Mejores prácticas para el Switches de los Catalyst 4500/4000, 5500/5000, y 6500/6000 Series que funciona con la configuración y la Administración de CatOS

Contenido

Introducción

En este documento se trata la implementación de Cisco Catalyst Series Switches en su red, específicamente de las plataformas Catalyst 4500/4000, 5500/5000 y 6500/6000. Tenga en cuenta que, cuando se hace referencia a las configuraciones y a los comandos, se da por sentado que usted está ejecutando la versión de implementación general del software Catalyst OS (CatOS) 6.4(3) o una versión posterior. Si bien se presentan algunos aspectos del diseño en este documento, no se trata el diseño global del campus.

prerrequisitos

Requisitos

En este documento, se da por hecho que usted está familiarizado con la Referencia de Comandos de Catalyst 6500 Series, 7.6.

Si bien se incluyen referencias a material público disponible en línea para una lectura adicional en todo el documento, a continuación figuran otras referencias que le servirán de base y para su formación:

- Conceptos Básicos para Proveedores de Servicio de Internet de Cisco: Funciones Esenciales del IOS que Cada Proveedor de Servicio de Internet Debe Tener en Cuenta.
- Guía de Consulta de Correlación de Eventos y Monitoreo de Red de Cisco
- Diseño de Red de Campus de Gigabit: Principios y Arquitectura
- Cisco SAFE: Un Plan General de Seguridad para Redes para Empresas

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Estas soluciones representan años de experiencia de campo de los ingenieros de Cisco que trabajan con muchos de nuestros clientes de mayor envergadura y con redes complejas. Por lo tanto, este documento hace hincapié en las configuraciones reales que posibilitan el correcto funcionamiento de las redes. Este documento ofrece las siguientes soluciones:

- Soluciones que, según las estadísticas, tienen el mayor uso en el campo y, por lo tanto,

menor riesgo.
- Soluciones simples mediante las cuales se negocia cierta flexibilidad para obtener resultados seguros.
- Las soluciones fáciles de manejar que son configuradas por equipos de operaciones de red.
- Soluciones que promueven la alta disponibilidad y la alta estabilidad.

Este documento se divide en estas cuatro secciones:

- Configuración básica: funciones usadas por la mayoría de las redes, como Spanning-Tree Protocol (STP) y trunking.
- Configuración de administración: aspectos del diseño junto con monitoreo del sistema y de eventos mediante el uso de Simple Network Management Protocol (SNMP), Remote Monitoring (RMON), Syslog, Cisco Discovery Protocol (CDP) y Network Time Protocol (NTP).
- Configuración de seguridad: contraseñas, seguridad de puertos, seguridad física, y autenticación con TACACS+.
- Lista de verificación de configuración: resumen de plantillas de configuración recomendadas.

Configuración Básica

En esta sección, se tratan las funciones que se implementan en la mayoría 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. Tener un conocimiento básico de estos protocolos le resultará de utilidad para abordar cada sección.

Tráfico de Supervisor

La mayoría de las funciones activadas en una red Catalyst requieren la cooperación de dos o más switches, de modo que debe haber un intercambio controlado de mensajes de mantenimiento, parámetros de configuración y cambios de administración. Independientemente de que estos protocolos sean propiedad de Cisco, como CDP, o basados en estándares, como IEEE 802.1D (STP), todos tienen ciertos elementos en común cuando se implementan en Catalyst Series.

En el reenvío de tramas básico, las tramas de datos del usuario se originan en los sistemas finales, y su dirección de origen y su dirección de destino no se cambian en los dominios de switch de la Capa 2 (L2). Las tablas de búsqueda de la memoria de contenido direccionable (CAM) en cada Supervisor Engine del switch se completan mediante un proceso de aprendizaje de dirección de origen e indican qué puerto de salida debe reenviar cada trama recibida. Si el proceso de aprendizaje de direcciones es incompleto (el destino es desconocido o la trama tiene una dirección broadcast o multicast como destino), todos los puertos en esa VLAN reenvían (inundan) la trama.

El switch debe también reconocer qué tramas deben ser conmutadas a través del sistema y cuáles se deben dirigir al CPU del switch (también conocida como procesador de administración de la red [NMP]).

El plano de control del Catalyst se crea usando entradas especiales en la tabla de CAM, llamadas **entradas del sistema**, para recibir el tráfico y dirigirlo al NMP en un puerto de switch interno. De

esta manera, al utilizar protocolos con direcciones de destino MAC conocidas, el tráfico de planos de control puede separarse del tráfico de datos. Ejecute el comando show CAM system en un switch para confirmar esto, como se muestra a continuación:

```
>show cam system

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -----------------    -----  ---------------------------------------
1     00-d0-ff-88-cb-ff  #          1/3
!--- NMP internal port. 1 01-00-0c-cc-cc-cc # 1/3 !--- CDP and so on. 1 01-00-0c-cc-cc-cd # 1/3
!--- Cisco STP. 1 01-80-c2-00-00-00 # 1/3 !--- IEEE STP. 1 01-80-c2-00-00-01 # 1/3 !--- IEEE
flow control. 1 00-03-6b-51-e1-82 R# 15/1 !--- Multilayer Switch Feature Card (MSFC) router. ...
```

Cisco tiene un rango reservado de direcciones Ethernet MAC y de protocolo, como se muestra. Estas direcciones se tratan más adelante en este documento. Sin embargo, esta tabla brinda un resumen para su comodidad.

Función	Tipo de Protocolo SNAP HDLC	MAC de Multicast de Destino
Port Aggregation Protocol (PAgP)	0x0104	01-00-0c-cc-cc-cc
Spanning Tree PVSTP+	0x010b	01-00-0c-cc-cc-cd
Bridge VLAN	0x010c	01-00-0c-cd-cd-ce
Unidirectional Link Detection (UDLD)	0x0111	01-00-0c-cc-cc-cc
Cisco Discovery Protocol	0x2000	01-00-0c-cc-cc-cc
Dynamic Trunking (DTP)	0x2004	01-00-0c-cc-cc-cc
Uplink Fast de STP	0x200a	01-00-0c-cd-cd-cd
IEEE Spanning Tree 802.1d	N/A - DSAP 42 SSAP 42	01-80-c2-00-00-00
Inter Switch Link (ISL)	N/A	01-00-0c-00-00-00
VLAN Trunking (VTP)	0x2003	01-00-0c-cc-cc-cc
Pausa IEEE 802.3x	N/A - DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

Las mayorías de los protocolos de control de Cisco utilizan una encapsulación SNAP de IEEE 802.3, que incluye **LLC 0xAAAA03, OUI 0x00000C**, que se puede ver en una traza del analizador de LAN. Otras propiedades comunes de estos protocolos incluyen las siguientes:

- Estos protocolos suponen conectividad de punto a punto. Observe que el uso deliberado de direcciones de multicast de destino permite que dos Catalyst se comuniquen de modo transparente por switches que no son de Cisco, ya que los dispositivos que no entienden ni interceptan las tramas sencillamente las inundan. Sin embargo, las conexiones de punto a multipunto a través de entornos de proveedores múltiples pueden dar lugar a un comportamiento inconsistente y deben generalmente ser evitadas.
- Estos protocolos terminan en los routers de la Capa 3 (L3); funcionan solamente dentro de un dominio conmutado.
- Estos protocolos reciben prioridad sobre los datos del usuario mediante el procesamiento y la programación del Circuito Integrado para Aplicaciones Específicas (ASIC) de entrada.

Después de la introducción de las direcciones de destino del protocolo de control, la dirección de origen debe también ser descrita para que esté completa. Los protocolos de switches utilizan una dirección MAC tomada de un banco de direcciones disponibles suministradas por EPROM en el chasis. Ejecute el comando show module para visualizar los rangos de direcciones disponibles para cada módulo cuando este origina tráfico, como unidades de datos del protocolo bridge (BPDU) STP o tramas ISL.

```
>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
!--- MACs for sourcing traffic. ... VLAN 1
```

VLAN 1

VLAN 1 tiene un significado especial en las redes Catalyst.

La Supervisor Engine de Catalyst siempre utiliza la VLAN predeterminada (VLAN1) para etiquetar varios protocolos de control y de administración al conectar mediante trunk, como CDP, VTP y PAgP. Todos los puertos, incluida la interfaz sc0 interna, se configuran de forma predeterminada para ser miembros de VLAN 1. Todos los trunks transportan la VLAN1 de forma predeterminada, y en las versiones del software CatOS anteriores a 5.4, no era posible bloquear los datos del usuario en la VLAN1.

Estas definiciones son necesarias para aclarar algunos términos bien usados en conexiones entre redes Catalyst:

- La VLAN de administración es en la que reside la interfaz sc0; esta VLAN se puede cambiar.
- La VLAN nativa se define como la VLAN a la cual regresa un puerto cuando no se conecta mediante trunking y es la VLAN sin etiqueta en un trunk 802.1q. De forma predeterminada, la VLAN 1 es la VLAN nativa.
- Para cambiar la VLAN nativa, ejecute el comando set vlan vlan-id mod/port.**Nota:** Cree la VLAN antes de que la establezca como la VLAN nativa del trunk.

Estas son varias buenas razones para ajustar una red y para alterar el comportamiento de los puertos en la VLAN 1:

- Cuando el diámetro de la VLAN 1, como el de cualquier otra VLAN, se vuelve tan grande que representa un riesgo para la estabilidad (especialmente, desde el punto de vista de un STP), hay que reducirlo. Esto se trata más detalladamente en la sección Administración en Banda de este documento.
- Los datos del plano de control en la VLAN 1 se deben guardar por separado de los datos del usuario para simplificar el troubleshooting y maximizar los ciclos disponibles del CPU.
- Se deben evitar loops L2 en la VLAN 1 cuando se diseñan redes de campus de varias capas sin STP y se sigue necesitando conexión mediante trunking a la capa de acceso si hay múltiples VLAN y subredes IP. Para esto, verifique VLAN 1 desde los puertos de trunk.

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 sucede incluso si VLAN 1 se borra de los trunks y no es la VLAN nativa. Si la VLAN 1 se borra para los datos del usuario, el tráfico del plano de control que todavía se envía por la VLAN 1 no se ve afectado.
- En un trunk ISL, los paquetes DTP se envían a través de VLAN1. Esto sucede incluso si VLAN 1 se borra del trunk y ya no es la VLAN nativa. En un trunk 802.1q, los paquetes DTP se envían a través de la VLAN nativa. Esto sucede incluso si la VLAN nativa se borra del trunk.
- En PVST+, las **BPDU de 802.1Q IEEE** se reenvían sin etiquetar por Spanning Tree VLAN 1 común para la interoperabilidad con otros proveedores, a menos que la VLAN 1 se borre 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. Consulte la sección Spanning-Tree Protocol en este documento 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 la VLAN 1 se borra de los trunks.
- No borre ni inhabilite VLAN 1 en los trunks entre los bridges MST y los bridges PVST+. De todos modos, si VLAN 1 se inhabilita, el bridge MST debe convertirse en root para que todas las VLAN eviten el bridge MST que pone sus puertos del límite en el estado root-inconsistent. Consulte Comprensión de Multiple Spanning Tree Protocol (802.1s)para conocer los detalles.

Recomendaciones

Para mantener una VLAN en un **estado de encendido/encendido** sin clientes ni hosts conectados en esa VLAN, usted debe tener por lo menos un dispositivo físico conectado en esa VLAN. De lo contrario, la VLAN tiene un **estado de encendido/apagado**. Actualmente, no hay ningún comando para poner una interfaz VLAN en estado de **encendido/encendido** cuando no hay puertos activos en el switch para esa VLAN.

Si usted no quiere conectar un dispositivo, conecte un cable de loopback en cualquier puerto para esa VLAN. De manera alternativa, intente con un cable crossover que conecte dos puertos en esa VLAN en el mismo switch. Este método hace que se encienda el puerto. Consulte la sección Cable de Loopback de Pruebas de Loopback para las Líneas T1/56K para obtener más información.

Cuando una red se conecta directamente a varios proveedores de servicio, la red funciona como red intermedia entre dos proveedores de servicio. Si el número de VLAN recibido en un paquete debe ser traducido o modificado cuando pasa de un proveedor de servicio a otro proveedor de servicio, es recomendable utilizar la función QinQ para traducirlo.

VLAN Trunking Protocol

Antes de que crear las VLAN, determine el modo de VTP que se utilizará en la red. VTP permite que los cambios de configuración de VLAN se realicen centralmente en uno o más switches. Todos esos cambios se distribuyen automáticamente a todos los otros switches en el dominio.

Información Operativa General

El VTP es un protocolo de mensajería L2 que mantiene la consistencia de la configuración de VLAN. El VTP administra la adición, la eliminación y la retitulación de las VLAN en toda la red. VTP minimiza los errores y las inconsistencias de configuración que pueden provocar una cantidad de problemas, tales como nombres de VLAN duplicados, especificaciones incorrectas del tipo de VLAN y violaciones de seguridad. La base de datos de la VLAN es un archivo binario y se almacena en la NVRAM en servidores VTP de forma separada al archivo de configuración.

El protocolo VTP se comunica entre switches por medio de una dirección MAC de multicast de destino Ethernet (**01-00-0c-cc-cc-cc**) y el protocolo SNAP HDLC tipo Ox2003. No funciona en puertos sin trunks (el VTP es un contenido de ISL o de 802.1Q), así que los mensajes no pueden ser enviados hasta que DTP haya puesto el trunk en línea.

Los tipos de mensaje incluyen anuncios de resumen cada cinco minutos, anuncios de subconjunto y anuncios de solicitud cuando hay cambios, y uniones cuando el recorte de VTP se encuentra habilitado. El número de revisiones de la configuración VTP se incrementa de uno en uno con cada cambio en un servidor, que a su vez propaga la nueva tabla en todo el dominio.

Si se elimina una VLAN, los puertos que alguna vez fueron miembros de esa VLAN se colocan en estado de inactividad. De manera similar, si un switch en modo de cliente no puede recibir la tabla de VLAN VTP en el inicio (desde un servidor VTP o desde otro cliente VTP), se desactivan todos los puertos en las VLAN, salvo la VLAN 1 predeterminada.

En esta tabla se comparan en forma resumida las funciones de diversos modos VTP:

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

En el modo transparente de VTP, se ignoran las actualizaciones de VTP (la dirección MAC de multicast VTP se quita de la CAM del sistema que se utiliza normalmente para tomar las tramas de control y para dirigirlas a la Supervisor Engine). Puesto que el protocolo utiliza a una dirección multicast, un switch en modo transparente (u otro switch de proveedor) inunda simplemente la trama a otros switches Cisco en el dominio.

[1] versión de software CatOS 7.1 introduce la opción para inhabilitar el VTP con el uso del `modo desconectado`. En el modo apagado de VTP, el switch se comporta de una manera muy similar al modo transparente de VTP, solo que el modo apagado también omite el reenvío de las actualizaciones de VTP.

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
Contraseña VTP	Ninguno
Recorte VTP	Inhabilitado

La versión 2 de VTP(VTPv2) incluye esta flexibilidad funcional. Sin embargo, no es interoperable con la versión 1 de VTP (VTPv1):

- Soporte Token Ring
- Soporte de información de VTP no reconocido; los switches ahora propagan los valores que no pueden analizar.
- modo transparente que depende de la versión; el modo transparente ya no verifica el nombre de dominio. 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 todos los switches, todos se pueden habilitar mediante la configuración de un un solo switch.

Consulte Comprensión y Configuración de VLAN Trunk Protocol (VTP) para obtener más información.

Versión 3 de VTP

La versión del software CatOS 8.1 introduce el soporte para la versión 3 de VTP (VTPv3). El VTPv3 es una versión mejorada de las versiones existentes. Ofrece mejoras que permiten lo siguiente:

- soporte para VLAN extendidas;
- soporte para la creación y la publicación de VLAN privadas;
- soporte para instancias de VLAN y para instancias de propagación de mapping de MST (admitidas en la versión 8.3 de CatOS);
- autenticación de servidor mejorada;
- protección contra la inserción accidental de la base de datos “incorrecta” en un dominio VTP;
- interacción con el VTPv1 y el VTPv2;
- la capacidad de ser configurado por puerto.

Una de las principales diferencias entre la implementación de VTPv3 y la implementación de la versión anterior es la introducción de un servidor primario VTP. Lo ideal es que haya solamente un servidor primario en un dominio VTPv3, si el dominio no se divide. Todos los cambios que realice en el dominio VTP se deben ejecutar en el servidor primario VTP para que se propaguen al dominio VTP. Puede haber múltiples servidores dentro de un dominio VTPv3, que también se conocen como servidores secundarios. Cuando un switch se configura para que sea un servidor, el switch se convierte en servidor secundario de forma predeterminada. El servidor secundario puede guardar la configuración del dominio, pero no puede modificar la configuración. Un servidor secundario puede convertirse en el servidor primario con una toma de mando exitosa del switch.

Los switches que ejecutan VTPv3 solamente aceptan bases de datos VTP con un número de revisión más alto que el del servidor primario actual. Este proceso difiere considerablemente del VTPv1 y del VTPv2, en los cuales un switch siempre acepta una configuración superior de un vecino en el mismo dominio. Este cambio con el VTPv3 ofrece protección. Un switch nuevo que se introduce en la red con un número de revisión VTP más alto no puede sobrescribir la configuración de VLAN del dominio entero.

VTPv3 también introduce una mejora en el modo en que VTP maneja las contraseñas. Si usted utiliza la opción de configuración de contraseña oculta para configurar una contraseña como “oculta”, sucede lo siguiente:

- La contraseña no aparece en texto sin formato en la configuración. El formato hexadecimal secreto de la contraseña se guarda en la configuración.
- Si intenta configurar el switch como servidor primario, se le pedirá la contraseña. Si su contraseña coincide con la contraseña secreta, el switch se convierte en un servidor primario, lo que le permite configurar el dominio.

Nota: Es importante observar que el servidor primario solamente es necesario cuando usted debe modificar la configuración de VTP para alguna instancia. Un dominio VTP puede funcionar sin ningún servidor primario activo porque los servidores secundarios aseguran la persistencia de la configuración durante recargas. El servidor primario sale de su estado por estas razones:

- Una recarga de switch.
- Un switchover de alta disponibilidad entre la supervisor engine activa y la supervisor engine redundante.
- Una toma de control de otro servidor.
- Un cambio en la configuración del modo.
- Un cambio en la configuración del dominio VTP, como un cambio en lo siguiente:VersiónNombre de dominioContraseña de dominio

VTPv3 también permite que los switches participen en múltiples instancias VTP. En este caso, el mismo switch puede ser el servidor VTP para una instancia y un cliente para otra instancia porque los modos VTP son específicos de diferentes instancias VTP. Por ejemplo, un switch puede funcionar en modo transparente para una instancia MST y estar configurado en modo de servidor para una instancia VLAN.

En términos de interacción con VTPv1 y VTPv2, el comportamiento predeterminado en todas las versiones de VTP ha sido que las versiones anteriores de VTP simplemente descarten las actualizaciones de la nueva versión. A menos que los switches VTPv1 y VTPv2 estén en modo transparente, todas las actualizaciones de VTPv3 se descartan. Por otra parte, después de que los switches VTPv3 reciben una trama de VTPv1 o VTPv2 heredada en un trunk, los switches pasan una versión reducida de la actualización de su base de datos a los switches VTPv1 y VTPv2. Sin embargo, este intercambio de información es unidireccional, ya que los switches

VTPv3 no aceptan ninguna actualización de los switches VTPv1 y VTPv2. En las conexiones de trunk, los switches VTPv3 continúan enviando actualizaciones reducidas, así como actualizaciones VTPv3 totalmente desarrolladas que sirven a los vecinos VTPv2 y VTPv3 en los puertos de trunk.

A fin de proporcionar soporte de VTPv3 a VLAN extendidas, se cambia el formato de la base de datos de VLAN, en la cual VTP asigna 70 bytes por VLAN. Este cambio permite codificar los valores no predeterminados solamente, en lugar de transportar campos sin modificar para los protocolos heredados. Debido a este cambio, un soporte VLAN de 4K es el tamaño de la base de datos de VLAN resultante.

Recomendación

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 de VTP a pesar de algunas consideraciones mencionadas más adelante. Se recomienda tener dos switches en modo de servidor en cada dominio para redundancia, normalmente los dos switches de capa de distribución. El resto de los switches en el dominio se debe configurar en modo de cliente. Cuando usted implementa el modo cliente/servidor con el uso de VTPv2, tenga presente que siempre se acepta un número de revisión más alto en el mismo dominio VTP. Si un switch que está configurado en modo de cliente o en modo de servidor de VTP se introduce en el dominio VTP y tiene un número de revisión más alto que los servidores VTP existentes, este sobrescribe la base de datos de VLAN dentro del dominio VTP. Si el cambio en la configuración es involuntario y las VLAN se eliminan, la sobrescritura puede causar una interrupción importante en la red. Para asegurarse de que los switches de cliente o de servidor siempre tengan un número de revisión de la configuración más bajo que el del servidor, cambie el nombre de dominio de VTP cliente por uno que no sea el nombre estándar. Luego, vuelva a usar el 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 el método cauteloso de modo transparente de VTP por estas razones:

- Fomenta una buena práctica de control de cambios, pues el requisito para modificar una VLAN en un switch o en un puerto trunk tiene que ser considerado en un switch por vez.
- Limita el riesgo de que se produzca un error del administrador que afecte el dominio entero, tal como la eliminación accidental de una VLAN.
- No implica el riesgo de que un nuevo switch introducido en la red con un número de revisión de VTP más alto pueda sobrescribir la configuración de VLAN del dominio entero.
- Fomenta que las VLAN sean recortadas de los trunks que se ejecutan a los switches que no tienen puertos en esa VLAN. Esto hace que la inundación de tramas sea más eficiente en relación con el ancho de banda. El recorte manual también es beneficioso porque reduce al diámetro del spanning tree (consulte la sección DTP de este documento). Antes del recorte de VLAN no utilizadas en trunks de canales de puertos, asegúrese de que los puertos conectados con teléfonos IP estén configurados como puertos de acceso con VLAN de voz.
- El rango de VLAN extendida en CatOS 6.x y en CatOS 7.x, números de 1025 a 4094, se puede configurar solamente de esta manera. Para más información, consulte Reducción de Dirección MAC y VLAN Extendida de este documento.
- El modo transparente de VTP es compatible en Campus Manager 3.1, parte de Cisco Works 2000. Se ha eliminado la vieja restricción mediante la cual se exigía al menos un servidor en

un dominio VTP.

Ejemplos de Comandos de VTP	Comentarios
set vtp domain name password x	El CDP verifica los nombres para ayudar a determinar si hay error en la conexión entre los dominios. El mero uso de una contraseña sirve para prevenir cambios involuntarios. Tenga cuidado con la mayúsculas y minúsculas en los nombres y con los espacios al copiar y pegar.
set vtp mode transparent	
set vlan vlan number name name	Por cada switch que tiene puertos en la VLAN.
set trunk mod/port vlan range	Habilita trunks para que transporten VLAN cuando sea necesario; el valor predeterminado es todas las VLAN.
clear trunk mod/port *vlan range*	Limita al diámetro de STP por el recorte manual, por ejemplo en trunks de la capa de distribución a la capa de acceso, si la VLAN no existe.

Nota: Si se especifican VLAN con el **comando set** solo se agregan VLAN, pero no se borran. Por ejemplo, el comando set trunk x/y 1-10 no configura la lista permitida en apenas VLAN de 1-10. Ejecute el comando clear trunk x/y 11-1005 para alcanzar el resultado deseado.

Aunque la función Token Ring Switching no se trata en este documento, observe que el modo transparente de VTP no se recomienda para las redes TR-ISL. La base para token ring switching es que la totalidad del dominio forme un solo bridge de puertos múltiples distribuido, así que cada switch debe tener la misma información de VLAN.

Otras Opciones

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

VTPv3 ofrece la posibilidad de implementar un control más riguroso de la autenticación y de la revisión de la configuración. En esencia, VTPv3 proporciona el mismo nivel de funciones, pero con una seguridad mejor que la que ofrece el modo transparente de VTPv1/VTPv2. Además, VTPv3 es parcialmente compatible con las versiones de VTP heredadas.

En este documento se exponen los beneficios del recorte de VLAN para reducir la inundación de tramas innecesaria. El comando set vtp pruning enable recorta las VLAN automáticamente, lo que detiene la inundación de tramas ineficaz cuando no es necesaria. A diferencia del recorte manual de VLAN, el recorte automático no limita al diámetro del Spanning Tree.

A partir de CatOS 5.1, los switches Catalyst pueden asociar los números 802.1Q VLAN mayores de 1000 con los números ISL VLAN. En CatOS 6.x, los switches Catalyst 6500/6000 admiten VLAN 4096 de acuerdo con el estándar IEEE 802.1Q. Estas VLAN se organizan en estos tres rangos, solo algunos de ellos se propagan a otros switches en la red con VTP:

- VLAN de normal rango: 1-1001
- VLAN de rango extendido: 1025-4094 (puede ser propagadas solamente por VTPv3)
- VLAN de rango reservado: 0, 1002-1024, 4095

El estándar IEEE ha producido una arquitectura basada en estándares para lograr resultados similares como VTP. Como miembro de 802.1Q Generic Attribute Registration Protocol (GARP), el protocolo Generic VLAN Registration Protocol (GVRP)permite la interoperabilidad de la administración de VLAN entre proveedores, pero no es un tema que se trata en este documento.

Nota: CatOS 7.x introduce la opción de configurar VTP en modo apagado, un modo muy similar a transparente. Sin embargo, el switch no reenvía tramas VTP. Esto puede ser útil en algunos diseños al conectar mediante trunking a los switches fuera de su control administrativo.

VLAN Extendida y Reducción de Dirección MAC

La función de reducción de direcciones MAC habilita la identificación de VLAN de rango extendido. Al habilitar la reducción de la dirección MAC, se inhabilita el conjunto de direcciones MAC que se utilizan para VLAN spanning tree y deja una sola dirección MAC. Esta dirección MAC identifica el switch. La versión del software CatOS 6.1(1) introduce la función de reducción de direcciones MAC para que los switches Catalyst 6500/6000 y Catalyst 4500/4000 VLAN 4096 de acuerdo con el estándar IEEE 802.1Q.

Descripción General de Funcionamiento

Los protocolos de switches utilizan una dirección MAC tomada de un banco de direcciones disponibles que un EPROM en el chasis proporciona como parte de los identificadores de bridge para VLAN que se ejecutan con PVST+. Los switches Catalyst 6500/6000 y Catalyst 4500/4000 admiten direcciones MAC 1024 o 64, esto depende del tipo de chasis.

Los switches Catalyst con direcciones MAC 1024 no habilitan la reducción de direcciones MAC de forma predeterminada. Los direcciones MAC se asignan en secuencia. La primera dirección MAC del rango se asigna a la VLAN 1. La segunda dirección MAC del rango se asigna a la VLAN 2, y

así sucesivamente. Esto hace que los switches puedan admitir VLAN 1024 con cada VLAN usando 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] reducción de la dirección MAC se habilita por abandono para el Switches que tiene 64 direcciones MAC, y la característica no puede ser inhabilitada.

Para los switches Catalyst con direcciones MAC 1024, la habilitación de la reducción de direcciones MAC permite que las VLAN 4096 que se ejecutan con PVST+ o con 16 instancias de Multiple Instance STP (MISTP) tengan identificadores únicos sin un aumento en el número de direcciones MAC necesarias en el switch. La reducción de direcciones MAC reduce el número de direcciones MAC que necesita STP de una por instancia de VLAN o MISTP a una por switch.

Esta figura muestra que la reducción del direcciones MAC de identificador de bridge no está habilitada. El identificador de bridge consiste en una prioridad de bridge de 2 bytes y una dirección MAC de 6 bytes:

La reducción de direcciones MAC modifica la parte del identificador de bridge STP de la BPDU. El campo de prioridad original de 2 bytes se divide en dos campos. Esta división da lugar a un campo de prioridad de bridge de 4 bits y a una extensión del ID del sistema de 12 bits que permite la enumeración de VLAN de 0 a 4095.

Cuando la función de reducción de direcciones MAC está habilitada en los switches Catalyst para aprovechar VLAN de rango extendido, habilite la reducción de direcciones MAC en todos los switches dentro del mismo dominio STP. Este paso es necesario para mantener la uniformidad de los cálculos de raíz STP en todos los switches. Después de que habilite la reducción de direcciones MAC, la prioridad de root bridge se convierte en un múltiplo de 4096 más el ID de VLAN. Los switches sin la reducción de direcciones MAC pueden asegurar ser la raíz sin querer porque tienen mayor precisión en la selección del ID del bridge.

Pautas de Configuración

Usted debe seguir ciertas pautas cuando configura una VLAN de rango extendido. El switch puede asignar un bloque de VLAN del rango extendido para fines internos. Por ejemplo, el switch puede asignar las VLAN para los puertos ruteados o para los módulos FlexWAN. La asignación del bloque de VLAN siempre empieza a partir de VLAN 1006 y luego aumenta. Si tiene alguna VLAN dentro del rango que el módulo FlexWAN requiere, no se asignan todas las VLAN requeridas porque estas nunca se asignan desde el área de VLAN del usuario. Ejecute el comando show vlan o el comando show vlan summary en un switch para visualizar las VLAN asignadas por el usuario y las VLAN internas.

```
>show vlan summary

Current Internal Vlan Allocation Policy - Ascending

Vlan status    Count  Vlans
-------------  -----  -----------------------------------------
VTP Active         7   1,17,174,1002-1005

Internal           7   1006-1011,1016
!--- These are internal VLANs. >show vlan
---- -------------------------------- --------- ------- --------

1    default                          active    7       4/1-48


!--- Output suppressed. 1006 Online Diagnostic Vlan1 active 0 internal 1007 Online Diagnostic
Vlan2 active 0 internal 1008 Online Diagnostic Vlan3 active 0 internal 1009 Voice Internal Vlan
active 0 internal 1010 Dtp Vlan active 0 internal 1011 Private Vlan Internal Vlan suspend 0
internal 1016 Online SP-RP Ping Vlan active 0 internal !--- These are internal VLANs.
```

Además, antes de usar las VLAN de rango extendido, debe eliminar cualquier mapping 802.1Q-to-ISL existente. Asimismo, en las versiones anteriores a VTPv3, debe configurar estáticamente la VLAN extendida en cada switch con el uso del modo transparente de VTP. Consulte la sección *Pautas de Configuración de VLAN de Rango Extendido* de Configuración de VLAN para obtener más información.

Nota: En las versiones de software anteriores a la versión 8.1(1), usted no puede configurar el nombre de VLAN para las VLAN de rango extendido. Esta capacidad es independiente de cualquier versión o modo de VTP.

Recomendación

Intente mantener una configuración de reducción de direcciones MAC constante dentro del mismo dominio STP. Sin embargo, la aplicación de la reducción de direcciones MAC en todos los dispositivos de red puede ser poco práctica cuando se introducen nuevos chasis con direcciones MAC 64 en el dominio STP. La función de reducción de direcciones MAC se habilita de forma predeterminada para los switches que tienen direcciones MAC 64 y no se puede inhabilitar. Entienda que, cuando dos sistemas se configuran con la misma prioridad de spanning-tree, el sistema sin reducción de direcciones MAC tiene una mejor prioridad de spanning-tree. Ejecute este comando para habilitar o inhabilitar la reducción de direcciones MAC:

```
set spantree macreduction enable | disable
```

La asignación de VLAN internas se realiza en orden ascendente y comienza a partir de VLAN 1006. Asigne las VLAN del usuario lo más cercano posible a VLAN 4094 para evitar conflictos entre las VLAN del usuario y las VLAN internas. Con los switches Catalyst 6500 que ejecutan el software del sistema IOS® de Cisco, usted puede configurar la asignación de VLAN interna en orden descendente. El equivalente de Interfaz de Línea de Comandos (CLI) para el software CatOS no es admitido oficialmente.

Autonegotiation

Ethernet/Fast Ethernet

La negociación automática es una función opcional del estándar Fast Ethernet IEEE 802.3u que les permite a los dispositivos intercambiar, automáticamente y a través de un link, información

sobre su **velocidad y dúplex**. La negociación automática funciona en la capa 1 (L1) y se dirige a los puertos de capa de acceso mediante los cuales los **usuarios transitorios**, como las PC, se conectan con la red.

Información Operativa General

La mayoría de las veces, los problemas de rendimiento en los links Ethernet de 10/100 Mbps ocurren cuando un puerto en el link funciona en modo duplex medio mientras que el otro funciona en modo dúplex completo. En ocasiones, esto sucede cuando cuando uno o ambos puertos en un link se restablecen y el proceso de negociación automática no hace que ambos partners de link tengan la misma configuración. También sucede cuando los usuarios vuelven a configurar solo un lado de un link y se olvidan de volver a configurar el otro lado. Los síntomas habituales de esto son aumento de la secuencia de verificación de trama (FCS), verificación de redundancia cíclica (CRC), alineación o contadores de tramas cortas en el switch.

Los siguientes documentos abordan la negociación automática en más profundidad. Estos documentos incluyen explicaciones del funcionamiento de la negociación automática y opciones de configuración.

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

Un concepto erróneo común sobre la negociación automática es que es posible configurar manualmente un partner de link en el modo dúplex completo de 100 Mbps y negociar automáticamente el modo dúplex completo para el otro partner de link. De hecho, si se intenta hacer esto, se obtienen modos dúplex desiguales. Esto es consecuencia de la negociación automática de un partner de link que no tiene en cuenta ningún parámetro de negociación automática del otro partner de link y que se configura en modo dúplex medio de forma predeterminada.

La mayoría de los módulos Catalyst Ethernet admiten 10/100 Mbps y dúplex medio/completo, pero el ***comando show port capabilities mod/port*** confirma esto.

FEFI

La indicación de falla en el extremo remoto (FEFI) protege las interfaces Gigabit y 100BASE-FX (fibra), mientras que la negociación automática protege a 100BASE-TX (cobre) contra las fallas relacionadas con capa física/señalización.

Una falla en el extremo remoto es un error en el link que una estación puede detectar mientras que la otra no; por ejemplo, un cable TX desconectado. En este ejemplo, la estación remitente podría todavía recibir datos válidos y detectar que el link es bueno a través del control de la integridad de los links. No detecta que su transmisión no está siendo recibida por la otra estación. Una estación 100BASE-FX que detecta una falla remota de este tipo puede modificar su flujo IDLE transmitido para enviar un patrón de bit especial (conocido como patrón FEFI IDLE) a fin de informar al vecino la falla remota; el patrón FEFI-IDLE apaga posteriormente el puerto remoto (errdisable). Consulte la sección UDLD de este documento para obtener más información sobre la protección contra fallas.

FEFI es compatible con este hardware y estos módulos:

- Catalyst 5500/5000: WS-X5201R, WS-X5305, WS-X5236, WS-X5237, WS-U5538 y WS-U5539
- Catalyst 6500/6000 y 4500/4000: Todos los módulos 100BASE-FX y módulos GE

Recomendación

Decidir si configurar la negociación automática en links 10/100 o si utilizar valores fijos (hard code) para la velocidad y el estado dúplex directamente depende, en última instancia, del tipo de partner de link o de dispositivo extremo que haya 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, pueden surgir problemas si las tarjetas de interfaz de red o los switches de proveedor no cumplen exactamente con la especificación. Problemas como la incompatibilidad del hardware y de otro tipo pueden también ocurrir como resultado de las funciones avanzadas específicas del proveedor, como polaridad automática o integridad del cableado, que no se describen en la especificación IEEE 802.3u para la negociación automática de 10/100 Mbps. Consulte Notificación: Problema de Rendimiento con Tarjetas de Interfaz de Red Intel Pro/1000T que se conectan con CAT4K/6K para obtener un ejemplo de este problema.

Sepa que habrá algunas situaciones que le exigirán configurar host, velocidad de puerto y dúplex. En general, siga estos pasos básicos de troubleshooting:

- Asegúrese de que la negociación automática o la utilización de valores fijos en un programa (hard coding) esté configurada en ambos lados del link.
- Revise las notas de la versión de CatOS para estar al tanto de las advertencias comunes.
- Verifique la versión del driver de tarjeta de interfaz de red o del sistema operativo que esté ejecutando, ya que suele necesitarse el último driver o parche.

Como regla, intente utilizar la negociación automática en primer lugar para cualquier tipo de partner de link. La configuración de la negociación automática para dispositivos transitorios, como laptops, ofrece beneficios evidentes. Se espera que la negociación automática también funcione bien con dispositivos no transitorios, como servidores y estaciones de trabajo fijas, o de switch a switch y de switch a router. Por algunas de las razones antes mencionadas, pueden surgir problemas con la negociación. De ser así, siga los pasos básicos de troubleshooting descritos en los links TAC proporcionados.

Si la velocidad de puerto se configura en auto en puerto Ethernet de 10/100 Mbps, tanto la velocidad como el dúplex se negocian automáticamente. Ejecute este comando para configurar el puerto en auto:

```
set port speed port range auto
!--- This is the default.
```

Si utiliza valores fijos en un programa (hard coding) para el puerto, ejecute estos comandos de configuración:

```
set port speed port range 10 | 100 set port duplex port range full | half
```

En CatOS 8.3 y posteriores, Cisco ha introducido la palabra clave **auto-10-100** opcional. Utilice la palabra clave **auto-10-100** en los puertos que admiten velocidades de 10/100/1000 Mbps, pero si no se desea la negociación automática a 1000 Mbps. El uso de la palabra clave **auto-10-100** hace que el puerto se comporte de la misma forma que un puerto de 10/100-Mbps con la velocidad configurada en **auto**. La velocidad y el dúplex se negocian para los puertos de 10/100-Mbps

solamente, y la velocidad de 1000-Mbps no participa en la negociación.

```
set port speed port_range auto-10-100
```

Otras Opciones

Cuando no se utiliza ninguna negociación automática entre los switches, la indicación de falla L1 también se puede perder debido a ciertos problemas. Resulta útil utilizar los protocolos L2 para aumentar la detección de fallas, como UDLD agresiva.

Ethernet de Gigabites

Ethernet de Gigabits (GE) tiene un procedimiento de negociación automática (IEEE 802.3Z) más extenso que el de Ethernet de 10/100 Mbps y se utiliza para intercambiar parámetros de control de flujo, información sobre fallas remotas e información sobre dúplex (aunque los puertos GE de las series Catalyst solamente admiten el modo dúplex completo).

Nota: El estándar 802.3z ha sido reemplazado por las especificaciones IEEE 802.3:2000. Consulte Suscripción En Línea a los Estándares LAN/MAN del IEEE: Archivos para más información.

Información Operativa General

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. A diferencia de FE, el link GE no funciona si la configuración de la negociación automática no es la misma en los puertos en cada extremo del link. Sin embargo, la única condición que se debe cumplir para que el link de un puerto con negociación automática inhabilitada funcione es una señal de Gigabit válida del extremo remoto. Este comportamiento es independiente de la configuración de la negociación automática del extremo remoto. Por ejemplo, suponga que hay dos dispositivos, A y B. Cada dispositivo puede tener la función de negociación automática habilitada o inhabilitada. En esta tabla se incluyen las posibles configuraciones y los estados de sus respectivos links:

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 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 durante 10 ms, se confirma la

condición "falla en la sincronización" y el link pasa al estado 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 se inhabilita la negociación automática en un puerto, la fase "autoneg" deja de ser una opción.

La especificación para puertos de cobre GE (1000BASE-T) admite la negociación automática a través de Next Page Exchange. Next Page Exchange permite la negociación automática para las velocidades de 10/100/1000-Mbps en puertos de cobre.

Nota: La especificación para puertos de fibra GE solamente incluye disposiciones para la negociación de dúplex, control de flujo y detección de fallas remotas. 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 set port sync-restart-delay solamente funciona cuando la negociación automática está configurada en enable.

Recomendación

La habilitación de la negociación automática es mucho más importante en un entorno GE que en entorno de 10/100. De hecho, la negociación automática se debe inhabilitar solamente en los puertos del switch que se conectan a dispositivos incapaces de admitir la negociación o si surgen problemas de conectividad a partir de problemas de interoperabilidad. Cisco recomienda habilitar la negociación Gigabit (opción predeterminada) en todos los links entre switches y generalmente todos los dispositivos GE. Ejecute este comando para habilitar la negociación automática:

```
set port negotiation port range enable
!--- This is the default.
```

Una excepción conocida es cuando hay una conexión a un Gigabit Switch Router (GSR) con una versión de Cisco IOS Software anterior a la versión 12.0(10)S, la versión que incorporó el control de flujo y la negociación automática. En este caso, inhabilite esas dos funciones o el puerto del switch se informará como no conectado y GSR informará errores. Esta es una secuencia de comandos de ejemplo:

```
set port flowcontrol receive port range off set port flowcontrol send port range off set port
negotiation port range disable
```

Las conexiones de switch a servidor deben revisarse de a un caso por vez. Los clientes de Cisco se han encontrado con problemas en la negociación de Gigabit respecto de los servidores Sun, HP e IBM.

Otras Opciones

El control de flujo es una parte opcional de la especificación 802.3x y debe ser negociado en caso de ser utilizado. Los dispositivos pueden o no pueden ser capaces de enviar o responder una trama PAUSE (**MAC conocido 01-80-C2-00-00-00 0F**). Además, no pueden aceptar la solicitud de control de flujo del vecino en el extremo remoto. Un puerto con un buffer de entrada que se llena envía una trama PAUSE a su partner de link, lo que detiene la transmisión, y contiene las tramas adicionales en los buffers de salida del partner de link. Esto no soluciona ningún problema de suscripciones excesivas en estado estable, pero aumenta eficazmente el tamaño del buffer de entrada en alguna fracción del buffer de salida del partner durante bursts.

Se recomienda usar esta función en los links entre los puertos de acceso y los hosts extremos, cuando el buffer de salida de host tenga posiblemente el mismo tamaño que su memoria virtual. El uso switch-a-switch tiene ventajas limitadas.

Ejecute estos comandos para controlar esto en los puertos del switch:

```
set port flowcontrol mod/port 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, WS-X4306) nunca envían las tramas PAUSEincluso si negocian esta función, ya que son módulos de no bloqueo.

Dynamic Trunking Protocol

Tipo de Encapsulación

Los trunks extienden las VLAN entre los dispositivos mediante la identificación y el etiquetado temporales (link-local) de las tramas Ethernet originales y, de esta manera, las habilitan para su multiplexación en un solo link. Esto también asegura que la transmisión VLAN separada y los dominios de seguridad se mantengan entre los switches. Las tablas CAM mantienen el mapping de trama a VLAN dentro de los switches.

Varios tipos de medios L2, incluidos LANE ATM, FDDI 802.10 y Ethernet, admiten la función trunking, pero Ethernet es el único que se presenta en este documento.

Descripción General sobre el Funcionamiento de ISL

Durante muchos años se ha usado el esquema de identificación o etiquetado propiedad de Cisco: ISL. El estándar IEEE 802.1Q también está disponible.

Mediante la encapsulación total de la trama original en un esquema de etiquetado de dos niveles, ISL es un protocolo de tunelización eficaz y ofrece el beneficio adicional de transportar tramas que no son Ethernet. Añade una cabecera de 26 bytes y una FCS de 4 bytes a la trama Ethernet estándar; las tramas Ethernet más grandes son esperadas y manejadas por los puertos

configurados para ser trunks. ISL admite 1024 VLAN.

Formato de Tramas ISL

40 bits	4 bits	4 bits	48 bits	16 bits	24 Bits	24 Bits	15 Bits	Bit	16 bits	16 bits	Longitud variable	32 bits
Dest. Addr	Tipo	USUARIO	SA	LARGO	SNAPLLC	HSA	VLAN	BPDU	ÍNDICE	Reserva	Trama Encapsulada	FCS
01-00-0c-00-00					AAAA03	000 00C						

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

Descripción General sobre el Funcionamiento de 802.1Q

El estándar IEEE 802.1Q incluye muchas más especificaciones aparte de las relativas a los tipos de encapsulación, entre las que se incluyen mejoras de Spanning Tree, GARP (consulte la sección VTP de este documento) y etiquetado de Calidad de Servicio (QoS) 802.1p.

El formato de trama 802.1Q preserva la dirección de origen y la dirección de destino de Ethernet originales, aún así los switches deben esperar recibir tramas del tipo baby giant (un poco más grandes que las permitidas por IEEE Ethernet), incluso en los puertos de acceso en los que los hosts pueden utilizar etiquetado para expresar la prioridad de usuario 802.1p para la señalización de QoS. La etiqueta es de 4 bytes, así que las tramas de v2 de Ethernet 802.1Q son de 1522 bytes, un logro del grupo de trabajo de IEEE 802.3ac. 802.1Q también admite el espacio de numeración para VLAN 4096.

Todas las tramas de datos transmitida y recibidas son etiquetadas por 802.1Q, salvo aquellas en la VLAN nativa (hay una etiqueta implícita basada en la configuración del puerto del switch de ingreso). Las tramas en la VLAN nativa siempre se transmiten sin etiquetar y normalmente se reciben sin etiquetar. Sin embargo, también pueden ser recibidas etiquetadas.

Consulte Estandarización de VLAN mediante IEEE 802.10 y Obtención de IEEE 802para conocer más detalles.

Formato de Tramas 802.1Q/801.1p

		Encabezado de Etiqueta						
		TPID	TCI					
48 bit	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Longitud	32 bits

s							variable	
DA	SA	**TPID**	Prioridad	**CFI**	**ID DE VLAN**	Longitud/ Tipo	Datos con PAD	FCS
		0x8100	**0-7**	**0-1**	**0-4095**			

Recomendación

Como todos los componentes de hardware más nuevos son compatibles con 802.1Q (y algunos son compatibles con 802.1Q solamente, como las series Catalyst 4500/4000 y CSS 11000), Cisco recomienda que todas las nuevas implementaciones cumplan con el estándar IEEE 802.1Q y que las redes más viejas emigren gradualmente de ISL.

El estándar IEEE permite la interoperabilidad entre proveedores. Esto resulta beneficioso para todos los entornos de Cisco porque nuevos dispositivos y tarjetas de interfaz de red compatibles con 802.1p de host se encuentran disponibles. Pese a que las implementaciones de ISL y de 802.1Q son experimentadas, el estándar IEEE tendrá en última instancia mayor exposición en el campo y mayor soporte de proveedores externos, tal como el soporte de analizador de red. La menor sobrecarga de encapsulación de 802.1Q en comparación con ISL es un beneficio mínimo también a favor de 802.1Q.

Como el tipo de encapsulación se negocia entre los switches mediante DTP, con ISL elegido como ganador de forma predeterminada si ambos extremos son compatibles con él, resulta necesario ejecutar este comando para especificar dot1q:

```
set trunk mod/port mode dot1q
```

Si VLAN 1 se borra de un trunk, como se trató en la sección Administración En Banda de este documento, aunque no se transmitan ni se reciban datos del usuario, NMP continúa pasando protocolos de control, tales como CDP y VTP, por la VLAN 1.

Además, como se analizó en la sección VLAN 1 de este documento, los paquetes CDP, VTP y PAgP siempre se envían en la VLAN 1 en la conexión mediante trunking. Al usar la encapsulación dot1q, estas tramas de control se etiquetan con VLAN 1 si la VLAN nativa del switch se cambia. Si la conexión mediante trunking dot1q a un router se habilita y la VLAN nativa se cambia en el switch, una subinterfaz en la VLAN 1 es necesaria para recibir las tramas CDP etiquetadas y proporcionar visibilidad de vecinos CDP en el router.

Nota: Hay una consideración de seguridad potencial con dot1q causada por el etiquetado implícito de la VLAN nativa, pues puede ser posible enviar tramas de una VLAN a otra sin un router. Consulte ¿Hay Vulnerabilidades en las Implementaciones de VLAN? para conocer más detalles. La solución temporal es utilizar un ID de VLAN para la VLAN nativa del trunk que no se utiliza para el acceso del usuario final. La mayoría de los clientes de Cisco deja la VLAN 1 como la VLAN nativa en un trunk y asigna los puertos de acceso a las otras VLAN (menos VLAN 1) para lograr esto fácilmente

Modo Trunking

El DTP es la segunda generación de Dynamic ISL (DISL) y existe para asegurarse de que los diferentes parámetros que participan en el envío de tramas ISL o 802.1Q, tales como el tipo de encapsulación configurado, la VLAN nativa y la capacidad del hardware, sean convenidos por los switches en ambos extremos de un trunk. Esto también ayuda a proteger contra inundaciones de puertos no troncales en tramas con etiquetas, un riesgo de seguridad posiblemente grave, al asegurar que los puertos y sus vecinos se encuentren en estados coherentes.

Información Operativa General

DTP es un protocolo L2 que negocia los parámetros de la configuración entre un puerto del switch y su vecino. Usa otra dirección MAC multicast (**01-00-0c-cc-cc-cc**) y un tipo de protocolo SNAP de 0x2004. En esta tabla se resumen los modos de configuración:

Modo	**Función**	**Tramas DTP Transmitidas**	**Etapa Final (Puerto Local)**
`Automático (predeterminado)`	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, periódicamente.	Trunking
Encendido	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, periódicamente.	Trunking, **sin condiciones**.
`Nonegotiate`	Coloca el puerto en modo trunking permanente, pero evita que el puerto genere tramas DTP. Debe configurar manualmente el puerto de vecindad como un puerto trunk para establecer un link trunk. Esto es útil para dispositivos que no soportan	No	Trunking, **sin condiciones**.

	DTP.		
Deseable	Hace que el puerto 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.	Sí, periódicamente.	Termina en estado trunking solamente si el modo remoto es encendido, automático o deseable.
Desactivado	Pone el puerto en modo no trunking permanente y negocia para convertir el link en un link no trunk. El puerto se transforma en un puerto no trunk incluso en el caso de que el puerto de vecindad no acepte el cambio.	No en estado estable, pero transmite informes para acelerar la detección en extremo remoto después del cambio de encendido.	NON-enlace

Estas son algunos aspectos destacados del protocolo:

- DTP supone una conexión punto a punto, y los dispositivos de Cisco solamente admiten puertos trunk 802.1q que son punto a punto.
- Durante la negociación de DTP, los puertos no participan en STP. Solamente después de que el puerto se convierte en uno de los tres tipos de DTP (access, ISL o 802.1Q), el puerto se añade a STP. Si no, PAgP, si está configurado, es el proceso siguiente que debe ejecutarse antes de que el puerto participe en STP.
- Si el puerto hace conexión mediante trunking en modo ISL, los paquetes DTP se envían por la VLAN 1; de lo contrario, (para los puertos trunking y no trunking 802.1Q) se envían por la VLAN nativa.
- En el modo deseable, los paquetes DTP transfieren el **nombre de dominio** de VTP (que debe corresponder con un trunk negociado para funcionar), además de la configuración del trunk y el **estado del administrador**.
- Los mensajes se envían cada segundo durante la negociación y cada 30 segundos después de ella.
- Asegúrese de comprender que los modos encendido, no negociar y apagado especifican explícitamente el estado en que termina el puerto. Una configuración incorrecta puede generar un estado peligroso/inconsistente en el que un lado es trunking y el otro no.
- Un puerto en modo encendido, automático o deseable envía las tramas DTP periódicamente. Si un puerto en modo automático o deseable no ve un paquete DTP en cinco minutos, se establece en no trunk.

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.

Recomendación

Cisco recomienda una configuración de trunk explícita de deseable en ambos extremos. En este modo, los operadores de la red pueden confiar en los mensajes de estado de syslog y de la línea de comando que informan que un puerto se encuentra en funcionamiento y trunking, a diferencia del modo encendido, que puede hacer que un puerto parezca en funcionamiento incluso si el vecino está mal configurado. Además, el modo deseable proporciona estabilidad en situaciones en las que un lado del link no puede convertirse en trunk o descarta el estado del trunk. Ejecute este comando para configurar el modo deseable:

```
set trunk mod/port desirable ISL | dot1q
```

Nota: Configure al trunk enapagado en todos los puertos no trunk. Esto ayuda a eliminar el tiempo de negociación perdido al encender los puertos host. Este comando también se ejecuta cuando se utiliza el **comando set port host**: Consulte la sección STP para obtener más información. Ejecute este comando para inhabilitar un trunk en un rango de puertos:

```
set trunk port range off
!--- Ports are not trunking; part of the set port host command.
```

Otras Opciones

Otra configuración del cliente común utiliza el modo deseable solamente en la capa de distribución y la configuración predeterminada más simple (modo automático) en la capa de acceso.

Algunos switches (como los Catalyst 2900XL), routers Cisco IOS o dispositivos de otros proveedores no admiten actualmente la negociación de trunk a través de DTP. Usted puede utilizar el modo de no negociación en los switches Catalyst 4500/4000, 5500/5000 y 6500/6000 a fin de configurar un puerto para que se conecte mediante trunking con estos dispositivos incondicionalmente, lo que puede ayudar a estandardizar con una configuración común en el campus. También puede implementar el modo de no negociación para reducir el tiempo de inicialización "total" del link.

Nota: Distintos factores, tales como el modo del canal y la configuración de STP, pueden también afectar el tiempo de inicialización.

Ejecute este comando para configurar el modo de no negociación:

```
set trunk mod/port nonegotiate ISL | dot1q
```

Cisco recomienda el modo de no negociación cuando hay una conexión a un router Cisco IOS porque, cuando se realiza un bridging, algunas tramas DTP recibidas del modo **encendido** pueden regresar al puerto trunk. Tras la recepción de la trama DTP, el puerto del switch intenta renegociar (o encender o apagar el trunk) innecesariamente. Si se habilita el modo de no negociación , el switch no envía tramas DTP.

Spanning Tree Protocol

Consideraciones Básicas

El Spanning-Tree Protocol (STP) mantiene un entorno L2 sin loops en redes conmutadas y puenteadas redundantes. Sin STP, las tramas forman loops o se multiplican indefinidamente, y esto hace que las redes colapsen porque todos los dispositivos en el dominio de broadcast son interrumpidos continuamente por mucho tráfico.

Si bien en algunos aspectos STP es un protocolo experimentado inicialmente desarrollado para especificaciones de puente basado en software lento (IEEE 802.1d), puede resultar difícil su implementación en redes grandes conmutadas con muchas VLAN, muchos switches en un dominio, soporte de varios proveedores y mejoras IEEE más recientes.

Para referencia futura, CatOS 6.x continúa adquiriendo los nuevos desarrollos de STP, tales como MISTP, función de protección contra loops, función de protección de raíz) y función de detección de desviación del tiempo de llegada de BPDU. Además, otros protocolos estandarizados están disponibles en CatOS 7.x, como IEEE 802.1s shared Spanning Tree y IEEE 802.1w rapid convergence Spanning Tree.

Información Operativa General

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, las BPDU se envían de todos los switches, que contienen el BID de cada switch y el costo de la trayectoria para alcanzar ese switch. Esto habilita que se determinen el root bridge y la trayectoria de costo más bajo a la raíz. Los parámetros adicionales de configuración transportados en las BPDU desde la raíz invalidan a aquellos que están configurados localmente para que la red entera use temporizadores consistentes.

La topología luego converge con estos pasos:

1. Se elige un único root bridge para todo el dominio Spanning Tree.
2. Se elige un puerto raíz (frente a un root bridge) en todos los non-root bridge.
3. Se elige un puerto designado para el reenvío de BPDU en cada segmento.
4. Los puertos no designados se vuelven bloqueadores.

Consulte Configuración de Spanning tree para obtener más información.

Opciones Básicas Predeterminadas del Temporizador (segundos)	Nombre	Función
2	Hello	Controla el envío de BPDU.
15	Demora de Reenvío (Fwdd	Controla el tiempo que dedica un puerto a escuchar y a aprender el estado y afecta el proceso del cambio de la topología (consulte la siguiente

	elay)	sección).
20	Maxage	Controla tiempo que el switch mantiene la topología actual antes de que busque una trayectoria alternativa. Después de los segundos de Maxage, una BPDU se considera desactualizada y el switch busca un nuevo puerto raíz del conjunto de puertos de bloqueo. Si no hay ningún puerto bloqueado disponible, el switch declara ser la raíz en los puertos designados.

Estados de Puertos	**Significado**	**Sincronización predeterminada al siguiente estado.**
Inhabilitado	Sin funcionamiento desde el punto de vista administrativo.	N/A
Bloqueo	Recepción de BPDU y cese de información del usuario.	Monitoree la recepción de BPDU. Espera de 20 segundos para alcanzar Maxage o cambio inmediato si se detecta una falla de link directo/local.
Escucha	Envío o recepción de BPDU para controlar si se necesita volver al bloqueo.	Temporizador de demora de reenvío (espere 15 segundos)
Aprendizaje	Construcción de tabla de topología/CAM.	Temporizador de demora de reenvío (espere 15 segundos)
Reenvío	Envío/recepción de datos.	
	Cambio de la topología básica total:	**20 + 2 (15) = 50 segundos si se espera para alcanzar Maxage o 30 segundos en caso de falla de link directo.**

Los dos tipos de BPDU en STP son BPDU de configuración y BPDU de notificación de cambio en la topología (TCN).

Flujo de BPDU de configuración

Las BPDU de configuración son originadas en cada intervalo de hello desde cada puerto en el root bridge y fluyen posteriormente hacia todos los switches de la hoja para mantener el estado

del Spanning Tree. En el estado constante, el flujo de BPDU es unidireccional: los puertos raíz y los puertos de bloqueo solo reciben BPDU de configuración, mientras que los puertos designados solo envían BPDU de configuración.

Por cada BPDU recibida por un switch de la raíz, una nueva es procesada por NMP central de Catalyst y enviada con la información de la raíz. Es decir, si se pierden el root bridge o todas las trayectorias al bridge raíz, dejan de recibirse las BPDU (hasta que el temporizador de maxage comienza la reelección).

Flujo de BPDU de TCN

Las BPDU de TCN se originan en los switches de la hoja y fluyen hacia el root bridge cuando se detecta un cambio en la topología en el spanning tree. Los puertos raíz envían solamente las TCN y los puertos señalados reciben solamente las TCN.

Una BPDU de TCN viaja hacia el bridge raíz y es reconocida en cada paso, así que este es un mecanismo confiable. Una vez que llega al root bridge, el bridge raíz alerta al dominio entero que un cambio ha ocurrido mediante el origen de BPDU de configuración con la etiqueta TCN establecida en **maxage + tiempo de fwddelay** (valor predeterminado: 35 segundos). Esto hace que todos los switches cambien su tiempo de envejecimiento CAM normal de cinco minutos (valor predeterminado) al intervalo especificado por **fwddelay** (valor predeterminado: 15 segundos). Consulte Comprensión de Campos en la Topología de Spanning Tree Protocol para conocer más detalles.

Modos de Spanning Tree

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

- Un solo Spanning Tree para todas las VLAN, o Spanning Tree Protocol único, como IEEE 802.1Q
- Un Spanning Tree por VLAN, o Spanning Tree compartido, como Cisco PVST
- Un Spanning Tree por conjunto de VLAN, o Spanning Tree múltiple, como Cisco MISTP e IEEE 802.1S

Un Spanning Tree único para todos las VLAN permite una topología activa solamente y, por lo tanto, no permite ningún balanceo de carga. Un puerto bloqueado STP bloquea todas las VLAN y no transporta ningún dato.

Un Spanning Tree por VLAN permite el balanceo de carga, pero requiere que el CPU procese más BPDU porque el número de VLAN aumenta. Las Release Notes de CatOS brindan pautas sobre el número de puertos lógicos recomendados en el Spanning Tree por switch. Por ejemplo, la fórmula Catalyst 6500/6000 Supervisor Engine 1 es la siguiente:

número de puertos + (número de trunks * número de VLAN en los trunks) < 4000

Cisco MISTP y el nuevo estándar 802.1s permiten la definición de solamente dos instancias/topologías STP activas y el mapping de todas las VLAN a cualquiera de estos dos árboles. Esta técnica permite que STP se amplíe a miles de VLAN mientras que el balanceo de carga está habilitado.

Formatos BPDU

Para ser compatible con el estándar IEEE 802.1Q, la implementación del STP de Cisco existente fue ampliada para convertirse en PVST+ agregando soporte para tunelización en una región de Spanning Tree único IEEE 802.1Q. Por lo tanto, PVST+ es compatible con IEEE 802.1Q MST y con los protocolos PVST de Cisco y no requiere comandos ni configuración adicionales. Además, PVST+ añade mecanismos de verificación para asegurarse de que no hay incoherencia en la configuración del trunking de puerto y de ID de VLAN en los switches.

Estos son algunos aspectos destacados del funcionamiento del protocolo PVST+:

- PVST+ interactúa con Spanning Tree 802.1Q único a través del conocido Common Spanning-Tree (CST) por un trunk 802.1q. El CST se encuentra siempre en la VLAN 1, por lo que esta VLAN debe estar habilitada en el trunk para interactuar con otros proveedores. Las BPDU CST se transmiten, siempre sin etiquetar, al grupo de bridges del estándar IEEE (dirección MAC 01-80-c2-00-00-00, DSAP 42, SSAP 42). Para una descripción completa, un conjunto paralelo de BPDU también se transmite a la dirección MAC del Spanning Tree compartido de Cisco para la VLAN 1.
- PVST+ realiza la tunelización de BPDU PVST a través de las regiones de VLAN 802.1Q como datos de multicast. Las BPDU de Spanning Tree compartido de Cisco se transmiten a la dirección MAC 01-00-0c-cc-cc-cd (SNAP HDLC tipo de protocolo 0x010b) para cada VLAN en un trunk. Las BPDU no están etiquetadas en la VLAN de origen y sí están etiquetadas en las demás VLAN.
- PVST+ verifica incoherencias de VLAN y puertos. PVST+ bloquea aquellos puertos que reciben BPDU inconsistentes a fin de impedir loops de reenvío. También notifica a los usuarios a través de los mensajes de syslog sobre cualquier discrepancia en la configuración.
- PVST+ es retrocompatible con los switches Cisco existentes que ejecutan PVST en trunks ISL. Los BPDU encapsulados ISL aún se transmiten o reciben mediante una dirección IEEE MAC. Es decir, cada tipo de BPDU es link-local; no hay problemas de traducción.

Recomendación

Todos los switches Catalyst tienen el STP habilitado de forma predeterminada. Esta es la configuración recomendada incluso si se opta por un diseño que no incluye loops L2 y STP no está habilitado porque está manteniendo activamente un puerto bloqueado.

```
set spantree enable all
!--- This is the default.
```

Cisco recomienda que el STP esté habilitado por estas razones:

- Si hay un loop (producto de error en la aplicación de parches, cable incorrecto, entre otros motivos), STP evita efectos perjudiciales para la red causados por datos de multicast y de broadcast.
- Protección frente a averías de EtherChannel.
- La mayoría de las redes se configuran con STP, lo que le da al protocolo una máxima exposición en el campo. Más exposición generalmente significa código estable.
- Protección contra el mal comportamiento de tarjetas de interfaz de red dobles conectadas (o activadas en bridging en servidores).
- El software para muchos protocolos (como PAgP, IGMP snooping y trunking) está estrechamente relacionado con STP. Trabajar sin STP puede dar lugar a resultados poco deseables.

No cambie los temporizadores, ya que esto puede afectar negativamente a la estabilidad. La mayoría de las redes implementadas no está ajustada. Los temporizadores STP simples accesibles a través de la línea de comandos, como intervalo hello y Maxage, comprenden un conjunto complejo de otros temporizadores intrínsecos y supuestos, así que es difícil ajustar los temporizadores y considerar todas las ramificaciones. Por otra parte, existe el riesgo de perjudicar la protección de UDLD.

Lo ideal es que mantenga el trafico de los usuarios fuera de la VLAN de administración. Especialmente con los procesadores de switches Catalyst más antiguos, es mejor evitar problemas con STP y, para hacerlo, debe mantener la VLAN de administración separada de los datos del usuario. Una estación terminal con un comportamiento incorrecto podría potencialmente mantener el procesador de la supervisor engine tan ocupado con los paquetes de broadcast que podría omitir una o más BPDU. Sin embargo, los switches más nuevos con controles de regulación y CPU más potentes restan importancia a esta consideración. Consulte la sección Administración En Banda de este documento para más detalles.

No aplique límites físicos exagerados para la redundancia. Esto puede dar lugar a una pesadilla de troubleshooting: demasiados puertos de bloqueo afectan negativamente la estabilidad a largo plazo. **Mantenga el diámetro STP total por debajo de siete saltos**. Para el diseño intente seguir el modelo de capas múltiples de Cisco, con sus dominios conmutados más pequeños, triángulos STP y puertos bloqueados seguros (como se explica en Diseño de Redes de Campus de Gigabit: Principios y Arquitectura) siempre que sea posible.

Controle y conozca dónde reside la funcionalidad Raíz y los puertos bloqueados y documéntelos en un diagrama de topología. El troubleshooting de STP comienza en los puertos bloqueados: lo que los hizo cambiar de bloqueo a reenvío a menudo es la parte clave del análisis de causas raíz. **Elija la capa de distribución y la capa central como la ubicación de raíz/raíz secundaria**, puesto que estas se consideran las partes más estables de la red. Verifique que la superposición de HSRP y L3 con las trayectorias de reenvío de datos L2 sea óptima. Este comando es una macro que configura la prioridad de bridge; la raíz lo configura con un valor mucho más bajo que el predeterminado (32768), mientras que la raíz secundaria lo configura razonablemente con un valor más bajo que el predeterminado:

```
set spantree root secondary vlan range
```

Nota: Esta macro configura la prioridad de la raíz para que sea 8192 (valor predeterminado), la prioridad de la raíz actual menos 1 (si se conoce otro root bridge) o la prioridad de la raíz actual (si su dirección MAC es inferior a la raíz actual).

Quite las VLAN innecesarias de los puertos trunk(un ejercicio bidireccional). Esto limita el diámetro de sobrecarga de procesamiento de STP y NMP en las partes de la red en las que ciertas VLAN no son necesarias. El recorte automático de VTP no quita el STP de un trunk. Consulte la sección VTP de este documento para obtener más información. La VLAN 1 predeterminada también se puede quitar de los trunks con CatOS 5.4 y versiones posteriores.

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

Otras Opciones

Cisco tiene otro STP conocido como VLAN-Bridge. Este protocolo funciona usando una dirección MAC de destino de **01-00-0c-cd-cd-ce** y un tipo de protocolo de 0x010c.

Esto es la más útil si hay una necesidad de interligar el no routable o los protocolos heredados entre los VLA N sin la interferencia con los casos del árbol de expansión IEEE que se ejecutan en esos VLA N. Si las interfaces VLAN para el tráfico no puenteado se bloquean para el tráfico L2 (y esto podría suceder fácilmente si participaron en el mismo STP que las VLAN IP), el tráfico L3 superpuesto se recorta inadvertidamente, un efecto colateral no deseado. VLAN-Bridge es, por lo tanto, una instancia de STP aparte para los protocolos puenteados, que proporciona una topología independiente que se puede manipular sin afectar al tráfico IP.

La recomendación de Cisco es ejecutar VLAN-bridge si se requiere una conexión en bridge entre las VLAN en los routers de Cisco, tal como las MSFC.

PortFast

PortFast se utiliza para evitar el funcionamiento normal del Spanning Tree en los puertos de acceso para acelerar la conectividad entre las estaciones terminales y los servicios a los que necesitan conectarse después de la inicialización del link. En algunos protocolos, tales como IPX/SPX, es importante ver el puerto de acceso en el modo de reenvío inmediatamente después que el link se haya encendido para evitar problemas de GNS.

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

Información Operativa General

PortFast omite los estados de escucha y aprendizaje normales del STP moviendo un puerto directamente del modo del bloqueo al modo de reenvío luego de haber detectado que el link se está ejecutando. 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. Esto podrá llevar hasta dos veces el tiempo de demora de envío (un total de 30 segundos de forma predeterminada).

El modo Portfast también evita que se genere una TCN STP cada vez que el estado de un puerto cambia del modo aprendizaje al modo de reenvío. Las TCN no son un problema en sí, pero si una ola de TCN alcanza el root bridge (normalmente por la mañana cuando la gente enciende sus PC), podría prolongar el tiempo de convergencia innecesariamente.

STP PortFast es particularmente importante en redes multicast CGMP y Catalyst 5500/5000 MLS. Las TCN en estos entornos pueden hacer que las entradas de tabla CAM CGMP estáticas expiren, lo que da lugar a la pérdida de paquetes de multicast hasta el siguiente informe IGMP, o entradas de MLS de la memoria caché flush que luego deben ser reconstruidas y esto podría generar un pico del CPU del router, según el tamaño de la memoria caché. (Las implementaciones de Catalyst 6500/6000 MLS y las entradas de multicast aprendidas a través de IGMP Snooping no se ven afectadas).

Recomendación

Cisco recomienda que STP PortFast esté habilitado para todos los puertos de host activos y e inhabilitado para los links de switch a switch y los puertos que no se utilizan.

También se deben inhabilitar las funciones de trunking y canalización 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 se

deja negociar a estos protocolos, la demora subsiguiente en la activación del puerto puede conducir a situaciones indeseables en las cuales los paquetes iniciales desde las estaciones de trabajo, como las solicitudes DHCP, no son reenviados.

CatOS 5.2 introdujo un comando macro, **set port *host port range*** , que implementa esta configuración para los puertos de acceso y ayuda en gran medida a la negociación automática y al rendimiento de la conexión:

```
set port host port range
!--- Macro command for these commands: set spantree portfast port range enable set trunk port
range off set port channel port range mode off
```

Nota: PortFast no implica que el Spanning Tree no se ejecute en absoluto en esos puertos. Aún se envían, se reciben y se procesan BDPU.

Otras Opciones

La protección de BPDU de PortFast brinda una manera de evitar loops; para ello, coloca a un puerto que no se conecta mediante trunking en un estado errdisable cuando una BPDU se recibe en ese puerto.

Un paquete de BPDU nunca se debe recibir en un puerto de acceso configurado para PortFast, puesto que los puertos de host no se deben conectar con los switches. Si se observa una BPDU, indica una configuración no válida y posiblemente peligrosa que necesita una acción administrativa. Cuando se habilita la función de protección de BPDU, el Spanning Tree apaga las interfaces configuradas con Portfast que reciben las BPDU en vez de ponerlas en el estado de bloqueo de STP.

El comando funciona por switch y no por puerto, como se muestra a continuación:

```
set spantree portfast bpdu-guard enable
```

Si el puerto deja de funcionar, el administrador de la red es notificado mediante una trampa SNMP o un mensaje syslog. También se puede configurar un tiempo de recuperación automática para los puertos en estado errdisabled. Consulte la sección UDLD de este documento para conocer más detalles. Si desea obtener más información, consulte Mejora de la Protección de BPDU de Spanning Tree Portfast.

Nota: La función PortFast para puertos trunk fue introducida en CatOS 7.x y no tiene ningún efecto sobre los puertos trunk en las versiones anteriores. La función PortFast para puertos trunk ha sido diseñada para aumentar el tiempo de convergencia para las redes L3. Para complementar esta función, CatOS 7.x también introdujo la posibilidad de configurar la protección de BPDU de PortFast por puerto.

UplinkFast

UplinkFast provee una rápida convergencia STP luego de una falla de enlace directo en la capa de acceso de la red. No modifica el STP y tiene como finalidad acelerar el tiempo de convergencia en una circunstancia específica para alcanzar una demora de menos de tres segundos, en lugar de la demora típica de 30 segundos. Consulte Comprensión y Configuración de la función Uplink Fast de Cisco para obtener más información.

Información Operativa General

Con el uso del modelo de diseño de múltiples capas de Cisco en la capa de acceso, si se pierde el uplink de reenvío, el uplink de bloqueo pasa inmediatamente a un estado de reenvío sin esperar los estados de escucha y de aprendizaje.

Un grupo de link ascendente es un conjunto de puertos por VLAN que puede considerarse como un puerto raíz y un puerto raíz de respaldo. En condiciones normales, el puerto raíz asegura la conectividad del acceso hacia la raíz. Si esta conexión con la raíz primaria falla por algún motivo, el link de raíz de respaldo se inicia inmediatamente sin tener que atravesar los 30 segundos típicos de demora de convergencia.

Puesto que esta acción evita con eficacia el proceso normal de manejo de cambios de la topología de STP (escucha y aprendizaje), un mecanismo de corrección de topología alternativo es necesario para actualizar los switches en el dominio en que las estaciones terminales locales son accesibles a través de una trayectoria alternativa. El switch de la capa de acceso que ejecuta UplinkFast también genera tramas para cada dirección MAC en su CAM en una dirección MAC de multicast (01-00-0c-cd-cd-cd, HDLC protocolo 0x200a) para actualizar la tabla CAM en todos los switches en el dominio con la nueva topología.

Recomendación

Cisco recomienda que se habilite UplinkFast para los switches con puertos bloqueados, normalmente en la capa de acceso. No utilice esta función en switches sin el conocimiento de topología implícita de un link raíz de respaldo; habitualmente switches centrales y de distribución en el diseño de múltiples capas de Cisco. Puede ser agregado sin interrupciones a una red de producción. Ejecute este comando para habilitar UplinkFast:

```
set spantree uplinkfast enable
```

Este comando también configura la **prioridad de bridge** en alta para minimizar el riesgo de que se convierta en root bridge y la **prioridad de puerto** en alta para minimizar la posibilidad de que se convierta en un puerto designado, lo que interrumpe las funciones. Cuando usted restablece un switch que tiene la función UplinkFast habilitada, hay que inhabilitar la función, borrar la base de datos con "borrar uplink" y restablecer manualmente las prioridades de bridge.

Nota: Se necesita la **palabra clave de todos los protocolos** para el comando UplinkFast cuando se habilita la función de filtrado de protocolo. Como la CAM registra el tipo de protocolo y la información de MAC y VLAN cuando se habilita el filtrado de protocolo, se debe generar una trama UplinkFast 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. No debe configurar BackboneFast con Rapid STP (RSTP) o IEEE 802.1W porque el mecanismo ya está incorporado y se habilita automáticamente en RSTP.

BackboneFast

BackboneFast proporciona una convergencia rápida después de que se produce una falla de link indirecto. Con la incorporación de esta función en STP, el tiempo de convergencia se puede reducir normalmente del valor predeterminado de 50 segundos al valor de 30 segundos.

Información Operativa General

El mecanismo se inicia cuando un puerto raíz o un puerto bloqueado en un switch recibe BPDU inferiores de su bridge designado. Esto puede suceder cuando un switch de flujo descendente ha perdido su conexión con la raíz y comienza a enviar sus propias BPDU para elegir una nueva raíz. Una **BPDU inferior** identifica a un switch como el root bridge y el bridge designado a la vez.

De acuerdo con las reglas normales del Spanning Tree, el switch de recepción ignora las BPDU inferiores durante el tiempo de envejecimiento máximo configurado, que es igual a 20 segundos de forma predeterminada. Sin embargo, con BackboneFast, el switch considera la BPDU inferior como una señal de que la topología podría haber cambiado e intenta determinar si tiene una trayectoria alternativa al root bridge usando BPDU de consultas del tipo Root Link Query (RLQ). Esta incorporación en el protocolo permite que un switch verifique si la raíz todavía se encuentra disponible, pasa un puerto de estado bloqueado a estado de reenvío en menos tiempo y notifica al switch aislado que envió la BPDU inferior que la raíz sigue estando allí.

Estos son algunas aspectos destacados del funcionamiento del protocolo:

- Un switch transmite el paquete de RLQ fuera del puerto raíz solamente (es decir, hacia el root bridge).
- Un switch que recibe una RLQ puede contestar si es el switch raíz o si sabe que ha perdido la conexión con la raíz. Si no conoce estos hechos debe reenviar el pedido fuera de su puerto raíz
- Si un switch pierde conexión con la raíz, debe responder a esta consulta de forma negativa.
- La respuesta debe ser enviada únicamente por el puerto desde donde surgió la consulta.
- El switch raíz debe responder siempre a esta consulta con una respuesta positiva.
- Si se recibe la respuesta en un puerto que no sea raíz, se la elimina.

Los tiempos de convergencia de STP se pueden, por lo tanto, reducir en hasta 20 segundos, ya que no se debe alcanzar maxage.

Consulte Comprensión y Configuración de BackboneFast en Switches Catalyst para obtener más información.

Recomendación

La recomendación de Cisco es habilitar BackboneFast en todos los switches que ejecutan STP. Puede ser agregado sin interrupciones a una red de producción. Ejecute este comando para habilitar BackboneFast:

```
set spantree backbonefast enable
```

Nota: Este comando global debe ser configurado en todos los switches en un dominio, ya que agrega funciones al protocolo STP que todos los switches deben entender.

Otras Opciones

BackboneFast no es compatible con 2900XLs y 3500s. Esta función no se debe habilitar si el dominio del switch contiene estos switches, además de los switches Catalyst 4500/4000, 5500/5000 y 6500/6000.

No necesita configurar BackboneFast con RSTP o IEEE 802.1W porque el mecanismo ya está incorporado en RSTP y se habilita automáticamente en este protocolo.

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. Esta función protege a las redes L2 contra loops causados por lo siguiente:

- funcionamiento incorrecto de las interfaces de la red;
- CPU ocupadas;
- todo aquello que impida el reenvío normal de BPDU.

Un loop STP ocurre cuando un puerto de bloqueo en una topología redundante pasa por error al estado de reenvío. Este pasaje suele suceder porque uno de los puertos en una topología física redundante (no necesariamente el puerto de bloqueo) deja de recibir BPDU.

La función de protección contra loops solo sirve en redes conmutadas en las que los switches están conectados por links de punto a punto. La mayoría de las redes de campus y centros de datos modernas son de este tipo. En un link punto a punto, un bridge designado no puede desaparecer a menos que envíe una BPDU inferior o haga que el link deje de funcionar. La función de protección contra loops de STP fue introducida en la versión CatOS 6.2(1) para las plataformas Catalyst 4000 y Catalyst 5000, y en la versión 6.2(2) para la plataforma Catalyst 6000.

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

Esta función hace la verificación correspondiente para determinar si un puerto raíz o un puerto raíz alternativo/de respaldo recibe BPDU. Si el puerto no recibe BPDU, la protección contra loops pone el puerto en un estado inconsistente (bloqueo) hasta que comience a recibir BPDU de nuevo. 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. El estado loop-inconsistent se quita del puerto y el STP determina al estado de puerto porque dicha 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. Esta función evita que se formen loops STP con la velocidad de la versión de STP en uso. No hay dependencia de STP (802.1d o 802.1w) ni cuando se ajustan los temporizadores STP. Por estas razones, la función de protección contra loops se debe implementar junto con UDLD en las topologías que dependen de STP y si el software admite la función.

Cuando la protección contra loops bloquea un puerto inconsistente, se registra este mensaje:

```
set spantree backbonefast enable
```

Cuando la BPDU se recibe en un puerto en un estado STP loop-inconsistent, el puerto pasa a otro estado STP. De acuerdo con la BPDU recibida, la recuperación es automática y no es necesario intervenir. Después de la recuperación, se registra este mensaje.

```
set spantree backbonefast enable
```

Interacción con Otras Funciones de STP

- **Protección de raíz**La protección de raíz hace que un puerto siempre sea puerto designado. La protección contra loops es eficaz solamente si el puerto es el puerto raíz o un puerto alternativo. Estas funciones son mutuamente exclusivas. La función de protección contra loops y la función de protección de raíz no se pueden habilitar en un puerto al mismo tiempo.
- **UplinkFast**La protección contra loops es compatible con UplinkFast. Si la protección contra loops pone a un puerto raíz en estado de bloqueo, UplinkFast pone a un nuevo puerto raíz en estado de reenvío. Además, UplinkFast no selecciona un puerto es estado loop-inconsistent como puerto raíz.
- **BackboneFast**La protección contra loops es compatible con BackboneFast. La recepción de una BPDU inferior que proviene de un bridge designado activa la función BackboneFast. Como las BPDU se reciben de este link, la protección contra loops no se activa, así que BackboneFast y la protección contra loops son compatibles.
- **PortFast**PortFast hace que un puerto ingrese en el estado de reenvío designado inmediatamente después de la conexión. Dado que un puerto con la función Portfast habilitada no puede ser un puerto raíz o alternativo, la protección contra loops y PortFast son mutuamente exclusivos.
- **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. Sin embargo, para formar un canal, todos los puertos físicos que se agrupan en el canal deben tener configuraciones compatibles. PAgP aplica la configuración uniforme de la protección contra loops en todos los puertos físicos para formar un canal.**Nota:** Estas son advertencias que debe tener en cuenta cuando configura la protección contra loops en un EtherChannel:STP siempre escoge el primer puerto operativo en el canal para enviar las 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 los puertos que ya están bloqueados por la protección contra loops se agrupan para formar un canal, STP pierde toda la información relativa al estado de esos puertos. El nuevo puerto del canal puede ingresar al estado de reenvío con un rol designado.Si la protección contra loops bloquea un canal y este deja de funcionar, STP pierde toda la información relativa al estado. Los puertos físicos individuales pueden ingresar al estado de reenvío con un rol designado, incluso si uno o más de los links que formaron el canal son unidireccionales.En los dos últimos casos de esta lista, existe la posibilidad de que se forme un loop hasta que UDLD detecte la falla. Pero la protección contra loops no puede detectar el loop.

Comparación de Protección contra Loops y UDLD

La función de protección contra loops y la función de UDLD se superponen en parte. Ambas funciones brindan protección contra las fallas del STP que causan los links unidireccionales. Sin embargo, abordan el problema y funcionan de distinta manera. Específicamente, hay ciertas fallas unidireccionales que la UDLD no puede detectar, como las fallas causados por una CPU que no envía 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.

La protección contra loops no funciona en links compartidos ni en situaciones en las cuales el link ha sido unidireccional desde la conexión. En caso de que el link haya sido unidireccional desde la conexión, el puerto nunca recibe BPDU y se convierte en designado. Este comportamiento puede ser normal, así que la protección contra loops no abarca este caso particular. UDLD brinda protección contra tal escenario.

Habilite ambas funciones (UDLD y protección contra loops) para proporcionar el más alto nivel de protección. Consulte la sección *Comparación entre Protección contra loops y Detección de Link Unidireccional* de Mejoras en Spanning-Tree Protocol con las Funciones Protección contra Loops y Detección de Desviación del Tiempo de Llegada de las BPDU para obtener una comparación entre protección contra loops y UDLD.

Recomendación

Cisco recomienda la habilitación global de la protección contra loops en una red de switch con loops físicos. En la versión 7.1(1) del software de Catalyst y en versiones posteriores, puede realizar la habilitación global de la protección contra loops en todos los puertos. De hecho, la función se habilita en todos los links punto a punto. El estado dúplex del link detecta el link punto a punto. Si el modo es dúplex completo, el link se considera de punto a punto. Ejecute este comando para la habilitación global de la protección contra loops:

```
set spantree global-default loopguard enable
```

Otras Opciones

Para los switches que no admiten la configuración global de la protección contra loops, habilite la función en todos los puertos individuales, que incluyen los puertos de canal. Aunque la habilitación de la protección contra loops en un puerto designado no ofrece beneficios, esta habilitación no es 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. Ejecute este comando para habilitar la protección contra loops:

```
set spantree guard loop mod/port
```

Las redes con topologías sin loops pueden, aún así, obtener beneficios con esta función en caso de que los loops se introduzcan accidentalmente. Sin embargo, la habilitación de la protección contra loops en este tipo de topología puede conllevar problemas de aislamiento de la red. A fin de construir topologías sin loops y evitar problemas de aislamiento de la red, ejecute estos comandos para inhabilitar la protección contra loops globalmente o individualmente. No habilite la protección contra loops en links compartidos.

- ```
  set spantree global-default loopguard disable
  !--- This is the global default.
  ```
  o
- ```
  set spantree guard none mod/port
  !--- This is the default port 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 de raíz hace asegura la posición de root bridge. La protección de raíz está disponible para Catalyst 29xx, 4500/4000, 5500/5000 y 6500/6000 en la versión de software CatOS 6.1.1 y versiones

posteriores.

Información Operativa General

La protección de raíz es un mecanismo incorporado de STP. La protección de raíz no tiene un temporizador y depende de la recepción de BPDU solamente. Cuando la protección de raíz se aplica a un puerto, la función no permite que un puerto se convierta en un puerto raíz. Si la recepción de una BPDU produce una convergencia de spanning tree que hace que un puerto designado se convierta en puerto raíz, el puerto ingresa al estado root-inconsistent. Este mensaje de syslog muestra la acción:

```
set spantree guard none mod/port
!--- This is the default port configuration.
```

Después de que el puerto deja de enviar BPDU superiores, vuelve a desbloquearse. Con STP, el puerto pasa del estado de escucha al estado de aprendizaje y por último pasa al estado de reenvío. La recuperación es automática y no es necesario que intervenga. Este mensaje de syslog brinda un ejemplo:

```
set spantree guard none mod/port
!--- This is the default port configuration.
```

La protección de raíz hace que un puerto sea puerto designado y la protección contra loops es eficaz solo si el puerto es el puerto raíz o un puerto alternativo. Por lo tanto, las dos funciones son mutuamente exclusivas. La función de protección contra loops y la función de protección de raíz no se pueden habilitar en un puerto al mismo tiempo.

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

Recomendación

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 la protección de raíz, ejecute este comando:

```
set spantree guard root mod/port
```

EtherChannel

Las tecnologías EtherChannel permiten la multiplexación inversa de múltiples canales (hasta ocho en Catalyst 6500/6000) en un solo link lógico. Si bien la implementación de cada plataforma es diferente, es importante comprender los requisitos comunes:

- un algoritmo para multiplexación estadística de tramas en múltiples canales;
- creación de un puerto lógico para que se pueda ejecutar una instancia única de STP;
- un protocolo de administración de canal, como PAgP o Link Aggregation Control Protocol (LACP).

Multiplexación de Tramas

EtherChannel abarca un algoritmo de distribución de tramas que multiplexa eficientemente las

tramas a través de links gigabit o 10/100 de componente. 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 distribución de carga es una opción global para ambos protocolos de 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. Sin embargo, cualquier algoritmo de distribución se asegura de que, cuando se reciben las tramas, el algoritmo no produzca un orden incorrecto de las tramas que son parte de una determinada conversación o duplicación de tramas.

Nota: Se debe tener en cuenta la siguiente información:

- Catalyst 6500/6000 tiene hardware de switching más reciente que Catalyst 5500/5000 y puede leer la información de la capa 4 (L4) de IP a velocidad de alambre para tomar una decisión de multiplexación más inteligente que la simple información de L2 de MAC.
- Las capacidades de Catalyst 5500/5000 dependen de la presencia de un Ethernet Bundling Chip (EBC) en el módulo. El *comando show port capabilities mod/port* confirma las acciones posibles para cada puerto.

Consulte esta tabla que ilustra el algoritmo de distribución de tramas detalladamente para cada plataforma incluida:

Plataforma	Algoritmo de Balanceo de Carga del Canal
Serie Catalyst 5500/5000	Un Catalyst 5500/5000 con los módulos necesarios permite dos a cuatro links a estar presentes por FEC1, aunque deben estar en el mismo módulo. Los pares de dirección de origen y destino de MAC determinan el link elegido para el reenvío de tramas. Se realiza una operación X-OR en los dos bits menos significativos de la dirección MAC de origen y la dirección MAC de destino. Esta operación arroja uno de cuatro resultados: (0 0), (0 1), (1 0), o (1 1). Cada uno de estos valores señala un link en el conjunto FEC. En el caso de un Fast EtherChannel de dos puertos, únicamente se utiliza un bit en la operación X-OR. Pueden surgir problemas cuando una de las direcciones en el par origen/destino es constante. Por ejemplo, el destino puede ser un servidor o, aún más probable, un router. En ese caso, el balanceo de carga estadístico se ve porque la dirección de origen es siempre diferente.
Series Catalyst 4500/4000	EtherChannel de Catalyst 4500/4000 distribuye las tramas a través de los links en un canal (en un solo módulo) y, para ello, se basa en los bits de orden bajo de las direcciones de origen y destino de MAC de cada trama. En comparación con Catalyst 5500/5000, el algoritmo tiene mayor participación y utiliza una función hash determinista de los campos de dirección de

	destino de MAC (bytes 3, 5, 6), dirección de origen (bytes 3, 5, 6), puerto de ingreso e ID de VLAN. El método de distribución de tramas no es configurable.
Serie Catalyst 6500/6000	Hay dos algoritmos de hash posibles, según el hardware de la Supervisor Engine. El hash es un polinomio de decimoséptimo grado implementado en hardware que, en todos los casos, tome el MAC address, el IP Address, o el número del puerto IP TCP/UDP2 y aplique el algoritmo para generar un valor en bits tres. Esto se realiza de manera separada para las direcciones de origen y destino. Luego se aplica XOR a los resultados para generar otro valor de tres bits que se utilice para determinar qué puerto en el canal se utiliza para reenviar el paquete. Los canales en Catalyst 6500/6000 se pueden formar entre los puertos en cualquier módulo y pueden ser hasta 8 puertos.

[1] FEC = Fast EtherChannel

[2] UDP = protocolo UDP

En esta tabla se indican los métodos de distribución soportados en los diversos modelos de Supervisor Engine de Catalyst 6500/6000 y su comportamiento predeterminado.

Hardware	Descripción	Métodos de Distribución
WS-F6020 (Motor L2)	Early Supervisor Engine 1	MAC L2: SA; DA; SA & DA
WS-F6020A (L2 Engine) WS-F6K-PFC (L3 Engine)	Later Supervisor Engine 1 y Supervisor Engine 1A/PFC1	MAC L2: SA; DA; IP L3 de dirección de origen y dirección de destino: SA; DA; Dirección de origen y dirección de destino (valor predeterminado)
WS-F6K-PFC2	Supervisor Engine 2/PFC2 (se necesita CatOS 6.x)	MAC L2: SA; DA; IP L3 de dirección de origen y dirección de destino: SA; DA; Sesión L4 (valor predeterminado) de dirección de origen y dirección de destino Puerto de origen; Puerto de destino; Puerto de origen y de destino (valor predeterminado)
WS-F6K-PFC3BXL	Supervisor Engine	MAC L2: SA; DA; IP L3 de dirección de origen y

WS-F6K-PFC3B WS-F6K-PFC3A	720/PFC3A (se necesita CatOS 8.1.x) Supervisor Engine 720/Supervisor Engine 32/PFC3B (se necesita CatOS 8.4.x) Supervisor Engine 720/PFC3BXL (se necesita CatOS 8.3.x)	dirección de destino: SA; DA; Sesión L4 (valor predeterminado) de dirección de origen y dirección de destino Puerto de origen; Puerto de destino; Sesión IP-VLAN-L4 de puerto de origen y de destino: Dirección de origen y VLAN y puerto de origen; Dirección de destino y VLAN y puerto de destino; Dirección de origen y dirección de destino y VLAN y puerto de origen y puerto de destino

Nota: Con la distribución L4, el primer paquete fragmentado utiliza la distribución L4. Todos los paquetes subsiguientes utilizan la distribución L3.

Más detalles sobre el soporte EtherChannel en otras plataformas y sobre la manera de configurarlo y de resolver problemas relacionados con él se pueden encontrar en estos documentos:

- Introducción a la Redundancia y el Balanceo de Carga de Etherchannel en Switches Catalyst
- Configuración de EtherChannel en Switches Catalyst 4500/4000, 5500/5000 y 6500/6000 que funcionan con el software del sistema CatOS
- Configuración de LACP (802.3ad) entre un Catalyst 6500/6000 y un Catalyst 4500/4000
- Configuración de EtherChannel de Capa 3 y Capa 2

Recomendación

Catalyst 6500/6000 Series Switches realizan balanceo de carga por dirección IP de manera predeterminada. Esto se recomienda en CatOS 5.5, siempre que IP sea el protocolo dominante. Ejecute este comando para configurar el balanceo de carga:

```
set port channel all distribution ip both
!--- This is the default.
```

La distribución de tramas de las series Catalyst 4500/4000 y 5500/5000 por dirección MAC L2 es aceptable en la mayoría de las redes. Sin embargo, el mismo link se utiliza para todo el tráfico si hay solamente dos dispositivos principales que se comunican por un canal (ya que la dirección MAC de origen y la dirección MAC de destino son constantes). Esto normalmente puede ser un problema para la copia de respaldo del servidor y otras transferencias de archivos grandes o para un segmento en tránsito entre dos routers.

Aunque el puerto de agregación (agport) lógico pueda ser manejado por el SNMP como una instancia independiente y se puedan recopilar estadísticas del rendimiento de agregación, Cisco recomienda, de todas formas, que usted maneje cada interfaz física por separado para verificar cómo funcionan los mecanismos de distribución de tramas y si se logra el balanceo de carga estadístico.

A través de un comando nuevo, el comando show channel traffic, en CatOS 6.x podrá visualizar estadísticas de distribución de porcentajes más fácilmente que si controlara los contadores de puerto individual con el *comando show counters mod/port* o con el *comando show mac mod/port* en CatOS 5.x. Otro comando nuevo, el comando show channel hash, en CatOS 6.x le permite verificar, sobre la base del modo de distribución, qué puerto sería seleccionado como el puerto saliente para determinadas direcciones o determinados números de puerto. Los comandos equivalentes para los canales LACP son el comando show lacp-channel traffic y el comando show lacp-channel hash.

Otras Opciones

A continuación se incluyen pasos que se podrían seguir si las limitaciones relativas de los algoritmos basados en MAC de Catalyst 4500/4000 o Catalyst 5500/5000 fueran un problema y no se lograra un balanceo de carga estadístico correcto:

- Implemente switches Catalyst 6500/6000.
- Aumente el ancho de banda sin canalización mediante switching, por ejemplo, de varios puertos FE a un puerto GE, o bien, de varios puertos GE a un puerto de 10 GE.
- Cambiar la dirección de pares de estaciones terminales con flujos de gran volumen.
- Proporcione links dedicados/VLAN para los dispositivos de ancho de banda altos.

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. Siga estas pautas para evitar problemas de conjuntos. Por ejemplo, si la QoS está habilitada, no se forman EtherChannels al combinar módulos de switching de la serie Catalyst 6500/6000 con deferentes capacidades de QoS. En Cisco IOS Software, usted puede inhabilitar el control de atributo de puerto de QoS en la combinación de EtherChannel con el comando de la interfaz de canal de puerto no mls qos channel-consistency. CatOS no ofrece un comando equivalente para inhabilitar el control de atributo del puerto de QoS. Usted puede ejecutar el *comando show port capability mod/port* para visualizar la capacidad de puerto de QoS y determinar si los puertos son compatibles.

Siga estas pautas correspondientes a diversas plataformas para evitar los problemas de configuración:

- La sección *Pautas de Configuración de EtherChannel* de Configuración de EtherChannel (Catalyst 6500/6000)
- La sección *Pautas y Restricciones para la Configuración de EtherChannel* de Configuración de Fast EtherChannel y Gigabit EtherChannel (Catalyst 4500/4000)
- La sección *Pautas y Restricciones para la Configuración de EtherChannel* de Configuración de Fast EtherChannel y Gigabit EtherChannel (Catalyst 5000)

Nota: El número máximo de canales de puerto que el Catalyst 4000 soporta es 126. Con las versiones de software 6.2(1) y anteriores, los switches Catalyst series 6500 de seis y nueve ranuras soportan un máximo de 128 EtherChannels. En las versiones de software 6.2(2) y posteriores, la función de spanning tree maneja el ID del puerto. Por lo tanto, el número máximo de EtherChannels con soporte es 126 para chasis de seis o nueve ranuras y 63 para un chasis de 13 ranuras.

Port Aggregation Protocol

PAgP es un protocolo de administración que verifica la consistencia de parámetros en cualquiera de los extremos del link y asistirá al canal en la adaptación a la falla o adición del link. Tenga en cuenta la siguiente información acerca de PAgP:

- PAgp requiere que todos los puertos del canal pertenezcan a la misma VLAN o estén configurados como puertos trunk. (Como las VLAN dinámicas pueden forzar el cambio de un puerto a una VLAN diferente, no están incluidas en la participación EtherChannel).
- Cuando un conjunto ya existe y se modifica la configuración de un puerto (como la modificación del modo de la concentración de enlaces o de la VLAN), todos los puertos del agrupamiento se modifican para coincidir con dicha configuración.
- 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 PAgP controla cada puerto de los físicos individuales (o lógico) que se agrupará. Los paquetes PAgP se envían a través de la misma dirección MAC de grupo de multicast que se usa para los paquetes CDP, **01-00-0c-cc-cc-cc**. El valor del protocolo es 0x0104. Este es un resumen del funcionamiento del protocolo:

- 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.
- El protocolo escucha paquetes PAgP que demuestran que el puerto físico tiene una conexión bidireccional con otro dispositivo apto para PAgP.
- Si se reciben paquetes de datos pero no paquetes PAgp, se asume que el puerto está conectado a un dispositivo no habilitado para Pagp.
- En cuanto un grupo de puertos físicos reciben dos paquetes PAgP, trata de formar un puerto agregado.
- Si los paquetes PAgP se detienen durante un período, el estado de PAgP se derriba.

Procesamiento Normal

Es conveniente definir los siguientes conceptos para facilitar una mejor comprensión del protocolo:

- **Puerto agregado:** un puerto lógico que se compone de todos los puertos físicos en la misma agrupación; se puede identificar mediante su propio ifIndex de SNMP. Por lo tanto, un puerto agregado no contiene puertos no operativos.
- **Canal**: una agregación que satisface los criterios de formación; en consecuencia puede contener puertos no operativos (los agports son un subconjunto de canales). Los protocolos, incluyendo STP y VTP, pero no CDP y DTP, se ejecutan en PAgP sobre los puertos agregados. Ninguno de estos protocolos puede enviar o recibir paquetes hasta que PAgP adjunte sus puertos agregados a uno o más puertos físicos.
- **Capacidad de grupo:** cada puerto físico y puerto agregado posee un parámetro de configuración llamado la capacidad de grupo. Un puerto físico puede ser agregado a otro

puerto físico sólo si tienen la misma capacidad de grupo.

- **Procedimiento de agregación:** cuando un puerto físico alcanza los estados UpData o UpPAgP, se asocia a un puerto agregado apropiado. Cuando deja cualquiera de esos estados para pasar a otro, se separa del puerto agregado.

La siguiente tabla ofrece definiciones de los diferentes estados y procedimientos de creación:

Estado	Significado
`UpData`	No se han recibido paquetes PAgP. Se envían paquetes PAgP. El puerto físico es el único puerto conectado al puerto agregado. Los paquetes Non-PAgP entran y salen entre el puerto físico y el puerto agregado.
`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 Non-PAgP entran y salen entre el puerto físico y el puerto agregado.

Los dos extremos de las dos conexiones deben coincidir sobre lo que será el agrupamiento, definido como el mayor grupo de puertos en el puerto agregado que está permitido por los dos extremos de la conexión.

Cuando un puerto físico alcanza el estado UpPAgP, se asigna al agport que entre sus miembros cuenta con puertos físicos que coinciden con la capacidad de grupo del puerto físico nuevo y cuyo estado es BiDir o UpPAgP. (El estado de cualquier puerto BiDir de estas características cambia al mismo tiempo al estado UpPAgP). Si no existe un puerto agregado cuyos parámetros de puerto físico constituyentes sean compatibles con el puerto físico recientemente activo, éste se asigna a un puerto agregado con parámetros adecuados que no tengan puertos físicos asociados.

El tiempo de espera PAgP puede producirse en el último vecino conocido del puerto físico. El intervalo de espera del puerto se elimina del puerto agregado. Al mismo tiempo, se eliminarán todos los puertos físicos en el mismo puerto agregado cuyos temporizadores también hayan agotado el tiempo de espera. 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 enlace en un canal que existe fallo (por ejemplo, si el puerto se desconecta, se extrae un convertidor de interfaz Gigabit (GBIC) o se rompe el conector de fibra), el puerto agregado se actualiza y el tráfico se trocea y se distribuye entre los links restantes en menos de un segundo. Si hay tráfico que no se tenga que trocear después de la falla (tráfico que sigue utilizando el mismo link), éste no sufre pérdidas. La restauración de los links fallidos activa otra actualización del puerto agregado y el tráfico se fragmenta nuevamente.

Nota: La respuesta al fallo de un enlace en un canal por una interrupción del suministro eléctrico o a la extracción de un módulo. Por definición, cada canal debe tener dos puertos físicos. Si se pierde un puerto del sistema en un canal de dos puertos, el puerto agregado es desmontado y se reinicia el puerto físico original teniendo en cuenta el árbol de expansión. Esto significa que el tráfico podrá descartarse hasta que el STP permita que el puerto vuelva a estar disponible para datos.

Existe una excepción a esta regla en los switches Catalyst 6500/6000. En las versiones de CatOS anteriores a 6.3, los puertos agregados no se rompen.durante la extracción del módulo si el canal se compone de puertos en los módulos 1 y 2 solamente.

Esta diferencia en los dos modos de fallo es importante si se tiene pensado llevar a cabo un mantenimiento de la red. Es importante porque es posible que se deba tener en cuenta una TCN del STP durante la extracción o inserción en línea de un módulo. Como se ha indicado, es muy importante que cada link físico en el canal se administre con NMS porque el puerto agregado puede permanecer sin cambios durante un fallo.

Para mitigar los efectos de un cambio de topología no deseado en un módulo Catalyst 6500/6000, siga estos pasos:

- Si el canal está formado sólo con un puerto por cada módulo, utilice tres o más módulos (para que el total sea de tres o más puertos).
- Si el canal abarca dos módulos, deben utilizarse dos puertos por cada módulo (cuatro puertos en total).
- Para utilizar un canal de dos puertos a través de dos tarjetas, utilice solo los puertos de Supervisor Engine.
- La actualización a CatOS 6.3, que administra la renovación de módulos sin recálculo de STP para la división de canales a través de los módulos.

Opciones de Configuración

Existen varias opciones de configuración para EtherChannels, como se muestra en esta tabla:

Modo	Opciones Configurables
Encendido	PAgP fuera de funcionamiento. El puerto está canalizando independientemente de la configuración del puerto vecino. Si el puerto del vecino está encendido se forma un canal.
Desactivado	El puerto no está canalizando, independientemente de la configuración del puerto vecino.
`Automático (predeterminado)`	La agregación está bajo el control del protocolo PAgP. Se coloca un puerto en estado de negociación pasivo y no se envían paquetes PAgP a la interfaz hasta que se reciba al menos un paquete PAgP que indique que el remitente opera en modo deseable.

Deseable	La agregación está bajo el control del protocolo PAgP. Coloca a un puerto en un estado de negociación activa, en el que el puerto inicia negociaciones con otros puertos al enviar paquetes PagP. Un canal está formado con otro grupo de puertos, ya sea en modo deseable o automático.
No silencioso (predeterminado en los puertos fibra FE y GE de Catalyst 5500/5000)	Un modo de palabra clave automático o deseable. Si se reciben los paquetes de datos pero no se recibe ningún paquete PAgP, esta no se adjunta a un puerto agregado y no se puede usar para datos. Esta verificación bidireccional fue proporcionada por un hardware específico de Catalyst 5500/5000 porque algunos fallos de link tienen como consecuencia la fragmentación del canal. Como el modo no silencioso está deshabilitado, el puerto vecino de recuperación no se le permite activarse y volver a interrumpir el canal sin necesidad. Una agrupación más flexible y verificaciones mejoradas de la bidireccionalidad se encuentran presentes de manera predeterminada en el hardware de las series Catalyst 4500/4000 y 6500/6000.
Silencioso (predeterminado en todos los puertos de Catalyst 6500/6000 y 4500/4000 y los puertos de cobre 5500/5000)	Un modo de palabra clave automático o deseable. Si no se reciben los paquetes de datos en la interfaz, después de un tiempo de espera de 15 segundos, esta se adjunta por sí misma a un puerto agregado, de este modo 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.

La configuración silencioso/no silencioso afecta cómo reaccionan los puertos a las situaciones que generan tráfico unidireccional y en cómo se logra la failover. Cuando un puerto es incapaz de transmitir (por un error en la subcapa física [PHY] o porque se ha seccionado una fibra o cable, por ejemplo), el puerto vecino puede seguir en estado operativo. El partner sigue transmitiendo datos, pero estos se pierden porque no se puede recibir al tráfico de retorno. También pueden formarse loops en el árbol de expansión a causa de la naturaleza unidireccional del link.

Algunos puertos de fibra tienen la capacidad de llevar al puerto a un estado no funcional cuando pierde la señal de recepción (FEFI). Esto hace que el puerto del partner cambie a un estado no operativo y efectivamente provoca que los puertos en ambos extremos se desactiven.

Si utiliza dispositivos que transmiten datos (como BPDU) pero que no pueden detectar condiciones unidireccionales, el modo no silencioso debe ser utilizado para permitir que los puertos permanezcan en estado no operativo hasta que lleguen los datos de recepción y se verifique que el link es bidireccional. El tiempo que tarda un PAgP en detectar un link unidireccional es cerca de 3,5 * 30 segundos = 105 segundos, en esta ecuación, 30 segundos es el tiempo entre dos mensajes PAgP sucesivos. Se recomienda el UDLD como un detector más rápido de links unidireccionales.

Si utiliza dispositivos que no transmiten datos, debe usarse el modo silencioso . Esto forzará al puerto a conectarse y permanecer operativo sin importar que los datos recibidos estén o no presentes. Además, para los puertos que pueden detectar la presencia de una condición unidireccional, como las plataformas más recientes con FEFI y UDLD en la L1, el modo silencioso es el modo predeterminado.

Verificación

la tabla describe un resumen de todos los escenarios posibles de los modos de canalización PAgP entre dos switches conectados en forma directa (Switch A y Switch B). Algunas de estas combinaciones pueden hacer que el STP cambie el estado de los puertos del lado de canalizaciónestado de errDisable (es decir, algunas de esas combinaciones cierran los puertos en el lado de canalización).

Modo de Canal de Switch-A	Modo de Canal del Switch B	Estado del Canal
Encendido	Encendido	Canal (no PAgP)
Encendido	Desactivado	No canal (errdisable)
Encendido	Auto	No canal (errdisable)
Encendido	Deseable	No canal (errdisable)
Desactivado	Encendido	No canal (errdisable)
Desactivado	Desactivado	Sin Canal
Desactivado	Auto	Sin Canal
Desactivado	Deseable	Sin Canal
Auto	Encendido	No canal (errdisable)
Auto	Desactivado	Sin Canal

Auto	Auto	Sin Canal
Auto	Deseable	Canal PAgP
Deseable	Encendido	No canal (errdisable)
Deseable	Desactivado	Sin Canal
Deseable	Auto	Canal PAgP
Deseable	Deseable	Canal PAgP

Recomendación

Cisco recomienda que se active PAgP en todas las conexiones de canal de switch a switch, y evite el modo on . El método preferido es configurar el modo desirable en ambos extremos de un link. También es recomendable dejar la palabra clave silencioso/ no silencioso como valor predeterminado, silencioso en los switches de Catalyst 6500/6000 and 4500/4000, no silencioso en los puertos de fibra de Catalyst 5500/5000.

Como se debate en este documento, la configuración explícita de la desactivación de la canalización en todos los demás puertos es útil para el reenvío rápido de datos. Es conveniente evitar las esperas de hasta 15 segundos que se requieren para agotar el tiempo de espera de PAgP en un puerto que no se utilizará para la canalización, especialmente porque el puerto se deriva luego al STP, que en sí puede tardar 30 segundos para permitir el envío de datos, más 5 segundos para el DTP, lo que significa un total de 50 segundos. El comando set port host se analiza más detalladamente en la sección STP de este documento.

```
set port channel port range mode desirable

set port channel port range mode off
!--- Ports not channeled; part of the set port hostcommand.
```

Este comando asigna a los canales un número de grupo de administradores, que puede verse mediante la ejecución del comando show channel group. Puede administrarse la adición o extracción de los puertos de canalización al mismo puerto agregado haciendo referencia al número de administración si lo desea.

Otras Opciones

Otra configuración común para los clientes que aplican un modelo de administración mínima en la capa de acceso es que el modo de las capas de distribución y de núcleo se configure como deseable , y los switches de la capa de acceso permanezcan en el valor de configuración predeterminado, configuración automática.

Si desea establecer una canalización a dispositivos que no son compatibles con PAgP, el canal debe estar codificado on. Esta instrucción se aplica a dispositivos como servidores, Local Director, switches de contenidos, routers, switches con software, los switches Catalyst XL y Catalyst 8540. Ejecutar este comando:

```
set port channel port range mode on
```

La nueva norma IEEE para LACP 802.3ad, disponible en CatOS 7.x, probablemente reemplazará a PAgP, ya que ofrece la ventaja del interfuncionamiento entre plataforma cruzada y proveedor.

Link Aggregation Control Protocol

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. PAgP es un protocolo patentado de Cisco que solo se puede ejecutar en switches Cisco y en switches adquiridos a proveedores con licencia de Cisco. 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. La compatibilidad con el LACAP se introdujo en la versión 7.x del software CatOS.

Existen pocas diferencias entre LACP y PAgP desde una perspectiva funcional. Ambos protocolos soportan un máximo de ocho puertos en cada canal, y las mismas propiedades de los puertos se comprueban antes de que se formen los conjuntos. Estas propiedades del puerto incluyen las siguientes:

- Velocidad
- Dúplex
- VLAN nativa
- Tipo de trunking

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

- El protocolo LACP puede ejecutarse solo en puertos dúplex completo y no soporta puertos semidúplex.
- El protocolo LACP es compatible con los puertos en espera en caliente. El LACP siempre intenta configurar el número máximo de puertos compatibles en un canal, hasta el máximo permitido por el hardware (ocho puertos). Si el LACP no puede agrupar todos los puertos compatibles, todos los puertos que no se pueden incluir activamente en el canal se ponen en estado de en espera en caliente y se utilizan solo si uno de los puertos en uso falla. Un ejemplo de una situación en la que el LACP no puede agrupar todos los puertos compatibles es si las limitaciones del hardware del sistema remoto son más restrictivas.

Nota: En CatOS, el número máximo de puertos que se puede asignar a la misma clave administrativa es ocho. En Cisco IOS Software, el LACP intenta configurar el número máximo de puertos compatibles en un EtherChannel, hasta el número máximo que el hardware permite (ocho puertos). Los ocho puertos adicionales se pueden configurar como puertos de la espera en caliente.

Información Operativa General

LACP controla cada puerto físico (o lógico) individual que se agrupará. Los paquetes LACP se envían conforme a la dirección MAC de grupos de multicast, **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 de manera regular, ***en cada*** link “de agregación”.
- 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 de agregación escuchan la información que se envía dentro del protocolo y deciden qué acciones tomar.

- Los puertos compatibles se configuran en un canal, hasta el número máximo permitido por el hardware (ocho puertos).
- Las agregaciones se mantienen por intercambio regular y oportuno de información de estado actualizada entre los socios de links. Si la configuración cambia (debido a una falla de link, por ejemplo), los partners del protocolo miden el tiempo de espera y realizan la acción apropiada en función del nuevo estado del sistema.
- Además de las transmisiones de unidades de datos LACP (LACPDU) periódicas, si hay un cambio en la información del estado, el protocolo transmite un LACPDU a los partners. Los partners del protocolo realizan la acción apropiada basada en el nuevo estado del sistema.

Parámetros LACP

Para permitir que el LACP determine si un conjunto de links se conecta con el mismo sistema y si esos links son compatibles desde el punto de vista de la agregación, la capacidad de establecer estos parámetros es necesaria:

- Un identificador global único para cada sistema que participa en la agregación del linkA cada sistema que ejecuta LACP se le debe asignar una prioridad que puede elegir automáticamente o permitir que la elija el administrador. La prioridad del sistema predeterminado es 32768. La prioridad del sistema se utiliza principalmente en conjunto con una dirección MAC del sistema para formar el identificador de sistema.
- Un medio para identificar el grupo de capacidades asociadas con cada puerto y con cada agregador, como l o entiende un sistema determinadoCada puerto en el sistema debe asignar una prioridad, ya sea de forma automática o por el administrador. El valor predeterminado es 128. La prioridad se utiliza en conjunto con el número de puerto para formar el identificador del puerto.
- n instrumento para la identificación de un grupo de agrupación de enlaces y a su agregador asociadoLa habilidad de un puerto para agruparse con otro se resume en un simple parámetro de número entero de 16 bits obligatoriamente mayor que cero. Este parámetro se llama “clave”. Diversos factores determinan cada clave, por ejemplo:Las características del puerto físico, que incluyen:Velocidad de datosDuplexityPunto a punto o medio compartidoRestricciones de configuración establecidas por el administradorDos claves se asocian a cada puerto:Una clave administrativo: esta clave permite la manipulación de los valores de la clave por la gestión. Un usuario puede elegir esta clave.Clave operativa: el sistema utiliza este dominante para formar las agregaciones. Un usuario no puede elegir o cambiar directamente esta clave.Todos los puertos en un sistema que comparten el mismo valor de clave operativa son miembros del mismo grupo de claves.

Si hay dos sistemas y un conjunto de puertos con la misma clave administrativa, ambos sistemas intentan agrupar los puertos. Cada sistema comienza desde el puerto con la prioridad más alta en sistema de prioridad más alta. Esto es posible porque cada sistema conoce su propia prioridad, que le fue asignada por un usuario o por el sistema; también conoce su prioridad de socio, que ha descubierto mediante los paquetes LACP.

Comportamiento en caso de Fallas

En caso de fallos, el comportamiento del LACP es igual al del PAgP. Si un link en un canal que existe falló, el puerto agregado se actualiza y el tráfico se fragmenta y se distribuye entre los links restantes en menos de un segundo. Un link puede fallar por estas razones y por otras:

- El puerto está desconectado
- Se quita un GBIC
- Una fibra está dañada
- Falla de hardware (interfaz o módulo)

Si hay tráfico que no se tenga que trocear después de la falla (tráfico que sigue utilizando el mismo link), éste no sufre pérdidas. La restauración de los links fallidos activa otra actualización del puerto agregado y el tráfico se fragmenta nuevamente.

Opciones de Configuración

Existen varias opciones de configuración para los EtherChannels de LACP, como se muestra en esta tabla:

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.
Desactivado	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. El peer (en el estado activo) envía un paquete LACP para iniciar la negociación. El switch recibe y responde al paquete y, finalmente, forma el canal de agregación con el peer.
Activo	Esto es similar al modo deseable en el PAgP. El switch inicia la negociación para formar un link agregado. Se forma el link agregado si el otro extremo se ejecuta en el modo activo o modo pasivo de LACP.

Verificación (LACP y LACP)

La siguiente tabla describe un resumen de todos los escenarios posibles de los modos de canalización PAgP entre dos switches conectados en forma directa (Switch A y Switch B). Algunas de estas combinaciones pueden hacer que el STP coloque los puertos en el lado de canalización en el estado errdisable. Esto significa que algunas de las combinaciones desactivan los puertos en el lado de canalización.

Modo de Canal de Switch-A	Modo de 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	No canal (errdisable)	Sin Canal
Encendido	Pasivo	No canal (errdisable)	Sin Canal
Encendido	Activo	No canal (errdisable)	Sin Canal
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

Verificación (LACP y PAgP)

La siguiente tabla describe un resumen de todos los escenarios posibles de los modos de canalización PAgP entre dos switches conectados en forma directa (Switch A y Switch B). Algunas de estas combinaciones pueden hacer que el STP coloque los puertos en el lado de canalización en el estado errdisable. Esto significa que algunas de las combinaciones desactivan los puertos en el lado de canalización.

Modo de Canal de Switch-A	Modo de Canal del Switch B	Estado del Canal del Switch A	Estado del Canal del Switch B
Encendido	Encendido	Canal (no LACP)	Canal (no PAgP)
Encendido	Desactivado	No canal (errdisable)	Sin Canal
Encendido	Auto	No canal (errdisable)	Sin Canal
Encendido	Deseable	No canal (errdisable)	Sin Canal
Desactivado	Encendido	Sin Canal	No canal (errdisable)
Desactivado	Desactivado	Sin Canal	Sin Canal
Desactivado	Auto	Sin Canal	Sin Canal
Desactivado	Deseable	Sin Canal	Sin Canal
Pasivo	Encendido	Sin Canal	No canal (errdisable)
Pasivo	Desactivado	Sin Canal	Sin Canal
Pasivo	Auto	Sin Canal	Sin Canal
Pasivo	Deseable	Sin Canal	Sin Canal
Activo	Encendido	Sin Canal	No canal (errdisable)
Activo	Desactivado	Sin Canal	Sin Canal
Activo	Auto	Sin Canal	Sin Canal

Activo	Deseable	Sin Canal	Sin Canal

Recomendación

Cisco recomienda habilitar PAgP en las conexiones de canales entre los switches de Cisco. Con los dispositivos de los canales que no soportan PAgP o LACP, habilite el LACP a través de la configuración de ebe LACP activo en ambos extremos de los dispositivos. Si el extremo de los dispositivos no soporta el LACP o el PAgP, debe codificar el canal a encendido.

- **set channelprotocol lacp** *module*

  En los switches que ejecutan CatOS, todos los puertos en un Catalyst 4500/4000 y un PAgP usan el protocolo del canal PAgP de forma predeterminada y, como tal, no ejecutan LACP. Para configurar los puertos para utilizar el LACP, debe configurar el protocolo del canal en los módulos a LACP. El LACP y el PAgP no pueden ejecutarse en el mismo módulo de los switches que ejecutan CatOS.
- **set port lacp-channel** *port_range admin-key*
  Un parámetro **admin key** (clave administrativa) se intercambia en el paquete LACP. Un canal se forma solamente entre los puertos que tienen la misma clave de administración. El comando ***set port lacp-channel port_range admin-key command*** asigna a los canales un número de clave administrativa. El **comando show lacp-channel group** muestra el número. El **comando set port lacp-channel port_range admin-key** asigna la mima clave administrativa a todos los puertos en el intervalo de puerto. La clave administrativa se asigna al azar si no hay una clave específica configurada. Si lo desea, puede consultar la clave administrativa para administrar la adición y la extracción del puerto de canalización al mismo puerto agregado.
- **set port lacp-channel** *port_range* **mode active**
  El comando **set port lacp-channel port_range mode active** cambia el modo del canal a activo para un conjunto de puertos que fueron asignados previamente a la misma clave administrativa.

Además, LACP utiliza un temporizador interno de 30 segundos (Slow_Periodic_Time) después que se establecen los LACP EtherChannels. La cantidad de segundos antes de invalidar la información de LACPDU recibida, que se calcula con el uso de tiempos de espera largos (3 x Slow_Periodic_Time), es de 90 segundos. Use el UDLD, que es el detector más rápido de enlaces unidireccionales. No puede ajustar los temporizadores LACP y, en este punto, no puede configurar los switches para utilizar la transmisión de unidad de datos de protocolo rápida (PDU) (cada segundo) para mantener el canal después de que este se haya formado.

Otras Opciones

Si su plataforma requiere una administración mínima en la capa de acceso, una configuración común es establecer el modo a activo en las capas de distribución y de núcleo. Los switches de la capa de acceso se deben dejar en la configuración pasiva.

Detección de Link Unidireccional

UDLD es propiedad de Cisco, protocolo liviano desarrollado para detectar instancias de comunicaciones unidireccionales entre los dispositivos. Existen otros métodos para detectar el

estado bidireccional de los medios de transmisión, como FEFI, hay casos en que los mecanismos de detección L1 no son suficientes. Estos escenarios pueden resultar en uno de estos eventos:

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

El objeto de la función de UDLD es solucionar las siguientes condiciones de error en las interfaces Ethernet de fibra y cobre:

- Debe supervisar las configuraciones del cableado físico y, si hay puertos mal conectados, como errdisable.
- Debe proteger contra los links unidireccionales. Si se detecta un link unidireccional, debido a una falla en el funcionamiento de los medios o del puerto o interfaz, el puerto afectado se cierra como errdisable, y se genera el mensaje de syslog correspondiente.
- Además, el modo UDLD agresivo verifica que un link que previamente era considerado bidireccional no pierda la conectividad durante la congestión y se vuelva inutilizable. El UDLD realiza las pruebas de conectividad en curso a través del link. El propósito primario del modo agresivo UDLD es evitar los agujeros negros de tráfico en ciertas condiciones falladas.

El Spanning Tree, con su flujo BPDU unidireccional de estado estacionario, fue una víctima importante de estas fallas. Es fácil ver cómo un puerto puede repentinament perder su capacidad de transmitir BPDU y, provocar con ello, que el estado del STP cambie de bloqueo a envío en el vecino. Este cambio crea un loop, puesto que el puerto todavía puede recibir.

Información Operativa General

El UDLD es un protocolo L2 que funciona sobre la capa LLC (MAC de destino 01-00-0c-cc-cc-cc, tipo de protocolo SNAP HDLC 0x0111). Al ejecutar el UDLD junto con los mecanismos FEFI y de auto L1, es posible validar la integridad física (L1) y lógica (L2) de un link.

UDLD brinda prestaciones para funciones y protección que FEFI y la negociación automática no pueden ejecutar, concretamente la detección y captación de información vecina, el cierre de cualquier puerto mal conectado, y la detección de mal funcionamiento o fallas lógicas de puerto/interfaz lógica en links que no son punto a punto (aquellos a atraviesan convertidores de medios o hubs).

El UDLD emplea dos mecanismos básicos; detecta los vecinos, y mantiene la información actualizada en un caché local, y envía un tren de los mensajes de sonda/eco UDLD (de saludo) siempre que detecte un nuevo vecino o siempre que un vecino solicite la resincronización de la memoria caché.

El UDLD envía constantemente mensajes de sonda en todos los puertos en los que se habilite el UDLD. Si un puerto recibe un mensaje específico de “iniciación” del UDLD, se inician, se activa una fase de detección y un proceso de validación. Si al final de este proceso, se cumplen todas la condiciones válidas, el estado del puerto no se modifica. Para cumplir las condiciones, el puerto debe ser bidireccional y los cables deben estar conectados correctamente. Si no, el puerto es errdisable, y se muestra un mensaje de syslog. El mensaje de syslog es similar a estos mensajes:

- `UDLD-3-DISABLE: Unidirectional link detected on port [dec]/[dec]. Port disabled`
- `UDLD-4-ONEWAYPATH: A unidirectional link from port [dec]/[dec] to port[dec]/[dec] of device [chars] was detected`

Consulte Mensajes y Procedimientos de Recuperación (Catalyst Series Switch, 7.6) para una lista

completa de mensajes del sistema por recurso, que incluye los eventos UDLD.

Después de establecer un enlace y clasificarlo como bidireccional, el UDLD continúa enviando mensajes sonda/eco cada 15 segundos, el intervalo predeterminado. En esta tabla, se muestran los estados de enlace UDLD válidos en función del resultado del comando **show udld port**:

Estado de Puerto	Comentario
Indeterminado	El proceso de detección está en progreso o una entidad UDLD vecina se ha deshabilitado o su transmisión se ha bloqueado.
No aplicable	Se ha inhabilitado el UDLD.
Apagado	Se ha detectado el link unidireccional y el puerto ha sido deshabilitado.
Bidireccional	Se ha detectado el link bidireccional.

- **Mantenimiento de la memoria caché del vecino** : UDLD envía periódicamente paquetes de saludo de sonda/eco en cada interfaz activa para mantener la integridad de la memoria caché de vecino UDLD. Toda vez que reciba un mensaje de saludo, este se guardará en memoria y se almacenará por un período de tiempo máximo definido como período de inactividad. Cuando finaliza la retención de tiempo, caduca la entrada de memoria caché correspondiente. Si se recibe un nuevo mensaje de saludo dentro del período de inactividad, la nueva entrada reemplaza a la anterior y el temporizador de tiempo de vida correspondiente se reinicia.
- Con el objeto de mantener la integridad de la memoria caché UDLD, cada vez que una interfaz habilitada para UDLD se inhabilita o se reinicia un dispositivo, todas las entradas de memoria caché existentes para las interfaces afectadas por el cambio de configuración se borran y el UDLD transmite por lo menos un mensaje para informar a sus respectivos vecinos que purguen las entradas de memoria caché correspondientes.
- **Mecanismo de detección de eco** : el mecanismo que produce eco forma la base del algoritmo de detección. Cada vez que un dispositivo UDLD detecta un nuevo vecino o recibe una solicitud de resincronización de un vecino desincronizado, inicia/reinicia la ventana de detección en su lado de la conexión y envía una ráfaga de mensajes eco como respuesta. Debido a que este comportamiento debe ser el mismo en todos los vecinos, el emisor de eco espera recibir ecos como respuesta. Si las ventanas de detección finalizan y no se ha recibido un mensaje de respuesta válida, el link se considera unidireccional y este se reestablece o el proceso de cierre de puerto puede ser accionado.

Tiempo de Convergencia

Para impedir los loops STP, en CatOS 5.4(3) redujo el intervalo entre mensajes predeterminado del UDLD de 60 segundos a 15 segundos para cerrar un link unidireccional antes de que un puerto bloqueado pueda pasar al estado de envío.

Nota: 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 se establecen los vecinos UDLD, se envía el intervalo de mensaje configurado y se calcula un intervalo de tiempo de espera para ese peer (3 * message_interval). Por lo tanto, una relación de peer mide el tiempo de espera después de que se pierdan tres saludos consecutivos (o sondas). Con los intervalos de mensajes diferentes en cada lado, este valor de tiempo de espera es diferente en cada lado.

El tiempo aproximado necesario para que UDLD detecte una falla unidireccional es de (2.5 * message_interval + 4 segundos), es decir, unos 41 segundos si se utiliza el intervalo de mensaje predeterminado de 15 segundos. Este valor se encuentra muy por debajo de los 50 segundos que generalmente necesita el STP para volver a converger. Si la CPU del NMP dispone de algunos ciclos libres y si el usuario supervisa cuidadosamente su nivel de utilización, puede reducir el intervalo de mensaje (aun) al mínimo de 7 segundos. Con este intervalo de mensaje, la detección se puede acelerar la detección por un factor importante.

Por lo tanto, el UDLD tiene una dependencia asumida de los temporizadores del spanning tree predeterminado. Aunque el STP se puede modificar para que converja más rápidamente que el UDLD, es preferible considerar mecanismos alternativos, como la función protector de loop de CatOS 6.2. También considere un mecanismo alternativo cuando implemente RSTP (IEEE 802.1W) porque el RSTP tiene características de convergencia en milisegundos, que depende de la topología. Para estos casos, use la protección de loop conjuntamente con el UDLD, que proporciona la mayor parte de la protección. La protección de loop previene los loops de STP con la velocidad de la versión de STP que esté en funcionamiento, y el UDLD detecta las conexiones unidireccionales en los links EtherChannel individuales o en los casos en los que las BPDU no fluyen a lo largo de la dirección dañada.

Nota: El UDLD no detecta todas las situaciones de falla en el STP, por ejemplo las fallas que son causadas por el CPU que no envían BPDU por un tiempo mayor que (2 * FwdDelay + Maxage). Por esta razón, Cisco recomienda que implemente el UDLD conjuntamente con la protección de loop (que fue introducida en CatOS 6.2) en las topologías que confían en el STP.

Precaución: Tenga cuidado con las versiones anteriores del UDLD ya que estas utilizaban un intervalo de mensajes predeterminado y no configurable de 60 segundos. Estas versiones son susceptibles a las condiciones del loop spanning-tree.

Modo Agresivo UDLD

El modo agresivo del UDLD se ha creado como respuesta específica para algunos (pocos) casos en el que es necesario probar la conectividad bidireccional. Como tal, la característica del modo agresivo proporciona protección mejorada contra las condiciones peligrosas de link unidireccional en estas situaciones:

- Cuando las PDU del UDLD se pierden de manera simétrica y el tiempo de espera de ambos extremos se agota, ninguno de los puertos es errdisabled.
- Un lado de un link tiene un puerto atascado (ambos transmiten [Tx] y Rx).
- Un lado del link permanece arriba mientras que el otro lado desciende.
- La negociación automática, u otro mecanismo de detección de errores de la L1, está inhabilitada.
- Una reducción de la confianza en los mecanismos FEFI L1 es deseable.
- La protección máxima contra los errores de link unidireccional en los links de punto a punto FE/GE es necesaria. Específicamente, en donde no se soporta ninguna falla entre dos vecinos, es recomendable utilizar sondas de UDLD agresivo como “metrónomo”; la presencia

del cual garantiza la salud del enlace.

El caso más común para una implementación del UDLD agresivo es para comprobar la conectividad de un miembro de una agrupación cuando la negociación automática u otro mecanismo de detección de errores de la L1 está desactivado o no se usa. Esto es particularmente cierto con las conexiones EtherChannel debido a que tanto PAgP como LACP, aun estando deshabilitado, utilizan tiempos insuficientemente cortos en los temporizadores de saludo en el estado constante. En este caso, el UDLD agresivo tiene la ventaja agregada de prevención de los loops de spanning-tree posibles.

Las circunstancias que contribuyen a la pérdida simétrica de los paquetes de sondeo UDLD son más difíciles de caracterizar. Es necesario comprender que el UDLD normal continúa rastreando por si hubiera una condición de link unidireccional, incluso después que el estado de un link alcanza el estado bidireccional. La intención del UDLD es detectar problemas en la L2 que puedan generar loops del STP, los problemas de este tipo normalmente son unidireccionales porque las BPDU solo fluyen en una dirección en estado constante. Por lo tanto, el uso de UDLD normal junto con la negociación automática y la protección de loop (para las redes que dependen de STP) casi siempre es suficiente. Sin embargo, el modo UDLD agresivo es útil en situaciones en las que la congestión se ve igualmente afectada en ambas direcciones, lo que lleva a la pérdida de las sondas UDLD en las dos direcciones. Por ejemplo, esta pérdida de sondas UDLD puede producirse si la utilización de la CPU en cada extremo del link se eleva. Otros ejemplos de la pérdida de conectividad bidireccional incluyen el incidente de uno de estos dispositivos:

- Un transpondedor de multiplexión por división de longitud de onda densa (DWDM)
- Un conversor de medios
- Un hub
- Otro dispositivo L1**Nota:** El incidente no puede ser detectado por la negociación automática.

El error del UDLD agresivo inhabilita el puerto en estas situaciones de falla. Es importante que tenga en cuenta las ramificaciones si habilita el modo UDLD agresivo en los links que no son de punto a punto. Los links con los conversores de medios, los hubs, o los dispositivos similares no son de punto a punto. Los dispositivos intermedios pueden impedir el reenvío de los paquetes UDLD y forzar el cierre innecesario de un link.

Después de que todos los vecinos de un puerto hayan caducado, el modo UDLD agresivo (si está activado) reinicia la secuencia de conexión en un intento por volver a sincronizarse con un posible vecino que no esté sincronizado. Este esfuerzo se produce en el anuncio o la fase de la detección. Si después de un tren de mensajes rápido (ocho reintentos fallados), el link es aun considerado indeterminado, el puerto se coloca en el estado errDisable.

Nota: Algunos switches no son aptos para el modo UDLD agresivo. Actualmente, Catalyst 2900XL y Catalyst 3500XL tienen intervalos de mensajes codificados de 60 segundos. Este intervalo no se considera suficientemente rápido para proteger contra los loopes potenciales STP (con el uso de los parámetros del STP predeterminado).

UDLD en los Links Ruteados

A los fines de esta discusión, un link ruteado es uno de dos tipos de conexión:

- Punto a punto entre dos nodos del routerEste link se configura con una máscara de subred de 30 bits.
- Un VLAN con varios puertos pero que soporta solamente las conexiones ruteadasUn ejemplo de esto es una topología de núcleo de la L2

Cada Interior Gateway Routing Protocol (IGRP) tiene características únicas con respecto a cómo administra las relaciones de vecinos y la convergencia de ruta. Las características, que se discuten en esta sección, son relevantes cuando compara dos de los protocolos de ruteo más prevalentes utilizados hoy, Protocolo Open Shortest Path First (OSPF) e IGRP mejorado (EIGRP).

Primero, debe tener en cuenta que, una falla en la L1 o L2 en cualquier red enrutada de punto a punto tiene como consecuencia el desmembramiento casi inmediato de la conexión con la L3. Debido a que el puerto del switch en esa VLAN pasa a un estado no conectado en la falla L1/L2, la característica de estado automático MSCF sincroniza los estado de puerto L2 y L3 en aproximadamente dos segundos. Esta sincronización coloca la interfaz VLAN L3 en un estado encendido/apagado (con el protocolo de línea desactivado).

Suponga que los valores de los temporizadores son los predeterminados. El OSPF envía los mensajes de saludo cada 10 segundos y tiene un intervalo muerto de 40 segundos (4 * saludos). Estos temporizadores son constantes para el OSPF de punto a punto y las redes de broadcast. Debido a que el OSPF requiere la comunicación bidireccional para formar una adyacencia, el failover del peor de los casos es 40 segundos. Este failover es aplicable incluso si el fallo en la L1/L2 no es una falla pura en una conexión punto a punto, que deja un escenario semioperativo con el que el protocolo L3 debe negociar. Debido a que el tiempo de detección es muy similar al tiempo de un temporizador muerto OSPF que vence (cerca de 40 segundos), las ventajas de la configuración del modo normal UDLD en un link punto a punto L3 OSPF son limitadas.

En muchos casos, el EIGRP converge más rápidamente que el OSPF. Sin embargo, debe observar que la comunicación bidireccional no es necesaria para que los vecinos intercambien la información de ruteo. En los escenarios de falla semioperativos, el EIGRP es vulnerable al tráfico de agujeros negros que dura hasta que otro evento vuelva a “activar” los trayectos que pasan por ese vecino. El modo del UDLD normal puede aliviar las circunstancias descritas en esta sección. El modo del UDLD normal detecta la falla del link unidireccional y aplica el comando errdisable para desactivar el puerto.

Para las conexiones L3 ruteadas que utilizan cualquier protocolo de ruteo, el UDLD normal todavía proporciona protección contra los problemas sobre la activación del link inicial. Tales problemas incluyen problemas de cableado o hardware defectuoso. Además, el modo agresivo UDLD proporciona estas ventajas en las conexiones L3 ruteadas:

- Previene los envíos a agujeros negros innecesarios de tráfico**Nota:** Los temporizadores mínimos se requieren en algunos casos.
- Coloca un link inestable en el estado errdisable
- Protege contra los loops que resultan de las configuraciones de EtherChannel L3

Comportamiento predeterminado del UDLD

El UDLD está globalmente desactivado y preparado para la habilitación en puertos de fibra de manera predeterminada. Debido a que UDLD es un protocolo de infraestructura necesaria entre los switches solamente, el UDLD está desactivado en los puertos de cobre de forma predeterminada. Los puertos de cobre tienden a ser utilizados para el acceso del host.

Nota: El UDLD se debe habilitar de forma global y en el nivel de la interfaz antes de que los vecinos puedan alcanzar el estado bidireccional. En CatOS 5.4(3) y posterior, el intervalo de mensajes predeterminado es 15 segundos y es configurable entre 7 y 90 segundos.

La recuperación errdisable global se inhabilita de forma predeterminada. Después de que se

habilite de forma global, si un puerto entra en el estado errdisable, el puerto se vuelve a habilitar 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. Puede prevenir manualmente una rehabilitación del puerto si establece el tiempo de espera errdisable para ese puerto a desactivado. Ejecute el comando ***set port errdisable-timeout mod/port disable***.

Nota: El uso de este comando depende de su versión de software.

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.

Consulte Configuring Ethernet, Fast Ethernet, Gigabit Ethernet, y 10-Gigabit Ethernet Switching para obtener más detalles sobre cómo configurar un período de tiempo de espera para los puertos que están en estado en el estado errdisable.

Recomendación

El modo normal UDLD es suficiente en la gran mayoría de los casos si lo utiliza correctamente y conjuntamente con las características y los protocolos apropiados. Estas características/protocolos incluyen:

- FEFI
- Autonegotiation
- Protección de loop

Cuando implementa el UDLD, considere si una prueba en curso de la conectividad bidireccional (modo agresivo) es necesaria. Típicamente, si se habilita la negociación automática, el modo agresivo no es necesario porque la negociación automática compensa la detección de falla en el L1.

Cisco recomienda la habilitación del modo del UDLD normal en todos los links de punto a punto FE/GE entre los switches Cisco en los cuales el intervalo de mensaje de UDLD se fija al valor predeterminado de 15 segundos. Esta configuración asume los temporizadores del spanning tree 802.1d predeterminados. Además, use el UDLD conjuntamente con la protección de loop en las redes que dependen en el STP para la redundancia y la convergencia. Esta recomendación se aplica a las redes en las que hay uno o más puertos en el estado de bloqueo STP en la topología.

Ejecute estos comandos para habilitar el UDLD:

```
set udld enable
!--- After global enablement, all FE and GE fiber !--- ports have UDLD enabled by default. set
udld enable port range
!--- This is for additional specific ports and copper media, if needed.
```

Debe habilitar manualmente los puertos que son inhabilitados por error debido a los síntomas del link unidireccional. Ejecute el **comando set port enable**.

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

Otras Opciones

Para la protección máxima contra los síntomas que resultan de los links unidireccionales, configure el UDLD de modo agresivo:

set udld aggressive-mode enable *port_range*

Además, puede ajustar el valor del intervalo de mensaje de UDLD entre 7 y 90 segundos en cada extremo, si es soportado, para una convergencia más rápida:

set udld interval *time*

Considere el uso de la característica del tiempo de espera errdisable en cualquier dispositivo que pueda aislarse de la red en caso de situación de errdisable. Esta situación de la capa de acceso suele ser real y cuando implemente el modo agresivo UDLD sin capacidades de administración de red fuera de banda.

Si un puerto se coloca en el estado errdisable, el puerto permanece desactivado de forma predeterminada. Puede ejecutar este comando, que vuelve a permitir los puertos después de un intervalo de tiempo de espera:

Nota: El intervalo de tiempo de espera es 300 segundos de forma predeterminada.

```
>set errdisable-timeout enable ?
bpdu-guard
!--- This is BPDU port-guard. channel-misconfig !--- This is a channel misconfiguration. duplex-
mismatch udld other !--- These are other reasons. all !--- Apply errdisable timeout to all
reasons.
```

Si el dispositivo asociado no es compatible con UDLD, por ejemplo, un host extremo o el router, no ejecute el protocolo. Ejecutar este comando:

set udld disable *port_range*

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, para una llevar a cabo una comprobación sencilla en la que se desconecta estado errdisable deseado, debe haber desactivado la negociación automática L1. De lo contrario, el puerto físico se desactiva, lo que reajusta la comunicación de mensaje UDLD. El extremo remoto pasa al estado indeterminado en el UDLD normal. Si utiliza al modo agresivo UDLD, el extremo remoto pasa al estado errdisable.

Hay un método adicional de la prueba para simular la pérdida de PDU vecino para el UDLD. Use filtros de la capa MAC para bloquear UDLD/CDP a la dirección de hardware pero permita que pasen otras direcciones.

Para monitorear el UDLD, ejecute estos comandos:

```
>show udld

UDLD              : enabled
Message Interval  : 15 seconds
```

```
>show udld port 3/1

UDLD              : enabled
Message Interval  : 15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ---------------
3/1      enabled       disabled         bidirectional
```

Además, desde el modo enable, puede ejecutar el comando show udld neighbor para verificar el contenido caché inmediato UDLD (de la manera que lo hace el CDP). Suele ser útil una comparación de caché inmediata UDLD a la caché CDP para verificar si hay una anomalía del protocol específico. Siempre que el CDP sea también afectado, generalmente significa que todas las BPDU/PDU están afectadas. Por lo tanto, también verifique el STP. Por ejemplo, verifique las modificaciones recientes de identidad o cambios en la ubicación de los puertos raíz o designados.

```
>show udld neighbor 3/1

Port  Device Name            Device ID    Port-ID OperState
----- --------------------  ------------ ------- ----------
3/1   TSC07117119M(Switch)   000c86a50433 3/1     bidirectional
```

Además, el estado y consistencia de la configuración del UDLD también se pueden consultar con las variables UDLD SNMP MIB de Cisco.

Trama Jumbo

La unidad de transmisión máxima (MTU) es de 1518 bytes para todos los puertos Ethernet, incluidos los puertos GE y 10 GE. La trama jumbo habilita las interfaces para conmutar las tramas que son más grandes que los tamaños de trama Ethernet estándar. La función es útil para optimizar el desempeño servidor a servidor y para poder utilizar aplicaciones como Switching de la Etiquetas de Protocolos Múltiples (MPLS), tunelización 802.1Q, L2 Tunneling Protocol Versión 3 (L2TPv3), que aumentan el tamaño de las tramas originales.

Información Operativa General

La especificación estándar de IEEE 802.3 define los tamaños de trama Ethernet máximos de 1518 bytes para las tramas regulares y de 1522 bytes para las tramas encapsuladas 802.1Q. Las tramas encapsuladas 802.1Q a veces se denominan “baby giants”. Los paquetes se clasifican generalmente como tramas Baby giant cuando exceden la longitud máxima Ethernet especificada Ethernet para una conexión de Ethernet específica. Los paquetes Baby giant también se conocen como tramas Jumbo.

Hay diversas razones por las que el tamaño de la MTU de ciertas tramas puede exceder los 1518 bytes. Los siguientes son algunos ejemplos:

- Requisitos Específicos del proveedor: las aplicaciones y ciertos NIC pueden especificar un tamaño de MTU fuera del estándar de 1500 bytes. La tendencia a especificar tales tamaños de MTU se debe a los estudios se han realizado, que prueban que un aumento en los tamaños 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. En la actualidad, las dos las formas más comunes de trunking son la encapsulación ISL patentada por Cisco y IEEE 802.1Q.
- MPLS — Después de que el MPLS se habilite en una interfaz, tiene el potencial para

aumentar el tamaño de trama de un paquete. Este aumento depende del número de etiquetas en la stack de etiquetas para un paquete con etiqueta MPLS. El tamaño total de la etiqueta es 4 bytes. El tamaño total de una stack de etiqueta es *n* x 4 bytes. Si se forma una pila de etiquetas, es posible que las tramas excedan la MTU.
- Tunelización 802.1Q: los paquetes de tunelización 802.1Q contienen dos etiquetas 802.1Q, de las cuales solo una a la vez es visible generalmente para el hardware. Por lo tanto, la etiqueta interna agrega 4 bytes al valor MTU (tamaño del contenido).
- Interfaz de Transporte Universal (UTI)/L2TPv3: la UTI/L2TPv3 encapsula los datos L2 que deben ser reenviados por la red IP. La encapsulación puede aumentar los tamaños de trama originales en hasta 50 bytes. La nueva trama incluye un nuevo encabezado IP (20 bytes), un encabezado L2TPv3 (12 bytes), y un nuevo encabezado L2. El contenido del L2TPv3 consiste en la trama completa L2, que incluye el encabezado L2.

La capacidad de los diversos switches de Catalyst de soportar los diversos tamaños de trama depende de muchos factores, que incluyen el hardware y software. Los módulos determinados pueden soportar tamaños de trama más grandes que otros, incluso dentro de la misma plataforma.

- Los switches Catalyst 5500/5000 proporcionan soporte para la trama Jumbo en la versión de CatOS 6.1. Cuando la característica de las tramas Jumbo se habilita en un puerto, el tamaño de MTU aumenta a 9216 bytes. En las tarjetas de línea de par trenzado sin blindaje (UTP) de 10/100 Mbps, el tamaños máximo de la trama que se soportan es solo 8092 bytes. Esta limitación es una limitación ASIC. Generalmente, no hay restricciones en la habilitación de la característica del tamaño de trama Jumbo. Puede utilizar esta característica con trunking/sin trunking y canalización/sin canalización.
- Los switches Catalyst 4000 (Supervisor Engine 1 [WS-X4012] y Supervisor Engine 2 [WS-X4013]) no soportan las tramas Jumbo debido a una limitación ASIC. Sin embargo, la excepción es el trunking 802.1Q.
- La plataforma de Catalyst 6500 Series puede soportar los tamaños de trama Jumbo en la versión de CatOS 6.1(1) y posterior. Sin embargo, este soporte depende del tipo de tarjetas de línea que utilice. Generalmente, no hay restricciones en la habilitación de la característica del tamaño de trama Jumbo. Puede utilizar esta característica con trunking/sin trunking y canalización/sin canalización. El tamaño de MTU predeterminado es 9216 bytes después de que el soporte de trama Jumbo se haya habilitado en el puerto individual. El MTU predeterminada no es configurable con el uso de CatOS. Sin embargo, Cisco IOS Software Release 12.1(13)E presentó el **comando system jumbomtu** para reemplazar la MTU predeterminado.

Consulte Ejemplo de Configuración del Soporte de Tramas Jumbo/Giant en los Switches Catalyst para obtener más información.

Esta tabla describe las tamaños de la MTU que son soportados por las tarjetas de línea diferentes para los switches Catalyst series 6500/6000:

Nota: El tamaño de la MTU o del paquete se refiere solamente al contenido de Ethernet.

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(V), WS-X6348-RJ-21(V)	8092 bytes (limitado por el chip PHY)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V) WS-X6148-45AF, WS-X6148-21AF	9100 bytes (a 100 Mbps) 9216 bytes (a 10 Mbps)
WS-X6148A-RJ-45, WS-X6148A-45AF, WS-X6148-FE-SFP	9216 bytes
WS-X6324-100FX-MM, -SM, WS-X6024-10FL-MT	9216 bytes
WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-MM WS-X6148X2-RJ-45, WS-X6148X2-45AF WS-X6196-RJ-21, WS-X6196-21AF WS-X6408-GBIC, WS-X6316-GE-TX , WS-X6416-GBIC WS-X6516-GBIC, WS-X6516A-GBIC, WS-X6816-GBIC Uplinks de Supervisor Engine 1, 2, 32 y 720	9216 bytes
WS-X6516-GE-TX	8092 bytes (a 100 Mbps) 9216 bytes (a 10 o 1000 Mbps)
WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF, WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF	1500 bytes (trama Jumbo no soportada)
WS-X6148A-GE-TX, WS-X6148A-GE-45AF, WS-X6502-10GE, WS-X67xx Series	9216 bytes
OS ATM (OC12c)	9180 bytes
OSM CHOC3, CHOC12, CHOC48, CT3	9216 bytes (OCx y DS3) 7673 bytes (T1/E1)

Flex WAN	7673 bytes (CT3 T1/DS0) 9216 bytes (OC3c POS) 7673 bytes (T1)
CSM (WS-X6066-SLB-APC)	9216 bytes (a partir de CS 3.1(5) y 3.2(1))
OSM POS OC3c, OC12c, OC48c; OSM DPT OC48c, OSM GE WAN	9216 bytes

Soporte de Trama Jumbo de la Capa 3

Con CatOS que se ejecuta en Supervisor Engine y Cisco IOS Software que se ejecuta en el MSFC, los switches Catalyst 6500/6000 también proporcionan el soporte de Trama Jumbo L3 en el Software Release 12.1(2)E y Posterior de Cisco IOS® con el uso de PFC/MSFC2, el PFC2/MSFC2, o el hardware posterior. Si las VLAN de ingreso y egreso se configuran para soportar el uso de tramas jumbo, el PFC conmuta por hardware a todos los paquetes a la velocidad permitida por los cables. Si la VLAN de ingreso se configura para las tramas jumbo y la VLAN de egreso no se configura, hay dos situaciones:

- Una trama jumbo enviada por el host final en la que se ha insertado el bit Don't Fragment: el paquete se descarta y se envía el mensaje de Internet Control Message Protocol (ICMP) al host final, en el que se indica la imposibilidad de establecer la conexión con el código de mensaje fragment needed and DF set.
- Una trama Jumbo enviada por el host final que no incluye el bit DF: los paquetes se rebotan al MSFC2/MSFC3 para fragmentarlos y conmutarlos en el software.

Esta tabla resume el soporte de Jumbo L3 para las diversas plataformas:

Switch L3 o Módulo	Talla de MTU L3 máximo
Catalyst serie 2948G-L3/4908G-L3	Las tramas Jumbo no se soportan.
Catalyst 5000 RSM1/RSFC2	Las tramas Jumbo no se soportan.
Catalyst 6500 MSFC1	Las tramas Jumbo no se soportan.
Catalyst 6500 MSFC2 y posterior	Cisco IOS Software Release 12.1(2)E: 9216 bytes

[1] RS = Route Switch Module

[2] RSFC = Route Switch Feature Card

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 que está basado en lo siguiente:

- El Tamaño Máximo de Segmento (MSS), que es la longitud MTU menos la longitud de los encabezados TCP/IP
- El Viaje de Ida y de Vuelta (RTT)
- La pérdida de paquetes

Según esta fórmula, el rendimiento de procesamiento de TCP máximo que es directamente proporcional al MSS. Con el RTT constante y la pérdida del paquete, puede duplicar el rendimiento de procesamiento de TCP si duplica el tamaño del paquete. 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.

En segundo lugar, las exigencias cada vez mayores de desempeño que se piden a los bloques de servidores requieren sistemas más eficaces para garantizar una mayor velocidad de datos con los datagramas UDP del Sistema de Archivos de Red (NFS). El NFS es el mecanismo de almacenamiento de datos para la transferencia de archivos entre servidores basados en UNIX de mayor implantación y cuneta con datagramas de 8400 bytes. Como la MTU extendida de 9 KB que se utiliza en Ethernet, una única trama jumbo es suficientemente grande como para transportar un datagrama de aplicación de 8KB (por ejemplo, NFS), incluida la carga adicional que supone el encabezado del paquete. Casualmente, esta capacidad permite transferencias más eficientes del acceso directo a memoria (DMA) en los hosts porque el software no necesita más para hacer fragmentos de los bloques NFS en los datagramas de UDP separados.

Recomendación

Si se desea soporte para las tramas jumbo, circunscriba el uso de la tramas jumbo solo a las áreas de la red en las que todos los módulos switch (L2) e interfaces (L3) soporten tramas Jumbo. Esta configuración previene la fragmentación en cualquier parte de la trayectoria. La aplicación de tramas jumbo cuyo tamaño es superior al de la longitud de trama en la trayectoria, inutiliza cualquier beneficio obtenido con el uso de esta función, la fragmentación de las tramas es necesaria. Como muestra la tabla en esta sección de Trama Jumbo, diferentes plataformas y tarjetas de línea ofrecen variaciones en cuanto al tamaño de paquete máximo que soportan.

Configure los dispositivos host detectores de tramas jumbo con un tamaño de MTU que sea el mínimo denominador común soportado por el hardware de red, para toda la VLAN de la L2 en la que está instalado el dispositivo host. Para habilitar el soporte de trama Jumbo para los módulos con el soporte de trama Jumbo, ejecute este comando:

```
set port jumbo mod/port enable
```

Además, si desea el soporte de trama Jumbo a través de los límites L3, configure el valor disponible más grande MTU de 9216 bytes en todas las interfaces VLAN aplicables. Ejecute el **comando mtu** en las interfaces VLAN:

interface vlan *vlan#* **mtu 9216**
Esta configuración garantiza que la trama L2 jumbo MTU que es soportada por los módulos sea siempre inferior, o igual al valor que se configura para las interfaces L3 que el tráfico atraviesa. Esto previene la fragmentación cuando el tráfico es ruteado a partir de la VLAN a través de la interfaz L3.

Configuración de la Administración

Las consideraciones para ayudar a controlar, proporcionar, y a resolver problemas en una red Catalyst se discuten en esta sección.

Diagramas de la Red

Los diagramas de redes limpios son fundamentales en el funcionamiento de las redes. Se vuelven críticos durante la resolución de problemas y son el único vehículo más importante para comunicar información mientras se deriva a los proveedores y partners durante una interrupción. Su preparación, disposición, y accesibilidad no deben ser subestimados.

Recomendación

Cisco recomienda que cree estos tres diagramas:

- **Diagrama general:** incluso para las redes más grandes, un diagrama que muestra que la conectividad de punta a punta y la conectividad lógica son importantes. Puede ser frecuente para las empresas que han implementado un diseño jerárquico para documentar cada capa por separado. Durante la planificación y la resolución de problemas, sin embargo, a menudo, el tener un conocimiento solvente de cómo enlazan los dominios es el factor más importante.
- **Diagrama físico** : muestra todo el hardware y cableado del switch y del router. Los trunks, los links, las velocidades, los grupos de canal, los números del puerto, las ranuras, los tipos de chasis, el software, los dominios VTP, el Root Bridge, la prioridad de root bridge de respaldo, la dirección MAC, y los puertos bloqueados por la VLAN deben ser etiquetados. Muchas veces es más claro mostrar los dispositivos internos, como la MSFC del Catalyst 6500/6000, como un router en un palillo conectado a través de un trunk.
- **Diagrama lógico**: muestra solo funcionalidad L3 (routers como objetos, VLAN como segmentos de Ethernet). Las direcciones IP, las subredes, el direccionamiento secundario, el HSRP activo y en espera, las capas de acceso, de distribución o de núcleo y la información de enrutamiento deben etiquetarse.

Administración en Banda

Según la configuración, la interfaz de administración (interna) del switch en banda (conocida como sc0) podría tener que manejar estos datos:

- Protocolos del administrador de switches tales como SNMP, Telnet, Secure Shell Protocol (SSH), y syslog
- Datos del usuario tales como broadcasts y multicasts
- Protocolos de control del switch tales como STP BPDU, VTP, DTP, CDP, etc.

Una práctica común en los sistemas Cisco con diseño multicapa es configurar una VLAN

administrativa que se extienda a todo el dominio conmutado y contenga todas las interfaces sc0. De este modo, el tráfico administrativo y el tráfico de usuarios se mantienen asilados y se mejora la seguridad de las interfaces de administración de switch. Esta sección describe la significación y los posibles problemas que implican el uso de la VLAN 1 predeterminada y que el tráfico administrativo se conduzca al switch a través de la misma VLAN que el tráfico de los usuarios.

Información Operativa General

El problema principal sobre el uso del VLAN1 para los datos del usuario es que el Supervisor Engine NMP en general no necesita ser interrumpido por el tráfico multicast y broadcast que es generado por las estaciones finales. El hardware Catalyst 5500/5000 anterior, los motores Supervisor I y Supervisor II, y en mayor medida este último, disponían de recursos limitados para la gestión de este tráfico, aunque la situación es común a todos los motores Supervisor Engine. Si la CPU de Supervisor Engine, el buffer, o el canal dentro de la banda al backplane está totalmente ocupado escuchando el tráfico innecesario, es posible que no se detecten las tramas de control. En el pero de los casos, esto podía llevar a un loop de Spanning-Tree o a una falla de EtherChannel.

Si se ejecutan los comandos show interface y show ip stats en Catalyst, pueden dar una cierta indicación de la proporción de tráfico broadcast a unicast y de la proporción de tráfico IP a tráfico no IP (vino se observa habitualmente en las VLAN administrativas).

Otra verificación de la integridad para un hardware anterior de Catalyst 5500/5000 es examinar la salida de **show inband** / ***biga*** (comando oculto) para los errores de recurso (RscrcErrors), similar a las caídas del buffer en un router. Si hay errores de recurso continuos, la memoria no está disponible para recibir los paquetes del sistema, quizás debido a una cantidad significativa de tráfico de broadcast en la VLAN administrativa. Un único error de recursos puede significar que el motor de supervisor no tiene capacidad para procesar un paquete, como una BPDU. Esta situación se puede volver problemática en poco tiempo porque los protocolos, como el spanning tree, no vuelven a enviar las BPDU perdidas.

Recomendación

Como se destacó en la sección de Control de Cat este documento, la VLAN1 es un VLAN especial que etiqueta y maneja la mayor parte del tráfico de plano del control. La VLAN1 se habilita en todos los trunks de forma predeterminada. Con redes de campus de mayor tamaño, debe obrarse con cautela acera del diámetro del **dominio STP** VLAN1; la inestabilidad en una parte de la red podía afectar la VLAN1, y repercutir en la estabilidad del plano de control y del STP para todas las otras VLAN. En CatOS 5.4 y posterior, ha sido posible limitar la VLAN1 del transporte los datos de usuarios y ejecute el STP, el comando es:

```
clear trunk mod/port vlan 1
```

Esto no hace que se detengan los paquetes de control enviados de switch a switch en la VLAN 1, tal como se ve con un analizador de red. Sin embargo, no se reenvían datos, y el STP no debe ejecutarse sobre este link. Por lo tanto, esta técnica se puede utilizar para dividir la VLAN 1 en dominios de fallas más pequeños.

Nota: Actualmente no es posible borrar los trunks VLAN1 en las versiones 3500 y 2900XL.

Incluso si se ha tenido cuidado de diseñar el campus para que el tamaño de los dominios conmutados de las VLAN de usuario sea relativamente pequeño y, en consecuencia, también los

límites de falla/L3 sean pequeñas, algunos clientes tratan la VLAN de administración de manera diferente y tratan de cubrir toda la red con una subred de administración simple. No hay un motivo técnico por el que una aplicación NMS central debe ser adyacente a L2 a los dispositivos que administra, ni tampoco es un argumento de seguridad calificado. Cisco recomienda que limite el diámetro de las VLAN administrativas a la misma estructura de dominio ruteada que las VLAN de usuarios y administración fuera de banda o soporte de CatOS 6.x SSH como una forma de aumentar la seguridad de la administración de red.

Otras Opciones

Sin embargo, hay aspectos del diseño para estas recomendaciones de Cisco en algunas topologías. Por ejemplo, un diseño común y deseable multicapa de Cisco es uno que evita el uso de un spanning-tree activo. Esto requiere que cada subred IP o VLAN se restrinja a un único switch de capa de acceso, o clúster de switches. En estos diseños, no hay trunking configurado hacia la capa de acceso.

No hay respuesta fácil a la pregunta de si una VLAN de administración separada está creada y el trunking está habilitado para llevarla entre el acceso L2 y las capas de distribución L3. Estas son dos opciones para la revisión del diseño con su ingeniero de Cisco:

- **Opción 1:** conecte mediante trunk dos o tres VLAN únicas de la capa de distribución a cada switch de capa de acceso. Esto permite una VLAN de datos, una VLAN de voz, y una VLAN de administración, por ejemplo, y aun tiene la ventaja de que el STP está inactivo. (Tenga en cuenta que si el VLAN1 se borra de los trunks, hay un paso de configuración adicional). En esta solución, también hay puntos de diseño que deben considerarse para evitar la confección de agujeros negros temporarios del tráfico ruteado durante la recuperación de errores: STP PortFast para trunks (CatOS 7.x y posterior) o sincronización Autostate VLAN con el reenvío STP (posterior a CatOS 5.5[9]).
- **Opción 2:** una solaq VLAN para los datos y la administración podía ser aceptable. Con un hardware más nuevo de switch, tal como CPU mucho más potentes y controles de limitación de la velocidad de la de plano de control, más un diseño con los dominios de broadcast relativamente pequeños apoyados por el diseño multicapa, la realidad para muchos clientes es que guardar la interfaz del sc0 separada de los datos del usuario es menos problemático que antes. Para tomar una decisión final, lo mejor es analizar el perfil de tráfico de broadcast para esa VLAN y una discusión de las capacidades del hardware del switch con el ingeniero de Cisco. Si la VLAN de administración contiene de hecho todos los usuarios en ese switch de capa de acceso, el uso de los filtros de entrada del IP se recomienda altamente para asegurar el switch de los usuarios, como se debate en la sección de Configuración de Seguridad de este documento.

Administración Fuera de Banda

Profundizando sobre los argumentos de la sección anterior, es posible mejorar la disponibilidad con una infraestructura autónoma de administración alrededor de la red de producción. Con esto se permite que los dispositivos estén siempre disponibles desde una posición remota sin que afecten los eventos del tráfico o del plano de control. Estos dos enfoques son típicos:

- Administración Fuera de Banda con una LAN exclusiva
- Administración Fuera de Banda con los Servidores Terminales

Información Operativa General

Los routers y switches de la red pueden incluir una interfaz de administración de Ethernet fuera de banda en una VLAN de administración. Un acceso de Ethernet en cada dispositivo se configura en la VLAN de administración y se conecta fuera de la red de producción a una una red de administración conmutada distinta a través de la interfaz sc0. Tenga en cuenta que los switches Catalyst 4500/4000 tienen una interfaz me1 especial en el Supervisor Engine que se utiliza exclusivamente para la administración fuera de banda, no como puerto de switch.

Además, la conectividad del servidor terminal se puede alcanzar con la configuración de Cisco 2600 o 3600 con los cables RJ-45 a serial para acceder al puerto de la consola de cada router y switch en la disposición. Un servidor terminal también evita la necesidad de la configuración de los escenarios de respaldo, tales como módems en los puertos auxiliares para cada dispositivo. Un solo módem se puede configurar en el puerto auxiliar del servidor terminal para proporcionar el servicio de marcación manual a los otros dispositivos durante una falla de conectividad de red.

Recomendación

Con este arreglo, dos trayectorias fuera de banda a cada switch y router son posibles además de las numerosas trayectorias dentro de la banda, lo que habilita la administración de red de gran disponibilidad. El soporte fuera de banda es responsable de:

- El soporte fuera de banda separa el tráfico de administración de los datos del usuario.
- El soporte fuera de banda tiene la dirección IP de administración en una subred, una VLAN, y un switch distintos para mayor seguridad.
- El soporte fuera de banda proporciona la garantía más alta para la entrega de datos de administración durante los desperfectos de la red.
- El soporte fuera de banda no tiene ningún Spanning-Tree activo en la VLAN de administración. La redundancia no es crítica.

Pruebas del Sistema

Diagnósticos de Arranque

Durante un arranque inicial del sistema, varios procesos se realizan para garantizar que una plataforma confiable y operativa está disponible de modo que el hardware defectuoso no interrumpa la red. Los diagnósticos de arranque de Catalyst se dividen entre la Prueba Automática de Encendido (POST) y el diagnóstico en línea.

Información Operativa General

Según la plataforma y la configuración del hardware, diversos diagnósticos se realizan en el arranque inicial y cuando una tarjeta se intercambia en caliente en el chasis. Un nivel más alto de diagnósticos resulta en un número más amplio de problemas detectados pero en un ciclo de arranque más largo. Estos tres niveles de diagnósticos del POST pueden ser seleccionados (todas las pruebas marcan DRAM, RAM, presencia y tamaño de caché, y los inicializan):

Información Operativa General			
Pue	N/A	3	No disponible en las

nte			series 4500/4000 con CatOS 5.5 o anterior.
Mínimo	Pruebas de escritura de patrones en el primer MB de DRAM solamente.	30	Predeterminado en las series 5500/5000 y 6500/6000; no disponible en las series 4500/4000.
Completo	Pruebas de escritura de patrones para toda la memoria.	60	Predeterminado en las series 4500/4000.

Diagnóstico en Línea

Estas pruebas verifican las trayectorias de paquetes internamente en el switch. Es importante tener en cuenta que los diagnósticos en línea son, en consecuencia, pruebas de todo el sistema, no solo de los puertos. En los switches Catalyst 5500/5000 y 6500/6000, las pruebas se realizan primero a partir del Supervisor Engine en espera, y otra vez a partir del Supervisor Engine principal. La longitud de los diagnósticos depende de la configuración del sistema (cantidad de ranuras, módulos y puertos). Hay tres categorías de prueba:

- Prueba de loopback: los paquetes de Supervisor Engine NMP se envían a cada puerto, después se vuelven al NMP y se examinan para determinar si tienen errores.
- Prueba de agrupamiento: los canales de hasta ocho puertos se crean y las pruebas de loopback se realizan en el puerto agregado para verificar el hash a los links específicos (consulte la sección EtherChannel de este documento para más información).
- Prueba de Lógica de Reconocimiento de Dirección Codificada (EARL): se prueban el Supervisor Engine central y los motores de reescritura del módulo L3 Ethernet. Se crean las entradas y los puertos ruteados del hardware que reenvía antes de que los paquetes de la muestra se envíen (para cada tipo de la encapsulación de protocolo) del NMP a través del hardware de switching en cada módulo y de nuevo al NMP. Esto es para los módulos Catalyst 6500/6000 y lo módulos más nuevos.

Los diagnósticos en línea completos pueden tardar aproximadamente dos minutos. Los diagnósticos mínimos no realizan la prueba de conjunto o de reescritura en los módulos que no sean Supervisor Engine, y pueden tardar aproximadamente 90 segundos.

Durante una prueba de memoria, si hay diferencias entre el patrón leído y el patrón escrito, el estado del puerto cambia adefectuoso. Los resultados de estas pruebas se pueden considerar si se ejecuta el **comando show test**, seguido por el número de módulo que se examinará:

```
>show test 9

Diagnostic mode: complete (mode at next reset: complete)
!--- Configuration setting. Module 9 : 4-port Multilayer Switch Line Card Status for Module 9 :
PASS Port Status : Ports 1 2 3 4 ---------------- . . . . Line Card Diag Status for Module 9 (.
= Pass, F = Fail, N = N/A) Loopback Status [Reported by Module 1] : Ports 1 2 3 4 ----------
--- . . F . !--- Faulty. Channel Status : Ports 1 2 3 4 ---------------- . . . .
```

Recomendación

Cisco recomienda que todos los switches estén configurados para utilizar los diagnósticos completos para proporcionar la máxima detección de fallas y para prevenir las interrupciones durante los funcionamientos normales.

Nota: Este cambio no surte efecto hasta la próxima vez que se inicia el dispositivo. Ejecute este comando para configurar los diagnósticos completos:

```
set test diaglevel complete
```

Otras Opciones

En algunas situaciones, un tiempo rápido de función de arranque puede ser preferible en lugar de esperar para ejecutar los diagnósticos completos. Hay otros factores y sincronizaciones implicados en la activación de un sistema, pero en general, el diagnóstico POST y el diagnóstico en línea agregan alrededor de un tercio más al tiempo de inicialización original. En la prueba con un solo chasis completamente poblado de nueve ranuras de Supervisor Engine con un Catalyst 6509, el tiempo total de arranque era de alrededor 380 segundos con los diagnósticos completos, alrededor de 300 segundos con los diagnósticos mínimos, y solamente 250 segundos con los diagnósticos desviados. Ejecute este comando para configurar la desviación:

```
set test diaglevel bypass
```

Nota: El Catalyst 4500/4000 puede ser configurado para los diagnósticos mínimos, aunque esto todavía da lugar a una prueba completa. El modo mínimo podría ser soportado en el futuro en esta plataforma.

Diagnósticos en Tiempo de Ejecución

Una vez que el sistema es operativo, Supervisor Engine del switch realiza varios monitoreos de los otros módulos. Si un módulo no es accesible a través de los mensajes de administración (Serial Control Protocol [SCP] que se ejecuta en el bus de administración fuera de banda), Supervisor Engine intenta reiniciar la tarjeta o toma otra medida adecuada.

Información Operativa General

Supervisor Engine realiza diversos monitoreos automáticamente; esto no requiere ninguna configuración Para Catalyst 5500/5000 y 6500/6000, estos componentes del switch se monitorean:

- NMP a través de un watchdog
- Errores del chip de la EARL mejorada
- Canal dentro de la banda de Supervisor Engine a backplane
- Módulos a través de keepalives sobre el canal fuera de banda (Catalyst 6500/6000)
- El estado del Supervisor Engine activo es monitoreado por el Supervisor Engine en espera (el Catalyst 6500/6000)

Detección de Errores del Sistema y de Hardware

Información Operativa General

En CatOS 6.2 y posterior, otras funciones se han agregado para monitorear los componentes del sistema crítico y del nivel del hardware. Se soportan estos tres componentes de hardware:

- Inband

- Contador de puerto
- Memoria

Cuando se habilita la característica y se detecta una condición de error, el switch genera un mensaje de syslog. El mensaje informa al administrador que existe un problema antes de que ocurra una degradación notable del rendimiento. En las versiones CatOS 6.4(16), 7.6(12), 8.4(2) y posterior, el modo predeterminado para los tres componentes pasa de deshabilitado a habilitado.

Inband

Si se detecta un error dentro de la banda, un mensaje de syslog le informa que existe un problema antes de que ocurra una degradación notable del rendimiento. El error muestra el tipo de ocurrencia de una falla dentro de la banda. Algunos ejemplos son los siguientes:

- La señal en banda está atascada
- Errores de recurso
- La señal en banda ha fallado durante la inicialización

En la detección de una falla de ping dentro de la banda, la característica también señala un mensaje de syslog adicional con una dispositiva de la velocidad actual del Tx y Rx en la conexión dentro de la banda, la CPU, y la carga de backplane del switch. Este mensaje le permite determinar correctamente si la señal en banda está atascada (ningún Tx/Rx) o sobrecargada (Tx/Rx excesivo). Esta información adicional puede ayudarle a determinar la causa de las fallas de ping dentro de la banda.

Contador de Puerto

Cuando habilita esta característica, crea y comienza un proceso para hacer el debug de los contadores de puerto. Los monitores del contador de puerto seleccionan periódicamente los contadores de errores del puerto interno. La arquitectura de la tarjeta de línea, y más específicamente los ASIC en el módulo, determina que contadores requiere la función. El Soporte Técnico de Cisco o la ingeniería de desarrollo de Cisco puede utilizar esta información para resolver problemas. Esta función no sondea los contadores de errores tales como FCS, CRC, alineación, y fragmentos minúsculos que se asocian directamente con la conectividad del partner de link. Consulte la sección Solución de Errores EtherChannel/Link de este documento para incorporar esta capacidad.

El sondeo se ejecuta cada 30 minutos y se ejecuta en el antecedente de los contadores de errores seleccionados. Si la cuenta va hacia arriba entre dos sondeos subsiguientes sobre el mismo puerto, un mensaje de syslog señala el incidente y le da al módulo/puerto detalles del contador de errores.

La opción del contador de puerto no se soporta en la plataforma del Catalyst 4500/4000.

Memoria

La habilitación de sta función realiza un monitoreo de fondo y la detección de condiciones de corrupción DRAM. Tales condiciones de corrupción de la memoria incluyen las siguientes:

- Asignación
- El liberar
- Fuera de rango

- Alineación defectuosa

Recomendación

Habilite todas las funciones de la detección de errores, entre ellas, señal en banda, contadores de puerto, y memoria, si se soportan. La habilitación de estas funciones alcanza el sistema y el diagnóstico de advertencia de hardware dinámico mejorado para la plataforma del switch Catalyst. Ejecute estos comandos para habilitar las tres funciones de la detección de errores:

```
set errordetection inband enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection
portcounters enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection memory
enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later.
```

Ejecute este comando para confirmar que la detección de errores está habilitada:

```
>show errordetection

Inband error detection:                  enabled
Memory error detection:                  enabled
Packet buffer error detection:           errdisable
Port counter error detection:            enabled
Port link-errors detection:              disabled
Port link-errors action:                 port-failover
Port link-errors interval:               30 seconds
```

Solución de Errores de EtherChannel/Link

Información Operativa General

En CatOS 8.4 y posterior, nueva función se ha introducido para proporcionar un failover automático del tráfico a partir de un puerto en un EtherChannel a otro puerto en el mismo EtherChannel. El failover del puerto se produce cuando uno de los puertos en el canal excede un umbral de error configurable dentro del intervalo especificado. El failover del puerto ocurre solamente si hay un puerto operativo en el EtherChannel. Si el puerto fallado es el puerto más reciente de EtherChannel, el puerto no ingresa el estado failover del puerto. Este puerto continúa pasando el tráfico, sin importar el tipo de errores que se reciban. Los puertos únicos, sin canalización no entran el estado failover del puerto. Estos puertos entran el estado errdisable cuando el umbral de error se excede dentro del intervalo especificado.

Esta función es solamente eficaz cuando habilita **set errordetection portcounters**. Los errores de link que se monitorearán están basados en tres contadores:

- InErrors
- RxCRCs (CRCAlignErrors)
- TxCRCs

Ejecute el comando show counters en un switch para visualizar el número de contadores de errores. Aquí tiene un ejemplo:

```
>show counters 4/48

.......
```

```
32 bit counters

0  rxCRCAlignErrors           =          0
.......

6  ifInErrors                 =          0
.......

12 txCRC                      =          0
```

Esta tabla es una lista de parámetros de la configuración posible y de la configuración predeterminada respectiva:

Parámetros	Predeterminado
Global	Inhabilitado
Monitor de puerto para RxCRC	Inhabilitado
Monitor de puerto para InErrors	Inhabilitado
Monitor de puerto para TxCRC	Inhabilitado
Acción	Puerto-Conmutación por falla
Intervalo	30 segundos
Conteo de la muestra	3 consecutivos
Umbral bajo	1000
Umbral elevado	1001

Si se habilita la función y el conteo de errores de un puerto alcanza el valor del umbral elevado configurable dentro del período especificado del conteo de la muestra, la acción configurable es la desactivación por error o el failover del puerto. La acción de desactivación por error coloca el puerto en el estado errdisable. Si configura la acción del failover del puerto, se considera el estado del canal de puerto. El puerto es deshabilitado por error solamente si el puerto está en un canal pero ese puerto no es el puerto operativo más reciente del canal. Además, si la acción configurada es failover del puerto y el puerto es un puerto único o no está canalizado, el puerto se coloca en el estado errdisable cuando el conteo de errores de puerto alcanza el valor de umbral elevado.

El intervalo es un temporizador constante para la lectura de los contadores de error del puerto. El valor predeterminado del intervalo de los errores de link es 30 segundos. El rango permitido es entre 30 y 1800 segundos.

Hay un riesgo de deshabilitación por error accidental de un puerto debido a un evento único inesperado. Para minimizar este riesgo, se toman medidas a un puerto solamente cuando la condición persiste a lo largo del número consecutivo de tiempos de muestreo. El valor predeterminado del muestreo es 3 y el rango permitido es de 1 a 255.

El umbral es un número absoluto que se marcará en función del intervalo de errores de link. El umbral bajo de errores de link predeterminado es 1000 y el rango permitido es 1 a 65.535. El umbral elevado predeterminado de errores de link es 1001. Cuando el número consecutivo de tiempos de muestreo alcanza el umbral bajo, se envía un syslog. Si el número consecutivo de tiempos de muestreo alcanza el umbral elevado, se emite un syslog y se activa la función de desactivación por error o failover del puerto.

Nota: use la misma configuración de detección de errores del puerto para todos los puertos en un canal. Consulte estas secciones de la guía de configuración de software de las Catalyst 6500 Series para más información:

- la sección *Configuración de la Solución de Errores EtherChannel/Link* de Verificación del Estado y Conectividad
- La sección *Configuración de la Detección de Errores del Puerto* de Configuración de Ethernet, Fast Ethernet, Gigabit Ethernet, y 10-Gigabit Ethernet Switching

Recomendaciones

Debido a que la función utiliza los mensajes SCP para registrar y comparar los datos, los números altos de puertos activos pueden provocar un uso intensivo de la CPU. Este uso es aún más intensivo cuando el intervalo del umbral se establece en un valor muy pequeño. Habilite esta función con discreción para los puertos que se señalan como links críticos y que transportan tráfico para las aplicaciones sensibles. Ejecute este comando para habilitar la detección del error de link global:

```
set errordetection link-errors enable
```

También, comience con el umbral, el intervalo, y los parámetros de muestreo predeterminados. Y use la acción predeterminada, failover del puerto.

Ejecute estos comandos para aplicar los parámetros globales del error de link a los puertos individuales:

```
set port errordetection mod/port inerrors enable

set port errordetection mod/port rxcrc enable

set port errordetection mod/port txcrc enable
```

Puede ejecutar estos comandos para verificar la configuración de los errores de link:

```
show errordetection

show port errordetection {mod | mod/port}
```

Diagnósticos de Buffer de Paquetes Catalyst 6500/6000

En las versiones CatOS 6.4(7), 7.6(5), y 8.2(1), se introdujo el diagnóstico de buffer de paquetes de Catalyst 6500/6000. El diagnóstico de buffer de paquetes, que se habilita de forma predeterminada, detecta las fallas del almacén intermedio de paquetes que son causadas por las fallas de la RAM estática (SRAM) transitoria. La detección está en estos módulos de línea de 48 puertos 10/100-Mbps:

- WS-X6248-RJ45
- WS-X6248-RJ21
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45
- WS-X6148-RJ21

Cuando se produce una condición de error, 12 de los 48 puertos 10/100-Mbps continúan conectados y pueden experimentar problemas de conectividad al azar. La única opción para subsanar esta situación es apagar y volver a encender el módulo.

Información Operativa General

La rutina de diagnóstico del buffer de paquetes comprueba los datos almacenados en un sector específico del buffer de paquetes para determinar si su falla se debe a errores transitorios de la SRAM. Si el proceso relee algo diferente que qué escribió, entonces realiza dos opciones de recuperación configurables posibles:

1. La acción predeterminada es a la desactivación por error de los puertos de la tarjeta de línea que son afectados por la falla del almacén intermedio.
2. La segunda opción es apagar y encender la tarjeta de línea.

Se han agregado dos mensajes de syslog. Los mensajes proporcionan una advertencia de la deshabilitación por error de los puertos o advierten que el módulo se ha apagado y vuelto a encender por errores del buffer de paquetes:

```
show errordetection

show port errordetection {mod | mod/port}
```

En las versiones CatOS que son anteriores a 8.3 y 8.4, el tiempo en que se apaga y vuelve a encender la tarjeta de línea es entre 30 y 40 segundos. Una función de arranque rápido fue introducida en las versiones CatOS 8.3 y 8.4. La función descarga automáticamente el firmware a las tarjetas de línea instaladas durante el proceso del primer arranque para minimizar el tiempo de arranque. La función de arranque rápido reduce el tiempo de apagado y encendido a aproximadamente 10 segundos.

Recomendación

Cisco recomienda la opción predeterminada de *errdisable*. Esta acción tiene el menos impacto en el servicio de red durante las horas de producción. Si es posible, mueva la conexión que es afectada por los puertos inhabilitados por error a otros puertos del switch disponibles para restablecer el servicio. Programe un encendido y apagado manual de la tarjeta de línea durante el periodo de mantenimiento. Ejecute el *comando reset module mod* para recuperación total de la condición del buffer de paquetes corrupto.

Nota: Si los errores continúan después de que se reajusta el módulo, vuelva a colocar el módulo.

Ejecute este comando para habilitar la *opción errdisable*:

```
set errordetection packet-buffer errdisable
!--- This is the default.
```

Otra Opción

Como es necesario utilizar una rutina de apagado y encendido de la tarjeta de línea para una recuperación completa de los puertos que se han visto afectados por el fallo de la SRAM, una acción alternativa de recuperación es configurar la opción de ciclo de apagado y encendido. Esta opción es útil en las circunstancias en las que una interrupción en los servicios de red que puede durar entre 30 y 40 segundos es aceptable. Este tiempo es lo que tarda un módulo de línea en

apagarse y volverse a encender completamente y estar en funcionamiento sin utilizar la función de inicio rápido. La función de arranque rápido puede reducir el tiempo de interrupción en los servicios de red a 10 segundos con la opción de rutina de apagado y encendido. Ejecute este comando para habilitar la opción de rutina de apagado y encendido:

```
set errordetection packet-buffer power-cycle
```

Diagnósticos de Buffer de Paquetes

Esta prueba se usa para los switches de Catalyst 5500/5000 solamente. Esta prueba está diseñadaq para encontrar el hardware defectuoso en los switches de Catalyst 5500/5000 que utilizan los módulos Ethernet con el hardware específico que proporcionan la conectividad 10/100-Mbps entre los puertos de usuario y el backplane del switch. Como no pueden realizar la verificación CRC de tramas de trunk, si un buffer de paquetes de puerto se daña durante el tiempo de ejecución, es posible que se dañen los paquetes o que se produzcan errores CRC. Lamentablemente, esto podría llevar a la propagación de tramas defectuosas adicionales en la red ISL de Catalyst 5500/5000, que potencialmente causa la interrupción del plano de control y las tormentas de broadcast en el peor de los casos.

Módulos más nuevos del Catalyst 5500/5000 y otras plataformas han actualizado la verificación de error de hardware incorporada y no necesitan las pruebas de buffer de paquetes, por lo que no hay opción para configurar.

Los módulos de línea que necesitan los diagnósticos de buffer de paquetes son WS-X5010, WS-X5011, WS-X5013, WS-X5020, WS-X5111, WS-X5113, WS-X5114, WS-X5201, WS-X5203, WS-X5213/a, WS-X5223, WS-X5224, WS-X5506, WS-X5509, WS-U5531, WS-U5533, y WS-U5535.

Información Operativa General

Este diagnóstico controla que los datos guardados en una sección específica del buffer de paquetes no se dañen accidentalmente debido al hardware defectuoso. Si el proceso relee algo diferente que escribió, apaga el puerto en el modo fallado, puesto que ese puerto podría corromper los datos. No se requiere umbral de errores. Los puertos fallados no pueden ser habilitados otra vez hasta que se haya reajustado el módulo (o sustituido).

Hay dos modos para las pruebas de buffer de paquetes: programado y a pedido. Cuando una prueba comienza, se generan mensajes de syslog para indicar la duración prevista de la prueba (redondeada hasta el minuto más cercano) y el hecho de que la prueba ha comenzado. La duración exacta de la prueba varía según el tipo de puerto, los tamaños del buffer, y el tipo de prueba ejecutada.

Las pruebas a pedido son dinámicas a fin de completarse en pocos minutos. Puesto que estas pruebas interfieren activamente con la memoria del paquete, los puertos se deben cerrar para cuestiones administrativas antes de ejecutar la prueba. Ejecute este comando para cerrar los puertos:

```
> (enable) test packetbuffer 4/1
Warning: only disabled ports may be tested on demand - 4/1 will be skipped.
> (enable) set port disable 4/1
> (enable) test packetbuffer 4/1
Packet buffer test started. Estimated test time: 1 minute.
%SYS-5-PKTTESTSTART:Packet buffer test started
%SYS-5-PKTTESTDONE:Packet buffer test done. Use 'show test' to see test results
```

Las pruebas programadas son mucho menos agresivas que las pruebas a pedido, y se ejecutan en el fondo. Las pruebas se realizan en paralelo cuando hay varios módulos pero de a un puerto por módulo a la vez. La prueba conserva, escribe y lee secciones pequeñas de la memoria buffer de los paquetes antes de restaurar la información de memoria intermedia de los paquetes de usuario y, por lo tanto, no genera errores. Sin embargo, puesto que la prueba escribe la memoria buffer, bloquea los paquetes entrantes por algunos milisegundos y causa una cierta pérdida en los links ocupados. De forma predeterminada, hay una pausa de ocho segundos entre cada prueba de escritura de buffer para minimizar cualquier pérdida del paquete, pero esto significa que un sistema por lleno de módulos que necesita la prueba de buffer de paquetes puede asumir el control 24 horas para que la prueba se complete. Esta prueba programada se habilita de forma predeterminada para ejecutarse semanalmente a las 03:30, los domingos en CatOS 5.4 o posterior, y el estado de la prueba puede ser confirmado con este comando:

```
>show test packetbuffer status

!--- When test is running, the command returns !--- this information: Current packet buffer test
details Test Type : scheduled Test Started : 03:30:08 Jul 20 2001 Test Status : 26% of ports
tested Ports under test : 10/5,11/2 Estimated time left : 11 minutes !--- When test is not
running, !--- the command returns this information: Last packet buffer test details Test Type :
scheduled Test Started : 03:30:08 Jul 20 2001 Test Finished : 06:48:57 Jul 21 2001
```

Recomendación

Cisco recomienda que use la función de prueba de buffer de paquetes programada para los sistemas de Catalyst 5500/5000, ya que la ventaja de detectar los problemas en los módulos sobrepasa el riesgo de una leve pérdida de paquetes.

Es importante programar una hora semanal estándar a lo largo de la red que permita que el cliente cambie los links de los puertos defectuosos o de los módulos RMA cuanto sea necesario. Como la ejecución de esta prueba puede suponer cierta pérdida de paquetes, en función de la carga de la red, es preferible programarla para las horas de menor intensidad de uso de la red, como la hora predeterminada, las 03:30, los domingos. Ejecute este comando para establecer la hora de la prueba:

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

Una vez activada (como sucede si se actualiza la versión de CatOS a la 5.4 y posteriores), existe la posibilidad de que surja algún problema de hardware o memoria que antes permanecía oculto y que un puerto se cierre automáticamente en consecuencia. Podría ver este mensaje:

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

Otras Opciones

Si no es aceptable arriesgar un nivel bajo de pérdida de paquetes por puerto semanalmente, se recomienda utilizar la función a pedido durante las interrupciones planificadas. Ejecute este comando para comenzar esta función manualmente en función del rango (aunque el puerto se debe inhabilitar primero para cuestiones administrativas):

```
test packetbuffer port range
```

Registro del Sistema

Los mensajes de syslog son específicos de Cisco y constituyen una parte clave de la administración proactiva de fallas. Los mensajes syslog permiten informar sobre un mayor rango de condiciones de red y protocolo que el SNMP estandarizado. Las plataformas de administración, tales como isco Resource Manager Essentials (RMEs) y Network Analysis Toolkit (NATkit) hacen uso potente de la información de syslog porque realizan estas tareas:

- Presentan un análisis por severidad, mensaje, dispositivo, y así sucesivamente
- Habilitan el filtrado de los mensajes que ingresan para el análisis
- Ponen en funcionamiento las herramientas de alerta, como localizadores, o la recolección a petición del inventario y los cambios de configuración

Recomendación

Un importante aspecto que debe tenerse en cuenta es la cantidad de información de registro que se generará localmente y se mantendrá en el buffer del switch en comparación con el que se envíe a un servidor de syslog (usando el *comando set logging server severity value*). Algunas organizaciones registran un nivel elevado de información centralmente, mientras que otras se dirigen al switch en sí mismo para mierar los registros más detallados para un evento o a habilitar un alto nivel de la captura syslog solamente durante el troubleshooting.

El debugging es diferente en las plataformas de CatOS que en las de Cisco IOS Software, pero el registro del sistema detallado se puede habilitar por sesión con **set logging session enable** sin modificar el registro predeterminado.

Cisco generalmente recomienda seleccionar el nivel 6 de syslog para supervisar el spantree y el sistema, dado que estas son las funciones de estabilidad fundamentales. Además, para los ambientes de multicast, es conveniente utilizar el nivel de registro 4 de la función mcast de modo que se produzcan mensajes syslog en caso de que los puertos del router sean eliminados. Desafortunadamente, antes de CatOS 5.5(5), esto podría hacer que se registren mensajes de syslog para incorporaciones y retiros de IGMP, lo cual es demasiado ruidoso para monitorear. Finalmente, si se utilizan las listas de entrada del IP, un nivel de registro mínimo de 4 se recomienda para capturar los intentos de inicio de sesión desautorizados. Ejecute estos comandos para establecer estas opciones:

```
set logging buffer 500
!--- This is the default. set logging server syslog server IP address set logging server enable
!--- This is the default. set logging timestamp enable
set logging level spantree 6 default
!--- Increase default STP syslog level. set logging level sys 6 default
!--- Increase default system syslog level. set logging server severity 4
!--- This is the default; !--- it limits messages exported to syslog server. set logging console
disable
```

Apague los mensajes de la consola para proteger contra el riesgo de que el switch se bloquee en espera de una respuesta de un terminal lento o ausente cuando el volumen de mensajes es muy elevado. El registro de la consola es de alta prioridad en CatOS y se utiliza principalmente para capturar los últimos mensajes localmente al solucionar problemas o en un escenario de caída del switch.

Esta tabla proporciona los recursos de registro individual, los niveles predeterminados, y los cambios recomendados para el Catalyst 6500/6000. Cada plataforma tiene recursos ligeramente diferentes, según las funciones soportadas.

Recurso	Nivel Predeterminado	Acción Recomendada
acl	5	No modificar.
cdp	4	No modificar.
polis	3	No modificar.
dtp	8	No modificar.
conde	2	No modificar.
ethc[1]	5	No modificar.
filesys	2	No modificar.
gvrp	2	No modificar.
ip	2	**Cambie a 4 si se usaron las listas de entrada de IP**.
kernel	2	No modificar.
1d	3	No modificar.
mcast	2	**Cambie a 4 si se usó multicast (CatOS 5.5[5] y posterior)**.
mgmt	5	No modificar.
mls	5	No modificar.
pagp	5	No modificar.
protfilt	2	No modificar.
poda	2	No modificar.
Privatevlan	3	No modificar.
qos	3	No modificar.
radius	2	No modificar.
rsvp	3	No modificar.
seguridad	2	No modificar.
snmp	2	No modificar.
spantree	2	**Cambie a 6.**
sys	5	**Cambie a 6.**
tac	2	No modificar.
tcp	2	No modificar.
telnet	2	No modificar.
Tftp	2	No modificar.
UDLD	4	No modificar.
VMPS	2	No modificar.
VTP	2	No modificar.

[1] en CatOS 7.x y posterior, el código de recurso del ethc substituye el código de recurso del pagp para reflejar el soporte LACP.

Nota: Actualmente, , los switches Catalyst registran un mensaje syslog de nivel 6 para cada **comando set o clear** ejecutado, a diferencia de Cisco IOS Software, que acciona el mensaje

solamente después que sale del modo de configuración. Si necesita RME para las configuraciones de respaldo en el tiempo real sobre este disparador, estos mensajes también deben ser enviados al servidor de syslog RME. Para la mayoría de los clientes, los respaldos periódicos de la configuración para los switches de Catalyst son suficientes, y no se necesita un cambio de la severidad de registro del servidor predeterminado.

Si ajusta sus alertas NMS, consulte la Guía de Mensajes del Sistema.

Simple Network Management Protocol

El protocolo SNMP se utiliza para recuperar estadísticas, contadores y tablas almacenados en bases de información para administración (MIB) de dispositivos de red. Los NMS (tales como HP OpenView) pueden usar la información recopilada para generar las alertas en tiempo real, medir la disponibilidad, y presentar la información sobre planificación de capacidad, así como para realizar las verificaciones de configuración y de troubleshooting.

Información Operativa General

Con algunos mecanismos de seguridad, una estación de administración de red puede extraer la información en los MIB mediante solicitudes get y get next del protocolo SNMP, y cambiar los parámetros con el **comando set**. Además, un dispositivo de red se puede configurar para generar un mensaje trampa para el NMS para la alerta en tiempo real. El sondeo de SNMP utiliza el puerto 161 UDP IP y las trampas SNMP utilizan el puerto 162.

Cisco soporta estas versiones del SNMP:

- SNMPv1: Norma de Internet RFC 1157, que utiliza la opción de seguridad de cadena comunitaria en texto sin cifrar. Una lista de control de acceso IP y la contraseña de la dirección IP definen la comunidad de administradores que pueden acceder al agente MIB.
- SNMPv2C: una combinación de SNMPv2, un proyecto de norma de Internet definida en RFCs 1902 a través de 1907, y SNMPv2C, un marco administrativo basado en la comunidad para SNMPv2 que es un borrador experimental definido en RFC 1901. Las ventajas incluyen un mecanismo de recuperación global que soporta la extracción de las tablas y de una gran cantidad de información, minimiza el número de viajes de ida y vuelta requeridos, y mejora la solución de errores.
- SNMPv3: El proyecto propuesto de RFC 2570 proporciona el acceso seguro a los dispositivos con la combinación de autenticación y el cifrado de paquetes en la red. Las funciones de seguridad proporcionadas en el SNMPv3 son las siguientes:Integridad del mensaje: asegura que un paquete no haya sido alterado en tránsitoAutenticación: determina que el mensaje sea de una fuente válidaCifrado: revuelve el contenido de un paquete para evitar que sea visto fácilmente por una fuente no autorizada

Esta tabla identifica las combinaciones de modelos de seguridad:

Nivel de Modelo	Autenticación	Cifrado	Resultado
v1	noAuthN	No	Usa una correspondencia de

	oPriv, identificación de comunidad		identificaciones de comunidad para autenticación.
v2c	noAuthNoPriv, identificación de comunidad	No	Usa una correspondencia de identificaciones de comunidad para autenticación.
v3	noAuthNoPriv, Username	No	Utiliza las coincidencias de nombre de usuario para autenticar.
v3	authNoPriv, MD5 o SHA	Np	Proporciona autenticación sobre la base de algoritmos HMAC-MD5 o HMAC-SHA.
v3	authPriv, MD5 o SHA	DES	Proporciona autenticación sobre la base de algoritmos HMAC-MD5 o HMAC-SHA. Proporciona cifrado DES de 56 bits además de autenticación basada en el estándar CBC-DES (DES-56).

Nota: Tenga en cuenta esta información sobre los objetos del SNMPv3:

- Cada usuario pertenece a un grupo.
- Un grupo define la política de acceso para un conjunto de usuarios.
- Una política de acceso define aqué objetos SNMP se puede acceder para leer, escribir, y crear.
- Un grupo determina la lista de notificaciones que sus usuarios pueden recibir.
- Un grupo también define el modelo de seguridad y el nivel de seguridad para sus usuarios.

Recomendación de Notificaciones de Trampa de SNMP

SNMP es la base de toda la administración de la red y se encuentra habilitado y en uso en todas las redes. El agente SNMP del switch se debe establecer de manera que utilice la versión de SNMP admitida por la estación de administración. Dado que un agente se puede comunicar con varios administradores, es posible configurar el software para admitir la comunicación con una estación de administración mediante el uso del protocolo SNMPv1 y con otra, por ejemplo, mediante el uso del protocolo SNMPv2.

La mayoría de las estaciones NMS actualmente usan SNMPv2C con esta configuración:

```
set snmp community read-only string
!--- Allow viewing of variables only. set snmp community read-write string
!--- Allow setting of variables. set snmp community read-write-all string<string>
!--- Include setting of SNMP strings.
```

Cisco recomienda habilitar las trampas SNMP traps para todas las funciones en uso (las

funciones no usadas pueden ser inhabilitadas si lo desea). Una vez que se habilita la trampa, puede ser probada con el comando test snmp y la configuración de solución adecuada en el NMS para el error (como un mensaje de alerta al localizador o una alerta emergente).

Todas las trampas está inhabilitadas de forma predeterminada y deben ser agregados a la configuración, individualmente o con el parámetro **all**, como se muestra:

```
set snmp trap enable all
set snmp trap server address read-only community string
```

Las trampas disponibles en CatOS 5.5 incluyen las siguientes:

Trampa	Descripción
autenticación	Autenticación
bridge	Bridge
chasis	Chasis
config	Configuración
entidad	Entidad
ippermit	IP permit
módulo	Módulo
repetidor	Repetidor
stpx	Extensión del Spanning Tree
syslog	Notificación de syslog
vmps	Servidor de Política de Pertenencia a VLAN
vtp	VLAN Trunk Protocol

Nota: La trampa de syslog envía todos los mensajes syslog generados por el switch al NMS como también como trampa SNMP. Si hay algún analizador que esté ejecutando las alertas de syslog como la función RME de Cisco Works 2000 RME, entonces no es necesariamente útil recibir esta información dos veces.

A diferencia del Cisco IOS Software, las trampas SNMP están inhabilitadas de forma predeterminada porque los switches pueden tener centenares de interfaces activas. Cisco recomienda que los puertos clave, como por ejemplo los links de infraestructura hacia los routers, switches y servidores principales tengan habilitadas las trampas SNMP de nivel de puerto. Otros puertos, como los puertos host del usuario, no son necesarios, lo cual ayuda a simplificar la administración de la red.

```
set port trap port range enable
!--- Enable on key ports only.
```

Recomendación del Sondeo SNMP

Una revisión de la administración de red se recomienda para analizar las necesidades específicas detalladamente. Sin embargo, se mencionan algunas filosofías básicas de Cisco para la administración de las redes grandes:

- Haga algo simple, y hágalo correctamente.

- Reduzca la sobrecarga del personal debido excesivos análisis manuales, herramientas, recopilación y datos de sondeo.
- La administración de red es posible con apenas algunas herramientas, por ejemplo, HP OpenView como NMS, Cisco RME como configuración, syslog, inventario, y administrador de software, Microsoft Excel como analizador de datos NMS, y CGI como una forma de publicar en la Web.
- La publicación de los informes web permite que los usuarios, tales como el equipo directivo y los analistas, a obtener información sin necesidad de interrumpir la labor del personal con solicitudes especiales.
- Descubrir qué funciona bien en la red y no modificarlo. Concéntrese en lo que no está funcionando.

La primera fase de implementación NMS debe ser a la línea de fondo el hardware de red. Puede inferirse mucho acerca del estado de los dispositivos y protocolos a partir del mero uso de CPU, memoria y buffer en routers y del uso de NMP CPU, memoria y backplane en switches. La línea de base de la carga de tráfico, tráfico máximo y tráfico promedio de las L2 y L3 no tiene sentido si antes no se ha realizado una línea de base del hardware. Las líneas de base normalmente se aplican en períodos de varios meses para poder detectar tendencias diarias, semanales y trimestrales, en función del ciclo productivo de la empresa.

Muchas redes tienen problema de rendimiento NMS y de capacidad causados por el sondeo excesivo. Por lo tanto, se recomienda, una vez que se establece la línea de base, fijar los umbrales RMON en los dispositivos mismos para advertir los cambios anormales en el NMS, y así quitar el sondeo. Habilita a la red para decirles a los operadores cuando algo no es normal, en lugar de sondear de manera continua para ver que todo esté normal. Los umbrales pueden establecerse en función de diversas reglas, como valor máximo más un porcentaje o desviación estándar a partir de una media, y están fuera del alcance de este documento.

La segunda fase de implementación NMS es sondear las áreas determinadas de la red más detalladamente con el SNMP. Esto incluye las áreas de duda, las áreas antes de un cambio, o las áreas cuyo funcionamiento se ha identificado como adecuado. use los sistemas NMS como reflector para explorar la red detalladamente y para iluminar los puntos calientes (no intente activar la red completa).

El grupo Consultores de Administración de la Red Cisco sugiere que se analicen y monitoreen MIB que son claves para detectar fallas en las redes de campus. Consulte Guía de Consulta de Correlación de Eventos y Supervisión de Red de Cisco para más información (por ejemplo, para saber qué MIB de desempeño consultar).

Nombre del Objeto	Descripción del Objeto	OID (ID del objeto)	Intervalo de Sondeo	Umbral
MIB-II				
sysUpTime	tiempo de actividad del sistema en 1/100 centésimas de segundo	1.3.6.1.2.1.1.3	5 min	< 30000

Nombre del Objeto	Descripción del Objeto	OID (ID del objeto)	Intervalo de Sond	Umbral

			eo	
CISCO-PROCESS-MIB				
cpmCPUTotal5min	El porcentaje de ocupación total de la CPU en el último período de 5 minutos	1.3.6.1.4.1.9.9.109.1.1.1.1.5	10 min	Línea de base

Nombre del Objeto	Descripción del Objeto	OID (ID del objeto)	Intervalo de Sondeo	Umbral
CISCO-STACK-MIB				
sysEnableChassisTraps	Indica si las trampas chassisAlarmOn y chassisAlarmOff en esta MIB deben ser generadas.	1.3.6.1.4.1.9.5.1.1.24	24 h	1
sysEnableModuleTraps	Indica si las trampas moduleUp y moduleDown en esta MIB deben ser generadas.	1.3.6.1.4.1.9.5.1.1.25	24 h	1
sysEnableBridgeTraps	Indica si la trampas newRoot y topologyChange en BRIDGE-MIB (RFC 1493) deben ser generadas.	1.3.6.1.4.1.9.5.1.1.26	24 h	1
sysEnableRepeaterTraps	Indica si las trampas en REPEATER-MIB (RFC1516) deben ser generadas.	1.3.6.1.4.1.9.5.1.1.29	24 h	1
sysEnableIpPermitTraps	Indica si las trampas IP permit en esta MIB deben ser generadas.	1.3.6.1.4.1.9.5.1.1.31	24 h	1
sysEnableVmpsTraps	Indica si la trampa vmVmpsChange definida en	1.3.6.1.4.1.9.5.1.1.33	24 h	1

	CISCO-VLAN-MEMBERSHIP-MIB debe ser generada.			
sysEnableConfigTraps	Indica si la trampa sysConfigChange en esta MIB debe ser generada.	1.3.6.1.4.1.9.5.1.1.35	24 h	1
sysEnableStpxTrap	Indica si la trampa stpxInconsistencyUpdate en CISCO-STP-EXTENSIONS-MIB debe ser generada.	1.3.6.1.4.1.9.5.1.1.40	24 h	1
chassisPs1status	Estado de la fuente de alimentación 1.	1.3.6.1.4.1.9.5.1.2.4	10 min	2
chassisPs1TestResult	Información detallada sobre el estado de la fuente de alimentación 1.	1.3.6.1.4.1.9.5.1.2.5	Según las necesidades.	
chassisPs2Status	Estado de la fuente de alimentación 2.	1.3.6.1.4.1.9.5.1.2.7	10 min	2
chassisPs2TestResult	Información detallada sobre el estado de la fuente de alimentación 2	1.3.6.1.4.1.9.5.1.2.8	Según las necesidades.	
chassisFanStatus	Estado del ventilador del chasis.	1.3.6.1.4.1.9.5.1.2.9	10 min	2
chassisFanTestResult	Información detallada sobre el estado del ventilador del chasis.	1.3.6.1.4.1.9.5.1.2.10	Según las necesidades.	
chassisMinorAlarm	Estado de la alarma menor del chasis.	1.3.6.1.4.1.9.5.1.2.11	10 min	1
chassis MajorAlarm (alarma principal del chasis)	Estado de la alarma principal del chasis	1.3.6.1.4.1.9.5.1.2.12	10 min	1

chassisTempAlarm	Estado de la alarma de temperatura del chasis.	1.3.6.1.4.1.9.5.1.2.13	10 min	1
moduleStatus	Estado operativo del módulo.	1.3.6.1.4.1.9.5.1.3.1.1.10	minuto 30	2
moduleTestResult	Información detallada sobre la condición de los módulos.	1.3.6.1.4.1.9.5.7.3.1.1.11	Según las necesidades.	
moduleStandbyStatus	Estatus de un módulo redundante.	1.3.6.1.4.1.9.5.7.3.1.1.21	minuto 30	=1 o =4

Nombre del Objeto	Descripción del Objeto	OID (ID del objeto)	Intervalo de Sondeo	Umbral
CISCO-MEMORY-POOL-MIB				
dot1dStpTimeSinceTopologyChange	El tiempo (en 1/100 segundos) desde la última vez que un cambio en la topología fue detectado por la entidad.	1.3.6.1.2.1.17.2.3	5 min	< 30000
dot1dStpTopChanges	El número total de cambios en la topología detectados por este bridge desde la última vez que se restableció o inició la entidad de administración.	1.3.6.1.2.1.17.2.4	Según las necesidades.	
dot1dStpPortState [1]	El estado actual del puerto	1.3.6.1.2.1.17.2.15.1.3	Según las necesi	

	según lo definido por la aplicación del Spanning-Tree Protocol. El valor de retorno puede ser uno de los siguientes: (1) inhabilitado, bloqueo (2), (3) escucha, aprendizaje (4), reenvío (5), o (6) dañado.		dades.	

Nombre del Objeto	Descripción del Objeto	OID (ID del objeto)	Intervalo de Sondeo	Umbral
CISCO-MEMORY-POOL-MIB				
ciscoMemoryPoolUsed	Indica la cantidad de bytes del conjunto de memoria actualmente en uso por las aplicaciones en el dispositivo administrado.	1.3.6.1.4.1.9.9.48.1.1.1.5	minuto 30	Línea de base
ciscoMemoryPoolFree	Indica la cantidad de bytes del conjunto de memoria que actualmente no se usa en el dispositivo administrado. **Nota:** La suma de ciscoMemoryPoolUsed y	1.3.6.1.4.1.9.9.48.1.1.1.6	minuto 30	Línea de base

	ciscoMemoryPoolFree es la cantidad total de memoria en el conjunto.			
ciscoMemoryPoolLargestFree	Indica la cantidad mayor de bytes contiguos del conjunto de memoria que actualmente no se usa en el dispositivo administrado.	1.3.6.1.4.1.9.9.48.1.1.1.7	minuto 30	Línea de base

Consulte Kit de Herramientas de Administración de red de Cisco - MIB para más información sobre el soporte de Cisco MIB.

Nota: Algunos MIB estándares asumen que una entidad SNMP determinada contiene solamente una instancia de MIB. Así, la MIB estándar no tiene ningún índice que permita que los usuarios accedan directamente a una instancia particular de la MIB. En estos casos, se proporciona indexación de cadenas de comunidad para acceder a cada instancia de MIB estándar. La sintaxis es [identificación de comunidad]@[número ejemplo], donde el ejemplo es típicamente un número de VLAN.

Otras Opciones

Los aspectos de seguridad del SNMPv3 significan que se espera que su uso remplace al SNMPv2 con el tiempo. Cisco recomienda que los clientes se preparen para este nuevo protocolo como parte de su estrategia NMS. Los beneficios son que se pueden recolectar los datos de forma segura desde los dispositivos SNMP sin temor a que se corrompan o se alteren. La información confidencial, tal como paquetes del comando snmp set que cambien una configuración del switch, se puede cifrar para evitar que su contenido sea expuesto en la red. Además, diversos grupos de usuarios pueden tener diversos privilegios.

Nota: La configuración del SNMPv3 es significativamente diferente que la línea del comando snmpv2, y se espera una mayor carga de la CPU en Supervisor Engine.

Supervisión Remota

El RMON permite que los datos MIB sean procesados previamente por el dispositivo de red en sí, en preparación para usos comunes o para la aplicación de esa información por parte del administrador de la red, tal como ejecución de la determinación histórica de la línea de base y análisis del umbral.

Los resultados del procesamiento RMON están almacenados en MIB RMON para una posterior recopilación por parte de un NMS, como se define en RFC 1757 .

Información Operativa General

Los switches Catalyst cuentan con soporte de hardware para mini-RMON en cada puerto, esta aplicación se compone de cuatro grupos RMON-1 básicos: Estadísticas (grupo 1), Historial (grupo 2), Alarmas (grupo 3) y Eventos (grupo 9).

La parte más potente de RMON-1 es el **mecanismo de umbral** provisto por los **grupos de eventos y la alarma**. Según lo discutido, la configuración de los umbrales RMON permite que el switch envíe una trampa SNMP cuando se produce una situación anómala. Una vez que se han identificado los puertos claves, el SNMP puede usarse para sondear los contadores o grupos del historial de RMON y crear líneas de base para registrar la actividad del tráfico normal para esos puertos. Luego, pueden configurarse los umbrales RMON ascendentes y descendentes y las alarmas configuradas para cuando existe una variación definida desde la línea de base.

La configuración de umbrales se realiza mejor con un paquete de administración RMON, puesto que la creación exitosa de las filas de los parámetros en las tablas Alarma y Eventos es tediosa. Los paquetes RMON NMS comerciales, por ejemplo Cisco Traffic Director, parte de Cisco Works 2000, incluyen GUI que simplifican en gran medida la configuración de los umbrales RMON.

Para los propósitos de la línea de base, el grupo de los etherStats proporciona un rango útil de estadísticas del tráfico L2. Los objetos en esta tabla se pueden utilizar para obtener las estadísticas sobre tráfico de unicast, multicast, y broadcast, así como una variedad de errores L2. El agente RMON en el switch también puede configurarse para almacenar estos valores de ejemplo en el grupo de historial. Este mecanismo permite reducir la cantidad de consultas sin disminuir la velocidad de muestreo. Los historiales de RMON pueden proporionar líneas de base precisas sin la sobrecarga sustancial del sondeo. Sin embargo, cuánto más historiales se recolecten, más recursos del switch se utilizarán.

Mientras que los switches proporcionan solamente cuatro grupos básicos de RMON-1, es importante no olvidar el resto de RMON-1 y RMON-2. Todos los grupos son definidos en RFC 2021, incluido UsrHistory (grupo 18) y ProbeConfig (grupo 19). Se puede extraer información sobre L3 y capas superiores de los switches con el puerto SPAN o las funciones de redirección VLAN ACL que lo habilitan para copiar tráfico a un SwitchProbe RMON externo o a un Módulo de Análisis de Red (NAM) interno.

Los NAM soportan todos los grupos RMON y pueden incluso examinar los **datos de la capa de aplicación**, incluidos los datos de NetFlow exportados de los Catalyst cuando se habilita el MLS. Elecutar el MLS significa que el router no conmuta todos los paquetes en un flujo, solamente los datos de exportación de Netflow y no los contadores de la interfaz proporcionan estadísticas de VLAN confiables.

Puede utilizar un puerto SPAN y una sonda de switch para capturar una secuencia de paquetes para un puerto determinado, un trunk, o una VLAN y para cargar los paquetes para decodificar con un paquete de administración de RMON. El puerto SPAN es controlable con SNMP a través del grupo del SPAN en el CISCO-STACK-MIB, así que este proceso es fácil de automatizar. El Traffic Director hace uso de estas funciones con la función del agente ambulante.

Hay advertencias para expandir una VLAN entera. Incluso si utiliza una sonda de 1 Gbps, la secuencia de paquetes entera a partir de un VLAN o incluso de un puerto dúplex completo de 1 Gbps puede exceder el ancho de banda del puerto SPAN. Si el puerto SPAN está funciona continuamente con el ancho de banda completa, es posible que se estén perdiendo datos. Consulte Configuración de la Función Analizador del Puerto Conmutado de Catalyst (SPAN) para más detalles.

Recomendación

Cisco recomienda que se implementen los umbrales RMON y el alerta para ayudar a la administración de red de un modo más inteligente que el sondeo SNMP solamente. Esto reduce la sobrecarga del tráfico de administración de red y permite que la red avise de forma inteligente cuando algo ha cambiado de la línea de fondo. El RMON debe ser conducido por un agente externo tal como Traffic Director; no hay soporte CLI. Ejecute estos comandos para habilitar el RMON:

```
set snmp rmon enable
set snmp extendedrmon netflow enable mod
!--- For use with NAM module only.
```

Es importante recordar que la función principal de un switch es la de reenviar tramas, no desempeñarse como una gran sonda RMON de varios puertos. Por lo tanto, cuando configura los historiales y los umbrales en los puertos múltiples para las condiciones múltiples, tenga en cuenta que se están consumiendo recursos. Considere un módulo NAM si ampliará RMON. También recuerde la regla del puerto crítica: sondear y establecer solamente los umbrales en los puertos identificados como importantes en la etapa de planificación.

Requisitos de Memoria

El uso de memoria de RMON es constante en todas las plataformas de switches en relación con estadísticas, historiales, alarmas y eventos. El RMON utiliza un compartimiento para almacenar los historiales y las estadísticas en el agente RMON (el switch, en este caso). Los tamaños del compartimiento se definen en la sonda RMON (Switch Probe) o la aplicación RMON (Traffic Director), después se envían al switch para ser establecidos. Típicamente, las restricciones de memoria son solamente una consideración en las versiones anteriores de Supervisor Engine con menos de 32 MB de DRAM. Consulte estas pautas:

- Aproximadamente 450 K del espacio de códigos se agrega a la imagen NMP para soportar el mini-RMON (que equivale a cuatro grupos de RMON: estadísticas, historial, alarmas, y eventos). El requisito de memoria dinámica para RMON varía dado que depende de la configuración del tiempo de ejecución. La información sobre el uso de la memoria RMON de tiempo de ejecución para cada grupo del mini RMON se explica aquí:Grupo Estadísticas de Ethernet: toma 800 bytes para cada interfaz conmutada Ethernet/FE.Grupo de historial: para la interfaz de Ethernet, cada entrada de control de historial configurada con 50 compartimientos toma el espacio de memoria aproximadamente de 3,6 KB y 56 bytes para cada compartimiento adicional.Grupos Alarmas y Eventos: toma 2,6 KB para cada alarma configurada y sus entradas de evento correspondiente.
- Para guardar la configuración relacionada con NVRAM, se necesitan aproximadamente 20 K NVRAM de espacio si el tamaño de NVRAM total del sistema es 256 K o más y 10 K NVRAM de espacio si el tamaño de NVRAM total es 128 K.

Network Time Protocol

El NTP, RFC 1305 , sincroniza la hora entre un grupo de servidores de tiempo y clientes distribuidos y permite que los eventos sean correlacionados cuando se crean los registros del sistema o se producen otros eventos específicos del tiempo.

NTP le brinda precisiones en los tiempos de cliente, normalmente dentro de un milisegundos en redes LAN y hasta unas pocas decenas de milisegundos en redes WAN, en comparación con un servidor primario sincronizado con el Tiempo Universal Coordinado (UTC). 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.

Información Operativa General

El NTP primero fue documentado en RFC 958 , pero se ha desarrollado con el RFC 1119 (la versión NTP 2) y ahora está en su tercera versión según lo definido en RFC 1305 . Se ejecuta en el puerto 123 UDP. Toda comunicación NTP utiliza UTC, que es el mismo tiempo que la Hora Media de Greenwich.

Acceso a Servidores de Tiempo Público

La subred NTP actualmente incluye a más de 50 servidores públicos primarios sincronizados directamente con UTC por radio, satélite o módem. Normalmente, las estaciones de trabajo clientes y los servidores con un número de clientes relativamente pequeño no sincronizan con los servidores primarios. Existen alrededor de 100 servidores secundarios públicos sincronizados al servidor principal, que brinda sincronización a más de 100.000 clientes y servidores en Internet. Las listas actuales se mantienen en la página de Lista de servidores NTP públicos, que se actualiza habitualmente. También existen numerosos servidores privados primarios y secundarios que por lo general no se encuentran disponibles al público. Para las listas del servidor público NTP y la información sobre cómo utilizarlos, consulte el sitio web Servidor de Sincronización Horaria de la Universidad de Delaware.

Puesto que no hay garantía de que estos servidores públicos NTP de Internet estén disponibles, o que proporcionen la hora correcta, se aconseja fuertemente que se consideren otras opciones. Esto podría incluir el uso de los diversos dispositivos independientes del Servicio de Posicionamiento Global (GPS) conectados directamente con varios routers.

Otra solución posible es el uso de varios routers configurados como principales en el estrato 1, aunque no se recomienda.

Estrato

Cada servidor NTP se ubica en un estrado que indica a qué distancia se encuentra el servidor de una fuente externa de tiempo. Los servidores Stratum 1 tienen acceso a algún tipo de fuente temporal externa, por ejemplo, un reloj de radio. Los servidores del nivel 2 obtienen detalles de tiempo de un conjunto designado de servidores del nivel 1, mientras que los servidores del nivel 3 obtienen detalles de tiempo de los servidores del nivel 2 y así sucesivamente.

Relación Peer del Servidor

- Un servidor es aquel que responde a los pedidos de cliente, pero no intenta incorporar ninguna información de la fecha de una fuente del tiempo de cliente.
- Un peer es aquel que responde a los pedidos de cliente, pero intenta utilizar los pedidos de cliente como potencial candidato para una mejor fuente horaria y ayudarlos en la estabilización de su frecuencia del reloj.
- Para ser un peer verdadero, ambos lados de la conexión deben ingresar en una relación peer en lugar que un usuario sea el peer y el otro el servidor. También se recomienda que los peers intercambien las claves de modo que solamente los host confiables se comuniquen

como peers.
- En un pedido de cliente a un servidor, el servidor contesta al cliente y olvida que el cliente alguna vez hizo una pregunta; en un pedido de cliente a un peer, el servidor contesta al cliente y guarda la información del estado sobre el cliente para hacer un seguimiento de sus funciones horarias y determinar qué estrato de servidor está ejecutando.**Nota:** CatOS puede actuar solamente como cliente NTP.

Un servidor NTP no tiene problema en manejar muchos miles de clientes. Sin embargo, la administración de centenares de peers tiene un impacto en la memoria, y el mantenimiento del estado consume más recursos de la CPU en el equipo y el ancho de banda.

Sondeo

El protocolo NTP permite a un cliente realizar una consulta a un servidor cuando lo desee. De hecho, cuando el NTP primero se configura en un dispositivo de Cisco, envía ocho consultas en la sucesión rápida en intervalos NTP_MINPOLL (24 = 16 segundos). NTP_MAXPOLL equivale a 214 segundos (que son 16.384 segundos o 4 horas, 33 minutos, 4 segundos), el tiempo máximo que lleva antes de que el NTP sondee otra vez para una respuesta. Actualmente, Cisco no tiene un método manual para forzar el tiempo de SONDEO de manera que pueda ser establecido por el usuario.

El contador de la interrogación NTP comienza en 2^6 (64) segundos y es incrementado por los poderes de dos (como los servidores sincronizan dos con uno a), a 2^{10}. Es decir, usted puede esperar que los mensajes de sincronización sean enviados en un intervalo de los segundos de 64, 128, 256, 512, o 1024 por el servidor configurado o el par. El tiempo varía entre 64 segundos y 1024 segundos como una potencia de dos basada en el loop con bloqueo de fase que envía y recibe paquetes. Si hay demasiada fluctuación en el tiempo, sondea más a menudo. Si el reloj de referencia es exacto y la conectividad de red constante, debería ver que los tiempos de sondeo convergen en 1024 segundos entre cada sondeo.

En el mundo real, esto significa que el intervalo de consulta NTP cambia a medida que cambia la conexión entre el cliente y el servidor. Cuanto mejor es la conexión, más largo será el intervalo de sondeo, lo que implica que el cliente NTP ha recibido ocho respuestas para sus ocho peticiones más recientes (lo que lleva a duplicar el intervalo de sondeo). Una sola respuesta omitida causará que el intervalo de sondeo se divida en dos. El intervalo de sondeo comienza en 64 segundos y llega a un máximo de 1024 segundos. En las mejores circunstancias, se requieren más de dos horas para que el intervalo de sondeo vaya pase de 64 segundos a 1024 segundos.

Difusiones

Las broadcasts NTP nunca se reenvían. **El comando ntp broadcast** hace que router origine broadcasts NTP en la interfaz en la que se configura. El comando broadcastclient NTP hace que el router o el switch escuchen las broadcasts NTP en la interfaz en la que se configuran.

Niveles de Tráfico de NTP

El ancho de banda utilizado por NTP es mínimo, ya que el intervalo entre los mensajes de consulta intercambiados por los pares normalmente se remonta a no más de un mensaje cada 17 minutos (1024 segundos). Con una planificación apropiada, esto se puede mantener dentro de redes de router en los links WAN. Los clientes de NTP deberían formar peers con los servidores locales de NTP y no en todo el transcurso de WAN a los routers principales de sitio central, que

son los servidores del estrato 2.

Un cliente NTP que haya convergido utiliza aproximadamente 0,6 bits por segundo por cada servidor.

Recomendación

Muchos clientes tienen hoy NTP configurado en modo cliente en sus plataformas CatOS, sincronizadas a partir de varias entradas confiables de Internet o de un reloj de radio. Sin embargo, una alternativa más simple para el modo de servidor cuando opera una gran cantidad de switches es habilitar NTP en el modo de cliente de difusión en la VLAN de administración en un dominio conmutado. Este mecanismo permite que un dominio de Catalysts entero reciba un reloj de un mensaje de broadcast único. Sin embargo, la precisión en el mantenimiento de la hora se ve reducida marginalmente debido a que el flujo de la información es en una dirección únicamente.

El uso de direcciones de loopback como fuente de actualizaciones también puede ayudar con la consistencia. Los problemas de seguridad se pueden abordar de estas dos maneras:

- Actualizaciones del servidor de filtrado
- Autenticación

La correlación de eventos es extremadamente valiosa en dos casos: troubleshooting y auditorías de seguridad. En cualquier caso, se debe actuar con precaución para proteger las fuentes y datos de tiempo y se recomienda el cifrado para que no se borren eventos esenciales ya sea intencionalmente o no.

Cisco recomienda estas configuraciones:

Configuración de Catalyst

```
set ntp broadcastclient enable
set ntp authentication enable
set ntp key key
!--- This is a Message Digest 5 (MD5) hash. set ntp
timezone <zone name>
set ntp summertime <date change details>
```

Configuración Alternativa de Catalyst

```
!--- This more traditional configuration creates !---
more configuration work and NTP peerings. set ntp client
enable
set ntp server IP address of time server set timezone
zone name set summertime date change details
```

Configuración del router

```
!--- This is a sample router configuration to distribute
!--- NTP broadcast information to the Catalyst broadcast
clients. ntp source loopback0
ntp server IP address of time server ntp update-calendar
clock timezone zone name clock summer-time date change
details ntp authentication key key ntp access-group
access-list
!--- To filter updates to allow only trusted sources of
NTP information. Interface to campus/management VLAN
```

```
containing switch sc0 ntp broadcast
```

Cisco Discovery Protocol

CDP intercambia información entre los dispositivos adyacentes sobre la capa del link de datos y es extremadamente útil en la determinación de la topología de red y de la configuración física fuera de la capa IP o lógica. Los dispositivos admitidos son principalmente switches, routers y teléfonos IP. Esta sección destaca algunas de las mejoras de la versión 2 de CDP en comparación con la versión 1.

Información Operativa General

El CDP utiliza la encapsulación SNAP con el código de tipo 2000. En los Ethernet, se utiliza el ATM, y el FDDI, la dirección multicast de destino **01-00-0c-cc-cc-cc, el tipo de protocolo HDLC 0x2000**. En Token Rings, se utiliza la dirección funcional c000.0800.0000. Las tramas CDP se envían periódicamente cada minuto de manera predeterminada.

Los mensajes CDP contienen uno o más el submensajes que permiten que los dispositivos de destino recopilen y guarden la información sobre cada dispositivo vecino.

La versión de CDP 1 soporta estos parámetros:

Parámetro	Tipo	Descripción
1	Id. del dispositivo	Nombre del dispositivo o número serial del hardware en ASCII.
2	Dirección	La dirección L3 de la interfaz que ha enviado la actualización.
3	ID del puerto	El puerto en el que se ha enviado la actualización de CDP.
4	Capacidades	Describe las capacidades funcionales del dispositivo: Router: Bridge TB 0x01: Bridge SR 0x02: Switch 0x04: Host 0x08 (Proporciona switching L2 y L3): Filtrado condicional 0x10 IGMP : 0x20 El puente o switch no reenvía los paquetes de reporte IGMP en los puertos que no son de un router. Repetidor: 0x40
5	Versión	Una cadena de caracteres que contiene la versión de software (como en **show version**).
6	Plataforma	Plataforma de hardware, tal como WS-C5000, WS-C6009, o Cisco RSP.

En la versión de CDP 2, se han introducido los campos adicionales del protocolo. La versión de CDP 2 soporta cualquier campo, pero los que están enumerados pueden ser particularmente útiles en los entornos conmutados y se utilizan en CatOS.

Nota: Cuando un switch ejecuta el CDPv1, descarta las tramas v2. Cuando un switch que ejecuta CDPv2 recibe una trama del CDPv1 en una interfaz, comienza a enviar las tramas del CDPv1 fuera de esa interfaz además de las tramas del CDPv2.

Parámetro	Tipo	Descripción
9	Dominio de VTP	El dominio VTP, si está configurado en el dispositivo.
10	VLAN nativa	En el dot1q, esta es la VLAN sin etiquetar.
11	Dúplex Medio/Total	Este campo contiene la configuración dúplex del puerto de envío.

Recomendación

El CDP se habilita de forma predeterminada y es esencial obtener la visibilidad de dispositivo adyacente y para solucionar problemas. También es utilizado por las aplicaciones de administración de red para construir correlaciones de topología L2. Ejecute estos comandos para configurar el CDP:

```
set cdp enable
!--- This is the default. set cdp version v2
!--- This is the default.
```

En las partes de la red donde se requiere un alto nivel de seguridad (por ejemplo, en las DMZ orientadas a Internet), el CDP se debe apagar como tal:

```
set cdp disable port range
```

El comando show cdp neighbors visualiza la tabla CDP local. Las entradas marcadas con un asterisco (*) indican una discrepancia de VLAN; las entradas marcadas con # indican una discordancia dúplex. Esto puede ser una ayuda valiosa para solucionar problemas.

```
>show cdp neighbors

* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port  Device-ID          Port-ID Platform
----- ------------------ ------- ------------
 3/1  TBA04060103(swi-2) 3/1     WS-C6506
 3/8  TBA03300081(swi-3) 1/1     WS-C6506
15/1  rtr-1-msfc         VLAN 1  cisco    Cat6k-MSFC
16/1  MSFC1b             Vlan2   cisco    Cat6k-MSFC
```

Otras Opciones

Algunos switches, como Catalyst 6500/6000, tienen la capacidad de suministrar energía por medio de cables UTP a los teléfonos IP. La información recibida por el CDP es de utilidad para la administración de energía en el switch.

Mientras que los teléfonos IP pueden tener un equipo conectado a ellos, y ambos dispositivos se conectan con el mismo puerto en el Catalyst, el switch tiene la capacidad de colocar el teléfono VoIP en una VLAN distinta, la auxiliar. Esto permite que el switch aplique fácilmente una Calidad de Servicio (QoS) diferente para el tráfico de VoIP.

Además, si se modifica la VLAN auxiliar (por ejemplo, para forzar al teléfono para que utilice una VLAN específica o un método de etiquetado específico), esta información se envía al teléfono por medio del CDP.

Parámetro	Tipo	Descripción
14	ID del aparato	Permite que el tráfico de VoIP sea distinguido de otro tráfico, por ejemplo, por una Id. de VLAN separada (VLAN auxiliar).
16	Consumo de Energía	La cantidad de energía que un teléfono VoIP consume, en milivatios.

Nota: Los Catalyst 2900 y 3500XL Switches no soportan actualmente el CDPv2.

Configuración de Seguridad

Idealmente, el cliente ya ha establecido una política de seguridad para ayudar a definir qué herramientas y tecnologías de Cisco se califican.

Nota: La seguridad del Cisco IOS Software, en comparación con CatOS, se analiza en varios documentos, tales como Cisco ISP Essentials.

Funciones de Seguridad Básicas

Contraseñas

Configurar una contraseña del nivel del usuario (login). Las contraseñas distinguen entre mayúsculas y minúsculas en CatOS 5.x y posterior, y pueden tener de 0 a 30 caracteres de longitud, incluidos los espacios. Establezca la contraseña de habilitación:

```
set password password set enablepass password
```

Todas las contraseñas deben cumplir los estándares de longitud mínima (por ejemplo, seis caracteres como mínimo, una combinación de letras y números, letras mayúsculas y minúsculas) para las contraseñas de login y de habilitación. Estas contraseñas se cifran usando el algoritmo de hash MD5.

Para tener tener más flexibilidad en el manejo de la seguridad de la contraseña y del acceso del dispositivo, Cisco recomienda el uso de un servidor TACACS+. Consulte la sección TACACS+ de este documento para más información.

Secure Shell

Use el cifrado SSH para proporcionar seguridad para las sesiones Telnet y otras conexiones remotas al switch. El cifrado SSH es admitido para los registros remotos al switch solamente. No puede cifrar las sesiones telnet que se inician a partir del switch. El SSH versión 1 es admitido en

CatOS 6.1, y el soporte de la versión 2 fue agregado en CatOS 8.3. El SSH versión 1 soporta los métodos de cifrado de la Norma de Cifrado de Datos (DES) y del DES triple (3-DES), y el SSH versión 2 soporta el 3-DES y los métodos de cifrado del Norma de Cifrado Avanzado (AES). Puede utilizar el cifrado SSH con RADIUS y autenticación de TACACS+. Esta función es admitida con las imágenes SSH (k9). Consulte Cómo configurar el SSH en los switches Catalyst que Ejecutan CatOS para conocer detalles.

set crypto key rsa 1024

Para inhabilitar el repliegue de la versión 1 y aceptar las conexiones de la versión 2, ejecute este comando:

set ssh mode v2

Filtros de Permiso de IP

Estos son filtros para proteger el acceso a la interfaz sc0 de administración a través de Telnet y otros protocolos. Estos son especialmente importantes cuando la VLAN que se utilizó para la administración también contiene usuarios. Ejecute estos comandos para habilitar la dirección IP y el filtrado del puerto:

set ip permit enable
set ip permit *IP address mask Telnet|ssh|snmp|all*

Sin embargo, si el acceso a Telnet se restringe con este comando, el acceso a los dispositivos CatOS se puede alcanzar solamente a través de algunas estaciones extremas confiables. Esta configuración puede ser un obstáculo en el troubleshooting. Tenga en cuenta que es posible imitar direcciones IP y burlar los accesos filtrados, por lo que esta es solo la primera capa de protección.

Seguridad de Puertos

Considere utilizar la seguridad de puerto para permitir que solamente una o varias direcciones MAC conocidas pasen los datos en un puerto determinado (para impedir que las estaciones terminales estáticas sean reemplazadas por estaciones nuevas que no posean control de cambios, por ejemplo). Esto es posible por con las direcciones MAC estáticas.

set port security *mod/port* **enable** *MAC address*

También es posible si se aprenden las direcciones MAC restringidas dinámicamente.

set port security *port range* **enable**

Estas opciones pueden ser configuradas:

- set port *security mod/port age time value*: especifica el tiempo durante el cual las direcciones en el puerto se resguardan antes de poder aprender direcciones nuevas. El tiempo válido en minutos es de 10 a 1440. El valor predeterminado es ningún envejecimiento.
- set port securitymod*/port maximum value*: palabra clave que especifica el número máximo de direcciones MAC para resguardar el puerto. Los valores válidos son 1 (predeterminado) - 1025.
- *set port security mod/port violation* shutdown : cierra el puerto (es el valor predeterminado) si

ocurre una infracción además de enviar un mensaje syslog (es la opción predeterminada) y desecha el tráfico.
- set port *security mod/port* shutdown *time value* : período de tiempo durante el cual ewl puerto permanece inhabilitado. Los valores válidos son 10 - 1440 minutos. El valor predeterminado es dejar el puerto inhabilitado de forma permanente.

Con CatOS 6.x y posterior, Cisco ha introducido la autentificación 802.1x que permite que los clientes autentiquen un servidor central antes de que los puertos se puedan habilitar para los datos. Esta función se encuentra en las primeras fases de soporte en las plataformas tales como Windows XP, pero se puede considerar una dirección estratégica por muchas empresas. Consulte Configuración de Seguridad del Puerto para obtener información sobre cómo configurar la seguridad del puerto en los switches que ejecutan el Cisco IOS Software.

Banners de Login

Cree anuncios de dispositivos apropiados para indicar específicamente las acciones del acceso no autorizado. No publique el nombre del sitio o datos de la red que les puedan proporcionar información a usuarios no autorizados. Estos banners proporcionan recursos en caso que la seguridad de un dispositivo se vea comprometida y se atrape al infractor.

```
# set banner motd ^C
*** Unauthorized Access Prohibited ***
***  All transactions are logged   ***
------------- Notice Board -------------
----Contact Joe Cisco at 1 800 go cisco for access problems----
^C
```

Seguridad Física

Los dispositivos no deben ser accesibles físicamente sin la autorización apropiada, así que el equipo debe estar en un espacio controlado (bloqueado). para garantizar que la red siga funcionando y no sea afectado por una mala manipulación o por factores ambientales, asegúrese de que todos los equipos tengan el USP adecuado (con fuentes redundantes de ser posible) y controles de temperatura (aire acondicionado). Recuerde, si el acceso físico es violado por una persona con intención maliciosa, la interrupción con la recuperación de contraseña u otros métodos es mucho más probable.

Terminal Access Controller Access Control System

De forma predeterminada, las contraseñas de modo con y sin privilegios son globales y aplicarse a cada usuario que accede al switch o al router, del puerto de la consola o a través de una sesión Telnet en la red. Su implementación en los dispositivos de red demanda mucho tiempo y no está centralizada. También es difícil implementar restricciones sobre el acceso mediante listas de acceso que pueden ser propensas a errores de configuración.

Existen tres sistemas de seguridad disponibles para ayudar a controlar y a regular el acceso a los dispositivos de red. Estos utilizan arquitecturas cliente/servidor para colocar toda la información sobre seguridad en una sola base de datos central. Estos tres sistemas de seguridad son los siguientes:

- TACACS+
- RADIUS
- Kerberos

TACACS+ es una implementación común en las redes de Cisco y es el aspecto central de este capítulo. Proporciona las siguientes características:

- Autentificación: la identificación y el proceso de verificación para un usuario. Se pueden utilizar varios métodos para autenticar un usuario, pero el más habitual incluye una combinación de nombre de usuario y contraseña.
- La autorización de los diversos comandos puede ser concedida una vez que el usuario es autenticado.
- Contabilización: el registro de lo que hace un usuario o ha hecho en el dispositivo.

Consulte Configuración de TACACS+, RADIUS, y Kerberos en los Switches de Cisco Catalyst para más detalles.

Información Operativa General

El protocolo TACACS+ reenvía nombres de usuario y contraseñas al servidor centralizado, cifrados en la red mediante el troceo unidireccional MD5 (RFC 1321). Utiliza el puerto TCP 49 como su protocolo de transporte; esto ofrece las siguientes ventajas sobre el UDP (usado por RADIUS):

- Transporte orientado a la conexión
- Reconocimiento separado de que se ha recibido una solicitud (TCP ACK), independientemente de la carga que soporte actualmente el mecanismo de autenticación del backend
- Indicación inmediata de un crash del servidor (paquetes RST)

Durante una sesión, si se necesita verificación adicional de la autorización, el switch verifica con TACACS+ para determinar si el usuario tiene permiso para usar un comando determinado. Esto brinda un mayor control sobre los comandos que pueden ejecutarse en el switch mientras se desconecta del mecanismo de autenticación. Con las estadísticas del comando, es posible revisar los comandos que un usuario específico ha ejecutado mientras se asociaba a un dispositivo de red determinado.

Cuando un usuario intenta un login ASCII simple al autenticar un dispositivo de red con el TACACS+, este proceso ocurre habitualmente:

- Cuando se establece la conexión, el switch entra en contacto con el daemon de TACACS+ para obtener una indicación de nombre de usuario, que luego se muestra al 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 la indicación de contraseña al usuario, que luego ingresa una contraseña que también se envía al daemon de TACACS+.
- El dispositivo de red recibe finalmente una de estas respuestas del daemon de TACACS+:ACCEPT: el usuario es autenticado y el servicio puede comenzar. Si el dispositivo de red se configura para requerir la autorización, la autorización comienza en este momento.REJECT: el usuario no pudo realizar la autenticación. Se le puede impedir el acceso adicional al usuario o se le solicita que vuelva a intentar la secuencia de inicio de sesión en función del daemon de TACACS+.ERROR: se produjo un error en algún momento durante la autenticación. Este puede existir en el daemon o en la conexión de red entre el daemon y el switch. Si se recibe una respuesta de ERROR, el dispositivo de red generalmente intenta utilizar un método alternativo para autenticar al usuario.CONTINUE: se

solicita al usuario información de autenticación adicional.
- Los usuarios deben primero completar con éxito la autenticación de TACACS+ antes de pasar a la autorización de TACACS+.
- Si se pide autenticación TACACS+, el daemon de TACACS+ se contacta nuevamente y devuelve una respuesta de autorización ACCEPT o REJECT. Si se devuelve la respuesta ACCEPT, la respuesta contiene los datos en la forma de atributos que se utilizan para dirigir la sesión EXEC o NETWORK para ese usuario, y determina los comandos a los que el usuario puede acceder.

Recomendación

Cisco recomienda el uso del TACACS+, ya que puede ser implementado fácilmente usando el CiscoSecure ACS para NT, Unix, u otro software de terceros. Las funciones TACACS+ incluyen una contabilidad detallada para proporcionar estadísticas sobre el uso de comandos y el uso de sistemas, el algoritmo de cifrado MD5, y el control administrativo de los procesos de autenticación y autorización.

En este ejemplo, los modos login y enable (inicio de sesión y activación) utilizan el servidor TACACS+ para autenticación y pueden replegarse para autenticación local si el servidor no está disponible. Esta solución es un recurso importante que se debe prever en la mayoría de las redes. Ejecute estos comandos para configurar el TACACS+:

```
set tacacs server server IP primary set tacacs server server IP
!--- Redundant servers are possible. set tacacs attempts 3
!--- This is the default. set tacacs key key
!--- MD5 encryption key. set tacacs timeout 15
!--- Longer server timeout (5 is default). set authentication login tacacs enable
set authentication enable tacacs enable
set authentication login local enable
set authentication enable local enable
!--- The last two commands are the default; they allow fallback !--- to local if no TACACS+
server available.
```

Otras Opciones

Es posible utilizar autorización de TACACS+ para controlar los comandos que puede ejecutar cada usuario o grupo de usuarios en el switch, pero es difícil hacer una recomendación porque todos los clientes tienen requisitos individuales en esta área. ConsulteControl de Acceso al Switch con Autenticación, Autorización y Contabilización para más información.

Por último, los comandos de contabilidad proporcionan una pista de auditoría de lo que cada usuario ha escrito y configurado. El siguiente es un ejemplo que se utiliza en el procedimiento recomendado de recibir la información de auditoría al final del comando:

```
set accounting connect enable start-stop tacacs+
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
set accounting commands enable all start-stop tacacs+
set accounting update periodic 1
```

Esta configuración tiene las siguientes funciones:

- El comando connect permite la contabilización de los eventos de conexión de salida en el

switch, como Telnet.
- El comando exec habilita la contabilidad de las sesiones de inicio en el switch como, por ejemplo, el personal de operaciones.
- **El comando system** habilita la contabilización de eventos del sistema en el switch tal como recarga o restablecimiento.
- El comando commands permite contabilizar lo que se ingresó en el switch, tanto para los comandos show como los comandos configuration.
- Las actualizaciones periódicas cada minuto al servidor son útiles para registrar si las sesiones de los usuarios continúan activas.

Configuración de Lista de Verificación

Esta sección proporciona un resumen de las configuraciones recomendadas, excepto los detalles de seguridad.

Es extremadamente útil etiquetar todos los puertos. Ejecute este comando para etiquetar los puertos:

`set port description` *`descriptive name`*

Use este clave conjuntamente con las tablas de Comando enumeradas:

Clave:
Texto en negrita: cambio recomendado
Texto normal: valor predeterminado, configuración recomendada

Comandos Global Configuration

Comando	Comentario
set vtp domain name passwordx	Proteja contra las actualizaciones del VTP no autorizadas provenientes de switches nuevos.
set vtp mode transparent	Seleccione el modo de VTP recomendado en este documento. Consulte la sección VLAN Trunking Protocol de este documento para más detalles.
set spantree enable all	Asegúrese de que el STP esté habilitado en todas las VLAN.
set spantree root vlan	Recomendado para situar los bridges root (y root secundario) de cada VLAN.
set spantree backbonefast enable	habilite la convergencia de STP rápida de las fallas indirectas (solamente si todos los switches en el dominio soportan la función).

set spantree uplinkfast enable	Habilite la convergencia de STP rápida de las fallas directas (para los switches de capa de acceso solamente).
set spantree portfast bpdu-guard enable	Habilite el puerto que se apagará automáticamente si hay una extensión desautorizada del Spanning Tree.
set udld enable	Habilite la detección de link unidireccional (también requiere que se configure el nivel de puerto).
set test diaglevel complete	Habilite el diagnóstico completo en el arranque (valor predeterminado en Catalyst 4500/4000).
set test packetbuffer sun 3:30	Habilite la verificación de errores de buffer (se aplica a Catalyst 5500/5000 solamente).
set logging buffer 500	Permite mantener el buffer de syslog interno máximo.
set logging server *IP address*	Permite configurar el servidor de syslog objetivo para el registro de mensajes de sistema.
set logging server enable	Soporta al servidor de registro externo.
set logging timestamp enable	Habilita el fechado de los mensajes en el registro.
set logging level spantree 6 default	Incremente el nivel predeterminado de syslog STP.
set logging level sys 6 default	Incremente el nivel predeterminado de registro de sistema.
set logging server severity 4	Permite la exportación del syslog de mayor nivel de gravedad solamente.
set logging console disable	Inhabilite la consola a menos que esté solucionando problemas.
set snmp community read-only string	Configure la contraseña para permitir la recolección remota de datos.
set snmp community read-write string	Configure la contraseña para permitir la configuración remota.
set snmp community read-write-all string	Configurar la contraseña para permitir la configuración remota, incluidas las contraseñas.
set snmp trap enable all	Habilite las trampas SNMP al servidor NMS para las alertas de eventos y fallas.

set snmp trap server address string	Configure la dirección del receptor de trampas NMS.
set snmp rmon enable	Habilite el RMON para la recolección estadística local. Consulte la sección Supervisión Remota de este documento para más detalles.
set ntp broadcastclient enable	Habilite la recepción de un reloj de sistema preciso de un router de flujo ascendente.
set ntp timezone zone name	Permite configurar la hora local para el dispositivo.
set ntp summertime date change details	Selecciona el horario de verano, si lo hay en la zona horaria.
set ntp authentication enable	Permite configurar la información de tiempo cifrada por motivos de seguridad.
set ntp key key	Permite configurar la clave de cifrado.
set cdp enable	Permite asegurarse de que el descubrimiento de vecinos está activado (la opción predeterminada es que también esté activado en los puertos).
set tacacs server IP address primary	Permite configurar la dirección del servidor de AAA.
set tacacs server IP address	Servidores de AAA redundantes si es posible.
set tacacs attempts 3	Permite 3 intentos para escribir la contraseña para la cuenta de usuario AAA.
set tacacs key key	Permite configurar la clave de cifrado MD5 del AAA.
set tacacs timeout 15	Permite un tiempo de espera del servidor más prolongado (cinco segundos es el valor predeterminado).
set authentication login tacacs enable	Permite usar el AAA para la autenticación para el login.
set authentication enable tacacs enable	Permite usar el AAA para la autenticación para el modo de habilitación.
set authentication login local enable	Valor por defecto; permite recurrir al sistema local si no hay ningún servidor AAA disponible.
set authentication enable local enable	Valor por defecto; permite recurrir al sistema local si no hay ningún servidor AAA disponible.

Comandos de Configuración de los Puertos de Host

Comando	Comentario
set port host port *range*	Permite cancelar el procesamiento innecesario del puerto. Esta macro activa PortFast en el spantree, y desactiva la canalización y los trunks.
set udld disable port range	Permite cancelar el procesamiento innecesario de los puertos (esta opción está desactivada de manera predeterminada en los puertos de cobre).
set port speed port range auto	Permite utilizar la negociación automática con los controladores de NIC host actualizados.
set port trap port range disable	Cancela el uso de trampas SNMP en las sesiones de los usuarios generales; solo el seguimiento de los puertos claves se mantiene activo.

Comandos de la Configuración del Servidor

Comando	Comentario
set port host port *range*	Permite cancelar el procesamiento innecesario del puerto. Esta macro activa PortFast en el spantree, y desactiva la canalización y los trunks.
set udld disable port range	Permite cancelar el procesamiento innecesario de los puertos (esta opción está desactivada de manera predeterminada en los puertos de cobre).
set port speed *port range 10* | *100*	Normalmente se utiliza para configurar los puertos estáticos o de servidor; o para la negociación automática.
set port duplex *port range full* | *semi*	Normalmente se utiliza para configurar los puertos estáticos o de servidor; o para la negociación automática.
set port trap port range enable	Establece que los puertos de servicios claves deben enviar una trampa al NMS.

Comandos de Configuración de los Puertos sin Utilizar

Comando	Comentario
set spantree portfast port range disable	Permite habilitar el procesamiento necesario del puerto y la protección del STP.
set port disable port range	Inhabilita los puertos sin utilizar.
set vlan unused dummy vlan port range	Permite dirigir el tráfico no autorizado a una VLAN no utilizada si el puerto está habilitado.
set trunk port range off	Permite inhabilitar el trunking en el puerto hasta su administración.
set port channel port range mode off	Permite deshabilitar la canalización en el puerto hasta su administración.

Puertos de Infraestructura (switch-switch, switch-router)

Comando	Comentario
set udld enable port range	Permite la activación de la detección de links unidireccionales (esta no es la opción predeterminada en los puertos de cobre).
set udld aggressive-mode enable port range	Permite habilitar el modo agresivo (en los dispositivos que lo soportan).
set port negotiation *port rangeenable*	Permite que se active la negociación automática predeterminada de GE para los parámetros de link.
set port trap port range enable	Permite habilitar las trampas SNMP para estos puertos claves.
set trunk port range off	Permite deshabilitar la función si no se usan los trunks.
**set trunk mod/port desirable *ISL*	*dot1q*	*negociar***	Si usa trunks, se prefiere el dot1q.
clear trunk mod/port *vlan range*	Permite limitar el diámetro del STP mediante el recorte de las VLAN en los trunks en los que no se les necesita.
set port channel port	Permite deshabilitar la función si no se usa la canalización.

range mode off	
set port channel port range mode desirable	Si usa los canales, esto habilita el PAgP.
set port channel all distribution ip both	Si usa las opciones de canalización, permite el balanceo de carga en la L3 de destino u origen (valor predeterminado en Catalyst 6500/6000).
set trunk mod/*port* nonegotiate *ISL* | *dot1q*	Permite deshabilitar los trunking del DTP con el router en los módulos Catalyst 2900XL, 3500 o terceros.
set port negotiation mod/port disable	Es posible que la negociación no sea compatible con algunos dispositivos GE.

Información Relacionada

- Mensajes de Error Comunes de CatOS en los Catalyst 4500/4000 Series Switches
- Mensajes de Error Comunes de CatOS en Catalyst 5000/5500 Series Switches
- Mensajes de Error Comunes de CatOS en los Catalyst 6500/6000 Series Switches
- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems