mod#/port# Cat6500(config-if)#speed auto
```

El valor predeterminado en las interfaces Gigabit es `negociación automática`. Pero publique estos comandos para asegurarse de que el autonegotiation está habilitado. Cisco recomienda la habilitación de la negociación Gigabit:

```
Cat6500(config-if)#interface gigabitethernet mod#/port# Cat6500(config-if)#no speed
```

Raíz del árbol de expansión

Con la consideración del diseño de la red, identifique el Switch que best suited para ser la raíz para cada VLA N. Generalmente, elija un Switch potente en el medio de la red. Ponga el Root Bridge en el centro de la red y conecte directamente el Root Bridge con los servidores y el Routers. Esta configuración reduce generalmente la distancia promedio de los clientes a los servidores y al Routers. Refiera a los problemas y a las consideraciones de diseño relacionadas del Spanning Tree Protocol para más información.

Para forzar un Switch para ser la raíz para un VLA N señalado, publique este comando:

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

Árbol de expansión Portfast

PortFast desvía atravesar normal - operación del árbol en los puertos de acceso para acelerar los retrasos en la conectividad iniciales que ocurren cuando las estaciones terminales están conectadas con un Switch. Refiérase con PortFast y otros comandos de reparar los retardos de la conectividad de inicialización de la estación de trabajo para más información sobre PortFast.

Fije el STP portfast a encendido para todos los puertos de acceso habilitados que estén conectados con un solo host. Aquí tiene un ejemplo:

```
Cat6500(config-if)#interface [type] mod#/port# Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION %Portfast has been configured on FastEthernet3/1 but will only have effect when the interface is in a non-trunking mode.
```

UDLD

Permita al UDLD solamente en los puertos de infraestructura o los cables Ethernet de cobre fibra-conectados para monitorear la configuración física de los cables. Ejecute estos comandos para habilitar el UDLD:

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#udld enable
```

Información de configuración de VLAN

VLA N de la configuración con estos comandos:

```
Cat6500(config)#vlan vlan_number Cat6500(config-vlan)#name vlan_name Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id Cat6500(config)#default spanning-tree vlan vlan_id
```

Relance los comandos para cada VLA N, y después salga. Ejecutar este comando:

```
Cat6500(config)#exit
```

Publique este comando para verificar todos los VLA N:

```
Cat6500#show vlan
```

SVI ruteados

Configure los SVI para el InterVLAN Routing. Ejecute estos comandos:

```
Cat6500(config)#interface vlan vlan_id Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description Cat6500(config-if)#no shutdown
```

Relance estos comandos para cada función de la interfaz que contenga un SVI ruteado, y después salga. Ejecutar este comando:

```
Cat6500(config-if)#^Z
```

Sola interfaz física ruteada

Publique estos comandos para configurar la interfaz ruteada predeterminada de la capa 3:

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

Relance estos comandos para cada función de la interfaz que contenga una interfaz física ruteada, y después salga. Ejecutar este comando:

```
Cat6500(config-if)#^Z
```

EtherChannel ruteado (L3)

Para configurar el EtherChannel en las interfaces de la capa 3, publique los comandos en esta sección.

Configure una interfaz lógica de canal de puerto de esta manera:

```
Cat6500(config)#interface port-channel port_channel_interface_# Cat6500(config-if)#description
port_channel_description Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

Realice los pasos en esta sección para los puertos que forma ese canal particular. Aplique la información restante al Canal de puerto, como este ejemplo muestra:

```
Cat6500(config)#interface range [type] mod/port_range Cat6500(config-if)#channel-group 1-64 mode
[active | auto | desirable | on | passive] Cat6500(config-if)#no shutdown Cat6500(config-if)#^Z
```

Nota: Después de que usted configure un EtherChannel, la configuración que usted aplica a la interfaz del Canal de puerto afecta al EtherChannel. La configuración que usted aplica a los puertos LAN afecta solamente al puerto LAN en donde usted aplica la configuración.

EtherChannel (L2) con el enlace

Configure el EtherChannel de la capa 2 para el enlace de esta manera:

```
Cat6500(config)#interface port-channel port_channel_interface_# Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type Cat6500(config-if)#switchport
trunk native vlan vlan_id Cat6500(config-if)#no shutdown Cat6500(config-if)#exit
```

Realice los pasos en esta sección solamente para los puertos que forma ese canal particular.

```
Cat6500(config)#interface range [type] mod/port_range Cat6500(config-if)#channel-group 1-64 mode
[active | auto | desirable | on | passive] Cat6500(config-if)#no shutdown Cat6500(config-
if)#exit
```

Nota: Después de que usted configure un EtherChannel, la configuración que usted aplica a la interfaz del Canal de puerto afecta al EtherChannel. La configuración que usted aplica a los puertos LAN afecta solamente al puerto LAN en donde usted aplica la configuración.

Verifique la creación de todos los EtherChanneles y trunks. Aquí tiene un ejemplo:

```
Cat6500#show etherchannel summary Cat6500#show interface trunk
```

Puertos de acceso

Si la función de la interfaz es un puerto de acceso que se configura como sola interfaz, publique estos comandos:

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id Cat6500(config-if)#exit
```

Relance estos comandos para cada interfaz que necesite ser configurada como puerto del 2 Switch de la capa.

Si se va el puerto del switch a ser conectado con las estaciones terminales, publique este comando:

```
Cat6500(config-if)#spanning-tree portfast
```

Puerto troncal (sola interfaz física)

Si la función de la interfaz es un puerto troncal que se configura como sola interfaz, publique estos comandos:

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#switchport Cat6500(config-
if)#switchport trunk encapsulation dot1q Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown Cat6500(config-if)#exit
```

Relance estos comandos para cada función de la interfaz que necesite ser configurada como puerto troncal.

Información de contraseña

Publique estos comandos para la información de contraseña:

```
Cat6500(config)#service password-encryption Cat6500(config)#enable secret password
CbrCat6500(config)#line con 0 Cat6500(config-line)#password password CbrCat6500(config-
line)#line vty 0 4 Cat6500(config-line)#password password Cat6500(config-line)#^Z
```

Salve la configuración

Publique este comando para salvar la configuración:

```
Cat6500#copy running-config startup-config
```

Nuevas funciones del software en el Cisco IOS Software Release 12.1(13)E

Refiera a configurar el soporte del Cisco IP Phone para más información sobre el soporte del teléfono del IP.

Refiera al reconocimiento de la aplicación basada en la red y al reconocimiento de la aplicación basada en la red distribuido para más información sobre el Network-Based Application Recognition (NBAR) para los puertos LAN.

Notas:

- El NBAR para los puertos LAN se soporta en el software en el MSFC2.
- El PFC2 proporciona el soporte del hardware para las entradas ACL en los puertos LAN en donde usted configura el NBAR.
- Cuando se habilita el PFC QoS, el tráfico a través de los puertos LAN en donde usted configura los pasos NBAR a través del ingreso y las colas de administración del tráfico y los umbrales de caída de la salida.
- Cuando se habilita el PFC QoS, el MSFC2 fija el Clase de Servicio (CoS) de la salida igual a la Prioridad IP de la salida.
- Después de que el tráfico pase a través de una cola del ingreso, todo el tráfico se procesa en el software en el MSFC2 en los puertos LAN en donde usted configura el NBAR.
- El NBAR distribuido está disponible en las interfaces del FlexWan con el Cisco IOS Software Release 12.1(6)E y Posterior.

Las mejoras de la Exportación de datos de NetFlow (NDE) incluyen:

- máscaras del flujo de la Destino-fuente-interfaz y de la interfaz plena
- NDE de la versión 5 del PFC2
- Sampled NetFlow
- Una opción para poblar estos campos adicionales en los expedientes NDE:Dirección IP del Next Hop RouterIfIndex SNMP de la interfaz de ingresoIfIndex SNMP de la interfaz de egresoNúmero del sistema autónomo de la fuente

Refiera a configurar el NDE para más información sobre estas mejoras.

Las mejoras de la otra función incluyen:

- Configuración de UDLD
- Configuración de VTP
- Configurar caché Web los servicios usando el WCCP

Estos comandos son comandos new:

- **recarga mínima del retardo espera**
- **debounce del link**
- **política de asignación interna vlan {que asciende | descenso}**
- **sistema jumbomtu**
- **borre el medidor del tráfico catalyst6000**

Estos comandos son comandos mejorados:

- **muestre el uso interno vlan** — Este comando fue aumentado de incluir los VLA N que las

interfaces de WAN utilizan.
- **muestre la identificación vlan** — Este comando fue aumentado de soportar la entrada de un rango de los VLA N.
- **demostración l2protocol-tunnel** — Este comando fue aumentado de soportar la entrada de un VLAN ID.

El Cisco IOS Software Release 12.1(13)E soporta estas funciones del software, que fueron soportadas previamente en las versiones del Cisco IOS Software Release 12.1 EX:

- Configuración de los EtherChanneles de la capa 2 que incluyen las interfaces en diversos módulos equipados con DFC de la transferenciaRefiera a las advertencias generales resueltas en la sección de la versión 12.1(13)E del Id. de bug Cisco CSCdt27074 (clientes registrados solamente).
- Redundancia del Redundancia plus de procesador de routing (RPR+)Refiera a configurar Redundancia del Supervisor Engine RPR o RPR+.**Nota:** En el Cisco IOS Software Release 12.1(13)E y Posterior, las funciones de redundancia RPR y RPR+ substituyen la alta disponibilidad de sistema mejorada (EHSA) de la Redundancia.
- VLA N de 4,096 capas 2Refiera a configurar los VLA N.**Nota:** Las versiones del Cisco IOS Software Release 12.1(13)E y Posterior soportan la configuración de las interfaces VLAN de 4,096 capas 3. Configure un total combinado de interfaces VLAN de no más que 2,000 capas 3 y los puertos de la capa 3 en un MSFC2 con un Supervisor Engine II o un Supervisor Engine I. Configure al total combinado de no más que 1,000 acodan 3 puertos de las interfaces VLAN y de la capa 3 en un MSFC.
- El hacer un túnel del IEEE 802.1QRefiera a configurar el IEEE 802.1Q que hace un túnel y acode el Tunelización de 2 protocolos.
- Tunelización del protocolo del IEEE 802.1QRefiera a configurar el IEEE 802.1Q que hace un túnel y acode el Tunelización de 2 protocolos.
- IEEE 802.1S Múltiples Árboles de expansión (MST)Refiera a configurar STP y el IEEE 802.1S MST.
- IEEE 802.1W STP rápido (RSTP)Refiera a configurar STP y el IEEE 802.1S MST.
- IEEE 802.3ad LACPRefiera a configurar el EtherChannel de la capa 3 y de la capa 2.
- Filtración de PortFast BPDURefiera a configurar las características STP.
- Creación automática de las interfaces VLAN de la capa 3 para soportar el VLA N ACL (VACL)Refiera a configurar la seguridad de la red.
- Puertos de la captura VACL que pueden ser cualquier acceso de Ethernet de la capa 2 en cualquier VLA NRefiera a configurar la seguridad de la red.
- Talla del MTU configurable en los puertos de la capa de físicos individuales 3Refiera a la descripción de la configuración de la interfaz.
- Configuración de los puertos destino del SPAN como trunks para marcar todo el tráfico del SPAN con etiquetaRefiera a configurar el Local y el SPAN remoto.

Información Relacionada

- Herramientas y recursos - Cisco Systems
- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems